Algèbre

Cours de 1ère année à l'École Normale Supérieure 2023/2024

Gaëtan Chenevier

gaetan.chenevier@math.cnrs.fr

Version du 26 août 2024

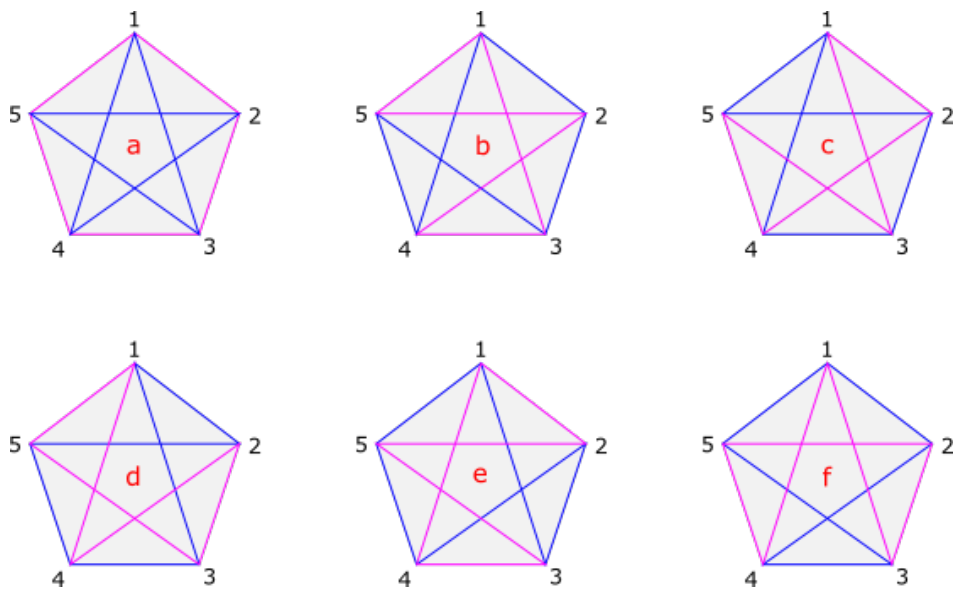


Figure 1. L'action exotique de S_5 sur 6 éléments

Table des matières

Introduction 1

Chapitre 1. Ensembles quotients 3
1. Partitions et relations d'équivalence 3
2. Passage au quotient 6
3. Sections et systèmes de représentants 7
4. Complément : Le lemme de Zorn et le théorème de Zermelo 8
5. Exercices 12

Chapitre 2. Généralités sur les groupes 17
1. Exemples de groupes 17
2. Isomorphismes et morphismes 22
3. Groupes cycliques et monogènes 27
4. Le théorème de Lagrange 30
5. Sous-groupes finis de $k^\times$ et $(\mathbb{Z}/n\mathbb{Z})^\times$ 32
6. Groupes quotients 35
7. Complément I : Groupes additifs et multiplicatif usuels 39
8. Complément II : Groupes libres 42
9. Exercices 47

Chapitre 3. Groupes abéliens de type fini 57
1. Caractères et $y^2 = x^3 + 1$ sur $\mathbb{Z}/p\mathbb{Z}$ 57
2. Décomposition de Fourier finie 64
3. Structure des groupes abéliens finis 67
4. Groupes abéliens de type fini 71
5. Complément I : Déterminant d'un groupe abélien fini 73
6. Compléments II : Réseaux et sous-groupes fermés de $\mathbb{R}^n$ 74
7. Courbes elliptiques (culturel) 76
8. Exercices 78

Chapitre 4. Le groupe symétrique et son dévissage 87
1. Actions de groupes 87
2. Groupes symétrique et alterné 92
3. Les cas $n \leqslant 5$ 97
4. Le langage des suites exactes 100
5. Le dévissage de S_n 101
6. Commutateurs et groupes dérivés 103
7. Le dévissage en produit semi-direct 106
8. Complément I : Filtrations et le théorème de Jordan-Hölder 111
9. Complément II : Groupe de Galois d'un polynôme (culturel) 113
10. Complément III : Le groupe affine et un théorème de Galois 114
11. Exercices 118

Chapitre 5. Groupes et symétries 127
1. Sous-groupes finis de O(2) et SO(3) 128
2. Le groupe Sp(1) et géométrie euclidienne en dimensions 3 et 4 138
3. Groupes linéaires et simplicité de $\mathrm{PSL}_n(k)$ 145
4. Le groupe $\mathrm{PGL}_2(k)$ et quelques (iso)morphismes miraculeux 151
5. Complément I : Polytopes réguliers (culturel) 154
6. Complément II : Frises et papiers peints (culturel) 158
7. Complément III : Groupes unitaires et un théorème de Jordan 161
8. Exercices 169

Chapitre 6. Éléments de structure des groupes finis 179
1. p-groupes 180
2. Les théorèmes de Sylow 182
3. Le théorème de Schur-Zassenhaus 184
4. Les théorèmes de P. Hall 185
5. Extensions et cohomologie 187
6. Complément I : Groupes nilpotents finis 193
7. Complément II : La caractérisation de Burnside-Dickson-Pazderski 195
8. Complément III : Générateurs et automorphismes d'un p-groupe 198
9. Exercices 200

Chapitre 7. Arithmétique des anneaux 209
1. Les anneaux $\mathbb{Z}[\sqrt{d}]$ 210
2. Vocabulaire de la divisibilité 212
3. Anneaux factoriels 213
4. Idéaux 215
5. Anneaux principaux 217
6. Anneaux euclidiens et exemples 217
7. L'anneau $\mathbb{Z}[i]$ et sommes de deux carrés 219
8. Une équation diophantienne 220
9. Complément I : Anneaux quotients 222
10. Complément II : Quaternions entiers, sommes de 4 carrés et sous-groupes libres de SO(3) 227
11. Exercices 238

Chapitre 8. Modules sur les anneaux principaux 245
1. Modules sur un anneau 246
2. Classes d'équivalence de matrices sur un anneau principal 251
3. Modules de type fini sur un anneau principal 254
4. Complément I : le groupe $\mathrm{SL}_n(A)$ et transvections 257
5. Complément II : deux démonstrations de l'assertion d'unicité 261
6. Exercices 264

Chapitre 9. Représentations linéaires des groupes finis 269
1. Représentations linéaires 270
2. Le point de vue $k[G]$-modules 271
3. Décomposition en irréductibles 273
4. Théorie des caractères 277
5. La table des caractères et exemples 283
6. Propriétés d'intégralité des caractères 291

7. Retour sur le déterminant d'un groupe fini 294
8. Décomposition à la Fourier de $\mathrm{L}^2(G)$ 297
9. Des théorèmes de Burnside et P. Hall 299
10. Exercices 303

Annexe A. Corrections des exercices 309
Exercices du chapitre 1 309
Exercices du chapitre 2 313
Exercices du chapitre 3 322
Exercices du chapitre 4 332
Exercices du chapitre 5 347
Exercices du chapitre 6 356
Exercices du chapitre 7 368

Annexe B. Sujets d'examens et corrigés 375
1. Examen partiel 2021-2022 375
2. Examen partiel 2022-2023 377
3. Examen partiel 2023-2024 379
4. Examen 2021-2022 382
5. Examen 2022-2023 385
6. Examen 2023-2014 387
7. Corrigé du partiel 2021-2022 390
8. Corrigé du partiel 2022-2023 393
9. Corrigé du partiel 2023-2024 397
10. Corrigé de l'examen 2021-2022 402
11. Corrigé de l'examen 2022-2023 407
12. Corrigé de l'examen 2023-2024 411

Annexe. Bibliographie 417

Introduction

Ce cours d'algèbre est une introduction à la théorie des groupes, et dans une moindre mesure, aux modules.

Les groupes sont nés avec les travaux de Lagrange et de Galois sur la résolubilité par radicaux des équations polynomiales à une variable (groupes de permutations). Ils apparaissent également en filigrane, et jouent un rôle important, dans les recherches arithmétiques de Gauss (arithmétique modulaire, groupes de classes de formes quadratiques).

La notion abstraite de groupe, dégagée par Cayley et Cauchy, et formalisée sous sa forme actuelle par Von Dyck, est remarquable par le peu d'axiomes qu'elle nécessite et la richesse de ses applications dans les mathématiques et les autres sciences. Elle intervient par exemple dans les fondements de l'algèbre linéaire, dans l'étude des symétries des structures géométriques ou algébriques, en cristallographie, ou dans diverses généralisations de l'analyse de Fourier (théorie des « représentations »), sans compter que de nombreux invariants construits en mathématiques sont des groupes, par exemple en topologie (groupes d'homotopie, ou d'homologie). La classification des groupes simples finis, annoncée par Gorenstein en 1983 mais dont certains aspects n'ont été clarifiés qu'au début des années 2000,[1] est l'un des résultats les plus marquants des mathématiques. La théorie des groupes continue de faire l'objet de nombreuses recherches sous divers déguisements : groupes de Lie, groupes algébriques, théorie géométrique des groupes, représentations, algèbres d'opérateurs...

1. Voir l'article The Status of the Classification of the Finite Simple Groups, par M. Ashbacher, Notices A.M.S. 51 (2004).

Chapitre 1

Ensembles quotients

Dans ce court chapitre préliminaire, nous rappelons quelques notions générales de théorie des ensembles. La notion de *relation d'équivalence* sur un ensemble X est l'outil qui permet en pratique d'identifier les éléments de X partageant une certaine propriété (les rendant "équivalents"). Nous rappelons comment la donnée d'une telle relation sur X définit une partition naturelle de X en *classes d'équivalence*. L'ensemble de ces classes, un sous-ensemble de l'ensemble de toutes les parties de X, est appelé *ensemble quotient* de X par R, et il est noté X/R. Sa propriété principale (dite "universelle") est qu'une application $f : X \to Y$ constante sur les classes d'équivalence de R se factorise canoniquement en une application $\overline{f} : X/R \to Y$, appelé *passage au quotient* de f. La notion de *système de représentants* de R, qui consiste à choisir un élément par classe, conduit naturellement à discuter l'*axiome du choix*, un énoncé bien intuitif mais qui a joué un rôle historiquement important dans les fondements des mathématiques (il ne jouera que peu de rôle dans ce cours). Dans un complément, nous discutons de plusieurs énoncés surprenants entrainés par (en fait équivalents à) l'axiome du choix, comme le *lemme de Zorn* ou le *théorème de Zermelo*. En particulier nous y donnerons une démonstration du Lemme de Zorn, dans laquelle nous nous approcherons, sans la définir, de la notion d'ordinal. Les exercices contiennent notamment un fascicule de résultats classiques de théorie des ensembles (dénombrabilité, cardinalité) utiles à tout mathématicien.

Quelques références : L'appendice 2 de *Algebra*, 3ème ed. (S. Lang), le premier chapitre de *Algèbres et théories galoisiennes* (R. & A. Douady).

1. Partitions et relations d'équivalence

Définition 1.1. *Soit X un ensemble. Une partition de X est la donnée d'un ensemble $\{X_i\}_{i\in I}$ de parties non vides X_i de X tel que X est la réunion disjointe des X_i, i.e. $X = \cup_{i\in I} X_i$ et $X_i \cap X_j = \varnothing$ pour $i \neq j$. On note alors simplement*

$$X = \coprod_{i\in I} X_i.$$

Par exemple, l'ensemble $X = \{1, 2, 3\}$ possède exactement 5 partitions, à savoir $\{\{1, 2, 3\}\}$, $\{\{1\}, \{2, 3\}\}$, $\{\{2\}, \{1, 3\}\}$, $\{\{3\}, \{1, 2\}\}$ et $\{\{1\}, \{2\}, \{3\}\}$.

Exemple 1.2. (*Partition en fibres*) *Soit $f : X \to Y$ une application et $y \in Y$. On appelle fibre de f en y l'ensemble*[1]

$$f^{-1}(\{y\}) = \{x \in X \mid f(x) = y\}$$

1. Le $(\{\})$ est lourd, et on la note donc parfois $f^{-1}(y)$, même si cette notation désigne aussi l'unique antécédant de y par f quand f est bijective.

des antécédants de y par f. Lorsque f est surjective, ses fibres $X_y := f^{-1}(\{y\})$, avec y parcourant X, sont non vides et forment une partition de X indexée par Y. Toutes les partitions de X s'obtiennent en fait ainsi : si l'on a $X = \coprod_{i\in I} X_i$ avec $X_i \neq \varnothing$ pour tout i, alors l'application $f : X \to I$, associant à $x \in X$ l'unique $i \in I$ vérifiant $x \in X_i$, est surjective et vérifie $f^{-1}(\{i\}) = X_i$.

Une *relation* sur un ensemble X est la donnée d'une partie R de $X \times X$. On note suggestivement « $x\,R\,y$ » pour « $(x, y) \in R$ ».

Définition 1.3. *Une relation R sur un ensemble X est une* relation d'équivalence *si elle vérifie :*

(i) $x\,R\,x$, pour tout x dans X (réflexivité),

(ii) $x\,R\,y \Rightarrow y\,R\,x$, pour tout $x, y \in X$ (symétrie), et

(iii) $x\,R\,y$ et $y\,R\,z \Rightarrow x\,R\,z$, pour tout x, y, z dans X (transitivité).

Des notations standards pour les relations d'équivalence sont $\sim$, $\simeq$ ou $\equiv$. Soient R une relation d'équivalence sur X et $x \in X$. La *classe de R-équivalence* de x est par définition $[x]_R = \{y \in X \mid y\,R\,x\}$. On la note aussi $x \bmod R$. Lorsque R est sous-entendue, on parle simplement de classe d'équivalence de x et on la note en général $[x]$ ou $\overline{x}$ au lieu de $[x]_R$. On a $x \in [x]_R$ (réflexivité) ainsi que

$$\forall\ x, y \in X,\ y \in [x]_R \implies [y]_R = [x]_R. \tag{1}$$

En effet, $z\,R\,y$ implique $z\,R\,x$ (transitivité), puis $[y]_R \subset [x]_R$. On conclut par symmétrie car $y \in [x]_R$ implique $y \in [x]_R$.

Proposition 1.4. *Si R est une relation d'équivalence sur X, ses classes d'équivalence forment une partition de X.*

Démonstration — On a $x \in [x]_R$ par (i), donc X est réunion des classes d'équivalence, et ces dernières sont non vides. On conclut car d'après (1), deux classes $[x]_R$ et $[y]_R$, avec $x, y \in X$, sont égales ou disjointes. □

Remarque 1.5. *Réciproquement, toute partition $X = \coprod_{i\in I} X_i$ est la partition en classes d'équivalence d'une unique relation d'équivalence sur X. En effet, on constate que $x\,R\,y \Leftrightarrow \exists i \in I,\ x \in X_i$ et $y \in X_i$ est une relation d'équivalence sur X (et même manifestement l'unique) dont les classes sont les X_i.*

On vérifie aisément qu'une intersection de relations d'équivalence sur X est d'équivalence. En revanche, c'est faux en général pour une réunion (pourquoi ?). Si X est un ensemble, on note $\mathrm{P}(X)$ l'ensemble des parties de X.

Définition 1.6. *Si R est une relation d'équivalence sur X, le sous-ensemble de $\mathrm{P}(X)$ constitué des classes de R-équivalence est appelé* ensemble quotient *de X par R, et il est noté X/R. L'application $\pi_R : X \to X/R$, $x \mapsto [x]_R$, est appelée* projection canonique *associée à R. C'est une surjection dont les fibres sont par définition les classes d'équivalence de R.*

Exemple 1.7. (*L'ensemble* $\mathbb{Z}/N\mathbb{Z}$) Soit $N \in \mathbb{Z}$. On définit une relation d'équivalence sur $\mathbb{Z}$ en posant $a\,R\,b \Leftrightarrow N|a-b$ (le vérifier). Depuis Gauss, on note en général $a \equiv b \bmod N$ pour $a\,R\,b$. L'ensemble $\mathbb{Z}/R$ est le familier $\mathbb{Z}/N\mathbb{Z}$ de l'arithmétique modulaire. La classe de $a \in \mathbb{Z}$ est le sous-ensemble $a + N\mathbb{Z} = \{a + Nm \mid m \in \mathbb{Z}\}$ de $\mathbb{Z}$, aussi noté $a \bmod N$ ou simplement $\overline{a}$.

Exemple 1.8. *(Décomposition en "translations" et "cycles" d'une bijection)* Soient X un ensemble et $f : X \to X$ une bijection. On pose [2]

$$x\,R\,y \Leftrightarrow \exists\, i \in \mathbb{Z}, \quad y = f^i(x).$$

C'est une relation d'équivalence sur X : on a $x = f^0(x)$, $y = f^i(x) \Leftrightarrow x = f^{-i}(y)$ et $f^i(f^j(x)) = f^{i+j}(x)$. On a en outre ici $x\,R\,f(x)$, donc f préserve les classes. Quelle est la classe de $x \in X$? Il y a deux cas, soit tous les $f^i(x)$, $i \in \mathbb{Z}$, sont distincts, auquel cas $\mathbb{Z} \to [x]$, $i \mapsto f^i(x)$ est bijective, et identifie f à la translation $i \mapsto i+1$. Soit il existe $i < j$, avec disons $d := j - i$ minimal, tel que $f^j(x) = f^i(x)$. Appliquant f^{-i} on a alors $f^d(x) = x$, puis que $a \equiv b \bmod d$ implique $f^a(x) = f^b(x)$. On en déduit

$$|[x]| = d \text{ et } [x] = \{x, f(x), f^2(x), \ldots, f^{d-1}(x)\},$$

par minimalité de d. Dans ce cas, f préserve, et permute circulairement, les d éléments de $[x]$.

L'Exemple 1.8 est en fait un cas particulier d'action de groupes, que nous introduirons plus tard (action du groupe $\mathbb{Z}$ sur X). L'Exemple 1.7 est aussi un cas particulier de l'Exemple 1.8 : considérer $X = \mathbb{Z}$ et $f : \mathbb{Z} \to \mathbb{Z}, x \mapsto x + N$. Une conséquence de l'Exemple 1.8 est la suivante :

Corollaire 1.9. *Soient X un ensemble fini et $f : X \to X$ une application telle que $f^p = \mathrm{id}_X$ avec p premier. Soit $\mathrm{Fix}\,X = \{x \in X \mid f(x) = x\}$ l'ensemble des points fixes de f. Alors on a $|X| \equiv |\mathrm{Fix}\,X| \bmod p$.*

Démonstration — On est dans la situation de l'Exemple 1.8, car f est bijective d'inverse f^{p-1}. Soient $x \in X$ et $d = |[x]|$. Montrons $d = 1$ (*i.e.* $x \in \mathrm{Fix}\,X$) ou $d = p$. On a $f^d(x) = x$ et $f^p(x) = x$ (donc $d \leqslant p$ par minimalité de d). On en déduit $f^i(x) = x$ pour tout i dans $d\mathbb{Z} + p\mathbb{Z}$. Si on a $d < p$ alors $1 \in d\mathbb{Z} + p\mathbb{Z}$ par Bezout (car p est premier), et donc $f(x) = x$, *i.e.* $d = 1$. On conclut en écrivant $|X| = \sum_{C \in X/R} |C|$ (partition en classes, Proposition 1.4). □

Ce corollaire peut être utilisé pour prouver l'existence de points fixes. En voici une application particulièrement amusante due à Zagier, dans le cas $p = 2$ (une application $f : X \to X$ telle que $f^2 = \mathrm{id}_X$ s'appelle une *involution*.) Il s'agit d'une démonstration « en une seule phrase » du fait que tout nombre premier $q \equiv 1 \bmod 4$ est somme de deux carrés d'entiers (un résultat fondateur de la théorie des nombres dû à Fermat, dont redonnerons une démonstration plus conceptuelle due à Dedekind un peu plus loin dans le cours).

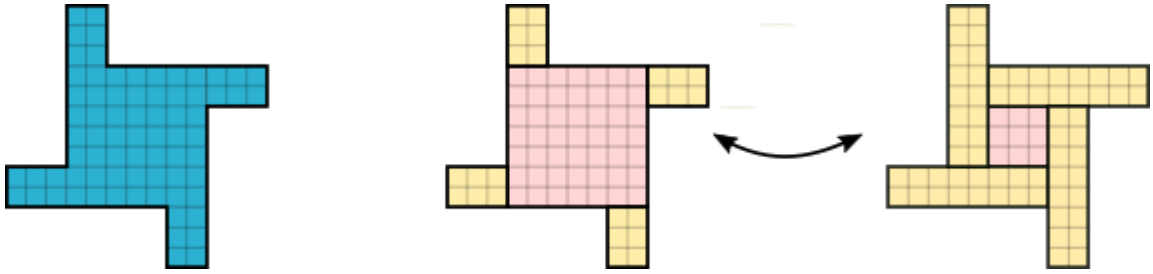
2. On rappelle que f^i désigne la composée $f \circ f \circ \cdots \circ f$ (i fois) pour $i > 0$, $(f^{-1})^{-i}$ pour $i < 0$, et la convention $f^0 = 1_X$. On a alors $f^{i+j} = f^i \circ f^j$ pour tout i, j dans $\mathbb{Z}$.

Exemple 1.10. (Zagier, Amer. Math. Monthly 97 (1990), no. 2, 144) « *The involution on the finite set* $S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = q\}$ *defined by*

$$(x,\, y,\, z) \mapsto \begin{cases} (x+2z,\, z,\, y-x-z) & \text{if} \quad x < y-z, \\ (2y-x,\, y,\, x-y+z) & \text{if} \quad y-z < x < 2y, \\ (x-2y,\, x-y+z,\, y) & \text{if} \quad x > 2y. \end{cases} \tag{2}$$

has only one fixed point, so $|S|$ *is odd and the involution defined by* $(x, y, z) \mapsto (x, z, y)$ *also has a fixed point.* »

Pour la petite histoire, le fait que l'application ci-dessus est une involution de S est laissée au lecteur par Zagier (et en effet, facile à vérifier), tout comme le fait que son unique point fixe est $(1, 1, \frac{q-1}{4})$ (c'est ici que l'on utilise que q est premier). Zagier n'explique pas d'où vient la formule donnée : on en trouvera sur la chaine Youtube de Mathologer https://www.youtube.com/watch?v=DjI1NICfjOk une explication géométrique limpide (les « moulins »), que l'on peut résumer en :



2. Passage au quotient

Examinons comment définir une application dont la source est un ensemble quotient. Observons que si l'on dispose d'une application $g : X/R \to Y$, alors l'application qui s'en déduit $f := g \circ \pi_R : X \to Y$ est manifestement constante sur chaque classe de R-équivalence. C'est la situation générale :

Proposition 2.1. *(Propriété universelle du quotient) Soient* $f : X \to Y$ *une application et* R *une relation d'équivalence sur* X*. On suppose que* f *est constante sur chaque classe d'équivalence : pour tout* $x, y \in X$, $x\,R\,y \Rightarrow f(x) = f(y)$*. Alors existe une unique application* $g : X/R \to Y$ *telle que* $g([x]_R) = f(x)$ *pour tout* $x \in X$*, ou ce qui revient au même, vérifiant* $g \circ \pi_R = f$*.*

Démonstration — L'unicité de g découle de la surjectivité de π_R. Pour son existence, on observe que si C est une classe de R-équivalence, il y a un sens à poser $g(C) = f(x)$ où x est un élément quelconque[3] de C, car C est non vide et f est constante sur C par hypothèses. Pour tout $x \in X$ on a alors $f(x) = g([x]_R)$, *i.e.* $f = g \circ \pi_R$. □

3. Dit comme ça, on a l'impression que l'on a utilisé l'axiome du choix (cf. plus bas). On peut faire sans : par hypothèse sur f, pour C une classe d'équivalence alors l'ensemble $f(C)$ est un singleton, et on définit alors $g(C)$ comme étant son unique élément.

L'application g de l'énoncé est appelée « passage au quotient de f », on la note souvent $\overline{f}$. Essentiellement, nous avons simplement vérifié *une fois pour toutes* que l'application $X/R \to Y, [x]_R \mapsto f(x)$, est bien définie... ce qui est assez trivial ! L'identité $f = \overline{f} \circ \pi_R$ est appelée « factorisation canonique de f ». À moins de bien savoir ce que l'on fait, on procèdera toujours de cette manière pour définir une application dont la source est un quotient. On retiendra le slogan : « *c'est la même chose de se donner une application $X/R \to Y$ et se donner une application $X \to Y$ constante sur les classes de R-équivalence* » (les bijections réciproques étant $g \mapsto g \circ \pi_R$ et $f \mapsto \overline{f}$).

Exemple 2.2. (*Contraction d'une partie*) Soit A une partie de X. La relation $x\,R\,y \Leftrightarrow x = y$ ou ($x \in A$ et $y \in A$), est une relation déquivalence sur X dont les classes d'équivalence sont A et les $\{x\}$ avec $x \in X \smallsetminus A$. Ainsi, la projection $\pi_R : X \to X/R$ est la « *contraction de A en un point* ». Considérons par exemple le cas $X = [0,1]$ et $A = \{0,1\}$. Alors X/R s'identifie naturellement au cercle unité S^1. En effet, l'application $f : x \mapsto e^{2i\pi x}, [0,1] \to \mathrm{S}^1$, est constante sur les classes de R car on a $f(0) = f(1)$. Elle se factorise donc en une application $\overline{f} : [0,1]/R \to \mathrm{S}^1, \overline{x} \mapsto e^{2i\pi x}$, qui est manifestement bijective. La notion de topologie quotient (voir le cours d'analyse) permettrait même de voir $\overline{f}$ comme un homéomorphisme.

3. Sections et systèmes de représentants

Définition 3.1. *Soit $f : X \to Y$ une application. Une section de f (ou "inverse à droite") est une application $s : Y \to X$ vérifiant $f \circ s = \mathrm{id}_Y$.*

Autrement dit, une application $s : Y \to X$ est une section de f si et seulement si pour tout $y \in Y$, $s(y)$ est un élément de la fibre $f^{-1}(\{y\})$. Une section est toujours injective, et uniquement déterminée par son image $s(Y)$, qui est une partie de X rencontrant chaque fibre de f en un et un seul point (*transversale de f*).

Si f possède une section, alors f est surjective. Réciproquement, intuitivement, toute surjection $f : X \to Y$ admet une section : il suffit de *choisir*, pour chaque $y \in Y$, un élément arbitraire de la fibre $f^{-1}(\{y\})$, et de l'appeler $s(y)$. L'axiome autorisant cette construction en théorie des ensemble s'appelle l'*axiome du choix*.

(AC) *Pour tout ensemble X, il existe une application $\tau : \mathrm{P}(X) - \{\varnothing\} \to X$ telle que $\tau(E) \in E$ pour toute partie non vide E de X.*

Une telle fonction τ est appelée *fonction de choix* sur X.

Proposition 3.2. *Les énoncés suivants sont équivalents à l'axiome du choix :*

(i) Toute surjection admet une section.

(ii) Pour toute famille $\{X_i\}_{i\in I}$ de sous-ensembles non vides X_i d'un ensemble X, le produit $\prod_{i\in I} X_i$ est non vide.

Démonstration — Si $f : X \to Y$ est une surjection, et si τ est une fonction de choix sur X, alors $s(y) := \tau(f^{-1}(\{y\}))$ est une section de f (noter $(f^{-1}(\{y\}) \neq \varnothing$ car f est surjective). Donc AC $\Rightarrow$ (i).

Soient $\{X_i\}_{i\in I}$ des ensembles non vides comme au (ii). Posons $X = \coprod_{i\in I} X_i$ leur réunion disjointe externe[4] On dispose d'une application $f : X \to I$ vérifiant $f^{-1}(i) = X_i$ pour $i \in I$ (déjà vue dans l'Exemple 1.2). Pour toute section s de f, on a $(s(i))_{i\in I} \in \prod_{i\in I} X_i$: cela montre (i) $\Rightarrow$ (ii).

Enfin, appliquant (ii) à l'ensemble de toutes les parties non vides de X, on en déduit que $\prod_{E\in \mathrm{P}(X)-\{\varnothing\}} E$ est non vide : un élément quelconque $\tau := (\tau(E))_E$ est une fonction choix sur X. $\square$

Bien que très intuitif, AC a aussi des conséquences surprenantes, comme le *paradoxe de Banach-Tarski*, ou plus simplement les théorèmes de Zorn et de Zermelo (voir le § 4). Pour de nombreux exemples concrets d'ensembles X, on peut construire une fonction de choix sur X sans appel à AC : « *Pour choisir une chaussette plutôt que l'autre pour chaque paire d'une collection infinie, on a besoin de l'axiome du choix. Mais pour les chaussures, ce n'est pas la peine* » (Russel).

Remarque 3.3. (Culturelle) On sait depuis Gödel et Cohen que si l'on rajoute l'axiome du choix, ou son contraire, à la théorie axiomatique des ensembles de Zermelo et Fraenkel (ZF), et si l'on suppose cette dernière cohérente, alors on obtient une théorie cohérente. Nous renvoyons au cours de logique pour comprendre le sens de cette affirmation !

Définition 3.4. *Soient X un ensemble et R une relation d'équivalence sur X. Un* représentant *d'une classe d'équivalence est la donnée d'un élément de cette classe. Un* système de représentants *de (X, R) est la donnée d'un sous-ensemble de X contenant un et un seul représentant de chaque classe d'équivalence ; autrement dit, c'est l'image d'une section de π_R.*

Le fait que toute relation d'équivalence possède un système de représentants est donc une autre formulation de AC. Dans le cas de $\mathbb{Z}/n\mathbb{Z}$ avec $n \geqslant 1$, l'unicité de la division euclidienne montre bien sûr que $\{0, \dots, n-1\}$ est un système de représentants (et donc $|\mathbb{Z}/n\mathbb{Z}| = n$), mais il y en a bien d'autres ! (une infinité dénombrable).

Exemple 3.5. (*Infinite prisonners wearing hats, without hearing*) Nous renvoyons à https://risingentropy.com/axiom-of-choice-and-hats/ pour une explication d'un puzzle surprenant montrant comment l'axiome du choix peut ... sauver des vies ! Il est basé sur le choix d'un système de représentants de la relation d'équivalence sur $\{0,1\}^{\mathbb{N}}$ définie par $(x_n) \sim (y_n) \Leftrightarrow \exists N \geqslant 1,\ x_n = y_n$ pour $n \geqslant N$.

4. Complément : Le lemme de Zorn et le théorème de Zermelo

Le premier but de ce complément est de discuter du Lemme de Zorn. C'est un énoncé moins intuitif qui se déduit de AC et qui a de nombreuses applications : existence d'une base dans un espace vectoriel général, existence des clôtures algébriques, théorème de prolongement de Hahn-Banach, théorème de Tychonoff, existence d'un idéal maximal dans un anneau commutatif non nul... Il nous faut d'abord faire quelques rappels sur les relations d'ordre.

4. Formellement, on identifie naturellement pour tout i l'ensemble X_i au sous-ensemble $Y_i = X_i \times \{i\}$ de $E \times I$, on observe que les Y_i y sont deux à deux disjoints, et on pose $X = \bigcup_{i\in I} Y_i$.

DÉFINITION 4.1. *Une relation d'ordre sur un ensemble X est une relation R sur X supposée réflexive, transitive et vérifiant en outre $x\,R\,y$* et *$y\,R\,x \Rightarrow x = y$, pour tout $x, y \in X$ (antisymétrie).*

Une relation d'ordre est en général notée $\leqslant$. On note alors aussi $x \geqslant y$ pour $y \leqslant x$, $x < y$ pour "$x \leqslant y$ et $x \neq y$", et $x > y$ pour $y < x$. L'ordre $\leqslant$ est dit *total* si deux éléments quelconques de X sont comparables : pour tout $x, y \in X$ on a $x \leqslant y$ ou $y \leqslant x$. Un ensemble muni d'une relation d'ordre est appelé *ensemble ordonné.*

Soit $(X, \leqslant)$ un ensemble ordonné. Toute partie Y de X est naturellement ordonnée par *l'ordre induit* $\leqslant \cap (Y \times Y)$, encore noté $\leqslant$ en général. De plus, on appelle *majorant* (resp. *majorant strict*) de Y tout élément $x \in X$ vérifiant $y \leqslant x$ (resp. $y < x$) pour tout $y \in Y$.

DÉFINITION 4.2. *Soient $(X, \leqslant)$ un ensemble ordonné et $x \in X$. On dit que x est un élément maximal si le seul élément $y \in X$ avec $x \leqslant y$ est $y = x$. On dit que x est un plus grand élément si c'est un majorant de X,* i.e. *si on a $y \leqslant x$ pour tout $y \in X$. Un plus grand élément est nécessairement maximal, et unique s'il existe, auquel cas on le note* $\max X$.

Par symétrie, on dispose aussi de notions de minorants, d'élément minimal (un $x \in X$ tel que $y \leqslant x \Rightarrow y = x$) et de plus petit élément (un $x \in X$ tel que pour tout $y \in X$ on a $x \leqslant y$) et on note $\min X$ l'unique plus petit élément de X s'il existe.

REMARQUE 4.3. Il faut bien noter que quand $\leqslant$ n'est pas total, un élément maximal n'est pas nécessairement un plus grand élément, et n'est pas nécessairement unique. Par exemple, soient n un entier $\geqslant 2$ et X l'ensemble des parties à $< n$ éléments de $\{1, \ldots, n\}$ muni de l'ordre $X \leqslant Y \Leftrightarrow X \subset Y$. Alors $(X, \leqslant)$ n'a pas de plus grand élément, ses éléments maximaux sont les parties à $n-1$ éléments de $\{1, \ldots, n\}$, et on a $\min X = \varnothing$.

Nous pouvons désormais énoncer le *lemme de Zorn.* Un ensemble ordonné est dit *inductif* si tout sous-ensemble totalement ordonné admet un majorant. Par exemple, un ensemble totalement ordonné est inductif si, et seulement si, il admet un plus grand élément.

THÉORÈME 4.4. (Zorn) *Tout ensemble ordonné inductif possède au moins un élément maximal.*

(Un ensemble ordonné inductif est non vide, comme on le voit en considérant un majorant de sa partie vide...) Une application typique de cet énoncé est la suivante.

COROLLAIRE 4.5. *Tout espace vectoriel possède une base.*

On rappelle qu'une partie X d'un k-espace vectoriel V est dite *libre*, si pour toute famille *finie* non vide $\{v_j\}_{j \in J}$ d'éléments distincts de X, la relation $\sum_{i \in J} \lambda_j v_j = 0$ avec les $\lambda_j \in k$ entraîne $\lambda_j = 0$ pour tout $j \in J$. De plus, X est dite *génératrice* si tout élément de V est combinaison linéaire *finie*[5] d'éléments de X . Enfin, X est une *base* si elle est à la fois libre et génératrice.

5. Bien noter que les combinaisons linéaires infinies n'ont pas de sens en général.

Démonstration — Soient k un corps et V un k-espace vectoriel. Soit $\mathscr{L} \subset \mathrm{P}(V)$ le sous-ensemble des parties libres de V (noter $\varnothing \subset \mathscr{L}$!). On le munit de la relation d'inclusion $\subset$ induite de $\mathrm{P}(V)$. Montrons que $(\mathscr{L}, \subset)$ est inductif. Soit $\{L_i\}_{i\in I} \subset \mathscr{L}$ une famille totalement ordonnée de parties libres de V. Alors leur réunion $L' = \cup_{i\in I} L_i$ est encore une partie libre, car toute famille finie d'éléments de L' appartient à un même L_i, et L' contient aussi chaque L_i : c'est un majorant de $\{L_i \mid i \in I\}$ dans $\mathscr{L}$. D'après Zorn, il existe un élément maximal de $\mathscr{L}$, notons-le B.

La fin de l'argument est comme en dimension finie. Supposons B non génératrice : il existe $b \in V$ non dans $\mathrm{Vect}_k B$ (en particulier, $b \notin B$). Alors $B \coprod \{b\}$ contient strictement B et elle est libre : si on a $\lambda b + \sum_{j\in J} \lambda_j b_j = 0$, avec les $\{b_j\}_{j\in J}$ distincts dans B, et λ et les λ_j dans k, on a $\lambda \neq 0$ car B est libre, donc λ inversible car k est un corps, puis $b = -\lambda^{-1} \sum_{j\in J} \lambda_j b_j$. On a contredit la maximalité de B. □

Remarque 4.6. Une modification simple de la démonstration montre que de toute famille génératrice on peut extraire une base. De plus, comme en dimension finie, on peut montrer que si $\{e_i\}_{i\in I}$ et $\{f_j\}_{j\in J}$ sont des bases d'un même espace vectoriel, alors I est en bijection avec J (voir l'Exercice 1.17).

Notre premier but est désormais de démontrer le lemme de Zorn. Un concept crucial pour cela est la notion d'ensemble *bien ordonné*.

Définition 4.7. *Soit $(X, \leqslant)$ un ensemble ordonné. On dit que $\leqslant$ est un bon ordre sur X, ou que $(X, \leqslant)$ est bien ordonné, si toute partie non vide de X admet un plus petit élément.*

Un bon ordre est total (considérer $\min\{x, y\}$), mais la réciproque est bien sûr fausse. Par exemple, l'usuel $(\mathbb{N}, \leqslant)$ est bien ordonné (Peano), mais pas $(\mathbb{Q}_{\geqslant 0}, \leqslant)$.

Un *segment initial* d'un ensemble ordonné $(X, \leqslant)$ est une partie $S \subset X$ telle que pour tout $s \in S$, et tout $x \in X \smallsetminus S$, on a $s < x$. On parle de segment initial *strict* si en outre $S \neq X$. Si S_1 et S_2 sont deux parties de X, on notera $S_1 \preceq S_2$ si S_1 est un segment initial de S_2 : c'est manifestement une relation d'ordre sur $\mathrm{P}(X)$.

Lemme 4.8. *Soit $(X, \leqslant)$ un ensemble ordonné.*

(i) Si $B \subset X$ est bien ordonné, et si $x \in X$ est un majorant strict de B, alors $B' = B \cup \{x\}$ est encore bien ordonné. De plus, les segments initiaux stricts de B' sont les segments initiaux de B.

(ii) On suppose que $(B_i)_{i\in I}$ est une famille de sous-ensembles bien ordonnés de X telle que pour tout $i, j \in I$, on a $B_i \preceq B_j$ ou $B_j \preceq B_i$. Alors, $B = \cup_{i\in I} B_i$ est un sous-ensemble bien ordonné de X, et on a $B_i \preceq B$ pour tout $i \in I$.

Une manière équivalente de formuler le (ii) est la suivante : si $\mathrm{B}(X)$ désigne l'ensemble des parties bien ordonnées de X, alors $(\mathrm{B}(X), \prec)$ est inductif ; mieux, toute collection totalement ordonnée d'éléments de $\mathrm{B}(X)$ admet un plus petit majorant ("*borne supérieure*"), à savoir leur réunion.

Démonstration — Montrons le (i). Si $S \subset B'$ on a soit $S = \{x\}$, auquel cas $x = \min S$, soit $\min S \cap B = \min S$. Pour la seconde assertion, on a par définition $B \prec B'$. Si S est un segment initial de B', alors soit $x \in S$ et $S = B'$, soit $S \prec B$.

Montrons le (ii). Soient $S \subset \cup_{i\in I} B_i$ et i tel que $S \cap B_i \neq \emptyset$. Soit $m := \min S \cap B_i$. Montrons $m = \min S$. Soit $s \in S \smallsetminus B_i$; il existe $j \in I$ tel que $s \in B_j$. Si $B_j \preceq B_i$ on a évidemment $B_j \subset B_i$ et donc $m \leqslant s$. Sinon, on a $B_i \preceq B_j$ par hypothèse, et $s \in B_j \smallsetminus B_i$, et donc encore $s \geqslant m$. Pour la dernière assertion, il suffit d'observer que pour $b \in B_i$, et $x \in B_j \smallsetminus B_i$ alors on a $b < x$ car B_i est un segment initial de B_j. □

Démonstration — (du Lemme de Zorn) Supposons par l'absurde que X n'a pas d'élément maximal. Soit $\mathscr{B}$ l'ensemble des parties bien ordonnées de X. Pour $B \in \mathscr{B}$ on note $\mathrm{M}(B) = \{x \in X \mid b < x, \forall\, b \in B\}$ l'ensemble de ses majorants stricts. On a $\mathrm{M}(B) \neq \emptyset$. En effet, on peut trouver par hypothèse un majorant x de B dans X, car B est totalement ordonnée. Comme x n'est pas maximal dans X, il existe $y \in X$ vérifiant $x < y$, et on a alors $y \in \mathrm{M}(B)$. Par AC, le produit $\prod_{B\in\mathscr{B}} \mathrm{M}(B)$ est donc non vide. On en choisit un élément $m = (m(B))_{B\in\mathscr{B}}$.

Appelons *m-ordinal* un sous-ensemble bien ordonné $B \subset X$ tel que pour tout segment initial strict S de B on a $\min(B \smallsetminus S) = m(S)$. On note $\mathscr{B}_m \subset \mathscr{B}$ le sous-ensemble des m-ordinaux. Par exemple, $\emptyset$ est un m-ordinal, et le seul singleton m-ordinal est $\{x_0\}$ avec $x_0 := m(\emptyset)$. Nous allons voir que les m-ordinaux sont emboités les uns dans les autres de manière très rigide (et infinie) :

Lemme : (O1) *Si B est un m-ordinal, alors $B^+ := B \coprod \{m(B)\}$ est un m-ordinal.*

(O2) *Si A et B sont deux m-ordinaux, on a $A \preceq B$ ou $B \preceq A$.*

Démonstration — (du Lemme) En effet, (O1) est conséquence directe du Lemme 4.8 (i). Montrons (O2). Soit T la réunion de tous les sous-ensembles de X qui sont des segments initiaux de A et de B. Comme une union de segments initiaux est trivialement un segment initial, T est encore un segment initial de A et de B, et c'est donc le plus grand segment initial à la fois de A et de B. Si T est strictement inclus dans A et dans B, alors $m(T) = \min A \smallsetminus T = \min B \smallsetminus T$ est dans $A \cap B$. Mézalor $T^+ = T \cup \{m(T)\}$ est un segment initial de A et de B : c'est l'ensemble de leurs éléments $\leqslant m(T)$. On a donc $T^+ \subset T$, puis $m(T) \in T$: une contradiction ! On a montré $T = A$ ou $T = B$, QED. □

Terminons la démonstration du théorème. On considère la réunion $U = \cup_{B\in\mathscr{B}_m} B$ de tous les m-ordinaux. Alors U est bien ordonné par le Lemme 4.8 (ii), qui s'applique par (O2). Vérifions qu'il est m-ordonné. Soit S un segment initial strict de U. Posons $u = \min U \smallsetminus S$, de sorte que l'on a $S = \{x \in U \mid x < u\}$. On a aussi $u \in B$ pour un certain $B \in \mathscr{B}_m$. Mais comme B est un segment initial de U par la deuxième assertion du Lemme 4.8 (ii), B contient S, et on a donc $u = \min U \smallsetminus S = \min B \smallsetminus S = m(S)$, *i.e.* $U \in \mathscr{B}_m$. Mézalor on a aussi $U^+ \in \mathscr{B}_m$ par (O1), et donc $U^+ \subset U$ par définition de U, *i.e.* $\mathrm{m}(U) \in U$: une contradiction. □

Terminons par une conséquence surprenante du Lemme de Zorn.

Théorème 4.9. (Zermelo) *Tout ensemble peut être muni d'un bon ordre.*

Démonstration — Soit X un ensemble. On note E l'ensemble des couples (B, R) avec $B \subset X$ et $R \subset B \times B$ une relation de bon ordre sur X. On munit E d'une relation d'ordre en posant $(B, R) \leqslant (B', R') \Leftrightarrow B \subset B'$, $R = R' \cap (B \times B)$ (de sorte

que B est une partie de B' et R l'ordre induit par R' sur cette partie), et si en outre B est un segment initial de B'. On va montrer que $(E, \leqslant)$ est inductif.

Soit $\{(B_i, R_i) \mid i \in I\}$ est une famille totalement ordonnée d'éléments de E, *i.e.* I est totalement ordonné et on a $(B_i, R_i) \leqslant (B_j, R_j)$ pour $i \leqslant j$. On pose $B = \cup_{i \in I} B_i$. Soient $x, y \in B$. Il existe $i, j \in I$ tels que $x \in B_i$ et $y \in B_j$. Alors $x \, R \, y := x \, R_k \, y$ est indépendant du choix de $k \geqslant \max\{i, j\}$, et définit manifestement une relation d'ordre sur B induisant R_i sur B_i. D'après le Lemme 4.8 (ii), (B, R) est dans E et c'est un majorant de $\{(B_i, R_i) \mid i \in I\}$. Ainsi, $(E, \leqslant)$ est inductif.

D'après le lemme de Zorn, E admet donc un élément maximal (B, R). Supposons $B \neq E$. On choisit $x \in E - B$ arbitrairement et l'on considère l'unique relation d'ordre R' sur $B' = B \cup \{x\}$ induisant R sur B et pour laquelle x est un majorant strict de B dans B'. On a alors $(B, R) < (B', R')$ par le Lemme 4.8 (i), en contradiction avec la maximalité de (B, R). Cela montre $B = E$, et R convient. $\square$

Remarquons que le théorème de Zermelo implique trivialement AC : si X est bien ordonné, alors $S \mapsto \min S$ est une fonction de choix sur X. Au final, nous avons montré (dans ZF), l'équivalence entre AC, le lemme de Zorn et le théorème de Zermelo (en montrant précisément AC $\Rightarrow$ Zorn $\Rightarrow$ Zermelo $\Rightarrow$ AC).

5. Exercices

Exercice 1.1. (Relation d'équivalence engendrée par une relation) *Soient X un ensemble et $R \subset X \times X$ une relation sur X.*

(i) Montrer qu'il existe une plus petite relation d'équivalence R' sur X contenant R (appelée « relation d'équivalence engendrée par R »).

(ii) Montrer que l'on a $x \, R' \, y$ si, et seulement si, il existe $n \geqslant 1$ et $x_1, \ldots, x_n \in X$ avec $x_1 = x$, $x_n = y$, et $x_i \, R \, x_{i+1}$ ou $x_{i+1} \, R \, x_i$ pour tout $1 \leqslant i < n$.

Exercice 1.2. *Montrer que la conclusion $|X| \equiv |\mathrm{Fix}\, X| \bmod p$ du Corollaire 1.9 vaut encore si l'on suppose $f^{p^m} = \mathrm{id}_X$ avec $m \geqslant 1$, au lieu de $f^p = \mathrm{id}_X$. Peut-on remplacer p par p^m dans cette congruence ?*

Exercice 1.3. (Congruence de Touchard) *Notons B_n le nombre de partitions d'un ensemble à n éléments, avec la convention $\mathrm{B}_0 = 1$. Soit p un nombre premier.*

(i) En considérant la bijection de $I \coprod \mathbb{Z}/p\mathbb{Z}$ qui vaut l'identité sur I et $x \mapsto x+1$ sur $\mathbb{Z}/p\mathbb{Z}$, montrer $\mathrm{B}_{n+p} \equiv \mathrm{B}_n + \mathrm{B}_{n+1} \bmod p$, pour tout $n \geqslant 0$.

(ii) Montrer plus généralement $\mathrm{B}_{n+p^m} \equiv m\,\mathrm{B}_n + \mathrm{B}_{n+1} \bmod p$ pour $m \geqslant 1$.

Exercice 1.4. *(i) Compléter la démonstration de l'Exemple 1.10, et comprendre géométriquement les trois cas de figure de l'involution de Zagier.*

(ii) Pouvez-vous démontrer, par une méthode géométrique de ce type, que tout nombre premier $p \equiv 1 \bmod 3$ est de la forme $a^2 + 3b^2$?[6]

6. Si oui, cela m'intéresse, car je ne connais pas de telle démonstration, ni pour cet exemple, ni pour d'autres similaires !

EXERCICE 1.5. *(i) Construire une fonction de choix sur $\mathbb{Q}$, puis sur $\mathbb{Q}^2$.*

(ii) Construire, sans l'axiome du choix, une fonction associant à tout ouvert non vide U de $\mathbb{R}^2$ un élément de U.

(iii) (suite) Est-ce possible avec les fermés ? les dénombrables[7] *?*

EXERCICE 1.6. *Soient (X, d) un espace metrique et ϵ un réel > 0. Une partie $A \subset X$ est dite* ϵ-séparée *si on a $d(x, y) \geqslant \epsilon$ pour tout x, y distincts dans A, et* ϵ-séparée maximale *si en outre la seule partie ϵ-séparée de X contenant A est A.*

(i) Vérifier que si $A \subset X$ est ϵ-séparée maximale, alors pour tout $x \in X$ il existe $a \in A$ avec $d(x, a) < \epsilon$.

(ii) Montrer que toute partie ϵ-séparée de X est incluse dans une partie ϵ-séparée maximale.

Deux ensembles ordonnés X et Y sont dits *isomorphes*[8] s'il existe une bijection $f : X \to Y$ telle que pour tout $x, y \in X$, $x \leqslant y \Leftrightarrow f(x) \leqslant f(y)$.

EXERCICE 1.7. (Ordre lexicographique)

(i) Soient X et Y des ensembles ordonnés. Vérifier que $(x, y) \leqslant (x', y') \Leftrightarrow (x < x')$ ou $(x = x'$ et $y < y')$ est une relation d'ordre sur $X \times Y$.

(ii) Montrer que si X et Y sont bien ordonnés, il en va de même de $X \times Y$.

(iii) On munit $\mathbb{N}$ de son ordre usuel, ainsi que sa partie $\{0, 1\}$. Est-ce que les ensembles (lexicographiquement) ordonnés $\{0, 1\} \times \mathbb{N}$ et $\mathbb{N} \times \{0, 1\}$ sont isomorphes entre eux ? à $\mathbb{N}$?

La série d'exercices suivants constitue des rappels sur la notion de cardinalité. Soient A et B deux ensembles. On dit que A et B sont *équipotents*, et on note $A \sim B$, s'il existe une bijection de A dans B. Comme l'identité, l'inverse d'une bijection, et la composée de deux bijections, sont encore des bijections, l'équipotence est une relation d'équivalence sur la classe des ensembles. La classe d'équipotence d'un ensemble A est aussi notée $|A|$ et appelée *cardinal* de A. On a donc $|A| = |B|$ si, et seulement si, $A \sim B$. On notera $A \hookrightarrow B$, ou $|A| \leqslant |B|$, s'il existe une injection de A dans B. L'exercice suivant montre que c'est une relation d'ordre.

EXERCICE 1.8. *On veut montrer que si A et B sont deux ensembles avec $A \hookrightarrow B$ et $B \hookrightarrow A$, alors on a $A \sim B$ (Théorème de Cantor-Schröder-Bernstein).*

(i) Montrer que l'on peut supposer $A \subset B$ et qu'il existe une injection $i : B \to A$.

(ii) Montrer que les $i^n(B \smallsetminus A)$, avec $n \geqslant 0$, sont deux à deux disjoints.

(iii) En déduire que $j : A \to B$, définie par $j(x) = i^{-1}(x)$ s'il existe $n \geqslant 1$ avec $x \in i^n(B \smallsetminus A)$, et $j(x) = x$ sinon, est une bijection ("on remonte l'escalier" de la figure 1).

---

7. On admettra ici que l'axiome du choix est nécessaire pour construire un sous-ensemble non Lebesgue-mesurable de $\mathbb{R}$ (Solovay), et on considèrera la relation d'équivalence sur $\mathbb{R}$ définie par $x \sim y \Leftrightarrow x - y \in \mathbb{Q}$ (exemple de Vitali).

8. Plus généralement, un *morphisme d'ensemble ordonnés* est une application $f : X \to Y$ vérifiant $x \leqslant y \implies f(x) \leqslant f(y)$ pour tout $x, y \in Y$ (on parle aussi d'application *croissante*).

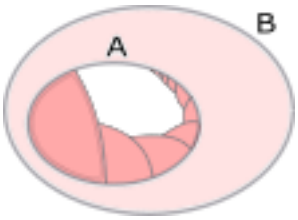


FIGURE 1

Si A et B sont deux ensembles, on notera $A \twoheadrightarrow B$, ou $|A| \geqslant |B|$, s'il existe une surjection de A dans B. Nous allons voir $|A| \geqslant |B| \iff |B| \leqslant |A|$.

EXERCICE 1.9. *(i) Soit $f : X \to Y$ une application. Une* retraction *de f (ou* inverse à gauche*) est une application $r : Y \to X$ vérifiant $r \circ f = \mathrm{id}_X$. Montrer que f admet une retraction si, et seulement si, f est injective.*

(ii) Montrer que $A \hookrightarrow B$ est équivalent à $B \twoheadrightarrow A$.

Vous remarquerez que votre démonstration du (ii) de l'exercice précédent utilise AC, contrairement à celle du (i) ou du théorème de Cantor-Schröder-Bernstein.

On rappelle qu'un ensemble A est dit *dénombrable* si l'on a une surjection $\mathbb{N} \to A$, ou ce qui revient au même, si on a $A \hookrightarrow \mathbb{N}$.

EXERCICE 1.10. *(Préservation de la dénombrabilité)*

(i) Montrer que si A est infini et dénombrable alors on a $A \sim \mathbb{N}$.

(ii) Montrer que si on a $A \twoheadrightarrow B$ avec A dénombrable, alors B est dénombrable.

(iii) Montrer que si A et B sont dénombrables, alors $A \times B$ est dénombrable.

(iv) Soient A un ensemble et $(A_n)_{n\in\mathbb{N}}$ une famille dénombrable de sous-ensembles dénombrables de A. Montrer que $\cup_{n\in\mathbb{N}} A_n$ est dénombrable.

EXERCICE 1.11. *(i) Montrer les équipotences $\mathbb{R} \sim [0,1] \sim \{0,1\}^{\mathbb{N}}$.*

(ii) Rappeler pourquoi $\{0,1\}^{\mathbb{N}}$, et donc $\mathbb{R}$, n'est pas dénombrable (argument diagonal de Cantor *: si $(\epsilon_{m,n})_{m,n} \in \{0,1\}^{\mathbb{N}\times\mathbb{N}}$, considérer $(1-\epsilon_{n,n})_n \in \{0,1\}^{\mathbb{N}}$).*

(iii) Montrer aussi $\mathbb{R} \sim \{0,1\}^{\mathbb{N}\times\mathbb{N}} \sim \mathbb{N}^{\mathbb{N}}$.

EXERCICE 1.12. *Soient A un ensemble infini et $n \geqslant 1$. On veut montrer*

$$A \sim A \times \{1, \ldots, n\} \text{ et } A \sim A \times \mathbb{N}.$$

(i) Montrer que A admet une partition en sous-ensembles infinis dénombrables.

(ii) En déduire $A \sim B \times \mathbb{N}$ pour un certain ensemble B, puis conclure.

L'exercice suivant montre que $|A| \leqslant |B|$ est une relation d'ordre total sur la classe des ensembles.

EXERCICE 1.13. *Montrer que si A et B sont deux ensembles, on a $A \hookrightarrow B$ ou $B \hookrightarrow A$. On pourra considérer l'ensemble des couples (X, f) avec $X \subset A$ et $f : X \to B$ une injection.*

EXERCICE 1.14. *Soient X un ensemble infini et $A, B \subset X$ avec $X = A \cup B$ et disons $B \hookrightarrow A$. Montrer $X \sim A$.*

EXERCICE 1.15. *Soit X un ensemble infini. On veut montrer $X \sim X \times X$.*

(i) On suppose que $f : X \times X \to X$ est une bijection. On considère $Y = X \coprod X'$ où X' est un ensemble en bijection avec X. Montrer qu'il existe une bijection $g : Y \times Y \to Y$ dont la restriction à $X \times X$ coïncide avec f.

(ii) Conclure en appliquant le lemme de Zorn à l'ensemble convenablement ordonné des couples (A, f) avec $A \subset X$ et f une bijection $A \times A \to A$.

EXERCICE 1.16. *Si X est un ensemble, on note $\mathrm{P}_f(X)$ l'ensemble des parties finies de X. Montrer que si X est infini on a $X \sim \mathrm{P}_f(X)$.*

Les exercices suivants traitent des espaces vectoriels de dimension quelconque.

EXERCICE 1.17. *Soient V un espace vectoriel, $e = \{e_i\}_{i \in I}$ une famille génératrice de V, et $f = \{f_j\}_{j \in J}$ une base de V.*

(i) Pour $i \in I$, on écrit $e_i = \sum_{j \in J} x_j f_j$ et on pose $J_i = \{j \in J, x_j \neq 0\}$ (un ensemble fini). Montrer $J = \cup_{i \in I} J_i$.

(ii) En déduire $I \times \mathbb{N} \twoheadrightarrow J$, puis $J \hookrightarrow I$.

(iii) En déduire que si e et f sont des bases de V alors $I \sim J$.

EXERCICE 1.18. *Soient V un k-espace vectoriel et $e = \{e_i\}_{i \in I}$ une base de V. On suppose I infini.*

(i) Montrer $V \sim k \times I$.

(ii) En déduire que l'on a $V \sim I$ ou $V \sim k$.

Chapitre 2

Généralités sur les groupes

Dans ce premier chapitre sur les groupes on commence par en rappeler la définition abstraite, puis on donne quelques uns des exemples principaux que nous étudierons par la suite : groupes de permutations, groupes linéaires, groupes abéliens, groupes de symétrie, groupes additifs et multiplicatifs des anneaux. On introduit les notions de sous-groupes, de groupes produits et de groupes engendrés par une partie, qui permettent de construire de nombreux nouveaux groupes à partir de groupes connus. On rappelle ensuite les notions de morphismes et d'isomorphismes, cruciales pour comparer des groupes définis de manières différentes, ou encore pour aborder les questions de classification. On étudie ensuite en détail la structure des groupes cycliques/monogènes (engendrés par un seul élément). La théorie de Lagrange (classes à gauche/droite) donne des contraintes fortes sur les sous-groupes possibles d'un groupe fini ; elle permet par exemple de montrer que tout groupe d'ordre premier p est cyclique. On l'utilise aussi pour étudier la structure du groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$, ce qui a des conséquences arithmétiques élémentaires intéressantes (Fermat, Euler, Gauss). On introduit enfin la notion de groupe quotient, cruciale à la méthode de dévissage, et qui donne aussi un autre point de vue sur des groupes familiers comme $\mathbb{Z}/n\mathbb{Z}$, $\mathrm{S}^1 \simeq \mathbb{R}/\mathbb{Z}$ ou $\mathbb{C}^\times \simeq \mathbb{C}/\mathbb{Z}$. Dans un premier compléments nous revenons sur la structure des groupes additifs et multiplicatifs des corps usuels $\mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$, et dans un second, nous introduisons la notion de groupe libre et de groupe défini par générateurs et relations.

Référence : (parmi tant d'autres) *Algebra*, 3ème ed. (S. Lang).

1. Exemples de groupes

On rappelle que si X est un ensemble, une *loi de composition*[1] sur X est la donnée d'une application $\star : X \times X \to X$. Autrement dit, c'est une recette *a priori arbitraire* associant à un couple ordonné (x, y) d'éléments de X, un autre élément $\star(x, y)$ (leur "produit"). Pour coller à la notion intuitive d'opération, on note en général $x \star y$ l'élément $\star(x, y)$; d'autres symboles classiquement utilisés au lieu de $\star$ sont $\circ, \cdot, +$ et $\times$. La définition suivante est due à Von Dyck[2] (voir aussi Cayley[3].).

Définition 1.1. *Un groupe est la donnée d'un ensemble G muni d'une loi de composition $\star$ vérifiant les propriétés (i), (ii) et (iii) suivantes :*

(i) (Associativité) $x \star (y \star z) = (x \star y) \star z$ pour tout $x, y, z \in G$.

(ii) (Neutre) Il existe $e \in G$ tel que pour tout $x \in G$ on a $e \star x = x$ et $x \star e = x$.

1. On parle parfois de loi de composition *interne*, par opposition aux lois externes $X \times Y \to Y$ avec X pas forcément égal à Y (comme en théorie des espaces vectoriels ou des modules).
2. *Gruppentheoretische Studien*, Math. Annalen 20 (1882).
3. *On the Theory of Groups as depending on the Symbolical Equation $\theta^n = 1$* (1854).

(iii) (Inverse) Pour tout $x \in G$, il existe $y \in G$ tel que $x \star y = e$ et $y \star x = e$.

Quelques commentaires s'imposent. Tout d'abord, si $(G, \star)$ est un groupe, il existe un *unique* élément $e \in G$ vérifiant $e \star x = x = x \star e$ pour tout $x \in G$: l'existence est assurée par (ii), et si e' en est un autre, on a $e = e' \star e = e'$. On l'appelle *l'élément neutre* du groupe G, et c'est de cet élément qu'il est question dans (iii). Pour $x \in G$, un élément $y \in G$ vérifiant $x \star y = e$ et $y \star x = e$ est appelé *inverse* de x dans G. Là encore, un tel élément y existe par (iii), et il est unique par (i) et (ii) : si y' en est un autre, on a $y' = y' \star e = y' \star (x \star y) = (y' \star x) \star y = e \star y = y$.

La notation $\star$, bien que pédagogique pour introduire les axiomes, est lourde en pratique. En général, on utilisera plutôt la notation dite *multiplicative* $(x, y) \mapsto x \cdot y$, voire simplement $(x, y) \mapsto xy$ (sans symbole !), pour désigner une loi de groupe. Ainsi, l'associativité s'écrit alors simplement $x(yz) = (xy)z$ pour tout $x, y, z \in G$. En particulier, on peut noter simplement xyz cet élément sans préciser le parenthésage utilisé pour effectuer le produit. Plus généralement, si $x_1, x_2, \ldots, x_n$ sont n éléments de G avec $n \geqslant 1$, il y a un sens à considérer leur produit $x_1 x_2 \cdots x_n$ sans spécifier de parenthésage : c'est intuitif, mais nous le justifierons quand même en détail ci-dessous. En revanche l'ordre des éléments est en général important (on n'a pas toujours $xy = yx$). De plus, on notera toujours 1, parfois 1_G en cas de confusions possibles, le neutre du groupe G ; on a donc $1\,x = x\,1 = x$ pour tout $x \in G$. L'inverse d'un élément $x \in G$ d'un groupe sera noté x^{-1} ; il vérifie $x\,x^{-1} = x^{-1}x = 1$ et $(x^{-1})^{-1} = x$. Enfin, pour $x \in G$ et $n \in \mathbb{Z}$, on pose $x^n = x\,x \cdots x$ (n fois) pour $n \geqslant 1$, $x^n = (x^{-1})^{-n}$ pour $n \leqslant -1$, et on adopte la convention $x^n = 1$ pour $n = 0$. On dira en général simplement « *soit G un groupe* » sans mentionner sa loi de groupe $(x, y) \mapsto xy$, mais elle sera toujours sous-entendue. L'ordre d'un groupe G est le cardinal (fini ou infini) de son ensemble sous-jacent ; on le note $|G|$.

Exemple 1.2. (*Groupe symétrique*) Soit X un ensemble. L'ensemble des bijections de X dans X (les "*permutations de X*"), muni de la loi $\circ$ de composition des applications, est un groupe appelé *groupe symétrique* de X, de neutre id_X. On le note S_X ou $\mathfrak{S}_X$. L'inverse d'une bijection σ est la bijection réciproque σ^{-1}. Dans le cas $X = \{1, \ldots, n\}$ avec $n \geqslant 1$ entier on le note S_n ou $\mathfrak{S}_n$; on a $|\mathrm{S}_n| = n!$.

Exemple 1.3. (*Groupe linéaire*) Soit V un espace vectoriel sur un corps k. L'ensemble des applications k-linéaires bijectives de V ("automorphismes de V"), muni de la loi $\circ$ de composition des applications, est un groupe appelé *groupe linéaire* de V et noté $\mathrm{GL}(V)$.

Exemple 1.4. (*Groupe produit*) Si $(G_i)_{i \in I}$ est une famille de groupes, alors l'ensemble produit $\prod_{i \in I} G_i$ muni de la loi $(g_i)_i (h_i)_i = (g_i h_i)_i$ est un groupe, appelé *groupe produit (directe externe) des G_i* et encore noté $\prod_{i \in I} G_i$. Son neutre est $(1_{G_i})_i$, l'inverse de $(g_i)_i$ étant $(g_i^{-1})_i$. En particulier, si $G_1, \ldots, G_n$ sont des groupes (éventuellement égaux !), on dispose du groupe produit $G_1 \times G_2 \times \cdots \times G_n$.

On dit que deux éléments x, y d'un groupe G *commutent* si on a $xy = yx$. Un rôle important sera joué par les groupes dans lesquels tous les éléments commutent entre eux :

Définition 1.5. *Un groupe G est dit commutatif, ou abélien, si l'on a $xy = yx$ pour tout $x, y \in G$.*

L'exemple le plus simple de groupe abélien est le groupe $(\mathbb{Z}, +)$, avec $+$ l'addition usuelle bien entendu. Pour cette raison, les lois de groupes abéliens sont souvent notées $(x, y) \mapsto x + y$ (notation *additive*), auquel cas on utilise la notation 0 (ou 0_G) pour l'ément neutre, $-x$ pour l'inverse de x, $\sum_i x_i$ pour le produit d'un ensemble fini d'éléments x_i de G (il ne dépend plus de l'ordre choisi sur les x_i), et nx pour l'élément x^n ($n \in \mathbb{Z}$). On a alors les formules de "distributivité" $(n+m)x = nx+mx$ et $n(x+y) = nx+ny$ pour tout $x, y \in G$ et tout $m, n \in \mathbb{Z}$. On note aussi $x - y$ pour $x + (-y)$. La structure de groupe abélien est particulièrement fondamentale, car elle fait partie des axiomes de nombreuses structures mathématiques. Par exemple, *le groupe additif d'un anneau ou d'espace vectoriel sur un corps est un groupe abélien.*

Exemple 1.6. Les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, munis de l'addition usuelle $+$, sont des groupes abéliens. De même, $\{\pm 1\}$, $\mathbb{Q}^\times$, $\mathbb{R}^\times$ et $\mathbb{C}^\times$, muni de la multiplication usuelle $\cdot$, sont aussi des groupes abéliens.

Exemple 1.7. Pour tout entier $n \geqslant 1$, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ muni de la loi $(\overline{a}, \overline{b}) \mapsto \overline{a+b}$) est un groupe abélien d'ordre n. Cette loi est bien définie car pour tout $a, a', b, b' \in \mathbb{Z}$ avec $a \equiv a' \bmod n$ et $b \equiv b' \bmod n$, alors $a + a' \equiv b + b' \bmod n$. Elle est de neutre $\overline{0}$ et on a l'égalité $-\overline{a} = \overline{-a}$.

En revanche, le groupe S_n pour $n > 2$, et le groupe $\mathrm{GL}(V)$ pour $\dim V > 1$, ne sont pas abéliens. Certains sous-ensembles d'un groupe donné héritent naturellement d'une structure de groupe.

Définition 1.8. *Une partie H d'un groupe G est un sous-groupe si l'on a $1 \in H$ et si pour tout $x, y \in H$ on a $xy \in H$ et $x^{-1} \in H$.*

Ainsi, si $(G, \cdot)$ est un groupe et si H est un sous-groupe de G, la loi $\cdot : H \times H \to H, (x, y) \mapsto xy$ induite par le produit dans G fait de H un groupe. Certains auteurs notent $H \leqslant G$ pour « H est un sous-groupe de G ». On a bien sur $\{1\} \leqslant G$ (sous-groupe *trivial*) et $G \leqslant G$ (sous-groupe *total*). Par exemple, $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ forment une tour de sous-groupes additifs, et $\{\pm 1\} \subset \mathbb{Q}^\times \subset \mathbb{R}^\times \subset \mathbb{C}^\times$ une tour de sous-groupes multiplicatifs.

Exemple 1.9. (*Racines de l'unité*) Pour $n \geqslant 1$, on note $\mu_n \subset \mathbb{C}^\times$ le sous-ensemble des racines n-èmes de l'unité. C'est un sous-groupe d'ordre n de $\mathbb{C}^\times$. On a par exemple $\mu_2 = \{\pm 1\}$.

Exemple 1.10. (*Groupes de permutations de degré n*) Ce sont les sous-groupes de S_n. Autrement dit, ce sont les sous-ensembles de permutations de $\{1, 2, \ldots, n\}$ stables par composition, inverse et contenant l'identité. Historiquement, ce sont parmi les premiers exemples de groupes étudiés (Lagrange, Galois), en lien avec la question de la résolubilité par radicaux des racines d'un polynôme à une variable.

Exemple 1.11. Soit V un k-espace vectoriel. Le groupe $\mathrm{GL}(V)$ est le sous-groupe de S_V constitué des bijections k-linéaires. Les sous-groupes de $\mathrm{GL}(V)$ sont particulièrement intéressants comme nous le verrons. Dans un registre différent, V lui-même est aussi un groupe pour l'addition comme on l'a dit. Les sous-espaces vectoriels de V sont alors des sous-groupes de V (mais ce sont loin d'être les seuls sous-groupes en général).

Remarquons que la réunion de deux sous-groupes est rarement un sous-groupe (penser à deux droites vectorielles distinctes dans un plan). En revanche, il est évident que si A et B sont des sous-groupes de G, il en va de même de $A \cap B$. Plus généralement, l'intersection $\cap_{i\in I} A_i$ d'une famille quelconque de sous-groupes A_i de G est un sous-groupe de G.

Exemple 1.12. (*Groupes d'isométries*) Soit E un espace euclidien, de distance euclidienne d. L'ensemble des isométries de E, c'est-à-dire des bijections $f : E \to E$ telles que $d(f(x), f(y)) = d(x, y)$ pour tout $x, y \in E$ est un sous-groupe de S_E noté $\mathrm{Iso}(E)$. Le sous-groupe $\mathrm{O}(E) := \mathrm{Iso}(E) \cap \mathrm{GL}(E)$ est appelé *groupe orthogonal* de E. Ces groupes sont notés $\mathrm{O}(n)$ et $\mathrm{Iso}(n)$ quand E est l'espace euclidien standard $\mathbb{R}^n$. Si $F \subset E$ est une partie quelconque de E (une "figure"), alors

$$\mathrm{Iso}_E(F) = \{g \in \mathrm{Iso}(E) \mid g(F) = F\}$$

est un sous-groupe $\mathrm{Iso}(E)$ est appelé *groupe d'isométries euclidiennes* de F, ou simplement *groupe des symétries* de F. Ce groupe (ordre, structure, etc..) révèle beaucoup de la géométrie de la figure F, au point que des mathématiciens comme Klein ont mis l'étude des groupes de symétries au coeur de la géométrie (programme d'Erlangen).

Exemple 1.13. (*Sous-groupe engendré par une partie*) Soit G un groupe et X une partie de G. Le groupe engendré par X est le sous-groupe $\langle X \rangle$ de G constitué de 1 et de tous les produits

$$g_1^{\epsilon_1} g_2^{\epsilon_2} \cdots g_n^{\epsilon_n}$$

avec $n \geqslant 1$, $g_1, g_2, \ldots, g_n \in X$ et $\epsilon_1, \epsilon_2, \ldots, \epsilon_n \in \{\pm 1\}$. Dans le cas $X = \{g_1, \ldots, g_r\}$, on note aussi $\langle g_1, \ldots, g_r \rangle$ pour $\langle X \rangle$. Si $G = \langle X \rangle$ on dit que X engendre G, que X est une famille génératice de G, ou encore que les éléments de X sont des générateurs de G. Enfin, on dit que G est de type fini s'il admet une famille génératrice finie.

Exemple 1.14. (*Produit restreint*) Si $(G_i)_{i\in I}$ est une famille de groupes, on note $\prod'_{i\in I} G_i$ le sous-ensemble du groupe $\prod_{i\in I} G_i$ constitué des $(g_i)_i$ avec $g_i = 1$ pour tout $i \in I$ sauf au plus un nombre fini. C'est un sous-groupe appelé *produit restreint des* G_i. Quand $G_i = G$ pour tout i, on note aussi $G^{(I)}$ ce sous-groupe de G^I.

Une grande partie du cours sera consacrée à l'étude de tous ces exemples.

Mentionnons que des structures plus ou moins riches que la structure de groupes, mais souvent en lien avec ceux-là, sont également fréquemment rencontrées en mathématiques. Un *monoïde* est la donnée d'un couple $(X, \star)$ avec X un ensemble et $\star$ une loi de composition sur X associative et possédant un élément neutre (alors unique). Par exemple, la composition des applications $\circ$ définit aussi une loi de monoïde sur l'ensemble X^X de toutes les applications $X \to X$. Les monoïdes sont plus complexes à étudier que les groupes (voir par exemple l'Exercice 2.3).

Exemple 1.15. (*Groupe des inversibles d'un monoïde*) Soit X un monoïde de neutre 1. L'ensemble $\{x \in X \mid \exists y \in Y,\ yx = xy = 1\}$ des éléments inversibles de X est stable par produit : si x' est l'inverse de x (nécessairement unique) et y' celui de y on vérifie de suite que $y'x'$ est l'inverse de xy. C'est donc un groupe de neutre 1 appelé *groupe des inversibles* de X, et noté $X^\times$. Par exemple, le groupe des inversibles de $(X^X, \circ)$ est S_X.

DÉFINITION 1.16. *Un anneau est un triplet* $(A, +, \cdot)$ *tel que* $(A, +)$ *est un groupe abélien,* $(A, \cdot)$ *est un monoïde, vérifiant, pour tout* a, b, c *dans* A *les relations de distributivité :* $a \cdot (b + c) = a \cdot b + a \cdot c$ *et* $(b + c) \cdot a = b \cdot a + c \cdot a$.

On dit que l'anneau A est commutatif si $\cdot$ est commutative : $a \cdot b = b \cdot a$ pour tout $a, b \in A$. On note alors toujours 0 (ou 0_A) le neutre de $(A, +)$, et 1 (ou 1_A) celui de $(A, \cdot)$. On note en général simplement $(x, y) \mapsto xy$ la seconde loi $(x, y) \mapsto x \cdot y$. En particulier, on a $(0 + 0)\, a = 0\, a = 0\, a + 0\, a$, et donc $0\, a = 0$ pour tout a dans A. Comme pour les groupes, on dit en général "soit A un anneau" pour "soit $(A, +, \cdot)$" un anneau (les deux lois sont sous-entendues, et toujours notées $+$ et $\cdot$). On suppose le lecteur familier avec les structures d'anneaux usuelles sur $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$. Un autre exemple classique d'anneau est, pour tout entier $n \in \mathbb{Z}$, l'anneau $\mathbb{Z}/n\mathbb{Z}$ de l'arithmétique modulaire (un enrichissement de l'Exemple 1.7).

EXEMPLE 1.17. *Pour tout* $n \in \mathbb{Z}$, *il existe une unique structure d'anneau sur l'ensemble quotient* $\mathbb{Z}/n\mathbb{Z}$ *telle que pour tout* $a, b \in \mathbb{Z}$ *on ait* $\overline{a} + \overline{b} = \overline{a + b}$ *(addition) et* $\overline{a}\overline{b} = \overline{ab}$ *(multiplication).*

En effet, c'est une reformulation du fait bien connu l'on peut additionner et multiplier des congruences : si on a $a \equiv a' \bmod n$ et $b \equiv b' \bmod n$, alors $a + a' \equiv b + b' \bmod n$ et $aa' \equiv bb' \bmod n$. La notion d'anneau quotient, que nous verrons plus tard, donnera plus de recul sur cette construction. Chaque anneau A a un groupe additif sous-jacent $(A, +)$ par définition, mais aussi un groupe multiplicatif associé $(A^\times, \cdot)$:

DÉFINITION 1.18. *Si* A *est un anneau, on note* $A^\times$ *le groupe des inversibles du monoïde* $(A, \cdot)$. *Autrement dit, c'est l'ensemble* $A^\times = \{a \in A \mid \exists b \in A,\ ab = ba = 1\}$ *muni de la loi* $\cdot$ *de* A.

Les groupes multiplicatifs de l'Exemple 1.6 sont bien sûr des cas particuliers de ces constructions. Le groupe linéaire $\mathrm{GL}(V)$ est aussi le groupe des inversibles de l'anneau $(\mathrm{End}(V), +, \circ)$. Dans le même esprit :

EXEMPLE 1.19. (*Groupes de matrices*) Soient A un anneau et $n \geqslant 0$ un entier. L'ensemble $\mathrm{M}_n(A)$ des matrices carrées de taille n est un anneau pour les loi $+$ et $\cdot$ d'addition et multiplication des matrices. Le groupe des inversibles de $\mathrm{M}_n(A)$ est noté $\mathrm{GL}_n(A)$.

EXEMPLE 1.20. (Le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$). Les groupes $(\mathbb{Z}/n\mathbb{Z}, +)$ et $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ sont particulièrement importants, et il ne faut surtout pas les confondre. Le groupe $\mathbb{Z}/n\mathbb{Z}$ sera le modèle le plus simple de *groupe cyclique*. Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ est un groupe abélien fini intéressant en théorie des nombres, et sa structure sera déterminée plus tard dans ce chapitre.

DÉFINITION 1.21. *Un corps est un anneau* commutatif k *non nul dans lequel tout élément non nul est inversible, ou ce qui revient au même, vérifiant l'égalité ensembliste* $k^\times = k \smallsetminus \{0\}$.

C'est le cas de $\mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$, ou encore de $\mathbb{Z}/p\mathbb{Z}$ quand p est premier, car $\varphi(p) = p - 1$, mais pas de $\mathbb{Z}$ bien sûr. Lorsqu'on voit $\mathbb{Z}/p\mathbb{Z}$ comme on corps, on le note par ailleurs souvent $\mathbb{F}_p$ (pour *« field with p elements »*). Noter que la convention

francaise, adoptée ici, est de supposer que *les corps sont commutatifs* : ce n'est pas suivi par tous les auteurs. Si l'on enlève la commutativité dans la définition d'un corps, on obtient un *anneau à division*, ou *corps gauche* (*skew field* en anglais). C'est le cas par exemple de l'anneau des quaternions que nous rencontrerons plus tard.

FORMULAIRE DE CALCUL DANS LES GROUPES :

Soient x, y, z des éléments d'un groupe G, on vérifie aisément les propriétés de « calcul » suivantes :

$$x^{n+m} = x^n x^m, \quad \forall m, n \in \mathbb{Z} \quad (\textit{loi des puissances}) \tag{3a}$$

$$(xy)^{-1} = y^{-1}x^{-1} \quad (\textit{inverse d'un produit}) \tag{3b}$$

$$xy = xz \Rightarrow y = z \text{ et } yx = zx \Rightarrow y = z \quad (\textit{simplification}) \tag{3c}$$

$$xy = z \Rightarrow y = x^{-1}z \text{ et } xy = z \Rightarrow x = zy^{-1} \quad (\textit{bascule}) \tag{3d}$$

Vérifions maintenant, comme promis, que si X est un ensemble muni d'une loi de composition $\star$ associative, *i.e.* vérifiant $x \star (y \star z) = (x \star y) \star z$ pour tout $x, y, z \in X$, alors on peut multiplier dans un ordre donné, mais sans se soucier du parenthésage, un nombre fini quelconque d'éléments de X. On pose pour cela

$$x_1 \star x_2 \star \cdots \star x_n := x_1 \star (x_2 \star (\cdots \star (x_{n-1} \star x_n) \cdots)), \tag{4}$$

pour tout $n \geqslant 2$ et $x_1, \ldots, x_n \in X$. On a donc $x_1 \star x_2 \star \cdots \star x_n = x_1 \star (x_2 \star \cdots \star x_n)$ pour $n \geqslant 3$. Tout produit "dans l'ordre" des x_i effectué avec un certain parenthésage est, dans sa dernière étape, de la forme $a(x_1, \ldots, x_k) \star b(x_{k+1}, \ldots, x_n)$ pour un certain entier $1 \leqslant k < n$, avec a (resp. b) un certain produit "dans l'ordre" des éléments x_i avec $i \leqslant k$ (resp. $i > k$). En raisonnant par récurrence sur n, on a $a(x_1, \ldots, x_k) = x_1 \star \cdots \star x_k$ et $b(x_{k+1}, \ldots, x_n) = x_{k+1} \star \cdots \star x_n$, de sorte qu'il suffit de démontrer :

LEMME 1.22. *Si $\star$ est un loi associative sur X, alors pour tous entiers $1 \leqslant k < n$, et tout $x_1, \ldots, x_n$ dans X, on a $(x_1 \star \cdots \star x_k) \star (x_{k+1} \star \cdots \star x_n) = x_1 \star \cdots \star x_n$.*

DÉMONSTRATION — On raisonne par récurrence sur n. Pour $k = 1$ c'est vrai par définition (Formule (4)). Sinon, on a $k \geqslant 2$, et on pose $u = x_2 \star \cdots \star x_k$ et $v = x_{k+1} \star \cdots \star x_n$. On a alors $(x_1 \star u) \star v = x_1 \star (u \star v)$ par associativité, et $u \star v = x_2 \star \cdots \star x_n$ par hypothèse de récurrence, ce qui nous ramène au cas $k = 1$. □

2. Isomorphismes et morphismes

La notion de morphisme est celle qui va nous permettre de mettre de l'ordre dans la multitude des exemples précédents, par exemple de comparer ou d'identifier des groupes définis de manière très différentes. Remarquons que la notion de *bijection* entre deux groupes a peu de pertinence, car les lois de deux groupes en bijection n'ont *a priori* aucun rapport. À la place, nous souhaitons considérer que deux groupes G et G' sont équivalents, on dira plutôt *isomorphes*, s'il y a une manière d'identifier les éléments de G et G', via une bijection $x \leftrightarrow x'$, de sorte que les produits se correspondent aussi : on veut $(xy)' = x'y'$ pour tout $x, y \in G$. Autrement dit, posant $f(x) = x'$, on veut $f(xy) = f(x)f(y)$. Cela conduit à la notion suivante :

Définition 2.1. *Soient G et G' deux groupes et $f : G \to G'$ une application. On dit que f est un* morphisme *(ou* homomorphisme*) de groupes si $f(xy) = f(x)f(y)$ pour tout $x, y \in G$. On dit que f est un isomorphisme si en outre f est bijective.*

Exemple 2.2. *Pour $n \geqslant 1$, l'application $\mathbb{Z}/n\mathbb{Z} \to \mu_n, \overline{k} \mapsto e^{2ik\pi/n}$, est bien définie, et c'est un isomorphisme de groupes.*

On dira souvent simplement « Soit $f : G \to G'$ un morphisme de groupes » à la place de « Soient G et G' des groupes et $f : G \to G'$ un morphisme de groupes ».

Définition 2.3. *Soient G et G' deux groupes. On dit que G est isomorphe à G', et on note $G \simeq G'$, s'il existe un isomorphisme de groupes $G \to G'$.*

On a manifestement $G \simeq G$: id_G est un isomorphisme de groupes. De plus, si $f : G \to G'$ est un isomorphisme de groupes, la bijection inverse $f^{-1} : G' \to G$ est également un morphisme de groupes (et donc un isomorphisme). En effet, pour tout $x', y' \in G'$, si l'on pose $x = f^{-1}(x')$ et $y = f^{-1}(y')$, on a

$$f^{-1}(x'y') = f^{-1}(f(x)f(y)) = f^{-1}f(xy) = xy = f^{-1}(x')f^{-1}(y').$$

On a donc $G \simeq G' \Rightarrow G' \simeq G$. Enfin, observons que l'on peut composer les morphismes : si $f : G \to G'$ et $f' : G' \to G''$ sont des morphisme de groupes, il en va de même de $f' \circ f : G \to G''$. Si $f : G \to G'$ et $f' : G' \to G''$ sont en outre des isomorphismes, il en va de même de $f' \circ f$, et donc G est isomorphe à G''. On a donc $G \simeq G'$ et $G' \simeq G'' \Rightarrow G \simeq G''$. On a montré que la relation d'isomorphie est une relation d'équivalence sur la classe des groupes (attention, les groupes ne forment pas un ensemble !). On peut donc parler sans ambages de *groupes isomorphes*.

Remarque 2.4. *(i)* (*Groupe trivial*) Un groupe est toujours non vide : on a $1 \in G$. Le *groupe trivial* est le groupe $G = \{1\}$ muni de la loi $1 \cdot 1 = 1$ (unique loi possible). On le note simplement 1. À isomorphisme près, c'est l'unique groupe d'ordre 1.

(ii) *(Groupes d'ordre 2)* Un groupe G d'ordre 2 est de la forme $\{1, g\}$ avec $g \neq 1$ et $g^2 = 1$, car $g^2 = g$ entraîne $g = 1$. La bijection $\mu_2 \to G$, $1 \mapsto 1$ et $-1 \mapsto g$ est manifestement un isomorphisme de groupes. Il existe donc aussi un unique groupe d'ordre 2 à isomorphisme près, à savoir $\mu_2 \simeq \mathbb{Z}/2\mathbb{Z}$. On verra très vite que plus généralement, pour p premier il existe un unique groupe d'ordre p à isomorphisme près, à savoir $\mathbb{Z}/p\mathbb{Z}$.

(iii) (Klein Vieregruppe) C'est le groupe $\mathrm{V} = \mu_2 \times \mu_2$, d'ordre 4. Il n'est pas isomorphe à μ_4 (ou donc à $\mathbb{Z}/4\mathbb{Z}$). En effet, on constate que l'on a $x^2 = 1$ pour tout $x \in \mathrm{V}$. Ainsi, si $\varphi : \mathrm{V} \to \mu_4$ est un morphisme de groupes, on a $\varphi(x)^2 = \varphi(x^2) = \varphi(1) = 1$ pour tout $x \in \mathrm{V}$ et donc $i \notin \varphi(\mathrm{V})$. Il y a donc au moins 2 groupes d'ordre 4 non isomorphes (en fait, il y en a exactement 2).

Un des fils conducteurs du cours, et qui nous permettra de jauger notre érudition en théorie des groupes, est la problématique naturelle suivante :

Problème 2.1. *Étant donné un entier $n \geqslant 1$, peut-on classifier à isomorphisme près les groupes d'ordre n ?*

C'est une question qui s'avèrera assez inextricable en général. Nous verrons toutefois comment la résoudre pour des valeurs petites ou particulières de n, et comment la

stratégie de *dévissage* en groupes dit *simples* permet de l'attaquer. Contentons-nous ici d'observer qu'il n'y a qu'un nombre fini de telles classes d'isomorphismes pour n donné. En effet, d'après la remarque qui suit (transport de structure !), tout groupe d'ordre n est isomorphe à un groupe dont l'ensemble sous-jacent est $\{1, \ldots, n\}$, et qu'il n'y a qu'un nombre fini de lois de composition sur un ensemble fini (exactement n^{n^2} sur $\{1, \ldots, n\}$, et bien sûr la plupart d'entre elles ne sont pas des lois de groupe).

Remarque 2.5. (Transport de structure) *Soient G un groupe, X un ensemble et $\varphi : X \to G$ une bijection. Il existe une unique loi de groupe $\star$ sur X telle que φ soit un isomorphisme de groupes, à savoir $x \star y = \varphi^{-1}(\varphi(x)\varphi(y))$. La vérification est immédiate !* Suivant Bourbaki, on dit que la loi $\star$ est *déduite de celle de G par transport de structure via φ*. Autrement dit, on a simplement indexé les éléments de X par les éléments de G, disons $x_g = \varphi^{-1}(g)$, et posé $x_g \star x_h = x_{gh}$. Par ce procédé, tout ensemble peut être muni d'une loi de groupe. En effet, si X est fini à n éléments, toute bijection $X \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z}$ munit X d'une loi de groupe (isomorphe à $\mathbb{Z}/n\mathbb{Z}$!) par transport de structure. De même, si X est infini, alors X est en bijection avec $(\mathbb{Z}/2\mathbb{Z})^{(X)}$ (Exercice 1.16 Chap. 1) et on peut donc transporter à X la loi de ce dernier. Ces lois étant arbitraires, elles ont toutefois peu d'intérêt en général.

Il existe en général plusieurs isomorphismes différents entre deux groupes isomorphes. Pour de nombreuses questions le choix importera peu, mais pas pour toutes. Si $f : G \to G'$ est un isomorphisme, tous les autres tels isomorphismes sont de la forme $f' = g \circ f$ où $g = f' \circ f^{-1}$ est un isomorphisme $G' \to G'$. Cela conduit à introduire la :

Définition 2.6. *Si G est un groupe, un automorphisme de G est un isomorphisme $G \to G$. L'ensemble de tous les automorphismes de G est un sous-groupe de S_G noté $\operatorname{Aut} G$.*

Exemple 2.7. *Si $g \in G$, l'application $\mathrm{int}_g : G \to G, x \mapsto gxg^{-1}$, est un automorphisme appelé automorphisme intérieur associé à g, ou conjugaison par g.*

Même si de prime abord la notion d'isomorphisme a l'air plus importante que celle de morphisme, c'est cette dernière qui s'avère à l'usage la plus cruciale. Par exemple, pour montrer que deux groupes sont isomorphes, on définira souvent d'abord un morphisme entre les deux, et on essaiera ensuite de montrer qu'il est bijectif.

Notons que si $f : G \to G'$ est un morphisme, alors on a $f(1) = 1$ car $f(1) = f(1^2) = f(1)f(1)$. De plus, pour tout $x \in G$ on a $f(x^{-1}) = f(x)^{-1}$, car $1 = f(1) = f(xx^{-1}) = f(x)f(x^{-1})$, et plus généralement $f(x^n) = f(x)^n$ pour tout $n \in \mathbb{Z}$.

Exemple 2.8. Pour $n \geqslant 2$, la signature d'une permutation définit un morphisme de groupes surjectif $\epsilon : \mathrm{S}_n \to \{\pm 1\}$ (nous le reverrons plus loin). Si V est un k-espace vectoriel de dimension finie non nul, le déterminant définit un morphisme surjectif $\det : \mathrm{GL}(V) \to k^\times$.

On note $\mathrm{Hom}(G, G')$ l'ensemble des morphismes de groupes de $G \to G'$. Il contient toujours au moins le *morphisme trivial* 1, envoyant tout $g \in G$ sur $1_{G'}$. Attention : il n'y a pas de loi de groupe naturelle sur $\mathrm{Hom}(G, G')$ en général, sauf si G' est abélien. Dans ce cas, on définit une loi de groupe sur $\mathrm{Hom}(G, G')$, $(f, f') \mapsto ff'$, en posant $(ff')(g) = f(g)f'(g)$ pour $g \in G$.

Il y a des liens forts entre sous-groupes et morphismes. Si $f : G \to G'$ est un morphisme de groupes, son *noyau* est défini par

$$\ker f = f^{-1}(\{1\}) = \{g \in G \mid f(g) = 1\}.$$

C'est manifestement un sous-groupe de G. Par exemple, le noyau de $\mathrm{GL}(V) \xrightarrow{\det} k^\times$ est un sous-groupe de $\mathrm{GL}(V)$ noté $\mathrm{SL}(V)$ et appelé *groupe spécial linéaire* de V. De même $\mathrm{Im} f = f(G)$ est un sous-groupe de G'. Plus généralement, on a :

Proposition 2.9. *Soit $f : G \to G'$ un morphisme de groupes. Si H est un sous-groupe de G alors $f(H)$ est un sous-groupe de G'. Si H' est un sous-groupe de G' alors $f^{-1}(H')$ est un sous-groupe de G.*

Démonstration — Découle immédiatement des définitions et des identités $f(1) = 1$, $f(xy) = f(x)f(y)$ et $f(x^{-1}) = f(x)^{-1}$ pour $x, y \in G$. □

L'énoncé suivant est simple mais important.

Proposition 2.10. *Soit $f : G \to G'$ un morphisme de groupes. Notons $\mathscr{A}$ l'ensemble des sous-groupes de G contenant* $\ker f$*, et $\mathscr{B}$ celui des sous-groupes de G' inclus dans* $\mathrm{Im}\, f$*, tous deux ordonnés par l'inclusion $\subset$. Alors les applications $\mathscr{A} \to \mathscr{B}, A \mapsto f(A)$, et $\mathscr{B} \to \mathscr{A}, B \mapsto f^{-1}(B)$, sont des bijections croissantes réciproques.*

Démonstration — Noter que pour tout sous-ensemble $H \subset G$ on a $f(H) \subset f(G) = \mathrm{Im}\, f$, et pour H' sous-groupe de G' on a $\ker f = f^{-1}(\{1\}) \subset f^{-1}(H')$: les applications du (iii) sont bien définies. Le fait qu'elles soient croissantes viennent des faits généraux $f(X) \subset f(Y)$ pour toutes parties $X \subset Y$ de G, et $f^{-1}(X') \subset f^{-1}(Y')$ pour toutes parties $X' \subset Y'$ de G'.

Pour toute partie $H' \subset \mathrm{Im}\, f$, on a trivialement $f(f^{-1}(H')) = H'$. Il ne reste donc qu'à montrer que pour tout sous-groupe H de G contenant $\ker f$, on a $f^{-1}(f(H)) = H$. L'inclusion $H \subset f^{-1}(f(H))$ est encore évidente. Réciproquement, soit $g \in f^{-1}(f(H))$. On a $f(g) \in f(H)$, donc $f(g) = f(h)$ pour un certain $h \in H$, puis $f(gh^{-1}) = 1$ et donc $gh^{-1} = k$ avec $k \in \ker f$. On en déduit $g = kh \in H$ car H est un sous-groupe de G contenant $\ker f$. On a montré $H = f^{-1}(f(H))$. □

Nous appliquerons souvent ce résultat dans le cas où f est surjective, auquel cas $\mathscr{B}$ est l'ensemble de tous les sous-groupes de G'. Un second énoncé important est :

Proposition 2.11. *Soit $f : G \to G'$ un morphisme de groupes. Alors les fibres non vides de f sont en bijection avec* $\ker f$*. En particulier :*

(i) f est injective si, et seulement si, on a $\ker f = \{1\}$.

(ii) si G est fini, on a $|G| = |\mathrm{Im}\, f|\, |\ker f|$.

Démonstration — Soit $g \in G$. L'application $\mathrm{L}_g : G \mapsto G, x \mapsto gx$, est bijective, d'inverse $\mathrm{L}_{g^{-1}}$. Comme f est un morphisme de groupes, L_g et $\mathrm{L}_{g^{-1}}$ induisent des bijections réciproques entre $\ker f = f^{-1}(\{1\})$ et $f^{-1}(\{h\})$, où $h = f(g)$. Cela montre la première assertion. Le (i) et (ii) s'en déduisent. □

Remarque 2.12. *Tout morphisme injectif $f : G \to G'$ définit un isomorphisme de groupes $f : G \xrightarrow{\sim} f(G)$.*

En guise d'application des concepts de ce paragraphe, montrons le résultat suivant dû à Cayley.

Proposition 2.13. *(Cayley) Tout groupe d'ordre fini n est isomorphe à un sous-groupe de S_n.*

Cela démontre d'une part le rôle central du groupe S_n en théorie des groupes finis, mais aussi toute la difficulté à classifier les sous-groupes de S_n en général.

Démonstration — Pour $g \in G$ notons $\mathrm{L}_g : G \to G, x \mapsto gx$, la multiplication à gauche par g. C'est une bijection de G d'inverse $\mathrm{L}_{g^{-1}}$. De plus, on a $\mathrm{L}_g \circ \mathrm{L}_h = \mathrm{L}_{gh}$, autrement dit l'application $G \to \mathrm{S}_G, g \mapsto \mathrm{L}_g$, est un morphisme de groupes. Il est injectif, car $\mathrm{L}_g = \mathrm{id}_G$ entraîne $g = 1$ (prendre $x = 1$). C'est donc un isomorphisme sur son image (Remarque 2.12), qui est un sous-groupe de S_G. On conclut par le lemme général suivant, appliqué à une bijection $\{1, \ldots, n\} \to G$ (autrement dit, à une numérotation des éléments de G). □

Lemme 2.14. *Soit $\varphi : X \to Y$ une bijection. Alors l'application $\varphi_{X,Y} : \mathrm{S}_X \to \mathrm{S}_Y, \sigma \mapsto \varphi \circ \sigma \circ \varphi^{-1}$, est un isomorphisme de groupes.*

Démonstration — On vérifie immédiatement que $\varphi_{X,Y}$ est un morphisme, ainsi que les égalités $\varphi_{X,Y} \circ (\varphi^{-1})_{Y,X} = \mathrm{id}_Y$ et donc $(\varphi^{-1})_{Y,X} \circ \varphi_{X,Y} = \mathrm{id}_X$ (par symétrie). □

On dispose de définitions naturelles de morphismes entre d'autres structures que les groupes. Un *morphisme de monoïdes* est une application $f : X \to Y$, avec X et Y des monoïdes, telle que $f(xy) = f(x)f(y)$ pour tout $x, y \in X$, et $f(1) = 1$.

Définition 2.15. *Un morphisme d'anneaux est une application $f : A \to B$, avec A et B des anneaux, qui est à la fois un morphisme de groupes additifs et de monoïdes multiplicatifs : pour tout $a, b \in A$ on a $f(a + b) = f(a) + f(b)$, $f(1) = 1$ et $f(ab) = f(a)f(b)$.*

Dans les deux cas, un isomorphisme est un morphisme bijectif (auquel cas, son inverse est également un morphisme). Tout (iso-)morphisme d'anneaux $A \to B$ induit un (iso-)morphisme de groupes $A^\times \to B^\times$. Plus généralement :

Exemple 2.16. Tout morphisme d'anneaux $f : A \to B$ induit un morphisme d'anneaux $\mathrm{M}_n(A) \to \mathrm{M}_n(B), (m_{i,j}) \mapsto (f(m_{i,j}))$, et donc un morphisme de groupes $\mathrm{GL}_n(A) \to \mathrm{GL}_n(B)$. Par exemple, le morphisme d'anneaux $\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}, k \mapsto \overline{k}$, induit un morphisme de groupes $\mathrm{GL}_n(\mathbb{Z}) \to \mathrm{GL}_n(\mathbb{Z}/N\mathbb{Z})$ (réduction modulo N).

Exemple 2.17. Si V est un k-espace vectoriel de dimension finie, et si l'on se donne une k-base $e = (e_1, \ldots, e_n)$ de V, alors l'application $u \mapsto \mathrm{Mat}_e(u)$ (matrice associée) induit un isomorphisme d'anneaux $\mathrm{End}(V) \xrightarrow{\sim} \mathrm{M}_n(k)$, et donc un isomorphisme de groupes $\mathrm{GL}(V) \xrightarrow{\sim} \mathrm{GL}_n(k)$.

3. Groupes cycliques et monogènes

Soient G un groupe et $g \in G$. On s'intéresse au sous-groupe de G

$$\langle g \rangle := \{g^m \mid m \in \mathbb{Z}\}$$

engendré par g. Quand la loi de G est notée additivement, ce sous-groupe est aussi noté $\mathbb{Z}\, g = \{mg | \, m \in \mathbb{Z}\}$. Rappelons d'abord la classique : [4]

PROPOSITION 3.1. *Les sous-groupes de $\mathbb{Z}$ sont les $\mathbb{Z}n$ avec $n \in \mathbb{Z}$.*

DÉMONSTRATION — Soit H un sous-groupe de $\mathbb{Z}$. On peut supposer $H \neq \{0\}$, car $\{0\} = \mathbb{Z}\, 0$. L'ensemble $A = H \cap \mathbb{N}_{>0}$ est alors non vide (considérer $h \mapsto -h$), et possède donc un plus petit élément, que l'on note n. On a clairement $\mathbb{Z}n \subset H$. Soit $h \in H$. Par division euclidienne on a $h = an + b$ avec $a, b \in \mathbb{Z}$ et $0 \leqslant b < n$, mézalor $b = h - an \in H$ car H est un sous-groupe, donc $b = 0$ par minimalité de n, *i.e.* $h \in \mathbb{Z}n$. □

Soient G un groupe et $g \in G$. Considérons l'application

$$\varphi : \mathbb{Z} \to \langle g \rangle, \;\; m \mapsto g^m. \tag{5}$$

On constate que c'est un morphisme de groupe surjectif. Deux cas se présentent :

(Cas a) Soit φ est injectif, *i.e.* tous les éléments g^m, avec $m \in \mathbb{Z}$, sont distincts. On dit alors que g est *d'ordre infini*. Dans ce cas φ définit un isomorphisme $\mathbb{Z} \simeq \langle g \rangle$.

(Cas b) Soit φ n'est pas injectif. Dans ce cas, son noyau $\ker \varphi$ est un sous-groupe non $\{0\}$ de $\mathbb{Z}$, donc de la forme $n\mathbb{Z}$ pour un unique $n \geqslant 1$ par la Proposition 3.1. On dit alors que g est d'ordre fini, et l'entier n est appellé *ordre de g*, et parfois noté $\mathrm{ord}(g)$ ou $|g|$. Par construction, c'est le plus petit entier $m \geqslant 1$ vérifiant $g^m = 1$. Pour tout $m \in \mathbb{Z}$, on a aussi $g^m = 1 \Leftrightarrow n|m$.

PROPOSITION 3.2. *Soit $g \in G$ d'ordre fini n, alors $\langle g \rangle$ a exactement n éléments, à savoir $1, g, \ldots, g^{n-1}$, et on a un isomorphisme de groupes $\mathbb{Z}/n\mathbb{Z} \to \langle g \rangle, \overline{m} \to g^m$.*

DÉMONSTRATION — La relation $g^n = 1$ entraîne $g^m \equiv g^{m'}$ pour $m \equiv m' \bmod n$. D'après la Proposition 2.1 Chap. 1, φ définit donc par passage au quotient une application $\overline{\varphi} : \mathbb{Z}/n\mathbb{Z} \to \langle g \rangle, \overline{m} \mapsto g^m$: c'est l'application de l'énoncé. Par définition de la loi de groupe sur $\mathbb{Z}/n\mathbb{Z}$, on constate que $\overline{\varphi}$ est un morphisme de groupes. Il est clairement surjectif. Mais son noyau est trivial car $g^m = 1$ équivaut à $\overline{m} = \overline{0}$ par le premier point : c'est donc un isomorphisme. Comme $\mathbb{Z}/n\mathbb{Z}$ admet pour représentants $\{0, 1, \ldots n-1\}$ (division euclidienne par n), on en déduit que $\langle g \rangle$ a exactement n éléments, à savoir les g^r pour $0 \leqslant r < n$. □

DÉFINITION 3.3. *Un groupe G est dit monogène s'il existe $g \in G$ avec $G = \langle g \rangle$. Un tel élément g est appelé générateur de G. On dit que G est cyclique s'il est monogène et fini.*

4. On préfère souvent la notation $n\mathbb{Z}$ pour $\mathbb{Z}n$. La seconde est pourtant plus naturelle du point de vue groupe, car on a $\langle n \rangle = \mathbb{Z}n$.

Par exemple, le groupe $\mathbb{Z}$ (additif) est monogène infini engendré par l'élément 1. De même, pour tout entier $n \geqslant 1$, le groupe μ_n (resp. $\mathbb{Z}/n\mathbb{Z}$) est cyclique d'ordre n engendré par $e^{2i\pi/n}$ (resp. $\overline{1}$). À isomorphisme près, les cas (a) et (b) ci-dessus montrent que ce sont les seules possibilités.

Corollaire 3.4. *Un groupe G est monogène infini si, et seulement si, on a $G \simeq \mathbb{Z}$. Un groupe G est cyclique d'ordre $n \geqslant 1$ si, et seulement si, on a $G \simeq \mathbb{Z}/n\mathbb{Z}$.*

Dans les deux cas, l'isomorphisme construit fait correspondre au générateur g (arbitrairement choisi) de G le générateur fixe 1 (resp. $\overline{1}$) de $\mathbb{Z}$ (resp. $\mathbb{Z}/n\mathbb{Z}$). On a montré en particulier qu'il existe, à isomorphisme près, un unique groupe cyclique d'ordre n. Certains auteurs notent C_n un groupe cyclique arbitraire d'ordre n. En notation additive, il y a presque toujours intérêt à avoir en tête $\mathrm{C}_n = \mathbb{Z}/n\mathbb{Z}$. En notation multiplicative, et suivant les goûts, choisir $\mathrm{C}_n = \mu_n$ permet d'éviter parfois les confusions.[5]

Les générateurs du groupe $\mathbb{Z}$ sont les $k \in \mathbb{Z}$ tels que $\mathbb{Z}k = \mathbb{Z}$, *i.e.* $k = \pm 1$. Décrivons tous ceux d'un groupe cyclique d'ordre n, disons engendré par un élément g donné. Pour $k \in \mathbb{Z}$, on a les équivalences :

(a) l'élément g^k engendre G,

(b) le sous-groupe $\langle g^k \rangle \subset G$ contient g,

(c) il existe $k' \in \mathbb{Z}$ tel que $kk' \equiv 1 \bmod n$,

(d) $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

(e) k et n sont premiers entre eux.

Seule l'équivalence (c) $\Leftrightarrow$ (e) n'est pas tautologique, mais c'est le théorème de Bezout. Par exemple, les générateurs de μ_n sont les racines *primitives* n-èmes de l'unité.

Corollaire 3.5. *Un groupe cyclique d'ordre n a exactement $\varphi(n)$ générateurs.*

Lemme 3.6. *Si $g \in G$ est d'ordre fini n, et si $d \geqslant 1$, alors g^d est d'ordre fini égal à $\frac{n}{(n,d)}$. En particulier, si d divise n alors g^d est d'ordre n/d.*

Démonstration — En effet, pour $k \in \mathbb{Z}$ on a

$$(g^d)^k = g^{dk} = 1 \;\Leftrightarrow\; n \,|\, dk \;\Leftrightarrow\; \frac{n}{(n,d)} \,|\, \frac{d}{(n,d)}k \;\Leftrightarrow\; \frac{n}{(n,d)} \,|\, k. \tag{6}$$

La dernière équivalence vient de ce que $\frac{n}{(n,d)}$ et $\frac{d}{(n,d)}$ sont premiers entre eux. □

Terminons par une description des sous-groupes d'un groupe cyclique. Si G est un groupe abélien, et pour $d \in \mathbb{Z}$, l'application $G \to G, x \mapsto x^d$, est un morphisme. Son image $G^{(d)} = \{x^d,\ x \in G\}$ est donc un sous-groupe (*puissances d-èmes*, c'est aussi $dG = \{dx,\ x \in G\}$ en loi additive). Son noyau est souvent noté $G[d] := \{g \in G \,|\, g^d = 1\}$ et appelé sous-groupe de *d-torsion* de G.

Lemme 3.7. *Soient $G = \langle g \rangle$ cyclique d'ordre n et $d \geqslant 1$ entier. Le sous-groupe $G^{(d)} = \langle\, g^d \,\rangle$ est cyclique d'ordre $n/(n,d)$, et on a $G[d] = \langle\, g^{n/(n,d)} \,\rangle = G^{(n/(n,d))}$.*

5. Une source potentielle de confusions est que $\mathbb{Z}/n\mathbb{Z}$ est muni d'une addition et d'une multiplication.

Démonstration — En effet, on a $G^{(d)} = \langle g^d \rangle$, et le Lemme 3.6 montre que g^d est d'ordre $n/(n,d)$. De plus, tout élément de G est de la forme g^k avec $k \in \mathbb{Z}$, et (6) montre que l'on a $(g^k)^d = 1 \iff \frac{n}{(n,d)} \mid k$. On a bien montré $G[d] = \langle g^{n/(n,d)} \rangle$. □

Proposition 3.8. *Soit G un groupe cyclique d'ordre n. L'application $d \mapsto G^{(d)}$ est une bijection de l'ensemble des diviseurs de n sur l'ensemble des sous-groupes de G, et pour deux diviseurs d, d' de n on a $d|d' \Leftrightarrow G^{(d)} \supset G^{(d')}$.*

En particulier, tout sous-groupe d'un groupe cyclique est cyclique, et uniquement déterminé par son ordre, car on a $|G^{(d)}| = n/d$ pour $d|n$.

Démonstration — Soit g un générateur de G. On applique la Proposition 2.10 (iii) au morphisme surjectif $\varphi : \mathbb{Z} \to G, m \mapsto g^m$, de noyau $n\mathbb{Z}$. Les sous-groupes de $\mathbb{Z}$ contenant $n\mathbb{Z}$ sont les $d\mathbb{Z}$ avec $n \in d\mathbb{Z}$, *i.e.* $d|n$. On conclut car on a $\varphi(d\mathbb{Z}) = \langle g^d \rangle = G^{(d)}$ et $d\mathbb{Z} \subset d'\mathbb{Z} \Leftrightarrow d'|d$. □

Décrivons maintenant les automorphismes d'un groupe cyclique.

Proposition 3.9. *Soit G un groupe cyclique d'ordre $n \geqslant 1$. Les automorphismes de G sont les $\varphi_k : g \mapsto g^k$, avec $k \in (\mathbb{Z}/n\mathbb{Z})^\times$. De plus, l'application $(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(G), k \mapsto \varphi_k$, est un isomorphisme de groupes.*

Démonstration — Pour tout $k \in \mathbb{Z}/n\mathbb{Z}$, l'application $\varphi_k : G \to G, g \mapsto g^k$, est bien définie car on a $g^n = 1$ pour tout $g \in G$. C'est clairement un morphisme de groupes. On a $\varphi_{kk'} = \varphi_k \circ \varphi_{k'}$ et $\varphi_1 = \mathrm{id}$: cela montre à la fois que φ_k est un isomorphisme pour $k \in (\mathbb{Z}/n\mathbb{Z})^\times$, et que l'application $\varphi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(G), k \mapsto \varphi_k$, est un morphisme de groupes. Pour voir que φ est bijectif on fixe un générateur g_0 de G. On a $\varphi_k(g_0) = g_0^k$, et donc $g_0^k = g_0$ implique $k \equiv 1$ dans $\mathbb{Z}/n\mathbb{Z}$ car g_0 est d'ordre n, donc φ est injectif. Soit α un automorphisme quelconque de G. Il envoie le générateur g_0 sur un autre générateur, nécessairement de la forme g_0^k avec $k \in (\mathbb{Z}/n\mathbb{Z})^\times$ par l'analyse ci-dessus. On a donc $\alpha(g_0) = \varphi_k(g_0)$, puis $\alpha = \varphi_k$ car g_0 engendre G. □

Terminons ce paragraphe par un rappel sur l'isomorphisme chinois des restes. Rappelons que si A et B sont deux anneaux, on dispose d'une structure d'anneau naturelle sur $A \times B$ appelé *anneau produit* : l'addition et la multiplication sont effectuées coordonnée par coordonnée, et le neutre multiplicatif est $(1,1)$.

Proposition 3.10. *(Isomorphisme chinois) Soient $m, n \in \mathbb{Z}$ premiers entre eux. L'application $\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$, $k \mapsto (k \bmod n, k \bmod m)$ définit par passage au quotient un isomorphisme d'anneaux $\mathbb{Z}/mn\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.*

Démonstration — Si on a $k \equiv k' \bmod mn$ alors $k \equiv k' \bmod n$ et $k \equiv k' \bmod m$: donc l'application de l'énoncé passe bien au quotient, et induit une application $f : \mathbb{Z}/mn\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, $\overline{k} \mapsto (\overline{k}, \overline{k})$ pour tout $k \in \mathbb{Z}$. Ce f est trivialement un morphisme d'anneaux. Si $\overline{k}$ est dans $\ker f$, on a $m|k$ et $n|k$, et donc $mn|k$ car m et n sont premiers entre eux, *i.e.* $\overline{k} = 0$. Ainsi, f est injective, puis bijective car sa source et son but ont même cardinal mn : c'est un isomorphisme. □

L'isomorphisme chinois est en particulier un isomorphisme de groupes additifs. Comme le groupe des inversibles de l'anneau produit $A \times B$ est le groupe produit $A^\times \times B^\times$. On en déduit aussi :

COROLLAIRE 3.11. *Soient $m, n \in \mathbb{Z}$ premiers entre eux. L'isomorphisme chinois induit des isomorphismes de groupes $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ et $(\mathbb{Z}/mn\mathbb{Z})^\times \xrightarrow{\sim} (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$. En particulier, on a $\varphi(mn) = \varphi(m)\varphi(n)$.*

4. Le théorème de Lagrange

Si A et B sont des parties d'un groupe G, on pose

$$AB = \{ab \mid a \in A,\, b \in B\} \subset G.$$

L'application $(A, B) \mapsto AB$ définit une loi de composition sur $\mathrm{P}(G)$, nous la noterons aussi $\bullet$. Elle est associative par associativité de la loi de G : on a $(AB)C = A(BC)$ pour tout $A, B, C \subset G$. Si $A_1, \ldots, A_n$ sont des $n \geqslant 1$ parties de G on a alors

$$A_1 A_2 \cdots A_n = \{a_1 a_2 \ldots a_n | a_i \in A_i \ \forall i = 1, \ldots, n\}.$$

Si $A = \{a\}$ est un singleton, on note aussi aB pour $\{a\}B$. La loi $\bullet$ sur $\mathrm{P}(G)$ admet manifestement pour élément neutre $\{1\}$, donc $(\mathrm{P}(G), \bullet)$ est un monoïde ! En revanche, ce n'est pas un groupe : pour $A \subset G$ on a $GA = AG = G$ si $A \neq \varnothing$, et $\varnothing A = A\varnothing = \varnothing$. Pour $A \subset G$, on pose néanmoins $A^{-1} = \{a^{-1} \mid a \in A\}$. On prendra garde qu'en général A^{-1} n'est pas un inverse de A pour $\bullet$ (*i.e.* $AA^{-1} \neq \{1\}$), contrairement aux conventions usuelles. On a en revanche les égalités $(AB)^{-1} = B^{-1}A^{-1}$ et $(A^{-1})^{-1} = A$.

LEMME 4.1. *Une partie H d'un groupe G un sous-groupe si, et seulement si, on a $H \neq \varnothing$, $HH = H$ et $H^{-1} = H$.*

DÉMONSTRATION — Supposons que H est un sous-groupe de G. On a $1 \in H$, donc $H \neq \varnothing$. On a $HH \subset H$, et aussi $H \subset HH$ en écrivant $h = 1\,h$, d'où $HH = H$. On a enfin $H^{-1} \subset H$, puis $H = (H^{-1})^{-1} \subset H^{-1}$, et donc $H = H^{-1}$. Réciproquement, un H comme dans l'énoncé est un sous-groupe : il ne manque que $1 \in H$, mais l'existence d'un élément $h_0 \in H$ entraîne bien $1 = h_0 h_0^{-1} \in HH^{-1} = HH = H$. □

DÉFINITION 4.2. *Soient G un groupe et H un sous-groupe. Une* classe à gauche *(resp.* à droite*) de H dans G est une partie de la forme gH (resp. Hg) pour un certain $g \in H$.*

L'involution $x \mapsto x^{-1}$ de G échange gH et Hg^{-1}, et induit une involution naturelle entre classes à gauche et classes à droite. Pour fixer les idées on se focalise sur les classes à gauche. On définit une relation $\sim_H$ sur G en posant

$$g \sim_H g' \ \Leftrightarrow\ \exists h \in H,\ g' = gh \ \Leftrightarrow\ g' \in gH.$$

C'est une relation déquivalence sur G : on a $g = g1$ avec $1 \in H$, $g' = gh$ avec $h \in H$ implique $g = g'h^{-1}$ avec $h^{-1} \in H$, et enfin $g' = gh$ et $g'' = g'h'$ avec $h, h' \in H$ entraîne $g'' = ghh'$ avec $hh' \in H$. Par définition, la classe d'équivalence de $g \in G$ pour $\sim_H$ est gH. Ainsi, les classes à gauche forment une partition de G (et deux classes à gauches sont soit disjointes, soit égales).

Définition 4.3. *On note G/H l'ensemble quotient de $\sim_H$. Autrement dit, G/H est le sous-ensemble de $\mathrm{P}(G)$ constitué des classes à gauche de H dans G. On appelle* indice *de H dans G le cardinal (fini ou infini) de G/H, et on le note $[G : H]$*

Remarque 4.4. On a une histoire parallèlle pour la relation d'équivalence $g \simeq_H g' \Leftrightarrow g' \in Hg$ ($\Leftrightarrow g^{-1} \sim_H (g')^{-1}$). On note $H\backslash G$ l'ensemble quotient de $\simeq_H$, constitué des classes à droite de H dans G, et on peut définir un indice à droite $[H : G] = |H\backslash G|$. Mais cet indice coïncide avec $[G : H]$ à cause de la bijection $A \mapsto A^{-1}$ entre classes à droite et classes à gauche.

Théorème 4.5. *(Lagrange) Soient G un groupe fini et H un sous-groupe de G. On a $|G| = |H|\ [G : H]$. En particulier, $|H|$ divise $|G|$.*

Démonstration — Soient $g_1, g_2, \ldots, g_n \in G$ des représentants de classes d'équivalence de $\sim_H$, avec $n = |G/H|$. On a $G = \coprod_{i=1}^n g_i H$ (Proposition 1.4 Chap. 1). Il reste qu'à voir que pour tout $g \in G$ on a $|H| = |gH|$. Mais la multiplication à gauche par g induit une bijection $H \to gH, h \mapsto gh$, de bijection réciproque $gH \to H, x \mapsto g^{-1}x$. On a donc $|H| = |gH|$, puis $|G| = \sum_{i=1}^n |g_i H| = n|H|$ avec $n = |G/H|$. □

Corollaire 4.6. *Si G est un groupe fini, et si $g \in G$, alors $g^{|G|} = 1$. Autrement dit, on a $\operatorname{ord} g \mid |G|$.*

En effet, l'ordre d de g satisfait $d = |\langle g \rangle|$ (Proposition 3.2). Par exemple, appliqué au groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ avec p premier, cela montre $n^{p-1} \equiv 1 \bmod p$ pour tout $n \in \mathbb{Z}$ premier à p, puis $n^p \equiv n \bmod p$ pour tout $n \in \mathbb{Z}$ (*petit théorème de Fermat*).

Corollaire 4.7. *Tout groupe d'ordre premier p est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.*

Démonstration — Soient G d'ordre premier p et $g \in G - \{1\}$. L'ordre de g est > 1 et divise $|G| = p$, c'est donc p et on a $\langle g \rangle = G$. On conclut par le Corollaire 3.4. □

Une question réciproque naturelle est la suivante « si n divise $|G|$ alors est-ce que G possède un sous-groupe d'ordre n ? » Nous verrons par la suite que la réponse est négative en général, le plus petit contre-exemple ayant lieu dans le groupe alterné A_4, mais affirmative quand G est abélien (Gauss) ou quand n est une puissance d'un nombre premier (Sylow). Nous nous contenterons ici du cas particulier où n est premier, dû à Cauchy. [6]

Théorème 4.8. *(Cauchy) Soient G un groupe fini et p un nombre premier divisant $|G|$. Alors G possède un élément d'ordre p.*

Démonstration — Notons n_p le nombre d'éléments d'ordre p de G. On va montrer $n_p \equiv -1 \bmod p$, et en particulier $n_p \geqslant p - 1 > 0$.

Le cas $p = 2$ est particulièrement simple. Pour $g \in G$ on a $g = g^{-1} \Leftrightarrow g^2 = 1 \Leftrightarrow g = 1$ ou g est d'ordre 2. Ainsi, si f désigne l'aplication $G \to G, g \mapsto g^{-1}$, alors f

6. Augustin-Louis Cauchy, *Mémoire sur les arrangements que l'on peut former avec des lettres données* (et sur les permutations ou substitutions à l'aide desquelles on passe d'un arrangement à un autre) (1845), œuvres complètes, série 2 tome 13 , https://gallica.bnf.fr/ark:/12148/bpt6k902053/f175.

est une involution possédant $1 + n_2$ points fixes. On a donc $|G| \equiv 1 + n_2 \bmod 2$ par le Corollaire 1.9 Chap. 1, et on conclut car $|G|$ est pair.

Suivant J. Mc Kay, cette démonstration se généralise à tout p de la manière suivante. Soit $X = \{(g_1, g_2, \ldots, g_p) \in G^p \mid g_1 g_2 \cdots g_p = 1\}$. Notons que si on a $g_1 g_2 \cdots g_p = 1$, on a aussi $g_p g_1 g_2 \cdots g_{p-1} = 1$ en multipliant à gauche par g_p et à droite par g_p^{-1}. Autrement dit, la permutation circulaire $f : G^p \to G^p$, définie par $f(g_1, g_2, \ldots, g_p) = (g_p, g_1, g_2, \ldots, g_{p-1})$, préserve X, et vérifie $f^p = \mathrm{id}$. Les points fixes de f dans X sont les éléments $(g, g, \cdots, g)$ avec $g \in G$ et $g^p = 1$, donc il y en a $1 + n_p$. On a enfin $|X| = |G|^{p-1}$ car pour définir un élément de X il suffit de choisir arbitrairement $g_1, ..., g_{p-1}$ et de définir g_p comme l'inverse de $g_1 g_2 \cdots g_{p-1}$. On conclut par $|X| = |G|^{p-1} \equiv 0 \bmod p$ et $|X| \equiv 1 + n_p \bmod p$ (Corollaire 1.9 Chap. 1). □

5. Sous-groupes finis de $k^\times$ et $(\mathbb{Z}/n\mathbb{Z})^\times$

Le résultat principal de cette partie est le suivant :

THÉORÈME 5.1. *Si k est un corps, tout sous-groupe fini de $k^\times$ est cyclique.*

Un cas particulier facile est le cas $k = \mathbb{C}$. En effet, un exemple de sous-groupe fini de $\mathbb{C}^\times$ est le sous-groupe μ_n, qui est bien cyclique engendré par $e^{\frac{2i\pi}{n}}$. Réciproquement, par Lagrange, tout sous-groupe d'ordre n est inclus dans μ_n, donc égal à μ_n (et donc cyclique) pour des raisons de cardinal. Comme nous le verrons, le théorème est non trivial en revanche pour k général, notamment pour k est fini.

REMARQUE 5.2. Pour tout corps k et tout entier $n \geqslant 1$, l'ensemble

$$\mu_n(k) = \{x \in k^\times, x^n = 1\}$$

est un sous-groupe de $k^\times$. C'est aussi l'ensemble des racines dans k du polynôme $X^n - 1 \in k[X]$, on a donc $|\mu_n(k)| \leqslant n$. L'inégalité est stricte en général : par exemple on a $\mu_n(\mathbb{R}) = \{1\}$ pour n impair. Le théorème montre que $\mu_n(k)$ est toujours cyclique (et d'ordre d divisant n).

Montrons d'abord le lemme suivant :

LEMME 5.3. (Cauchy) *Soient G un groupe et $x, y \in G$ deux éléments qui commutent, d'ordres finis a et b. Si $(a, b) = 1$ alors xy est d'ordre ab.*

DÉMONSTRATION — Considérons $M = \langle x \rangle \cap \langle y \rangle$. C'est un sous-groupe de $\langle x \rangle$ et de $\langle y \rangle$. D'après Lagrange, $|M|$ divise $a = |\langle x \rangle|$ et $b = |\langle y \rangle|$ et donc $M = \{1\}$. (On peut d'ailleurs se passer de Lagrange ici en disant simplement que l'on a $m^a = m^b = 1$, et donc $m = 1$, pour tout m dans M.) Vérifions maintenant que xy est d'ordre ab. Soit $k \in \mathbb{Z}$. Comme $xy = yx$, on a $(xy)^k = x^k y^k$. En particulier, $(xy)^{ab} = 1$. Réciproquement, si $(xy)^k = 1$ alors $x^k = y^{-k} \in M = \{1\}$, et donc $x^k = y^{-k} = 1$. Ainsi, $a|k$ et $b|k$ puis $ab|k$ car $(a, b) = 1$. □

REMARQUE 5.4. Si on ne suppose plus que x et y commutent, alors xy peut être d'ordre quelconque, et ce même si G est fini : voir l'Exercice 2.20.

Démonstration — (du Théorème) Soient k un corps et $G \subset k^\times$ un sous-groupe fini. Posons $n = |G|$. Il suffit de démontrer que, si $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ est la décomposition en facteurs premiers de n, alors G possède un élément g_i d'ordre $p_i^{\alpha_i}$ pour tout i. En effet, le lemme ci-dessus assurera alors que l'élément $g_1 g_2 \cdots g_r$ est d'ordre n.

Considérons le polynôme $P = X^n - 1 \in k[X]$. Comme k est un corps, P admet au plus n racines dans k. D'autre part, le théorème de Lagrange assure que les n éléments de G sont racines de P : il est donc scindé à racines distinctes, égales aux éléments de G. On a montré l'égalité dans $k[X]$

$$X^{|G|} - 1 = \prod_{g \in G} (X - g). \tag{7}$$

Remarquons que si d est un diviseur de n, alors $X^d - 1$ divise $X^n - 1$ dans $k[X]$, le quotient étant $\sum_{i=0}^{n/d-1} X^{id}$. En particulier, $X^d - 1$ est aussi scindé à racines distinctes dans G. Pour tout i, il existe donc au moins une racine g_i de $X^{p_i^{\alpha_i}} - 1$ dans G qui n'est pas racine de $X^{p_i^{\alpha_i - 1}} - 1$. Un tel élément est donc d'ordre $p_i^{\alpha_i}$, ce qui conclut la démonstration. □

Le théorème suivant est démontré par Gauss quand $k = \mathbb{F}_p$ dans ses *Disquisitones Arithmeticae.*

Corollaire 5.5. *(Gauss) Pour p premier, le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique.*

Par exemple, les puissances successives de 2 modulo 11 sont (les classes de)

$$2, 4, 8, 5, 10, 9, 7, 3, 6, 1$$

et donc 2 est un générateur de $(\mathbb{Z}/11\mathbb{Z})^\times$. En revanche, ce n'est pas le cas de $5 \equiv 2^4$, qui est d'ordre $10/(10, 4) = 5$. Un entier a dont la classe dans $\mathbb{Z}/p\mathbb{Z}$ engendre $(\mathbb{Z}/p\mathbb{Z})^\times$ est appelé une *racine primitive modulo p*. Le théorème de Gauss assure l'existence de racines primitives modulo tout nombre premier p, mais de nombreuses questions persistent quant à leur construction. Par exemple, E. Artin a conjecturé que « *tout entier $a \neq -1$ qui n'est pas un carré est une racine primitive modulo p pour une infinité de nombres premiers p* ». On ne connaît aucun entier a pour lequel cette conjecture est vraie ! [7]

Remarque 5.6. *Un isomorphisme de groupes $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ (il en existe par le corollaire) s'appelle un logarithme discret, par analogie avec l'isomorphisme* $\log : (\mathbb{R}_{>0}, \times) \xrightarrow{\sim} (\mathbb{R}, +)$.

Une première conséquence classique du théorème de Gauss concerne l'étude des puissances n-èmes dans $(\mathbb{Z}/p\mathbb{Z})^\times$. Pour $n \in \mathbb{Z}$, posons

$$(\mathbb{Z}/p\mathbb{Z})^{\times,(n)} = \{x^n \mid x \in (\mathbb{Z}/p\mathbb{Z})^\times\}$$

l'ensemble des puissances n-èmes. C'est manifestement un sous-groupe de $(\mathbb{Z}/p\mathbb{Z})^\times$, à savoir l'image du morphisme de groupes $(\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times, x \mapsto x^n$. Comme $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p - 1$, le Lemme 3.7 montre :

Corollaire 5.7. *Soient p premier, $n \geqslant 1$ un entier et $m = (p - 1, n)$.*

7. En revanche, un théorème de Heath-Brown montre qu'il y a au plus 2 nombres premiers qui ne satisfont pas cette conjecture : D. R. Heath-Brown, « Artin's conjecture for primitive roots », Quart. J. Math. Oxford vol. 37 (1986), 27-38.

(i) Le groupe $(\mathbb{Z}/p\mathbb{Z})^{\times,(n)}$ *est cyclique d'ordre* $\frac{p-1}{m}$*, et égal à* $(\mathbb{Z}/p\mathbb{Z})^{\times,(m)}$*.*

(ii) pour $x \in (\mathbb{Z}/p\mathbb{Z})^{\times}$ *on a* $x \in (\mathbb{Z}/p\mathbb{Z})^{\times,(n)}$ *si, et seulement si,* $x^{\frac{p-1}{m}} = 1$*.*

Pour le (ii) on peut aussi dire que le polynôme $X^{\frac{p-1}{m}} - 1$ a au plus $\frac{p-1}{m}$ racines dans $\mathbb{Z}/p\mathbb{Z}$, et donc ses racines sont exactement les puissances n-èmes, par le (i).

Exemple 5.8. (*Carrés*) Le groupe $(\mathbb{Z}/p\mathbb{Z})^{\times,(2)}$ est le groupe des *carrés* de $(\mathbb{Z}/p\mathbb{Z})^{\times}$. Pour $p > 2$, il est d'ordre $\frac{p-1}{2}$ d'après le corollaire ci-dessus (i). On a aussi

$$(\mathbb{Z}/p\mathbb{Z})^{\times,(2)} = \{\bar{i}^2 \mid 1 \leqslant i \leqslant \frac{p-1}{2}\},$$

car $(-i)^2 = i^2$, et donc tous les éléments de l'ensemble de droite sont distincts. Une application classique du (ii), due à Euler, est que -1 *est un carré modulo* p *si et seulement si* $p = 2$ *ou* $(-1)^{\frac{p-1}{2}} \equiv 1 \bmod p$*, i.e.* $p \equiv 1 \bmod 4$*.*

Décrivons enfin la structure de $(\mathbb{Z}/n\mathbb{Z})^{\times}$ pour $n \geqslant 1$ quelconque. D'après l'isomorphisme chinois (Corollaire 3.11) il suffit de traiter le cas où n est une puissance d'un nombre premier.

Corollaire 5.9. *(i) Si* p *est premier impair, et* $m \geqslant 1$*, alors le groupe* $(\mathbb{Z}/p^m\mathbb{Z})^{\times}$ *est cyclique.*

(ii) Si $m \geqslant 2$ *on a* $(\mathbb{Z}/2^m\mathbb{Z})^{\times} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z}$*.*

Avant de montrer ce corollaire, commençons par établir une congruence utile.

Lemme 5.10. *Soit* $k \geqslant 0$ *un entier.*

(i) Si p *est un nombre premier impair, alors* $(1+p)^{p^k} \equiv 1 + p^{k+1} \bmod p^{k+2}$*.*

(ii) De plus, on a $(1+4)^{2^k} \equiv 1 + 2^{k+2} \bmod 2^{k+3}$*.*

Démonstration — Si p est un nombre premier, on rappelle la congruence $\binom{p}{i} \equiv 0 \bmod p$ si $i = 1, \ldots, p-1$. On en déduit que pour $k \geqslant 1$, $a \equiv b \bmod p^k$ entraîne $a^p \equiv b^p \bmod p^{k+1}$, puis (i) et (ii), par récurrence sur k. □

Démonstration — (du corollaire) Supposons p premier impair. Le lemme précédent (i) montre que $\overline{1+p}$ est d'ordre p^{m-1} dans $(\mathbb{Z}/p^m\mathbb{Z})^{\times}$. On a $|(\mathbb{Z}/p^m\mathbb{Z})^{\times}| = \varphi(p^m) = (p-1)p^{m-1}$ avec $(p-1, p^{m-1}) = 1$. D'après le Lemme 5.3, il suffit de trouver un élément d'ordre $p-1$ dans $(\mathbb{Z}/p^m\mathbb{Z})^{\times}$. Mais d'après Gauss, il existe $a \in \mathbb{Z}$ premier à p (et donc à p^m) dont la classe engendre $(\mathbb{Z}/p\mathbb{Z})^{\times}$ modulo p. Soit d l'ordre de la classe de a dans $(\mathbb{Z}/p^m\mathbb{Z})^{\times}$. En réduisant modulo p la relation $a^d \equiv 1 \bmod p^m$, il vient que $p-1$ divise d. Mézalor $a^{\frac{d}{p-1}}$ est d'ordre $p-1$ (Lemme 3.6).

Supposons maintenant $p = 2$ et $m \geqslant 2$. Le lemme précédent (ii) assure que $\overline{5}$ est d'ordre 2^{m-2} dans $(\mathbb{Z}/2^m\mathbb{Z})^{\times}$. Vérifions que le morphisme de groupes

$$\mathbb{Z}/2 \times \mathbb{Z}/2^{m-2}\mathbb{Z} \longrightarrow (\mathbb{Z}/2^m\mathbb{Z})^{\times},\ (p,q) \mapsto (-1)^p 5^q \bmod 2^m,$$

est un isomorphisme. Pour des raisons de cardinal, il suffit de voir qu'il est injectif. Mais si $(-1)^p 5^q \equiv 1 \bmod 2^m$, alors par réduction modulo 4 il vient $(-1)^p = 1$, puis $5^q \equiv 1 \bmod 2^m$ et donc $q \equiv 0$ car 5 est d'orde 2^{m-2} modulo 2^m, QED. □

6. Groupes quotients

Soient G un groupe et H un sous-groupe de G. Comme sur tout ensemble, il existe en général une quantité de lois de groupes sur G/H, mais ces dernières n'ont en général aucun lien avec la structure du groupe G. Une bien meilleure question est la suivante : existe-t-il une loi de groupe sur G/H telle que la projection canonique $\pi : G \to G/H, g \mapsto gH$, est un morphisme de groupes ?

Observons d'abord que si une telle loi $\star$ existe, alors elle est unique. En effet, elle satisfait, $(gH) \star (g'H) = \pi(g) \star \pi(g') = \pi(gg') = gg'H$ pour tout $g, g' \in G$. En outre, le neutre de $\star$ doit être l'image du neutre de G par π, c'est donc $\pi(1) = H$. En particulier, le noyau du morphisme π est

$$\pi^{-1}(H) = \{g \in G,\ gH = H\} = H.$$

Il se trouve que les noyau des morphismes de groupes ne sont pas des sous-groupes quelconques : ce sont des sous-groupes *distingués*.

Proposition-Définition 6.1. *Un sous-groupe H du groupe G est dit* distingué, *ou* normal, *si l'une des propriétés équivalentes suivantes est satisfaite :*

(i) $gHg^{-1} \subset H$ pour tout $g \in G$,

(ii) $gHg^{-1} = H$ pour tout $g \in G$,

(iii) $gH = Hg$ pour tout $g \in G$.

Démonstration — L'équivalence (ii) $\Leftrightarrow$ (iii) est évidente, ainsi que (ii) $\Rightarrow$ (i). Supposons (i). Soit $g \in G$. On a $gHg^{-1} \subset H$ par (i), ainsi que $g^{-1}Hg \subset H$ encore par (i) appliquée à g^{-1}, ce qui équivaut à $H \subset gHg^{-1}$, et au final $gHg^{-1} = H$. $\square$

On note en général $H \lhd G$ pour dire « *H est un sous-groupe distingué du groupe G* ». Les sous-groupes évidents $\{1\}$ et G sont trivialement distingués. Ajoutons que pour $g \in G$ fixé, et pour un sous-groupe $H \subset G$ infini, il est possible d'avoir une inclusion stricte $gHg^{-1} \subsetneq H$ (voir l'Exercice 2.30). Si G est abélien, noter que *tous ses sous-groupes sont (trivialement) distingués*. La réciproque est fausse :

Exemple 6.2. (Le groupe H_8) *Considérons les éléments*

$$I = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix},\ J = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \text{ et } K := IJ = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}$$

de $\mathrm{GL}_2(\mathbb{C})$. *On a clairement $I^2 = -1$, $J^2 = -1$ et $JIJ^{-1} = -I$, i.e. $IJ = -JI$, puis*

$$I^2 = J^2 = K^2 = -1,\ IJ = K,\ JK = I,\ KI = J \text{ et } JI = -K,\ KJ = -I,\ IK = -J.$$

Ainsi $\mathrm{H}_8 := \langle I, J\rangle = \{\pm 1, \pm I \pm J, \pm K\}$ *est un sous-groupe de* $\mathrm{GL}_2(\mathbb{C})$ *d'ordre* 8, *appelé* groupe des quaternions d'ordre 8. *Les relations ci-dessus montrent que ses sous-groupes sont* $1, \langle -1\rangle, \langle I\rangle, \langle J\rangle, \langle K\rangle$ *et* H_8, *et qu'ils sont tous distingués.* [8]

Toutefois, nous verrons par la suite que les sous-groupes d'un groupe non abélien sont en général rarement distingués. Indiquons quelques moyens de construire des sous-groupes distingués.

8. Comme nous le verrons au Chapitre 2, le sous-$\mathbb{R}$-espace vectoriel $\mathbb{H}$ de $\mathrm{M}_2(\mathbb{C})$ engendré par H_8 est un sous-anneau à division (non commutatif), dont le groupe multiplicatif contient H_8. Cela montre aussi que le Théorème 5.1 ne s'étend pas aux corps gauches (car H_8 n'est pas cyclique).

Exemple 6.3. *Si $f : G \to G'$ est un morphisme de groupes, on a* $\ker f \lhd G$. En effet, si $f(h) = 1$ et $g \in G$ alors $f(ghg^{-1}) = f(g)f(h)f(g)^{-1} = f(g)f(g)^{-1} = 1$ et donc $ghg^{-1} \in \ker f$.

Exemple 6.4. Plus généralement, *si $f : G \to G'$ est un morphisme de groupes on vérifie immédiatement que si $H' \lhd G'$ alors $f^{-1}(H') \lhd G$, et si f est surjective, que l'on a aussi $H \lhd G$ alors $f(H) \lhd G'$.*

Exemple 6.5. *Un sous-groupe H d'indice* 2 *dans G est nécessairement distingué.* En effet, pour $g \notin H$ on a à la fois $G = H \coprod Hg$ et $G = H \coprod gH$ (car $x \mapsto x^{-1}$ est une bijection des classes à droites sur les classes à gauche), donc $Hg = gH = G \smallsetminus H$.

Exemple 6.6. (Normalisateur) Si H est un sous-groupe d'un groupe G, le *normalisateur de H dans G* est le sous-groupe de G défini par $\mathrm{N}_G(H) = \{g \in G \mid gHg^{-1} = H\}$. C'est manifestement *le plus grand sous-groupe de G dans lequel H est distingué.* En particulier, on a $H \lhd G \iff \mathrm{N}_G(H) = G$.

Le théorème principal concernant les groupes quotients est le suivant.

Théorème 6.7. *Soit H un sous-groupe d'un groupe G.*

(i) Il existe au plus une loi de groupe sur G/H telle que la projection canonique $G \to G/H$ est un morphisme de groupes.

(ii) Une telle loi existe si, et seulement si, on a $H \lhd G$, auquel cas elle coïncide avec la loi sur G/H induite par $\bullet$ sur $\mathrm{P}(G)$.

Démonstration — Le (i) a déjà été démontré, ainsi que le fait que si la loi existe on a $H \lhd G$. Supposons donc $H \lhd G$. Pour $g, g' \in H$ on a

$$(gH)(g'H) = g(Hg')H = g(g'H)H = gg'HH = gg'H$$

(associativité de $\bullet$ sur $\mathrm{P}(G)$, propriété (iii) des sous-groupes distingués et Lemme 4.1). Cela montre que G/H est stable par $\bullet$, et donc que $\bullet$ est une loi associative sur G/H (car sur $\mathrm{P}(G)$), et aussi que la projection canonique $\pi : G \to G/H$ vérifie $\pi(g)\pi(g') = \pi(gg')$ pour tout $g, g' \in G$. Le fait que $(G/H, \bullet)$ est un groupe se déduit alors formellement du fait que G est un groupe et que π est surjective. On peut le vérifier directement : l'élément H est un neutre car on a $H(gH) = gHH = gH$ pour tout $g \in G$, et pour tout $g \in G$ on a $(gH)(g^{-1}H) = gg^{-1}H = H$ et de même $(g^{-1}H)(gH) = H$, donc gH est inversible d'inverse $g^{-1}H$. □

Proposition-Définition 6.8. *Si H est un sous-groupe distingué de G, le* groupe quotient *G/H est la donnée de l'ensemble G/H muni de son unique loi de groupe telle que la projection canonique $\pi : G \to G/H$ est un morphisme de groupes.*

Le neutre de G/H est H, l'inverse de l'élément gH, pour $g \in G$, est $g^{-1}H = Hg^{-1} = (gH)^{-1}$, et pour tout $g, g' \in G$ on a $(gH)(g'H) = gg'H = (gH) \bullet (g'H)$. On a aussi déjà dit que le noyau du morphisme $\pi : G \to G/H$ est H. En particulier, on a démontré que tout sous-groupe distingué est le noyau d'un morphisme.

Remarque 6.9. (i) Pour de nombreuses questions, il n'est pas nécessaire de savoir que la loi de groupe quotient $\star$ sur G/H est induite par la multiplication des parties dans $\mathrm{P}(G)$, mais simplement qu'elle satisfait $(gH)\star(g'H) = gg'H$ pour tout $g, g' \in G$.

(ii) Pour montrer l'existence de $\star$ nous aurions aussi pu nous passer de $\bullet$ et remarquer que comme H est distingué dans G, si $a, a', b, b' \in G$ sont tels que $aH = a'H$ et $bH = b'H$, alors on a aussi $abH = a'b'H$: on peut « multiplier les congruences modulo H ». Cela montre qu'il y a un sens à poser sans ambiguité $aH \star bH := abH$, *i.e.* que l'application $G \times G \to G/H, (a, b) \mapsto abH$ passe au quotient $G/H \times G/H \to G/H, (aH, bH) \mapsto abH$. C'est l'approche suivie traditionnellement pour définir l'addition sur $\mathbb{Z}/n\mathbb{Z}$!

Exemple 6.10. (*Retour sur* $\mathbb{Z}/n\mathbb{Z}$) Le groupe additif $\mathbb{Z}/n\mathbb{Z}$ est (comme on s'en doutait !) le groupe quotient de $\mathbb{Z}$ par son sous-groupe $n\mathbb{Z}$. En effet, la loi d'addition sur $\mathbb{Z}/n\mathbb{Z}$ satisfait $\overline{k} + \overline{k'} = \overline{k + k'}$ pour tout $k, k' \in \mathbb{Z}$, mais cela signifie exactement que la projection canonique $\mathbb{Z} \mapsto \mathbb{Z}/n\mathbb{Z}, k \mapsto \overline{k}$, est un morphisme de groupes.

Donnons une application aux carrés de $(\mathbb{Z}/p\mathbb{Z})^\times$. Soit p premier impair. Écrivons $(\mathbb{Z}/p\mathbb{Z})^\times = \mathrm{C}_p \coprod \mathrm{N}_p$ où C_p est l'ensemble des carrés. On a vu que C_p est un sous-groupe d'indice 2. Ainsi, le groupe quotient $(\mathbb{Z}/p\mathbb{Z})^\times/\mathrm{C}_p = \{\mathrm{C}_p, \mathrm{N}_p\}$ a deux éléments, et il est de neutre C_p. Il est donc isomorphe à $\mathbb{Z}/2\mathbb{Z}$ (ou à $\{\pm 1\}$) et on a

$$\mathrm{C}_p\mathrm{C}_p = \mathrm{C}_p,\ \mathrm{C}_p\mathrm{N}_p = \mathrm{N}_p \text{ et } \mathrm{N}_p\mathrm{N}_p = \mathrm{C}_p. \tag{8}$$

Cette dernière égalité dit par exemple que le produit de deux non-carrés est un carré ! Suivant Legendre, pour $x \in \mathbb{Z}/p\mathbb{Z}$ on pose $(\frac{x}{p}) = 1$ si x est un carré non nul, $(\frac{0}{p}) = 0$, et $(\frac{x}{p}) = -1$ si x n'est pas un carré. En particulier, $x \mapsto (\frac{x}{p})$ n'est rien d'autre que la composée des morphismes naturels $(\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times/\mathrm{C}_p$ et $(\mathbb{Z}/p\mathbb{Z})^\times/\mathrm{C}_p \simeq \{\pm 1\}$. Le fait que c'est un morphisme, ou les égalités (8), se reformulent en :

Corollaire 6.11. (*Multiplicativité du symbole de Legendre*) *Pour p premier impair et $x, y \in (\mathbb{Z}/p\mathbb{Z})^\times$ on a $(\frac{xy}{p}) = (\frac{x}{p})(\frac{y}{p})$.*

Cette multiplicativité ramène l'étude de $(\frac{q}{p})$, avec $q \in \mathbb{Z}$, aux cas $q = -1$ et q premier. On a déjà vu $(\frac{-1}{p}) =(-1)^{\frac{p-1}{2}}$ (Exemple 5.8). Le cas q premier est l'objet de la fameuse *loi de réciprocité quadratique* (conjecturée par Euler, formulée ainsi par Legendre, et démontrée par Gauss), pour laquelle nous renvoyons aux exercices.

Remarque 6.12. Le symbole de Legendre définit donc un morphisme de groupes $(\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}, x \mapsto (\frac{x}{p})$. On peut y penser comme un analogue du morphisme *signe* : $\mathbb{R}^\times \to \{\pm 1\}$, $x \mapsto \frac{x}{|x|}$. Plus généralement, pour tout sous-groupe H d'indice 2 d'un groupe G (automatiquement distingué par l'Exemple 6.5), il existe un unique morphisme $\epsilon_H : G \to \{\pm 1\}$ de noyau H.

Le théorème d'existence des groupes quotients est le point de départ de la *stratégie de dévissage* pour étudier les groupes : étant donné G, on cherche un sous-groupe distingué nontrivial $H \subsetneq G$ (ou ce qui revient au même, un morphisme non trivial $G \to G'$) et on commence par étudier H et G/H, qui sont d'ordre plus petit. Les groupes G pour pour lesquels cette stratégie échoue sont dit simples.

Définition 6.13. *Un groupe G est dit simple si on a $G \neq 1$ et si les seuls sous-groupes distingués de G sont $\{1\}$ et G.*

Exemple 6.14. *Les groupes abéliens simples sont les $\mathbb{Z}/p\mathbb{Z}$ avec p premier.* En effet, tout sous-groupe d'un groupe abélien est distingué, donc un groupe abélien simple est monogène. Il est cyclique car $2\mathbb{Z}$ est un sous-groupe distingué strict de $\mathbb{Z}$. On conclut car les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont en bijection avec les diviseurs de n.

Exemple 6.15. Si H et K sont deux groupes, alors $H' = H \times \{1\}$ est un sous-groupe distingué de $H \times K$, et on a $H' \simeq H$ et $(H \times K)/H' \simeq K$ (utiliser par exemple le Théorème 6.17 ci-dessous). En revanche, il n'est pas du tout vrai en général que pour $H \lhd G$, on a $G \simeq H \times (G/H)$. Par exemple le groupe abélien $G = \mathbb{Z}/4\mathbb{Z}$ n'est pas isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ alors qu'il quotient un sous-groupe H d'ordre 2, à savoir $\langle \overline{2} \rangle$, et donc $H \simeq G/H \simeq \mathbb{Z}/2\mathbb{Z}$. Pire, ce n'est pas parce que H et G/H sont abéliens que G l'est : voir l'Exercice 2.27.

Dégageons maintenant quelques propriétés générales des groupes quotients. Supposons $H \lhd G$ et soit $f : G/H \to G'$ un morphisme de groupes. La composée $g = f \circ \pi : G \to G'$, où $\pi : G \to G/H$ est la projection canonique, est un morphisme de groupes vérifiant $g(H) = f(\pi(H)) = f(H) = \{1\}$. Réciproquement :

Proposition 6.16. *(Propriété universelle des groupes quotients) Soient H un sous-groupe distingué du groupe G et $f : G \to G'$ un morphisme de groupes vérifiant $H \subset \ker f$. Alors il existe un unique morphisme de groupes $\overline{f} : G/H \to G'$ envoyant gH sur $f(g)$ pour tout $g \in G$.*

Bien sûr, la propriété $\overline{f}(gH) = f(g)$ s'écrit aussi $f = \overline{f} \circ \pi$ avec $\pi : G \to G/H$ la projection canonique.

Démonstration — L'unicité de $\overline{f} : G/H \to G'$ vérifiant $\overline{f}(gH) = f(g)$ est évidente (car π est surjective). Un tel $\overline{f}$ est automatiquement un morphisme de groupes : pour $g, g' \in G$ on a $\overline{f}(gHg'H) = \overline{f}(gg'H) = f(gg') = f(g)f(g') = \overline{f}(gH)\overline{f}(g'H)$. Il ne reste qu'à montrer l'existence de $\overline{f}$. Soient $g, g' \in G$ avec $g \sim_H g'$. On a $g' = gh$ avec $h \in H$ donc $f(g') = f(g)f(h) = f(g)$ car $H \subset \ker f$: l'existence de $\overline{f}$ découle de la Proposition 2.1. □

On retiendra : « c'est la même chose de se donner un morphisme $G/H \to G'$ et un morphisme de $G \to G'$ trivial sur H ». De manière plus précise, pour tout groupe G' l'application $f \mapsto f \circ \pi$ est une bijection de $\mathrm{Hom}(G/H, G')$ sur $\{f \in \mathrm{Hom}(G, G') \mid f(H) = \{1\}\}$. Dans le cas $G = \mathbb{Z}$ et $H = n\mathbb{Z}$ (Exemple 6.10), on obtient par exemple que se donner un morphisme $\mathbb{Z}/n\mathbb{Z} \to G'$ est la même chose que se donner un morphisme de $f : \mathbb{Z} \to G'$, *i.e.* $f(1) = g \in G'$, tel que $f(n) = 1$, *i.e.* avec $g^n = 1$. Un corollaire particulièrement utile est le suivant, appelé parfois le *premier théorème d'isomorphisme.*

Théorème 6.17. *Si $f : G \to G'$ est un morphisme de groupes, alors f induit par passage au quotient un isomorphisme de groupes $\overline{f} : G/\ker f \xrightarrow{\sim} \mathrm{Im}\, f$.*

Démonstration — Quitte à remplacer G' par son sous-groupe $\mathrm{Im}\, f$, on peut supposer f surjective. La proposition 2.1 appliquée à $H = \ker f$ montre que f induit par passage au quotient un morphisme de groupes $\overline{f} : G/\ker f \to G'$, envoyant $g \ker f$

sur $f(g)$ pour tout $g \in G$. Le morphisme $\overline{f}$ est donc surjectif car f l'est. Son noyau est l'ensemble des $g \ker f \in G/\ker f$ tels que $f(g) = 1$, ce qui force $g \in \ker f$ et donc $g \ker f = \ker f$. Ainsi, $\overline{f}$ est également injective : c'est un isomorphisme. □

EXEMPLE 6.18. *L'application $z \mapsto e^{2\pi i z}$ définit des morphismes surjectifs $\mathbb{R} \to \mathbb{U}$ et $\mathbb{C} \to \mathbb{C}^\times$, de même noyau $\mathbb{Z}$. Elle induit donc des isomorphismes*

$$\mathbb{R}/\mathbb{Z} \simeq \mathbb{U} \text{ et } \mathbb{C}/\mathbb{Z} \simeq \mathbb{C}^\times.$$

Ainsi, tout morphisme de groupes $f : G \to G'$ se décompose naturellement comme composé de trois morphismes naturels : d'abord la projection canonique $G \to G/\ker f$, envoyant g sur $g \ker f$ (surjective), suivie de l'isomorphisme canonique $G/\ker f \xrightarrow{\sim} \operatorname{Im} f$ de l'énoncé, envoyant $g \ker f$ sur $f(g)$, et enfin le morphisme d'inclusion $\operatorname{Im} f \to G'$ (injectif). C'est le *dévissage canonique* d'un morphisme.

Terminons par une étude des sous-groupes et des quotients du groupe quotient G/H.

PROPOSITION 6.19. *Soit H un sous-groupe distingué d'un groupe G.*

(i) L'application $K \mapsto K/H$ induit une bijection croissante entre sous-groupes K de G contenant H et sous-groupes de G/H.

(ii) Dans cette bijection, on a $K/H \lhd G/H \Leftrightarrow K \lhd G$, auquel cas le morphisme naturel $G/H \to G/K$ induit un isomorphisme $(G/H)/(K/H) \xrightarrow{\sim} G/K$.

L'isomorphisme du (ii) est parfois appelé *troisième théorème d'isomorphisme.*

DÉMONSTRATION — Appliquons la Proposition 2.10 au morphisme surjectif $\pi : G \to G/H$. Le (i) s'en déduit car pour K un sous-groupe de G avec $H \subset K \subset G$, on constate $\pi(K) = K/H$. Le premier point du (ii) résulte de l'Exemple 6.4. Pour $g \in G$ on a $gHK = gK$ car $HK = K$ puisque H est inclus dans K. La multiplication à droite par K induit donc une application $\varphi : G/H \to G/K, gH \mapsto gK$, qui est manifestement surjective et un morphisme de groupes : c'est l'application sous-entendue dans l'énoncé. On a $\ker \varphi = \{gH \mid gK = K\} = K/H$, car pour $g \in G$ on a $gK = K \Leftrightarrow g \in K$. On conclut par le Théorème 6.17. □

7. Complément I : Groupes additifs et multiplicatif usuels

On discute dans ce complément de quelques aspects de la structure des groupes additifs et multiplicatifs des anneaux $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$. Tous les groupes considérés ici seront donc abéliens. On a déjà vu que les sous-groupes de $\mathbb{Z}$ sont les $\mathbb{Z}n$ avec $n \in \mathbb{Z}$, on en déduit le :

COROLLAIRE 7.1. *Les sous-groupes de type fini de $\mathbb{Q}$ sont les $\mathbb{Z}\lambda$ avec $\lambda \in \mathbb{Q}$.*

DÉMONSTRATION — Soit $H = \sum_{i=1}^n \mathbb{Z}\lambda_i \subset \mathbb{Q}$. En considérant un dénominateur commun $m \geqslant 1$ des λ_i, on a $mH \subset \mathbb{Z}$, où $mH = \{mh \mid h \in H\}$. Mais alors mH est un sous-groupe de $\mathbb{Z}$, et donc de la forme $\mathbb{Z}n$. On en déduit $H = \mathbb{Z}\frac{n}{m}$. □

Remarque 7.2. *Il existe des sous-groupes de $\mathbb{Q}$ qui ne sont pas de type fini, comme le sous-groupe*[9] $\cup_{n\geqslant 1}\mathbb{Z}\frac{1}{10^n}$ *des nombres décimaux. Nous renvoyons à l'Exercice 2.32 pour une classification de tous les sous-groupes de $\mathbb{Q}$ (elle ne nous servira pas par la suite).*

Considérons maintenant le groupe additif de $\mathbb{R}$. C'est un groupe exotique ! En effet, l'inclusion $\mathbb{Q} \subset \mathbb{R}$ permet de voir $\mathbb{R}$ comme un $\mathbb{Q}$-espace vectoriel. D'après le Théorème 4.5, on peut en considérer une base $(b_i)_{i\in I}$ et donc un isomorphisme de $\mathbb{Q}$-espaces vectoriels $\mathbb{R} \simeq \mathbb{Q}^{(I)}$, le $\mathbb{Q}$-espace vectoriel des suites $(x_i)_{i\in I} \in \mathbb{Q}^I$ avec $x_i = 0$ pour tout $i \in I$ sauf un nombre fini (on renvoie à l'Exemple 1.14 Chap. 1 pour les produits restreints). Comme $\mathbb{R}$ est indénombrable, alors que $\mathbb{Q}^n$ l'est pour tout entier $n \geqslant 1$, on constate que I est infini.[10] Il y a donc toute une zoologie de sous-groupes additifs de $\mathbb{R}$, que l'on n'a pas envie d'étudier en première approche. Une manière de contourner ce problème est de prendre en compte la topologie naturelle de $\mathbb{R}$. Si $H \subset \mathbb{R}$ est un sous-groupe, on constate immédiatement que son adhérence $\overline{H}$ est un sous-groupe (fermé) de $\mathbb{R}$. Ces derniers sont beaucoup plus sympathiques :

Proposition 7.3. *Les sous-groupes fermés de $\mathbb{R}$ sont $\mathbb{R}$ et les $\mathbb{Z}\lambda$ avec $\lambda \in \mathbb{R}$.*

Démonstration — Soit H un sous-groupe fermé de $\mathbb{R}$. On peut supposer $H \neq \{0\}$, auquel cas on a l'ensemble $A := H \cap \mathbb{R}_{>0}$ est non vide (considérer $h \mapsto -h$). Supposons d'abord $a = 0$. Comme $0 \notin A$, il existe une suite $h_n \in A$ tendant vers a. Soient $x \in \mathbb{R}$ et $N \geqslant 1$ un entier. Pour n assez grand on a $0 < h_n < 1/N$ et donc il existe $m \in \mathbb{Z}$ avec $|mh_n - x| \leqslant 1/N$. Ainsi, les éléments de H de la forme mh_n, avec $m \in \mathbb{Z}$ et $n \geqslant 1$ sont denses dans $\mathbb{R}$, puis $H = \mathbb{R}$. On peut donc supposer $a = 0$. Soit $h \in H$. Il existe $n \in \mathbb{Z}$ avec $0 \leqslant h - na < a$, et donc $h - na \in H$ est nul par définition de a. On a montré $H = \mathbb{Z}\,a$. □

Enfin, on a $\mathbb{C} \simeq \mathbb{R}^2$ comme $\mathbb{R}$-espace vectoriel, et donc comme groupe additif. Là encore, c'est une question un peu exotique d'étudier tous les sous-groupes de $\mathbb{C}$: en fait on a les isomorphismes de $\mathbb{Q}$-espaces vectoriels suivants (noter $I \sim I \coprod I$ pour I infini) :

$$\mathbb{R} \simeq \mathbb{Q}^{(I)} \simeq \mathbb{Q}^{(I \coprod I)} \simeq \mathbb{Q}^{(I)} \times \mathbb{Q}^{(I)} \simeq \mathbb{R}^2 \simeq \mathbb{C}$$

Bien sûr, un tel isomorphisme n'est pas continu en tant qu'application $\mathbb{R} \to \mathbb{C}$! Dans la lignée de la Proposition 7.3, nous verrons au Complément 6 que les sous-groupes *fermés* de $\mathbb{R}^n$, avec $n \geqslant 1$ quelconque, admettent une description intéressante.

Discutons maintenant des *groupes multiplicatifs*. Déjà, le groupe

$$\mathbb{Z}^\times = \{\pm 1\}$$

est à isomorphisme près l'unique groupe à 2 éléments. Pour décrire $\mathbb{Q}^\times$ on note P l'ensemble des nombres premiers et on considère le sous-groupe $\mathbb{Z}^{(\mathrm{P})} \subset \mathbb{Z}^{\mathrm{P}}$ des (x_p) avec $x_p = 0$ pour tout p sauf un nombre fini. On constate que l'application $(\epsilon, (n_p)_{p\in P}) \mapsto \epsilon \prod_{p\in \mathrm{P}} p^{n_p}$ définit un isomorphisme de groupes

$$\{\pm 1\} \times \mathbb{Z}^{(\mathrm{P})} \xrightarrow{\sim} \mathbb{Q}^\times,$$

9. On vérifie aisément que si G est un groupe, et si $\{G_n\}_{n\geqslant 0}$ est une famille *croissante* de sous-groupes de G, *i.e.* vérifiant $G_n \subset G_{n+1}$, alors $\cup_{n\geqslant 0} G_n$ est un sous-groupe de G.

10. On peut en fait montrer que I est en bijection avec $\mathbb{R}$: voir l'Exercice 1.17 Chap. 1

le caractère bijectif de cette application venant de la factorisation unique d'un entier en produit de nombres premiers. On constate aussi que $\mathbb{R}_{>0}$ est un sous-groupe de $\mathbb{R}^\times$, et que l'application $(\epsilon, \lambda) \mapsto \epsilon\lambda$ induit un isomorphisme de groupes

$$\{\pm 1\} \times \mathbb{R}_{>0} \xrightarrow{\sim} \mathbb{R}^\times.$$

Enfin, l'application exponentielle $\exp : \mathbb{R} \to \mathbb{R}_{>0}$ induit un isomorphisme

$$\mathbb{R} \simeq \mathbb{R}_{>0},$$

et le groupe additif $\mathbb{R}$ a déjà étudié. Notons que l'exponentielle est continue d'inverse (le logarithme) continu : c'est un homéomorphisme, de sorte que les sous-groupes fermés de $\mathbb{R}_{>0}$ (pour la topologie usuelle) se déduisent aussi de ceux de $\mathbb{R}$: ce sont donc $\mathbb{R}_{>0}$ et les $a^{\mathbb{Z}}$ avec $a \in \mathbb{R}_{>0}$. On note enfin $\mathbb{U}$, $\mathrm{U}(1)$ ou S^1 le sous-groupe des éléments de $\mathbb{C}^\times$ de valeur absolue 1 (*cercle unité*). La multiplication dans $\mathbb{C}^\times$ induit un isomorphisme

$$\mathbb{R}_{>0} \times \mathbb{U} \xrightarrow{\sim} \mathbb{C}^\times.$$

Décrivons les sous-groupes de $\mathbb{U}$. On considère pour cela l'application

$$\psi : \mathbb{R} \to \mathbb{U},\ x \mapsto e^{2i\pi x}.$$

C'est un morphisme de groupes, surjectif de noyau $\mathbb{Z}$. Elle induit donc un isomorphisme de groupes

$$\mathbb{R}/\mathbb{Z} \simeq \mathbb{U},\ x + \mathbb{Z} \mapsto e^{2i\pi x}.$$

En particulier, tout sous-groupe H de $\mathbb{U}$ est de la forme $H = \psi(H')$ où H' est un sous-groupe de $\mathbb{R}$ contenant $\mathbb{Z}$ (Proposition 2.10 Chap. 1), et on a alors $H' = \psi^{-1}(H)$. Nous nous sommes donc encore ramenés aux sous-groupes de $\mathbb{R}$. Là encore, les sous-groupes fermés de $\mathbb{U}$ (pour la topologie usuelle) sont les plus raisonnables. Rappelons que $\mu_n \subset \mathbb{C}^\times$ désigne le sous-groupe (cyclique d'ordre n) des racines n-èmes de l'unité.

Proposition 7.4. *Les sous-groupes fermés de $\mathbb{U}$ sont $\mathbb{U}$ et les μ_n avec $n \geqslant 1$.*

Démonstration — Si H est un sous-groupe fermé de $\mathbb{U}$ alors, par continuité de ψ, $H' = \psi^{-1}(H)$ est un sous-groupe fermé de $\mathbb{R}$. Si $H' = \mathbb{R}$ on a $H = \psi(H') = \mathbb{U}$. Sinon, il existe $\lambda \in \mathbb{R}$ tel que $H' = \mathbb{Z}\lambda$. Mais on a aussi $H' \supset \ker\psi = \mathbb{Z}$, donc il existe $n \in \mathbb{Z}$ tel que $n\lambda = 1$, *i.e.* $\lambda = 1/n$. Cela montre $H = \psi(\mathbb{Z}\frac{1}{n}) = \mu_n$. □

Remarque 7.5. (Groupes topologiques) Un *groupe topologique* est la donnée d'un groupe G, et d'une topologie sur l'ensemble G, tels que la loi de groupe $G \times G \to G, (x, y) \mapsto xy$ et l'inversion $G \to G, x \mapsto x^{-1}$, soient continues. Quand $k = \mathbb{R}$ ou $\mathbb{C}$, auquel cas on le note souvent $\mathbb{K}$, c'est le cas des groupes additifs $\mathbb{K}$ et $\mathbb{K}^n$ (topologie d'espace vectoriel normé) et aussi du groupe multiplicatif $\mathbb{K}^\times$, et plus généralement de $\mathrm{GL}_n(\mathbb{K})$ (ouvert de l'espace vectoriel normé $\mathrm{M}_n(\mathbb{K})$ défini par $\det \neq 0$). Dans tous ces cas, comme on l'a entrevu, les sous-groupes *fermés* sont alors les plus pertinents à considérer. Les outils idoines pour les étudier sont les notions de *groupes de Lie* et d'*algèbre de Lie*. Bien entendu, ces notions n'ont pas leur place dans un cours introductif comme celui-ci, et c'est pourquoi nous restreindrons le plus souvent dans ce cours à l'étude de leurs sous-groupes finis (voire *discrets*), sur lesquels les notions de Lie ne disent absolument rien par ailleurs (en fait, c'est même le cas le plus difficile !).

8. Complément II : Groupes libres

Soit X un ensemble. On se propose dans ce complément d'introduire le *groupe libre sur* X. Le cas où X est fini sera déjà très intéressant. Pensons à X comme à un alphabet et introduisons l'ensemble des *mots sur* X comme étant

$$\mathrm{Mots}(X) = \coprod_{n \geqslant 0} X^n.$$

Par convention, on a posé ici $X^0 = \{1\}$, et on note aussi $\varnothing$ son unique élément 1, appelé *mot vide*. Un élément de $X^n \subset \mathrm{Mots}(X)$ sera appelé *mot de longueur* n sur X, et on notera simplement $x_1 \cdots x_n$ le n-uplet $(x_1, \cdots, x_n)$. On définit une loi de composition sur $\mathrm{Mots}(X)$ par la concaténations des mots :

$$X^n \times X^m \to X^{n+m}, (x_1 \cdots x_n, y_1 \cdots y_m) \mapsto x_1 \cdots x_n y_1 \cdots y_n.$$

Cette loi est manifestement associative, de neutre le mot vide $\varnothing$, et fait donc de $\mathrm{Mots}(X)$ un monoïde. On a une inclusion évidente $X \subset \mathrm{Mots}(X)$ (mots de longueur 1). La *propriété universelle* de $\mathrm{Mots}(X)$ est la suivante :

Proposition 8.1. *Soient X un ensemble et M un monoïde. Toute application $X \to M$ s'étend de manière unique en un morphisme de monoïdes* $\mathrm{Mots}(X) \to M$.

Démonstration — Soit $f : X \to M$ une application. Supposons que $g : \mathrm{Mots}(X) \to M$ est un morphisme de monoïdes vérifiant $g(x) = f(x)$ pour $x \in X$. On a $g(\varnothing) = 1$ par définition et, pour $n \geqslant 1$ et $x_1, \ldots, x_n \in X$, on a

$$g(x_1 \cdots x_n) = g(x_1) \cdots g(x_n) = f(x_1) \cdots f(x_n),$$

de sorte que g est uniquement déterminé par f : c'est l'assertion d'unicité. Pour l'existence de g, on pose simplement $g(\varnothing) = 1$ et pour $n \geqslant 1$, $g(x_1, \ldots, x_n) = f(x_1) \cdots f(x_n)$: c'est clairement un morphisme de monoïdes étendant f. □

On pose maintenant $X^{\pm} = X \coprod X$. On a deux inclusions naturelles $X \to X^{\pm}$, à *gauche* et à *droite*. Pour fixer les idées on écrira $X \subset X^{\pm}$ l'inclusion dans le X de gauche. Tout élément $x \in X^{\pm}$ dans la copie de X à gauche (resp. droite) a un correspondant que l'on notera x^{-1} dans celle de droite (resp. de gauche). On a ainsi défini une involution $X^{\pm} \to X^{\pm}, x \mapsto x^{-1}$, échangeant les deux facteurs. Nous voudrons à terme penser à x^{-1} comme à un inverse de x, mais prenons garde que cela n'en est pas un dans le monoïde $\mathrm{Mots}(X^{\pm})$. Par exemple si $X = \{a, b\}$ a deux éléments, on a $X^{\pm} = \{a, a^{-1}, b, b^{-1}\}$ et les $2^4 = 16$ mots de longueur 2 sur $X^{\pm}$ sont

$$aa,\ aa^{-1},\ ab,\ ab^{-1},\ a^{-1}a,\ a^{-1}a^{-1},\ a^{-1}b,\ a^{-1}b^{-1},\ ba,\ ba^{-1},\ bb,\ bb^{-1},\ b^{-1}a,\ b^{-1}a^{-1},\ b^{-1}b,\ b^{-1}b^{-1}.$$

Au final, on retiendra qu'en définissant $X^{\pm}$ on a simplement « dédoublé l'alphabet X en rajoutant formellement, pour chaque lettre $x \in X$, la lettre x^{-1} ». Nous renvoyons à l'Exercice 1.1 pour la notion précise de relation d'équivalence engendrée par une relation, utilisée ci-dessous.

Définition 8.2. *Si m et m' sont deux mots sur $X^{\pm}$, on dit que m est une* contraction élémentaire *de m', et on note $m\,C\,m'$, s'il existe $n_1, n_2 \in \mathrm{Mots}(X^{\pm})$ et $x \in X^{\pm}$ tels que $m = n_1 n_2$ et $m' = n_1 x x^{-1} n_2$. On note R la relation d'équivalence sur $\mathrm{Mots}(X^{\pm})$ engendrée par la relation C, et on note l'ensemble quotient associé*

$$\mathrm{F}_X = \mathrm{Mots}(X^{\pm})/R.$$

On dira simplement que deux mots sur $X^{\pm}$ sont *équivalents* s'ils le sont pour R, et on notera $[m]$ la classe d'équivalence de m. Par définition, deux mots sont équivalents si l'un s'obtient à partir de l'autre après une suite finie d'insertions ou suppressions de morceaux de la forme xx^{-1} avec $x \in X^{\pm}$. Il découle facilement des définitions que « la multiplication des mots passe aux classes d'équivalence » :

LEMME 8.3. *Soit M un monoïde, C une relation sur M et R la relation d'équivalence sur M engendrée par C. On suppose que pour tout $m, m', n \in M$ avec $m\,C\,m'$, on a : (i) $mn\,R\,m'n$ et (ii) $nm\,R\,nm'$. Alors il existe une unique loi de monoïde sur M/R telle que la projection canonique $M \to M/R$ est un morphisme de monoïde.*

DÉMONSTRATION — Soit $\pi : M \to M/R$ la projection canonique. Toute loi de composition $\star$ sur M/R telle que π est un morphisme vérifie $[m]_R \star [m']_R = \pi(m) \star \pi(m') = \pi(mm') = [mm']_R$. Comme π est surjective, $\star$ est donc unique si elle existe, nécessairement associative car la loi de M l'est, et admet $\pi(1) = [1]_R$ pour neutre.

Pour l'existence, il s'agit de montrer que l'application $M \times M \to M/R$, $(m, n) \mapsto [mn]_R$, passe au quotient $M/R \times M/R \to M/R$, c'est-à-dire que pour tous éléments m, m', n, n' dans M vérifiant $m\,R\,m'$ et $n\,R\,n'$, on a $mn\,R\,m'n'$. Fixons donc de tels $m, m', n, n' \in M$. Comme R est engendrée par C, on a une suite d'éléments $m_1, \ldots, m_r$ de M vérifiant $m_1 = m$, $m_r = m'$, et soit $m_i\,C\,m_{i+1}$, soit $m_{i+1}\,C\,m_i$ pour $1 \leqslant i < r$. Par l'hypothèse (i) sur C, on a donc $m_i n\,R\,m_{i+1} n$ pour $1 \leqslant i < r$, puis $m_1 n\,R\,m_r n$ par transitivité de R, *i.e.* $mn\,R\,m'n$. Raisonnant de même en utilisant (ii) au lieu de (i), on montre aussi $m'n\,R\,m'n'$, et donc $mn\,R\,m'n'$. □

Ce lemme s'applique bien sûr à $M = \mathrm{Mots}(X^{\pm})$ et à sa relation de contraction C : pour tout $m, m', n \in M$ avec $m\,C\,m'$, on a même $mn\,C\,m'n$ et $nm\,C\,nm'$. Il existe donc une unique structure de monoïde sur F_X telle que la surjection naturelle

$$\mathrm{Mots}(X^{\pm}) \to \mathrm{F}_X,\ m \mapsto [m], \tag{9}$$

est un morphisme de monoïdes. Mais par définition de C on a aussi $[x][x^{-1}] = [xx^{-1}] = 1 = [x^{-1}x] = [x^{-1}][x]$ pour tout $x \in X^{\pm}$, de sorte que $[x^{-1}]$ est un inverse de $[x]$ dans F_X, ce qui était l'effet recherché ! Mais comme $X^{\pm}$ engendre le monoïde $\mathrm{Mots}(X)$, les $[x]$ avec $x \in X^{\pm}$ engendrent aussi F_X, qui est donc un groupe :

DÉFINITION 8.4. *Le groupe* F_X *ainsi défini est* le groupe libre sur X.

Le F dans F_X vient de l'anglais *free group*. Par construction, la projection canonique (9) induit par restriction aux inclusions naturelles $X \to X^{\pm} \to \mathrm{Mots}(X^{\pm})$ une application $X \to \mathrm{F}_X, x \mapsto [x]$. La *propriété universelle de* F_X est la suivante :

PROPOSITION 8.5. *Soient X un ensemble et G un groupe. Pour toute application $f : X \to G$, il existe un unique morphisme de groupes $f' : \mathrm{F}_X \to G$ tel que $f'([x]) = f(x)$ pour tout $x \in X$.*

DÉMONSTRATION — Le morphisme f' est unique s'il existe car les $[x]$ avec $x \in X$ engendrent le groupe F_X. Pour l'existence, on étend d'abord f en une application encore notée $f : X^{\pm} \to G$ en posant $f(x^{-1}) = f(x)^{-1}$ pour $x \in X$. Par la Proposition 8.1, il existe un morphisme de monoïdes $g : \mathrm{Mots}(X^{\pm}) \to G$ tel que $g(x) = f(x)$ et $g(x^{-1}) = f(x)^{-1}$ pour $x \in X$, et donc avec $g(x^{-1}) = g(x)^{-1}$ pour tout $x \in X^{\pm}$.

Supposons que l'on ait $m, m' \in \mathrm{Mots}(X^{\pm})$ avec m contraction élémentaire de m'. On a $m' = n_1 x x^{-1} n_2$ et $m = n_1 n_2$, avec $x \in X^{\pm}$ et n_1, n_2 des mots sur $X^{\pm}$, puis

$$g(m') = g(n_1)g(x)g(x)^{-1}g(n_2) = g(n_1)g(n_2) = g(m).$$

Cela montre que g est constante sur les classes d'équivalence de mots sur $X^{\pm}$, et donc induit par passage au quotient une application $f' : \mathrm{F}_X \to G$ vérifiant $f'([m]) = g(m)$ pour tout $m \in \mathrm{Mots}(X^{\pm})$. Par définition de la loi quotient sur F_X, c'est automatiquement un morphisme de groupes : pour $m, m' \in \mathrm{Mots}(X^{\pm})$ on a les égalités $f'([m][m']) = f'([mm']) = g(mm') = g(m)g(m') = f'([m])f'([m'])$. □

La notion suivante de *mot réduit* nous donnera au final un représentant naturel de chaque classe d'équivalence de mots sur $X^{\pm}$:

Définition 8.6. *Un mot sur $X^{\pm}$ est dit réduit s'il est vide ou de la forme $x_1 \dots x_n$ avec $x_i \in X^{\pm}$ pour $1 \leqslant i \leqslant n$ et $x_{i+1} \neq x_i^{-1}$ pour $1 \leqslant i < n$.*

Par exemple, pour $a, b \in X$ les mots abb^{-1} et $a^{-1}ab$ ne sont pas réduits, mais aba^{-1} l'est pour $a \neq b$. Un mot de longueur $\leqslant 1$ est trivialement réduit. Il est clair que tout mot sur $X^{\pm}$ est équivalent à un mot réduit : considérer par exemple un mot de longueur minimale dans sa classe d'équivalence. Il est moins évident, mais vrai, que deux mots réduits distincts ne sont pas équivalents.

Théorème 8.7. *L'application canonique* $\mathrm{Mots}(X^{\pm}) \to \mathrm{F}_X, m \mapsto [m]$, *induit une bijection entre le sous-ensemble des mots réduits sur $X^{\pm}$ et F_X.*

Démonstration — La surjectivité a déjà été justifiée. Montrons l'injectivité. Pour tout $x \in X^{\pm}$, et tout mot m sur $X^{\pm}$, on définit $\mathrm{L}_x(m)$ comme suit : si m ne commence pas par x^{-1} on pose $\mathrm{L}_x(m) = xm$, sinon on a $m = x^{-1}n$ pour un unique mot n et on pose $\mathrm{L}_x(m) = n$. Observons que si m est réduit, il en va de même de $\mathrm{L}_x(m)$. De plus, on a $\mathrm{L}_{x^{-1}}(\mathrm{L}_x(m)) = m$ pour tout mot réduit m. En effet, si $m = x^{-1}n$ on a $\mathrm{L}_{x^{-1}}(\mathrm{L}_x(m)) = \mathrm{L}_{x^{-1}}(n) = x^{-1}n = m$ car n ne commence pas par x, et si m ne commence pas par x^{-1} on a $\mathrm{L}_{x^{-1}}(\mathrm{L}_x(m)) = \mathrm{L}_{x^{-1}}(xm) = m$. Ainsi, si $\Omega \subset \mathrm{Mots}(X^{\pm})$ désigne le sous-ensemble des mots réduits, on a défini une application

$$f : X \to \mathrm{S}_\Omega,\ x \mapsto \mathrm{L}_x.$$

Par la propriété universelle du groupe libre, il existe donc un morphisme de groupes $f' : \mathrm{F}_X \to \mathrm{S}_\Omega$ envoyant $[x]$ sur L_x pour tout $x \in X^{\pm}$. Soit $m = x_1 \cdots x_r \in \Omega$. On a $[m] = [x_1] \cdots [x_r]$ dans F_X, et donc $f'([m]) = \mathrm{L}_{x_1} \circ \cdots \circ \mathrm{L}_{x_r}$. Mézalor on constate

$$f'([m])(\varnothing) = \mathrm{L}_{x_1} \circ \cdots \circ \mathrm{L}_{x_r}(\varnothing) = \mathrm{L}_{x_1} \circ \cdots \circ \mathrm{L}_{x_{r-1}}(x_r) = \cdots = x_1 \cdots x_r = m,$$

car on a $x_i \neq x_{i+1}^{-1}$ pour $1 \leqslant i < r$. Ainsi, pour $m, m' \in \Omega$ avec $[m] = [m']$, on a $f'([m']) = f'([m])$, et donc $m = f'([m])(\varnothing) = f'([m'])(\varnothing) = m'$. □

En particulier, l'application naturelle $X^{\pm} \to \mathrm{F}_X, x \mapsto [x]$, est injective : on fait très souvent l'abus de langage de noter simplement x la classe $[x]$, ou encore

$$X^{\pm} \subset \mathrm{F}_X.$$

On a clairement $F_X = \{1\}$ pour $X = \varnothing$. Si $X = \{x\}$ est un singleton, les (classes des) mots réduits sur X sont les x^n avec $n \in \mathbb{Z}$, et on a donc un isomorphisme

$$\mathbb{Z} \xrightarrow{\sim} \mathrm{F}_X,\ n \mapsto x^n, \quad \text{si } X = \{x\},$$

d'après le Théorème 8.7. En revanche, pour $|X| \geqslant 2$, le groupe F_X est non commutatif : pour $a \neq b$ dans X, les (classes des) deux mots réduits ab et ba sont distincts dans F_X toujours par le théorème. Par la propriété universelle du groupe libre, *toute application $X \to Y$ (resp. bijection) induit un morphisme (resp. isomorphisme) de groupes* $\mathrm{F}_X \to \mathrm{F}_Y$. Cela donne sens à la seconde définition suivante.

Définition 8.8. *Un groupe G est dit* libre *s'il est isomorphe à F_X pour un certain X. Pour $n \geqslant 1$, on note F_n un groupe libre sur un ensemble à n éléments.*

Il est aisé de vérifier à l'aide du Théorème 8.7, que pour $X \subset Y$ le morphisme naturel $\mathrm{F}_X \to \mathrm{F}_Y$ est injectif. En particulier, F_n est isomorphe à un sous-groupe de F_m pour $n \leqslant m$. De plus, la théorie des *groupes abéliens libres* vue au chapitre suivant permettra de montrer simplement que $\mathrm{F}_n \simeq \mathrm{F}_m$ implique $n = m$. De manière plus intéressante, on peut montrer que pour tout $n \geqslant 3$, le groupe F_n est isomorphe à un sous-groupe de F_2, que l'on peut même choisir distingué d'indice $n-1$ (Nielsen-Schreier). Par exemple, le sous-groupe $\langle a^2, ab, b^2 \rangle$ du groupe F_2 libre sur $\{a, b\}$ est d'indice 2 (il coïncide avec les classes de mots de longueur paire sur $\{a, b\}^{\pm}$), et il est isomorphe à F_3 (ce n'est pas évident !).

Remarque 8.9. *Nielsen et Schreier ont montré plus généralement que* tout sous-groupe d'un groupe libre est isomorphe à un groupe libre*, et aussi que tout sous-groupe d'indice d de F_n est isomorphe à F_m avec $m = d(n-1)+1$. Pour démontrer ce type de résultats, il est commode d'avoir une approche plus géométrique à la construction de F_X, qui sera abordée en cours de topologie algébrique. Par exemple, le groupe F_2 est isomorphe au groupe fondamental de la figure* ∞.

Terminons cette courte introduction au groupe libre en discutant la notion de groupe défini par générateurs et relations. Soient G un groupe ainsi que $\{g_x\}_{x \in X}$ une famille d'éléments de G indexée par un ensemble X. Par propriété universelle de F_X, il existe un unique morphisme de groupes

$$f : \mathrm{F}_X \to G, \text{ avec } f(x) = g_x \ \ \forall x \in X. \tag{10}$$

Définition 8.10. *Dans le contexte de* (10) *ci-dessus, on dit qu'un mot $m \in \mathrm{Mots}(X^{\pm})$ est une* relation *entre les g_x si on a $f([m]) = 1$. Tout mot m' équivalent à une relation m entre les g_x est bien sûr encore une relation entre les g_x, de sorte que l'on dira aussi que $[m] \in \mathrm{F}_X$ est une relation entre les g_x.*

L'ensemble de toutes les relations entre les g_x est donc simplement $\ker f \subset \mathrm{F}_X$. Comme les $x \in X$ engendrent F_X, le morphisme est surjectif si, et seulement si, les g_x engendrent G, auquel cas on a alors bien sûr $\mathrm{F}_X / \ker f \simeq G$.

Exemple 8.11. Dans tout groupe commutatif G, le mot $aba^{-1}b^{-1}$ est une relation entre a et $b \in G$. Dans tout groupe G d'ordre n, et $g \in G$, le mot g^n est une relation satisfaite par g (Lagrange), ainsi que les mot g^{-n}, g^{2n} etc... Dans le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, les mots a^2, b^4 et $aba^{-1}b^{-1}$ sont des relations entre $a = (1, 0)$ et $b = (0, 1)$. Nous verrons plus d'exemples quand nous aurons vu plus de groupes !

En pratique, on s'intéresse à trouver des générateurs du sous-groupe $\ker f$ des relations entre les g_x. Une construction utile à ce sujet est la suivante. Observons d'abord que pour toute partie X d'un groupe G, il existe un plus petit sous-groupe *distingué* de G contenant X, à savoir le sous-groupe engendré par $\cup_{g \in G} gXg^{-1}$. Nous le noterons $\langle X \rangle^{\lhd}$.

Définition 8.12. *Soient $\mathscr{G}$ un ensemble et $\mathscr{R} \subset \mathrm{Mots}(\mathscr{G}^{\pm})$ un sous-ensemble. Le groupe quotient $\mathrm{F}_{\mathscr{G}}/\langle\mathscr{R}\rangle^{\lhd}$ est appelé* groupe défini par les générateurs $\mathscr{G}$ et par les relations $\mathscr{R}$ *; on le note aussi $\langle \mathscr{G} \mid r = 1,\ \forall r \in \mathscr{R}\rangle$.*

Lorsque $\mathscr{G}$ et $\mathscr{R}$ sont finis, disons $\mathscr{G} = \{g_1, \ldots, g_n\}$ (tous distincts) et $\mathscr{R} = \{r_1, \ldots, r_s\}$, on le note aussi $\langle g_1, \ldots, g_n \mid r_1 = r_2 = \cdots = r_s = 1\rangle$. La propriété universelle d'un groupe défini par générateurs et relations est alors la suivante.

Proposition 8.13. *Soient $\mathscr{G}$ un ensemble, $\mathscr{R} \subset \mathrm{Mots}(\mathscr{G}^{\pm})$ et G un groupe. Il est équivalent de se donner un morphisme de groupes $\langle \mathscr{G} \mid r = 1,\ \forall r \in \mathscr{R}\rangle \to G$ et une application $f : \mathscr{G} \to G$ telle que $f(r) = 1$ pour tout $r \in \mathscr{R}$.*

Démonstration — On applique simplement la propriété universelle du groupe quotient (Proposition 6.16 Chap. 1), puis celle du groupe libre (Proposition 8.5). □

Exemple 8.14. *Pour tout entier $n \geqslant 1$ on a des isomorphismes*

$$\langle a \mid a^n = 1\rangle \simeq \mu_n \quad \text{et} \quad \langle a, b \mid aba^{-1}b^{-1} = 1\rangle \simeq \mathbb{Z} \times \mathbb{Z}.$$

Démonstration — Soit $G_1 = \langle a \mid a^n = 1\rangle$. Par la propriété universelle, il existe un unique morphisme de groupes $f : G_1 \to \mu_n$ envoyant a sur $\zeta := e^{2i\pi/n}$, car on a $\zeta^n = 1$. Ce morphisme est surjectif car ζ engendre μ_n. Mais comme (la classe de) a engendre G_1, avec $a^n = 1$, tout élément de G_1 est de la forme a^m avec $0 \leqslant m < n$, puis $|G_1| \leqslant n$, et f est bijectif pour des raisons de cardinal.

Soit $G_2 = \langle a, b \mid aba^{-1}b^{-1} = 1\rangle$. Par la propriété universelle, il existe un unique morphisme de groupes $f : G_2 \to \mathbb{Z} \times \mathbb{Z}$ envoyant a sur $(1, 0)$ et b sur $(0, 1)$, car $(1, 0)$ et $(0, 1)$ commutent dans le groupe (abélien) $\mathbb{Z} \times \mathbb{Z}$. Mais comme (les classes de) a et b engendrent G_2, et que l'on a $ab = ba$ par construction, tout élément x de G_2 s'écrit $a^m b^n$ avec $m, n \in \mathbb{Z}$. Mézalor on constate $f(x) = f(a)^m f(b)^n = (m, n) \in \mathbb{Z}^2$, de sorte que l'écriture $x = a^m b^n$ est unique, et f est bijective. □

Exemple 8.15. *On a $\langle i,\ j,\ \epsilon \mid\ i^2 = \epsilon,\ j^2 = \epsilon,\ \epsilon^2 = 1,\ ij = \epsilon ji\} \simeq \mathrm{H}_8$.*

Démonstration — Soit G le groupe de gauche défini par générateurs et relations. Comme on a $I^2 = J^2 = -1$ et $IJ = -JI$ dans H_8, la propriété universelle de G montre qu'il existe un unique morphisme de groupes $f : G \to \mathrm{H}_8$ vérifiant $f(i) = I$, $f(j) = J$ et $f(\epsilon) = -1$. Ce morphisme est surjectif car I et J engendrent H_8. Pour voir qu'il est injectif, il suffit donc de voir $|G| \leqslant 8$.

Par définition, G est engendré par i, j et ϵ, avec $i^2 = j^2 = \epsilon$, $\epsilon^2 = 1$ et $ji = \epsilon ij$. Ces relations montrent que tout élément de G est de la forme $i^a\, j^b\, \epsilon^c$ avec $0 \leqslant a, b, c \leqslant 1$. On a donc bien $|G| \leqslant 2^3 = 8$, et au final, un isomorphisme $f : G \simeq \mathrm{H}_8$. □

Remarque 8.16. *Étant donné un groupe G, un isomorphisme*

$$\langle \mathscr{G} \mid r = 1,\ \forall r \in \mathscr{R}\rangle \xrightarrow{\sim} G$$

s'appelle une présentation *de G (par les générateurs $\mathscr{G}$ et les relations $\mathscr{R}$).*

9. Exercices

On commence par quelques exercices sur les axiomes et les monoïdes.

Exercice 2.1. (Quelques cas où l'existence des inverses est automatique)

(i) Un monoïde M est dit régulier *si pour tout $x, y, z \in M$, on a $xy = xz \Rightarrow y = z$. Montrer qu'un monoïde régulier fini est un groupe.*

(ii) Un anneau A est dit intègre *si pour tout $a, b \in A$ on a $ab = 0 \Rightarrow a = 0$ ou $b = 0$. Montrer qu'un anneau intègre fini est à division.*

(iii) Montrer que si G est un groupe fini, et si H est une partie de G, alors H est un sous-groupe si, et seulement si, H est non vide et stable par produits.

Si M est un monoïde et $m \in M$, on pose $\langle m \rangle = \{m^n \mid n \in \mathbb{N}\}$ (sous-monoïde engendré par m). On dit que M est *monogène* s'il existe $m \in M$ tel que $M = \langle m \rangle$.

Exercice 2.2. *Soient $n \geqslant 1$ un entier et $\mathrm{F}(n)$ le monoïde des fonctions de $\{0, 1, \ldots, n-1\}$ dans lui-même pour la composition $\circ$. Pour $0 \leqslant i < n$, on note $f_i \in \mathrm{F}(n)$ la fonction définie par $f_i(j) = j + 1$ pour $0 \leqslant j < n - 1$ et $f_i(n-1) = i$.*

(i) On pose $M_i = \langle f_i \rangle$. Montrer $|M_i| = n$.

(ii) (suite) Montrer $M_i \simeq M_j \iff i = j$.

(iii) Montrer qu'à isomorphisme près, il existe exactement n monoïdes monogènes de cardinal n.

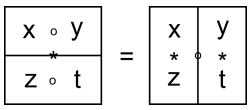
Exercice 2.3. (Monoïdes de cardinal $\leqslant 3$)

(i) Montrer qu'à isomorphisme près, il existe exactement 2 monoïdes de cardinal 2, à savoir $(\mathbb{Z}/2\mathbb{Z}, +)$ et $(\mathbb{Z}/2\mathbb{Z}, \times)$.

(ii) Soit M un monoïde à 3 éléments. Montrer que soit M est monogène, soit on a $M \simeq (\mathbb{Z}/3\mathbb{Z}, \times)$, soit on a $x^2 = x$ pour tout $x \in M$.

(iii) En déduire qu'à isomorphisme près, il existe exactement 7 monoïdes de cardinal 3.

Exercice 2.4. (L'argument de Eckmann-Hilton) *Soit X un ensemble muni de deux lois unitaires $\circ$ et $\star$ avec $(x \circ y) \star (z \circ t) = (x \star z) \circ (y \star t)$ pour tout $x, y, z, t \in X$. Montrer $\circ = \star$, et que ces lois sont associatives et commutatives.*



Exercice 2.5. (*Sous-monoïdes de $(\mathbb{N}, +)$, partie I*)

(i) Soient $m, n \in \mathbb{N}$ premiers entre eux. Montrer que tout élément de $\mathbb{Z}$ s'écrit de manière unique sous la forme $am + bn$ avec $a, b \in \mathbb{Z}$ et $0 \leqslant b < m$.

(ii) (suite) En déduire que $\mathbb{N}m + \mathbb{N}n$ contient tous les entiers $> mn - m - n$, mais pas $mn - m - n$.

(iii) Soient $m_1, \ldots, m_n \in \mathbb{N}$ non nuls et premiers entre eux. Montrer qu'il existe un $r \in \mathbb{N}$ tel que $\mathbb{N}m_1 + \mathbb{N}m_2 + \cdots + \mathbb{N}m_n$ contient tous les entiers $\geqslant r$.

(iv) (suite) Pour $k \in \mathbb{N}$ on note f_k le nombre de n-uples $(a_1, \ldots, a_n) \in \mathbb{N}^n$ avec $k = a_1 m_1 + a_2 m_2 + \cdots + a_n m_n$. Montrer $f_k = \frac{k^{n-1}}{m_1 \cdots m_n} + \mathrm{O}(k^{n-2})$ pour $k \to \infty$ (Schur). On pourra examiner les pôles de la fraction rationnelle $\prod_{i=1}^n \frac{1}{1-z^{m_i}}$.

Exercice 2.6. (*Sous-monoïdes de $(\mathbb{N}, +)$, partie II*) *Un sous-monoïde M de $\mathbb{N}$ sera dit primitif si on a $M \neq \{0\}$ et si le pgcd de tous les éléments de M est 1.*

(i) Montrer qu'un sous-monoïde de $\mathbb{N}$ est primitif si, et seulement si, il contient tous les entiers $\geqslant r$ pour un certain $r \geqslant 0$.

(ii) Montrer que tout sous-monoïde de $\mathbb{N}$ est finiment engendré.

(iii) Montrer que deux sous-monoïdes primitifs de $\mathbb{N}$ isomorphes sont égaux.

(iv) En déduire qu'il existe une infinité de sous-monoïdes de $\mathbb{N}$ engendrés par 2 éléments, et deux à deux non isomorphes.

Soient M un monoïde et $x, y \in M$. On dit que y est un *inverse à droite* (resp. *inverse à gauche*) de x si on a $xy = 1$ (resp. $yx = 1$).

Exercice 2.7. (Neutres et inverses partiels) *Soient X un ensemble et M le monoïde des fonctions $X \to X$ pour la composition $\circ$.*

(i) Caractériser les éléments $f \in M$ ayant un inverse à droite (resp. à gauche).

(ii) Montrer que si X est infini alors M possède un élément ayant une infinité d'inverses à droite (resp. à gauche).

(iii) Montrer que dans tout monoïde, si un élément admet à la fois un inverse à droite et un inverse à gauche, alors ils sont égaux et uniques.

(iv) Caractériser les éléments $e \in M$ vérifiant $e^2 = e$. De plus, pour $e \in M$ avec $e^2 = e$, caractériser les $f \in M$ vérifiant $ef = f$ (resp. $fe = f$).

(v) Soit $e \in M$ vérifiant $e^2 = e$. Vérifier que $\circ$ induit une loi de composition associative sur eM, avec $e \in eM$ et $ex = x$ pour tout $x \in eM$. Montrer que e est un élément neutre de $(eM, \circ)$ si, et seulement si, on a $e = 1$ ou $|\mathrm{Im}\, e| = 1$.

Les exercices qui suivent portent sur les produits de parties et de groupes.

Exercice 2.8. *Soient G un groupe et H, K deux sous-groupes de G. On considère l'application $f : H \times K \to G$, $(h, k) \mapsto hk$. Donner une condition nécessaire et suffisante portant sur H et K pour que f soit respectivement :*

(i) un morphisme de groupes,

(ii) injective,

(iii) surjective,

(iv) un isomorphisme de groupes.

Exercice 2.9. *Soient G un groupe et H, K deux sous-groupes finis de G.*

(i) Montrer $|HK| = \frac{|H||K|}{|H \cap K|}$.

(ii) On suppose $|H|$ et $|K|$ premiers entre eux. Montrer $|HK| = |H|\,|K|$.

Exercice 2.10. *Soient G un groupe et H, K deux sous-groupes de G.*

(i) Montrer que HK est un sous-groupe de G, si et seulement si, $HK = KH$.

(ii) Donner un exemple où HK n'est pas un sous-groupe de G.

(iii) On suppose $H \lhd G$. Montrer que HK est un sous-groupe de G.

Exercice 2.11. *Soient G un groupe et H, K deux sous-groupes distingués avec $H \cap K = \{1\}$ et $G = HK$. Montrer que G est produit direct interne de H et K.*

Exercice 2.12. (Vrai ou faux) *Soient G un groupe et H, K deux sous-groupes de G avec $G = HK$. Une seule des affirmations suivantes est fausse : laquelle ?*

(i) On a $G = KH$.

(ii) Pour tout $a, b \in G$, on a $G = (aHa^{-1})(bKb^{-1})$.

(iii) Supposons $G = HL$ avec L un sous-groupe de G, ainsi que $H \cap K = H \cap L = \{1\}$, alors on a $K = L$.

Exercice 2.13. (Propriété universelle[11] des produits) *Soit $\{G_i\}_{i \in I}$ une famille de groupes. On pose $P = \prod_{i \in I} G_i$ (groupe produit), et pour $j \in I$, on note $\pi_j : P \to G_j, (g_i)_i \mapsto g_j$ la projection canonique. Vérifier $\pi_j \in \mathrm{Hom}(P, G_j)$ et montrer que pour tout groupe G, l'application $\mathrm{Hom}(G, P) \to \prod_{i \in I} \mathrm{Hom}(G, G_i)$, $f \mapsto (\pi_i \circ f)_i$, est bijective.*

L'exercice qui suit est un contre-exemple à la philosophie (pas si mauvaise) qui consiste à penser que tout énoncé trés général en théorie des groupes est soit faux, soit trivialement vrai, soit extrêmement difficile !

Exercice 2.14. *Soient G, H et K des groupes finis vérifiant $G \times H \simeq G \times K$. On se propose de montrer $H \simeq K$. Pour deux groupes X, Y, on notera $\mathrm{Inj}(X, Y) \subset \mathrm{Hom}(X, Y)$ le sous-ensemble des morphismes injectifs.*

(i) Montrer que pour tout groupe fini S, on a $|\mathrm{Hom}(S, H)| = |\mathrm{Hom}(S, K)|$.

(ii) En déduire que pour tout groupe fini S, on a $|\mathrm{Inj}(S, H)| = |\mathrm{Inj}(S, K)|$.

(iii) Conclure.

(iv) Donner un exemple de groupe infini G vérifiant $G \times \mathbb{Z}/2\mathbb{Z} \simeq G \simeq G \times G$.

Exercice 2.15. (Anneau de Boole) *Si X est un ensemble, on considère la loi Δ sur $\mathrm{P}(X)$ définie par $A \,\Delta\, B = (A \cup B) \smallsetminus (A \cap B)$* (différence symétrique). *Montrer que $(\mathrm{P}(X), \Delta, \cap)$ est un anneau, naturellement isomorphe à l'anneau produit $(\mathbb{Z}/2\mathbb{Z})^X$.*

On donne maintenant deux premiers exercices sur le groupe des isométries d'un espace euclidien E. On rappelle que si H est un hyperplan affine de E, et si D désigne la droite vectorielle de E orthogonale à la direction de H, la *reflexion affine* d'hyperplan H est l'isométrie τ_H de E donnée par la formule $\tau_H(h + d) = h - d$ pour tout $d \in D$ et tout $h \in H$.

11. Étant donné un groupe connu H, c'est souvent une bonne idée que d'essayer de comprendre les $\mathrm{Hom}(H, G)$ ou $\mathrm{Hom}(G, H)$ (*propriété universelle du groupe H*).

Exercice 2.16. (Théorème de Cartan-Dieudonné) *Soient E un espace euclidien de dimension $n \geqslant 1$ et $f \in \mathrm{Iso}(E)$.*

(i) Montrer que l'ensemble $\mathrm{Fix}\, f$ *des points fixes de f est soit vide, soit un sous-espace affine de E.*

Si $\mathrm{Fix}\, f = \varnothing$ *on pose $p = -1$. Sinon, on pose $p = \dim \mathrm{Fix}\, f$.*

(ii) Montrer que f est produit d'au plus $n - p$ réflexions affines (Théorème de Cartan-Dieudonné).

(iii) En déduire que f est affine : on a $f(\lambda x + \mu y) = \lambda f(x) + \mu f(y)$ pour tout $x, y \in E$ et $\lambda, \mu \in \mathbb{R}$ avec $\lambda + \mu = 1$.

Exercice 2.17. *Soit $E = \mathbb{R}$ muni de la distance (euclidienne !) usuelle. On s'intéresse au groupe* $\mathrm{Iso}(1) = \mathrm{Iso}(E)$.

(i) Décrire les réflexions affines de E.

(ii) Montrer que tout élément non trivial de $\mathrm{Iso}(1)$ *est soit une translation, soit une réflexion affine.*

(iii) Montrer que l'on a $\mathrm{Iso}(1) = HK$ *avec H, K des sous-groupes vérifiant $H \simeq \mathbb{R}$ et $K \simeq \mathbb{Z}/2\mathbb{Z}$. A-t-on* $\mathrm{Iso}(1) \simeq \mathbb{R} \times \mathbb{Z}/2\mathbb{Z}$ *?*

Les exercices suivant traitent de la notion d'ordre d'un élément.

Exercice 2.18. *(i) Donner un exemple de groupe infini dont tous les éléments sont d'ordre fini.*

(ii) Donner un exemple de groupe possédant deux éléments a, b avec $a^2 = 1$, $b^2 = 1$ et ab d'ordre infini.

Exercice 2.19. (Cauchy abélien) *On suppose que le groupe abélien fini G est engendré par des éléments $x_1, \ldots, x_n$, avec x_i d'ordre d_i.*

(i) Montrer que $|G|$ divise $d_1 \ldots d_n$.

(ii) En déduire que si p premier divise $|G|$, alors G admet un élément d'ordre p.

Exercice 2.20. *Soient a et b des entiers avec $a, b \geqslant 3$. On pose $\zeta_n = e^{2i\pi/n}$ pour $n \geqslant 1$ et l'on considère les éléments A, B et U_t de* $\mathrm{SL}_2(\mathbb{C})$ *définis par*

$$A = \begin{pmatrix} \zeta_a & 0 \\ 0 & \zeta_a^{-1} \end{pmatrix} \quad B = \begin{pmatrix} 0 & -1 \\ 1 & \zeta_b + \zeta_b^{-1} \end{pmatrix} \quad \text{et} \quad U_t = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \quad \text{avec } t \in \mathbb{C}.$$

(i) Montrer que A est d'ordre a, et que B est d'ordre[12] *b, dans le groupe* $\mathrm{SL}_2(\mathbb{C})$.

(ii) On pose $B_t = U_t\, B\, U_t^{-1}$. Calculer la trace de AB_t.

(iii) On suppose $c \geqslant 3$ entier, ou $c = \infty$. Montrer que pour t bien choisi, le produit $A\, B_t$ est d'ordre c.

(iv) En travaillant[13] *dans $\mathbb{Z}/p\mathbb{Z}$ pour $p \equiv 1 \bmod abc$ (avec p premier), à la place du corps $\mathbb{C}$, montrer que pour tous entiers $a, b, c \geqslant 3$, il existe un groupe fini possédant un élément d'ordre a, un autre d'ordre b, de produit d'ordre c.*

12. Observer que si $g \in \mathrm{SL}_2(\mathbb{C})$ est de trace $x + x^{-1}$ avec $x \in \mathbb{C}^\times$, le polynôme caractéristique de g est $(X - x)(X - x^{-1})$.

13. Voir l'Exercice 2.41.

(v) Montrer que si l'on a g et h dans $\mathrm{GL}_2(\mathbb{C})$, avec g d'ordre 2, h d'ordre impair, et gh d'ordre fini, alors gh est d'ordre pair.

(vi) En se plaçant dans GL_3 ou dans le groupe quotient $\mathrm{SL}_2/\{\pm 1\}$, généraliser le (iv) à tout $a, b, c \geqslant 2$.

Exercice 2.21. (Propriétés universelles des groupes monogènes) *Soient G un groupe monogène engendré par l'élément $g \in G$ et H un groupe arbitraire. On considère l'application* $\mathrm{ev}_g : \mathrm{Hom}(G, H) \to H,\ f \mapsto f(g)$ (« évaluation en g ») .

(i) Montrer que ev_g est injective et que son image vaut H si G est infini, et $\{x \in G,\ x^N = 1\}$ si G est d'ordre $N \geqslant 1$.

(ii) On suppose H abélien. Montrer que ev_g est un morphisme de groupes.

Les exercices suivants portent sur les notions d'indice et de sous-groupe distingué.

Exercice 2.22. *Montrer que tout sous-groupe d'indice fini d'un groupe G contient un sous-groupe à la fois distingué et d'indice fini dans G.*

Exercice 2.23. *Soient H un sous-groupe distingué d'indice fini n de G, et $g \in G$. Montrer $g^n \in H$.*

Exercice 2.24. *Soient G un groupe et H un sous-groupe d'indice 2 de G. On suppose que G est engendré par $g_1, \ldots, g_n$. On considère la partition $\{1, \ldots, n\} = I \coprod J$ définie par $i \in I \iff g_i \in H$, et le sous-ensemble X de G suivant :*

$$X = \{g_i \mid i \in I\} \ \cup\ \{g_j g_{j'} \mid j, j' \in J\} \ \cup\ \{g_j g_i g_j \mid i \in I, j \in J\}.$$

Montrer que X est une famille génératrice de H.

Exercice 2.25. *Soient G un groupe et A, B deux sous-groupes de G.*

(i) On suppose $A \subset B$. Montrer $[G : A] = [G : B]\,[B : A]$, au sens où si deux de ces trois quantités sont finies, la troisième l'est aussi, et cette égalité est vérifiée.

(ii) Soit AB/B le sous-ensemble de G/B constitué des parties de la forme aB avec $a \in A$. Montrer que AB/B est en bijection naturelle avec $A/(A \cap B)$.

(iii) Montrer que si A et B sont d'indice fini dans G, il en va de même de $A \cap B$.

(iv) On suppose A et B d'indices finis et premiers entre eux. Montrer $G = AB$.

Exercice 2.26. (Centre et automorphismes intérieurs) *Soit G un groupe. On pose $\mathrm{Z}(G) = \{g \in G \mid gh = hg,\ \forall h \in G\}$ (le « centre » de G).*

(i) Montrer que $\mathrm{Int} : G \to \mathrm{Aut}(G), g \mapsto \mathrm{int}_g$, est un morphisme de groupes de noyau $\mathrm{Z}(G)$.

(ii) En déduire que l'image $\mathrm{Int}(G)$ est un sous-groupe de $\mathrm{Aut}(G)$ (sous-groupe des automorphismes intérieurs), que $\mathrm{Z}(G)$ est un sous-groupe distingué de G, puis $G/\mathrm{Z}(G) \simeq \mathrm{Int}(G)$.

(iii) Montrer que $\mathrm{Int}(G)$ est distingué dans $\mathrm{Aut}(G)$.

Exercice 2.27. *(i) Montrer que si G est un groupe tel que $G/\mathrm{Z}(G)$ est monogène, alors G est abélien.*

(ii) Examiner le cas $G = \mathrm{H}_8$.

Exercice 2.28. *Soit G un groupe tel que $\mathrm{Aut}(G) = \{1\}$. Montrer $|G| \leqslant 2$.*

Exercice 2.29. *Soient G un groupe et H une partie*[14] *de G. On pose*

$$\mathrm{N}_G(H) = \{g \in G \mid gHg^{-1} = H\} \quad \text{et} \quad \mathrm{C}_G(H) = \{g \in G \mid gh = hg,\ \forall h \in H\}$$

(respectivement, le normalisateur *de H dans G et le* centralisateur *de H dans G).*

(i) Montrer que $\mathrm{C}_G(H)$ et $\mathrm{N}_G(H)$ sont des sous-groupes de G.

(ii) Montrer que $\mathrm{N}_G(H)$ est le plus grand sous-groupe de G contenant H et dans lequel H est distingué.

(iii) Montrer aussi que $\mathrm{C}_G(H)$ est un sous-groupe distingué de $\mathrm{N}_G(H)$, et que $\mathrm{N}_G(H)/\mathrm{C}_G(H)$ est isomorphe à un sous-groupe de $\mathrm{Aut}(H)$.

(iv) (Exemple) On suppose $G = \mathrm{GL}_2(k)$ avec k un corps et $H = \{\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix},\ x \in k\}$. Déterminer $\mathrm{C}_G(H)$ et $\mathrm{N}_G(H)$.

Exercice 2.30. *On se place dans le groupe $\mathrm{GL}_2(\mathbb{Q})$ et on considère l'élément $g = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$ et le sous-groupe $H = \{\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix},\ n \in \mathbb{Z}\}$ (justifier).*

(i) Vérifier $gHg^{-1} \subsetneq H$.

(ii) Vérifier que $H' := \cup_{n \geqslant 0} g^{-n} H g^n$ est le plus petit sous-groupe de $\mathrm{GL}_2(\mathbb{Q})$ contenant H tel que $gH'g^{-1} = H'$, puis le déterminer.

Exercice 2.31. *Soient $(G_i)_{i \in I}$ une famille de groupes et, pour tout $i \in I$, H_i un sous-groupe distingué de G_i.*

(i) Monter que le sous-groupe $H = \prod_{i \in I} H_i$ est distingué dans $G = \prod_{i \in I} G_i$.

(ii) Montrer que le groupe G/H est naturellement isomorphe à $\prod_{i \in I} G_i/H_i$.

On donne maintenant quelques exercices sur les groupes usuels. On s'intéresse d'abord aux sous-groupes additifs de $\mathbb{Q}$. On notera P l'ensemble des nombres premiers, et suivant Steinitz, on appellera *super rationel* toute collection $s = (s_p)_{p \in \mathrm{P}}$, avec $s_p \in \mathbb{Z} \coprod \{+\infty\}$ pour tout $p \in \mathrm{P}$, et $s_p \geqslant 0$ pour tout p assez grand. On notera S l'ensemble des super rationels. On rappelle aussi, pour $p \in \mathrm{P}$, la *valuation* p-adique[15] $\mathrm{v}_p : \mathbb{Q} \to \mathbb{Z} \coprod \{+\infty\}$.

Exercice 2.32. (Sous groupes de $\mathbb{Q}$) *Pour tout super rationnel s, on note $H_s \subset \mathbb{Q}$ l'ensemble des $x \in \mathbb{Q}$ vérifiant $\mathrm{v}_p(x) \geqslant -s_p$ pour tout $p \in \mathrm{P}$.*

(i) Soit $s \in S$. Vérifier que H_s est un sous-groupe de $\mathbb{Q}$.

(ii) Montrer que le sous-groupe des rationels décimaux est de la forme H_s.

(iii) Soient $\lambda \in \mathbb{Q}$ et $s, t \in S$. Montrer que les sous-groupes $\mathbb{Z}\lambda$, $H_s + H_t$ et $H_s \cap H_t$ sont tous de la forme H_r pour un certain $r \in S$ à déterminer.

14. En pratique, H sera souvent un sous-groupe de G.

15. Par définition, on a $\mathrm{v}_p(0) = +\infty$, et pour tout $x \in \mathbb{Q}$ non nul, $\mathrm{v}_p(x)$ est l'unique entier $m \in \mathbb{Z}$ tel que x s'écrive sous la forme $p^m a/b$ avec a et b entiers premiers à p.

(iv) Montrer que tout sous-groupe de $\mathbb{Q}$ est de la forme H_s pour un unique $s \in S$.

(v) En déduire une description des sous-groupes de $\mathbb{Q}/\mathbb{Z}$.

(vii) Soient $s, t \in S$. À quelle condition les groupes H_s et H_t sont-ils isomorphes ?

EXERCICE 2.33. *(i)* (Kronecker) *Montrer que si $\alpha \in \mathbb{R} \smallsetminus \mathbb{Q}$, alors $\mathbb{Z} + \mathbb{Z}\alpha$ est dense dans $\mathbb{R}$.*

(ii) Montrer que la suite $(\cos n)_{n \geqslant 1}$ est dense dans $[-1, 1]$.

EXERCICE 2.34. *(i) Montrer que tout morphisme continu $\mathbb{R} \to \mathbb{C}$ est de la forme $x \mapsto \alpha x$ avec $\alpha \in \mathbb{C}$. Est-ce encore vrai sans l'hypothèse de continuité ?*

(ii) Montrer[16] *que tout morphisme continu $\mathbb{R} \to \mathbb{C}^\times$ est de la forme $x \mapsto e^{\alpha x}$ avec $\alpha \in \mathbb{C}$.*

(iii) En déduire que tout morphisme continu $\mathrm{S}^1 \to \mathbb{C}^\times$ est de la forme $z \mapsto z^n$ avec $n \in \mathbb{Z}$.

(iv) Plus généralement, montrer que tout morphisme continu $\mathbb{R} \to \mathrm{GL}_n(\mathbb{C})$ est de la forme $x \mapsto e^{Ax}$ avec $A \in \mathrm{M}_n(\mathbb{C})$.

On termine par quelques applications des groupes à la théorie des nombres.

EXERCICE 2.35. *Soit $n \geqslant 1$ un entier premier à 10. Montrer que la période du nombre rationnel $1/n$ coïncide avec l'ordre de 10 dans $(\mathbb{Z}/n\mathbb{Z})^\times$.*

EXERCICE 2.36. *(i) Soient G un groupe fini et S, T des parties de G vérifiant $|S| + |T| > |G|$. Montrer $G = ST$.*

(ii) (Application) *Soient p premier et $a, b \in (\mathbb{Z}/p\mathbb{Z})^\times$. Montrer que tout élément de $\mathbb{Z}/p\mathbb{Z}$ est de la forme $ax^2 + by^2$ avec $x, y \in \mathbb{Z}/p\mathbb{Z}$.*

(iii) Montrer que (i) ne vaut pas en général si l'on suppose $|S| + |T| = |G|$.

EXERCICE 2.37. *Soient p un nombre premier impair et $a \in \mathbb{Z}$ premier à p. On rappelle que l'on pose $(\frac{a}{p}) = 1$ si a est un carré modulo p, et $(\frac{a}{p}) = -1$ sinon (symbole de Legendre).*

(i) En utilisant l'involution $x \mapsto a/x$, montrer $(p-1)! \equiv -(\frac{a}{p})\, a^{(p-1)/2} \bmod p$.

(ii) En déduire $(p-1)! \equiv -1 \bmod p$ (théorème de Wilson), ainsi que $(\frac{a}{p}) \equiv a^{(p-1)/2} \bmod p$ (congruence d'Euler).

(iii) Retrouver $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$ pour tout $a, b \in \mathbb{Z}$.

EXERCICE 2.38. (Symboles de Legendre de $-1, 2$ et 3) *Soit p premier impair.*

(i) Montrer que pour $p \equiv 1 \bmod 4$, et $x = \frac{p-1}{2}!$, on a $x^2 \equiv -1 \bmod p$.

(ii) En s'inspirant de l'égalité $2\, e^{2i\pi/3} = -1 + i\sqrt{3}$ dans $\mathbb{C}$, montrer que -3 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si, et seulement si, on a $p \equiv 1 \bmod 3$ ou $p = 3$.

16. On pourra soit utiliser le *théorème de relèvement* : toute application continue $f : \mathbb{R} \to \mathbb{C}^\times$ est de la forme e^g avec $g : \mathbb{R} \to \mathbb{C}$ continue, soit montrer qu'un morphisme continu $f : \mathbb{R} \to \mathbb{C}^\times$ est automatiquement dérivable en observant, pour tout $x, \epsilon \in \mathbb{R}$, l'égalité $\int_x^{x+\epsilon} f(t)dt = f(x) \int_0^\epsilon f(t)dt$.

(iii) En déduire une condition nécessaire et suffisante sur p pour que 3 soit un carré dans $\mathbb{Z}/p\mathbb{Z}$.

(iv) En s'inspirant de l'égalité $\sqrt{2} = e^{2i\pi/8} + e^{-2i\pi/8}$ dans $\mathbb{C}$, montrer que si $p \equiv 1 \bmod 8$ alors 2 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ (Euler).

(v) (suite) En admettant l'existence d'un corps à p^2 éléments contenant $\mathbb{Z}/p\mathbb{Z}$, montrer que 2 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si, et seulement si, $p \equiv \pm 1 \bmod 8$.

On rappelle qu'un nombre premier est dit *de Fermat* s'il est de la forme $2^m + 1$ avec $m \geqslant 1$ (en fait, m est nécessairement une puissance de 2). Les seuls premiers de Fermat connus actuellement sont $3, 5, 17, 257$ et 65537...

Exercice 2.39. *Soit p un nombre premier de Fermat.*

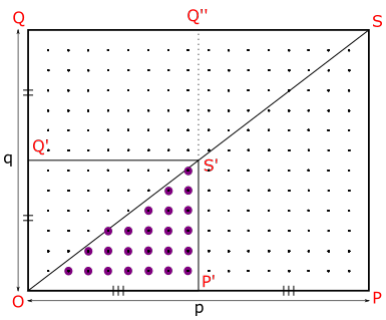
(i) Soit $x \in (\mathbb{Z}/p\mathbb{Z})^\times$. Montrer que x engendre $(\mathbb{Z}/p\mathbb{Z})^\times$ si, et seulement si, x n'est pas un carré.

(ii) En déduire que 3 engendre $(\mathbb{Z}/p\mathbb{Z})^\times$ pour $p \neq 3$.

Exercice 2.40. (Une démonstration géométrique de la loi de réciprocité quadratique, d'après Eisenstein [17]) *Soit p un nombre premier impair et soit $q \geqslant 1$ un entier impair premier à p. On se propose de montrer, suivant Eisenstein, la relation*

$$\left(\frac{q}{p}\right) = (-1)^e,$$

où e est le nombre de points de coordonnées entières du triangle OP'S' ci-dessous :



(i) En déduire que pour p et q premiers impair on a $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{(p-1)(q-1)}{2}}$ (« loi de réciprocité quadratique »).

On suppose d'abord simplement l'entier $q \geqslant 1$ premier à p. On pose $X = \{2, 4, \ldots, p-1\}$ et on note $R \subset \{1, \ldots, p-1\}$ l'ensemble des restes de la division par p des qx, pour $x \in X$.

(ii) Vérifier que l'application $\{1, \ldots, p-1\} \to X$, définie par

$$r \mapsto \begin{cases} r & \text{si } r \text{ est pair,} \\ p - r & \text{sinon,} \end{cases}$$

induit une bijection de R sur X.

17. *Geometrischer Beweis des Fundamentaltheorems für die quadratischen Reste*, Crelle's Journal 28, 246–249 (1844).

(iii) En déduire $(\frac{q}{p}) = (-1)^{\sum r}$*, la somme portant sur les* $r \in R$*. (On pourra considérer le produit des éléments de* X *modulo* p*)*

(iv) Vérifier que si $x \in X$*, et si* r *est le reste de la division de* qx *par* p*, on a* $r \equiv [qx/p] \bmod 2$*.*

(v) En déduire $(\frac{q}{p}) = (-1)^f$ *où* f *désigne le nombre des points à l'intérieur du triangle* OPS *dont les coordonnées sont entières, et d'abscisse paire.*

(vi) On suppose q *impair. Soit* A *(resp.* B*) le nombre des points à coordonnées entières et d'abscisse paire à l'intérieur du trapèze* $P'PSS'$ *(resp. du triangle* $S'SQ''$*). Montrer* $A \equiv B \bmod 2$*.*

(vii) En déduire la relation d'Eisenstein.

(viii) Montrer aussi $(\frac{2}{p}) = (-1)^f$ *où* f *désigne le nombre d'entiers pairs compris entre* $p/2$ *et* p*, puis* $f \equiv \frac{p^2-1}{8} \bmod 2$ *(« loi complémentaire »).*

L'exercice complémentaire suivant a été utilisé au (iv) de l'Exercice 2.20.

Exercice 2.41. (Théorème de Dirichlet faible) *Soit* $n \geqslant 1$ *un entier. On se propose de montrer qu'il existe une infinité de nombres premiers* $p \equiv 1 \bmod n$*. On considère le* n*-ème polynôme cyclotomique* $\Phi_n = \prod_{1 \leqslant k < n, (k,n)=1} (X - e^{2ik\pi/n})$*. C'est un polynôme unitaire de degré* $\varphi(n)$ *dans* $\mathbb{C}[X]$*.*

(i) Montrer $X^n - 1 = \prod_{d|n} \Phi_d$*, et en déduire*[18] $\Phi_n \in \mathbb{Z}[X]$*.*

(ii) Montrer que si k *est un corps dans lequel* $n.1 \neq 0$*, le polynôme* $X^n - 1$ *n'a pas de racine double dans* k*.*

(iii) (suite) En déduire qu'un élément $x \in k^\times$ *et d'ordre* n *si, et seulement si, on a* $\Phi_n(x) = 0$*.*

(iv) Montrer que pour tout polynôme $P \in \mathbb{Z}[X]$ *non constant, l'ensemble des nombres premiers divisant l'un des entiers* $P(n)$ *avec* $n \in \mathbb{Z}$*, est infini.*

(v) Conclure.

18. On rappelle que si on a $P, Q \in \mathbb{Z}[X]$ avec Q unitaire, on dispose d'une *division euclidienne* $P = AQ + B$ avec $A, B \in \mathbb{Z}[X]$ et $\deg B < \deg Q$.

Chapitre 3

Groupes abéliens de type fini

Le premier but de ce chapitre est de classifier à isomorphisme près les groupes abéliens de type fini. C'est le cas par exemple du sous-groupe d'un groupe donné quelconque engendré par une famille finie d'éléments qui commutent 2 à 2. Le cas crucial est celui des groupes abéliens finis.

La méthode suivie passe par l'étude des caractères d'un tel groupe G, c'est à dire des morphismes $G \to \mathbb{C}^\times$. C'est pourquoi nous commençons par illustrer l'intérêt de ces derniers en expliquant, suivant Gauss et Weil, comment utiliser les caractères du groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ (comme le symbole de Legendre) pour déterminer le nombre de solutions dans $\mathbb{Z}/p\mathbb{Z}$ de l'équation $y^2 = x^3 + 1$.

Nous montrons ensuite comment les caractères de G, pour G abélien fini, permettent de décomposer à la Fourier l'espace des fonctions $G \to \mathbb{C}$. C'est l'un des points de départ de la théorie des *représentations des groupes finis*, qui fera l'objet du dernier chapitre du cours, et dont on donne une première application ici aux *déterminants de groupes*, suivant Dedekind. Le lemme technique clé est le lemme de *prolongement des caractères*, dont on donne deux démonstrations différentes. L'analogie à avoir en tête ici est que les caractères sont aux groupes abéliens finis ce que les formes linéaires sont aux espaces vectoriels.

Le lemme de prolongement permet de montrer simplement que tout groupe abélien fini est produit de groupes cycliques. La question de l'unicité d'une telle décomposition, plus délicate, est aussi étudiée. Une méthode assez similaire permet de donner la structure des groupes abéliens de type fini généraux. Le cas particulier des réseaux de $\mathbb{R}^n$ est important. On conclut par une discussion culturelle du groupe des points d'une courbe elliptique.

1. Caractères et $y^2 = x^3 + 1$ sur $\mathbb{Z}/p\mathbb{Z}$

Définition 1.1. *Un* caractère *(ou caractère linéaire) d'un groupe G est un morphisme de groupes $G \to \mathbb{C}^\times$. On note $\widehat{G}$ l'ensemble des caractères de G.*

Le groupe $\mathbb{C}^\times$ étant commutatif, rappelons que $\widehat{G} = \mathrm{Hom}(G, \mathbb{C}^\times)$ est muni d'une loi de groupe abélien naturelle : le produit de deux caractères $\chi, \psi \in \widehat{G}$ est la fonction $\chi\psi : G \to \mathbb{C}^\times$, $g \mapsto \chi(g)\psi(g)$. Son élément neutre est le caractère trivial 1 (envoyant tout $g \in G$ sur 1) et l'inverse d'un caractère χ est le caractère $\chi^{-1} : g \mapsto \chi(g)^{-1}$. Pour cette loi, $\widehat{G}$ est appelé *groupe des caractères*, ou *groupe dual*, du groupe G. Comme nous le verrons, l'étude de $\widehat{G}$ s'avèrera particulièrement pertinente quand G est abélien fini.

Remarque 1.2. *Si G est fini d'ordre n, et si $\chi \in \widehat{G}$, on a $\chi(G) \subset \mu_n$. En effet, la relation $g^n = 1$ dans G (Lagrange) entraîne $\chi(g)^n = 1$ dans $\mathbb{C}^\times$ pour tout $\chi \in \widehat{G}$. En particulier, $\widehat{G}$ est un groupe abélien fini, et on a aussi $\chi^{-1} = \overline{\chi}$.*

Il est aisé de déterminer les caractères d'un groupe cyclique :

PROPOSITION 1.3. *Soit G un groupe cyclique d'ordre n engendré par $g \in G$. Pour tout $\zeta \in \mu_n$ il existe un unique caractère χ_ζ de G tel que $\chi_\zeta(g) = \zeta$. De plus, l'application $\zeta \mapsto \chi_\zeta$ est un isomorphisme de groupes $\mu_n \xrightarrow{\sim} \widehat{G}$.*

DÉMONSTRATION — Soit $\zeta \in \mu_n$. L'unicité de χ_ζ est claire car on a nécessairement $\chi_\zeta(g^k) = \zeta^k$ pour $k \in \mathbb{Z}$. Pour l'existence, on constate que l'application $\chi_\zeta : G \to \mathbb{C}^\times, g^k \mapsto \zeta^k$, est bien définie, car pour $k, k' \in \mathbb{Z}$ on a $g^k = g^{k'} \implies k \equiv k' \bmod n \implies \zeta^k = \zeta^{k'}$. C'est clairement un morphisme de groupes, *i.e.* un caractère de G, vérifiant $\chi_\zeta(g) = \zeta$. On a donc défini une application $\mu_n \to \widehat{G}, \zeta \mapsto \chi_\zeta$, injective (car $\chi_\zeta(g) = \zeta$) et surjective par la Remarque précédente. C'est trivialement un morphisme de groupes car on a $\chi_\zeta \chi_{\zeta'} = \chi_{\zeta\zeta'}$, c'est donc un isomorphisme. □

Les caractères du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$, appelés *caractères de Dirichlet*, ont un côté plus mystérieux. Un exemple typique est donné par le *caractère de Legendre*

$$\lambda : (\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}, \quad x \mapsto (\frac{x}{p}),$$

déjà rencontré, qui est défini pour p premier impair et encode la répartition des carrés de $(\mathbb{Z}/p\mathbb{Z})^\times$. C'est l'unique caractère d'ordre 2 de $(\mathbb{Z}/p\mathbb{Z})^\times$. En effet, un tel caractère doit envoyer un générateur g de $(\mathbb{Z}/p\mathbb{Z})^\times$ sur -1, et donc un carré g^{2k} sur 1, et un non carré g^{2k+1} sur -1 : c'est λ. Donnons un autre exemple.

EXEMPLE 1.4. (*Cubes de $(\mathbb{Z}/p\mathbb{Z})^\times$ et caractères cubiques*) Considérons le morphisme $f : (\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$, $x \mapsto x^3$, d'image le sous-groupe Cubes_p des cubes de $(\mathbb{Z}/p\mathbb{Z})^\times$ (aussi noté $(\mathbb{Z}/p\mathbb{Z})^{\times,(3)}$ au §5 Chap. 2). Pour fixer les idées, choisissons un générateur g du groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ (Gauss), de sorte que Cubes_p est engendré par g^3, et donc d'indice $\mathrm{pgcd}(p-1, 3)$. Il y a deux cas très différents :

(Cas a) $p \not\equiv 1 \bmod 3$. On a $\mathrm{Cubes}_p = (\mathbb{Z}/p\mathbb{Z})^\times$, donc tout élément est un cube. C'est même le cube d'un unique élément. En effet, f est surjective et est donc bijective pour des raisons de cardinal. Alternativement, on peut dire aussi que $\ker f$ est trivial car un élément non trivial de $\ker f$ serait d'ordre 3 dans $(\mathbb{Z}/p\mathbb{Z})^\times$, mais 3 ne divise pas $p-1$.

(Cas b) $p \equiv 1 \bmod 3$. Dans ce cas, le plus intéressant !, Cubes_p est un sous-groupe d'indice 3 de $(\mathbb{Z}/p\mathbb{Z})^\times$. On a donc trois classes

$$(\mathbb{Z}/p\mathbb{Z})^\times/\mathrm{Cubes}_p = \{\mathrm{Cubes}_p,\ g\,\mathrm{Cubes}_p,\ g^2\,\mathrm{Cubes}_p\} \simeq \mathbb{Z}/3\mathbb{Z}.$$

Posons $j = e^{2i\pi/3}$. D'après la Proposition 1.3, il existe exactement 2 caractères non triviaux $c : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$ tels que $c^3 = 1$, à savoir les caractères χ_j et $\chi_{j^2} = \chi_j^2$, avec $\chi_j(g) = j$. On pose $c = \chi_j$. Il faut bien noter qu'il dépend du choix du générateur g, mais que l'ensemble $\{c, c^2\}$ ne dépend pas de ce choix : c'est l'ensemble des deux caractères d'ordre 3 de $(\mathbb{Z}/p\mathbb{Z})^\times$. Observons que c prend l'unique valeur 1 sur Cubes_p, j sur $g\mathrm{Cubes}_p$ et j^2 sur $g^2\mathrm{Cubes}_p$. En particulier, on a encore $c(x) = 1$ si, et seulement si, x est un cube, mais il y a deux types de non cubes : les x tels que $c(x) = j$, et ceux tels que $c(x) = j^2$.

Les caractère de Dirichlet sont particulièrement importants en théorie des nombres, notamment car ils interviennent de manière cruciale dans la démonstration du théorème de la progression arithmétique (Dirichlet). Cette démonstration, de nature

analytique, sort du cadre de ce cours. [1] À la place, en guise de motivation, nous allons voir comment les caractères de $(\mathbb{Z}/p\mathbb{Z})^\times$, avec p premier, permettent aussi d'étudier le nombre de solutions de certaines équation polynomiales sur $\mathbb{Z}/p\mathbb{Z}$, en considérant précisément le cas de l'équation

$$y^2 = x^3 + 1, \text{ avec } x, y \in \mathbb{Z}/p\mathbb{Z}.$$

Nous suivrons pour cela la méthode introduite par Weil dans son article fameux *Numbers of solutions of equations in finite fields.* [2] On pose donc

$$\mathrm{S}_p = \{(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2 \mid y^2 = x^3 + 1\}.$$

En général, on a $|\mathrm{S}_p| \leqslant 2p$ car pour chaque x, l'élément x^3+1 a au plus deux racines carrés (opposées) y dans $\mathbb{Z}/p\mathbb{Z}$. Par exemple, pour $p = 2$ on a $\mathrm{S}_2 = \{(1, 0), (0, 1)\}$, puis $|\mathrm{S}_2| = 2$. Plus généralement :

Lemme 1.5. *Pour $p \not\equiv 1 \bmod 3$ on a $|\mathrm{S}_p| = p$.*

Démonstration — En effet, pour un tel p l'application $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}, x \mapsto x^3$, est bijective par le cas (a) de la Remarque 1.4, de sorte que l'application $\mathrm{S}_p \to \mathbb{Z}/p\mathbb{Z}, (x, y) \mapsto y$, est aussi bijective. □

Le cas $p \equiv 1 \bmod 3$ est sensiblement plus fin ! Supposons par exemple $p = 7$. Les carrés de $\mathbb{Z}/7\mathbb{Z}$ sont $\{\overline{0}, \overline{1}, \overline{2}, \overline{4}\}$, et les cubes $\{\overline{0}, \overline{1}, \overline{-1}\}$, donc les seules solutions sont celles associées aux identités $1 \equiv 0 + 1$ ($1 \cdot 2$ solutions), $2 \equiv 1 + 1$ ($3 \cdot 2$ solutions) et $0 \equiv -1 + 1$ ($3 \cdot 1$ solutions), et on a donc $|\mathrm{S}_7| = 2 + 6 + 3 = 11$. On a aussi l'observation élémentaire :

Lemme 1.6. *Pour $p \equiv 1 \bmod 3$ on a $|\mathrm{S}_p| \equiv 2 \bmod 3$ et $|\mathrm{S}_p| \equiv 1 \bmod 2$.*

Démonstration — Pour $p \equiv 1 \bmod 3$, les fibres de $(\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times, x \mapsto x^3$ ont 3 éléments. En particulier, $(\mathbb{Z}/p\mathbb{Z})^\times$ contient un élément d'ordre 3, disons ω. L'application $\varphi : (x, y) \mapsto (\omega x, y)$ est alors une bijection de S_p vérifiant $\varphi^3 = \mathrm{id}$. Comme ses uniques points fixes sont les deux éléments $(0, \pm 1)$, on a $|\mathrm{S}_p| \equiv 2 \bmod 3$ par le Corollaire 1.9 Chap. 1. La seconde congruence se démontre de même en considérant l'involution $(x, y) \mapsto (x, -y)$, qui a pour points fixes les $(x, 0)$ avec $x^3 = -1$, *i.e.* $x = -1, -\omega, -\omega^2$ (on a utilisé $p \neq 2$). □

On suppose désormais $p \equiv 1 \bmod 3$. Nous allons voir d'une part que p s'écrit de manière unique sous la forme $A^2 + 3B^2$ avec $A, B \in \mathbb{N}$, et d'autre part qu'il existe un lien surprenant cette écriture et $|\mathrm{S}_p|$. Nous attribuerons cet énoncé à Gauss, car c'est une variante de la célèbre *last entry* de son journal mathématique (1814). À ce stade il sera plus clair de faire l'observation élémentaire suivante :

Lemme 1.7. *Soient $d \geqslant 1$ entier et p un nombre premier. Il existe au plus un couple d'entiers $(a, b) \in \mathbb{N}^2$, ou deux pour $d = 1$, avec $p = a^2 + db^2$.*

Reportons la démonstration de ce lemme à la fin de la section. Le résultat de Gauss est le suivant :

1. Voir le *cours d'Arthmétique* de J.-P. Serre, ou *Multiplicative number theory* de H. Davenport.
2. Bull. Amer. Math. Soc. 55(5), 497–508 (1949). Cette méthode est elle-même inspirée de travaux de Gauss, Jacobi, Hasse et Davenport : nous renvoyons à l'article de Weil pour plus de références historiques.

THÉORÈME 1.8. (Gauss) *Soit p un nombre premier $\equiv 1 \bmod 3$. Alors p s'écrit de manière unique sous la forme $p = A^2 + 3B^2$ avec $A, B \in \mathbb{Z}$, $B \geqslant 0$ et $A \equiv -1 \bmod 3$. De plus, on a la relation $|\mathrm{S}_p| = p + 2A$.*

Par exemple pour $p = 7$, on a $7 = 2^2 + 3 \cdot 1^2$ donc $A = 2$, et on retrouve $|\mathrm{S}_7| = 7+4 = 11$. Voir la Table 1 pour plus d'exemples. En pratique, A est beaucoup

p	7	13	19	31	37	43	61	67	73	79	97	103	109
$\lvert\mathrm{S}_p\rvert$	11	11	11	35	47	35	47	83	83	83	83	83	107
A	2	-1	-4	2	5	-4	-7	8	5	2	-7	-10	-1
B	1	2	1	3	2	3	2	3	2	5	4	1	6

TABLE 1. Quelques valeurs de $|\mathrm{S}_p|$, A et B.

plus simple à déterminer que $|\mathrm{S}_p|$! Bien noter que la congruence sur A détermine le signe à choisir pour A. L'inégalité évidente $A^2 < p$ entraîne l'inégalité suivante, qui confirme et précise l'heuristique naturelle [3] selon laquelle on pourrait avoir $|\mathrm{S}_p| \approx p$.

COROLLAIRE 1.9. *Pour tout premier p on a $||\mathrm{S}_p| - p| < 2\sqrt{p}$.*

La démonstration du Théorème 1.8 va nous occuper jusqu'à la fin de cette section. Nous allons faire grand usage des caractères de $(\mathbb{Z}/p\mathbb{Z})^\times$, et ce dès la proposition suivante. Pour $a \in \mathbb{Z}/p\mathbb{Z}$ et $n \geqslant 1$ on pose

$$\mathrm{N}(x^n = a) = |\{x \in \mathbb{Z}/p\mathbb{Z} \mid x^n = a\}|.$$

Si χ est un caractère de $(\mathbb{Z}/p\mathbb{Z})^\times$, on le prolongera toujours en une fonction $\mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ en posant $\chi(0) = 0$, sauf si $\chi = 1$ auquel cas on pose $\chi(0) = 1$. Cette convention d'apparence curieuse assurera l'élégance des énoncés (comme le suivant). Noter qu'on a encore $\chi(ab) = \chi(a)\chi(b)$ pour tout $a, b \in \mathbb{Z}/p\mathbb{Z}$ (car $ab = 0 \Leftrightarrow a = 0$ ou $b = 0\}$).

PROPOSITION 1.10. *Pour tout $a \in \mathbb{Z}/p\mathbb{Z}$ on a $\mathrm{N}(x^n = a) = \sum_\chi \chi(a)$, la somme portant sur les m caractères χ de $(\mathbb{Z}/p\mathbb{Z})^\times$ vérifiant $\chi^m = 1$, avec $m = (n, p-1)$.*

Démontrons d'abord seulement les deux cas particuliers $n = 2$ et 3 de cette proposition, les seuls nécessaires à la démonstration du le Théorème 1.8. Dans le cas $n = 2$ et $p > 2$, la Proposition s'écrit :

$$\mathrm{N}(x^2 = a) = 1 + (\frac{a}{p}). \tag{11}$$

C'est vrai, comme on le voit en distinguant les 3 cas $a = 0$ (les deux termes valent 1), a carré non nul (les deux termes valent 2) et a non carré (les deux termes valent 0) ! Pour $n = 3$ et $p \equiv 1 \bmod 3$, l'Exemple 1.4 montre que la Proposition s'écrit :

$$\mathrm{N}(x^3 = a) = 1 + c(a) + c^2(a). \tag{12}$$

Là encore, on constate que les deux termes valent 1 si $a = 0$. Si $a = b^3 \neq 0$ est un cube, alors $x^3 = a$ a pour trois solutions $b, b\omega$ et $b\omega^2$ et on a par définition $a \in \ker c$:

3. En effet, il y a environ $p/2$ carrés et $p/3$ cubes dans $\mathbb{Z}/p\mathbb{Z}$, de sorte que s'il sont "bien répartis" on s'attend à ce qu'environ $p/6$ carrés soient des cubes plus 1. Comme un carré (resp. un cube) non nul est le carré de 2 (resp. 3) éléments, on s'attend donc à avoir $|\mathrm{S}_p| \simeq 6 \cdot p/6 = p$.

ça marche encore. Enfin, si a n'est pas un cube on a $c(a) = j$ ou j^2, et on conclut car $0 = 1 + j + j^2$. La démonstration de la Proposition 1.10 est similaire en général, et reportée à la fin de la section. ▫

On a $\mathrm{S}_p \sim \{(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2 \mid y^2 + x^3 = 1\}$ par changement de variable $x \mapsto -x$. Le point de départ de la méthode de Weil est la formule évidente :

$$|\mathrm{S}_p| = \sum_{a+b=1} \mathrm{N}(y^2 = a)\,\mathrm{N}(x^3 = b), \tag{13}$$

la somme portant sur les couples $(a, b) \in (\mathbb{Z}/p\mathbb{Z})^2$ avec $a + b = 1$. En appliquant les Formules (11) et (12), la Formule (13) s'écrit alors :

$$|\mathrm{S}_p| = \sum_{a+b=1} (1 + \lambda(a))(1 + c(b) + c^2(b)). \tag{14}$$

Cela conduit à introduire, pour deux caractères χ, ψ de $(\mathbb{Z}/p\mathbb{Z})^\times$ la *somme de Jacobi*

$$\mathrm{J}(\chi, \psi) = \sum_{a+b=1} \chi(a)\psi(b),$$

la somme portant sur les $(a, b) \in (\mathbb{Z}/p\mathbb{Z})^2$ avec $a + b = 1$. C'est un nombre complexe qui est somme finie de racines $p - 1$-èmes de l'unités. La Formule (14) se ré-écrit $|\mathrm{S}_p| = \mathrm{J}(1, 1) + \mathrm{J}(1, c) + \mathrm{J}(1, c^2) + \mathrm{J}(\lambda, 1) + \mathrm{J}(\lambda, c) + \mathrm{J}(\lambda, c^2)$.

Lemme 1.11. *On a* $\mathrm{J}(1, \chi) = \mathrm{J}(1, \chi) = 0$ *pour* $\chi \neq 1$, *et* $\mathrm{J}(1, 1) = p$.

Démonstration — On a $\mathrm{J}(1, \chi) = \mathrm{J}(1, \chi) = \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \chi(a)$. L'égalité $\mathrm{J}(1, 1) = p$ est donc évidente. L'annulation $\mathrm{J}(1, \lambda) = 0$ résulte alors par exemple de ce qu'il y a autant de carrés que de non carrés dans $(\mathbb{Z}/p\mathbb{Z})^\times$. Pour χ général et $x \in (\mathbb{Z}/p\mathbb{Z})^\times$, on a $\chi(x)\mathrm{J}(1, \chi) = \mathrm{J}(1, \chi)$ par le changement de variable bijectif $a \mapsto ax$ dans $\mathbb{Z}/p\mathbb{Z}$. On en déduit $\mathrm{J}(1, \chi) = 0$ pour $\chi \neq 1$ en choisissant x tel que $\chi(x) \neq 1$. □

En utilisant $\mathrm{J}(\lambda, c^2) = \overline{\mathrm{J}(\lambda, c)}$ (car $\overline{\lambda} = \lambda$ et $\overline{c} = c^2$) on obtient finalement

$$|\mathrm{S}_p| = p + \mathrm{J}(\lambda, c) + \overline{\mathrm{J}(\lambda, c)}. \tag{15}$$

L'information finale cruciale sur les $\mathrm{J}(\lambda, c)$ est donnée par la proposition suivante :

Proposition 1.12. *Pour* $\chi, \psi, \chi\psi$ *non triviaux, on a* $|\mathrm{J}(\chi, \psi)|^2 = p$.

Expliquons d'abord comment elle entraîne le Théorème.

Démonstration — (du Théorème 1.8) Par définition, $\mathrm{J}(\lambda, c)$ est une somme d'éléments de la forme $\pm 1, \pm j$ et $\pm j^2$, avec $j = e^{2i\pi/3}$. Comme $j^2 = -1 - j$, on a $\mathrm{J}(\lambda, c) = a + bj$ avec $a, b \in \mathbb{Z}$. La Proposition 1.12 entraîne $p = |a + bj|^2 = a^2 - ab + b^2$. On a aussi $\mathrm{J}(\lambda, c) + \overline{\mathrm{J}(\lambda, c)} = 2a - b$. La formule (15) montre donc

$$|\mathrm{S}_p| = p + 2a - b.$$

Mais $|\mathrm{S}_p|$ est impair par le Lemme 1.6, et on a $p \neq 2$, donc b est pair. On pose $A = a - b/2$ et $B = |b/2|$. On a donc $|\mathrm{S}_p| = p + 2A$ et $p = a^2 - ab + b^2 = (a - b/2)^2 + 3b^2/4 = A^2 + 3B^2$. Enfin, le Lemme 1.6 montre $A \equiv -1 \bmod 3$. □

La Proposition 1.12 va résulter de l'étude des *sommes de Gauss*. Pour un caractère χ de $(\mathbb{Z}/p\mathbb{Z})^\times$ donné, c'est la somme $\mathrm{G}(\chi) = \sum_{a\in\mathbb{Z}/p\mathbb{Z}} \chi(a)\zeta^a$, avec $\zeta = e^{2i\pi/p}$.

Proposition 1.13. *Soient $\chi, \psi \in \widehat{(\mathbb{Z}/p\mathbb{Z})}^\times$ des caractères non triviaux. On a :*

(i) $|\mathrm{G}(\chi)|^2 = p$,

(ii) $\mathrm{G}(\chi)\mathrm{G}(\psi) = \mathrm{J}(\chi,\psi)\mathrm{G}(\chi\psi)$ *si* $\chi\psi \neq 1$.

Le côté très surprenant de l'égalité (i) est qu'une somme de $p-1$ racines de l'unité soit de module $\sqrt{p}$. Noter que (i) et (ii) entraînent la Proposition 1.12, et terminent donc la démonstration du théorème de Gauss.

Démonstration — Montrons le (i). On a $\overline{\mathrm{G}(\chi)} = \sum_{a\in\mathbb{Z}/p\mathbb{Z}} \chi^{-1}(a)\zeta^{-a}$, et donc

$$|\mathrm{G}(\chi)|^2 = \mathrm{G}(\chi)\overline{\mathrm{G}(\chi)} = \sum_{a,b\in\mathbb{Z}/p\mathbb{Z}} \chi(a)\chi^{-1}(b)\zeta^{a-b}$$

par un développement brutal. La convention $\chi(0) = \chi^{-1}(0) = 0$ montre que l'on peut supposer $a, b \in (\mathbb{Z}/p\mathbb{Z})^\times$ dans la somme ci-dessus. Le changement de variable $b = at$ avec $t \in (\mathbb{Z}/p\mathbb{Z})^\times$ permet alors de ré-écrire :

$$|\mathrm{G}(\chi)|^2 = \sum_{a,t\in(\mathbb{Z}/p\mathbb{Z})^\times} \chi^{-1}(t)\zeta^{a(1-t)} = \sum_{t\in(\mathbb{Z}/p\mathbb{Z})^\times} \chi^{-1}(t) \sum_{a\in(\mathbb{Z}/p\mathbb{Z})^\times} \zeta^{a(1-t)}.$$

Mais $\sum_{a\in(\mathbb{Z}/p\mathbb{Z})^\times} \zeta^{a(1-t)}$ vaut -1 pour $t \neq 1$, et $p-1$ pour $t = 1$. On en déduit

$$|\mathrm{G}(\chi)|^2 = -\sum_{t\in(\mathbb{Z}/p\mathbb{Z})^\times} \chi^{-1}(t) + \chi^{-1}(1) + p - 1 = 0 + 1 + p - 1 = p.$$

Montrons le (ii). On a encore $\mathrm{G}(\chi)\mathrm{G}(\psi) = \sum_{a,b\in\mathbb{Z}/p\mathbb{Z}} \chi(a)\psi(b)\zeta^{a+b}$, puis

$$\mathrm{G}(\chi)\mathrm{G}(\psi) = \sum_{k\in\mathbb{Z}/p\mathbb{Z}} \Big(\sum_{a+b=k} \chi(a)\psi(b) \Big) \zeta^k.$$

Pour $k = 0$, la somme entre parenthèses vaut $\sum_{a\in\mathbb{Z}/p\mathbb{Z}} \chi(a)\psi(-a) = \mathrm{J}(1,\chi\psi)\psi(-1) = 0$ car $\chi\psi \neq 1$. Pour $k \neq 0$, le changement de variables $a = ka'$ et $b = kb'$ montre qu'elle vaut $\sum_{a'+b'=1} \chi(a'k)\psi(b'k) = \chi(k)\psi(k)\mathrm{J}(\chi,\psi)$. On a donc

$$\mathrm{G}(\chi)\mathrm{G}(\psi) = \sum_{k\in(\mathbb{Z}/p\mathbb{Z})^\times} \chi(k)\psi(k)\mathrm{J}(\chi,\psi)\zeta^k = \mathrm{J}(\chi,\psi)\mathrm{G}(\chi\psi).$$

□

Il nous reste encore à démontrer le Lemme 1.7, laissé de côté.

Démonstration — (du Lemme 1.7) Supposons $p = a^2 + db^2$ avec $a, b \in \mathbb{N}$. On peut supposer $p \nmid d$, sinon on a $d = p$ et une unique solution $(a,b) = (0,1)$, puis $a, b \geqslant 1$. On a alors les inégalités $1 \leqslant a < \sqrt{p}$ et $1 \leqslant b < \sqrt{p/d}$. On a aussi $\mathrm{pgcd}(a,b) = 1$, et $p \nmid b$, sinon on aurait $p \mid a$ et $p^2 \mid p$, une contradiction. On a donc $(a/b)^2 \equiv -d \bmod p$.

Supposons enfin $p = a^2 + db^2 = (a')^2 + d(b')^2$ avec $a, a', b, b' \in \mathbb{N}$. L'analyse ci-dessus montre $(a/b)^2 \equiv -d \equiv (a'/b')^2 \bmod p$, puis $a/b \equiv \pm a'/b' \bmod p$ car p est premier. Ceci et les inégalités ci-dessus montrent donc

$$ab' \equiv \pm a'b \bmod p \quad \text{et} \quad 1 \leqslant ab', a'b < p/d. \tag{16}$$

Pour $d \geqslant 2$ cela entraîne $ab' = a'b$. Mais on a $\mathrm{pgcd}(a,b) = \mathrm{pgcd}(a',b') = 1$, donc $a \mid a'$, $a' \mid a$, $a = a'$ et $b = b'$. Dans le cas $d = 1$, la relation (16) entraîne soit $ab' = a'b$, et donc $(a,b) = (a',b)$ comme ci-dessus, soit $ab' + a'b = p$. Mais dans ce cas, les vecteurs $u = (a,b)$ et $v = (b',a')$ de $\mathbb{R}^2$ vérifient $u.u = v.v = u.v = p$ et on a $u = v$ par Cauchy-Schwarz : les deux solutions sont (of course !) (a,b) et (b,a). $\square$

Remarque 1.14. (Retour sur les premiers 1 mod 4) La Proposition 1.12 entraîne aussi qu'un nombre premier $p \equiv 1 \bmod 4$ est somme de deux carrés. En effet, pour $p \equiv 1 \bmod 4$ on peut trouver un caractère χ d'ordre 4 de $(\mathbb{Z}/p\mathbb{Z})^\times$ (pourquoi ?). D'après la proposition, on a $|\mathrm{J}(\chi,\chi)|^2 = p$, ou encore $|\mathrm{J}(\chi,\lambda)|^2 = p$. Ces deux sommes de Jacobi sont de la forme $a + bi$ avec $a, b \in \mathbb{Z}$, et donc $p = a^2 + b^2$. Voir l'Exercice 3.31 pour une suite !

Remarque 1.15. (Somme de Gauss quadratique) Pour $p \neq 2$, c'est la somme $\mathrm{G}_p := \mathrm{G}(\lambda) = \sum_{k\in\mathbb{Z}/p\mathbb{Z}} \left(\frac{k}{p}\right) e^{\frac{2ik\pi}{p}}$. En utilisant $\sum_{k=0}^{p-1} e^{\frac{2ik\pi}{p}} = 0$, on constate aussi

$$\mathrm{G}_p = \sum_{k=0}^{p-1} e^{\frac{2i\pi k^2}{p}}.$$

Pour tout caractère χ, on a aussi $\chi(-1) = \pm 1$, et par la bijection $x \mapsto -x$,

$$\overline{\mathrm{G}(\chi)} = \sum_{x\in\mathbb{Z}/p\mathbb{Z}} \overline{\chi(x)}\zeta^{-x} = \chi(-1)\mathrm{G}(\overline{\chi}). \tag{17}$$

Comme $\lambda = \overline{\lambda}$, on a $\overline{\mathrm{G}_p} = (\frac{-1}{p})\mathrm{G}_p$, mais aussi $|\mathrm{G}_p|^2 = p$ par la proposition, puis

$$\mathrm{G}_p^2 = \left(\frac{-1}{p}\right) p = (-1)^{\frac{p-1}{2}} p.$$

On a donc $\mathrm{G}_p = \pm\sqrt{p}$ pour $p \equiv 1 \bmod 4$ et $\mathrm{G}_p \equiv \pm i\sqrt{p}$ pour $p \equiv 3 \bmod 4$. Gauss a démontré (de son aveu, avec difficulté !) que ces signes sont toujours $+$. Nous renvoyons aux exercices pour une démonstration due à Dirichlet de ce résultat, et pour une preuve simple de la loi de réciprocité quadratique qui s'en déduit. Pour $\chi \neq \lambda$, il n'y a pas de formule simple connue pour $\mathrm{G}(\chi)$ (ni même pour la *somme de Gauss cubique* $\mathrm{G}(c)$, qui a fait l'objet de nombreux travaux initiés par Kummer : voir l'Exercice 3.30).

Terminons cette section par une démonstration de la Proposition 1.10.

Démonstration — (de la Proposition 1.10, omise en classe) Dans le cas $a = 0$, le terme de gauche vaut 1 (0 est seule solution) et celui de droite vaut aussi 1 par la convention $\chi(0) = 0$ pour $\chi \neq 1$, et $\chi(0) = 1$ pour $\chi = 1$. On suppose donc $a \neq 0$.

Fixons g un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$. D'après la Proposition 1.3, les caractères de $(\mathbb{Z}/p\mathbb{Z})^\times$ sont les $g^k \mapsto \zeta^k$ avec $\zeta^{p-1} = 1$. Un tel caractère χ vérifie $\chi^m = 1$ si, et seulement si, $\zeta^m = 1$. Noter $\mu_m \subset \mu_{p-1}$. Écrivons $a = g^k$ pour $k \in \mathbb{Z}$. On a donc

$$\sum_{\{\chi \,|\, \chi^m = 1\}} \chi(a) = \sum_{\zeta\in\mu_m} \zeta^k.$$

Cette somme qui vaut m si $k \equiv 0 \bmod m$, et 0 sinon. Il suffit donc de montrer

$$\mathrm{N}(x^n = g^k) = m \ \text{ si } k \equiv 0 \bmod m, \ 0 \text{ sinon}. \tag{18}$$

Mais d'un autre côté, on sait que le morphisme

$$(\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times, x \mapsto x^n,$$

a pour image les $(p-1)/m$ puissances n-èmes de $(\mathbb{Z}/p\mathbb{Z})^\times$, et que ses fibres sont donc de cardinal 0 ou m. Il ne reste qu'à observer que g^k est une puissance n-ème dans $(\mathbb{Z}/p\mathbb{Z})^\times$ si, et seulement si, on a $k \equiv 0 \bmod m$. Mais on a vu que c'est équivalent à $g^{k\frac{p-1}{m}} = 1$ (Corollaire 5.7 Chap. 2 (ii)), et donc à $k\frac{p-1}{m} \equiv 0 \bmod p-1$, ce qui est bien équivalent à $k \equiv 0 \bmod m$. □

Remarque 1.16. (Culturelle) La même méthode s'applique plus généralement aux équations *diagonales*, *i.e.* de la forme $ax^n + by^m = c$ avec $a, b, c \in \mathbb{Z}/p\mathbb{Z}$ et $n, m \geqslant 1$, et même plus généralement à celles de la forme $a_1x_1^{n_1} + a_2x_2^{n_2} + \cdots + a_mx_m^{n_m} = b$ (*hypersurfaces diagonales*). Nous renvoyons à l'article sus-cité de Weil et au chapitre 8 du livre de Ireland et Rosen pour de nombreux exemples détaillés. Ces résultats sont à l'origine des fameuses *conjectures de Weil*, qui s'appliquent à toutes les variétés algébriques sur $\mathbb{Z}/p\mathbb{Z}$, et dont la résolution par Grothendieck et Deligne a modifié le paysage de la géométrie algébrique.

2. Décomposition de Fourier finie

L'analyse de Fourier classique affirme notamment que l'espace de Hilbert $\mathrm{L}^2(\mathbb{R}/\mathbb{Z})$ des fonctions 1-périodique de carré intégrable sur le cercle $\mathbb{R}/\mathbb{Z}$[4] admet pour base Hilbertienne les fonctions $x \mapsto e^{2i\pi nx}$ pour $n \in \mathbb{Z}$ ("décomposition de Fourier"). La propriété particulière de ces fonctions est que ce sont des caractères continus du groupe abélien (topologique compact) $\mathbb{R}/\mathbb{Z}$. C'est même un exercice de voir que tout morphisme continu $\mathbb{R}/\mathbb{Z} \to \mathbb{C}^\times$ est de la forme $x \mapsto e^{2i\pi nx}$ (Exercice 2.34 Chap. 2). Cette théorie admet un analogue plus simple, mais utile et instructif, dans le cadre des groupes finis. C'est aussi l'un des chemins qui mène à la théorie des représentations des groupes finis, qui sera étudiée à la fin du cours.

Pour G un groupe *fini*, on note $\mathrm{L}^2(G)$ le $\mathbb{C}$-espace vectoriel des fonctions $G \to \mathbb{C}$, muni du produit scalaire hermitien $\langle f, f'\rangle = \frac{1}{|G|}\sum_{g\in G} f(g)\overline{f'(g)}$. C'est un espace de dimension finie $|G|$.

Théorème 2.1. *Soit G un groupe fini.*

(i) L'ensemble $\widehat{G}$ est une famille libre et orthonormée de $\mathrm{L}^2(G)$,

(ii) si G est abélien, alors $\widehat{G}$ est une base de $\mathrm{L}^2(G)$.

On appelle souvent le (i) la propriété d'*orthogonalité des caractères.*

Avant d'entamer la démonstration, observons que pour tout $g \in G$ on dispose d'un endomorphisme R_g de $\mathrm{L}^2(G)$ défini par $f \mapsto \mathrm{R}_g(f)$, $h \mapsto f(hg)$ (translation par g). Cet endomorphisme est unitaire : si $f, f' \in \mathrm{L}^2(G)$, et si $g \in G$, alors $\langle \mathrm{R}_g(f), \mathrm{R}_g(f')\rangle = \langle f, f'\rangle$. De plus, on a $\mathrm{R}_1 = \mathrm{id}$ et $\mathrm{R}_{gh} = \mathrm{R}_g \circ \mathrm{R}_h$ pour tout $g, h \in G$. Autrement dit, $g \mapsto \mathrm{R}_g$ défini un morphisme de groupes $G \to \mathrm{GL}(V)$ avec $V = \mathrm{L}^2(G)$. Ce morphisme est appelé *représentation régulière de G*. Observons

4. C'est à dire les fonctions 1-périodiques Lebesgue mesurables $f : \mathbb{R} \to \mathbb{C}$ telles que $\int_0^1 |f(t)|^2 dt < \infty$.

déjà que tout $\chi \in \widehat{G}$ vérifie $\mathrm{R}_g\chi = \chi(g)\chi$. Autrement dit, χ est vecteur propre de (chaque) R_g, de valeur propre $\chi(g)$.

Démonstration — Montrons le (i). Pour $\chi \in \widehat{G}$ on a déjà vu que $|\chi(g)| = 1$ pour tout $g \in G$. On en déduit $\langle \chi, \chi \rangle = \frac{1}{|G|} \cdot |G| = 1$. Pour voir qu'ils sont orthogonaux, il suffit de dire que pour $\chi \neq \chi'$, il existe $g \in G$ tel que $\chi(g) \neq \chi'(g)$, et donc χ et χ' sont dans des espaces propres pour des valeurs propres distinctes de l'endomorphisme unitaire R_g. Ils sont donc orthogonaux : on a $\langle \chi, \chi' \rangle = \langle \mathrm{R}_g\chi, \mathrm{R}_g\chi' \rangle = \langle \chi(g)\chi, \chi'(g)\chi' \rangle = \chi(g)\overline{\chi'(g)}\langle \chi, \chi' \rangle$, et donc $\langle \chi, \chi' \rangle = 0$ car $\chi(g)\overline{\chi'(g)} = \chi(g)\chi'(g)^{-1} \neq 1$. Prouvons enfin que les caractères sont linéairement indépendants. Si on a $0 = \sum_{\psi \in \widehat{G}} \mu_\psi \psi$ avec $\mu_\psi \in \mathbb{C}$ pour tout ψ, en faisant $\langle -, \chi \rangle$ on en déduit $\mu_\chi = 0$.

Montrons le (ii). Si G est abélien, les endomorphismes R_g avec $g \in G$ commutent. Comme un endomorphisme unitaire est diagonalisable, les R_g sont diagonalisables.[5] Ils sont donc co-diagonalisables : $\mathrm{L}^2(G)$ possède une base constituée de vecteurs propres communs à tous les R_g. Si f est un tel vecteur propre, on a $\mathrm{R}_g f = \lambda_g f$ pour tout $g \in G$, avec $\lambda_g \in \mathbb{C}^\times$ (car R_g est inversible, d'inverse $\mathrm{R}_{g^{-1}}$, ou encore car R_g est unitaire). La relation $\mathrm{R}_{gh} = \mathrm{R}_g \circ \mathrm{R}_h$ entraîne $\lambda_{gh} = \lambda_g\lambda_h$ pour $g, h \in G$. Autrement dit, la fonction $g \mapsto \lambda_g$ est dans $\widehat{G}$. Enfin, on a par définition $(\mathrm{R}_g f)(h) = f(hg)$, donc $f(hg) = \lambda_g f(h)$ pour tout $g, h \in G$, puis $f(g) = \lambda_g f(1)$. Comme $f \neq 0$, on a $f(1) \neq 0$, et quitte à remplacer f par $f/f(1)$ on peut supposer $f(1) = 1$, *i.e.* f est dans $\widehat{G}$. □

Corollaire 2.2. *Soit G un groupe abélien fini.*

(i) On a $|\widehat{G}| = |G|$.
(ii) Pour toute fonction $f : G \to \mathbb{C}$, on a $f = \sum_{\chi \in \widehat{G}} \langle f, \chi \rangle \chi$.

Les $\langle f, \chi \rangle$ sont appelés *coefficients de Fourier* de f, et la fonction $\widehat{f} \in \mathrm{L}^2(\widehat{G})$ définie par $\widehat{f}(\chi) = |G|\langle f, \chi \rangle$ est appelée *transformée de Fourier* de f. On constate alors que $f \mapsto \frac{1}{\sqrt{|G|}}\widehat{f}$ est une isométrie linéaire $\mathrm{L}^2(G) \to \mathrm{L}^2(\widehat{G})$, par le point (ii).

Démonstration — On a clairement $|G| = \dim \mathrm{L}^2(G)$, et aussi $\dim \mathrm{L}^2(G) = |\widehat{G}|$ par le (ii) du théorème. Cela montre le (i). Pour le (ii), on écrit $f = \sum_{\chi \in \widehat{G}} \lambda_\chi \chi$ pour certains $\lambda_\chi \in \mathbb{C}$ par le (ii) du théorème. Par le (i), on a $\langle f, \chi \rangle = \lambda_\chi$. □

Exemple 2.3. Dans le cas $G = \mathbb{Z}/n\mathbb{Z}$ on a déjà vu que les caractères de G sont les $\overline{k} \mapsto \zeta^k$ avec $\zeta^n = 1$. Le théorème montre donc que toute fonction $\mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$ est combinaison linéaire unique de ces fonctions. C'est le point de départ de la théorie de la *transformée de Fourier discrète*, utile en traitement du signal, et un outil important dans la *combinatoire additive*. Nous ne nous aventurerons pas ici dans ces directions !

Exemple 2.4. Supposons $G = \mathbb{Z}/p\mathbb{Z}$ avec p premier. Soit c un caractère non trivial du groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\times$. On peut voir c comme une fonction $\mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ en le prolongeant par 0 en 0 comme au §1. Attention, ce prolongement n'est pas du

5. On peut dire aussi ici que pour $n = |G|$ on a $g^n = 1$ par Lagrange, et donc $(\mathrm{R}_g)^n = \mathrm{id}$ de sorte que R_g est annulé par le polynôme $X^n - 1$, scindé à racines distinctes.

tout un caractère de $\mathbb{Z}/p\mathbb{Z}$, et de fait ses coefficients de Fourier sont intéressants ! En effet, si $\chi : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}^\times$ désigne le caractère $\overline{k} \mapsto \zeta^{-k}$ avec $\zeta = e^{2i\pi/p}$, on constate $\widehat{c}(\chi) = \mathrm{G}(c)$ (la somme de Gauss de c). Certaines des formules de la Proposition 1.13 prennent un peu plus de sens avec ce point de vue (sans toutefois simplifier substantiellement leur démonstration). Par exemple, la formule (ii) pourrait être déduite de l'Exercice 3.35 sur la convolution et du fait que $c \star c'(1)$ coïncide avec la somme de Jacobi $\mathrm{J}(c, c')$.

Une application du Théorème 2.1 due à Dedekind, qui est d'apparence anecdotique mais historiquement importante dans le développement par Frobenius de la théorie des représentations, est la question du calcul du *déterminant* d'un groupe fini G : nous renvoyons au court Complément 5 pour une discussion de cette anecdote, sur laquelle nous reviendrons également dans le dernier chapitre. Terminons ce paragraphe par un énoncé important de *prolongement des caractères.*

Proposition 2.5. *Soit G un groupe abélien fini et $H \subset G$ un sous-groupe. Pour tout caractère χ de H, il existe un caractère $\widetilde{\chi}$ de G vérifiant $\widetilde{\chi}_{|H} = \chi$.*

Démonstration — En effet, considérons l'application de restriction $r : \widehat{G} \to \widehat{H}$, $\chi \mapsto \chi_{|H}$. C'est clairement un morphisme de groupes. Son noyau est le sous-groupe des caractères de G triviaux sur H. Par la propriété universelle du groupe quotient G/H, si $\pi : G \to G/H$ désigne la projection canonique, alors l'application $\psi \mapsto \psi \circ G$ définit une bijection entre $\widehat{G/H}$ et $\ker r$. D'après le Corollaire 2.2, on a

$$|\widehat{G}| = |G|, \quad |\widehat{H}| = |H| \text{ et } |\ker r| = |\widehat{G/H}| = |G/H| = |G|/|H|.$$

On en déduit $|\mathrm{Im}\, r| = |\widehat{G}|/|\ker r| = |H| = |\widehat{H}|$, et donc r est surjective. □

Étant donné l'importance de ce résultat pour la section suivante, nous en donnons une seconde démonstration, à la fois plus directe et plus générale. Dans cet énoncé, les groupes en question ne sont plus nécessairement finis. Un groupe abélien D est dit *divisible* si pour tout entier $n \geqslant 1$, le morphisme de groupes $D \to D, x \mapsto x^n$, est surjectif. Par exemple, le groupe multiplicatif $\mathbb{C}^\times$, et les groupes additifs $\mathbb{Q}$ et $\mathbb{Q}/\mathbb{Z}$, sont des groupes abéliens divisibles, mais pas $\mathbb{Z}$ ou $\mathbb{Z}/m\mathbb{Z}$.

Proposition 2.6. (Prolongement des morphismes) *Soient G, H, D des groupes* abéliens *avec $H \subset G$, D divisible, et $f : H \to D$ un morphisme de groupes. Alors il existe un morphisme de groupes $\widetilde{f} : G \to D$ tel que $\widetilde{f}_{|H} = f$.*

Démonstration — Supposons d'abord que G est engendré par H et un élément $g \in G$. Tout élément de G s'écrit donc sous la forme hg^n pour certains $h \in H$ et $n \in \mathbb{Z}$, par commutativité de G. Cette écriture n'est pas nécessairement unique. En effet, considérons $K = \{n \in \mathbb{Z} \,|\, g^n \in H\}$; c'est un sous-groupe de $\mathbb{Z}$, donc de la forme $d\mathbb{Z}$ avec $d \geqslant 0$. Ainsi, si on a $hg^n = h'g^m$ avec $h, h' \in H$ et $n, m \in \mathbb{Z}$, on a $h^{-1}h' = g^{n-m}$ puis $n \equiv m \bmod d$ et $h' = h\,(g^d)^{\frac{n-m}{d}}$ avec $g^d \in H$. Comme g^d est dans H, il y a un sens à considérer $f(g^d) \in D$, et par divisibilité de G on peut choisir un élément $x \in D$ tel que $x^d = f(g^d)$ (si $d = 0$ on a $f(g^d) = f(1) = 1$ et on peut prendre $x = 1$). On a tout fait pour que l'application

$$\widetilde{f} : G \to D, \ hg^n \mapsto f(h)x^n,$$

soit bien définie : si on a $hg^n = h'g^m$ avec $h, h' \in H$ et $n, m \in \mathbb{Z}$, on a vu $n \equiv m \bmod d$ et $h' = h.(g^d)^{\frac{n-m}{d}}$ avec $g^d \in H$, de sorte qu'en appliquant f à cette dernière égalité on trouve $f(h') = f(h)(x^d)^{\frac{n-m}{d}}$ puis $f(h)x^n = f(h')x^m$. Enfin, il est clair que $\widetilde{f}$ ainsi définie est un morphisme de groupes tel que $\widetilde{f}_{|H} = f$.

Quand G est fini, ou plus généralement de type fini, disons $G = \langle b_1\rangle\langle b_2\rangle \cdots \langle b_r\rangle$ (car G est commutatif), on conclut en prolongeant f successivement à chaque sous-groupe $H_i := H\langle b_1\rangle\langle b_2\rangle \cdots \langle b_i\rangle$ pour $i = 1, \ldots, r$.

Pour un G général, on peut encore conclure par le lemme de Zorn. En effet, soit X l'ensemble des couples (H', f') avec H' un sous-groupe de G contenant H et $f' : H' \to D$ un morphisme prolongeant f. On munit X d'une relation d'ordre en posant $(H', f') \leqslant (H'', f'')$ si on a $H' \subset H''$ et $f''_{|H'} = f'$. On constate que $(X, \leqslant)$ est inductif. Si (H', f') est maximal, alors on a $H' = G$. En effet, sinon il existe $g \in G - H'$ et on peut prolonger f' à $H'\langle b\rangle$ par le premier cas étudié plus haut, ce qui contredit la maximalité de (H', f'). □

Remarque 2.7. L'énoncé est bien sûr très faux si D n'est pas divisible. Par exemple, si on prend $G = \mathbb{Z}/4\mathbb{Z}$ et $H = D = \mathbb{Z}/2\mathbb{Z}$, alors pour tout morphisme $\varphi : G \to D$ on a $\varphi(\overline{2}) = \varphi(2.\overline{1}) = 2\varphi(\overline{1}) = 0$. Ainsi, l'identité $f : H \to D, x \mapsto x$, ne se prolonge pas à G.

3. Structure des groupes abéliens finis

On se propose de classifier à isomorphismes près les groupes abéliens finis.

Théorème 3.1. *Soit G un groupe abélien fini. Il existe un unique entier*[6] *n, et des uniques entiers $a_i > 1$ pour $i = 1, \ldots, n$, vérifiant $a_1 \mid a_2 \mid \cdots \mid a_n$ et*

$$G \simeq \prod_{i=1}^{n} \mathbb{Z}/a_i\mathbb{Z}.$$

En particulier, tout groupe fini est isomorphe à un produit de groupes cycliques. Bien sûr, nous pouvons remplacer chaque $\mathbb{Z}/a_i\mathbb{Z}$ dans le produit ci-dessus par n'importe quel groupe cyclique d'ordre a_i, par exemple par μ_i.

Les entiers a_i de l'énoncé s'appellent les *facteurs invariants* de G. Ils vérifient bien sûr $|G| = a_1a_2 \cdots a_n$. Les a_i sont donc des diviseurs (ou *facteurs*) canoniques de $|G|$, au sens où ils sont uniquement déterminés par la structure de G.

Exemple 3.2. *D'après le Théorème 3.1, les groupes* abéliens *de cardinal* 8 *sont, à isomorphisme près, les groupes $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Bien noter qu'il existe aussi des groupes non abéliens d'ordre* 8*, comme le groupe* H_8*, sur lesquels le théorème ne dit rien et que nous étudierons plus tard.*

Attention aussi à bien comprendre l'énoncé : dans le cas du groupe abélien $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ on a nécessairement $n = 1$ et $a_1 = 6$, et donc $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z}$. L'existence d'un tel isomorphisme est aussi conséquence directe de l'isomorphisme chinois des restes (Corollaire 3.11). En guise d'autre exemple, les facteurs invariants

6. On convient qu'un produit vide de groupes vaut 1, de sorte que l'on a $G = \{1\}$ si, et seulement si, $n = 0$.

de $G = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ sont 2 et 30, car on a $2|30$. C'est bien cohérent avec la suite d'isomorphismes chinois suivante :

$$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}.$$

3.1. Démonstration de l'existence. Le principe de la démonstration va consister à caractériser d'abord le facteur invariant a_n comme étant l'*exposant* de G.

Définition 3.3. *L'*exposant *d'un groupe fini G est le plus petit entier $e \geqslant 1$ vérifiant $g^e = 1$ pour tout $g \in G$. On le note* $\exp G$.

Par définition, $\exp G$ est aussi le ppcm des ordres des éléments de G. En effet, pour $e \in \mathbb{Z}$ on a $g^e = 1$ pour tout $g \in G$ si, et seulement si, $\operatorname{ord} g, \mid e$ pour pour $g \in G$. On constate aussi que si on a $G = \prod_{i=1}^n \mathbb{Z}/a_i\mathbb{Z}$ alors l'exposant de G est le ppcm des a_i, c'est donc a_n si on suppose en outre $a_1 \mid a_2 \mid \cdots \mid a_n$.

Lemme 3.4. *Si G est un groupe abélien fini, il existe un élément $g \in G$ d'ordre l'exposant de G.*

Démonstration — Soient $e = \exp G$, de décomposition en facteurs premiers $e = \prod_i p_i^{\alpha_i}$. Comme e est le ppcm des ordres des éléments de G, pour tout i il existe un élément $g_i \in G$ d'ordre de la forme $p_i^{\alpha_i} m_i$. En particulier, $g_i^{m_i}$ est d'ordre exactement $p_i^{\alpha_i}$ (Lemme 3.6 Chap. 2). Le produit g des $g_i^{m_i}$ convient (Lemme 5.3 Chap. 2). □

Le dévissage en produit se fera ensuite grâce à l'énoncé suivant.

Proposition 3.5. *Soient G un groupe et H et K deux sous-groupes de G. On suppose $H \cap K = 1$, $G = HK$ et enfin $hk = kh$ pour tout $h \in H$ et tout $k \in K$. Alors l'application $(h, k) \mapsto hk$ définit un isomorphisme de groupes $H \times K \xrightarrow{\sim} G$.*

Sous les hypothèses de l'énoncé, on dit que G est *produit direct interne* de H et K. Noter que les groupes H et K ne sont pas supposés ici commutatifs (même s'ils le seront dans l'application ci-après).

Démonstration — Soit φ l'application de l'énoncé. Elle est surjective car $G = HK$. C'est un morphisme de groupes car on a $\varphi((h,k)(h',k')) = \varphi(hh', kk') = hh'kk' = hkh'k'$ puisque $h'k = kh'$ pour tout $h' \in H$ et $k' \in K$. Elle est injective car $hk = 1$ entraîne $h = k^{-1} \in H \cap K = \{1\}$. □

Démonstration — (partie existence du théorème) Soient G un groupe abélien fini, a l'exposant de G et $x \in G$ d'ordre a (Lemme 3.4). Le groupe cyclique $\langle x \rangle$ est d'ordre a. On peut donc trouver un caractère $\chi : \langle x \rangle \to \mathbb{C}^\times$ envoyant x sur $e^{2i\pi/a}$ (Proposition 1.3). Par prolongement des caractères, on peut trouver un caractère $\widetilde{\chi} : G \to \mathbb{C}^\times$ prolongeant χ (Proposition 2.5 ou 2.6).

Soit $g \in G$. On a $g^a = 1$ car a est l'exposant de G, donc $\widetilde{\chi}(g)^a = 1$, puis $\widetilde{\chi}(g) \in \mu_a$. Il existe donc $k \in \mathbb{Z}$ tel que $\widetilde{\chi}(g) = \widetilde{\chi}(x^k)$, puis $gx^{-k} \in \ker \widetilde{\chi}$. On a montré $G = \langle x \rangle \ker \widetilde{\chi}$. Comme d'autre part on a $\langle x \rangle \cap \ker \widetilde{\chi} = \{1\}$ car on a

$$\widetilde{\chi}(x^k) = 1 \iff \chi(x^k) = 1 \iff e^{2ik\pi/a} = 1 \iff k \equiv 0 \bmod a \iff x^k = 1,$$

c'est une situation de produit direct interne : la Proposition 3.5 montre $G \simeq \langle x \rangle \times \ker \widetilde{\chi}$. On conclut par récurrence sur $|G|$ car on a $\langle x \rangle \simeq \mathbb{Z}/a\mathbb{Z}$ et car l'exposant

du sous-groupe $\ker \widetilde{\chi}$ divise nécessairement a. (L'exposant d'un sous-groupe divise toujours l'exposant du groupe.) $\square$

3.2. Un exemple direct : les p-groupes abéliens élémentaires.

Définition 3.6. *Soit p un nombre premier. Un groupe abélien fini est dit p-*élémentaire *si on a $g^p = 1$ pour tout $g \in G$, soit encore en notation additive, si on a $px = 0$ pour tout $x \in G$.*

L'observation importante est qu'un tel groupe G est le groupe additif d'une unique structure de $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel. En effet, pour $n \in \mathbb{Z}$ et $x \in G$, l'élément nx ne dépend que de $\overline{n} \in \mathbb{Z}/p\mathbb{Z}$, et l'application $\mathbb{Z}/p\mathbb{Z} \times G \to G$, $(\overline{n}, x) \mapsto nx$ munit le groupe G d'une structure d'espace vectoriel sur le corps $\mathbb{Z}/p\mathbb{Z}$: on a $1x = x$, $m(nx) = (mn)x$, et $(m+n)x = mx + nx$ et $m(x+y) = mx + my$. Notons $G^\sharp$ ce $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel. On constate que les sous-groupes de G coïncident avec les sous-espaces vectoriels de $G^\sharp$, que les familles génératrices du groupe G et coïncident avec celle de l'espace vectoriel $G^\sharp$, qu'un morphisme $G \to H$ est la même chose une application linéaire $G^\sharp \to H^\sharp$ etc...

Proposition 3.7. *Soient p premier et G un groupe abélien fini. Alors G est p-élémentaire si, et seulement si, on a $G \simeq (\mathbb{Z}/p\mathbb{Z})^n$ pour un certain entier $n \geqslant 1$. De plus, le nombre minimal de générateurs de G est* $\dim_{\mathbb{Z}/p\mathbb{Z}} G^\sharp$.

Démonstration — Pour la première assertion, il suffit de considérer une base de $G^\sharp$ comme $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel. Pour la seconde, c'est le fait qu'une famille d'éléments de G engendre G si, et seulement si, elle engendre le $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel $G^\sharp$. $\square$

Cela redémontre (directement et facilement !) le Théorème 3.1 pour les groupes abéliens p-élémentaires : tous les facteurs invariants sont égaux à p, et il y en a exactement n où $|G| = p^n$.

3.3. Démonstration de l'unicité. Si G est un groupe, on note $\min(G)$ le nombre minimal de générateurs de G. Par définition, il est fini si, et seulement si, G est de type fini. Par la Proposition 3.7 par exemple $\min((\mathbb{Z}/p\mathbb{Z})^n) = n$ pour p premier et $n \geqslant 1$.

Remarque 3.8. Soient G et G' deux groupes et $n \geqslant 1$ un entier. Si $g_1, \ldots, g_n$ engendrent G, et si $f : G \to G'$ est un morphisme surjectif, alors $f(g_1), \ldots, f(g_n)$ engendrent G'. En particulier, on a $\min(G') \leqslant \min(G)$. En considérant la projection $G \times G' \to G, (g, g') \to g$, on en déduit par exemple $\min(G) \leqslant \min(G \times G')$.

Illustrons cette notion en montrant d'abord l'unicité du n dans le Théorème 3.1.

Proposition 3.9. *Supposons $G = \mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}$ avec $n \geqslant 1$ et les a_i entiers tels que $a_1 \mid a_2 \mid \cdots \mid a_n$ et $a_1 > 1$. On a $n = \min(G)$.*

Démonstration — Le groupe G est engendré par les n éléments par e_i avec $e_i = (0, \ldots, 0, \overline{1}, 0, \ldots, 0)$ (le $\overline{1}$ à la place i). On a donc $\min(G) \leqslant n$. D'autre part, pour p premier divisant a_1 on a $p \mid a_i$ pour tout i et on peut donc considérer un morphisme surjectif $f : G \to (\mathbb{Z}/p\mathbb{Z})^n$ en considérant coordonnée par coordonnée le morphisme évident $\mathbb{Z}/a_i\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}, n \bmod a_i \mapsto n \bmod p$ (bien défini car $p \mid a_i$). D'après la Remarque 3.8, on a alors $\min(G) \geqslant \min((\mathbb{Z}/p\mathbb{Z})^n) = n$. $\square$

Pour terminer la démonstration, nous allons considérer des sous-groupes naturels et judicieux des groupes abéliens finis.

Définition 3.10. *Soient G un groupe abélien et $n \geqslant 1$. Le sous-ensemble $G[n] = \{g \in G \mid g^n = 1\}$ est un sous-groupe de G appelée n-torsion de G.*

Ce groupe est le noyau du morphisme $G \to G,\ g \mapsto g^n$ (dont l'image, les puissance n-èmes, est intéressante aussi mais laissée de côté ici). Un élément de $G[n]$ est appelé aussi élément de n-torsion : c'est par définition un élément d'ordre fini divisant n. Si $n = p$ est premier, et si G est fini, alors $G[p]$ est abélien p-élémentaire.

Lemme 3.11. *Soient G et H deux groupes abéliens et $n \geqslant 1$.*

(i) On a $(G \times H)[n] = G[n] \times H[n]$.

(ii) Tout (iso-)morphisme $G \to H$ induit un (iso-)morphisme $G[n] \to H[n]$.

(iii) Supposons G cyclique d'ordre m et p premier. On a $G[p] = \{1\}$ sauf si $p|m$, auquel cas on a $G[p] \simeq \mathbb{Z}/p\mathbb{Z}$ et $G/G[p] \simeq \mathbb{Z}/(m/p)\mathbb{Z}$.

Démonstration — Les (i) et (ii) sont évidents. Le (iii) est par exemple conséquence du Lemme 3.7 Chap. 2. De manière directe, écrivons $G = \langle g \rangle$ avec g d'ordre m. Pour $k \in \mathbb{Z}$ on a $(g^k)^p = 1$ si, et seulement si, $m \mid kp$. Si $p \nmid m$, cela équivaut à $k \equiv 0 \bmod m$, et donc $G[p] = \{1\}$. Si $p|m$, cela équivaut à $k \equiv 0 \bmod m/p$. On a donc $G[p] = \langle g^{m/p} \rangle \simeq \mathbb{Z}/p\mathbb{Z}$, et le groupe $G/G[p]$, qui est engendré par l'image de g dans $G/G[p]$, est donc isomorphe à $\mathbb{Z}/(m/p)\mathbb{Z}$. □

Démonstration — (de assertion d'unicité du Théorème 3.1) Soit $\mathscr{A}_n$ l'ensemble des suites finies $a = (a_1, \ldots, a_n)$ d'entiers $\geqslant 1$ avec $a_1 \mid a_2 \mid \cdots \mid a_n$ (il est plus simple dans l'argument qui suit de ne pas supposer $a_1 > 1$). Pour $a \in \mathscr{A}_n$ on pose $G_a = \prod_{i=1}^n \mathbb{Z}/a_i\mathbb{Z}$. On suppose $a, b \in \mathscr{A}_n$ et $G_a \simeq G_b$, on veut montrer $a = b$.

On raisonne par récurrence sur $\sum_{i=1}^n (a_i + b_i)$. On conclut par récurrence si $a_1 = b_1 = 1$ car on a $\mathbb{Z}/\mathbb{Z} \simeq 1$ et $G \times 1 \simeq G$. Quitte à échanger a et b on peut supposer $a_1 > 1$. Soit p premier divisant a_1, et donc tous les a_i. Par le Lemme 3.11 (i) et (iii), on a donc $|G_a[p]| = p^n$, et $|G_b[p]| = p^r$ où r est le nombre d'entiers $1 \leqslant i \leqslant n$ tels que $p|b_i$. Mais on a aussi

$$G_a[p] \simeq G_b[p] \text{ et } G_a/G_a[p] \simeq G_b/G_b[p]$$

par le point (ii) du Lemme 3.11. De l'identité de gauche on déduit $r = n$ puis $p|b_i$ pour tout i. Mais toujours par le (iii) on constate que $G_a/G_a[p]$ et $G_b/G_b[p]$ sont respectivement isomorphes à[7] $G_{a'}$ et $G_{b'}$ avec $a'_i = a_i/p$ et $b'_i = b_i/p$ pour tout i (voir l'Exercice 2.31 Chap. 2). Par récurrence on en déduit $a' = b'$, puis $a = b$. □

7. On pourrait se passer de l'usage de quotients ici en disant que les sous-groupes des multiples de p dans G_a et G_b sont isomorphes, et respectivement isomorphes à $G_{a'}$ et $G_{b'}$.

3.4. Digression : sommes directes de groupes abéliens. Notre expérience des espaces vectoriels rend la notion de somme directe interne plus intuitive que celle de produit direct du point de vue additif. On fixe donc A un groupe abélien noté additivement. Si $A_1, A_2, \ldots, A_n$ sont des sous-groupes de A, on pose

$$A_1 + A_2 + \cdots + A_n = \{\sum_{i=1}^{n} a_i \mid a_i \in A_i\}.$$

C'est manifestement un sous-groupe de A, appelé *somme* des A_i, encore noté $\sum_i A_i$. Par exemple, si $A_i = \mathbb{Z}a_i$ pour tout i, alors $A_1 + A_2 + \cdots + A_n$ coïncide avec le sous-groupe $\langle a_1, a_2, \ldots, a_n\rangle$ de A engendré par les a_i. En général, l'application

$$\varphi : A_1 \times A_2 \times \cdots \times A_n \to A, (a_i) \mapsto \sum_i a_i, \tag{19}$$

est manifestement un morphisme de groupes d'image $\sum_i A_i$. Elle est surjective si, et seulement si, on a $A = \sum_i A_i$. Si φ est injectif (*i.e.* $\ker\varphi = \{0\}$), on dit que les A_i sont en *somme directe*, et on note alors aussi $\oplus_i A_i$ la somme des A_i.

Définition 3.12. *On dit que A est somme directe interne de ses sous-groupes A_i si l'application* (19) *est bijective, i.e. si on a $A = \oplus_i A_i$.*

Discutons enfin du point de vue *externe*. Maintenant $A_1, \ldots, A_n$ sont des groupes abéliens quelconques et on pose $A = \prod_{i=1}^n A_i$. Pour tout i, le sous-groupe $A'_i = \{(a_j) \mid a_j = 0, \forall j \neq i\}$ de A est manifestement isomorphe à A_i, via l'inclusion $a \mapsto (0, \ldots, a, \ldots, 0)$, c'est pourquoi on le note souvent encore A_i. On a alors

$$\prod_{i=1}^{n} A_i = \bigoplus_{i=1}^{n} A'_i, \text{ avec } A'_i \simeq A_i \text{ pour tout } i = 1, \ldots, n.$$

C'est pourquoi lorsqu'on le voit ainsi, le groupe produit $\prod_{i=1}^n A_i$ est aussi noté $\bigoplus_{i=1}^n A_i$ et il est appelé *somme directe externe des A_i*. En particulier, on obtient la formulation suivante du Théorème 3.1.

Corollaire 3.13. *Pour tout groupe abélien fini G, de facteurs invariants a_1, a_2, $\cdots$, a_n, on a une décomposition $G = \oplus_{i=1}^n C_i$ avec C_i cyclique d'ordre a_i.*

⚠ Il faut bien noter que *la décomposition ci-dessus n'est pas unique*. En effet, considérons le cas $G = (\mathbb{Z}/p\mathbb{Z})^2$ avec p premier. Se donner une écriture $G = C_1 \oplus C_2$ avec $C_1 \simeq C_2 \simeq \mathbb{Z}/p\mathbb{Z}$ est la même chose que se donner une décomposition en somme directe de deux droites du plan $G^\sharp$: il y a exactement $p+1$ droites dans $G^\sharp$ (pourquoi ?) et donc $\frac{p(p+1)}{2}$ telles décompositions.

4. Groupes abéliens de type fini

Dans toute cette section G est un groupe abélien noté additivement.

Définition 4.1. *Soient $\mathscr{F} = \{g_1, \ldots, g_n\}$ une famille d'éléments de G, et*

$$f : \mathbb{Z}^n \to G, (m_i) \mapsto \sum_{i=1}^{n} m_i g_i.$$

le morphisme de groupes associé. On dit que $\mathscr{F}$ est libre (ou $\mathbb{Z}$-libre) si f est injectif. On rappelle que $\mathscr{F}$ est génératrice (ou $\mathbb{Z}$-génératrice) si f est surjective. On dit enfin que $\mathscr{F}$ est une base (ou une $\mathbb{Z}$-base) si f est bijective.

Par exemple, la *base canonique* ϵ_i de $\mathbb{Z}^n$, définie par $(\epsilon_i)_j = \delta_{i,j}$, est clairement une $\mathbb{Z}$-base de $\mathbb{Z}^n$. L'anneau $\mathbb{Z}$ n'étant pas un corps, des différences substantielles apparaissent entre ces notions et les notions analogues dans les espaces vectoriels. Par exemple, la famille singleton $\{g\}$, avec $g \in G$, est libre si, et seulement si, g est d'ordre infini. Dans le groupe $G = \mathbb{Z}$, la famille $\{2, 3\}$ est génératrice, non libre car $2 \cdot 3 - 3 \cdot 2 = 0$, et on ne peut en extraire de base ! De même, la famille $\{2\}$ de $\mathbb{Z}$ est libre, mais elle ne se complète pas en une base : une famille $\{a, b\}$ a deux éléments non nuls de $\mathbb{Z}$ n'est jamais libre à cause de la relation $ba - ab = 0$.

Définition 4.2. *Un groupe abélien est dit* libre de rang n *s'il possède une $\mathbb{Z}$-base à n éléments, ou ce qui revient au même, s'il est isomorphe à $\mathbb{Z}^n$.*

Par conventions, $\{0\}$ est libre de rang 0. Le lemme suivant montre que l'entier n dans la définition ci-dessus est uniquement déterminé.

Lemme 4.3. *Pour tout entier $n \geqslant 0$ on a $\min(\mathbb{Z}^n) = n$. En particulier, on a $\mathbb{Z}^n \simeq \mathbb{Z}^m$ si, et seulement si, $n = m$.*

Démonstration — L'inégalité $\min(\mathbb{Z}^n) \leqslant n$ est évidente. En considérant le morphisme $\mathbb{Z}^n \to (\mathbb{Z}/2\mathbb{Z})^n$ de réduction modulo 2 sur chaque coordonnée, qui est surjectif, on a l'inégalité opposée $\min(\mathbb{Z}^n) \geqslant \min((\mathbb{Z}/2\mathbb{Z})^n) = n$. La seconde assertion s'en déduit car $G \simeq G'$ implique $\min(G) = \min(G')$ (Remarque 3.8 !). □

Parmi les exemples les plus importants de groupes abélien libres, on trouve les *réseaux* des espaces vectoriels réels de dimension finie.

Exemple 4.4. (*Réseaux*) Soit V un $\mathbb{R}$-espace vectoriel de dimension finie n. Un *réseau* de V est un sous-groupe additif $\Lambda \subset V$ de la forme $\Lambda = \oplus_{i=1}^n \mathbb{Z}e_i$ avec $e_1, \ldots, e_n$ une $\mathbb{R}$-base de V. En particulier, un réseau est libre de rang n. Par exemple, $\mathbb{Z}^n$ est un réseau de $\mathbb{R}^n$. On peut démontrer la caractérisation topologique suivante : un sous-groupe H de V est un réseau si, et seulement si, (i) H et discret et (ii) H engendre V comme $\mathbb{R}$-espace vectoriel. Nous renvoyons au Complément 6 pour une démonstration de cet énoncé.

Le résulat principal suivant ramène la structure des groupes abéliens de type fini à celle des groupes abéliens finis, déjà élucidée. On pose

$$G_{\mathrm{tor}} = \{g \in G \mid \exists n \geqslant 1,\ ng = 0\}$$

l'ensemble des éléments *de torsion* de G. C'est manifestement un sous-groupe de G, appelé *sous-groupe de torsion*, égal à la réunion des $G[n]$ pour $n \geqslant 1$.

Théorème 4.5. (Dirichlet) *Si G est un groupe abélien de type fini, son sous-groupe G_{tor} est fini et il existe un unique entier $n \geqslant 0$ tel que $G \simeq G_{\mathrm{tor}} \times \mathbb{Z}^n$.*

L'entier n ci-dessus est appelé *rang* de G. On dit que G est *sans torsion* si $G_{\mathrm{tor}} = \{0\}$.

Corollaire 4.6. *Un groupe abélien de type fini sans torsion est libre*

Pour démontrer le Théorème 4.5, nous aurons besoin du lemme suivant, qui dégage une propriété remarquable de $\mathbb{Z}$, appelée *projectivité*.

Lemme 4.7. *Soient G un groupe abélien et $f : G \to \mathbb{Z}$ un morphisme surjectif. Alors G est isomorphe à $\mathbb{Z} \times \ker f$.*

Démonstration — Par surjectivité de f, il existe $h \in G$ tel que $f(h) = 1$. L'élément h est d'ordre infini, car $nh = 0$ implique $0 = nf(h) = n \in \mathbb{Z}$. On a donc $H := \langle h \rangle \simeq \mathbb{Z}$. Vérifions que G est produit direct interne de H et de $\ker f$. On vient juste de montrer $H \cap \ker f = \{0\}$. Vérifions $G = H + \ker f$. Soit $g \in G$. Posons $n := f(g) \in \mathbb{Z}$, on a alors $f(g) = n = f(nh)$ et donc $g - nh \in \ker f$. □

Démonstration — (du Théorème) Soit G un groupe abélien de type fini. Montrons d'abord que s'il existe un élément d'ordre infini dans G, alors G est isomorphe à $G' \times \mathbb{Z}$ pour un certain groupe G'. Un tel G' est alors nécessairement abélien, et vérifie $\min(G') \leqslant \min(G) < \infty$ par la Remarque 3.8.

Supposons donc qu'il existe $g \in G$ d'ordre infini. Choisissons un isomorphisme $f : \langle g \rangle \xrightarrow{\sim} \mathbb{Z}$. D'après la Proposition 2.6, on peut étendre f en un morphisme $\widetilde{f} : G \to \mathbb{Q}$, car $\mathbb{Q}$ est divisible. Mais $\widetilde{f}(G)$ est un sous-groupe de type fini de $\mathbb{Q}$, donc de la forme $\mathbb{Z}\lambda$ pour un certain $\lambda \in \mathbb{Q}$ (Cor. 7.1 Chap. 1). On a $\lambda \neq 0$ car $\widetilde{f}(G)$ contient $f(G) = \mathbb{Z}$. Quitte à diviser $\widetilde{f}$ par λ, on a donc trouvé un morphisme surjectif $G \to \mathbb{Z}$. On conclut par le Lemme 4.7.

Posons $N = \min(G)$. Si on a $G \simeq G' \times \mathbb{Z}^n$ alors $N \leqslant n$ par le Lemme 4.3 et la Remarque 3.8. On en déduit que l'on peut itérer au plus N fois la première étape, *i.e.* qu'il existe $n \leqslant N$ tel que $G \simeq G' \times \mathbb{Z}^n$ et tel que tous les éléments de G' sont d'ordre fini. Mais alors on a aussi $\min(G') \leqslant \min(G) < \infty$, donc G' est de type fini, et comme ses él'ements sont d'ordre fini il est alors nécessairement fini (pourquoi ?). Le Lemme 4.8 montre alors $G' \simeq G_{\mathrm{tor}}$ et $n = \min(G/G_{\mathrm{tor}})$, d'où l'assertion d'unicité. □

Lemme 4.8. *Soient A et B deux groupes abéliens avec A fini et B libre de rang fini. Alors si on pose $G = A \times B$ on a $G_{\mathrm{tors}} = A \times \{0\}$ et $G/G_{\mathrm{tors}} \simeq B$.*

Démonstration — On a $G_{\mathrm{tor}} = A_{\mathrm{tor}} \times B_{\mathrm{tor}}$ (Lemme 3.11) avec $A_{\mathrm{tor}} = A$ et $B_{\mathrm{tor}} = \{0\}$, donc $G_{\mathrm{tors}} = A \times \{0\}$. On conclut car le morphisme de projection $G \to B, (a, b) \mapsto b$, est surjectif de noyau G_{tors}. □

5. Complément I : Déterminant d'un groupe abélien fini

Soit G un groupe fini. Suivant Dedekind, le *déterminant de* G est le polynôme

$$\det G := \det(X_{gh^{-1}})_{g,h \in G},$$

où les X_g sont des indéterminées indexées par les éléments de G. C'est donc un polynôme homogène de degré $|G|$ en les X_g, et la question posée par Dedekind est de le factoriser dans $\mathbb{C}[\{X_g,\, g \in G\}]$. Par exemple, det $\mathbb{Z}/n\mathbb{Z}$ est le déterminant de la matrice circulante $(X_{i-j \bmod n})_{1 \leqslant i,j \leqslant n}$, et pour le groupe de Klein on a

$$\det \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \det \begin{bmatrix} E & A & B & C \\ A & E & C & B \\ B & C & E & A \\ C & B & A & E \end{bmatrix},$$

avec $E = X_{(\bar{0},\bar{0})}$, $A = X_{(\bar{1},\bar{0})}$, $B = X_{(\bar{0},\bar{1})}$ et $C = X_{(\bar{1},\bar{1})}$.

Proposition 5.1. (Dedekind) *Si G est un groupe abélien fini, on a*

$$\det G = \prod_{\chi \in \widehat{G}} (\sum_{g \in G} \chi(g) X_g).$$

Démonstration — Soit $(x_g)_g \in \mathbb{C}^G$. Il suffit de montrer l'égalité des deux polynômes de l'énoncé aprés évaluation des X_g en x_g. Considérons l'endomorphisme $u = \sum_{g \in G} x_g \mathrm{R}_g$ de $\mathrm{L}^2(G)$. Notons $e_h : G \to \mathbb{C}$ la fonction caractéristique du singleton $\{h\}$. Les e_h, $h \in H$, forment une base de $\mathrm{L}^2(G)$. On a $\mathrm{R}_g(e_h) = e_{hg^{-1}}$, et donc $u(e_h) = \sum_{g \in G} x_g e_{hg^{-1}} = \sum_{g \in G} x_{g^{-1}h} e_g$. On en déduit que $\det(G)$, évalué en les x_g, coïncide avec $\det u$. Mais on a aussi $u(\chi) = (\sum_g x_g \chi(g))\chi$ pour tout $\chi \in \widehat{G}$. D'après le Théorème 2.1, cela conclut si G est abélien, car les χ forment une base de $\mathrm{L}^2(G)$ constituée de vecteurs propres de u, de valeurs propres les $\sum_g \chi(g) x_g$. □

Exemple 5.2. Par exemple, on retrouve la formule classique pour le déterminant circulant $\det \mathbb{Z}/n\mathbb{Z} = \prod_{\zeta^n=1} (\sum_{i \in \mathbb{Z}/n\mathbb{Z}} \zeta^i X_i)$, et on a aussi la formule $\det \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = (E+A+B+C)(E-A+B-C)(E+A-B-C)(E-A-B+C)$ (pourquoi ?).

Pour G non commutatif, la démonstration ci-dessus montre que $\det G$ est divisible par $\prod_{\chi \in \widehat{G}} (\sum_{g \in G} \chi(g) X_g)$, mais qu'il a d'autres facteurs. C'est en souhaitant déterminer ces facteurs que Frobenius a inventé la théorie des représentations des groupes finis : nous reviendrons sur ce point dans le complément 7. Par exemple pour $G = \mathrm{S}_3$, alors $\det G$ contient aussi un facteur irréductible de degré 2 (avec multiplicité 2).

6. Compléments II : Réseaux et sous-groupes fermés de $\mathbb{R}^n$

Soit V un $\mathbb{R}$-espace vectoriel de dimension finie, que l'on munit de sa topologie d'espace vectoriel normé. On se propose dans ce complément de déterminer les sous-groupes fermés du groupe additif de V. Le cas de la dimension 1 a déjà été traité dans la Proposition 7.3 du Complément 7 Chap. 2 : un sous-groupe fermé de $\mathbb{R}$ est soit égal à $\mathbb{R}$, soit de la forme $a\mathbb{Z}$ avec $a \in \mathbb{R}$. Une notion clé en général est celle de sous-groupe *discret*.

Proposition-Définition 6.1. *Soit H un sous-groupe de V. On dit que H est* discret *dans V si les propriétés équivalentes suivantes sont satisfaites :*

(i) il existe un voisinage U de 0 dans V avec $U \cap H = \{0\}$,

(ii) pour tout compact K de V alors $K \cap H$ est fini.

Démonstration — Il est clair que l'on a (ii) $\Longrightarrow$ (i) pour tout sous-ensemble H de V. Soient U comme au (i) et K un compact de V. Si $K \cap H$ est infini, il existe une suite d'éléments distincts k_n de $K \cap H$. Quitte à extraire, on peut la supposer convergente dans V par compacité. Les éléments $k_{n+1} - k_n$ sont dans H, non nuls, tendent vers 0, et sont donc dans U pour n assez grand : une contradiction. □

On rappelle qu'un *réseau* de V est un sous-groupe de V de la forme

$$H = \bigoplus_{i=1}^{n} \mathbb{Z} e_i$$

où $e_1, \ldots, e_n$ une base de l'espace vectoriel V. Un réseau est discret. En effet, par équivalence des normes il suffit d'observer que pour $\|\cdot\|$ la norme sup. dans la base des e_i, et $m \geqslant 0$ entier, on a $|\{h \in H \mid \|h\| \leqslant m\}| = (2m+1)^n < +\infty$. Le résultat remarquable est que la réciproque est aussi vraie.

THÉORÈME 6.2. *Soient H un sous-groupe discret d'un $\mathbb{R}$-espace vectoriel de dimension finie et V le sous-espace engendré par H. Alors H est un réseau de V. En particulier, H est un groupe abélien libre de rang* $\dim V$.

DÉMONSTRATION — Comme H engendre V comme $\mathbb{R}$-espace vectoriel, il contient une $\mathbb{R}$-base de V (base incomplète). Fixons $(e_1, \ldots, e_n)$ une base de V avec $e_i \in H$ pour tout i. Tout élément $v = \sum_{i=1}^n v_i e_i$ de V, avec $v_i \in \mathbb{R}$, s'écrit aussi $v = [v] + \{v\}$ avec $[v] := \sum_{i=1}^n \lfloor v_i \rfloor e_i \in H$ et $\{v\} := \sum_{i=1}^n \{v_i\} e_i$, où $\lfloor x \rfloor$ et $\{x\}$ désignent respectivement la partie entière inférieure et la partie fractionnaire du réel x. Notons que $\{v\}$ est un élément du compact

$$\Pi = \{\sum_{i=1}^{n} x_i e_i \mid 0 \leqslant x_i \leqslant 1\}.$$

Pour $v \in H$ on constate $\{v\} = v - [v] \in H \cap \Pi$. Mais H étant discret, l'ensemble $X := H \cap \Pi$ est fini. Regardons alors la projection linéaire

$$f : V \to \mathbb{R}, \ \sum_{i=1}^{n} v_i e_i \mapsto v_1.$$

Pour $h \in H$ on a $f(h) = f([h]) + f(\{h\})$ avec $f([h]) \in \mathbb{Z}$ et $f(\{h\}) \in f(X)$. Ainsi, $f(H)$ est un sous-groupe de $\mathbb{R}$, inclus dans la réunion finie des $\mathbb{Z} + f(x)$ avec $x \in X$. Il est donc discret dans $\mathbb{R}$, puis de la forme $\mathbb{Z}\lambda$ pour un certain $\lambda \in \mathbb{R}$ par la Proposition 7.3. On a aussi $f(H) \neq \{0\}$ car H n'est pas inclus dans l'hyperplan $U := \ker f$. Fixons $h_0 \in H$ tel que $\lambda = f(h_0)$. On a alors

$$H = \mathbb{Z}\, h_0 \oplus (H \cap U).$$

En effet, on a bien sûr $V = \mathbb{R}\, h_0 \oplus U$, donc la somme de droite est directe (et incluse dans H). Enfin, pour $h \in H$ il existe $n \in \mathbb{Z}$ avec $f(h) = n\lambda = f(nh_0)$, et donc on a bien $h = nh_0 + (h - nh_0) \in \mathbb{Z}h_0 + (H \cap U)$. On conclut par récurrence sur $\dim V$ car $H \cap U$ est clairement discret dans U, et engendre U comme $\mathbb{R}$-espace vectoriel. □

COROLLAIRE 6.3. *Tout sous-groupe de $\mathbb{Z}^n$ est isomorphe à $\mathbb{Z}^m$ pour $m \leqslant n$.*

DÉMONSTRATION — Le groupe $\mathbb{Z}^n$ peut être vu comme un réseau de $\mathbb{R}^n$. Ses sous-groupes sont donc discrets dans $\mathbb{R}^n$, et engendrent un sous-espace vectoriel réel de dimension $m \leqslant n$. On conclut par le théorème. □

Pour une démonstration plus directe de ce résultat nous renvoyons à l'Exercice 3.11. Nous en verrons une généralisation lorsque nous parlerons de *modules sur les anneaux principaux*. On peut déduire enfin du Théorème 6.2 une classification de tous les sous-groupes *fermés* de $\mathbb{R}^n$.

THÉORÈME 6.4. *Soient V un $\mathbb{R}$-espace vectoriel de dimension finie et $H \subset V$ un sous-groupe fermé. Soient A le plus grand sous-espace vectoriel de V inclus dans H, W le sous-espace de V engendré par H, et B un supplémentaire de A dans W. Alors $H \cap B$ est un réseau de B, on a $H = A \oplus (H \cap B)$, et*

$$H \simeq \mathbb{R}^a \times \mathbb{Z}^b, \text{ avec } a = \dim A \text{ et } b = \dim B.$$

Nous allons d'abord montrer le lemme suivant.

LEMME 6.5. *Soit H un sous-groupe fermé du $\mathbb{R}$-espace vectoriel de dimension finie V. Si H n'est pas discret alors H contient une droite de V.*

DÉMONSTRATION — On fixe une norme $\|\cdot\|$ sur V. Si x est un réel, on notera $\lfloor x \rfloor \in \mathbb{Z}$ sa partie entière inférieure, vérifiant $x - \lfloor x \rfloor \in [0, 1[$. Si H n'est pas discret, il existe une suite $(h_n)_{n \geqslant 1}$ d'éléments de $H \smallsetminus \{0\}$ avec $h_n \to 0$ dans V. Si l'on pose $k_n = \lfloor 1/\|h_n\| \rfloor$ on a alors

$$k_n \in \mathbb{Z}_{\geqslant 0}, \ k_n \to \infty \ \text{ et } \ \|k_n h_n\| \to 1$$

(car $|\,\|k_n\, h_n\| - k_n |h_n|| \leqslant |h_n|$). Par compacité des fermés bornés de V, et quitte à extraire une sous-suite, on peut supposer $k_n h_n \to e$, pour un certain $e \in V$ de norme 1. On a $e \in H$ car H est fermé dans V et $k_n h_n \in H$. Montrons $\mathbb{R}e \subset H$. Soit $\lambda \in \mathbb{R}$. On pose $a_n = \lfloor \lambda k_n \rfloor$ et $b_n = \lambda k_n - a_n \in [0, 1[$. On a alors $\lambda k_n h_n = a_n h_n + b_n h_n$, et en faisant tendre n vers l'infini on en déduit $a_n h_n \to \lambda e$, puis $\lambda e \in H$. □

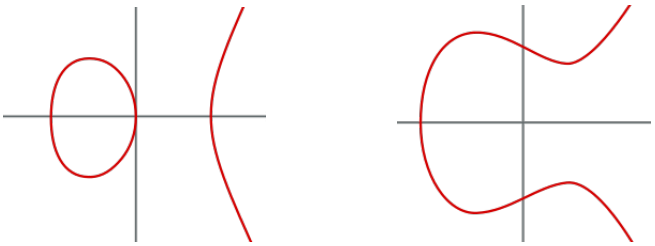
DÉMONSTRATION — (du Théorème 6.4) Comme la somme de deux sous-espaces de V inclus dans H est encore inclus dans H, le sous-espace A de l'énoncé existe, et coïncide avec le sous-espace de dimension maximale de V inclus dans H. Si B est un supplémentaire de A dans W, on constate que l'on $H = A \oplus (H \cap B)$. En effet, tout élément w de W s'écrit $w = a + b$ avec $a \in A$ et $b \in B$. Comme on a $A \subset H$, on a $w \in H$ si, et seulement si $b \in H$. Enfin, $H \cap B$ est un sous-groupe fermé de B (comme intersection), et il engendre B car H engendre W. Enfin, $H \cap B$ est discret dans B par le Lemme 6.5 et par définition de A. On conclut par le Théorème 6.2. □

7. Courbes elliptiques (culturel)

On fixe un corps k, supposé de caractéristique $\neq 2, 3$ pour simplifier. Une *courbe elliptique* sur k est une courbe plane de la forme

$$C = \{(x, y) \in k^2 \mid y^2 = f(x)\},$$

où $f \in k[X]$ un polynôme de degré 3 *donné* et supposé sans racine double dans k. Par exemple pour $k = \mathbb{R}$, la courbe C est une courbe lisse qui a l'une des deux allures suivantes, selon que f a 3 ou 1 racines réelles.



L'ensemble C a une involution naturelle, $(x, y) \mapsto (x, -y)$, que l'on note simplement $P \mapsto -P$. Il sera important aussi de rajouter un point supplémentaire à C, noté O, auquel on pense comme étant à « l'infini verticalement », et on pose $E = C \coprod \{O\}$. La méthode des *cordes et des tangentes*[8] permet alors de définir une loi de composition $E \times E \to E, (P, Q) \mapsto P + Q$, de neutre O, de la manière suivante.[9] Si P et Q sont deux points de C, la *corde-tangente* associée est la droite affine (PQ) dans le cas $P \neq Q$, et la tangente à C en $P = Q$ sinon. Cette tangente est bien définie par les hypothèses sur f et k, et on la note encore (PQ).

(i) Si (PQ) n'est pas verticale, donc d'équation $y = ax + b$ avec $a, b \in k$, on constate que le système d'équations $y = ax+b$ et $y^2 = f(x)$, définissant l'intersection $C \cap (PQ)$, a toujours exactement trois solutions (avec possibles multiplicités), disons $\{\{P, Q, R\}\}$, et on pose $P + Q = -R$.

(ii) Si (PQ) est verticale, on pose $P + Q = O$.

Il se trouve que cette loi est associative, un fait géométrique peu évident que l'on peut vérifier péniblement par calcul direct, ou de manière plus élégante en utilisant le théorème de Bézout en géométrie projective. La loi $+$ est par définition commutative, et même alors une loi de groupe, l'inverse d'un point P étant le point $-P$ par définition. Voici quelques résultats connus remarquables sur ce groupe :

Théorème 7.1. (Culturel) *Soit E une courbe elliptique sur le corps k.*

(i) (Weierstrass) *Si $k = \mathbb{C}$, alors $E \simeq \mathbb{C}/\Lambda$ pour un certain réseau Λ de $\mathbb{C}$.*

(ii) Si $k = \mathbb{R}$, alors E est isomorphe à $\mathrm{S}^1 \times \mathbb{Z}/2\mathbb{Z}$ ou à S^1.

(iii) (Mordell) *Si $k = \mathbb{Q}$, alors E est un groupe abélien de type fini.*

(iv) (Hasse) *Si $k = \mathbb{Z}/p\mathbb{Z}$, alors E est un groupe abélien fini à $\leqslant 2$ générateurs, et on a $|p + 1 - |E|| < 2\sqrt{p}$.*

Les (i) et (ii) sont parfois vus dans le cours d'analyse complexe de première année. Notons que l'on en déduit par exemple $E[N] \simeq (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$ pour tout $N \geqslant 1$ dans le cas $k = \mathbb{C}$. (Que vaut $E[2]$ en général ? et $E[3]$?) Dans le cas $k = \mathbb{R}$, on est bien sûr dans le premier cas si f a 3 racines réelles, et dans le second s'il en a une seule. (Voyez-vous bien les cercles ?).

Dans le cas $k = \mathbb{Q}$, le (iii) exprime le fait remarquable que toutes les solutions de E s'expriment à partir d'un nombre fini d'entre elles par la méthode des cordes et tangentes. Nous renvoyons par exemple au livre assez élémentaire de Silverman-Tate *Rational points on elliptic curves* pour une démonstration. Pour $y^2 = x^3 + 1$ on peut par exemple montrer que l'on a $E \simeq \mathbb{Z}/6\mathbb{Z}$, avec pour générateur le point $(2, 3)$. En

8. Certains auteurs l'appellent aussi *méthode des sécantes et tangentes*.

9. Avec des connaissances élémentaires de géométrie projective on pourrait mieux comprendre l'apparition du point O et éviter la disjonction des cas (i) et (ii).

guise d'autre exemple (Billing, 1938), pour la courbe $y^2 = x^3 - 82x$ on a $E \simeq \mathbb{Z}^3$ avec pour $\mathbb{Z}$-base les points

$$P_1 = (-8, 12),\ P_2 = (-1, 9) \text{ et } P_3 = (49/4, 231/8).$$

Toujours dans le cas $k = \mathbb{Q}$, un résultat fameux (et difficile) de Mazur [10] décrit tous les cas possibles pour le groupe fini E_{tor} : ce sont les groupes cycliques $\mathbb{Z}/m\mathbb{Z}$ avec $m \leqslant 12$ et $m \neq 11$, ainsi que les groupes $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ avec $m \leqslant 4$. En revanche, on ne sait encore que peu de choses sur le rang de E. Le record, dû à Elkies, est un exemple de E dont le rang est 28. On conjecture maintenant que le rang ne prend qu'un nombre fini de valeurs possibles, alors qu'il y a quelques années on conjecturait le contraire ! Surtout, la fameuse *conjecture de Birch-Swinnerton Dyer* (une conjecture à un million de dollars) relie ce rang aux propriétés analytiques de la *fonction ζ de Hasse-Weil de E*.

L'inégalité de Hasse dans le cas particulier $y^2 = x^3 + 1$ du (iv) est le théorème principal du §1. Les courbes elliptiques sur les corps finis sont très utilisées en cryptographie.

8. Exercices

On commence par quelques exercices sur la structure des groupes abéliens finis.

Exercice 3.1. *Déterminer, à isomorphisme près, les groupes abéliens d'ordre* 2025*, et préciser dans chacun des cas leurs facteurs invariants.*

Exercice 3.2. *Déterminer tous les sous-groupes de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.*

Exercice 3.3. *Déterminer, à isomorphisme près, tous les groupes abéliens G possédant un sous-groupe H vérifiant $H \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq G/H$.*

Exercice 3.4. *Soient G un groupe abélien.*

(i) Soient $m, n \in \mathbb{Z}$ premiers entre eux. Montrer $G[mn] = G[n] \oplus G[m]$.

(ii) En déduire qu'il aurait suffit de montrer le Théorème 3.1 pour les groupes abéliens finis d'ordre une puissance d'un nombre premier.

Exercice 3.5. *Soit G un groupe abélien fini. Montrer que pour tout diviseur d de $|G|$ il existe un sous-groupe de G d'ordre d.*

Un sous-groupe H d'un groupe G est dit *caractéristique* si on a $\alpha(H) = H$ pour tout $\alpha \in \mathrm{Aut}(G)$.

Exercice 3.6. *Soient p un nombre premier, $n \geqslant 1$ et $G = (\mathbb{Z}/p\mathbb{Z})^n$.*

(i) Monter $\mathrm{Aut}(G) \simeq \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$.

(ii) En déduire les sous-groupes caractéristiques de G.

10. Mazur, Barry, *Modular curves and the Eisenstein ideal*, Publ. Math. IHÉS. 47 (1) : 33–186 (1977).

EXERCICE 3.7. *Soit G un groupe fini tel que $g^2 = 1$ pour tout $g \in G$. Montrer que G est abélien, puis $G \simeq (\mathbb{Z}/2\mathbb{Z})^n$ pour un certain entier $n \geqslant 0$.*

L'exercice suivant montre que l'on ne peut pas remplacer 2 par p premier dans l'exercice ci-dessus, ou encore que la condition *abélien* est nécessaire dans la définition des groupes abéliens p-élémentaires. Si k est un corps et $n \geqslant 1$ est un entier, on note $\mathrm{U}_n(k)$ le sous-ensemble de $\mathrm{M}_n(k)$ constitué des matrices de la forme $\mathrm{I}_n + N$ avec $N_{ij} = 0$ pour $i \geqslant j$ (autrement dit, N est triangulaire supérieure nilpotente). C'est un sous-groupe de $\mathrm{GL}_n(k)$ (justifier).

EXERCICE 3.8. *Soit p un nombre premier.*

(i) On suppose $p \geqslant n$. Montrer $g^p = 1$ pour tout $g \in \mathrm{U}_n(\mathbb{Z}/p\mathbb{Z})$.

(ii) En déduire que pour $p \geqslant 3$, il existe un groupe non abélien G d'ordre p^3 tel que $g^p = 1$ pour tout $g \in G$.

On continue par des exercices sur les groupes abéliens de type fini. On commence par un Vrai ou Faux sur les notions de familles libres et génératrices. Dans cet exercice, la notion de maximalité/minimalité est sous-entendue relativement à la relation d'inclusion.

EXERCICE 3.9. *Soit G un groupe abélien de type fini. Deux seulement des assertions suivantes sont exactes : lesquelles ? (justifier !)*

(a) *Si G est sans torsion, une famille génératrice minimale de G est libre.*

(b) *Si G est sans torsion, une famille libre maximale de G est génératrice.*

(c) *Si G est sans torsion, il existe une famille génératrice et libre de G.*

(d) *Le cardinal des familles libres de G est uniformément borné.*

(e) *Le cardinal des familles génératrices minimales de G est uniformément borné.*

(f) *Si G est fini, les familles génératrices minimales de G ont même cardinal.*

EXERCICE 3.10. *Montrer que si H est un sous-groupe distingué d'un groupe G, et si les groupes H et G/H sont de type fini, alors G est de type fini et on a*

$$\min(G) \leqslant \min(H) + \min(G/H).$$

EXERCICE 3.11. *On se propose de montrer que si G est abélien de type fini, et si H est un sous-groupe de G, alors on a $\min(H) \leqslant \min(G)$.*

(i) Traiter le cas $\min(G) = 1$.

(ii) On suppose $\min(G) > 1$. Montrer que l'on peut trouver $g \in G$ tel que $\min(G') < \min(G)$, où l'on a posé $G' = G/\langle g \rangle$.

(iii) Conclure en considérant le morphisme $H \to G'$, $h \mapsto h\langle g \rangle$.

(iv) (Application) En déduire une démonstration du fait qu'un sous-groupe de $\mathbb{Z}^n$ est isomorphe à $\mathbb{Z}^m$ pour $m \leqslant n$.

L'exercice suivant montre que l'hypothèse « G est abélien » dans l'exercice ci-dessus est nécessaire.

Exercice 3.12. *Montrer que le sous-groupe de* $\mathrm{GL}_2(\mathbb{Q})$ *engendré par* $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$ *et* $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ *possède un sous-groupe (abélien) qui n'est pas de type fini.*

On peut montrer qu'un sous-groupe H *d'indice fini* d'un groupe de type fini G est encore de type fini (Schreier), mais il n'est pas vrai en général qu'on a $\min(H) \leqslant \min(G)$ si G n'est pas abélien :

Exercice 3.13. *Donner un exemple de groupe fini* G *avec* $\min(G) = 2$*, ayant un sous-groupe abélien* H *avec* $\min(H) = 3$.

On donne maintenant quelques exercices sur les caractères.

Exercice 3.14. *(i) Montrer* $\mathrm{H}_8/\langle -1\rangle \simeq \mu_2 \times \mu_2$.

(ii) En déduire les caractères de H_8.

(iii) Donner un exemple de caractère d'un sous-groupe de H_8 *qui ne se prolonge pas à* H_8.

Exercice 3.15. *Soient* V *un* $\mathbb{C}$*-espace vectoriel de dimension finie et* G *un sous-groupe abélien fini de* $\mathrm{GL}(V)$*. Pour tout* $\chi \in \widehat{G}$ *on pose*

$$V_\chi = \{v \in V \mid g(v) = \chi(g)v \ \forall g \in G\}.$$

(i) Montrer que V_χ *est un sous-espace vectoriel de* V.

(ii) Montrer $V = \bigoplus_{\chi \in \widehat{G}} V_\chi$.

Exercice 3.16. *(i) Montrer que si* G_1 *et* G_2 *sont deux groupes, on a un isomorphisme naturel* $\widehat{G_1 \times G_2} \xrightarrow{\sim} \widehat{G_1} \times \widehat{G_2}$.

(ii) En déduire que si G *est un groupe abélien fini, alors* $\widehat{G}$ *est isomorphe à* G.

Le (i) de l'exercice qui suit montre qu'un groupe abélien fini est canoniquement isomorphe à son bidual.

Exercice 3.17. (Bidualité) *Soit* G *un groupe abélien fini.*

(i) Montrer que l'application $\iota_G : G \to \widehat{\widehat{G}},\ g \mapsto (\chi \mapsto \chi(g))$*, est un morphisme injectif, puis bijectif.*

(ii) Énoncer les relations d'orthogonalité des caractères pour $\widehat{G}$ *en terme de l'isomorphisme du (i).*

Dans la série d'exercices suivants, on répond à la question suivante : est-ce qu'un groupe abélien fini G est *naturellement* isomorphe à son dual $\widehat{G}$? Bien entendu, il s'agira entre autres de préciser ce qu'on entend par « naturellement ».

Exercice 3.18. *(Groupes abéliens finis naturellement isomorphes à leur dual I)*

(i) Soit G *un groupe abélien isomorphe à* $(\mathbb{Z}/2\mathbb{Z})^2$ *(mais on ne fixe pas de tel isomorphisme). Construire un isomorphisme* $G \to \widehat{G}$ *qui vous semble naturel.*

On suppose désormais G *cyclique d'ordre* n*. Pour tout générateur* g *de* G*, on note* $\chi_g \in \widehat{G}$ *l'unique caractère vérifiant* $\chi_g(g) = e^{2i\pi/n}$ *(justifier).*

(ii) Supposons qu'il existe $\varphi \in \mathrm{Hom}(G, \widehat{G})$ *avec* $\varphi(g) = \chi_g$ *pour tout générateur* g *de* G*. Montrer que* φ *est unique et que l'on a* $k^2 \equiv 1 \bmod n$ *pour tout* $k \in (\mathbb{Z}/n\mathbb{Z})^\times$*.*

(iii) (suite) En déduire que l'entier n *divise* 24*.*

(iv) Réciproquement, montrer que si n *divise* 24*, il existe un isomorphisme* $G \to \widehat{G}$ *envoyant tout générateur* g *de* G *sur* χ_g*.*

Exercice 3.19. *(Dualité et formes bilinéaires) Soit* $(G, +)$ *un groupe abélien. On note* $\mathrm{Bil}(G)$ *l'ensemble des applications* $b : G \times G \to \mathbb{C}^\times$ *qui vérifient*

$$b(g + g', h) = b(g, h)b(g', h) \quad \text{et} \quad b(h, g + g') = b(h, g)b(h, g'), \quad \forall g, g', h \in G.$$

On dira qu'une telle application est bilinéaire*. Pour tout morphisme* $f \in \mathrm{Hom}(G, \widehat{G})$*, on définit* $\mathrm{b}_f : G \times G \to \mathbb{C}^\times$ *par* $\mathrm{b}_f(g, g') = f(g)(g')$*.*

(i) Montrer que $f \mapsto \mathrm{b}_f$ *est une bijection* $\mathrm{Hom}(G, \widehat{G}) \to \mathrm{Bil}(G)$*.*

Une application bilinéaire $b : G \times G \to \mathbb{C}^\times$ *est dite non dégénérée à droite (resp. à gauche) si l'unique élément* $g \in G$ *tel que* $b(h, g) = 1$ *(resp.* $b(g, h) = 1$*) pour tout* $h \in G$ *est* $g = 1$*.*

(ii) Soit $f \in \mathrm{Hom}(G, \widehat{G})$*. Montrer qu'il y a équivalence entre : (a)* f *est un isomorphisme, (b)* b_f *est non dégénérée à droite, (c)* b_f *est non dégénérée à gauche.*

Pour tout morphisme de groupes $\alpha : G \to G'$, on dispose d'un morphisme évident $\widehat{\alpha} : \widehat{G'} \to \widehat{G}, \chi \mapsto \chi \circ \alpha$ (noter l'échange de G et G'). On dira qu'un isomorphisme $f : G \to \widehat{G}$ est *naturel* si pour tout $\alpha \in \mathrm{Aut}(G)$ on a $f \circ \alpha = \widehat{\alpha}^{-1} \circ f$. Si un tel isomorphisme f existe on dira alors que G est *naturellement isomorphe à son dual.*

Exercice 3.20. *(Groupes abéliens finis naturellement isomorphes à leur dual II) On se propose de démontrer qu'un groupe abélien fini* G *est* naturellement isomorphe à son dual *(au sens ci-dessus) si, et seulement si, soit* $|G|$ *divise* 12*, soit* $G \simeq \mathbb{Z}/24\mathbb{Z}$*.*

(i) Vérifier qu'un isomorphisme $f : G \to \widehat{G}$ *est* naturel *si, et seulement si, pour tout* $\alpha \in \mathrm{Aut}(G)$ *et tout* $g, h \in G$*, on a* $\mathrm{b}_f(\alpha(g), \alpha(h)) = \mathrm{b}_f(g, h)$*.*

(ii) Montrer que les isomorphismes $f : G \to \widehat{G}$ *construits dans l'Exercice 3.19 (i) et (iv) sont bien* naturels *et expliciter* b_f *dans les deux cas.*

(iii) Montrer que si G *est* naturellement isomorphe à son dual*, alors l'exposant de* G *divise* 24*.*

(iv) Soit G *un groupe abélien d'ordre* mn *avec* $(m, n) = 1$*. Montrer que* G *est* naturellement isomorphe à son dual *si, et seulement si,* $G[m]$ *et* $G[n]$ *le sont.*

Soit $b : G \times G \to \mathbb{C}^\times$ *bilinéaire vérifiant* $b(\alpha(g), \alpha(h)) = b(g, h)$ *pour tout* g, h *dans* G*, et tout* $\alpha \in \mathrm{Aut}(G)$*. On suppose* $G = C_1 \oplus C_2 \oplus \cdots \oplus C_n$ *avec* $n \geqslant 2$*,* C_i *cyclique d'ordre* e_i*, disons engendré par l'élément* $x_i \in C_i$*, et enfin* $e_1 \,|\, e_2 \,|\, \ldots \,|\, e_n$*.*

(v) Montrer $f(x_i, x_j) = \pm 1$ *pour* $i \neq j$*.*

(vi) Montrer $f(x_i, x_j) = 1$ *pour tout* $1 \leqslant i, j < n$*.*

(vii) On suppose $e_1 = 2$ *(et donc* e_n *pair). Montrer* $f(x_n, y) = 1$ *avec* $y = x_n^{e_n/2}$*.*

On suppose désormais b non dégénérée (voir l'Exercice 3.19).

(viii) Montrer $e_n \mid 24$.

(ix) Montrer $e_i = 2$ pour $i < n$, $n = 2$, puis $e_n \not\equiv 0 \bmod 4$.

(x) Conclure.

On poursuit par quelques exercices sur les groupes abéliens généraux.

Exercice 3.21. *Soit G un groupe abélien.*

(i) Montrer que l'application $G \to (\mathbb{C}^\times)^{\widehat{G}}, g \mapsto (\chi(g))_\chi$, est injective.

(ii) En déduire que G se plonge dans un groupe divisible (de manière naturelle !).

Exercice 3.22. *Soit G un groupe abélien supposé divisible et sans torsion.*

(i) Montrer qu'il existe un ensemble I tel que G est isomorphe à $\mathbb{Q}^{(I)}$.

(ii) (suite) On suppose G indénombrable. Montrer $I \sim G$.

Exercice 3.23. *Soit A le groupe abélien $\prod_p \mathbb{Z}/p\mathbb{Z}$, le produit portant sur tous les nombres premiers p. On va montrer qu'il existe un morphisme surjectif $A \to \mathbb{Q}$,*

(i) Déterminer A_{tor}.

(ii) Montrer que A/A_{tor} est divisible.

(iii) Conclure.

(iv) Montrer qu'on a en fait $A/A_{\mathrm{tor}} \simeq \mathbb{Q}^{(\mathbb{R})}$.

Exercice 3.24. *Soit G le sous-groupe additif de $\mathbb{Q}$ engendré par tous les $1/p$ avec p premier.*

(i) Vérifier que G est l'ensemble des rationnels de la forme a/b avec $a \in \mathbb{Z}$ et $b \in \mathbb{N}_{>0}$ sans facteur carré, puis que G n'est pas de type fini.

(ii) Montrer que tout morphisme $G \to G$ est de la forme $x \mapsto nx$ avec $n \in \mathbb{Z}$.

(iii) En déduire $\operatorname{Aut} G \simeq \mathbb{Z}/2\mathbb{Z}$.

Exercice 3.25. (Le groupe des entiers p-adiques) *Soit p un nombre premier. On note $\mathbb{Z}_p$ le sous-ensemble du produit $\prod_{n\geqslant 1} \mathbb{Z}/p^n\mathbb{Z}$ constitué des suites (x_n) telles que $x_{n+1} \bmod p^n = x_n$ pour tout $n \geqslant 1$. Une telle suite est appelée* entier p-adique.

(i) Montrer que $\mathbb{Z}_p$ est un sous-groupe du groupe produit $\prod_{n\geqslant 1} \mathbb{Z}/p^n\mathbb{Z}$, et que l'application $\mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}, (x_n) \mapsto x_n$, est un morphisme surjectif.

(ii) Montrer que $\mathbb{Z}_p$ est en bijection avec $\mathbb{R}$.

(iii) Montrer que $\mathbb{Z}_p$ n'a aucun élément non trivial d'ordre fini.

On note $\mu_{p^\infty} = \cup_{n\geqslant 1} \mu_{p^n}$ le sous-groupe de $\mathbb{C}^\times$ constitué des racines de l'unité d'ordre une puissance de p.

(iv) Montrer que pour tout caractère $\chi \in \widehat{\mu_{p^\infty}}$ il existe un unique entier p-adique $(\overline{k_n}) \in \mathbb{Z}_p$ vérifiant $\chi(e^{2i\pi/p^n}) = e^{2i\pi k_n/p^n}$ pour tout $n \geqslant 1$.

(v) Montrer $\widehat{\mu_{p^\infty}} \simeq \mathbb{Z}_p$.

EXERCICE 3.26. (Propriété universelle des sommes directes de groupes abéliens) *Soient* $\{G_i\}_{i\in I}$ *une famille de groupes abéliens, et* $S = \oplus_{i\in I} G_i$ *leur somme directe externe. Pour* $j \in I$*, on note* $\iota_j \in \mathrm{Hom}(G_j, S)$ *l'inclusion canonique (justifier). Montrer que pour tout groupe abélien* G*, l'application* $\mathrm{Hom}(S, G) \to \prod_{i\in I} \mathrm{Hom}(G_i, G)$*,* $f \mapsto (f \circ \iota_i)_i$*, est bijective.*

On donne maintenant quelques exercices concernant la Section 1.

EXERCICE 3.27. (Coniques sur $\mathbb{Z}/p\mathbb{Z}$) *Soit* p *un nombre premier impair.*

(i) Montrer $\mathrm{J}(\chi, \chi^{-1}) = -\chi(-1)$ *pour tout* $\chi \in \widehat{(\mathbb{Z}/p\mathbb{Z})}^\times \smallsetminus \{1\}$.

(ii) En déduire[11] *que si l'on pose* $C = \{(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2 \mid \alpha\, x^2 + \beta\, y^2 = 1\}$ *avec* $\alpha, \beta \in (\mathbb{Z}/p\mathbb{Z})^\times$*, on a l'égalité* $|C| = p - (\frac{-\alpha\beta}{p})$.

(iii) Montrer qu'il existe $\frac{p\pm1}{4}$ *carrés* $x \in \mathbb{Z}/p\mathbb{Z}$ *tels que* $x + 1$ *n'est pas un carré.*

EXERCICE 3.28. *En examinant la Table 1, on constate pour* $p \equiv 1 \bmod 3$ *:*

(i) $|\mathrm{S}_p| \equiv -1 \bmod 12$,

(ii) $|\mathrm{S}_p| \equiv -1 \bmod 24 \;\Rightarrow\; p \equiv 1 \bmod 4$.

Démontrer ces congruences.

EXERCICE 3.29. *Soit* p *un nombre premier impair.*

(i) Déterminer $\sum_{x\in\mathbb{Z}/p\mathbb{Z}} (\frac{x^2+1}{p})$.

(ii) Déterminer $\sum_{x\in\mathbb{Z}/p\mathbb{Z}} (\frac{x^3+1}{p})$.

(iii) Soient $n \geqslant 1$ *un entier et* $m = \mathrm{pgcd}\,(p-1, n)$*. Montrer*

$$\Big|\sum_{x\in\mathbb{Z}/p\mathbb{Z}} (\frac{x^n+1}{p})\Big| \leqslant \begin{cases} (m-1)\sqrt{p} & \text{pour } m \text{ impair,} \\ (m-2)\sqrt{p}+1 & \text{pour } m \text{ pair.} \end{cases}$$

EXERCICE 3.30. (Somme de Gauss cubique) *Soient* p *premier* $\equiv 1 \bmod 3$*,* c *un caractère d'ordre* 3 *de* $(\mathbb{Z}/p\mathbb{Z})^\times$*,* $G = \mathrm{G}(c)$ *la somme de Gauss associée et* $J = \mathrm{J}(c, c)$.

(i) Montrer $G^3 = J\,p$.

(ii) Soit $A = J + \overline{J}$*. Montrer* $A \in \mathbb{Z}$ *et qu'il existe* $B \in \mathbb{Z}$ *avec* $4p = A^2 + 3B^2$.

(iii) Soit $x = \sum_{k=0}^{p-1} \cos(\frac{2\pi k^3}{p})$*. Montrer* $x = G + \overline{G}$.

(iv) (suite) En déduire que x *est l'une des trois racines réelles du polynôme à coefficients entiers* $X^3 - 3pX - Ap$.

EXERCICE 3.31. (Un théorème de Gauss) *Soit* p *un nombre premier. On considère*

$$\mathrm{T}_p = \{(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2 \mid x^4 + y^2 = 1\}.$$

(i) En utilisant l'Exercice 3.27 (ii), montrer $|\mathrm{T}_p| = p + 1$ *pour* $p \equiv 3 \bmod 4$.

11. Une autre démonstration consisterait à dire qu'il y a $\frac{p+1}{2}$ carrés dans $\mathbb{Z}/p\mathbb{Z}$, et donc aussi $\frac{p+1}{2}$ éléments de la forme $\beta^{-1}(1 - \alpha x^2)$, de sorte qu'il y a au moins un point P sur la conique C. Les autres points sont obtenus en paramétrant les cordes (ou tangente) de C passant par P.

On suppose désormais $p \equiv 1 \bmod 4$.

(ii) Montrer $|\mathrm{T}_p| \equiv 6 \bmod 8$.

(iii) Montrer qu'il existe des uniques $A, B \in \mathbb{Z}$ *avec* $A \equiv -\frac{p+1}{2} \bmod 4$ *et* $B > 0$ *tels que* $p = A^2 + 4B^2$, *et que l'on a en outre* $|\mathrm{T}_p| = p + 2A - 1$.

Exercice 3.32. (Le signe de la somme de Gauss, d'après Dirichlet) *Soient* $N \geqslant 1$ *et* $\mathrm{G}_N = \sum_{a=0}^{N-1} e^{\frac{2i\pi a^2}{N}}$.

(i) Soient $a < b$ *deux entiers et* $f : [a, b] \to \mathbb{C}$ *une fonction continue et* $\mathscr{C}^1$ *par morceaux. Montrer* $\frac{f(a)+f(b)}{2} + \sum_{k=a+1}^{b-1} f(k) = \sum_{n\in\mathbb{Z}} \int_a^b f(t)e^{2i\pi nt}dt$.

(ii) En déduire $\mathrm{G}_N = (1 + i^{-N})N^{\frac{1}{2}}I$ *où* $I = \int_{-\infty}^{+\infty} e^{2i\pi t^2}dt$.

(iii) Montrer $I = \frac{1+i}{2}$ *(intégrale de Gauss) et*

$$\mathrm{G}_N = \begin{cases} (1+i)N^{\frac{1}{2}} & \text{si } N \equiv 0 \bmod 4, \\ N^{\frac{1}{2}} & \text{si } N \equiv 1 \bmod 4, \\ 0 & \text{si } N \equiv 2 \bmod 4, \\ iN^{\frac{1}{2}} & \text{si } N \equiv 3 \bmod 4. \end{cases}$$

Dans l'exercice suivant, on utilise le résultat ci-dessus pour démontrer, suivant Gauss, la *loi de réciprocité quadratique.*

Exercice 3.33. *Pour* $N, M \geqslant 1$, *on pose* $\mathrm{G}_{N,M} = \sum_{k=0}^{N-1} e^{\frac{2i\pi Mk^2}{N}}$ *et* $\mathrm{G}_N = \mathrm{G}_{N,1}$. *On se donne* p *et* q *deux nombres premiers impairs distincts.*

(i) Montrer $\mathrm{G}_{p,q}\,\mathrm{G}_{q,p} = \mathrm{G}_{pq}$.

(ii) Montrer $\mathrm{G}_{p,a} = \left(\frac{a}{p}\right)\mathrm{G}_p$ *pour tout* $a \in \mathbb{Z}$.

(iii) En déduire $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{(p-1)(q-1)}{2}}$ *(« la loi de réciprocité quadratique »).*

(iv) Montrer $\mathrm{G}_{p,8}\,\mathrm{G}_{8,p} = \mathrm{G}_{8p}$ *et vérifier* $\mathrm{G}_{8,p} = 4\,e^{\frac{2i\pi\,p}{8}}$.

(v) En déduire $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ *(« loi complémentaire »).*

La série d'exercices suivante revient sur l'analyse de Fourier sur un groupe abélien fini. Le premier fait notamment suite à l'Exercice 3.17. Le dernier donne un point de vue plus éclairant sur certains calculs de la section 1 (dans l'esprit de l'Exemple 2.4).

Exercice 3.34. (Inversion de Fourier)

(i) Vérifier que l'application $\mathrm{j}_G : \mathrm{L}^2(G) \to \mathrm{L}^2(\widehat{\widehat{G}}), f \mapsto (x \mapsto f(\iota_G^{-1}(x^{-1})))$, *est* $\mathbb{C}$*-linéaire bijective.*

(ii) Soit $\mathscr{F}_G : \mathrm{L}^2(G) \to \mathrm{L}^2(\widehat{G}), f \mapsto \frac{1}{\sqrt{|G|}}\widehat{f}$. *Montrer* $\mathscr{F}_{\widehat{G}} \circ \mathscr{F}_G = \mathrm{j}_G$.

Exercice 3.35. (Convolution) *Soit* G *un groupe fini. Le produit de convolution de* $f, f' \in \mathrm{L}^2(G)$ *est défini par* $f \star f'(g) = \sum f(a)f'(b)$, *la somme portant sur tous les couples* $(a, b) \in G \times G$ *tels que* $ab = g$.

(i) Montrer que $(\mathrm{L}^2(G), +, \star)$ *est un anneau, de neutre le dirac en* 1.

(ii) Soient $\chi \in \widehat{G}$ *et* $f \in \mathrm{L}^2(G)$. *Vérifier* $f \star \chi = \widehat{f}(\chi)\,\chi$.

(iii) En déduire $\widehat{f \star f'}(\chi) = \widehat{f}(\chi)\,\widehat{f'}(\chi)$*, pour tout* $f, f' \in \mathrm{L}^2(G)$ *et* $\chi \in \widehat{G}$*.*

L'exercice suivant fait suite au précédent (cas $G = \mathbb{Z}/p\mathbb{Z}$) et donne un point de vue plus conceptuel sur certaines des formules démontrées en Section 1. Comme dans cette section, on étend tout caractère c de $(\mathbb{Z}/p\mathbb{Z})^\times$ en une fonction $\mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ en posant $c(0) = 0$ pour $c \neq 1$, et $c(0) = 1$ pour $c = 1$.

Exercice 3.36. (Convolution et sommes de Gauss et de Jacobi) *Soit* p *un nombre premier. On identifie* μ_p *à* $\widehat{\mathbb{Z}/p\mathbb{Z}}$ *comme dans la Proposition 1.3, en faisant correspondre à* $\zeta \in \mu_p$ *le caractère* $\overline{k} \mapsto \zeta^k$ *de* $\mathbb{Z}/p\mathbb{Z}$*. Soient* $c, c' \in (\widehat{\mathbb{Z}/p\mathbb{Z}})^\times$*.*

(i) Vérifier que pour tout $\zeta \in \mu_p$ *on a* $\widehat{c}(\zeta) = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} c(x)\zeta^{-x}$*.*

(ii) Si $cc' \neq 1$*, montrer* $c * c' = \mathrm{J}(c, c')cc'$ *et retrouver* $\mathrm{G}(c)\mathrm{G}(c') = \mathrm{J}(c, c')\mathrm{G}(cc')$*.*

(iii) On suppose $c \neq 1$*. En utilisant l'Exercice 3.27 (i), montrer que l'on a la relation* $c * c^{-1} = -c(-1) + p\,c(-1)\delta$*, où* δ *désigne le Dirac en* 0*.*

(iv) (suite) Retrouver $|\mathrm{G}(c)|^2 = p$*.*

Chapitre 4

Le groupe symétrique et son dévissage

Le but de ce chapitre est d'étudier la structure du groupe symétrique S_n. Ce dernier agit naturellement sur $\{1, \ldots, n\}$ mais aussi sur tout un tas d'autres ensembles naturels. Cela nous conduit naturellement à discuter d'abord la notion d'action de groupe, qui de toutes façons est l'une des notions essentielles de ce cours. Au passage, en guise de première illustration de l'action de conjuguaison, nous démontrons le premier théorème de Sylow, mais nous reportons à plus tard les autres applications dans le même esprit à la structure des groupes finis.

Nous étudions ensuite S_n de manière systématique (systèmes de générateurs, classes de conjugaison), ainsi que son groupe alterné A_n. Les cas des petites valeurs de n est à la fois irrégulier et intéressant. C'est pourquoi nous dévisserons d'abord concrètement S_n pour $n \leqslant 4$, puis étudierons l'action *exotique* de S_5 sur 6 éléments. Nous introduirons ensuite le langage des suites exactes, agréable pour décrire les dévissages. Nous dévisserons ensuite S_n pour $n \geqslant 5$. Un énoncé crucial, connu de Galois, est la simplicité du groupe non abélien A_n.

Ces dévissages seront l'occasion d'introduire certains concepts importants, comme les notions de *commutateurs*, *groupes dérivés* et *résolubilité*. Le groupe S_n est résoluble si, et seulement si, on a $n \leqslant 4$, un énoncé particulièrement significatif en théorie de Galois, brièvement discutée dans un complément culturel. Nous expliquerons enfin la notion de *produit semi-direct*, que nous appliquerons ici aux structures de S_3 et S_4, ainsi qu'à la classification de groupes de petit ordre.

Nous terminerons par deux autres compléments importants : l'un sur la notion de filtration, avec notamment une démonstration du théorème de Jordan-Hölder et la détermination des facteurs de Jordan-Hölder de S_n, et l'autre sur la classification par Galois des sous-groupes résolubles et transitifs de S_p avec p premier.

1. Actions de groupes

1.1. Définition. Dans cette partie, on fixe un groupe G et un ensemble X.

Définition 1.1. *Une action de G sur X est une application*

$$\bullet : G \times X \to X, \ \ (g, x) \mapsto g \bullet x,$$

vérifiant $1 \bullet x = x$ et $g \bullet (h \bullet x) = (gh) \bullet x$ pour tout $x \in X$ et tout $g, h \in G$.

On notera en général simplement $g.x$ ou gx au lieu de $g \bullet x$. Un ensemble muni d'une action de G est aussi appelé G-ensemble. La plupart des groupes rencontrés agissent naturellement sur quelque chose !

Exemple 1.2. *(i) L'exemple canonique d'action est celle du groupe symétrique S_X sur X définie par $\mathrm{S}_X \times X \to X$, $(\sigma, x) \mapsto \sigma(x)$. Le groupe S_X agit aussi naturellement $\mathrm{P}(X)$ via $(\sigma, A) \mapsto \sigma(A)$, sur l'ensemble produit*

$X \times X$ via $(\sigma, (x, y)) \mapsto (\sigma(x), \sigma(y))$, sur l'ensemble des partitions de X via $(\sigma, \{P_i\}_{i \in I}) \mapsto \{\sigma(P_i)\}_{i \in I}$, etc...

(iii) Si V est un k-espace vectoriel, alors $\mathrm{GL}(V)$ agit naturellement sur V, sur l'ensemble $\mathbb{P}(V)$ des droites de V, sur l'ensemble des plans de V, etc..

(iv) Noter que si G agit sur X, il agit aussi naturellement sur tout sous-ensemble $Y \subset X$ qui est stable, i.e. tel que $gY \subset Y$ pour tout $g \in G$.

(v) Si G agit sur X, et si $f : H \to G$ est un morphisme de groupes, alors $H \times X \to X, (h, x) \mapsto f(h)x$, est une action de H sur X, dite déduite de celle de G par restriction selon f.

En particulier, tout morphisme $f : G \to \mathrm{S}_X$ définit par (i) et (v), *i.e.* $(g, x) \mapsto f(g)(x)$, une action de G sur X. Nous allons voir que toute action de G sur X s'obtient ainsi. En effet, fixons une action $\bullet$ de G sur X, et pour $g \in G$, regardons

$$\mathrm{m}_g : X \to X, x \mapsto g \bullet x$$

(la *translation par g* associée à $\bullet$). Par hypothèse, on a $\mathrm{m}_1 = \mathrm{id}_X$, et $\mathrm{m}_g \circ \mathrm{m}_h = \mathrm{m}_{gh}$. Ainsi, m_g est inversible d'inverse $\mathrm{m}_{g^{-1}}$, et l'application $\mathrm{m}^\bullet : G \to \mathrm{S}_X, g \mapsto \mathrm{m}_g$, est un morphisme de groupes, appelé *morphisme associé à l'action* $\bullet$. Les deux constructions ci-dessus étant clairement inverses l'une de l'autre, on a montré :

Scholie 1.3. (*Propriété universelle de S_X*) *L'application $\bullet \mapsto \mathrm{m}^\bullet$ induit une bijection de l'ensemble des actions de G sur X sur celui des morphismes $G \to \mathrm{S}_X$.*

On passera en général d'un point de vue à l'autre sans commentaire.

Exemple 1.4. *(i) Se donner une action de G sur $\{1, \ldots, n\}$ est la même chose que se donner un morphisme $G \to \mathrm{S}_n$.*

(ii) (Action de Cayley) *La multiplication de G définit une action de G sur lui-même, et correspond au morphisme $G \to \mathrm{S}_G$ de Cayley.*

(iii) (Action triviale) *Tout groupe G agit trivialement sur tout ensemble X en posant $g.x = x$ pour tout $g \in G$ et tout $x \in X$. C'est l'action correspondant au morphisme triviale $G \to \mathrm{S}_X$, $g \mapsto 1$. Cette action est moins inutile*[1] *qu'elle n'en a l'air !*

Remarque 1.5. *(Action à droite)* La notion d'action donnée ici est appelée parfois *action à gauche* de G sur X. La notion concurrente est celle d'*action à droite*, qui est une application $X \times G \to X, (x, g) \mapsto xg$ vérifiant $x1 = x$ et $(xg)h = x(gh)$ pour tout $x \in X$ et tout $g, h \in G$. En fait, si G agit à droite sur X, il y agit aussi à gauche par la formule $(g, x) \mapsto xg^{-1}$, (et réciproquement !) de sorte que la théorie des actions à droite se déduit de celle des actions à gauche. Pour cette raison, on ne considèrera que des actions à gauche dans ce cours.

1.2. Orbites et stabilisateurs.

Définition 1.6. *Soient G un groupe agissant sur l'ensemble X et $x \in X$.*

(i) Le sous-ensemble $\mathrm{O}_x = \{gx \mid g \in G\} \subset X$ est appelé orbite *de x sous (l'action de) G.*

1. L'intérêt typique d'une telle notion est que l'on peut avoir à démontrer qu'une action donnée est l'action triviale.

(ii) Le sous-groupe $G_x = \{g \in G \mid gx = x\}$ *de* G *est appelé* stabilisateur *de* x *(ou* groupe d'isotropie *de* x*). On le note aussi* $\mathrm{Stab}_G(x)$.

Dans le (ii) ci-dessus, le fait que G_x est un sous-groupe de G est immédiat.

EXEMPLE 1.7. *(i) Soit* E *un plan euclidien et* $G = \mathrm{O}(E)$ *son groupe orthogonal. L'action naturelle de* G *sur* E *a pour orbites le cercles centrés en l'origine* O*. Le stabilisateur d'un point* $P \neq 0$ *est le groupe d'ordre* 2 *engendré par la symétrie axiale d'axe* (OP).

(ii) Si k *est un corps, le groupe* $\mathrm{GL}_n(k)$ *agit par conjugaison sur* $\mathrm{M}_n(k)$*, via* $(g, M) \mapsto gMg^{-1}$*. L'orbite d'une matrice* $M \in \mathrm{M}_n(k)$ *est sa classe de conjugaison/de similitude, le stabilisateur de* M *est son commutant dans* $\mathrm{GL}_n(k)$.

La propriété suivante est élémentaire mais importante (*principe de conjugaison*) :

LEMME 1.8. *Soient* G *agissant sur* X*,* $x \in X$ *et* $g \in G$*. On a* $G_{gx} = gG_xg^{-1}$.

DÉMONSTRATION — En effet, pour tout $h \in G$ on a

$$h \in G_{gx} \iff hgx = gx \iff g^{-1}hgx = x \iff g^{-1}hg \in G_x \iff h \in gG_xg^{-1}.$$

□

Soit G agissant sur X. À cette action est associée la relation R sur X définie par

$$y\,R\,x \iff \exists g \in G,\ y = gx.$$

C'est une relation d'équivalence. En effet, on a $x = 1x$ (reflexivité), $y = gx \Leftrightarrow x = g^{-1}y$ (symétrie), et enfin $y = gx$ et $z = hy$ entraînent $z = ghx$ (transitivité). La classe d'équivalence d'un point $x \in X$ est son orbite O_x. L'ensemble quotient X/R, sous-ensemble de $\mathrm{P}(X)$ constitué des orbites sous G, est parfois noté $G\backslash X$. Les classes d'équivalence formant une partition de X on a montré :

PROPOSITION 1.9. *Si* G *agit sur* X*, les orbites forment une partition de* X.

EXEMPLE 1.10. Se donner une action de $\mathbb{Z}$ sur X est la même chose que se donner une bijection de X. En effet, se donner un morphisme $\mathbb{Z} \to \mathrm{S}_X$ revient à se donner l'image de 1, un élément *a priori* quelconque de S_X. De même, se donner une action de $\mathbb{Z}/n\mathbb{Z}$ sur X est la même chose que se donner $\sigma \in \mathrm{S}_X$ tel que $\sigma^n = \mathrm{id}_X$. La relation ci-dessus, dans le cas de ces actions, n'est autre que la relation d'équivalence de l'Exemple 1.8 Chap. 1.

Un des énoncés les plus importants sur les actions de groupes est le suivant.

PROPOSITION 1.11. (Formule orbite-stabilisateur) *Soit* G *un groupe agissant sur l'ensemble* X*, et soit* $x \in X$*. On a une bijection* $G/G_x \xrightarrow{\sim} \mathrm{O}_x$ *envoyant* gG_x *sur* gx *pour tout* $g \in G$*. En particulier, si* G *est fini on a* $|G| = |G_x||\mathrm{O}_x|$.

DÉMONSTRATION — Soi $\pi : G \to \mathrm{O}_x, g \mapsto gx$. Par définition, π est surjective et on a

$$\pi(g') = \pi(g) \iff g'x = gx \iff g^{-1}g' \in G_x \iff g' \sim_{G_x} g.$$

Cela montre que π passe au quotient G/G_x, et aussi que l'application induite $\overline{\pi} : G/G_x \to \mathrm{O}_x, gG_x \mapsto gx$, est injective, donc bijective. Le dernier point résulte de $|G/G_x| = |G|/|G_x|$ (Lagrange). □

Corollaire 1.12. (Équation aux classes) *On suppose X et G finis, et se donne $x_1, \ldots, x_n \in X$ des représentants des orbites sous G. On a*

$$|X| = \sum_{i=1}^{n} |\mathrm{O}_{x_i}| = \sum_{i=1}^{n} |G|/|G_{x_i}|.$$

1.3. Un exemple : l'action de conjugaison. Nous verrons de nombreux exemples concrets d'actions de groupes par la suite. L'exemple suivant est aussi général qu'important.

Exemple 1.13. (*Action de conjugaison*) Soit G un groupe. L'application $G \times G \to G, (g, x) \mapsto gxg^{-1}$ est manifestement une action de G sur lui-même appelée *action de conjugaison*. Pour cette action, l'orbite d'un élément $x \in G$ est appelée *classe de conjugaison* de x, et notée $\mathrm{Conj}(x) = \{gxg^{-1} \mid g \in G\}$. De plus, le stabilisateur de x est appelé *centralisateur* ou *commutant* de x, et il est noté $\mathrm{C}_G(x) = \{g \in G \mid gx = xg\}$. On a $\langle x \rangle \subset \mathrm{C}_G(x)$ (inclusion stricte en générale).

Donnons-en ici une application typique. Notons que pour $x \in G$, on a $|\mathrm{Conj}(x)| = 1$ si, et seulement si, $x \in \mathrm{Z}(G)$. Supposons G fini et choisissons $x_1, \ldots, x_n \in G \smallsetminus \mathrm{Z}(G)$ des représentants des classes de conjugaison non triviales de G. On a alors

$$|G| = |\mathrm{Z}(G)| + \sum_{i=1}^{n} |\mathrm{Conj}(x_i)|, \text{ avec } |\mathrm{Conj}(x_i)|\,|\mathrm{C}_G(x_i)| = |G|, \tag{20}$$

d'après l'équation aux classes. Cette égalité permet par exemple de montrer le :

Théorème 1.14. (Premier théorème de Sylow) *Soit G un groupe fini d'ordre $p^n m$ avec p premier ne divisant pas m. Alors G possède un sous-groupe d'ordre p^n.*

Un tel sous-groupe s'appelle un p-Sylow de G.

Démonstration — On raisonne par récurrence sur $|G|$. Supposons qu'il existe $x \in G \smallsetminus \mathrm{Z}(G)$ tel que $|\mathrm{Conj}(x)|$ est premier à p. Dans ce cas $H = \mathrm{C}_G(x)$ est un sous-groupe de G d'indice premier à p, donc de la forme $p^n m'$ avec $m' | m$ et $m' < m$ (Lagrange). Par hypothèse de récurrence, H a un sous-groupe d'ordre p^n, ainsi donc que G. On peut donc supposer $p \mid |\mathrm{Conj}(x)|$ pour tout $x \in G \smallsetminus \mathrm{Z}(G)$. Par l'équation aux classes (20) on a alors $p \mid |\mathrm{Z}(G)|$. Choisissons $x \in \mathrm{Z}(G)$ d'ordre p (par exemple par Cauchy, mais c'est plus élémentaire ici car G est abélien). Alors $H = \langle x \rangle$ est d'ordre p et distingué dans G. Par hypothèse de récurrence, le groupe quotient G/H a un sous-groupe d'ordre p^{n-1}. Il est donc de la forme P/H, avec P sous-groupe de G contenant H, et on a $|P| = |P/H||H| = p^n$. □

Nous poursuivrons ce type d'applications théoriques à la structure générale des groupes finis au Chapitre 6.

1.4. Vocabulaire : actions transitives, fidèles et libres.

Définition 1.15. *Une action de G sur X est dite* transitive *si on a $X \neq \varnothing$ et si pour tout $x, y \in X$ il existe $g \in G$ tel que $y = gx$. Il est équivalent de demander qu'il existe $x \in X$ avec $X = \mathrm{O}_x$.*

Exemple 1.16. (i) Pour tout $1 \leqslant k \leqslant n$, l'action naturelle de S_n sur l'ensemble des parties à k éléments de $\{1, \ldots, n\}$ est transitive.

(ii) L'action naturelle de $\mathrm{GL}(V)$ sur V n'est pas transitive pour $V \neq \{0\}$. Elle a exactement deux orbites : celle de 0 et celle d'un vecteur non nul quelconque.

Un exemple aussi important que général d'action transitive est le suivant.

Exemple 1.17. *(Action par translations de G sur G/H)* Supposons que l'on ait un groupe G et H un sous-groupe de G. Alors la multiplication des parties dans G induit une action de G sur G/H

$$G \times G/H \to G/H, (g, xH) \mapsto gxH,$$

appelée action par translations de G sur G/H. Cette action est clairement transitive car l'orbite de H sous G est G/H. De plus, le stabilisateur de l'élément $H \in G/H$ dans G est par définition $\{g \in G \mid gH = H\} = H$. Le stabilisateur dans G de l'élément $xH \in G/H$ est xHx^{-1} par le principe de conjugaison.

Étant donné un sous-groupe arbitraire H de G, on a donc construit une action transitive de G sur un ensemble (à savoir G/H) dont H est un stabilisateur.

Définition 1.18. *Le noyau d'une action donnée de G sur X est le sous-groupe*

$$\cap_{x \in X} G_x = \{g \in G | \ gx = x \quad \forall x \in X\}$$

de G. Autrement dit, c'est le noyau du morphisme $G \to \mathrm{S}_X$ associé à l'action. C'est donc un sous-groupe distingué de G. Une action est dite fidèle *si son noyau est $\{1\}$, i.e. si le morphisme associé $G \to \mathrm{S}_X$ est injectif.*

Exemple 1.19. (i) Le noyau de l'action de conjugaison de G sur lui-même est $\mathrm{Z}(G)$. Pour l'action par translations de G sur G/H, c'est $\cap_{g \in G} gHg^{-1}$.

(ii) Le noyau de l'action naturelle de $\mathrm{GL}(V)$ sur $\mathbb{P}(V)$ est le sous-groupe $k^\times$ des homothéties de V.

(iii) L'action la moins fidèle possible est l'action triviale, dont le noyau est G.

Définition 1.20. *Une action de G sur X est dite libre si on a $G_x = \{1\}$ pour tout $x \in X$.*

Les orbites d'une action libre de G sont donc en bijection avec G. Il ne faut pas confondre libre et fidèle : une action libre est fidèle, mais la réciproque est (très) fausse.

Exemple 1.21. (i) L'action de Cayley est libre.

(ii) L'action naturelle de S_n sur $\{1, \ldots, n\}$ est fidèle, mais pas libre pour $n > 2$.

1.5. Classification des actions d'un groupe donné. Comme pour la notion d'isomorphisme entre groupes, la notion naturelle d'isomorphismes entre actions de G est la suivante.

Définition 1.22. *Soient $(X, \bullet)$ et $(Y, \star)$ deux actions d'un même groupe G. Un* isomorphisme *de $(X, \bullet)$ vers $(Y, \star)$ est une bijection $f : X \to Y$ vérifiant $f(g \bullet x) = g \star f(x)$ pour tout $g \in G$ et $x \in X$. On dit que $(X, \bullet)$ et $(Y, \star)$ sont* isomorphes*, et on note $(X, \bullet) \simeq (Y, \star)$, s'il existe un isomorphisme de l'une vers l'autre.*

On constate que l'identité définit un isomorphisme entre $(X, \bullet)$ et lui-même, que l'inverse d'un isomorphisme est un isomorphisme, et que les isomorphismes entre actions se composent quand cela a un sens : la notion d'isomorphisme entre actions est une relation d'équivalence ! Nous allons restreindre notre étude aux actions transitives. C'est en fait le cas important, et nous renvoyons aux exercices pour voir comment le cas général s'en déduit (Exercice 4.27) et pour de nombreux exemples.

PROPOSITION 1.23. *Soient $(X, \bullet)$ une action transitive de G et $x \in X$. Alors $(X, \bullet)$ est isomorphe à l'action par translations de G sur G/G_x.*

DÉMONSTRATION — On a $X = \mathrm{O}_x$ par transitivité. Par le (ii) de la Proposition 1.11, on a une bijection $f : G/G_x \xrightarrow{\sim} X$ envoyant gG_x sur $g \bullet x$ pour tout $g \in G$. C'est un isomorphisme d'actions : pour $h, g \in G$ on a $f(hgG_x) = hg \bullet x = h \bullet f(gG_x)$. □

Le groupe G agit par conjugaison $(g, H) \mapsto gHg^{-1}$ sur l'ensemble de ses sous-groupes. L'orbite d'un sous-groupe H pour cette action, appelée *classe de conjugaison* de H, est alors $\mathrm{Conj}_G(H) := \{gHg^{-1} \mid g \in G\}$. Ceci étant dit, supposons donnée une action transitive $(X, \bullet)$ de G. Observons que les stabilisateurs associés G_x, avec $x \in X$, forment une classe de conjugaison de sous-groupes de G. En effet, par le principe de conjugaison on a $G_{g \bullet x} = gG_xg^{-1}$ pour tout $x \in X$ et tout $g \in G$, et pour x donné tout $y \in X$ est de la forme $g \bullet x$ pour un g bien choisi par transitivité. On note $\mathrm{Stab}(X, \bullet)$ cette classe de conjugaison de sous-groupes de G associé à $\bullet$.

PROPOSITION 1.24. *Deux actions transitives $(X, \bullet)$ et $(Y, \star)$ d'un même groupe G sont isomorphes si, et seulement si, on a $\mathrm{Stab}(X, \bullet) = \mathrm{Stab}(Y, \star)$.*

DÉMONSTRATION — Soit $f : X \to Y$ un isomorphisme entre $(X, \bullet)$ et $(Y, \star)$. Pour $x \in X$ et $g \in G$, $g \bullet x = x \iff f(g \bullet x) = f(x) \iff g \star f(x) = f(x)$ par injectivité de f. On a donc $G_x = G_{f(x)}$, puis $\mathrm{Stab}(X, \bullet) = \mathrm{Stab}(Y, \star)$. Supposons réciproquement $\mathrm{Stab}(X, \bullet) = \mathrm{Stab}(Y, \star)$. Il existe $x \in X$ et $y \in Y$ avec $H := G_x = G_y$. Par la Proposition 1.23, on a alors $(X, \bullet) \simeq (G/H, \text{translations}) \simeq (Y, \star)$. □

SCHOLIE 1.25. *Il est équivalent de se donner une classe d'isomorphisme d'actions transitives de G sur un ensemble à n éléments, et de se donner une classe de conjugaison de sous-groupes d'indice n de G.*

REMARQUE 1.26. (Transport de structure) Si G agit sur X et si $\varphi : Y \to X$ est une bijection. Il existe une unique action de G sur Y telle que φ soit un isomorphisme d'actions. Par exemple, si X est fini à n éléments, et si $\varphi : \{1, \ldots, n\} \xrightarrow{\sim} X$ est une numérotation des éléments de X, on en déduit une action de G sur $\{1, \ldots, n\}$ isomorphe à celle sur X.

2. Groupes symétrique et alterné

On rappelle que pour $n \geqslant 1$, S_n désigne le groupe des bijections, aussi appellées *permutations*, de l'ensemble $\{1, \ldots, n\}$. C'est un groupe d'ordre $n!$. Un élément σ de S_n est parfois noté sous la forme de la matrice $2 \times n$

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

On note $\operatorname{Fix}\sigma$ l'ensemble des $i \in \{1,\dots,n\}$ tels que $\sigma(i) = i$ (*points fixes* de σ), et $\operatorname{Supp}\sigma$ le complémentaire de $\operatorname{Fix}\sigma$ dans $\{1,\dots,n\}$ (*support* de σ). Deux permutations à supports disjoints commutent (mais la réciproque est fausse !) : si σ est de support S et τ de support T avec $S \cap T = \varnothing$, alors $\sigma\tau$ et $\tau\sigma$ coincident avec σ sur S, avec τ sur T, et valent l'identité sur $\{1,\dots,n\} \smallsetminus (S \cup T)$.

Si $2 \leqslant k \leqslant n$ est un entier, on appelle *k-cycle*, ou cycle de longueur k, une permutation σ dont le support est une partie à k éléments de la forme $\{i_1, i_2, \dots, i_k\}$, avec $\sigma(i_m) = i_{m+1}$ pour $m = 1,\dots,k-1$ et $\sigma(i_k) = i_1$. On note alors $\sigma = (i_1\, i_2 \cdots i_k)$, et on a aussi $\sigma = (i_2\, i_3 \cdots i_k\, i_1)$, etc... Un k-cycle est d'ordre exactement k : on a $\sigma^n(i_m) = i_{n+m}$, les indices étant pris modulo k. Dans le cas particulier $k = 2$, on parle de *transposition* : une transposition $(i\,j)$, avec $i \neq j$, échange i et j et fixe tous les autres éléments. Les cycles engendrent S_n. Beaucoup plus précisément, on a :

Proposition 2.1. (Décomposition en cycles d'une permutation) *Pour tout élément $\sigma \in \mathrm{S}_n$, il existe une unique famille de cycles $\{c_i\}_{i\in I}$ à supports disjoints et tels que $\sigma = \prod_i c_i$.*

Noter que deux cycles à supports disjoints commutent, donc il n'est pas nécessaire de préciser l'ordre dans le produit ci-dessus. De plus, dans le cas $\sigma = 1$ tous les points de $\{1,\dots,n\}$ sont fixés donc la famille de cycles associée est vide ! et on utilise la convention usuelle qu'un produit vide vaut 1 dans un groupe.

Exemple 2.2. Par exemple, on a la décomposition en cycles suivante dans S_8

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 8 & 6 & 1 & 3 & 4 & 7 & 2 \end{pmatrix} = (1\,5\,3\,6\,4)(2\,8).$$

Attention, on a $(1\,2\,3) = (1\,2)\,(2\,3)$ dans S_3 mais ce n'est pas *la* décomposition en cycles car les supports de $(1\,2)$ et $(2\,3)$ ne sont pas disjoints.

Pour démontrer la proposition on considère l'action naturelle du sous-groupe $\langle\sigma\rangle \subset \mathrm{S}_n$ sur $\{1,\dots,n\}$. La relation d'équivalence sur $\{1,\dots,n\}$ associée à ce sous-groupe n'est rien d'autre que celle étudiée à l'Exemple 1.8 Chap. 1, appliqué à la bijection $f = \sigma$ de $X = \{1,\dots,n\}$. Ses classes, *i.e.* les orbites de $\langle\sigma\rangle$ pour cette action, sont simplement appelées *orbites* de σ. Les orbites de cardinal 1 sont les points fixes de σ, ils sont ignorés dans la décomposition [2] ci-dessus. Notons $\{C_i\}_{i\in I}$ les autres orbites, dont ont sait qu'elles sont disjointes. Pour tout i, on constate que σ préserve C_i et en permute circulairement les éléments (comme déjà mis en évidence dans l'Exemple 1.8 Chap. 1), ce qui définit le cycle c_i recherché. On a alors bien $\sigma = \prod_i c_i$, car sur C_j ces deux permutations valent toutes deux c_j, et hors des C_j elles valent l'identité. Cette observation montre aussi l'unicité de la décomposition.

Une première application de la décomposition en cycles concerne la détermination (efficace algorithmiquement !) de l'ordre d'une permutation.

Proposition 2.3. *Soit $\sigma \in \mathrm{S}_n$ de décomposition en cycles $\sigma = \prod_i c_i$. Alors l'ordre de σ est le ppcm des longueurs des c_i.*

Démonstration — Soit $k \in \mathbb{Z}$. On a $\sigma^k = \prod_i c_i^k$ car les c_i commutent. Comme $\operatorname{Supp}(c_i^k) \subset \operatorname{Supp}(c_i)$ et que les $\operatorname{Supp} c_i$ sont disjoints, on constate σ^k coincide avec

2. Nous aurions pu autoriser les cycles de longueur 1, mais comme ils sont tous égaux à l'identité, il faudrait ajouter leur support dans la définition, ce qui est lourd.

c_i^k sur $\mathrm{Supp}(c_i)$, et donc $\sigma^k = 1 \Leftrightarrow c_i^k = 1$ pour tout i. On conclut car l'ordre d'un cycle est sa longueur. □

Remarque 2.4. *On prendra garde qu'une puissance d'un cycle n'est pas forcément un cycle. Par exemple on a* $(1\,2\,3\,4)^2 = (1\,3)\,(2\,4)$. *En revanche, si c est un k-cycle et si n est premier à k, alors c^n est encore un k-cycle (Exercice 4.7).*

La Proposition 2.1 montre que S_n est engendré par les cycles. Pour une partie $\{i_1, \ldots, i_k\}$ à k éléments, la relation

$$(i_1\, i_2 \ldots i_k) \;=\; (i_1 i_2)\,(i_2\, i_3 \ldots i_k) \;=\; (i_1 i_2)\,(i_2\, i_3) \cdots (i_{k-1} i_k) \tag{21}$$

(immédiate !) montre aussi que :

Proposition 2.5. *Les transpositions engendrent* S_n.

Le groupe S_n a beaucoup d'autres systèmes de générateurs intéressants. Avant d'en donner deux autres, montrons lemme important suivant, qui évite souvent bien des calculs !

Lemme 2.6. (Conjugué d'un cycle) *Soient $\sigma \in \mathrm{S}_n$ et $c = (i_1, i_2, \ldots, i_k)$ un k-cycle. Alors $\sigma c \sigma^{-1}$ est le k-cycle $(\sigma(i_1)\,\sigma(i_2)\,\ldots\,\sigma(i_k))$.*

Démonstration — On a $\sigma c \sigma^{-1}(\sigma(i_m)) = \sigma c(i_m) = \sigma(i_{m+1})$. Soit $C = \{i_1, i_2, \ldots, i_m\}$. Pour $j \notin \sigma(C)$, on a $\sigma^{-1}(j) \notin C$ et donc $c(\sigma^{-1}(j)) = \sigma^{-1}(j)$, puis $\sigma c \sigma^{-1}(j) = j$. □

Proposition 2.7. *(i) Les*[3] $(i\ i+1)$ *avec* $1 \leqslant i < n$ *engendrent* S_n.

(ii) La transposition $(1\,2)$ *et le n-cycle* $(1\,2 \ldots n)$ *engendrent* S_n.

En particulier, on a $\min(\mathrm{S}_n) = 2$ *pour* $n > 2$.

Démonstration — Soit H le sous-groupe de S_n engendré par les $(i\ i+1)$. Fixons $1 \leqslant i < j \leqslant n$. En conjuguant $(1\,2) \in H$ successivement par $(2\,3)$, $(3\,4)$, …, $(j-1\ j)$, on a $(1\,j) \in H$. En conjuguant $(1\,j)$ successivement par $(1\,2)$, $(3,4)$, …, $(i-1\,i)$, on a $(i\,j) \in H$. Ainsi, H contient toutes les transpositions, puis $H = \mathrm{S_n}$. Le (ii) se déduit du (i) et de la relation $c^{i-1}(1\,2)c^{1-i} = (i\ i+1)$, où $c = (1\,2 \ldots n)$, elle-même conséquence du Lemme 2.6 ci-dessus. □

Notre but est maintenant de décrire les classes de conjugaison dans S_n.

Définition 2.8. *(i) Une partition de l'entier n est la donnée d'une suite décroissante $n_1 \geqslant n_2 \geqslant \cdots \geqslant n_r$ d'entiers > 0 tels que $n = n_1 + n_2 + \cdots + n_r$.*

(ii) Le type de $\sigma \in \mathrm{S}_n$ est la partition de l'entier n définie par les cardinaux[4] *des orbites de σ dans $\{1, \ldots, n\}$.*

3. Les $s_i = (i\,i+1)$ sont appelés *générateurs de Coxeter* de S_n. Ils vérifient $s_i^2 = 1$, $s_i s_j = s_j s_i$ pour $|i-j| > 1$ et $(s_i s_{i+1})^3 = 1$, ou ce qui revient au même, $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$ (on a en fait $s_i s_{i+1} = (i\ i{+}1\ i{+}2)$). On peut montrer que « toute relation entre les s_i se déduit de ces identités : voir l'Exercice 4.14.

4. Autrement dit, par les longueurs des cycles intervenant dans la décomposition en cycles de σ, et où chaque point fixe est vu comme un cycle de longueur 1.

Les partitions de 4 sont par exemple 4, $3+1$, $2+2$, $2+1+1$ et $1+1+1+1$. La partition $n = n_1 + \cdots + n_r$ est souvent notée symboliquement $1^{l_1}2^{l_2}\cdots n^{l_n}$ où l_i est le nombre de $1 \leqslant j \leqslant r$ tels que $n_j = i$; on omet alors le symbole i^{l_i} quand $l_i = 0$, et on écrit i pour i^1. Par exemple, les partitions de 4 deviennent 4, $1\,3$, 2^2, $1^2\,2$ et 1^4. Ainsi, la permutation $(1\,4)(2\,3)(5\,7\,6)$ de S_8 est de type $1\,2^2\,3$.

Proposition 2.9. *Deux éléments de* S_n *sont conjugués si, et seulement si, ils ont même type.*

Démonstration — Pour $\sigma, \tau, \tau' \in \mathrm{S}_n$ on a $\sigma\tau\tau'\sigma^{-1} = \sigma\tau\sigma^{-1}\sigma\tau'\sigma^{-1}$. Soit $\sigma \in \mathrm{S}_n$ de décomposition en cycles $\sigma = c_1 \cdots c_r$, avec $C_i \subset \{1, \ldots, n\}$ le support de c_i. Pour $\tau \in \mathrm{S}_n$ on a donc $\tau\sigma\tau^{-1} = (\tau c_1 \tau^{-1}) \cdots (\tau c_r \tau^{-1})$. Les $\tau c_i \tau^{-1}$ sont des cycles de support les $\tau(C_i)$ par le Lemme 2.6, encore disjoints : c'est la décomposition en cycles de $\tau\sigma\tau^{-1}$. En particulier, σ et $\tau\sigma\tau^{-1}$ ont même type. Réciproquement, supposons σ et σ' de même type, disons décomposés respectivement en produits de cycles c_i et c'_i pour $i = 1, \ldots, r$, avec c_i et c'_i de même longueur pour tout i. Les supports I_i (resp. I'_i) et des c_i (resp. c'_i) sont disjoints et de même cardinal. Par le Lemme 2.6, on peut trouver $\tau \in \mathrm{S}_n$ avec $\tau(I_i) = I'_i$ et même $\tau c_i \tau^{-1} = c'_i$ pour tout i, puis $\tau\sigma\tau^{-1} = \sigma'$. $\square$

Mettons en évidence une propriété de S_n que l'on vient d'utiliser pour affirmer l'existence de τ dans la dernière phrase de cette démonstration.

Définition 2.10. *Pour $k \geqslant 1$ entier, et G agissant sur X avec $|X| \geqslant k$, on dit que G agit k-transitivement sur X si pour $(x_1, \ldots, x_k)$ et $(y_1, \ldots, y_k)$ deux k-uples d'éléments distincts de X il existe $g \in G$ tel que $gx_i = y_i$ pour tout $i = 1 \ldots k$.*

Par définition 1-transitif équivaut à transitif, et k+1-transitif implique k-transitif.

Exemple 2.11. *(i)* $\mathrm{GL}(V)$ *agit* 2*-transitivement sur* $\mathbb{P}(V)$ *si* $\dim V > 1$. *Il agit même* 3*-transitivement si* $\dim V = 2$ *comme on le verra plus tard !*

(ii) S_n *agit n-transitivement sur* $\{1, \ldots, n\}$ *(c'est ce que l'on a utilisé ci-dessus).*

(iii) Pour $n \geqslant 4$, S_n *agit transitivement, mais pas* 2*-transitivement, sur l'ensemble des parties à* 2 *éléments de* $\{1, \ldots, n\}$.

Un sous-groupe de S_n particulièrement important est le *groupe alterné*. Il est relié à la notion de *signature* d'un permutation σ. Elle est définie par la formule [5]

$$\varepsilon(\sigma) = \prod_{\{i,j\}} \frac{\sigma(j) - \sigma(i)}{j - i},$$

le produit étant pris sur toutes les parties $\{i, j\}$ à deux éléments de $\{1, 2, \ldots, n\}$.

Proposition 2.12. *La signature ε est un morphisme de groupes* $\mathrm{S}_n \to \{\pm 1\}$. *On a $\varepsilon(\tau) = -1$ pour toute transposition τ.*

En particulier, $\varepsilon(\sigma)$ est un signe ± 1 : c'est donc $(-1)^{\mathrm{n}(\sigma)}$ où $\mathrm{n}(\sigma)$ est le nombre de couples $\{i, j\}$ avec $i < j$ et $\sigma(j) < \sigma(i)$ (nombre d'*inversions* de σ).

Démonstration — Le groupe S_n agit naturellement sur l'ensemble des parties à 2 éléments de $\{1, \ldots, n\}$. On en déduit $\prod_{i<j}(\sigma(j) - \sigma(i)) = \pm \prod_{i<j}(i - j)$, et donc

5. Pour $n = 1$, ce produit "vide" vaut 1 par convention.

$\varepsilon(\sigma) = \pm 1$, pour $\sigma \in \mathrm{S}_n$. On en déduit aussi, pour tout $\sigma, \tau \in \mathrm{S}_n$, l'égalité

$$\varepsilon(\sigma) = \prod_{\{i,j\}} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} = \varepsilon(\sigma\tau)/\varepsilon(\tau)$$

ce qui prouve la première assertion. Pour la seconde, soit $\tau = (a\,b)$ une transposition. On peut écrire $\tau = \sigma(1\,2)\sigma^{-1}$ où σ est n'importe quelle permutation envoyant 1 sur a et 2 sur b. On a alors $\varepsilon(\tau) = \varepsilon(\sigma)\varepsilon((1\,2))\varepsilon(\sigma)^{-1} = \varepsilon((1\,2))$ (des signes commutent...). On peut donc supposer $a = 1$ et $b = 2$. Mais dans ce cas, on constate que $\mathrm{n}((1\,2)) = 1$: la seule inversion de $(1\,2)$ est $\{1, 2\}$. On a donc $\varepsilon((1\,2)) = (-1)^1 = -1$. □

Définition 2.13. *Le* groupe alterné A_n *est le sous-groupe des éléments* $\sigma \in \mathrm{S}_n$ *tels que* $\varepsilon(\sigma) = 1$ *(permutations* paires*). C'est un sous-groupe distingué, et on a* $|\mathrm{A}_n| = n!/2$ *pour* $n \geqslant 2$.

Remarque 2.14. (Groupe alterné et jeu de taquin) La notion de permutation paire, bien qu'élémentaire, n'est pas si intuitive que cela ! Elle permet par exemple comprendre pourquoi le challenge à 1000 dollars posé par Sam Loyd au 19ème siècle concernant les positions accessibles du populaire *jeu de Taquin* était impossible : voir ce billet de Michel Coste et l'Exercice 4.15.

Si $c = (i_1\, i_2 \ldots i_k)$ est un k-cycle, la formule (21) montre $\varepsilon(c) = (-1)^{k-1}$. Ainsi, un k-cycle est dans A_n si, et seulement si, on a $k \equiv 1 \bmod 2$. Donnons quelques générateurs de A_n.

Proposition 2.15. *(i) Les produits de deux transpositions engendrent* A_n.
(ii) Les 3*-cycles engendrent* A_n.

Démonstration — On a vu que les transpositions engendrent S_n. Écrivons $\sigma \in \mathrm{S}_n$ comme produit $\sigma = \tau_1 \cdots \tau_n$ de transpositions. On alors $\varepsilon(\sigma) = (-1)^n$, donc $\sigma \in \mathrm{A}_n$ si, et seulement si, n est pair : le (i) s'en déduit.

On a $(a\,b)(a\,b) = 1$, $(a\,b)(b\,c) = (a\,b\,c)$ pour a, b, c distincts, et $(a\,c)(b\,d) = (a\,b\,c)(a\,b\,d)$ pour a, b, c, d distincts. Ainsi, tout produit de 2 transpositions est un produit de 3-cycles. Le (i) implique donc le (ii). □

Remarque 2.16. Un produit de deux transpositions à supports disjoints est appelé *double transposition*. On parle de même de *triple tanspositions* etc...

Les classes de conjugaison de A_n sont légèrement plus subtiles à classer que celles de S_n (voir l'Exercice 4.13).

Proposition 2.17. *Pour* $n \geqslant 3$*, le groupe* A_n *agit* $(n-2)$*-transitivement sur* $\{1, \ldots, n\}$*. En particulier, pour* $2 \leqslant k \leqslant n-2$*, les* k*-cycles de* S_n *sont conjugués sous l'action de* A_n.

Démonstration — En effet, soient $(x_1, \ldots, x_{n-2})$ et $(y_1, \ldots, y_{n-2})$ deux $(n-2)$-uples d'éléments distincts de $\{1, \ldots, n\}$. On peut trouver $\sigma \in \mathrm{S}_n$ avec $\sigma(x_i) = y_i$ pour tout $1 \leqslant i \leqslant n-2$, par n-transitivité de S_n. Le complémentaire des y_i dans $\{1, \ldots, n\}$ est une partie à 2 éléments, disons $\{a, b\}$. On a encore $(a\,b)\sigma(x_i) = y_i$ pour tout $1 \leqslant i \leqslant n-2$. On conclut car une (et une seule) des deux permutations σ et $(a\,b)\sigma$ est dans S_n. La dernière assertion découle du Lemme 2.6. □

3. Les cas $n \leqslant 5$

On a évidemment $\mathrm{A}_1 = \mathrm{S}_1 \simeq 1$ (groupe trivial), et aussi $\mathrm{S}_2 = \{1, (1\,2)\} \simeq \mathbb{Z}/2\mathbb{Z}$ et $\mathrm{A}_2 \simeq 1$. Examinons la structure du groupe S_3. Ses $3! = 6$ éléments sont 1, les trois transpositions $(1\,2)$, $(1\,3)$ et $(2\,3)$, ainsi que les deux 3-cycles $c = (1\,2\,3)$ et $c^2 = (1\,3\,2) = c^{-1}$. On a en particulier

$$\mathrm{A}_3 = \langle c \rangle \simeq \mathbb{Z}/3\mathbb{Z}.$$

Posons $\tau = (1\,3)$. On a $\tau c \tau^{-1} = (3\,2\,1) = c^2$ (Lemme 2.6) et donc $\tau c = c^2 \tau$. Un petit calcul montre en fait $\tau c = c^2 \tau = (1\,2)$ et $c\tau = \tau c^2 = (2\,3)$. En particulier, S_3 n'est pas commutatif[6] et on a

$$\mathrm{S}_3 = \langle \tau, \sigma \rangle.$$

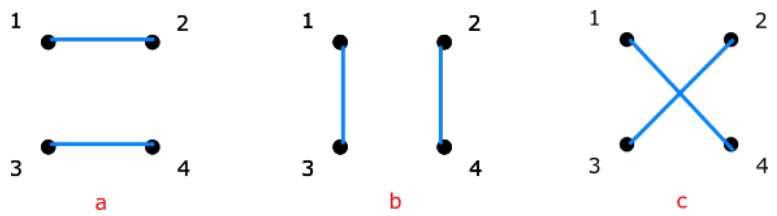
Au final, tout élément de S_3 s'écrit sous la forme (unique) $c^k \tau^q$ avec $0 \leqslant k < 2$ et $0 \leqslant q < 1$. D'autre part, le produit de deux tels éléments se déduit simplement des relations $c^3 = 1$, $\tau^2 = 1$ et $\tau c = c^{-1}\tau$, cette dernière entraînant $\tau c^k = c^{-k}\tau$ pour tout $k \in \mathbb{Z}$. On en déduit la *table de multiplication* de S_3 (Table 1).

$\cdot$	1	c	c^2	τ	τc	τc^2
1	1	c	c^2	τ	τc	τc^2
c	c	c^2	1	τc^2	τ	τc
c^2	c^2	1	c	τc	τc^2	τ
τ	τ	τc	τc^2	1	c	c^2
τc	τc	τc^2	τ	c^2	1	c
τc^2	τc^2	τ	τc	c	c^2	1

TABLE 1. Table de multiplication de S_3

En fait, une analyse similaire s'applique à tout groupe non abélien d'ordre 6 et permet de montrer que tout groupe non abélien d'ordre 6 est isomorphe à S_3 (voir la Proposition 7.10). La structure dégagée ci-dessus de S_3 ne s'étend pas du tout à S_n pour $n \geqslant 4$, mais conduit plutôt à la notion de groupe diédral, que nous verrons plus loin.

Considérons maintenant le cas du groupe S_4, qui a 24 éléments. Il se trouve qu'il existe un morphisme un peu surprenant $\mathrm{S}_4 \to \mathrm{S}_3$, qui permet largement de ramener la structure de S_4 à celle de S_3, et que l'on va décrire maintenant. Observons que l'ensemble $\{1, 2, 3, 4\}$ possède exactement 3 partitions en parties à 2 éléments :



6. On en déduit que S_X n'est pas abélien pour $|X| \geqslant 3$, car alors S_X admet des sous-groupes isomorphes à S_3.

On a donc $a = \{\{1,2\},\{3,4\}\}$, $b = \{\{1,\,3\},\{2,4\}\}$ et $c = \{\{1,4\},\{2,3\}\}$. Le groupe S_4 agit naturellement sur l'ensemble $\mathscr{P} = \{a,b,c\}$ de ces 3 partitions, ce qui fournit un morphisme de groupes

$$f : \mathrm{S}_4 \to \mathrm{S}_{\mathscr{P}}, \quad \text{avec} \quad \mathrm{S}_{\mathscr{P}} \simeq \mathrm{S}_3.$$

Par exemple, on constate que $f((1\,3)) = f((2\,4))$ est la transposition $(a\,c)$ de $\mathscr{P}$, et on a de même $f((2\,3\,4)) = (a\,b\,c)$.

PROPOSITION 3.1. *Le morphisme f ci-dessus est surjectif, de noyau*

$$\mathrm{K}_4 := \{1,\,(1\,3)(2\,4),(1\,2)(3\,4),\,(1\,4)(2\,3)\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Noter que $(1\,2)(3\,4)$ et $(1\,3)(2\,4)$ commutent, même s'ils ne sont pas à support disjoint.

DÉMONSTRATION — Comme $(a\,c) = f((1\,3))$ et $(a\,b\,c) = f((2\,3\,4))$ engendrent $\mathrm{S}_{\mathscr{P}}$ par l'étude de S_3, on a montré que f est surjectif. Son noyau a donc 4 éléments, et les éléments de $\{1,\,(1\,3)(2\,4),(1\,2)(3\,4),\,(1\,4)(2\,3)\}$ conviennent manifestement. C'est un groupe d'ordre 4 dont tous les éléments sont de carré 1 (donc commutatif !), il est donc isomorphe au groupe de Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. □

On a clairement $\mathrm{K}_4 \subset \mathrm{A}_4$ et f induit de même morphisme surjectif $\mathrm{A}_4 \to \mathrm{A}_{\mathscr{P}} \simeq \mathrm{A}_3 \simeq \mathbb{Z}/3\mathbb{Z}$ (un 3-cycle est envoyé sur un 3 cycle) de noyau K_4. Nous verrons au §5 que ces dévissages non triviaux de S_n et A_n pour $n \leqslant 4$ cessent pour $n \geqslant 5$. En revanche, un phénomène remarquable supplémentaire se produit pour $n = 5$.

THÉORÈME 3.2. *Il existe une action transitive de S_5 sur un ensemble à 6 éléments.*

Nous verrons plus tard que cette action est unique à isomorphisme près, et aussi qu'elle est fidèle et 3-transitive ! (Voir l'Exercice 4.24 et le Corollaire 10.8) Nous allons en donner deux descriptions ci-dessous.

La première, d'apparence assez magique mais particulièrement esthétique, est issue d'un article de Howard-Millson-Snowden-Vakil [7]. On considère le graphe complet $\mathscr{G}$ (non orienté) de sommets $\{1,2,3,4,5\}$. Ce graphe a exactement 10 arêtes. On se convainc aisément qu'il existe exactement 6 manières de partitionner ces 10 arêtes en réunion disjointe de deux circuits hamiltoniens [8] de $\mathscr{G}$: ce sont les 6 "*pentagones mystiques*", représentés dans la Figure 1 ci-dessous.

Hormis dans le cas du pentagone a, on constate que chaque pentagone est formé d'un *poisson* et d'une *chauve-souris* ! Notons $X = \{a,b,c,d,e,f\}$ l'ensemble de ces 6 partitions de $\mathscr{G}$. L'action évidente de S_5 agit sur $\{1,\ldots,5\}$ induit naturellement une action de S_5 sur X, et fournit donc un morphisme de groupes

$$\phi : \mathrm{S}_5 \to \mathrm{S}_X \simeq \mathrm{S}_6.$$

Il est aisé d'étudier l'action de chaque élément de S_5 sur X. Un exemple particulièrement simple est celui de la permutation $(1\,2\,3\,4\,5)$ de S_5, qui fixe manifestement le pentagone a et permute cycliquement les 5 autres, via $(b\,c\,d\,e\,f)$. On a donc $\phi((1\,2\,3\,4\,5)) = (b\,c\,d\,e\,f)$. Autre exemple : on a $\phi((1\,2)) = (a\,d)(b\,c)(e\,f)$. En effet,

7. *A description of the outer automorphism of* S_6 *and the invariants of* 6 *points in the projective space.*

8. *i.e.* de circuit de longueur 5 passant une et une seule fois par chaque sommet.

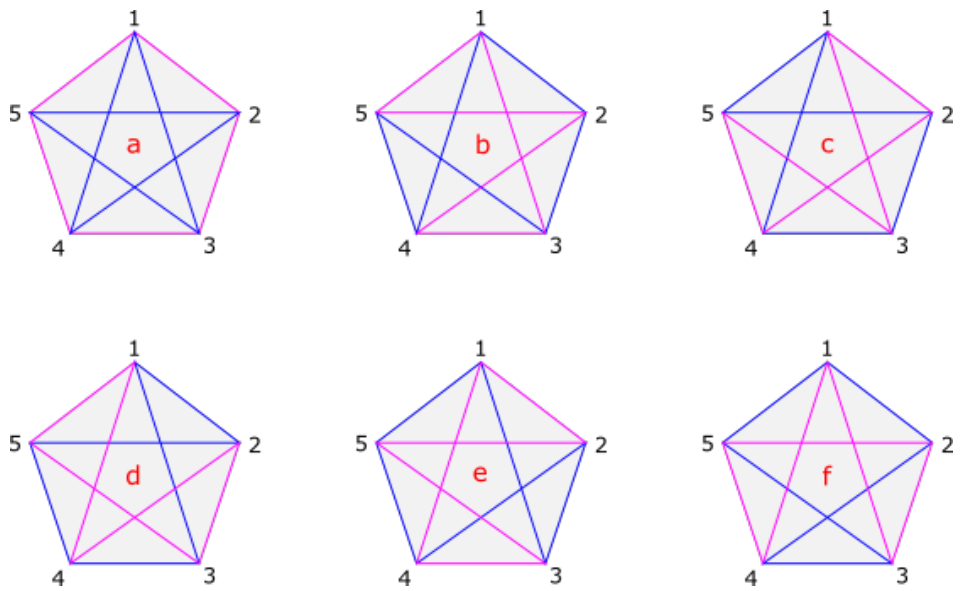


FIGURE 1. Les 6 « pentagones mystiques »

$(1\,2)$ envoie le « contour » $(1\,2\,3\,4\,5)$ du a sur $(2\,1\,3\,4\,5)$ (poisson du d), le poisson $(1\,2\,3\,5\,4)$ du b sur $(2\,1\,3\,5\,4)$ (chauve-souris du c), et la chauve-souris $(1\,2\,5\,4\,3)$ du e sur $(2\,1\,5\,3\,4)$ (poisson du f). Cela démontre que l'action de S_5 sur X est transitive, comme annoncé. De même, on verrait que le 3-cycle $(1\,2\,3)$ agit comme $(a\,f\,c)(b\,e\,d)$ et le 4-cycle $(1\,2\,3\,4)$ comme $(a\,c\,e\,b)$.

Donnons maintenant une seconde description, à la fois plus classique et plus naturelle, de l'action ci-dessus. Notons Y l'ensemble des sous-groupes d'ordre 5 de S_5. On a $|Y| = 6$. En effet, un sous-groupe d'ordre 5 est engendré par un 5-cycle, et contient en fait un unique 5-cycle envoyant 1 sur 2, *i.e.* de la forme $(1\,2\,a\,b\,c)$ avec $\{a, b, c\} = \{3, 4, 5\}$. Le groupe S_5 agit par conjugaison sur Y, via $(\sigma, H) \mapsto \sigma H \sigma^{-1}$. Cette action est transitive car deux 5-cycles quelconques sont conjugués dans S_5 : elle répond bien au théorème. Mieux, cette description rend évident le fait que le sous-groupe de S_5 isomorphe à S_3 fixant 1 et 2 agit 3-transitivement sur Y !

Vérifions enfin que les actions ci-dessus de S_5 sur X et Y sont isomorphes. En effet, tout sous-groupe $H = \langle c \rangle$ d'ordre 5 de S_5 définit un unique pentagone $\mathrm{p}(H)$ donné par les deux chemins non orientés $c^{\pm 1}$ et $c^{\pm 2}$. L'application $\mathrm{p} : Y \to X, H \mapsto \mathrm{p}(H)$, est manifestement bijective. Enfin, pour $\sigma \in \mathrm{S}_5$ et $c = (i_1\, i_2\, i_3\, i_4\, i_5)$ on a $\sigma c \sigma^{-1} = (\sigma(i_1)\, \sigma(i_2)\, \sigma(i_3)\, \sigma(i_4)\, \sigma(i_5))$. On a donc $\mathrm{p}(\sigma H \sigma^{-1}) = \sigma \cdot \mathrm{p}(H)$ pour tout $H \in Y$: c'est un isomorphisme d'action.

REMARQUE 3.3. Cette action exotique de S_5 est à l'origine de nombreuses autres constructions (encore plus) exotiques concernant la géométrie des ensembles de petit cardinal. C'est par exemple un point de départ pour construire un automorphisme *non intérieur de* S_6. Elle est très spécifique : on peut montrer que S_n n'admet pas d'action transitive sur un ensemble à $n + 1$ éléments pour $n \neq 5$, et que tout automorphisme de S_n est intérieur pour $n \neq 6$.

4. Le langage des suites exactes

Le langage des *suites exactes* est commode pour exprimer le genre de phénomènes observés ci-dessus pour $n \leqslant 4$, et plus généralement les dévissages.

DÉFINITION 4.1. *Une suite de $n \geqslant 2$ morphismes de groupes*

$$G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} \cdots \xrightarrow{f_n} G_{n+1},$$

est dite exacte, si on a $\operatorname{Im} f_i = \ker f_{i+1}$ *pour* $i = 1, \ldots, n-1$.

Par exemple, dire que $1 \to G \xrightarrow{f} G'$ est exacte signifie donc $\{1\} = \ker f$, *i.e.* que le morphisme f est injectif : on ne précise par le morphisme $1 \to G$, nécessairement trivial. De même, $G \xrightarrow{f} G' \to 1$ est exacte si, et seulement si, f est surjective.

DÉFINITION 4.2. *Une suite exacte de la forme* $1 \to H \xrightarrow{i} G \xrightarrow{\pi} K \to 1$ *s'appelle une suite exacte courte (en abrégé,* s.e.c.*).*

L'exactitude d'une telle suite signifie donc que le morphisme i est injectif, que π est surjectif, et que l'on a $\ker \pi = \operatorname{Im} i$. Comme nous le verrons, les exemples de suites exactes courtes abondent :

EXEMPLE 4.3. *(i) Pour tout entier $n \geqslant 2$ on a une s.e.c.*

$$1 \to \mathrm{A}_n \xrightarrow{i} \mathrm{S}_n \xrightarrow{\varepsilon} \{\pm 1\} \to 1,$$

où i désigne encore l'inclusion naturelle et ε la signature.

(ii) Pour tout k-espace vectoriel V avec $1 \leqslant \dim V < \infty$ on a une s.e.c.

$$1 \to \mathrm{SL}(V) \xrightarrow{i} \mathrm{GL}(V) \xrightarrow{\det} k^\times \to 1.$$

(iii) Pour tout sous-groupe distingué H d'un groupe G on a une s.e.c. naturelle

$$1 \to H \xrightarrow{i} G \xrightarrow{\pi} G/H \to 1,$$

où i est le morphisme d'inclusion et π la projection canonique.

La proposition facile suivante fait le lien entre dévissage et suite exacte courte.

PROPOSITION 4.4. *Soient H, G, K trois groupes. Il est équivalent de se donner :*

(i) une suite exacte $1 \to H \xrightarrow{i} G \xrightarrow{\pi} K \to 1$,

(ii) un sous-groupe distingué $H' \subset G$ et des isomorphismes $i' : H \xrightarrow{\sim} H'$ et $\pi' : G/H' \xrightarrow{\sim} K$.

DÉMONSTRATION — Soit $1 \to H \xrightarrow{i} G \xrightarrow{\pi} K \to 1$ une suite exacte. Alors $H' := \operatorname{Im} i$ est un sous-groupe de G. On a aussi $H' = \ker \pi$ par exactitude "au milieu", et donc H' est distingué dans G. Le morphisme injectif i induit un isomorphisme $i' : H \xrightarrow{\sim} H'$, et par le premier théorème d'isomorphisme, le morphisme surjectif π induit un isomorphisme $\pi' : G/H' \to K$.

Réciproquement, soient (H', i', π') comme dans le (ii). On pose $i : H \to G$, $h \mapsto i'(h)$, et on note $\pi : G \to K$ la composée de la projection canonique $G \to G/H'$ et de l'isomorphisme $\pi' : G/H' \to K$. Par construction, i est un morphisme injectif,

π est un morphisme surjectif, et on a $\ker \pi = H' = \operatorname{Im} i$. Ainsi, la suite $1 \to H \xrightarrow{i} G \xrightarrow{\pi} K \to 1$ est exacte. Cela conclut car il est clair que les deux constructions $(i, \pi) \leftrightarrow (H', i', \pi')$ sont inverses l'une de l'autre. □

C'est toujours plus précis de nommer les morphismes apparaissant dans une suite exacte. On omet parfois de le faire, soit pour ceux qui sont naturels (inclusion canonique d'un sous-groupe, projection canonique...), soit parce que cela ne présente pas d'intérêt particulier pour notre propos, ou encore quand les morphismes utilisés sont le fruit d'un choix que l'on ne veut pas préciser (comme les choix, arbitraires, d'isomorphisme $\mathrm{S}_{\mathscr{P}} \simeq \mathrm{S}_3$ et $\ker f \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ plus haut). Dans ce langage, et par la Proposition 4.4, les dévissages de S_3, S_4 et A_4 étudiés en Section 3 s'écrivent :

Corollaire 4.5. *Il existe des suites exactes :*

(i) $1 \to \mathbb{Z}/3\mathbb{Z} \to \mathrm{S}_3 \to \mathbb{Z}/2\mathbb{Z} \to 1$,

(ii) $1 \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathrm{S}_4 \to \mathrm{S}_3 \to 1$,

(iii) $1 \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathrm{A}_4 \to \mathbb{Z}/3\mathbb{Z} \to 1$.

Bien noter en revanche que le morphisme $\mathrm{S}_5 \to \mathrm{S}_6$ étudié au chapitre précédent ne s'insère pas dans une suite exacte courte : il n'est pas surjectif et son image n'est (comme on le verra !) pas distinguée dans S_6.

Exemple 4.6. (*Groupe diédral*) Soit $n \geqslant 3$. Le groupe diédral D_{2n} est le sous-groupe de S_n engendré par le n-cycle $c = (1\ 2\ \dots\ n)$ et l'élément τ défini par $\tau(i) = n+1-i$ pour $i = 1, \dots, n$. On a les relations $\tau^2 = 1$ et $\tau c \tau^{-1} = (n\ n-1\ \dots\ 2\ 1) = c^{-1}$. Le sous-groupe $C = \langle c \rangle$ de D_{2n}, cyclique d'ordre n, est donc distingué. Il ne contient pas τ (car $\tau c \tau^{-1} = c^{-1} \neq c$ pour $n > 2$), et on a donc $\mathrm{D}_{2n} = C\langle \tau \rangle$ puis

$$\mathrm{D}_{2n} = C \coprod C\tau \ \text{ et } \ |\mathrm{D}_{2n}| = 2n.$$

Par exemple, on a $\mathrm{D}_6 = \mathrm{S}_3$ (plus petit groupe diédral), et D_8 est un 2-Sylow de S_4. On a $C \simeq \mathbb{Z}/n\mathbb{Z}$ et donc (Proposition 4.4) une s.e.c.

$$1 \to \mathbb{Z}/n\mathbb{Z} \to \mathrm{D}_{2n} \to \mathbb{Z}/2\mathbb{Z} \to 1.$$

Le groupe D_{2n} n'est pas commutatif, en particulier il n'est pas isomorphe à $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Comme nous le verrons, il s'identifie naturellement au groupe des isométries d'un polygone régulier du plan à n côtés.

Définition 4.7. *Si G, H et K sont des groupes donnés, on dira que G est extension de K par H s'il existe une suite exacte courte $1 \to H \to G \to K \to 1$*[9]*. On appelle aussi extension de K par H la donnée d'une telle suite.*

Ainsi, S_4 est une extension de S_3 par le groupe de Klein, et D_{2n} est une extension de $\mathbb{Z}/2\mathbb{Z}$ par $\mathbb{Z}/n\mathbb{Z}$.

5. Le dévissage de S_n

Les résultats suivants étaient connus de Galois, mais les premières démonstrations semblent dues à Jordan.

9. Bien noter l'ordre de K et H dans cette terminologie Bourbakiste.

THÉORÈME 5.1. *Les seuls sous-groupes distingués de* S_n *sont* $\{1\}$, A_n, S_n, *ainsi que* K_4 *dans le cas particulier* $n = 4$.

DÉMONSTRATION — On a déjà vu que les sous-groupes de l'énoncé sont distingués. Soit H un sous-groupe distingué non trivial de S_n. Notons que si H contient une transposition, alors H contient toutes les transpositions (elles sont conjuguées) et on a donc $H = \mathrm{S}_n$ (elles sont génératrices). De plus, pour $h \in H$ et $\sigma \in \mathrm{S}_n$ observons

$$[h, \sigma] := h\sigma h^{-1}\sigma^{-1} = (h\sigma h^{-1})\sigma^{-1} = h(\sigma h^{-1}\sigma^{-1}).$$

La dernière écriture, et $H \lhd \mathrm{S}_n$, montrent $[h, \sigma] \in H$. La seconde écriture montre *e.g.*

$$[h, (i\,j)] = (h(i)\,h(j))(i\,j)^{-1} \in H, \quad \forall 1 \leqslant i < j \leqslant n.$$

Ainsi, on a trouvé un élément de H dont le support est dans $\{i, j, h(i), h(j)\}$ (technique dite de *réduction du support*).

Supposons d'abord que H contienne un élément h possédant un cycle de longueur $\geqslant 3$ dans sa décomposition en cycles. Écrivant ce cycle $(i\,j\,k\,\ldots)$, on a alors

$$[h, (i\,j)] = (j\,k)(i\,j) = (i\,k\,j) \in H.$$

Comme les 3-cycles sont conjugués dans S_n pour $n \geqslant 3$, on a donc $H \supset \mathrm{A}_n$, puis $H = \mathrm{A}_n$ ou $H = \mathrm{S}_n$.

On peut donc supposer que tous les éléments non triviaux de H sont des produits de $\geqslant 2$ transpositions à supports disjoints, et en particulier $n \geqslant 4$. Dans le cas $n = 4$, ce sont nécessairement des doubles transpositions, et comme ces dernieres sont conjuguées dans S_4, on constate $H = \mathrm{K}_4$. On peut donc supposer $n \geqslant 5$. Écrivons $h = (i\,j)(k\,l)$... (décomposition en cycles). On en déduit que H contient la double transposition $[h, (i\,k)] = (j\,l)(i\,k)$, et donc toutes les doubles transpositions par conjugaison. Il contient donc $(j\,l)(i\,m)$ pour tout entier m distinct de i, j, k et l (il en existe car $n \geqslant 5$). Mais alors H contient le 3-cycle $(j\,l)(i\,k)(j\,l)(i\,m) = (i\,m\,k)$, qui n'est pas produit de transpositions à supports disjoints. □

On a déjà vu $\mathrm{A}_1 = \mathrm{A}_2 = \{1\}$, $\mathrm{A}_3 \simeq \mathbb{Z}/3\mathbb{Z}$ et que le groupe A_4 n'est pas simple. Nous laissons au lecteur le soin de montrer que les sous-groupes distingués de A_4 sont $1, \mathrm{K}_4$ et A_4. La situation est radicalement différente pour $n \geqslant 5$.

THÉORÈME 5.2. *Le groupe* A_n *est simple (non abélien) pour* $n \geqslant 5$.

Bien noter que ce résultat ne se déduit pas immédiatement du précédent, car si on a $K \lhd H$ et $H \lhd G$ il n'est pas vrai en général que l'on a $K \lhd G$ (voir l'Exercice 4.11). On s'en sort toutefois par une approche est similaire à celle de la preuve du théorème ci-dessus.

DÉMONSTRATION — Soit $H \subset \mathrm{A}_n$ distingué avec $H \neq 1$ et $n \geqslant 5$. On va montrer $H = \mathrm{A}_n$. Il suffit de voir que H contient un 3-cycle car ces derniers sont conjugués dans A_n et l'engendrent pour $n \geqslant 5$ (Propositions 2.15 et 2.17). Fixons $h \in H - \{1\}$.

Supposons d'abord $n = 5$. En considérant les décompositions en cycles possibles, on constate que h est soit un 3-cycle, soit une double-transposition, soit un 5-cycle. Si h est un 3-cycle, on a gagné. Si h est une double-transposition $(a\,b)(c\,d)$, H contient aussi $[h, (c\,d\,e)] = (c\,e\,d)(c\,d\,e)^{-1} = (c\,e\,d)^2 = (c\,d\,e)$: encore gagné. Enfin si h est

un 5-cycle $(a\,b\,c\,d\,e)$, H contient aussi $[h,(c\,d\,e)] = (d\,e\,a)\,(c\,d\,e)^{-1} = (a\,d\,c)$, ce qui conclut.

Considérons maintenant le cas général. Fixons $\tau = (a\,b\,c)$ un 3-cycle, et regardons

$$[h,(a\,b\,c)] = (h(a)\,h(b)\,h(c))\,(a\,c\,b) \in H$$

Vérifions qu'on peut choisir τ tel que $[h,(a\,b\,c)] \neq 1$. Comme $h \neq 1$, il existe a tel que $h(a) \neq a$, et on peut donc poser $b = h(a)$, puis choisir $c \notin \{a, b, h(b)\}$ car $n \geqslant 4$. Dans ce cas $[h,(a\,b\,c)]$ envoie c sur $h(b) \neq c$, ce que l'on voulait. D'autre part, le support de $s := [h,(a\,b\,c)]$ est inclus dans $\{a, b, c, h(b), h(c)\}$ qui a $\leqslant 5$ éléments. On peut donc voir s comme une permutation paire (non triviale) d'un sous-ensemble C à 5 éléments de $\{1, \ldots, n\}$, et fixant le complémentaire C' de C. Le sous-groupe G de A_n fixant C' est isomorphe à A_5. De plus, $H \cap G$ est trivialement distingué dans G, car $H \lhd \mathrm{A}_n$, et il contient l'élément $s \neq 1$. D'après le cas $n = 5$ on a donc $H \cap G = G$, *i.e.* $G \subset H$, et donc H contient tous les 3-cycles de support dans C. □

Un exemple de corollaire à ces résultats est le suivant. Il montre par exemple que l'action exotique de S_5 sur 6 éléments est automatiquement fidèle.

Corollaire 5.3. *(i) Pour $n \neq 4$, toute action de A_n est fidèle ou triviale.*

(ii) Une action transitive de S_n sur un ensemble à $m > 2$ éléments est fidèle, sauf peut-être si $n = 4$ et $m = 3$ ou 6.

Démonstration — Le (i) vaut pour tout groupe simple (ou trivial) : le noyau d'une action d'un tel groupe G est un sous-groupe distingué, c'est donc soit $\{1\}$ (action fidèle), soit G (action triviale).

Pour le (ii), supposons que $G := \mathrm{S}_n$ agit transitivement sur X avec $|X| = m$. Soit $x \in X$; on a $|\mathrm{O}_x| = m$ (action transitive) et donc $|G_x| = |\mathrm{S}_n|/m < n!/2$ (orbite-stabilisateur). Mais le noyau de l'action de G sur X est un sous-groupe distingué $K \subset \mathrm{S}_n$ inclus dans G_x, et donc de cardinal $< n!/2$. Par le Théorème 5.1 on a donc soit $K = \{1\}$, soit $n = 4$, $K = \mathrm{K}_4$ et par Lagrange $4 = |K|$ divise $4!/m = |G_x|$, *i.e.* $m \mid 6$. □

Remarque 5.4. En utilisant un morphisme surjectif $\mathrm{S}_4 \to \mathrm{S}_3$ on construit aisément des actions transitives de S_4 de noyau K_4 sur des ensembles à 3 ou 6 éléments. Le morphisme surjectif $\mathrm{S}_n \to \mathrm{S}_2$ (signature !) construit aussi une action transitive de S_n sur $\{1, 2\}$ pour tout $n \geqslant 2$, de noyau A_n.

6. Commutateurs et groupes dérivés

La notion de *commutateur* a joué un rôle important dans les démonstrations ci-dessus. Discutons-les plus généralement. Si $x, y \in G$, on appelle commutateur du couple (x, y) l'élément [10]

$$[x, y] = xyx^{-1}y^{-1}.$$

On a donc $[x, y] = 1$ si et seulement si $xy = yx$. Si A et B sont deux parties de G, on note $[A, B]$ le sous-groupe de G engendré par les $[a, b]$ avec $a \in A$ et $b \in B$.

Définition 6.1. *Le groupe dérivé d'un groupe G est le sous-groupe $\mathrm{D}(G) := [G, G]$ engendré par les $[x, y]$ avec $x, y \in G$.*

10. Certains auteurs le définissent plutôt comme $x^{-1}y^{-1}xy$. Cela n'a que peu d'incidence.

On a évidement $\mathrm{D}(G) = \{1\}$ si, et seulement si, G est abélien.

Remarque 6.2. ⚠ Les commutateurs ne forment pas un sous-groupe en général, d'où la nécessité de considérer le sous-groupe engendré dans la définition de $\mathrm{D}(G)$. Par exemple, Guralnick a montré [11] que le plus petit groupe fini G pour lequel $\mathrm{D}(G)$ n'est pas constitué de commutateurs est d'ordre 96.

Exemple 6.3. Si $\sigma \in G$ est conjugué dans G à son carré, alors σ est un commutateur. En effet, on a $\sigma^2 = \tau\sigma\tau^{-1}$, et donc $\sigma = [\sigma^{-1}, \tau]$ (voir l'Exercice 4.28 pour une généralisation). Comme le carré d'un 3-cycle est un 3-cycle, et que les 3-cycles sont conjugués dans S_n pour tout n, et même dans A_n pour $n \geqslant 5$, on en déduit que les 3-cycles sont des commutateurs de S_n, et même des commutateurs de A_n pour $n \geqslant 5$.

L'observation suivante est aussi importante que triviale.

Fait 6.4. *Si $f : G \to G'$ est un morphisme de groupes, on a pour tout $x, y \in G$ $f([x, y]) = [f(x), f(y)]$, et donc $f(\mathrm{D}(G)) \subset \mathrm{D}(G')$, avec égalité si f est surjective*

Par exemple, on a $\mathrm{D}(H) \subset \mathrm{D}(G)$ pour H sous-groupe de G. Un sous-groupe C d'un groupe G est dit *caractéristique* si on a $\alpha(C) \subset C$ pour tout $\alpha \in \mathrm{Aut}(G)$. On a alors $\alpha(C) = C$ pour tout $\alpha \in \mathrm{Aut}(G)$ (considérer α^{-1}) et aussi $C \lhd G$ (prendre pour α un automorphisme intérieur).

Corollaire 6.5. *$\mathrm{D}(G)$ est un sous-groupe caractéristique de G.*

Démonstration — C'est le fait ci-dessus appliqué à un automorphisme de G. □

Corollaire 6.6. *Soit G un groupe.*

(i) Tout morphisme $f : G \to G'$ avec G' abélien vérifie $\mathrm{D}(G) \subset \ker f$.

(ii) Pour $H \lhd G$, alors G/H est abélien si, et seulement si, H contient $\mathrm{D}(G)$.

Démonstration — Pour le (i), on a $f([x, y]) = [f(x), f(y)] = 1$ pour tout $x, y \in G$, donc $\mathrm{D}(G) \subset \ker f$. Pour le (ii), on constate $[xH, yH] = [x, y]H$. C'est aussi la relation $\pi([x, y]) = [\pi(x), \pi(y)]$ pour $\pi : G \to G/H$. Ainsi, xH et yH commutent dans G/H si, et seulement si, on a $[x, y] \in H$. □

D'après le (ii) ci-dessus, $\mathrm{D}(G)$ est le plus petit sous-groupe distingué de G de quotient abélien. Le groupe quotient $G_{\mathrm{ab}} := G/\mathrm{D}(G)$ s'appelle l'*abélianisé* G. C'est le plus grand quotient abélien de G. Terminons par une étude des groupes dérivés successifs de S_n.

Proposition 6.7. *Soit $n \geqslant 1$ un entier. On a*

(i) $\mathrm{D}(\mathrm{S}_n) = \mathrm{A}_n$,

(ii) $\mathrm{D}(\mathrm{A}_n) = \mathrm{A}_n$ *pour* $n \geqslant 5$,

(iii) $\mathrm{D}(\mathrm{A}_4) = \mathrm{K}_4$ *et* $\mathrm{D}(\mathrm{A}_n) = \{1\}$ *pour* $n \leqslant 3$.

11. Robert Guralnick, *Commutators and commutator subgroups*, Adv. in Math. 45, 319–330 (1982)

Démonstration — En[12] considérant la signature, on constate $\mathrm{D}(\mathrm{S}_n) \subset \mathrm{A}_n$. Ces deux groupes sont triviaux pour $n \leqslant 2$, donc on suppose définitivement $n \geqslant 3$. Comme les 3-cycles engendrent A_n, l'Exemple 6.3 montre les point (i) et (ii).

Pour le cas restant $n = 4$ on a $\mathrm{D}(\mathrm{A}_4) \subset \mathrm{K}_4$ en considérant un morphisme $\mathrm{A}_4 \to \mathrm{A}_3$ de noyau K_4. On a l'égalité en observant, pour a, b, c, d distincts, l'égalité $[(a\,b\,c), (a\,b\,d)] = (b\,c\,d)(a\,b\,d)^{-1} = (a\,b)(c\,d)$. □

Remarque 6.8. Ore a démontré dans cet article[13] que tout élément de A_n est un commutateur de deux éléments de S_n, et que pour $n \geqslant 5$ tout élément de A_n est un commutateur de deux éléments de A_n.

Pour $n \geqslant 0$ on pose $\mathrm{D}^0(G) = G$ et on définit récursivement, pour $n > 1$,

$$\mathrm{D}^n(G) = \mathrm{D}(\mathrm{D}^{n-1}(G)).$$

C'est une suite décroissante (au sens large) de sous-groupes caractéristiques de G.

Définition 6.9. *Un groupe G est dit résoluble s'il existe un entier $n \geqslant 0$ tel que $\mathrm{D}^n(G) = \{1\}$. Le plus petit tel n est alors appelé classe (de résolubilité) de G.*

Les groupes abéliens sont trivialement résolubles de classe $\leqslant 1$. D'après la Proposition 6.7, on a :

Corollaire 6.10. *Le groupe S_n (resp. A_n) est résoluble, si et seulement si, on a $n \leqslant 4$.*

Ce résultat est particulièrement significatif du point de vue de la théorie de Galois (voir le Complément en Section 9). La Proposition 6.7 montre aussi que S_3 et S_4 sont résolubles de classe 2 et 3 respectivement. De même, D_{2n} est résoluble de classe 2 pour $n \geqslant 3$. La propriété d'être résoluble est stable par passage au sous-groupe, au quotient et par extension :

Proposition 6.11. *Soient G un groupe et H un sous-groupe distingué de G. Alors G est résoluble si, et seulement si, les groupes H et G/H le sont. En outre, si G, H, K sont résolubles de classes n, a, b respectivement, alors $a, b \leqslant n$ et $n \leqslant a + b$.*

Démonstration — Pour tout $j \geqslant 0$, on a $\mathrm{D}^j(H) \subset \mathrm{D}^j(G)$, et si $\pi : G \to G/H$ est la projection canonique, on a aussi $\pi(\mathrm{D}^j(G)) = \mathrm{D}^j(G/H)$ par le Fait 6.4. Ainsi, si $\mathrm{D}^n(G) = \{1\}$ pour un certain $n \geqslant 1$ on a $\mathrm{D}^n(H) = \{1\} = \mathrm{D}^n(G/H)$. Si réciproquement $\mathrm{D}^a(H) = \{1\}$ et $\mathrm{D}^b(G/H) = 1$ pour certains $a, b \geqslant 1$. On a alors $\pi(\mathrm{D}^b(G)) = \{1\}$, donc $\mathrm{D}^b(G) \subset H$, puis $\mathrm{D}^{a+b}(G) \subset \mathrm{D}^a(H) = \{1\}$, et donc $\mathrm{D}^{a+b}(G) = \{1\}$. □

Remarque 6.12. (i) On peut montrer que *le plus petit groupe simple non abélien est* A_5. On en déduit par récurrence sur le cardinal du groupe que *tout groupe d'ordre* < 60 *est résoluble*, d'après la Proposition 6.11.

(ii) Burnside a démontré que *tout groupe d'ordre $p^a q^b$, avec p, q premiers, est résoluble*. Nous reviendrons sur ce résultat à la fin du cours.

12. Un argument massue serait d'utiliser la simplicité de A_n pour $n \geqslant 5$.
13. O. Ore, *Some remarks on commutators*, Proc. A. M. S. Vol. 2, 307–314 (1951).

(iii) Un résultat difficile et fameux, dû à Feit-Thompson,[14] affirme que *tout groupe d'ordre impair est résoluble*. C'est un indicateur du fait qu'il est très difficile de classifier les groupes finis résolubles.

Terminons par un exemple important de groupes résolubles. Fixons k un corps, $n \geqslant 1$ un entier, notons $\mathrm{T}_n(k) \subset \mathrm{GL}_n(k)$ le sous-groupe des matrices triangulaires supérieures, et On a $\mathrm{T}_1(k) = k^\times$ qui est abélien, donc résoluble. Plus généralement, pour $n \geqslant 1$ on a une suite exacte courte

$$1 \longrightarrow \mathrm{U}_n(k) \xrightarrow{\text{can}} \mathrm{T}_n(k) \xrightarrow{\text{diag}} (k^\times)^n \to 1,$$

où $\mathrm{U}_n(k)$ est le sous-groupe de $\mathrm{T}_n(k)$ constitué des g tels que $g_{j,j} = 1$ pour tout $1 \leqslant j \leqslant n$ (*groupe des unipotents supérieurs*). Cela montre $\mathrm{D}(\mathrm{T}_n(k)) \subset \mathrm{U}_n(k)$. Pour $n = 2$, on constate que l'application $k \to \mathrm{U}_2(k)$, $x \mapsto \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$, est un isomorphisme de groupes (où k est vu comme groupe additif), donc $\mathrm{T}_2(k)$ est résoluble.

Proposition 6.13. *Le groupe* $\mathrm{T}_n(k)$ *est résoluble de classe* $\leqslant 1 + \lceil \log_2(n) \rceil$.

Démonstration — Soient $G = \mathrm{T}_n(k)$ et $e_1, \ldots, e_n$ la base canonique de k^n. Pour $1 \leqslant i \leqslant n$, on pose $V_i = \sum_{j=1}^{i} ke_j$, et aussi $V_i = \{0\}$ pour $i \leqslant 0$. Pour tout $g \in G$ on a $g(V_i) \subset V_i$ pour tout i. Pour tout $j \geqslant 1$, on pose

$$G_j = \{g \in G \mid (g-1)(V_i) \subset V_{i-j}, \quad \forall\, i = 1, \ldots, n\}.$$

On a $G_1 = \mathrm{U}_n(k)$, $G_{j+1} \subset G_j$, et $G_j = \{1\}$ pour $j \geqslant n$. Pour $j > 1$, observons que G_j est le sous-ensemble de $\mathrm{U}_n(k)$ des éléments de $j-1$ premières surdiagonales nulles. Un peu de calcul matriciel montre que G_i est un sous-groupe de G. Alternativement, on peut remarquer que pour $g \in G_j$ et $g' \in G_j$ on a $gg' - 1 = g(g'-1) + (g-1)$ puis $(gg'-1)(V_i) \subset V_{i-j} + V_{i-j} \subset V_{i-j}$. De plus, on a aussi $1 \in G_j$ et $g^{-1} \in G_j$ par l'écriture $g^{-1} - 1 = (1-g)g^{-1}$. Enfin, pour $g \in G_j$ et $h \in G_{j'}$ on a

$$[g,h] - 1 = ghg^{-1}h^{-1} - 1 = ((g-1)(h-1) - (h-1)(g-1))g^{-1}h^{-1},$$

et donc $[G_j, G_{j'}] \subset G_{j+j'}$. On en déduit $\mathrm{D}^m(G_1) \subset G_{2^m}$ pour $m \geqslant 1$, puis $\mathrm{D}^m(G_1) \subset G_n = \{1\}$ pour $2^m \geqslant n$. On conclut car on a $\mathrm{D}(G) \subset G_1$. □

7. Le dévissage en produit semi-direct

Commençons par définir la notion de *complément* d'un sous-groupe.

Définition 7.1. *Si H est un sous-groupe d'un groupe G, un complément de H dans G est un sous-groupe K vérifiant $G = HK$ et $H \cap K = \{1\}$.*

La notion est bien sûr symétrique en H et K.

Lemme 7.2. *Soient H et K deux sous-groupes de G.*

(i) H et K sont complémentaires si, et seulement si, l'application $H \times K \to G, (h,k) \mapsto hk$, est bijective.

14. W. Feit & J. G. Thompson, *Solvability of groups of odd order*, Pac. J. Math. 13, 775–1029 (1963).

(ii) On suppose H et K finis. On a $|HK| = |H||K|/|H \cap K|$. En particulier, H et K sont complémentaires si, et seulement si, on a $H \cap K = \{1\}$ et $|G| = |H||K|$.

Démonstration — Soit $f : H \times K \to G, (h,k) \mapsto hk$. On a bien sûr f surjective $\iff G = HK$. Pour (h,k) et (h',k') dans $H \times K$, on a aussi

$$h'k' = hk \iff h^{-1}h' = k(k')^{-1} \iff \exists x \in H \cap K \text{ avec } h' = hx \text{ et } k' = x^{-1}k.$$

On en déduit que f est injective si, et seulement si, $H \cap K = \{1\}$. On en déduit aussi que si H et K sont finis, les fibres de f ont $|H \cap K|$ éléments, ce qui montre $|KH||H \cap K| = |K||H|$. Supposant $H \cap K = \{1\}$ on a donc $|G| = |HK| \iff |G| = |H||K|$. □

Exemple 7.3. *(i) Les compléments de A_n dans S_n sont les $\langle\sigma\rangle$ avec $\sigma \in \mathrm{S}_n \smallsetminus \mathrm{A}_n$ d'ordre 2.*

(ii) Soit $S \subset \mathrm{S}_4$ le stabilisateur d'un point dans $\{1,\dots,4\}$. On a $S \simeq \mathrm{S}_3$ et S est un complément de K_4 dans S_4.

(iii) Soient G abélien p-élémentaire et H un sous-groupe de G. Les compléments de H dans G sont les supplémentaires de $H^\sharp$ dans $G^\sharp$.

(iv) Si G est cyclique d'ordre 4, disons $G = \mu_4$, le sous-groupe $H = \mu_2$ n'admet pas de complément. En effet, un complément serait d'ordre 2, mais H est l'unique sous-groupe d'ordre 2 de G.

(v) Si $G = \mathrm{H}_8$, le sous-groupe $H = \langle I\rangle \simeq \mathbb{Z}/4\mathbb{Z}$ n'admet pas de complément. En effet, un complément serait d'ordre 2, mais l'unique sous-groupe d'ordre 2 de G est $\{\pm 1\}$, qui est inclus dans H.

On s'intéresse maintenant à la structure d'un groupe G possédant deux sous-groupes[15] N et K avec N distingué dans G et K complément de N dans G. L'observation importante, à la base de toute la discussion qui suit, est que l'on peut écrire, pour tout $n, n' \in N$ et $k, k' \in K$,

$$(nk)(n'k') = n(kn'k^{-1})kk' \quad \text{avec } kn'k^{-1} \in N. \tag{22}$$

Autrement dit, on a $(nk)(n'k') = n\,\mathrm{int}_k(n')\,kk'$. Ainsi, *la structure de groupe de G se déduit de celle de N, K et de la connaissance de l'application*

$$\alpha : K \to \mathrm{Aut}(N), k \mapsto \mathrm{int}_{k|N}.$$

Noter que α est un morphisme de groupes. Cela suggère l'existence d'une construction intrinsèque de G à partir de N, K et α : c'est ce qui va nous conduire à la notion de produit semi-direct.

On oublie donc temporairement le groupe G et l'on se fixe N et K deux groupes ainsi qu'un morphisme de groupes $\alpha : K \to \mathrm{Aut}(N), k \mapsto \alpha_k$. *Insistons sur le fait que les groupes N et K, ainsi que le morphisme α, sont arbitraires.* On munit *l'ensemble produit* $N \times K$ d'une nouvelle loi $\star_\alpha$, dépendante du choix de α, par la formule

$$(n,k) \star_\alpha (n',k') := (n\,\alpha_k(n'), kk'). \tag{23}$$

15. Nous noterons désormais N ce sous-groupe distingué, plutôt que H, d'une part pour rappeler qu'il est *normal*, d'autre part car la similarité des lettres h et k au tableau crée des confusions. Bien noter que la situation n'est pas symétrique en N et K, car K n'est pas supposé distingué.

Lemme 7.4. *La loi* $\star_\alpha$ *sur l'ensemble* $N \times K$ *définie par* (23) *est une loi de groupe. Son neutre est* $(1,1)$ *et on a* $(n,k)^{-1} = (\alpha_{k^{-1}}(n^{-1}), k^{-1})$.

Démonstration — Pour le neutre, on a $(1,1) \star_\alpha (n,k) = (\alpha_1(n), k) = (n,k)$ et $(n,k) \star_\alpha (1,1) = (n\alpha_k(1), k) = (n,k)$. Pour l'associativité, c'est le calcul suivant, dans lequel on a $h, h', h'' \in H$ et $k, k', k'' \in K$: on a d'une part

$$((n,k) \star_\alpha (n,k')) \star_\alpha (n'',k'') = (n\alpha_k(n'), kk') \star_\alpha (n'',k'') = (n\alpha_k(n')\alpha_{kk'}(n''), kk'k'')$$

et d'autre part

$$(n,k) \star_\alpha ((n',k') \star_\alpha (n'',k'')) = (n,k) \star_\alpha (n'\alpha_{k'}(n''), k'k'') = (n\alpha_k(n'\alpha_{k'}(n'')), kk'k'')$$
$$= (n\alpha_k(n')\alpha_k(\alpha_{k'}(n'')), kk'k'') = (n\alpha_k(n')\alpha_{kk'}(n''), kk'k'')$$

puis l'associativité. L'assertion sur l'inverse est un simple calcul. Une autre manière de la vérifier consiste à constater que l'inverse de $(1,k)$ est $(1,k^{-1})$, l'inverse de $(n,1)$ est $(n^{-1},1)$, donc $(n,k) = (n,1)\star_\alpha(1,k)$ est nécessairement inversible d'inverse $(1,k^{-1}) \star_\alpha (n^{-1},1) = (\alpha_{k^{-1}}(n^{-1}), k^{-1})$. □

Définition 7.5. *Soient* N *et* K *deux groupes et* $\alpha : K \to \mathrm{Aut}(N)$ *un morphisme de groupes. La loi* $\star_\alpha$ *munit l'ensemble* $N \times K$ *d'une structure de groupe noté* $N \rtimes_\alpha K$ *et appelé* produit semi-direct (externe) de K par N associé à α.

Noter que dans le cas particulier $\alpha_k = \mathrm{id}_N$ pour tout k (morphisme trivial $\alpha = 1$), la loi $\star_\alpha$ est simplement la loi de groupe produit, et on a l'égalité de groupes

$$N \rtimes_1 K = N \times K.$$

Donnons un autre exemple plus intéressant.

Exemple 7.6. Soit $\alpha : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$, le morphisme défini par $\alpha_{\overline{k}}(x) = (-1)^k x$, pour $\overline{k} \in \mathbb{Z}/2\mathbb{Z}$ et $x \in \mathbb{Z}/m\mathbb{Z}$. La loi du groupe $\mathbb{Z}/n\mathbb{Z} \rtimes_\alpha \mathbb{Z}/2\mathbb{Z}$ s'écrit alors

$$(\overline{m}, \overline{k}) \star_\alpha (\overline{m'}, \overline{k'}) = (\overline{m} + (-1)^k \overline{m'}, \overline{k+k'}).$$

Pour $n \geqslant 3$, c'est un groupe non commutatif et on a un isomorphisme

$$\mathbb{Z}/n\mathbb{Z} \rtimes_\alpha \mathbb{Z}/2\mathbb{Z} \xrightarrow{\sim} \mathrm{D}_{2n}, \ (\overline{m}, \overline{k}) \mapsto c^m \tau^k.$$

En effet, la bijectivité est le fait que C et $\langle \tau \rangle$ sont compléments dans D_{2n} et le fait que c'est un morphisme est la relation $c^m \tau^k c^{m'} \tau^{k'} = c^{m+(-1)^k m'} \tau^{k+k'}$ pour $m, m', k, k' \in \mathbb{Z}$, qui se déduit de $\tau c = c^{-1}\tau$.

Revenons à la situation de la Définition 7.5 et terminons l'analyse-synthèse entamée depuis le début. Observons que $N' = N \times \{1\}$ et $K' = \{1\} \times K$ sont des sous-groupes de $N \rtimes_\alpha K$ respectivement isomorphes à N et K via $n \mapsto (n,1)$ et $k \mapsto (1,k)$. De plus, K' est un complément de N' dans $N \rtimes_\alpha K$: on a $N' \cap K' = \{(1,1)\}$ et $(n,k) = (n,1) \star_\alpha (1,k)$. Mieux, on a une suite exacte courte manifeste

$$1 \longrightarrow N \xrightarrow{n \mapsto (n,1)} N \rtimes_\alpha K \xrightarrow{(n,k) \mapsto k} K \longrightarrow 1.$$

Ainsi, N' est distingué dans $N \times_\alpha K$. Enfin, on a $(1,k) \star_\alpha (n,1) \star_\alpha (1,k)^{-1} = (\alpha_k(n), k) \star_\alpha (1,k^{-1}) = (\alpha_k(n), 1)$: on est bien retombé sur la situation initiale ! La proposition suivante conclut cette longue discussion.

PROPOSITION 7.7. *Soient G un groupe, N un sous-groupe distingué de G et K un complément de N dans G. Soit $\alpha : K \to \mathrm{Aut}(N), k \mapsto \alpha_k$, le morphisme de groupes défini par $\alpha_k(n) = knk^{-1}$. Alors la bijection $N \times K \to G$, $(n,k) \mapsto nk$, est un isomorphisme de groupes $N \rtimes_\alpha K \xrightarrow{\sim} G$.*

Noter que le morphisme α de l'énoncé est bien défini car on a $N \lhd G$. On dit aussi que G est *produit semi-direct interne* de K par N et on écrit $G = N \rtimes K$. Le morphisme α est alors sous-entendu : c'est l'action de K par conjugaison sur N.

DÉMONSTRATION — On a $f((n,k) \star_\alpha (n',k')) = f(n\alpha_k(n'), kk') = n\alpha_k(n')kk' = nkn'k^{-1}kk' = nkn'k' = f(n,k)f(n,k')$ (c'est juste l'observation initiale (22) !). □

L'Exemple 7.3 fournit déjà quelques situations de produits semi-directs internes Mentionnons que lorsqu'on ne cherche pas à préciser le choix du morphisme α dans un produit semi-direct externe, on le note (dangereusement) parfois aussi $N \rtimes K$. Une proposition utile est alors la suivante.

PROPOSITION 7.8. (Suivi des isomorphismes) *Soient G, N et K comme dans la Prop. 7.7. Soient $a : N' \xrightarrow{\sim} N$ et $b : K' \xrightarrow{\sim} K$ des isomorphismes de groupes. Alors la bijection $N' \times K' \to G, (n',k') \mapsto a(n')b(k')$ est un isomorphisme de groupes $N' \rtimes'_\alpha K' \xrightarrow{\sim} G$, où $\alpha' : K' \to \mathrm{Aut}(N'), k' \mapsto \alpha_{k'}$, est le morphisme défini par*

$$\alpha'_{k'} = a^{-1} \circ \mathrm{int}_{b(k')} \circ a, \text{ pour } k' \in K'.$$

Autrement dit, si f désigne la bijection $N' \times K' \to G$ de l'énoncé, la loi défini sur $N' \times K'$ par transport de structure de celle de G via f est la loi $\star_{\alpha'}$.

DÉMONSTRATION — La formule donnée montre $\alpha_{k'} \in \mathrm{Aut}(N)$ (composé d'isomorphismes). On a bien $\alpha'_{k'k''} = \alpha'_{k'}\alpha'_{k''}$, donc α' est un morphisme de groupes. On conclut car pour, $n, n' \in N'$ et $k, k' \in K'$, et f comme ci-dessus, on a :

$$a(n')b(k')a(n'')b(k'') = a(n')\mathrm{int}_{b(k')}(a(n''))b(k'k'') = a(n'\alpha'_{k'}(n''))b(k'k'').$$

□

EXEMPLE 7.9. On a un isomorphisme $\mathrm{S}_4 \simeq (\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathrm{S}_3$. En effet, on a $\mathrm{S}_4 = \mathrm{K}_4 \rtimes S$ (produit semi-direct interne) par l'Exemple 7.3 (iii) et la Proposition 7.7. On a $\mathrm{K}_4 \simeq (\mathbb{Z}/2\mathbb{Z})^2$ et $S \simeq \mathrm{S}_3$. Il ne serait en fait pas très difficile de voir que pour tout isomorphisme $\alpha : \mathrm{S}_3 \xrightarrow{\sim} \mathrm{Aut}((\mathbb{Z}/2\mathbb{Z})^2) = \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ on a $\mathrm{S}_4 \simeq (\mathbb{Z}/2\mathbb{Z})^2 \rtimes_\alpha \mathrm{S}_3$.

Illustrons cette discussion par une application à la classification des groupes d'ordre $2p$ avec p premier impair.

PROPOSITION 7.10. *Un groupe d'ordre $2p$ avec p premier impair est soit isomorphe à $\mathbb{Z}/p\mathbb{Z}$, soit isomorphe à D_{2p}.*

DÉMONSTRATION — Par Cauchy (Théorème 4.8 Chap. 2), il existe $c \in G$ d'ordre p et $\tau \in G$ d'ordre 2. Le sous-groupe $C = \langle c \rangle$ est d'indice 2 dans G. On a $\tau \notin C$ (car $p > 2$) et donc $G = C \coprod \tau C$, ce qui montre que $D = \langle \tau \rangle$ est un complément de C dans G. On est donc dans une situation de produit semi-direct interne $G = C \rtimes D$. On a des isomorphismes $a : \mathbb{Z}/p\mathbb{Z} \xrightarrow{\sim} C, m \mapsto c^m$, et $b : \mathbb{Z}/2\mathbb{Z} \xrightarrow{\sim} D, m \mapsto \tau^m$, de sorte que par suivi des isomorphismes on en déduit un isomorphisme

$$\mathbb{Z}/p\mathbb{Z} \rtimes_\alpha \mathbb{Z}/2\mathbb{Z} \simeq G$$

pour un certain morphisme de groupes $\alpha : \mathbb{Z}/2\mathbb{Z} \to \operatorname{Aut} \mathbb{Z}/p\mathbb{Z}$.

En fait, il n'existe que deux morphismes de groupes $\alpha : \mathbb{Z}/2\mathbb{Z} \to \operatorname{Aut} \mathbb{Z}/p\mathbb{Z}$. En effet, on rappelle qu'on a un isomorphisme de groupes $\varphi : (\mathbb{Z}/p\mathbb{Z})^\times \xrightarrow{\sim} \operatorname{Aut}(\mathbb{Z}/p\mathbb{Z}), k \mapsto \varphi_k$, défini par $\varphi_k(x) = kx$ pour $x \in \mathbb{Z}/p\mathbb{Z}$ (Prop. 3.9 Chap. 2). Mais pour $k \in (\mathbb{Z}/p\mathbb{Z})^\times$, on a $k^2 = 1$ si, et seulement si, $(k-1)(k+1) = 0$ dans le corps $\mathbb{Z}/p\mathbb{Z}$, soit encore $k = \pm 1$. On en déduit que les deux seuls morphismes de groupes $\mathbb{Z}/2\mathbb{Z} \to \operatorname{Aut} \mathbb{Z}/p\mathbb{Z}$ sont le morphisme trivial, et le morphisme envoyant $\overline{1}$ sur φ_1. Ce dernier n'est autre que le morphisme de l'Exemple 7.6. Ainsi, on a montré que l'on a soit $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (produit direct), soit $G \simeq \mathbb{Z}/p\mathbb{Z} \rtimes_\alpha \mathbb{Z}/2\mathbb{Z}$ (produit semi-direct de l'exemple ci-dessus), auquel cas on a déjà vu $G \simeq \mathrm{D}_{2p}$ (ce que l'on retrouverait aussi en appliquant cette discussion à D_{2p} lui-même !). On conclut car $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est cyclique d'ordre $2p$ (par exemple, par l'isomorphisme chinois). $\square$

⚠ Il faut être prudent avec l'écriture $N \rtimes K$ pour un produit semi-direct externe car il est très possible d'avoir $N \rtimes_{\alpha_1} K \not\simeq N \rtimes_{\alpha_2} K$ pour des choix différents de α_1 et α_2, même tous deux non triviaux, comme dans l'exemple ci-dessous.

Exemple 7.11. Soient p, q deux nombres premiers impairs distincts, et $n := pq$. Par l'isomorphisme chinois, il existe $a, b \in (\mathbb{Z}/n\mathbb{Z})^\times$ tels que $a \equiv 1 \bmod p$, $a \equiv -1 \bmod q$, $b \equiv -1 \bmod p$ et $b \equiv 1 \bmod q$. Il existe exactement 4 éléments $s \in (\mathbb{Z}/n\mathbb{Z})^\times$ tels que $s^2 = 1$, à savoir $1, a, b$ et $ab = -1$. Pour chaque tel s, il existe un unique morphisme $\alpha : \mathbb{Z}/2\mathbb{Z} \to \operatorname{Aut}(\mathbb{Z}/n\mathbb{Z})$ envoyant $\overline{1}$ sur l'automorphisme $x \mapsto sx$ de $\mathbb{Z}/n\mathbb{Z}$ (de carré 1). Notons $G_s = \mathbb{Z}/n\mathbb{Z} \rtimes_\alpha \mathbb{Z}/2\mathbb{Z}$ le produit semi-direct défini par ce α (il dépend de s). On a par exemple $G_1 = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $G_{-1} \simeq \mathrm{D}_{2n}$. Il n'est pas difficile de vérifier que le centre de G_s est de cardinal $2n$, 2, $2p$, $2q$ quand s vaut respectivement $1, -1, a, b$. Ces 4 produits semi-directs sont donc non isomorphes.

Proposition 7.12. *À isomorphisme près, les groupes non abéliens d'ordre* $\leqslant 8$ *sont* S_3, D_8 *et* H_8.

Démonstration — Un groupe d'ordre premier est cyclique, donc abélien. Un groupe non abélien d'ordre 6 est isomorphe à $\mathrm{D}_6 = \mathrm{S}_3$ (Proposition 7.10). On peut donc supposer G non abélien d'ordre 8. Alors G n'a pas d'élément d'ordre 8 (sinon il serait cyclique), et tous ses éléments ne sont pas d'ordre 2 (Exercice 3.7 Chap. 3). Il existe donc $x \in G$ d'ordre 4. Le groupe $H = \langle x \rangle$ est distingué dans G, car d'indice 2. Choisissons $y \in G \smallsetminus H$ et posons $K = \langle y \rangle$. On a $G = \langle x, y \rangle$. Comme H est distingué dans G, int_y est un automorphisme de H, il envoie donc le générateur x de $H \simeq \mathbb{Z}/4\mathbb{Z}$ sur un autre générateur, *i.e.* sur x ou x^{-1}. Le premier cas est exclus car sinon $G = \langle x, y \rangle$ serait abélien. On a donc $yxy^{-1} = x^{-1}$. Si y est d'ordre 2, alors G est produit semi-direct de $\mathbb{Z}/2\mathbb{Z}$ par $\mathbb{Z}/4\mathbb{Z}$ pour l'inversion : on a $G \simeq \mathrm{D}_8$. Sinon y est d'ordre 4. Alors y^2 est d'ordre 2 et dans H, et donc $y^2 = x^2$. Ainsi, x^2 est dans le centre de $G = \langle x, y \rangle$, et on a $yx = x^{-1}y = (x^2)xy$. On constate qu'on a un isomorphisme $\mathrm{H}_8 \xrightarrow{\sim} G$ envoyant I sur x, J sur y et $x^2 = y^2$ sur -1. $\square$

8. Complément I : Filtrations et le théorème de Jordan-Hölder

Si G est un groupe, on appelle *filtration* de G de longueur n la donnée d'une suite finie décroissante[16] $G_\bullet$ de sous-groupes

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n = \{1\}$$

avec G_{i+1} distingué dans G_i pour tout $0 \leqslant i < n$. On appelle alors *gradués* de $G_\bullet$ les n groupes quotients $\mathrm{gr}_i\, G_\bullet := G_i/G_{i+1}$ pour $0 \leqslant i < n$. Une filtration est dite *de Jordan-Hölder* si ses gradués sont des groupes simples.

Proposition 8.1. *Tout groupe fini admet une filtration de Jordan-Hölder.*

Démonstration — On procède par récurrence sur le cardinal du groupe fini G. Si G est simple, il n'y a rien à démontrer (prendre $G_0 = G$ et $G_1 = \{1\}$). Sinon, soit H un sous-groupe distingué de G de cardinal maximal et $\neq G$. Comme les sous-groupes distingués de G/H sont en bijection avec les sous-groupes distingués de G contenant H (Proposition 6.19 Chap. 2), le groupe quotient G/H est simple. Si $H_\bullet$ est une filtration de Jordan-Hölder de H, alors $G \supset H \supset H_1 \supset H_2 \cdots \supset H_n = \{1\}$ en est une de G. □

Remarque 8.2. Un groupe admet en général plusieurs filtrations de Jordan-Hölder. Par exemple, le groupe abélien p-élémentaire $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel de dimension 2, admet exactement $p+1$ sous-groupes $H \simeq \mathbb{Z}/p\mathbb{Z}$ (nécessairement distingués), et pour tous ces groupes on a $G/H \simeq \mathbb{Z}/p\mathbb{Z}$, de sorte que $G \supset H \supset \{1\}$ est de Jordan-Hölder.

Théorème 8.3. (Jordan-Hölder) *Si $G_\bullet$ et $G'_\bullet$ sont deux filtrations de Jordan-Hölder d'un même groupe G, alors elles ont même longueur, disons n, et il existe $\sigma \in \mathrm{S}_n$ tel que $\mathrm{gr}_i G_\bullet \simeq \mathrm{gr}_{\sigma(i)} G'_\bullet$ pour tout $0 \leqslant i < n$.*

En particulier, les gradués d'une filtration de Jordan-Hölder d'un groupe fini G sont bien définis à permutation et isomorphisme près : on les appelle les *facteurs de Jordan-Hölder* de G. Noter que dans le cas $G = \mathrm{S}_n$, le théorème de Jordan-Hölder découle facilement des Théorèmes 5.1 et 5.2. Ils démontrent :

Corollaire 8.4. *Pour $n \geqslant 5$, les facteurs de Jordan-Hölder de S_n sont A_n et $\mathbb{Z}/2\mathbb{Z}$. Le facteurs de Jordan-Hölder de S_4 sont $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$, et ceux de S_3 sont $\mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z}$.*

Pour démontrer le théorème de Jordan-Hölder, nous aurons besoin du lemme suivant. Soit $G_\bullet$ une filtration du groupe G. Si H est un sous-groupe de G, alors $H_i := G_i \cap H$ définit manifestement une filtration du groupe H. De plus, si H est distingué dans G, et si $\pi : G \to G/H$ est la projection canonique, alors $K_i := \pi(G_i)$ définit manifestement une filtration du groupe $K := G/H$ (Exemple 6.4 Chap. 2). Ces deux filtrations ont même longueur que $G_\bullet$ et sont dites *induites* par cette dernière. Comparons leurs gradués.

16. Il est plus souple de ne pas imposer aux G_i d'être distincts. La terminologie *suite de composition* (ou *composition series* en anglais) est parfois utilisée pour *filtration*. Nous préférons la seconde pour éviter la confusion avec les suites exactes, juste introduites. Noter enfin que les G_i avec $i > 1$ ne sont pas nécessairement distingués dans G.

LEMME 8.5. *Soient $G_\bullet$ une filtration de longueur n du groupe G, H un sous-groupe de G, ainsi que $H_\bullet$ et $K_\bullet$ les filtrations induites par $G_\bullet$ sur H et $K := G/H$. Pour tout $0 \leqslant i < n$ on a une suite exacte naturelle*

$$1 \to \mathrm{gr}_i\, H_\bullet \to \mathrm{gr}_i\, G_\bullet \to \mathrm{gr}_i\, K_\bullet \to 1.$$

DÉMONSTRATION — Soit $\pi : G \to K$ la projection canonique. Soit π_i la composé des morphismes surjectifs naturels $G_i \xrightarrow{\pi} K_i \to K_i/K_{i+1}$. On a clairement $H_i G_{i+1} \subset \ker \pi_i \subset G_i$. Précisément, pour $g \in G_i$ on a les équivalences

$$g \in \ker \pi_i \;\Leftrightarrow\; \pi(g) \in K_{i+1} \;\Leftrightarrow\; \exists g' \in G_{i+1},\ \pi(g) = \pi(g') \Leftrightarrow g \in (G_{i+1}H) \cap G_i = H_i \cap G_{i+1}.$$

Considérons le morphisme $\iota_i : H_i \to G_i/G_{i+1}, h \mapsto hG_{i+1}$. On a montré que la suite

$$H_i \xrightarrow{\iota_i} G_i/G_{i+1} \xrightarrow{\overline{\pi_i}} K_i/K_{i+1} \to 1$$

est exacte. Il ne reste qu'à voir que le noyau de ι_i est H_{i+1}. Mais c'est l'ensemble des $h \in H_i$ tels que $hG_{i+1} = G_{i+1}$, c'est donc bien $H_i \cap G_{i+1} = H_{i+1}$. □

DÉMONSTRATION — (du théorème de Jordan-Hölder) On raisonne par récurrence sur $|G|$. Il n'y a rien à démontrer si G est simple. Sinon, fixons $1 \subsetneq H \subsetneq G$ un sous-groupe distingué strict de G. Soit $G_\bullet$ une tour de Jordan-Hölder de G de longueur n, ainsi que $H_\bullet$ et $K_\bullet$ les filtrations induites par $G_\bullet$ comme ci-dessus sur H et $K = G/H$. Par hypthèse, $\mathrm{gr}_i\, G$ est simple pour tout i. La suite exacte montre donc que pour tout i, on a donc soit $\mathrm{gr}_i\, H_\bullet \simeq \mathrm{gr}_i\, G_\bullet$ (simple) et $\mathrm{gr}_i\, K_\bullet \simeq 1$, soit $\mathrm{gr}_i\, H_\bullet \simeq 1$ et $\mathrm{gr}_i\, G_\bullet \simeq \mathrm{gr}_i\, K_\bullet$ (simple). Notons I et J l'ensemble des indices i dans le premier et second cas respectivement, de sorte que $\{1, \ldots, n\} = I \coprod J$. Par hypothèse de récurrence appliquée à H et G/H, les gradués de $H_\bullet$ et $K_\bullet$ (modulo isomorphismes et permutations) ne dépendent pas de ces filtrations de H et K respectivement. La même chose vaut donc pour les gradués de G, qui sont réunion avec multiplicité, de ceux de H et de K. □

EXEMPLE 8.6. (*Où l'on retrouve ... le théorème fondamental de l'arithmétique !*) Remarquons que ce théorème appliqué à $\mathbb{Z}/n\mathbb{Z}$ redémontre l'unicité de la décomposition d'un entier en facteurs premiers. En effet, à toute écriture $n = p_1 \ldots p_r$ avec les p_i premier, on peut associer une filtration de Jordan-Hölder du groupe cyclique $\mathbb{Z}/n\mathbb{Z}$ de gradués les $\mathbb{Z}/p_i\mathbb{Z}$.

Dans le reste de ce complément, on rediscute de la notion de résolubilité en terme de filtrations à gradués abéliens. Commençons par une traduction des Propositions 6.11 et 4.4.

PROPOSITION 8.7. *Soit $1 \to H \xrightarrow{i} G \xrightarrow{\pi} K \to 1$ une suite exacte de groupes. Alors G est résoluble si, et seulement si, H et K le sont.*

Une filtration $G_\bullet$ de G est dite *normale* si on a $G_i \lhd G$ pour tout i.

PROPOSITION 8.8. *Soit G un groupe. Il y a équivalence entre :*

(i) G est résoluble,

(ii) G possède une filtration normale à gradués abéliens,

(iii) G possède une filtration à gradués abéliens.

De plus, tout groupe résoluble fini possède une filtration à gradués cycliques d'ordre premier.

Démonstration — Si G est résoluble de classe n, alors les $G_i := \mathrm{D}^i(G)$, pour $i = 0, \ldots, n$, définissent une filtration de longueur n de G à gradués $\mathrm{D}^i(G)_{\mathrm{ab}}$ abéliens. Cette filtration est normale car $\mathrm{D}^i(G)$ est caractéristique dans G pour tout i, donc distingué. Cela montre (i) $\Rightarrow$ (ii). L'implication (ii) $\Rightarrow$ (iii) est évidente. Supposons enfin que $G_\bullet$ est une filtration de longueur n de G à gradués abéliens. L'hypothèse $G_n = 1$, la Proposition 8.7 et, pour $i = 0, \ldots, n-1$, les suites exactes naturelles

$$1 \to G_{i+1} \to G_i \to \mathrm{gr}_i\, G_\bullet \to 1$$

entraînent successivement que G_{n-1}, G_{n-2}, $\ldots$, G_1, $G_0 = G$ sont résolubles. Cela montre (iii) $\Rightarrow$ (i).

Supposons maintenant G résoluble fini. Considérons une filtration de Jordan-Hölder de G. Par la Proposition 8.7, ses gradués sont résolubles. Ils sont aussi simples et finis. Mais un groupe simple résoluble H est de groupe dérivé $\mathrm{D}(H)$ trivial (sinon on aurait $\mathrm{D}^n(H) = H$ pour tout $n \geqslant 1$), donc H est abélien, puis cyclique d'ordre premier par l'Exemple 6.14. □

9. Complément II : Groupe de Galois d'un polynôme (culturel)

C'est Galois qui introduit le premier, vers 1830, la notion et la terminologie de *groupe*, dans ses recherches sur la *résolubilité par radicaux* des racines d'un polynôme P à une variable (dans la lignée de travaux de Lagrange). Informellement, on entend par là le fait de pouvoir écrire ou non les racines de P comme somme de radicaux emboités de termes dépendant simplement des coefficients de P.

Galois, tout comme Lagrange, s'intéresse aux relations de nature algébrique entre les différentes racines d'un même polynôme à une variable. De manière moderne, on considère le sous-groupe

$$\Sigma = \mathrm{Aut}(\mathbb{C}) \subset \mathrm{S}_{\mathbb{C}}$$

de tous les automorphismes du corps $\mathbb{C}$. Par exemple, la conjugaison complexe $z \mapsto \overline{z}$ est un élément de Σ, mais il y en a beaucoup d'autres, en fait, une infinité indénombrable ! Noter qu'un élément $\sigma \in \Sigma$ vérifie toujours $\sigma(x) = x$ pour $x \in \mathbb{Q}$, puis $\sigma(P(x_1, \ldots, x_n)) = P(\sigma(x_1), \ldots, \sigma(x_n))$ pour tout $P \in \mathbb{Q}[X_1, \ldots, X_n]$ et $x_1, \ldots, x_n \in \mathbb{C}$. En particulier, σ préserve l'ensemble des zéros des polynômes à coefficients rationnels.

Fixons donc $P \in \mathbb{Q}[X]$, et notons $R \subset \mathbb{C}$ l'ensemble fini de ses racines.[17] L'action naturelle de $\mathrm{Aut}(\mathbb{C})$ sur $\mathbb{C}$ préserve R, ce qui fournit un morphisme de groupes

$$\mathrm{Aut}(\mathbb{C}) \to \mathrm{S}_R.$$

L'image de ce morphisme est par définition le groupe de Galois du polynôme P. Il est noté $\mathrm{Gal}(P/\mathbb{Q})$. Autrement dit, ce sont les permutations des racines de P induites par un automorphisme du corps $\mathbb{C}$. Il est non trivial : on montre par exemple assez formellement que si P est irréductible dans $\mathbb{Q}[X]$ alors $\mathrm{Gal}(P/\mathbb{Q})$ agit transitivement sur R.

17. Si P est irréductible dans $\mathbb{Q}[X]$, alors il est premier à P' dans $\mathbb{Q}[X]$, et donc par Bezout P n'a pas de racine multiple dans $\mathbb{C}$: ainsi, P a exactement $\deg P$ racines complexes.

Exemple 9.1. En guise d'exemple, considérons $P = X^4 - 2$. On a

$$R = \{\alpha, i\alpha, -\alpha, -i\alpha\} \quad \text{avec } i^2 = -1 \text{ et } \alpha = \sqrt[4]{2}.$$

Identifions respectivement $\alpha, i\alpha, -\alpha, -i\alpha$ à $1, 2, 3, 4$, et donc $\mathrm{Gal}(P/\mathbb{Q})$ à un sous-groupe G de S_4. L'élément de G induit par la conjugaison complexe τ est la transposition $(2\,4)$, mais il y a bien d'autres éléments dans G. Par exemple, P étant irréductible dans $\mathbb{Q}[X]$ l'action de G sur $\{1, 2, 3, 4\}$ doit être transitive, et donc il doit exister $\sigma \in \mathrm{Gal}(P/\mathbb{Q})$ tel que $\sigma(\alpha) = i\alpha$. La relation $i^2 = -1$ montre $\sigma(i)^2 = -1$, puis $\sigma(i) = \pm i$. Quitte à remplacer σ par $\tau\sigma$ on peut donc supposer $\sigma(i) = i$ et $\sigma(\alpha) = i\alpha$. On constate alors que σ agit comme le 4-cycle $(1\,2\,3\,4)$, puis que G contient le groupe D_8, car on a $\mathrm{D}_8 = \langle (1\,2\,3\,4), (2\,4) \rangle$. En fait, on peut montrer $G = \mathrm{D}_8$. En effet, la relation $\sigma(-x) = -\sigma(x)$ pour tout $\sigma \in \mathrm{Aut}(\mathbb{C})$ montre que les éléments G commutent avec la double transposition $(1\,3)(2\,4)$, dont le commutant dans S_4 est en fait D_8.

Un résultat spectaculaire de Galois est le fait que P est résoluble par radicaux si, et seulement si, le groupe $\mathrm{Gal}(P/\mathbb{Q})$ est *résoluble* au sens de la Définition 6.9. Comme un polynôme générique de degré n a pour groupe de Galois S_n, et que ce dernier n'est résoluble que pour $n \leqslant 4$ (Proposition 6.7), il retrouve que le polynôme générique n'est pas résoluble par radicaux en degré $\geqslant 5$, un résultat déjà connu de Abel et Ruffini. De même, la résolubilité du groupe D_8 est compatible avec l'écriture par radicaux triviale des racines de $X^4 - 2$. Ces résultats, et bien d'autres, feront l'objet du cours d'algèbre 2. Ils constituent une motivation forte à l'étude des sous-groupes de S_n.

10. Complément III : Le groupe affine et un théorème de Galois

Soit V un espace vectoriel[18] sur un corps k. On rappelle qu'une bijection $f : V \to V$ est dite *affine* si on a, pour tout $x, y \in V$ et tout $\lambda, \mu \in k$ avec $\lambda + \mu = 1$,

$$f(\lambda x + \mu y) \;=\; \lambda f(x) + \mu f(y).$$

Alternativement, il est équivalent de demander que f est affine et :

(a) qu'il existe $\vec{f} \in \mathrm{GL}(V)$, nécessairement unique et appelée *application linéaire tangente*, vérifiant $f(x + h) = f(x) + \vec{f}(h)$ pour tout $x, h \in V$.

(b) qu'il existe $a \in \mathrm{GL}(V)$ et $b \in V$ avec $f(x) = a(x) + b$. On a alors nécessairement $a = \vec{f}$ et $b = f(0)$.

Définition 10.1. *On note* $\mathrm{Aff}(V) \subset \mathrm{S}_V$ *le sous-groupe des bijections affines* f *de* V.

Un sous-groupe important de $\mathrm{Aff}(V)$ est le sous-groupe $\mathrm{T}(V)$ constitué des translations, *i.e.* des applications de la forme $\tau_v(x) = x + v$, avec $v \in V$. L'application $v \mapsto \tau_v$ est un isomorphisme $V \simeq \mathrm{T}(V)$. Le groupe $\mathrm{Aff}(V)$ agit naturellement sur

18. Le cadre le plus clair, mais évité ici pour aller droit au but, serait en fait de se placer dans un espace affine général sous V, c'est-à-dire d'un ensemble muni d'un action libre et transitive de l'espace vectoriel V. Dans un espace affine, non seulement on ne favorise pas d'origine, mais on distingue deux groupes identifiés ici potentiellement de manière perturbante : le sous-groupe $\mathrm{GL}(V)$ de $\mathrm{Aff}(V)$ fixant 0, et le quotient $\mathrm{GL}(V)$ de $\mathrm{Aff}(V)$ des applications linéaires tangentes.

V, et ce transitivement, car c'est déjà le cas de $\mathrm{T}(V)$. Le stabilisateur de l'origine 0 de V coïncide avec $\mathrm{GL}(V)$. On a un morphisme

$$d : \mathrm{Aff}(V) \to \mathrm{GL}(V), f \mapsto \vec{f}$$

(le vérifier !). Ce morphisme d est surjectif car on a $df = f$ pour $f \in \mathrm{GL}(V)$. Son noyau est le sous-groupe $\mathrm{T}(V)$ (c'est clair sur (b)), qui est donc distingué dans $\mathrm{Aff}(V)$.

Proposition 10.2. *On a une suite exacte courte naturelle*

$$1 \longrightarrow V \xrightarrow{v \mapsto \tau_v} \mathrm{Aff}(V) \xrightarrow{d} \mathrm{GL}(V) \longrightarrow 1.$$

Le sous-groupe $\mathrm{GL}(V)$ *de* $\mathrm{Aff}(V)$ *est un complément de* $\mathrm{T}(V)$*, et on a* $\mathrm{Aff}(V) \simeq V \rtimes_\alpha \mathrm{GL}(V)$ *pour le morphisme tautologique* $\alpha : \mathrm{GL}(V) \to \mathrm{Aut}(V)$.

Démonstration — On a clairement $\mathrm{T}(V) \cap \mathrm{GL}(V) = \{1\}$ et $\mathrm{Aff}(V) = \mathrm{T}(V)\mathrm{GL}(V)$ (propriété (b)), donc $\mathrm{GL}(V)$ est un complément de $\mathrm{T}(V)$ dans $\mathrm{Aff}(V)$. Ainsi, on a $\mathrm{Aff}(V) = \mathrm{T}(V) \rtimes \mathrm{GL}(V)$ (produit semi-direct interne). Pour $g \in \mathrm{GL}(V)$ et $v \in V$ on a la formule immédiate $g\tau_v g^{-1} = \tau_{g(v)}$. On conclut par suivi des isomorphismes (Proposition 7.8 appliquée à $a : V \xrightarrow{\sim} \mathrm{T}(V), v \mapsto \tau_v$ et $b = \mathrm{id}$). □

Considérons le cas de la dimension 1. Le groupe $\mathrm{Aff}(k)$ est simplement le groupe des bijections de k de la forme $x \mapsto ax + b$ avec $a \in k^\times$ et $b \in k$. Il est dans une suite exacte $1 \to k \to \mathrm{Aff}(k) \to k^\times \to 1$, et les deux groupes k et $k^\times$ sont abéliens, on en déduit :

Corollaire 10.3. *Le groupe* $\mathrm{Aff}(k)$ *est résoluble.*

Plutôt que de développer de la géométrie affine, on se propose dans ce complément de voir comment le groupe $\mathrm{Aff}(\mathbb{Z}/p\mathbb{Z})$ intervient, suivant Galois, dans la classification des sous-groupes résolubles de S_p qui sont *transitifs*, *i.e.* agissant transitivement sur $\{1, \ldots, p\}$. Commençons par donner quelques conditions nécessaires et suffisantes simples pour qu'un sous-groupe de S_p avec p premier soit transitif.

Lemme 10.4. *Soit* G *un sous-groupe de* S_p *avec* p *premier. Les conditions suivantes sont équivalentes :*

(i) G *est transitif,*

(ii) p *divise* $|G|$,

(iii) G *contient un* p*-cycle.*

Démonstration — Soient $X = \{1, 2, \ldots, p\}$ et $x \in X$. Supposons (i). Alors l'orbite de x sous G est $\mathrm{O}_x = X$. La formule orbite-stabilisateur montre $|G| = |\mathrm{G}_x|\,|X|$, et donc p divise $|G|$. On a montré (ii). Si p divise $|G|$ alors par Cauchy G contient un élément c d'ordre p. L'ordre d'un élément de S_p étant le ppcm des longueurs de ces cycles, cela montre que c est produit de p-cycles à supports disjoints, puis c est un p-cycles car $|X| = p$. On a montré (ii) $\Longrightarrow$ (iii). L'implication (iii) $\Longrightarrow$ (ii) est évidente. □

Considérons la bijection $\{1,\dots,p\} \xrightarrow{\sim} \mathbb{Z}/p\mathbb{Z}$, $i \mapsto \bar{i}$. Elle permet d'identifier S_p avec $\mathrm{S}_{\mathbb{Z}/p\mathbb{Z}}$, et nous verrons définitivement $\mathrm{Aff}(\mathbb{Z}/p\mathbb{Z})$ comme un sous-groupe de S_p au moyen de cette identification. Par exemple, la translation $\tau(x) = x+1$ coïncide alors avec le p-cycle $(1\,2\ \dots\ p)$. Ainsi, $\mathrm{Aff}(\mathbb{Z}/p\mathbb{Z})$ est un sous-groupe résoluble et transitif de S_p. D'après la Proposition 10.2, il est de cardinal $|\mathrm{Aff}(\mathbb{Z}/p\mathbb{Z})| = p(p-1)$. On se propose de démontrer le résultat suivant, dû à Galois. [19]

Théorème 10.5. (Galois) *Soit G un sous-groupe transitif de S_p avec p premier. Il y a équivalence entre :*

(i) G est résoluble,

(ii) G possède un sous-groupe distingué d'ordre p,

(iii) G est conjugué à un sous-groupe de $\mathrm{Aff}(\mathbb{Z}/p\mathbb{Z})$,

(iv) tout élément de G fixant 2 points de $\{1,\dots,p\}$ est l'identité,

(v) on a $|G| \leqslant p(p-1)$.

Nous aurons besoin du lemme suivant.

Lemme 10.6. *Soient p premier, c un élément d'ordre p dans S_p (i.e. un p-cycle), $C = \langle c\rangle$ et $N = \{\sigma \in \mathrm{S}_p \mid \sigma C \sigma^{-1} = C\}$ le normalisateur de C dans S_p. Alors :*

(a) il existe $g \in \mathrm{S}_p$ tel que $gNg^{-1} = \mathrm{Aff}(\mathbb{Z}/p\mathbb{Z})$.

(b) le centralisateur de c dans S_p est C.

Démonstration — Quitte à remplacer c par un conjugué, on peut supposer que c est la translation $x \mapsto x+1$ via l'identification $\mathbb{Z}/p\mathbb{Z} \xrightarrow{\sim} \{1,\dots,p\}$ ci-dessus, et donc $\mathrm{T}(\mathbb{Z}/p\mathbb{Z}) = C$. Soit $\sigma \in \mathrm{S}_p$ commutant avec c. On a alors

$$\sigma(x+1) = \sigma(x) + 1, \quad \forall\, x \in \mathbb{Z}/p\mathbb{Z}.$$

On en déduit $\sigma(x) = x + \sigma(0)$, et donc $\sigma = c^k$ avec $k \equiv \sigma(0)$. Cela montre le (b). De même, supposons que $\sigma \in \mathrm{S}_p$ normalise C. Il existe $k \in (\mathbb{Z}/p\mathbb{Z})^\times$ avec $\sigma c \sigma^{-1} = c^k$, car c^k doit engendrer $\langle c\rangle$. Mais $\sigma c = c^k \sigma$ s'écrit

$$\sigma(x+1) = \sigma(x) + k, \quad \forall\, x \in \mathbb{Z}/p\mathbb{Z}.$$

Cela implique $g(x) = kx + g(0)$: on a montré $N \subset \mathrm{Aff}(\mathbb{Z}/p\mathbb{Z})$. L'autre inclusion est claire car $\mathrm{T}(\mathbb{Z}/p\mathbb{Z}) = \langle c\rangle$ est distingué dans $\mathrm{Aff}(\mathbb{Z}/p\mathbb{Z})$. □

Démonstration — (du Théorème de Galois) Montrons (i) implique (ii). Noter que G est non trivial (car transitif). Supposons G résoluble. Alors G possède un sous-groupe distingué abélien non trivial A. En effet, si on a $\mathrm{D}^n(G) = \{1\}$ et $\mathrm{D}^{n-1}(G) \neq \{1\}$, le sous-groupe $A = \mathrm{D}^{n-1}(G)$ convient (il est même caractéristique dans G). Vérifions que A agit transitivement sur $\{1,\dots,p\}$. Soient $\Omega_1,\dots,\Omega_r$ les orbites de A dans $\{1,\dots,p\}$. Les Ω_i sont permutées (transitivement) par G car A est distingué dans G : on a $gAx = gAg^{-1}gx = Agx$. En particulier, les Ω_i ont même cardinal s, et donc on a $p = rs$. Le cas $s = 1$ signifie $A = \{1\}$, qui est absurde car A est non trivial. On a donc bien $r = 1$: A agit transitivement sur $\{1,\dots,p\}$. Par le Lemme 10.4, A

19. Dans la théorie de Galois, ce résultat s'interprête notamment en disant que si un polynôme $P \in \mathbb{Q}[X]$ de degré premier est résoluble par radicaux, alors chaque racine de P s'exprime comme un polynôme à coefficients rationnels en deux quelconques des racines de P.

contient donc un p-cycle c de S_p. Mais le commutant de c est $\langle c \rangle$ par le Lemme 10.6 (b). On a donc $A = \langle c \rangle$ car A est abélien : on a montré le (ii).

L'implication (ii) $\Longrightarrow$ (iii) se déduit des Lemmes 10.4 et 10.6 (a).

L'implication (iii) $\Longrightarrow$ (iv) est une propriété générale de l'action naturelle de $\mathrm{Aff}(k)$ sur k. En effet, si l'équation $ax + b = x$ admet deux solutions $x \in k$, c'est qu'on a $b = 0$ et $a = 1$.

Pour l'implication (iv) $\Longrightarrow$ (v), on observe d'abord que l'application $G \to \{1, \ldots, p\} \times \{1, \ldots, p\}, g \mapsto (g(1), g(2))$, est injective par l'hypothèse. Son image est incluse dans le sous-ensemble X des couples (i, j) avec $j \neq i$. On on conclut car on a $|X| = p(p-1)$.

Montrons (iv) $\Longrightarrow$ (v). On sait que p divise $|G|$ car G est transitif. De plus, l'hypothèse (iv) implique que pour $i \in \{1, \ldots, p\}$, le stabilisateur G_i agit librement sur $\{1, \ldots, p\} \backslash \{i\}$, et donc $|G_i|$ divise $p - 1$ par l'Exercice 4.18. On en déduit que $|G| = p|G_i|$ divise $p(p-1)$.

Montrons enfin (v) $\Longrightarrow$ (ii). Soit C un sous-groupe cyclique d'ordre p de G (Lemme 10.4). Il suffit de montrer que C est distingué dans G. Sinon, il existe $g \in G$ tel que $C' := gCg^{-1}$ est distinct de C. On a donc $C \cap C' = \{1\}$ (c'est un sous-groupe strict de $C \simeq \mathbb{Z}/p\mathbb{Z}$). Mézalor l'application $C \times C' \to G, (c, c') \mapsto cc'$ est injective, et donc on a $|CC'| = p^2$. C'est absurde car on a $|G| \leqslant p(p-1)$ et $CC' \subset G$. $\square$

Au passage, nous en déduisons le :

Corollaire 10.7. *Si p est premier, il existe à isomorphisme près, une et une seule action transitive de S_p sur un ensemble à $(p-2)!$ éléments. Elle a pour stabilisateurs les conjugués de $\mathrm{Aff}(\mathbb{Z}/p\mathbb{Z})$.*

Démonstration — D'après la classification des actions transitives, il suffit de montrer la seconde assertion. Mais un tel stabilisateur H est d'ordre $p(p-1)$. Par le Lemme 10.4, il agit transitivement sur $\{1, \ldots, p\}$. On conclut d'après le (v) $\Longrightarrow$ (iii) du Théorème. $\square$

Dans le cas $p = 5$ on retrouve l'existence, et surtout l'unicité jusqu'alors laissée de côté !, de l'action exotique de S_5 sur 6 éléments :

Corollaire 10.8. *À isomorphisme près, il existe une unique action transitive de S_5 sur un ensemble à 6 éléments. Le groupe affine $\mathrm{Aff}(\mathbb{Z}/5\mathbb{Z})$ en est un stabilisateur.*

11. Exercices

EXERCICE 4.1. *Montrer que le centre de* S_n *est trivial pour* $n > 2$.

EXERCICE 4.2. *Soit* $n \geqslant 2$ *un entier.*

(i) Montrer qu'il existe un unique morphisme non trivial $\mathrm{S}_n \to \{\pm 1\}$.

(ii) En déduire que A_n *est le seul sous-groupe d'indice* 2 *de* S_n.

EXERCICE 4.3. *Soit* G *un sous-groupe de* S_n *contenant une transposition.*

(i) Montrer $G = \mathrm{S}_n$ *si, et seulement si,* G *agit* 2*-transitivement sur* $\{1, \ldots, n\}$.

(ii) On suppose que G *contient un* n*-cycle et un* $n-1$ *cycle. Montrer* $G = \mathrm{S}_n$.

EXERCICE 4.4. *Soit* $T \subset \mathrm{S}_n$ *un sous-ensemble constitué de transpositions. On note* $\mathscr{G}$ *le graphe dont les sommets sont les éléments de* $\{1, \ldots, n\}$ *et dont les arètes sont les* $\{i, j\}$ *avec* $(i\, j) \in T$. *Montrer l'équivalence entre :*

(a) *l'ensemble* T *engendre* S_n,

(b) *le graphe* $\mathscr{G}$ *est connexe.*[20]

On pourra d'abord montrer que si $X = \{x_1, \ldots, x_m\}$ *est un ensemble fini avec* $x_i \neq x_{i+1}$ *pour* $1 \leqslant i < m$,[21] *les transpositions* $(x_i\ x_{i+1})$ *avec* $1 \leqslant i < m$ *engendrent* S_X.

EXERCICE 4.5. *(i) Montrer que tout morphisme* $\mathrm{A}_n \to \{\pm 1\}$ *est trivial.*

(ii) En déduire que A_4 *ne possède pas de sous-groupe d'ordre* 6.

EXERCICE 4.6. *Montrer que les* 3*-cycles* $(i\ i+1\ i+2)$ *avec* $1 \leqslant i < n-1$ *engendrent* A_n. *On pourra commencer par les cas* $n \leqslant 4$.

EXERCICE 4.7. *Soient* c *un cycle de longueur* m *dans* S_n, $k \in \mathbb{Z}$ *et* $d = (m, k)$. *Montrer que* c^k *est produit de* m/d *cycles de longueurs* d *et à supports disjoints.*

EXERCICE 4.8. *(i) Montrer que si* p *est un nombre premier, alors une transposition et un* p*-cycle quelconques engendrent* S_p.

(ii) Donner un contre-exemple pour $p = 4$.

EXERCICE 4.9. *Montrer que le* n*-cycle* $(1\, 2 \cdots n)$ *et la transposition* $(i\, j)$ *engendrent* S_n *si, et seulement si, on a* $(i - j, n) = 1$.

EXERCICE 4.10. *Soit* p *un nombre premier. On se propose de montrer qu'il existe exactement* $(p-2)!$ *sous-groupes d'ordre* p *dans* S_p. *Soit* $\sigma \in \mathrm{S}_p$ *d'ordre* p.

---

20. Un graphe d'ensemble de sommets S et d'ensemble d'arètes $\mathscr{A}$ (un ensemble de parties à 2 éléments de S) est dit *connexe* si pour tout couple de sommets distincts $s, s' \in S$, il existe $m \geqslant 1$ et une suite d'arètes $A_1, \ldots, A_m \in \mathscr{A}$, telle que $s \in A_1$, $s' \in A_m$ et $A_i \cap A_{i+1} \neq \varnothing$ pour $1 \leqslant i < m$. On vérifie aisément qu'un graphe de sommets S est connexe si, et seulement si, il n'existe aucune partition $S = S_1 \coprod S_2$ avec S_1 et S_2 non vides, telle que toute arète du graphe est soit incluse dans S_1, soit incluse dans S_2.

21. Noter que l'on ne suppose pas les x_i tous distincts a priori.

(i) Montrer que σ est un p-cycle.

(ii) Montrer qu'il existe un unique p-cycle $c \in \langle \sigma \rangle$ tel que $c(1) = 2$.

(iii) Conclure.

Exercice 4.11. *Soient G, H, K trois groupes avec $H \lhd K$ et $K \lhd G$.*

(i) En examinant A_4, montrer que l'on n'a pas nécessairement $H \lhd G$.

(ii) On suppose H caractéristique dans K. Montrer $H \lhd G$.

Exercice 4.12. (Quelques centralisateurs)

(i) Soit c un cycle de longueur k dans S_n, $S \subset \{1, \ldots, n\}$ le support de c, et C le centralisateur de c dans S_n. Montrer que C est produit direct interne de $\langle c \rangle$ et du sous-groupe $\simeq \mathrm{S}_{n-k}$ des éléments de S_n à support dans $\{1, \ldots, n\} \smallsetminus S$.

(ii) Déterminer le centralisateur de $(1\,2)$, $(1\,2\,3)$, $(1\,2\,3\,4)$ et $(1\,2)(3\,4)$ dans S_4.

Exercice 4.13. (Classes de conjugaison de A_n) *Soit $\sigma \in \mathrm{A}_n$. On dira que σ est* non spécial *s'il existe $\tau \in \mathrm{S}_n$ avec $\tau\sigma = \sigma\tau$ et $\varepsilon(\tau) = -1$, et qu'il est* spécial *sinon.*

(i) Montrer que σ est non spécial si, et seulement si, il existe une σ-orbite de cardinal pair ou deux σ-orbites de même cardinal impair.

(ii) Montrer que si σ est non spécial, on a $\mathrm{Conj}_{\mathrm{S}_n}(\sigma) = \mathrm{Conj}_{\mathrm{A}_n}(\sigma)$.

(iii) On suppose σ spécial et $s \in \mathrm{S}_n \smallsetminus \mathrm{A}_n$. Montrer

$$\mathrm{Conj}_{\mathrm{S}_n}(\sigma) = \mathrm{Conj}_{\mathrm{A}_n}(\sigma) \coprod \mathrm{Conj}_{\mathrm{A}_n}(s\sigma s^{-1}).$$

(iv) En déduire des représentants des classes de conjugaison de A_4 et A_5.

Exercice 4.14. (Une présentation de S_n) *Pour $n \geqslant 2$ et $1 \leqslant i \leqslant j < n$ on définit $m_{i,j}$ en posant $m_{i,i} = 2$, $m_{i,j} = 3$ pour $j = i+1$, et $m_{i,j} = 0$ sinon. Soit G un groupe engendré par des éléments $s_1, \ldots, s_{n-1}$ vérifiant*

$$(s_i s_j)^{m_{i,j}} = 1 \text{ pour tout } 1 \leqslant i \leqslant j < n.$$

(i) Vérifier que pour tout $1 \leqslant i, j < n$ on a $s_i^2 = 1$, $s_i s_j = s_j s_i$ pour $|j - i| > 1$, ainsi que $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$ (relation de tresse) *pour $i < n-1$.*

(ii) On pose $f_i = s_i s_{i+1} \cdots s_n$ pour $1 \leqslant i < n$, et $f_n = 1$. Montrer que pour tout $g \in G$, il existe $1 \leqslant i \leqslant n$ et $h \in \langle s_1, \ldots, s_{n-2} \rangle$ vérifiant $g = f_i\, h$.

(iii) En déduire que G est fini de cardinal $\leqslant n!$.

(iv) Montrer[22] $\mathrm{S}_n \simeq \langle s_1, \ldots, s_{n-1} \mid (s_i\, s_j)^{m_{i,j}} = 1,\ 1 \leqslant i \leqslant j < n \rangle$.

On rappelle que le *taquin* est un jeu constitué d'un carré 4×4, lui-même constitué de 15 cases 1×1 mobiles numérotées de 1 à 15, et d'une case vide. Partant de la configuration initiale indiquée à gauche ci-dessous, et en déplaçant d'une case autant de fois qu'on le souhaite la case vide, on se trouve donc dans un état du jeu comme celui représenté à droite :

22. Cette question utilise la notion de groupe défini par générateurs et relations vue dans le complément §8 Chap. 2.

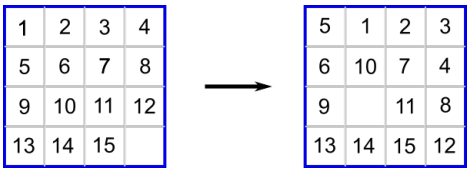
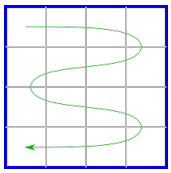


FIGURE 2. Le jeu de taquin

EXERCICE 4.15. (Taquin et serpents[23]) *Notons $\mathscr{E}$ l'ensemble des états possibles du jeu de Taquin. À chaque état $E \in \mathscr{E}$ on associe son* serpent $\mathrm{s}(E)$ *qui est la suite $(x_1, x_2, \ldots, x_{15})$ de tous les nombres de 1 à 15 obtenue en lisant le taquin dans l'ordre indiqué ci-dessous et en omettant la case vide :*



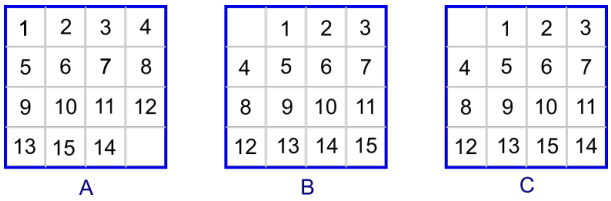
Par exemple, si $E_0 \in \mathscr{E}$ désigne l'état initial du jeu, son serpent est la suite $\mathrm{s}(E_0) = (1, 2, 3, 4, 8, 7, 6, 5, 9, 10, 11, 12, 15, 14, 13)$. Pour $E \in \mathscr{E}$ et $\mathrm{s}(E) = (x_1, x_2, \ldots, x_{15})$, on note aussi $\sigma(E)$ l'unique élément de S_{15} tel que $x_i = \sigma(i)$.

(i) Soient $E, F \in \mathscr{E}$ tels que F est obtenu à partir de E et d'un seul déplacement de la case vide. Vérifier que l'élément $\sigma(E)^{-1}\sigma(F) \in \mathrm{S}_{15}$ ne dépend que des positions originale et finale de la case vide (et non de E), et donner son type.

(ii) (Problème de Loyd) *Est-ce que le dessin* A *ci-dessous est dans $\mathscr{E}$?*

(iii) Déterminer $\{\sigma(E)^{-1}\sigma(F) \mid E, F \in \mathscr{E}\} \subset \mathrm{S}_{15}$.

(iv) Parmi les dessins B *et* C *ci-dessous, lequel est dans $\mathscr{E}$?*



(v) Montrer $|\mathscr{E}| = \frac{16!}{2}$.

EXERCICE 4.16. (Invariances de la signature) *Soit X un ensemble fini non vide.*

(i) Soient $\sigma \in \mathrm{S}_X$ et $f : \{1, \ldots, n\} \to X$ une bijection. Montrer que l'élément $\varepsilon(\sigma) := \varepsilon(f^{-1} \circ \sigma \circ f)$ de $\{\pm 1\}$ ne dépend pas du choix de f.

(ii) (suite) Vérifier que $\varepsilon : \mathrm{S}_X \to \{\pm 1\}$ est un morphisme de groupes et en déduire une définition inambiguë de A_X (groupe alterné de X).

(iii) Soient $Y \subset X$ un sous-ensemble, $\sigma \in \mathrm{S}_X$ à support dans Y, et $\tau = \sigma_{|Y} \in \mathrm{S}_Y$ la permutation associée. Vérifier $\varepsilon(\sigma) = \varepsilon(\tau)$.

EXERCICE 4.17. *Soit G un groupe simple fini d'ordre pair. En considérant la signature de l'action de G sur lui-même par translation, montrer $|G| \equiv 0 \bmod 4$, ou $G \simeq \mathbb{Z}/2\mathbb{Z}$.*

23. A. F. Archer, A modern treatment of the 15-puzzle, American Math. Monthly 106 (1999).

EXERCICE 4.18. *Soit G un groupe fini agissant sur un ensemble fini à $n \geqslant 1$ éléments.*

(i) On suppose l'action transitive. Montrer que n divise $|G|$.

(ii) On suppose l'action fidèle. Montrer que $|G|$ divise $n!$.

(iii) On suppose l'action libre. Montrer que $|G|$ divise n.

EXERCICE 4.19. *Soient $n \geqslant 1$ un entier et G cyclique d'ordre n.*

(i) Pour tout diviseur d de n, définir une action transitive de G sur un ensemble à d éléments.

(ii) Montrer que toute action transitive de G est isomorphe à une et une seule des actions définies au (i).

EXERCICE 4.20. *Montrer qu'à isomorphisme près, il existe exactement 4 actions transitives du groupe S_3 : l'action triviale sur $\{1\}$, une action à déterminer sur $\{1, -1\}$, l'action naturelle sur $\{1, 2, 3\}$, et l'action de Cayley.*

Nous renvoyons au sujet du partiel 2021-2022 (§1 App. B) pour une classification des actions transitives de S_4 sur 6 éléments.

EXERCICE 4.21. *(i) Exhiber un sous-groupe de S_6 isomorphe à S_3 et agissant transitivement sur $\{1, 2, 3, 4, 5, 6\}$.*

(ii) Exhiber un sous-groupe de S_8 isomorphe à H_8.

(iii) Montrer que pour $n < 8$, aucun sous-groupe de S_n n'est isomorphe à H_8.

EXERCICE 4.22. *Soient G un groupe fini et p le plus petit facteur premier de $|G|$.*

(i) On suppose que G agit sur un ensemble X à p éléments. Montrer que G_x agit trivialement sur X pour tout $x \in X$.

(ii) En déduire qu'un sous-groupe de G d'indice p est distingué (Lemme de Ore).

EXERCICE 4.23. *Soient G un groupe agissant sur X, $k \geqslant 1$ un entier, et $x \in X$.*

(i) Montrer que G agit $k+1$-transitivement sur X si, et seulement si, G agit transitivement sur X et G_x agit k-transitivement sur $X \smallsetminus \{x\}$.

(ii) En déduire que si G est fini, et agit k-transitivement sur X, alors l'entier $|X|(|X|-1)(|X|-2)\cdots(|X|-k+1)$ divise $|G|$.

(iii) Montrer que si un sous-groupe $G \subset \mathrm{S}_n$ agit $(n-2)$-transitivement sur $\{1, \ldots, n\}$, alors on a $G = \mathrm{A}_n$ ou $G = \mathrm{S}_n$.

EXERCICE 4.24. (Un sous-groupe 3-transitif de S_6 isomorphe à S_5) *Soit G le sous-groupe de S_6 engendré par $(1\,2\,3\,4\,5)$ et $(1\,2)(3\,6)(5\,4)$.*

(i) Montrer que l'action naturelle de G sur $\{1, 2, \ldots, 6\}$ est 3-transitive.

(ii) En déduire que l'action de S_5 sur les pentagones mystiques est fidèle, et que l'on a $G \simeq \mathrm{S}_5$.

L'exercice ci-dessous est inspiré de l'article *Three lectures on exceptionnal groups*, de J. Conway (1993).

Exercice 4.25. (*Le groupe de Mathieu* M_{11}) *Soit* M_{11} *le sous-groupe de* A_{11} *engendré par les éléments* $a = (1\,2\,3\,4\,5\,6\,7\,8\,9\,10\,11)$ *et* $b = (3\,7\,11\,8)(4\,10\,5\,6)$.

(i) Montrer que M_{11} *possède des éléments de type* 11, $1\,2\,8$, $1\,5^2$, $1^2\,3^3$ *et* $1^3\,4^2$. *Pour cela, on pourra vérifier les égalités* $b^2a = (1\,2\,11)(3\,5\,10)(6\,8\,9)$,

$$aba^{-1}b^{-1} = (1\,9\,4\,7\,3)(5\,10\,8\,6\,11) \quad \text{et} \quad aba = (1\,3\,11\,2\,8\,10\,9\,6)(4\,7).$$

(ii) En déduire (sans calcul) que M_{11} *agit* 3*-transitivement sur* $\{1, \ldots, 11\}$.

Soit $E = \{1, \ldots, 11\}$. *Pour* $F \subset E$ *on pose* $G_F = \{g \in \mathrm{M}_{11} \mid g(F) = F\}$.

(iii) Montrer (sans calcul) que si $F \subset E$ *a trois éléments, alors* G_F *agit transitivement sur* $E \smallsetminus F$. *En déduire que* M_{11} *agit transitivement sur l'ensemble des parties à* 4 *éléments de* E.

(iv) Soient $F \subset E$ *avec* $|F| = 4$, *et* $f : G_F \to \mathrm{S}_F$ *le morphisme naturel. Montrer (sans calcul) que* $f(G_F)$ *contient un* 4*-cycle et un* 3*-cycle.*

(v) (suite) En déduire $f(G_F) = \mathrm{S}_F$.

(vi) Montrer que M_{11} *agit* 4*-transitivement sur* $\{1, 2, \ldots, 11\}$, *puis montrer que* $|\mathrm{M}_{11}|$ *est multiple de* $\frac{11!}{7!} = 7920$.

Mathieu a démontré l'égalité $|\mathrm{M}_{11}| = 7920$ et que M_{11} *est simple* : c'est le plus petit des groupes simples dits *sporadiques*. Mathieu a en fait construit explicitement, entre 1861 et 1873, 5 groupes simples $\mathrm{M}_n \subset \mathrm{S}_n$, pour $n = 11, 12, 22, 23$ et 24. La détermination de leur cardinal fut un temps controversée, ou même simplement le fait qu'ils ne sont pas égaux à A_n.

Exercice 4.26. *Soient* G *un groupe et* H *un sous-groupe de* G. *On note* $\bullet$ *l'action par translations de* G *sur* G/H *et* $N = \mathrm{N}_G(H)$ *le normalisateur de* H.

(i) Montrer que pour tout $n \in N$, *l'application* $G/H \to G/H, gH \mapsto gHn$, *définit bien un isomorphisme* $(G/H, \bullet)$ *dans lui-même (ou* automorphisme*).*

(ii) Montrer que le groupe des automorphismes de $(G/H, \bullet)$ *est naturellement isomorphe à* N/H.

Exercice 4.27. *Soient* G *un groupe, et* $\bullet$ *et* $\star$ *des actions de* G *sur des ensembles* X *et* Y. *Soit* $X = \coprod_{i \in I} X_i$ *la partition en orbites de* X, *et* $Y = \coprod_{j \in J} Y_j$ *celle de* Y.

(i) Soit $f : (X, \bullet) \to (Y, \star)$ *un isomorphisme d'actions. Montrer que pour tout* $i \in I$, *il existe un unique* $j \in J$ *vérifiant* $f(X_i) = Y_j$. *On pose* $\varphi(i) := j$.

(ii) (suite) Montrer que $\varphi : I \to J$ *est bijective, et que pour tout* $i \in I$, *les actions* $(X_i, \bullet)$ *et* $(Y_{\varphi(i)}, \star)$ *de* G *sont transitives et isomorphes.*

(iii) On suppose réciproquement qu'il existe une bijection $\varphi : I \to J$, *et pour tout* $i \in I$ *un isomorphisme* $f_i : (X_i, \bullet) \to (Y_{\varphi(i)}, \star)$. *Montrer que* $(X, \bullet)$ *est* $(Y, \star)$ *sont isomorphes.*

On donne maintenant quelques exercices sur les notions de commutateur et groupe dérivé.

Exercice 4.28. *Soient* G *un groupe,* $g \in G$ *d'ordre fini* n, *et* $i, j \in \mathbb{Z}$ *tels que* g^i *et* g^j *sont conjugués dans* G.

(i) On suppose $j - i = \pm 1$. Montrer que g est un commutateur dans G.
(ii) On suppose $(j - i, n) = 1$. Montrer $g \in \mathrm{D}(G)$.

EXERCICE 4.29. *Soit G un groupe. Montrer que tout sous-groupe de G contenant $\mathrm{D}(G)$ est distingué dans G.*

Dans l'exercice suivant, on note ${}^h g$ l'élément hgh^{-1}.

EXERCICE 4.30. *Soient G un groupe et $x, y, z \in G$.*
(i) Montrer $[x, y]^{-1} = [y, x]$, $[x, yz] = [x, y]\, {}^y[x, z]$ et $[xy, z] = [y, z]\, {}^x[x\, z]$.
(ii) En déduire $[x, y^n] = [x, y]\, {}^y[x, y]\, {}^{y^2}[x, y] \cdots {}^{y^{n-1}}[x, y]$ pour tout $n \geqslant 1$.

EXERCICE 4.31. *(i) Déterminer le groupe dérivé et l'abélianisé de H_8.*
(ii) Déterminer le groupe dérivé et l'abélianisé de D_{2n}.

EXERCICE 4.32. *(i) On se donne $n \geqslant 1$ et une suite exacte de groupes*

$$1 \longrightarrow G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} \cdots \xrightarrow{f_{n-1}} G_n \longrightarrow 1.$$

On suppose que les G_i sont finis pour tout i. Montrer $\prod_{i=1}^n |G_i|^{(-1)^i} = 1$.
(ii) Soient G un groupe abélien fini et $n \geqslant 1$ un entier. On rappelle les sous-groupes $G[n] = \{g \in G \mid g^n = 1\}$ et $G^{(n)} = \{g^n \mid g \in G\}$ de G. Montrer

$$|G[n]| = |G/G^{(n)}|$$

sans utiliser le théorème de structure.

Dans les exercices suivants, k est un corps fixé.

EXERCICE 4.33. *Montrer que l'action de $\mathrm{GL}_2(k)$ sur $\mathbb{P}(k^2)$ est 3-transitive.*

Soit $n \geqslant 1$. On rappelle que $\mathrm{T}_n(k) \subset \mathrm{GL}_n(k)$ désigne le sous-groupe des matrices triangulaires supérieures, et $\mathrm{U}_n(k) \subset \mathrm{T}_n(k)$ celui des matrices unipotentes supérieures (coefficients égaux à 1 sur la diagonale). Pour $i < j$ et $x \in k$ on note $\mathrm{e}_{i,j}(x)$ la matrice $m \in \mathrm{U}_n(k)$ vérifiant $m_{i,j} = x$ et $m_{p,q} = 0$ pour $p < q$ et $(p, q) \neq (i, j)$. On pose aussi $\mathrm{e}_{i,j} = \mathrm{e}_{i,j}(1)$.

EXERCICE 4.34. *(i) Montrer que les $\mathrm{e}_{i,j}(x)$ avec $1 \leqslant i < j \leqslant n$ et $x \in k$ engendrent $\mathrm{U}_n(k)$.*
(ii) Déterminer le centre de $\mathrm{T}_n(k)$ et celui de $\mathrm{U}_n(k)$.

EXERCICE 4.35. *(i) Montrer $\mathrm{D}(\mathrm{T}_n(k)) = \mathrm{U}_n(k)$ pour $k \neq \mathbb{Z}/2\mathbb{Z}$.*
(ii) Montrer $[\mathrm{e}_{i,i+2^m}, \mathrm{e}_{i+2^m,i+2^{m+1}}] = \mathrm{e}_{i,i+2^{m+1}}$ pour $m \geqslant 0$ et $1 \leqslant i + 2^{m+1} \leqslant n$.
(iii) En déduire $\mathrm{e}_{i,j} \in \mathrm{D}^m(\mathrm{U}_n(k))$ pour $1 \leqslant i < j \leqslant n$ et $i \equiv j \bmod 2^m$.
(iv) Montrer que $\mathrm{U}_n(k)$ est de classe $1 + \lfloor \log_2(n-1) \rfloor = \lceil \log_2 n \rceil$ pour $n \geqslant 2$.

Soit V un k-espace vectoriel de dimension $n \geqslant 1$. On appelle *drapeau complet* de V la donnée d'une suite croissante de sous-espaces $\{0\} = V_0 \subset V_1 \subset \cdots \subset V_n = V$ avec $\dim V_i = i$ pour tout i. Le *drapeau standard* de $V = k^n$ est le drapeau défini pour $1 \leqslant i \leqslant n$ par $V_i = \mathrm{Vect}(e_1, \ldots, e_i)$, où e_i est la base canonique de k^n.

Exercice 4.36. *Soit $\mathscr{F}$ l'ensemble des drapeaux complets de V.*

(i) Montrer que l'action naturelle de $\mathrm{GL}(V)$ sur $\mathscr{F}$ est transitive.

(ii) Quel est le stabilisateur du drapeau standard de k^n ?

(iii) En déduire que pour G un sous-groupe de $\mathrm{GL}_n(k)$, il y a équivalence entre :

(a) G préserve un drapeau complet de k^n,

(b) il existe $p \in \mathrm{GL}_n(k)$ tel que $p\,G\,p^{-1} \subset \mathrm{T}_n(k)$ (G est co-trigonalisable).

Exercice 4.37. (Le théorème de Lie-Kolchin) *Soient $n \geqslant 1$ et G un sous-groupe résoluble connexe de $\mathrm{GL}_n(\mathbb{C})$. On se propose de montrer que G est co-trigonalisable. On raisonne par récurrence sur $n + r$ où r est la classe de résolubilité de G.*

(i) Montrer que $\mathrm{D}(G)$ est connexe.

(ii) Montrer que $\mathrm{D}(G)$ est inclus dans $\mathrm{SL}_n(\mathbb{C})$.

(iii) Conclure si $\mathrm{D}(G)$ est constitué d'homothéties.

(iv) Conclure s'il existe un sous-espace $\{0\} \subsetneq W \subsetneq \mathbb{C}^n$ avec $g(W) \subset W$ pour tout $g \in G$.

Soit $\mathscr{C} = \widehat{\mathrm{D}(G)}$. Pour un caractère $\chi \in \mathscr{C}$ on considère le sous-espace vectoriel

$$V_\chi = \{v \in \mathbb{C}^n \mid g(v) = \chi(g)v, \ \ \forall g \in \mathrm{D}(G)\}.$$

On pose $S = \{\chi \in \mathscr{C} \mid V_\chi \neq 0\}$ et $V = \sum_{\chi \in S} V_\chi$.

(v) Montrer $S \neq \varnothing$.

(vi) Montrer $V = \oplus_{\chi \in S} V_\chi$.

(vii) En déduire que S est fini.

Pour $g \in G$ et $\chi \in \mathscr{C}$ on pose ${}^g\chi : \mathrm{D}(G) \to \mathbb{C}^\times, x \mapsto \chi(g^{-1}xg)$.

(viii) Montrer que $(g, \chi) \mapsto {}^g\chi$ est une action de G sur $\mathscr{C}$, et vérifier $g(V_\chi) = V_{{}^g\chi}$.

(ix) (suite) En déduire que cette action de G sur S est triviale.

(x) Conclure.

(xi) Donner un contre-exemple dans le cas $n = 2$ pour G non connexe.

On termine par quelques exercices sur le produit semi-direct.

Exercice 4.38. *Déterminer le centre des groupes G_s définis dans l'Exemple 7.11.*

Le titre de l'exercice suivant est évidemment provocateur.

Exercice 4.39. (Tout automorphisme est intérieur) *Soient G un groupe et $\alpha \in \mathrm{Aut}(G)$. Montrer qu'il existe un groupe G', un morphisme injectif $f : G \to G'$ et un élément $x \in G'$, tels que pour tout $g \in G$ on a $f(\alpha(g)) = xf(g)x^{-1}$.*

Exercice 4.40. (Groupes d'ordre pq) *Soient p et q deux nombres premiers avec $p < q$, et G un groupe d'ordre pq.*

(i) Montrer que G possède un sous-groupe d'ordre p et un sous-groupe distingué d'ordre q.

(ii) On suppose que p ne divise pas $q - 1$. Montrer $G \simeq \mathbb{Z}/pq\mathbb{Z}$.

(iii) On suppose que p divise $q-1$. Montrer qu'il existe un groupe non abélien $\Gamma_{p,q}$ d'ordre pq.

(iv) (suite) Montrer que l'on a soit $G \simeq \mathbb{Z}/pq\mathbb{Z}$, soit $G \simeq \Gamma_{p,q}$.

(v) (suite) Exhiber un sous-groupe de $\mathrm{GL}_p(\mathbb{C})$ isomorphe à $\Gamma_{p,q}$.

Dans les deux exercices suivants on étend la définition de D_{2n} à $1 \leqslant n \leqslant 2$ en posant $\mathrm{D}_2 = \mathbb{Z}/2\mathbb{Z}$ et $\mathrm{D}_4 := \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Avec cette définition, on constate que l'on a $\mathrm{D}_{2n} \simeq \mathbb{Z}/n\mathbb{Z} \rtimes_\alpha \mathbb{Z}/2\mathbb{Z}$ pour tout entier $n \geqslant 1$, où α est comme dans l'Exemple 7.6. De plus, l'Exercice 4.42 utilise la notion de groupe défini par générateurs et relations vue dans le complément §8 Chap. 2.

Exercice 4.41. *Soient $m, n \geqslant 1$ des entiers. Montrer que D_{2m} possède un sous-groupe isomorphe à D_{2n} si, et seulement si, on a $n|m$.*

Exercice 4.42. *Montrer $\mathrm{D}_{2n} \simeq \langle\, s,\, t \mid s^2 = t^2 = (st)^n = 1 \,\rangle$ pour tout $n \geqslant 1$.*

Exercice 4.43. *Soit $n \geqslant 2$ un entier. L'action de S_n sur $\{1, \ldots, n\}$ induit un morphisme $\alpha : \mathrm{S}_n \to \mathrm{Aut}((\mathbb{Z}/2\mathbb{Z})^n)$ par permutation des coordonnées, et on pose*

$$G_n = (\mathbb{Z}/2\mathbb{Z})^n \rtimes_\alpha \mathrm{S}_n.$$

On introduit aussi $\varphi : (\mathbb{Z}/2\mathbb{Z})^n \to \mathbb{Z}/2\mathbb{Z}$ le morphisme de groupes $\varphi(x_1, \ldots, x_n) = \sum_{i=1}^n x_i$, son noyau $H_n = \ker \varphi$ et l'élément $e := (1, 1, \ldots, 1) \in (\mathbb{Z}/2\mathbb{Z})^n$.

(i) Déterminer le centre de G_n.

(ii) Soit $V \subset (\mathbb{Z}/2\mathbb{Z})^n$ un sous-groupe vérifiant $\alpha_\sigma(V) \subset V$ pour tout $\sigma \in \mathrm{S}_n$. Montrer que l'on a soit $V \subset \langle e \rangle$, soit $H_n \subset V$.

(iii) Vérifier que l'application $G_n \to \mathbb{Z}/2\mathbb{Z} \times \mathrm{S}_n$ envoyant (v, σ) sur $(\varphi(v), \sigma)$ est un morphisme de groupes.

(iv) Montrer que le sous-groupe dérivé de G_n est $H_n \rtimes_\alpha \mathrm{A}_n$.

(v) Pour quels entiers n est-ce que G_n est résoluble ?

(vi) Montrer que $H_n \rtimes_\alpha \mathrm{S}_n$ agit sur H_n via $((v, \sigma), w) \mapsto v + \sigma(w)$, et que cette action est fidèle pour $n \geqslant 3$.

(vii) (suite) En déduire $H_3 \rtimes_\alpha \mathrm{S}_3 \simeq \mathrm{S}_4$.

Exercice 4.44. (Groupe diédral infini) *Soient s et t les isométries de la droite euclidienne $\mathbb{R}$ définies par $x \mapsto -x$ et $x \mapsto 1 - x$, et $G := \langle s, t \rangle \subset \mathrm{Iso}(\mathbb{R})$.*

(i) Montrer que $H := \langle st \rangle$ est un sous-groupe distingué de G isomorphe à $\mathbb{Z}$.

(ii) Montrer que la conjugaison par s induit l'automorphisme $x \mapsto x^{-1}$ de H.

(iii) En déduire $G \simeq \mathbb{Z} \rtimes_\alpha \mathbb{Z}/2\mathbb{Z}$ où $\alpha : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z})$ envoie $\overline{1}$ sur $x \mapsto -x$.

Chapitre 5

Groupes et symétries

Le but de ce chapitre est d'étudier quelques groupes de symétries importants. Nous commençons par revisiter les polyèdres (convexes, compacts) [1] *réguliers* de dimension 2 (polygones réguliers) et 3 (solides de Platon) en étudiant au cas par cas leurs *groupes de symétries* (ou *groupes d'isométries*). C'est l'occasion de revoir "en action" les groupes cycliques et diédraux, de représenter les désormais familiers A_4, S_4 et A_5 comme groupes de rotations en ces dimensions, et de retrouver de manière géométrique et assez limpide des éléments de structure de ces groupes évoqués aux chapitres précédents. Suivant Klein, on démontre ensuite qu'à conjugaison près ce sont les seuls sous-groupes finis de $\mathrm{SO}(3)$. En particulier, il n'y a pas d'autre groupe de rotations fini possible pour une figure quelconque de l'espace. Une autre conséquence amusante est que tout sous-groupe d'un des groupes de la liste ci-dessus est isomorphe à un autre sous-groupe de cette liste.

Ce phénomène cesse quand la dimension n grandit : il devient rapidement inextricable de classifier les sous-groupes finis de $\mathrm{O}(n)$. Par exemple, le groupe S_n, et donc tout groupe fini d'ordre n peut apparaître. Paradoxalement, on sait depuis Schläfli que les polyèdres réguliers peuvent être classifiés en toute dimension $n \geqslant 4$: à similitude près, il y a le *n-simplexe*, le *n-hypercube*, le *n-hyperoctaèdre*, ainsi que 3 autres polyèdres exceptionnels en dimension $n = 4$. Nous renvoyons à l'un des compléments culturels pour plus d'informations. Dans un autre complément culturel, nous parlerons de sous-groupes discrets de $\mathrm{Iso}(2)$: *les groupes de frises* (chers aux architectes) et les *groupes de papiers peints* (chers aux décorateurs).

Dans une deuxième partie, nous expliquerons comment les quaternions peuvent être utilisés pour étudier les groupes $\mathrm{SO}(3)$ et $\mathrm{SO}(4)$. Le sous-groupe $\mathrm{Sp}(1)$ des quaternions de norme 1 (un sous-groupe de $\mathrm{SL}_2(\mathbb{C})$) joue un rôle central. Il s'identifie à la sphère euclidienne [2] S^3, et munit donc cette dernière d'une loi de groupe topologique. Cette structure joue un rôle important en géométrie, en topologie de basse dimension et en physique quantique. Nous classifions ensuite les sous-groupes finis de $\mathrm{Sp}(1)$ et introduisons les groupes d'isométries "binaires" des solides de Platon. En plus de donner des exemples de groupes intéressants, ils permettent également d'étudier les polyèdres réguliers exceptionnels de dimension 4.

Dans une dernière partie, nous étudions le dévissage du groupe linéaire $\mathrm{GL}_n(k)$. Le résultat central est la simplicité de $\mathrm{PSL}_n(k)$ (sauf pour $n = 2$ et $|k| \leqslant 3$), que nous démontrons en utilisant la *méthode d'Iwasawa*. Quand k est un corps fini, cela fournit une nouvelle série infinie de groupes simples finis. Dans le cas $n = 2$, le groupe $\mathrm{PGL}_2(k)$ s'identifie aussi au groupe des homographies de la droite projective sur k. Le cas des petits n ou $|k|$ est particulièrement intéressant, à cause de l'existence

1. Dans le cours, nous bornerons à développer quelques exemples élémentaires qui peuvent se traiter sans la théorie générale des polyèdres. Nous en dirons un peu plus dans le Complément 5.

2. ... ou encore au groupe $\mathrm{SU}(2)$ de la géométrie hermitienne.

de certains isomorphismes miraculeux. Cela nous permet aussi de discuter l'un des énoncés de la dernière lettre de Galois à Chevalier concernant les actions transitives exceptionnelles de $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ sur p éléments.

1. Sous-groupes finis de $\mathrm{O}(2)$ et $\mathrm{SO}(3)$

1.1. Rappels sur le groupe orthogonal. Soit E un espace euclidien de dimension $n \geqslant 1$. On note $(x, y) \mapsto x.y$ désigne le produit scalaire de E et $||x|| = (x.x)^{1/2}$ la norme Euclidienne associée. On rappelle que le *groupe orthogonal* de E est le sous-groupe $\mathrm{O}(E)$ de $\mathrm{GL}(E)$ constitué des isométries de E. Par polarisation, on a aussi

$$\mathrm{O}(E) = \{g \in \mathrm{GL}(E) \mid gx.gy = x.y \ \forall x, y \in E\}.$$

On sait que si $e = (e_1, \ldots, e_n)$ désigne une base orthonormée de E, l'application $u \mapsto \mathrm{Mat}_e(u)$ est un isomorphisme de $\mathrm{O}(E)$ sur le sous-groupe suivant de $\mathrm{GL}_n(\mathbb{R})$:

$$\mathrm{O}(n) := \{g \in \mathrm{GL}_n(\mathbb{R}) \mid gg^t = 1_n\} \tag{24}$$

(qui ne dépend que de $n = \dim E$). On identifie souvent $\mathrm{O}(n)$ au groupe orthogonal de l'espace euclidien standard $\mathbb{R}^n$ de produit scalaire $\sum_i x_i y_i$ à l'aide de la base orthonormée canonique de $\mathbb{R}^n$. La Formule (24) montre que l'on a $\det g = \pm 1$ pour tout $g \in \mathrm{O}(n)$, puis que $\det : \mathrm{O}(n) \to \{\pm 1\}$ est surjectif. On note $\mathrm{SO}(n)$ son noyau. Plus généralement, on définit le *groupe spécial orthogonal de* E comme le sous-groupe

$$\mathrm{SO}(E) = \{g \in \mathrm{O}(E) \mid \det g = 1\}$$

de $\mathrm{O}(E)$. Il est aussi appelé groupe des *isométries directes*, ou groupe des *rotations*, de E. Il est distingué et d'indice 2 dans $\mathrm{O}(E)$.

Définition 1.1. *Soient H un hyperplan vectoriel de E. La* réflexion par rapport à H *est l'élément* s_H *de* $\mathrm{O}(E)$ *défini par* $\mathrm{s}_H(h + d) = h - d$ *pour* $h \in H$ *et* $d \in H^\perp$.

Une réflexion est un cas particulier de *symétrie orthogonale*, c'est-à-dire d'élément $s \in \mathrm{O}(E)$ avec $s^2 = 1$. Elles vérifient en outre $\det \mathrm{s}_H = -1$. Les réflexions sont les éléments (non triviaux) de $\mathrm{O}(E)$ dont l'espace des points fixes est de dimension maximale ; elles joueront un peu le rôle des transpositions du groupe symétrique. Par exemple, *toutes les réflexions sont conjuguées dans* $\mathrm{O}(E)$. En effet, pour tout $g \in \mathrm{O}(E)$ et tout hyperplan $H \subset E$, on a $g(H)^\perp = g(H^\perp)$ puis

$$g\, \mathrm{s}_H\, g^{-1} = \mathrm{s}_{g(H)},$$

et $\mathrm{O}(E)$ permute transitivement les hyperplans de E. De plus, les réflexions engendrent $\mathrm{O}(E)$, et plus précisément :

Proposition 1.2. (Cartan-Dieudonné) *Tout élément de* $\mathrm{O}(E)$ *est produit d'au plus* $n = \dim E$ *réflexions. En particulier, tout élément de* $\mathrm{SO}(E)$ *est produit d'au plus* $n/2$ *produits de deux réflexions.*

Démonstration — Le (i) est très classique (voir l'Exercice 2.16 Chap. 2, qui est plus général). Le (ii) se déduit du (i) en prenant le déterminant. □

Exemple 1.3. (i) On a bien sûr $\mathrm{O}(1) = \{\pm 1\}$.

(ii) Supposons $\dim E = 2$. Dans ce cas $\mathrm{O}(E) \smallsetminus \mathrm{SO}(E)$ est exactement l'ensemble des réflexions, et $\mathrm{SO}(E)$ celui des produits de deux réflexions. Comme le produit de deux réflexions planes est une rotation d'angle double de l'angle entre les axes, le groupe $\mathrm{SO}(E)$ est le groupe des rotations du plan, isomorphe à S^1.

Rappelons aussi la proposition suivante, attribuée parfois à Euler.

Proposition 1.4. (Euler) *Si* $\dim E = 3$, *tout élément non trivial de* $\mathrm{SO}(E)$ *possède une et une seule droite fixe dans* E.

Démonstration — Par la Proposition 1.2, tout élément g de $\mathrm{SO}(3)$ est trivial ou produit de 2 réflexions orthogonales d'hyperplans distincts H_1, H_2 et donc fixe la droite $H_1 \cap H_2$. Si g fixe deux droites distinctes, il fixe le plan P qu'elles engendrent, et donc stabilise la droite $P^\perp$. La condition $\det g = 1$ assure alors qu'il fixe aussi $P^\perp$, et donc $g = 1$. □

Nous avons utilisé, et réutiliserons constamment, le fait suivant :

Lemme 1.5. *Si* $g \in \mathrm{O}(E)$ *préserve* $F \subset E$, *il préserve aussi* $F^\perp$.

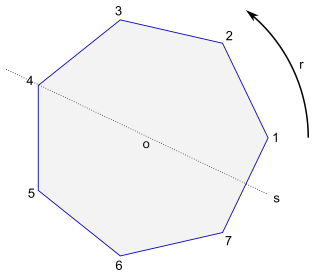
Démonstration — Si g préserve F, il préserve aussi le sous-espace vectoriel engendré, qui a même orthogonal. On peut donc supposer que F est un sous-espace vectoriel, et donc $g(F) = F$ pour des raisons de dimension. Pour $f \in F$ et $e \in F^\perp$ on a alors $f.ge = g^{-1}f.e = 0$ car $g^{-1}f \in F$. Cela montre bien $g(F^\perp) \subset F^\perp$. □

1.2. Quelques sous-groupes finis de $\mathrm{O}(2)$ **et** $\mathrm{SO}(3)$**.** Pour toute partie P de E, le *groupe des isométries orthogonales de* P *dans* E est le sous-groupe

$$\mathrm{Iso}(P) = \{g \in \mathrm{O}(E) \mid g(P) = P\}$$

On pose aussi $\mathrm{Iso}^+(P) = \mathrm{Iso}(P) \cap \mathrm{SO}(E)$.

On suppose d'abord $\dim E = 2$. Soit $\mathscr{P}_m \subset E$ un polygone régulier du plan à $m \geqslant 3$ côtés, disons centré en 0. Notons que $\mathrm{Iso}(\mathscr{P}_m)$ agit sur E en préservant l'ensemble $\mathscr{S}$ des m sommets de $\mathscr{P}_m$: ce sont les points de $\mathscr{P}_m$ à distance maximale de 0. Numérotons ces sommets *de manière consécutive et directe* par $1, ..., m$. L'action de $\mathrm{Iso}(\mathscr{P}_m)$ sur $\mathscr{S}$ définit alors un morphisme $f : \mathrm{Iso}(\mathscr{P}_m) \to \mathrm{S}_m$.



Proposition 1.6. *Pour* $m \geqslant 3$, *le morphisme* f *ci-dessus induit un isomorphisme* $\mathrm{Iso}(\mathscr{P}_m) \xrightarrow{\sim} \mathrm{D}_{2m}$. *De plus, on a* $\mathrm{Iso}^+(\mathscr{P}_m) \simeq \mathbb{Z}/m\mathbb{Z}$.

Démonstration — Le stabilisateur dans $\mathrm{Iso}(\mathscr{P}_m)$ d'un sommet S de $\mathscr{P}_m$ est le groupe d'ordre 2 engendré par la symétrie orthogonale fixant (OS). En considérant deux sommets non opposés, il en existe car $n \geqslant 3$, on en déduit que cette action est fidèle, *i.e.* f est injectif. De plus, la rotation r de centre 0 d'angle $\frac{2\pi}{m}$ est dans $\mathrm{Iso}(\mathscr{P}_m)$ et vérifie $f(r) = (1\,2\,...\,m) = c$, donc l'action de $\mathrm{Iso}(\mathscr{P}_m)$ sur $\mathscr{S}$ est transitive. On en déduit $|\mathrm{Iso}(\mathscr{P}_m)| = 2\,m$ (formule orbite-stabilisateur). La réflexion orthogonale s échangeant les sommets 1 et n vérifie $f(s) = (1\,m)(2\,m-1)\,... = \tau$. On a donc $\mathrm{D}_{2m} = \langle c, \tau\rangle \subset \mathrm{Im}\, f$, puis une égalité pour des raisons de cardinal. Comme $\det s = -1$ on en déduit $|\mathrm{Iso}^+(\mathscr{P}_m)| = m$, et donc que l'inclusion $\langle c\rangle \subset \mathrm{Iso}^+(\mathscr{P}_m)$ est une égalité. □

Remarque 1.7. (Le groupe de Klein) Posons $\mathscr{P}_2 = [-1,1]\times[-\epsilon,\epsilon]$ avec $0 \leqslant \epsilon < 1$ (un segment pour $\epsilon = 0$, ou *polygone dégénéré*). On constate $\mathrm{Iso}(\mathscr{P}_2) = \langle s_1, s_2\rangle$ où s_1 et s_2 sont les réflexions verticales et horizontales. En particulier on a $\mathrm{Iso}(\mathscr{P}_2) \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ et $\mathrm{Iso}^+(\mathscr{P}_2) = \{\pm\mathrm{id}_E\} \simeq \mathbb{Z}/2\mathbb{Z}$. On pose parfois $\mathrm{D}_4 := \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

Proposition 1.8. *Soit G un sous-groupe fini non trivial de $\mathrm{O}(2)$. Alors soit G est d'ordre 2 engendré par une réflexion, soit il existe un polygone régulier $\mathscr{P}$ du plan euclidien, éventuellement dégénéré, avec soit $G = \mathrm{Iso}(\mathscr{P})$, soit $G = \mathrm{Iso}^+(\mathscr{P})$.*

Démonstration — Considérons le groupe fini $G' := G \cap \mathrm{SO}(2)$, de cardinal disons m. Comme $\mathrm{SO}(2)$ est isomorphe à S^1 et que le seul sous-groupe d'ordre m de S^1 est μ_m, le groupe G' est le sous-groupe des rotations d'angle $\frac{2\pi}{m}\mathbb{Z}$. Pour $m \geqslant 2$, on a $G' = \mathrm{Iso}^+(\mathscr{P}_m)$. Cela conclut si on a $G' = G \subset \mathrm{SO}(2)$.

Supposons donc G' d'indice 2 dans G. Soit $s \in G \smallsetminus G'$ (une réflexion). Si on a $m \geqslant 2$ et quitte à faire tourner $\mathscr{P}_m$ de sorte que l'un des sommets soit fixe par s, on peut supposer $s(\mathscr{P}_m) = \mathscr{P}_m$. Mézalor on a $G = \langle s, G'\rangle \subset \mathrm{Iso}(\mathscr{P}_m)$, puis l'égalité pour des raisons de cardinal par la Proposition 1.6 (remarque ci-dessus pour $m = 2$). Enfin, pour $m = 1$ on a $G = \langle s\rangle \simeq \mathbb{Z}/2\mathbb{Z}$. □

On s'intéresse maintenant aux sous-groupes finis de $\mathrm{SO}(3)$ (pour le cas $\mathrm{O}(3)$, voir la Remarque 1.17). Commençons par les sous-groupes dit *réductibles*.

Remarque 1.9. (Sous-groupes réductibles) Soit E un espace euclidien de dimension 3. Un sous-groupe de $\mathrm{SO}(E)$ est dit *réductible* s'il préserve une droite D de E, ou ce qui revient au même, un plan $P \subset E$ (Lemme 1.5, on passe de l'un à l'autre en prenant l'orthogonal). ll est dit *irréductible* sinon. Mais le stabilisateur d'un plan P dans $\mathrm{SO}(E) \simeq \mathrm{SO}(3)$ s'identifie naturellement à $\mathrm{O}(P) \simeq \mathrm{O}(2)$. En effet, écrivant par exemple $D = \mathbb{R}\epsilon_3$ et $P = \mathbb{R}\epsilon_1 \oplus \mathbb{R}\epsilon_2$, avec les ϵ_i orthonormés dans E, nous sommes simplement en train de parler du morphisme injectif *diagonal*

$$\mathrm{O}(2) \longrightarrow \mathrm{SO}(3), \quad g \mapsto \begin{bmatrix} g & 0 \\ 0 & \det g \end{bmatrix}.$$

Ainsi, l'étude des sous-groupes réductibles de $\mathrm{SO}(3)$ se ramène entièrement à celle des sous-groupes de $\mathrm{O}(2)$, déjà résolue. En particulier, tout sous-groupe de $\mathrm{O}(2)$ peut être vu un sous-groupe de $\mathrm{SO}(3)$ via le plongement ci-dessus. Noter qu'une reflexion orthogonale dans $\mathrm{O}(2)$ est un *retournement* vu dans $\mathrm{SO}(3)$.

Des sous-groupes plus intéressants sont obtenus en considérant les *solides de Platon*. Ce sont les *polyèdres (convexes, compacts) réguliers* de l'espace euclidien de dimension 3. Nous renvoyons aux compléments pour la signification mathématique exacte de ces termes, qu'il ne sera pas utile de connaître en première approche ici. [3] À similitude euclidienne près, il y a exactement 5 solides de Platon représentés ci-après, [4] et dont nous allons étudier les groupes de symétrie.

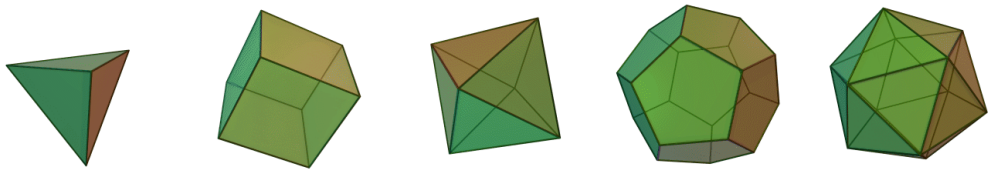


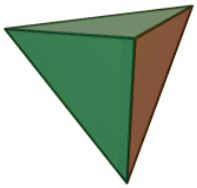
FIGURE 1. Les 5 solides de Platon.

Soit $P \subset E$ un tel polyèdre. On supposera toujours que P est centré en 0. Parmi les parties remarquables de P, il y a ses *sommets*, ses *arêtes* et ses *faces*. On voit bien sur chaque figure ce que l'on entend par là ! On peut aussi rigoureusement les définir comme les parties convexes non vides $F \subsetneq P$ vérifiant la propriété d'*extrémalité* :

$$(\star) \quad \forall x, y \in P, \ ]x, y[\cap F \neq \varnothing \implies [x, y] \subset F.$$

On constate qu'une telle partie est soit un point (sommet), soit un segment (arête), soit un polygone régulier (face). L'hypothèse "centré en 0" dit que l'isobarycentre des sommets est 0. L'action évidente de $\mathrm{Iso}(P)$ sur E et ses parties préserve $(\star)$ (propriété affine) et donc l'ensemble $\mathscr{S}$ des sommets de P, celui $\mathscr{A}$ des *arêtes* de P, et celui $\mathscr{F}$ des faces de P. L'action de $\mathrm{Iso}(P)$ sur $\mathscr{S}$ est fidèle car $\mathscr{S}$ engendre E, ainsi donc que celles sur $\mathscr{A}$ et $\mathscr{F}$ (tout sommet est intersection de deux arêtes, toute arête est intersection de deux faces). Noter que dès que $-1 \in \mathrm{Iso}(P)$ (symétrie centrale) on a $\mathrm{Iso}(P) = \{\pm 1\} \times \mathrm{Iso}^+(P)$. Regardons la situation au cas par cas.

(A) Le tétraètre régulier



Soit T un tel polyèdre (4 faces triangles équilatérales, 4 sommets, 6 arêtes). L'action fidèle de $\mathrm{Iso}(\mathrm{T})$ sur les 4 sommets, numérotés de manière arbitraire, définit un morphisme injectif $f : \mathrm{Iso}(\mathrm{T}) \to \mathrm{S}_4$. On constate que les rotations d'ordre 3 fixant un sommet de T ont pour image par f un 3-cycle des 3 sommets restants. Le retournement d'une arête échange les deux sommets restants, son image par f est une double transposition. Enfin, la symétrie orthogonale d'axe engendré par une

3. Disons simplement qu'un polytope de E est l'enveloppe convexe d'un ensemble fini de points, et qu'on dit qu'il est régulier si son groupe d'isométries agit transitivement sur ses *drapeaux de faces*.

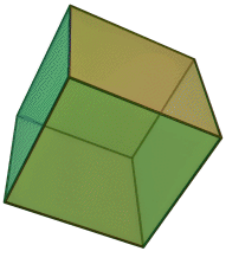
4. Cette illustration est issue de https://fr.wikipedia.org/wiki/Solide_de_Platon

arête A échange les deux sommets de cette arête et fixe les deux sommets restants : son image par f la transposition des sommets de A. On a donc $f(\mathrm{Iso}(\mathrm{T})) = \mathrm{S}_4$ et $f(\mathrm{Iso}^+(\mathrm{T})) = \mathrm{A}_4$, et on a démontré la :

Proposition 1.10. *On a* $\mathrm{Iso}(\mathrm{T}) \simeq \mathrm{S}_4$ *et* $\mathrm{Iso}^+(\mathrm{T}) \simeq \mathrm{A}_4$.

Noter que, dans l'isomorphisme ci-dessus, le déterminant sur Iso(T) correspond à la signature sur S_4. De plus, on constate que T possède exactement 3 paires d'arêtes orthogonales, ce qui fournit un morphisme $\mathrm{Iso}(T) \to \mathrm{S}_3$, et on retrouve une réalisation concrète du morphisme $\mathrm{S}_4 \to \mathrm{S}_3$ étudié au chapitre précédent !

(B) Le cube (ou hexaèdre régulier)

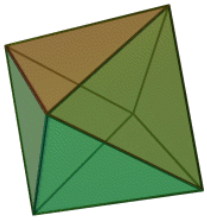


Soit C un cube (6 faces carrées, 8 sommets, 12 arêtes). On a $-1 \in \mathrm{Iso}(\mathrm{C})$ et donc $\mathrm{Iso}(\mathrm{C}) = \{\pm 1\} \times \mathrm{Iso}^+(\mathrm{C})$. Chacun des 8 sommets de C vient par paire $\{S, -S\}$, de sorte que Iso(C) agit naturellement sur l'ensemble $\mathscr{S}'$ des 4 paires de sommets du cube. On vérifie aisément que le noyau de cette action est $\{\pm 1\}$.[5] Comme -1 n'est pas dans SO(3), l'action de $\mathrm{Iso}^+(\mathrm{C})$ sur $\mathscr{S}'$ est donc fidèle. En regardant une rotation d'ordre 4 du cube fixant le centre d'une face, et une rotation d'ordre 3 fixant un sommet, on constate que l'image du morphisme $\mathrm{Iso}^+(\mathrm{C}) \to \mathrm{S}_{\mathscr{S}'} \simeq \mathrm{S}_4$ contient des 4 cycles et tous les 3-cycles : c'est donc S_4 et on a montré

Proposition 1.11. *On a* $\mathrm{Iso}^+(\mathrm{C}) \simeq \mathrm{S}_4$ *et* $\mathrm{Iso}(\mathrm{C}) = \{\pm 1\} \times \mathrm{Iso}^+(\mathrm{C})$.

Là encore, en considérant l'action de $\mathrm{Iso}^+(\mathrm{C})$ sur les 3 paires de faces opposées du cube on retrouverait un morphisme surjectif $\mathrm{S}_4 \to \mathrm{S}_3$!

(C) L'octaèdre régulier



Soit O un tel polyèdre (8 faces triangles équilatérales, 6 sommets, 12 arêtes). Les centres des 8 faces de O sont les sommets d'un cube C, appelé cube dual de O. De

5. Si on a une base e_1, e_2, e_3 de E et $g \in \mathrm{O}(E)$ tels que $g(e_i) = \pm e_i$ pour tout i, ainsi que $g(f) = \pm f$ pour $f = e_1 + e_2 + e_3$, alors on a $g = \pm 1$.

plus, les centres des faces de C sont les sommets d'un nouvel octaèdre régulier O′, aussi appelé dual de C. On constate que O′ et O sont homothétiques. On en déduit $\mathrm{Iso}(\mathrm{O}) = \mathrm{Iso}(\mathrm{C}) = \mathrm{Iso}(\mathrm{O}')$: on est ramené au cas précédent. On peut bien sûr aussi l'étudier directement !

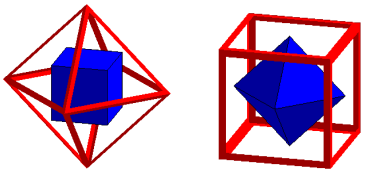
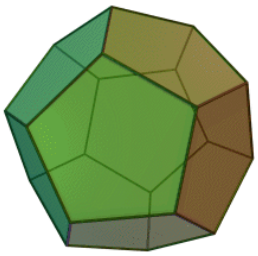


FIGURE 2. La dualité entre octaèdres et cubes

LE DODÉCAÈDRE RÉGULIER



Soit D un tel polyèdre (12 faces pentagonales, 20 sommets, 30 arêtes). On a $-1 \in \mathrm{Iso}(\mathrm{D})$ et donc $\mathrm{Iso}(\mathrm{D}) = \{\pm 1\} \times \mathrm{Iso}^+(\mathrm{D})$. Montrons d'abord $|\mathrm{Iso}^+(\mathrm{D})| = 60$. Pour cela, regardons l'action (fidèle) de $\mathrm{Iso}^+(\mathrm{D})$ sur les 20 de sommets de D. Elle est transitive, comme on le constate en regardant les rotations d'ordre 5 centrées en chacune des faces. Le stabilisateur d'un sommet S est le sous-groupe des 3 rotations de Iso(D) fixant S et permutant cycliquement les trois faces de D contenant S. La formule orbite-stabilisateur conclut $|\mathrm{Iso}^+(\mathrm{D})| = 60$. Montrons maintenant $\mathrm{Iso}^+(\mathrm{D}) \simeq \mathrm{A}_5$. Il faut d'abord trouver un ensemble à 5 éléments sur lequel $\mathrm{Iso}^+(\mathrm{D})$ agit. On observe d'abord que D a $30/2 = 15$ couples d'arêtes parallèlles, nous appelerons *diarête* un tel couple. Ces 15 diarètes se regroupent en 5 paquets de 3 naturels comme suit. Appelons *repère* de D un triplet de diarêtes deux à deux orthogonales. On constate que chaque diarête de D appartient à un repère. De plus, deux repères sont nécessairement disjoints car on est en dimension 3, de sorte qu'il existe exactement 5 repères. Notons $\mathscr{R}$ l'ensemble des 5 repères de D. [6] [7]

Le groupe $\mathrm{Iso}^+(\mathrm{D})$ agit naturellement sur $\mathscr{R}$. Pour chaque face F de D, observons que chacune des 5 arêtes de F appartient à un unique repère de D, de sorte que le pentagone F identifie $\mathscr{R}$ à l'ensemble des 5 côtés de F. Chacune des 4 rotations non triviales de F définit alors un 5-cycle de $\mathscr{R}$. La rotation d'ordre 3 de D fixant un

6. Les repères correspondent aussi bijectivement aux *grands cubes* que l'on peut inscrire dans D, ou encore aux 5 *très grands cubes* circonscrits à D (chaque face du cube étant partagée en 2 par l'une des arêtes du repère) : voir la Figure 3 ci-contre.

7. Comme le souligne Coxeter dans son livre, ces constructions sont déjà présentes dans les éléments d'Euclide livre XV, 3-5. Les figures ci-dessus sont empruntées au contributeur *aes* de cette discussion MSE, et à ce site. Internet regorge d'illustrations sur le dodécaèdre, et de patrons pour le construire (un exemple).

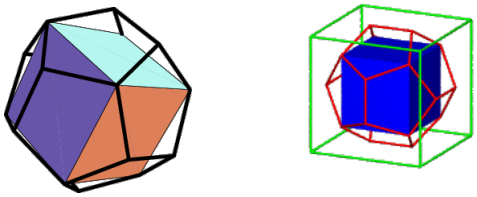


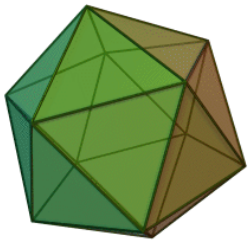
FIGURE 3. L'un des 5 cubes inscrits ou circonscrits au dodécaèdre

sommet de F induit manifestement un élément non trivial de $\mathscr{R}$, donc un 3-cycle. Comme un 3-cycle et un 5-cycle de S_5 engendrent A_5, on a démontré la :

PROPOSITION 1.12. *On a* $\mathrm{Iso}^+(\mathrm{D}) \simeq \mathrm{A}_5$ *et* $\mathrm{Iso}(\mathrm{D}) = \{\pm 1\} \times \mathrm{Iso}^+(\mathrm{D})$.

Remarquons que l'action naturelle de $\mathrm{Iso}^+(\mathrm{D})$ sur les 6 paires de faces opposées est manifestement transitive. Elle définit donc une action transitive de A_5 sur un ensemble à 6 éléments : c'est la restriction à A_5 de l'action exotique du chapitre précédent !

L'ICOSAÈDRE RÉGULIER



Soit I un tel polyèdre (20 faces triangles équilatérales, 12 sommets, 30 arêtes). On vérifie comme pour le cube que le dual de I est un dodécaèdre D et que l'on a $\mathrm{Iso}(\mathrm{I}) = \mathrm{Iso}(\mathrm{D})$: on est ramené au cas précédent. Nous renvoyons à l'Exercice 5.2 pour une construction très simple de l'icosaèdre et du dodécaèdre.

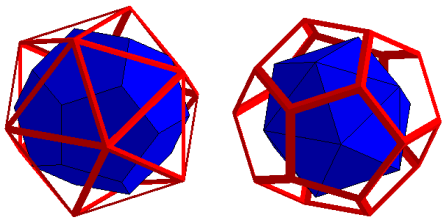


FIGURE 4. La dualité entre icosaèdres et dodécaèdres

1.3. Le théorème de Klein. Un résultat remarquable dû à Klein [8] est qu'il n'y a pas d'autres sous-groupes finis de SO(3), *à conjugaison près*, que les groupes évoqués ci-dessus.

8. *Lectures on the ikosahedron and the solution of equations of the fifth degree.*

THÉORÈME 1.13. (Klein) *Tout sous-groupe fini irréductible de* $\mathrm{SO}(3)$ *est le groupe des isométries directes d'un solide de Platon, et donc isomorphe à* A_4, S_4 *ou* A_5.

Remarquer que le groupe des isométries directes d'un solide de Platon est bien irréductible, car ses rotations fixant un sommet sont d'ordre > 2 et ont des axes distincts. Le reste de la section est consacré à la démonstration[9] du théorème de Klein. Nous aurons besoin du lemme suivant :

LEMME 1.14. (Burnside-Frobenius) *Soit G un groupe fini agissant sur un ensemble fini X. On note r le nombre de G-orbites dans X, et pour $g \in G$, on note* $\mathrm{Fix}(g)$ *l'ensemble des points fixes de g dans X. On a alors* $r = \frac{1}{|G|}\sum_{g\in G} |\mathrm{Fix}(g)|$.

Autrement dit, *le nombre d'orbites de G dans X est la moyenne arithmétique des nombres de points fixes des éléments de G dans X.*

DÉMONSTRATION — On calcule de deux façons le cardinal de l'ensemble

$$S = \{(g, x) \mid g \in G, x \in X, gx = x\}.$$

En sommant d'abord sur $g \in G$ on a d'une part $|S| = \sum_{g\in G} |\mathrm{Fix}(g)|$. Soient $\Omega_1, \ldots, \Omega_r$ les orbites de G dans X. En sommant d'abord sur $x \in X$, on a aussi

$$|S| = \sum_{x\in X} |G_x| = \sum_{x\in X} \frac{|G|}{|\mathrm{O}_x|} = |G| \sum_{i=1}^{r} \left(|\Omega_i| \times \frac{1}{|\Omega_i|} \right) = |G|\, r,$$

et on conclut en égalisant les deux formules pour $|S|$. □

REMARQUE 1.15. Ce résultat permet de résoudre plusieurs problèmes d'énumérations, comme ceux du type *colliers de Polya* : voir l'Exercice 5.8. Une autre application classique, due à Jordan, est la suivante. *Soit G un groupe agissant transitivement sur ensemble fini X avec $|X| > 1$. Alors il existe au moins un élément de G qui n'a aucun point fixe dans X.* Voir l'Exercice 5.9.

OBSERVATION PRÉLIMINAIRE IMPORTANTE : Avant d'entamer la démonstration du théorème de Klein, commençons par une analyse utile. Supposons que le sous-groupe $G \subset \mathrm{SO}(3)$ préserve un solide de Platon P. Tout élément non trivial $g \in G$ a une unique droite fixe dans $\mathbb{R}^3$ par Euler. On constate que cette droite intersecte P en un segment dont chaque extrémité (fixe par g) est soit un sommet, soit le milieu d'un segment, soit le centre d'une face. Réciproquement, tout sommet/milieu d'une arête/centre d'une face, est fixé par une rotation non triviale de G bien choisie. Ainsi, ces éléments particuliers de P se déduisent dans leur ensemble du groupe G.

Ceci étant dit, fixons maintenant $G \neq 1$ un sous-groupe fini arbitraire de $\mathrm{SO}(3)$. Le groupe G agit naturellement sur la sphère euclidienne S^2, et tout élément $g \neq 1$ admet exactement deux points fixes x et $-x$ dans S^2 par Euler. Suivant Euler, ces deux éléments seront appelés *pôles* de g. On introduit l'ensemble $X \subset \mathrm{S}^2$ des pôles des éléments non triviaux de G. Conformément à l'observation ci-dessus, nous allons montrer *in fine* que les éléments de X correspondent aux sommets/arêtes/faces du polyèdre cherché. Notons que $X \subset \mathrm{S}^2$ est stable par G : c'est l'ensemble des points $x \in \mathrm{S}^2$ tels que $G_x \neq \{1\}$, et on a $G_{gx} = gG_xg^{-1}$ pour $g \in G$ et $x \in X$. Ainsi, G agit sur X et :

9. La preuve employée est classique mais nous n'en connaissons pas l'origine. La preuve donnée par Coxeter, qu'il attribue à Bravais, et assez similaire mais utilise un peu de géométrie sphérique.

(a) tout élément de $G \smallsetminus \{1\}$ a exactement deux points fixes dans X,

(b) tout point de X est fixé par au moins un élément de $G \smallsetminus \{1\}$.

Lemme 1.16. *Soient $x_1, \dots, x_r$ des représentants des orbites de G dans X, et $n_i = |G_{x_i}|$ avec $n_1 \leqslant \cdots \leqslant n_r$. Alors on a soit $r = 2$, $|X| = 2$ et $G = G_{x_1} = G_{x_2}$, soit $r = 3$ et $|G|$ et les n_i sont donnés par la table ci-dessous :*

$\lvert G\rvert$	n_1	n_2	n_3	$\lvert \mathrm{O}_{x_1}\rvert$	$\lvert \mathrm{O}_{x_2}\rvert$	$\lvert \mathrm{O}_{x_3}\rvert$	$\lvert X\rvert$
$2m$	2	2	m	m	m	2	$2m+2$
12	2	3	3	6	4	4	14
24	2	3	4	12	8	6	26
60	2	3	5	30	20	12	60

Démonstration — D'après Burnside-Frobenius et (a), pour $n = |G|$ on a

$$r = |X|/n + 2(n-1)/n.$$

L'équation aux classes pour X s'écrit $|X| = \sum_{i=1}^r |\mathrm{O}_{x_i}|$. On a aussi $n_i|\mathrm{O}_{x_i}| = n$ pour tout i, et donc $|X|/n = \sum_{i=1}^r 1/n_i$ puis [10]

$$2 - 2/n = \sum_{i=1}^r (1 - 1/n_i), \tag{25}$$

en incorporant la formule plus haut pour r. Noter $n_i \mid n$, et aussi $n_i \geqslant 2$ par (b). Comme $n > 1$ on en déduit $2 \leqslant r \leqslant 3$.

(Cas $r = 2$) On a alors $2 - 2/n = 1 - 1/n_1 + 1 - 1/n_2$ avec $n_1 \leqslant n_2 \leqslant n$. Cela force $n_1 = n_2 = n$, puis $|X| = 2$ et donc $X = \{x_1, x_2\}$ et $G_{x_1} = G_{x_2}$ par (a) .

(Cas $r = 3$) Supposant $n_1 \geqslant 3$ on constate que le terme de droite est $\geqslant 6/3 = 2$, donc on a $n_1 = 2$. De même, si $n_2 \geqslant 4$, le terme de droite est encore $\geqslant 1/2 + 3/4 + 3/4 = 2$, donc on a $2 \leqslant n_2 \leqslant 3$. Le cas $n_1 = n_2 = 2$ conduit à $n = 2n_3$. On peut donc supposer $n_2 = 3$. L'équation (25) devient $2 - 2/n = 7/6 + 1 - 1/n_3$ avec $n_3 \geqslant 3$. Pour $n_3 \geqslant 6$ le terme de droite est > 2 : absurde. Enfin, pour $n_3 = 3, 4, 5$ on trouve respectivement $n = 12, 24, 60$. □

Démonstration — (du Théorème 1.13) On peut supposer $n = |G| > 1$. Pour $x \in X$, le stabilisateur G_x est un sous-groupe fini de $\mathrm{SO}(x^\perp) \simeq \mathrm{SO}(2) \simeq \mathrm{S}^1$. Il est donc cyclique. Soient $x_1, \dots, x_r$ comme dans le lemme ci-dessus. On choisit c_i un générateur de G_{x_i} (une rotation d'angle $2\pi/n_i$ dans $x_i^\perp$.) Faisons d'abord deux remarques :

(R1) Si Ω est une G-orbite avec $|\Omega| > 2$ alors le morphisme $G \to \mathrm{S}_\Omega$ est injectif, par la propriété (a).

(R2) L'ensemble X est stable par $x \mapsto -x$, et si Ω est une G-orbite alors il en va de même de $-\Omega$. De plus, pour $x, y \in X$ on a $G_y = G_x \Leftrightarrow y = \pm x$ par (a).

10. Avec plus de bagage en géométrie différentielle des surfaces, on peut aussi obtenir directement cette formule en appliquant la formule de Gauss-Bonnet à l'orbifold S^2/G.

(Cas 0) Dans le cas $r = 2$, le lemme entraîne $X = \{x_1, x_2\}$ avec $G = G_{x_1} = G_{x_2}$, donc $G = \langle c_1 \rangle$ est cyclique d'ordre n. Dans ce cas, G n'est pas irréductible. On suppose donc désormais $r = 3$.

(Cas 1) Cas $|G| = 2m$ et $(n_1, n_2, n_3) = (2, 2, m)$, avec $m \geqslant 2$. Pour $m = 2$, on a $|G| = 4$ et trois éléments distincts d'ordre 2 : les pôles de ces éléments sont donc deux à deux orthogonaux (le produit de deux retournements est une rotation du double de l'angle entre les deux pôles) et G est un groupe de Klein. On suppose maintenant $m > 2$. Dans ce cas O_{x_3} est l'unique orbite à 2 éléments, et elle donc égale à $-\mathrm{O}_{x_3}$ par (R2), *i.e.* $\mathrm{O}_{x_3} = \{x_3, -x_3\}$. Par (b) on en déduit $g(x_3) = \pm x_3$ pour tout $g \in G$. Là encore, G n'est pas irréductible (on pourrait voir qu'il est diédral).

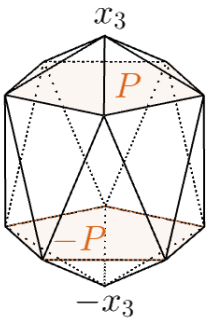
(Cas 2) Cas $|G| = 12$ et $(n_1, n_2, n_3) = (2, 3, 3)$. On considère la G-orbite $T = \mathrm{O}_{x_3}$, qui a $12/3 = 4$ éléments. Pour $x \in T$, le groupe G_x est cyclique d'ordre 3 (conjugué dans G à G_{x_3}). L'action de $G_x = \langle \sigma \rangle$ sur T a au moins un point fixe (à savoir x), et au plus 2 par (a), donc σ est un 3-cycle de T. Au final, chaque élément de T est à même distance des 3 autres éléments : T est l'ensemble des sommets d'un tétraèdre régulier T dans E. Ainsi G préserve ce tétraèdre régulier (enveloppe convexe de T) et on a donc $G \subset \mathrm{Iso}^+(\mathrm{T})$, puis égalité pour des raisons de cardinal (et donc $G \simeq \mathrm{A}_4$).

(Cas 3) Cas $|G| = 24$ et $(n_1, n_2, n_3) = (2, 3, 4)$. On considère l'unique G-orbite O de X à $6 = 24/4$ éléments, à savoir $O = \mathrm{O}_{x_4}$. Montrons que c'est l'ensemble des sommets d'un octaèdre régulier O. Par le même argument que ci-dessus, cela montrera $G \subset \mathrm{Iso}^+(\mathrm{O})$ puis $G = \mathrm{Iso}^+(\mathrm{O}) \simeq \mathrm{S}_4$ pour des raisons de cardinal. Pour $x \in O$, le stabilisateur $G_x \simeq \mathbb{Z}/4\mathbb{Z}$ fixe x, $-x$, et est une rotation d'ordre 4 de $x^\perp$. Il induit donc un 4-cycle de l'ensemble $\mathscr{C}_x = O \smallsetminus \{x, -x\} = -\mathscr{C}_x$. Ainsi, $\mathscr{C}_x$ est un carré de centre 0 dans le plan orthogonal à x, et $|x - y|$ ne dépend pas de $y \in \mathscr{C}_x$. Comme le choix initial de x dans O est arbitraire, on a montré aussi que deux éléments non égaux ou opposés de O sont toujours à la même distance : c'est bien l'ensemble des sommets d'un octaèdre régulier.

(Cas 4) Cas $|G| = 60$ et $(n_1, n_2, n_3) = (2, 3, 5)$. On considère l'unique G-orbite $I \subset X$ ayant $60/5 = 12$ éléments, à savoir $I = \mathrm{O}_{x_3}$. Nous allons (un peu laborieusement !) montrer que I est l'ensemble des sommets d'un icosaèdre régulier. On en déduira $G = \mathrm{Iso}(I)^+ \simeq \mathrm{A}_5$ comme ci-dessus. Le stabilisateur $G_{x_3} = \langle c_3 \rangle \simeq \mathbb{Z}/5\mathbb{Z}$ fixe x_3 et $-x_3$. Cette rotation c_3 induit donc un produit de deux 5-cycles à supports disjoints de l'ensemble à 10 éléments $I \smallsetminus \{x_3, -x_3\}$. Notons P et P' ces supports : chacun est l'ensemble des sommets d'un pentagone régulier d'un plan affine orthogonal à x_3.

La relation $I = -I$ montre que $I \smallsetminus \{x_3, -x_3\}$ est stable par $x \mapsto -x$, puis $P' = -P$. En effet, $P = -P$ est impossible car on a $|P| \equiv 1 \bmod 2$. Quitte à échanger P et P', on peut aussi supposer que P est « du côté de x », c'est à dire que la quantité $h := p.x_3$ pour $p \in P$ (elle ne dépend pas du choix de p) est $\geqslant 0$. On ne peut avoir $h = 0$, car alors les pentagones P et $P' = -P$ seraient tous deux dans le plan $x_3^\perp$, et x_3 serait équidistant des 10 éléments de $X \smallsetminus \{\pm x_3\}$ (sommets d'un décagone régulier). Cela contredit la transitivité de G sur X car un sommet d'un polygone régulier n'est équidistant qu'à deux autres sommets au plus de ce polygone. On a donc $h > 0$.

Soit I l'enveloppe convexe de I. On constate que ce polyèdre convexe a pour 12 sommets les éléments de I et 20 faces triangulaires (avec $\pm x_3$ les pôles nord et sud) :



C'est donc un icosaèdre et il reste à voir qu'il est régulier. Mieux, il y a exactement 5 faces de I contenant le sommet x_3, à savoir les triangles $x_3\, p\, c_3(p)$ avec p dans P. Ces 5 triangles sont isométriques, car permutés transitivement par c_3, et isocèles en x_3. Comme G agit transitivement sur l'orbite I, la même chose vaut pour chacun des 12 sommets de I, de sorte que les triangles ci-desus sont isocèles en chacun de leurs trois sommets : ils sont équilatéraux. Ainsi, I est un icosaèdre régulier. □

Remarque 1.17. (Sous-groupes de O(3)) Soit H un sous-groupe de O(3). La décomposition en produit direct interne $\mathrm{O}(3) \simeq \{\pm 1\} \times \mathrm{SO}(3)$ montre que si H contient -1, il est de la forme $\{\pm 1\} \times H'$ avec $H' = H \cap \mathrm{SO}(3)$. En revanche, si $-1 \notin H$ il faut faire attention qu'on n'a pas nécessairement $H \subset \mathrm{SO}(3)$. Par exemple, $\mathrm{Iso}(\mathrm{T}) \simeq \mathrm{S}_4$ ne contient pas -1, est distinct de $\mathrm{Iso}^+(\mathrm{T})$. Toutefois, le morphisme $\mathrm{O}(3) \to \mathrm{SO}(3)$ donné par la décomposition en produit direct interne, envoyant g sur $(\det g)g$, a pour noyau $\{\pm 1\}$, de sorte qu'il identifie tout de même un tel H à un sous-groupe de SO(3). Par exemple, $\mathrm{Iso}(\mathrm{T}) \simeq \mathrm{S}_4$ est bien isomorphe à un sous-groupe de SO(3), à savoir un Iso(C) !

2. Le groupe Sp(1) et géométrie euclidienne en dimensions 3 et 4

2.1. L'algèbre des quaternions de Hamilton. On se place dans $\mathrm{M}_2(\mathbb{C})$ et l'on reconsidère les matrices I, J et $K = IJ$ de l'Exemple 6.2 Chap. 2 utilisées pour définir le sous-groupe $\mathrm{H}_8 = \{\pm 1, \pm I, \pm J, \pm K\}$ de $\mathrm{GL}_2(\mathbb{C})$. Suivant Hamilton, on pose

$$\mathbb{H} := \mathrm{Vect}_{\mathbb{R}}(1, I, J, K) \subset \mathrm{M}_2(\mathbb{C}).$$

C'est à la fois un sous $\mathbb{R}$-espace vectoriel et un sous-anneau de $\mathrm{M}_2(\mathbb{C})$ (on dit que c'est une sous $\mathbb{R}$-algèbre) car H_8 est un sous-groupe de $\mathrm{GL}_2(\mathbb{C})$. On a

$$t\,1 + x\,I + y\,J + z\,K = \begin{bmatrix} t + ix & -y - iz \\ y - iz & t - ix \end{bmatrix}, \tag{26}$$

de sorte que $1, I, J, K$ est une $\mathbb{C}$-base de $\mathrm{M}_2(\mathbb{C})$. En particulier, c'est une $\mathbb{R}$-base de $\mathbb{H}$ et on a $\dim_{\mathbb{R}} \mathbb{H} = 4$. On constate aussi que l'on a

$$\mathbb{H} = \{\begin{bmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{bmatrix},\ \alpha, \beta \in \mathbb{C}\}.$$

On identifie $\mathbb{R}$ au sous-corps $\mathbb{R}\,1 \subset \mathbb{H}$. La découverte de Hamilton est :

Proposition 2.1. *$\mathbb{H}$ est un corps gauche de centre $\mathbb{R}$.*

La clé pour comprendre cela sans calcul est *l'identité de Cayley-Hamilton*. On définit la *trace*, la *norme* et le *conjugué* d'un quaternion $q \in \mathbb{H}$ par les formules

$$\mathrm{t}(q) = \operatorname{trace} q,\ \mathrm{n}(q) = \det q \ \text{ et } \ q^\star = {}^t\overline{q} = \mathrm{t}(q)1 - q \in \mathbb{H}.$$

Dans les coordonnées $t, x, y, z \in \mathbb{R}$ on a donc

$$\mathrm{t}(q) = 2t,\ \mathrm{n}(q) = t^2 + x^2 + y^2 + z^2 \ \text{ et } q^\star = t\,1 - x\,I - y\,J - z\,K. \tag{27}$$

En particulier, on a $\mathrm{n}(q) = 0 \iff q = 0$. Le théorème de Cayley-Hamilton dans $\mathrm{M}_2(\mathbb{C})$ s'écrit $q^2 - \mathrm{t}(q)q + \mathrm{n}(q)\,1 = 0$. Il est donc valable aussi dans $\mathbb{H}$ et s'écrit :

$$qq^\star = q^\star q = \mathrm{n}(q)\,1, \quad \forall q \in \mathbb{H}. \tag{28}$$

Démonstration — (de la Proposition 2.1) Soit $q \in \mathbb{H} - \{0\}$. On a vu $\mathrm{n}(q) \neq 0$ et donc $q \neq 0$ est inversible d'inverse $\frac{1}{\mathrm{n}(q)} q^\star \in \mathbb{H}$ par (28). Soit q dans le centre de $\mathbb{H}$. Alors q commute à $\mathrm{vect}_{\mathbb{C}}\mathrm{H}_8 = \mathrm{M}_2(\mathbb{C})$. Mais comme le centre de $\mathrm{M}_n(k)$ est généralement constitué de scalaires, on a $q \in \mathbb{C}1 \cap \mathbb{H} = \mathbb{R}1$. □

2.2. Le groupe Sp(1)**.** D'après la Proposition 2.1, le groupe multiplicatif $\mathbb{H}^\times$ a pour ensemble sous-jacent $\mathbb{H} \smallsetminus \{0\}$. Il est particulièrement intéressant ! Il n'est pas commutatif, par exemple il contient H_8 comme sous-groupe. La norme $\mathrm{n} : \mathbb{H} \to \mathbb{R}$ est multiplicative[11] $\mathrm{n}(qq') = \mathrm{n}(q)\mathrm{n}(q')$ car det est multiplicatif, et on a aussi $\mathrm{n}(q) > 0$ pour $q \neq 0$. Elle définit donc un morphisme de groupes

$$\mathbb{H}^\times \to \mathbb{R}_{>0}. \tag{29}$$

En particulier, les éléments de norme 1 de $\mathbb{H}^\times$ forment un sous-groupe :

Définition 2.2. *On pose* $\mathrm{Sp}(1) = \{q \in \mathbb{H} \mid \mathrm{n}(q) = 1\}$. *C'est un sous-groupe du groupe multiplicatif* $\mathbb{H}^\times$.

Considérons l'application $\mathbb{R}^4 \to \mathbb{H}$, $(t, x, y, z) \mapsto t + xI + yJ + zK$. Elle identifie la sphère unité euclidienne S^3 à Sp(1). La loi de groupe de Sp(1) *munit donc cette sphère d'une loi de groupe par transport de structure*, de la mème manière que le cercle unité S^1 de $\mathbb{R}^2$ s'identifie au groupe des nombres complexes de module 1. C'est la loi de groupe que nous mettrons par la suite sur S^3. C'est une loi non commutative ! On sait depuis E. Cartan ($\simeq$ 1940) que ce sont les deux seules sphères S^n, avec $n \geqslant 1$, que l'on peut munir d'une loi de groupe topologique (voir la Remarque 7.5 Chap. 2).

Remarque 2.3. *Remarquons aussi que* Sp(1) *s'identifie au sous-groupe suivant*

$$\mathrm{Sp}(1) = \{\begin{bmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{bmatrix} \in \mathrm{M}_2(\mathbb{C}),\ |\alpha|^2 + |\beta|^2 = 1\}$$

de $\mathrm{SL}_2(\mathbb{C})$. *Le lecteur connaissant la géometrie hermitienne reconnaitra l'égalité* $\mathrm{Sp}(1) = \mathrm{SU}(2)$ *(voir le Complément 7), et le physicien reconnaitra aussi l'égalité* $\mathrm{Sp}(1) = \mathrm{Spin}(3)$ *!*

11. L'identité remarquable $\mathrm{n}(qq') = \mathrm{n}(q)\mathrm{n}(q')$ s'écrit aussi, en coordonnées,

$$(T^2 + X^2 + Y^2 + Z^2)(T'^2 + X'^2 + Y'^2 + Z'^2) = A^2 + B^2 + C^2 + D^2$$

avec $A = TT' - XX' - YY' - ZZ'$, $B = TX' + XT' + YZ' - ZY'$, $C = TY' + YT' - XZ' + ZX'$ et $D = TZ' + ZT' - YX' + XY'$. Elle montre qu'un produit de deux sommes de 4 carrés est "universellement" une somme de 4 carrés. Elle joue par exemple un rôle, ainsi que les quaternions, dans la démonstration du Théorème de Lagrange : voir le complément 7 Chap. 10.

Noter que $\mathbb{R}^\times$ est un sous-groupe central de $\mathbb{H}^\times$, et que l'on a $\mathrm{n}(\lambda) = \lambda^2$ pour $\lambda \in \mathbb{R}^\times$. Ainsi, tout $q \in \mathbb{H}^\times$ s'écrit de manière unique $q = \lambda u$ avec $\lambda \in \mathbb{R}_{>0}$, $u \in \mathrm{Sp}(1)$ et $\lambda = \sqrt{\mathrm{n}(q)}$ (*décomposition polaire*), et on a un produit direct interne

$$\mathbb{H}^\times = \mathbb{R}_{>0} \times \mathrm{Sp}(1). \tag{30}$$

En guise d'exemple, regardons les éléments d'ordre fini de $\mathbb{H}^\times$. Un élément $q \in \mathbb{H}$ vérifiant $q^m = 1$ satisfait $\mathrm{n}(q)^m = 1$ et donc $\mathrm{n}(q) = 1$ car la norme est $\geqslant 0$: il est donc dans $\mathrm{Sp}(1)$. Commençons par l'ordre 2, qui est à part.

Proposition 2.4. *L'élément -1 est l'unique élément d'ordre 2 de $\mathrm{Sp}(1)$.*

Démonstration — Pour $q \in \mathbb{H}$ on a $q^2 = 1 \iff (q-1)(q+1) = 0 \iff q = \pm 1$, car $\mathbb{H}$ est un corps gauche. □

Regardons maintenant les éléments d'ordre 4.

Proposition 2.5. *Soit $q \in \mathrm{Sp}(1)$. On a des équivalences entre : (i) q est d'ordre 4, (ii) $q^2 = -1$, et (iii) $\mathrm{t}(q) = 0$.*

Démonstration — Si q est d'ordre 4 si, et seulement si, q^2 est d'ordre 2, de sorte que l'on a (i) $\implies$ (ii) par la proposition précédente. Par Cayley-Hamilton, on a $q^2 - \mathrm{t}(q)q + 1 = 0$. On en déduit $q^2 = -1 \iff \mathrm{t}(q)q = 0 \iff \mathrm{t}(q) = 0$ (car q est inversible). □

On pose $\mathbb{H}^0 = \{q \in \mathbb{H} \mid \mathrm{t}(q) = 0\} = \mathbb{R}I + \mathbb{R}J + \mathbb{R}K$. un élément de $\mathbb{H}^0$ est appelé *quaternion pur*. Ainsi, les éléments $q \in \mathrm{Sp}(1)$ avec $q^2 = -1$ constituent la sphére unité euclidienne $\{xI + yJ + zK \mid x^2 + y^2 + z^2 = 1\}$, et en particulier il y en a une infinité ![12]. Pour chaque tel q on constate que

$$\mathbb{C}_q = \{a + bq \mid a, b \in \mathbb{R}\}$$

est une sous-$\mathbb{R}$-algèbre de $\mathbb{H}$ isomorphe à $\mathbb{C}$ (via $a + bi \mapsto a + bq$). Aucune de ces copies de $\mathbb{C}$ à l'intérieure de $\mathbb{H}$ n'est plus naturelle que les autres ![13] Pour $q \in \mathrm{Sp}(1)$ avec $q^2 = -1$ on a $q^* = q^{-1} = -q$. Autrement dit, l'application $h \mapsto h^*$ induit la conjugaison complexe usuelle sur $\mathbb{C}_q$. En particulier, $\mathbb{C}_q^\times \cap \mathrm{Sp}(1)$ est un sous-groupe de $\mathrm{Sp}(1)$ isomorphe à S^1, ce qui démontre que $\mathrm{Sp}(1)$ contient des éléments de tout ordre fini possible.

2.3. L'espace euclidien $\mathbb{H}$. Nous allons maintenant utiliser la structure de quaternions pour faire de la géométrie euclidienne en dimensions 3 et 4. L'expression (27) pour n montre que $q \mapsto \mathrm{n}(q)^{1/2}$ est une norme euclidienne sur le $\mathbb{R}$-espace vectoriel $\mathbb{H}$ de dimension 4. Mieux, elle dit que $1, I, J, K$ en est une base orthonormée. Le produit scalaire associé est donné par la formule suivante :

$$\langle q, q' \rangle = \frac{1}{2}\mathrm{t}(q^\star q') = \frac{1}{2}(q^\star q' + (q')^\star q). \tag{31}$$

12. Le polynôme $X^2 + 1$ a donc une infinité de racines dans $\mathbb{H}$. C'est par ce que $\mathbb{H}$ n'est pas commutatif ! Par exemple, on a $h^2 + 1 \neq (h + I)(h - I)$ pour tout $h \in \mathbb{H}$, car le terme de droite vaut plutôt $h^2 + 1 + Ih - hI$.

13. Il n'est pas difficile de montrer que toute sous-$\mathbb{R}$-algèbre de $\mathbb{H}$ est soit $\mathbb{R}$, soit $\mathbb{H}$, soit un $\mathbb{C}_q$ (Exercice 5.28).

(On a utilisé $q + q^\star = \mathrm{t}(q)$ et $(qq')^\star = (q')^\star q^\star$ pour tout $q, q' \in \mathbb{H}$, qui découle de $q^\star = {}^t\,\overline{q}$.). En effet, il est manifestement $\mathbb{R}$-bilinéaire symétrique, et vérifie $\langle q, q\rangle = \mathrm{n}(q)$ (et donc défini positif). On dispose alors gratuitement des jolies isométries suivantes :

(a) Pour $q \in \mathbb{H}^\times$ on définit deux éléments $\mathrm{L}_q, \mathrm{R}_q \in \mathrm{GL}(\mathbb{H})$ en posant $\mathrm{L}_q(h) = qh$ et $\mathrm{R}_q(h) = hq^{-1}$. Pour $q \in \mathrm{Sp}(1)$ ce sont des isométries ! car pour tout $h \in \mathbb{H}$ on a $\mathrm{n}(qh) = \mathrm{n}(q)\mathrm{n}(h) = \mathrm{n}(h)$ et de même $\mathrm{n}(hq^{-1}) = \mathrm{n}(h)$. On a les formules évidentes

$$\mathrm{L}_{qq'} = \mathrm{L}_q \circ \mathrm{L}_{q'}, \quad \mathrm{R}_{qq'} = \mathrm{R}_q \circ \mathrm{R}_{q'}, \quad \mathrm{L}_q \circ \mathrm{R}_{q'} = \mathrm{R}_{q'} \circ \mathrm{L}_q, \quad \forall q, q' \in \mathrm{Sp}(1). \tag{32}$$

(b) Pour $h \in \mathbb{H}$ on pose aussi $\mathrm{s}(h) = -h^\star$. On constate en coordonnées t, x, y, z que c'est la réflexion orthogonale par rapport à $1^\perp$. On a les formules évidentes

$$\mathrm{s} \circ \mathrm{L}_q = \mathrm{R}_q \circ \mathrm{s} \text{ et } \mathrm{s} \circ \mathrm{R}_q = \mathrm{L}_q \circ \mathrm{s}, \quad \forall q \in \mathrm{Sp}(1). \tag{33}$$

Si $q \in \mathbb{H}$ est de norme 1, la réflexion orthogonale s_q de $\mathbb{H}$ par rapport à l'orthogonal de $q = \mathrm{L}_q(1)$ est donc donnée par la formule $\mathrm{s}_q = \mathrm{L}_q\,\mathrm{s}\,\mathrm{L}_{q^{-1}} = \mathrm{L}_q\,\mathrm{R}_{q^{-1}}\,\mathrm{s} = \mathrm{s}\,\mathrm{R}_q\,\mathrm{L}_{q^{-1}}$.

Proposition 2.6. *L'application* $\mathrm{Sp}(1) \times \mathrm{Sp}(1) \to \mathrm{O}(\mathbb{H}), (q_1, q_2) \mapsto \mathrm{L}_{q_1}\mathrm{R}_{q_2}$, *est un morphisme d'image* $\mathrm{SO}(\mathbb{H})$ *et de noyau d'ordre* 2, *engendré par* $(-1, -1)$.

Démonstration — L'application π de l'énoncé est un morphisme de groupes par la Formule (32). Si (q, q') est dans $\ker \pi$, on a d'abord $qh = hq'$ pour tout $h \in \mathbb{H}$ puis $q = q'$ (cas particulier $h = 1$), puis $q \in \mathbb{R}$ par la Proposition 2.1, et donc $q = q' \in \mathbb{R} \cap \mathrm{Sp}(1) = \{\pm 1\}$.

L'application $\mathrm{Sp}(1) \to \{\pm 1\}$, $q \mapsto \det \mathrm{L}_q$, est continue donc constante égale à 1, car $\mathrm{Sp}(1)$ est homéomorphe au connexe $\mathbb{S}^3$. On a donc $\mathrm{L}_q \in \mathrm{SO}(\mathbb{H})$, et de même $\mathrm{R}_q \in \mathrm{SO}(\mathbb{H})$. On en déduit $\mathrm{Im}\,\pi \subset \mathrm{SO}(\mathbb{H})$. On conclut par Cartan-Dieudonné car le produit de deux réflexions orthogonales de $\mathbb{H}$ de vecteurs unités quelconques q_1 et q_2 est dans l'image de π : on a $\mathrm{s}_{q_1}\,\mathrm{s}_{q_2} = \mathrm{L}_{q_1}\,\mathrm{R}_{q_1^{-1}}\,\mathrm{s}^2\,\mathrm{R}_{q_2}\,\mathrm{L}_{q_2^{-1}} = \mathrm{L}_{q_1 q_2^{-1}}\mathrm{R}_{q_1^{-1} q_2}$. □

Ainsi, le choix d'une base orthonormée de $\mathbb{H}$, par exemple $1, I, J, K$ pour fixer les idées, nous permet d'identifier $\mathrm{SO}(\mathbb{H})$ à $\mathrm{SO}(4)$, et nous fournit donc une s.e.c.

$$1 \to \mathbb{Z}/2\mathbb{Z} \to \mathrm{Sp}(1) \times \mathrm{Sp}(1) \to \mathrm{SO}(4) \to 1. \tag{34}$$

Le cas de la dimension 3 n'est pas en reste. Considérons le sous-espace euclidien

$$\mathbb{H}^0 = 1^\perp = \{q \in \mathbb{H} \mid \mathrm{t}(q) = 0\} = \mathbb{R}\,I + \mathbb{R}\,J + \mathbb{R}\,K.$$

Les éléments de $\mathbb{H}^0$ sont appelés *quaternions purs.*[14] Pour $q \in \mathbb{H}^\times$ et $x \in \mathbb{H}$, on pose $\mathrm{int}_q(x) = qxq^{-1}$. Autrement dit, on a $\mathrm{int}_q = \mathrm{L}_q\mathrm{R}_q$. C'est un élément de $\mathrm{SO}(\mathbb{H})$ fixant 1 : il préserve donc $\mathbb{H}^0$ et définit un élément de $\mathrm{SO}(\mathbb{H}^0)$.

Proposition 2.7. *L'application* $\mathrm{Sp}(1) \to \mathrm{SO}(\mathbb{H}^0), q \mapsto \mathrm{int}_{q|\mathbb{H}^0}$, *est un morphisme surjectif noyau d'ordre* 2 *engendré par* -1.

Démonstration — Soit π l'application de l'énoncé. C'est clairement un morphisme de groupes. Si $q \in \ker \pi$ on a $qh = hq$ pour tout $h \in \mathbb{H}$, donc $q \in \mathbb{R}^\times$ par la Proposition 2.1, puis $q = \pm 1$. Toute isométrie directe de $\mathbb{H}^0$ se prolonge uniquement en une isométrie directe de $\mathbb{H}$ fixant 1. Mais les isométries directes de $\mathbb{H}$ sont de la forme $\mathrm{L}_q\mathrm{R}_{q'}$ par la Proposition 2.6. Une telle isométrie fixe 1 si et seulement si on a $qq'^{-1} = 1$, *i.e.* $q' = q$ et donc π est surjectif. □

14. Le théorème de Cayley-Hamilton montre que l'on a $q \in \mathbb{H}^0$ si, et seulement si, $q^2 \in \mathbb{R}_{\leqslant 0}$.

Là encore, le choix d'une base orthonormée de $\mathbb{H}^0$, par exemple I, J, K pour fixer les idées, nous permet d'identifier $\mathrm{SO}(\mathbb{H}^0)$ à $\mathrm{SO}(3)$, et fournit donc une suite exacte

$$1 \to \mathbb{Z}/2\mathbb{Z} \to \mathrm{Sp}(1) \to \mathrm{SO}(3) \to 1. \tag{35}$$

Cette suite exacte est assez importante en mathématiques et en physique. Elle permet par exemple d'étudier la topologie de $\mathrm{SO}(3)$, vu comme fermé (en fait, compact) du sous-espace vectoriel $\mathrm{M}_3(\mathbb{R})$. Sans rentrer dans les détails, qui seront abordés dans d'autres cours, le morphisme $\mathrm{Sp}(1) \to \mathrm{SO}(3)$ est continu, et c'est même un revêtement à deux feuillets. Il montre que $\mathrm{SO}(3)$ est homéomorphe au quotient de S^3 par l'antipode $x \mapsto -x$: c'est l'espace projectif réel $\mathbb{P}(\mathbb{R}^4)$. En particulier, l'espace topologique $\mathrm{SO}(3)$ n'est pas *simplement connexe*, et son *revêtement universel* est la sphère S^3 (qui le recouvre avec deux feuillets).[15] Cela permet notamment de justifier mathématiquement le phénomène de torsion/détorsion du bras se produisant lorsque l'on fait faire deux tours complets à une tasse posée à plat dans sa main, ou encore le dénouage par translation d'une ceinture vrillée un nombre paire de fois (*expérience de la ceinture* de Dirac, comme sur cette animation issue du site analysis situs).

Remarque 2.8. Définissons $\mathrm{PSO}(n)$ comme le groupe quotient de $\mathrm{SO}(n)$ par son sous-groupe d'homothéties : on a $\mathrm{PSO}(n) = \mathrm{SO}(n)$ pour n impair et $\mathrm{PSO}(n) = \mathrm{SO}(n)/\{\pm 1\}$ pour n pair. Les suites exactes (35) et (34) montrent

$$\mathrm{PSO}(4) \simeq \mathrm{SO}(3) \times \mathrm{SO}(3).$$

Ce comportement est exceptionnel : on peut montrer que pour $n \geqslant 3$ et $n \neq 4$, le groupe $\mathrm{PSO}(n)$ est simple : voir les Exercices 5.14 et 5.16.

2.4. Sous-groupes finis de $\mathrm{Sp}(1)$**.** Nous allons maintenant utiliser la suite exacte (35) pour déterminer les sous-groupes finis de la sphère $\mathrm{Sp}(1)$. Fixons $\pi : \mathrm{Sp}(1) \to \mathrm{SO}(3)$ le morphisme ci-dessus, surjectif de noyau $\{\pm 1\}$. On sait que π^{-1} induit une bijection entre sous-groupes de $\mathrm{SO}(3)$ et sous-groupes de G contenant $\{\pm 1\}$. Pour tout sous-groupe G de $\mathrm{SO}(3)$, on posera $\widetilde{G} = \pi^{-1}(G)$. Par définition on a une suite exacte

$$1 \to \{\pm 1\} \to \widetilde{G} \xrightarrow{\pi} G \to 1.$$

En particulier on a $|\widetilde{G}| = 2|G|$ et $\{\pm 1\}$ est dans le centre de G.

Exemple 2.9. *Le sous-groupe* H_8 *de* $\mathrm{Sp}(1)$ *contient* ± 1. *Son image* $\pi(\mathrm{H}_8) \subset \mathrm{SO}(3)$ *est le groupe de Klein préservant chaque droite* $\mathbb{R}\,I$, $\mathbb{R}\,J$ *et* $\mathbb{R}\,K$. *Par exemple* $\mathrm{int}_I(I) = I$, $\mathrm{int}_I(J) = -J$ *et* $\mathrm{int}_I(K) = -K$.

Le théorème suivant ramène la classification des sous-groupes finis de $\mathrm{Sp}(1)$ à celle des sous-groupes de $\mathrm{SO}(3)$, déjà comprise.

Théorème 2.10. *Un sous-groupe fini de* $\mathrm{Sp}(1)$ *est soit d'ordre impair et cyclique, soit d'ordre pair et de la forme* $\widetilde{G}$ *pour un unique sous-groupe* G *de* $\mathrm{SO}(3)$.

15. En faisant agit $\mathrm{Sp}(1)$ sur la sphère euclidienne S^2 via le morphisme $\mathrm{Sp}(1) \to \mathrm{SO}(3)$ ci-dessus, on construit aussi une application continue $\mathrm{S}^3 \to \mathrm{S}^2$ de fibres homéomorphes à S^1 : c'est la *fibration de Hopf*, chère aux topologues.

Démonstration — On a déjà dit que $G \mapsto \widetilde{G}$ est une bijection entre sous-groupes (d'ordre n) de SO(3) et sous-groupes (d'ordre $2n$) de Sp(1) contenant -1.

Observons d'abord que H est d'ordre pair si, et seulement si, on a $-1 \in H$. En effet, si l'élément -1 (d'ordre 2) est dans H alors $|H|$ est pair par Lagrange. Réciproquement, si on a $|H|$ alors H possède un élément d'ordre 2, mais on sait que le seul élément d'ordre 2 de $\mathbb{H}^\times$ est -1 par la Proposition 2.4, on a donc $-1 \in H$.

Soit enfin H un sous-groupe fini de Sp(1) ne contenant pas -1, ou ce qui revient au même, d'ordre impair. Le morphisme $\pi_{|H} : H \to \mathrm{SO}(3)$ est alors injectif, donc $H \simeq \pi(H)$ est isomorphe à un sous-groupe d'ordre impair de SO(3). Mais on constate sur la classification de Klein que les seuls sous-groupes d'ordres impairs de SO(3) sont cycliques, donc H est cyclique. □

2.5. Groupes binaires des solides de Platon. Identifions encore l'espace euclidien $\mathbb{H}^0$ à l'espace euclidien standard $\mathbb{R}^3$ via la base orthonormée I, J, K. Soit $P \subset \mathbb{R}^3$ un solide de Platon centré en 0. Le sous-groupe

$$\widetilde{\mathrm{Iso}^+(P)}$$

est appelé *groupe binaire de* P, c'est un groupe intéressant ! Si P est un tétraèdre (resp. cube, octaèdre, dodécaèdre, icosaèdre), on a vu que $\mathrm{Iso}^+(P)$ est un A_4 (resp. S_4, S_4, A_5, A_5), de sorte que l'on note aussi

$$\widetilde{\mathrm{A}_4},\ \widetilde{\mathrm{S}_4} \text{ et } \widetilde{\mathrm{A}_5}$$

les 3 groupes binaires correspondants. L'abus de langage consistant à oublier le solide P est assez anodin. En effet, les groupes d'isométries directes de deux solides de Platon P et P' centrés en 0 supposés similaires ou duaux l'un de l'autre sont conjugués dans SO(3), disons $\mathrm{Iso}^+(P') = g\mathrm{Iso}^+(P)g^{-1}$ avec $g \in \mathrm{SO}(3)$. Par surjectivité de $\pi : \mathrm{Sp}(1) \to \mathrm{SO}(3)$ on peut choisir $q \in \mathrm{Sp}(1)$ vérifiant $\pi(q) = g$, et on constate

$$\widetilde{\mathrm{Iso}^+(P')} \;=\; q\,\widetilde{\mathrm{Iso}^+(P)}\,q^{-1}.$$

Ainsi, $\widetilde{\mathrm{A}_4}$, $\widetilde{\mathrm{S}_4}$ et $\widetilde{\mathrm{A}_5}$ sont des sous-groupes bien définis à conjugaison près dans Sp(1).

Exemple 2.11. (i) Le groupe $\widetilde{\mathrm{A}_4}$ est aussi appelé *groupe binaire tétraédral.* Il est d'ordre 24. Remarquer que $\widetilde{\mathrm{A}_4}$ n'est ni isomorphe à S_4, ni à $\mathrm{A}_4 \times \mathbb{Z}/2\mathbb{Z}$, qui ont eux de nombreux éléments d'ordre 2. On verra ci-dessous qu'il est conjugué dans Sp(1) au sous-groupe $\{\pm 1, \pm I, \pm J, \pm K, \frac{\pm 1 \pm I \pm J \pm K}{2}\}$ (inversibles des quaternions de Hurwitz), aussi étudié dans l'Exercice 5.33. Ce n'est pas tout : on verra aussi que $\widetilde{\mathrm{A}_4}$ est l'ensemble des sommets d'un 4-polytope régulier exceptionnel de $\mathbb{H}$, appelé 24 *cellules* : voir l'Exemple 5.6.

(ii) Les groupes $\widetilde{\mathrm{S}_4}$ et $\widetilde{\mathrm{A}_5}$, d'ordres respectifs 48 et 120, sont respectivement appelés *groupe binaire octaédral et icoscosaédral.* Comme il a un seul élément d'ordre 2, $\widetilde{\mathrm{S}_4}$ n'est pas isomorphe à $\mathrm{S}_4 \times \mathbb{Z}/2\mathbb{Z}$. De même, $\widetilde{\mathrm{A}_5}$ n'est pas isomorphe à S_5 ou à $\mathrm{A}_5 \times \mathbb{Z}/2\mathbb{Z}$. Enfin, on peut montrer que les 120 éléments de $\widetilde{\mathrm{A}_5} \subset \mathbb{H}$, aussi appelés *icosiens*, sont les sommets du fameux 600-cellules (voir le Théorème 5.5). L'espace quotient $\mathrm{Sp}(1)/\widetilde{\mathrm{A}_5}$ est bien connu des topologues : c'est la *sphère d'homologie* de Poincaré. [16]

16. C'est une variété compacte de dimension 3 ayant même groupes d'homologie singulière que la sphère $\mathbb{S}^3$, mais qui est non simplement connexe : son groupe fondamental est $\widetilde{\mathrm{A}_5}$.

Revisitons pour finir les groupes d'isométries des solides de Platon du point de vue des quaternions. C'est un bon exercice pour se familiariser avec les constructions ci-dessus. (Ce qui suit n'a pas été traité en classe). Considérons pour cela les éléments

$$\pm I, \pm J, \pm K$$

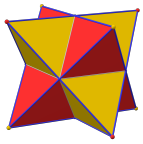
dans l'espace euclidien $\mathbb{H}^0$ de dimension 3. Ce sont manifestement les 6 sommets d'un octaèdre régulier O. Le dual de O est homothétique au cube C de sommets les

$$\pm I \pm J \pm K.$$

Partitionnons les sommets de ce cube C en les deux sous ensembles

$$\mathrm{C} = T^+ \coprod T^- \text{ avec } T^\pm = \{\epsilon_I I + \epsilon_J J + \epsilon_K K \mid \epsilon_I \epsilon_J \epsilon_K = \pm 1\}.$$

Ce sont les sommets de deux tétraèdres réguliers $\mathrm{T}^\pm$:



La conjugaison par $I \in \mathrm{Sp}(1)$ fixe I et envoie J sur $-J$ et K sur $-K$. Elle induit donc des isométries de O, C et $\mathrm{T}^\pm$, et de même pour celle par J et par K. L'image du morphisme $\mathrm{int} : \mathrm{H}_8 \to \mathrm{SO}(\mathbb{H}^0)$ est donc un groupe de Klein, inclus dans ces quatre groupes d'isométries. Posons

$$\omega = \frac{1}{2}(1 + I + J + K) \in \mathrm{Sp}(1).$$

Il est de trace 1, donc vérifie $\omega^2 - \omega + 1 = 0$, puis $\omega^3 = -1$ (ordre 6). Les 16 éléments distincts ωh et $\omega^{-1} h = \omega^\star h$, avec $h \in \mathrm{H}_8$, sont les

$$\frac{1}{2}(\pm 1 \pm I \pm J \pm K)$$

et sont aussi d'ordre 6 (cas de trace 1) ou 3 (cas de trace -1). Le même argument vaut bien sûr pour les $h\omega$ et $h\omega^\star$, et on constate en fait

$$\omega I = J\omega, \ \omega J = -K\omega \text{ et } \omega K = -I\omega.$$

En particulier, ω normalise H_8 et int_ω préserve aussi T^+ et T^- (et O et C). Posons

$$G_1 = \langle \mathrm{H}_8, \omega \rangle = \mathrm{H}_8 \coprod \omega \mathrm{H}_8 \coprod \omega^2 \mathrm{H}_8.$$

C'est un groupe d'ordre 24, et on a reconnu $G_1 = \mathrm{Hur}^\times$ de l'Exercice 5.33 Chap. 2. Le morphisme $\mathrm{int} : G_1 \to \mathrm{SO}(\mathbb{H}^0)$, de noyau ± 1, a son image d'ordre 12 et incluse dans $\mathrm{Iso}(T^\pm)$. On en déduit

$$\mathrm{int}(G_1) = \mathrm{Iso}^+(\mathrm{T}^+) =^+ \mathrm{Iso}(T^-) \simeq \mathrm{A}_4 \text{ et donc } \mathrm{Hur}^\times = G_1 \simeq \widetilde{\mathrm{A}_4}. \tag{36}$$

Regardons maintenant l'élément

$$\zeta = \frac{1 + I}{\sqrt{2}} \in \mathrm{Sp}(1).$$

On a $\zeta^2 = -I$: c'est une racine 8-ème de l'unité dans $\mathbb{H}^\times$. On constate

$$\zeta I = I\zeta, \ \zeta J = K\zeta, \ \zeta K = -J\zeta.$$

Donc ζ normalise G_1, int_ζ échange les tétraèdres T^+ et T^-, et préserve C et O. Soit

$$G_2 = \langle G_1, \zeta \rangle = G_1 \coprod \zeta G_1.$$

C'est un groupe d'ordre 48, et $\mathrm{int} : G_2 \to \mathrm{SO}(\mathbb{H}^0)$ a pour noyau ± 1 et son image d'ordre 24 et incluse dans $\mathrm{Iso}(\mathrm{C}) = \mathrm{Iso}(\mathrm{O})$. On en déduit

$$\mathrm{int}(G_2) = \mathrm{Iso}^+(\mathrm{C}) = \mathrm{Iso}^+(\mathrm{O}) \simeq \mathrm{S}_4 \text{ et donc } G_2 \simeq \widetilde{\mathrm{S}_4}. \tag{37}$$

Considérons enfin l'icosaèdre régulier I de $\mathbb{H}^0$ ayant pour sommets les

$$\pm J \pm \varphi K,\ \pm I \pm \varphi J \text{ et } \pm K \pm \varphi I,$$

avec φ le nombre d'or (voir l'Exercice 5.2). Explicitons, sans démonstration, le groupe $\mathrm{Iso}^+(\mathrm{I})$ et le groupe binaire associé. L'élément $\xi = \frac{1}{2}(\varphi + I + \varphi^{-1}J) \in \mathrm{Sp}(1)$ est de trace φ donc vérifie $\xi^2 - \varphi\xi + 1 = 0$ par Cayley-Hamilton. Il est donc d'ordre 10 car on a $\varphi = e^{i\pi/5} + e^{-i\pi/5}$ dans $\mathbb{C}$. Il n'est pas difficile de vérifier qu'il satisfait $\mathrm{int}_\xi(\mathrm{I}) = \mathrm{I}$. En posant $G_3 = \langle G_1, \xi \rangle$ on peut montrer que l'on a

$$\mathrm{int}(G_3) = \mathrm{Iso}^+(\mathrm{I}) \simeq \mathrm{A}_5 \text{ et donc } G_3 \simeq \widetilde{\mathrm{A}_5}. \tag{38}$$

3. Groupes linéaires et simplicité de $\mathrm{PSL}_n(k)$

Dans cette partie, on fixe un corps k un entier $n \geqslant 2$. Le groupe $\mathrm{GL}_n(k)$ contient $\mathrm{SL}_n(k)$ comme sous-groupe distingué, et det induit un isomorphisme

$$\mathrm{GL}_n(k)/\mathrm{SL}_n(k) \simeq k^\times.$$

Reste à étudier le dévissage de $\mathrm{SL}_n(k)$. On notera $\mathrm{Z}_n(k)$ le sous-groupe des homothéties dans $\mathrm{SL}_n(k)$. C'est un sous-groupe central, donc distingué, de $\mathrm{SL}_n(k)$. On a un isomorphisme de groupes

$$\mu_n(k) \xrightarrow{\sim} \mathrm{Z}_n(k), \lambda \mapsto \lambda 1_n,$$

avec $\mu_n(k) = \{x \in k^\times \mid x^n = 1\}$ (sous-groupe des racines n-ièmes de l'unité dans $k^\times$, un sous-groupe cyclique de $k^\times$ d'ordre divisant n). Notre but principal est de démontrer le résultat suivant, connu semble-t-il de Galois pour $n = 2$ et $k = \mathbb{Z}/p\mathbb{Z}$, et dû à Jordan et Dickson en général.

Théorème 3.1. *On suppose $n \geqslant 3$, ou $n = 2$ et $|k| > 3$. Alors tout sous-groupe distingué de $\mathrm{SL}_n(k)$ est égal à $\mathrm{SL}_n(k)$, ou est inclus dans $\mathrm{Z}_n(k)$.*

Pour $H \lhd G$, les sous-groupes distingués de G/H sont en bijection avec ceux de G contenant H. On en déduit, posant $\mathrm{PSL}_n(k) = \mathrm{SL}_n(k)/\mathrm{Z}_n(k)$:

Corollaire 3.2. *Sous les même hypothèses, le groupe $\mathrm{PSL}_n(k)$ est simple.*

Nous reviendrons sur les deux cas $n = 2$ et $k = \mathbb{Z}/2\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z}$ un peu plus loin.

3.1. Transvections. Tout comme dans l'étude des groupes S_n et $\mathrm{O}(n)$, les éléments de $\mathrm{SL}_n(k)$ ayant un maximum de points fixes, c'est-à-dire un hyperplan fixe, joueront un rôle particulièrement important.

Définition 3.3. *Soit V un k-espace vectoriel de dimension $n \geqslant 2$. Une transvection de V est un élément t de $\mathrm{SL}(V)$ tel que $\dim \ker(t - \mathrm{id}_V) = n - 1$, ou ce qui revient au même, tel que $t - \mathrm{id}_V$ est de rang 1.*

Exemple 3.4. (*Transvections standards de* $\mathrm{SL}_n(k)$) Ce sont les matrices de la forme $\mathrm{T}_{i,j}(\lambda) := \mathrm{I}_n + \lambda \mathrm{E}_{i,j}$ avec $\lambda \in k^\times$ et $1 \leqslant i \neq j \leqslant n$ (pour avoir $\det \mathrm{T}_{i,j}(\lambda) = 1$). La transvection standard $\mathrm{T}_{i,j}(\lambda)$ est une transvection de k^n d'hyperplan fixe $x_j = 0$. Il sera commode d'en choisir une, c'est pourquoi on pose

$$\mathrm{t}_n := \mathrm{T}_{n,n-1}(1) = \begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & 1 \\ & & & 1 \end{bmatrix}$$

Non seulement les transvections engendrent $\mathrm{SL}_n(k)$, mais on a :

Proposition 3.5. *Les transvections standards engendrent* $\mathrm{SL}_n(k)$.

Démonstration — C'est un argument classique d'opérations sur les lignes et les colonnes (*pivot de Gauss*), qui sera revu plus tard dans le cours dans le contexte plus général des anneaux euclidiens : voir le Théorème 4.1 Chap. 8. □

Soit H un hyperplan de V fixé. Décrivons les transvections d'hyperplan fixe H. Fixons pour cela $e = (e_1, \ldots, e_n)$ une base de V avec $H = \mathrm{Vect}_k(e_1, \ldots, e_{n-1})$. Un élément t de $\mathrm{SL}(V)$ vaut l'identité sur H si et seulement si il existe $x \in k^{n-1}$ avec

$$\mathrm{Mat}_e\, t = \begin{bmatrix} 1_{n-1} & x \\ 0 & 1 \end{bmatrix} \in \mathrm{SL}_n(k) \tag{39}$$

L'image de $t - \mathrm{id}_V$ est alors engendrée par $v := \sum_{i=1}^{n-1} x_i e_i$, qui est un vecteur quelconque de H. Ainsi, t est une transvection si, et seulement si, on a $v \neq 0$.

Proposition 3.6. *Les transvections sont conjuguées dans* $\mathrm{GL}_n(k)$*, et pour* $n > 2$ *elles sont conjuguées dans* $\mathrm{SL}_n(k)$.

Démonstration — Soit t une transvection d'hyperplan fixe H. Pour $g \in \mathrm{GL}(V)$ on a $\det(gtg^{-1}) = \det t = 1$, et $gtg^{-1} - \mathrm{id}_V = g(t - \mathrm{id}_V)g^{-1}$ a même rang que $t - 1_V$ (et pour noyau l'hyperplan $g(H)$). Le conjugué par $\mathrm{GL}(V)$ d'une transvection est donc une transvection.

Soit maintenant t une transvection de V d'hyperplan fixe H. Fixons $e_n \in V \smallsetminus H$ arbitrairement. L'élément $e_{n-1} := t(e_n) - e_n$ est dans H par la discussion ci-dessus. Complétons-le en une base $e_1, \ldots, e_{n-1}$ de H. On constate que dans la base $\mathrm{e} = (e_1, \ldots, e_n)$, la matrice de t est t_n. On a montré que toute transvection dans $\mathrm{GL}_n(k)$ est conjuguée à t_n, d'où le premier point.

Pour le second, soit $t \in \mathrm{SL}_n(k)$ une transvection. On a montré qu'il existe $g \in \mathrm{GL}_n(k)$ tel que $gtg^{-1} = \mathrm{t}_n$. Observons que pour $n > 2$, et tout $\lambda \in k^\times$, il existe $h \in \mathrm{GL}_n(k)$ qui commute avec t_n et tel que $\det h = \lambda$: l'élément $\mathrm{diag}(\lambda, 1, \ldots, 1)$ convient ! Prenant un tel h pour $\lambda = (\det g)^{-1}$, on a alors $(hg)t(hg)^{-1} = \mathrm{t}_n$ et $\det hg = \lambda \det g = 1$. □

Remarque 3.7. *On peut montrer que pour* $x, y \in k$*, les transvections standards* $\left[\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right]$ *et* $\left[\begin{smallmatrix} 1 & y \\ 0 & 1 \end{smallmatrix}\right]$ *sont conjuguées dans* $\mathrm{SL}_2(k)$ *si, et seulement si, on a* $y = u^2 x$ *pour un certain* $u \in k^\times$ *(voir l'Exercice 5.41). Par exemple,* $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$ *et* $\left[\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right]$ *sont conjuguées dans* $\mathrm{GL}_2(\mathbb{R})$ *mais pas dans* $\mathrm{SL}_2(\mathbb{R})$.

3.2. Centre et groupe dérivé de $\mathrm{SL}_n(k)$. En guise de premier pas vers le Théorème 3.1, on étudie le centre et le groupe dérivé de $\mathrm{SL}_n(k)$.

PROPOSITION 3.8. *Soit $g \in \mathrm{GL}_n(k)$. Il y a équivalence entre :*

(i) g commute avec tous les éléments de $\mathrm{SL}_n(k)$,

(ii) g préserve toutes les droites de k^n,

(iii) g est une homothétie.

DÉMONSTRATION — On peut supposer $n \geqslant 2$ car les trois propriétés sont toujours satisfaites pour $n = 1$. De plus, l'implication (iii) $\Longrightarrow$ (i) est évidente. Montrons (i) $\Longrightarrow$ (ii). Pour tout vecteur $v \in k^n$ non nul, et pour tout choix d'hyperplan H de k^n contenant v, l'analyse plus haut montre qu'il existe une transvection $t \in \mathrm{SL}_n(k)$ d'hyperplan fixe H telle que $\mathrm{Im}(t - \mathrm{I}_n) = kv$. Comme g commute avec t, alors g préserve $\mathrm{Im}(t - \mathrm{id})$, et donc la droite kv, ce qui montre (ii). Montrons enfin (ii) $\Longrightarrow$ (iii). Soient $e_1, \ldots, e_n$ une base de k^n et $w = \sum_i e_i$. On a $g(e_i) = \lambda_i e_i$ avec $\lambda_i \in k^\times$, et $g(w) = \lambda w$, donc $\lambda = \lambda_i$ pour tout i. □

COROLLAIRE 3.9. *Le centre de $\mathrm{GL}_n(k)$ est $k^\times 1_n$, et celui de $\mathrm{SL}_n(k)$ est $\mathrm{Z}_n(k)$.*

PROPOSITION 3.10. *On suppose $n \neq 2$ ou $|k| > 3$. On a*

$$\mathrm{D}(\mathrm{GL}_n(k)) = \mathrm{SL}_n(k) \text{ et } \mathrm{D}(\mathrm{SL}_n(k)) = \mathrm{SL}_n(k).$$

DÉMONSTRATION — Le morphisme déterminant $\det : \mathrm{GL}_n(k) \to k^\times$, et la commutativité de $k^\times$, montrent que l'on a $\mathrm{D}(\mathrm{GL}_n(k)) \subset \ker \det = \mathrm{SL}_n(k)$. Il suffit donc de montrer $\mathrm{SL}_n(k) \subset \mathrm{D}(\mathrm{SL}_n(k))$.

Observons qu'il suffit de montrer qu'il existe une transvection de $\mathrm{SL}_n(k)$ qui est un commutateur. En effet, si on a $t = [x, y]$ avec $x, y \in \mathrm{SL}_n(k)$, alors pour tout $g \in \mathrm{GL}_n(k)$ on a

$$gtg^{-1} = \mathrm{int}_g(t) = [\mathrm{int}_g(x), \mathrm{int}_g(y)]$$

avec $\mathrm{int}_g(x)$ et $\mathrm{int}_g(y)$ dans $\mathrm{SL}_n(k)$, puisque $\mathrm{SL}_n(k)$ est distingué dans $\mathrm{GL}_n(k)$. L'observation découle alors du fait que les transvections sont conjuguées sous $\mathrm{GL}_n(k)$ (Proposition 3.6).

Pour $\mu \in k^\times$, on constate l'identité dans $\mathrm{SL}_2(k)$

$$[\begin{pmatrix} \mu & 0 \\ 0 & \mu^{-1} \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}] = \begin{pmatrix} 1 & \mu^2 - 1 \\ 0 & 1 \end{pmatrix} \tag{40}$$

Si $|k| > 3$, il existe $\mu \in k^\times \smallsetminus \{\pm 1\}$, et donc $\mu^2 \neq 1$. Ainsi, on a trouvé une transvection standard qui est un commutateur dans $\mathrm{SL}_2(k)$. Supposons donc $n \geqslant 3$. Pour $h \in \mathrm{SL}_{n-1}(k)$ et $v \in k^{n-1}$ on a

$$[\begin{pmatrix} h & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \mathrm{I}_{n-1} & v \\ 0 & 1 \end{pmatrix}] = \begin{pmatrix} \mathrm{I}_{n-1} & hv - v \\ 0 & 1 \end{pmatrix} \tag{41}$$

Pour $n \geqslant 3$, il existe $g \in \mathrm{SL}_{n-1}(k)$ qui n'est pas l'identité ! Choisissant v tel que $gv \neq v$, le commutateur ci-dessus est une transvection. □

3.3. Le critère de simplicité d'Iwasawa. Pour démontrer le Théorème 3.1 nous allons utiliser un critère de simplicité découvert par K. Iwasawa. Formulé de manière optimale (voir l'Exercice 5.36), ce critère semble curieusement permettre de démontrer théoriquement la simplicité de tous les groupes simples finis ! [17]

PROPOSITION 3.11. (Critère de simplicité d'Iwasawa) *Soit G un groupe agissant 2-transitivement sur l'ensemble X. On suppose qu'il existe $x \in X$ et $A \subset G_x$ avec :*

(i) A est un sous-groupe abélien et distingué de G_x,

(ii) $\cup_{g \in G} gAg^{-1}$ engendre G.

Si N est un sous-groupe distingué de G, alors soit N contient $\mathrm{D}(G)$, soit N est inclus dans le noyau de l'action de G sur X.

EXEMPLE 3.12. Esquissons comment retrouver la simplicité de A_5 par cette proposition et le fait (plus simple) $\mathrm{D}(\mathrm{A}_5) = \mathrm{A}_5$. Noter que A_5 agit 2-transitivement sur $\{1, 2, 3, 4, 5\}$. De plus, le stabilisateur du point 5 est $\simeq \mathrm{A}_4$, qui contient le sous-groupe abélien distingué $\mathrm{K}_4 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Mais les doubles transpositions sont conjuguées dans A_5, et on vérifie qu'elles engendrent A_5. Cela conclut !

DÉMONSTRATION — Soit K le noyau de l'action de G sur X. Soit N un sous-groupe distingué de G non inclus dans K. Montrons que l'action de N sur X est transitive. Fixons $x \in X$ (arbitraire) et regardons la N-orbite de x, disons Nx. Elle est stable par G_x : en effet, pour $g \in G_x$ on a $gNx = gNg^{-1}gx = Nx$ car N est distingué dans G. Mais G_x agit transitivement sur $X \smallsetminus \{x\}$ car G agit 2-transitivement sur X. On en déduit que si $Nx \neq \{x\}$ alors $Nx = X$. Mais si $Nx = \{x\}$ pour tout $x \in X$, alors on a $N \subset K$. On a bien montré que N agit transitivement sur X.

Fixons maintenant x dans X comme dans l'énoncé. On a $G = NG_x$. En effet, pour tout $g \in G$, l'élément gx est de la forme nx avec $n \in N$, et donc $n^{-1}g \in G_x$, puis $g \in NG_x$. Fixons x, et $A \lhd G_x$ comme dans l'énoncé. Pour $g \in G$ on a vu $g = nh$ avec $n \in N$ et $h \in G_x$, et donc

$$gAg^{-1} = nhAh^{-1}n^{-1} = nAn^{-1}$$

car A est distingué dans G_x. On déduit de (ii) que les nAn^{-1} avec $n \in N$ engendrent G, et en particulier $G = \langle N, A \rangle = NA$ par $N \lhd G$. Ainsi, le morphisme $A \to G/N, a \mapsto aN$, est surjectif, donc G/N est abélien car A l'est, et donc N contient $\mathrm{D}(G)$. □

3.4. Démonstration du Théorème 3.1. On peut supposer $n \geqslant 2$. Faisons agir $\mathrm{GL}_n(k)$ sur l'ensemble X des droites vectorielles de k^n. Elle est 2-transitive, et ce même restreinte à $\mathrm{SL}_n(k)$. En effet, si (e_1, e_2) et (f_1, f_2) sont deux couples de vecteurs linéairement indépendants de k^n, on peut les compléter en des bases e_i et f_i, et il existe $g \in \mathrm{GL}_n(k)$ avec $g(ke_i) = kf_i$ pour tout i. Quitte à composer g à la source par un élément de $\mathrm{GL}_n(k)$ diagonal dans la base e_i, on peut supposer $g \in \mathrm{SL}_n(k)$.

17. Formulé en terme d'action primitive comme dans les exercices, il s'agirait de savoir si pour tout groupe simple fini non abélien, il existe un sous-groupe maximal possédant un sous-groupe abélien distingué non trivial. C'est loin d'être évident, mais cela semble vrai par la classification des groupes simples finis s'il on croit ce post Mathoverflow de Derek Holt.

Regardons par exemple le vecteur $e = (1, 0, 0, \ldots, 0)$. Le stabilisateur de ke dans $\mathrm{SL}_n(k)$ est le sous-groupe P des matrices de la forme

$$p_{g,x} = \begin{pmatrix} \det g^{-1} & x \\ 0 & g \end{pmatrix}$$

avec $g \in \mathrm{GL}_{n-1}(k)$ et x un vecteur ligne dans k^{n-1}. On a $p_{g,x}p_{g',x'} = p_{gg',x''}$ avec $x'' = (\det g)^{-1}x' + gx$. On a donc une suite exacte courte naturelle (scindée !)

$$1 \to k^n \xrightarrow{x \mapsto p_{1,x}} P \xrightarrow{p_{g,x} \mapsto g} \mathrm{GL}_{n-1}(k) \to 1.$$

De sorte que $A := \{p_{1,x},\ x \in k^{n-1}\}$ est un sous-groupe distingué de P isomorphe à $(k^{n-1}, +)$ (donc abélien). Noter que A contient par exemple les transvections standards $\mathrm{T}_{1,j}(\lambda)$ avec $\lambda \in k^\times$ et $j > 1$ (en fait tout élément non trivial de A est une transvection !). Mais les $\mathrm{SL}_n(k)$-conjugués de ces transvections engendrent $\mathrm{SL}_n(k)$. En effet, pour $n \geqslant 3$ cela découle de la Proposition 3.6. Pour $n = 2$, cela vient de ce que pour $w = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{SL}_2(k)$ on a $w\mathrm{T}_{1,2}(\lambda)w^{-1} = \mathrm{T}_{2,1}(-\lambda)$, puis de la Proposition 3.5. On a montré que A vérifie les conditions (i) et (ii) d'Iwasawa.

Ainsi, le critère d'Iwasawa s'applique, et montre que tout sous-groupe distingué de $\mathrm{SL}_n(k)$ contient soit $\mathrm{D}(\mathrm{SL}_n(k)) = \mathrm{SL}_n(k)$ (Proposition 3.10 (ii)), soit est inclus dans le noyau de l'action, à savoir $\mu_n(k)$ (Proposition 3.8).

La même démonstration (en plus simple), montre aussi :

Corollaire 3.13. *Sous les même hypothèses, tout sous-groupe distingué de* $\mathrm{GL}_n(k)$ *est soit inclus dans* $k^\times$*, soit contient* $\mathrm{SL}_n(k)$.

Remarque 3.14. Les sous-groupes de $\mathrm{GL}_n(k)$ contenant $\mathrm{SL}_n(k)$ s'identifient à ceux de $\mathrm{GL}_n(k)/\mathrm{SL}_n(k) \simeq k^\times$ (surjectivité du déterminant). Comme $k^\times$ est abélien, ils sont tous distingués.

3.5. Groupes linéaires sur les corps finis. Lorsque k est un corps fini, le Théorème 3.1 fournit donc une série doublement infinie de groupes simples finis. On sait depuis Galois que le cardinal q d'un corps fini est toujours de la forme $q = p^n$ avec p premier et $n \geqslant 1$, et que pour tout tel q il existe un unique tel que corps à isomorphisme près, noté génériquement $\mathbb{F}_q$. On peut prendre bien sûr $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ pour p premier. On a aussi $\mathbb{F}_4 = \{0, 1, \omega, 1 + \omega\}$ avec $\omega^2 = \omega + 1$. Ces corps seront étudiés dans le cours Algèbre 2. Le cas $q = p$ sera déjà suffisamment riche pour nous ! Depuis Artin, les théoriciens des groupes notent souvent $\mathrm{L}_n(q)$ le groupe $\mathrm{PSL}_n(\mathbb{F}_q)$, une notation pratique mais qui prête à confusion (et peu utilisée hors de ce sujet).

Lemme 3.15. *Si k est un corps fini à q éléments, on a*

$$|\mathrm{GL}_n(k)| = \prod_{i=0}^{n-1}(q^n - q^i) = q^{\frac{n(n-1)}{2}} \prod_{i=1}^{n}(q^i - 1).$$

Démonstration — Une matrice $M \in \mathrm{M}_n(k)$ est inversible si, et seulement si, ses colonnes forment une k-base de k^n. Il s'agit donc de dénombrer les bases ordonnées $e_1, e_2, ..., e_n$ de k^n. L'élément e_1 est quelconque non nul ($q^n - 1$ possibiliés), et pour $i = 2, ..., n$, on choisit récursivement e_i arbitrairement hors du sous-espace de dimension $i - 1$ engendré par les e_j avec $j < i$: il y a $q^n - q^{i-1}$ possibilités. $\square$

Toujous sous l'hypothèse que k a un nombre fini q d'éléments, on en déduit les cardinaux de $\mathrm{SL}_n(k)$ et $\mathrm{PSL}_n(k)$. En effet, la surjectivité du déterminant $\mathrm{GL}_n(k) \to k^\times$, et $|k^\times| = q-1$, montrent

$$|\mathrm{SL}_n(k)| = \frac{|\mathrm{GL}_n(k)|}{q-1} = q^{\frac{n(n-1)}{2}} \prod_{i=2}^{n} (q^i - 1). \tag{42}$$

De plus, le groupe multiplicatif $k^\times$ est cyclique car k est fini d'après le Théorème 5.1 Chap. 2. On en déduit $|\mu_m(k)| = n \wedge (q-1)$ puis

$$|\mathrm{PSL}_n(k)| = \frac{|\mathrm{SL}_n(k)|}{m} \text{ avec } m = |\mu_n(k)| = n \wedge (q-1). \tag{43}$$

3.6. Le groupe $\mathrm{PGL}_n(k)$ versus $\mathrm{PSL}_n(k)$. On pose aussi

$$\mathrm{PGL}_n(k) = \mathrm{GL}_n(k)/k^\times.$$

On pose $k^{\times,n} = (k^\times)^{(n)} = \{x^n \mid x \in k^\times\}$ pour des raisons de lisibilité.

Proposition 3.16. *On a une suite exacte courte naturelle*

$$1 \to \mathrm{PSL}_n(k) \longrightarrow \mathrm{PGL}_n(k) \longrightarrow k^\times/k^{\times,n} \to 1.$$

Démonstration — Notons Z le sous-groupe des homothéties de $\mathrm{GL}_n(k)$, on a $Z \simeq k^\times$. En composant l'injection naturelle $\mathrm{SL}_n(k) \to \mathrm{GL}_n(k)$ avec la projection naturelle $\mathrm{GL}_n(k) \to \mathrm{PGL}_n(k)$, on obtient un morphisme naturel $\mathrm{SL}_n(k) \to \mathrm{PGL}_n(k), g \mapsto gZ$. Il a pour noyau $Z \cap \mathrm{SL}_n(k) = \mathrm{Z}_n(k)$. Il induit donc un morphisme injectif

$$\mathrm{PSL}_n(k) \xrightarrow{i} \mathrm{PGL}_n(k),\ g\mathrm{Z}_n(k) \mapsto gZ.$$

D'autre part, on composant le déterminant $\mathrm{GL}_n(k) \to k^\times$ (surjectif) et la projection canonique $k^\times \to k^\times/k^{\times,n}$, on obtient un morphisme surjectif $f : \mathrm{GL}_n(k) \to k^\times/k^{\times,n}, g \mapsto (\det g)\, k^{\times,n}$. Comme on a $\det Z \subset k^{\times,n}$, ce morphisme f se factorise en

$$\pi : \mathrm{PGL}_n(k) \to k^\times/k^{\times,n}, gZ \mapsto (\det g) k^{\times,n},$$

toujours un morphisme surjectif. Observons que pour $g \in \mathrm{GL}_n(k)$, on a $\det g \in k^{\times,n} \iff \exists \lambda \in Z,\ g\lambda \in \mathrm{SL}_n(k)$ (pourquoi ?). On en déduit bien $\ker \pi = \operatorname{Im} i$. □

On verra souvent $\mathrm{PSL}_n(k)$ comme un sous-groupe (distingué) de $\mathrm{PGL}_n(k)$ via l'injection naturelle i introduite ci-dessus.

Exemple 3.17. *(i) Si le sous-groupe des carrés de $k^\times$ est d'indice 2, par exemple pour $k = \mathbb{R}$ ou $k = \mathbb{Z}/p\mathbb{Z}$ avec $p > 2$, alors $\mathrm{PSL}_2(k)$ est un sous-groupe d'indice 2 dans $\mathrm{PGL}_2(k)$.*

(ii) Le groupe $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ est d'ordre $p(p-1)(p+1) = p^3 - p$.

(iii) Les groupes $\mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})$ et $\mathrm{PGL}_n(\mathbb{Z}/p\mathbb{Z})$ ont même cardinal. Ils sont isomorphes si, et seulement si, n est premier à $p-1$. En effet, cette condition est nécessaire car le centre de $\mathrm{PGL}_n(\mathbb{Z}/p\mathbb{Z})$ est trivial, alors que celui $\mathrm{Z}_n(\mathbb{Z}/p\mathbb{Z})$ de $\mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})$ l'est si et seulement si on a $\mu_n(\mathbb{Z}/p\mathbb{Z}) = \{1\}$, *i.e.* n premier à $p-1$. Elle est suffisante car le morphisme naturel $\mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z}) \to \mathrm{PGL}_n(\mathbb{Z}/p\mathbb{Z})$ est alors injectif entre deux groupes de même cardinal, et donc bijectif.

4. Le groupe $\mathrm{PGL}_2(k)$ et quelques (iso)morphismes miraculeux

Regardons $\mathrm{PGL}_2(k)$ d'un peu plus près. Considérons pour cela l'ensemble $\mathrm{P}^1(k)$ des droites vectorielles du plan vectoriel k^2 (*droite projective sur* k). Posons

$$\widehat{k} \quad = \quad k \coprod \{\infty\}.$$

(pas de confusion possible avec un dual ici !). On définit $\beta : \widehat{k} \to \mathrm{P}^1(k)$ par

$$\beta(x) \;=\; k\begin{pmatrix} x \\ 1 \end{pmatrix} \;\; \forall\, x \in k, \;\; \text{et} \;\; \beta(\infty) \;=\; k\begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Comme toute les droites vectorielles de k^2 sont de cette forme de manière unique, on a montré :

Lemme 4.1. *L'application β est une bijection $\widehat{k} \xrightarrow{\sim} \mathrm{P}^1(k)$.*

Comme on l'a déjà dit, le groupe $\mathrm{GL}_2(k)$ agit naturellement, et transitivement, sur $\mathrm{P}^1(k)$. Cette action n'est pas fidèle : par la Proposition 3.8, son noyau est le sous-groupe $k^\times$ des homothéties, de sorte que le groupe $\mathrm{PGL}_2(k)$ agit fidèlement sur $\mathrm{P}^1(k)$. Par transport de structure via β il agit donc sur $\widehat{k}$ (formule : $g.x = \beta^{-1}(g\beta(x))$). Pour cette action, l'élément $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $\mathrm{GL}_2(k)$ envoie le point $x \in \widehat{k}$ sur l'élément

$$g.x = \frac{ax+b}{cx+d} \in \widehat{k}$$

avec l'interprétation usuelle de ce quotient quand $cx+d$ est nul ou $x = \infty$. En effet, soit $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ dans $\mathrm{GL}_2(k)$. Pour $x \in k$ et $cx+d \neq 0$, on a

$$g\begin{pmatrix} x \\ 1 \end{pmatrix} \;=\; \begin{pmatrix} ax+b \\ cx+d \end{pmatrix} \;=\; (cx+d)\begin{pmatrix} \frac{ax+b}{cx+d} \\ 1 \end{pmatrix}, \tag{44}$$

ainsi que $g.(-c/d) = \infty$. De même, on a $g\begin{pmatrix} 0 \\ 1 \end{pmatrix} \;=\; \begin{pmatrix} a \\ c \end{pmatrix}$, donc $g.\infty = a/c$ pour $c \neq 0$ et $g.\infty = \infty$ pour $c = 0$.

Définition 4.2. *Les bijections de $\widehat{k}$ de la forme $x \mapsto \frac{ax+b}{cx+d}$ avec $ad - bc \neq 0$ sont appelées homographies. Elles forment un sous-groupe de $\mathrm{S}_{\widehat{k}}$ isomorphe à $\mathrm{PGL}_2(k)$.*

Par exemple $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ correspond à l'homographie affine $x \mapsto ax+b$ sur k (fixant ∞), et $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ à *l'inversion* $x \mapsto 1/x$. On a déjà vu au cours précédent que $\mathrm{PGL}_n(k)$ agit 2-transitivement sur $\mathrm{P}(k^n)$ pour $n \geqslant 2$. Pour $n = 3$ il y a mieux : le groupe $\mathrm{PGL}_2(k)$ agit exactement 3 fois transitivement sur l'ensemble $\mathrm{P}^1(k)$.

Proposition 4.3. *Pour tout triplet (α, β, γ) de points distincts dans $\widehat{k}$, il existe une et une seule homographie $g \in \mathrm{PGL}_2(k)$ telle que $(g(\alpha), g(\beta), g(\gamma)) = (0, 1, \infty)$.*

Cette proposition conduit naturellement à la notion de *birapport*, qui sera abordée en TD.

Démonstration — En effet, $\mathrm{PGL}_2(k)$ agit manifestement transitivement sur $\widehat{k}$, donc on peut supposer $\gamma = \infty$. Le stabilisateur de ∞ dans $\mathrm{PGL}_2(k)$ est exactement l'ensemble des homographies affines, de la forme $x \mapsto ax+b$ avec $a \neq 0$. L'unique telle transformation envoyant (α, β) sur $(0, 1)$ est $x \mapsto (x-\alpha)/(\beta-\alpha)$. $\square$

Exemple 4.4. (*Action de* $\mathrm{SL}_2(\mathbb{R})$ *sur le demi-plan de Poincaré*) L'ensemble $\widehat{\mathbb{C}}$ peut aussi être vu comme la *sphère de Riemann*. Le sous-groupe $\mathrm{GL}_2(\mathbb{R}) \subset \mathrm{GL}_2(\mathbb{C})$ agit sur $\widehat{\mathbb{C}}$ par restriction, en préservant $\widehat{\mathbb{R}}$, ainsi donc son complémentaire $\widehat{\mathbb{C}} \smallsetminus \widehat{\mathbb{R}} = \mathbb{C} - \mathbb{R}$. Cet ouvert de $\mathbb{C}$ a deux composantes connexes, l'une d'elles étant l'ouvert $\mathbb{H} = \{\tau \in \mathbb{C} \mid \operatorname{Im} \tau > 0\}$ appelé *demi-plan de Poincaré*. On vérifie facilement [18] que $\mathbb{H}$ est préservé par $\mathrm{SL}_2(\mathbb{R})$. Cette action est particulièrement importante en géométrie hyperbolique et en théorie des nombres.

Pour p premier, l'action fidèle de $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ sur l'ensemble $\mathrm{P}^1(\mathbb{Z}/p\mathbb{Z}) \simeq \widehat{\mathbb{Z}/p\mathbb{Z}}$ à $p+1$ éléments définit donc un morphisme injectif

$$\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z}) \hookrightarrow \mathrm{S}_{p+1}. \tag{45}$$

Il est particulièrement intéressant pour les petites valeurs de p. En effet, on a l'égalité $(p+1)! = (p+1)p(p-1)(p-2)!$, de sorte que (miracle !) :

Corollaire 4.5. *Pour* $p = 2$ *et* $p = 3$, *le morphisme* (45) *induit des isomorphismes* $\mathrm{PGL}_2(\mathbb{Z}/2\mathbb{Z}) \simeq \mathrm{S}_3$ *et* $\mathrm{PGL}_2(\mathbb{Z}/3\mathbb{Z}) \simeq \mathrm{S}_4$.

Noter que les morphismes naturels

$$\mathrm{PSL}_2(\mathbb{Z}/2\mathbb{Z}) \leftarrow \mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}) \rightarrow \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \rightarrow \mathrm{PGL}_2(\mathbb{Z}/2\mathbb{Z})$$

sont tous des isomorphismes ! Ainsi, tous ces groupes sont isomorphes à S_3. Cela explique pourquoi $\mathrm{PSL}_2(\mathbb{Z}/2\mathbb{Z})$ n'est pas simple. De même, $\mathrm{PSL}_2(\mathbb{Z}/3\mathbb{Z})$ est d'indice 2 dans $\mathrm{PGL}_2(\mathbb{Z}/3\mathbb{Z}) \simeq \mathrm{S}_4$, et donc on a (Exercice 4.2 Chap. 4)

$$\mathrm{PSL}_2(\mathbb{Z}/3\mathbb{Z}) \simeq \mathrm{A}_4,$$

qui est non simple. Cela justifie les exceptions dans l'énoncé du Théorème 3.1. Ce n'est pas tout, le cas $p = 5$ est également intéressant ! En effet, on a $|\mathrm{PGL}_2(\mathbb{Z}/5\mathbb{Z})| = 120 = |\mathrm{S}_6|/6$, de sorte que $\mathrm{PGL}_2(\mathbb{Z}/5\mathbb{Z})$ est isomorphe à un sous-groupe d'indice 6 de S_6. Mais (pour $n \geqslant 2$) on a la :

Proposition 4.6. *Tout sous-groupe d'indice* n *de* S_n *est isomorphe à* S_{n-1}.

Démonstration — Soit H un sous-groupe d'indice n de S_n. Faisons agit S_n par translations sur l'ensemble $X = \mathrm{S}_n/H$ à n éléments. Identifions X à $\{1, 2, \ldots, n\}$ en faisant correspondre à $H \in X$ l'élément $n \in \{1, \ldots, n\}$. On en déduit un morphisme $f : \mathrm{S}_n \to \mathrm{S}_n$ tel que $f(H)$ est le stabilisateur de l'élément n dans $f(\mathrm{S}_n)$. Mais f est injectif par le Lemme 5.3 Chap. 4, donc un isomorphisme pour des raisons de cardinal. On a donc $f(\mathrm{S}_n) = \mathrm{S}_n$, $f(H) = \mathrm{S}_{n;n} \simeq \mathrm{S}_{n-1}$, et $H \simeq f(H)$. □

Corollaire 4.7. $\mathrm{PGL}_2(\mathbb{Z}/5\mathbb{Z})$ *est isomorphe à* S_5.

L'action transitive de $\mathrm{PGL}_2(\mathbb{Z}/5\mathbb{Z}) \simeq \mathrm{S}_5$ sur l'ensemble à 6 éléments $\mathrm{P}^1(\mathbb{Z}/5\mathbb{Z})$ est alors une autre réalisation de l'action exotique de S_5 ! Nous renvoyons au Complément §10 Chap. 4 pour une justification et une remarque sur cette assertion. Comme le sous-groupe $\mathrm{PSL}_2(\mathbb{Z}/5\mathbb{Z})$ est d'indice 2 dans $\mathrm{PGL}_2(\mathbb{Z}/5\mathbb{Z}) \simeq \mathrm{S}_5$, on en déduit

$$\mathrm{PSL}_2(\mathbb{Z}/5\mathbb{Z}) \simeq \mathrm{A}_5,$$

18. Pour $g \in \mathrm{GL}_2(\mathbb{R})$ et $z \in \mathbb{C} - \mathbb{R}$, on a la formule $\operatorname{Im} g.z = \det g \, \frac{\operatorname{Im} z}{|cz+d|^2}$. Sans calcul, on peut aussi utiliser la connexité de $\mathrm{SL}_2(\mathbb{R})$.

un isomophisme là encore exceptionnel. En effet, cela ne se reproduit plus pour p plus grand :

PROPOSITION 4.8. *Soient $n, p \geqslant 5$ avec p premier. On a $\mathrm{A}_n \simeq \mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ si, et seulement si, $n = p = 5$.*

DÉMONSTRATION — Observons que l'élément t_2 est d'ordre p dans $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ (car $p \neq 2$). Ainsi, si on a un isomorphisme $\mathrm{A}_n \simeq \mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ alors A_n possède un élément d'ordre p. Mais un élément d'ordre p dans S_n est un produit d'un certain nombre de p-cycles à supports disjoints. On a donc $n \geqslant p$. Comme pour $p \geqslant 5$ on a $3 \leqslant (p+1)/2 \leqslant p-2$ pour $p \geqslant 5$, on a aussi les inégalités immédiates

$$|\mathrm{A}_n| \;=\; n!/2 \;\geqslant\; p!/2 \;\geqslant\; p(p-1)(p+1)/2 \;=\; |\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})|$$

Ces sont des égalités si, et seulement si, on a $n = p$ (pour la première) et $p = 5$ (pour la seconde !). □

REMARQUE 4.9. (*Autres isomorphismes exceptionnels*) Parmi les groupes simples de la forme A_n et $\mathrm{PSL}_n(\mathbb{Z}/p\mathbb{Z})$, les seuls isomorphismes sont en fait

$$\mathrm{A}_5 \simeq \mathrm{PSL}_2(\mathbb{Z}/5\mathbb{Z}),\;\; \mathrm{PSL}_2(\mathbb{Z}/7\mathbb{Z}) \simeq \mathrm{PSL}_3(\mathbb{Z}/2\mathbb{Z}) \;\text{ et }\; \mathrm{PSL}_4(\mathbb{Z}/2\mathbb{Z}) \simeq \mathrm{A}_8.$$

Si l'on s'autorise des corps finis $\mathbb{F}_q$ plus généraux que $\mathbb{Z}/p\mathbb{Z}$, on a aussi $\mathrm{A}_5 \simeq \mathrm{PSL}_2(\mathbb{F}_4)$, $\mathrm{A}_6 \simeq \mathrm{PSL}_2(\mathbb{F}_9)$, et le fait que $\mathrm{PSL}_3(\mathbb{F}_4)$ a même ordre que A_8 mais ne lui est pas isomorphe.

Les miracles ne s'arrêtent en fait pas là. Les groupes $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ avec $p = 7$ et 11 ont également des comportements inhabituels, comme l'avait expliqué Galois dans sa fameuse lettre à son ami Chevalier, écrite le jour avant le duel qui causa sa mort. Le groupe $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ agit transitivement sur $\mathrm{P}^1(\mathbb{Z}/p\mathbb{Z})$, qui a $p+1$ éléments. Galois se demande s'il agit aussi transitivement sur un ensemble à $1 < n \leqslant p$ éléments (nécessairement fidèlement pour $p \geqslant 5$). Une condition nécessaire, comme ci-dessus, est $p \,|\, n!$, et donc $p = n$.

THÉORÈME 4.10. (Galois) *Le groupe $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ agit transitivement sur un ensemble à p éléments si, et seulement si, on a $p \leqslant 11$. Pour $p = 5, 7, 11$ les stabilisateurs de ces actions exceptionnelles sont respectivement isomorphes aux groupes platoniciens A_4, S_4 et A_5.*

Nous renvoyons à cette note de votre serviteur pour une démonstration élémentaire de cet énoncé. Nous nous contenterons d'observer ici que la question est équivalente à savoir si $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ possède un sous-groupe d'indice p, *i.e.* d'ordre $\frac{p^2-1}{2}$, et de constater la coïncidence numérique

$$\frac{p^2-1}{2} = 12,\; 24 \text{ et } 60,\;\; \text{pour } \; p \;=\; 5,\; 7 \text{ et } 11,$$

qui sont les cardinaux respectifs des groupes A_4, S_4 et A_5. Pour $p = 2$ et 3, les actions transitives en question se déduisent de celles de $\mathrm{PSL}_2(\mathbb{Z}/2\mathbb{Z}) \simeq \mathrm{S}_3$ et $\mathrm{PSL}_2(\mathbb{Z}/3\mathbb{Z}) \simeq \mathrm{A}_4$ sur 2 et 3 éléments respectivement (lesquelles ?). Pour $p = 5$, on vu $\mathrm{PSL}_2(\mathbb{Z}/5\mathbb{Z}) \simeq \mathrm{A}_5$, qui agit bien transitivement sur 5 éléments. Ces comportement inhabituels pour $p = 7$ et 11 se sont avérés être aussi la clé de la construction de plusieurs des *groupes sporadiques*, comme les groupes de Mathieu : voir l'article *Three lectures on exceptional groups*, par J. Conway.

5. Complément I : Polytopes réguliers (culturel)

Dans ce complément culturel, nous discutons des polyèdres de dimension générale, aussi appelés *polytopes*. Deux belles références sont les livres de M. Berger *Géométrie* (Tome 2, Chapitre 12), et de H. Coxeter *Regular Polyopes*.

Fixons E un espace euclidien. Un polytope de E est [19] *un sous-ensemble P qui est l'enveloppe convexe d'un ensemble fini non vide de points*. Autrement dit, il existe un entier $m \geqslant 1$ et des points $P_1, \ldots, P_m \in E$ avec

$$P = \mathrm{conv}(P_1, \ldots, P_m) := \{\sum_{i=1}^{m} \lambda_i P_i \mid 0 \leqslant \lambda_i \text{ et } \sum_{i=1}^{m} \lambda_i = 1\}.$$

Un polytope P a une dimension n, qui est celle de l'espace affine engendré par P ; on parle alors de n-polytope. Un polytope de dimension 0, 1, 2, 3 ou 4 est communément appelé respectivement *point*, *segment*, *polygone*, *polyèdre* ou *polychore*.

Définition 5.1. *Une* face *d'un polytope P est une partie convexe non vide $F \subset P$ telle que pour tout $x, y \in P$, si on a $]x, y[\cap F \neq \varnothing$ alors $[x, y] \subset F$.*

Un peu de réflexion montre par exemple que dans le cas d'un solide P de Platon (enveloppe convexe de ses sommets), les faces strictes de P sont non seulement les faces de ce polyèdre au sens usuel, mais aussi ses arêtes et ses sommets. On reviendra sur ce léger conflit de terminologie plus bas. Pour illustrer toutefois l'efficacité de la définition ci-dessus de face, vérifions les propriétés suivantes :

Lemme 5.2. *Soient $T \subset E$ finie non vide et $P = \mathrm{conv}(T)$ le polytope engendré.*

(i) Toute face F de P est de la forme $\mathrm{conv}(T')$ avec $T' = T \cap F$.

(ii) Le polytope P a au plus $2^m - 1$ faces avec $m = |T|$.

(iii) Une face d'une face de P est une face de P.

(iv) Supposons $f : E \to \mathbb{R}$ affine, $f(x) \geqslant 0$ pour tout $x \in P$, et que l'hyperplan $H = \{x \in E \mid f(x) = 0\}$ rencontre P. Alors $P \cap H$ est une face de P.

(v) Soient F une face de P et A le sous-espace affine de E engendré par F. Alors F est d'intérieur non vide dans A et on a $P \cap A = F$.

Démonstration — Montrons le (i). Supposons que l'on ait $f := \sum_i \lambda_i x_i \in F$ avec $0 < \lambda_i$ pour tout i, les x_i dans T distincts, et $\sum_i \lambda_i = 1$ (et donc $\lambda_i < 1$). On peut alors écrire $f = \lambda_i x_i + (1 - \lambda_i) y_i$ avec $y_i = \frac{1}{1-\lambda_i} \sum_{j \neq i} \lambda_j x_j \in P$. Comme F est une face, on en déduit $x_i \in F$. On a montré $T' \subset F \subset \mathrm{conv}(T')$, puis $F = \mathrm{conv}(T')$ car F est convexe. Le (ii) se déduit du (i) et de ce que T a $2^m - 1$ parties non vides.

Montrons le (iii). Soient F une face de P et F' une face de F (un polytope par le (i)). Soient $x, y \in P$ avec $]x, y[\cap F' \neq \varnothing$. On a $]x, y[\cap F \neq \varnothing$ car $F \subset F'$, et donc $[x, y] \subset F$ car F est une face de P, puis $[x, y] \subset F'$ car F' est une face de F.

Montrons le (iv). La partie $F = P \cap H$ est convexe comme intersection de deux convexes, non vide par hypothèse. Soient $x, y \in P$ avec $]x, y[\cap F \neq \varnothing$. La restriction de f au segment $[x, y]$ est une fonction affine $\geqslant 0$ et s'annule sur $]x, y[$. Elle est donc constante égale à 0. Ainsi, on a $[x, y] \subset H$.

19. Il existe une seconde définition équivalente, ou *duale*, des polytopes : ce sont les *parties bornées du plan qui sont intersection finie de demi-espaces affines fermés*. L'équivalence entre les deux est utile et non triviale : voir le chapitre du livre de Berger susmentioné.

Vérifions enfin le (v). L'inclusion $F \subset A \cap P$ est évidente. Par l'algèbre linéaire, F contient un repère affine $e_0, \ldots, e_r$ de A (avec $r = \dim F$). Par convexité, F contient $\mathrm{Conv}(\{e_0, \ldots, e_r\})$ qui est d'intérieur non vide dans A. Fixons x un point dans cet intérieur. Soit $y \in A \cap P \smallsetminus F$. Alors $[x, y]$ est dans le convexe $P \cap A$ et $]x, y[$ rencontre $F \cap A$ par choix de x. On en déduit $[x, y] \subset F$ car F est une face, puis $y \in F$. □

Remarque 5.3. *Il est important de souligner que la réciproque du (i) est fausse. Par exemple, les diagonales d'un carré ne sont pas des faces du carré.*

On parle aussi de k-face pour *face de dimension* k. Une 0-face de P s'appelle un *sommet* de P (ou *point extrémal*). Les sommets de P sont en nombre fini par le (ii) du Lemme ci-dessus. On peut montrer que P est toujours l'enveloppe convexe de ses sommets (théorème de Krein-Milman). D'après le (v), P est l'unique face de dimension $\dim P$. Enfin, une face de dimension $\dim P - 1$ est appelée *cellule* de P. On peut montrer que toute k-face de P avec $k < \dim P$ est incluse dans une $k+1$-face de P. Au final, toute face de P s'insère dans un *drapeau* de P, c'est-à-dire dans une suite de faces $F_0 \subset F_1 \subset \cdots \subset F_n = P$ avec $\dim F_i = i$. On est maintenant en mesure de définir un polytope *régulier*.

Définition 5.4. *Un polytope P d'un espace euclidien E est dit* régulier *si l'action naturelle de* $\mathrm{Iso}(P)$ *sur l'ensemble des drapeaux de P est transitive.*

Les polygones réguliers plans et les solides de Platon sont manifestement des polytopes réguliers, de dimensions respectives 2 et 3. Noter aussi qu'une face d'un polytope régulier est un polytope régulier. De plus, pour tout $n \geqslant 0$ les trois familles infinies suivantes sont aussi des n-polytopes réguliers (notations de Coxeter) :

$$\alpha_n = \{(x_0, \ldots, x_n) \in \mathbb{R}^{n+1}_{\geqslant 0} \mid \sum_{i=0}^{n} x_i = 1\},$$

$$\gamma_n = [-1, 1]^n,$$

$$\beta_n = \{(x_1, \ldots, x_n) \in \mathbb{R}^n \mid \sum_{i=1}^{n} |x_i| \leqslant 1\}.$$

– Le polytope α_n est appelé *n-simplexe* régulier. Il a $n+1$ sommets (base canonique ϵ_i de $\mathbb{R}^{n+1}$) et $n+1$ cellules. Pour $n \geqslant 0$ ces cellules sont définies par $x_i = 0$ et sont des $n-1$-simplexes. Son groupe d'isométries est S_{n+1} (permutation des coordonnées). Pour $n = 0, 1, 2, 3$ on trouve respectivement un point, un segment, un triangle équilatéral et un tétraèdre régulier. Pour $n = 4$, on l'appelle aussi 5-*cellules* ou *pentachore*.

– Le polytope γ_n, avec $n \geqslant 1$, est le *n-hypercube* ou simplement *n-cube*. Il a 2^n sommets (les $(\pm 1, \pm 1, \ldots, \pm 1)$) et $2n$ cellules (définies par $x_i = \pm 1$), qui sont des $n-1$-cubes pour $n > 1$. Son groupe d'isométries est le groupe à $2^n n!$ éléments des permutations et changements de signes des coordonnées de $\mathbb{R}^n$, c'est un produit semi-direct $\{\pm 1\}^n \rtimes \mathrm{S}_n$. Pour $n = 0, 1, 2, 3$ on trouve respectivement un point, un segment, un carré et un cube. Pour $n = 4$, on l'appelle aussi 8-*cellules* ou *tesseract*.

– Le polytope β_n, avec $n \geqslant 1$, est le *n-hyperoctaèdre*. Il a $2n$ sommets (les $\pm\epsilon_i$) et 2^n cellules (définies par $\sum_i \pm x_i = 1$), qui sont des $n-1$-simplexes. Ce polytope est

dual de γ_n en un sens naturel, et a donc même groupe d'isométries (le n-simplexe, lui, est autodual). Pour $n = 0, 1, 2, 3$ on trouve respectivement un point, un segment, un carré et un octaèdre régulier. Pour $n = 4$, c'est aussi le 16-*cellules*.

La relation d'équivalence que l'on met sur les polytopes est la relation de similitude euclidienne. Les seuls isomorphismes entre les polytopes ci-dessus sont manifestement $\alpha_1 \simeq \beta_1 \simeq \gamma_1$ et $\beta_2 \simeq \gamma_2$. On dispose enfin du résultat surprenant suivant, démontré par Schläfli ($\simeq$ 1850) dans le cas $n \geqslant 4$ (et connu d'Euclide pour $n \leqslant 3$).

THÉORÈME 5.5. *À similitude près les n-polytopes réguliers sont :*

(i) le point pour $n = 0$, le segment pour $n = 1$, les polygones réguliers pour $n = 2$, les solides de Platon pour $n = 3$,

(ii) les trois polytopes $\alpha_n, \beta_n, \gamma_n$ pour $n \geqslant 4$,

et trois polytopes supplémentaires pour $n = 4$:

(a) le 24-cellules, *qui a* 24 *cellules octaèdres,* 24 *sommets et* 96 *arêtes et faces triangulaires,*

(b) le 120-cellules, *qui a* 120 *cellules dodécaèdres,* 600 *sommets,* 1200 *arêtes et* 720 *faces pentagonales,*

(c) et le 600-cellules, *dual du* 120-*cellules, qui a* 600 *cellules tétraèdres,* 120 *sommets,* 720 *arêtes et* 1200 *faces triangulaires.*

Nous renvoyons à Berger ou Coxeter pour une démonstration de ce théorème. Une propriété mise en avant par Coxeter est que les groupes d'isométries des polytopes réguliers sont engendrés par des réflexions. Pour deux belles animations représentant le 120-cellules, nous renvoyons à aux chaînes youtube Henri Paul de Saint-Gervais et DeltaSimplex.

EXEMPLE 5.6. (Le 24-cellules) Considérons le 4-polytope P de $\mathbb{R}^4$ défini par $|x_i \pm x_j| \leqslant 1$ pour tout $1 \leqslant i < j \leqslant 4$. Il n'est pas difficile de voir que, si $\{\epsilon_i\}$ est la base canonique de $\mathbb{R}^4$, l'ensemble des sommets de P est constitué des 24 points

$$\pm\,\epsilon_i \ \text{ et } \ \frac{1}{2}\sum_{i=1}^{4} \pm\epsilon_i. \tag{46}$$

De même, on peut montrer que P a exactement 24 cellules, définies par l'une des 24 équations $\pm x_i \pm x_j = 1$ avec $i \neq j$. Ce sont des octaèdres réguliers. Par exemple, les sommets de la face C de P définie par $x_1 + x_2 = 1$ sont, posant $o = \frac{1}{2}(\epsilon_1 + \epsilon_2)$,

$$o + \frac{1}{2}(\epsilon_1 - \epsilon_2),\ \ o - \frac{1}{2}(\epsilon_1 - \epsilon_2) \text{ et les } \ o + \frac{1}{2}(\pm\epsilon_3 \pm \epsilon_4),$$

et donc C est un octaèdre régulier de centre o. Le groupe $\mathrm{Iso}(P)$ des isométries de P contient le sous-groupe G d'ordre $2^4 4!$ constitué des permutations et changements de signes des 4 coordonnées. Ce dernier, ainsi donc que $\mathrm{Iso}(P)$, permute transitivement les 24 cellules de P. Le stabilisateur $\mathrm{Iso}(P)_C$ de C dans $\mathrm{Iso}(P)$ s'identifie à un sous-groupe de $\mathrm{Iso}(C) \simeq \mathrm{S}_4 \times \{\pm 1\}$. Ainsi, $|\mathrm{Iso}(P)|$ est un multiple de $|G| = 2^4\, 4! = 384$, et divise $2 \cdot 24^2 = 1152 = 3 \cdot 384$. Mais on observe que la symétrie orthogonale exceptionnelle de vecteur $\epsilon_1 - \frac{1}{2}\sum_i \epsilon_i$ préserve les sommets de P (Liste (46)) ; c'est donc un élément de $\mathrm{Iso}(P) \smallsetminus G$. On a donc $|\mathrm{Iso}(P)| = 2.24^2$ et $\mathrm{Iso}(P)_C \simeq \mathrm{Iso}(C)$. En particulier, le polytope P est régulier. ▫

Contrairement au cas des polyèdres réguliers, il paraît impossible de classifier les sous-groupes finis de $\mathrm{O}(n)$ quand n grandit. En effet, S_n se plonge dans $\mathrm{O}(n)$ (permutations des coordonnées), et donc tous les groupes d'ordre n se plongent aussi dans $\mathrm{O}(n)$ par Cayley. Dans le même esprit, on a le résultat suivant.

Proposition 5.7. *Soient V un $\mathbb{R}$-espace vectoriel de dimension finie et G un sous-groupe fini de $\mathrm{GL}(V)$. Il existe une structure d'espace euclidien sur V telle que l'on a $G \subset \mathrm{O}(V)$. En particulier, tout sous-groupe fini de $\mathrm{GL}_n(\mathbb{R})$ est conjugué à un sous-groupe de $\mathrm{O}(n)$.*

Démonstration — Soit $f : V \times V \to \mathbb{R}$ un produit scalaire sur V. Pour $x, y \in V$ on pose $x\dot{y} = \sum_{g\in G} f(gx, gy)$. L'application $(x, y) \mapsto x.y, V \times V \to \mathbb{R}$, est manifestement $\mathbb{R}$-bilinéaire symétrique. Elle est définie positive car on a $x \cdot x = \sum_{g\in G} f(gx, gx) \geqslant f(x, x)$ et f est défini. Pour $h \in H$ on a $hx.hy = x.y$ par simple changement de variable $g \mapsto gh^{-1}$ dans G. Ainsi, V est euclidien pour la norme

$$(x.x)^{1/2} \;=\; (\sum_{g\in G} \|g(x)\|^2\,)^{1/2},$$

et pour cette norme on a $G \subset \mathrm{O}(V)$. Pour la seconde assertion, on a montré que si $G \subset \mathrm{GL}_n(\mathbb{R})$ est un sous-groupe fini, il existe un produit scalaire sur $V = \mathbb{R}^n$ pour lequel G est constitué d'isométries. Soit $e = (e_1, \ldots, e_n)$ une base orthonormée de $\mathbb{R}^n$ pour ce produit scalaire et P une matrice de passage entre e et la base canonique de $\mathbb{R}^n$. On a alors $\mathrm{Mat}_e(g) = PgP^{-1}$ (formule de changement de base) et $\mathrm{Mat}_e(g) \in \mathrm{O}(n)$, donc $PGP^{-1} \subset \mathrm{O}(n)$. □

Un dernier résultat amusant est que tout sous-groupe fini de $\mathrm{O}(n)$ est le groupe d'isométries d'un polytope bien choisi de $\mathbb{R}^n$ (bien entendu, non régulier en général !). Il s'agit d'un énoncé du folklore discuté par exemple dans ce post mathoverflow. Nous en donnons ci-dessous une démonstration très inspirée de l'article *Linear groups as stabilizers of sets*[20] de M. Isaacs, que nous avons élaborée lors de discussions avec S. Bronstein.

Proposition 5.8. *Soient E un espace euclidien et $G \subset \mathrm{O}(E)$ un sous-groupe fini. Il existe un polytope $P \subset E$ avec $G = \mathrm{Iso}(P)$.*

Démonstration — Choisissons d'abord une partie finie $Y \subset E$ qui est stable par G, qui engendre E, et qui vérifie $||y|| = 1$ pour tout $y \in E$. Par exemple, si $\epsilon_1, \ldots, \epsilon_n$ est une base orthonormée de E, on peut prendre pour Y l'ensemble des $g(\epsilon_i)$ pour $g \in G$ et $i = 1, \ldots, n$. Comme Y engendre E, l'action naturelle du groupe $\mathrm{Iso}(Y)$ sur Y est fidèle, et donc $\mathrm{Iso}(Y)$ est fini (d'ordre $\leqslant |Y|!$).

Pour chaque $\gamma \in \mathrm{Iso}(Y) \smallsetminus \{1\}$, le sous-espace $E_\gamma \subset E$ des points fixes de γ est strict, et donc la réunion finie $\cup_{\gamma\in\mathrm{Iso}(Y)\smallsetminus\{1\}} E_\gamma$ est de complémentaire infini dans E (car $\mathbb{R}$ est infini !). On peut donc choisir $v \in E$ de norme 1, non dans Y, et fixé par aucun élément non trivial de $\mathrm{Iso}(Y)$. Notons X l'orbite de v sous l'action de G. Vérifions que l'on a :

$$\mathrm{Iso}(X) \cap \mathrm{Iso}(Y) = G. \tag{47}$$

En effet, l'inclusion $G \subset \mathrm{Iso}(X) \cap \mathrm{Iso}(Y)$ est évidente. Dans l'autre sens, si on a $\gamma \in \mathrm{Iso}(X) \cap \mathrm{Iso}(Y)$, alors on a $\gamma(v) \in X$, et donc $\gamma(v) = g(v)$ pour un certain

20. Proc. Amer. Math. Soc. 62, 28–30 (1976).

$g \in G$, puis $g^{-1}\gamma \in \mathrm{Iso}(Y)$ fixe v, et donc $g^{-1}\gamma = 1$ et $\gamma = g \in G$. Pour $n \geqslant 2$ entier considérons maintenant le sous-ensemble fini G-stable de E

$$X_n := Y \cup (1 - \frac{1}{n})X.$$

Comme tous les éléments de Y sont de norme 1, et que ceux de $(1 - \frac{1}{n})X$ sont de norme $1 - \frac{1}{n} \in [1/2, 1[$, on a $\mathrm{Iso}(X_n) = \mathrm{Iso}(Y) \cap \mathrm{Iso}(X)$, puis $G = \mathrm{Iso}(X_n)$ par l'Égalité (47). On considère enfin le polytope

$$P_n = \mathrm{Conv}(X_n).$$

Notons S_n l'ensemble des sommets (ou points extrémaux) de P_n. On a les inclusions évidentes $G = \mathrm{Iso}(X_n) \subset \mathrm{Iso}(P_n) \subset \mathrm{Iso}(S_n)$. Il suffit donc pour conclure de démontrer qu'il existe $n \geqslant 1$ tel que $S_n = X_n$.

Mais on a $S_n \subset X_n$ par le Lemme 5.2 (i). On a $||x|| \leqslant 1$ pour tout $x \in X_n$, $||y|| = 1$ pour $y \in Y$ et aussi $v \notin Y$. Une norme euclidienne étant strictement convexe,[21] on en déduit d'une part $Y \subset S_n$, et d'autre part $v \notin \mathrm{Conv}(Y)$. Comme $\mathrm{Conv}(Y)$ est compact, on en déduit $(1 - 1/n)v \notin \mathrm{Conv}(Y)$ pour un n assez grand, puis $Y \subsetneq S_n$. Mais comme S_n est G-stable et inclus dans X_n, et que $(1 - 1/n)X$ est une G-orbite, on en déduit $X_n = S_n$ pour n assez grand. □

Remarque 5.9. Si $G \subset \mathrm{O}(E)$ est irréductible (*i.e. ne préserve aucun sous-espace strict*), n'importe quelle orbite non nulle Y de G dans E engendre E, de sorte que l'on peut choisir pour Y une seule G-orbite dans la preuve ci-dessus, puis un polytope P dont les sommets forment deux orbites sous G. En général, on ne peut pas trouver de polytope P tel que $G = \mathrm{Iso}(P)$ et dont les sommets ne forment qu'une seule G-orbite, comme le montre le cas de la dimension 2 et d'un sous-groupe fini non diédral (voir l'Exercice 5.5). Un argument assez simple et donné par Isaacs *loc. cit.* montre que c'est toutefois possible si G agit irréductiblement sur le complexifié de E.[22]

6. Complément II : Frises et papiers peints (culturel)

On considère dans ce complément le groupe $\mathrm{Iso}(2)$ de toutes les isométries du plan euclidien $P = \mathbb{R}^2$. Soit g une telle isométrie. Notons $F \subset P$ le sous-ensemble des points fixes de g (le vide, ou un sous-espace affine). On montre aisément qu'il y a exactement 5 cas possibles (exclusifs) :

(Identité) $\dim F = 2$ et $g = \mathrm{id}_P$,

(Symétrie) $\dim F = 1$ et g est la symétrie s_F par rapport à la droite affine F,

(Rotation) $\dim F = 0$ et g est une rotation non triviale de centre F,

(Translation) $F = \varnothing$ et g est une translation non triviale,

(Symétrie glissée) $F = \varnothing$ et il existe une droite affine D telle que g est la composée de la symétrie s_D et d'une translation non triviale préservant D.

21. Si on a $x, y \in E$ distincts et $\lambda \in [0, 1]$ vérifiant $||x|| \leqslant 1$, $||y|| \leqslant 1$ et $||\lambda x + (1 - \lambda)y|| = 1$, alors on a $||x|| = ||y|| = 1$ et soit $\lambda = 0$, soit $\lambda = 1$ (cas d'égalité triangulaire). En particulier, pour toute partie finie $S \subset E$ avec $||s|| \leqslant 1$ pour tout $s \in S$, les éléments de norme 1 de S sont parmi les sommets de $\mathrm{Conv}(S)$.

22. Voir aussi l'article de László Babai, *Symmetry groups of vertex-transitive polytopes*, Geometriae Dedicata 6, 331–337 (1977), pour d'autres résultats.

Les deux derniers types de symétries ci-dessus sont *indirects* (*i.e.* envoient un repère direct sur un repère indirect), et les autres sont directs (on parle aussi de *déplacements*). Toute isométrie est produit d'au plus 3 symétries. On a une suite exacte

$$1 \to \mathrm{T}(2) \longrightarrow \mathrm{Iso}(2) \xrightarrow{g \mapsto \vec{g}} \mathrm{O}(2) \to 1,$$

où $\mathrm{T}(2)$ désigne le sous-groupe des translations de $\mathbb{R}^2$, naturellement isomorphe à $\mathbb{R}^2$. Le sous-groupe $\mathrm{O}(2) \subset \mathrm{Iso}(2)$ est d'ailleurs un complément de $\mathrm{T}(2)$ dans $\mathrm{Iso}(2)$. Les isométries directes de $\mathrm{Iso}(2)$ forment un sous-groupe d'indice 2, à savoir

$$\mathrm{Iso}^+(2) = \{g \in \mathrm{Iso}(2) \mid \det \vec{g} = 1\}.$$

On va s'intéresser aux sous-groupes (éventuellement infinis) *discrets* de $\mathrm{Iso}(2)$, c'est-à-dire qui ne contiennent pas de translation de vecteur arbitrairement petit, ou encore de rotation d'angle arbitrairement petit. Comme nous le verrons, ce sont les groupes d'isométries de certains *motifs* réguliers du plan. Fixons $G \subset \mathrm{Iso}(2)$ un sous-groupe discret. On pose $G^+ = G \cap \mathrm{Iso}^+(2)$ (un sous-groupe de G d'indice 1 ou 2). Par définition, $G \cap \mathrm{T}(2)$ est un sous-groupe discret de $\mathbb{R}^2$, il y a donc exactement trois possibilités pour ce sous-groupe : il est soit $\{0\}$, soit isomorphe à $\mathbb{Z}$, soit à $\mathbb{Z}^2$.

Cas (a) $G \cap \mathrm{T}(2) \simeq \{0\}$: il n'y a pas de translation dans G. Dans ce cas, G est fini et conjugué à un sous-groupe fini de $\mathrm{O}(2)$. En effet, tout élément non trivial de G^+ est alors une rotation, et il suffit de voir que toutes ces rotations ont même centre. Mais la suite exacte ci-dessus, et la commutativité de $\mathrm{SO}(2)$, montrent que pour $a, b \in \mathrm{Iso}^+(2)$ le commutateur $[a, b]$ est dans $\mathrm{T}(2)$. Ainsi, G^+ est commutatif, et on conclut car deux rotations qui commutent ont même centre.

Cas (b) $G \cap \mathrm{T}(2) \simeq \mathbb{Z}$. Dans ce cas, on dit que G est un *groupe de frise*. Il n'est pas très difficile de montrer qu'à conjugaison près dans $\mathrm{Iso}(2)$, il y en a exactement 7, à savoir les groupes d'isométries des 7 *frises* de la Figure 5 ci-après. Noter que

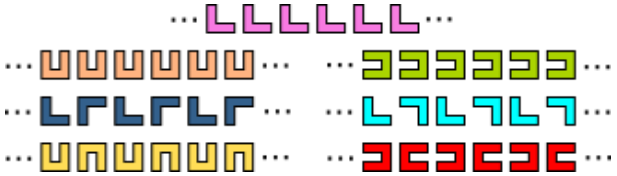


FIGURE 5. Les 7 types de frises

$G \cap \mathrm{T}(2) = \mathbb{Z}v$ engendre une droite privilégiée dans $\mathbb{R}^2$, appelée *direction de la frise*, disons D. L'axe d'une symétrie $s \in G$ est donc soit parallèlle à D (cas $svs^{-1} = v$, dit *horizontale*) soit perpendiculaire à D (cas $svs^{-1} = -v$, dit *vertical*). Comme dans cette intéressante video de M. Launay, notons H, V, R et G respectivement, la propriété pour une frise de posséder une réflexion horizontale, verticale, une rotation (nécessairement d'angle π) ou une symétrie glissée. Une inspection, résumée dans la première ligne du tableau ci-après, montre que ces propriétés distinguent les 7 frises ci-dessus. Leurs groupes d'isométries sont donc non conjugués dans $\mathrm{Iso}(2)$. Nous invitons le lecteur à vérifier que la classe d'isomorphisme des 7 groupes de frise ci-dessus est bien celle indiquée dans le tableau. On a noté $\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ le produit semi-direct défini par l'involution $x \mapsto -x$ de $\mathbb{Z}$.

frise	rose	beige	verte	bleue	turquoise	jaune	rouge
propriétés		V	HG	G	R	VRG	HVRG
G	$\mathbb{Z}$	$\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}$	$\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$	$(\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}/2\mathbb{Z}$
G^+	$\mathbb{Z}$	$\mathbb{Z}$	$\mathbb{Z}$	$2\mathbb{Z}$	$\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$	$2\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$

TABLE 1. Les groupes d'isométries des 7 types de frises.

Cas (c) $G \cap \mathrm{T}(2) \simeq \mathbb{Z}^2$. Dans ce cas, on dit que G est un *groupe de papier peint*. Ce cas est plus complexe. Feodorov et Polya ont montré indépendamment qu'à conjugaison près dans Iso(2), il y en a exactement 17, représentés en Figure 6 ci-dessous (voir aussi cette intéressante video).

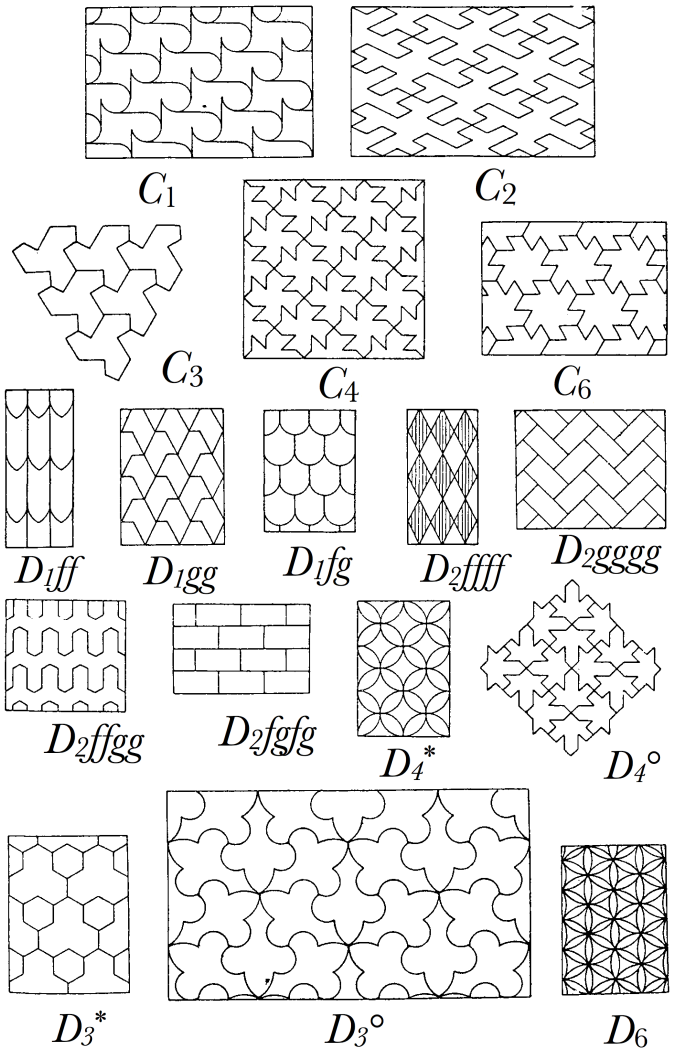


FIGURE 6. Pòlya, *Über die Analogie der Kristallsymmetrie in der Ebene* (1924)

7. Complément III : Groupes unitaires et un théorème de Jordan

Ce complément a pour but [23] d'introduire la géométrie hermitienne, analogue complexe naturel de la géométrie euclidienne, ainsi que le groupe de symétries naturellement associé : *le groupe unitaire*. Le groupe unitaire de l'espace hermitien standard $\mathbb{C}^n$ peut être simplement défini comme étant le sous-groupe suivant

$$\mathrm{U}(n) = \{g \in \mathrm{GL}_n(\mathbb{C}) \mid {}^t\overline{g}g = 1_n\}$$

de $\mathrm{GL}_n(\mathbb{C})$. À bien des égards il est plus simple à étudier que le groupe orthogonal, essentiellement car tout endomorphisme de $\mathbb{C}^n$ admet une droite propre. Par exemple, il est toujours connexe et il se comporte de la même manière en dimensions paires et impaires. En guise d'illustration, nous en donnerons une application à la démonstration d'un théorème classique de Jordan.

7.1. Normes hermitiennes. Comme on a $\mathbb{R} \subset \mathbb{C}$, tout $\mathbb{C}$-espace vectoriel espace vectoriel V peut-être vu comme un $\mathbb{R}$-espace vectoriel ("de dimension double") par restriction des scalaires. Pour des raisons de clarté, on notera $V^\flat$ ce $\mathbb{R}$-espace vectoriel sous-jacent, même si bien sûr on a $V^\flat = V$ en tant qu'ensembles. On note $|\cdot|$ la valeur absolue usuelle sur $\mathbb{C}$.

Définition 7.1. *Soit V un $\mathbb{C}$-espace vectoriel de dimension finie. Une* norme hermitienne *sur V est une norme euclidienne $\|\cdot\|$ sur $V^\flat$ vérifiant $\|\lambda v\| = |\lambda|\|v\|$ pour tout $\lambda \in \mathbb{C}$ et $v \in V$. Un espace hermitien est un $\mathbb{C}$-espace vectoriel V de dimension finie muni d'une norme hermitienne.*

L'exemple fondamental de norme hermitienne est la valeur absolue sur $\mathbb{C}$ (vu comme $\mathbb{C}$-espace vectoriel de dimension 1). En effet, on a $|x + iy|^2 = x^2 + y^2$ pour $x, y \in \mathbb{R}$ et $|\lambda\lambda'| = |\lambda||\lambda'|$ pour $\lambda, \lambda' \in \mathbb{C}$. Plus généralement :

Exemple 7.2. L'*espace hermitien standard de dimension n* est l'espace $V = \mathbb{C}^n$ muni de la norme $\|\cdot\|$ définie par $\|(z_1, \ldots, z_n)\|^2 = \sum_{j=1}^n |z_j|^2$. En effet, si $\epsilon_1, \ldots, \epsilon_n$ est la $\mathbb{C}$-base canonique de $\mathbb{C}^n$, alors $\epsilon_1, i\epsilon_1, \ldots, \epsilon_n, i\epsilon_n$ est une $\mathbb{R}$-base de $(\mathbb{C}^n)^\flat$ et on a pour $x_1, \ldots, x_n, y_1, \ldots, y_n \in \mathbb{R}$ on a $\|\sum_{j=1}^n (\, x_j\, \epsilon_j \,+\, y_j\, i\, \epsilon_j \,)\|^2 = \sum_{j=1}^n x_j^2 + y_j^2$ qui est une norme euclidienne, et on a $\|\lambda v\| = |\lambda|\|v\|$ pour $\lambda \in \mathbb{C}$ et $v \in V$.

Si V est un espace hermitien pour $\|\cdot\|$, alors $V^\flat$ est par définition un espace euclidien. Si $x.y$ désigne le produit scalaire sur $V^\flat$ vérifiant $x.x = \|x\|^2$ pour tout $x \in V$, la propriété $\|\lambda x\| = |\lambda|\|x\|$ pour tout $\lambda \in \mathbb{C}$ et $x \in V$ implique que pour tout $x, y \in V$ et $\lambda \in \mathbb{C}$ on a $\lambda x \cdot \lambda y = |\lambda|^2 x.y$ par polarisation. En particulier, si $W \subset V$ est un sous $\mathbb{C}$-espace vectoriel, son orthogonal $W^\perp$ dans $V^\flat$ est encore un sous $\mathbb{C}$-espace vectoriel, vérifiant $W \perp W^\perp = V^\flat$. Nous reviendrons plus en détail sur l'algèbre bilinéaire derrière ces considérations un peu plus loin. Utilisons déjà ces remarques pour voir que les normes hermitiennes admettent une caractérisation similaire à celle des normes euclidiennes.

Proposition 7.3. *Soit $(V, \|\cdot\|)$ un $\mathbb{C}$-espace vectoriel normé de dimension finie $n \geqslant 1$. Il y a équivalence entre :*

23. Le contenu de ce complément a pendant longtemps fait partie du programme de mathématique spéciale, mais n'a pas survécu aux derniers changements de programme. Le point de vue adopté suppose le lecteur familier avec la géométrie euclidienne.

(i) $\|\cdot\|$ *est une norme hermitienne sur* V*,*

(ii) il existe une $\mathbb{C}$*-base* $e_1, \ldots, e_n$ *de* V *telle que pour tout* $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ *on ait*

$$\|\sum_{i=1}^{n} \lambda_i e_i\|^2 = \sum_{i=1}^{n} |\lambda_i|^2. \tag{48}$$

Une base $e_1, \ldots, e_n$ *de* V *comme au (ii) est appelée* base orthonormée *de* $(V, \|\cdot\|)$*.*

Démonstration — Le fait que (ii) entraîne (i) est immédiat par l'Exemple 7.2. Supposons (i) et montrons (ii) par récurrence sur n. La restriction de la norme hermitienne de V à tout sous-espace W de V est encore une norme hermitienne sur W par définition. Choisissons pour W un hyperplan. Par les remarques ci-dessus, on a $V^\flat = W \perp W^\perp$ et $W^\perp$ est un sous $\mathbb{C}$-espace vectoriel de W, nécessairement une droite. Pour tout $w \in W$ et $w' \in W^\perp$ on a $\|w + w'\|^2 = \|w\|^2 + \|w'\|^2$ par définition. Ainsi, si $e_1, \ldots, e_{n-1}$ est une base orthonormée de W choisie par récurrence, et si $e_n \in W^\perp$ est un vecteur de norme 1, alors $e_1, \ldots, e_n$ est une base orthonormée de V. □

Remarque 7.4. *Par définition, une* $\mathbb{C}$*-base* $e_1, \ldots, e_n$ *de l'espace hermitien* V *est orthonormée si, et seulement si, la* $\mathbb{R}$*-base* $e_1, \ldots, e_n, ie_1, \ldots, ie_n$ *est orthonormée dans l'espace euclidien* $V^\flat$*.*

7.2. Groupe unitaire d'un espace hermitien. Le groupe $\mathrm{GL}(V)$ des bijections $\mathbb{C}$-linéaires d'un $\mathbb{C}$-espace vectoriel V est un sous-groupe du groupe $\mathrm{GL}(V^\flat)$ des bijections $\mathbb{R}$-linéaires de V.

Définition 7.5. *Si* V *un espace hermitien, le groupe unitaire de* V *est le sous-groupe des isométries* $\mathbb{C}$*-linéaires de l'espace euclidien* $V^\flat$ *; on le note* $\mathrm{U}(V)$*. Autrement, on a* $\mathrm{U}(V) = \mathrm{GL}(V) \cap \mathrm{O}(V^\flat)$ *dans* $\mathrm{GL}(V^\flat)$*. On pose aussi* $\mathrm{SU}(V) = \{g \in \mathrm{U}(V) \mid \det g = 1\}$ *(groupe spécial unitaire de* V*).*

Par exemple, si $\mathbb{C}$ est vu comme espace hermitien de dimension 1 comme ci-dessus, alors $\mathrm{U}(\mathbb{C})$ est le groupe des homothéties de rapport $\lambda \in \mathbb{C}^\times$ avec $|\lambda| = 1$. Il est donc isomorphe à S^1. En guise de première application de cette notion donnons une variante complexe de la Proposition 5.7 parfois appelée *astuce unitaire de Weyl.*

Proposition 7.6. *Soient* V *un* $\mathbb{C}$*-espace vectoriel de dimension finie et* $G \subset \mathrm{GL}(V)$ *un sous-groupe fini. Il existe une norme hermitienne sur* V *pour laquelle on a* $G \subset \mathrm{U}(V)$*.*

Démonstration — Soit $\|\cdot\|$ une norme hermitienne quelconque sur V (définie par exemple par la Formule (48) dans une base $e_1, \ldots, e_n$ arbitraire de V). La démonstration de la Proposition 5.7 montre que $N(x) = (\sum_{g \in G} \|g(x)\|^2)^{1/2}$ est une norme euclidienne sur $V^\flat$ vérifiant $G \subset \mathrm{O}(V^\flat)$. Comme on a $\|\lambda v\| = |\lambda| \|v\|$, on a aussi $N(\lambda v) = |\lambda| N(v)$. □

Comme dans le cas du groupe orthogonal, on a la caractérisation suivante :

Proposition 7.7. *Soient* V *un espace hermitien,* $e_1, \ldots, e_n$ *une base orthonormée de* V*, et* $g \in \mathrm{GL}(V)$*. On a* $g \in \mathrm{U}(V)$ *si, et seulement si,* $g(e_1), \ldots, g(e_n)$ *est une base orthonormée de* V*.*

Démonstration — Soient $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ et $v = \sum_{j=1}^n \lambda_j e_j$. On a $g(v) = \sum_{j=1}^n \lambda_j g(e_j)$. Pour $g \in \mathrm{U}(V)$, on a $\|g(v)\|^2 = \|v\|^2 = \sum_{j=1}^n |\lambda_j|^2$, et donc $g(e) := (g(e_1), \ldots, g(e_n))$ est orthonormée. Réciproquement, si $g(e)$ est orthonormée on a $\|g(v)\|^2 = \|v\|^2$ pour tout $v \in V$ et donc $g \in \mathrm{U}(V)$. □

La proposition suivante fait que la structure du groupe unitaire à tendance à être plus simple que celle du groupe orthogonal.

Proposition 7.8. *Soient V un espace hermitien et $g \in \mathrm{U}(V)$. Alors g est diagonalisable dans une base orthonormée de V.*

Démonstration — Observons d'abord que si $W \subset V$ est un sous $\mathbb{C}$-espace vectoriel vérifiant $g(W) = W$, alors son orthogonal $W^\perp$ (un sous-$\mathbb{C}$-espace vectoriel de V en somme directe avec W dans V) vérifie $g(W^\perp) = W^\perp$, car on a $\mathrm{U}(V) \subset \mathrm{O}(V^\flat)$.

Ceci étant dit, comme V est un $\mathbb{C}$-espace vectoriel de dimension finie alors g admet un vecteur propre e_1. On a $e_1 \neq 0$ donc $\|e_1\| \neq 0$, et quitte à remplacer e_1 par $e_1/\|e_1\|$ on peut supposer $\|e_1\| = 1$. Posons $D = \mathbb{C}e_1$ et $H = D^\perp$, de sorte que l'on a une décomposition $V = D \perp H$. Munissant l'hyperplan H de la norme hermitienne induite par celle de V, on a clairement $g_{|H} \in \mathrm{U}(H)$, et donc une base orthonormée $e_2, \ldots, e_n$ dans laquelle g est diagonalisable par récurrence sur $n = \dim V$. La base $e_1, \ldots, e_n$ de V est manifestement orthonormée, et diagonalise g. □

Si $e = (e_1, \ldots, e_n)$ est une base orthonormée de l'espace hermitien V, on note T_e le sous-groupe des éléments $g \in \mathrm{U}(V)$ préservant chacune des droites $\mathbb{C}e_i$. On a donc $g(e_i) = \lambda_i(g)e_i$ avec $\lambda_i(g) \in \mathbb{C}^\times$ de module 1, et l'application

$$\mathrm{T}_e \to (\mathrm{S}^1)^n, g \mapsto (\lambda_1(g), \ldots, \lambda_n(g))$$

est un isomorphisme de groupes.

Corollaire 7.9. *On a $\mathrm{U}(V) = \cup_e \mathrm{T}_e$, la réunion portant sur les bases orthonormées e de V. En particulier, $\mathrm{U}(V)$ est une partie connexe par arcs de $\mathrm{End}_{\mathbb{C}}(V)$.*

Démonstration — Le premier point est une traduction de la Proposition 7.8. Pour le second, il suffit de voir que chaque T_e est connexe par arcs car on a $1 \in \mathrm{T}_e \cap \mathrm{T}_f$ pour tout e, f. Mais dans la base e, T_e s'identifie au sous-groupe des matrices diagonales à coefficients dans S^1, qui est bien connexe par arcs dans $\mathrm{M}_n(\mathbb{C})$. □

Remarque 7.10. (Tores maximaux) Un sous-groupe de $\mathrm{U}(V)$ de la forme T_e est appelé *tore maximal*, de sorte que $\mathrm{U}(V)$ *est réunion de ses tores maximaux.* Noter que si f est une autre base orthonormée de e, on a $f = g(e)$ pour un unique $g \in \mathrm{U}(V)$ par la Proposition 7.7, puis $\mathrm{T}_f = g\mathrm{T}_e g^{-1}$ par le principe de conjugaison : *deux tores maximaux sont conjugués.* Ces éléments de structure de $\mathrm{U}(V)$ s'étendent aux groupes orthogonaux : voir les Exercices 5.25 et 5.26.

7.3. Produits scalaires hermitiens et écritures matricielles. Soit V un $\mathbb{C}$-espace vectoriel de dimension $n \geqslant 1$. Comme on l'a déjà dit, se donner une norme hermitienne sur V est la même chose que se donner un produit scalaire $x.y$ sur $V^\flat$ vérifiant $\lambda x.\lambda y = |\lambda|^2 x.y$. Le concept de *forme hermitienne* est une linéarisation plus souple de cette condition. Il permettra notamment d'écrire simplement les équations définissant $\mathrm{U}(V)$ dans $\mathrm{End}_{\mathbb{C}}(V)$.

Une forme *sesquilinéaire*[24] sur un $\mathbb{C}$-espace vectoriel V est une application $\mathbb{R}$-bilinéaire $f : V \times V \to \mathbb{C}$ telle que pour tout $x, y \in V$ et tout $\lambda \in \mathbb{C}$ on a

$$f(\lambda x, y) = \lambda f(x, y) \text{ et } f(x, \lambda y) = \overline{\lambda} f(x, y).$$

Soient f une telle forme et $e = (e_1, \ldots, e_n)$ une $\mathbb{C}$-base de V. On appelle *matrice de Gram de f dans la base e* la matrice $\mathrm{Gram}_e f := (f(e_i, e_j))_{1 \leqslant i,j \leqslant n} \in \mathrm{M}_n(\mathbb{C})$. Soient $X = (x_i)$ et $Y = (y_j)$ dans $\mathbb{C}^n$ (vecteurs colonnes) et $M = \mathrm{Gram}_e f$, on a alors

$$f(\sum_i x_i e_i, \sum_j y_j e_j) = \sum_{i,j} x_i \overline{y_j}\, f(e_i, e_j) \;=\; {}^t X\, M\, \overline{Y}. \tag{49}$$

Réciproquement, tout $M \in \mathrm{M}_n(\mathbb{C})$ définit par cette même formule une unique forme sesquilinéaire f sur V avec $\mathrm{Gram}_e f = M$. Une matrice $M \in \mathrm{M}_n(\mathbb{C})$ est dite *hermitienne*, ou *auto-adjointe*, si on a ${}^t\overline{M} = M$.

Proposition-Définition 7.11. *Soient V un $\mathbb{C}$-espace vectoriel de dimension finie n et f une forme sesquilinéaire sur V. Il y a équivalence entre :*

(i) $f(x, x) \in \mathbb{R}$ pour tout $x \in V$,

(ii) $f(y, x) = \overline{f(x, y)}$ pour tout $x, y \in V$,

(iii) il existe une base e de V telle que $\mathrm{Gram}_e f$ est hermitienne,

(iv) pour toute base e de V, $\mathrm{Gram}_e f$ est hermitienne.

Sous ces hypothèses on dit que f est hermitienne.

Démonstration — Les implications (ii) $\Longrightarrow$ (iv) $\Longrightarrow$ (iii) sont triviales, et (iii) $\Longrightarrow$ (ii) découle de l'identité (49). De plus, l'implication (ii) $\Longrightarrow$ (i) est claire. Supposons (i). Appliquée à x, y et $x + y$ on trouve $f(x, y) + f(y, x) \in \mathbb{R}$ pour tout $x, y \in V$, puis $\Im f(y, x) = -\Im f(x, y)$. Remplaçant x par ix on en déduit $\Re f(y, x) = \Re f(x, y)$, puis (ii). □

Définition 7.12. *Un produit scalaire hermitien sur V est une forme sesquilinéaire hermitienne f qui est* positive, *i.e. avec $f(x, x) \geqslant 0$ pour tout $x \in V$, et* définie *i.e vérifiant $f(x, x) = 0 \Longrightarrow x = 0$.*

L'exemple fondamental de produit scalaire hermitien, dans lequel on a $V = \mathbb{C}$ ($\mathbb{C}$-espace vectoriel de dimension 1), est $f(x, y) = x\overline{y}$. Plus généralement :

Exemple 7.13. Le produit scalaire hermitien standard sur $\mathbb{C}^n$ est $f(x, y) = \sum_j x_j \overline{y_j}$. Sa matrice dans la base canonique $\epsilon_1, \ldots, \epsilon_n$ est I_n.

Si f est un produit scalaire hermitien sur le $\mathbb{C}$-espace vectoriel de dimension finie V, alors $g := \Re f$ est un produit scalaire euclidien sur $V^\flat$. De plus, on a $f(\lambda x, \lambda x) = |\lambda|^2 f(x, x)$ et $f(x, x) = g(x, x)$ pour tout $\lambda \in \mathbb{C}$ et tout $x \in V$. Ainsi, l'application $\mathrm{N}_f : V \to \mathbb{R}_{\geqslant 0}, x \mapsto f(x, x)^{1/2}$, est une norme hermitienne sur V.

24. Comprendre *linéaire* (d'un côté) *et semi-linéaire* (de l'autre).

PROPOSITION 7.14. *Soit V un $\mathbb{C}$-espace vectoriel de dimension finie. L'application $f \mapsto \mathrm{N}_f$ est une bijection entre produits scalaires hermitiens sur V et normes hermitiennes sur V.*

DÉMONSTRATION — On vient de voir que si f est un produit scalaire hermitien sur V alors $\mathrm{N}_f(x) = f(x,x)^{1/2}$ est une norme hermitienne sur V. Notons que le produit scalaire euclidien $x.y$ sur $V^\flat$ associé à N_f vérifie nécessairement

$$x.y := \frac{1}{2}(\mathrm{N}_f(x+y)^2 - \mathrm{N}_f(x)^2 - \mathrm{N}_f(y)^2) = \frac{1}{2}(f(x+y,x+y) - f(x,x) - f(y,y)) = \Re f(x,y).$$

On a donc aussi $\Im f(x,y) = \Re f(x,iy) = x.iy$, puis pour tout $x,y \in V$,

$$f(x,y) \;=\; x.y \;+\; i\; x.iy.$$

ce qui montre que $f \mapsto \mathrm{N}_f$ est injective. Réciproquement, si N est une norme hermitienne sur V, notons $x.y = \frac{1}{2}(N(x+y)^2 - N(x)^2 - N(y)^2)$ le produit scalaire euclidien associé sur $V^\flat$. On pose $f(x,y) = x.y + i\; x.iy$. C'est une application $\mathbb{R}$-bilinéaire $V \times V \to \mathbb{C}$. Pour tout $x,y,v \in V$, on a $N(iv) = N(v)$ et donc

$$ix.iy = x.y \;\text{ et }\; x.iy = -ix.y = -y.ix.$$

Cela montre $f(ix,y) = if(x,y)$, $f(x,iy) = -if(x,y)$ et $f(y,x) = \overline{f(x,y)}$: la forme f est sesquilinéaire hermitienne. On a $f(x,x) = x.x$ car $x.ix = -x.ix = 0$, elle est donc définie positive et vérifie $\mathrm{N}_f = N$. □

Soit V un espace hermitien de norme hermitienne N. Ainsi, de manière analogue au cas euclidien, on parlera de *la forme hermitienne f associée à N*, ou encore de *la forme hermitienne* de V. Comme on l'a vu, f et N se déduisent l'une de l'autre par les formules

$$N(x)^2 = f(x,x),\;\; 2\Re f(x,y) = N(x+y)^2 - N(x)^2 - N(y)^2,\;\; \Im f(x,y) = \Re f(x,iy),$$

celle du milieu étant appelée *identité de polarisation*. Posons $x.y = \Re f(x,y)$. On prendra garde que la relation $x.y = 0$ n'implique pas nécessairement $f(x,y) = 0$, mais seulement $f(x,y) \in i\mathbb{R}$. Toutefois, on a le résultat suivant :

LEMME 7.15. *Soit V un espace hermitien de norme N, de forme hermitienne f, et de produit scalaire euclidien associé $x.y = \Re f(x,y)$. Soit $W \subset V$ un sous $\mathbb{C}$-espace vectoriel, et $W^\perp := \{v \in V \mid v.w = 0,\ \forall w \in W\}$ son orthogonal. On a*

$$W^\perp = \{v \in V \mid f(v,w) = 0,\ \forall w \in W\} = \{v \in V \mid f(w,v) = 0,\ \forall w \in W\},$$

et $W^\perp$ est un sous-$\mathbb{C}$-espace vectoriel de V.

DÉMONSTRATION — En effet, on a $iW \subset W$ et $f(v,w) = 0$ si et seulement si $v.w = 0$ et $v.iw = 0$. De plus, la relation $f(v,w) = \overline{f(w,v)}$ montre $f(v,w) = 0 \iff f(w,v) = 0$. □

La propriété pour une $\mathbb{C}$-base de V d'être orthonormée s'exprime aussi de manière très naturelle en terme de la forme hermitienne :

PROPOSITION 7.16. *Soient V un espace hermitien de dimension n, de forme hermitienne f, et $e = (e_1, \ldots, e_n)$ une $\mathbb{C}$-base de V. Alors e est orthonormée si, et seulement si, on a $\mathrm{Gram}_e f = \mathrm{I}_n$.*

Démonstration — Par la Remarque 7.4, e est orthonormée si, et seulement si, pour tout $1 \leqslant k, l \leqslant n$ on a $e_k.e_l = \delta_{k,l}$ et $e_k.ie_l = 0$. C'est équivalent à $f(e_k, e_l) = \delta_{k,l}$ pour tout $1 \leqslant k, l \leqslant n$, *i.e* à $\mathrm{Gram}_e f = \mathrm{I}_n$. □

Terminons par décrire le *groupe unitaire standard de rang* n. On pose

$$\mathrm{U}(n) = \{g \in \mathrm{GL}_n(\mathbb{C}) \mid {}^t\overline{g}g = \mathrm{I}_n\}.$$

L'application $g \mapsto {}^t\overline{g}^{-1}$ étant un automorphisme du groupe $\mathrm{GL}_n(\mathbb{C})$, on constate que $\mathrm{U}(n)$ est un sous-groupe de $\mathrm{GL}_n(\mathbb{C})$ (le sous-groupe des points fixes).

Proposition 7.17. *Soient V un espace hermitien de forme hermitienne f, et e une base orthonormée de V.*

(i) Pour $g \in \mathrm{GL}(V)$ on a $g \in \mathrm{U}(V) \iff f(g(x), g(y)) = f(x, y),\ \forall x, y \in V$.

(ii) L'application $g \mapsto \mathrm{Mat}_e g$ est un isomorphisme de groupes entre $\mathrm{U}(V)$ et $\mathrm{U}(n)$.

Démonstration — Montrons le (i). Si on a $f(g(x), g(y)) = f(x, y),\ \forall x, y \in V$ alors on a bien $g \in \mathrm{U}(V)$ en prenant $x = y$. Réciproquement, si on suppose $g \in \mathrm{U}(V)$, et si on note $x.y$ le produit scalaire euclidien de $V^\flat$, on a $gx.gy = x.y$ pour tout $x, y \in V$, puis $f(gx, gy) = gx.gy + i\, gx.ig(y) = f(x, y)$ car on a $g(iy) = ig(y)$.

Quelque soit la base e, on sait que l'application $g \mapsto \mathrm{Mat}_e g$ est un isomorphisme $\mathrm{GL}(V) \xrightarrow{\sim} \mathrm{GL}_n(\mathbb{C})$. Vérifions qu'elle identifie $\mathrm{U}(V)$ à $\mathrm{U}(n)$. Notons $X(v) \in \mathbb{C}^n$ le vecteur colonne des coordonnées de $v \in V$ dans la base e. Fixons $g \in \mathrm{GL}(V)$ et posons $P = \mathrm{Mat}_e\, g$. Le calcul matriciel affirme $X(gv) = P\,X(v)$. Ainsi, la relation $f(g(x), f(g(y)) = f(x, y)$ pour tout $x, y \in V$ s'écrit matriciellement

$${}^tX\,\overline{Y} = {}^t(PX)\overline{PY} = {}^tX\,({}^tP\overline{P})\,\overline{Y}, \quad \forall X, Y \in \mathbb{C}^n.$$

Mais cela équivaut à ${}^tP\overline{P} = \mathrm{I}_n$, *i.e.* $P \in \mathrm{U}(n)$. □

Ainsi, le groupe $\mathrm{U}(n)$ s'identifie naturellement au groupe unitaire $\mathrm{U}(\mathbb{C}^n)$ de l'espace hermitien standard $\mathbb{C}^n$, dont la base canonique est orthonormée. On pose aussi

$$\mathrm{SU}(n) = \{g \in \mathrm{U}(n) \mid \det g = 1\}.$$

Le choix d'une base orthonormée de V identifie bien entendu $\mathrm{SU}(V)$ à $\mathrm{SU}(n)$, avec $n = \dim V$. On a $\mathrm{SU}(1) = \{1\}$. Montrons pour finir

$$\mathrm{SU}(2) = \{\begin{bmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{bmatrix} \mid \alpha, \beta \in \mathbb{C},\ |\alpha|^2 + |\beta|^2 = 1\} = \mathrm{Sp}(1).$$

En effet, l'égalité de droite a déjà été vue (Remarque 2.3). Pour celle de gauche, considérons $g = \begin{bmatrix} \alpha & \gamma \\ \beta & \delta \end{bmatrix} \in \mathrm{SL}_2(\mathbb{C})$. On a $g^{-1} = \begin{bmatrix} \delta & -\gamma \\ -\beta & \alpha \end{bmatrix}$, puis ${}^tg^{-1} = \overline{g}$ si, et seulement si, $\delta = \overline{\alpha}$ et $\gamma = -\overline{\beta}$. La relation $\det g = 1$ s'écrit alors $|\alpha|^2 + |\beta|^2 = 1$.

Corollaire 7.18. *Tout sous-groupe fini de $\mathrm{GL}_n(\mathbb{C})$ est conjugué à un sous-groupe de $\mathrm{U}(n)$.*

Démonstration — Soit $G \subset \mathrm{GL}_n(\mathbb{C})$ un sous-groupe fini. D'après la Proposition 7.6, G est inclus dans le groupe unitaire d'une norme hermitienne N bien choisie sur $\mathbb{C}^n$. D'après la Proposition 7.3, il existe une base e de $\mathbb{C}^n$ orthonormée pour N. Si P est

une matrice de passage entre e et la base canonique de $\mathbb{C}^n$, la Proposition 7.17 (ii) implique $PGP^{-1} \subset \mathrm{U}(n)$. $\square$

7.4. Une application à un théorème de Jordan. C'est le théorème suivant :

THÉORÈME 7.19. *Soit $n \geqslant 1$ un entier. Il existe une constante $\mathrm{c}(n)$ telle que pour tout sous-groupe fini $G \subset \mathrm{GL}_n(\mathbb{C})$, il existe un sous-groupe abélien distingué $A \subset G$ avec $|G/A| \leqslant \mathrm{c}(n)$.*

REMARQUE 7.20. (i) Il existe des sous-groupes finis arbitrairement grands dans $\mathrm{GL}_n(\mathbb{C})$. Par exemple pour tout $m \geqslant 1$ on a le sous-groupe $G_{m,n}$, de cardinal $m^n n!$, des matrices ayant un seul coefficient non nul par ligne et par colonne, et appartenant à μ_m. Le sous-groupe $\simeq \mu_m^n$ des matrices diagonales de $G_{m,n}$ est abélien, distingué et d'indice $n!$ (qui ne dépend que de n).

(ii) Le théorème implique aussi qu'un sous-groupe fini simple non abélien de $\mathrm{GL}_n(\mathbb{C})$ est de cardinal $\leqslant \mathrm{c}(n)$. En particulier, $\mathrm{GL}_n(\mathbb{C})$ ne contient qu'un nombre fini de classes d'isomorphie de sous-groupes simples finis non abéliens.

La démonstration que nous donnons ci-dessous du théorème de Jordan est très inspirée de l'exposition de T. Tao dans cette entrée de son blog. D'après le Corollaire 7.18, on peut supposer $G \subset \mathrm{U}(n)$ dans l'énoncé du théorème. Soit $(V, \|\cdot\|)$ un espace hermitien. On munit $\mathrm{End}_{\mathbb{C}}(V)$ de la norme triple

$$|||u||| \;=\; \mathrm{Sup}_{\{v \in V,\ \|v\|=1\}} \|u(v)\|$$

subordonnée à $\|\cdot\|$. Pour $u \in \mathrm{End}_{\mathbb{C}}(V)$ et $g \in \mathrm{U}(V)$ on a $|||gu||| = |||ug||| = |||u|||$. Si $G \subset \mathrm{U}(V)$ est un sous-groupe, et pour $\epsilon > 0$ un réel, on note G_ϵ le sous-groupe de G engendré par les $g \in G$ avec $|||g - 1||| < \epsilon$.

LEMME 7.21. *Soient V un espace hermitien de dimension n, $G \subset \mathrm{U}(V)$ un sous-groupe, et ϵ un réel > 0. Alors G_ϵ est un sous-groupe distingué de G et on a*

$$|G/G_\epsilon| \leqslant (1 + 2/\epsilon)^{2n^2}.$$

DÉMONSTRATION — Le sous-groupe G_ϵ est engendré par les $g \in G$ avec $|||g - 1||| < \epsilon$. Pour voir que G_ϵ est distingué dans G, il suffit donc de monter que pour $g, h \in G$ avec $|||g - 1||| < \epsilon$ on a $|||hgh^{-1} - 1||| < \epsilon$. Mais c'est évident par les égalités $|||hgh^{-1} - 1||| = |||hg - h||| = |||g - 1|||$.

Pour majorer le cardinal de $|G/G_\epsilon|$ on utilise un argument de volume. Considérons une partie finie $X \subset G$ vérifiant $|||x - y||| \geqslant \epsilon$ pour tout $x, y \in X$ distincts ; une telle partie sera dite ϵ-séparée.[25] Soit $\mathrm{B}_r \subset \mathrm{End}_{\mathbb{C}}(V)$ la boule ouverte de centre 0 de rayon $r > 0$ pour $|||\cdot|||$. Fixant une mesure de Lebesgue vol sur $\mathrm{End}_{\mathbb{C}}(V)$, on a

$$\mathrm{vol}\,\mathrm{B}_r \;= c\, r^{2n^2} \quad \text{pour tout } r > 0,$$

où c est un certaine constante > 0. Par l'inégalité triangulaire, les $|X|$ parties de la forme $x + \mathrm{B}_{\epsilon/2} \subset \mathrm{End}_{\mathbb{C}}(V)$ avec $x \in X$ sont disjointes. Elle sont de même volume $\mathrm{vol}\,\mathrm{B}_{\epsilon/2}$, et on a $x + \mathrm{B}_{\epsilon/2} \subset \mathrm{B}_{1+\epsilon/2}$ car $|||x||| = 1$ pour tout $x \in X$. On en déduit

$$|X| \leqslant \mathrm{vol}(\mathrm{B}_{1+\epsilon/2})/\mathrm{vol}(\mathrm{B}_{\epsilon/2}) = \frac{(1+\epsilon/2)^{2n^2}}{(\epsilon/2)^{2n^2}} = (1 + 2/\epsilon)^{2n^2}.$$

25. Voir l'Exercice 1.6 Chap. 1 pour des considérations élémentaires sur cette notion.

Choisissons maintenant une partie $X \subset G$ qui est ϵ-séparée et de cardinal maximal : c'est possible par l'inégalité ci-dessus. Soit $g \in G$. Il existe $x \in X$ avec $|||g - x||| < \epsilon$, sinon $X \cup \{g\} \subset G$ serait ϵ-séparée et de cardinal $> |X|$. On a donc $|||x^{-1}g - 1||| < \epsilon$, puis $x^{-1}g \in G_\epsilon$, *i.e.* $g \in xG_\epsilon$. On a montré que l'application $X \to G/G_\epsilon$, $x \mapsto xG_\epsilon$, est surjective, puis $|G/G_\epsilon| \leqslant |X| \leqslant (1 + 2/\epsilon)^{2n^2}$. □

Le deuxième ingrédient clé est le *lemme de rapprochement des commutateurs* ci-dessous, souvent attribué à Schur.

Lemme 7.22. *Soient V un espace hermitien et $g, h \in \mathrm{U}(V)$. On a*

$$\left|\left|\left|ghg^{-1}h^{-1} - 1\right|\right|\right| \leqslant 2\,|||g - 1|||\,|||h - 1|||.$$

Démonstration — On a $|||ghg^{-1}h^{-1} - 1||| = |||gh - hg|||$ car $g, h \in \mathrm{U}(V)$. On a aussi $gh - hg = (g - 1)(h - 1) - (h - 1)(g - 1)$, et donc $|||gh - hg||| \leqslant 2|||g - 1|||\,|||h - 1|||$ en utilisant l'inégalité $|||uv||| \leqslant |||u|||\,|||v|||$ pour $u, v \in \mathrm{End}_{\mathbb{C}}(V)$. □

Nous sommes maintenant en mesure de démontrer le résultat suivant, qui implique le Théorème 7.19 par le Lemme 7.21. On pose $\epsilon_n = \frac{1}{4}|e^{2i\pi/n} - 1|$ pour $n > 1$, et aussi $\epsilon_1 = \frac{1}{2}$. On a $\epsilon_{n+1} \leqslant \epsilon_n \leqslant \frac{1}{2}$ pour tout $n \geqslant 0$.

Lemme 7.23. *Soient V un espace hermitien de dimension $n \geqslant 1$ et $G \subset \mathrm{U}(V)$ un sous-groupe fini. Alors G_ϵ est un sous-groupe abélien de G pour $\epsilon \leqslant \epsilon_n$.*

Démonstration — On procède par récurrence sur n, le cas $n = 1$ étant évident car $\mathrm{U}(1)$ est commutatif. On a clairement $(G_\epsilon)_\epsilon = G_\epsilon$, on peut donc supposer $G = G_\epsilon$. Si G est constitué d'homothéties (par exemple pour $n = 1$), alors G est abélien et il n'y a rien à démontrer. Sinon, le groupe G étant fini, il existe $z \in G$ non homothétie et avec $|||z - 1|||$ minimal. Fixons $g \in G$ avec $|||g - 1||| < \epsilon$. On a

$$\left|\left|\left|gzg^{-1}z^{-1} - 1\right|\right|\right| < 2\,\epsilon\,|||z - 1||| \leqslant |||z - 1|||, \tag{50}$$

par le Lemme 7.22. Par minimalité, l'élément $gzg^{-1}z^{-1}$ de G (Lemme 7.21) est donc une homothétie. On a donc $gzg^{-1}z^{-1} = \lambda 1$ pour un certain $\lambda \in \mathrm{S}^1$, puis $\lambda \in \mu_n$ en prenant le déterminant. Mais on a aussi $|||z - 1||| \leqslant |||z||| + 1 = 2$ et donc

$$|\lambda - 1| = \left|\left|\left|gzg^{-1}z^{-1} - 1\right|\right|\right| < 4\epsilon \leqslant 4\epsilon_n$$

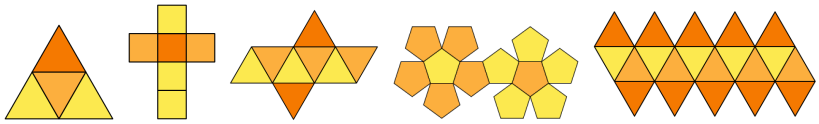
par l'inégalité (50). Mais pour $\zeta \in \mu_n \smallsetminus \{1\}$ on a $|\zeta - 1| \geqslant |e^{2i\pi/n} - 1|$. On en déduit $\lambda = 1$, et donc que z commute à g. Comme G est engendré par les $g \in G$ avec $|||g - 1||| < \epsilon$, on en déduit que z est dans le centre de G.

Mais z est diagonalisable par la Proposition 7.8. On a donc une décomposition orthogonale $V = \perp_i V_i$ en somme directe de sous-espaces propres V_i pour z, avec $\{0\} \subsetneq V_i \subsetneq V$ car z n'est pas une homothétie. Pour tout $g \in G$ on a donc $g(V_i) = V_i$ car g commute à z. On a donc un morphisme bien défini $r_i : G \to \mathrm{U}(V_i), g \mapsto g_{|V_i}$. L'inégalité évidente $|||r_i(g) - 1||| \leqslant |||g - 1|||$, et l'hypothèse $G = G_\epsilon$, entraînent donc $r_i(G) = r_i(G)_\epsilon$. L'entier $n_i = \dim V_i$ vérifie $1 \leqslant n_i < n$, et on a $\epsilon \leqslant \epsilon_n \leqslant \epsilon_{n_i}$. Le groupe fini $r_i(G)$ est donc abélien par récurrence sur n. Le morphisme naturel $G \to \prod_i r_i(G)$, $g \mapsto (g_{|V_i})$, étant injectif, on en déduit que G est abélien. □

8. Exercices

On commence par trois exercices de géométrie que l'on prendra avec légèreté.

EXERCICE 5.1. (Patrons des solides de Platon) *Indiquer les identifications des patrons suivants des solides de Platon :*



EXERCICE 5.2. (Une construction de l'icosaèdre) *Soit* $\varphi = \frac{1+\sqrt{5}}{2}$ *le* nombre d'or. *On considère les* 4 *points* $(0, \pm 1, \pm\varphi) \in \mathbb{R}^3$, *sommets d'un* rectangle d'or, *ainsi que les* 8 *autres points obtenus en permutant circulairement leurs coordonnées*[26] *:*

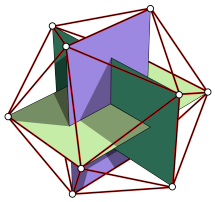


FIGURE 7. *Un triplet de rectangles d'or orthogonaux dans l'icosaèdre*

(i) En calculant une longueur bien choisie, montrer que les 12 *points ci-dessus sont les sommets d'un icosaèdre régulier*[27] I.

(ii) Montrer que les 20 *sommets du dodécaèdre dual à* I *sont*

$$\frac{1}{3}(\varphi, 0, \varphi^3), \quad \frac{1}{3}(\varphi^2, \varphi^2, \varphi^2),$$

et les 18 *autres points qui s'en déduisent par permutation circulaire des coordonnées et changements de signes.*

EXERCICE 5.3. *On suppose donnés* $f \geqslant 3$ *segments du plan ayant un sommet commun et d'angles consécutifs strictement plus grands que l'angle au sommet d'un polygone régulier à* $n \geqslant 3$ *côtés.*

(i) Montrer $\frac{1}{2} < \frac{1}{n} + \frac{1}{f}$.

(ii) En déduire les valeurs possibles de (n, f) *et retrouver la classification des solides de Platon.*

EXERCICE 5.4. *Expliquer en quel sens le groupe de Klein est*[28] *« le groupe des retournements d'un matelas ».*

EXERCICE 5.5. *Soient* $n \geqslant 1$ *un entier et* E *un plan euclidien. Montrer qu'il existe un polygone convexe compact* $P \subset E$ *vérifiant* $\mathrm{Iso}(P) \simeq \mathbb{Z}/n\mathbb{Z}$.

26. Cette image est issue du site de J. Baez.
27. On notera que le nombre d'or est l'unique réel $\varphi > 1$ pour lequel cette assertion est vraie.
28. Voir aussi Brian Hayes, *Group Theory in the Bedroom, and other mathematical diversions*.

Exercice 5.6. *Montrer que tout sous-groupe fini de* A_5 *est isomorphe à*

$$\mathrm{A}_5,\ \mathrm{A}_4,\ \mathrm{D}_{10},\ \mathrm{S}_3,\ \mathbb{Z}/5\mathbb{Z},\ \mathrm{K}_4,\ \mathbb{Z}/3\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z} \text{ ou } 1.$$

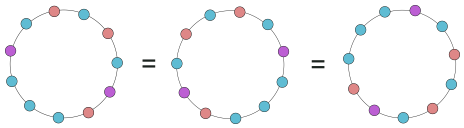
Exercice 5.7. *Soient* $m \geqslant 3$, $\mathscr{P}_m$ *un polygone régulier à* m *côtés d'un plan euclidien, et* G *le groupe d'isométries de* $\mathscr{P}_m$ *(on a vu* $G \simeq \mathrm{D}_{2m}$*).*

(i) Montrer qu'il y a exactement une ou deux classes de conjugaison de réflexions orthogonales dans G*, selon que* m *est impair ou non.*

(ii) Soient s *et* t *deux réflexions de* $\mathscr{P}_m$ *dont les axes forment un angle* $\frac{\pi}{m}$ *(justifier). Montrer* $G = \langle s, t\rangle$*.*

Les exercices suivants sont des applications de la formule de Burnside-Frobenius.

Exercice 5.8. (Colliers de Polya) *Combien peut-on fabriquer de colliers non similaires contenant* 2 *perles violettes,* 3 *perles rouges et* 6 *perles bleues ?*



Exercice 5.9. (Lemme de Jordan) *Soit* G *un groupe fini.*

(i) On suppose que G *agit transitivement sur un ensemble* X *avec* $|X| > 1$*. Montrer qu'il existe un élément de* G *n'ayant aucun point fixe dans* X*.*

(ii) Soit H *un sous-groupe de* G *avec* $H \neq G$*. Montrer* $\cup_{g\in G}\, gHg^{-1} \neq G$*.*

(iii) (Application) On suppose que le sous-groupe H *de* G *contient un représentant de chaque classe de conjugaison de* G*. Montrer* $H = G$*.*

(iv) Donner des contre-exemples à (i), (ii) et (iii) pour $G = \mathrm{SO}(3)$*.*

Exercice 5.10. *Soit* G *un groupe fini agissant sur un ensemble fini non vide* X*. On suppose que les propriétés suivantes sont satisfaites :*

(a) Pour tout $x \in X$ *on a* $G_x \neq 1$*,*

(b) Le seul élément de G *fixant deux points distincts de* X *est son neutre* 1*.*

Montrer que G *agit transitivement sur* X*.*

Dans la série d'exercices qui suivent, on s'intéresse aux sous-groupes distingués de $\mathrm{O}(n)$ et $\mathrm{SO}(n)$.

Exercice 5.11. *Soit* $n \geqslant 1$ *un entier.*

(i) Déterminer le centre de $\mathrm{O}(n)$*.*

(ii) Montrer $\mathrm{D}(\mathrm{O}(n)) = \mathrm{SO}(n)$*.*

(iii) Montrer que l'on a $\mathrm{O}(n) \simeq \mathrm{SO}(n) \times \{\pm 1\}$ *si, et seulement si,* n *est impair.*

Exercice 5.12. *Un retournement d'un espace euclidien* E *de dimension* $n \geqslant 3$ *est une symétrie orthogonale dont l'espace des points fixes est de dimension* $n-2$*.*

(i) Montrer que pour $n \geqslant 3$, les retournements de $\mathrm{SO}(n)$ sont conjugués et engendrent $\mathrm{SO}(n)$.

(ii) Déterminer le centre et le groupe dérivé de $\mathrm{SO}(n)$ pour tout $n \geqslant 1$.

Exercice 5.13. *Montrer qu'un sous-groupe G de $\mathrm{O}(2)$ est distingué si, et seulement si, on a $G \subset \mathrm{SO}(2)$ ou $G = \mathrm{O}(2)$.*

Exercice 5.14. *On se propose de montrer que le groupe $\mathrm{SO}(3)$ est simple.*

(i) Soit g dans $\mathrm{SO}(3)$ une rotation d'angle[29] θ. Montrer $\operatorname{tr} g = 1 + 2\cos\theta$.

(ii) Montrer que deux éléments de $\mathrm{SO}(3)$ sont conjugués si, et seulement si, ils ont même trace.

(iii) Quels sont les $g \in \mathrm{SO}(3)$ avec $\operatorname{tr} g = 3$?

On fixe H un sous-groupe distingué non trivial de $\mathrm{SO}(3)$.

(iv) On suppose $\operatorname{tr} H \supset]x, 3]$ avec $x < 3$. Montrer $H = \mathrm{SO}(3)$.

(v) Conclure en considérant l'application $\mathrm{SO}(3) \times H \to \mathbb{R}$, $(g, h) \mapsto \operatorname{tr}[g, h]$.

Exercice 5.15. (Sous-groupes distingués de $\mathrm{Sp}(1)$ et $\mathrm{SO}(4)$)

(i) En utilisant la simplicité de $\mathrm{SO}(3)$, lister les sous-groupes distingués de $\mathrm{Sp}(1)$.

(ii) En déduire les sous-groupes distingués de $\mathrm{SO}(4)$.

Exercice 5.16. *En utilisant la simplicité de $\mathrm{SO}(3)$ et des commutateurs bien choisis, montrer que pour $n > 1$:*

(i) le groupe $\mathrm{SO}(2n+1)$ est simple,

(ii) les seuls sous-groupes distingués de $\mathrm{SO}(2n+2)$ sont 1, $\{\pm 1\}$ et $\mathrm{SO}(2n+2)$.

Exercice 5.17. (Structures complexes) *Soient un entier $n \geqslant 1$ et $\mathrm{C}(n) = \{g \in \mathrm{O}(n) \mid g^2 = -1\}$. Le groupe $\mathrm{O}(n)$ agit naturellement sur $\mathrm{C}(n)$ par conjugaison.*

(i) Montrer $\mathrm{C}(n) \neq \varnothing \iff n \equiv 0 \bmod 2$, et $\mathrm{C}(n) \subset \mathrm{SO}(n)$.

(ii) Montrer que $\mathrm{C}(2n)$ admet deux orbites sous l'action de $\mathrm{SO}(2n)$, et une seule orbite sous celle de $\mathrm{O}(2n)$.

On notera $\mathrm{C}_+(2n)$ et $\mathrm{C}_-(2n)$ les deux orbites ci-dessus, ainsi que $\mathrm{G}_+(2n)$ et $\mathrm{G}_-(2n)$ les sous-groupes de $\mathrm{SO}(2n)$ qu'elles engendrent respectivement.

(iii) Que valent $-\mathrm{C}_+(2n)$ et $-\mathrm{C}_-(2n)$?

(iv) On suppose $n > 2$. Montrer $\mathrm{G}_\pm(2n) = \mathrm{SO}(2n)$.

(v) Montrer que pour tout $x \in \mathrm{C}_+(4)$ et $y \in \mathrm{C}_-(4)$ on a $xy = yx$, puis que $\mathrm{G}_+(4)$ et $\mathrm{G}_-(4)$ sont deux sous-groupes distingués de $\mathrm{SO}(4)$ vérifiant $\mathrm{G}_\pm(4) \simeq \mathrm{Sp}(1)$, $\mathrm{SO}(4) = \mathrm{G}_+(4)\mathrm{G}_-(4)$ et $\mathrm{G}_+(4) \cap \mathrm{G}_-(4) = \{\pm 1\}$.

29. On rappelle que si $g \neq 1$, g a une unique droite fixe, et définit une rotation du plan orthogonal : c'est de l'angle de cette rotation dont on parle. On convient qu'il est nul pour $\theta = 1$.

Dans les exercices suivants, on utilise la notion de *bloc* d'une action pour redémontrer que le groupe $\mathrm{SO}(3)$ est simple. Soient G un groupe agissant sur un ensemble X et $B \subset X$ un sous-ensemble non vide. On dira que B est *équilibré* pour cette action si pour tout $b \in B$ et tout $g \in G_b$ on a $g(B) \subset B$. On dit que B est un *bloc* pour cette action si pour tout $g \in G$ on a soit $g(B) = B$, soit $g(B) \cap B = \varnothing$. Un bloc $B \subset X$ est dit *trivial* si on a soit $B = X$, soit $|B| = 1$.

Exercice 5.18. (Blocs, équilibres et sous-groupes distingués) *Soit G un groupe agissant transitivement sur un ensemble X.*

(i) Montrer que $B \subset X$ est un bloc si, et seulement si, les parties de la forme $g(B)$ avec $g \in G$ forment une partition de X.

(ii) Montrer que si $B \subset X$ est un bloc, alors B est équilibré.

(iii) Vérifier que la réciproque est fausse en général.

(iv) Soit N un sous-groupe distingué de G. Montrer que les orbites de X sous N sont des blocs pour l'action de G sur X.

Exercice 5.19. *Soit $n \geqslant 1$ un entier. On considère l'action naturelle de $\mathrm{SO}(n)$ sur la sphère unité euclidienne S^{n-1}.*

(i) On suppose[30] *$n \neq 2$. Montrer que pour cette action, les seules parties équilibrées de S^{n-1} de cardinal > 1 sont S^{n-1} et les $\{x, -x\}$ avec $x \in \mathrm{S}^{n-1}$.*

(ii) (Cas $n = 2$) *Montrer que S^1 admet des blocs de tout cardinal fini.*

Exercice 5.20. *On se propose de donner une seconde démonstration de la simplicité de $\mathrm{SO}(3)$. Soit $H \subset \mathrm{SO}(3)$ un sous-groupe distingué non trivial.*

(i) Montrer[31] *que H agit transitivement sur S^2.*

(ii) Conclure en utilisant des commutateurs bien choisis.

On donne maintenant quelques propriétés et applications des éléments d'ordre 2 de $\mathrm{O}(n)$ (symétries orthogonales), ainsi que des sous-groupes engendrés par un nombre fini de symétries orthogonales qui commutent entre elles.

Exercice 5.21. (Sous-groupes abéliens 2-élémentaires de $\mathrm{O}(n)$)

(i) Montrer que le groupe $\mathrm{O}(n)$ a exactement n classes de conjugaison constituées d'éléments d'ordre 2.

(ii) Soit $G \subset \mathrm{O}(n)$ un sous-groupe abélien 2-élémentaire. Montrer $|G| \leqslant 2^n$.

(iii) On suppose $\mathrm{O}(m) \simeq \mathrm{O}(n)$. Montrer $m = n$.

(iv) On suppose $\mathrm{O}(a) \times \mathrm{O}(b) \simeq \mathrm{O}(a') \times \mathrm{O}(b')$. Montrer $\{a, b\} = \{a', b'\}$.

Exercice 5.22. (Quelques automorphismes non intérieurs)

(i) Soit n un entier pair $\geqslant 2$. Montrer que l'application $g \mapsto (\det g)g$ est un automorphisme non intérieur de $\mathrm{O}(n)$.

(ii) Montrer que $\mathrm{SO}(2)$ et $\mathrm{SO}(4)$ admettent tout deux un automorphisme non intérieur.

30. Le cas $n = 3$ étant suffisamment intéressant, on pourra s'en contenter.

31. On utilisera les deux exercices précédents.

Exercice 5.23. (Automorphismes de $\mathrm{O}(n)$) *On se propose de montrer que tout automorphisme de* $\mathrm{O}(n)$ *est soit intérieur, soit de la forme* $g \mapsto (\det g)\, p\, g\, p^{-1}$ *avec* $p \in \mathrm{O}(n)$ *quand* n *est pair. On note* $\mathcal{S} \subset \mathrm{O}(n)$ *le sous-ensemble des réflexions et on fixe* $s \in \mathcal{S}$ *et* $\alpha \in \mathrm{Aut}\,\mathrm{O}(n)$.

(i) Montrer[32] *que l'on a soit* $\alpha(s) \in \mathcal{S}$, *soit* n *est pair et* $-\alpha(s) \in \mathcal{S}$.

(ii) On suppose $\alpha(s) \in \mathcal{S}$. *Montrer* $\alpha(\mathcal{S}) \subset \mathcal{S}$.

(iii) (suite) En déduire que α *est intérieur par récurrence sur* n.

(iv) Conclure.

Exercice 5.24. (Automorphismes de $\mathrm{SO}(n)$)

(i) On suppose $n \neq 2, 4$. *Montrer que tout automorphisme de* $\mathrm{SO}(n)$ *est intérieur.*

(ii) On suppose $n = 2, 4$. *Montrer que* $\mathrm{Aut}\,\mathrm{SO}(n)/\mathrm{Int}\,\mathrm{SO}(n) \simeq \mathbb{Z}/2\mathbb{Z}$.

Dans les exercices suivants on s'intéresse à la fois à la réduction des endomorphismes orthogonaux et à la topologie du groupe orthogonal. On munit $\mathrm{O}(E)$ de la topologie induite par celle du $\mathbb{R}$-espace vectoriel de dimension finie $\mathrm{End}_{\mathbb{R}}(E)$.

Exercice 5.25. *Soient* E *un espace euclidien de dimension* $n \geqslant 1$ *et* $u \in \mathrm{O}(E)$.

(i) Montrer que u *possède soit une droite stable, soit un plan stable dans* E.[33]

(ii) On suppose $u \in \mathrm{SO}(E)$. *Montrer qu'il existe une décomposition orthogonale*

$$E = P_1 \perp P_2 \perp \cdots \perp P_r \perp D$$

avec $r = [n/2]$ *et* $\dim P_i = 2$, $u(P_i) \subset P_i$ *et* $u_{|P_i} \in \mathrm{SO}(P_i)$ *pour tout* $1 \leqslant i \leqslant r$.

(iii) On suppose $\det u = -1$. *Montrer qu'il existe* $v \in E$ *et une décomposition orthogonale* $E = F \perp \mathbb{R}v$ *avec* $u(v) = -v$, $u(F) \subset F$ *et* $u_{|F} \in \mathrm{SO}(F)$.

On notera $\mathscr{F}(E)$ l'ensemble des r-uples $F = (P_1, \ldots, P_r)$ de plans $P_i \subset E$ qui sont deux à deux orthogonaux, avec $r = [n/2]$ et $n = \dim E$. Pour chaque $F \in \mathscr{F}(E)$, on a une décomposition associée $E = P_1 \perp P_2 \perp \cdots \perp P_r \perp D$ avec $\dim D = n - 2r \leqslant 1$, et on note T_F le sous-groupe des $g \in \mathrm{SO}(E)$ tels que $g(P_i) = P_i$ pour tout i et $g_{|P_i} \in \mathrm{SO}(P_i)$ (*« tore défini par le drapeau* F *»*).

Exercice 5.26. *Soient* E *un espace euclidien de dimension* $n \geqslant 1$.

(i) Montrer que $\mathrm{O}(E)$ *est compact dans* $\mathrm{End}_{\mathbb{R}}(E)$.

(ii) Montrer que pour tout $F \in \mathscr{F}(E)$, *le sous-groupe* T_F *est fermé dans* $\mathrm{O}(E)$ *et continûment isomorphe à* $(\mathrm{S}^1)^r$ *avec* $r = [n/2]$.

(iii) Montrer que l'action naturelle de $\mathrm{SO}(E)$ *sur* $\mathscr{F}(E)$ *est transitive et que l'on a* $T_{gF} = gT_Fg^{-1}$ *pour tout* $g \in \mathrm{SO}(E)$ *et tout* $F \in \mathscr{F}(E)$.

(iv) Montrer $\mathrm{SO}(E) = \bigcup_{F \in \mathscr{F}(E)} T_F$.

(v) En déduire que $\mathrm{SO}(E)$ *est connexe par arcs.*

Exercice 5.27. (Sous groupes infinis fermés de $\mathrm{O}(2)$ et $\mathrm{SO}(3)$).

32. On pourra examiner le centralisateur de $\alpha(s)$ dans $\mathrm{O}(n)$ et utiliser l'Exercice 5.21.

33. Plus généralement, montrer que tout endomorphisme d'un espace vectoriel réel de dimension finie possède soit une droite stable, soit un plan stable.

(i) Montrer que les sous-groupes infinis fermés de $\mathrm{O}(2)$ *sont* $\mathrm{SO}(2)$ *et* $\mathrm{O}(2)$.

(ii) En déduire les sous-groupes infinis, fermés et réductibles de $\mathrm{SO}(3)$.

(iii) Montrer que le seul sous-groupe fermé, infini et irréductible de $\mathrm{SO}(3)$ *est* $\mathrm{SO}(3)$ *tout entier.*

On s'intéresse maintenant à la structure de la $\mathbb{R}$-algèbre des quaternions.

Exercice 5.28. (Les copies de $\mathbb{C}$ dans $\mathbb{H}$) *Posons* $\mathscr{I} = \{q \in \mathbb{H} \mid q^2 = -1\}$. *On rappelle que pour tout* $q \in \mathscr{I}$ *on a posé* $\mathbb{C}_q = \mathbb{R} + q\mathbb{R}$, *on sait que c'est une sous-*$\mathbb{R}$*-algèbre de* $\mathbb{H}$ *isomorphe à* $\mathbb{C}$.

(i) Montrer que l'action par conjugaison de $\mathrm{Sp}(1)$ *sur* $\mathscr{I}$ *est transitive.*

(ii) Soit $q \in \mathscr{I}$. *Montrer que si* A *est un sous-anneau de* $\mathbb{H}$ *contenant* $\mathbb{C}_q$, *alors on a* $A = \mathbb{C}_q$ *ou* $A = \mathbb{H}$. *(On pourra regarder* $\mathbb{H}$ *comme* $\mathbb{C}_q$*-espace vectoriel).*

(iii) Soit $q \in \mathbb{H} \smallsetminus \mathbb{R}1$. *Montrer qu'il existe* $q' \in \mathscr{I}$ *avec* $\mathbb{R} + \mathbb{R}q = \mathbb{C}_{q'}$.

(iv) En déduire que les sous-$\mathbb{R}$*-algèbres de* $\mathbb{H}$ *sont* $\mathbb{R}$, $\mathbb{H}$, *et les* $\mathbb{C}_q$ *pour* $q \in \mathscr{I}$, *et que ces dernières sont permutées transitivement par conjugaison par* $\mathrm{Sp}(1)$.

Exercice 5.29. *Soient* q *et* q' *deux éléments de* $\mathrm{Sp}(1)$. *Montrer que* q *et* q' *sont conjugués dans* $\mathrm{Sp}(1)$ *si, et seulement si, on a* $\mathrm{t}(q) = \mathrm{t}(q')$.

Exercice 5.30. *Soit* $m > 2$ *entier. Montrer qu'un élément* $q \in \mathrm{Sp}(1)$ *est d'ordre* m *si, et seulement si, on a* $\mathrm{t}(q) = 2\cos(2k\pi/m)$ *avec* $k \in \mathbb{Z}$ *et* $(k, m) = 1$.

Les deux exercices suivants concernent les quaternions *entiers*. Le premier montre notamment que pour p premier impair, $\mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$ peut être vu comme un anneau de *quaternions modulo* p.

Exercice 5.31. *Soit* p *un nombre premier impair.*

(i) Montrer qu'il existe $x, y \in \mathbb{Z}/p\mathbb{Z}$ *tels que* $x^2 + y^2 = -1$.

On considère les deux matrices $I = \begin{bmatrix} x & y \\ y & -x \end{bmatrix}$ *et* $J = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ *de* $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$.

(ii) Vérifier $I^2 = -1$, $J^2 = -1$ *et* $IJ = -IJ$.

(iii) Montrer que $\{1, I, J, IJ\}$ *est une base du* $\mathbb{Z}/p\mathbb{Z}$*-espace vectoriel* $\mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$.

(iv) En déduire que H_8 *est isomorphe à un sous-groupe de* $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ *pour tout nombre premier* $p > 2$.

Pour $q \in \mathbb{H}$ on pose $\chi_q = t^2 - \mathrm{t}(q)t + \mathrm{n}(q)$ (polynôme caractéristique de q).

Exercice 5.32. (Quaternions de Hurwitz, partie I) *On considère l'élément* $\omega = \frac{1+I+J+K}{2}$ *de* $\mathbb{H}$ *et on pose* $\mathrm{Hur} = \mathbb{Z} + \mathbb{Z}\,I + \mathbb{Z}\,J + \mathbb{Z}\,K + \mathbb{Z}\omega$.

(i) Montrer que Hur *est un sous-anneau de* $\mathbb{H}$, *et* $\chi_q \in \mathbb{Z}[t]$ *pour tout* $q \in \mathrm{Hur}$.

(ii) Montrer $\mathrm{Hur}^\times = \{q \in \mathrm{Hur} \mid \mathrm{n}(q) = 1\}$.

(iii) En déduire $|\mathrm{Hur}^\times| = 24$ *et lister les* 24 *éléments de* $\mathrm{Hur}^\times$ *ainsi que leurs polynômes caractéristiques.*

(iv) Montrer que $\mathrm{Hur}^\times$ *contient* H_8 *comme sous-groupe distingué d'indice* 3.

Dans l'exercice suivant, on se propose de montrer que $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ est isomorphe à un sous-groupe de $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ pour tout premier $p \neq 2$ (un fait assez surprenant !).

Exercice 5.33. (Quaternions de Hurwitz, partie II) *Soit p premier impair.*

(i) Exhiber[34] *un morphisme d'anneaux surjectif $\varphi : \mathrm{Hur} \to \mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$.*

(ii) Vérifier $\mathrm{trace}(\varphi(q)) \equiv \mathrm{tr}(q) \bmod p$, *et en déduire* $\det \varphi(q) \equiv \mathrm{n}(q) \bmod p$, *pour tout $q \in \mathrm{Hur}$.*

(iii) En déduire $\mathrm{Hur}^\times \simeq \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$.

(iv) Montrer que $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ *est isomorphe à un sous-groupe de* $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$.

Exercice 5.34. *(i) Montrer que* $\mathrm{Aut}(\mathrm{H}_8)$ *est naturellement isomorphe au groupe des isométries directes de l'octaèdre de sommets $\pm I, \pm J, \pm K$ de $\mathbb{H}^0$.*

(ii) En déduire $\mathrm{Aut}(\mathrm{H}_8) \simeq \mathrm{S}_4$.

Les Exercices 5.35 à 5.39 portent sur la notion d'action *primitive*, due à Galois. On rappelle que la notion de bloc d'une action a été introduite avant l'Exercice 5.18.

Exercice 5.35. (*Blocs d'une action transitive*) *Soit G un groupe agissant transitivement sur X. Pour toute partie $B \subset X$ on pose $G_B = \{g \in G \mid g(B) = B\}$, c'est un sous-groupe de G.*

(i) Montrer que si B est un bloc alors G_B agit transitivement sur B et contient G_x pour tout $x \in B$.

(ii) Soient $x \in X$ et H un sous-groupe de G contenant G_x. Montrer que $B := Hx$ est un bloc contenant x et vérifiant $G_B = H$.

(iii) En déduire que $B \mapsto G_B$ est une bijection croissante entre l'ensemble des blocs de X contenant x, et l'ensemble des sous-groupes de G contenant G_x.

Exercice 5.36. *Une action transitive d'un groupe G sur un ensemble X est dite* primitive *si on a $|X| \geqslant 2$ et si ses seuls blocs sont les blocs triviaux.*

(i) Montrer qu'une action 2-transitive est primitive.

(ii) Soit N un sous-groupe distingué de G agissant non trivialement sur X. Montrer que si G agit primitivement sur X, alors N agit transitivement sur X.

(iii) En déduire que le critère d'Iwasawa vaut encore en remplaçant dans son énoncé l'hypothèse « 2-transitivement » par « primitivement ».

(iv) En utilisant l'exercice précédent, montrer qu'une action transitive de G sur X est primitive si, et seulement si, ses stabilisateurs sont des sous-groupes maximaux de G.

(v) Supposons que G agit transitivement sur X avec $|X| \geqslant 2$. Montrer que G agit 2-transitivement sur X si, et seulement si, pour un $x \in X$ (ou tous) et $g \in G \smallsetminus G_x$, on a $G = G_x \cup G_x g G_x$.

Dans les exercices ci-dessous on retrouve la classification des sous-groupes distingués de S_n et A_n à l'aide du critère d'Iwasawa.

34. On pourra utiliser l'exercice 5.31 (iii).

Exercice 5.37. *Soient $n \geqslant 3$ et X_n l'ensemble des parties à 2 éléments de $\{1, \ldots, n\}$. On rappelle que S_n agit transitivement sur X_n.*

(i) Montrer que S_n agit 2-transitivement sur X_n, si et seulement si, $n = 3$.

(ii) Montrer que S_n agit primitivement sur X_n pour $n \neq 4$.

(iii) Retrouver les sous-groupes distingués de S_n à l'aide du critère d'Iwasawa.

Exercice 5.38. *Soient $n \geqslant 5$ et X_n l'ensemble des parties à 3 éléments de $\{1, \ldots, n\}$. On rappelle que A_n agit transitivement sur X_n.*

(i) Montrer que A_n n'agit pas 2-transitivement sur X_n.

(ii) Montrer que A_n agit primitivement sur X_n pour $n \neq 6$.

(iii) Montrer que les blocs non triviaux de l'action de A_6 sur X_6 ont deux éléments, et décrire leurs stabilisateurs.

On donne aussi une troisième démonstration de la simplicité de $\mathrm{SO}(3)$.

Exercice 5.39. *On considère l'action naturelle de $\mathrm{SO}(3)$ sur $\mathbb{P}(\mathbb{R}^3)$.*

(i) Montrer que cette action est primitive.

(ii) Est-elle 2-transitive ?

(iii) Redémontrer la simplicité de $\mathrm{SO}(3)$ en utilisant le critère d'Iwasawa.

Exercice 5.40. *Soit G un groupe fini $\neq 1$ agissant sur un ensemble X tel que :*

(a) tout élément de $G \smallsetminus \{1\}$ a exactement deux points fixes dans X,

(b) tout point de X est fixé par au moins un élément de $G \smallsetminus \{1\}$.

Montrer que les conclusions du Lemme 1.16 sont encore vérifiées.

On donne maintenant quelques exercices sur les groupes linéaires.

Exercice 5.41. *Soit k un corps.*

(i) Montrer que toute transvection de $\mathrm{SL}_2(k)$ est conjuguée dans $\mathrm{SL}_2(k)$ à $\mathrm{T}_{1,2}(\lambda)$, pour un certain $\lambda \in k^\times$.

(ii) Montrer que $\mathrm{T}_{1,2}(\lambda)$ et $\mathrm{T}_{1,2}(\mu)$ sont conjuguées dans $\mathrm{SL}_2(k)$ si, et seulement si, μ/λ est un carré dans $k^\times$.

Le (ii) ci-dessous montre que le groupe $\mathrm{SL}_2(\mathbb{R})$, dont on a vu en cours qu'il est égal à son groupe dérivé, possède un élément qui n'est pas un commutateur.

Exercice 5.42. *Si k est un corps, on note $\mathrm{P}(k)$ la propriété* « -1_2 est un commutateur dans $\mathrm{SL}_2(k)$ ».

(i) Montrer que $\mathrm{P}(\mathbb{C})$ est vraie.

(ii) Montrer que $\mathrm{P}(\mathbb{R})$ est fausse.

(iii) Montrer $\mathrm{P}(k) \iff$ « -1 est somme de deux carrés dans k ».

(iv) Que se passe-t-il si l'on remplace $\mathrm{SL}_2(k)$ par $\mathrm{GL}_2(k)$?

Dans l'exercice suivant on note $\mathbb{F}_4$ un corps à 4 éléments. Par exemple, on peut prendre pour $\mathbb{F}_4$ le sous $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel de $\mathrm{M}_2(\mathbb{Z}/2\mathbb{Z})$ engendré par 1 et

$$\omega = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}.$$

C'est un sous-anneau de $\mathrm{M}_2(\mathbb{Z}/2\mathbb{Z})$ par la relation $\omega^2 = \omega + 1$, et même un corps car cette relation entraîne $\omega^3 = 1$.

Exercice 5.43. *On se propose de montrer que les groupes simples* A_8 *et* $\mathrm{PSL}_3(\mathbb{F}_4)$ *ne sont pas isomorphes, bien que de même cardinal.*

(i) Vérifier $|\mathrm{A}_8| = |\mathrm{PSL}_3(\mathbb{F}_4)|$.

(ii) Montrer que $\mathrm{SL}_3(\mathbb{F}_4)$ *a exactement une classe de conjugaison d'éléments d'ordre* 2*, à savoir les transvections.*

(iii) Montrer que la surjection naturelle $\mathrm{SL}_3(\mathbb{F}_4) \to \mathrm{PSL}_3(\mathbb{F}_4)$ *induit une bijection sur les sous-ensembles respectifs des éléments d'ordre* 2.

(iv) Conclure.

Exercice 5.44. *Soient* k *un corps,* $n \geqslant 1$ *un entier,* D *le sous-groupe des matrices diagonales dans* $\mathrm{GL}_n(k)$ *et* N *le normalisateur de* D *dans* $\mathrm{GL}_n(k)$*. Montrer que l'on a un isomorphisme*

$$N \simeq (k^\times)^n \rtimes_\alpha \mathrm{S}_n,$$

avec pour morphisme $\alpha : \mathrm{S}_n \to \mathrm{Aut}((k^\times)^n)$ *celui induit par les permutations des coordonnées.*

Exercice 5.45. *On se propose de montrer que* $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ *possède un sous-groupe isomorphe à* D_{2n} *avec* $n = p^2 - 1$*. On fixe* $a \in \mathbb{Z}/p\mathbb{Z}$.

(i) Montrer qu'il existe $g, h \in \mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$ *avec* $g^2 = a1_2$*,* $gh = -hg$ *et* $h^2 = 1_2$.

(ii) On suppose que a *n'est pas un carré. Montrer que le sous* $\mathbb{Z}/p\mathbb{Z}$*-espace vectoriel de* $\mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$ *engendré par* 1_2 *et* g *est un sous-corps de cardinal* p^2.

(iii) Conclure.

Exercice 5.46. *Soient* p *premier et* α *un générateur du groupe* $(\mathbb{Z}/p\mathbb{Z})^\times$*. Montrer que* $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ *est engendré par les trois homographies* $x \mapsto -1/x$*,* $x \mapsto x + 1$ *et* $x \mapsto \alpha^2 x$.

Exercice 5.47. *Soient* p *un nombre premier et* $f : \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z}) \to \mathrm{S}_{p+1}$ *un morphisme associé à l'action de* $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ *sur* $\widehat{\mathbb{Z}/p\mathbb{Z}}$*. Déterminer* $\varepsilon \circ f$*, où* $\varepsilon : \mathrm{S}_{p+1} \to \{\pm 1\}$ *désigne la signature.*

Exercice 5.48. (Un théorème de Carlitz, suivant Zieve) *Soit* p *un nombre premier* > 2*. On se propose de montrer que* $\mathrm{S}_{\mathbb{Z}/p\mathbb{Z}}$ *est engendré par les bijections affines* $x \mapsto ax + b$*, et la bijection* $x \mapsto x^{p-2}$ *(justifier).*

(i) Montrer que l'homographie $1 - 1/x$ *est d'ordre* 3 *et permute* $\{0, 1, \infty\}$.

(ii) En déduire $h \circ h \circ h$*, où* $h(x) = 1 - x^{p-2}$.

(iii) Conclure.

Exercice 5.49. *Montrer que l'action par homographies de* $\mathrm{SL}_2(\mathbb{Z})$ *sur* $\widehat{\mathbb{Q}}$ *est transitive.*

Chapitre 6

Éléments de structure des groupes finis

Dans ce chapitre, on se propose de démontrer quelques uns des résultats emblématiques de la théorie élémentaire des groupes finis : les théorèmes de Sylow, de Schur-Zassenhaus et de P. Hall. Dans chacun des cas, il s'agit de formes de réciproques au théorème de Lagrange.

Nous commençons par donner quelques propriétés des p-groupes, c'est-à-dire des groupes d'ordre une puissance du nombre premier p. Les p-groupes abondent par le premier théorème de Sylow que l'on a déjà vu. Leur propriété la plus importante est que toute action d'un p-groupe sur un ensemble fini de cardinal premier à p admet un point fixe. Contrairement aux groupes simples finis, les p-groupes ne sont pas raisonnablement classifiables, mais cela ne les empêche pas de jouer un rôle important dans la théorie.

Les théorèmes de Sylow affirment que les p-Sylow du groupe fini G sont conjugués et que leur nombre est un diviseur de $|G|$ congru à 1 modulo p. L'exemple fondamental est celui de $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$, et par de nombreux aspects on essaiera de montrer que certaines propriétés de cet exemple valent encore en général.

Le théorème de Schur-Zassenhaus affirme que dans un groupe d'ordre mn avec $m \wedge n = 1$, tout sous-groupe distingué N de G d'ordre n admet un complément (d'ordre m). En particulier, un tel groupe est un produit semi-direct. Bien que simple à formuler, tout le chapitre est orienté vers sa démonstration. On commencera par montrer, à l'aide des théorèmes de Sylow, que le cas particulier N abélien, implique le cas général.

Le théorème de P. Hall affirme que dans un groupe *résoluble* d'ordre mn avec $m \wedge n = 1$, il existe un sous-groupe d'ordre m. Comme nous le verrons, il se déduit assez simplement du théorème de Schur-Zassenhaus. En fait, Hall a aussi démontré la réciproque : si G est fini et si pour tout diviseur d de $n = |G|$ premier avec n/d il existe un sous-groupe d'ordre d, alors G est résoluble. Il faut la théorie des représentations des groupes finis pour comprendre cette réciproque : voir le Complément § 9 Chap. 9.

Dans une dernière partie, nous revenons sur l'étude des *extensions* d'un groupe par un sous-groupe abélien : étant donné un groupe G et un groupe abélien A, on cherche à déterminer les groupes E possédant un sous-groupe distingué A' vérifiant $A' \simeq A$ et $E/A' \simeq G$. Autrement dit, on cherche les groupes E qui s'insèrent dans une suite exacte courte de la forme

$$1 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1.$$

Un cas particulier important est celui où A' est dans le centre de E (extension *centrale*). Il y a beaucoup d'exemples intéressants de telles extensions : par exemple $\mathrm{SL}_n(k)$ est une extension centrale de $\mathrm{PSL}_n(k)$ par $\mu_n(k)$, $\mathrm{Sp}(1)$ en est une de $\mathrm{SO}(3)$ par $\mathbb{Z}/2\mathbb{Z}$, et les groupes $\widetilde{\mathrm{A}_4}, \widetilde{\mathrm{S}_4}$ et $\widetilde{\mathrm{A}_5}$ sont des extensions centrales des groupes des

solides de Platon par $\mathbb{Z}/2\mathbb{Z}$. Le théorème principal est que les extensions de G par un groupe abélien A sont classifiées par un groupe annexe $\mathrm{H}^2(G, A)$ (2-ème groupe de cohomologie de G à valeurs dans A). Il devient alors facile de démontrer le cas abélien du théorème de Schur-Zassenhaus.

Enfin, dans un complément, nous discutons de la structure des groupes *nilpotents* finis (une condition plus forte que la résolubilité) et montrons que ce sont exactement les produits directs de p-groupes. Nous caractérisons, suivant Burnside, Dickson et Pazderski, les entiers $n \geqslant 1$ tels que tout groupe d'ordre n est cyclique (resp. abélien, resp. nilpotent). Nous étudions enfin le nombre minimal de générateurs d'un p-groupe, suivant Frattini et Burnside, ainsi que la structure du groupe des automorphismes d'un p-groupe, suivant P. Hall.

1. p-groupes

Dans toute cette partie p désigne un nombre premier.

Définition 1.1. *Un p-groupe est un groupe fini d'ordre p^n avec $n \geqslant 0$.*

Un produit fini de p-groupes est un p-groupe. Parmi les p-groupes rencontrés jusqu'à présent, on a les $\mathbb{Z}/p^n\mathbb{Z}$ avec $n \geqslant 1$, et les 2-groupes non abéliens D_8 et H_8. Les p-groupes abondent d'après le premier théorème de Sylow : tout groupe d'ordre $p^n m$ avec $(p, m) = 1$ possède un sous-groupe qui est un p-groupe d'ordre p^n (un tel sous-groupe est appelé p-Sylow de G). Par exemple, D_8 est un 2-Sylow de S_4. L'exemple le plus important de p-groupe est peut-être le suivant.

Exemple 1.2. *Le sous-groupe unipotent supérieur*

$$\mathrm{U}_n(\mathbb{Z}/p\mathbb{Z}) \subset \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$$

constitué des matrices triangulaires supérieures $(m_{i,j})$ avec $m_{i,i} = 1$ pour tout i est d'ordre $p^{\frac{n(n-1)}{2}}$. D'après la Proposition 3.15 Chap. 5, $\frac{n(n-1)}{2}$ est aussi la valuation en p de $|\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})|$, de sorte que $\mathrm{U}_n(\mathbb{Z}/p\mathbb{Z})$ est un p-Sylow de $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$.

Nombreuses propriétés des p-groupes se déduisent de la propriété suivante, qui généralise la Propsition 1.9 Chap. 1 (Cas $G = \mathbb{Z}/p\mathbb{Z}$).

Proposition 1.3. *Soit G un p-groupe agissant sur un ensemble fini X. On note $\mathrm{Fix}\, X = \{x \in X \mid gx = x \ \forall g \in G\}$ l'ensemble des points fixes de X sous l'action de G. On a la congruence $|X| \equiv |\mathrm{Fix}\, X| \bmod p$.*

Démonstration — En effet, pour $x \in X$ l'orbite O_x de x est de cardinal $|G|/|G_x|$, qui est un diviseur de $|G|$. Il y a donc deux cas : soit $|\mathrm{O}_x| = 1$, *i.e.* $x \in \mathrm{Fix}\, X$, soit $|\mathrm{O}_x| \equiv 0 \bmod p$. On conclut par l'équation aux classes. □

Proposition 1.4. *Pour tout p-groupe $P \subset \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ il existe $g \in \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ tel que gPg^{-1} est inclus dans $\mathrm{U}_n(\mathbb{Z}/p\mathbb{Z})$.*

Démonstration — Soit V le $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel $(\mathbb{Z}/p\mathbb{Z})^n$. Le groupe $\mathrm{GL}(V) = \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ agit naturellement sur l'ensemble des hyperplans vectoriels de V. Il y

a autant d'hyperplans vectoriels que de droites dans l'espace vectoriel dual. Il y a donc

$$\frac{p^n-1}{p-1} = 1 + p + \cdots + p^{n-1}$$

hyperplans. En particulier, leur nombre est premier à p. Si P est un p-groupe inclus dans $\mathrm{GL}(V)$, il préserve donc un hyperplan. L'image de P dans $\mathrm{GL}(H)$ est encore un p-groupe (c'est un quotient de P), donc par récurrence sur $\dim V$, il existe un suite croissante V_i de sous-espaces de V avec $\dim V_i = i$ pour $i = 1, \ldots, n-1$, préservée par P. Choisissons une base $e_1, \ldots, e_n$ de V telle que $e_1, \ldots, e_i$ engendre V_i. Dans cette base, P est constitué de matrices triangulaires supérieures : on a montré qu'il existe $g \in \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ avec $gPg^{-1} \subset \mathrm{T}_n(k)$. On peut donc supposer $P \subset \mathrm{T}_n(k)$. On conclut car le morphisme $P \to ((\mathbb{Z}/p\mathbb{Z})^\times)^n$, $(p_{i,j}) \mapsto (p_{i,i})$ est trivial car $|P|$ et $((\mathbb{Z}/p\mathbb{Z})^\times)^n$ sont d'ordre premiers entre eux, QED. □

Corollaire 1.5. *Tout p-groupe fini est isomorphe à un sous-groupe de* $\mathrm{U}_n(\mathbb{Z}/p\mathbb{Z})$ *pour n assez grand.*

Démonstration — En effet, on sait que tout groupe fini P se plonge dans S_n avec $n = |P|$, qui lui-même se plonge dans $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ pour tout p (matrices de permutations). On conclut par la proposition ci-dessus. □

Appliquons maintenant la Proposition 1.3 à l'action d'un groupe sur lui-même par conjugaison. On en déduit :

Proposition 1.6. *Si P est un p-groupe non trivial, alors son centre* $\mathrm{Z}(P)$ *est non trivial.*

Démonstration — En effet, d'après la Proposition 1.3 on a $|\mathrm{Z}(P)| \equiv |P| \equiv 0 \bmod p$. On en déduit $|\mathrm{Z}(P)| = p^m$ avec $m \geqslant 1$. □

Par exemple, un petit exercice montrerait que le centre de $\mathrm{U}_n(\mathbb{Z}/p\mathbb{Z})$ est d'ordre p (matrices m telles que $m_{i,j} = 0$ pour $(i,j) \neq (1,n)$ et $i \neq j$).

Corollaire 1.7. *Un groupe d'ordre p^2 est abélien, donc isomorphe à*

$$(\mathbb{Z}/p\mathbb{Z})^2 \quad \text{ou} \quad \mathbb{Z}/p^2\mathbb{Z}.$$

Démonstration — En effet, pour un tel groupe P on a $P/\mathrm{Z}(P)$ d'ordre 1 ou p car $\mathrm{Z}(P) \neq 1$. Dans tous les cas $P/\mathrm{Z}(P)$ est cyclique et donc P est abélien. La dernière assertion s'en déduit soit par la classification des groupes abéliens finis, soit directement en observant que si P n'a pas d'élément d'ordre p^2, alors il est abélien p-élémentaire par Lagrange. □

Remarque 1.8. Il existe des groupes d'ordre p^3 non abéliens, comme le p-groupe $\mathrm{U}_3(\mathbb{Z}/p\mathbb{Z})$, aussi appelé *groupe de Heisenberg*. En fait, nous verrons en exercice qu'il n'existe à isomorphisme près que deux groupes non abéliens d'ordre p^3. Pour $p = 2$, ce sont H_8 et $\mathrm{D}_8 \simeq \mathrm{U}_3(\mathbb{Z}/2\mathbb{Z})$. Pour $p > 2$, $\mathrm{U}_3(\mathbb{Z}/p\mathbb{Z})$ est le seul ayant la propriété que tous ses éléments non triviaux sont d'ordre p. L'autre peut être défini par $\mathbb{Z}/p^2\mathbb{Z} \rtimes_\alpha \mathbb{Z}/p\mathbb{Z}$ avec $\alpha_{\overline{k}}(x) = (1+p)^k x$ pour $\overline{k} \in \mathbb{Z}/p\mathbb{Z}$ et $x \in \mathbb{Z}/p^2\mathbb{Z}$. Il s'avère que *classifier* les p-groupes n'est pas une question (possédant une réponse) raisonnable. Par exemple,

il existe 14 groupes d'ordre 16, 51 d'ordre 32, 267 d'ordre 64, ..., 49487365422 d'ordre 1024, et on ne connaît pas leur nombre d'ordre 2048.

COROLLAIRE 1.9. *Les p-groupes sont résolubles.*

DÉMONSTRATION — On montre par récurrence sur $n \geqslant 0$ qu'un p-groupe P d'ordre p^n est résoluble. C'est clair pour $n = 0$. Pour $n > 0$ on sait que le centre $\mathrm{Z}(P)$ de P est non trivial. Si on a $\mathrm{Z}(P) = P$ alors P est abélien, donc résoluble. Sinon, $\mathrm{Z}(P)$ et $P/\mathrm{Z}(P)$ sont deux p-groupes d'ordre $< p^n$, résolubles par récurrence, et donc P est résoluble par la Proposition 6.11 Chap. 4. □

En fait, les p-groupes vérifient une condition beaucoup plus forte que la résolubilité, appelée *nilpotence*. Nous renvoyons au Complément 6 pour une discussion de cette notion importante, et aux exercices pour des compléments sur les p-groupes.

2. Les théorèmes de Sylow

Soient G un groupe fini et p un nombre premier divisant $|G|$. On peut donc écrire $|G| = p^\alpha m$ avec $p \wedge m = 1$ et $\alpha \geqslant 1$. On rappelle qu'un p-Sylow de G est un sous groupe de G de cardinal exactement p^α. On a déjà démontré le premier théorème de Sylow (Théorème 4 Chap. 1.14), qui affirme que G possède au moins un p-Sylow. Si P est un p-Sylow de G, il en va de même de chaque conjugué gPg^{-1} pour $g \in G$ (un sous-groupe isomorphe à P via l'automorphisme $x \mapsto gxg^{-1}$). On a en fait les énoncés plus précis suivants.

THÉORÈME 2.1. (Sylow) *Soient G un groupe fini et p premier divisant $|G|$.*

(i) G possède des p-Sylow,

(ii) Tout p-sous-groupe[1] *de G est inclus dans un p-Sylow de G,*

(iii) Deux p-Sylow de G sont conjugués (en particulier, isomorphes).

EXEMPLE 2.2. Le groupe S_4 est d'ordre $24 = 3 \cdot 8$. Les 3-Sylow de S_4 sont donc ses sous-groupes d'ordre 3, nécessairement engendrés par un 3-cycle. Ils sont bien conjugués car les 3-cycles sont conjugués dans S_n pour $n \geqslant 3$. Les 2-Sylow de S_4 sont ses sous-groupes d'ordre 8. Un exemple est $\mathrm{D}_8 \subset \mathrm{S}_4$, et tout 2-Sylow est donc conjugué à D_8 par le théorème. Observons cependant que $A := \mathrm{K}_4$, $B := \langle (1\,2\,3\,4) \rangle$ et $C := \langle (1\,3), (2\,4) \rangle$ sont 3 sous-groupes d'ordre 4 de S_4 (en fait, ce sont les 3 sous-groupes d'ordre 4 de D_8), et qu'ils sont deux-à-deux non conjugués dans S_4 ! Ainsi, il n'est pas vrai que deux p-sous groupes de G de même ordre sont conjugués, ni même isomorphes (cas de A et B), et il n'est pas vrai non plus que deux p-sous groupes isomorphes sont conjugués (cas de A et C).

Ce théorème va découler entièrement du lemme suivant, qui peut-être vu comme une version abstraite de la Proposition 1.4.

LEMME 2.3. (Alignement des p-Sylow) *Soient G un groupe fini, H un sous-groupe de G et p premier divisant $|H|$. Si P est un p-Sylow de G, il existe $g \in G$ tel que $gPg^{-1} \cap H$ est un p-Sylow de H.*

1. Un p-sous-groupe d'un groupe G est un sous-groupe de G qui est un p-groupe.

Démonstration — On considère la restriction à H de l'action par translations de G sur G/P. Comme $|G/P| = |G|/|P|$ est premier à p, au moins une des orbites $O \subset G/P$ sous l'action de H est de cardinal premièr à p, par l'équation aux classes. Disons que O est l'orbite de gP, pour un certain $g \in G$. Le stabilisateur de gP dans H est $gPg^{-1} \cap H$. Il est d'indice $|O|$ dans H (Formule orbite-stabilisateur), qui est premier à p par hypothèse. C'est aussi un p-sous groupe de H car il est inclus dans le p-groupe gPg^{-1} : c'est un p-Sylow de H. □

Démonstration — (Du Théorème 2.1). Re-démontrons le (i). On sait que tout groupe fini G est isomorphe à un sous-groupe de S_n. Mais S_n est isomorphe à un sous-groupe de $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ (matrices de permutations). On peut donc supposer que G est inclus dans $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$. Mais ce dernier possède $P = \mathrm{U}_n(\mathbb{Z}/p\mathbb{Z})$ pour p-Sylow. Il existe donc $g \in \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ tel que $gPg^{-1} \cap G$ est un p-Sylow de G.

Le (ii) est une conséquence directe du lemme. En effet, si H est un p-sous groupe de G, et si P est un p-Sylow de G (on sait qu'il en existe par le (i)), il existe $g \in G$ tel que $gPg^{-1} \cap H$ est un p-Sylow de H. Mais comme H est un p-groupe, cela veut dire $gPg^{-1} \cap H = H$, et donc $H \subset gPg^{-1}$. Ainsi, gPg^{-1} est le p-Sylow de G cherché. Dans le cas particulier où H est un p-Sylow, l'inclusion $H \subset gPg^{-1}$ est une égalité pour une raison de cardinal, on a donc $H = gPg^{-1}$: on a montré le (iii). □

Définition 2.4. *On notera* $\mathrm{Syl}_p(G)$ *l'ensemble des p-Sylow de G et* $\mathrm{n}_p(G)$ *le nombre de p-Sylow de G. Autrement dit, on a* $\mathrm{n}_p(G) = |\mathrm{Syl}_p(G)|$.

Corollaire 2.5. *On a* $\mathrm{n}_p(G) = 1 \iff G$ *possède un p-Sylow distingué.*

Démonstration — Si on a $\mathrm{n}_p(G) = 1$ alors G possède un unique p-Sylow P, nécessairement distingué car on a alors $gPg^{-1} = P$ pour tout $g \in G$. Réciproquement, si P est un p-Sylow de G, alors tout autre p-Sylow est un conjugué de P par le théorème (iii), et donc égal à P si ce dernier est distingué. □

Théorème 2.6. (Sylow) *Soit G un groupe fini de cardinal $p^\alpha m$ avec $\alpha \geqslant 1$ et $p \wedge m = 1$. On a* $\mathrm{n}_p(G) \mid m$ *et* $\mathrm{n}_p(G) \equiv 1 \bmod p$.

Démonstration — Soit $S := \mathrm{Syl}_p(G)$. On a $S \neq \varnothing$ par le Théorème 2.1 (i). Le groupe G agit par conjugaison sur S, $(g, P) \mapsto gPg^{-1}$, transitivement par le (iii) du même théorème. Le stabilisateur de $P \in S$ est son normalisateur $\mathrm{N}_G(P)$ par définitions. Par la formule orbite-stabilisateur on a donc

$$\mathrm{n}_p(G) = |S| = |G|/|\mathrm{N}_G(P)|, \text{ puis } \mathrm{n}_p(G) \mid |G|.$$

Fixons $P \in S$ et considérons son action sur S (donc par $(g, Q) \mapsto gQg^{-1}$). Montrons que son unique point fixe est P lui-même. On aura alors bien $|S| \equiv 1 \bmod p$ par la Proposition 1.6. Soit Q un p-Sylow de G qui est fixe, *i.e.* avec $gQg^{-1} = Q$ pour tout $g \in P$. Autrement dit, on a $P \subset \mathrm{N}_G(Q)$ et donc P est un p-Sylow de $\mathrm{N}_G(Q)$. Mais Q est manifestement un p-Sylow distingué de $\mathrm{N}_G(Q)$, et donc l'unique p-Sylow de ce dernier par le Corollaire 2.5 appliqué à $\mathrm{N}_G(Q)$, donc on a $P = Q$. □

Exemple 2.7. Les p-Sylow de S_p sont ses sous-groupes d'ordre p. Chaque tel sous-groupe est engendré par un unique p-cycle de la forme $(1\,2\,\cdots)$. Il y en a donc $(p-2)! \equiv 1 \bmod p$ (Wilson), conformément à $\mathrm{n}_p(G) \equiv 1 \bmod p$, et ils sont bien tous conjugués car les p-cycles le sont dans S_p.

Comme nous le verrons dans les exercices, ce théorème permet typiquement de montrer que G possède un p-Sylow distingué. Donnons une autre application.

Exemple 2.8. *Un groupe simple d'ordre* 60 *est isomorphe à* A_5. En effet, soit G un tel groupe. On a $60 = 12 \cdot 5$, donc $\mathrm{n}_5(G) \mid 12$ et $\mathrm{n}_5(G) \equiv 1 \bmod 5$, puis $\mathrm{n}_5(G) = 6$ (1 est interdit car G est simple). Ainsi, l'action naturelle de G par conjugaison sur l'ensemble des six 5-Sylow de G définit un morphisme $f : G \to \mathrm{S}_6$ d'image transitive par Sylow. Comme G est simple, ce morphisme est injectif, et pour la même raison on a aussi $\varepsilon \circ f = 1$, donc $f(G) \subset \mathrm{A}_6$. La même démonstration que pour S_n montre qu'un sous-groupe d'indice n de A_n est isomorphe à A_{n-1}. On en déduit $G \simeq \mathrm{A}_5$ (et que f est l'action exotique !).

Une conséquence technique utile de la conjugaison des p-Sylow est le lemme suivant, dont la démonstration est souvent appelée *argument de Frattini.*

Lemme 2.9. (Frattini) *Soient G un groupe fini, N un sous-groupe distingué de G, P un p-Sylow de N et $\mathrm{N}_G(P)$ le normalisateur de P dans G. On a $G = N\ \mathrm{N}_G(P)$.*

Démonstration — Soit g dans G. Le p-groupe gPg^{-1} est inclus dans N, car N est distingué dans G. C'est donc encore un p-Sylow de N. Par conjugaison des p-Sylow de N dans N, il existe $n \in N$ tel que $gPg^{-1} = nPn^{-1}$. On en déduit $n^{-1}g \in \mathrm{N}_G(P)$, et donc $g \in n\mathrm{N}_G(P)$. □

3. Le théorème de Schur-Zassenhaus

Théorème 3.1. (Schur-Zassenhaus) *Soient G un groupe fini d'ordre mn avec $m \wedge n = 1$ et possédant un sous-groupe distingué d'ordre n. Alors G possède un sous-groupe d'ordre m.*

Remarquer que si on a $|G| = mn$ comme ci-dessus, avec $N \lhd G$ d'ordre n et $M \leqslant G$ d'ordre m, alors on a $M \cap N = \{1\}$ par Lagrange, et $|G| = |M||N|$. Ainsi, M est un complément de N dans G et on a $G = N \rtimes M$ (produit semi-direct interne). Cela démontre que l'intérêt du théorème de Schur-Zassenhaus dans des questions de dévissage.

Exemple 3.2. (i) Supposons qu'un groupe fini G possède un p-Sylow P distingué. Le théorème de Schur-Zassenhaus implique que P possède un complément K, puis $G \simeq P \rtimes K$ avec $|K|$ premier à p.

(ii) Soient H un groupe fini et P un p-Sylow de H. Le (i) s'applique à $G = \mathrm{N}_H(P)$ car P est un p-Sylow de G. Ainsi, un p-Sylow admet toujours un complément dans son normalisateur.

(iii) Soient $H = \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ et $P = \mathrm{U}_n(\mathbb{Z}/p\mathbb{Z})$. On peut montrer que le normalisateur de P dans H est le sous-groupe $\mathrm{T}_n(\mathbb{Z}/p\mathbb{Z})$ des matrices triangulaires supérieures dans $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ (Exercice 6.3). On constate que le sous-groupe P admet bien un complément dans G, par exemple le sous-groupe des matrices diagonales, d'ordre $(p-1)^n$, illustrant le (ii).

La démonstration du Théorème 3.1 est assez difficile, et sera découpée en plusieurs étapes. En particulier, il conviendra de traiter à part le cas particulier du théorème dans lequel on suppose en plus que N est abélien, ce que nous ferons au § 5. Nous allons montrer ici que ce cas abélien entraîne le cas général :

Lemme 3.3. *Le cas particulier N abélien du théorème de Schur-Zassenhaus implique le cas général.*

Démonstration — Soient G un groupe fini d'ordre mn avec $m \wedge n = 1$, et N un sous-groupe distingué de G d'ordre n. On raisonne par récurrence sur $|G|$. On peut supposer $1 < n$, sans quoi $M = G$ convient.

Soient p un diviseur premier de n et P un p-Sylow de N. On pose $G' = \mathrm{N}_G(P)$ et $N' = N \cap G'$. On a $N' \lhd G'$ et le Lemme de Frattini s'écrit $G = G'N$. Le morphisme de groupes $G' \to G/N, g \mapsto gN$, est donc surjectif. Son noyau est $N \cap G' = N'$, donc on a un isomorphisme naturel

$$G'/N' \xrightarrow{\sim} G/N.$$

Ainsi, N' est d'indice $m = |G'/N'| = |G/N|$ dans G', et d'ordre divisant n (car $N' \subset N$). Ainsi, si on a $G' \neq G$, alors par récurrence sur $|G|$ le groupe G' possède un sous-groupe d'ordre m, ainsi donc que G car on a $G' \leqslant G$.

On peut donc supposer $G' = G$, *i.e.* P distingué dans N. Soit Z le centre du p-groupe P. On a $Z \neq \{1\}$ par la Proposition 1.6. On a Z caractéristique dans P, et P distingué dans G, donc Z est distingué dans G (Exercice 4 Chap. 4.11 (ii)). On considère alors le groupe quotient G/Z. Son sous-groupe N/Z est d'ordre $n/|Z|$ (noter $Z \subset N$) et d'indice $(mn/|Z|)/(n/|Z|) = m$. Par récurrence, G/Z possède un sous-groupe d'ordre m, nécessairement de la forme G''/Z avec G'' un sous-groupe de G contenant Z. Ainsi, on a $|G''| = |Z|m$ avec Z abélien distingué dans G'' et $|Z| \mid n$. Par le cas abélien du théorème de Schur-Zassenhaus, G'' possède un sous-groupe d'ordre m, ainsi donc que G. (Noter que l'on peut très bien avoir $Z = P = N$, et donc $G'' = G$, auquel cas on ne peut appliquer l'hypothèse de récurrence.) □

Remarque 3.4. On peut raffiner l'énoncé du théorème de Schur-Zassenhaus : Si N est abélien (voire même résoluble), alors les sous-groupes d'ordre m de G sont conjugués dans G : voir l'Exercice 6.36.

4. Les théorèmes de P. Hall

C'est le théorème suivant : [2]

Théorème 4.1. (P. Hall) *Soit G un groupe fini résoluble. On suppose $|G| = mn$ avec $m \wedge n = 1$. Alors G possède un sous-groupe d'ordre m.*

Un sous-groupe H d'un groupe G tel que $|H|$ et $|G|/|H|$ sont premiers entre eux est appelé *sous-groupe de Hall.*

2. P. Hall, *A note on soluble groups*, Journal London Math. Soc. 3 (1928).

Remarque 4.2. Le groupe A_5 n'est pas résoluble, et il est d'ordre $60 = 3 \cdot 4 \cdot 5$. Il possède bien des sous-groupes d'ordre 3, 4 et 5 (ses Sylow), ainsi qu'un sous-groupe d'ordre $3 \cdot 4 = 12$ (à savoir A_4). Par contre, il n'a pas de sous-groupe d'ordre 15 ou 20. En effet si H était un tel sous-groupe, l'action par translations de A_5 sur A_5/H (un ensemble à $n \leqslant 4$ éléments) fournirait un morphisme $\mathrm{A}_5 \to \mathrm{S}_n$ d'image transitive (donc non triviale). Un tel morphisme serait injectif car A_5 est simple : absurde car $|\mathrm{S}_n| < 60$ pour $n = 3$ ou 4.

Remarque 4.3. Le groupe A_4 est résoluble d'ordre 12. Il possède des sous-groupes cycliques d'ordre $1, 2, 3$, et un sous-groupe d'ordre 4 (à savoir K_4). En revanche, il ne possède pas de sous-groupe d'ordre 6. En fait, A_n n'a jamais de sous-groupe d'indice 2, car il contiendrait le carré (et donc l'inverse) de tout 3 cycle, et donc tous les 3-cycles, alors qu'on a vu que ces derniers engendrent A_n. Cela montre que l'hypothèse $m \wedge n = 1$ est nécessaire, même pour les groupes résolubles.

Démonstration — On procède par récurrence sur $|G|$, et on peut supposer $|G| \neq 1$. Comme G est résoluble, il possède un sous-groupe abélien distingué A non trivial. En effet, si r le plus petit entier $\geqslant 1$ tel que $\mathrm{D}^r(G) = 1$, alors $A = \mathrm{D}^{r-1}(G)$ convient (il est même caractéristique). Soit p premier divisant $|A|$. Le sous-groupe $A[p] = \{a \in A \mid a^p = 1\}$ est abélien p-élementaire, et non trivial par Cauchy. Il est caractéristique dans A, et donc distingué dans G. Quitte à remplacer A par $A[p]$ on peut donc supposer que A est un p-groupe abélien non trivial distingué dans G. Il y a deux cas :

Cas (a) : p divise m. Dans ce cas, on a $|A|$ divise m. Par récurrence, le groupe (résoluble !) G/A possède donc un sous-groupe d'ordre $m/|A|$. Il est donc de la forme H/A avec $A \subset H$, et on a donc $|H| = |H/A||A| = m$, ce que l'on voulait démontrer.

Cas (b) : p divise n. Dans ce cas, on a $|A|$ premier à m. Par récurrence, le groupe G/A possède un sous-groupe d'ordre m. Il est donc de la forme H/A avec A inclus dans H, et on a donc $|H| = |A|m$. Comme A est distingué dans H, on peut appliquer le théorème de Schur-Zassenhaus (dans le cas "abélien"), qui assure alors que H contient un sous-groupe d'ordre m. □

P. Hall démontre aussi que, sous les hypothèses du théorème ci-dessus, *tous les sous-groupes d'ordre m sont conjugués.* De manière tout aussi intéressante, Hall montre aussi une réciproque au théorème ci-dessus :

Théorème 4.4. (P. Hall) *Soit G un groupe fini d'ordre d. On suppose que pour toute factorisation $d = mn$ avec $m \wedge n = 1$, le groupe G possède un sous-groupe d'ordre m. Alors G est résoluble.*

Par exemple, supposons que l'on a $|G| = p^a q^b$ avec p, q premiers distincts. On sait que G a des sous-groupes d'ordre p^a et q^b, d'après Sylow ! On doit donc pouvoir en déduire que G est résoluble. C'est effectivement le cas, et c'est un théorème dû à Burnside. Sa démonstration utilise la théorie des caractères, et sera reportée à la toute fin du cours. Ce résultat de Burnside est un ingrédient essentiel dans la démonstration du théorème ci-dessus de Hall, dont nous reportons donc aussi la démonstration à plus tard.

5. Extensions et cohomologie

Le premier but de cette section est de démontrer le cas abélien du théorème de Schur-Zassenhaus, et donc de compléter les démonstrations des théorèmes précédents. Cela va nous conduire à réexaminer d'un peu plus près la théorie des extensions de groupes (Hölder, Schreier), et d'aborder des notions de *cohomologie des groupes*. Pour une exposition plus systématique, nous renvoyons par exemple au Chapitre 4 du cours *Groupes finis* de J.-P. Serre.

Fixons deux groupes A et G (non nécessairement finis). On s'intéresse aux *extensions* (E) *de* G *par* A, c'est-à-dire aux suites exactes courtes

$$(E) \qquad 1 \longrightarrow A \xrightarrow{i} \widetilde{G} \xrightarrow{\pi} G \longrightarrow 1$$

Deux questions naturelles sont : peut-on classifier toutes ces extensions ? Une extension étant donnée, à quelle condition est-ce que le sous-groupe distingué $i(A) = \ker \pi$ de $\widetilde{G}$ admet un complément K dans $\widetilde{G}$? En effet, si c'est le cas alors $\widetilde{G}$ est produit semi-direct interne de K par $i(A)$ par la Proposition 7.7 Chap. 4.

On rappelle que la notion de section d'une surjection a été introduite au chapitre 1. Si $\pi : G \to G'$ est un *morphisme de groupes surjectif*, on appellera *section de groupes* une section de π qui est en outre un morphisme de groupes $G' \to G$.

Lemme 5.1. *Soit* (E) *comme ci-dessus. Il y a équivalence entre :*

(i) $i(A)$ *admet un complément dans* $\widetilde{G}$*,*

(ii) π *admet une section de groupes* $s : G \to \widetilde{G}$*,*

Plus précisément, $s \mapsto s(G)$ *est une bijection entre l'ensemble des sections de groupes de* π *et l'ensemble des compléments de* $i(A)$ *dans* $\widetilde{G}$*.*

Démonstration — Montrons d'abord (ii) $\Longrightarrow$ (i). Soit s une section (ensembliste) de $\pi : \widetilde{G} \to G$. Tout élément de $\widetilde{G}$ s'écrit de manière unique $i(a)s(g)$ pour certains $a \in A$ et $g \in G$, et on a $i(A) \cap s(G) = \{s(1)\}$. Si s est un morphisme de groupes, le sous-groupe $K = s(G)$ vérifie donc $\widetilde{G} = i(A)K$ et $i(A) \cap s(G) = \{1\}$: c'est un complément de $i(A)$.

Supposons réciproquement que K est un complément de $i(A)$ dans $\widetilde{G}$: on a donc $i(A) \cap K = \{1\}$ et $\widetilde{G} = i(A)K$. Le morphisme $\pi_{|K} : K \to G$ a donc pour noyau $i(A) \cap K = \{1\}$, et pour image $\pi(K) = \pi(i(A)K) = \pi(\widetilde{G}) = G$ car $\pi(i(A)) = \{1\}$. C'est donc un isomorphisme. Notons $s : G \to K$ l'inverse de $\pi_{|K}$. C'est aussi un morphisme de groupes $G \to \widetilde{G}$ vérifiant $\pi \circ s = \mathrm{id}$: c'est la section de groupes de π vérifiant $s(G) = K$.

Les deux applications ci-dessus $K \mapsto s$ et $s \mapsto K$ sont clairement bijectives, d'où la dernière assertion. □

Définition 5.2. *On dit que la suite exacte courte* (E) *est scindée si les conditions équivalentes du Lemme 5.1 sont satisfaites.*

Notre premier but dans ce qui suit sera d'examiner en détails l'obstruction à ce que la suite exacte courte (E) soit scindée *dans le cas particulier où* A *est abélien.* Soulignons cette hypothèse.

Hypothèse : *On suppose désormais que le groupe A est abélien, noté additivement.*

Nous allons commencer par observer que sous cette hypothèse, la donnée d'une suite exacte (E) munit le groupe abélien A d'une structure de G-*module*.

Définition 5.3. *Un G-module est la donnée d'un groupe abélien $(A,+)$, muni d'une action $(g,a)\mapsto g.a$ de G sur A, vérifiant $g.(a+b)=g.a+g.b$ pour tout $g\in G$ et $a,b\in A$, ou ce qui revient au même, telle que le morphisme $G\to \mathrm{S}_A$ associé à l'action de G sur A est à valeurs dans* $\mathrm{Aut}(A)$.

Vérifions que la donnée de la suite exacte courte (E) munit naturellement le groupe abélien A d'une structure de G-module. Pour $g\in G$ et $a\in A$ on pose

$$g.a \;=\; i^{-1}(\widetilde{g}\,i(a)\,\widetilde{g}^{-1}), \tag{51}$$

où $\widetilde{g}\in\widetilde{G}$ est un élément quelconque de la fibre de π au dessus de g, *i.e.* avec $\pi(\widetilde{g})=g$. Cette définition a un sens car $i(A)$ est distingué dans $\widetilde{G}$ et i est injective. De plus, elle ne dépend pas du choix de $\widetilde{g}$. En effet, tout autre élément de cette fibre est de la forme $\widetilde{g}i(b)$ avec $b\in A$, et on a $\widetilde{g}\,i(b)\,i(a)\,i(b)^{-1}\,\widetilde{g}^{-1} \;=\; \widetilde{g}\,i(a)\,\widetilde{g}^{-1}$ car $A\simeq i(A)$ est abélien.

Proposition-Définition 5.4. *Pour toute extension (E) de G par un groupe abélien A, la formule* (51) *munit A s'une structure de G-module. On l'appellera structure de G-module* induite *par (E), et on dira aussi que (E) est une extension de G par le G-module A.*

Démonstration — Il est clair que l'on a $1.a=a$ (prendre $\widetilde{1}=1$), $g.(h.a)=(gh).a$ (prendre $\widetilde{gh}:=\widetilde{g}\widetilde{h}$) et $g.(a+b)=g.a+g.b$ car on a $\mathrm{int}_{\widetilde{g}|A}\in\mathrm{Aut}(i(A))$. □

Exemple 5.5. (Extensions centrales) Une extension (E) de G par A est dite *centrale* si on a $i(A)\subset \mathrm{Z}(\widetilde{G})$, ou ce qui revient au même, si on a $g.a=a$ pour tout $g\in G$ et $a\in A$ (de sorte que le G-module A associé est trivial). Ce cas est déjà très intéressant. Par exemple, les extensions $1\to\mu_n(k)\to\mathrm{SL}_n(k)\to\mathrm{PSL}_n(k)\to 1$, $1\to\{\pm1\}\to\mathrm{Sp}(1)\to\mathrm{SO}(3)\to 1$, ou encore les extensions de $\mathrm{A}_4,\mathrm{S}_4$ et A_5 par $\{\pm1\}$ qui s'en déduisent, sont des extensions centrales.

Fixons une extension (E) de G par A et considérons une section *ensembliste* $s:\widetilde{G}\to G$. Il en existe car π est surjective. Bien entendu, s n'a aucune raison d'être un morphisme de groupes. Observons que pour $g,g'\in G$, il existe un unique élément $c(g,g')\in A$ tel que

$$s(g)s(g') \;=\; i(c(g,g'))\,s(gg'). \tag{52}$$

En effet, on a $\pi(s(g)s(g'))=\pi(s(g))\pi(s(g'))=gg'=\pi(s(gg'))$, et donc l'élément $s(gg')^{-1}s(g)s(g')$ est dans $i(A)=\ker\pi$. Par définition s est un morphisme de groupes si, et seulement si, on a $c(g,g')=0$ pour tout $g,g'\in A$ (on rappelle que A est noté additivement). Ainsi, la fonction $c:G\times G\to A$ mesure l'obstruction à ce que s soit un morphisme de groupes. On la note $\mathrm{Ob}(s)$. Ce n'est pas une fonction quelconque :

Lemme 5.6. *Soient $(\widetilde{G},i,\pi)$ une extension de G par A, s une section ensembliste de π et $c=\mathrm{Ob}(s)$. On a*

$$g.c(g',g'')-c(gg',g'')+c(g,g'g'')-c(g,g')=0,\quad \forall g,g',g''\in G. \tag{53}$$

Démonstration — Pour $g, g', g'' \in G$ on calcule de deux façons, par associativité de la loi de groupes de $\widetilde{G}$, l'élément $s(g)s(g')s(g'')$. On obtient d'une part

$$s(g)\,(s(g')s(g'')) \;=\; s(g)\,i(c(g',g''))\,s(g'g'') =$$

$$=\; s(g)\,i(c(g',g''))\,s(g)^{-1}s(g)s(g'g'') \;=\; i(g.c(g',g''))\,i(c(g',g''))\,s(gg'g'')$$

(noter que $s(g)$ est un relèvement de g), et d'autre part

$$(s(g)s(g'))s(g'') \;=\; i(c(g,g'))\,s(gg')s(g'') \;=\; i(c(g,g'))\,i(c(gg',g''))\,s(gg'g''),$$

puis la formule de l'énoncé (en notation additive) en simplifiant par $s(gg'g'')$ et par injectivité du morphisme i. □

Définition 5.7. *Si A est un G-module, on note $\mathrm{Z}^2(G,A)$ l'ensemble des fonctions $G \times G \to A$ vérifiant l'identité* (53). *Une telle fonction est appelée* 2-cocycle de G à valeurs dans A.

Que se passe-t-il si l'on change de section ? Une autre section de π est nécessairement de la forme $s_\epsilon : g \mapsto i(\epsilon(g))\,s(g)$, où ϵ est une fonction arbitraire $G \to A$. Les 2-cocycles $c = \mathrm{Ob}(s)$ et $c_\epsilon = \mathrm{Ob}(s_\epsilon)$ sont alors liés par la formule

$$c_\epsilon(g,g') = c(g,g') + g.\epsilon(g') - \epsilon(gg') + \epsilon(g), \quad \forall\, g,g' \in G. \tag{54}$$

En effet, il suffit de constater

$$s_\epsilon(g)s_\epsilon(g') = i(c_\epsilon(g,g'))s_\epsilon(gg') = i(c_\epsilon(g,g'))\,i(\epsilon(gg'))\,s(gg')$$

$$=\; i(\epsilon(g))\,s(g)\,i(\epsilon(g'))\,s(g') = i(\epsilon(g))i(g.\epsilon(g'))\,s(g)s(g') = i(\epsilon(g)+g.\epsilon(g')+c(g,g'))s(gg').$$

Définition 5.8. *Si A est un G-module, on note $\mathrm{B}^2(G,A)$ l'ensemble des fonctions $f : G \times G \to A$ de la forme $(g,g') \mapsto g.\epsilon(g') - \epsilon(gg') + \epsilon(g)$, avec $\epsilon : G \to A$. Une telle fonction f est appelée* 2-cobord de G *à valeurs dans A.*

Notons que $\mathrm{Z}^2(G,A)$ et $\mathrm{B}^2(G,A)$ sont manifestement des sous-groupes du groupe abélien de toutes les fonctions $G \times G \to A$ (pour l'addition des fonctions).

Proposition-Définition 5.9. *Pour tout G-module A, le groupe $\mathrm{B}^2(G,A)$ est un sous-groupe de $\mathrm{Z}^2(G,A)$ et on définit le 2ème groupe de cohomologie de G à valeurs dans A comme le groupe abélien quotient*

$$\mathrm{H}^2(G,A) = \mathrm{Z}^2(G,A)/\mathrm{B}^2(G,A).$$

Démonstration — Quand le G-module A est issu de notre construction, (ce qui est en fait toujours le cas comme on le verra plus loin) on constate que tout cobord est la différence de deux cocycles par la Formule (54). En général, le calcul trivial suivant montre $\mathrm{B}^2(G,A) \subset \mathrm{Z}^2(G,A)$:

$$gg'.\epsilon(g'') - g.\epsilon(g'g'') + g.\epsilon(g') - gg'.\epsilon(g'') + \epsilon(gg'g'') - \epsilon(gg') + g.\epsilon(g'g'') - \epsilon(gg'g'') + \epsilon(g) - g.\epsilon(g') + \epsilon(gg') - \epsilon(g) = 0$$

□

Scholie : Résumons les observations ci-dessus. Chaque extension (E) d'un groupe G par un groupe abélien A définit d'abord une structure de G-module sur A. De plus, si s est une section ensembliste de $\pi : \widetilde{G} \to G$, la classe

$$[\mathrm{Ob}(s)] \in \mathrm{H}^2(G, A)$$

ne dépend pas du choix de la section s par la formule (52), on la note $[E]$ et on l'appelle *classe de cohomologie* associée à (E).

Proposition 5.10. *La suite exacte courte (E) est scindée si, et seulement si sa classe* $[E] \in \mathrm{H}^2(G, A)$ *est nulle.*

Démonstration — Si (E) est scindée, on peut trouver une section s qui est un morphisme de groupes par le Lemme 5.1. Pour une telle section, on a $\mathrm{Ob}(s) = 0$, et on a donc $[E] = [\mathrm{Ob}(s)] = [0] = 0$. Supposons inversement $[E] = 0$. Soient s une section arbitraire de π et $c = \mathrm{Ob}(s) \in \mathrm{Z}^2(G, A)$. On a donc $[E] = [c] = 0$ et donc $c \in \mathrm{B}^2(G, A)$. Autrement dit, il existe $\epsilon : G \to A$ avec $c(g, g') = g.\epsilon(g') - \epsilon(gg') + \epsilon(g)$. Mais par la Formule (54) cela signifie $c_{-\epsilon} = \mathrm{Obs}(s_{-\epsilon}) = 0$, autrement dit la section $s_{-\epsilon}$ est un morphisme de groupes, et la suite est scindée par le Lemme 5.1. □

Exemple 5.11. Pour tout sous-groupe fini G d'ordre pair dans $\mathrm{SO}(3)$, par exemple $G \simeq \mathbb{Z}/2n\mathbb{Z}, \mathrm{D}_{2n}, \mathrm{A}_4, \mathrm{S}_4$ et A_5, on a construit à l'aide du morphisme $\mathrm{Sp}(1) \to \mathrm{SO}(3)$ une extension centrale non scindée

$$1 \to \mathbb{Z}/2\mathbb{Z} \to \widetilde{G} \to G \to 1.$$

On en déduit dans chacun de ces cas que l'on a $\mathrm{H}^2(G, \mathbb{Z}/2\mathbb{Z}) \neq 0$, où $\mathbb{Z}/2\mathbb{Z}$ est vu comme G-module trivial. De même on a $\mathrm{H}^2(\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z}), \mathbb{Z}/2\mathbb{Z}) \neq 0$ pour $p \neq 2$, car l'extension centrale $1 \to \mathbb{Z}/2\mathbb{Z} \to \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z}) \to 1$ est non scindée.

Le cas abélien du théorème de Schur-Zassenhaus découle alors du :

Théorème 5.12. (Schur-Zassenhaus, version cohomologique) *Soient G un groupe et A un G-module.*

(i) Si G est fini, alors on a $|G|x = 0$ pour tout $x \in \mathrm{H}^2(G, A)$.

(ii) Si A est fini, alors on a $|A|x = 0$ pour tout $x \in \mathrm{H}^2(G, A)$.

En particulier, si G et A sont finis avec $|G| \wedge |A| = 1$ on a $\mathrm{H}^2(G, A) = 0$.

Démonstration — Montrons le (i). Soit $c \in \mathrm{Z}^2(G, A)$. Il faut montrer $|G|\, c \in \mathrm{B}^2(G, A)$. Mais on a

$$c(g, g') = g.c(g', g'') - c(gg', g'') + c(g, g'g''), \quad \forall g, g', g'' \in G.$$

Pour $g \in G$, considérons la somme finie $\epsilon(g) = \sum_{h \in G} c(g, h)$. Fixant g, g' et sommant sur tous les g'' dans le groupe fini G l'équation ci-dessus, on constate

$$|G|\, c(g, g') \;=\; g.\epsilon(g') - \epsilon(gg') + \epsilon(g),$$

et on a gagné ! Pour le (ii), on observe que pour toute fonction $f : G \times G \to A$ on a $|A|\, f = 0$ (Lagrange). Enfin, la dernière assertion découle de Bézout : il existe $u, v \in \mathbb{Z}$ tels que $u|A| + v|G| = 1$. Pour tout $x \in \mathrm{H}^2(G, A)$ on a donc $x = u|A|x + v|G|x = 0 + 0 = 0$ par (i) et (ii). □

Terminons cette section en expliquant, suivant Hölder et Schreier, comment $\mathrm{H}^2(G, A)$ permet de classifier, pour une relation d'isomorphisme adéquate, les extensions de G par A. Il y a deux énoncés, de type existence et unicité.

Proposition 5.13. (Existence) *Pour tout G-module A, et tout $x \in \mathrm{H}^2(G, A)$, il existe une extension (E) de G par le G-module A vérifiant $[E] = x$.*

Démonstration — Fixons $c \in Z^2(G, A)$. Observons d'abord que quitte à ajouter à c le cobord $(g, g') \mapsto -c(1, g) - g.c(1, g') + c(1, gg')$, qui vaut $-c(1, 1)$ en $(1, 1)$, on peut supposer $c(1, 1) = 0$.[3] En prenant respectivement $(g, 1, 1)$, $(1, g, g^{-1})$ et (g^{-1}, g, g^{-1}) pour (g, g', g'') dans l'équation fonctionnelle de c on trouve alors

$$c(1, g) = c(g, 1) = 0 \text{ et } c(g, g^{-1}) = g.c(g^{-1}, g), \quad \forall g \in G. \tag{55}$$

On définit une loi de composition $\star$ sur l'ensemble produit $A \times G$ en posant

$$(a, g) \star (a', g') = (a + g.a' + c(g, g'), gg').$$

(C'est une loi de produit semi-direct si $c = 0$!) La propriété $c \in \mathrm{Z}^2(G, A)$ est alors équivalente à l'associativité de $\star$: c'est exactement le calcul fait dans le Lemme 5.6. La relation $c(1, g) = c(g, 1) = 0$ pour tout g montre que $(0, 1)$ est un élément neutre de $\star$, puis que (a, g) a pour inverse (a', g^{-1}) avec a' l'unique élément de A tel que $a + g.a' + c(g, g^{-1}) = 0$, ou ce qui revient au même $a' + g^{-1}a + c(g^{-1}, g) = 0$ car $c(g^{-1}, g) = g^{-1}c(g, g^{-1})$. Cela montre que $\star$ est une loi de groupe sur $A \times G$.

L'application $i : A \to A \times G, a \mapsto (a, 1)$, est clairement injective, et un morphisme de $(A, +)$ dans $(A \times G, \star)$ par $\mathrm{c}(1, 1) = 0$. La surjection canonique $\pi : A \times G \to G, (a, g) \mapsto g$, est clairement un morphisme de noyau $i(A)$. Une section ensembliste naturelle de π est $s(g) = (0, g)$. On a bien défini une suite exacte courte du type (E) avec $\widetilde{G} = (A \times G, \star)$. Pour $a \in A$ et $g \in G$, un calcule direct montre

$$s(g) \star i(a) \star s(g)^{-1} = (g.a, 1) = i(g.a)$$

(utiliser $s(g)^{-1} = (-c(g^{-1}, g), g^{-1})$ et $c(g^{-1}, g) = g^{-1}.c(g, g^{-1})$) de sorte que la structure de G-module sur A induite par $\widetilde{G}$ est bien le G-module A dont on est parti. Enfin, par définition on a

$$s(g) \star s(g') = (0, g) \star (0, g') = (c(g, g'), gg') = (c(g, g'), 1) \star (0, gg')$$

et on a donc $c = \mathrm{Ob}(s)$, puis $[c] = [E]$. □

Proposition 5.14. (Unicité) *Soient A un G-module et $E_k = (\widetilde{G}_k, i_k, \pi_k)$ pour $k = 1, 2$ deux extensions de G par le même G-module A. On a $[E_1] = [E_2]$ si, et seulement si, il existe un isomorphisme $\varphi : \widetilde{G}_1 \to \widetilde{G}_2$ vérifiant $\varphi \circ i_1 = i_2$ et $\pi_2 \circ \varphi = \pi_1$.*

Démonstration — Si $\varphi : \widetilde{G}_1 \to \widetilde{G}_2$ est un morphisme comme dans l'énoncé, et si s_1 est une section de π_1, on constate que $s_2 := \varphi \circ s_1$ est une section de π_2. De plus, appliquant φ à $s_1(g)s_1(g') = i_1(c(g, g'))s_1(gg')$, et en utilisant $i_2 = \varphi \circ i_1$, on a $\mathrm{Ob}(s_2) = \mathrm{Ob}(s_1)$, puis $[E_1] = [E_2]$.

Supposons réciproquement $[E_1] = [E_2]$. Soient s_1 une section de π_1, et $c = \mathrm{Ob}(s_1)$. Comme $[E_2] = [c]$, on peut également trouver une section s_2 de π_2 avec

3. C'est typiquement ce qui se passe si on a $c = \mathrm{Ob}(s)$ avec s vérifiant $s(1) = 1$, et c'est cela qui nous permet de deviner le calcul à faire.

$\mathrm{Ob}(s_2) = c$. On a donc $s_k(g)s_k(g') = i_k(c(g,g'))s_k(gg')$ pour tout $g, g' \in G$ et $k = 1, 2$. Comme tout élément $\widetilde{G_k}$ s'écrit de manière unique sous la forme $i_k(a)\, s_k(g)$ avec $a \in A$ et $g \in G$, on dispose d'une bijection $\varphi : \widetilde{G_1} \to \widetilde{G_2}, i_1(a)\, s_1(g) \mapsto i_2(a)\, s_2(g)$, vérifiant manifestement $\varphi \circ i_1 = i_2$ et $\pi_2 \circ \varphi = \pi_1$. Pour $a, a' \in A$, $g, g' \in G$, et $k = 1, 2$, on constate $i_k(a)s_k(g)i_k(a')s_k(g') = i_k(a + g.a' + c(g,g'))s_k(gg')$, donc φ est un morphisme de groupes. □

La notion d'isomorphisme entre deux extensions mise en avant dans l'énoncé ci-dessus s'exprime garphiquement par la commutativité du diagramme :

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r, "i_1"] \arrow[d, "\mathrm{id}"] \arrow[dr, phantom, "\circlearrowleft"] & \widetilde{G_1} \arrow[r, "\pi_1"] \arrow[d, "\varphi"] \arrow[dr, phantom, "\circlearrowleft"] & G \arrow[r] \arrow[d, "\mathrm{id}"] & 1 \\
1 \arrow[r] & A \arrow[r, "i_2"] & \widetilde{G_2} \arrow[r, "\pi_2"] & G \arrow[r] & 1
\end{tikzcd}$$

On prendra garde que la notion d'isomorphisme ci-dessus est très fine : il est fréquent d'avoir deux extensions $(\widetilde{G}_1, i_1, \pi_1)$ et $(\widetilde{G}_2, i_2, \pi_2)$ non isomorphes en tant qu'extensions, mais avec $\widetilde{G}_1 \simeq \widetilde{G}_2$. Toutefois, c'est cette notion d'isomorphisme qui donne lieu à des énoncés élégants.

Corollaire 5.15. *Soit A un G-module. L'application $(E) \mapsto [E]$ induit une bijection entre l'ensemble $\mathscr{E}(G, A)$ des classes d'isomorphisme d'extensions de G par le G-module A et l'ensemble* $\mathrm{H}^2(G, A)$.

On en déduit, par transport de structure, que $\mathscr{E}(G, A)$ est muni d'une loi de groupe abélien ! (Nous verrons dans l'Exercice 6.32, suivant Baer, comment définir cette loi de manière directe.) Par la Proposition 5.10, son élément neutre est l'extension naturelle de G par A définie par le produit semi-direct $A \rtimes G$ associé au morphisme donné $G \to \mathrm{Aut}(A)$.

Tout ceci est un point de départ pour une étude plus appronfondie de $\mathscr{E}(G, A)$, ou ce qui revient au même, des groupes $\mathrm{H}^2(G, A)$. C'est une question en générale difficile. Pour aller plus loin, par exemple pour être en mesure de déterminer $\mathrm{H}^2(G, A)$ pour des A et G concrets, il devient nécessaire d'avoir un point de vue plus abstrait sur les groupes $\mathrm{H}^2(G, A)$ (voire même un point de vue topologique !). Ces développements dépassent le cadre introductif de ce cours. Mentionnons simplement le théorème suivant, dû à Schur (1911), qui classifie les extensions centrales de A_n par $\mathbb{Z}/2\mathbb{Z}$.

Théorème 5.16. (Schur) *Considérons $\mathbb{Z}/2\mathbb{Z}$ comme A_n-module trivial. On a*

$$\mathrm{H}^2(\mathrm{A}_n, \mathbb{Z}/2\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \ \text{ pour } \ n \geqslant 4.$$

On a aussi $\mathrm{H}^2(\mathrm{A}_3, \mathbb{Z}/2\mathbb{Z}) = \mathrm{H}^2(\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) = 0$, par exemple par Schur-Zassenhaus ou même simplement par la classification des groupes d'ordre 6. On a déjà vu que $\widetilde{\mathrm{A}}_4$ et $\widetilde{\mathrm{A}}_5$ définissent des extensions centrales non scindées de A_4 et A_5 par $\mathbb{Z}/2\mathbb{Z}$ respectivement : ce sont des générateurs de $\mathrm{H}^2(\mathrm{A}_n, \mathbb{Z}/2\mathbb{Z})$. D'après le théorème ci-dessus, ces groupes $\widetilde{\mathrm{A}_n}$ ont donc des analogues pour tout $n > 5$. En fait, Schur a aussi étudié les extensions centrales de A_n par $\mathbb{Z}/p\mathbb{Z}$ avec p premier impair. Pour $n \geqslant 3$, il a montré qu'elles sont toutes scindées, *i.e.* $\mathrm{H}^2(\mathrm{A}_n, \mathbb{Z}/p\mathbb{Z}) = 0$, sauf pour $p = 3$ et $n = 3, 4, 6$ ou 7, auquel cas on a $\mathrm{H}^2(\mathrm{A}_n, \mathbb{Z}/3\mathbb{Z}) \simeq \mathbb{Z}/3\mathbb{Z}$.

6. Complément I : Groupes nilpotents finis

Soit G un groupe. Pour $A, B \subset G$, on note $[A, B]$ le sous-groupe engendré par les commutateurs $aba^{-1}b^{-1}$ avec $a \in A$ et $b \in B$. On définit une suite de sous-groupes $\mathscr{C}^i(G)$ de G en posant $\mathscr{C}^0(G) = G$ puis, pour tout $i \geqslant 0$,

$$\mathscr{C}^{i+1}(G) = [G, \mathscr{C}^i(G)].$$

Définition 6.1. *Un groupe G est dit nilpotent s'il existe $i \geqslant 0$ avec $\mathscr{C}^i(G) = \{1\}$.*

Par exemple, on a $\mathscr{C}^1(G) = \mathrm{D}(G)$ (groupe dérivé de G). En revanche, le sous-groupe $\mathscr{C}^2(G) = [G, \mathrm{D}(G)]$ contient en général strictement $\mathrm{D}^2(G) = [\mathrm{D}(G), \mathrm{D}(G)]$.

Exemple 6.2. *Pour $G = \mathrm{S}_3$ on a $\mathrm{D}(G) = \mathrm{A}_3$, donc $\mathrm{D}^2(G) = \{1\}$, mais $\mathscr{C}^i(G) = \mathrm{A}_3$ pour tout $i \geqslant 1$. En particulier, le groupe résoluble S_3 n'est pas nilpotent.*

Comme pour les groupes dérivés, on constate que pour tout morphisme $f : G \to G'$ on a $f(\mathscr{C}^i(G)) \subset \mathscr{C}^i(G')$, avec égalité si f est surjectif. En particulier, on en déduit :

Proposition 6.3. *Pour tout $i \geqslant 0$, $\mathscr{C}^i(G)$ est un sous-groupe caractéristique (en particulier distingué) de G. De plus, on a $\mathscr{C}^i(G) \supset \mathscr{C}^{i+1}(G)$ et $\mathscr{C}^i(G) \supset \mathrm{D}^i(G)$ pour tout $i \geqslant 0$.*

Démonstration — Le premier point résulte de la remarque précédente appliquée aux automorphismes intérieurs de G. Pour le second, il suffit de voir que si H est distingué dans G, et $g \in G$, on a $[g, H] \subset H$. Mais cela vient de $[g, h] = (ghg^{-1})h^{-1}$. □

On en déduit que *nilpotent* implique *résoluble*, et que l'exemple de S_3 montre que la réciproque est fausse. Les groupes abéliens sont trivialement nilpotents. On vérifie immédiatement que les produits finis de groupes nilpotents sont nilpotents : on a $\mathscr{C}^i(G_1 \times G_2) = \mathscr{C}^i(G_1) \times \mathscr{C}^i(G_2)$.

Remarque 6.4. Un groupe nilpotent non trivial a un centre non trivial. En effet, soit i le plus petit entier $\geqslant 1$ tel que $\mathscr{C}^i(G) = \{1\}$. Si $i = 1$ alors G est abélien. Sinon, $\mathscr{C}^{i-1}(G) \neq \{1\}$ est inclus dans $\mathrm{Z}(G)$.

Les groupes nilpotents vérifient les propriétés de stabilité suivantes :

Proposition 6.5. *(i) Un sous-groupe d'un groupe nilpotent est nilpotent.*

(ii) Le quotient d'un groupe nilpotent par un sous-groupe distingué est nilpotent.

(iii) Si H est un sous-groupe central d'un groupe nilpotent G, et si G/H est nilpotent, alors G est nilpotent.

Démonstration — Si H est un sous-groupe de G, on constate $\mathscr{C}^i(H) \subset \mathscr{C}^i(G)$ pour tout $i \geqslant 0$. Cela montre le (i). Si $\pi : G \to G'$ est surjectif, on a déjà dit que $\pi(\mathscr{C}^i(G)) = \mathscr{C}^i(G')$. Cela montre le (ii) (prendre pour π la projection canonique). Cela montre aussi, dans le contexte du (iii), qu'il existe $i \geqslant 0$ tel que $\mathscr{C}^i(G) \subset H \subset \mathrm{Z}(G)$. On en déduit $\mathscr{C}^{i+1}(G) = \{1\}$. □

Corollaire 6.6. *Les p-groupes sont nilpotents.*

Démonstration — Soit P un p-groupe. On montre qu'il est nilpotent par récurrence sur $|P|$. On sait $\mathrm{Z}(P) \neq \{1\}$. Donc $P/\mathrm{Z}(P)$ est un p-groupe d'ordre $< |P|$. Par récurrence il est nilpotent, ainsi donc que P par la Proposition 6.5 (iii). □

En particulier, $\mathrm{U}_n(\mathbb{Z}/p\mathbb{Z})$ est un groupe nilpotent. En fait, on a plus généralement (vérification laissée au lecteur) :

Proposition 6.7. *Pour tout corps k, le sous-groupe $\mathrm{U}_n(k)$ de $\mathrm{GL}_n(k)$ est nilpotent.*

De manière un peu surprenante, les groupes nilpotents finis se ramènent aux p-groupes. Le théorème suivant est démontré par M. Hall dans son classique *The theory of Groups* (Chapitre 10 p.155), certaines des équivalences étant dues à Wielandt.

Théorème 6.8. *Soit G un groupe fini. Il y a équivalence entre :*

(i) G est nilpotent,

(ii) pour tout sous-groupe strict H de G on a $H \subsetneq \mathrm{N}_G(H)$,

(iii) les sous-groupes maximaux de G sont distingués,

(iv) les p-Sylow de G sont distingués,

(v) G est produit direct de ses p-Sylow.

Démonstration — On a déjà vu (iv) $\Longrightarrow$ (i), car les p-groupes sont nilpotents et un produit fini de groupes nilpotents et nilpotent.

Montrons (i) $\Longrightarrow$ (ii) par récurrence sur $|G|$. On peut supposer G non trivial. On sait alors que $Z := \mathrm{Z}(G)$ est non trivial. Soit H un sous-groupe strict de G. Si Z n'est pas inclus dans H, alors Z est un sous-groupe de $\mathrm{N}_G(H)$ non inclus dans H, ce qui conclut. Supposons donc Z est inclus dans H. Le sous-groupe H/Z de G/Z est strict, car H est strict dans G. Mais G/Z est nilpotent par la Proposition 6.5, donc par récurrence il existe $g \in G \smallsetminus H$ tel que gZ normalise H/Z. Mais cela signifie $gHg^{-1} \subset HZ = Z$, et donc $g \in \mathrm{N}_G(H) \smallsetminus H$.

L'implication (ii) $\Longrightarrow$ (iii) est évidente. Montrons (iii) $\Longrightarrow$ (iv). Soit P un p-Sylow de G. Si P n'est pas distingué dans G, alors son normalisateur $\mathrm{N}_G(P)$ est strict, et s'inclut donc dans un sous-groupe maximal M de G. Par (ii), M est distingué. De plus P est clairement un p-Sylow de M. On a donc $G = M\mathrm{N}_G(P)$ par le Lemme de Frattini, puis $G \subset M$: absurde.

Montrons enfin (iv) $\Longrightarrow$ (v). Écrivons $|G| = \prod_{i=1}^n p_i^{\alpha_i}$ la décomposition en facteurs premiers de $|G|$. Soit P_i un p_i-Sylow de G. Soient i et j distincts. On a $P_i \cap P_j = \{1\}$ par Lagrange. Pour $x \in P_i$ et $y \in P_j$ on a (« deux façons de voir un commutateur ») $xyx^{-1}y^{-1} = (xyx^{-1})y^{-1} = x(yxy^{-1}) \in P_i \cap P_j = \{1\}$ et donc $xy = yx$. On en déduit que l'application

$$\varphi : \prod_{i=1}^n P_i \to G, (x_1, \ldots, x_n) \mapsto x_1 x_2 \cdots x_n,$$

est un morphisme de groupes. Son image contient P_i pour tout i. On a donc $p_i^{\alpha_i} \mid |\mathrm{Im}\,\varphi|$ pour tout i, puis $\mathrm{Im}\,\varphi = G$, et donc $\ker \varphi = \{1\}$: c'est un isomorphisme. □

COROLLAIRE 6.9. *Dans un groupe nilpotent fini, deux éléments x et y d'ordres premiers entre eux commutent.*

DÉMONSTRATION — En effet, par le théorème on peut supposer que notre groupe nilpotent fini est produit direct d'un nombre fini de p-groupes P_i, disons $i = 1, \ldots, r$, avec les $|P_i|$ premiers entre eux. Soit $x = (x_1, \ldots, x_r)$ dans $\prod_{i=1}^r P_i$. Si x est d'ordre a, on a $x_i^a = 1$ pour tout i, et donc $x_i = 1$ pour $(a, |P_i|) = 1$. Ainsi, si x et y sont d'ordres premiers entre eux, alors pour tout i on a soit $x_i = 1$, soit $y_i = 1$, et on a donc bien $xy = yx$. □

COROLLAIRE 6.10. *Soient G un groupe nilpotent fini, ainsi que $P_1, \ldots, P_n$ ses sous-groupes de Sylow (distingués). On a un isomorphisme de groupes*

$$\mathrm{Aut}(G) \simeq \prod_{i=1}^{n} \mathrm{Aut}(P_i).$$

DÉMONSTRATION — En effet, comme chaque p-Sylow de G est distingué, il est aussi caractéristique (unique sous-groupe ayant l'ordre en question), de sorte que l'application $\mathrm{Aut}(G) \to \prod_{i=1}^n \mathrm{Aut}(P_i), \varphi \mapsto (\varphi_{|P_i})$, est bien définie. C'est clairement un morphisme de groupes. Comme G est produit direct interne des P_i par le Théorème 6.8, il est manifestement injectif et surjectif, donc bijectif. □

7. Complément II : La caractérisation de Burnside-Dickson-Pazderski

Dans ce complément, qui fait suite au précédent, on se propose de prouver le théorème suivant, démontré dans G. Pazderski, *Die Ordnungen, zu denen nur Gruppen mit gegebener Eigenschaft gehören*, Arch. Math., 10, 331–343 (1959). Un entier n sera dit *nilpotent* si sa décomposition en facteurs premiers $n = \prod_{i=1}^r {p_i}^{k_i}$, avec les p_i distincts, est telle que pour tout $i \neq j$, et tout $1 \leqslant k \leqslant k_j$, p_i ne divise pas $p_j^k - 1$.

THÉORÈME 7.1. (Pazderski) *L'entier $n \geqslant 1$ est nilpotent si, et seulement si, tout groupe d'ordre n est nilpotent.*

L'exposition qui suit est inspirée de notes d'un cours de N. Tosel (1995). Montrons d'abord que si tout groupe d'ordre n est nilpotent alors n est nilpotent.

LEMME 7.2. *Soient p et q deux nombres premier, et $k \geqslant 1$, avec $q \mid p^k - 1$. Alors il existe un groupe non nilpotent d'ordre $p^k q$.*

DÉMONSTRATION — Posons $P = (\mathbb{Z}/p\mathbb{Z})^k$. C'est un groupe abélien p-élémentaire. Son groupe d'automorphisme coïncide donc avec celui du $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel associé, ce qui démontre $\mathrm{Aut}(P) = \mathrm{GL}_k(\mathbb{Z}/p\mathbb{Z})$. De la formule pour $|\mathrm{GL}_k(\mathbb{Z}/p\mathbb{Z})|$, on déduit que le cardinal de $\mathrm{Aut}(P)$ est multiple de $p^k - 1$. Par hypothèse, on en déduit que q divise $|\mathrm{Aut}(P)|$ et donc qu'il existe un morphisme injectif $\varphi : \mathbb{Z}/q\mathbb{Z} \to \mathrm{Aut}(P)$. Considérons le produit semi-direct associé $G = (\mathbb{Z}/p\mathbb{Z})^k \rtimes_\varphi \mathbb{Z}/q\mathbb{Z}$. Il est d'ordre $p^k q$. S'il était nilpotent, son unique p-Sylow serait $P' = P \times \{0\}$, et son unique q-Sylow serait $Q' = \{0\} \times \mathbb{Z}/q\mathbb{Z}$, et on aurait $ab = ba$ pour tout $a \in P'$ et $b' \in Q'$. C'est absurde car l'action de Q' par conjugaison sur P' est donnée par φ, donc non triviale. □

Corollaire 7.3. *Si tout groupe d'ordre n est nilpotent, alors n est nilpotent.*

Démonstration — En effet, si on a p_i, q_i et $1 \leqslant k \leqslant k_i$ avec $q_i \mid p_i^k - 1$, et si G est non nilpotent d'ordre $p_i^k q_i$ (par le lemme), alors $G \times \mathbb{Z}/m\mathbb{Z}$ avec $m = n/(p_i^k q_i)$ est non nilpotent d'ordre n (Proposition 6.5). □

La réciproque est plus délicate et nécessitera plusieurs étapes. On commence par montrer la proposition suivante, qui généralise au cas nilpotent (plutôt qu'abélien) le Problème 2 du partiel 2021-2022 (voir §1 App. B).

Proposition 7.4. (Non simplicité d'un groupe non nilpotent minimal) *Soit G un groupe fini non nilpotent dont tous les sous-groupes stricts sont nilpotents. Alors G n'est pas simple.*

La démonstration repose sur un examen des sous-groupes maximaux de G. Pour G fini on notera $\mathscr{M}(G)$ l'ensemble des sous-groupes $\{1\} \subsetneq M \subsetneq G$ maximaux pour l'inclusion.

Lemme 7.5. *On suppose G fini simple non cyclique. Alors il existe $A, B \in \mathscr{M}(G)$ avec $A \neq B$ et $A \cap B \neq \{1\}$.*

Démonstration — [4] Comme G n'est pas cyclique, observons que pour tout $g \in G \smallsetminus \{1\}$ on a $\{1\} \subsetneq \langle g \rangle \subsetneq G$, et donc il existe $M \in \mathscr{M}(G)$ avec $g \in M$. En particulier, l'ensemble $\mathscr{M}(G)$ est non vide.

Le groupe G agit sur $\mathscr{M}(G)$ par conjugaison. Observons que le stabilisateur dans G d'un $M \in \mathscr{M}(G)$ coïncide avec M. En effet, ce stabilisateur est $\mathrm{N}_G(M)$, contient M, et vaut donc M ou G par maximalité de M. Mais on a $M \neq \{1\}$ et $M \lhd \mathrm{N}_G(M)$, et donc $\mathrm{N}_G(M) = M$ par simplicité de G.

Supposons par l'absurde que le seul élément de G agissant sur $\mathscr{M}(G)$ avec au moins deux points fixes est l'identité. D'après l'Exercice 5.10, le groupe G agit transitivement sur $\mathscr{M}(G)$. D'après le lemme de Jordan (Exercice 5.9 (ii)), il existe alors $g \in G$ sans point fixe dans $\mathscr{M}(G)$, autrement dit n'appartenant à aucun sous-groupe maximal de G, en contradiction avec le premier paragraphe. □

Démonstration — (de la Proposition 7.4). Supposons G simple. D'après le Lemme 7.5, il suffit de montrer que pour tout $A, B \in \mathscr{M}(G)$, on a $A \cap B = \{1\}$ ou $A = B$. Considérons $\{A, B\} \subset \mathscr{M}(G)$ avec $A \neq B$ et $|A \cap B|$ maximal, et supposons par l'absurde $A \cap B \neq \{1\}$. Posons $H = \mathrm{N}_G(A \cap B)$; on a $H \neq G$, car G est simple, et $H \neq \{1\}$ car $A \cap B \neq \{1\}$. On peut donc choisir $C \in \mathscr{M}(G)$ contenant H. Quitte à échanger les rôles de A et B on peut supposer $C \neq A$, car on a $A \neq B$. On constate

$$C \cap A \supset \mathrm{N}_G(A \cap B) \cap A = \mathrm{N}_A(A \cap B).$$

Mais $A \cap B = A$ implique $A \subset B$, une contradiction, donc $A \cap B$ est un sous-groupe strict du groupe nilpotent A. On en déduit $\mathrm{N}_A(A \cap B) \supsetneq A \cap B$ par le Théorème 6.8 (ii), puis $C \cap A \supsetneq B \cap A$ et $C \neq A$, contredisant la maximalité de $|A \cap B|$. □

4. La preuve ci-dessous est une variante de celle donnée dans le corrigé des questions (iv) à (viii) du Problème 2 du partiel 2021-2022, Sect. 7 App. B, utilisant les Exercices 5.9 et 5.10.

Démonstration — (du Théorème 7.1) D'après le Corollaire 7.3, il ne reste qu'à montrer que si n est nilpotent, alors tout groupe d'ordre n est nilpotent. On procède par récurrence sur l'entier nilpotent $n \geqslant 1$. Soit G d'ordre n. Tout diviseur de n étant encore nilpotent par définition, on en déduit par Lagrange et par récurrence que tout sous-groupe strict de G, et tout quotient strict de G, est nilpotent. Par la Proposition 7.4, on peut supposer que G n'est pas simple. On se donne H distingué dans G avec $1 < |H| < |G|$. On va utiliser ce H pour montrer $\mathrm{Z}(G) \neq \{1\}$ aux Faits 2 et 3 ci-dessous. Cela concluera car cela montre que $G/\mathrm{Z}(G)$ est nilpotent par récurrence, puis que G est nilpotent par la Proposition 6.5.

Fait 1 : *G possède un p-Sylow distingué.* Soient p premier divisant $|H|$ et P un p-Sylow de H. Comme H est nilpotent, P est l'unique p-Sylow de H. Il est donc caractéristique dans H, puis distingué dans G. Si P est un p-Sylow de G on a gagné. Sinon, on regarde G/P. Il est nilpotent et d'ordre mutiple de p, donc possède un p-Sylow distingué P' par récurrence. Mais alors on a $P' = Q/P$ avec Q un p-Sylow de G, ce qui conclut.

Fait 2 : *G possède un sous-groupe abélien p-élémentaire non trivial et distingué.* En effet, soit P un p-Sylow distingué de G (Fait 1). Alors $\mathrm{Z}(P)$ est non trivial, distingué dans P, et son sous-groupe caractéristique $\{x \in \mathrm{Z}(P) \mid x^p = 1\}$ convient.

Fait 3 : *Soit A un sous-groupe abélien p-élémentaire non trivial et distingué dans G, on a $A \subset \mathrm{Z}(G)$.* On a $A \simeq (\mathbb{Z}/p\mathbb{Z})^m$ pour un certain $m \geqslant 1$. Soient $\ell \neq p$ divisant $|G|$ et S un ℓ-Sylow de G. On regarde l'action naturelle de S par conjugaison sur A. Elle induit un morphisme $S \to \mathrm{Aut}(A)$. Mais $|S|$ est une puissance de ℓ et on a $|\mathrm{Aut}(A)| = |\mathrm{GL}_m(\mathbb{Z}/p\mathbb{Z})| = p^{m(m-1)/2} \prod_{1 \leqslant i < m}(p^i - 1)$. Comme n est nilpotent (enfin !), et que p^m et ℓ sont des diviseurs de $n = |G|$, on a $(|S|, |\mathrm{Aut}(A)|) = 1$ et tout morphisme $S \to \mathrm{Aut}(A)$ est trivial. Ainsi, S agit trivialement par conjugaison sur A, et donc S est inclus dans le centralisateur $\mathrm{C}_G(A)$ de A dans G. Ainsi, $\mathrm{C}_G(A)$ contient P (car $A \subset \mathrm{Z}(P)$) et tous les ℓ-Sylow de G avec $\ell \neq p$. Il est donc d'ordre n par Lagrange, et on a $\mathrm{C}_G(A) = G$, *i.e.* $A \subset \mathrm{Z}(G)$. □

Donnons deux corollaires historiquement bien antérieurs au théorème précédent.

Corollaire 7.6. (Dickson) *Soit $n \geqslant 1$ un entier. Tout groupe d'ordre n est abélien si, et seulement si, l'entier n est nilpotent et sans facteur cube.* [5]

Démonstration — Supposons que tout groupe d'ordre n est abélien. Supposons $n = p^3 m$ avec p premier. Alors $\mathrm{U}_3(\mathbb{Z}/p\mathbb{Z}) \times \mathbb{Z}/m\mathbb{Z}$ est d'ordre n, donc abélien : absurde. Réciproquement, supposons n nilpotent sans facteur cube. Soit G d'ordre n. Alors G est nilpotent par le Théorème 7.1, et donc produit fini de p-groupes par le Théorème 6.8. Mais un p-groupe d'ordre p ou p^2 est abélien, donc G est abélien. □

Corollaire 7.7. (Burnside) *Soit $n \geqslant 1$ un entier. Il y a équivalence entre :*

(i) Tout groupe d'ordre n est cyclique,

(ii) l'entier n est nilpotent sans facteur carré,

(iii) n est premier à $\varphi(n)$.

5. Autrement dit, si p divise n alors p^3 ne divise pas n.

Démonstration — Supposons que tout groupe d'ordre n est cyclique. Supposons $n = p^2 m$ avec p premier. Alors $(\mathbb{Z}/p\mathbb{Z})^2 \times \mathbb{Z}/m\mathbb{Z}$ est d'ordre n, donc cyclique : absurde car il est annulé par $pm < n$. On a montré (i) $\Longrightarrow$ (ii). Réciproquement, supposons n nilpotent sans facteur carré. On a donc $n = p_1 \dots p_r$ avec les p_i distincts. Soit G d'ordre n. Alors G est abélien par le Corollaire 7.6. Si $x_i \in G$ est d'ordre p_i, alors $x_1 \dots x_r$ est donc d'ordre $p_1 \dots p_r = n$ (Cauchy), et G est cyclique. On a montré (ii) $\Longrightarrow$ (i). L'équivalence entre (ii) et (iii) vient de la formule $\varphi(\prod_{i=1}^r p_i^{m_i}) = \prod_{i=1}^r (p_i - 1) p_i^{m_i - 1}$, où les p_i sont des premiers distincts. □

8. Complément III : Générateurs et automorphismes d'un p-groupe

Dans ce complément, on se propose détudier, suivant Burnside et P. Hall, les systèmes de générateurs et le groupe d'automorphisme d'un p-groupe. On fixe donc p premier. On a déjà dit que les systèmes de générateurs du groupe $V = (\mathbb{Z}/p\mathbb{Z})^n$ coïncident avec ceux de l'espace vectoriel $V^\sharp$ sur $\mathbb{Z}/p\mathbb{Z}$, et on a aussi déjà vu et utilisé $\mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^n) \simeq \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$. Commençons par étudier les systèmes minimaux de générateurs d'un p-groupe général, suivant Frattini et Burnside.

Définition 8.1. *Le sous-groupe de Frattini d'un groupe fini G est l'intersection des sous-groupes maximaux de G. C'est un sous-groupe caractéristique de G noté $\Phi(G)$, et le quotient $G/\Phi(G)$ s'appelle aussi quotient de Frattini de G.*

On a donc $\Phi(G) = \cap_M M$ où M parcourt les sous-groupes maximaux de G. Noter que si $\varphi : G \to G$ est un automorphisme, et si $M \subset G$ est maximal, alors le sous-groupe $\varphi(M)$ est encore maximal. Ainsi, φ permute l'ensemble fini des sous-groupes maximaux de G et on a bien $\varphi(\Phi(G)) = \Phi(G)$, comme affirmé ci-dessus.

Exemple 8.2. (i) Les sous-groupes maximaux de $(\mathbb{Z}/p\mathbb{Z})^n$ sont les hyperplans vectoriels du $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel associé. L'intersection de ces hyperplans est nulle : on a donc $\Phi((\mathbb{Z}/p\mathbb{Z})^n) = \{0\}$.

(ii) Les sous-groupes maximaux de H_8 sont $\langle I \rangle, \langle J \rangle$ et $\langle K \rangle$. On a donc $\Phi(\mathrm{H}_8) = \{\pm 1\}$.

(iii) Pour $G = \mathrm{S}_n$, on peut montrer que chacun des sous-groupes $\simeq \mathrm{S}_{n-1}$ obtenus en fixant l'un des points de $\{1, \dots, n\}$ est maximal (observer qu'il agit transitivement sur le complémentaire du point). On a donc encore $\Phi(\mathrm{S}_n) = \{1\}$.

En plus de fournir un sous-groupe distingué naturel, l'intérêt majeur du sous-groupe de Frattini est sa propriété suivante d'être « non-générateur » :

Proposition 8.3. (Frattini) *Soit X un sous-ensemble de G. On a $\langle X \rangle = G$ si, et seulement si, $\langle X, \Phi(G) \rangle = G$. En particulier, X engendre G si, et seulement si, son image dans $G/\Phi(G)$ engendre $G/\Phi(G)$.*

Démonstration — Il est clair que $\langle X \rangle = G$ implique $\langle X, \Phi(G) \rangle = G$. Supposons donc $\langle X, \Phi(G) \rangle = G$. Si $\langle X \rangle$ est un sous-groupe strict de G (un groupe fini), alors il s'inclut dans un sous-groupe maximal M de G. On a donc $\langle X \rangle \subset M$. Mais on a aussi $\Phi(G) \subset M$ par définition. On a donc $\langle X, \Phi(G) \rangle M$: une contradiction. Enfin, si la projection canonique $\langle X \rangle \to G/\Phi(G)$ est surjective, alors on a $\langle X, \Phi(G) \rangle = G$ (pourquoi ?), et donc $\langle X \rangle = G$. □

COROLLAIRE 8.4. *Les groupes G et $G/\Phi(G)$ on même nombre minimal de générateurs.*

Le résultat suivant est appellé *théorème de la base* de Burnside.

THÉORÈME 8.5. (Burnside) *Si P est un p-groupe et si r est le nombre minimal de générateurs de P, alors on a $P/\Phi(P) \simeq (\mathbb{Z}/p\mathbb{Z})^r$.*

DÉMONSTRATION — Le nombre minimal de générateurs de $(\mathbb{Z}/p\mathbb{Z})^r$ est r comme on l'a déjà vu (Proposition 3.7 Chap. 3). D'après le Corollaire 8.4, il suffit donc de démontrer que $P/\Phi(P)$ est abélien p-élémentaire. Mais si M est un sous-groupe maximal de P, on a vu que M est distingué dans P, et que l'on a $P/M \simeq \mathbb{Z}/p\mathbb{Z}$. On en déduit donc $\mathrm{D}(P) \subset M$ (car P/M est abélien) et aussi $g^p \subset M$ pour tout $g \in P$. Comme c'est vrai pour tout M maximal, on a donc $\mathrm{D}(P) \subset \Phi(P)$, *i.e.* $P/\Phi(P)$ est abélien, et $g^p \in \Phi(P)$ pour tout $g \in P$, et donc $P/\Phi(P)$ est p-élémentaire. □

Soit P un p-groupe. Comme $\Phi(P)$ est caractéristique dans P, le groupe P agit naturellement sur $\Phi(P)$ et $P/\Phi(P)$ par automorphismes de groupes, de sorte qu'on a une suite exacte naturelle

$$1 \to \mathrm{I}(P) \to \mathrm{Aut}(P) \to \mathrm{Aut}(P/\Phi(P)),$$

où $\mathrm{I}(P)$ est par définition le sous-groupe de $\mathrm{Aut}(P)$ agissant trivialement sur $P/\Phi(P)$. Attention, nous n'avons pas mis de 1 à droite, de sorte que nous n'affirmons pas du tout que le morphisme de droite est surjectif. Choisissons un isomorphisme $P/\Phi(P) \simeq (\mathbb{Z}/p\mathbb{Z})^r$ avec r le nombre minimal de générateurs de P, on a alors $\mathrm{Aut}(P/\Phi(P)) \simeq \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$, un groupe familier. Il ne reste qu'à étudier $\mathrm{I}(P)$.

PROPOSITION 8.6. (P. Hall) *Pour tout p-groupe P, le groupe $\mathrm{I}(P)$ est un p-groupe.*

DÉMONSTRATION — Si $\mathrm{I}(P)$ n'est pas un p-groupe, alors il possède par Cauchy un sous-groupe $H = \langle\varphi\rangle$ d'ordre premier $\ell \neq p$. Comme H est inclus $\mathrm{I}(P)$, il préserve par définition chaque partie de P de la forme $g\Phi(P)$ avec $g \in P$. Fixons $X = g\Phi(P)$ une telle partie. On a $|X| = |\Phi(P)|$, qui est une puissance de p, et donc un entier premier à ℓ. D'après la Proposition 1.3 appliquée au ℓ-groupe H agissant sur X, on en déduit que H admet un point fixe dans X. On peut donc choisir des représentants $g_1, \ldots, g_s$ des classes à gauche de $\Phi(P)$ dans P qui sont chacun point fixe de φ. Mais $g_1, \ldots, g_s$ engendrent évidemment $P/\Phi(P)$ car on a

$$P/\Phi(P) = \{g_i\Phi(P) \mid i = 1, \ldots, s\},$$

donc on a $P = \langle g_1, \ldots, g_s\rangle$ par la Proposition 8.3. On en déduit $\varphi(g) = g$ pour tout $g \in P$, et $\varphi = \mathrm{id}_P$, une contradiction. □

EXEMPLE 8.7. Si $P = (\mathbb{Z}/p^2\mathbb{Z})^n$, alors on peut montrer $\mathrm{Aut}(P) = \mathrm{GL}_n(\mathbb{Z}/p^2\mathbb{Z})$ et que $\mathrm{I}(P)$ s'identifie aux sous-groupe A de $\mathrm{GL}_n(\mathbb{Z}/p^2\mathbb{Z})$ constitué des matrices de la forme $\mathrm{I}_n + p\mathrm{M}_n(\mathbb{Z}/p^2\mathbb{Z})$. Il y en a bien une puissance de p. En fait, on a $(1+pa)(1+pb) = 1 + p(a+b)$ pour $a, b \in \mathrm{M}_n(\mathbb{Z}/p^2\mathbb{Z})$, de sorte que ce groupe A est isomorphe à $(\mathrm{M}_n(\mathbb{Z}/p\mathbb{Z}), +)$.

9. Exercices

Commençons par quelques exercices sur les p-groupes. Dans tous ces exercices, p est un nombre premier. On montre d'abord que les p-groupes satisfont une forme forte de réciproque au théorème de Lagrange.

EXERCICE 6.1. *Soit P un p-groupe de cardinal p^n avec $n \geqslant 1$.*

(i) Montrer que P a un sous-groupe distingué d'ordre p.

(ii) Montrer que pour tout entier $0 \leqslant i \leqslant n$, il existe un sous-groupe distingué $P_i \subset P$ d'ordre p^i, et que l'on peut même supposer $P_i \subset P_{i+1}$ pour $0 \leqslant i < n$.

D'après le Lemme de Ore (Exercice 4.22 Chap. 4), tout sous-groupe d'indice p d'un p-groupe est distingué. On peut aussi déduire ce fait du résultat plus fort suivant.

EXERCICE 6.2. *(i) Montrer que les sous-groupes maximaux*[6] *d'un p-groupe sont distingués et d'indice p.*

(ii) Donner un exemple de p-groupe ayant un sous-groupe d'indice p^2 non distingué.

EXERCICE 6.3. *Soient k un corps, $n \geqslant 1$ un entier, $\mathrm{T}_n(k)$ le sous-groupe des matrices triangulaires supérieures de $\mathrm{GL}_n(k)$, et $\mathrm{U}_n(k) \subset \mathrm{T}_n(k)$ le sous-groupe des éléments de coefficients diagonaux égaux à 1.*

(i) Montrer que le normalisateur de $\mathrm{U}_n(k)$ dans $\mathrm{GL}_n(k)$ est $\mathrm{T}_n(k)$.

(ii) Montrer que $\mathrm{T}_n(k)$ est égal à son normalisateur dans $\mathrm{GL}_n(k)$.

Dans les trois exercices suivants, on classifie les groupes non abéliens d'ordre p^3.

EXERCICE 6.4. *Soit G un p-groupe non abélien d'ordre p^3 et d'exposant p. On se propose de montrer $G \simeq \mathrm{U}_3(\mathbb{Z}/p\mathbb{Z})$.*

(i) Montrer que G possède un sous-groupe distingué isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

(ii) Montrer que tout élément d'ordre p de $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ est conjugué à

$$t := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

(iii) En déduire $G \simeq (\mathbb{Z}/p\mathbb{Z})^2 \rtimes_\varphi \mathbb{Z}/p\mathbb{Z}$, où φ envoie le générateur $\overline{1}$ de $\mathbb{Z}/p\mathbb{Z}$ sur l'élément t de $\mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^2) = \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

(iv) Conclure.

EXERCICE 6.5. *Soit G un p-groupe non abélien d'ordre p^3 et d'exposant $> p$, avec $p \neq 2$.*

(i) Montrer que G a un sous-groupe distingué H cyclique et d'ordre p^2.

(ii) En déduire qu'il existe $g \in G \smallsetminus H$ tel que $ghg^{-1} = h^{1+p}$ pour tout $h \in H$.

(iii) En déduire qu'il existe $h \in H$ tel que hg est d'ordre p.

6. On rappelle qu'un sous-groupe $M \subset G$ est dit maximal si on a $M \neq G$ et si le seul sous-groupe de G contenant M est G. Il est clair qu'un sous-groupe d'indice premier est maximal, par Lagrange.

(iv) Montrer $G \simeq \mathbb{Z}/p^2\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z}$*, où* φ *envoie le générateur* $\overline{1}$ *de* $\mathbb{Z}/p\mathbb{Z}$ *sur l'automorphisme* $x \mapsto (1+p)x$ *de* $\mathbb{Z}/p^2\mathbb{Z}$*.*

Exercice 6.6. *Déterminer, à isomorphisme près, les groupes d'ordre* p^3*.*

Exercice 6.7. *Soit* G *un groupe fini tel que l'action naturelle de* $\mathrm{Aut}(G)$ *sur* $G \smallsetminus \{1\}$ *est transitive. On se propose de montrer que* G *est abélien* p*-élémentaire.*

(i) Montrer que les éléments non triviaux de G *un même ordre premier, noté* p*.*

(ii) Montrer que G *est un* p*-groupe abélien.*

(iii) Conclure et discuter la réciproque.

On donne maintenant quelques exercices sur les p-Sylow.

Exercice 6.8. *Soient* $n \geqslant 3$ *et* S *un* p*-Sylow de* D_{2n} *avec* $p \mid 2n$*.*

(i) On suppose $p \neq 2$*. Montrer que* S *est cyclique.*

(ii) On suppose $p = 2$*. Montrer* $S \simeq \mathrm{D}_{2^k}$ *pour un certain entier* $k \geqslant 1$*.*

Exercice 6.9. *Soient* $n \geqslant 1$ *un entier et* p *un nombre premier.*

(i) On suppose $n < p^2$*. Exhiber un* p*-Sylow de* S_n*.*

(ii) On suppose $p \nmid n+1$*. Montrer que* S_n *et* S_{n+1} *ont des* p*-Sylow isomorphes.*

Exercice 6.10. *Déterminer, à isomorphisme près, les sous-groupes de Sylow de* S_n *pour* $n \leqslant 8$*.*

Exercice 6.11. *Soient* p *premier et* S *un* p*-Sylow de* S_{p^2}*. Montrer que l'on a*

$$S \simeq (\mathbb{Z}/p\mathbb{Z})^p \rtimes_\varphi \mathbb{Z}/p\mathbb{Z},$$

où φ *envoie le générateur* $\overline{1}$ *de* $\mathbb{Z}/p\mathbb{Z}$ *sur la permutation circulaire* $(x_1, \ldots, x_p) \mapsto (x_2, \ldots, x_p, x_1)$ *de* $(\mathbb{Z}/p\mathbb{Z})^p$*.*

Dans l'exercice qui suit on s'intéresse aux sous-groupes de Sylow de $\mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$ avec q premier. On sait que l'on a $|\mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})| = q(q-1)^2(q+1)$. On a vu aussi qu'un q-Sylow de $\mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$ est $\mathrm{U}_2(q) \simeq \mathbb{Z}/q\mathbb{Z}$.

Exercice 6.12. (Sous-groupes de Sylow de $\mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$) *Soient* p, q *des nombres premiers distincts et* S *un* p*-Sylow de* $\mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$*. On cherche à déterminer la classe d'isomorphisme de* S*. On pose* $\alpha = \mathrm{v}_p(q-1)$ *et* $\beta = \mathrm{v}_p(q+1)$*.*

(i) On suppose $p \mid q-1$ *et* $p > 2$*. Montrer* $S \simeq \mathbb{Z}/p^\alpha\mathbb{Z} \times \mathbb{Z}/p^\alpha\mathbb{Z}$*.*

(ii) On suppose $p \mid q+1$ *et* $p > 2$*. Montrer* $S \simeq \mathbb{Z}/p^\beta\mathbb{Z}$*.*

(iii) On suppose $p = 2$*. Montrer que l'on a soit* $\alpha = 1$ *et* $\mathrm{S} \simeq \mathrm{D}_{2^{\beta+2}}$*, soit* $\beta = 1$ *et* $\mathrm{S} \simeq (\mathbb{Z}/2^\alpha\mathbb{Z})^2 \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$ *avec* $\varphi_{\overline{1}}(x, y) = (y, x)$*.*

Exercice 6.13. *Soit* G *un groupe d'ordre* $p^\alpha n$ *avec* $p \wedge n = 1$ *et* $\alpha \geqslant 1$*.*

(i) Montrer $\binom{|G|}{p^\alpha} \not\equiv 0 \bmod p$*.*

(ii) En considérant l'action de G par translations sur l'ensemble de ses parties à p^α éléments, re-démontrer que G possède un p-Sylow.

Exercice 6.14. *Soient G un groupe fini et p un nombre premier. On s'intéresse à l'ensemble $\mathcal{N}_p(G)$ des p-sous-groupes de G qui sont distingués dans G.*

(i) Monter que $\mathcal{N}_p(G)$ a un plus grand élément pour l'inclusion, noté $\mathrm{O}_p(G)$.

(ii) Montrer que $\mathrm{O}_p(G)$ est l'intersection des p-Sylow de G.

(iii) Soit $G' := G/\mathrm{O}_p(G)$. Montrer $\mathrm{O}_p(G') = 1$.

Exercice 6.15. (Fusion) *Soient G un groupe fini et P un p-Sylow de G.*

(i) Montrer $\mathrm{N}_G(\mathrm{N}_G(P)) = \mathrm{N}_G(P)$.

(ii) Montrer que deux éléments de $\mathrm{C}_G(P)$ conjugués dans G sont conjugués dans $\mathrm{N}_G(P)$ (Burnside).

On donne maintenant quelques applications des théorèmes de Sylow à la classification des groupes de petit cardinal, ou plus généralement ayant peu de diviseurs premiers.

Exercice 6.16. *On se propose de classifier à isomorphisme près les groupes G d'ordre pq avec $p < q$ premiers. Soit G un tel groupe.*

(i) Montrer que G possède un sous-groupe distingué $\simeq \mathbb{Z}/q\mathbb{Z}$.

(ii) On suppose $q \not\equiv 1 \bmod p$. Montrer $G \simeq \mathbb{Z}/pq\mathbb{Z}$.

On suppose désormais $q \equiv 1 \bmod p$. On fixe $\zeta \in (\mathbb{Z}/q\mathbb{Z})^\times$ d'ordre p (justifier) et on pose $G_\zeta = \mathbb{Z}/q\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z}$ où φ envoie le générateur $\overline{1}$ de $\mathbb{Z}/p\mathbb{Z}$ sur l'automorphisme $x \mapsto \zeta x$ de $\mathbb{Z}/q\mathbb{Z}$.

(iii) Montrer que l'on a, exclusivement, soit $G \simeq \mathbb{Z}/pq\mathbb{Z}$, soit $G \simeq G_\zeta$.

Dans l'exercice suivant, on introduit un argument de comptage classique qui, combiné aux théorèmes de Sylow, permet dans des cas favorables de montrer qu'un groupe d'ordre donné n'est pas simple.

Exercice 6.17. *Soit G un groupe d'ordre pm avec p premier et $(p, m) = 1$.*

(i) Montrer que G possède exactement $\mathrm{n}_p(G)(p-1)$ éléments d'ordre p.

(ii) On suppose $\mathrm{n}_p(G) = m$ et que m est une puissance d'un nombre premier q. Montrer $\mathrm{n}_q(G) = 1$.

(iii) (Application 1) *On suppose $|G| = pq^2$, avec q premier $\neq p$. Montrer que G possède un sous-groupe de Sylow distingué.*

(iv) (Application 2) *On suppose $|G| = pqr$, avec p, q, r premiers distincts. Montrer que G possède un sous-groupe de Sylow distingué.*

Exercice 6.18. *Soit G un groupe tel que $|G|$ est produit d'au plus 3 nombres premiers (pas nécessairement distincts). Montrer que :*

(i) soit G est cyclique d'ordre premier, soit G n'est pas simple,

(ii) G est résoluble.

Exercice 6.19. *Soit G un groupe simple fini.*

(i) On suppose que G admet un sous-groupe d'indice $n > 1$. Montrer $|G| \mid n!$.

(ii) Soit p premier divisant $|G|$. Montrer que l'on a soit $G \simeq \mathbb{Z}/p\mathbb{Z}$, soit $|G|$ divise $\mathrm{n}_p(G)!$.

Exercice 6.20. (Groupes simples non abéliens d'ordre $\leqslant 60$) *Soit G un groupe simple non abélien d'ordre $\leqslant 60$. On se propose de montrer $|G| = 60$, et donc $G \simeq \mathrm{A}_5$ par un exemple du cours.*

(i) En utilisant l'Exercice 6.18, montrer $|G| \in \{24, 36, 40, 48, 54, 56, 60\}$.

(ii) En utilisant l'Exercice 6.19, montrer $|G| \in \{56, 60\}$.

(iii) Conclure.

Exercice 6.21. *Montrer qu'à isomorphisme près il existe exactement 3 groupes non abéliens d'ordre 12, à savoir*

$$\mathrm{A}_4,\ \widetilde{\mathrm{D}_6} \text{ et } \mathbb{Z}/2\mathbb{Z} \times \mathrm{S}_3.$$

On pourra utiliser l'Exercice 6.17. Lequel d'entre eux est-il isomorphe à D_{12} ?

L'exercice suivant, plus technique, généralise le précédent et classifie à isomorphisme près les groupes d'ordre pq^2 avec p, q des premiers distincts. Nous renvoyons aussi au problème 2 du partiel 2022-2023 §2 App. B pour le cas particulier $q = 2$.

Exercice 6.22. (Groupes d'ordre pq^2) *Soient p, q deux nombres premiers distincts. On note $\mathrm{a}(p,q)$, $\mathrm{b}(p,q)$ et $\mathrm{c}(p,q)$ les nombres de classes d'isomorphisme de groupes non abéliens d'ordre pq^2 possédant respectivement un p-Sylow distingué, un q-Sylow cyclique distingué et un q-Sylow non cyclique distingué.*

(i) Montrer qu'à isomorphisme près, il y a exactement $\mathrm{a}(p,b) + \mathrm{b}(p,q) + \mathrm{c}(p,q)$ groupes non abéliens d'ordre pq^2.

(ii) Montrer que $\mathrm{a}(p,q)$ vaut 2 pour $p \equiv 1 \bmod q$, et 0 sinon.

(iii) Montrer que $\mathrm{b}(p,q)$ vaut 1 pour $q \equiv 1 \bmod p$, et 0 sinon.

(iv) Montrer que $\mathrm{c}(p,q)$ est le nombre de classes de conjugaison de sous-groupes d'ordre p de $\mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$.

(v) En déduire $\mathrm{c}(p,q)$ pour $p = 2$ ou $q = 2$.

(vi) On suppose $p, q > 2$. Montrer $\mathrm{c}(p,q) = 1$ pour $q \equiv -1 \bmod p$, $\mathrm{c}(p,q) = \frac{p+3}{2}$ pour $q \equiv 1 \bmod p$, et $\mathrm{c}(p,q) = 0$ sinon.

(vii) Expliquer et justifier la Table 1.

Dans l'exercice suivant, on s'intéresse aux classes d'isomorphisme de groupes d'ordre pqr avec p, q, r premiers distincts. D'après l'Exercice 6.17 (iv), un tel groupe possède toujours un sous-groupe de Sylow distingué.

Exercice 6.23. (Groupes d'ordre pqr) *Soient $p < q < r$ des nombres premiers et G un groupe d'ordre pqr.*

(i) On suppose G abélien. Montrer $G \simeq \mathbb{Z}/pqr\mathbb{Z}$.

Sylow distingué	$\mathbb{Z}/p\mathbb{Z}$		$\mathbb{Z}/q^2\mathbb{Z}$	$(\mathbb{Z}/q\mathbb{Z})^2$
Groupe	$\mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/q^2\mathbb{Z}$	$\mathbb{Z}/p\mathbb{Z} \rtimes (\mathbb{Z}/q\mathbb{Z})^2$	$\mathbb{Z}/q^2\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$	$(\mathbb{Z}/q\mathbb{Z})^2 \rtimes H$, avec $H \subset \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$
Condition	$q \mid p-1$	$q \mid p-1$	$p \mid q-1$	$p \mid q^2-1$
$\sharp$	1	1	1	$\frac{p+3}{2}$ si $p, q > 2$, 2 si $p = 2$ et 1 si $q = 2$.

TABLE 1. Les groupes non abéliens d'ordre pq^2 avec $p \neq q$ premiers

(ii) Montrer que tout groupe d'ordre pr ou qr possède un r-Sylow distingué.

(iii) Montrer que G possède un r-Sylow distingué R et un sous-groupe K d'ordre pq tels que $G = RK$.

(iv) Montrer que les classes d'isomorphisme de groupes non abéliens d'ordre pqr sont décrites par la table 2 ci-contre.

$\mathbb{Z}/r\mathbb{Z} \times (\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z})$	$\mathbb{Z}/r\mathbb{Z} \rtimes (\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z})$	$\mathbb{Z}/r\mathbb{Z} \rtimes_p \mathbb{Z}/pq\mathbb{Z}$	$\mathbb{Z}/r\mathbb{Z} \rtimes_q \mathbb{Z}/pq\mathbb{Z}$	$\mathbb{Z}/r\mathbb{Z} \rtimes_{pq} \mathbb{Z}/pq\mathbb{Z}$
$p \mid q-1$	$p \mid q-1$ et $p \mid r-1$	$p \mid r-1$	$q \mid r-1$	$pq \mid r-1$

TABLE 2. Les groupes non abéliens d'ordre pqr avec $p < q < r$ premiers

La Table 3 liste les entiers $n \leqslant 64$ tels qu'il existe un groupe non abélien d'ordre n, et donne le nombre $\mathrm{N}(n)$ de classes d'isomorphismes de tels groupes. On rappelle que les entiers n tels que tout groupe d'ordre n est abélien sont classifiés par le Théorème de Dickson (Corollaire 7.6).

n	6	8	10	12	14	16	18	20	21	22	24	26	27	28	30	32	34	36
$\mathrm{N}(n)$	1	2	1	3	1	9	3	3	1	1	12	1	2	2	3	44	1	10
n	38	39	40	42	44	46	48	50	52	54	55	56	57	58	60	62	63	64
$\mathrm{N}(n)$	1	1	11	5	2	1	47	3	3	12	1	10	1	1	11	1	2	256

TABLE 3. Pour $n \leqslant 64$, le nombre $\mathrm{N}(n)$ de classes d'isomorphisme de groupes non abéliens d'ordre n, quand il est non nul, suivant OEIS A060689.

EXERCICE 6.24. *Vérifier les valeurs $\leqslant 5$ de la Table 3.*

La série d'exercices suivante porte sur la notion de *morphisme de transfert*. On rappelle que l'*abélianisé* d'un groupe G est le groupe abélien quotient $G_{\mathrm{ab}} := G/\mathrm{D}(G)$. Les exercices 6.25, 6.26, 6.28 et 6.29 sont inspirés de la présentation de Serre dans [**SER78**].

EXERCICE 6.25. (Le transfert, suivant Schur) *Soient G un groupe et H un sous-groupe d'indice fini de G. On pose $X = G/H$ et on choisit d'abord, pour tout $x \in X$, un représentant $\widetilde{x}$ de x dans G. Le groupe G agit par translations sur X. Pour $g \in G$, et $x \in X$, on note $h_{g,x}$ l'unique élément de H vérifiant $g\,\widetilde{x} = \widetilde{gx}\,h_{g,x}$, et on pose*

$$\mathrm{Ver}(g) := \prod_{x \in X} h_{g,x} \mod \mathrm{D}(H).$$

Cela définit une application $\mathrm{Ver} : G \to H_{\mathrm{ab}}$ (de l'allemand *Verlagerung*).

(i) Soit $x \mapsto \widehat{x}$ un autre système de représentants de X. Pour $x \in X$ on note h_x l'unique élément de H tel que $\widehat{x} = \widetilde{x}\,h_x$. Pour $g \in G$ et $x \in X$, on définit aussi $h'_{g,x} \in H$ par $g\,\widehat{x} = \widehat{gx}\,h'_{g,x}$. Montrer $h'_{g,x} = h_{gx}^{-1}\,h_{g,x}\,h_x$.

(ii) (suite) En déduire que $\mathrm{Ver}(g)$ *ne dépend pas du choix de $x \mapsto \widetilde{x}$.*

(iii) Montrer que pour $g, g' \in G$ on a $h_{gg',x} = h_{g,g'x}\,h_{g',x}$.

(iv) En déduire que Ver *est un morphisme de groupes $G \to H_{\mathrm{ab}}$.*

On appelle aussi *transfert* le morphisme $G_{\mathrm{ab}} \to H_{\mathrm{ab}}$ qui se déduit du (iv).

EXERCICE 6.26. (Restriction et transfert) *Soient G un groupe, H un sous-groupe d'indice fini,* $\mathrm{Ver} : G \to H_{\mathrm{ab}}$ *le morphisme de transfert, et* $\mathrm{Res} : H_{\mathrm{ab}} \to G_{\mathrm{ab}}$ *le morphisme naturel $h\mathrm{D}(H) \mapsto h\mathrm{D}(G)$.*

(i) Soit $g \in G$. Pour chaque orbite Ω_i de $\langle g \rangle$ agissant sur G/H, on choisit un représentant g_iH de Ω_i et on pose $n_i = |\Omega_i|$. Montrer

$$g_i^{-1} g^{n_i} g_i \in H \ \text{ et } \ \mathrm{Ver}(g) \equiv \prod_i g_i^{-1} g^{n_i} g_i \mod \mathrm{D}(H).$$

(ii) En déduire que $\mathrm{Res} \circ \mathrm{Ver} : G_{\mathrm{ab}} \to G_{\mathrm{ab}}$ *est le morphisme $g \mapsto g^{|G/H|}$.*

(iii) On suppose G abélien. Montrer que l'on a $\mathrm{Ver} : G \to H, g \mapsto g^{|G/H|}$.

EXERCICE 6.27. (Transfert de S_{n+1} à S_n) *Dans cet exercice, on identifie S_n au sous-groupe de S_{n+1} fixant $n+1$. On suppose $n \geqslant 2$.*

(i) Montrer $(\mathrm{S}_n)_{\mathrm{ab}} \simeq \mathbb{Z}/2\mathbb{Z}$.

(ii) Montrer que $\mathrm{Res} : (\mathrm{S}_n)_{\mathrm{ab}} \to (\mathrm{S}_{n+1})_{\mathrm{ab}}$ *est un isomorphisme.*

(iii) Montrer que $\mathrm{Ver} : (\mathrm{S}_{n+1})_{\mathrm{ab}} \to (\mathrm{S}_n)_{\mathrm{ab}}$ *est un isomorphisme si n est pair, le morphisme nul si n est impair.*

EXERCICE 6.28. (Théorème du complément de Burnside) *Soient G un groupe fini et P un p-Sylow de G. On suppose que P est dans le centre de son normalisateur $\mathrm{N}_G(P)$ (en particulier, P est abélien). On va montrer que P admet un complément distingué dans G (Burnside).*

(i) Soient $g \in P$, $h \in G$, ainsi que n le plus petit entier $\geqslant 1$ tel que $h^{-1}g^nh \in P$. Montrer $h^{-1}g^nh = g^n$ (utiliser le (ii) de l'Exercice 6.15).

(ii) En déduire que $\mathrm{Ver} : G \to P$ *vérifie* $\mathrm{Ver}(g) = g^{|G/P|}$ *pour tout $g \in P$.*

(iii) Conclure en considérant $\ker \mathrm{Ver}$.

Exercice 6.29. (Quelques conséquences du théorème de Burnside) *Soient G un groupe fini, p le plus petit facteur premier de $|G|$ et P un p-Sylow de G.*

(i) On suppose P cyclique. Montrer que P admet un complément distingué.

(ii) On suppose $P \simeq (\mathbb{Z}/p\mathbb{Z})^2$. Montrer que soit P admet un complément distingué, soit $p = 2$ et $|G| \equiv 0 \bmod 3$.

(iii) En déduire que si G est simple non abélien on a soit $p^3 \mid |G|$, soit $12 \mid |G|$.

On donne maintenant quelques exercices sur la cohomologie des groupes.

Exercice 6.30. *Soient G un groupe fini et A un G-module. On pose*

$$A^G = \{a \in A \mid g.a = a \ \forall g \in G\},$$

et on considère l'application norme : $\mathrm{N} : A \to A,\ a \mapsto \sum_{g\in G} g.a$.

(i) Montrer que A^G et $N(A)$ sont des sous-groupes de A avec $N(A) \subset A^G$.

On note $\mathrm{Q}(A)$ le groupe abélien quotient $A^G/N(A)$.

(ii) On suppose que G agit trivialement sur A. Déterminer $\mathrm{Q}(A)$.

(iii) On suppose que $G = \mathbb{Z}/p\mathbb{Z}$ agit non trivialement $A = \mathbb{Z}/p^2\mathbb{Z}$. Montrer $\mathrm{Q}(A) = 0$ pour $p > 2$, et $\mathrm{Q}(A) \simeq \mathbb{Z}/2\mathbb{Z}$ pour $p = 2$.

(iv) On suppose que $G = \mathbb{Z}/p\mathbb{Z}$ agit non trivialement sur $A = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Montrer $\mathrm{Q}(A) = 0$ pour $p > 2$, et $\mathrm{Q}(A) \simeq \mathbb{Z}/2\mathbb{Z}$ pour $p = 2$.

Exercice 6.31. *Soient $n \geqslant 1$ un entier, $G = \langle \tau \rangle$ un groupe cyclique d'ordre n et A un G-module. On considère une suite exacte courte (ou extension)*

$$(E) \qquad 1 \to A \xrightarrow{i} \widetilde{G} \xrightarrow{\pi} G \to 1. \tag{56}$$

On pose $X = \pi^{-1}(\{\tau\}) = \{g \in \widetilde{G} \mid \pi(g) = \tau\}$.

(i) Montrer que pour tout $g \in X$ on a $g^n \in i(A^G)$.

(ii) Montrer que l'élément $i^{-1}(g^n) \bmod N(A)$ ne dépend pas du choix de $g \in X$.

(iii) (suite) Montrer cet élément de $\mathrm{Q}(A)$ est nul $\iff$ (E) est scindée.

(iv) En déduire que si $\mathrm{Q}(A) = 0$ alors $\mathrm{H}^2(G, A) = 0$.

(v) (Application 1) Montrer que pour $p > 2$, toute extension de $\mathbb{Z}/p\mathbb{Z}$ par $\mathbb{Z}/p^2\mathbb{Z}$ induisant une action non triviale sur ce dernier est scindée. (Comparer avec l'Exercice 6.4.)

(vi) (Application 2) Soit G un groupe cyclique agissant trivialement sur $\mathbb{C}^\times$. Montrer $\mathrm{H}^2(G, \mathbb{C}^\times) = 0$ (Schur).

(vii) Montrer que pour G cyclique on a un isomorphisme $\mathrm{Q}(A) \xrightarrow{\sim} \mathrm{H}^2(G, A)$.

Exercice 6.32. *Soient G un groupe et A un G-module. On se donne $E_1 = (\widetilde{G}_1, i_1, \pi_1)$ et $E_2 = (\widetilde{G}_2, i_2, \pi_2)$ deux extensions de G par le G-module A et on se propose de définir leur somme de Baer $E_1 + E_2$. On pose*

$$\Gamma = \{(g_1, g_2) \in \widetilde{G}_1 \times \widetilde{G}_2 \mid \pi_1(g_1) = \pi_2(g_2)\} \ \text{ et } \ Z = \{(i_1(a), -i_2(a)) \mid a \in A\}.$$

(i) Vérifier que Γ est un sous-groupe de $\widetilde{G}_1 \times \widetilde{G}_2$ et que $\pi : \Gamma \to G, (g_1, g_2) \mapsto \pi_1(g_1)$ $(= \pi_2(g_1))$ est un morphisme surjectif de noyau $i_1(A) \times i_2(A)$.

(ii) Vérifier que Z est un sous-groupe distingué de Γ inclus dans $\ker \pi$.

(iii) On pose $\widetilde{G} = \Gamma/Z$ et $i : A \to \widetilde{G}, a \mapsto \overline{(i_1(a), 0)}$ $(= \overline{(0, i_2(a))})$. Montrer que

$$1 \longrightarrow A \xrightarrow{i} \widetilde{G} \xrightarrow{\pi} G \longrightarrow 1.$$

est une extension de G par le G-module A. On la note $E_1 + E_2$.

(iv) Soit s_1, s_2 des sections de π_1, π_2. Vérifier que $s(g) = (s_1(g), s_2(g))$ est une section de π et que l'on a $\mathrm{Ob}(s) = \mathrm{Ob}(s_1) + \mathrm{Ob}(s_2)$.

(v) En déduire $[E_1 + E_2] = [E_1] + [E_2]$, puis que si on a E_1, E_2, E_1', E_2' des extensions de G par A, avec[7] *$E_1 \simeq E_1'$ et $E_2 \simeq E_2'$, on a $E_1 + E_2 \simeq E_1' + E_2'$.*

(vi) En déduire que l'application $+$ induit une loi de groupe abélien sur $\mathscr{E}(G, A)$ et que $E \mapsto [E]$ est un isomorphisme entre ce groupe et $\mathrm{H}^2(G, A)$

Exercice 6.33. *Soient G un groupe et G un A-module. Pour tout entier $n \geqslant 0$, on note $\mathrm{C}^n(G, A)$ l'ensemble des fonctions $G^n \to A$ (n-*cochaines de G à valeurs dans A*), avec la convention $\mathrm{C}^0(G, A) = A$. C'est un groupe abélien pour l'addition induite par celle de A. Pour $f \in \mathrm{C}^n(G, A)$ on note $d_n f$ l'élément de $\mathrm{C}^{n+1}(G, A)$ défini par la formule*[8]

$$d_n f(g_1, \dots, g_{n+1}) = g_1.f(g_2, \dots, g_{n+1}) + \sum_{i=1}^{n} (-1)^i f(g_1, \dots, g_{i-1}, g_i g_{i+1}, \dots) + (-1)^{n+1} f(g_1, \dots, g_n).$$

On a un morphisme de groupes abéliens $d_n : \mathrm{C}^n(G, A) \to \mathrm{C}^{n+1}(G, A)$.

(i) Vérifier $\mathrm{Im}\, d_1 = \mathrm{B}^2(G, A)$ et $\ker d_2 = \mathrm{Z}^2(G, A)$.

(ii) Montrer $d_{n+1} \circ d_n = 0$ pour tout $n \geqslant 0$.

*On pose $\mathrm{B}^n(G, A) = \mathrm{Im}\, d_{n-1}$ (n-*cobords de G à valeurs dans A*), avec la convention $d_{-1} = 0$, et $\mathrm{Z}^n(G, A) = \ker d_n$ (n-*cocycles de G à valeurs dans A*). On a donc $\mathrm{B}^n(G, A) \subset \mathrm{Z}^n(G, A)$, et il y a un sens à poser, pour $n \geqslant 0$,*

$$\mathrm{H}^n(G, A) = \mathrm{Z}^n(G, A)/\mathrm{B}^n(G, A)$$

($n$ème groupe de cohomologie de G à valeurs dans A*).*

(iii) Montrer $\mathrm{H}^0(G, A) = A^G$.

(iv) On suppose le G-module A trivial. Montrer $\mathrm{B}^1(G, A) = 0$ et $\mathrm{H}^1(G, A) = \mathrm{Z}^1(G, A) = \mathrm{Hom}(G, A)$.

Exercice 6.34. (Généralisation du théorème de Schur-Zassenhaus). *Soient G un groupe et A un G-module, avec G et A finis d'ordres premiers entre eux. Montrer*

$$\mathrm{H}^n(G, A) = 0, \quad \forall\, n \geqslant 1.$$

Exercice 6.35. *Soient G un groupe et A un G-module. On suppose donnée une extension* scindée *$(\widetilde{G}, i, \pi)$ de G par A. On s'intéresse à l'ensemble $\mathscr{K}$ de tous les compléments de $i(A)$ dans $\widetilde{G}$, et on note $\mathscr{S}$ l'ensemble des sections de groupes de π.*

(i) Rappeler pourquoi $\mathscr{S} \to \mathscr{K}, s \mapsto s(G)$, est bijective.

(ii) Supposons $K, K' \in \mathscr{K}$. Montrer que K et K' sont conjugués dans $\widetilde{G}$ si, et seulement si, il existe $a \in A$ tel que $K' = i(a) K i(a)^{-1}$.

7. Au sens des isomorphismes d'extensions !

8. Pour d_0 il faut comprendre $(d_0 a)g = g.a - a$.

(iii) Fixons $s \in \mathcal{S}$. Vérifier que toute section de π est de la forme $s_\epsilon(g) = i(\epsilon(g))s(g)$ avec $\epsilon : G \to A$, et que l'on a $s_\epsilon \in \mathcal{S} \iff \epsilon \in \mathrm{Z}^1(G, A)$.

(iv) (suite) Supposons ϵ et $\epsilon' \in \mathrm{Z}^1(G, A)$. Montrer que les compléments $s_\epsilon(G)$ et $s_{\epsilon'}(G)$ de $i(A)$ dans $\widetilde{G}$ sont conjugués si, et seulement si, on a

$$\epsilon \equiv \epsilon' \bmod \mathrm{B}^1(G, A).$$

(v) En déduire que l'ensemble des classes de conjugaison de compléments de $i(A)$ dans $\widetilde{G}$ est en bijection avec $\mathrm{H}^1(G, A)$.

(vi) (Application) Montrer que si $\mathrm{H}^1(G, A) = 0$ alors les compléments de $i(A)$ dans $\widetilde{G}$ sont conjugués.

Exercice 6.36. (Un supplément à Schur-Zassenhaus) *Soit G un groupe fini d'ordre mn avec $m \wedge n = 1$ et possédant un sous-groupe distingué* résoluble *H d'ordre m. Montrer que tous les compléments de H dans G sont conjugués dans G. On pourra d'abord traiter le cas H abélien en utilisant les exercices précédents.*

Chapitre 7

Arithmétique des anneaux

Le but de ce chapitre est d'introduire l'*arithmétique des anneaux* généraux, en l'illustrant principalement sur les anneaux A de la forme $\mathbb{Z}[\sqrt{d}]$. Il s'agit d'étudier la relation de divisibilité, et de comprendre quelles propriétés arithmétiques de l'anneau $\mathbb{Z}$ des entiers, ou de l'anneau des polynômes $k[X]$ avec un corps, persistent en général. Par exemple, est-ce que tout élément de A s'écrit de manière unique comme produit d'éléments premiers/irréductibles ? (*théorème fondamental de l'arithmétique*). On dit que A est *factoriel* si cette propriété est vraie. Bien sûr, il nous faudra d'abord préciser ces notions (divisibilité, irréductibilité, relation d'association, etc...).

C'est Gauss qui le premier a rigoureusement démontré que l'anneau $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$ (*entiers de Gauss*) est factoriel, et qui l'a appliqué à l'étude des sommes de deux carrés dans $\mathbb{Z}$ (méthode de l'*arithmétique transcendante*). Comme nous le verrons, cela permet non seulement de redémontrer que tout premier $\equiv 1 \bmod 4$ est somme de deux carrés, mais aussi de voir (de manière limpide !) qu'il l'est d'une unique manière. C'est aussi la propriété de factorialité qui rend de grands services dans l'étude des équations diophantiennes (comme l'équation de Fermat $x^n + y^n = z^n$). Nous détaillerons l'exemple plus simple mais historiquement important de l'équation $y^2 = x^3 - 2$.

Une notion clé est celle d'*idéal* d'un anneau. Elle généralise celle d'élément (Kummer parle d'élément "idéal"), ces derniers correspondants alors aux idéaux *principaux*. L'analogue de la divisibilité pour les idéaux est simplement la *contenance* $\supset$ ("contenir c'est diviser"). De ce point de vue, les idéaux se comportent mieux que les éléments ! Par exemple pgcd et ppcm existent toujours (sommes et intersections), et certaines questions de base se reformulent alors en terme de principalité de certains idéaux. Les anneaux les plus simples de ce point de vue sont ceux, dit *principaux*, dans lesquels tout idéal est principal. On démontre qu'ils sont factoriels. De plus, les anneaux *euclidiens*, dans lesquels une variante de la division euclidienne existe, sont automatiquement principaux. On a donc la hierarchie

$$\text{euclidien} \implies \text{principal} \implies \text{factoriel}.$$

Nous verrons que ces trois classes d'anneaux sont distinctes.

Une étude plus poussée des anneaux $\mathbb{Z}[\sqrt{d}]$, par exemple des substituts à la non factorialité, dépasse le cadre ce cours (*théorie algébrique des nombres*). Les concepts de ce chapitre s'appliquent aussi avec intérêt à d'autres types d'anneaux, par exemple à $\mathbb{C}[x_1, \ldots, x_n]$ et à ses quotients par un idéal I. Ils sont alors souvent un lien avec les propriétés géométriques de la sous-variété *algébrique* de $\mathbb{C}^n$ définie par l'annulation des éléments de I. Nous n'aborderons pas non plus ces aspects, qui appartiennent plus à un second cours d'algèbre (*géométrie algébrique*).

Références : On pourra consulter le chapitre 4 du livre de Stewart & Tall, le chapitre 1 du livre de Samuel, le chapitre du *Cours d'algèbre* de Perrin concernant l'arithmétique des anneaux, ou le cours de votre serviteur à l'École Polytechnique Théorie algébrique des nombres.

1. Les anneaux $\mathbb{Z}[\sqrt{d}]$

Un exemple historiquement important d'anneaux dont l'arithmétique est intéressante est celui des anneaux d'*entiers algébriques*. Nous nous contenterons ici de considérer le cas des entiers *quadratiques*. Fixons donc $d \in \mathbb{Z}$ *non carré*, ainsi qu'une racine carrée $\sqrt{d} \in \mathbb{C}$ de d. Son choix aura peu d'importance, mais pour fixer les idées on suppose $\sqrt{d} > 0$ pour $d > 0$ (cas dit *réel*), et $\sqrt{d}$ de partie imaginaire > 0 pour $d < 0$ (cas dit *imaginaire*). On considère les sous-groupes additifs de $\mathbb{C}$

$$\mathbb{Z}[\sqrt{d}] \subset \mathbb{Q}[\sqrt{d}] \subset \mathbb{C},$$

avec $\mathbb{Z}[\sqrt{d}] := \mathbb{Z} + \mathbb{Z}\sqrt{d}$ et $\mathbb{Q}[\sqrt{d}] := \mathbb{Q} + \mathbb{Q}\sqrt{d}$. Ces deux sous-groupes contiennent 1 et sont des sous-anneaux de $\mathbb{C}$ car on a la formule :

$$(x + y\sqrt{d})(x' + y'\sqrt{d}) \;=\; (xx' + dyy') \;+\; (xy' + x'y)\sqrt{d}. \tag{57}$$

Remarque 1.1. (i) L'anneau $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$ s'appelle l'anneau des *entiers de Gauss*. Il sera utile pour étudier les sommes de deux carrés dans $\mathbb{Z}$ à cause de la factorisation $a^2 + b^2 = (a + bi)(a - bi)$ dans $\mathbb{Z}[i]$.

(ii) L'anneau $\mathbb{Z}[\sqrt{d}]$ sera par exemple utile pour étudier les solutions d'une équation diophantienne comme $y^2 = x^3 + d$ avec $x, y \in \mathbb{Z}$, à cause de la factorisation $(y - \sqrt{d})(y + \sqrt{d}) = x^3$.

(iii) Pour $d < 0$, on constate que $\mathbb{Z} + \mathbb{Z}\sqrt{d}$ est un réseau de $\mathbb{C}$, alors que pour $d > 0$, c'est un sous-groupe dense de $\mathbb{R}$.

Noter que $\mathbb{Q}[\sqrt{d}]$ est même un sous $\mathbb{Q}$-espace vectoriel de $\mathbb{C}$. La famille $1, \sqrt{d}$ en est une base car d n'est pas un carré dans $\mathbb{Z}$, et donc dans $\mathbb{Q}$. C'est donc aussi une $\mathbb{Z}$-base du groupe additif $\mathbb{Z}[\sqrt{d}]$. Pour $x, y \in \mathbb{Q}$, et $z := x + y\sqrt{d}$, on pose

$$\begin{cases} \overline{z} = x - y\sqrt{d}, & \text{le } \textit{conjugué} \text{ de } z, \\ \mathrm{T}(z) = z + \overline{z} = 2x, & \text{la } \textit{trace} \text{ de } z, \\ \mathrm{N}(z) = z\overline{z} = x^2 - dy^2, & \text{la } \textit{norme de } z. \end{cases} \tag{58}$$

On a donc $z^2 - \mathrm{T}(z)z + \mathrm{N}(z) = 0 = (z - z)(z - \overline{z})$ (*identité de Cayley-Hamilton*).

Lemme 1.2. *(i) $z \mapsto \overline{z}$ est un automorphisme des anneaux $\mathbb{Q}[\sqrt{d}]$ et $\mathbb{Z}[\sqrt{d}]$.*

(ii) $\mathbb{Q}[\sqrt{d}]$ est le corps des fractions de $\mathbb{Z}[\sqrt{d}]$.

(iii) $\mathrm{N} : \mathbb{Q}[\sqrt{d}]^\times \to \mathbb{Q}^\times$ est un morphisme de groupes et on a $\mathrm{N}(\mathbb{Z}[\sqrt{d}]) \subset \mathbb{Z}$.

Démonstration — L'application $z \mapsto \overline{z}$ est manifestement un endomorphisme $\mathbb{Q}$-linéaire de $\mathbb{Q}[\sqrt{d}]$ vérifiant $\overline{1} = 1$. De plus, pour $a, b \in \mathbb{Q}[\sqrt{d}]$ la Formule (57) montre $\overline{ab} = \overline{a}\overline{b}$, puis le (i). Pour $b \neq 0$, on a $\mathrm{N}(b) \in \mathbb{Q}^\times$ puis $a/b = ab/\mathrm{N}(b) \in \mathbb{Q}[\sqrt{d}]$, ce qui montre le (ii). Le (i) montre aussi $\mathrm{N}(ab) = ab\overline{ab} = ab\overline{a}\overline{b} = \mathrm{N}(a)\mathrm{N}(b)$, puis le (iii). $\square$

Remarque 1.3. Pour $d < 0$, $\overline{z}$ n'est rien d'autre que le conjugué complexe de z, et $\mathrm{N}(z) = |z|^2$ est le carré de la norme $|.|$ usuelle sur $\mathbb{C}$. En particulier, on a $\mathrm{N}(z) \geqslant 0$ pour tout z.

Terminons ce paragraphe en examinant le groupe des inversibles de $\mathbb{Z}[\sqrt{d}]$.

Lemme 1.4. *On a* $\mathbb{Z}[\sqrt{d}]^\times = \{z \in \mathbb{Z}[\sqrt{d}] \mid \mathrm{N}(z) = \pm 1\}$.

Démonstration — En effet, si $ab = 1$ dans $\mathbb{Z}[\sqrt{d}]$ on a $\mathrm{N}(a)\mathrm{N}(b) = \mathrm{N}(1) = 1$, puis $\mathrm{N}(a), \mathrm{N}(b) \in \mathbb{Z}^\times = \{\pm 1\}$. Réciproquement, si on a $\mathrm{N}(a) = \epsilon$ avec $a \in \mathbb{Z}[\sqrt{d}]$ et $\epsilon = \pm 1$, on a $a\overline{a} = \epsilon$ avec $\overline{a} \in \mathbb{Z}[\sqrt{d}]$, et donc $\epsilon\overline{a} = a^{-1} \in \mathbb{Z}[\sqrt{d}]$. □

Dans le cas $d < 0$, l'équation $x^2 - dy^2 = \pm 1$, avec $x, y \in \mathbb{Z}$, est triviale à résoudre.

Corollaire 1.5. *On a* $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ *et* $\mathbb{Z}[\sqrt{d}]^\times = \{\pm 1\}$ *pour* $d < -1$.

La situation est assez différente pour $d > 0$. Dans ce cas, l'équation $x^2 - dy^2 = 1$ est appelée *équation de Pell-Fermat*, et a une très riche histoire. On vérifie facilement sur des exemples qu'elle a toujours des solutions (x, y) avec $y \neq 0$. Par exemple on a $3^2 - 2 \cdot 2^2 = 1$ pour $d = 2$. Nous renvoyons à l'Exercice 7.7 pour une démonstration de cette propriété en général (Lagrange). On en déduit le résultat suivant :

Proposition 1.6. *Soit $d > 0$ non carré. Alors tout élément > 1 de $\mathbb{Z}[\sqrt{d}]^\times$ est de la forme $x + y\sqrt{d}$ avec $x, y \in \mathbb{Z}_{\geqslant 1}$. De plus, il existe un unique plus petit tel élément η_d, appelé unité fondamentale de $\mathbb{Z}[\sqrt{d}]$, et on a $\mathbb{Z}[\sqrt{d}]^\times = \langle -1, \eta_d \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.*

Par exemple, prenons $d = 2$. On a $1+\sqrt{2} > 1$ et $\mathrm{N}(1+\sqrt{2}) = -1$ donc $\eta_2 = 1+\sqrt{2}$. On en déduit par exemple $\eta_2^6 = (1 + \sqrt{2})^6 = 99 + 70\sqrt{2}$ et donc $99^2 - 2 \cdot 70^2 = 1$.

Démonstration — Soit $u = x + y\sqrt{d}$ dans $\mathbb{Z}[\sqrt{d}]^\times \smallsetminus \{\pm 1\}$. Quitte à remplacer u par $-u$, on peut supposer $u > 0$, puis quitte à le remplacer par $1/u$ on peut supposer $u > 1$. Mais l'ensemble de 4 inversibles $\{u, u^{-1}, -u, -u^{-1}\} = \{\pm u, \pm \overline{u}\} = \{\pm x \pm y\sqrt{d}\}$ rencontre chacun des intervalles

$$]-\infty, -1[,\ ]-1, 0[,\ ]0, 1[\text{ et }]1, \infty[$$

en un point. Le plus grand des 4 est u, ce qui montre $x, y > 0$, et la première assertion. On en déduit que le sous-groupe des inversibles > 0 de $\mathbb{Z}[\sqrt{d}]$ est discret dans le groupe multiplicatif $\mathbb{R}_{>0}^\times \overset{\log}{\simeq} \mathbb{R}$. Comme il est non trivial par l'Exercice 7.7, la Proposition 7.3 Chap. 2 montre qu'il est monogène engendré par η_d. □

d	2	3	5	6	7	8	10	11	12
η_d	$1+\sqrt{2}$	$2+\sqrt{3}$	$2+\sqrt{5}$	$5+2\sqrt{6}$	$8+3\sqrt{7}$	$3+\sqrt{8}$	$3+\sqrt{10}$	$10+3\sqrt{11}$	$7+2\sqrt{12}$

Table 1. L'unité fondamentale de $\mathbb{Z}[\sqrt{d}]$ pour $0 < d \leqslant 12$.

2. Vocabulaire de la divisibilité

Dans tout ce paragraphe, A désigne un anneau *commutatif*. On supposera aussi que A est *intègre*, ce qui signifie qu'il est non nul, et que pour tout $a, b \in A$, $ab = 0$ entraîne $a = 0$ ou $b = 0$. Tout sous-anneau d'un corps est intègre.

DÉFINITION 2.1. *Si $a, b \in A$, on dit que « a divise b », ou que « b est multiple de a », et on écrit $a|b$, s'il existe $c \in A$ tel que $b = ac$.*

L'intégrité de A assure que le c ci-dessus est unique si $a \neq 0$. Pour tout $a, b, c \in A$, alors $a|a$, et si $a|b$ et $b|c$ alors $a|c$. Autrement dit, la relation de divisibilité est une relation de *préordre* sur A au sens de Bourbaki. Son étude est souvent appelée *arithmétique de A*. Par exemple, l'arithmétique d'un corps est inintéressante car deux éléments non nuls se divisent toujours l'un l'autre.

DÉFINITION 2.2. (Relation d'association) *On dit que $a, b \in A$ sont associés si on a $b|a$ et $a|b$. C'est une relation d'équivalence sur A que l'on notera $a \sim b$.*

Les diviseurs de 1 sont exactement les éléments inversibles de A. C'est pourquoi on les appelle aussi *unités* de A. Ils divisent tout élément de A.

LEMME 2.3. *Pour $a, b \in A$, on a $b|a$ et $a|b \iff$ il existe $u \in A^\times$ avec $a = bu$.*

DÉMONSTRATION — Si on a $a = bu$ avec $u \in A^\times$, on a aussi $b = au^{-1}$ puis $a \mid b$ et $b \mid a$. Réciproquement, supposons $a|b$ et $b|a$. Si a est nul alors b est nul car $a|b$, et donc $a = b$. Sinon, on écrit $a = bc$ et $b = ad$ pour certains $c, d \in A$ puis $a = abd$, $a(1 - bd) = 0$ et $1 = bd$ par intégrité de A, *i.e.* $c, d \in A^\times$. □

Ces considérations montrent qu'il est important en pratique de savoir déterminer le groupe $A^\times$ des unités de A. Le cas de $\mathbb{Z}[\sqrt{d}]$ a déjà été traité.

EXEMPLE 2.4. *Si A est intègre, alors $A[X]$ l'est encore (on a $\deg PQ = \deg P + \deg Q$ pour $P, Q \neq 0$). On a aussi $A[X]^\times = A^\times$ (polynomes constants inversibles).*

Introduisons maintenant une première notion d'*irréductibilité*.

DÉFINITION 2.5. *Un élément non nul $\pi \in A$ est dit irréductible si ce n'est pas une unité, et si pour tout $a, b \in A$, la relation $\pi = ab$ implique $a \in A^\times$ ou $b \in A^\times$.*

Autrement dit, aux unités près un irréductible a exactement deux diviseurs : à savoir 1 et lui-même. Si π est irréductible, il en va de même de tout élément associé.

EXEMPLE 2.6. *Les irréductibles de $\mathbb{Z}$ sont les $\pm p$ avec p un nombre premier. Pour k un corps, les irréductibles de $k[X]$ (voire même de $k[X_1, \ldots, X_n]$) sont les polynômes irréductibles au sens usuel.*

Donnons quelques exemples et contre-exemples dans $\mathbb{Z}[\sqrt{d}]$. La multiplicativité de la norme N rendra bien des services pour étudier l'arithmétique de $\mathbb{Z}[\sqrt{d}]$, notamment car si a divise b dans $\mathbb{Z}[\sqrt{d}]$, alors $\mathrm{N}(a)$ divise $\mathrm{N}(b)$ dans $\mathbb{Z}$. (Mais la réciproque est très fausse !)

EXEMPLE 2.7. (i) Soit $\pi \in \mathbb{Z}[\sqrt{d}]$ avec $p = \mathrm{N}(\pi)$ irréductible dans $\mathbb{Z}$ (donc $\pm p$ premier). Alors π est irréductible dans $\mathbb{Z}[\sqrt{d}]$. Par exemple, $1 + 2i$ est

irréductible dans $\mathbb{Z}[i]$. En effet, si on a $\pi = ab$ on en déduit $\mathrm{N}(a) = \pm 1$ ou $\mathrm{N}(b) = \pm 1$ donc a ou $b \in \mathbb{Z}[\sqrt{d}]^\times$ (Lemme 1.4). La réciproque est fausse comme le montre l'exemple suivant.

(ii) Considérons $\mathbb{Z}[\sqrt{-3}]$ (d'unités ± 1). Comme $x^2 + 3y^2 = 2$ n'a pas de solution $(x, y) \in \mathbb{Z}^2$, il n'y a pas d'élément $a \in \mathbb{Z}[\sqrt{-3}]$ de norme ± 2. On en déduit que les éléments de norme 4 de $\mathbb{Z}[\sqrt{-3}]$ sont irréductibles : ce sont les 6 éléments $\pm 2, \pm(1 + \sqrt{3})$ et $\pm(1 - \sqrt{3})$.

Une notion concurrente à l'irréductibilité est la suivante.

Définition 2.8. *Un élément non nul $\pi \in A$ est dit premier si ce n'est pas une unité et s'il satisfait à la propriété d'Euclide-Gauss : pour tout $a, b \in A$, on a*

$$\pi \mid ab \implies \pi \mid a \text{ ou } \pi \mid b.$$

Exemple 2.9. (i) Un élément premier est irréductible. En effet, si $\pi = ab$ alors π divise a ou b. Si par exemple $\pi | a$, de sorte que $a = \pi c$ où $c \in A$, alors $\pi = \pi cb$ puis $1 = cb$, et donc b est une unité.

(ii) La réciproque est vraie dans $\mathbb{Z}$ ou $k[X]$ avec k un corps, mais pas en général. En effet, l'élément 2 est irréductible dans $\mathbb{Z}[\sqrt{-3}]$ comme on l'a vu. Il ne divise pas $1 \pm \sqrt{-3}$, car sinon on aurait $1 \pm \sqrt{-3} = 2(x + y\sqrt{-3}) = 2x + 2y\sqrt{-3}$ et donc $2x = \pm 1$ et $2y = \pm 1$ avec $x, y \in \mathbb{Z}$: absurde. Pourtant il divise $2.2 = (1 - \sqrt{-3})(1 + \sqrt{-3})$: il n'est pas premier.

3. Anneaux factoriels

On note toujours A un anneau commutatif intègre. On convient qu'un produit indexé par l'ensemble vide dans un anneau vaut 1, et aussi que l'on a $a^0 = 1$ pour tout $a \in A$. Il sera commode pour la suite de choisir un ensemble (arbitraire) $\mathscr{P}$ de représentants des éléments irréductibles pour la relation d'association. Dans le cas $A = \mathbb{Z}$ (d'unités ± 1), le choix classique est de prendre l'ensemble des nombres premiers positifs ! De même un choix standard dans le cas $A = k[X]$ est celui des polynômes irréductibles *unitaires*. On note $\mathbb{N}^{(\mathscr{P})}$ l'ensemble des familles $(n_\pi)_{\pi \in \mathscr{P}}$ telles que $\{\pi | \, n_\pi \neq 0\}$ est fini. La définition suivante, abstraction du *théorème fondamental de l'arithmétique*, est importante.

Définition 3.1. *(i) On dit que A a la* propriété de factorisation (notée (PF)) *si tout élément de $A \smallsetminus \{0\}$ est un produit fini (éventuellement vide) d'éléments irréductibles et d'une unité.*

(ii) On dit que A est factoriel *si pour tout $a \in A \smallsetminus \{0\}$ il existe un unique $u \in A^\times$ et une unique élément $(v_\pi(a)) \in \mathbb{N}^{(\mathscr{P})}$ vérifiant $a = u \prod_{\pi \in P} \pi^{v_\pi(a)}$.*

Le sens donné au produit ci-dessus est bien entendu le produit fini de u et des $\pi^{v_\pi(a)}$ avec $v_\pi(a) \neq 0$, mais il est commode de le noter ainsi. Il est facile de voir que la propriété d'être factoriel ne dépend pas du choix de l'ensemble de représentants $\mathscr{P}$ des irréductibles de A.

Exemple 3.2. (i) *Les anneaux $\mathbb{Z}$ et $k[X]$ avec k un corps sont factoriels*, nous le redémontrerons plus loin.

(ii) Les anneaux $\mathbb{Z}[\sqrt{d}]$ sont (PF). En effet, vérifions par récurrence sur l'entier $|\mathrm{N}(a)| \geqslant 1$ que tout $a \in A$ non nul est produit fini d'irréductibles et d'une unité. Si a est une unité, *i.e.* $|\mathrm{N}(a)| = 1$ par le Lemme 1.4, ou irréductible, il y a rien à démontrer. Sinon, on a $a = bc$ avec $1 < |\mathrm{N}(b)|, |\mathrm{N}(c)| < |\mathrm{N}(a)|$ toujours par le Lemme 1.4. Ainsi, b et c sont produits finis d'irréductibles, ainsi donc que $a = bc$.

(iii) *L'anneau* $\mathbb{Z}[\sqrt{-3}]$ *n'est pas factoriel* : on a $2.2 = (1-\sqrt{-3})(1+\sqrt{-3})$ alors que $2, 1+\sqrt{-3}$ et $1-\sqrt{-3}$ sont irréductibles deux à deux non associés (Exemple 2.7).

(iv) *L'anneau* $\mathrm{H}(\mathbb{C})$ *des séries entières convergentes sur* $\mathbb{C}$ *est intègre*, par le principe des zéros isolés. On peut montrer que *les unités de* $\mathrm{H}(\mathbb{C})$ *sont exactement les fonctions qui ne s'annulent pas sur* $\mathbb{C}$*, et ses irréductibles sont les associés des* $z-a$ *avec* $a \in \mathbb{C}$. Mais certains éléments de $\mathrm{H}(\mathbb{C})$ ont une infinité de 0, comme par exemple $\sin(\pi z)$, donc *l'anneau* $\mathrm{H}(\mathbb{C})$ *ne vérifie pas* (PF) (voir l'Exercice 7.21).

L'arithmétique des anneaux factoriels est particulièrement simple. En effet, supposons A factoriel. Pour $a \in A$ non nul et $\pi \in \mathscr{P}$, l'entier $v_\pi(a) \in \mathbb{N}$ est appelée *valuation de* a *en* π, ou *valuation* π-adique de a. La factorialité impose que pour tout $a, b \in A\backslash\{0\}$ et tout $\pi \in \mathscr{P}$, on a $v_\pi(ab) = v_\pi(a) + v_\pi(b)$. En particulier, on a

$$a \mid b \Leftrightarrow \quad \forall \pi \in \mathscr{P},\ v_\pi(a) \leqslant v_\pi(b). \tag{59}$$

Proposition 3.3. (Caractérisation d'Euclide-Gauss des anneaux factoriels). *Supposons que* A *satisfait* (PF). *Alors* A *est factoriel si, et seulement si, tout irréductible de* A *est premier.*

Démonstration — Supposons A factoriel. Soit π un irréductible de A, que l'on peut supposer dans $\mathscr{P}$. Si π divise ab, alors $1 \leqslant v_\pi(ab) = v_\pi(a) + v_\pi(b)$ et donc soit $v_\pi(a) \geqslant 1$ soit $v_\pi(b) \geqslant 1$. Ainsi, π est premier.

Supposons réciproquement que tout irréductible de A est premier et montrons A factoriel. Supposons que l'on ait $u, v \in A^\times$ et $(m_\pi), (n_\pi) \in \mathbb{N}^{(\mathscr{P})}$ avec

$$u \prod_{\pi \in \mathscr{P}} \pi^{m_\pi} = v \prod_{\pi \in \mathscr{P}} \pi^{n_\pi}, \tag{60}$$

Montrons $u = v$ et $(m_\pi) = (n_\pi)$ par récurrence sur $\sum_\pi (m_\pi + n_\pi)$. C'est clair si cette somme est nulle. Supposons par exemple $m_\pi \geqslant 1$. Alors π divise le membre de gauche de (60), et donc celui de droite. De plus, π ne divise pas d'unité car on a $\pi \notin A^\times$. Comme π est premier, il divise donc $\pi'^{n_{\pi'}}$ pour un certain $\pi' \in \mathscr{P}$ avec $n_{\pi'} \geqslant 1$, et en particulier π divise π'. Comme π' est irréductible cela implique $\pi \sim \pi'$ puis $\pi' = \pi$ par définition de $\mathscr{P}$, et donc $n_\pi \geqslant 1$. Par intégrité, on peut donc diviser par π des deux côtés l'Équation (60), et on conclut par récurrence. □

Remarque 3.4. *À l'aide de la notion de contenu d'un polynôme, on peut montrer que si* A *est factoriel, alors* $A[X]$ *est factoriel (un argument connu de Gauss) : voir l'Exercice 7.20.*

Terminons par une discussion de la notion de pgcd et ppcm.

Définition 3.5. *Soient $a_1, \dots, a_n \in A$, on appelle plus grand diviseur commun (ou pgcd) des a_i un élément $d \in A$ vérifiant les deux propriétés suivantes :*

(i) d divise a_i pour tout i,

(ii) pour tout $b \in A$, si b divise a_i pour tout i alors b divise d.

En particulier, $a_1, \dots, a_n$ sont dits premiers entre eux si 1 en est un pgcd.

Autrement dit, c'est "le" plus grand élément de l'ensemble des éléments inférieurs aux a_i pour la relation de divisibilité. Observons que s'ils existent, *deux pgcd se divisent entre eux, et sont donc associés.* En revanche, les pgcds n'existent pas toujours, même si les a_i ne sont pas tous nuls (voir les exercices). On définit de même la notion de *plus petit multiple commun* (ou ppcm) des a_i comme étant un plus petit élément de l'ensemble des éléments plus grands que les a_i pour la relation de divisibilité (les même remarques s'appliquent).

Lemme 3.6. *Pgcd et ppcm existent dans un anneau factoriel.*

Démonstration — En effet, un pgcd de $a_1, \dots, a_n \in A \smallsetminus \{0\}$ est $\prod_{\pi \in \mathscr{P}} \pi^{m_\pi}$ avec $m_\pi = \mathrm{Min}\{\mathrm{v}_\pi(a_1), \dots, \mathrm{v}_\pi(a_n)\}$. Un ppcm s'obtient de même en remplaçant le Min par un Max. □

4. Idéaux

Dans cette section, A désigne un anneau commutatif[1] quelconque.

Définition 4.1. *Un idéal de A est un sous-groupe additif $I \subset A$ tel que pour tout $a \in A$ et tout $x \in I$ on ait $ax \in I$.*

L'ensemble $aA = \{ax \mid x \in A\}$ des multiples de a dans A est un idéal appelé *idéal principal engendré par $a \in A$*. On note aussi $(a) = aA$. En particulier, *l'idéal nul* $\{0\}$ et *l'idéal total* A sont des idéaux de A. De plus, la divisibilité entre éléments s'exprime simplement en terme des idéaux principaux associés : pour $a, b \in A$ on a

$$bA \subset aA \iff b \in aA \iff a|b$$

La devise à retenir est "contenir c'est diviser". En particulier, on a $aA = A \iff a \in A^\times$, et $aA = bA \iff a \sim b$.

Remarque 4.2. (*Nombres idéaux de Kummer*) La terminologie *idéal*, introduite par Dedekind, est empruntée à celle de *nombres idéaux* utilisée par Kummer dans son étude des anneaux de la forme $\mathbb{Z}[e^{2i\pi/n}]$. Suivant Kummer, on peut penser à un idéal de A comme une partie qui satisfait axiomatiquement tout pour être l'ensemble des multiples de "quelque chose", mais que ce "quelque chose" n'est pas forcément un élément de A. Typiquement, chez Kummer, A est un sous-anneau d'un anneau B, et pour $b \in B$ (le « nombre idéal ») et il considère l'idéal $I = bB \cap A$ de A.

Indiquons quelques constuctions générales d'idéaux :

1. La condition de commutativité de A n'est pas cruciale, mais sans elle il conviendrait de distinguer les notions d'idéal à gauche, idéal à droite, et idéal bilatère. Cette généralité est hors de propos ici, mais d'un grand intérêt dans d'autres situations.

(a) (Sommes) Si $(I_j)_{j\in J}$ est une famille d'idéaux de A (avec J finie ou non), on désigne par $\sum_j I_j$ l'ensemble des sommes finies d'éléments de $\bigcup_j I_j$. C'est le plus petit idéal de A contenant les I_j. Pour $a_1, \ldots, a_n \in A$, on pose aussi

$$(a_1, \ldots, a_n) = a_1A + a_2A + \cdots + a_nA = \{\sum_{i=1}^{n} a_i x_i \mid x_i \in A \ \forall i\}.$$

Un idéal de A de cette forme est dit *de type fini*, ou *finiment engendré*.

(b) (Intersections) De même, si $(I_j)_{j\in J}$ est une famille d'idéaux de A, alors $\cap_j I_j$ est un idéal de A : c'est le plus grand idéal inclus dans tous les I_j.

Les notions de somme et d'intersection sont donc les analogues dans le langage des idéaux des notions respectives de pgcd et ppcm pour les éléments. Elles existent toujours : c'est une première indication du fait que les idéaux se comportent mieux que les éléments.

(c) (Comportement vis-à-vis des morphismes) Soit $f : A \to B$ un morphisme d'anneaux. Alors $\ker f := \{a \in A \mid f(a) = 0\}$ est un idéal de A. Plus généralement, si I est un idéal de B alors $f^{-1}(I)$ est un idéal de A. Enfin, si f est surjective, et si I est un idéal de A, alors $f(I)$ est un idéal de B. À bien des égards, *les idéaux sont aux anneaux ce que les sous-groupes distingués sont aux groupes*. Nous renvoyons au Complément 9 pour une discussion de la notion importante d'*anneau quotient*.

Définition 4.3. *Un anneau est dit* noethérien *si ses idéaux sont de type fini.*

La Proposition suivante n'a pas été traitée en classe, et la Proposition 4.5 a été mentionnée sans démonstration. Les anneaux noethériens seront étudiés plus en détail en cours d'Algèbre 2.

Proposition 4.4. *Soit A un anneau commutatif. Il y a équivalence entre :*

(i) A est noethérien,

(ii) toute suite croissante *$(I_m)_{m\geqslant 1}$ d'idéaux de A, c'est-à-dire avec $I_m \subset I_{m+1}$ pour tout $m \geqslant 1$, est constante à partir d'un certain rang.*

(iii) toute famille non vide d'idéaux de A admet un élément maximal pour l'inclusion.

Démonstration — Pour (i) $\Longrightarrow$ (ii), on constate que $I = \bigcup_{m\geqslant 1} I_m$ est un idéal de A, car $(I_m)_{m\geqslant 1}$ est croissante. Il est donc de la forme $(a_1, \ldots, a_n)$ pour certains éléments $a_i \in A$. Si N est assez grand de sorte que $a_i \in I_N$ pour $i = 1, \ldots, n$, on constate $I_m \subset I \subset I_N$ pour tout $m \geqslant 1$, d'où l'on tire $I_m = I_N$ si $m \geqslant N$.

Le (ii) implique (iii) dans tout ensemble ordonné : s'il n'y a pas d'élément maximal, on fabrique par induction une suite strictement croissante d'éléments.

Montrons enfin que (iii) implique (i). Soit I un idéal de A. Soit $\mathscr{F}$ l'ensemble des idéaux de type fini de A inclus dans I, ordonné par l'inclusion. Il contient $\{0\} = 0A$ donc est non vide. Par le (iii), il admet un élément maximal, disons $J \subset I$. Si $J \neq I$, il existe $x \in I \backslash J$, et on a donc $J \subsetneq J + xA \subset I$, une contradiction car $J + xA$ est de type fini. Cela montre que $I = J$ est de type fini. $\square$

PROPOSITION 4.5. *Si A est intègre noethérien alors A vérifie* (PF).

DÉMONSTRATION — Soit $S \subset A \smallsetminus \{0\}$ l'ensemble des éléments qui sont produits d'unités et d'irréductibles. Si $a \notin S$, alors a n'est pas irréductible, et donc de la forme bc avec b et c non unités. Comme S est stable par produits, soit b soit c n'est pas dans S. Si $S \neq A \smallsetminus \{0\}$, on construit donc récursivement une suite d'éléments non nuls $a_m \in A \smallsetminus S$ pour $m \geqslant 1$ avec a_{m+1} divise a_m et a_m non associé à a_{m+1}. Ainsi, $I_m = (a_m)$ est une suite strictement croissante d'idéaux de A, ce qui est absurde par noethérianité . □

5. Anneaux principaux

DÉFINITION 5.1. *Un anneau principal est un anneau intègre dont tous les idéaux sont principaux.*

Un anneau principal est trivialement noethérien. Dans un anneau principal, on a des relations de Bezout :

PROPOSITION 5.2. (Relations de Bézout) *Soient A un anneau principal et $a, b \in A$. Alors a et b admettent un pgcd d dans A, et il existe $u, v \in A$ tels que $au + bv = d$.*

DÉMONSTRATION — L'idéal $aA + bA$ est principal, donc de la forme dA pour un certain $d \in A$. On a $a, b \in dA$, donc d est un diviseur de a et de b. On a aussi $d \in aA + bA$, donc il existe $u, v \in A$ avec $d = au + bv$, et tout diviseur de a et b divise donc d : c'est un pgcd. □

Le résultat principal de cette section est alors le suivant.

THÉORÈME 5.3. *Un anneau principal est factoriel.*

DÉMONSTRATION — Un anneau principal est clairement noethérien, donc satisfait (PF) par la Proposition 4.5. D'après la Proposition 3.3, il suffit donc de montrer que tout irréductible π de l'anneau principal A, alors π est premier.

Supposons donc que π divise ab avec $a, b \in A$. Soit d un pgcd de π et a. C'est un diviseur de l'irréductible π, donc on a soit $d \sim 1$, soit $d \sim \pi$. Dans le second cas on a $\pi \sim d$ divise a. Dans le premier, on a $1 = \pi u + av$ avec $u, v \in A$, et donc $b = \pi bu + abv$, puis π divise b. □

6. Anneaux euclidiens et exemples

DÉFINITION 6.1. *Un anneau commutatif A est dit euclidien s'il possède une fonction $\varphi : A \backslash \{0\} \to \mathbb{N}$ telle que $\forall a, b \in A \backslash \{0\}$, il existe q et $r \in A$ tels que $a = bq + r$ avec :*

(i) soit $r = 0$,

(ii) soit $r \neq 0$ et $\varphi(r) < \varphi(b)$.

On appelle *stathme euclidien* une telle fonction (du grec ancien $\sigma\tau\alpha\theta\mu\nu$ signifiant « *fil à plomb, règle, mesure* », la terminologie semble due à F. Dress [2]). On parle aussi communément de *fonction euclidienne* ou d'*algorithme euclidien.*

Exemple 6.2. (i) *L'anneau $\mathbb{Z}$ est euclidien pour $\varphi(n) = |n|$.* De même, l'anneau $\mathbb{Z}/N\mathbb{Z}$ est euclidien pour $\varphi(\overline{n}) = n$ pour $n \in \{0, \dots, N-1\}$.

(ii) *Pour k un corps, l'anneau $k[X]$ est euclidien pour* deg.

(iii) Pour k commutatif général, $k[X]$ n'est pas nécessairement euclidien. Néanmoins pour tout $A, B \in k[X]$ avec B *unitaire*, il existe $P, Q \in k[X]$ tels que $A = BQ + R$, avec soit $R = 0$, soit $R \neq 0$ et $\deg R < \deg B$.

Proposition 6.3. *Pour $d = -2, -1, 2$, l'anneau $\mathbb{Z}[\sqrt{d}]$ est euclidien pour* $|\mathrm{N}|$.

Démonstration — Observons qu'il suffit de montrer que pour tout $t \in \mathbb{Q}[\sqrt{d}]$, il existe $q \in \mathbb{Z}[\sqrt{d}]$ avec $|\mathrm{N}(t-q)| < 1$. En effet, si on a $a, b \in \mathbb{Z}[\sqrt{d}]$ avec $a, b \neq 0$, appliquant ceci à $t = a/b \in \mathbb{Q}[\sqrt{d}]$ il existe $q \in \mathbb{Z}[\sqrt{d}]$ avec $|\mathrm{N}(a/b - q)| < 1$. Par multiplicativité de la norme, on a $|\mathrm{N}(a - bq)| < |\mathrm{N}(b)|$ puis $r := a - qb$ convient.

Pour montrer l'observation on écrit $t = x + y\sqrt{d}$ avec $x, y \in \mathbb{Q}$. Il existe $u, v \in \mathbb{Z}$ avec $|u - x| \leqslant 1/2$ et $|v - y| \leqslant 1/2$. Posons $q = u + v\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. On a bien $|\mathrm{N}(t-q)| \leqslant (x-u)^2 + |d|(y-v)^2 \leqslant \frac{1+|d|}{4} < 1$ pour $|d| < 3$. □

Proposition 6.4. *Un anneau intègre euclidien est principal.*

Démonstration — L'idéal nul étant principal, il suffit de voir que tout idéal non nul I de A est principal. Soit φ un stathme euclidien sur A, la partie $\varphi(I \backslash \{0\}) \subset \mathbb{N}$ est non vide, on peut donc trouver un élément $b \in I \backslash \{0\}$ pour lequel $\varphi(b)$ est minimal. Bien entendu, on a $bA \subset I$. Vérifions l'inclusion réciproque. Soit $a \in I$. Il existe $q, r \in A$ tels que $a = bq + r$, avec de plus $\varphi(r) < \varphi(b)$ si r est non nul. Mais $r = a - bq \in I$ car I est un idéal, donc on a $r = 0$ par minimalité de $\varphi(b)$. On a donc $a = bq$ puis $I \subset bA$, et $I = bA$. □

Corollaire 6.5. *Les anneaux $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{-2}]$, ainsi que $k[X]$ quand k est un corps, sont principaux, et donc factoriels.*

Remarque 6.6. *Toujours si k est un corps, l'anneau $k[X, Y]$ n'est pas principal. Par exemple, l'idéal (X, Y) n'est pas principal (pourquoi ?). En revanche, on peut montrer que $k[X_1, \dots, X_n]$ est factoriel pour tout $n \geqslant 1$ (voir l'Exercice 7.20). En particulier, il existe des anneaux factoriels non principaux.*

Terminons par des remarques culturelles sur la famille d'anneaux $\mathbb{Z}[\sqrt{d}]$.

Remarque 6.7. (i) On peut montrer que pour les anneaux $\mathbb{Z}[\sqrt{d}]$, *principal équivaut à factoriel* : voir l'Exercice 7.30.

2. F. Dress, Stathmes euclidiens et séries formelles, Acta Arithmetica (1971).

(ii) Il n'est pas difficile de montrer que l'anneau $\mathbb{Z}[\sqrt{d}]$ n'est jamais principal pour $d < -2$: voir l'Exercice 7.5. En revanche, c'est un problème ouvert de déterminer les entiers $d > 0$ tels que $\mathbb{Z}[\sqrt{d}]$ est principal. Les premiers sont $d = 2, 3, 6, 7, 11, 14, 19, 22, 23, 31$: voir cette suite. On ne sait même pas s'il y en a un nombre fini !

(iii) On conjecture qu'il y a une infinité d'entiers $d > 0$ tels que $\mathbb{Z}[\sqrt{d}]$ est euclidien. On sait que $\mathbb{Z}[\sqrt{d}]$ est euclidien pour $|\mathrm{N}|$ si, et seulement si, $d = -2, -1, 2, 3, 6, 7, 11, 19$ (Chatland-Davenport, Inkeri). Il a été démontré seulement en 2004 par Harper que $\mathbb{Z}[\sqrt{14}]$ est euclidien (mais pas pour $|\mathrm{N}|$, donc).

7. L'anneau $\mathbb{Z}[i]$ et sommes de deux carrés

On a vu que l'anneau $\mathbb{Z}[i]$ est euclidien, donc principal, donc factoriel. Ainsi, tout entier de Gauss non nul est produit de manière unique d'une des 4 unités $\pm 1, \pm i$ et d'irréductibles de $\mathbb{Z}[i]$ (disons appartenant à un système de représentants fixé). Pour utiliser ce résultat, il est important de savoir décrire ces irréductibles :

Théorème 7.1. *Tout irréductible de $\mathbb{Z}[i]$ divise un et un seul nombre premier $p \in \mathbb{Z}$ usuel. De plus, pour un tel p on est dans un et un seul des cas suivants :*

(i) $p = 2$, et on a $2 = -i(1+i)^2$ avec $1+i$ irréductible (de norme 2),

(ii) $p \equiv 3 \bmod 4$, et p est irréductible dans $\mathbb{Z}[i]$ (de norme p^2),

(iii) $p \equiv 1 \bmod 4$, et on a $p = \pi\overline{\pi}$ avec π et $\overline{\pi}$ des irréductibles de $\mathbb{Z}[i]$ non associés (de norme p).

Démonstration — Soit π un irréductible de $\mathbb{Z}[i]$. Alors $n := \mathrm{N}(\pi) = \pi\overline{\pi}$ est un entier $n > 1$. Comme π est premier, car $\mathbb{Z}[i]$ est principal, il divise donc dans $\mathbb{Z}[i]$ l'un des facteurs premiers de n dans $\mathbb{Z}$. Soit p un tel facteur. On a $p = \pi\eta$ avec $\eta \in \mathbb{Z}[i]$. On en déduit $p^2 = \mathrm{N}(\pi)\mathrm{N}(\eta)$, puis $\mathrm{N}(\pi) = p$ ou p^2. Cela montre que p est uniquement déterminé par π et conclut la première assertion. Il reste à décomposer en irréductibles dans $\mathbb{Z}[i]$ chaque premier p usuel (!).

L'assertion sur $p = 2$ est claire. Supposons $p \equiv 3 \bmod 4$. Si p n'est pas irréductible, on peut écrire $p = \alpha\beta$ avec α, β dans $\mathbb{Z}[i]$ de normes > 1. Comme on a $\mathrm{N}(p) = p^2 = \mathrm{N}(\alpha)\mathrm{N}(\beta)$, on a donc $\mathrm{N}(\alpha) = p$. Écrivant $\alpha = a + bi$ avec $a, b \in \mathbb{Z}$ on a alors $p = a^2 + b^2$. Comme p est impair, alors a et b n'ont pas même parité, et donc on a $p \equiv 1 \bmod 4$: contradiction.

Supposons enfin $p \equiv 1 \bmod 4$. Montrons que p n'est pas irréductible. En effet, on sait que -1 est un carré modulo p (Euler). Il existe donc $n \in \mathbb{Z}$ tel que p divise n^2+1. On a la décomposition $n^2+1 = (n+i)(n-i)$ dans $\mathbb{Z}[i]$. Si p était irréductible dans $\mathbb{Z}[i]$, il serait premier (car $\mathbb{Z}[i]$ factoriel), et on aurait donc $p \mid n+i$ ou $p \mid n-i$ dans $\mathbb{Z}[i]$. C'est absurde car $p\mathbb{Z}[i]$ est l'ensemble des $a + bi$ avec $a \in p\mathbb{Z}$ et $b \in p\mathbb{Z}$, et $n \pm i$ n'a pas cette propriété. On en déduit $p = \alpha\beta$ avec α, β non inversibles, puis $\mathrm{N}(\alpha) = \mathrm{N}(\beta) = p$ comme plus haut. Posons $\pi = \alpha = a + bi$. On a montré $p = \mathrm{N}(\pi) = a^2 + b^2$, et donc redémontré que p est somme de deux carrés. En outre π est irréductible car de norme première, et $p = \pi\overline{\pi}$ est donc sa décomposition en irréductibles. Il ne reste qu'à voir que π et $\overline{\pi}$ sont non associés. Mais comme on a $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$, les associés de $\pi = a + bi$ sont $a + bi$, $-a - bi$, $-b + ai$ et $b - ai$.

Cette liste contient $\overline{\pi} = a - bi$ si, et seulement si, $b = 0$, $a = 0$ ou $a = \pm b$, et donc $p = a^2$, b^2 ou $p = 2a^2$: aucune de ces solutions n'est possible (on a $p > 2$). $\square$

Le point (iii) du Théorème ci-dessus redémontre en particulier que tout premier $p \equiv 1 \bmod 4$ est somme de 2 carrés (Fermat) : c'est la troisième démonstration que nous en donnons, et sans doute la plus conceptuelle ! De plus, la factorialité de $\mathbb{Z}[i]$ permet aussi de comprendre de manière limpide l'unicité d'une telle écriture, un résultat dû à Gauss (voir le Lemme 1.7 Chap. 3) :

Proposition 7.2. *Tout nombre premier $p \equiv 1 \bmod 4$ s'écrit de manière unique sous la forme $p = a^2 + b^2$ avec $a, b \in \mathbb{N}$.*

Démonstration — Soit p premier $\equiv 1 \bmod 4$. On a vu que la décomposition en irréductibles de p dans $\mathbb{Z}[i]$ est $p = \pi\overline{\pi}$, avec π et $\overline{\pi}$ des irréductibles (non associés). En particulier, posant $\pi = a + bi$, on a $p = a^2 + b^2$.

Supposons maintenant que l'on a $x, y \in \mathbb{Z}$ avec $x^2 + y^2 = p$. L'élément $z = x + ix$ vérifie donc $\mathrm{N}(z) = p = z\overline{z}$. C'est donc un facteur irréductible (car de norme première) de p dans $\mathbb{Z}[i]$. Par factorialité de $\mathbb{Z}[i]$, les seules possibilités sont donc $z \sim \pi$ ou $z \sim \overline{\pi}$. Mais on a $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$, de sorte que les 4 associés de π sont $a + bi$, $-a - bi$, $-b + ai$ et $b - ai$, et ceux de $\overline{\pi}$ sont $a - bi$, $-a + bi$, $-b - ai$, et $b + ai$. Au final, on a bien $(x, y) = (\pm a, \pm b)$ ou $(\pm b, \pm a)$. $\square$

L'arithmétique de $\mathbb{Z}[i]$ permet plus généralement de déterminer, pour tout entier $n \geqslant 0$, le nombre de couples $(a, b) \in \mathbb{Z}^2$ avec $n = a^2 + b^2$: voir l'Exercice 7.4.

8. Une équation diophantienne

Donnons une application typique de la factorialité des anneaux de la forme $\mathbb{Z}[\sqrt{d}]$ à l'étude des équations diophantiennes. La proposition suivante avait été formulée par Fermat. On prétend qu'il l'avait lancé en défi aux mathématiciens anglais de son époque (le milieu du 17eme siècle).

Proposition 8.1. *Les seules solutions $x, y \in \mathbb{Z}$ de l'équation $y^2 = x^3 - 2$ sont les solutions évidentes $(x, y) = (3, \pm 5)$.*

Démonstration — Soient $x, y \in \mathbb{Z}$ tels que $y^2 = x^3 - 2$. Comme 2 n'est pas un cube dans $\mathbb{Z}/4\mathbb{Z}$, on constate que y est impair. Considérons la factorisation

$$(y + \sqrt{-2})(y - \sqrt{-2}) = x^3$$

dans $\mathbb{Z}[\sqrt{-2}]$. On a vu que ce dernier est euclidien, donc principal et factoriel. Vérifions que $y + \sqrt{-2}$ et $y - \sqrt{-2}$ sont premiers entre eux dans $\mathbb{Z}[\sqrt{-2}]$. Il suffit de voir qu'il n'y a pas d'irréductible π divisant $y + \sqrt{-2}$ et $y - \sqrt{-2}$. Mais un tel π diviserait $2\sqrt{-2} = -\sqrt{-2}^3$, et donc $\sqrt{-2}$ (car π est également premier), et donc y. Mais alors $\mathrm{N}(\sqrt{-2}) = 2$ diviserait $\mathrm{N}(y) = y^2$ dans $\mathbb{Z}$: absurde car y est impair.

Si dans un anneau factoriel A, on a une relation $a^n = bc$ avec b et c premiers entre eux, et n un entier $\geqslant 1$, on constate en décomposant b et c en irréductibles qu'il existe $d \in A$ et $u \in A^\times$ tels que $b = d^n u$. Comme on a montré $\mathbb{Z}[\sqrt{-2}]^\times = \{\pm 1\}$,

on en déduit l'existence de $z \in \mathbb{Z}[\sqrt{-2}]$ tel que $y + \sqrt{-2} = \pm z^3 = (\pm z)^3$. Posons $\pm z = u + v\sqrt{-2}$ avec $u, v \in \mathbb{Z}$. On a donc

$$y + \sqrt{-2} = (u + v\sqrt{-2})^3 = u^3 - 6uv^2 + (3u^2v - 2v^3)\sqrt{-2}.$$

En prenant la coordonnée en $\sqrt{-2}$, il vient $1 = v(3u^2 - 2v^2)$, d'où l'on tire $v = \pm 1$ puis $3u^2 = v + 2$ et donc $v = 1$ et $u = \pm 1$. On a donc $y = u^3 - 6uv^2 = \pm 5$, puis $x^3 = 27$, et donc nécessairement $x = 3$, ce qui conclut ! $\square$

Cette méthode admet de multiples applications. La plus célèbre est certainement la stratégie qu'elle fournit pour étudier l'équation de Fermat $x^n + y^n = z^n$, qui s'écrit aussi $x^n = \prod_{i=0}^{n-1}(z - \zeta^i y)$ où $\zeta = e^{\frac{2i\pi}{n}}$. Plusieurs mathématiciens ont crû démontrer ainsi, avec du travail, le *grand théorème de Fermat*. Malheureusement, le sous-anneau $\mathbb{Z}[\zeta] = \sum_{k=0}^{n-1} \mathbb{Z}\zeta^k \subset \mathbb{C}$ est rarement factoriel (le premier cas problématique étant $n = 23$), et il faut se plonger dans la théorie de Kummer pour comprendre comment remédier partiellement à ce problème. Nous renvoyons à tout cours de théorie algébrique des nombres, par exemple à celui de l'auteur, pour une étude de ces questions.

9. Complément I : Anneaux quotients

Dans ce complément on explique la construction des anneaux quotients. On se donne un anneau $(A, +, \cdot)$, que l'on ne supposera pas nécessairement commutatif par souci de généralité. Un *idéal bilatère* de A est un sous-groupe additif $I \subset A$ tel que pour tout $a \in A$ et tout $x \in I$ on a $ax \in I$ et $xa \in I$. Quand A est commutatif, on retrouve la notion d'idéal (tout court). Commençons par metttre en évidence l'énoncé immédiat suivant déjà mentionné dans le chapitre.

LEMME 9.1. *Soit $f : A \to B$ un morphisme d'anneaux.*

(i) Alors $\ker f := \{a \in A \mid f(a) = 0\}$ *est un idéal bilatère de A.*

(ii) Plus généralement, si I est un idéal (à droite, à gauche, bilatère) de B alors $f^{-1}(I)$ est un idéal du même type A.

(iii) Si f est surjective, et si I est un idéal (à droite, à gauche, bilatère) de A, alors $f(I)$ est un idéal du même type de B.

Pour I un sous-groupe additif de A, et pour $a, b \in A$ on rappelle que la notation $a \equiv b \bmod I$ signifie $a - b \in I$, ou encore $a + I = b + I$. Le lemme suivant dit que l'on peut *additionner, soustraire ou multiplier les congruences modulo un idéal bilatère.*

LEMME 9.2. *Soient A un anneau, I un idéal bilatère de A et $a, a', b, b' \in A$ avec $a \equiv a' \bmod I$ et $b \equiv b' \bmod I$. Alors on a*

$$a + b \equiv a' + b' \bmod I, \quad a - a' \equiv b - b' \bmod I \quad \text{et} \quad ab \equiv a'b' \bmod I. \tag{61}$$

DÉMONSTRATION — Pour l'addition et la soustraction, cela découle simplement du fait que I est un sous-groupe additif de A. Pour la multiplication, on écrit $a = a' + i$ et $b = b' + j$ avec $i, j \in I$ et on constate que l'on a $ab = a'b' + a'j + ib' + ij$ avec $a'j + ib' + ij \in I$ car I est un idéal bilatère. □

Cette observation élémentaire constitue l'essentiel du (ii) du résultat suivant. Le (i) est une variante de l'argument d'unicité de la loi de groupe quotient vu au §6 Chap. 2.

THÉORÈME 9.3. *Soit A un anneau et I un sous-groupe additif de A.*

(i) Il existe au plus une structure d'anneau sur le groupe quotient A/I telle que la projection canonique $A \to A/I$ est un morphisme d'anneaux.

(ii) Une telle structure existe si, et seulement si, I est un idéal bilatère de A.

DÉMONSTRATION — Montrons d'abord la condition suffisante du (ii). On définit deux lois $+$ et $\star$ sur A/I en posant, pour $a, b \in A$,

$$(a + I) + (b + I) := (a + b) + I \quad \text{et} \quad (a + I) \star (b + I) := ab + I. \tag{62}$$

Le Lemme 9.2 montre que ces deux lois sont bien définies, au sens où les éléments $(a+b)+I$ et $ab+I$ ne dépendent que des classes $a+I$ et $b+I$ et non des représentants a et b choisis dans ces classes. Par construction, $\pi : A \to A/I$ vérifie $\pi(a + b) = \pi(a) + \pi(b)$ et $\pi(ab) = \pi(a) \star \pi(b)$ pour tout $a, b \in A$. Par surjectivité de π, le fait que $(A, +, \cdot)$ est un anneau implique immédiatement que $(A, +, \star)$ est un anneau, et que π est un morphisme d'anneaux. Par exemple,

$$(a + I) \star ((b + I) + (c + I)) = \pi(a) \star \pi(b + c) = \pi(a(b + c))$$

$$= \pi(ab + ac) = \pi(a)\pi(b) + \pi(a)\pi(c) = (a + I) \star (b + I) + (a + I) \star (c + I),$$

démontrent la distributivité d'un côté. On vérifie de même la distributivité de l'autre côté, l'associativité de $+$ et $\star$, et que les neutres additifs et multiplicatifs de $(A/I, +, \star)$ sont $\pi(0) = I$ et $\pi(1) = 1 + I$.

Vérifions maintenant le (i). Supposons qu'il existe une structure d'anneau sur A/I, disons $(A/I, +, \star)$, telle que la projection canonique $\pi : A \to A/I, a \mapsto a+I$, est un morphisme d'anneaux. Les formules $\pi(a+b) = \pi(a)+\pi(b)$ et $\pi(ab) = \pi(a) \star \pi(b)$ montrent bien que que $+$ et $\star$ sont uniquement déterminés par l'addition et la multiplication de A, et vérifient nécessairement (62). Ce conclut la démonstration du (i). Un condition nécessaire supplémentaire est que I est un idéal bilatère de A. En effet, on sait $I = \ker \pi$, et pour $a, b \in A$ et $x \in I$, on a $\pi(axb) = \pi(a) \star \pi(x) \star \pi(b) = 0$ car $\pi(x) = 0$. □

Remarque 9.4. Tout comme pour les groupes quotients, nous aurions aussi pu observer que la loi multiplicative de l'anneau A/I, vu comme sous-ensemble de $\mathrm{P}(A)$, est induite par $(X, Y) \mapsto XY + I$ (produit et somme des parties, l'ajout de I est cette fois-ci nécessaire).

Définition 9.5. *Si A est un anneau et I un idéal bilatère de A, l'anneau quotient A/I est l'ensemble A/I muni de son unique structure d'anneaux telle que la projection canonique $\pi : A \to A/I$ est un morphisme d'anneaux.*

Exemple 9.6. (Retour sur $\mathbb{Z}/N\mathbb{Z}$) Pour $N \in \mathbb{Z}$, $N\mathbb{Z}$ est un idéal de l'anneau $\mathbb{Z}$. La structure d'anneau quotient sur $\mathbb{Z}/N\mathbb{Z}$ est celle rendant la projection $\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}, k \mapsto \overline{k}$ un morphisme d'anneaux, *i.e.* $\overline{k + k'} = \overline{k} + \overline{k'}$, $\overline{kk'} = \overline{k} \cdot \overline{k'}$. C'est bien celle considérée au chapitre 2.

Exemple 9.7. (L'anneau $k[X]/(P)$) Soient k un anneau commutatif et $P \in k[X]$. La structure d'anneau quotient sur le groupe additif quotient $k[X]/(P)$ est l'unique telle que pour tout $A, B \in k[X]$, on a $\overline{A} \cdot \overline{B} = \overline{AB}$, où $\overline{A}$ désigne la classe de A modulo (P). Faisons deux observations supplémentaires :

(i) Supposons P de degré de $n \geqslant 1$ et de coefficient dominant dans $k^\times$. Tout élément de $k[X]/(P)$ possède alors un unique représentant dans $k[X]$ de degré $< n$. En effet, pour tout $Q \in k[X]$ il existe des uniques $A, B \in k[X]$ avec $Q = AP + B$ et $\deg B < n$ si B est non nul (*division euclidienne par un polynôme de coefficient dominant inversible*).

(ii) Si k est un corps, l'hypothèse sur le coefficient dominant de P est automatiquement satisfaite. De plus, l'anneau $k[X]/(P)$ est un k-espace vectoriel de manière naturelle (laquelle ?), et on vient de voir qu'il a pour base les classes des n monômes $1, X, \ldots, X^{n-1}$.

Proposition 9.8. *(Propriété universelle des anneaux quotients) Soient A un anneau, I un idéal bilatère de A et $f : A \to B$ un morphisme d'anneaux vérifiant $I \subset \ker f$. Alors il existe un unique morphisme d'anneaux $\overline{f} : A/I \to B$ envoyant $a + I$ sur $f(a)$ pour tout $a \in A$.*

Bien sûr, la propriété $\overline{f}(a+I) = f(a)$ s'écrit aussi $f = \overline{f} \circ \pi$ avec $\pi : A \to A/I$ la projection canonique.

Démonstration — L'existence et unicité d'un morphisme de groupes additifs $\overline{f} : A/I \to B$ vérifiant $\overline{f}(a+I) = f(a)$ pour tout $a \in A$ découle par exemple de la Proposition 6.16 Chap. 2. Cette propriété entraîne automatiquement que $\overline{f}$ est un morphisme d'anneaux. En effet, on a $\overline{f}(1+I) = f(1) = 1$, et pour $a, a' \in A$ on a

$$\overline{f}((a+I)(a'+I)) = \overline{f}(aa'+I) = f(aa') = f(a)f(a') = \overline{f}(a+I)\overline{f}(a'+I).$$

(On n'a finalement utilisé l'hypothèse I bilatère que pour assurer l'existence de l'anneau quotient A/I). □

Corollaire 9.9. *(même hypothèses) Si en outre f est surjective et vérifie* $\ker f = I$, *alors $\overline{f}$ est un isomorphisme d'anneaux $A/I \xrightarrow{\sim} B$.*

Démonstration — En effet, le noyau de $\overline{f}$ est $\{a+I \mid f(a) = 0\}$, c'est donc $\{I\}$ (élément neutre de $(A/I, +)$). Ainsi, $\overline{f}$ est injective. Comme elle est clairement surjective car f l'est, elle est bijective : c'est un isomorphisme. □

La proposition suivante est l'analogue pour les anneaux de la Proposition 6.19 Chap. 2.

Proposition 9.10. *Soit I un idéal bilatère de l'anneau A.*

(i) L'application $J \mapsto J/I$ induit une bijection croissante entre idéaux bilatères J de A (resp. à gauche, resp. à droite) contenant I et idéaux bilatères (resp. à gauche, resp. à droite) de A/I.

(ii) Si J est un idéal bilatère de A contenant I, le morphisme d'anneaux naturel $A/I \to A/J$ est surjectif de noyau J/I, et induit un isomorphisme d'anneaux $(A/I)/(J/I) \simeq A/J$.

Démonstration — On sait déjà que $J \mapsto J/I$ induit une bijection entre sous-groupes J de A contenant I et sous-groupes du groupe additif quotient A/I, de bijection réciproque $K \mapsto \pi^{-1}(K)$, par la Proposition 6.19 Chap. 2. Le (i) se déduit du fait que pour un morphisme surjectif d'anneaux quelconque $A \to B$, l'image d'un idéal bilatère (resp. à gauche, resp. à droite) de A est un idéal bilatère (resp. à gauche, resp. à droite) de B, et l'image inverse d'un idéal bilatère de B (resp. à gauche, resp. à droite) est un idéal bilatère (resp. à gauche, resp. à droite) de A (Lemme 9.1).

Pour le (ii), la Proposition 9.8 montre qu'il existe un unique morphisme d'anneaux $A/I \to A/J, a+I \mapsto a+J$. Il est clairement surjectif de noyau $\{a+I \in A/I \mid a+J = J\} = J/I$. On conclut par le Corollaire 9.9. □

En guise d'application des anneaux quotients, discutons quelques constructions d'anneaux simples et de corps.

Définition 9.11. *Un anneau A est dit* simple *s'il est non nul, et si ses seuls idéaux bilatères sont* $\{0\}$ *et A.*

Exemple 9.12. *(i) Si k un anneau à division, alors k est simple.* En effet, soit I un idéal bilatère de k contenant un élément x non nul. Alors x est inversible dans k, donc il existe $y \in k$ avec $yx = 1$. On a alors $1 = yx \in I$, puis $a = a.1 \in I$ pour tout $a \in k$, et enfin $I = k$.

(ii) Un anneau commutatif est simple si, et seulement si, c'est un corps. En effet, on a vu au (i) qu'un corps est simple. Réciproquement, soit A un anneau simple et commutatif, et soit $x \in A$ non nul. Alors $Ax \subset A$ est un idéal bilatère de A car A est commutatif. Comme on a $Ax \neq \{0\}$, on a donc $Ax = A$ car A est simple, puis $x \sim 1$ et $x \in A^\times$.

(iii) Si k est un anneau à division, l'anneau $\mathrm{M}_n(k)$ est simple (non commutatif pour $n > 1$). En effet, soient I idéal bilatère $\mathrm{M}_n(k)$ et $X \in I$ non nul. Il existe $1 \leqslant i, j \leqslant n$ avec $X_{i,j} \in k^\times$. Notant $\mathrm{E}_{i,j}$ les matrices élémentaires usuelles, pour tout $1 \leqslant p, q \leqslant n$ on a donc $X_{i,j}^{-1}\mathrm{E}_{p,i}X\mathrm{E}_{j,q} = \mathrm{E}_{p,q} \in I$ car I est bilatère, puis $I = \mathrm{M}_n(k)$. Plus généralement, pour un anneau A quelconque cet argument montre que les idéaux bilatères de $\mathrm{M}_n(A)$ sont les $\mathrm{M}_n(I)$ avec I idéal bilatère de A.

Définition 9.13. *Un idéal bilatère I d'un anneau A est dit* maximal *si on a $I \neq A$, et si pour tout idéal bilatère J de A contenant I on a $J = I$ ou $J = A$.*

Lemme 9.14. *Soient A un anneau et I un idéal bilatère de A. L'anneau quotient A/I est simple si, et seulement si, I est maximal.*

Démonstration — L'assertion (i) de la Proposition 9.10 affirme que les idéaux bilatères de A/I sont en bijection naturelle avec les idéaux bilatères de A contenant I. Ainsi, I est maximal si, et seulement si, A/I a pour uniques idéaux les deux idéaux distincts $\{0\}$ et A/I, ce qui équivaut à dire que A/I est simple. □

On suppose désormais A commutatif. Le lemme ci-dessus affirme qu'un idéal $I \subsetneq A$ est maximal si, et seulement si, l'anneau quotient A/I est un corps. Cela fournit une technique importante de construction de corps.

Exemple 9.15. (*Une construction du corps des réels*) Soit A l'ensemble des suites de Cauchy de rationnels.[3] On constate que A est un sous-anneau de l'anneau produit $\mathbb{Q}^{\mathbb{N}}$, et que le sous-ensemble $I \subset A$ constitué des suites (x_n) qui tendent vers 0 est un idéal de A. On a $I \neq A$ car la suite constante $1 = (1)$ est dans $A \smallsetminus I$. L'idéal I est maximal. En effet, si une suite de Cauchy $x = (x_n) \in A$ ne tend pas vers 0, il existe $\epsilon > 0$ et $N \geqslant 1$ avec $|x_n| \geqslant \epsilon$ pour tout $n \geqslant N$ (couper les ϵ en deux). Ainsi, la suite $y = (y_n)$ définie par $y_n = 0$ pour $n < N$, et $y_n = 1/x_n$ pour $n \geqslant N$, est une suite de Cauchy, et on a $yx - 1 \in I$. Ainsi, A/I est un corps : c'est l'une des constructions possibles du corps $\mathbb{R}$ des réels à partir de $\mathbb{Q}$.

Corollaire 9.16. *Soient A un anneau principal et $\pi \in A$ un irréductible. Alors l'anneau quotient $A/\pi A$ est un corps.*

3. On rappelle que cela signifie que pour tout $\epsilon \in \mathbb{Q}_{>0}$, il existe $N \geqslant 1$ tel que $|x_n - x_m| < \epsilon$ pour tout $m, n \geqslant N$. Dans le cas particulier $\epsilon = 1$, et posant $M = \mathrm{Max}_{m \leqslant N}|x_m|$, on a alors $|x_n| \leqslant M + 1$ pour tout $n \geqslant 0$, et donc (x_n) est bornée.

Démonstration — Soit I un idéal de A contenant π. On peut écrire $I = \omega A$ car A est principal. On a $\pi \in I$ donc $\omega \mid \pi$. Comme π est irréductible, on a soit $\omega \sim \pi$, soit $\omega \sim 1$, ou ce qui revient au même, soit $I = \pi A$, soit $I = A$. Comme on a $\pi A \neq \{0\}$ (car π est irréductible), on a montré que πA est maximal. □

Par exemple, on retrouve que si $p \in \mathbb{Z}$ est un nombre premier, alors l'anneau quotient $\mathbb{Z}/p\mathbb{Z}$ est un corps. Pour $A = k[X]$ on en déduit aussi :

Corollaire 9.17. *Soient k un corps et $P \in k[X]$ un polynôme irréductible. Alors l'anneau quotient $k[X]/(P)$ est un corps.*

Ce corollaire est la source de nombreuses constructions d'*extensions de corps*. En effet, l'application $k \mapsto K := k[X]/(P)$, $\lambda \mapsto \overline{\lambda}$, est un morphisme injectif de corps, souvent simplement vu comme une inclusion. Le corps K est alors un k-espace vectoriel de dimension $n := \deg P$, avec pour base naturelle les classes de $1, X, X^2, \ldots, X^{n-1}$ (Exemple 9.7).

Exemple 9.18. (i) Le polynôme $X^2 + 1$ est irréductible dans $\mathbb{R}[X]$, et le corps quotient $C := \mathbb{R}[X]/(X^2+1)$ est une définition possible du corps $\mathbb{C}$ des nombres complexes. On pose simplement $i := X \bmod (X^2 + 1)$ dans C.

(ii) Soit p un nombre premier. Il existe p^2 polynômes unitaires de degré 2 dans $(\mathbb{Z}/p\mathbb{Z})[X]$. Comme $\frac{p(p+1)}{2}$ d'entre eux sont réductibles, il y en a $\frac{p(p-1)}{2} \geqslant 1$ qui sont irréductibles. Si P est un tel polynôme, le corps $(\mathbb{Z}/p\mathbb{Z})[X]/(P)$ est un surcorps de $\mathbb{Z}/p\mathbb{Z}$ de cardinal p^2. En fait, pour $p \neq 2$ on peut prendre $P = X^2 - a$ où $a \in \mathbb{Z}/p\mathbb{Z}$ n'est pas un carré (il en existe !). Pour $p = 2$, l'unique possibilié pour P est $X^2 + X + 1$.

(iii) Dans le cours d'Algèbre 2 nous verrons qu'il existe des polynômes irréductibles de tout degré à coefficients dans $\mathbb{Z}/p\mathbb{Z}$, et en particulier des surcorps de $\mathbb{Z}/p\mathbb{Z}$ de cardinal p^n pour tout $n \geqslant 1$. Mieux, un tel corps est unique à isomorphisme près : c'est le corps $\mathbb{F}_{p^n}$ de Galois.

Terminons par une application du Lemme de Zorn importante dans ce contexte.

Proposition 9.19. (Théorème de Krull) *Soient A un anneau et I un idéal bilatère de A avec $I \subsetneq A$. Il existe un idéal maximal M de A contenant I.*

Démonstration — L'ensemble $\mathscr{J}$ des idéaux bilatères J de A avec $I \subset J$ et $J \subsetneq A$ est non vide, car il contient I par hypothèse. Ordonné par l'inclusion, il est inductif. En effet, si $\{J_i\}$ est une famille totalement ordonnée d'idéaux bilatères de A avec $I \subset J_i \subsetneq A$, alors $J = \bigcup_i J_i$ est encore un idéal bilatère de A contenant I. Il est strict car sinon $1 \in J$ et donc $1 \in J_i$ pour un certain i, puis $A = J_i$, une absurdité. D'après le Lemme de Zorn, $\mathscr{J}$ possède un élément maximal M, qui répond à la question. □

10. Complément II : Quaternions entiers, sommes de 4 carrés et sous-groupes libres de SO(3)

On se propose dans ce complément d'aborder l'arithmétique du sous-anneau

$$\mathrm{H}_{\mathbb{Z}} := \mathbb{Z} \oplus \mathbb{Z}\, I \oplus \mathbb{Z}\, J \oplus \mathbb{Z}\, K \subset \mathbb{H}$$

des *quaternions entiers*, aussi appelés *quaternions de Lipschitz*, revisitant notamment des travaux de Hurwitz [4] et Dickson [5]. Cet anneau non commutatif contient par exemple les "copies" $\mathbb{Z}[I]$, $\mathbb{Z}[J]$ et $\mathbb{Z}[K]$ de l'anneau des entiers de Gauss, ainsi que tous les $\mathbb{Z}[\sqrt{-d}]$ quand d est somme de 3 carrés. [6] Comme nous le verrons, il n'est pas très loin d'être principal (des deux côtés !) et des assertions de factorisation unique seront valables dans cet anneau, malgré sa non commutativité. Nous en donnerons dans ce complément deux applications, l'une à l'étude des sommes de 4 carrés, et l'autre à la construction de sous-groupes libres de SO(3).

10.1. Sommes de 4 carrés. Parallèlement aux liens entre $\mathbb{Z}[i]$ et les sommes de deux carrés, l'arithmétique de $\mathrm{H}_{\mathbb{Z}}$ est très reliée à l'étude des sommes de 4 carrés d'entiers. En effet, si l'on pose

$$\mathrm{r}_4(n) = |\,\{(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4 \mid x_1^2 + x_2^2 + x_3^2 + x_4^2 = n\}\,|$$

pour $n \in \mathbb{N}$, on a bien sûr $\mathrm{r}_4(n) = |\{q \in \mathrm{H}_{\mathbb{Z}} \mid \mathrm{n}(q) = n\}|$. Nous allons démontrer les deux résultats classiques suivants :

THÉORÈME 10.1. (Lagrange, 1770) *Tout entier $\geqslant 0$ est somme de 4 carrés.*

Notons $\upsilon(n)$ la somme des diviseurs *impairs* de l'entier $n \geqslant 1$. En particulier, on a $\upsilon(n) = \sum_{d|n} d$ pour n impair, et $\upsilon(2n) = \upsilon(n)$ pour tout n.

THÉORÈME 10.2. (Jacobi, 1834) *Soit $n \geqslant 1$. On a $\mathrm{r}_4(n) = 8\,\upsilon(n)$ pour n impair, $\mathrm{r}_4(n) = 24\,\upsilon(n)$ pour n pair. En particulier, pour tout nombre premier p on a*

$$\mathrm{r}_4(p) = 8\,(p+1).$$

Le théorème de Jacobi entraîne évidemment celui de Lagrange, qui s'écrit aussi $\mathrm{r}_4(n) \geqslant 1$ pour tout $n \geqslant 1$. Examinons l'énoncé de Jacobi sur quelques exemples, en considérant les écritures $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$ avec les $x_i \in \mathbb{Z}$:

($n = 2$) Deux x_i sont nuls et les autres valent ± 1, on a bien $\mathrm{r}_4(2) = \binom{4}{2} 2^2 = 24$.

($n = 3$) Un des x_i est nul et les autres valent ± 1, on a bien $\mathrm{r}_4(3) = 4 \cdot 2^3 = 8 \cdot 4$.

($n = 4$) Soit tous les x_i valent ± 1, soit tous les x_i sont nuls sauf 1 qui vaut ± 2, et on a bien $\mathrm{r}_4(4) = 2^4 + 4 \cdot 2 = 24 \cdot 1$.

($n = 13$) De même, il y a $4 \cdot 3 \cdot 2^2 = 8 \cdot 6$ écritures de la forme $13 = 2^2 + 3^2 + 0 + 0$, et $2^4 \cdot 4 = 8 \cdot 8$ écritures de la forme $13 = 1 + 4 + 4 + 4$, puis $\mathrm{r}_4(13) = 8 \cdot 14$.

La démonstration originale de Jacobi, de nature analytique, consiste à montrer et utiliser le fait que la série génératrice $\sum_{n \geqslant 0} \mathrm{r}_4(n)\, q^n$ est le développement de Fourier d'une « forme modulaire ». La preuve exposée ci-dessous, dont les idées remontent à Lipchitz, Hurwitz et Dickson, est basée sur l'arithmétique de l'anneau $\mathrm{H}_{\mathbb{Z}}$. Terminons cette partie par des réductions élémentaires :

4. A. Hurwitz, *Vorlesungen Über die Zahlentheorie der Quaternionen*, Springer Verlag (1919).
5. L. E. Dickson, *Arithmetic of Quaternions*, Proc. London Math. Soc. (1922), 225–232.
6. En effet, pour $q = aI + bJ + cK$ avec $a, b, c \in \mathbb{Z}$ on a $q^2 = -d$ avec $d = a^2 + b^2 + c^2$.

Lemme 10.3. *Pour $n \geqslant 1$ on pose $f(n) = \frac{1}{8}\mathrm{r}_4(n)$. On a*

(i) $f(mn) = f(m)f(n)$ pour $m, n \geqslant 1$ avec $m \wedge n = 1$,
(ii) $f(p^k) = 1 + p + \cdots + p^k$ pour p premier impair et $k \geqslant 0$,
(iii) $f(2^k) = 3$ pour $k \geqslant 1$.

Les points (i) et (ii) de ce lemme constituent le coeur de la démonstration, et seront démontrés dans les sections suivantes. Montrons immédiatement le point (iii), qui s'écrit aussi $\mathrm{r}_4(2^m) = 24$ pour $m \geqslant 1$. On a déjà vu $\mathrm{r}_4(2) = \mathrm{r}_4(4) = 24$ ci-dessus. Soient $x \in \mathbb{Z}^4$ avec $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 2^m$ et $m \geqslant 3$. Comme le carré d'un nombre impair est $\equiv 1 \bmod 8$, on en déduit que tous les x_i sont pairs. On a montré $\mathrm{r}_4(2^m) = \mathrm{r}_4(2^{m-2})$ pour $m \geqslant 3$, ce qui conclut.

Démonstration — (Le Lemme 10.3 entraîne le Théorème 10.2). Soient $m, n \geqslant 1$ premiers entre eux. Tout diviseur impair de mn s'écrit de manière unique ab avec $a|m$, $b|m$ et a, b impairs. On a donc $\upsilon(mn) = \upsilon(m)\upsilon(n)$. Pour n impairs on a aussi $f(mn) = f(m)f(n)$ par le (i) du lemme, et pour p premier impair, on a $f(p^k) = \upsilon(p^k)$ par le (ii). On en déduit $f(2^k n) = f(2^k)\upsilon(n)$ pour tout n impair et tout $k \geqslant 0$ en décomposant n en produit de puissances de premiers impairs distincts. Par le (iii) du lemme on a $f(2^k) = 3$ pour $k > 0$, et on a $f(1) = 1$. Pour conclure il suffit d'observer que l'on a $\upsilon(2^k n) = \upsilon(2^k)\upsilon(n) = \upsilon(n)$. □

10.2. La divisibilité dans l'anneau $\mathrm{H}_{\mathbb{Z}}$. On s'intéresse aux questions de divisibilité dans l'anneau $\mathrm{H}_{\mathbb{Z}}$. Soient q et q' dans $\mathrm{H}_{\mathbb{Z}}$. Nous dirons que q divise q', et noterons $q \,|\, q'$ s'il existe $h \in \mathrm{H}_{\mathbb{Z}}$ avec $q' = hq$. Autrement dit, on a

$$q \,|\, q' \iff q' \in \mathrm{H}_{\mathbb{Z}}\, q \tag{63}$$

Dans cette situation non commutative, cette notion de divisibilité *par la droite* est bien sûr concurrente à celle de divisibilité *par la gauche*, qui consisterait à demander $q' \in q\,\mathrm{H}_{\mathbb{Z}}$. Nous n'utiliserons pas cette dernière dans ce qui suit au delà de l'exemple ci-dessous, qui montre que les deux notions ne sont pas équivalentes en général (sauf bien sûr si quand l'élement q est en fait dans $\mathbb{Z}$).

Exemple 10.4. *Considérons les éléments $q = 1 + 2I$ et $q' = 1 + 2J$, tous deux de norme 5, on a donc $qq' = 1 + 2I + 2J + 4K$. Mais q ne divise pas qq' ! En effet, si on avait $qq' = hq$ avec $h \in \mathrm{H}_{\mathbb{Z}}$ on aurait $qq'q^{-1} \in \mathrm{H}_{\mathbb{Z}}$, mais on constate*

$$qq'q^{-1} = \frac{1}{5}qq'q^\star = \frac{1}{5}(1 + 2I + 2J + 4K)(1 - 2I) = \frac{1}{5}(5 - 6J + 8K) \notin \mathrm{H}_{\mathbb{Z}}.$$

On a toujours manifestement $q \,|\, q'$ et $q' \,|\, q'' \implies q \,|\, q''$. De plus, comme dans le cas commutatif, on dira que q et q' sont *associés* si on a $q \,|\, q'$ et $q' \,|\, q$, c'est une relation d'équivalence sur $\mathrm{H}_{\mathbb{Z}}$ que l'on notera $q \sim q'$. On vérifie immédiatement :

$$q \sim q' \iff \mathrm{H}_{\mathbb{Z}}\, q = \mathrm{H}_{\mathbb{Z}}\, q' \iff \exists\, u \in \mathrm{H}_{\mathbb{Z}}^\times \,|\, q' = uq. \tag{64}$$

Il nous faut maintenant déterminer le groupe des inversibles $\mathrm{H}_{\mathbb{Z}}^\times$ de $\mathrm{H}_{\mathbb{Z}}$. On rappelle

$$\mathrm{H}_8 = \{\pm 1, \pm I, \pm J, \pm K\} \subset \mathrm{H}_{\mathbb{Z}}.$$

De plus, $\mathrm{H}_{\mathbb{Z}}$ est stable par la *conjugaison* $q \mapsto q^\star$.

Proposition 10.5. *On a $\mathrm{H}_{\mathbb{Z}}^\times = \{q \in \mathrm{L} \mid \mathrm{n}(q) = 1\} = \mathrm{H}_8$.*

Démonstration — La seconde égalité est immédiate, car les seuls éléments $x \in \mathbb{Z}^4$ vérifiant $\sum_{i=1}^4 x_i^2 = 1$ sont les 8 avec 3 coordonnées nulles et la dernière égale à ± 1. Montrons la première. Supposons $qq' = 1$ avec $q, q' \in \mathrm{H}_{\mathbb{Z}}^{\times}$. En prenant la norme on a $\mathrm{n}(q)\mathrm{n}(q') = 1$ puis $\mathrm{n}(q) = 1$ car $\mathrm{n}(\mathrm{H}_{\mathbb{Z}}) \subset \mathbb{Z}_{\geqslant 0}$. Réciproquement, comme L est stable par conjugaison, pour $q \in \mathrm{L}$ avec $\mathrm{n}(q) = qq^\star = q^\star q = 1$, on a $q \in \mathrm{L}^\times$ et $q^{-1} = q^\star$. □

La multiplicativité de la norme $\mathrm{n} : \mathrm{H}_{\mathbb{Z}} \to \mathbb{N}$ a joué un rôle ci-dessus. Comme pour les anneaux $\mathbb{Z}[\sqrt{d}]$ c'est un outil important pour comprendre la divisibilité dans $\mathrm{H}_{\mathbb{Z}}$:

Lemme 10.6. *Soient $q, q' \in \mathrm{H}_{\mathbb{Z}}$ avec q non nul et $q \,|\, q'$. On a la divisibilité $\mathrm{n}(q) \,|\, \mathrm{n}(q')$ dans $\mathbb{Z}$, et on a $q \sim q'$ si et seulement si, $\mathrm{n}(q) = \mathrm{n}(q')$.*

Démonstration — Écrivons $q' = hq$ avec $h \in \mathrm{H}_{\mathbb{Z}}$. En prenant la norme on a $\mathrm{n}(q') = \mathrm{n}(h)\mathrm{n}(q)$ puis $\mathrm{n}(q) \,|\, \mathrm{n}(q')$. Supposant $\mathrm{n}(q) = \mathrm{n}(q')$, on a $\mathrm{n}(h) = 1$ puis $h \in L^\times$ par la Proposition 10.5, et donc $q \sim q'$. Si réciproquement on a $q = \xi q'$ avec $\xi' \in \mathrm{H}_{\mathbb{Z}}^{\times}$, on a $\mathrm{n}(q) = \mathrm{n}(q')$ car $\mathrm{n}(\xi) = 1$. □

Comme on s'intéresse à la divisibilité par la droite nous allons étudier les idéaux à gauche de $\mathrm{H}_{\mathbb{Z}}$ (Définition (63)). Pour faire court, *nous utiliserons désormais la terminologie « idéal » pour « idéal à gauche ».*[7] Un idéal de $\mathrm{H}_{\mathbb{Z}}$ sera dit *impair* s'il contient un élément de norme impaire. Un idéal de $\mathrm{H}_{\mathbb{Z}}$ sera dit principal s'il est de la forme $\mathrm{H}_{\mathbb{Z}}\, q$ avec $q \in \mathrm{H}_{\mathbb{Z}}$. Nous allons montrer la :

Proposition 10.7. (Dickson) *Tout idéal impair de $\mathrm{H}_{\mathbb{Z}}$ est principal.*

On commence par établir une forme de division euclidienne. L'élément *de Hurwitz*

$$\omega = \frac{1}{2}(1 + I + J + K) \quad \in \quad \mathbb{H}$$

jouera un rôle important. On a $2\,\omega \in \mathrm{H}_{\mathbb{Z}}$, mais ω n'est pas dans $\mathrm{H}_{\mathbb{Z}}$.

Lemme 10.8. *Soit $h \in \mathbb{H}$, il existe $q \in \mathrm{H}_{\mathbb{Z}}$ avec soit $\mathrm{n}(h - q) < 1$, soit $h - q = \omega$.*

Démonstration — Écrivons $h = x_1 + x_2 I + x_3 J + x_4 K$ avec $x_1, x_2, x_3, x_4 \in \mathbb{R}$, on peut toujours trouver $x_1', x_2', x_3', x_4' \in \mathbb{Z}$ avec $|x_i - x_i'| \leqslant 1/2$ pour tout i. Posant $q = x_1' + x_2' I + x_3' J + x_4' K \in \mathrm{H}_{\mathbb{Z}}$ on a alors $\mathrm{n}(h - q) = \sum_{i=1}^4 (x_i - x_i')^2 \leqslant 1/4 + 1/4 + 1/4 + 1/4 = 1$, avec égalité si, et seulement si, on a $h - q = \frac{1}{2}(\pm 1 \pm I \pm J \pm K)$. Dans ce cas d'égalité, on a en particulier $h \in \mathrm{H}_{\mathbb{Z}} + \omega$. □

Pour gérer l'alternative donnée par le Lemme 10.8, nous aurons besoin de deux observations simples sur l'élément ω, connues de Hurwitz.

Lemme 10.9. *(i) Pour tout $q \in \mathrm{H}_{\mathbb{Z}}$ on a $\mathrm{n}(q + \omega) \in \mathbb{Z}$.*

(ii) Pour $q \in \mathrm{H}_{\mathbb{Z}}$ de norme impaire, on a $\omega q \notin \mathrm{H}_{\mathbb{Z}}$.

7. En fait, l'involution $q \mapsto q^\star$ de $\mathrm{H}_{\mathbb{Z}}$ vérifie $(xy)^\star = y^\star x^\star$ et donc échange idéaux à gauche et idéaux à droite, de sorte que tout ce que nous prouverons sur les idéaux (à gauche) aura un analogue sur ceux à droite, que nous n'expliciterons pas car cela ne nous servira pas.

Démonstration — Pour le (i), on constate que l'on a $q+\omega = \frac{1}{2}(x_1+x_2I+x_3J+x_4K)$ avec $x_i \in 2\mathbb{Z}+1$ pour tout i. En particulier, on a $x_i^2 \equiv 1 \bmod 4$, et donc $\mathrm{n}(q+\omega) \in \frac{1}{4}(4+4\mathbb{Z}) = \mathbb{Z}$. Pour le (ii), supposons $\mathrm{n}(q) = 2k+1$ impair. En multipliant à gauche par ω on trouve $\omega = (\omega q)\overline{q} - (2\omega)k$, puis $\omega \in \mathrm{H}_\mathbb{Z}$ si $\omega q \in \mathrm{H}_\mathbb{Z}$, une contradiction. □

Démonstration — (de la Proposition 10.7) Soit $I \subset \mathrm{H}_\mathbb{Z}$ un idéal non nul. On a alors $\mathrm{n}(I \smallsetminus \{0\}) \subset \mathbb{Z}_{>0}$. Considérons $m \in I \smallsetminus \{0\}$ de norme minimale. Il est inversible dans le corps gauche $\mathbb{H}$. Pour $h \in I$, on peut trouver par le Lemme 10.8 un $q \in \mathrm{H}_\mathbb{Z}$ avec soit $\mathrm{n}(hm^{-1}-q) < 1$, soit $hm^{-1} = q+\omega$. Dans le premier cas, on a $\mathrm{n}(h-qm) < \mathrm{n}(m)$ par multiplicativité de la norme, et aussi $h-qm \in I$, et donc $h = qm$ par minimalité de m. Dans le second cas, on a $h = qm + \omega m$. En particulier, on a montré

$$\mathrm{H}_\mathbb{Z}\, m \subset I \subset \mathrm{H}_\mathbb{Z}\, m \cup (\mathrm{H}_\mathbb{Z} + \omega)\, m.$$

Par hypothèse sur I, la réunion $\mathrm{H}_\mathbb{Z}\, m \cup (\mathrm{H}_\mathbb{Z} + \omega)\, m$ contient donc un élément de norme impaire. Par le (i) du lemme précédent, on en déduit que $\mathrm{n}(m)$ est impair. Mais alors par le (ii) du même lemme, le second cas ci-dessus ne peut se produire pour aucun $h \in I$, car on aurait alors $q \in \mathrm{H}_\mathbb{Z}$ avec $h - qm = \omega m \in \mathrm{H}_\mathbb{Z}$. Ainsi, on est toujours dans le premier cas et on a $I = \mathrm{H}_\mathbb{Z}\, m$. □

Pour utilisation future, mentionnons la proposition suivante, conséquence immédiate de la relation (64), du Lemme 10.6 et de la Proposition 10.5. Bien sûr, un *générateur* d'un idéal I est un élément $q \in I$ avec $I = \mathrm{H}_\mathbb{Z}\, q$.

Proposition 10.10. *Chaque idéal principal non nul de* $\mathrm{H}_\mathbb{Z}$ *possède exactement* 8 *générateurs, associés, et qui sont ses éléments non nuls de plus petite norme.*

Nous sommes maintenant en mesure de démontrer le (i) du Lemme 10.3.

Lemme 10.11. *Soit* $q \in \mathrm{H}_\mathbb{Z}$ *de norme* mn *avec* $m \wedge n = 1$ *et* n *impair. Il existe* $h, h' \in \mathrm{H}_\mathbb{Z}$ *avec* $q = h'h$ *et* $\mathrm{n}(h) = n$. *De plus, si on a* $h'h = z'z$ *avec* $\mathrm{n}(z) = \mathrm{n}(h)$, *il existe un unique* $\xi \in \mathrm{H}_\mathbb{Z}^\times$ *tel que* $z = \xi h$ *et* $z' = h'\xi^{-1}$.

Démonstration — Soit $I = \mathrm{H}_\mathbb{Z}\, q + \mathrm{H}_\mathbb{Z}\, n$. C'est un idéal impair de $\mathrm{H}_\mathbb{Z}$ car il contient n. Il est donc principal, puis de la forme $I = \mathrm{H}_\mathbb{Z}\, h$ avec h standard. Tout élément de I est de norme $\equiv 0 \bmod n$. En effet, pour tout $u, v \in \mathrm{H}_\mathbb{Z}$ on a

$$\mathrm{n}(uq + vn) = \mathrm{n}(u)\mathrm{n}(q) + n\mathrm{tr}(uq\overline{v}) + n^2\mathrm{n}(v) \equiv 0 \bmod n.$$

En particulier, on a $\mathrm{n}(h) \equiv 0 \bmod n$. On a $q \in I = \mathrm{H}_\mathbb{Z}\, h$, donc il existe $h' \in \mathrm{H}_\mathbb{Z}$ avec $q = h'h$. L'égalité $nm = \mathrm{n}(h')\mathrm{n}(h)$ implique alors $\mathrm{n}(h) = n$ car $m \wedge n = 1$.

Montrons enfin l'assertion d'unicité. Pour h comme ci-dessus on peut écrire $h = uq + vn$ avec $u, v \in \mathrm{H}_\mathbb{Z}$. Supposons $q = z'z$ avec $z \in \mathrm{H}_\mathbb{Z}$ de norme n. On a alors $h = uz'z + vz^\star z \in \mathrm{H}_\mathbb{Z} z$ et $\mathrm{n}(h) = \mathrm{n}(z)$, donc $z = \xi h$ pour un unique $\xi \in \mathrm{H}_\mathbb{Z}^\times$ par le Lemme 10.6. On a donc $h'h = z'\xi h$, puis $z' = h'\xi^{-1}$. □

Démonstration — (de Lemme 10.3 (i)) Posons $\mathrm{Q}(n) = \{q \in \mathrm{H}_\mathbb{Z} \,|\, \mathrm{n}(q) = n\}$. On a $|\mathrm{Q}(n)| = \mathrm{r}_4(n) = 8f(n)$. Pour $m, n \geqslant 1$, la multiplication dans $\mathrm{H}_\mathbb{Z}$, $(h', h) \mapsto h$, définit par multiplicativité de la norme une application $\mathrm{Q}(m) \times \mathrm{Q}(n) \to \mathrm{Q}(mn)$. Pour $m \wedge n = 1$, alors soit m soit n est impair ; on peut supposer que c'est n quitte à les échanger. Le Lemme 10.11 montre que cette application est surjective, et que ses fibres ont chacune $|\mathrm{H}_\mathbb{Z}^\times| = 8$ éléments. On a montré $|\mathrm{Q}(m)||\mathrm{Q}(n)| = 8|\mathrm{Q}(mn)|$. □

Remarque 10.12. La Proposition 10.7 ne vaut pas pour les idéaux non impairs. En effet, soit $B \subset \mathrm{H}_{\mathbb{Z}}$ le sous-ensemble des quaternions de norme paire. On a

$$B = \{t + xI + yJ + zK \in \mathrm{H}_{\mathbb{Z}} \mid t + x + y + z \equiv 0 \bmod 2\},$$

car on a $n^2 \equiv n \bmod 2$ pour tout $n \in \mathbb{Z}$. En particulier, B est un *sous-groupe* d'indice 2 de $\mathrm{H}_{\mathbb{Z}}$. C'est alors clairement un idéal bilatère. Mais il n'est pas principal. En effet, B contient les 24 éléments de $\mathrm{H}_{\mathbb{Z}}$ de norme 2, à savoir

$$\pm 1 \pm I, \pm 1 \pm J, \pm 1 \pm K, \pm I \pm J, \pm I \pm K \text{ et } \pm J \pm K.$$

Mais si l'idéal B était principal, il n'aurait que 8 éléments de norme minimale, par la Proposition 10.10. Et en effet, on constate que l'on a

$$(1 + I)(1 - J)^{-1} = \frac{1}{2}(1 + I)(1 + J) = \omega \notin \mathrm{H}_{\mathbb{Z}}^{\times}.$$

Hurwitz a observé que l'on peut remédier à ces problèmes en considérant

$$\mathrm{Hur} := \mathrm{H}_{\mathbb{Z}} + \mathbb{Z}\,\omega$$

(quaternions à coordonnées soit toutes dans $\mathbb{Z}$, soit toutes dans $\frac{1}{2} + \mathbb{Z}$). Il observe que Hur est un sous-anneau de $\mathbb{H}$. Les arguments de cette section montrent immédiatement que tout idéal de Hur est principal (Hurwitz). Nous aurions pu étudier plutôt cet anneau dans cette partie, mais il est un peu moins naturel, et surtout moins commode pour l'étude des sommes de 4 carrés. Ajoutons que l'on a $|\mathrm{Hur}^{\times}| = 24$.

10.3. Quaternions entiers de norme première. Notre but dans cette partie est de montrer que pour tout premier p impair on a $\mathrm{r}_4(p) = 8(p + 1)$.

Lemme 10.13. *Soient p un nombre premier et $q \in \mathrm{H}_{\mathbb{Z}}$. On a*

$$\mathrm{n}(q) = p \iff \mathrm{H}_{\mathbb{Z}}\, p \subsetneq \mathrm{H}_{\mathbb{Z}}\, q \subsetneq \mathrm{H}_{\mathbb{Z}}.$$

Démonstration — La relation $\mathrm{n}(q) = p$ entraîne $p = \overline{q}q \in \mathrm{H}_{\mathbb{Z}}\, q$. On peut donc supposer $\mathrm{H}_{\mathbb{Z}}\, p \subset \mathrm{H}_{\mathbb{Z}}\, q \subset \mathrm{H}_{\mathbb{Z}}$. D'après le Lemme 10.6, on a

$$\mathrm{n}(1) \mid \mathrm{n}(q) \mid \mathrm{n}(p), \quad \text{avec } \mathrm{n}(1) = 1 \text{ et } \mathrm{n}(p) = p^2,$$

et les deux inclusions ci-dessus sont strictes si, et seulement si, les deux divisibilités ci-dessus sont strictes. Comme p est premier, c'est équivalent à $\mathrm{n}(q) = p$. □

D'après le Lemme 10.13 et les Propositions 10.10 et 10.7, il faut donc montrer la :

Proposition 10.14. *Pour p premier impair, il existe exactement $p + 1$ idéaux I de $\mathrm{H}_{\mathbb{Z}}$ vérifiant $\mathrm{H}_{\mathbb{Z}}\, p \subsetneq I \subsetneq \mathrm{H}_{\mathbb{Z}}$.*

Observons que pour $n \in \mathbb{Z}$, l'idéal $\mathrm{H}_{\mathbb{Z}}\, n = n\, \mathrm{H}_{\mathbb{Z}}$ est un idéal *bilatère* de $\mathrm{H}_{\mathbb{Z}}$, car n est central dans $\mathrm{H}_{\mathbb{Z}}$. En particulier, pour p premier on dispose de l'anneau quotient $\mathrm{H}_{\mathbb{Z}}/p\,\mathrm{H}_{\mathbb{Z}}$. D'après la générale Proposition 9.10, les idéaux à gauche de $\mathrm{H}_{\mathbb{Z}}$ contenant p sont en bijection naturelle avec les idéaux à gauche de l'anneau quotient $\mathrm{H}_{\mathbb{Z}}/p\,\mathrm{H}_{\mathbb{Z}}$. Il s'agit donc de monter que cet anneau a exactement $p + 1$ idéaux pour p impair. Il se trouve que cet anneau est familier :

Proposition 10.15. *Pour p premier impair on a un isomorphisme d'anneaux*

$$\mathrm{H}_{\mathbb{Z}}/p\,\mathrm{H}_{\mathbb{Z}} \simeq \mathrm{M}_2(\mathbb{Z}/p\mathbb{Z}).$$

Autrement dit, pour p premier impair, l'anneau $\mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$ peut-être vu comme un anneau de *quaternions modulo* p ! Nous aurons besoin du lemme :

LEMME 10.16. *Soit p premier impair. Il existe $A, B \in \mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$ avec*

$$A^2 = -1_2,\ B^2 = -1_2 \text{ et } AB = -BA.$$

De plus, $1_2, A, B, AB$ est une base du $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel $\mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$.

DÉMONSTRATION — On prend pour $B \in \mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$ la matrice compagnon

$$B = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},$$

qui vérifie $B^2 = -1_2$. Les matrices $A \in \mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$ vérifiant $AB = -BA$ sont les

$$A_{x,y} := \begin{bmatrix} x & y \\ y & -x \end{bmatrix}, \text{ avec } x, y \in \mathbb{Z}/p\mathbb{Z},$$

comme le montre un petit calcul immédiat. On a aussi $A_{x,y}^2 = (x^2 + y^2)1_2$. Or il existe $x, y \in \mathbb{Z}/p\mathbb{Z}$ vérifiant $x^2 + y^2 \equiv -1$. En effet, on sait qu'il existe $\frac{p+1}{2}$ carrés dans $\mathbb{Z}/p\mathbb{Z}$, et donc aussi $\frac{p+1}{2}$ éléments de la forme $-1 - y^2$ avec $y \in \mathbb{Z}/p\mathbb{Z}$, et on conclut car ces $p + 1$ éléments au total ne peuvent être tous distincts. On fixe donc de tels x, y, et on pose $A := A_{x,y}$. Il ne reste qu'à vérifier que $1_2, A, B$ et AB forme nécessairement une famille libre. Mais 1_2 et B sont clairement linéairement indépendantes : on a $AB = -BA$ et $-BA \neq BA$ car $p > 2$. Donc A et AB le sont aussi car A est inversible. On conclut car elles ne sont pas dans le même espace propre de la symétrie $\mathrm{M}_2(\mathbb{Z}/p\mathbb{Z}) \to \mathrm{M}_2(\mathbb{Z}/p\mathbb{Z}), X \mapsto BXB^{-1}$ (car $p > 2$). □

La Proposition 10.15 est maintenant à portée de main.

DÉMONSTRATION — (de la Proposition 10.15) Soit $1_2, A, B, AB$ une base de $\mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$ comme dans la Proposition 10.16. Soit $f : \mathrm{M}_2(\mathbb{Z}/p\mathbb{Z}) \to \mathrm{H}_{\mathbb{Z}}/p\,\mathrm{H}_{\mathbb{Z}}$ l'application $\mathbb{Z}/p\mathbb{Z}$-linéaire envoyant $1_2, A, B, AB$ sur $1, I, J, K$ mod $p\,\mathrm{H}_{\mathbb{Z}}$ respectivement. C'est un isomorphisme de $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel.[8] On a $f(1) = 1$ et il ne reste qu'à montrer que l'on a $f(xy) = f(x)f(y)$ pour tout $x, y \in \mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$. Par bilinéarité, on peut supposer $x, y \in \{1_2, A, B, AB\}$, et même $x, y \neq 1_2$. Mais pour les 9 tels (x, y) restants, cela découle immédiatement des relations correspondantes $I^2 = -1$, $J^2 = -1$ et $IJ = -JI$. □

Il ne reste qu'à rappeler la structure des idéaux de $\mathrm{M}_n(k)$.

PROPOSITION 10.17. *Soient V un espace vectoriel de dimension finie sur un corps k et $A = \mathrm{End}_k(V)$ l'anneau des endomorphismes de V. Pour tout sous-espace $W \subset V$ on note $\mathrm{I}_W \subset A$ l'idéal à gauche des endomorphismes de V s'annulant sur W.*

(i) On a $\mathrm{I}_W = A\,u$ pour tout $u \in A$ de noyau W.

(ii) L'application $W \mapsto \mathrm{I}_W$ est une bijection entre sous-espaces de V et idéaux à gauche de A.

8. Comme $1, I, J, K$ est une $\mathbb{Z}$-base du groupe additif de $\mathrm{H}_{\mathbb{Z}}$, sa réduction modulo $p\mathrm{H}_{\mathbb{Z}}$ est une $\mathbb{Z}/p\mathbb{Z}$-base du groupe abélien p-élémentaire $\mathrm{H}_{\mathbb{Z}}/p\,\mathrm{H}_{\mathbb{Z}}$.

Démonstration — Soit I un idéal à gauche de A. Soient $f_1, \cdots, f_n \in I$ avec $I = \sum_{i=1}^n Af_i$. De tels éléments existent toujours (en nombre fini) car I est de dimension finie comme k-espace vectoriel. Posons $W = \cap_{i=1}^n \ker f_i$. On a clairement $I \subset \mathrm{I}_W$, et nous allons montrer $\mathrm{I}_W = I$. Considérons l'application linéaire

$$f : V \to V^n, x \mapsto (f_1(x), \ldots, f_n(x)).$$

On a $\ker f = W$. Soit $h \in I_W$. Par définition, on a $\ker f \subset \ker h$. Par un énoncé classique de factorisation,[9] il existe une application linéaire $g : V^n \to V$ vérifiant $g \circ f = h$. Mais on peut écrire $g(x_1, x_2, \ldots, x_n) = \sum_{i=1}^n g_i(x_i)$ pour des endomorphismes $g_1, \ldots, g_n$ de V (uniquement déterminés par g). La relation $g \circ f = h$ s'écrit alors $\sum_{i=1}^n g_i f_i = h$ dans A. Comme I est un idéal à gauche, on en déduit $h \in I$, puis $\mathrm{I}_W = I$. Cela montre le (i) (cas $n = 1$), ainsi que la surjectivité dans le (ii). L'assertion d'injectivité du (ii) est une conséquence immédiate du (i). □

Démonstration — (de la Proposition 10.14, et donc de $\mathrm{r}_4(p) = 8(p+1)$) D'après la Proposition 10.16, il faut montrer que $\mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$ possède $p+1$ idéaux à gauche *stricts*. Mais d'après la Proposition 10.17, ces idéaux sont en bijection avec les sous-espaces $0 \subsetneq W \subsetneq (\mathbb{Z}/p\mathbb{Z})^2$, c'est à dire avec les droites de $(\mathbb{Z}/p\mathbb{Z})^2$ (*i.e.* avec $\mathrm{P}^1(\mathbb{Z}/p\mathbb{Z})$). Mais on sait qu'il y a exactement $p+1$ telles droites (par exemple, par le Lemme 5 Chap. 4.1). □

10.4. Factorisation des quaternions de norme puissance d'un premier impair. Soit p un nombre premier impair. Pour démontrer le Lemme 10.3 (ii), nous allons étudier les factorisations des quaternions de norme p^k comme produit de quaternions de norme p. Il faudra particulièrement prendre garde au fait que pour chacun des $8(p+1)$ éléments $\pi \in \mathrm{H}_\mathbb{Z}$ de norme p on a la décomposition

$$p = \pi^\star \pi. \tag{65}$$

Un quaternion $q \in \mathrm{H}_\mathbb{Z}$ sera dit *primitif* s'il n'est pas dans $n\,\mathrm{H}_\mathbb{Z}$ pour $n \in \mathbb{Z}_{>1}$. Si $q \in \mathrm{H}_\mathbb{Z}$ est de la forme nq' avec $q' \in \mathrm{H}_\mathbb{Z}$ et $n \in \mathbb{Z}_{\geqslant 1}$, on a bien sur $n^2 \mid \mathrm{n}(q)$. En particulier, si p est premier un quaternion de norme p est primitif, et un quaternion de norme p^k est non primitif si, et seulement si, il est dans $p\,\mathrm{H}_\mathbb{Z}$.

On a vu au § 10.3 qu'il existe exactement $p+1$ classes d'association d'éléments de norme p dans $\mathrm{H}_\mathbb{Z}$. Nous noterons en général Π un ensemble de représentants de ces classes. Par exemple pour $p = 5$, on peut prendre $\Pi = \{1 \pm 2I, 1 \pm 2J, 1 \pm 2K\}$.

Théorème 10.18. *Soient p premier impair, Π un ensemble de représentants des éléments de norme p de $\mathrm{H}_\mathbb{Z}$ pour $\sim$, et $k \geqslant 1$ entier. Tout quaternion primitif $q \in \mathrm{H}_\mathbb{Z}$ de norme p^k s'écrit de manière unique sous la forme $q = \xi\pi_1 \cdots \pi_k$ avec*

$$\xi \in \mathrm{H}_\mathbb{Z}^\times,\ \pi_i \in \Pi \text{ pour } 1 < i \leqslant k, \text{ et } \pi_{i-1} \not\sim \pi_i^\star \text{ pour } 1 < i \leqslant k.$$

Réciproquement, tout tel produit définit un quaternion primitif de norme p^k.

Nous aurons besoin de plusieurs lemmes pour démontrer ce résultat.

Lemme 10.19. *Soient p premier impair et $q \in \mathrm{H}_\mathbb{Z}$ primitif de norme $\equiv 0 \bmod p$. Alors il existe $\pi \in \mathrm{H}_\mathbb{Z}$ de norme p, unique modulo association, tel que $q \in \mathrm{H}_\mathbb{Z}\,\pi$.*

9. Il suffit d'introduire un supplémentaire S de $\mathrm{Im}\, f$ dans V^n et de poser $g(x) = 0$ pour $x \in S$, et $g(f(x)) = h(x)$ pour $x \in V$. C'est bien défini car pour $x, x' \in V$, on a $f(x) = f(x') \implies x - x' \in \ker f \implies x - x' \in \ker h \implies h(x) = h(x')$. L'application g est trivialement linéaire.

Autrement dit, sous les hypothèses q a un unique diviseur dans Π ! Bien remarquer que ce lemme est faux pour q non primitif, par exemple on a $p \in \mathrm{H}_{\mathbb{Z}}\,\pi$ pour tout $\pi \in \Pi$ par la Formule (65).

Démonstration — Regardons l'idéal $I = \mathrm{H}_{\mathbb{Z}}\,p + \mathrm{H}_{\mathbb{Z}}\,q$ de $\mathrm{H}_{\mathbb{Z}}$. Il est impair car il contient p, il est donc principal, *i.e.* de la forme $I = \mathrm{H}_{\mathbb{Z}}\,\pi$ avec $\pi \in \mathrm{H}_{\mathbb{Z}}$. Mais tout élément de I est de norme $\equiv 0 \bmod p$. En effet, pour tout $h, h' \in \mathrm{H}_{\mathbb{Z}}$ on a

$$\mathrm{n}(hp + h'q) \;=\; p^2\,\mathrm{n}(h) \;+\; \mathrm{n}(q)\mathrm{n}(h') \;+\; p\,\mathrm{tr}(h^\star h'q) \in p\,\mathbb{Z}.$$

On en déduit $\mathrm{n}(\pi) \equiv 0 \bmod p$. Mais I n'est pas inclus dans $\mathrm{H}_{\mathbb{Z}}\,p$ car q est primitif, on a donc une inclusion stricte $\mathrm{H}_{\mathbb{Z}}\,p \subset \mathrm{H}_{\mathbb{Z}}\,\pi$, et donc $\mathrm{n}(\pi)$ est un diviseur strict de $\mathrm{n}(p) = p^2$, c'est donc p. Enfin, si on a $q \in \mathrm{H}_{\mathbb{Z}}\,\pi'$ avec $\mathrm{n}(\pi') = p$, on a $I \subset \mathrm{H}_{\mathbb{Z}}\,\pi'$ puis $\pi \in \mathrm{H}_{\mathbb{Z}}\,\pi'$ et $\pi \sim \pi'$ par le Lemme 10.6. □

Démonstration — (du Théorème 10.18, première partie) Montrons par récurrence sur $k \geqslant 1$ que tout $q \in \mathrm{H}_{\mathbb{Z}}$ primitif de norme p^k est le la forme $\xi\pi_1 \cdots \pi_k$ avec $\xi \in L^\times$ et les $\pi_i \in \Pi$ uniques. Il n'y rien à montrer pour $k = 0$, on suppose donc $k \geqslant 1$. Le lemme montre qu'il existe un unique $\pi \in \Pi$ avec $q \in \mathrm{H}_{\mathbb{Z}}\,\pi$. On a donc $q = q'\pi$ pour $q' \in \mathrm{H}_{\mathbb{Z}}$, nécessairement primitif car q l'est, de norme p^{k-1}. On conclut par récurrence. □

Il reste à montrer la condition portant sur les π_i dans la décomposirtion de q. Le lemme clé (et un peu surprenant !) est le suivant.

Lemme 10.20. *Soient p premier impair et $h, \pi, h' \in \mathrm{H}_{\mathbb{Z}}$ avec $\mathrm{n}(\pi) = p$. On a*

$$h\pi h' \in p\,\mathrm{H}_{\mathbb{Z}} \iff h\pi \in p\,\mathrm{H}_{\mathbb{Z}} \text{ ou } \pi h' \in p\,\mathrm{H}_{\mathbb{Z}}.$$

Démonstration — Fixons un morphisme surjectif d'anneaux $f : \mathrm{Hur} \to \mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$ de noyau $p\mathrm{Hur}$ comme dans la Proposition. La relation $p = \pi\overline{\pi}$ dans Hur donne $0 = f(\pi)f(\overline{\pi})$ dans $\mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$. Mais ni $f(\pi)$, ni $f(\overline{\pi})$ n'est nul car $\pi, \overline{\pi} \notin p\mathrm{Hur}$ (sinon la norme de π serait multiple de p^2). Donc $X := f(\pi)$ est une matrice de rang 1. Posons $H = f(h)$ et $H' = f(h')$. On a H, X, H' dans $\mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$ avec X de rang 1. Supposons $XH' \neq 0$. Comme on est en dimension 2, XH' est aussi de rang 1 avec même image que X. Mais alors $\mathrm{Im}\,HXH' = \mathrm{Im}\,HX$, et donc HXH' est nul si, et seulement si, HX est nul. □

Corollaire 10.21. *Soient p premier impair et $\pi_1, \pi_2, \ldots, \pi_k \in \mathrm{H}_{\mathbb{Z}}$ avec $\mathrm{n}(\pi_i) = p$ pour tout i et $\pi_1\pi_2 \cdots \pi_k \in p\,\mathrm{H}_{\mathbb{Z}}$. Alors il existe $1 \leqslant i < k$ tel que $\pi_i\pi_{i+1} \in p\,\mathrm{H}_{\mathbb{Z}}$.*

Démonstration — Par récurrence sur l'entier $k \geqslant 1$, les cas $k = 1, 2$ étant évidents. Soit $h = \pi_1\pi_2 \cdots \pi_{k-2}$. Si $h\pi_{k-1}$ est dans $p\,\mathrm{H}_{\mathbb{Z}}$ on conclut par récurrence. Sinon, on applique le lemme précédent à h, $\pi = \pi_{k-1}$ et $h' = \pi_k$, et on en déduit $\pi_{k-1}\pi_k \in p\,\mathrm{H}_{\mathbb{Z}}$. □

Démonstration — (fin de la preuve du Théorème 10.18) Les assertions restantes résultent du Corollaire 10.21 et de la remarque suivante. □

Remarque 10.22. *Soient $\pi, \pi' \in \mathrm{H}_{\mathbb{Z}}$ de norme p. La condition $\pi'\pi \in p\,\mathrm{H}_{\mathbb{Z}}$ signifie $\pi'\pi = p\,\xi$ pour un certain $\xi \in \mathrm{H}_{\mathbb{Z}}$ de norme 1, i.e. $\xi \in \mathrm{H}_{\mathbb{Z}}^{\times}$, soit encore $\pi' = \xi\pi^{\star}$ en multipliant à droite par $\pi^{\star}$. Autrement dit, on a $\pi'\pi \in p\,\mathrm{H}_{\mathbb{Z}} \iff \pi' \sim \pi^{\star}$.*

En guise d'application, nous obtenons le corollaire suivant, qui entraîne le Lemme 10.3 (ii) et termine donc la démonstration du théorème de Jacobi.

Corollaire 10.23. *Pour p premier impair et si $k \geqslant 1$, il existe exactement $8(1 + p + \cdots + p^k)$ éléments de $\mathrm{H}_{\mathbb{Z}}$ de norme p^k.*

Démonstration — Notons $\mathrm{a}_k(p)$ le nombre de quaternions *primitifs* de norme p^m. On a déja vu $\mathrm{a}_0(p) = 8$ et $\mathrm{a}_1(p) = 8(p+1)$. D'après le Théorème 10.18 et la remarque qui le suit, on a $\mathrm{a}_k(p) = 8(p+1)p^{k-1} = 8(p^k + p^{k-1})$. En effet, il y a $p + 1 = |\Pi|$ pour l'élément π_k, p choix pour l'élément π_{k-1} (un élément de Π non associé à $\pi_k^{\star}$), p choix pour π_{k-2} (un élément de Π non associé à $\pi_{k-1}^{\star}$), $\cdots$, et enfin 8 choix pour l'unité. Mais tout quaternion de norme p^k s'écrit de manière unique sous la forme $p^m q$ avec $0 \leqslant n \leqslant k/2$ et q primitif de norme $k - 2n$. Le nombre cherché est donc $\mathrm{a}_k(p) + \mathrm{a}_{k-2}(p) + \ldots$ qui est bien le nombre donné ! $\square$

10.5. Une application à la construction de sous-groupes libres de $\mathrm{SO}(3)$.

.

On se propose d'utiliser l'arithmétique de $\mathrm{H}_{\mathbb{Z}}$ pour démonter le théorème suivant. On rappelle que F_n le groupe libre sur $n \geqslant 1$ générateurs (§ 8 Chap. 2).

Théorème 10.24. *Pour tout entier $n \geqslant 1$, le groupe $\mathrm{SO}(3)$ possède un sous-groupe isomorphe à F_n.*

Cet énoncé, pour $n = 2$, est par exemple l'un des ingrédients clés pour démontrer le fameux *paradoxe de Banach-Tarski*, pour lequel nous renvoyons à ce court exposé de T. Tao. On rappelle que l'on a un morphisme de groupes

$$f : \mathbb{H}^{\times} \longrightarrow \mathrm{SO}(3),$$

associant à $h \in \mathbb{H}^{\times}$ la matrice de l'isométrie int_h de l'espace euclidien des quaternions purs dans la base orthonormée I, J, K (§2 Chap. 5). On a montré *loc. cit.* que f est surjectif de noyau $\mathbb{R}^{\times}$.

Lemme 10.25. *Soient p premier impair et $\pi_1, \pi_2, \ldots, \pi_n \in \mathrm{H}_{\mathbb{Z}}$ de norme p. On suppose que les $2n$ éléments $\pi_1, \pi_1^*, \pi_2, \pi_2^*, \ldots, \pi_n, \pi_n^*$ sont deux à deux non associés. Alors $f(\pi_1), f(\pi_2), \ldots, f(\pi_n)$ engendrent un sous-groupe de $\mathrm{SO}(3)$ isomorphe à F_n.*

Démonstration — Posons $S = \{\pi_1, \pi_1^{\star}, \ldots, \pi_n, \pi_n^{\star}\}$. Pour tout $s \in S$ on a $ss^{\star} = p$ dans $\mathbb{H}^{\times}$, et donc $f(s^{\star}) = f(s)^{-1}$. Soient $k \geqslant 1$ et $m_1, m_2, \ldots, m_k \in S$ avec $m_{i-1} \neq m_i^{\star}$ pour tout $1 < i \leqslant k$. Il faut montrer $f(m_1)f(m_2)\cdots f(m_k) \neq 1$ dans $\mathrm{SO}(3)$. Posons $m = m_1 m_2 \cdots m_k \in \mathrm{H}_{\mathbb{Z}}$ et supposons donc par l'absurde $f(m) = 1$, ou ce qui revient au même $m \in \mathbb{R}^{\times} = \ker f$. On a donc $m \in \mathrm{H}_{\mathbb{Z}} \cap \mathbb{R} = \mathbb{Z}$, et aussi $\mathrm{n}(m) = \prod_{i=1}^{k} \mathrm{n}(\pi_i) = p^k$. On en déduit $m = \pm p^{k/2}$, $k \equiv 0 \bmod 2$, et en particulier, $m \in p\,\mathrm{H}_{\mathbb{Z}}$. Le Corollaire 10.21 et la Remarque 10.22 entraînent donc qu'il existe $1 < i \leqslant k$ avec $m_{i-1} \sim m_i^*$. Cela contredit notre hypothèse $m_{i-1} \neq m_i^*$, car on a $s \not\sim s'$ pour s, s' distincts dans S. $\square$

Il existe bien d'autres méthodes pour construire des sous-groupes libres de SO(3). L'un des charmes de celle-ci est qu'elle produit des exemples explicites de matrices à petits coefficients, comme le montrent les deux exemples ci-dessous.

EXEMPLE 10.26. *Pour $p = 3$, on constate aisément*[10] *que les deux éléments $\pi_1 = 1 + I + J$ et $\pi_2 = 1 + I - J$ vérifient l'hypothèse du Lemme 10.25. Un simple calcul montre que l'on a*

$$f(\pi_1) = \frac{1}{3}\begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & -2 \\ -2 & 2 & -1 \end{bmatrix} \quad \text{et} \quad f(\pi_2) = \frac{1}{3}\begin{bmatrix} 1 & -2 & -2 \\ -2 & 1 & -2 \\ 2 & 2 & -1 \end{bmatrix}.$$

Ces deux matrices engendrent donc un sous-groupe de SO(3) *isomorphe à* F_2.

Notons que les éléments π_1 et π_2 ci-dessus ont été bien choisis ! Par exemple, les éléments $\pi_1' = K\pi_1 = -I + J + K$ et $\pi_2' = K\pi_2 = -I - J - K$, bien qu'associés respectivement à π_1 et π_2, ne conviennent pas : pour $\pi = \pi_1'$ ou π_2' on a même $\pi^* = -\pi$ et donc $f(\pi)^2 = 1$. Donnons un second exemple.

EXEMPLE 10.27. *Pour $p = 5$, les éléments $\pi_1 = 1+2I$, $\pi_2 = 1+2J$ et $\pi_3 = 1+2K$ vérifient l'hypothèse du Lemme 10.25. On en déduit que les* 3 *rotations*

$$f(\pi_1) = \frac{1}{5}\begin{bmatrix} 5 & 0 & 0 \\ 0 & -3 & -4 \\ 0 & 4 & -3 \end{bmatrix}, \; f(\pi_2) = \frac{1}{5}\begin{bmatrix} -3 & 0 & 4 \\ 0 & 5 & 0 \\ -4 & 0 & -3 \end{bmatrix} \quad \text{et} \quad f(\pi_3) = \frac{1}{5}\begin{bmatrix} -3 & -4 & 0 \\ 4 & -3 & 0 \\ 0 & 0 & 5 \end{bmatrix}$$

engendrent un sous-groupe de SO(3) *isomorphe à* F_3. *Autrement dit, on a montré que « trois rotations de $\mathbb{R}^3$ d'axes deux à deux orthogonaux et d'angles* $\arccos(-3/5)$ *engendrent un groupe libre isomorphe à* F_3 *».*

Terminons enfin la démonstration du Théorème 10.24.

DÉMONSTRATION — (du Théorème 10.24). Soit p un nombre premier avec $p \equiv 1 \bmod 4$. Soit Π l'ensemble des éléments de norme p de $\mathrm{H}_{\mathbb{Z}}$ dont le coefficient en 1 dans la base $1, I, J, K$ est impair et > 0. Observons que Π est un système de représentants des éléments de norme p de $\mathrm{H}_{\mathbb{Z}}$ pour $\sim$. En effet, si on a $(x_i) \in \mathbb{Z}^4$ avec $p = x_1^2+x_2^2+x_3^2+x_4^2$ on constate par réduction modulo 4 que un, et un seul, des x_i est impair. Ainsi, tout $\pi \in \mathrm{H}_{\mathbb{Z}}$ de norme p a un unique associé dans Π.

L'involution $\pi \mapsto \pi^\star$ préserve Π. Elle est sans point fixe, car si on a $\pi = \pi^\star$ alors π est dans $\mathbb{Z}$ puis $p = \mathrm{n}(\pi)$ est un carré : absude. Ainsi, si n est un entier $\leqslant \frac{p+1}{2}$, on peut trouver $\pi_1, \ldots, \pi_n$ dans Π tels que les $2n$ éléments $\pi_1, \pi_1^*, \ldots, \pi_n, \pi_n^*$ sont distincts et dans Π, donc deux à deux non associés. On conclut alors par le Lemme 10.25 et le classique Lemme 10.28 (il existe des premiers $\equiv 1 \bmod 4$ arbitrairement grands !). $\square$

LEMME 10.28. *Il existe une infinité de nombres premiers* $\equiv 1 \bmod 4$.

DÉMONSTRATION — Supposons qu'il n'y en ait qu'un nombre fini $p_1, \ldots, p_n$. Considérons l'entier $N = 4(p_1p_2\cdots p_n)^2 + 1$. Il est > 1 et donc admet un diviseur premier p. On a $(2p_1\cdots p_n)^2 \equiv -1 \bmod p$. En particulier, p est impair, distinct des p_i, et -1 est un carré modulo p. Par Euler (Exemple 5.8 Chap. 2), on sait que cette dernière propriété entraîne $p \equiv 1 \bmod 4$: une contradiction. $\square$

10. Soient $X = \{\pi_1, \pi_2, \pi_1^\star, \pi_2^\star\}$ et $Y := X \cup -X$. L'ensemble Y a 8 éléments et coïncide avec $\{\pm 1 \pm I \pm J\}$. Pour $\xi \in \mathrm{H}_{\mathbb{Z}}^\times$ on constate $\xi Y \cap Y \neq \varnothing \iff \xi = \pm 1$. On conclut car $X \cap -X = \varnothing$.

Les constructions ci-dessus jouent un rôle important dans les travaux de Lubotsky, Philllips et Sarnak sur les distributions *uniformes* de points sur la sphère S^2 et les *graphes de Ramanujan.* [11] Ce sont des cas particuliers de *groupes arithmétiques*, très étudiés en géométrie et théorie des nombres.

11. A. Lubotsky, R. Philllips et P. Sarnak, *Ramanujan graphs*, Combinatorica 8 (1988), 261–277.

11. Exercices

On commence par quelques exercices sur les entiers de Gauss.

EXERCICE 7.1. *Factoriser* $-3+15i$ *et* $4+7i$ *en irréductibles dans* $\mathbb{Z}[i]$.

EXERCICE 7.2. *Trouver tous les* $(x,y)\in\mathbb{Z}^2$ *avec* $y^2=x^3-1$.

EXERCICE 7.3. (Un choix de représentants des irréductibles de $\mathbb{Z}[i]$)

(i) Montrer que l'idéal $(2+2i)$ *de* $\mathbb{Z}[i]$ *admet pour* $\mathbb{Z}$*-base* $4, 2(1+i)$.

(ii) En déduire un isomorphisme de groupes abéliens bien défini

$$\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\xrightarrow{\sim}\mathbb{Z}[i]/(2+2i),\ (\overline{a},\overline{b})\mapsto\overline{a+bi}.$$

À quelle condition sur $a,b\in\mathbb{Z}$ *a-t-on* $a+bi\equiv 3 \bmod 2+2i$ *?*

(iii) On munit $A:=\mathbb{Z}[i]/(2+2i)\mathbb{Z}[i]$ *de sa structure d'anneau quotient. Montrer que l'application naturelle* $\mathbb{Z}[i]^\times\to A^\times$ *est un isomorphisme de groupes.*

(iv) Montrer que l'ensemble des irréductibles de $\mathbb{Z}[i]$ *de la forme* $1+i$*, ou congrus à* 3 *modulo* $2+2i$*, est un système de représentants de tous les irréductibles.*

Dans l'exercice suivant, on dira qu'une fonction $f:\mathbb{N}_{\geqslant 1}\to\mathbb{C}$ est *arithmétiquement multiplicative* si on a $f(mn)=f(m)f(n)$ pour $m,n\geqslant 1$ avec $m\wedge n=1$.

EXERCICE 7.4. *Pour* n *un entier* $\geqslant 1$ *on pose* $\Sigma_n=\{(a,b)\in\mathbb{Z}^2\mid n=a^2+b^2\}$. *On se propose de montrer* $|\Sigma_n|=4(\mathrm{d}_1(n)-\mathrm{d}_3(n))$*, où* $\mathrm{d}_i(n)$ *désigne le nombre de diviseurs* $d\geqslant 1$ *de* n *vérifiant* $d\equiv i \bmod 4$.

(i) Montrer que l'on a $\Sigma_n\neq\varnothing$ *si, et seulement si, on a* $\mathrm{v}_p(n)\equiv 0 \bmod 2$ *pour tout facteur premier* p *de* n *avec* $p\equiv 3 \bmod 4$.

(ii) Montrer que les deux fonctions $n\mapsto\frac{1}{4}|\Sigma_n|$ *et* $n\mapsto\mathrm{d}_1(n)-\mathrm{d}_3(n)$ *sont arithmétiquement multiplicatives.*

(iii) Conclure.

On s'intéresse maintenant aux anneaux $\mathbb{Z}[\sqrt{d}]$ généraux.

EXERCICE 7.5. *On se propose de montrer que l'anneau* $\mathbb{Z}[\sqrt{d}]$ *est non principal pour* $d<-2$. *On pose* $\alpha=\sqrt{d}$ *si* d *est pair,* $\alpha=1+\sqrt{d}$ *sinon.*

(i) Traiter directement les cas $d=-3,-4$.

(ii) Montrer $(2,\alpha)=2\mathbb{Z}+\alpha\mathbb{Z}$.

(iii) Montrer que pour $d<-4$*, les éléments de* $\mathbb{Z}[\sqrt{d}]$ *de norme* $\leqslant 4$ *sont* $\pm1,\pm2$.

(iv) En déduire que l'idéal $(2,\alpha)$ *n'est pas principal.*

EXERCICE 7.6. (Noethérianité de $\mathbb{Z}[\sqrt{d}]$) *Soient* $d\in\mathbb{Z}$ *non carré et* $A=\mathbb{Z}[\sqrt{d}]$.

(i) Montrer que tout idéal non nul I *de* A *contient un entier* $n\in\mathbb{Z}_{>0}$.

(ii) Montrer qu'il n'y a qu'un nombre fini d'idéaux de A *contenant un entier* $n\in\mathbb{Z}_{>0}$ *donné.*

(iii) Montrer que A *est noethérien, et que tout idéal non nul y est d'indice fini.*

(iv) Montrer que A n'a qu'un nombre fini d'idéaux principaux zA avec $\mathrm{N}(z)$ fixé.

Exercice 7.7. (Unités de $\mathbb{Z}[\sqrt{d}]$ avec $d > 0$) *Soit $d > 0$ un entier non carré. On se propose de montrer que $\mathbb{Z}[\sqrt{d}]^\times$ est infini.*

(i) Montrer que pour tout $\alpha \in \mathbb{R}$, et tout entier $N \geqslant 1$, il existe $p \in \mathbb{Z}$ et $1 \leqslant q \leqslant N$ tels que $|p - q\alpha| < 1/N$ (principe de Dirichlet).

(ii) Montrer qu'il existe une suite d'éléments $x_n \in \mathbb{Z}[\sqrt{d}]$ non nuls avec $x_n \to 0$ dans $\mathbb{R}$ et $(\mathrm{N}(x_n))_{n\geqslant 1}$ bornée.

(iii) (suite) Montrer que quitte à extraire une sous-suite de x_n, on peut supposer qu'il existe $k \in \mathbb{Z}$ tel que $\mathrm{N}(x_n) = k$ et $x_n\overline{x_m} \in k\mathbb{Z}[\sqrt{d}]$, pour tout $n, m \geqslant 1$.

(iv) Conclure.

Exercice 7.8. *(i) Soient (a, b) et $(c, d) \in \mathbb{Z}^2$ avec $ad - bc$ non nul. Montrer que le sous-groupe de $\mathbb{Z}^2$ qu'ils engendrent est d'indice fini, égal à $|ad - bc|$.*

(ii) Soit $d \in \mathbb{Z}$ non carré, $A = \mathbb{Z}[\sqrt{d}]$ et $z \in A$ non nul. Montrer que le groupe additif quotient A/zA est fini de cardinal $|\mathrm{N}(z)|$.

Dans les deux exercices suivants, on se propose d'examiner les idéaux d'une poignée de $\mathbb{Z}[\sqrt{d}]$ non principaux. Si A est un anneau commutatif intègre, et si I et J sont deux idéaux non nuls de A, on dira que I et J sont *équivalents*, et on notera $I \sim J$, s'il existe $a, b \in A \smallsetminus \{0\}$ avec $aI = bJ$. C'est clairement une relation d'équivalence sur les idéaux non nuls de A, dont on notera $\mathrm{Cl}(A)$ l'ensemble des classes.

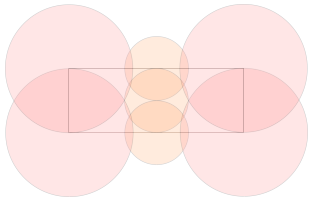
Exercice 7.9. *Soit A un anneau commutatif intègre.*

(i) Montrer qu'un idéal non nul de A est principal si, et seulement si, il est équivalent à A.

(ii) En déduire que A est principal si, et seulement si, on a $|\mathrm{Cl}(A)| = 1$.

Exercice 7.10. *On considère $A = \mathbb{Z}[\sqrt{d}]$ avec $-7 \leqslant d \leqslant -3$.*

(i) Soit $t \in \mathbb{R}$ avec $0 < t < 1+\sqrt{3}$. En observant la figure ci-dessous, montrer que pour tout $z \in \mathbb{C}$, il existe $v \in \mathbb{Z}+\mathbb{Z}\,it$ avec soit $|z-v| < 1$, soit $|z-v/2| < 1/2$.



(ii) En déduire que pour tout $a, b \in A$ avec $b \neq 0$, il existe des éléments $q, r \in A$ avec $\mathrm{N}(r) < \mathrm{N}(b)$ et soit $a = qb + r$, soit $2a = qb + r$.

(iii) Montrer que tout idéal non nul de A est équivalent à un idéal contenant $2A$.

(iv) Montrer que les idéaux de A contenant $2A$ sont $2A$, J et A, où J est l'idéal $(2, \alpha)$ introduit à l'Exercice 7.5.

(v) (suite) Démontrer $\mathrm{Cl}(A) = \{[A], [J]\}$ et que J est non équivalent à A.

Les exercices qui suivent introduisent une variante importante des anneaux $\mathbb{Z}[\sqrt{d}]$. Dans le premier, on utilisera à profit l'identité suivante, valable pour $x, y \in \mathbb{R}$:

$$|x - jy|^2 = x^2 + xy + y^2 = \frac{1}{4}\left((2x+y)^2 + 3y^2\right).$$

Exercice 7.11. (Entiers d'Eisenstein) *On pose* $j = e^{2i\pi/3}$ *et* $\mathbb{Z}[j] = \mathbb{Z} + \mathbb{Z}j$.

(i) Montrer que $\mathbb{Z}[j]$ *est un sous-anneau de* $\mathbb{C}$.

(ii) Montrer $\mathbb{Z}[j]^\times = \{\pm 1, \pm j, \pm j^2\} = \mu_6$.

(iii) Montrer que $\mathbb{Z}[j]$ *est euclidien pour* $z \mapsto |z|^2$.

(iv) Soit p *un nombre premier* $\equiv 1 \bmod 3$. *Montrer que l'on a* $p = \pi\overline{\pi}$ *avec* π *et* $\overline{\pi}$ *des irréductibles non associés de* $\mathbb{Z}[j]$.

(v) (suite) En déduire qu'il existe exactement 12 *couples* $(a, b) \in \mathbb{Z}^2$ *tels que* $p = a^2 + ab + b^2$.

(vi) (suite) Retrouver qu'il existe un unique $(a, b) \in \mathbb{N}^2$ *avec* $p = a^2 + 3b^2$.

Pour $d \in \mathbb{Z}$ non carré et $d \equiv 1 \bmod 4$, on pose

$$\tau_d = \frac{1+\sqrt{d}}{2} \quad \text{et} \quad \mathrm{A}_d = \mathbb{Z} + \mathbb{Z}\tau_d \subset \mathbb{Q}[\sqrt{d}].$$

La relation $\tau_d^2 = \tau_d + \frac{d-1}{4} \in \mathbb{Z} + \mathbb{Z}\,\tau_d$ montre que c'est un sous-anneau de $\mathbb{Q}[\sqrt{d}]$ contenant strictement $\mathbb{Z}[\sqrt{d}]$. Par exemple, on a $\tau_{-3} = e^{2i\pi/6} = -j^2$ et donc $\mathrm{A}_{-3} = \mathbb{Z}[j]$ est l'anneau des entiers d'Eisenstein (Exercice 7.11). On a aussi $\overline{\tau_d} = \frac{1-\sqrt{d}}{2} = 1 - \tau_d \in \mathbb{Z}[\sqrt{d}]$, de sorte que $z \mapsto \overline{z}$ préserve A_d, et pour $x, y \in \mathbb{Q}$, on a enfin

$$\mathrm{N}(x + y\,\tau_d) = x^2 + xy + \frac{1-d}{4}\,y^2,$$

et en particulier $\mathrm{N}(\mathrm{A}_d) \subset \mathbb{Z}$.

Exercice 7.12. *(i) Montrer* $\mathrm{A}_d^\times = \{z \in \mathrm{A}_d \mid \mathrm{N}(z) = \pm 1\}$ *puis* $\mathrm{A}_{-3}^\times = \mu_6$ *et* $\mathrm{A}_d^\times = \{\pm 1\}$ *pour* $d < -3$.

(ii) Montrer que les résultats de l'Exercice 7.8 (ii) et de l'Exercice 7.6 sont encore vrais pour $A = \mathrm{A}_d$.

Exercice 7.13. *Montrer que* A_{-3}, A_{-7} *et* A_{-11} *sont euclidiens pour* N.

Exercice 7.14. *On se propose de montrer que l'anneau* A_{-19} *est principal.*

(i) Montrer que pour tout $a, b \in \mathrm{A}_{-19}$ *on a soit* $a = bq + r$ *avec* $\mathrm{N}(r) < \mathrm{N}(b)$, *soit* $2a = bq + r$ *avec* $\mathrm{N}(r) < \mathrm{N}(b)$.

(ii) Montrer que les seuls idéaux de A_{-19} *contenant* 2 *sont* A_{-19} *et* $2\,\mathrm{A}_{-19}$.

(iii) En déduire que A_{-19} *est principal.*

On peut montrer que A_d est encore principal pour $d = -43, -67$ et -163.

Exercice 7.15. *On se propose de montrer, suivant Samuel, que* A_d *n'est pas euclidien pour* $d < -11$ *(et ce quelque soit le stathme).*

(i) Soit A un anneau euclidien qui n'est pas un corps. Montrer qu'il existe $x \in A$ non zero ou unité, tel que l'application naturelle $\{0\} \cup A^\times \to A/xA$ est surjective.

(ii) Montrer que pour $d < -11$, A_d ne possède aucun élément de norme 2 ou 3.

(iii) Conclure (on utilisera les résultats de l'Exercice 7.12).

Ainsi, A_{-19} est un anneau principal non euclidien. Les deux exercices suivants examinent les notions de pgcd et ppcm.

Exercice 7.16. (Pgcd et ppcm, généralités) *Soient A intègre et $a, b, c \in A \smallsetminus \{0\}$.*

(i) Montrer $(a) \cap (b) = (c)$ si, et seulement si, c est un ppcm de a et b.

(ii) On suppose a premier et $a \nmid b$. Montrer que ab est un ppcm de a et b.

(iii) On suppose $(a) + (b) = (c)$. Montrer que c est un pgcd de a et b.

Exercice 7.17. (Pgcd et ppcm, exemples et contre-exemples) *On se place dans l'anneau $\mathbb{Z}[\sqrt{-5}]$.*

(i) Montrer que 2 et $1 + \sqrt{-5}$ admettent un pgcd.

(ii) Montrer que 2 et $1 + \sqrt{-5}$ n'admettent pas de ppcm.

(iii) Montrer que $3(1+\sqrt{-5})$ et $3(1-\sqrt{-5}) = (1+\sqrt{-5})(-2-\sqrt{-5})$ n'admettent pas de pgcd.

(iv) Montrer que l'idéal $I = (2, 1 + \sqrt{-5})$ admet pour $\mathbb{Z}$-base $2, 1 + \sqrt{-5}$.

(v) (suite) Montrer que I n'est pas principal, puis que la réciproque du (iii) de l'exercice précédent est fausse.

On poursuit par quelques exercices généraux sur les anneaux principaux et factoriels.

Exercice 7.18. *Soit A le sous-anneau des fonctions $\mathbb{R} \to \mathbb{R}$ de la forme $t \mapsto P(\cos t, \sin t)$ avec $P \in \mathbb{R}[X, Y]$ (justifier).*

(i) Montrer que A est un anneau intègre.

(ii) Montrer que les éléments $\cos t$ et $\sin t$ sont irréductibles dans A.

(iii) Montrer que A n'est pas factoriel.

Exercice 7.19. *(i) Montrer que si k est un corps, l'idéal (X, Y) de $k[X, Y]$ n'est pas principal.*

(ii) Montrer de même que $\mathbb{Z}[X]$ n'est pas principal.

Exercice 7.20. (Lemme du contenu de Gauss) *Soit A un anneau factoriel de corps de fractions K. Si $P \in A[X]$ est non nul, on note $\mathrm{c}(P)$ le pgcd des coefficients de P, c'est un élément de A bien défini aux unités près. On dit que P est primitif si $\mathrm{c}(P)$ est une unité.*

(i) Montrer $A[X]^\times = A^\times$.

(ii) Montrer que si $P, Q \in A[X]$ sont primitifs alors PQ est primitif.

(iii) En déduire que si $P, Q \in A[X]$ sont non nuls, on a $\mathrm{c}(PQ) = \mathrm{c}(P)\mathrm{c}(Q)$ (aux unités près).

(iv) Montrer que si $P \in A[X]$ est non constant, alors P est irréductible dans $A[X]$ si et seulement si $\mathrm{c}(P) = 1$ et P est irréductible dans $K[X]$.

(v) En déduire que les irréductibles de $A[X]$ sont les irréductibles de A et les polynômes primitifs non constant.

(vi) Montrer que $A[X]$ est factoriel.

(vii) En déduire que $\mathbb{Z}[X_1, \ldots, X_n]$ et $k[X_1, \ldots, X_n]$ sont factoriels si $n \geqslant 1$ et si k est un corps.

Il est mieux d'avoir suivi un cours de fonctions d'une variable complexe avant de traiter l'exercice suivant.

Exercice 7.21. *Soit A l'anneau des séries entières $\sum_{n\geqslant 0} a_n z^n$, à coefficients a_n dans $\mathbb{C}$ et de rayon de convergence infini.*

(i) Montrer que A est intègre.

(ii) Montrer que les unités de A sont exactement les fonctions $f \in A$ telles que $f(z) \neq 0$ pour tout $z \in \mathbb{C}$.

(iii) Montrer que les irréductibles de A sont, aux unités près, les $z - a$ avec $a \in \mathbb{C}$.

(iv) En déduire que A n'a pas la propriété de factorisation (en particulier, A n'est pas noethérien).

Exercice 7.22. *Soient k un corps et $k[[X]]$ l'anneau des séries formelles $\sum_{n\geqslant 0} a_n X^n$ à coefficients $a_n \in k$ pour tout $n \geqslant 0$.*

(i) Expliquer pourquoi une définition possible de l'anneau $k[[X]]$ est de considérer les fonctions $a : \mathbb{N} \to k$ munies du produit de convolution

$$(a \star b)(n) = \sum_{0\leqslant p\leqslant n} a(p)b(n-p).$$

(ii) Montrer qu'une série formelle $f = \sum_{n\geqslant 0} a_n X^n$ est inversible dans $k[[X]]$ si, et seulement si, on a $a_0 \neq 0$.

(iii) Montrer que X est l'unique irréductible de $k[[X]]$, modulo association.

(iv) Montrer que pour tout $f \in k[[X]]$ non nul, il existe un unique entier $n \geqslant 0$ (appelé valuation *de f) et un unique $u \in k[[X]]^\times$ tels que $f = X^n u$.*

(v) En déduire que $k[[X]]$ est principal.

(vi) Montrer que la valuation est un stathme euclidien sur $k[[X]]$.

Les deux exercices suivants introduisent la notion d'anneau *intégralement clos*. Soit A un anneau intègre de corps de fractions K. On note $\widetilde{A}$ l'ensemble des éléments $x \in K$ tels qu'il existe $P \in A[X]$ unitaire avec $P(x) = 0$. On a clairement $A \subset \widetilde{A}$ (considérer les $X - a$ avec $a \in A$). On dit que A est intégralement clos si on a $A = \widetilde{A}$.

Exercice 7.23. *Montrer qu'un anneau factoriel est intégralement clos.*

Exercice 7.24. (Exemples et contre-exemples d'anneaux intégralement clos)

(i) Montrer[12] *que si* $\mathbb{Z}[\sqrt{d}]$ *est intégralement clos, alors* d *est sans facteur carré et on a* $d \equiv 2, 3 \bmod 4$.

(ii) Soient k *un corps et* A *le sous-anneau des* $P \in k[X]$ *vérifiant* $P(0) = P(1)$ *(justifier). Montrer que* A *n'est pas intégralement clos.*

(iii) Soient k *un corps et* A *le sous-anneau des* $P \in k[X]$ *vérifiant* $P'(0) = 0$ *(justifier). Montrer que* A *n'est pas intégralement clos.*

On termine par quelques exercices sur les anneaux euclidiens.

Exercice 7.25. (Deux (autres) stathmes euclidiens sur $\mathbb{Z}$). *Montrer que les deux fonctions suivantes* $\varphi : \mathbb{Z} \to \mathbb{N}$ *définissent des stathmes euclidiens sur* $\mathbb{Z}$ *:*

(i) $\varphi(n) = |n|$ *si* n *est pair,* $\varphi(n) = \frac{|n|-1}{2}$ *sinon.*

(ii) (Samuel) $\varphi(n) = |n|$ *si* $n \neq 2$*, et* $\varphi(2)$ *est un entier arbitraire* $\geqslant 2$.

Les deux exercices suivants exposent quelques uns des résultats de Mozkin[13] et Samuel[14] sur les anneaux euclidiens.

Exercice 7.26. *Un stathme euclidien* $\varphi : A\backslash\{0\} \to \mathbb{N}$ *est dit* fort *s'il satisfait de plus : si* $a, b \neq 0$ *et si* b *divise* a *alors* $\varphi(b) \leqslant \varphi(a)$.

(i) Donner des exemples de stathmes forts, et des exemples qui ne le sont pas.

(ii) Montrer que tout anneau euclidien admet un stathme euclidien fort (Motzkin)*. Un stathme euclidien* φ *étant donné on pourra considérer*

$$\varphi'(a) \;=\; \inf_{y \in aA} \varphi(y).$$

Exercice 7.27. (Caractérisation de Motzkin-Samuel des anneaux euclidiens). *Soit* A *un anneau*[15]*. On définit par récurrence une suite de sous-ensembles* $\{\mathrm{E}_n(A)\}_{n\geqslant 0}$ *de* A *en posant* $\mathrm{E}_0(A) = \varnothing$, $\mathrm{E}'_n(A) = \mathrm{E}_n(A) \cup \{0\}$ *et*

$$\mathrm{E}_{n+1}(A) = \{a \in A \mid aA + \mathrm{E}'_n(A) = A\}.$$

On pose aussi $\mathrm{Eucl}(A) = \bigcup_{n\geqslant 0} \mathrm{E}_n(A)$*, et pour* $a \in \mathrm{Eucl}(A)$ *on note* $\upsilon(a)$ *le plus petit entier* $n \geqslant 0$ *vérifiant* $a \in \mathrm{E}_{n+1}(A)$.

(i) Déterminer $\mathrm{E}_n(\mathbb{Z})$ *pour tout entier* $n \geqslant 1$*, ainsi que* υ.

(ii) Pour k *un corps, déterminer* $\mathrm{E}_n(k[X])$ *pour tout entier* $n \geqslant 1$*, ainsi que* υ.

(iii) Montrer $\mathrm{E}_1(A) = A^\times$ *et que* $\{\mathrm{E}_n(A)\}_{n\geqslant 0}$ *est croissante pour l'inclusion.*

(iv) On suppose A *euclidien pour le stathme* φ*. Montrer* $\upsilon \leqslant \varphi$ *et*

$$A = \mathrm{Eucl}(A) \cup \{0\}.$$

(v) Réciproquement, montrer que si on a $A = \mathrm{Eucl}(A) \cup \{0\}$ *alors* A *est euclidien pour le stathme* υ.

---

12. On peut montrer que la réciproque est aussi vraie.

13. T. Motzkin, The Euclidean algorithm, Bull. Amer. Math. Soc. 55 (12), 1142-1146 (1949).

14. P. Samuel, *About Euclidean Rings*, Journal of Algebra 19, 282-301 (1979). Cet article est particulièrement accessible.

15. Pour coller aux conventions du cours, on pourra supposer A commutatif, mais cette hypothèse n'interviendra pas, sauf à la question (v) pour une raison de convention.

Exercice 7.28. *Soit A un anneau intègre. Une fonction $f : A \smallsetminus \{0\} \to \mathbb{N}$ est dite* presque euclidienne *si pour tout $a, b \in A \smallsetminus \{0\}$, on a soit $b \mid a$, soit il existe $c \in aA + bA$ tel que $f(c) < f(a)$. Si une telle fonction existe, on dit que A est presque euclidien.*

(i) Montrer que si A est presque euclidien, alors A est principal.

(ii) On suppose A principal. Montrer que la fonction $f : A \smallsetminus \{0\} \to \mathbb{N}$ associant à tout élément le nombre de ses facteurs premiers, est presque euclidienne.

(iii) En déduire que A est principal si, et seulement si, il est presque euclidien (Dedekind, Hasse).

Dans l'exercice suivant on utilisera la notion d'anneau quotient.

Exercice 7.29. (Idéaux premiers) *Soient A un anneau commutatif et P un idéal de A. On dit que P est premier si on a $P \neq A$ et si pour tout $x, y \in A$ tels que $xy \in P$, on a soit $x \in P$, soit $y \in P$.*

(i) Soit $f \in A$. Montrer que l'idéal fA est premier $\iff$ l'élément f est premier.

(ii) Montrer que P est premier $\iff$ l'anneau quotient A/P est intègre.

(iii) Montrer que si P est maximal alors P est premier.

(iv) Donner un exemple d'idéal premier non maximal.

(v) Montrer que si P est premier, et si A/P est fini, alors P est maximal.

L'exercice suivant montre que pour les anneaux comme $\mathbb{Z}[\sqrt{d}]$ ou A_d, factoriel équivaut à principal.

Exercice 7.30. *Soit A un anneau factoriel tel que pour tout $f \in A$ non nul alors A/fA est fini. On veut montrer que A est principal.*

(i) Montrer que A est noethérien.

(ii) Montrer que pour tout $f \in A$ premier, l'idéal fA est maximal.

(iii) Montrer que tout idéal maximal de A est de la forme fA avec $f \in A$ premier.

(iv) Soit $f \in A$ non nul ou unité, et $I \subset A$ un idéal non nul, montrer $fI \subsetneq I$.

(v) Conclure.

Chapitre 8

Modules sur les anneaux principaux

Le premier but de ce chapitre est d'introduire la notion de module sur un anneau A (une notion introduite par Dedekind [1] en 1871). Pour faire court, « les modules sont aux anneaux ce que les espaces vectoriels sont aux corps ». L'algèbre linéaire, dite A-linéaire, fait sens de manière intéressante dans cette généralité, et a de très nombreuses applications.

Par exemple, un groupe abélien est strictement la même chose qu'un $\mathbb{Z}$-module, et certaines constructions étudiées au chapitre 3 sont plus naturelles de ce point de vue "additif". En guise d'autre exemple important, il est équivalent d'étudier les classes d'isomorphisme de $k[X]$-modules, disons avec k un corps, et les classes de similitudes d'endomorphismes des k-espaces vectoriels. De plus, les idéaux d'un anneau sont ses sous-modules, et c'est d'ailleurs pour étudier les idéaux que Dedekind a introduit les modules. Enfin, comme nous le verrons plus tard, la notion de module fournit un langage particulièrement adapté à la théorie des représentations.

Dans une première partie, nous développons en l'illustrant le vocabulaire de base de la théorie des modules. Pour l'essentiel, l'anneau A n'y est pas nécessairement commutatif. On montre par exemple que tout sous-module d'un module de type fini sur un anneau noethérien est encore de type fini. On montre aussi que le *rang* d'un A-module libre est bien défini si A est commutatif. En dépit des ressemblances avec la théorie des espaces vectoriels, il faut prendre garde que la plupart des propriétés les plus élémentaires des espaces vectoriels sont en défaut en général pour les modules, comme l'existence des suppémentaires ou certaines propriétés des familles libres et génératrices. L'exemple des $\mathbb{Z}$-modules, bien qu'encore trop simple, est un bon exemple à avoir en tête en première approche.

Dans une seconde partie, nous étudions en détail la structure des modules de type fini sur un anneau principal. Nous suivons une approche matricielle, qui est complémentaire à l'approche par prolongement de caractères mise en avant pour les $\mathbb{Z}$-modules au Chapitre 3. Le théorème principal, dans le cas particulier des $\mathbb{Z}$-modules, se réduit au théorème de structure des groupes abéliens finis ou de type fini. Dans le cas des $k[X]$-modules, il conduit à la notion d'invariants de similitude, et contient par exemple théorie de la réduction de Jordan. Il est assez satisfaisant d'englober dans un même énoncé deux résultats en apparence aussi différents.

1. Voir R. Dedekind, *Theory of algebraic integers*, Cambridge Math. Lib.

1. Modules sur un anneau

1.1. La notion de A-module.

DÉFINITION 1.1. *Soit A un anneau. Un A-module est la donnée d'un groupe abélien*[2] $(M,+)$ *et d'une application $A \times M \to M$, $(a,m) \mapsto a.m$, telle que pour tout $a, a' \in A$ et tout $m, m' \in M$ on ait :*

(M1) $a.(m+m') = a.m + a.m'$,
(M2) $(a+a').m = a.m + a'.m$,
(M3) $a.(a'.m) = (aa').m$,
(M4) $1.m = m$.

On n'a pas supposé A commutatif car cela n'est pas nécessaire. Étant donnés A un anneau, M un groupe abélien et $A \times M \to M, (a,m) \mapsto a.m$ une application quelconque, et comme dans le cas des actions de groupes, on peut reformuler les axiomes (M1)–(M4) en terme des *translations*

$$\mathrm{L}_a : M \to M, m \mapsto a.m.$$

En effet, si on note $(\mathrm{End}_{\mathbb{Z}}(M), +, \circ)$ l'anneau des des applications $\mathbb{Z}$-linéaires $M \to M$ (pour l'addition $+$ des fonctions et la composition $\circ$), on constate que la propriété (M1) se traduit en $\mathrm{L}_a \in \mathrm{End}_{\mathbb{Z}}(M)$ pour tout $a \in A$, et que les axiomes (M2), (M3) et (M4) disent exactement que $A \to \mathrm{End}_{\mathbb{Z}}(M), a \mapsto \mathrm{L}_a$, est un morphisme d'anneaux.

Voici quelques exemples suffisamment intéressants pour justifier ce chapitre.

EXEMPLE 1.2. (i) L'anneau A lui-même peut être vu comme un A-module via l'application $A \times A \to A, (a,b) \mapsto ab$.

(ii) (*Espaces vectoriels*) Si $A = k$ est un corps, un A-module est (par définition) la même chose qu'un k-espace vectoriel.

(iii) ($\mathbb{Z}$-*modules*) Tout groupe abélien M est muni d'une, et une seule, structure de $\mathbb{Z}$-module. En effet, $\mathbb{Z} \times M \to M, (n,m) \mapsto nm$, convient. D'autre part, (M2) montre que pour $m \in M$ alors $\mathbb{Z} \to M, n \mapsto n.m$ est un morphisme de groupes, envoyant 1 sur m par (M4), et donc n sur nm pour tout $n \in \mathbb{Z}$.

EXEMPLE 1.3. (*Polynômes d'endomorphismes*) Soient k un corps, V un k-espace vectoriel et u un endomorphisme de V. L'application $k[X] \times V \to V$, $(P,v) \mapsto P(u)(v)$, est une structure de $k[X]$-module sur le groupe abélien V. En effet, on a $P(u) \in \mathrm{End}(V)$ pour tout $P \in k[X]$, donc (M1). On a aussi

$$(P+Q)(u) = P(u) + Q(u), \ \ (PQ)(u) = P(u) \circ Q(u) \ \text{ et } 1(u) = \mathrm{id}_V$$

dans $\mathrm{End}(V)$, et donc (M2), (M3) et (M4). On note V_u ce $k[X]$-module.

EXEMPLE 1.4. (*Une variante entière sur un exemple*) Soient $d \in \mathbb{Z}$ non carré et $X \in \mathrm{M}_n(\mathbb{Z})$ avec $X^2 = d\,1_n$. Alors

$$\mathbb{Z}[\sqrt{d}] \times \mathbb{Z}^n \to \mathbb{Z}^n, (a + b\sqrt{d}, v) \mapsto (a + bX)v,$$

est une structure de $\mathbb{Z}[\sqrt{d}]$-module sur $\mathbb{Z}^n$. Elle est bien définie car $1, \sqrt{d}$ est une $\mathbb{Z}$-base de $\mathbb{Z}[\sqrt{d}]$. La vérification des axiomes est encore immédiate.

2. Dans ce chapitre, tous les groupes abéliens seront notés additivement.

EXEMPLE 1.5. (*Restriction des scalaires*) Soient $f : A \to B$ un morphisme d'anneaux (par exemple, l'inclusion d'un sous-anneau) et M un B-module. Alors $A \times M \to M, a \mapsto f(a).m$, est une structure de A-module sur M appelé *restriction des scalaires de M à A* (ou mieux à f, pour être plus précis). Par exemple, si M est un $k[X]$-module, sa restriction au morphisme $k \to k[X], \lambda \mapsto \lambda$, est un k-espace vectoriel. Si on note V ce k-espace vectoriel, et si on pose $u : V \to V, v \mapsto X.v$, alors u est k-linéaire et on constate que l'on a $M = V_u$.

NOTATION : Comme pour les groupes et les actions de groupes, on notera souvent $(a, m) \mapsto am$ (plutôt que $a.m$) une loi de A-module.

1.2. Sous-modules. Toutes les constructions que l'on a faites en théorie des groupes abéliens admettent un enrichissement naturel en théorie des modules.

DÉFINITION 1.6. *Soient A un anneau et M un A-module. Un sous-module de M est un sous-groupe $N \subset M$ tel que $an \in N$ pour tout $a \in A$ et $n \in N$. C'est un A-module pour la loi induite $(a, n) \mapsto an$.*

EXEMPLE 1.7. *(i) Les sous-modules du A-module A sont ses idéaux. On parle aussi* d'idéaux à gauche*, si A n'est pas commutatif.*

(ii) Quand A est un corps (resp. $A = \mathbb{Z}$), un sous-module d'un A-module est simplement un sous-espace vectoriel (resp. sous-groupe).

(iii) Les sous-modules du $k[X]$-module V_u sont les sous-espaces vectoriels de V stables par l'endomorphisme u de V.

(iv) Soient M un A-module et $M_1, \ldots, M_n$ des sous-modules de A. Alors la somme $M_1 + \cdots + M_n$ et l'intersection $\cap_{i=1}^n M_i$ des sous-groupes M_i de M sont des sous-A-modules de M.

(v) Si les M_i, $i \in I$, sont des A-modules, alors le groupe abélien produit $\prod_{i \in I} M_i$ est un A-module pour $a.(m_i) = (am_i)$. De même, la somme directe externe de $\oplus_{i \in I} M_i$ des groupes abéliens M_i est un sous A-module de $\prod_{i \in I} M_i$ (éléments dont toutes les coordonnées sauf un nombre fini sont nulles). En particulier, A^I et $A^{(I)}$ sont des A-modules de manière naturelle.

1.3. Applications A-linéaires. La notion de morphisme adéquate pour les modules est la suivante :

DÉFINITION 1.8. *Soient M et N des A-modules. Un morphisme de M vers N, aussi appelé* application A-linéaire*, est une application $f : M \to N$ vérifiant $f(m + m') = f(m) + f(m')$ et $f(am) = af(m)$ pour tout $a \in A$ et $m, m' \in M$.*

L'observation 1.2 (ii) s'étend en disant que tout morphisme de groupes abéliens est automatiquement un morphisme des $\mathbb{Z}$-modules associés. En guise de second exemple, regardons maintenant ce qu'est un morphisme de $k[X]$-modules.

EXEMPLE 1.9. Soient k un corps, V_1 et V_2 deux k-espaces vectoriels, ainsi que u_1 et u_2 des endomorphismes de V_1 et V_2. Pour $i = 1, 2$ on note M_i le $k[X]$-module $(V_i)_{u_i}$. Vérifions qu'un morphisme $M_1 \to M_2$ est exactement une application k-linéaire $f : V_1 \to V_2$ telle que $f \circ u_1 = u_2 \circ f$. En effet, si f est un morphisme, on a $f(v + v') = f(v) + f(v')$ (additivité), $f(\lambda v) = \lambda f(v)$ pour $\lambda \in k$ (prendre $a = \lambda \in k[X]$) et $f(u_1(v)) = u_2(f(v))$ (prendre $a = X \in k[X]$), et donc

$f \circ u_1 = u_2 \circ f$. Réciproquement, ces deux propriétés impliquent manifestement $f(P(u_1)(v)) = P(u_2)f(v)$ pour tout $P \in k[X]$ (considérer les monômes X^k puis conclure par linéarité).

Isomorphismes. Un morphisme bijectif entre deux A-modules est appelé *isomorphisme*, auquel cas son inverse est aussi un morphisme. La composée de deux (iso-)morphismes est encore un (iso-)morphisme. On dit que deux A-modules sont isomorphes s'il existe un isomorphisme entre eux.

Exemple 1.10. Soient V un k-espace vectoriel, a et b deux endomorphismes de V, et V_a et V_b les $k[X]$-modules associés. *Alors V_a et V_b sont isomorphes si, et seulement si, les endomorphismes a et b sont semblables.*

Ainsi, il est équivalent de classifier les $k[X]$-modules à isomorphisme près, disons de k-espace vectoriel sous-jacent de dimension finie n, et de déterminer les classes de similitude d'éléments de $\mathrm{M}_n(k)$.

À ce stade du cours, la proposition suivante est immédiate.

Proposition 1.11. *(i) (Image et noyau) Si M et N sont des A-modules, et $u : M \to N$ est A-linéaire, alors les sous-groupes $\operatorname{Im} u$ et $\ker u$ sont des sous-A-modules de N et M respectivement.*

(ii) (Quotient par un sous-module) Si N est un sous-A-module de M, il existe une unique structure de A-module sur le groupe quotient M/N telle que la projection canonique $\pi : M \to M/N$ est A-linéaire.

(iii) Pour toute application A-linéaire $u : M \to N$, et pour tout sous-A-module $K \subset \ker u$, l'application quotient $\overline{u} : M/K \to N$ est A-linéaire. Elle est injective si $K = \ker u$, un isomorphisme si en outre $N = \operatorname{Im} u$.

La structure de A-module sur le groupe quotient M/N évoquée au (ii) est bien entendu $(a, m + N) \mapsto am + N$. Le A-module M/N ainsi définit s'appelle *A-module quotient de M par N*.

1.4. Modules monogènes. Pour $m \in M$, on pose $A\,m = \{am \mid a \in A\}$ (*sous-A-module de M engendré par m*) : c'est le plus petit sous-module de M contenant m.

Définition 1.12. *Un A-module M est dit* monogène *si on a $M = Am$ pour un certain $m \in M$.*

Par exemple, un $\mathbb{Z}$-module monogène est un groupe monogène, un k-espace vectoriel est monogène s'il est de dimension $\leqslant 1$. Considérons A comme A-module comme dans l'Exemple 1.7 (i), lui aussi est monogène ($A = A.1$). Plus généralement, si I est un idéal (=sous-module) de A, le A-module quotient A/I est encore monogène, engendré par la classe de 1 : on a $a.(1 + I) = a + I$ pour tout $a \in A$.

Proposition 1.13. *Tout A-module monogène M est isomorphe à A/I pour un certain idéal (à gauche I) de A.*

Démonstration — Soit $m \in M$ avec $M = Am$. L'application $f : A \to M,\ a \mapsto am$, est manifestement A-linéaire, et par hypothèse surjective. Son noyau I est un idéal de A (car un sous-module !) et f induit donc un isomorphisme de A-modules $A/I \simeq M$. $\square$

Exemple 1.14. Pour $A = \mathbb{Z}$ on retrouve bien sûr la classification des groupes abéliens monogènes. Considérons maintenant k un corps et étudions les $k[X]$-modules $M = k[X]/I$, avec I idéal de $k[X]$. Si I est nul, on a $M \simeq k[X]$. En particulier, le k-espace vectoriel sous-jacent est de dimension infinie, avec pour base les X^i pour $i \geqslant 0$. Si I est non nul, on a $I = (P)$ pour un unique polynôme unitaire $P \in k[X]$, disons de degré n. Dans ce cas, la division euclidienne par P assure que tout élément de M est représenté par un unique $Q \in k[X]$ avec $\deg Q < n$. Autrement dit, le k-espace vectoriel sous-jacent à M possède pour base les classes des n éléments $1, X, \ldots, X^{n-1}$. Posons $P = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$. Comme $XX^{n-1} \equiv -a_{n-1}X^{n-1} - \cdots - a_1X - a_0 \bmod P$, l'endomorphisme de multiplication par X dans cette base a pour matrice

$$\mathrm{C}(P) := \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \ddots & \vdots & -a_1 \\ 0 & 1 & \ddots & 0 & -a_2 \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & -a_{n-1} \end{bmatrix} \quad \text{(matrice compagnon de } P\text{)}.$$

1.5. Modules de type fini. Soient $e_1, \ldots, e_n \in M$ des éléments de M. On dispose de l'application A-linéaire

$$u : A^n \to M,\ (a_i) \mapsto \sum_{i=1}^{n} a_i e_i.$$

On dit que $e = \{e_i\}$ est une *famille génératrice* de M si u est surjective, *i.e.* $M = Ae_1 + \cdots + Ae_n$. On dit que e est *libre* si u est injective. On dit enfin que e est une base si elle est libre et génératrice, ou ce qui revient au même, si u est un isomorphisme.

Définition 1.15. *Un A-module est dit* de type fini *s'il possède une famille finie génératrice. Un A-module est dit libre de rang n s'il possède une base à n éléments.*

Par exemple, la famille d'éléments e_i de A^n définis par $(e_i)_j = \delta_{i,j}$ (symbole de Kronecker), est une base à n éléments du A-module A^n ("base canonique"). Par définition, M est donc libre de rang n si, et seulement si, il est isomorphe à A^n. Par conventions, le A-module nul $\{0\} = A^0$ est libre de base la famille vide.

Remarque 1.16. (i) Il est clair que si $u : M \to N$ est A-linéaire surjective, et si M est de type fini, alors N l'est aussi. En effet, si $M = \sum_{i=1}^{n} Ae_i$ alors $N = u(M) = \sum_{i=1}^{n} A\,u(e_i)$. En particulier, *tout quotient d'un module de type fini est encore de type fini.*

(ii) En revanche, il n'est pas vrai en général qu'un sous-module d'un module de type fini est de type fini. Par exemple, A est toujours de type fini comme module sur lui-même, mais ses sous-modules sont de type fini si, et seulement si, A est noethérien.

(iii) Il n'est pas vrai en général qu'un sous-module d'un module libre est libre : considérer A non principal et $M = A$.

La théorie des $\mathbb{Z}$-modules nous a déjà mise en garde sur le fait que lorsque A n'est pas un corps ces notions ne se comportent pas aussi bien en général que dans le cas des espaces vectoriels. Donnons toutefois deux énoncé positifs très utiles.

THÉORÈME 1.17. *Soit M un module de type fini sur un anneau noethérien. Alors tout sous-module de M est de type fini.*

DÉMONSTRATION — Soit N un sous-module de M. On veut montrer qu'il est de type fini. On procède par récurrence sur le cardinal minimal r d'une famille génératrice de M. On peut supposer M non nul. Considérons d'abord le cas $r = 1$ (M monogène). On a donc $M = Ae$ avec $e \in M$. On constate que $I = \{x \in A \mid xe \in N\}$ est un idéal de A, et aussi $N = Ie$. Mais I est un idéal de A, donc il est de la forme $Af_1 + \cdots + Af_r$ avec $f_i \in A$. On a donc $N = Af_1e + Af_2e + \cdots + Af_re$: il est de type fini.

Supposons maintenant $r > 1$ et écrivons $M = A\,m_1 + \ldots + A\,m_r$ et posons $M' = A\,m_1 + \ldots + A\,m_{r-1}$. On regarde la projection canonique

$$\pi : M \to M/M', m \mapsto m + M',$$

qui est A-linéaire de noyau M'. Le A-module M/M' est manifestement engendré par la classe de m_r, donc monogène. Par le cas $r = 1$, le sous-module $\pi(N)$ de M/M' est donc de type fini, disons engendré par les éléments $\pi(n_1), \cdots, \pi(n_s)$ avec $n_i \in N$. On a alors

$$N = N \cap M' + \sum_{i=1}^{s} A\,n_i.$$

En effet, l'inclusion $\supset$ est claire. Pour l'autre, on constate que pour $n \in N$, on a $\pi(n) \in \pi(N)$ et donc $\pi(n) = \sum_{i=1}^{s} a_i\pi(n_i)$ pour certains $a_1, \ldots, a_s \in A$, puis $n - \sum_{i=1}^{s} a_i\,n_i \in (\ker \pi) \cap N = M' \cap N$, et donc $n \in N' + M' \cap N$. Pour conclure, on constate que M' est engendré par $\leqslant r - 1$ éléments, et que $N \cap M'$ en est un sous-module, donc finiment engendré par récurrence. □

THÉORÈME 1.18. *Soient A un anneau commutatif non nul et m, n des entiers $\geqslant 0$. Les A-modules A^m et A^n sont isomorphes si, et seulement si, on a $m = n$. En particulier, toutes les bases d'un A-module libre de rang fini ont même cardinal.*

L'énoncé est inexact si A n'est pas commutatif : pour $A = \mathrm{End}_k(k^{(\mathbb{N})})$ on a $A \simeq A^2$ (voir l'Exercice 8.10).

DÉMONSTRATION — (On utilise quelques résultats du Complément §9 Chap. 7). Soient M un idéal maximal de A et k le corps quotient A/M. On regarde la projection naturelle $f : A^m \to k^m$, $(a_i) \mapsto (a_i \bmod M)$. Si $e_1, \ldots, e_n$ est une famille génératrice du A-module A^m, alors les $f(e_i)$ forment une famille génératrice du k-espace vectoriel k^m. On a donc $n \geqslant m$ par la théorie des espaces vectoriels. Ainsi, le cardinal d'une famille génératrice minimale du A-module A^m est m. Cela démontre le théorème. □

2. Classes d'équivalence de matrices sur un anneau principal

Soient A un anneau *commutatif* et $n \geqslant 1$ un entier. On rappelle l'anneau des matrices $\mathrm{M}_n(A)$, ainsi que son groupe des inversibles $\mathrm{GL}_n(A) := \mathrm{M}_n(A)^\times$. Dans cette généralité on dispose d'une application polynomiale

$$\det : \mathrm{M}_n(A) \to A,\ (m_{i,j}) \mapsto \sum_{\sigma \in \mathrm{S}_n} \varepsilon(\sigma) \prod_{j=1}^{n} m_{\sigma(j),j},$$

qui généralise la définition bien connue pour $A = \mathbb{C}$ (voire A un corps). Par définition, $M \mapsto \det M$ est une fonction multi-A-linéaire des lignes et des colonnes de M, qui est également alternée pour la même raison que dans le cas des corps.

Lemme 2.1. *Pour tout anneau commutatif A, et tout $M, N \in \mathrm{M}_n(A)$ on a*

$$\det MN \ = \ \det M \det N \ \text{ et } \ M\,{}^t\mathrm{Co}(M) \ = \ {}^t\mathrm{Co}(M)\,M = \det M\ 1_n.$$

Démonstration — Ce sont des identités polynomiales en les $2n^2$ entrées $m_{i,j}$ et $n_{i,j}$ de M et N, à coefficients entiers. Elle sont bien connues pour $A = \mathbb{C}$. En utilisant qu'un polynôme $P \in \mathbb{C}[X_1, \ldots, X_r]$ est identiquement nul si, et seulement si, on a $P(x_1, \ldots, x_r) = 0$ pour tout $x_1, \ldots, x_r \in \mathbb{C}$, on en déduit que le lemme vaut pour tout anneau A de la forme $\mathbb{Z}[X_1, \ldots, X_r]$.

Si on a un morphisme d'anneaux commutatifs $\varphi : A \to B$, et si on note $\varphi_n : \mathrm{M}_n(A) \to \mathrm{M}_n(B)$ le morphisme d'anneaux défini par $\varphi_n((m_{i,j}) = (\varphi(m_{i,j}))$, alors pour tout $M \in \mathrm{M}_n(A)$ on a $\det \varphi_n(M) = \varphi(\det M)$ et $\varphi_n({}^t\mathrm{Co}(M)) = {}^t\mathrm{Co}(\varphi_n(M))$. On en déduit que si le lemme est vrai pour le triplet (A, M, N), il est vrai pour le triplet $(B, \varphi_n(M), \varphi_n(N))$.

Soient enfin B un anneau commutatif général ainsi que $M', N' \in \mathrm{M}_n(B)$. Posons $A = \mathbb{Z}[\{X_{i,j}\}_{1 \leqslant i,j \leqslant n}, \{Y_{i,j}\}_{1 \leqslant i,j \leqslant n}]$, $M = (X_{i,j})_{1 \leqslant i,j \leqslant n}$ et $N = (Y_{i,j})_{1 \leqslant i,j \leqslant n}$: le lemme est vrai pour le triplet (A, M, N) par le premier paragraphe. Soit $\varphi : A \to B$ le morphisme d'anneaux envoyant $X_{i,j}$ sur $m_{i,j}$ et $Y_{i,j}$ sur $n_{i,j}$. On a $\varphi_n(M) = M'$, $\varphi_n(N) = N'$ et donc le lemme est vrai pour le triplet (B, M', N'). □

Proposition 2.2. *Pour tout anneau commutatif A on a*

$$\mathrm{GL}_n(A) = \{M \in \mathrm{M}_n(A) \mid \det M \in A^\times\}.$$

Démonstration — Pour $M \in \mathrm{M}_n(A)$, il existe $N \in \mathrm{M}_n(A)$ avec $MN = 1_n$. On en déduit $\det M \det N = \det 1_n = 1$ par le Lemme 2.1. Comme on a $\det M, \det N \in A$, on en déduit $\det M \in A^\times$. Réciproquement, si on a $\det M \in A^\times$ on constate que $N := (\det M)^{-1}\ {}^t\mathrm{Co}(M)$ est un inverse de M dans $\mathrm{M}_n(A)$ par le Lemme 2.1. □

Par le Lemme 2.1, on dispose d'un morphisme de groupes $\det : \mathrm{GL}_n(A) \to A^\times$, manifestement surjectif (considérer des matrices diagonales). Son noyau est particulièrement important :

Définition 2.3. *On note $\mathrm{SL}_n(A)$ le noyau du morphisme $\det : \mathrm{GL}_n(A) \to A^\times$. C'est un sous-groupe distingué de $\mathrm{GL}_n(A)$.*

On fixe $p, q \geqslant 1$ et on s'intéresse à l'action du groupe $\mathrm{GL}_p(A) \times \mathrm{GL}_q(A)$ sur $\mathrm{M}_{p,q}(A)$, définie par $(P, Q).M = PMQ^{-1}$. Deux matrices $M, N \in \mathrm{M}_{p,q}(A)$ dans la même orbite pour cette action sont dites *équivalentes* (à ne pas confondre avec la conjugaison !). Le résultat principal de cette section est la description des classes d'équivalence quand A est un anneau principal. Cette énoncé a une riche histoire, avec des contributions de Gauss, Smith, Frobenius, Jordan...

Théorème 2.4. (Forme normale de Smith) *Soient A un anneau principal et $M \in \mathrm{M}_{p,q}(A)$ avec $p, q \geqslant 1$, et $r = \min(p, q)$. Il existe $P \in \mathrm{GL}_p(A)$, $Q \in \mathrm{GL}_q(A)$, ainsi que $a_1, a_2, \dots a_r \in A$ uniques modulo association, avec $a_1 \mid a_2 \mid \cdots \mid a_r$ et*

$$PMQ = \begin{bmatrix} a_1 & & & \\ & a_2 & & \\ & & \ddots & \\ & & & a_r \end{bmatrix} \text{ (avec des 0 partout ailleurs).} \tag{66}$$

(La situation dessinée est celle avec $r = p$.) Noter qu'il est très possible d'avoir $a_i = 0$, par exemple pour $M = 0$!, mais qu'alors on a $a_j = 0$ pour tout $j \geqslant i$.

Définition 2.5. *Les éléments $a_i \in A$ non nuls ci-dessus, uniques modulo $A^\times$, sont appelés* facteurs invariants *de la matrice $M \in \mathrm{M}_{p,q}(A)$.*

Avant de débuter la démonstration du théorème, revisitons les *opérations sur les lignes et les colonnes*. Pour $\lambda \in A$, et pour $1 \leqslant i \neq j \leqslant n$, on dispose des *transvections standards* $\mathrm{T}_{i,j}(\lambda) := \mathrm{I}_n + \lambda \mathrm{E}_{i,j}$. Ce sont des éléments de $\mathrm{SL}_n(A)$. Pour $M \in \mathrm{M}_{n,m}(A)$, la matrice $\mathrm{T}_{i,j}(\lambda)M$ est obtenue à partir de M en ajoutant à la ligne i de M, λ fois la ligne j de M. De même (en transposant !), pour $M \in \mathrm{M}_{m,n}(A)$, $M\,\mathrm{T}_{i,j}(\lambda)$ est obtenue à partir de M en ajoutant à la colonne j de M, λ fois la colonne i de M. Pour $1 \leqslant i < j \leqslant n$, on dispose d'un morphisme de groupes naturel

$$f_n^{i,j} : \mathrm{GL}_2(A) \to \mathrm{GL}_n(A), \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{array}{c} \\ \\ i \\ \\ j \\ \\ \end{array} \begin{array}{c} \begin{array}{ccccc} & i & & j & \end{array} \\ \begin{bmatrix} \mathrm{I}_{i-1} & \vdots & & \vdots & \\ \cdots & a & & b & \\ & & \mathrm{I}_{j-i-1} & & \\ \cdots & c & & d & \\ & & & & \mathrm{I}_{n-j} \end{bmatrix} \end{array}. \tag{67}$$

On a par exemple $f_n^{i,j}(\begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix}) = \mathrm{T}_{i,j}(\lambda)$ et $f_n^{i,j}(\begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix}) = \mathrm{T}_{j,i}(\lambda)$ pour $\lambda \in A$. De plus, pour $M \in \mathrm{M}_{n,m}(A)$ et $\tau = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, on constate que $f_n^{i,j}(\tau)M$ est la matrice obtenue à partir de M en échangeant les lignes i et j. Idem pour $M f_n^{i,j}(\tau)$ quand $M \in \mathrm{M}_{m,n}(A)$.

Démonstration — (de l'existence) Pour $a \in A$ non nul on note $\nu(a) \in \mathbb{N}$ le nombre de facteurs irréductibles de a, et on pose $\nu(0) = +\infty$. On peut supposer $M = (m_{i,j})$ non nulle et on pose aussi $\nu(M) = \inf_{i,j} \nu(m_{i,j})$. On procède par récurrence sur le couple $(p + q, \nu(M)) \in \mathbb{N}^2$ pour l'ordre lexicographique, qui est un bon ordre.[3] On a $p + q \geqslant 2$. Le cas $p + q = 2$ (initialisation), qui force $p = q = 1$, est trivial. Soit

3. Merci aux étudiants d'avoir suggéré ceci en classe !

(i_0, j_0) tel que $\nu(m_{i_0,j_0}) = \nu(M)$. Quitte à effectuer des transpositions des lignes $1, i_0$ et des colonnes de $1, j_0$ de M, on peut supposer $(i_0, j_0) = (1, 1)$.

(Cas 1) Il existe $j > 1$ tel que $m_{1,1}$ ne divise pas $m_{1,j}$. Comme A est principal, $m_{1,1}$ et $m_{1,j}$ ont un pgcd, disons d, et on a alors $\nu(d) < \nu(m_{1,1})$. De plus, il existe $u, v \in A$ avec $m_{1,1}u - m_{1,j}v = d$. La matrice

$$Q = \begin{bmatrix} u & m_{1,j}/d \\ v & m_{1,1}/d \end{bmatrix}$$

est donc dans $\mathrm{SL}_2(A)$, et le coefficient $(1, 1)$ de $M' := M f_q^{1,j}(Q)$ vaut d. On a donc $\nu(M') < \nu(M)$ et $M' \sim M$, et on conclut par récurrence.

(Cas 2) Il existe $i > 1$ tel que $m_{1,1}$ ne divise pas $m_{i,1}$. On conclut de même par récurrence (ou en transposant l'argument ci-dessus).

(Cas 3) Dans le cas restant, $m_{1,1}$ divise $m_{i,1}$ et $m_{1,j}$ pour tout $1 \leqslant i \leqslant q$ et $1 \leqslant j \leqslant p$. En multipliant M à gauche successivement par les transvections $\mathrm{T}_{1,i}(-m_{i,1}/m_{1,1})$ pour $i = 2, \ldots, p$, ce qui ne modifie à chaque fois que la i-ème ligne de M, on peut alors supposer successivement sans changer la première ligne (et en particulier $m_{1,1}$), que l'on a $m_{1,j} = 0$ pour $j = 2, \ldots, q$. Puis en multipliant de même des transvections bien choisies à droite, on peut supposer en plus $m_{1,j} = 0$ pour $j = 2, \ldots, q$, sans changer $m_{1,1}$. Noter qu'après chacune des $p + q - 2$ opérations ci-dessus, on peut toujours supposer que la matrice M' obtenue vérifie $\nu(M') = \nu(m_{1,1})$. En effet, $m_{1,1}$ en est un coefficient, et si on a $\nu(M') < \nu(m_{1,1})$ on conclut par récurrence.

Dans les cas particulier $p = 1$ ou $q = 1$, on a manifestement terminé. Considérons un coefficient $m_{k,l}$ avec $k, l > 1$ n'est pas divisible par $m_{1,1}$. S'il on ajoute à M sa k-ème ligne, on obtient une matrice équivalente M' avec de coefficients $(1, 1)$ et $(1, l)$ égaux à $m_{1,1}$ et $m_{k,l}$, avec $m_{1,1}$ ne divisant pas $m_{k,l}$. L'argument du Cas 1 montre que M' est équivalente à une matrice M'' avec $\nu(M'') < \nu(m_{1,1})$, et on conclut par récurrence.

On peut donc supposer que tous les coefficients $m_{k,l}$ avec $k, l > 1$ sont divisibles par $m_{1,1}$. Alors le bloc $[2, p] \times [2, q]$ de M est de la forme $m_{1,1}N$ avec $N \in \mathrm{M}_{p-1,q-1}(A)$. On applique alors l'hypothèse de récurrence à N, et on conclut par un calcul par blocs immédiat. □

La démonstration de l'unicité nécéssitera une définition préliminaire. L'anneau A y est à nouveau commutatif quelconque. Fixons $M = (m_{i,j}) \in \mathrm{M}_{p,q}(A)$. Rappelons que pour $1 \leqslant k \leqslant \min(p, q)$, un *mineur de taille* k de M est un élément de A de la forme $\pm \det M_{I,J}$, où $I \subset \{1, \ldots, p\}$ et $J \subset \{1, \ldots, q\}$ sont des sous-ensembles de cardinal k et $M_{I,J}$ désigne la matrice extraite $(m_{i,j})_{(i,j) \in I \times J}$.

Définition 2.6. *Soit A un anneau commutatif, $M \in \mathrm{M}_{p,q}(A)$ et $k \in \mathbb{Z}$. Le contenu d'ordre k de M l'idéal $\mathrm{c}_k(M)$ de A engendré par les mineurs de taille k de M, avec les conventions $\mathrm{c}_k(M) = A$ pour $k \leqslant 0$ et $\mathrm{c}_k(M) = \{0\}$ pour $k > \min(p, q)$.*

Par exemple, on a $\mathrm{c}_1(M) = \sum_{i,j} A\, m_{i,j}$ (*idéal pgcd des coefficients de M*).

Lemme 2.7. *Soient A un anneau commutatif, ainsi que $M, N \in \mathrm{M}_{p,q}(A)$ deux matrices équivalentes. Pour tout $k \in \mathbb{Z}$ on a $\mathrm{c}_k(M) = \mathrm{c}_k(N)$.*

Démonstration — On peut supposer $k \leqslant \min(p,q)$. Vérifions $\mathrm{c}_k(MN) \subset \mathrm{c}_k(M)$ pour tout $M \in \mathrm{M}_{p,q}(A)$ et tout $N \in \mathrm{M}_q(A)$. On a $(MN)_{i,j} = \sum_{r=1}^q m_{i,r} n_{r,j}$, de sorte que si $\mathrm{col}_j(X)$ désigne la j-ème colonne de la matrice X, cette égalité s'écrit aussi $\mathrm{col}_j(MN) = \sum_{r=1}^q n_{r,j}\,\mathrm{col}_r(M)$. Le caractère multi-$A$-linéaire alterné de det montre alors que pour $I \subset \{1,\dots,p\}$ et $J \subset \{1,\dots,q\}$ de tailles k on a

$$\det(MN)_{I,J} \quad \in \sum_{K \subset \{1,\dots,q\}} A \ \det M_{I,K},$$

la somme portant sur les parties K à k éléments[4] de $\{1,\dots,q\}$. On en déduit $\mathrm{c}_k(MN) \subset \mathrm{c}_k(M)$. On en tire $\mathrm{c}_k(M) = \mathrm{c}_k(MQ)$ pour $Q \in \mathrm{GL}_q(A)$, car $\mathrm{c}_k(M) = \mathrm{c}_k(MQQ^{-1}) \subset \mathrm{c}_k(MQ) \subset \mathrm{c}_k(M)$. On a de même en travaillant sur les lignes (ou en transposant) $\mathrm{c}_k(PM) = \mathrm{c}_k(M)$ pour $P \in \mathrm{GL}_p(A)$. □

Démonstration — (Assertion d'unicité du Théorème 2.4, seule l'hypothèse A intègre sera utilisée) Par le Lemme 2.7, et comme A est intègre, il suffit de montrer que pour $D \in \mathrm{M}_{p,q}(A)$ diagonale de coefficients $a_1 \,|\, a_2 \,|\, \dots \,|\, a_r$ on a $\mathrm{c}_k(D) = a_1 a_2 \dots a_k A$ pour $1 \leqslant k \leqslant r$. L'inclusion $a_1 a_2 \dots a_k A \subset \mathrm{c}_k(M)$ est évidente en considérant le mineur d'indices $1 \leqslant i,j \leqslant k$. Réciproquement, pour I, J de taille k quelconques on a $\det D_{I,J} = 0$ sauf pour $I = J$, auquel cas on a $\det D_{I,I} = \prod_{i \in I} a_i$, qui est bien divisible par $a_1 a_2 \dots a_k$ dans A. □

3. Modules de type fini sur un anneau principal

Soient A un anneau commutatif, ainsi que E et F deux A-modules. On suppose E et F libres de rangs finis, disons respectivement q et p, et on se donne $u : E \to F$ une application A-linéaire. Soit $e_1,\dots,e_q$ une base de E et $f_1,\dots,f_p$ une base de F. Il existe une unique matrice $(u_{i,j}) \in \mathrm{M}_{p,q}(A)$ telle que $u(e_j) = \sum_{i=1}^p u_{i,j} f_i$ pour tout $1 \leqslant j \leqslant q$. C'est la *matrice de u dans les bases e et f*, notée $\mathrm{Mat}_{e,f} u$. Bien sûr, comme e et f sont des bases de E et F, toute $M \in \mathrm{M}_{p,q}(A)$ est même la matrice d'une unique application A-linéaire $F \to E$. Cette discussion matricielle est strictement identique à celle bien connue dans le cadre des espaces vectoriels. En particulier, si on a une autre application A-linéaire $v : F \to G$ avec G libre de rang o, et $g = (g_1,\dots,g_o)$ une A-base de G, on vérifie immédiatement l'identité matricielle

$$\mathrm{Mat}_{e,g}\, v \circ u \;=\; \mathrm{Mat}_{f,g} v \ \mathrm{Mat}_{e,f} u.$$

Cette formule implique d'abord que pour $E = F$ et u l'identité alors $\mathrm{P}_{e,f} := \mathrm{Mat}_{e,f}\mathrm{id}_E$ est dans $\mathrm{GL}_p(A)$ (*matrice de passage de f vers e*), et d'inverse $\mathrm{P}_{f,e}$. Ensuite, elle montre que si e' est une autre base à q éléments de E, et si f' est une autre base à p éléments de F, on a

$$\mathrm{Mat}_{e',f'} u \;=\; P \ \mathrm{Mat}_{e,f}\, u \ Q,$$

avec $Q = \mathrm{P}_{e',e} \in \mathrm{GL}_q(A)$ et $P = \mathrm{P}_{f,f'} \in \mathrm{GL}_p(A)$. On déduit de cette discussion et du Théorème 2.4 le :

4. On peut raffiner l'analyse ci-dessus pour obtenir une formule plus précise appelée *formule de Cauchy-Binet*.

THÉORÈME 3.1. (Théorème de la base adaptée pour les applications linéaires) *Soient E et F des A-modules et $u : E \to F$ une application A-linéaire. On suppose A principal, E et F libres sur A de rangs respectifs q et p. Alors il existe une base $e = (e_1, \dots, e_q)$ de E, une base $f = (f_1, \dots, f_p)$ de F, et des éléments non nuls $a_1, \dots, a_r \in A$ avec $r = \min(p, q)$ et $a_1 \,|\, a_2 \,|\, \dots \,|\, a_r$, vérifiant*

$$u(f_i) = a_i e_i \text{ pour } i \leqslant r, \text{ et } u(f_i) = 0 \text{ pour } i > r.$$

Une seconde version de ce théorème concerne les sous-modules d'un module libre de type fini sur un anneau principal.

THÉORÈME 3.2. (Théorème de la base adaptée pour les sous-modules) *Soient A un anneau principal, M un A-module libre de rang fini m, et N un sous-module de M. Il existe une base $e_1, \dots, e_m$ de M, un entier $0 \leqslant s \leqslant m$, et des éléments $a_1, \dots, a_s \in A$ non nuls, tels que :*

(i) $a_1 e_1,\ a_2 e_2,\ \dots,\ a_s e_s$ est une base de N.

(ii) $a_1 \mid a_2 \mid \cdots \mid a_s$.

En particulier, N est libre sur A de rang $s \leqslant n$.

Le cas particulier $A = \mathbb{Z}$ du Théorème 3.2 est déjà intéressant, et n'avait pas été démontré au chapitre 3.

DÉMONSTRATION — On peut supposer M non nul, et donc $n \geqslant 1$, sinon il n'y a rien à démontrer. Comme un anneau principal est noethérien, on sait que N est de type fini par le Théorème 1.17. On peut donc trouver un entier $n \geqslant 1$ une application A-linéaire $u : A^n \to M$ avec $\operatorname{Im} u = N$. Posons $r = \min(m, n)$. D'après le Théorème 3.1, il existe une base $e_1, \dots, e_n$ de A^n, et une base $f_1, \dots, f_m$ de M, ainsi que $a_1 \mid a_2 \mid \cdots \mid a_r$, tels que $u(e_i) = a_i f_i$ pour $i \leqslant r$ et $u(e_i) = 0$ pour $i > r$. Soit s le plus grand entier $1 \leqslant i \leqslant r$ tel que a_i est non nul (s'il n'en existe pas, on pose $s = 0$, et c'est que l'on a $N = \{0\}$). On a $N = u(\sum_{i=1}^m A f_i) = \sum_{i=1}^p A a_i e_i$, et les $a_i e_i$ sont A-libres car les e_i le sont (et les a_i sont non nuls). □

THÉORÈME 3.3. *Soient A un anneau principal et M un A-module de type fini. Il existe un unique entier $r \geqslant 0$, appelé rang de M, un unique entier $s \geqslant 0$, et des éléments non nuls $a_1, \dots, a_s \in A$, uniques modulo association, avec*

$$M \simeq A^r \times A/a_1 A \times A/a_2 A \times \cdots \times A/a_s A, \ \ a_1 \mid a_2 \mid \cdots \mid a_s \text{ et } a_1 \notin A^\times$$

Les éléments a_i ci-dessus sont appelés *facteurs invariants de M*. Quand $s = 0$, l'énoncé signifie simplement $M \simeq A^r$, *i.e.* que M est libre de rang r.

DÉMONSTRATION — (de la partie existence) Comme M est un A-module de type fini, on peut trouver un entier $m \geqslant 1$ et une application A-linéaire surjective $u : A^m \to M$. Cela montre $M \simeq A^m / \ker u$. On conclut [5] l'existence en appliquant le théorème de la base adaptée au sous-module $\ker u$ du A-module libre A^m. □

5. Il est clair que que si on a $M = \prod_{i=1}^m M_i$ avec les M_i des A-modules, et si pour tout i on a N_i un sous-A-module de M_i, alors la projection canonique $M \to \prod_{i=1}^m M_i/N_i, (m_i) \mapsto (m_i + N_i)$, a pour noyau $N := \prod_{i=1}^m N_i$, et donc induit un isomorphisme $M/N \simeq \prod_{i=1}^m M_i/N_i$.

Pour démontrer l'unicité, nous pourrions procéder par un argument très similaire à celui du cas $A = \mathbb{Z}$ démontré en détail dans le Chapitre 3, c'est pourquoi l'argument a été omis en classe. Nous renvoyons au Complément 5 pour deux démonstrations détaillées. Terminons plutôt par une application à la réduction des endomorphismes.

THÉORÈME 3.4. *Soient k un corps et V un k-espace vectoriel de dimension finie.*

(i) Pour tout endomorphisme u de V, il existe une unique entier $s \leqslant \dim V$ et une unique suite de polynômes $P_1, \ldots, P_s \in k[X]$ unitaires de degré $\geqslant 1$ avec $P_1 \mid P_2 \mid \cdots \mid P_s$, tels que dans une base e convenable de V on ait

$$\mathrm{Mat}_e u = \begin{bmatrix} \mathrm{C}(P_1) & & & \\ & \mathrm{C}(P_2) & & \\ & & \ddots & \\ & & & \mathrm{C}(P_s) \end{bmatrix}.$$

Les polynômes $P_1, \ldots, P_s$ sont appelés *invariants de similitude* de u.

(ii) Deux endomorphismes de V sont conjugués si, et seulement si, ils ont même invariants de similitudes.

DÉMONSTRATION — Pour $u \in \mathrm{End}_k(V)$, on considère le $k[X]$-module V_u. Il est de dimension finie comme k-espace vectoriel, donc *a fortiori* de type fini comme $k[X]$-module. On peut donc lui appliquer le Théorème 3.3. Il est de rang nul car il ne possède aucun sous-module isomorphe à $k[X]$ (de dimension infinie comme k-espace vectoriel). Le (i) et (ii) se déduisent alors de ce théorème et des Exemples 1.10 et 1.14. □

REMARQUE 3.5. (i) Comme la matrice compagnon $\mathrm{C}(P)$ a pour polynôme caractéristique P, on constate que le produit $P_1 \ldots P_s$ des invariants de similitudes de u est le polynôme caractéristique de u. De plus, le polynôme P_s est le polynôme minimal de u.

(ii) Cet énoncé contient la *décomposition de Jordan*. En effet, dans le cas particulier où u est nilpotent, les P_i sont de la forme X^{p_i}, et $\mathrm{C}(P_i)$ est alors un *bloc de Jordan*.

(iii) Soit u un endomorphisme d'un k-espace vectoriel V de dimension n, et soit $M \in \mathrm{M}_n(k)$ la matrice de u dans une certaine base de V. On peut montrer que les invariants de similitude de u sont les facteurs invariants non inversibles de la matrice $M - X1_n$ de $\mathrm{M}_n(k[X])$ (voir l'Exercice 8.18). Comme $k[X]$ est euclidien, cela fournit un procédé algorithmique pour déterminer les invariants de similitude de u.

(iv) Si on a $u \in \mathrm{M}_n(k)$ et si K est un surcorps de k, l'assertion d'unicité montre que les invariants de similitude de u sont les même que ceux de u vu dans $\mathrm{M}_n(K)$. On en déduit que si u et u' sont dans $\mathrm{M}_n(k)$, et s'ils sont conjugués dans $\mathrm{M}_n(K)$, alors ils sont conjugués dans $\mathrm{M}_n(k)$. (Un énoncé pas si facile à démontrer directement, notamment si k est fini).

4. Complément I : le groupe $\mathrm{SL}_n(A)$ et transvections

Quand l'anneau A est supposé euclidien, la démonstration du Théorème 2.4 peut-être rendue entièrement algorithmique, car c'est le cas des relations de Bézout :

THÉORÈME 4.1. *Si A est un euclidien, alors $\mathrm{SL}_n(A)$ est engendré par les transvections standards.*

Un corps étant trivialement euclidien, cet énoncé généralise la Proposition 3.5 Chap. 5. Dans le cas $A = \mathbb{Z}$, on a $\mathrm{T}_{i,j}(m) = \mathrm{T}_{i,j}(1)^m$ pour tout $m \in \mathbb{Z}$, de sorte que $\mathrm{SL}_n(\mathbb{Z})$ est engendré par les $\mathrm{T}_{i,j}(1)$ avec $1 \leqslant i \neq j \leqslant n$, qui sont en nombre fini.

COROLLAIRE 4.2. *Le groupe $\mathrm{SL}_n(\mathbb{Z})$ est de type fini.*

Le groupe infini $\mathrm{SL}_n(\mathbb{Z})$ est très intéressant, et intervient dans de nombreux aspects de la géométrie et de la théorie des nombres. Le cas $n = 2$ est tout particulièrement important. On pose

$$\mathrm{T} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad \mathrm{L} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \quad \text{et} \quad \mathrm{S} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Ce sont des éléments de $\mathrm{SL}_2(A)$ pour tout anneau A.

COROLLAIRE 4.3. $\mathrm{SL}_2(\mathbb{Z})$ *est engendré par* T *et* L*, ou encore par* S *et* T.

En effet, la première assertion se déduit du Théorème 4.1 et de la discussion ci-dessus. Pour la seconde, un petit calcul montre que l'on a $\mathrm{T}\,\mathrm{S} = \mathrm{L}\,\mathrm{T}^{-1}$.

DÉMONSTRATION — (Démonstration du Théorème 4.1) C'est une variante de la démonstration du Théorème 2.4 dans laquelle on part d'une matrice $M \in \mathrm{SL}_n(A)$ (avec $n = p = q$, donc). On ne s'autorise qu'à multiplier à gauche et à droite par des produits finis de transvections standards (équivalences *élémentaires*), et on veut aboutir à l'identité. On remplace dans la récurrence la fonction ν par un stathme euclidien φ sur A donné par hypothèse. Pour échanger deux lignes ou deux colonnes, on remplace τ par la matrice $\pm S$ ci-dessus (ce qui force à changer le signe d'une des deux lignes ou colonnes, celle que l'on veut, mais c'est sans indicence), qui est un produit de transvections par la formule $\mathrm{S} = \mathrm{T}^{-1}\,\mathrm{L}\,\mathrm{T}^{-1}$. Dans le Cas 1, on écrit plutôt $m_{1,j} = qm_{1,1} + r$ avec $\varphi(r) < \varphi(m_{1,1})$, et on remplace Q par la transvection $\mathrm{T}_{j,1}(-q)$. Idem dans le Cas 2. Après le Cas 2, on a $m_{i,1} = m_{1,j} = 0$ pour $i, j \neq 1$, et donc $m_{1,1} \in A^\times$ car alors $m_{1,1}$ divise $\det M = 1$. À ce stade il est plus simple de rajouter à la deuxième colonne $m_{1,1}^{-1}$ fois la première, de sorte que M contient le coefficient 1, puis de placer ce 1 en position $(1, 1)$, et de recommencer l'argument en supposant $m_{1,1} = 1$. □

REMARQUE 4.4. (i) Une autre démonstration du Corollaire 4.3, plus géométrique, consiste à faire agir $\mathrm{SL}_2(\mathbb{Z})$ par homographies sur $\widehat{\mathbb{C}} \smallsetminus \widehat{\mathbb{R}} = \mathbb{C} \smallsetminus \mathbb{R}$. Cette action préserve le demi-plan supérieur $\{\tau \in \mathbb{C} \mid \Im\,\tau > 0\}$, aussi appelé *demi-plan de Poincaré*. C'est l'un des points de départ de la théorie des *formes modulaires*, pour laquelle nous renvoyons au Ch. VII du cours d'arithmétique de Serre [**SER70**] ou encore aux notes de votre serviteur [**CHE15**].

(ii) P. Cohn et K. Dennis ont montré que pour $d < 0$, $\mathrm{SL}_2(\mathbb{Z}[\sqrt{d}])$ est engendré par les transvections si, et seulement si, $d = -1, -2, -3$. Noter que $\mathbb{Z}[\sqrt{-3}]$ n'est pas principal comme on l'a vu. Ils ont aussi montré que pour $d < 0$ et $d \equiv 1 \bmod 4$, alors $\mathrm{SL}_2(\mathbb{Z}[\frac{1+\sqrt{d}}{2}])$ est engendré par les transvections si, et seulement si, $d = -3, -7, -11$. En particulier, ce n'est pas le cas de $d = -19$, pour lesquels $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ est pourtant principal. En revanche, dans tous ces cas, $\mathrm{SL}_n(A)$ est engendré par les transvections pour $n \geqslant 3$.

(ii) Nous renvoyons à l'Exercice 8.15 pour un autre exemple particulièrement intéressant d'anneau A dans lequel $\mathrm{SL}_2(A)$ n'est pas engendré par les transvections (*exemple de Bass-Milnor-Serre*).

Discutons un peu plus certains aspects de la structure du groupe infini $\mathrm{SL}_n(\mathbb{Z})$. On rappelle que pour tout morphisme d'anneaux $f : A \to B$, on a un morphisme de groupes $\mathrm{GL}_n(A) \to \mathrm{GL}_n(B), (m_{i,j}) \mapsto (f(m_{i,j}))$, induisant un morphisme $\mathrm{SL}_n(A) \to \mathrm{SL}_n(B)$ si en outre A et B sont commutatifs. Appliquant cette observation au morphisme canonique $f : \mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$ de réduction modulo N, on en déduit un morphisme naturel $\mathrm{SL}_n(\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{Z}/N\mathbb{Z})$.

Corollaire 4.5. *Pour tout entier $n, N \geqslant 1$, le morphisme de groupes $\mathrm{SL}_n(\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{Z}/N\mathbb{Z})$, induit par la réduction modulo N des coefficients, est surjectif.*

Démonstration — En effet, l'anneau $\mathbb{Z}/N\mathbb{Z}$ est euclidien par la Remarque 6.2, donc le groupe $\mathrm{SL}_n(\mathbb{Z}/N\mathbb{Z})$ est engendré par les $\mathrm{T}_{i,j}(\overline{m})$ avec $m \in \mathbb{Z}$, par le Théorème 4.1. Mais cette transvection est l'image de $\mathrm{T}_{i,j}(m) \in \mathrm{SL}_n(\mathbb{Z})$ par le morphisme de l'énoncé, qui est donc surjectif. □

Le noyau du morphisme ci-dessus est le sous-groupe $\Gamma_n(N)$ des matrices $M \in \mathrm{SL}_n(\mathbb{Z})$ avec $M \equiv 1_n \bmod N$. On l'appelle *sous-groupe de congruence principal de niveau N*. C'est un sous-groupe distingué et d'indice fini de $\mathrm{SL}_n(\mathbb{Z})$. D'après le corollaire on a même un isomorphisme

$$\mathrm{SL}_n(\mathbb{Z})/\Gamma_n(N) \simeq \mathrm{SL}_n(\mathbb{Z}/N\mathbb{Z}). \tag{68}$$

Définition 4.6. *Un sous-groupe d'indice fini $\Gamma \subset \mathrm{SL}_n(\mathbb{Z})$ est dit de congruence s'il existe un entier $N \geqslant 1$ avec $\Gamma_n(N) \subset \Gamma$.*

Étant donné que l'on a $\cap_{N\geqslant 1} N\mathbb{Z} = \{0\}$, on a aussi $\cap_{N\geqslant 1}\Gamma_n(N) = \{1\}$. On dit que le groupe $\mathrm{SL}_n(\mathbb{Z})$ est *résiduellement fini*. Du coup, on peut se demander si tout sous-groupe d'indice fini de $\mathrm{SL}_n(\mathbb{Z})$ est de congruence. Un fait remarquable, démontré par Bass, Milnor et Serre[6], et indépendamment par Mennicke (1968), est que c'est le cas pour tout $n \geqslant 3$. On se propose dans ce qui suit de démontrer que cette propriété est fausse pour $\mathrm{SL}_2(\mathbb{Z})$, un énoncé plus ancien connu de Klein, Fricke et Pick, et dont la démonstration illustrera bien certaines notions du cours.

Théorème 4.7. (Klein, Fricke, Pick) *Il existe des sous-groupes d'indice fini de $\mathrm{SL}_2(\mathbb{Z})$ qui ne sont pas de congruence.*

6. H. Bass, J. Milnor & J.-P. Serre, *A solution of the congruence subgroup problem for* SL_n *($n \geqslant 3$) and* Sp_{2n} *($n \geqslant 2$)*, Publications Mathématiques de l'IHÉS 33 (1967).

Pour $N \geqslant 1$, on pose $\Gamma(N) = \Gamma_2(N)$. Pour démontrer le théorème, on commence par examiner la structure du sous-groupe $\Gamma(2)$. Il contient dans son centre la matrice -1_2, et il contient aussi les deux matrices

$$A = \mathrm{T}^2 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \quad \text{et} \quad B = \mathrm{L}^2 = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}.$$

Lemme 4.8. *On a* $\Gamma(2) = \langle -1_2, A, B \rangle$.

Démonstration — Soit $H = \langle A, B \rangle$ le sous-groupe de $\Gamma(2)$ engendré par A et B. Pour $g \in \Gamma(2)$ on pose $\mathrm{m}(g) = \mathrm{Min}\{|g_{1,1}|, |g_{1,2}|, |g_{2,1}|, |g_{2,2}|\}$. Observons que si on a $\mathrm{m}(g) = 0$ alors on a $g_{1,2} = 0$ ou $g_{2,1} = 0$ car $g_{1,1}$ et $g_{2,2}$ sont impairs, et donc $g_{1,1} = g_{2,2} = \pm 1$ et $\pm g \in \langle A \rangle \cup \langle B \rangle \subset H$. Sinon, il suffit par récurrence de montrer qu'il existe $h \in H$ avec $\mathrm{m}(gh) < \mathrm{m}(g)$ ou $\mathrm{m}(hg) < \mathrm{m}(g)$.

Quitte à remplacer g par sa transposée (la transposition préserve H et m) on peut supposer que l'on a $\mathrm{m}(g) = |g_{1,1}|$ ou $|g_{1,2}|$. Dans le cas $\mathrm{m}(g) = |g_{1,1}| > 0$, on constate que pour m bien choisi, le coefficient $(gA^{-m})_{1,2} = g_{1,2} - 2mg_{1,1}$ est $\leqslant |g_{1,1}|$, et donc $< |g_{1,1}|$ pour des raisons de parité. De même, dans le cas $\mathrm{m}(g) = |g_{1,2}| > 0$, pour m bien choisi, le coefficient $(gB^{-m})_{1,1} = g_{1,1} - 2mg_{1,2}$ est $\leqslant |g_{1,2}|$, et donc $< |g_{1,2}|$ pour des raisons de parité. □

Proposition 4.9. *Le sous-groupe* $\langle A, B \rangle$ *de* $\mathrm{SL}_2(\mathbb{Z})$ *est libre de rang* 2 *sur* $\{A, B\}$.

Démonstration — Soit F_2 le groupe libre sur l'ensemble à deux éléments $\{a, b\}$ (voir le Complément § 8 Chap. 2). Soit $f : \mathrm{F}_2 \to \mathrm{SL}_2(\mathbb{Z})$ le morphisme de groupes envoyant a sur A et b sur B. Par définition, l'image de f est $\langle A, B \rangle$, et on veut montrer son injectivité.

On considère pour cela l'action par homographies de $\mathrm{SL}_2(\mathbb{Z})$ sur $\widehat{\mathbb{R}} = \mathbb{R} \coprod \{\infty\}$. On pose $X = \{t \in \mathbb{R},\ |t| < 1\}$ et $Y = \{t \in \mathbb{R},\ |t| > 1\}$. On a $X \coprod Y \subset \widehat{\mathbb{R}}$ et

$$A^m X \subset Y \quad \text{et} \quad B^m Y \subset X \quad \text{pour tout} \quad m \in \mathbb{Z} \quad \text{non nul.} \tag{69}$$

En effet, pour $|t| < 1$ on a $|t + 2m| > 1$, et donc pour $|t| > 1$ on a aussi $|t/(2mt+1)| < 1$. Soit $w \in \mathrm{F}_2$ un mot réduit en a et b non trivial. Pour montrer $f(w) \neq 1$, on peut d'abord conjuguer w par une puissance convenable de b, puis de a, de sorte que l'on peut supposer que w est de la forme

$$w = a^{m_1} b^{m_2} a^{m_3} \cdots b^{m_{k-1}} a^{m_k}$$

avec $k \geqslant 3$ et les m_i, pour $i = 1, \ldots, k$, *tous non nuls*. Mais alors par (69) on constate que l'on a $f(w)(X) \subset Y$. Cela montre $f(w) \neq 1_2$ (cette méthode s'appelle *l'argument du ping pong* de J. Tits). □

Corollaire 4.10. *On a* $\Gamma(2) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathrm{F}_2$.

Démonstration — L'élément -1_2 est dans le centre de $\Gamma(2)$. Le Lemme 4.8 montre $\Gamma(2) = \{\pm 1_2\} H$ avec $H = \langle A, B \rangle$. Pour voir que c'est un produit direct interne de $\{\pm 1_2\}$ et H, il suffit de justifier $-1_2 \notin H$. Pour cela, il suffit d'observer que tout élément de H a ses coefficient diagonaux $\equiv 1 \bmod 4$, ce qui n'est pas le cas de -1_2. On conclut par la Proposition 4.9. □

Corollaire 4.11. *Pour tout entier $n \geqslant 1$, il existe un morphisme de groupes surjectif* $\Gamma(2) \to \mathrm{A}_n$.

Démonstration — Le groupe A_n est engendré par deux éléments. Par exemple, pour n impair, le 3-cycle $(1\,2\,3)$ et le n-cycle standard $(1\,2\,\cdots\,n)$ conviennent, car le groupe engendré contient tous les $(i\ i+1\ i+2)$ avec $1 \leqslant i \leqslant n-2$ et ces derniers engendrent A_n (voir l'Exercice 4.6). Pour n pair, le 3-cycle $(1\,2\,3)$ et le $n-1$-cycle $(2\,3\,\cdots\,n)$ conviennent, car les $(1\ i\ i{+}1)$ engendrent aussi A_n à cause par exemple de l'identité $(1\ i\ i+1)(1\ i+1\ i+2) = (i\ i+1\ i+2)$. Ainsi, par la propriété universelle du groupe libre, il existe un morphisme surjectif $\mathrm{F}_2 \to \mathrm{A}_n$, et on conclut en le composant avec le morphisme $\Gamma(2) \to \mathrm{F}_2$ donné par le Corollaire 4.10. □

Pour démontrer le Théorème 4.7, il suffit donc de démontrer la :

Proposition 4.12. *Pour $n \geqslant 6$, le noyau d'un morphisme surjectif* $\Gamma(2) \to \mathrm{A}_n$ *n'est pas de congruence.*

Démonstration — Soit $f : \Gamma(2) \to \mathrm{A}_n$ un morphisme surjectif et notons H son noyau. Supposons H de congruence, disons $H \supset \Gamma(N)$ pour un certain $N \geqslant 1$. L'inclusion $T^N \subset \Gamma(N) \subset H \subsetneq \Gamma(2)$ montre $N \equiv 0 \bmod 2$ et $N > 2$. Comme $\Gamma(N)$ est distingué dans $\Gamma(2)$, et que A_n est simple pour $n \geqslant 6$, le groupe $\Gamma(2)/\Gamma(N)$ a donc un facteur de Jordan-Hölder [7] isomorphe à A_n, ainsi donc que $\mathrm{SL}_2(\mathbb{Z})/\Gamma(N) \simeq \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, car $\Gamma(2)$ est distingué dans $\mathrm{SL}_2(\mathbb{Z})$.

Or on connaît les facteurs de Jordan-Hölder de $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ d'après le Lemme 4.13 suivant : oubliant les multiplicités, ce sont ceux des groupes $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ avec $p|N$, ainsi que $\mathbb{Z}/p\mathbb{Z}$ si p^2 divise N. D'après le Théorème 3.1 Chap. 5, les facteurs de Jordan-Hölder de $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ sont $\mathbb{Z}/2\mathbb{Z}$ et le groupe simple $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ pour $p \geqslant 5$, et par les isomorphismes miraculeux, ce sont $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$ pour $p = 2, 3$. Aucun d'entre eux n'est isomorphe à A_n pour $n \geqslant 6$ d'après la Proposition 4.8 Chap. 5. [8] □

Dans la démonstration ci-dessus, on a utilisé le dévissage suivant du groupe fini $\mathrm{SL}_n(\mathbb{Z}/N\mathbb{Z})$, dans lequel $n \geqslant 1$ est un entier arbitraire.

Lemme 4.13. *(i) Pour $M, N \geqslant 1$ premiers entre eux on a un isomorphisme*

$$\mathrm{SL}_n(\mathbb{Z}/MN\mathbb{Z}) \xrightarrow{\sim} \mathrm{SL}_n(\mathbb{Z}/M\mathbb{Z}) \times \mathrm{SL}_n(\mathbb{Z}/N\mathbb{Z}).$$

(ii) Pour tout p premier et $m \geqslant 1$, on a une suite exacte courte

$$1 \longrightarrow (\mathbb{Z}/p\mathbb{Z})^{n^2-1} \longrightarrow \mathrm{SL}_n(\mathbb{Z}/p^{m+1}\mathbb{Z}) \longrightarrow \mathrm{SL}_n(\mathbb{Z}/p^m\mathbb{Z}) \longrightarrow 1.$$

Démonstration — Pour le (i), on utilise l'isomorphisme chinois et le fait immédiat suivant. Si $f : A \times B \to C$ est un isomorphisme entre anneaux commutatifs, alors $((a_{i,j}), (b_{i,j})) \mapsto (f(a_{i,j}, b_{i,j})_{i,j})$ est un isomorphisme de groupes $\mathrm{SL}_n(A) \times \mathrm{SL}_n(B) \to \mathrm{SL}_n(C)$.

Pour le (ii), le morphisme d'anneaux $\mathbb{Z}/p^{m+1}\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ de réduction modulo p^m induit un morphisme de groupes $f : \mathrm{SL}_n(\mathbb{Z}/p^{m+1}\mathbb{Z}) \longrightarrow \mathrm{SL}_n(\mathbb{Z}/p^m\mathbb{Z})$. Ce morphisme

7. Nous renvoyons au Complément §8 Chap. 2 pour la notion de facteur de Jordan-Hölder.

8. Notons que l'on a utilisé sans le dire le théorème de Jordan-Hölder (Théorème 8.3 Chap. 2), on aurait pu s'en passer mais c'est tout de même agréable et intuitif ici de l'utiliser.

est surjectif car son image contient les transvections standards de $\mathrm{SL}_n(\mathbb{Z}/p^m\mathbb{Z})$, et ces dernières sont génératrices comme on l'a vu dans la démonstration du Corollaire 4.5. Il ne reste qu'à étudier son noyau $\ker f$.

Soit $M \in \mathrm{M}_n(\mathbb{Z}/p^{m+1}\mathbb{Z})$ dont la réduction modulo p^m est l'identité. On peut écrire $M \equiv 1_n + p^m X$ pour un certain $X \in \mathrm{M}_n(\mathbb{Z})$ dont la réduction modulo p est uniquement déterminée par M : on la note $r(M)$. En utilisant la congruence $p^{2m} \equiv 0 \bmod p^{m+1}$ dans $\mathbb{Z}$, on constate par multilinéarité alternée du déterminant

$$\det M \equiv \det(1_n + p^m X) \equiv 1 + p^m \mathrm{tr}\, X \bmod p^{m+1}.$$

On en déduit que l'on a $M \in \ker f \iff \mathrm{tr}\, r(M) = 0$. Ainsi, $r : M \mapsto r(M)$ définit une bijection entre $\ker f$ et le sous-groupe $V \subset \mathrm{M}_n(\mathbb{Z}/p\mathbb{Z})$ des matrices de trace nulel. Ce dernier est un sous $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel de codimension 1, donc isomorphe à $(\mathbb{Z}/p\mathbb{Z})^{n^2-1}$, et il ne reste qu'à vérifier que r est un morphisme de groupes $\ker f \to V$. Mais si on a $M = 1_n + p^m X$ et $N = 1_n + p^m Y$ avec $X, Y \in \mathrm{M}_n(\mathbb{Z})$, on a

$$MN = (1_n + p^m X)(1_n + p^m Y) \equiv 1_n + p^m(X + Y) \bmod p^{m+1}\mathrm{M}_n(\mathbb{Z})$$

toujours car $p^{2m} \equiv 0 \bmod p^{m+1}$, ce qui signifie exactement $r(MN) = r(M) + r(N)$. $\square$

5. Complément II : deux démonstrations de l'assertion d'unicité

Dans ce complément nous détaillons deux démonstrations de l'assertion d'unicité du Théorème 3.3.

5.1. Méthode 1 : une variante du cas $A = \mathbb{Z}$. On explique d'abord comment montrer cette unicité en utilisant une variante de l'argument donné dans le cas $A = \mathbb{Z}$ au Chapitre 3.

Pour tout anneau intègre A, et tout A-module M, posons

$$M_{\mathrm{tor}} = \{m \in M \mid \exists a \in A \smallsetminus \{0\},\ am = 0\}.$$

C'est alors un sous-module de M appelé *sous-module de torsion* (et ses éléments sont les *éléments de torsion* de M). Tout isomorphisme A-linéaire $M \simeq N$ induit un isomorphisme A-linéaire $M_{\mathrm{tor}} \simeq N_{\mathrm{tor}}$. Si M est comme dans l'énoncé, la torsion du module de droite est $\{0\} \oplus A/a_1A \oplus A/a_2A \oplus \cdots \oplus A/a_nA$ et en particulier on a $M/M_{\mathrm{tor}} \simeq A^r$. Le Théorème 1.18 conclut alors l'unicité du r, et on peut donc supposer $r = 0$ et $M = M_{\mathrm{tor}}$.

On procède alors de manière similaire à l'argument d'unicité dans le théorème de structure des groupes abéliens finis (Théorème 3.1 Chap. 3, voir la fin de la Section 3). Pour une suite $a = (a_1 \mid a_2 \mid \cdots \mid a_n)$ d'éléments non nuls de A on pose

$$M_a := A/a_1A \oplus A/a_2A \oplus \cdots \oplus A/a_nA.$$

On suppose $M_a \simeq M_b$ avec $b = (b_1 \mid b_2 \mid \cdots \mid b_m)$ et on veut montrer $n = m$ et $a_i \sim b_i$ pour tout $i = 1, \ldots, n$. On raisonne par récurrence sur l'entier r somme de $n + m$ et du nombre miminal de diviseurs irréductibles de a_nb_m (comptés avec multiplicités). Le cas minimal $r = 2$ est trivial. De plus, si a_1 et b_1 sont des unités, on peut supprimer a_1 et b_1 et donc diminuer $n + m$ de 2 et conclure par récurrence.

Disons que a_1 est non inversible, et choisissons un facteur irréductible π de a_1, qui divise alors tous les a_i. Pour M un A-module quelconque, on pose

$$M[\pi] = \{x \in M \mid \pi x = 0\}.$$

C'est un $A/\pi A$-module de manière naturelle, via $(a + \pi A, x) \mapsto ax$, donc un espace vectoriel sur le corps $k = A/\pi A$ (Corollaire 9.16). On a un isomorphisme de $A/\pi A$-espaces vectoriels $M_a[\pi] \simeq M_b[\pi]$ car on a $M_a \simeq M_b$. Mais on constate que pour $f \in A$, on a $(A/fA)[\pi] = \{0\}$ si π est premier avec f (par Bézout), et $A/fA[\pi] = gA/fA \simeq A/\pi A$ (de dimension 1 sur k) si $f = \pi g$. On a donc

$$n = \dim_k M_a[\pi] = \dim_k M_b[\pi]$$

et n éléments b_i sont divisibles par π. Cela montre d'abord $n \leqslant m$, puis $m \leqslant n$ par symétrie, et donc $n = m$ et π divise tous les b_i. Posons maintenant

$$\pi M = \{\pi x \mid x \in M\},$$

encore un sous-A-module de M. Pour $f = \pi g \in A$ avec $g \in A$, on constate que le A-module $\pi A/fA$ est isomorphe à A/gA. Ainsi, on a $\pi M_a \simeq M_{a'}$ avec $a'_i = a_i/\pi$, $\pi M_b \simeq M_{b'}$ avec $b'_i = b_i/\pi$ et $M_{a'} \simeq M_{b'}$ car $M_a \simeq M_b$. On conclut donc par récurrence, car $b'_n b_n$ a deux diviseurs irréductibles de moins que $a_n b_m$.

5.2. Méthode 2 : une preuve par les idéaux de Fitting. Cette autre démonstration, à la fois plus générale et plus dans l'esprit des arguments de la Section 2, est basée sur la construction des *idéaux de Fitting*[9] d'un module de type fini. Soient A un anneau commutatif noethérien,[10] et M un A-module de type fini. Fixons $\underline{g} = (g_1, \ldots, g_p)$ une famille génératrice de M, avec $p = |\underline{g}|$, et notons

$$\pi_{\underline{g}} : A^p \longrightarrow M, \quad (a_1, \ldots, a_p) \mapsto \sum_{i=1}^{p} a_i g_i,$$

la surjection A-linéaire associée. Le noyau de $\pi_{\underline{g}}$ est un sous-A-module de A^p appelé *module des relations entre les éléments de* $\underline{g}$. Il est de type fini car A est noethérien. Soit $\underline{r} = (r_1, \ldots, r_q)$ une famille génératrice du A-module $\ker \pi_{\underline{g}}$. On a une application linéaire $u_{\underline{g},\underline{r}} : A^q \longrightarrow A^p$, $(x_i) \mapsto \sum_{i=1}^{q} x_i r_i$, d'image $\ker \pi_{\underline{g}}$. Si on écrit $r_j = (a_{1,j}, a_{2,j}, \ldots, a_{p,j})$, la matrice de $u_{\underline{g},\underline{r}}$ dans les bases canoniques respectives est

$$M_{\underline{g},\underline{r}} := \mathrm{Mat}_{\mathrm{can},\mathrm{can}}\, u_{\underline{g},\underline{r}} = (a_{i,j}) \in \mathrm{M}_{p,q}(A).$$

On rappelle que l'on a défini $\mathrm{c}_k(N)$ pour tout $N \in \mathrm{M}_{p,q}(A)$ et $k \in \mathbb{Z}$.

Lemme 5.1. *Dans les notations ci-dessus, et pour tout $i \in \mathbb{Z}$, l'idéal $\mathrm{c}_{p-i}(M_{\underline{g},\underline{r}})$ de A ne dépend que de la classe d'isomorphisme du A-module de type fini M.*

La présence du $-i$ (plutôt que $+i$) est faite pour coller avec la convention usuelle d'indexation des idéaux de Fitting dans la Définition 5.2 ci-dessous. Bien noter en revanche que p désigne ci-dessus le cardinal de $\underline{g}$.

Démonstration — Supposons d'abord $\underline{g}$ fixée, et que $\underline{r'}$ est réunion de $\underline{r}$ et d'une autre relation. La matrice $M_{\underline{g},\underline{r'}}$ est dans $\mathrm{M}_{p,q+1}(A)$ et est obtenue à partir de $M_{\underline{g},\underline{r}}$ en ajoutant une colonne qui est combinaison A-linéaire des autres. On a donc clairement

9. H. Fitting, *Die Determinantenideale eines Moduls*, Jahresbericht der Deutschen Mathematiker-Vereinigung, p. 195–228 (1936).

10. L'hypothèse noethérienne est en fait inutile, mais nous la faisons pour simplifier l'argument.

$\mathrm{c}_k(M_{\underline{g},\underline{r}'}) = \mathrm{c}_k(M_{\underline{g},\underline{r}})$ pour tout $k \in \mathbb{Z}$. On en déduit que cette égalité vaut plus généralement pour tout $\underline{r}$ et $\underline{r}'$, en ajoutant un à un les éléments de $\underline{r}'$ à $\underline{r}$, puis en supprimant un à un ceux de $\underline{r}$.

Supposons maintenant que la famille génératrice $\underline{g}'$ est obtenue à partir de $\underline{g}$ en rajoutant un seul élément, disons l'élément $g_{p+1} \in M$. Écrivons $g_{p+1} = \sum_{i=1}^{p} a_i g_i$. On constate que le noyau de $\pi_{\underline{g}'}$ est le sous-module de A^{q+1} engendré par la famille $\underline{r}'$ constituée des $r_i \times 0$ avec $r_i \in \underline{r}$ et par l'élément $x = (-a_1, -a_2, \ldots, -a_p, 1)$. En effet, si $v = (b_1, \ldots, b_q)$ est dans $\ker \pi_{\underline{g}'}$ alors $v - b_q x$ est dans $(\ker \pi_{\underline{g}'}) \cap (A^q \times \{0\}) = (\ker \pi_{\underline{g}}) \times \{0\}$. On a donc l'égalité matricielle

$$M_{\underline{g}',\underline{r}'} = \begin{bmatrix} M_{\underline{g},\underline{r}'} & X \\ 0_{1\times q} & 1 \end{bmatrix} \in \mathrm{M}_{p+1,q+1}(A), \text{ avec } X = \begin{bmatrix} -a_1 & \vdots & -a_p \end{bmatrix} \in A^p.$$

On a alors $\mathrm{c}_{k+1}(M_{\underline{g}',\underline{r}'}) = \mathrm{c}_k(M_{\underline{g},\underline{r}})$. En effet, tout mineur de taille $1 \leqslant k \leqslant \min(p,q)$ de $M_{\underline{g},\underline{r}}$ est un mineur de taille $k+1$ de $M_{\underline{g}',\underline{r}'}$ (ajouter la dernière ligne et la dernière colonne). De même, tout mineur de taille $k+1$ de $M_{\underline{g}',\underline{r}'}$ est soit nul, soit un mineur de taille k ou $k+1$ de $M_{\underline{g},\underline{r}}$, et donc dans $\mathrm{c}_k(M_{\underline{g},\underline{r}})$ dans tous les cas, ce qui conclut. Au final, on en déduit que l'idéal $\mathrm{c}_{|\underline{g}|+k}(M_{\underline{g},\underline{r}})$, dont on sait déjà qu'il ne dépend pas de $\underline{r}$, ne dépend pas non plus du choix de $\underline{g}$: pour deux familles génératrices $\underline{g}$ et $\underline{g}'$ on passe de $\underline{g}$ à $\underline{g} \cup \underline{g}'$ en ajoutant un par un les éléments de $\underline{g}'$, puis à $\underline{g}'$ en enlevant un par un les éléments de $\underline{g}$.

On a montré que M étant donné, l'idéal de l'énoncé ne dépend pas des choix de $\underline{g}$ et $\underline{r}$. Enfin, si $f : M' \xrightarrow{\sim} M$ est un isomorphisme de A-modules, et si on pose $\underline{g}' = f^{-1}(\underline{g})$, on a clairement $M_{\underline{g},\underline{r}} = M'_{\underline{g}',\underline{r}}$, d'où la dernière assertion. □

Définition 5.2. *Pour tout $i \in \mathbb{Z}$ l'idéal du Lemme 5.1 est appelé i-ème idéal de Fitting du A-module de type fini M, et noté* $\mathrm{Fitt}_i(M)$. *Il ne dépend que de la classe d'isomorphisme de M.*

Pour conclure l'unicité, il ne reste qu'à déterminer les $\mathrm{Fitt}_k(M)$ avec $M = A^r \oplus A/a_1A \oplus \cdots \oplus A/a_nA$ et $a_1 \,|\, a_2 \,|\, \cdots \,|\, a_n$ et les $a_i \in A$ non nuls. En utilisant les générateurs et relations évidents définissant M on a pour tout $k \in \mathbb{Z}$

$$\mathrm{Fitt}_k(M) = \mathrm{c}_{n+r-k}(D) \text{ avec } D = \begin{bmatrix} a_1 & & & \\ & a_2 & & \\ & & \ddots & \\ & & & a_n \end{bmatrix}.$$

On a déjà vu $\mathrm{c}_i(D) = a_1 \cdots a_i A$ pour $1 \leqslant i \leqslant n$ en fin de Section 2, et on a $\mathrm{c}_i(D) = 0$ pour $i > n$. Autrement dit, on a $\mathrm{Fitt}_k(M) = \{0\}$ pour $k < r$, et pour $r \leqslant k < r+n$ on a $\mathrm{Fitt}_r(M) = a_1 a_2 \cdots a_{n+r-k} A$ (non nul). Cela montre l'unicité du r et des a_i modulo association. ▫

Remarque 5.3. Par définition on a $\mathrm{Fitt}_i(M) = \{0\}$ pour $i < 0$ et $\mathrm{Fitt}_i(M) \subset \mathrm{Fitt}_{i+1}(M)$ pour tout $i \in \mathbb{Z}$ (un mineur de taille $k+1$ est toujours combinaison A-linéaire de mineurs de taille k, en développant une colonne). D'une certaine manière, $\mathrm{Fitt}_i(M)$ mesure l'aptitude de M à être engendré par i éléments.

6. Exercices

Exercice 8.1. *Soient k un corps et $n \geqslant 1$ un entier. Montrer qu'il est équivalent de se donner un $k[X_1, \ldots, X_n]$-module et un k-espace vectoriel V muni de n endomorphismes $u_1, \ldots, u_n \in \mathrm{End}_k(V)$ vérifiant $u_i u_j = u_j u_i$ pour tout $1 \leqslant i, j \leqslant n$.*

Exercice 8.2. *Soit k un anneau à division.*[11]

(i) Montrer que tout k-module de type fini est libre.

(ii) Montrer que l'on a un isomorphisme de k-modules $k^n \simeq k^m$ si, et seulement si, $n = m$.

Exercice 8.3. *On rappelle que $\mathbb{H}$ désigne l'anneau des quaternions de Hamilton.*

(i) Montrer qu'il est équivalent de se donner un $\mathbb{H}$-module et un $\mathbb{R}$-espace vectoriel V muni de deux endomorphismes I et J vérifiant $I^2 = J^2 = -\mathrm{id}_V$ et $IJ = -JI$.

(ii) Montrer que si l'on a $I, J \in \mathrm{M}_n(\mathbb{R})$ avec $I^2 = J^2 = -\mathrm{I}_n$ et $IJ = -JI$, alors $n \equiv 0 \bmod 4$.

On rappelle qu'un corps k est dit *de caractéristique* 0 si pour tout entier $n \geqslant 1$ on a $n.1 \in k^\times$.

Exercice 8.4. *Soient k un corps, $V = k[t]$ le k-espace vectoriel des polynômes en t, $u : V \to V$, $P \mapsto P'$, l'application de dérivation (k-linéaire), et $M = V_u$ le $k[X]$-module associé.*

(i) Montrer que M n'est pas de type fini.

(ii) On suppose k de caractéristique 0. Montrer que tous les sous-modules N de M avec $N \neq M$ sont monogènes.

Exercice 8.5. (Algèbre de Weyl) *Soient k un corps et V le k-espace vectoriel $k[X]$. On note W_k le sous anneau de $\mathrm{End}_k(V)$ engendré par $k\,\mathrm{id}_V$ et les endomorphismes x et y définis par $x(P) = XP$ et $y(P) = P'$. On verra V comme un W_k-module. Dans les questions (i) et (iii) on suppose k de caractéristique 0.*

(i) Montrer que les seuls sous-modules de V sont $\{0\}$ et V.

(ii) Déterminer $yx - xy$ dans l'anneau W_k.

(iii) Soit M un W_k-module de k-espace vectoriel sous-jacent de dimension finie. Montrer $M = \{0\}$.

(iv) On suppose maintenant $k = \mathbb{Z}/p\mathbb{Z}$. Montrer que (i) et (iii) sont en défaut.

On rappelle que si A est un anneau non nécessairement commutatif, un idéal à gauche (resp. à droite, resp. bilatère) de A est un sous-groupe additif $I \subset A$ tel que pour tout $a \in A$ et tout $x \in I$ on a $ax \in I$ (resp. $xa \in I$, resp ax et $xa \in I$). Un idéal à gauche (resp. à droite) de A est dit principal s'il est de la forme Aa (resp. aA) pour un certain $a \in A$.

11. C'est-à-dire, un anneau non nul dans lequel tout élément non nul est inversible.

EXERCICE 8.6. *Soit A un anneau. Montrer que tout idéal bilatère de $\mathrm{M}_n(A)$ est de la forme $\mathrm{M}_n(I)$ avec I un idéal bilatère de A.*

EXERCICE 8.7. (Idéaux de $\mathrm{M}_n(k)$) *Soient k un corps, V un k-espace vectoriel de dimension finie n et $A = \mathrm{End}_k(V)$. On se propose de déterminer les idéaux à droite, et les idéaux à gauche, de l'anneau A. Pour $W \subset V$ un sous-espace de V on note $I_W \subset A$ le sous-ensemble des $u \in A$ avec $W \subset \ker u$, et $J_W \subset A$ le sous-ensemble des $u \in A$ avec $\mathrm{Im}\, u \subset W$.*

(i) Montrer que I_W est un idéal à gauche principal de A.

(ii) Montrer que $W \mapsto I_W$ est une bijection décroissante entre sous-espaces de V et idéaux à gauche de A.

(iii) Montrer que J_W est un idéal à droite principal de A.

(iv) Montrer que $W \mapsto J_W$ est une bijection croissante entre sous-espaces de V et idéaux à droite de A.

EXERCICE 8.8. *Déterminer le nombre d'idéaux à gauche de l'anneau $\mathrm{M}_n(\mathbb{Z}/p\mathbb{Z})$ pour p un nombre premier.*

Si $(A, +, \cdot)$ est un anneau, son anneau *opposé* est l'anneau $(A, +, \star)$ avec $x \star y = yx$ (justifier que c'est bien un anneau !). On le note A^{opp}. Si A est commutatif, on a bien sûr $A = A^{\mathrm{opp}}$. Si M est un A-module on notera $\mathrm{End}_A(M)$ l'anneau des endomorphismes A-linéaires de M (pour $+$ et $\circ$).

EXERCICE 8.9. (Sur l'anneau opposé) *Soient A un anneau et $n \geqslant 1$ un entier.*

(i) Montrer que l'on a un isomorphisme d'anneaux $\mathrm{M}_n(A)^{\mathrm{opp}} \simeq \mathrm{M}_n(A^{\mathrm{opp}})$.

(ii) (suite) Qu'en déduire si A est commutatif ?

(iii) Montrer que $u \mapsto u(1)$ induit un isomorphisme d'anneaux $\mathrm{End}_A(A) \xrightarrow{\sim} A^{\mathrm{opp}}$.

(iv) Plus généralement, soient M un A-module libre de rang n et $e_1, \ldots, e_n$ une base de M. Pour $u \in \mathrm{End}_A(M)$ on note $\mathrm{Mat}_e u = (u_{i,j}) \in \mathrm{M}_n(A)$ l'élément déterminé par les relations $u(e_j) = \sum_{i=1}^n u_{i,j} e_i$, pour $1 \leqslant j \leqslant n$. Montrer que

$$\mathrm{End}_A(M) \to \mathrm{M}_n(A^{\mathrm{opp}}), u \mapsto \mathrm{Mat}_e u,$$

est un isomorphisme d'anneaux.

EXERCICE 8.10. *Soient V le k-espace vectoriel $k^{(\mathbb{N})}$ et $A = \mathrm{End}_k(V)$.*

(i) Montrer que les A-modules A et A^2 sont isomorphes.

(ii) Montrer que les k-algèbres A et $\mathrm{M}_2(A)$ sont isomorphes.

On rappelle la notion d'idéaux équivalents introduite dans l'Exercice 7.9.

EXERCICE 8.11. (Idéaux équivalents, partie II) *Soit A un anneau commutatif intègre de corps de fractions K.*

(i) Montrer que deux idéaux de A sont équivalents si, et seulement si, ils sont isomorphes en tant que A-modules.

(ii) Soit M un idéal fractionnaire *de K, c'est-à-dire un sous-A-module de K tel qu'il existe $a \in A$ non nul avec $aM \subset A$. Montrer que M est isomorphe à un idéal de A.*

(iii) Soit M un sous-A-module de type fini d'un K-espace vectoriel de dimension 1. Montrer que M est isomorphe à un idéal de A.

Exercice 8.12. *Soit $d \in \mathbb{Z}$ non carré. Notons $\mathrm{S}_2(d)$ l'ensemble des matrices $S \in \mathrm{M}_2(\mathbb{Z})$ avec $S^2 = d\mathrm{I}_2$. Le groupe $\mathrm{GL}_2(\mathbb{Z})$ agit par conjugaison sur $\mathrm{S}_2(d)$ et on notera $\mathrm{Cl}(d)$ l'ensemble de ses orbites (classes de conjugaison).*

(i) Montrer $\mathrm{S}_2(d) \neq \varnothing$.

(ii) Soit $S \in \mathrm{M}_2(\mathbb{Z})$. Vérifier $S \in \mathrm{S}_2(d) \iff \operatorname{tr} S = 0$ et $\det S = -d$.

(iii) Montrer qu'il existe des bijections entre :

(a) $\mathrm{Cl}(d)$,

(b) classes d'isomorphisme de structures de $\mathbb{Z}[\sqrt{d}]$-modules sur $\mathbb{Z}^2$,

(c) classes d'équivalence d'idéaux non nuls de $\mathbb{Z}[\sqrt{d}]$.

(iv) En déduire des représentants de $\mathrm{Cl}(d)$ pour $d = -2, -1, 2$.

(v) On suppose que l'entier d est un carré modulo $n \in \mathbb{Z}$, et $|\mathrm{Cl}(d)| = 1$. Montrer que $\pm n$ est de la forme $a^2 - db^2$ avec $a, b \in \mathbb{Z}$.

(vi) En considérant l'idéal $(2, \sqrt{-3} + 1)$ de $\mathbb{Z}[\sqrt{-3}]$, exhiber deux éléments de $\mathrm{S}_2(-3)$ non conjugués.

L'exercice suivant fait suite au précédent.

Exercice 8.13. *Soit $d \in \mathbb{Z}$ non carré. Pour $a, b, c \in \mathbb{Z}$ on pose*

$$[a, b, c] := \begin{bmatrix} b & c \\ a & -b \end{bmatrix} \in \mathrm{M}_2(\mathbb{Z}).$$

On a donc $[a, b, c] \in \mathrm{S}_2(d) \iff b^2 + ac = d$ (auquel cas a et c sont non nuls).

(i) Montrer que $[a, b, c]$ est $\mathrm{GL}_2(\mathbb{Z})$-conjugué à

$$[-a, b, -c],\ [c, -b, a],\ [a, b + a, c - a - 2b] \text{ et } [a, b - a, c - a + 2b].$$

(ii) Soit $[a, b, c] \in \mathrm{S}_2(d)$. Montrer que $[a, b, c]$ est $\mathrm{GL}_2(\mathbb{Z})$-conjugué à $[a', b', c']$ avec $2|b| \leqslant a \leqslant |c|$, puis l'inégalité $1 \leqslant a \leqslant 2\sqrt{|d|/3}$.

(iii) En déduire que les ensembles de la question (iii) de l'Exercice 8.12 sont finis.

(iv) Redémontrer la principalité de $\mathbb{Z}[\sqrt{d}]$ pour $d = -2, -1, 2$.

(v) Montrer les égalités

$$\mathrm{Cl}(3) = \{\overline{[1, 0, 3]}\},\ \mathrm{Cl}(-3) = \{\overline{[1, 0, -3]}, \overline{[2, 1, -2]}\} \text{ et } \mathrm{Cl}(5) = \{\overline{[1, 0, 5]}, \overline{[2, 1, 2]}\}.$$

(vi) En déduire que $\mathbb{Z}[\sqrt{3}]$ est principal, mais pas $\mathbb{Z}[\sqrt{5}]$.

Exercice 8.14. *Pour $N \geqslant 1$ on note $\Gamma(N)$ le sous-groupe des matrices $M \in \mathrm{SL}_2(\mathbb{Z})$ telles que $M \equiv \mathrm{I}_2 \bmod N$.*

(i) Montrer que $\Gamma(N)$ est un sous-groupe distingué d'indice fini de $\mathrm{SL}_2(\mathbb{Z})$.

(ii) Montrer que $\Gamma(2)$ *est engendré par* $\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$, $\begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$ *et* $-\mathrm{I}_2$.

(iii) (suite) Montrer qu'on ne peut pas supprimer $-\mathrm{I}_2$ *dans cet énoncé.*

(iv) Montrer qu'il existe un isomorphisme de groupes $\Gamma(N)/\Gamma(N^2) \simeq (\mathbb{Z}/N\mathbb{Z})^3$. *(On pourra utiliser le (ii) de l'exercice précédent).*

(v) En déduire que pour $N > 2$, *le groupe* $\Gamma(N)$ *n'est pas engendré par* $-\mathrm{I}_2$ *et deux transvections.*

Exercice 8.15. (L'exemple de Bass-Milnor-Serre) *Soient* $A = \mathbb{R}[\cos t, \sin t]$ *l'anneau*[12] *des polynômes trigonométriques* 2π*-périodiques sur* $\mathbb{R}$. *On se propose de montrer que l'élément*

$$\begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix} \in \mathrm{SL}_2(A)$$

n'est pas un produit de transvections. On verra $G = \mathrm{SL}_2(\mathbb{R})$ *comme le fermé de* $\mathrm{M}_2(\mathbb{R})$ *défini par* $\det = 1$. *On note* B *le sous-groupe des matrices triangulaires supérieures de* G, *et on pose* $K = \mathrm{SO}_2(\mathbb{R})$.

(i) Montrer que K *et* B *sont homéomorphes à* S^1 *et* $\mathbb{R}^2$ *respectivement.*

(ii) Montrer que la multiplication de G *induit un homéomorphisme* $K \times B \simeq G$.

(iii) Montrer, ou admettre, qu'il n'existe pas d'application continue

$$f : [0,1]^2 \to \mathrm{S}^1, (s,t) \mapsto f(s,t),$$

avec $f(0,t) = e^{2i\pi t}$ *et* $f(1,t) = f(s,0) = f(s,1) = 1$ *pour tout* $s, t \in [0,1]$.

(iv) Conclure.

Exercice 8.16. *Soient* A *un anneau principal,* $n \geqslant 2$ *et* $a_1, \ldots, a_n \in A$ *premiers entre eux dans leur ensemble.*

(i) En considérant une forme linéaire adéquate $A^n \to A$, $(x_i) \mapsto \sum_{i=1}^n b_i x_i$, *montrer que le vecteur* $(a_1, \ldots, a_n) \in A^n$ *se complète en une base de* A^n.

(ii) En déduire qu'il existe un élément de $\mathrm{SL}_n(A)$ *de première ligne* $(a_1, \ldots, a_n)$.

L'exercice suivant généralise substantiellement l'Exercice 7.8.

Exercice 8.17. *Soit* $M \simeq \mathbb{Z}^n$ *un groupe abélien libre de rang fini, et soit* $u : M \to M$ *une application* $\mathbb{Z}$*-linéaire injective. Montrer que* $u(M)$ *est un sous-groupe d'indice fini* $|\det u|$ *de* M.

Exercice 8.18. *Soient* k *un corps,* V *un* k*-espace vectoriel de dimension finie* $n \geqslant 1$, $u \in \mathrm{End}_k(V)$, e *une base de* V *et* $M = \mathrm{Mat}_e u \in \mathrm{M}_n(k)$. *On se propose de montrer que les invariants de similitude de* u *sont les facteurs invariants non inversibles de la matrice* $M - X1_n$ *vue comme élément de* $\mathrm{M}_n(k[X])$.

(i) On suppose d'abord $M = \mathrm{C}(P)$ *avec* $P \in k[X]$ *unitaire de degré* n. *Montrer que les facteurs invariants de* $\mathrm{C}(P) - X1_n \in \mathrm{M}_n(k[X])$ *sont* $\sim 1, 1, \ldots, 1, P$.

(ii) Conclure.

12. Cet anneau a déjà été étudié dans l'Exercice 7.18.

Chapitre 9

Représentations linéaires des groupes finis

1. Représentations linéaires

Dans cette partie et la suivante, G désigne un groupe et k un corps, tous deux quelconques.

DÉFINITION 1.1. *Une représentation k-linéaire de G est la donnée d'un k-espace vectoriel V et d'un morphisme de groupes $\rho : G \to \mathrm{GL}(V)$.*

On parle aussi de représentation de G *sur* l'espace vectoriel V. L'inclusion $\mathrm{S}_V \subset \mathrm{GL}(V)$ montre qu'il est équivalent de se donner une représentation ρ de G sur V, et une action de G sur V, disons $(g, v) \mapsto g.v$, telle que pour tout $g \in G$ la bijection $\mathrm{L}_g : v \mapsto g.v$ est k-linéaire. Le lien entre les deux points de vue est bien sûr la formule $\mathrm{L}_g = \rho(g)$ pour $g \in G$.

On note souvent (V, ρ), ou même simplement V ou ρ, une représentation de G. La *dimension*, ou le *degré*, de (V, ρ) est la dimension du k-espace vectoriel V. Dans ce cours on considérera surtout des représentations de dimension finie.

EXEMPLE 1.2. *Si G est un sous-groupe de $\mathrm{GL}_n(k)$, son action naturelle sur k^n définit une représentation k-linéaire de G.* Par exemple, tout sous-groupe de $\mathrm{SO}(3)$ admet une représentation $\mathbb{R}$-linéaire naturelle sur $\mathbb{R}^3$, et tout sous-groupe de $\mathrm{Sp}(1)$ possède une représentation naturelle $\mathbb{C}$-linéaire sur $\mathbb{C}^2$.

Si (V, ρ) est une représentation k-linéaire de dimension n de G, le choix d'une base e de V définit un morphisme de groupes

$$\rho^e : G \to \mathrm{GL}_n(k),\ g \mapsto \mathrm{Mat}_e \rho(g).$$

Changer de base e revient simplement a conjuguer ρ^e par un élément de $\mathrm{GL}_n(k)$ (matrice de changement de base).

DÉFINITION 1.3. *Deux représentations k-linéaires (V_1, ρ_1) et (V_2, ρ_2) de G de même dimension finie seront dites isomorphes, ou équivalentes, s'il existe des bases e_1 et e_2 de V_1 et V_2, avec $\rho_1^{e_1} = \rho_2^{e_2}$.*

Ainsi, *on s'intéresse essentiellement aux classes de conjugaison de morphismes $G \to \mathrm{GL}_n(k)$.*

EXEMPLE 1.4. *(i) Une représentation k-linéaire de G de dimension 1 est la donnée d'un morphisme $G \to k^\times$.* Pour $k = \mathbb{C}$, c'est donc un élément de $\widehat{G} = \mathrm{Hom}(G, \mathbb{C}^\times)$.

(ii) L'action triviale de G sur $V = k$ est une représentation linéaire de dimension 1 appelée *représentation triviale de G.*

(iii) Se donner une représentation ρ de $G = \mathbb{Z}$ sur V est la même chose que se donner l'image de $\rho(1)$, qui est un élément arbitraire de $\mathrm{GL}(V)$. Classifier à isomorphisme près les représentations k-linéaires de $\mathbb{Z}$ de dimension n revient donc à déterminer les classes de conjugaison d'éléments de $\mathrm{GL}_n(k)$.

En guise d'autre exemple, supposons donnée une action du groupe G sur un ensemble X. Notons kX le k-espace vectoriel *libre sur l'ensemble* X, c'est-à-dire l'espace $k^{(X)}$ muni de sa base canonique des e_x avec $x \in X$. On a donc une somme directe $kX = \bigoplus_{x \in X} k\,\mathrm{e}_x$. On dispose d'un morphisme naturel $\rho : G \to \mathrm{GL}(kX)$ défini par $\rho(g)(\mathrm{e}_x) = \mathrm{e}_{gx}$ pour tout $g \in G$ et tout $x \in X$.

DÉFINITION 1.5. *Si G agit sur X, la représentation ci-dessus de G sur $k\,X$ est appelée* représentation de permutation *associée.*

Ces représentations sont très particulières : dans la base $\{\mathrm{e}_x\}$ de kX, la matrice de chaque $\rho(g)$ avec $g \in G$ a un unique coefficient non nul, égal à 1, sur chaque colonne et sur chaque ligne.

EXEMPLE 1.6. Considérons l'action naturelle de $G = \mathrm{S}_n$ sur $X = \{1, \ldots, n\}$. Elle définit une représentation de permutation de S_n sur $kX = k^n = \oplus_{i=1}^n k\mathrm{e}_i$ vérifiant $\sigma(\mathrm{e}_i) = \mathrm{e}_{\sigma(i)}$ pour $\sigma \in \mathrm{S}_n$ et $i \in \{1, \ldots, n\}$, soit encore $\sigma(x_1, \ldots, x_n) = (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)})$ pour $x \in k^n$. Dans la base des e_i, c'est le morphisme $\mathrm{S}_n \to \mathrm{GL}_n(k)$ déjà rencontré dans la démonstration du Théorème 2.1 Chap. 6.

2. Le point de vue $k[G]$-modules

Nous verrons de nombreux autres exemples un peu plus tard. Expliquons d'abord comment les représentations k-linéaires de G peuvent être vue alternativement, et avec profit, comme des modules sur un anneau adéquat, appelée *k-algèbre du groupe G*. Rappelons d'abord la définition d'une k-algèbre.

DÉFINITION 2.1. *Une k-algèbre est un anneau A muni d'un morphisme d'anneau $k \to A$.*

Par exemple, l'anneau $\mathrm{M}_n(k)$ est une k-algèbre via $k \to \mathrm{M}_n(k)$, $\lambda \mapsto \lambda \mathrm{I}_n$. De même, l'anneau $k[X]$ est une k-algèbre via l'inclusion évidente ("les constantes"). Comme tout morphisme d'anneau d'un corps vers un anneau non nul est injectif, le morphisme $k \to A$ est souvent simplement vu comme une inclusion. Il permet de voir A comme un k-espace vectoriel, ainsi que tout A-module par restriction des scalaires.

CONSTRUCTION DE $k[G]$: La donnée de k et G permet de construire une structure de k-algèbre sur le k-espace vectoriel $A =: k\,G$. En effet, on munit A de l'unique loi de composition k-bilinéaire $\mu : A \times A \to A, (x, y) \mapsto xy$, qui dans la base des $\{\mathrm{e}_g\}_{g \in G}$ est donnée par la formule $\mathrm{e}_g\,\mathrm{e}_h := \mathrm{e}_{gh}$. Elle est associative par associativité de la loi de groupe de G (voir l'Exercice 9.33) et de neutre e_1. Elle est distributive vis-à-vis de $(A, +)$, par bilinéarité. Autrement dit, $(A, +, \mu)$ est un anneau. Par construction, $\lambda \mapsto \lambda \mathrm{e}_1$ est un morphisme d'anneaux $k \to A$, faisant donc de A une k-algèbre. On notera presque toujours g l'élément e_g de A pour alléger les écritures.

DÉFINITION 2.2. *Soient k un corps et G un groupe. La k-algèbre d'espace sous-jacent $k\,G$ construite ci-dessus s'appelle* l'algèbre du groupe G à coefficients dans k *et est notée $k[G]$. Sa dimension comme k-espace vectoriel est $|G|$.*

EXEMPLE 2.3. L'anneau $k[G]$ est commutatif si, et seulement si, G l'est. Il n'est pas difficile de montrer que l'on a $k[\mathbb{Z}] \simeq k[T, T^{-1}]$ et, pour tout entier $n \geqslant 1$, on a $k[\mathbb{Z}/n\mathbb{Z}] \simeq k[T]/(T^n - 1)$. La structure de $\mathbb{C}[G]$ pour G fini sera élucidée plus loin dans le cours : voir la Remarque 7.7.

Qu'est-ce qu'un $k[G]$-module ? D'abord, tout $k[G]$-module V est *a fortiori* un k-espace vectoriel, par restriction des scalaires au sous-corps $k1$ de $k[G]$, que l'on identifie à k via $x \mapsto x1$. De plus, il induit une application $G \times V \to V$, $(g, v) \mapsto gv$ qui

est manifestement une action de G sur V. Enfin, cette action est par automorphismes k-linéaires : on a

$$g(\lambda v) = g(\lambda 1\, v) = (g\lambda 1)v = (\lambda 1 g)v = (\lambda 1)(gv) = \lambda gv$$

(car g et $\lambda 1$ commutent par construction dans $k[G]$). Ainsi, *à tout $k[G]$-module V est associé une représentation k-linéaire ρ_V de G sur V*, vérifiant $\rho_V(g)(v) = gv$. Réciproquement, toute action de G sur un k-espace vectoriel V par automorphismes k-linéaires s'étend de manière unique en une structure de $k[G]$-module sur V. En effet, comme $\{g\}_{g\in G}$ est une k-base de $k[G]$ il y a un sens à considérer

$$\nu : k[G] \times V \to V, (\sum_{g\in G} \lambda_g\, g, v) \mapsto \sum_{g\in G} \lambda_g \rho(g)v.$$

C'est trivialement une structure de $k[G]$-module sur V ![1] On a montré :

Proposition-Définition 2.4. (Propriété universelle de l'algèbre du groupe) *Il est équivalent de se donner une représentation k-linéaire du groupe G et un $k[G]$-module. Plus précisément :*

(i) Si V est un $k[G]$-module, il existe une unique représentation k-linéaire de G sur le k-espace vectoriel sous-jacent à V, notée $\rho_V : G \to \mathrm{GL}(V)$, vérifiant $\rho_V(g)(v) = g.v$ pour tout $g \in G$ et $v \in V$. On l'appelle la représentation associée à V.

(ii) Reciproquement, si (V, ρ) est une repésentation k-linéaire de G, il existe une unique structure de $k[G]$-module sur V étendant celle de k-espace vectoriel, et vérifiant $g.v = \rho(g)(v)$ pour tout $g \in G$ et $v \in V$. On l'appelle $k[G]$-module associé à (V, ρ), et on le note en général simplement V.

Ces deux constructions sont inverses l'une de l'autre.

Dans la suite, nous jonglerons souvent entre les points de vue « représentation » et « $k[G]$-module » sans commentaire, via la proposition ci-dessus. Ainsi, étudier les représentations de G est la même chose qu'étudier l'algèbre $k[G]$-linéaire ! Toutes les notions s'appliquant aux modules s'appliquent en particulier aux représentations, ce qui nous évite en particulier de les redéfinir (même si nous en retraduirons certaines ci-dessous) : sous-modules, produits, sommes, sommes directes ... ainsi que la notion de morphisme et d'isomorphisme. Par exemple, un *morphisme* entre deux représentations k-linéaires (V_1, ρ_1) et (V_2, ρ_2) de G est par définition une application $k[G]$-linéaire entre les $k[G]$-modules V_1 et V_2 associés.

Définition 2.5. *Si V_1 et V_2 sont des $k[G]$-modules, on note $\mathrm{Hom}_{k[G]}(V_1, V_2)$ le k-espace vectoriel des applications $k[G]$-linéaires de V_1 vers V_2.*

Une application k-linéaire $u : V_1 \to V_2$ est $k[G]$-linéaire si, et seulement si, on a

$$u \circ \rho_1(g) = \rho_2(g) \circ u, \ \ \forall\ g \in G,$$

(on parle aussi d'*opérateur d'entrelacement*). C'est un isomorphisme si, et seulement si, elle est bijective. On retrouve bien la notion d'isomorphisme de représentations déjà introduite plus haut :

1. En effet, ν est k-bilinéaire, donc (M1) et (M2) sont satisfaits et il suffit de vérifier (M3) pour $a, a' \in G$, mais c'est la définition d'une action de G sur V.

PROPOSITION 2.6. *Deux $k[G]$-modules de dimension finie U et V sont isomorphes, si et seulement si, les représentations associées (U, ρ_U) et (V, ρ_V) le sont.*

DÉMONSTRATION — Soient $e = (e_1, \ldots, e_n)$ et $f = (f_1, \ldots, f_n)$ des k-bases de U et V respectivement, et $u : U \to V$ la bijection k-linéaire définie par $u(e_i) = f_i$ pour tout i. Pour $g \in G$ on a clairement $\mathrm{Mat}_f\, u \circ \rho_U(g) \circ u^{-1} = \mathrm{Mat}_e\, \rho_U(g)$. On a donc $\mathrm{Mat}_e\, \rho_U(g) = \mathrm{Mat}_f\, \rho_V(g) \iff u \circ \rho_U(g) \circ u^{-1} = \rho_V(g)$. □

3. Décomposition en irréductibles

Soit V un $k[G]$-module. Un sous-k-espace vectoriel $W \subset V$ est dit *G-invariant* (ou *G-stable*, ou une *sous-représentation de V*) si on a $g.w \in W$ pour tout $w \in W$ et tout $g \in G$, *i.e.* si c'est un *sous-module* de V. Soient $e = (e_1, \ldots, e_{p+q})$ une base de V telle que $e_1, \ldots, e_p$ est une base de W. Alors W est G-invariant si, et seulement si, on a

$$\mathrm{Mat}_e\, \rho_V(g) = \begin{bmatrix} \star_p & \star \\ 0 & \star_q \end{bmatrix}, \quad \forall\, g \in G.$$

DÉFINITION 3.1. *Soit V un $k[G]$-module, ou ce qui revient au même, une représentation k-linéaire de G. On dit que V est* irréductible (*ou* simple)*, si on a $V \neq \{0\}$ et si les seuls sous-modules de V sont $\{0\}$ et V.*

Une représentation de dimension 1 (comme la triviale) est irréductible.

PROPOSITION 3.2. *Supposons k algébriquement clos, G abélien et V un $k[G]$-module irréductible de dimension finie. Alors V est de dimension* 1.

DÉMONSTRATION — En effet, les $\rho_V(g)$ sont trigonalisables car k est algébriquement clos et V de k-dimension finie. Ils commutent entre eux car G est abélien. Ils possèdent donc une droite G-stable commune (cotrigonalisabilité) $D \subset V$. Par irréductibilité de V, on a $D = V$. □

PROPOSITION 3.3. *Un $k[G]$-module V non nul est irréductible si, et seulement si, on a $k[G]v = V$ pour tout $v \neq 0$ dans V.*

DÉMONSTRATION — En effet, si V est irréductible, et $v \in V$ est non nul, alors $k[G]v$ est un sous-module de V, nécessairement égal à V. Réciproquement, si W est un sous-module non nul de V, et si $v \in W$ est non nul, on a $V = k[G]v \subset W$, et donc $W = V$. □

En particulier, un $k[G]$-module irréductible est monogène. Attention, la réciproque est fausse : voir l'Exercice 9.10. Développons maintenant un exemple instructif. Considérons, pour $n \geqslant 2$, la représentation de permutation de S_n sur $k^n = \bigoplus_{i=1}^n k e_i$ de l'Exemple 1.6. Elle n'est pas irréductible. En effet, la droite D engendrée par le vecteur $(1, 1, \ldots, 1) = \sum_{i=1}^n e_i$ est fixée, donc G-stable, et définit donc une représentation de S_n isomorphe à k (la triviale). De plus, l'hyperplan $H \subset k^n$ défini par $\sum_i x_i = 0$ est également manifestement G-stable.

PROPOSITION 3.4. *Les seuls sous-modules de la représentation de permutation naturelle de* S_n *sur* k^n *sont* $\{0\}, D, H$ *et* V. *En outre, on a*

$$V = H \oplus D \iff n \in k^\times.$$

DÉMONSTRATION — Il est clair que l'on a $D \subset H \iff \sum_{i=1}^n e_i \in H \iff n.1 = 0$ dans k, d'où la seconde assertion. Montrons la première. Soit W un sous $k[\mathrm{S}_n]$-module de k^n non inclus dans la droite D. Il existe donc $x \in W$ et $i \neq j$ tels que $x_i \neq x_j$. Mais alors l'élément $x - (i\,j)\,x$ est dans W, et il est égal à

$$(x_i - x_j)(e_i - e_j).$$

Quitte à diviser par $x_i - x_j$ (non nul), on a donc $e_i - e_j \in W$. Quitte à appliquer encore des éléments de S_n, on a aussi $e_i - e_l$ dans W pour tout $l \neq i$, puis $H = \mathrm{vect}_k(e_i - e_l) \subset W$. Comme H est un hyperplan, on a $W = H$ ou $W = V$. □

DÉFINITION 3.5. *Un* $k[G]$*-module* V *est dit* semi-simple *s'il existe une décomposition en somme directe* $V = \oplus_{i \in I} V_i$ *où les* V_i *sont des sous-modules irréductibles.*

On trouve aussi la terminologie *complètement réductible* pour *semi-simple*. Il est clair que irréductible (ou nul) implique semi-simple.

PROPOSITION 3.6. (Caractérisation de la semi-simplicité) *Soit* V *un* $k[G]$*-module de dimension finie. Il y a équivalence entre :*

(a) V *est semi-simple.*

(b) V *est somme (pas forcément directe) de sous-modules irréductibles.*

(c) Pour tout sous-module W *de* V*, il existe un sous-module* S *de* V *vérifiant* $V = W \oplus S$ *(« existence d'un supplémentaire stable »).*

(d) tout sous-module de V *est semi-simple.*

DÉMONSTRATION — Les implication (a) $\implies$ (b) et (d) $\implies$ (a) sont triviales.

Montrons (b) $\implies$ (c). Supposons $V = \sum_{i \in I} V_i$ avec les V_i irréductibles. Soit W un sous-module de V. Si W contient tous les V_i, on a $W = V$ et $S = \{0\}$ convient. Sinon, il existe $i \in I$ avec V_i non inclus dans W. Dans ce cas, $V_i \cap W$ est un sous-module de V_i distinct de V_i. Par irréductibilité de V_i, on a $V_i \cap W = \{0\}$. Ainsi, V_i et W sont en somme directe dans V, et $W' := V_i \oplus W$ est un sous-module de V. Par récurrence descendante sur $\dim W$, il existe un sous-module $S' \subset V$ avec $W' \oplus S' = V$. On conclut en posant $S = S' \oplus V_i$.

Montrons (c) $\implies$ (d) par récurrence sur la dimension du sous-module $W \subset V$ en question. Le cas $W = \{0\}$ est trivial par convention, donc on suppose W non nul. Soit U un sous-module non nul de W de dimension minimale. Alors U est nécessairement irréductible. Par (c), il existe un suppémentaire G-stable S de U dans V. Tout élément de $w \in W$ s'écrit de manière unique $u + s$ avec $u \in U$ et $s \in S$, et donc $s = w - u \in S \cap W$. On a donc $W = U \oplus (S \cap W)$ avec $S \cap W$ un sous-module de V de dimension $< \dim W$, et on conclut par récurrence. □

Remarque 3.7. En utilisant notamment le lemme de Zorn, on pourrait montrer que l'hypothèse $\dim V < \infty$ est en fait inutile.

Exemple 3.8. *Soient E un espace euclidien et $\rho : G \to \mathrm{O}(E)$ une représentation de G sur E par isométries euclidiennes. Alors le $\mathbb{R}[G]$-module E est semi-simple.* En effet, si $W \subset E$ est un sous-espace G-invariant, alors son orthogonal $W^\perp$ est un supplémentaire G-invariant de W.

Exemple 3.9. (*Éléments semi-simples*) Soient $g \in \mathrm{GL}_n(k)$ et $\rho : \mathbb{Z} \to \mathrm{GL}_n(k)$, $m \mapsto g^m$, la représentation de $\mathbb{Z}$ associée (Exemple 1.2 (ii)). Alors *ρ est semis-simple si, et seulement si, tout sous-espace de k^n stable par g admet un supplémentaire stable par g* ; on dit aussi dans ce cas que g est *semi-simple*. Par exemple, l'élément $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ de $\mathrm{GL}_2(k)$ n'est pas semi-simple. *Si k est algébriquement clos, on a g semi-simple $\iff$ g diagonalisable*, par la propriété (b) et la Proposition 3.2.

Théorème 3.10. (Maschke) *On suppose G fini et $|G|$ dans $k^\times$. Alors tout $k[G]$-module de dimension finie est semi-simple.*

Démonstration — Soient V un $k[G]$-module de dimension finie. Soit $W \subset V$ un sous-module. Soit $p \in \mathrm{End}_k(V)$ un projecteur arbitraire d'image W. On a $V = W \oplus \ker p$. Supposons d'abord que p commute à l'action de G, *i.e.* $p \circ \rho_V(g) = \rho_V(g) \circ p$ pour tout g dans G. Alors $\ker p$ est stable par $\rho_V(g)$ pour tout g : c'est un supplémentaire G-stable de W. En général, on pose

$$p' = \frac{1}{|G|} \sum_{g \in G} \rho_V(g) \circ p \circ \rho_V(g)^{-1}.$$

C'est un élément bien défini de $\mathrm{End}_k(V)$ car $|G|$ est inversible dans k. On a $\mathrm{Im}\, p' \subset \mathrm{Im}\, p = W$ car W est G-stable. Pour $x \in W$ et $g \in G$, on a $\rho_V(g)^{-1}(x) \in W$ et donc $p \circ \rho_V(g)^{-1}(x) = \rho_V(g)^{-1}(x)$, et donc $p'(x) = \frac{1}{|G|}|G|x = x$. Ainsi, p' est un projecteur d'image W. Enfin, p' commute à l'action de G, car le changement de variable $g \mapsto hg$ dans G montre $\rho_V(h) \circ p \circ \rho_V(h)^{-1} = p$ pour tout $h \in H$: on est donc ramené au cas précédent. □

Remarque 3.11. L'exemple de la représentation de permutation de S_n sur k^n avec $k = \mathbb{Z}/p\mathbb{Z}$ et $p \mid n$, montre que l'hypothèse sur $|G|$ est nécessaire.

Remarque 3.12. (*Astuce unitaire de Weyl*) Dans les cas particuliers $k = \mathbb{R}$ ou $k = \mathbb{C}$, le raisonnement suivant fournit une seconde démonstration du Théorème de Maschke. Soit V un $\mathbb{R}[G]$-module de dimension finie. Fixons $\langle -, - \rangle$ un produit scalaire arbitraire sur V. On construit un autre produit scalaire sur V en posant

$$x.y = \sum_{g \in G} \langle g.x | g.y \rangle, \quad \forall x, y \in V.$$

En effet, sa bilinéarité est évidente et il est défini positif par l'inégalité $x.x \geqslant \langle x|x \rangle$. Enfin, on constate $hx.hy = x.y$ pour tout $h \in G$. Pour ce produit scalaire sur V on a $\rho(G) \subset \mathrm{O}(V)$, et donc V est semi-simple par l'Exemple 3.8. Dans le cas $k = \mathbb{C}$ on procède de même en moyennant par G un produit scalaire hermitien sur V. Ces deux remarques sont détaillées dans les Propositions 5.7 et 7.6 du Chapitre 5.

Soit V un $k[G]$-module semisimple de dimension finie. Il existe en général plusieurs décompositions distinctes $V = \oplus_{i=1}^n V_i$ où les V_i sont des sous-$k[G]$-modules irréductibles. Par exemple, si G agit trivialement sur V, toute décomposition de V en somme directe de droites convient, et il y a plusieurs telles décompositions si $\dim V > 1$. Nous allons voir qu'une forme forte d'unicité persiste toutefois. L'ingrédient important pour cela est le *lemme de Schur*. (Le (ii) ne nous servira que plus tard).

Lemme 3.13. (Schur) *Soient U et V deux $k[G]$-modules irréductibles.*

(i) Toute application $k[G]$-linéaire $U \to V$ est soit nulle, soit un isomorphisme.

(ii) Si de plus k est algébriquement clos, et si U est de dimension finie, les applications $k[G]$-linéaires $U \to U$ sont exactement les homothéties.

Démonstration — Soit $u : U \to V$ une application $k[G]$-linéaire non nulle. Alors $\ker u$ et $\operatorname{Im} u$ sont des sous-modules de U et V respectivement : donc égaux à 0 ou au tout. Comme u est non nulle, on a $\ker u = \{0\}$ et $\operatorname{Im} u = V$, puis u est bijective : c'est un isomorphisme. Cela montre le (i).

Montrons le (ii). Les homothéties $\lambda \mathrm{id}_U$, avec $\lambda \in k$ sont clairement $k[G]$-linéaires. Réciproquement, soit $u \in \operatorname{Hom}_{k[G]}(U, U)$. Par hypothèse sur U et k, u admet une valeur propre $\lambda \in k$. Mézalor $u - \lambda \mathrm{id}_U \in \operatorname{End}_k U$ est $k[G]$-linéaire, et non injective, donc nulle par le (i), puis $u = \lambda \mathrm{id}_U$. □

Proposition 3.14. *Soit V un $k[G]$-module semi-simple de dimension finie. On suppose donnée une décomposition $V = \oplus_{i \in I} V_i$, et pour tout $i \in I$, un $k[G]$-module irréductible de dimension finie S_i, tels que :*

(a) $V_i \subset V$ est un sous-module isomorphe à $S_i^{\oplus n_i}$ pour un certain $n_i \geqslant 1$,

(b) S_i et $S_{i'}$ ne sont pas isomorphes si $i \neq i'$.

Alors pour tout sous-module irréductible S de V, il existe un unique $i \in I$ tel que $S \simeq S_i$, et on a $S \subset V_i$.

On a utilisé la notation $M^{\oplus n}$ pour la somme directe externe de n copies de M (aussi isomorphe à M^n).

Démonstration — (de la Proposition 3.14) Pour tout $i \in I$, écrivons $V_i = \oplus_{j=1}^{n_i} V_{i,j}$, avec $V_{i,j}$ un sous-module irréductible isomorphe à S_i. Tout élément v de V s'écrit alors de manière unique $v = \sum_{i,j} v_{i,j}$ avec $v_{i,j} \in V_{i,j}$. Notons $\pi_{i,j} : V \to V_{i,j}, v \mapsto v_{i,j}$, la projection canonique. Elle est $k[G]$-linéaire car les $V_{i,j}$ sont G-stables. Soit $S \subset V$ un sous-module irréductible. Alors $(\pi_{i,j})_{|S} : S \to V_{i,j}$ est soit nulle, soit un isomorphisme, par le lemme de Schur (i). Soit $v \in S$ non nul. Il existe (i, j) tels que $v_{i,j} \neq 0$: on a donc $v_{i,j} \in \pi_{i,j}(S) \neq \{0\}$. Ainsi, $(\pi_{i,j})_{|S}$ est un isomorphisme, et en particulier, on a $S \simeq S_i$. Mézalor $\pi_{i',j'}(S) = 0$ pour $i' \neq i$, toujours par Schur, ce qui signifie exactement $S \subset V_i$. □

Noter que pour tout $k[G]$-module V semi-simple de dimension finie, il existe par définition des V_i, des S_i et des n_i comme dans l'énoncé. Cette proposition montre que $V_i \subset V$ est canonique : c'est la somme des sous-modules de V isomorphes à S_i. On l'appelle *composante isotypique de S_i dans V*. L'entier n_i est appelé *multiplicité*

de S_i dans V, ou encore *nombre de fois que* S_i *intervient dans* V. Il coincide avec $\frac{\dim V_i}{\dim S_i}$. Un problème important restant est donc :

Problème : *Peut-on classifier, à isomorphisme près, toutes les représentations* k*-linéaires irréductibles d'un groupe donné ?*

4. Théorie des caractères

Dans toute cette partie, G désigne un groupe fini et on s'intéresse aux représentations de G qui sont $\mathbb{C}$-linéaires et de dimension finie ($k = \mathbb{C}$). D'après Maschke, elle sont toutes semi-simples. On se propose d'étudier les classes d'isomorphismes de représentations irréductibles de G, suivant Frobenius, Burnside et Schur. Nous allons notamment démontrer les résultats frappants suivants, dûs à Frobenius.

THÉORÈME 4.1. (Frobenius) *Soit* h *le nombre de classes de conjugaison du groupe fini* G.

(i) À isomorphisme près, il existe exactement h $\mathbb{C}[G]$*-modules irréductibles.*

(ii) Leurs dimensions $n_1, \ldots, n_h$ *vérifient* $|G| = \sum_{i=1}^{h} n_i^2$.

L'outil principal est la notion de caractère d'une représentation, inventée par Frobenius. (Elle aurait un sens sur tout corps k.) [2]

DÉFINITION 4.2. *Soient* V *un* $\mathbb{C}[G]$*-module de dimension finie et* $\rho : G \to \mathrm{GL}(V)$ *le morphisme associé. Le* caractère *de* V *est la fonction* $G \to \mathbb{C}, g \mapsto \mathrm{trace}(\rho(g))$. *On le note* χ_V *(ou* χ_ρ*). On a en particulier* $\chi_V(1) = \dim V$.

EXEMPLE 4.3. (i) Les caractères des représentations de dimension 1 de G sont exactement les éléments de $\widehat{G}$. Les éléments de $\widehat{G}$ seront dans ce chapitre appelés *caractères de degré* 1 de G, pour éviter le conflit de terminologie.

(ii) Le caractère de la représentation triviale est la fonction 1 (constante égale à 1 sur G).

Une fonction $f : G \to \mathbb{C}$ est dite *centrale* si elle est constante sur les classes de conjugaison de G, ou ce qui revient au même, si on a

$$f(ghg^{-1}) = f(h) \ \forall g, h \in G.$$

Il est équivalent de demander $f(gh) = f(hg)$ pour tout $g, h \in G$.

PROPOSITION 4.4. *Pour tout* $\mathbb{C}[G]$*-module* V *de dimension finie, alors* χ_V *est une fonction centrale sur* G. *De plus, si* U *et* V *sont isomorphes, on a* $\chi_U = \chi_V$.

DÉMONSTRATION — Le premier point est la formule $\mathrm{trace}(AB) = \mathrm{trace}(BA)$, pour $A, B \in \mathrm{GL}(V)$. Le second s'en déduit car deux $\mathbb{C}[G]$-modules de dimension finie isomorphes ont même représentation matricielle dans des bases bien choisies. □

2. En fait, la définition initiale d'un caractère chez Frobenius, en 1896, ne fait pas intervenir la notion de représentation !

Nous verrons bientôt que la réciproque a la seconde assertion est vraie ! Avant cela donnons deux exemples importants de calcul de caractère.

EXEMPLE 4.5. (i) *(Représentations de permutation)* Supposons que G agit sur l'ensemble fini X et soit $V = \mathbb{C}X$ la représentation de permutation associée. Soit $g \in G$. Regardons sa matrice dans la base des e_x : la formule $\rho(g)e_x = e_{g.x}$ montre que $\mathrm{tr}(\rho(g))$ est le nombre de points fixes de G dans X.

(ii) *(Représentation régulière)* C'est le cas particulier $X = G$, et donc $V = \mathbb{C}G = \mathbb{C}[G]$. On note $\chi_{\mathrm{reg}} := \chi_{\mathbb{C}G}$ son caractère. On a $\chi_{\mathrm{reg}}(1) = |G|$ et $\chi_{\mathrm{reg}}(g) = 0$ pour $g \neq 1$.

Le caractère d'une somme directe est la somme des caractères :

PROPOSITION 4.6. *Soient U, V des $\mathbb{C}[G]$-modules de dimension finie, et $W = U \oplus V$. On a $\chi_W = \chi_U + \chi_V$.*

DÉMONSTRATION — C'est évident ! Donnons les détails. Par définition de la somme directe externe W de U et V, on a $W = U \oplus V$ comme $\mathbb{C}$-espace vectoriel, et pour $g \in G$, $u \in U$ et $v \in V$, $\rho_W(g)(u + v) = \rho_U(g)(u) + \rho_V(g)(v)$. Ainsi, si l'on considère une base w de W de la forme $(u_1, \ldots, u_n, v_1, \ldots, v_m)$ avec les u_i une base de U et les v_j une base de V, on a

$$\mathrm{Mat}_w \rho_W(g) = \begin{bmatrix} \mathrm{Mat}_u \rho_U(g) & 0 \\ 0 & \mathrm{Mat}_v \rho_V(g) \end{bmatrix}.$$

On conclut en prenant la trace. □

Si U et V sont des $k[G]$-modules, l'espace $\mathrm{Hom}_k(U, V)$ des applications k-linéaires $\phi : U \to V$ est muni d'une structure naturelle de $k[G]$-module en posant

$$(g.\phi)(x) = g.\phi(g^{-1}.x). \tag{70}$$

On note $\mathrm{Hom}(U, V)$ ce $k[G]$-module. Dans le cas particulier $V = k$ (représentation triviale), on pose aussi $U^\vee = \mathrm{Hom}(U, k)$ et on parle de *représentation duale*, ou *contragrédiente*, de U.

PROPOSITION 4.7. *Soient U, V des $\mathbb{C}[G]$-modules de dimension finie.*

(i) Pour $W = \mathrm{Hom}(U, V)$ on a $\chi_W(g) = \chi_U(g^{-1})\chi_V(g)$, $\forall g \in G$.

(ii) En particulier, on a $\chi_{U^\vee}(g) = \chi_U(g^{-1})$ pour tout $g \in G$.

DÉMONSTRATION — Le (ii) se déduit du (i) (cas $V = \mathbb{C}$ trivial, donc $\chi_V = 1$). Pour tous endomorphismes A de U et B de V, on dispose de l'endomorphisme $f_{A,B} : M \mapsto B \circ M \circ A$ de $W = \mathrm{Hom}_{\mathbb{C}}(U, V)$. Montrons

$$\mathrm{tr}(f_{A,B}) = \mathrm{tr}(A)\,\mathrm{tr}(B).$$

La proposition s'en déduira car par définition de la représentation W, on a pour $g \in G$ la relation $\rho_W(g) = f_{\rho_U(g)^{-1}, \rho_V(g)}$ (Formule 70). Soient $u = (u_i)_i$ et $v = (v_j)_j$ des bases de U et V, ainsi que u_i^* et $v_j^\star$ les bases duales associées. Notons $A_{i,i'}$ et $B_{j,j'}$ les matrices respectives de A et B dans u_i et v_j. On dispose d'une base $w_{i,j}$ de

$\mathrm{Hom}_{\mathbb{C}}(U,V)$ en posant $w_{i,j}(x) = u_i^*(x)\, v_j$, pour $x \in U$. On conclut en observant que pour i, j donnés, le coefficient en $w_{i,j}$ de $f_{A,B}(w_{i,j})$ est [3]

$$v_j^*(f_{A,B}(w_{i,j})(u_i)) = v_j^*(B(w_{i,j}(A(u_i)))) = v_j^*(B(u_i^*(A(u_i))v_j)) = A_{ii}v_j^*(B(v_j)) = A_{ii}B_{jj}.$$

□

Proposition 4.8. *Soit $g \in G$ d'ordre d et V un $\mathbb{C}[G]$-module de dimension n. Alors $\rho_V(g)$ est diagonalisable et $\chi_V(g)$ est somme de n racines d-èmes de l'unité. De plus, on a $\chi_{V^\vee} = \overline{\chi_V}$.*

Démonstration — En effet, la relation $g^d = 1$ dans G entraîne $\rho_V(g)^d = \mathrm{Id}_V$. Comme $X^d - 1$ est scindé à racines simples dans $\mathbb{C}[X]$, $\rho_V(g)$ est diagonalisable de valeurs propres $\lambda_1, \ldots, \lambda_n$ vérifiant $\lambda_i^d = 1$. Celles de $\rho_V(g^{-1}) = \rho_V(g)^{-1}$ sont donc les λ_i^{-1}. En particulier, on a $\chi_{V^\vee}(g) = \chi_V(g^{-1}) = \sum_i \lambda_i^{-1} = \overline{\chi_V(g)}$.

□

Les trois derniers lemmes impliquent en particulier.

Corollaire 4.9. *Si χ et χ' sont des caractères (de $\mathbb{C}[G]$-modules de dimension finie), il en va de même de $\chi + \chi'$, $\chi\chi'$ et $\overline{\chi}$.*

Une propriéte importante des caractères résulte du simple lemme suivant. Si V est un $\mathbb{C}[G]$-module, on pose

$$V^G = \{v \in V \mid g.v = v,\ \forall g \in G\}.$$

C'est le plus grand sous-espace vectoriel de V sur lequel G agit trivialement.

Lemme 4.10. *Si V est un $\mathbb{C}[G]$-module de dimension finie on a*

$$\dim V^G = \frac{1}{|G|} \sum_{g \in G} \chi_V(g).$$

Démonstration — On regarde l'endomorphisme $p : V \to V, v \mapsto \frac{1}{|G|}\sum_{g\in G} g.v$. Un changement de variables montre $g.p(v) = p(v)$ pour tout $v \in V$ et $g \in G$. On a donc $\mathrm{Im}\, p \subset V^G$. Mais pour $v \in V^G$ on a aussi $p(v) = \frac{1}{|G|}|G|v = v$, donc p est un projecteur d'image V^G. On conclut car la trace d'un projecteur est égale à son rang. □

Reformulons ce résultat. Reconsidérons le $\mathbb{C}$-espace vectoriel $\mathrm{L}^2(G)$ de toutes les fonctions $G \to \mathbb{C}$, muni du produit scalaire hermitien $\langle f, f' \rangle = \frac{1}{|G|}\sum_{g\in G} f(g)\overline{f'(g)}$.

Corollaire 4.11. *(même hypothèses) On a $\dim V^G = \langle \chi_V, 1 \rangle$.*

3. Une autre manière de dire est que si l'on a $A \in \mathrm{M}_q(\mathbb{C})$ et $B \in \mathrm{M}_p(\mathbb{C})$, alors pour tout $1 \leqslant i \leqslant p$ et $1 \leqslant j \leqslant q$ on constate $(BE_{i,j}A)_{i,j} = B_{i,i}A_{j,j}$. Ainsi, la trace de l'endomorphisme $\mathrm{M}_{p,q}(\mathbb{C}) \to \mathrm{M}_{p,q}(\mathbb{C})$, $M \mapsto BMA$, est $\sum_{1\leqslant i\leqslant p, 1\leqslant j\leqslant q} A_{i,i}B_{j,j} = (\mathrm{tr}\, A)(\mathrm{tr}\, B)$.

Exemple 4.12. (*Où l'on retrouve la formule de Burnside-Frobenius*, Lemme 1.14 Chap. 5) Supposons que G agit sur l'ensemble fini X et $V = \mathbb{C}\,X$. Un élément $\sum_{x\in X} \lambda_x\, x$ est dans V^G si et seulement si la fonction $X \to \mathbb{C}, x \mapsto \lambda_x$, est constante sur les G-orbites. En particulier, $\dim V^G$ est le nombre r de G-orbites de X. On en déduit $r = \frac{1}{|G|}\sum_{g\in G} \chi_V(g)$. Mais comme $\chi_V(g)$ est le nombre de points fixes de G dans V (Exemple 4.5) on retrouve Burnside-Frobenius.

Un des résultats phares de la théorie est le résultat suivant, dû à Frobenius et Schur.

Théorème 4.13. (Orthogonalité des caractères) *Soient U et V deux $\mathbb{C}[G]$-modules irréductibles. On a*

$$\langle \chi_U, \chi_V \rangle = \begin{cases} 1 & \text{si } U \text{ et } V \text{ sont isomorphes,} \\ 0 & \text{sinon.} \end{cases}$$

Démonstration — Posons $W = \mathrm{Hom}(V, U)$. On constate sur la Formule (70) que l'on a $W^G = \mathrm{Hom}_{\mathbb{C}[G]}(V, U)$. Le Corollaire 4.11 montre donc $\dim \mathrm{Hom}_{\mathbb{C}[G]}(V, U) = \langle \chi_W, 1\rangle$. Mais on a $\chi_W = \chi_V \overline{\chi_U}$ par les Propositions 4.7 et 4.8, et donc $\langle \chi_W, 1\rangle = \langle \chi_V, \chi_U\rangle$ par la formule définissant $\langle -, -\rangle$. On conclut par le Lemme de Schur 3.13, cas (i) et (ii) (pour $V \simeq U$ on a $\chi_V = \chi_U$ et donc on peut supposer $V = U$). □

Dans le corollaire suivant, on convient $M^0 = \{0\}$.

Corollaire 4.14. *Soit U un $\mathbb{C}[G]$-module de dimension finie. On suppose $U \simeq \oplus_{i=1}^r S_i^{\oplus n_i}$ où les S_i sont des $\mathbb{C}[G]$-modules irréductibles deux à deux non isomorphes, et les n_i sont des entiers $\geqslant 0$. Alors on a $n_i = \langle \chi_U, \chi_{S_i}\rangle$ pour tout $i = 1, \ldots, r$.*

Démonstration — Le première assertion se déduit de la formule $\chi_U = \sum_i n_i \chi_{S_i}$ (Proposition 4.6), de la bilinéarité de $\langle -, -\rangle$, et de $\langle \chi_{S_i}, \chi_{S_j}\rangle = \delta_{i,j}$ (Théorème 4.13) □

Corollaire 4.15. *Si U et V sont des $\mathbb{C}[G]$-modules de dimension finie, on a*

$$U \simeq V \iff \chi_U = \chi_V.$$

Démonstration — Par semi-simplicité (Maschke) il existe des $\mathbb{C}[G]$-modules irréductibles $S_1, \ldots, S_r$ deux à deux non isomorphes, ainsi que des entiers $n_i, m_i \geqslant 0$ pour $i = 1, \ldots, r$, tels que l'on a $U \simeq \oplus_{i=1}^r S_i^{\oplus n_i}$ et $V \simeq \oplus_{i=1}^r S_i^{\oplus m_i}$. Supposons $\chi_U = \chi_V$. Pour tout $1 \leqslant i \leqslant r$ on a

$$n_i = \langle \chi_U, \chi_{S_i}\rangle = \langle \chi_V, \chi_{S_i}\rangle = m_i,$$

par la première assertion, et donc $U \simeq V$. □

On en profite pour poser les définitions suivantes :

Définition 4.16. *Un* caractère *de G est une fonction $\chi : G \to \mathbb{C}$ de la forme $\chi = \chi_V$ où V est un $\mathbb{C}[G]$-module de dimension finie. La fonction χ détermine uniquement V à isomorphisme près. On dit que χ est irréductible si V l'est. On note $\mathrm{Car}\, G$ l'ensemble des caractères de G, et $\mathrm{Irr}\, G \subset \mathrm{Car}\, G$ le sous-ensemble des caractères irréductibles.*

On a par exemple $\widehat{G} \subset \mathrm{Irr}(G)$ (caractères de degré 1, voir la Remarque 4.3). Un autre corollaire des relations d'orthogonalité est le critère d'irréductibilité suivant.

COROLLAIRE 4.17. *Soit* $\chi \in \mathrm{Car}\, G$. *On a* $\chi \in \mathrm{Irr}\, G \iff \langle \chi, \chi \rangle = 1$.

DÉMONSTRATION — Par Maschke et la Proposition 4.6, tout caractère χ s'écrit $\chi = \sum_{i=1}^{r} n_i \chi_i$ où les χ_i sont des caractères irréductibles distincts, et $n_i \in \mathbb{N}$. Les relations d'orthogonalité donnent $\langle \chi, \chi \rangle = \sum_{i=1}^{r} n_i^2$, et donc $\langle \chi, \chi \rangle = 1 \iff$ un et un seul des n_i vaut 1 (*i.e.* ssi χ est l'un des χ_i). □

On rappelle que la représentation régulière de G (sur $\mathbb{C}G$) a été introduite dans l'Exemple 4.5 (ii), et que son caractère est noté χ_{reg}.

COROLLAIRE 4.18. *Tout* $\mathbb{C}[G]$*-module irréductible* S *apparaît dans la décomposition en irréductibles de la représentation régulière, et ce avec une multiplicité* $\dim S$.

DÉMONSTRATION — Soit S un $\mathbb{C}[G]$-module irréductible. D'après le corrollaire 4.14, il faut montrer $\langle \chi_{\mathrm{reg}}, \chi_S \rangle = \dim S$. On a vu $\chi_{\mathrm{reg}}(g) = 0$ pour $g \neq 1$, $\chi_{\mathrm{reg}}(1) = \dim \mathbb{C}\, G = |G|$ et $\chi_S(1) = \dim S$. On a donc bien $\langle \chi_{\mathrm{reg}}, \chi_S \rangle = \frac{1}{|G|}(|G| \dim S + 0) = \dim S$. □

On en déduit une partie du Théorème 4.1.

COROLLAIRE 4.19. *(Frobenius) Il n'y a qu'un nombre fini de* $\mathbb{C}[G]$*-modules irréductibles à isomorphisme près, et leurs dimensions* $n_1, \ldots, n_r$ *vérifient*

$$|G| = \sum_{i=1}^{r} n_i^2.$$

DÉMONSTRATION — D'après le corollaire précédent, on a $\mathbb{C}\, G \simeq \oplus_{i=1}^{s} S_i^{\oplus n_i}$ où les S_i parcourent les classes d'isomorphismes de $\mathbb{C}[G]$-modules irréductibles, nécessairement en nombre fini car $\mathbb{C}G$ est de dimension finie, et $n_i = \dim S_i$. On conclut car $|G| = \dim \mathbb{C}G = \sum_{i=1}^{s} n_i^2$. □

Soit $\mathrm{L}^2(G)_{\mathrm{cent}} \subset \mathrm{L}^2(G)$ le sous-espace vectoriel des fonctions centrales. Une fonction $f : G \to \mathbb{C}$ est centrale si, et seulement si, elle est constante sur les classes de conjugaison. Comme ces classes sont disjointes, il en découle que $\mathrm{L}^2(G)_{\mathrm{cent}}$ a pour base les fonctions caractéristiques des classes de conjugaison de G. En particulier, si h est le nombre de telles classes, on en déduit :

$$\dim \mathrm{L}^2(G)_{\mathrm{cent}} = h \tag{71}$$

Le point culminant de cette partie est le théorème suivant, dû à Schur et Frobenius.

THÉORÈME 4.20. *Les caractères irréductibles de* G *forment une base orthonormée de* $\mathrm{L}^2(G)_{\mathrm{cent}}$. *En particulier, on a* $|\mathrm{Irr}\, G| = h$.

À ce stade, presque tous les ingrédients sont en place. Notons $\mathrm{Z}(\mathbb{C}[G])$ le centre de l'anneau $\mathbb{C}[G]$. C'est une sous-$\mathbb{C}$-algèbre de $\mathbb{C}[G]$ contenant le centre Z de G, et donc $\mathbb{C}[Z]$, mais elle contient bien d'autres éléments en général. Par exemple, on constate qu'elle contient l'élément $\sum_{g \in G} g$. Plus généralement, on a :

Lemme 4.21. (Centre de l'algèbre du groupe) *Soient $f : G \to \mathbb{C}$ une fonction et $z := \sum_{g\in G} f(g)g \in \mathbb{C}[G]$. Alors $z \in \mathrm{Z}(\mathbb{C}[G]) \iff f$ est centrale.*

Démonstration — Pour $h \in G$, on a

$$hzh^{-1} = \sum_{g\in G} f(g)hgh^{-1} = \sum_{g\in G} f(h^{-1}gh)g.$$

Comme G est une $\mathbb{C}$-base de $\mathbb{C}[G]$, cela conclut. □

Soit S un $\mathbb{C}[G]$-module et $z \in \mathrm{Z}(\mathbb{C}[G])$. L'application $\mathrm{m}_z : S \to S, v \mapsto z.v$, est alors $\mathbb{C}[G]$-linéaire. Supposons S irréductible. Par le Lemme de Schur, m_z est donc une homothétie, de rapport que l'on notera $\lambda_S(z)$. On a défini une application

$$\lambda_S : \mathrm{Z}(\mathbb{C}[G]) \to \mathbb{C},\ z \mapsto \lambda_S(z).$$

C'est trivialement un morphisme de $\mathbb{C}$-algèbres. Décrivons-le plus précisément :

Lemme 4.22. *Soient $f : G \to \mathbb{C}$ une fonction centrale, $z := \sum_{g\in G} f(g)g \in \mathrm{Z}(\mathbb{C}[G])$, et S un $\mathbb{C}[G]$-module simple. On a $\lambda(z) = \frac{|G|}{\dim S}\langle f, \chi_{S^\vee}\rangle$.*

Démonstration — Comme $S \to S, v \mapsto zv$, est l'homothétie de rapport $\lambda_S(z)$, on a

$$\lambda_S(z) = \frac{\mathrm{trace}(z \mid S)}{\dim S} = \frac{\sum_{g\in G} f(g)\chi_S(g)}{\dim S} = \frac{|G|}{\dim S}\langle f, \chi_{S^\vee}\rangle.$$

□

Démonstration — (du Théorème 4.20) Soient $\chi_1, \ldots, \chi_n$ les caractères irréductibles de G. Les relations d'orthogonalité montrent $\langle \chi_i, \chi_j\rangle = \delta_{i,j}$. Les χ_i sont donc $\mathbb{C}$-linéairement indépendants dans $\mathrm{L}^2(G)$: si on a $0 = \sum_i \lambda_i\chi_i$, on en déduit en prenant $\langle -, \chi_j\rangle$ l'égalité $\lambda_j = 0$. En particulier, on a $n \leqslant \dim \mathrm{L}^2(G)_{\mathrm{cent}} = h$. Soit $f : G \to \mathbb{C}$ centrale. On veut montrer que f est combinaison $\mathbb{C}$-linéaire des χ_i. Quitte à remplacer f par $f - \sum_{i=1}^n \langle f, \chi_i\rangle\chi_i$, on peut supposer $\langle f, \chi_i\rangle = 0$ pour tout $i = 1, \ldots, n$, et donc $\langle f, \chi\rangle = 0$ pour tout caractère χ (par Maschke). Mais le Lemme 4.22 montre alors que l'élément $z := \sum_{g\in G} f(g)g$ agit par 0 dans toutes les représentations irréductibles de G, et donc dans tous les $\mathbb{C}[G]$-modules de dimension finie. Il agit donc par 0 sur le $\mathbb{C}[G]$-module $\mathbb{C}\,G = \mathbb{C}[G]$ (représentation régulière). Mais on a $z.1 = z$, et donc $z = 0$ dans $\mathbb{C}[G]$, puis $f = 0$. □

Cela termine d'abord de démontrer le Théorème 4.1. La décomposition obtenue

$$\mathrm{L}^2(G)_{\mathrm{cent}} = \bigoplus_{\chi\in\mathrm{Irr}\,G}^{\perp} \mathbb{C}\chi,$$

redonne pour G abélien la décomposition du Théorème 2.1 Chap. 3, et peut donc être vue comme une généralisation de ce dernier. C'est la *décomposition de Fourier des fonctions centrales*. Il existe également une décomposition de Fourier de toutes les fonctions : voir le Complément § 8.

Exemple 4.23. Soient C une classe de conjugaison dans G et $1_C \in \mathrm{L}^2(G)_{\mathrm{cent}}$ sa fonction caractéristique. Comme pour toutes les fonctions (Théorème 4.20), on a

$$1_C = \sum_{\chi \in \operatorname{Irr} G} \lambda_\chi \chi$$

avec $\lambda_\chi = \langle 1_C, \chi \rangle$ (relations d'orthogonalité). Par définition de $\langle -, - \rangle$ on a aussi $\lambda_\chi = \frac{|C|}{|G|}\overline{\chi(C)}$, où $\chi(C)$ désigne $\chi(g)$ pour un g arbitraire de C. Soient maintenant C et C' deux classes de conjugaison de G. On constate $\langle 1_C, 1_{C'} \rangle = \frac{|C|}{|G|}\delta_{C,C'}$. En développant, il vient $\langle 1_C, 1_{C'} \rangle = \sum_{\chi \in \operatorname{Irr} G} \frac{|C||C'|}{|G|^2}\overline{\chi(C)}\chi(C')$. On a donc montré

$$\sum_{\chi \in \operatorname{Irr} G} \chi(C)\overline{\chi(C')} = \begin{cases} 0 & \text{si } C \neq C', \\ \frac{|G|}{|C|} & \text{sinon.} \end{cases}$$

Cette relation s'appelle la *seconde relation d'orthogonalité*. Pour $C = C' = \{1\}$ elle redonne $\sum_\chi \chi(1)^2 = |G|$.

5. La table des caractères et exemples

Fixons G un groupe fini. Notons $C_1, \ldots, C_h$ les classes de conjugaison de G, choisissons $g_j \in C_j$ pour tout j, et notons $\chi_1, \ldots, \chi_h$ les caractères irréductibles de G (numérotations arbitraires). La *table des caractères* de G est le tableau :

	g_1	g_2	$\cdots$	g_h
χ_1	$\chi_1(g_1)$	$\chi_1(g_2)$	$\cdots$	$\chi_1(g_h)$
χ_2	$\chi_2(g_1)$	$\chi_2(g_2)$	$\cdots$	$\chi_2(g_h)$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
χ_h	$\chi_h(g_1)$	$\chi_h(g_2)$	$\cdots$	$\chi_h(g_h)$

On rajoutera souvent en dessus de la premiere ligne la ligne des cardinaux $|C_j|$ des classes de conjugaison, et encore au dessus celle des $|G|/|C_j|$ (cardinal du centralisateur de g_j). Ces données permettent de vérifier *de visu* les deux familles de *relations d'orthogonalité* (colonnes et lignes) : pour tout $1 \leqslant a, b \leqslant h$

$$\sum_{j=1}^{h} |C_j|\, \chi_a(g_j)\overline{\chi_b(g_j)} = |G|\, \delta_{a,b} \quad \text{et} \quad \sum_{i=1}^{h} \chi_i(g_a)\overline{\chi_i(g_b)} = \frac{|G|}{|C_a|}\delta_{a,b}.$$

On retrouve par exemple $|G| = \sum_j |C_j|$ et $|G| = \sum_i \dim \chi^2$ pour $a = b = 1$. En général, on prend $g_1 = 1$ et on ordonne les g_i par ordre croissant, et on prend aussi $\chi_1 = 1$ (caractère trivial) et on ordonne les χ_i par dimension croissante. Dans ce cas, la ligne χ_1 ne contient que des 1, et la colonne g_1 les dimensions des χ_i.

Groupes abéliens

Pour G abélien, on a clairement $h = |G|$ et aussi $\operatorname{Irr} G = \widehat{G}$ (Proposition 3.2). Ce cas n'est donc pas très interessant ! Par exemple, les tables de caractères de $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$ sont donnés par la Table 1.

Le groupe S_3

	1	τ
1	1	1
η	1	-1

	1	τ	τ^2
1	1	1	1
η	1	j	j^2
η^2	1	j^2	j

TABLE 1. Table des caractères de $G \simeq \mathbb{Z}/2\mathbb{Z}$ et $G \simeq \mathbb{Z}/3\mathbb{Z}$, avec $j = e^{2i\pi/3}$.

Considérons maintenant $G = \mathrm{S}_3$. Il a 3 classes de conjugaisons, avec pour représentants disons 1, $(1\,2)$ et $(1\,2\,3)$, et de cardinaux respectifs 1, 3 et 2. Il y a donc 3 caractères irréductibles à trouver. Les caractères irréductibles de degré 1 sont les éléments de $\widehat{G}$, et il y en a 2 évidents à savoir $\chi_1 = 1$ et $\chi_2 = \varepsilon$ (la signature). La formule $|G| = \sum_{i=1}^{h} \chi_i(1)^2$, ici $6 = 1^2 + 1^2 + 2^2$, donne donc $\chi_3(1) = \dim \chi_3 = 2$. Des relations d'orthogonalité des colonnes on déduit :

$\sharp$cent	6	2	3
$\sharp$conj	1	3	2
	1	$(1\,2)$	$(1\,2\,3)$
1	1	1	1
ε	1	-1	1
χ_3	2	0	-1

TABLE 2. Table des caractères de S_3.

En fait, nous avons déjà rencontré à plusieurs reprise la représentation irréductible de dimension 2 de S_3 découverte ci-dessus :

– Par exemple, si T est un triangle équilatéral du plan euclidien (centré en 0), le groupe d'isométries de T est naturellement isomorphe à S_3 (permutation des 3 sommets). On a donc une représentation

$$\mathrm{S}_3 \xrightarrow{\sim} \mathrm{Iso}(T) \subset \mathrm{O}(2) \subset \mathrm{GL}_2(\mathbb{C}).$$

Elle a bien χ_3 pour caractère car elle envoie une transposition sur une réflexion orthogonale (de trace nulle) et un 3-cycle sur une rotation d'ordre 3 (de trace $2\cos(\pm 2\pi/3) = -1$).

– On a aussi montré, pour tout $n \geqslant 2$, que la représentation naturelle de permutation de S_n sur $\mathbb{C}^n$ se décompose sous la forme

$$\mathbb{C}^n \simeq \mathbb{C} \oplus H, \text{ avec } H = \{(x_1, \ldots, x_n) \in \mathbb{C}^n \mid \sum_i x_i = 0\},$$

et aussi que H irréductible de dimension $n-1$. Pour $n = 3$ on a donc nécessairement $\chi_H = \chi_3$. On peut le vérifier simplement car on connait le caractère de χ_H : on a $\chi_{\mathbb{C}^n} = \chi_H + 1$ et $\chi_{\mathbb{C}^n}(\sigma)$ est le nombre de point fixe de $\sigma \in \mathrm{S}_n$ sur $\{1, \ldots, n\}$. Cela colle manifestement avec la table ci-dessus. Dans la base $e_1 - e_2, e_2 - e_3$ de H, remarquons que les éléments $(1\,2)$ et $(1\,2\,3)$ de S_3 on pour matrices matrices respectives $\begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix}$ et $\begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}$.

On a donc montré que toute représentation de dimension finie de S_3 est somme directe de a copies de la représentation triviale, b copies de la signature, et c copies de H, avec a, b, c uniques. Concrètement, cela signifie :

PROPOSITION 5.1. *Pour tout morphisme de groupe $\rho : \mathrm{S}_3 \to \mathrm{GL}_n(\mathbb{C})$, il existe une unique décomposition $n = a+b+2c$, avec $a, b, c \in \mathbb{N}$, telle que quitte à conjuguer ρ par une matrice $P \in \mathrm{GL}_n(\mathbb{C})$, on ait*

$$\rho(\,(1\,2)\,) = \begin{bmatrix} 1_a & 0 & 0 & 0 \\ 0 & -1_b & 0 & 0 \\ 0 & 0 & -1_c & 1_c \\ 0 & 0 & 0 & 1_c \end{bmatrix} \text{ et } \rho(\,(1\,2\,3)\,) = \begin{bmatrix} 1_a & 0 & 0 & 0 \\ 0 & 1_b & 0 & 0 \\ 0 & 0 & 0 & -1_c \\ 0 & 0 & 1_c & -1_c \end{bmatrix}.$$

LES GROUPES S_4 ET A_4

Considérons maintenant le cas $G = \mathrm{S}_4$. D'après la Prop. 2.9 Chap. 4, il a 5 classes de conjugaisons, avec pour représentants disons 1, $(1\,2)$, $(1\,2)(3\,4)$, $(1\,2\,3)$ et $(1\,2\,3\,4)$, et de cardinal 1, 6, 3, 8 et 6 respectivement. Il y a donc 5 caractères irréductibles à trouver. On prend encore $\chi_1 = 1$ et $\chi_2 = \varepsilon$. On dispose aussi du caractère irréductible $\chi_H = \chi_{\mathbb{C}^4} - 1$, de degré 3, donné par

$$\chi_H \mid 3\ 1\ \ -1\ 0\ \ -1.$$

On rappelle que le produit de deux caractères est un caractère (Cor.4.9). On constate que le caractère $\varepsilon\chi_H$ est distinct de χ_H (valeurs différentes sur $(1\,2)$ par exemple). Comme ε est de degré 1, il est nécessairement irréductible car on a $\langle \varepsilon\chi, \varepsilon\chi \rangle = \langle \chi, \chi \rangle$ pour tout caractère χ : voir l'Exercice 9.26 pour une explication plus directe (et raisonnable). Ainsi, $\varepsilon\chi_H$ est un second caractère irréductible de dimension 3. Le caractère restant χ_3 est donc de dimension 2 car on a $24 - 1^2 - 1^2 - 3^2 - 3^2 = 2^2$. Des relations d'orthogonalité des colonnes on déduit par exemple les valeurs de χ_3, et donc la table des caractères toute entière de S_4 :

$\sharp$cent	24	4	8	3	4
$\sharp$conj	1	6	3	8	6
	1	$(1\,2)$	$(1\,2)(3\,4)$	$(1\,2\,3)$	$(1\,2\,3\,4)$
1	1	1	1	1	1
ε	1	-1	1	1	-1
χ_3	2	0	2	-1	0
χ_H	3	1	-1	0	-1
$\varepsilon\chi_H$	3	-1	-1	0	1

TABLE 3. Table des caractères de S_4.

En fait, nous aurions pu deviner "la" représentation irréductible de dimension 2. En effet, on sait qu'il existe un morphisme surjectif $f : \mathrm{S}_4 \to \mathrm{S}_3$, et de sorte que "la" représentation irréductible de dimension 2 de S_3 mentionnée plus haut définit par composition (on dit aussi par *restriction*, voir aussi l'Exercice 9.27) une représentation irréductible de dimension 2 de S_4. On sait que l'on a $f((1\,2)(3\,4)) = 1$, que $f(1\,2)$ et $f(1\,2\,3\,4)$ sont des transpositions, et que $f(1\,2\,3)$ est un 3-cycle, de sorte que son caractère se déduit de la dernière ligne de la table des caractères de S_3 : on retrouve bien χ_3 ! Noter enfin que l'on a $\varepsilon\chi_3 = \chi_3$.

REMARQUE 5.2. C'est un exercice de vérifier que χ_H (resp. $\varepsilon\chi_H$) est le caractère de la représentation de dimension 3 obtenue en réalisant S_4 comme groupe des isométries d'un tétraèdre régulier (resp. groupe des isométries directes d'un cube).

En utilisant que f induit un morphisme surjectif $\mathrm{A}_4 \to \mathrm{A}_3 \simeq \mathbb{Z}/3\mathbb{Z}$, ainsi que la restriction à A_4 de la représentation H de S_4, on vérifierait que la table des caractères de A_4 est :

$\sharp$cent	12	4	3	3
$\sharp$conj	1	3	4	4
	1	$(1\,2)(3\,4)$	$(1\,2\,3)$	$(1\,3\,2)$
1	1	1	1	1
η	1	1	j	j^2
η^2	1	1	j^2	j
χ_H	3	1	0	0

TABLE 4. Table des caractères de A_4.

LE GROUPE A_5

Considérons maintenant le cas du groupe simple $G = \mathrm{A}_5$, d'ordre 60. D'après l'Exercice 4.13 Chap. 4, il a exactement 5 classes de conjugaison, avec pour représentants disons 1, $(1\,2)(3\,4)$, $(1\,2\,3)$, $(1\,2\,3\,4\,5)$ et $(1\,2\,3\,5\,4)$, de cardinal 1, 15, 20, 12 et 12 respectivement. Il y a donc 5 caractères irréductibles à trouver. Comme $\mathrm{D}(\mathrm{A}_5) = \mathrm{A}_5$, il n'y a qu'un caractère de degré 1 : le caractère trivial.

On dispose encore de la restriction à A_5 du caractère $\chi_H = \chi_{\mathbb{C}^5} - 1$, de degré 4, donné par

$$\chi_H \mid 4\ 0\ 1\ \ -1\ \ -1.$$

On constate $\langle \chi_H, \chi_H \rangle = \frac{1}{60}(4^2 + 15 \cdot 0 + 20 \cdot 1^2 + 12 \cdot 1^2 + 12 \cdot 1^2) = 1$: c'est donc un caractère irréductible de A_5 par le Corollaire 4.17. [4]

Les degrés a, b, c des trois autres caractères vérifient donc $60 - 1^2 - 4^2 = 43 = a^2 + b^2 + c^2$. En regardant modulo 8 on constate que a, b, c sont impairs, donc égaux à 3 ou 5, et que la seule possibilité est $43 = 9 + 9 + 25$. On a donc $\chi_3(1) = \chi_4(1) = 3$ et $\chi_5(1) = 4$.

En fait, on connait un caractère de degré 5. En effet, on sait que A_5 agit transitivement sur un ensemble Y à 6 éléments (encore l'action exotique !). On a donc encore une décomposition en somme directe de deux sous-modules

$$\mathbb{C}\,Y = D \oplus H'$$

avec $D = \mathbb{C} \sum_{y \in Y} e_y \simeq \mathbb{C}$ (trivial) et $H' = \{\sum_{y \in Y} \lambda_y e_y \mid \sum_y \lambda_y = 0\}$, puis $\chi_{H'} = \chi_{\mathbb{C}Y} - 1$. On a vu que dans l'action exotique, un 3-cycle de A_5 agit par un double 3-cycle de Y, un 5-cycle de A_5 agit par un 5-cycle de Y, et une double-transposition de A_5 par une double-transposition de Y. On en déduit

$$\chi_{H'} \mid 5\ 1\ \ -1\ 0\ 0.$$

Comme $5^2 + 15 + 20 = 60$ c'est bien un caractère irréductible ! En fait l'action exotique est 3-transitive, donc cela suivrait aussi de l'Exercice 9.1.

4. On aurait pu aussi le déduire du fait que A_5 agit 2-transitivement sur $\{1, \ldots, 5\}$: voir l'Exercice 9.1).

Remarque 5.3. Si l'on ne connaissait pas l'action exotique, nous aurions en fait pu retrouver $\chi_{H'}$ comme suit. Considérons l'action naturelle de A_5 sur l'ensemble Z des parties à 2 éléments de $\{1,\dots,5\}$. C'est une action transitive et on a $|Z| = 10$. On a clairement

$$\chi_{\mathbb{C}Z} \mid 10\ 2\ 1\ 0\ 0,$$

ainsi que $\langle \chi_{\mathbb{C}Z}, 1\rangle = \frac{1}{60}(10+2\cdot 15+20) = 1$ et $\langle \chi_{\mathbb{C}Z}, \chi_H\rangle = \frac{1}{60}(40+20) = 1$, de sorte que $\chi = \chi_{\mathbb{C}Z} - 1 - \chi_H$ est un caractère de degré 5, et on constate que c'est $\chi_{H'}$.

Reste à déterminer les deux caractères de degré 3. On suppute qu'ils sont reliés au fait que A_5 se plonge dans $\mathrm{O}(3) \subset \mathrm{GL}_3(\mathbb{C})$ comme groupe d'isométrie de l'icosaèdre, et on pourrait en effet calculer ainsi ces caractères. Déduisons-les plutôt des relations d'orthogonalité. Posons

$$\begin{array}{c|ccccc} \chi_2 & 3 & a & b & c & d \\ \chi_3 & 3 & a' & b' & c' & d' \end{array}$$

On fait les observations suivantes :

– En contemplant la colonne $(1\,2\,3)$ on a $|b|^2 + |b'|^2 = 0$, donc $b = b' = 0$.

– En écrivant $\langle \chi_2, \chi_{H'}\rangle = \langle \chi_3, \chi_{H'}\rangle = 0$, on a aussi $15 + 15a = 15 + 15a' = 0$, donc $a = a' = -1$.

– Tout 5-cycle $c = (s\,u\,p\,e\,r)$ est conjugué dans à $c^{-1} = (r\,e\,p\,u\,s)$ par la double transposition $(r\,s)(e\,u) \in \mathrm{A}_5$. On a donc $\chi(c) = \chi(c^{-1}) = \overline{\chi(c)}$ pout tout caractère χ de A_5. On en déduit que c, d, c', d' sont des nombres réels.

– En contemplant chacune des deux dernières colonnes, on trouve donc $c^2+(c')^2 = d^2+(d')^2 = 3$ (cela utilise l'observation précédente), et par orthogonalité des colonnes $\{1,4,5\}$ on a aussi $1 + 3c + 3c' - 4 = 0$ et donc $c + c' = 1$, et de même $d + d' = 1$, de sorte que c et c' sont solutions de $x^2 + (1-x)^2 = 3$, *i.e* $x^2 = x + 1$.

On a donc $c, c' \in \{\phi, \phi'\}$ avec

$$\phi = \frac{1+\sqrt{5}}{2} \quad \text{et} \quad \phi' = \frac{1-\sqrt{5}}{2}$$

(le nombre d'or et son conjugué, chers à l'icosaèdre !). Si on a $c = c'$, alors $1 - c = d = d' = 1 - c'$ et $\chi_2 = \chi_3$, une contradiction. Quitte à échanger χ_2 et χ_3, on peut supposer $c = \phi$, et donc $d = 1 - \phi = \phi'$, et $c' = \phi'$ puis $d' = 1 - \phi' = \phi$. Cela conduit à la Table 5 ci-après !

$\sharp$cent	60	4	3	5	5
$\sharp$conj	1	15	20	12	12
	1	$(1\,2)(3\,4)$	$(1\,2\,3)$	$(1\,2\,3\,4\,5)$	$(1\,2\,3\,5\,4)$
1	1	1	1	1	1
χ_2	3	-1	0	ϕ	ϕ'
χ_3	3	-1	0	ϕ'	ϕ
χ_H	4	0	1	-1	-1
$\chi_{H'}$	5	1	-1	0	0

Table 5. Table des caractères de A_5.

On a vu que SO(3) ne possède qu'une classe de conjugaison de sous-groupes isomorphes à A_5 : les groupes d'isométries directes des icosaèdres et dodécaèdres réguliers de l'espace euclidien de dimension 3 qui sont centrés en 0. Il peut donc sembler curieux qu'il y ait deux lignes de dimension 3. On rappelle que si D est un dodécaèdre régulier, son groupe d'isométries directes s'identifie au groupe alterné sur l'ensemble des 5 repères de D (Proposition 1.12 Chap. 4). C'est le choix d'une numérotation de ces 5 repères qui donne un isomorphisme $\mathrm{Iso}^+(\mathrm{D}) \simeq \mathrm{A}_5$, puis par composition une représentation

$$\rho : \mathrm{A}_5 \xrightarrow{\sim} \mathrm{Iso}^+(\mathrm{D}) \subset \mathrm{O}(3) \subset \mathrm{GL}_3(\mathbb{C}) \subset \mathrm{GL}_3(\mathbb{C}).$$

Changer de numérotation des 5 repères revient à composer ρ à la source le morphisme ci-dessus par un int_σ avec $\sigma \in \mathrm{S}_5$ (on rappelle que A_5 est distingué dans S_5). Si σ est dans A_5, la représentation $\rho \circ \mathrm{int}_\sigma$ de A_5 est isomorphe à ρ. En effet, on a $\rho \circ \mathrm{int}_\sigma(g) = \rho(\sigma)\rho(g)\rho(\sigma)^{-1}$ pour $g \in \mathrm{A}_5$. Mais il n'y a pas de raison que ce soit encore le cas si σ ne l'est pas... et ce n'est pas le cas pour χ_2 et χ_3 ! En effet, dans tous les cas le caractère de $\rho \circ \mathrm{int}_\sigma$ est clairement $\chi_\rho \circ \mathrm{int}_\sigma$. Pour $\sigma = (4\,5)$, on constate que int_σ préserve les classes de conjugaison de $1, (1\,2)(3\,4)$ et $(1\,2\,3)$ dans A_5, mais échange $(1\,2\,3\,4\,5)$ et $(1\,2\,3\,5\,4)$. Comme χ_2 ne prend pas les même valeurs sur ces deux éléments (ce sont ϕ et ϕ'), $\chi_2 \circ \mathrm{int}_{(4\,5)}$ et χ_2 sont différents, et tout s'éclaircit !

Remarque 5.4. (𝔸𝕋𝕃𝔸𝕊 *des groupes finis*) Nous renvoyons au fabuleux 𝔸𝕋𝕃𝔸𝕊 *des groupes finis*, par Conway, Curtis, Norton, Parker & Wilson, pour des tables de caractères des 93 premiers groupes simples (incluant tous les 26 groupes sporadiques), ainsi qu'une multitude de renseignements les concernant. Les Figures 1 et 2 ci-contre reproduisent par exemple la page A_5 de 𝔸𝕋𝕃𝔸𝕊 (pour que ce soit lisible, nous en avons fait deux pages, le format de 𝔸𝕋𝕃𝔸𝕊 étant 42 cm × 30 cm). Bien que la plus simple de toutes, une des caractéristique de l'𝔸𝕋𝕃𝔸𝕊 est déjà frappante sur cette page : le côté minimaliste, et admettons-le, un peu cryptique, des notations et des explications ! Nous renvoyons à l'introduction de l'𝔸𝕋𝕃𝔸𝕊 pour le détail des conventions et notations. Par exemple, la page A_5 ci-dessus contient aussi les tables des caractères de S_5 (noté $G.2$) et de $\widetilde{\mathrm{A}_5}$ (noté $2.G$).

$A_5 \cong L_2(4) \cong L_2(5)$

Alternating group A_5; Linear group $L_2(4) \cong A_1(4) \cong U_2(4) \cong S_2(4) \cong O_3(4) \cong O_4^-(2)$;

Linear group $L_2(5) \cong A_1(5) \cong U_2(5) \cong S_2(5) \cong O_3(5)$

Order = $60 = 2^2.3.5$ Mult = 2 Out = 2

Constructions

Alternating $S_5 \cong G.2$: all permutations of 5 letters;

$A_5 \cong G$: all even permutations; 2.G and 2.G.2 : the Schur double covers

Linear (4) $GL_2(4) \cong 3 \times G$: all non-singular 2 x 2 matrices over $\mathbf{F}_4$;

$SL_2(4) \cong PGL_2(4) \cong PSL_2(4) \cong G$; $\Gamma L_2(4) \cong (3 \times G).2$; $P\Gamma L_2(4) \cong \Sigma L_2(4) \cong P\Sigma L_2(4) \cong G.2$

Unitary (4) $GU_2(4) \cong 5 \times G$: all 2 x 2 matrices over $\mathbf{F}_{16}$ preserving a non-singular Hermitian form;

$PGU_2(4) \cong SU_2(4) \cong PSU_2(4) \cong G$

Orthogonal (4) $GO_3(4) \cong PGO_3(4) \cong SO_3(4) \cong PSO_3(4) \cong O_3(4) \cong G$: all 2 x 2 matrices over $\mathbf{F}_4$ preserving a non-singular quadratic form; $\Gamma O_3(4) \cong P\Gamma O_3(4) \cong \Sigma O_3(4) \cong P\Sigma O_3(4) \cong G.2$

Orthogonal (2) $GO_4^-(2) \cong PGO_4^-(2) \cong SO_4^-(2) \cong PSO_4^-(2) \cong G.2$: all 4 x 4 matrices over $\mathbf{F}_2$ preserving a quadratic form of Witt defect 1, for example $x_1^2 + x_1x_2 + x_2^2 + x_3x_4$; $O_4^-(2) \cong G$

Linear (5) $GL_2(5) \cong 2.(G \times 2).2$: all non-singular 2 x 2 matrices over $\mathbf{F}_5$;

$PGL_2(5) \cong G.2$; $SL_2(5) \cong 2.G$; $PSL_2(5) \cong G$

Unitary (5) $GU_2(5) \cong 3 \times 2.G.2$: all 2 x 2 matrices over $\mathbf{F}_{25}$ preserving a non-singular Hermitian form;

$PGU_2(5) \cong G.2$; $SU_2(5) \cong 2.G$; $PSU_2(5) \cong G$

Orthogonal (5) $GO_3(5) \cong 2 \times G.2$: the 3 x 3 matrices over $\mathbf{F}_5$ preserving a non-singular quadratic form;

$PGO_3(5) \cong SO_3(5) \cong PSO_3(5) \cong G.2$; $O_3(5) \cong G$

Quaternionic 2.G is the group of those quaternions q for which the coordinates of 2q are :

$(\pm 2,0,0,0)^A$, $(\pm 1,\pm 1,\pm 1,\pm 1)$, $(0,\pm 1,\pm b5,\pm b5^*)^A$; these generate the icosian ring

Icosahedral G x 2 : symmetries of the vectors $(0,\pm 1,\pm b5^*)^C$ (vertices of icosahedron), or of $(\pm 1,\pm 1,\pm 1)$, $(0,\pm b5^*,\pm b5)^C$ (dodecahedron), or of $(\pm 2,0,0)^C$, $(\pm 1,\pm b5,\pm b5^*)^C$ (icosidodecahedron: the reflections in these generate G x 2). These vectors are obtained by deleting the real parts of the above quaternions. G is the group of symmetries of determinant 1.

Presentations $2.G \cong \langle 2,3,5\rangle$; $G \cong (2,3,5) \cong G^{3,5,5} \cong \langle x_1,x_2,x_3 \mid x_i^3=(x_ix_j)^2=1\rangle$;

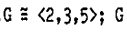
$G.2 \cong (2,4,5;3) \cong (2,5,6;2)$; $G \times 2 \cong$  $\cong G^{3,5,10}$; $G.2 \times 2 \cong G^{4,5,6}$

FIGURE 1. La page A_5 de l'ATLAS (moitié supérieure).

Maximal subgroups					Specifications			
Order	Index	Structure	G.2	Character	Abstract	Alternating	Linear (4)	Orthogonal (4)
12	5	A_4	$: S_4$	1a+4a	$N(2A^2)$	point	point	isotropic point
10	6	D_{10}	: 5:4	1a+5a	N(5AB)		$O_2^-(4)$, $L_1(16)$	minus line
6	10	S_3	$: 2 \times S_3$	1a+4a+5a	N(3A)	duad	$O_2^+(4)$, base	plus line

Orthogonal (2)	Linear (5)	Orthogonal (5)	Icosahedral
isotropic point		base	base
$O_2^-(4)$	point	isotropic point	pentad axis
non-isotropic point	$O_2^-(5)$, $L_1(25)$	minus point	triad axis

	;	@	@	@	@	@	;	;	@	@	@
		60	4	3	5	5			6	2	3
	p power		A	A	A	A			A	A	AB
	p' part		A	A	A	A			A	A	AB
	ind	1A	2A	3A	5A	B*	fus	ind	2B	4A	6A
χ_1	+	1	1	1	1	1	:	++	1	1	1
χ_2	+	3	-1	0	-b5	*		+	0	0	0
χ_3	+	3	-1	0	*	-b5					
χ_4	+	4	0	1	-1	-1	:	++	2	0	-1
χ_5	+	5	1	-1	0	0	:	++	1	-1	1
	ind	1	4	3	5	5	fus	ind	2	8	6
		2		6	10	10				8	6
χ_6	-	2	0	-1	b5	*		-	0	0	0
χ_7	-	2	0	-1	*	b5					
χ_8	-	4	0	1	-1	-1	:	oo	0	0	i3
χ_9	-	6	0	0	1	1	:	oo	0	i2	0

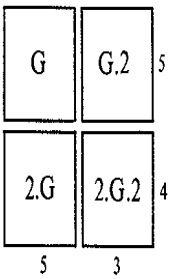


FIGURE 2. La page A_5 de l'ATLAS (moitié inférieure).

6. Propriétés d'intégralité des caractères

Définition 6.1. *(Dedekind) Un entier algébrique est un nombre complexe annulé par un polynôme* unitaire *à coefficients entiers. On note $\overline{\mathbb{Z}} \subset \mathbb{C}$ l'ensemble des entiers algébriques.*

En particulier, un entier algébrique est un nombre algébrique. Par exemple, les complexes $\sqrt{N}$ et $e^{2i\pi/N}$ pour $N \in \mathbb{Z}$, les entiers usuels, ou encore tout $x \in \mathbb{C}$ tel que $x^3 = x + 1$, sont des entiers algébriques. On peut dire que les entiers algébriques sont aux nombres algébriques ce que les entiers sont aux nombres rationnels. La proposition suivante, classique à sa formulation près, en est un premier indicateur.

Proposition 6.2. *Les entiers algébriques qui sont rationnels sont dans $\mathbb{Z}$. Autrement dit, on a $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$.*

Démonstration — C'est le fait bien connu que si le rationnel p/q, avec $(p, q) = 1$, est racine d'un polynôme $P \in \mathbb{Z}[X]$, alors q divise le coefficient dominant de P, comme on le voit en regardant l'égalité $q^n P(p/q) = 0$ avec $n = \deg(P)$. Si P est unitaire, on a donc $q = \pm 1$, puis $p/q \in \mathbb{Z}$. □

Proposition 6.3. *$\overline{\mathbb{Z}}$ est un sous-anneau de $\mathbb{C}$.*

Observons cependant que $\overline{\mathbb{Z}}$ n'est pas un sous-corps de $\mathbb{C}$. En effet, on a $1/N \notin \overline{\mathbb{Z}}$ pour $N \geqslant 2$ d'après la proposition précédente. Pour démontrer la Proposition 6.3, nous aurons besoin du critère d'intégralité suivant.

Proposition 6.4. *Soit R un anneau de groupe additif (abélien) de type fini et sans torsion.*[5] *Alors pour tout $x \in R$ il existe $P \in \mathbb{Z}[X]$ unitaire tel que $P(x) = 0$.*

Démonstration — Un groupe abélien de type fini sans torsion est libre. Pour $x \in R$, on considère l'application $\mathbb{Z}$-linéaire $\mathrm{m}_x : R \to R, r \mapsto xr$, de multiplication par x. Comme R est un $\mathbb{Z}$-module libre de rang fini, on sait que la donnée d'une $\mathbb{Z}$-base à n éléments $e_1, \ldots, e_n$ de R identifie l'anneau $\mathrm{End}_{\mathbb{Z}}(R)$ à $\mathrm{M}_n(\mathbb{Z})$. Concrètement, on a $xe_j = \sum_{i=1}^n m_{i,j} e_i$ pour des uniques $m_{i,j} \in \mathbb{Z}$, et on a

$$\mathrm{Mat}_e \mathrm{m}_x = (m_{i,j}) \in \mathrm{M}_n(\mathbb{Z}).$$

Mais toute matrice dans $\mathrm{M}_n(\mathbb{Z})$ est annulée par un polynôme unitaire à coefficients entiers : son polynôme caractéristique. Si P est celui de $\mathrm{Mat}_e \mathrm{m}_x$, on a donc $P(\mathrm{m}_x) = 0 = \mathrm{m}_{P(x)}$ et donc $P(x)1 = P(x) = 0$ dans R. □

Démonstration — (de la Proposition 6.3) Soient $x, y \in \overline{\mathbb{Z}}$. Supposons x et y annulés par des polynômes dans $\mathbb{Z}[X]$ unitaires de degrés respectifs m et n. On a donc $x^m \in X := \sum_{i=0}^{m-1} \mathbb{Z}x^i$ et $y^n \in Y := \sum_{j=0}^{n-1} \mathbb{Z}y^j$. On en déduit $x^a \in X$ et $y^b \in Y$ pour tout $a, b \geqslant 0$. Il en résulte que $R := \sum_{0 \leqslant i < m, 0 \leqslant j < n} \mathbb{Z}x^i y^j$ est un sous-anneau de $\mathbb{C}$. Mais le groupe additif de R de type fini, et sans torsion car $R \subset \mathbb{C}$. La Proposition 6.4 entraîne $R \subset \overline{\mathbb{Z}}$. On conclut car on a xy et $x \pm y \in R$. □

5. L'hypothèse « sans torsion » n'est pas nécessaire mais simplifie quelque peu l'argument.

La proposition 6.3 permet de vérifier que certains nombres algébriques ne sont pas des entiers algébriques. Par exemple $x = \frac{1+\sqrt{3}}{2}$ est un nombre algébrique, satisfaisant $x^2 - x - 1/2 = 0$. Si x était entier algébrique, il en serait de même de $x^2 - x = 1/2$, ce qui n'est pas. Mentionnons tout de même qu'il ne faut pas toujours se fier aux apparences : le nombre d'or $\phi = \frac{1+\sqrt{5}}{2}$ est un entier algébrique, car on a $\phi^2 = \phi + 1$.

Retournons aux caractères des groupes finis. On fixe désormais G un groupe fini. La première observation est la suivante.

Proposition 6.5. *Pour tout caractère χ de G, et tout $g \in G$, on a $\chi(g) \in \overline{\mathbb{Z}}$.*

Démonstration — En effet, on sait que $\chi(g)$ est une somme finie de racines de l'unité (Proposition 4.8). Mais toute racine n-ème de l'unité est dans $\overline{\mathbb{Z}}$, car annulée par $X^n - 1$. On conclut par la Proposition 6.3. □

Le résultat clé est le suivant, car un quotient n'a pas tendance à être entier :

Proposition 6.6. (Frobenius) *Pour tout $\chi \in \operatorname{Irr} G$, de dimension $n = \chi(1)$, et tout $g \in G$, on a*

$$\frac{1}{n}\,|\mathrm{Conj}(g)|\;\chi(g) \in \overline{\mathbb{Z}}.$$

Démonstration — (Démonstration de Burnside) En effet notons $\mathbb{Z}[G] \subset \mathbb{C}[G]$ le sous-groupe $\oplus_{g\in G}\mathbb{Z}g$. C'est clairement un sous-anneau, et il est libre de rang $|G|$ comme $\mathbb{Z}$-module, avec pour base les $g \in G$. D'après la Proposition 6.4, tout élément de $\mathbb{Z}[G]$ est donc annulé par un polynôme unitaire à coefficients entiers.

Soit $C \subset G$ la classe de conjugaison de g. L'élément $z = \sum_{h\in C} h$ est dans $\mathbb{Z}[G] \cap \mathrm{Z}(\mathbb{C}[G])$ par le Lemme 4.22 (i). Par le paragraphe précédent, il est annulé par un polynôme unitaire $P \in \mathbb{Z}[X]$. Mais par le Lemme 4.22 (i), on sait aussi que z agit sur tout $\mathbb{C}[G]$-module irréductible S par l'homothétie de rapport

$$\lambda_S(z) \;=\; \frac{1}{\dim S}\,|C|\,\chi_S(g).$$

Mais on a clairement $\lambda_S(Q(z)) = Q(\lambda_S(z))$ pour tout $Q \in \mathbb{C}[X]$, car $\lambda_S : \mathrm{Z}(\mathbb{C}[G]) \to \mathbb{C}$ est un morphisme de $\mathbb{C}$-algèbres. De $P(z) = 0$ on déduit donc $P(\lambda_S(z)) = 0$, c'est-à-dire $\lambda_S(z) \in \overline{\mathbb{Z}}$. On conclut en posant $\chi = \chi_V$. □

En guise d'application de cette propriété, montrons le théorème suivant.

Théorème 6.7. (Frobenius) Soit V un $\mathbb{C}[G]$-module irréductible de dimension finie. Alors $\dim V$ divise $|G|$.

Démonstration — Si $g_1, \ldots, g_h$ sont des représentants des classes de conjugaison de G, la relation d'orthogonalité $\langle \chi_V, \chi_V \rangle = 1$ montre

$$\frac{|G|}{\dim V} = \frac{|G|}{\dim V}\langle \chi_V, \chi_V \rangle = \sum_{i=1}^{h} \left(\frac{1}{\dim V}\,|\mathrm{Conj}(g_i)|\,\chi_V(g_i) \right) \overline{\chi_V(g_i)}.$$

D'après les Propositions 6.3, 6.5 et 6.6, cet élément est dans $\overline{\mathbb{Z}}$. (Il est clair que $\overline{\mathbb{Z}}$ est stable par conjugaison complexe). On conclut par la Proposition 6.2. □

Exemple 6.8. Si G est d'ordre pq avec p, q premiers et $p \leqslant q$. Les représentations irréductibles de G sont de degré 1 ou p. En effet, celles de degré $n > 1$ vérifient $n^2 < |G| = pq$ et $n \mid pq$.

Exemple 6.9. Soit G un p-groupe non abélien d'ordre p^3, par exemple le groupe de Heisenberg $\mathrm{U}_3(\mathbb{Z}/p\mathbb{Z})$. Alors les représentations irréductibles de G sont de dimension p^n avec $n \leqslant 3$. Mais $p^{2n} \leqslant |G| = p^3$ implique $n \leqslant 1$. Donc les seules dimensions possibles sont 1 et p. En fait, le centre Z de G est nécessairement cyclique d'ordre p (il est non trivial, et G/Z n'est pas cyclique), donc G/Z est d'ordre p^2, et donc abélien. On en déduit $\mathrm{D}(G) = Z$, puis que G a exactement $|G/Z| = p^2$ caractères de degré 1. La formule $p^3 = p^2 + p^2(p-1)$ montre qu'il y a exactement $p-1$ caractères irréductibles de degré p.

Comme nous le verrons dans le Complément 9, Burnside a donné d'autres applications frappantes de ces idées !

7. Retour sur le déterminant d'un groupe fini

Revenons, comme promis, sur la question de Dedekind consistant à factoriser le déterminant

$$\det G \;=\; \det(X_{gh^{-1}})_{g,h\in G}$$

d'un groupe fini G, introduit au §2 Chap. 3. C'est manifestement un polynôme homogène de degré $|G|$ à coefficients dans $\mathbb{Z}$ en les indéterminées X_g indexées par les éléments de G. Notons $\mathbb{C}[X_G]$ l'anneau de polynômes $\mathbb{C}[\{X_g\}_{g\in G}]$ en ces $|G|$ variables et à coefficients *complexes*.

Théorème 7.1. (Frobenius) *Si G est un groupe fini, et si $n_1,\dots,n_h$ sont les dimensions des h caractères irréductibles de G, alors on a une décomposition*

$$\det G = \prod_{i=1}^{h} F_i^{n_i}$$

où les F_i sont des polynômes irréductibles, homogènes de degré n_i, en les X_g, et 2 à 2 non associés.

Pour cela, associons à chaque $\mathbb{C}[G]$-module de dimension finie V un polynôme $\mathrm{D}_V \in \mathbb{C}[X_G]$ en posant, pour tout $|G|$-uple $x_G = (x_1,\dots,x_g,\dots) \in \mathbb{C}^G$,

$$\mathrm{D}_V(x_G) \;:=\; \det(\sum_{g\in G} x_g\,\rho_V(g)\,).$$

Ce polynôme D_V est manifestement homogène de degré $\dim V$, et ne dépend que de la classe d'isomorphisme de V. De plus, on a

$$\mathrm{D}_{V\oplus U} = \mathrm{D}_V\mathrm{D}_U.$$

Exemple 7.2. Si V est de dimension 1, de caractère de degré 1 associé $\chi : G \to \mathbb{C}^\times$, on a clairement $\mathrm{D}_V = \sum_{g\in G}\chi(g)\mathrm{X}_g$.

Exemple 7.3. Considérons $V = \mathbb{C}^3$ la représentation de permutation standard de $G = \mathrm{S}_3$. On a vu $V = \mathbb{C}\oplus H$ avec H irréductible. Posant $E = X_1$, $T_1 = X_{(23)}$, $T_2 = X_{(13)}$, $T_3 = X_{(12)}$, $C_1 = X_{(1\,2\,3)}$ et $C_2 = X_{(1\,3\,2)}$ on constate

$$\det\begin{bmatrix} E+T_1 & T_3+C_2 & T_2+C_1 \\ T_3+C_1 & E+T_2 & T_1+C_3 \\ T_2+C_2 & T_1+C_1 & E+T_3 \end{bmatrix} = \mathrm{D}_V = (E+T_1+T_2+T_3+C_1+C_2)\,\mathrm{D}_H.$$

En se plaçant dans la base e_1-e_2, e_2-e_3 de H, on vérifierait (exercice !)

$$\mathrm{D}_H = \det\begin{bmatrix} E+T_1-T_3+C_2 & -T_2+T_3-C_1+C_2 \\ T_1-T_2+C_1-C_2 & E-T_1+T_3-C_1 \end{bmatrix}.$$

On a donc $\det \mathrm{S}_3 = \mathrm{D}_1\mathrm{D}_\varepsilon\mathrm{D}_H^2$ (Théorème 7.1 et Table 2).

Exemple 7.4. Pour $V = \mathbb{C}\,G$ (représentation régulière), on constate

$$\mathrm{D}_{\mathbb{C}G} = \det G. \tag{72}$$

En effet, soit $z = \sum_{g\in G} x_g g \in \mathbb{C}[G]$. Pout $h \in G \subset \mathbb{C}\,G$ on constate $zh = \sum_{g\in G} x_g\, gh = \sum_{g\in G} x_{gh^{-1}} g$, de sorte que la matrice de la multiplication par z dans la base canonique de $\mathbb{C}\,G$, est $(x_{gh^{-1}})_{g,h\in G}$.

L'exemple précédent indique clairement la marche à suivre pour démontrer le théorème. D'après le Corollaire 4.18, on a aussi une décomposition

$$\mathbb{C}\,G \simeq \oplus_{i=1}^{h} S_i^{\oplus n_i}$$

où S_i est un $\mathbb{C}[G]$-module irréductible de dimension n_i, non isomorphe à S_j pour $j \neq i$. On en déduit

$$\det G = \prod_{i=1}^{h} \mathrm{D}_{S_i}^{n_i}.$$

Posant $F_i = \mathrm{D}_{S_i}$, le Théorème 7.1 découle du lemme suivant.

Lemme 7.5. *Soient U et V deux $\mathbb{C}[G]$-modules irréductibles.*

(i) Le polynôme D_U est irréductible dans $\mathbb{C}[X_G]$.

(ii) Si U est V sont non isomorphes, alors D_U et D_V sont non proportionnels.

L'ingrédient restant pour prouver ce lemme est le théorème important suivant. Si V est un $\mathbb{C}[G]$-module, on dispose d'un morphisme de $\mathbb{C}$-algèbres naturel

$$\pi_U : \mathbb{C}[G] \to \mathrm{End}_{\mathbb{C}}(V),\ x \mapsto (v \mapsto x.v).$$

Théorème 7.6. *Soit G un groupe fini.*

(i) (Burnside) *Si V est un $\mathbb{C}[G]$-module irréductible, alors π_V est surjectif. Autrement dit, les $\rho_V(g)$ avec $g \in G$ engendrent $\mathbb{C}$-linéairement $\mathrm{End}_{\mathbb{C}}(V)$.*

(ii) (Maschke) *Si $S_1, \ldots, S_h$ sont "les" $\mathbb{C}[G]$-modules irréductibles de G, deux à deux non isomorphes, alors le morphisme de $\mathbb{C}$-algèbres*

$$\pi : \mathbb{C}[G] \to \mathrm{End}_{\mathbb{C}}(S_1) \times \mathrm{End}_{\mathbb{C}}(S_2) \times \cdots \times \mathrm{End}_{\mathbb{C}}(S_h),$$

$$x \mapsto (\pi_{S_1}(x), \pi_{S_2}(x), \ldots, \pi_{S_h}(x)),$$

est un isomorphisme.

Démonstration — Le morphisme π est injectif ! En effet, si on a $z \in \mathbb{C}[G]$ avec $\pi(z) = 0$, alors l'élément z agit par 0 dans tout $\mathbb{C}[G]$-module irréductible, puis donc par Maschke dans tout $\mathbb{C}[G]$-module de dimension finie. Dans le cas de la représentation régulière, on a $z.1 = z$ et donc $z = 0$. (On a déjà rencontré cet argument dans la démonstration du Théorème 4.20). Mais on a

$$\dim \mathbb{C}G = \sum_{i=1}^{h} (\dim S_i)^2 = \dim \prod_{i=1}^{h} \mathrm{End}_{\mathbb{C}}(V_i),$$

de sorte que l'injectivité de π implique sa bijectivité, d'où le (ii). En particulier, pour tout $i = 1, \ldots, h$ on a $\mathrm{Im}\,\pi_i = \mathrm{End}_{\mathbb{C}}(S_i)$, ce qui démontre le (i). □

Remarque 7.7. En particulier, on a montré qu'il existe un isomorphisme de $\mathbb{C}$-algèbres $\mathbb{C}[G] \xrightarrow{\sim} \prod_{i=1}^{h} \mathrm{M}_{n_i}(\mathbb{C})$, où les n_i sont les dimensions des représentations irréductibles de G. Mentionnons aussi que le Théorème de Burnside vaut encore (par une preuve différente) si G est quelconque (pas forcément fini) et si $\mathbb{C}$ est remplacé par un corps algébriquement clos quelconque.

Nous pouvons enfin démontrer le Lemme 7.5 (et donc le Théorème 7.1).

Démonstration — (Preuve du Lemme 7.5). Montrons d'abord l'assertion (ii). Soient U et V deux $\mathbb{C}[G]$-modules irréductibles non isomorphes. D'après le Théorème 7.6 (ii), il existe $z \in \mathbb{C}[G]$ tel que $\pi_U(z) = \mathrm{Id}_U$ et $\pi_V(z) = 0$. Écrivons $z = \sum_{g\in G} x_g g$ et posons $x = (x_g)_{g\in G} \in \mathbb{C}^G$. Alors on a $\mathrm{D}_U(x) = \det \pi_U(x) = 1$ et $\mathrm{D}_V(x) = \det \pi_V(x) = 0$. Cela montre le (ii).

Montrons mainenant le (i). On fixe une base $e = (e_1, \ldots, e_n)$ de V et on pose $\mathrm{Mat}_e \rho_V(g) = (m_{i,j}(g))_{1\leqslant i,j\leqslant n}$. Les n^2 formes linéaires

$$\mathrm{L}_{i,j} : \mathbb{C}^G \to \mathbb{C}, (x_g)_{g\in G} \mapsto \sum_{g\in G} x_g\, m_{i,j}(g),$$

sont linéairement indépendantes d'après le Théorème 7.6 (i). On les complète arbitrairement en une base du dual de $\mathbb{C}^G$, en ajoutant $\mathrm{L}_1, \ldots, \mathrm{L}_r$ (avec $r = |G| - n^2$). Dans ces nouvelles variables linéaires, on a donc $\mathbb{C}[X_G] = \mathbb{C}[\{\mathrm{L}_{i,j}\}_{i,j}][\mathrm{L}_1, \ldots, \mathrm{L}_r]$. Mais par définition, on a aussi

$$\mathrm{D}_V = \det((\mathrm{L}_{i,j})_{1\leqslant i,j\leqslant n}).$$

On conclut par le fait, classique !, que le déterminant de la matrice $(\mathrm{T}_{i,j})_{1\leqslant i,j\leqslant n}$ (à coefficients indéterminées) est irréductible dans $\mathbb{C}[\{\mathrm{T}_{i,j}\}_{1\leqslant i,j\leqslant n}]$: voir l'Exercice 9.32. $\square$

8. Décomposition à la Fourier de $\mathrm{L}^2(G)$

Soit G un groupe fini. Le groupe G admet une représentation $\mathbb{C}$-linéaire naturelle sur $\mathrm{L}^2(G)$ par translations à droite, que nous avions noté $(g, f) \mapsto \mathrm{R}_g(f)$ au Chapitre 3. Nous avions aussi vu que cette représentation est *unitaire* relativement au produit scalaire $\langle -, - \rangle$ de $\mathrm{L}^2(G)$, c'est à dire que l'on a

$$\langle \mathrm{R}_g(f), \mathrm{R}_g(f') \rangle = \langle f, f' \rangle \tag{73}$$

pour tout $g \in G$ et tout $f, f' \in \mathrm{L}^2(G)$. On se propose dans cette partie d'étudier la décomposition en irréductibles de la représentation $\mathrm{L}^2(G)$.

Lemme 8.1. *L'application* $\mathrm{L}^2(G) \to \mathbb{C}[G]$, $f \mapsto \sum_{g \in G} f(g^{-1})g$ *et un isomorphisme de* $\mathbb{C}[G]$*-modules.*

Démonstration — L'application ψ de l'énoncé est clairement un isomorphisme de $\mathbb{C}$-espace vectoriel. Il ne reste qu'à voir que pour $h \in G$ et $f \in \mathrm{L}^2(G)$ on a $\psi(\mathrm{R}_h(f)) = h\psi(f)$. On conclut car par changement de variables $g \mapsto hg$ on a

$$\psi(\mathrm{R}_h(f)) = \sum_{g \in G} \mathrm{R}_h(f)(g^{-1})g = \sum_{g \in G} f(g^{-1}h)g = \sum_{g \in G} f(g^{-1})hg = h\psi(f).$$

□

D'après le Corollaire 4.18, on en déduit que toute représentation irréductible U de G intervient dans $\mathrm{L}^2(G)$ avec une multiplicité $\dim U$. Nous allons raffiner ce résultat en identifiant concrètement les composantes isotypiques de $\mathrm{L}^2(G)$. La notion clé est celle de *coefficient matriciel.*

Définition 8.2. *Soit U un $\mathbb{C}[G]$-module de dimension finie. Pour $u \in U$ et $\varphi \in U^*$, on pose $\mathrm{c}_{u,\varphi} : G \to \mathbb{C}, g \mapsto \varphi(g.u)$. Une application $G \to \mathbb{C}$ de cette forme s'appelle un* coefficient matriciel *de U. On note* $\mathrm{Coeff}(U) \subset \mathrm{L}^2(G)$ *le sous-espace vectoriel engendré par les coefficients matriciels de U.*

Par exemple, si l'on choisit une base $e = (e_1, \ldots, e_n)$ de U, et si l'on pose

$$\mathrm{Mat}_e\, \rho_U(g) \;=\; (\, m_{i,j}(g)\,)_{1 \leqslant i,j \leqslant n} \in \mathrm{GL}_n(\mathbb{C}),$$

alors pour tout $1 \leqslant i, j \leqslant n$ l'application $G \mapsto \mathbb{C}, g \mapsto m_{i,j}(g)$, est un coefficient matriciel de U. En effet, on a $m_{i,j} = \mathrm{c}_{e_i, e_j^\star}$ où les $e_i^\star \in U^\star$ désignent la base duale de e_i. Cela explique la terminologie. Comme l'application

$$U \times U^\vee \to \mathrm{L}^2(G), (u, \varphi) \mapsto \mathrm{c}_{u,\varphi}, \tag{74}$$

est manifestement $\mathbb{C}$-bilinéaire, on en déduit

$$\mathrm{Coeff}(U) \;=\; \sum_{1 \leqslant i,j \leqslant n} \mathbb{C}\, m_{i,j}. \tag{75}$$

Par exemple, le caractère $\chi_U = \sum_{i=1}^n m_{i,i}$ est une somme de coefficients matriciels, et on a $\chi_U \in \mathrm{Coeff}(U)$. Comme deux représentation isomorphes ont même représentations matricielles associés dans des bases convenables, on en déduit aussi que *le sous-espace* $\mathrm{Coeff}(U)$ *de* $\mathrm{L}^2(G)$ *ne dépend que de la classe d'isomorphisme de U.*

Lemme 8.3. *Soit U un $\mathbb{C}[G]$-module de dimension finie. Le sous-espace* $\mathrm{Coeff}(U)$ *de* $\mathrm{L}^2(G)$ *est un sous-$\mathbb{C}[G]$ module stable par les translations à gauche par G.*

La translation à gauche par $g \in G$ est définie par $\mathrm{L}_g(f)(h) = f(g^{-1}h)$.

Démonstration — Pour $g, h \in H$, $u \in U$ et $\varphi \in U^\vee$ on constate

$$\mathrm{R}_h(\mathrm{c}_{u,\varphi})(g) = \varphi(ghu) = \mathrm{c}_{hu,\varphi}(g) \tag{76}$$

et donc $\mathrm{R}_h(\mathrm{c}_{u,\varphi}) = \mathrm{c}_{hu,\varphi}$. Un calcul similaire montre $\mathrm{L}_h(\mathrm{c}_{u,\varphi}) = \mathrm{c}_{u,h.\varphi}$. Cela montre que $\mathrm{Coeff}(U)$ est G-stable dans $\mathrm{L}^2(G)$, stable également par les translations à gauche. □

Lemme 8.4. *Si U est un $\mathbb{C}[G]$-module irréductible, alors* $\mathrm{Coeff}(U)$ *coïncide avec la composante U-isotypique de* $\mathrm{L}^2(G)$.

Démonstration — À $\varphi \in V^*$ fixé, l'application $U \to \mathrm{L}^2(G)$, $u \mapsto \mathrm{c}_{u,\varphi}$, qui est $\mathbb{C}$-linéaire par bilinéarité de (74), est $\mathbb{C}[G]$-linéaire par la Formule (76). En particulier, si U est irréductible, chaque $\mathrm{c}_{u,\varphi}$ non nul engendre une sous-représentation de $\mathrm{L}^2(G)$ isomorphe à U. Cela implique que $\mathrm{Coeff}(U)$ est inclus dans la composante isotypique de U dans $\mathrm{L}^2(G)$.

Réciproquement, soit $V \subset \mathrm{L}^2(G)$ une sous-représentation (irréductible) isomorphe à U. Montrons qu'elle est incluse dans $\mathrm{Coeff}(U)$. Soit $\phi \in V$ non nulle. Il existe $x \in G$ tel que $\phi(x) \neq 0$. Considérons la forme linéaire $\varphi : \mathrm{L}^2(G) \to \mathbb{C}, f \mapsto f(x)$. Alors $\mathrm{c}_{\phi,\varphi} : G \mapsto \mathbb{C}, g \mapsto \phi(xg)$ est dans $\mathrm{Coeff}(S)$. Mais on a $\mathrm{Coeff}(S) = \mathrm{Coeff}(U)$ car U et S sont isomorphes. Ainsi $\mathrm{L}_x\mathrm{c}_{\phi,x.\varphi} = \phi$ est aussi dans $\mathrm{Coeff}(U)$, puis $S = \mathbb{C}[G].\phi \subset \mathrm{Coeff}(U)$, par le Lemme 8.4. □

Le résultat principal est alors le suivant :

Théorème 8.5. *Soient $S_1, \ldots, S_h$ des représentants des classes d'isomorphisme de $\mathbb{C}[G]$-modules irréductibles. On a une décomposition orthogonale*

$$\mathrm{L}^2(G) = \bigoplus_{1 \leqslant i \leqslant h}^{\perp} \mathrm{Coeff}(S_i),$$

ainsi que l'égalité $\dim \mathrm{Coeff}(S_i) = (\dim S_i)^2$ *pour tout $i = 1, \ldots, h$.*

Démonstration — Par unitarité (73), on peut écrire $\mathrm{L}^2(G)$ comme somme directe *orthogonale* de sous-représentations irréductibles. En regroupant entre eux les facteurs isomorphes, on en déduit une décomposition

$$\mathrm{L}^2(G) = \bigoplus_{1 \leqslant i \leqslant h}^{\perp} U_i.$$

où U_i est une somme directe de sous-représentations irréductibles isomorphes à S_i. D'après la Proposition 3.14, U_i est la composante isotypique de S_i dans $\mathrm{L}^2(G)$. D'après le Lemme 8.4, on a donc $U_i = \mathrm{Coeff}(S_i)$. D'après le Lemme 8.1 et le Corollaire 4.18, on a $U_i \simeq S_i^{\oplus \dim S_i}$, et en particulier, $\dim U_i = (\dim S_i)^2$. □

Remarque 8.6. La Formule montre que l'égalité $\dim \mathrm{Coeff}(U) = (\dim U)^2$ est équivalente à dire que les n^2 fonctions $m_{i,j} : G \to \mathbb{C}$ *loc. cit.* sont $\mathbb{C}$-linéairement indépendantes, ou encore que les $\rho_U(g)$ avec $g \in G$ engendrent linéairement $\mathrm{End}_{\mathbb{C}}(U)$. Cela donne une autre démonstration du Théorème 7.6.

9. Des théorèmes de Burnside et P. Hall

Le résultat suivant est connu pour être l'une des premières applications spectaculaires de la théorie des caractères à la structure des groupes finis.

THÉORÈME 9.1. (Burnside, 1904) *Soit G un groupe fini d'ordre $p^a q^b$ avec p, q des nombres premiers et $a, b \in \mathbb{Z}_{\geqslant 0}$. Alors G est résoluble.*

La démonstration qui suit est celle de Burnside. Il a fallu attendre 1972 pour que H. Bender [6] en donne une seconde démonstration (pas franchement plus simple) n'utilisant pas la théorie des caractères. La démonstration de Burnside repose sur le résultat suivant, aussi dû à Burnside.

THÉORÈME 9.2. (Burnside) *Soit G un groupe fini possédant une classe de conjugaison de cardinal p^n avec p premier et $n \geqslant 1$. Alors G n'est pas simple.*

DÉMONSTRATION — (Théorème 9.2 $\Longrightarrow$ Théorème 9.1) On raisonne par récurrence sur $|G|$. Il suffit de montrer que G n'est pas simple. En effet, si H est un sous-groupe distingué de G distinct de 1 et G, alors H et G/H sont d'ordre $p^{a'} q^{b'} < |G|$, et donc résolubles par récurrence, ainsi donc que G par la Proposition 8.7 Chap. 4.

On peut supposer $p \neq q$, ainsi que $a, b \geqslant 1$, car un p-groupe non abélien n'est pas simple (par exemple, son centre est non trivial). Soit $g \in G$ non central. On sait que $|\mathrm{Conj}\, g| > 1$ est un diviseur de $|G|$. Par le Théorème 9.2, on peut supposer que $|\mathrm{Conj}\, g|$ est multiple de pq pour tout $g \neq 1$, car sinon G est simple.

Écrivons alors l'équation aux classes pour l'action de conjugaison de G sur lui-même. On a $|G| = |\mathrm{Z}(G)| + \sum_{i=1}^{s} |\mathrm{Conj}\, g_i|$, où $g_1, \ldots, g_s$ sont des représentants des classes de conjugaisons non centrales de G. Alors pq divise $|\mathrm{Conj}\, g_i|$ pour tout $i = 1, \ldots, s$, et donc pq divise $\mathrm{Z}(G)$, et $\mathrm{Z}(G) \neq \{1\}$: G n'est pas simple. □

Pour démontrer le Théorème 9.2, nous aurons besoin du lemme d'arithmétique suivant.

LEMME 9.3. *Soient $\lambda_1, \ldots, \lambda_n \in \mathbb{C}^\times$ des racines de l'unité. On suppose que $\frac{1}{n}(\lambda_1 + \cdots + \lambda_n)$ est non nul et dans $\overline{\mathbb{Z}}$. Alors tous les λ_i sont égaux.*

DÉMONSTRATION — Ce lemme admet une démonstration assez limpide lorsqu'on dispose d'un peu de théorie des corps (voir le cours d'Algèbre 2 !). Pour être complet nous en donnerons une démonstration directe, mais un peu technique, à la fin de cette section. □

DÉMONSTRATION — (du Théorème 9.2) Soit g avec $|\mathrm{Conj}(g)| = p^n$ comme dans l'énoncé. La seconde relation d'orthogonalité (entre 1 et g) s'écrit

$$1 + \sum_{\chi \in \mathrm{Irr} G \smallsetminus \{1\}} \chi(g)\chi(1) = 0.$$

Comme $1/p$ n'est pas dans $\overline{\mathbb{Z}}$, on en déduit qu'il existe $\chi \neq 1$ tel que

$$\frac{1}{p}\chi(1)\chi(g) \notin \overline{\mathbb{Z}}.$$

6. *A group theoretic proof of Bunside's $p^a q^b$ theorem*, Math. Z. (1972).

En particulier, p ne divise par $\chi(1)$, et $\chi(g)$ est non nul. Mais d'autre part, on sait que $\frac{1}{\chi(1)}|\mathrm{Conj}(g)|\,\chi(g)$ est dans $\overline{\mathbb{Z}}$. Comme $\chi(1)$ est premier à $p^n = |\mathrm{Conj}(g)|$, on a

$$\frac{\chi(g)}{\chi(1)} \in \overline{\mathbb{Z}}. \tag{77}$$

En effet, soient $a, b \in \mathbb{Z}$ avec $a\chi(1) + b|\mathrm{Conj}(g)| = 1$ (Bezout). On a alors $\frac{\chi(g)}{\chi(1)} = a\chi(g) + b\frac{1}{\chi(1)}|\mathrm{Conj}(g)|\,\chi(g) \in \overline{\mathbb{Z}}$ par les Propositions 6.5 et 6.6.

Soit $\rho : G \to \mathrm{GL}(V)$ une représentation irréductible de caractère χ. D'après le Lemme 9.3 (et la Proposition 4.8), la relation (77) implique que $\rho(g)$ a toutes ses valeurs propres égales : c'est une homothétie. Comme les homothéties forment un sous-groupe distingué de $\mathrm{GL}(V)$, $H := \rho^{-1}(\mathbb{C}^\times \mathrm{id}_V)$ est un sous-groupe distingué de G contenant g, donc non trivial. Si G est simple, on a $H = G$, *i.e.* $\rho(H) \subset \mathbb{C}^\times \mathrm{id}_V$, puis $\dim V = 1$ par irréductibilité de V. Ainsi χ est un caractère non trivial de degré 1. Si G est simple, le morphisme $\chi : G \to \mathbb{C}^\times$ est injectif, et donc G est abélien, ce qui contredit l'existence d'une classe de conjugaison à > 1 éléments. □

Le théorème de Burnside admet la généralisation suivante, que nous avions simplement énoncé au Chapitre 6 (Théorème 4.4).

Théorème 9.4. (P. Hall) *Soit G un groupe fini. On suppose que pour tout diviseur n de $|G|$ tel que n et $|G|/n$ sont premiers entre eux, G possède un sous-groupe d'ordre n. Alors G est résoluble*

Reformulons l'hypothèse. Notons $\Pi(G)$ l'ensemble des diviseurs premiers distincts de $|G|$, de sorte que l'on a $|G| = \prod_{p\in\Pi(G)} p^{v_p}$. L'hypothèse du Théorème ci-dessus est que pour tout sous ensemble fini $\pi \subset \Pi(G)$, le groupe G possède un sous-groupe d'ordre $\prod_{p\in\pi} p^{v_p}$. Un tel sous-groupe s'appelle un *π-sous groupe (de Hall)*. On a déjà démontré au Chapitre 6 que si G est résoluble, alors il possède des π-sous groupes pour tout $\pi \subset \Pi(G)$, de sorte que le résultat ci-dessus est l'assertion réciproque. Pour $\pi = \{p\}$ un singleton, un π-sous groupe de G est simplement un p-Sylow. On sait qu'ils exisent toujours, par Sylow. Ainsi, si $|\Pi(G)| = 2$, les hypothèses sont automatiquement satisfaites, et dans ce cas la conclusion (G résoluble) est simplement le théorème de Burnside. Noter aussi que dans le cas $|\Pi(G)| = 1$, *i.e.* G est un p-groupe, l'hypothèse est vide, et la conclusion vaut car les p-groupes sont résolubles (Corollaire 1.9 Chap. 6).

Nous suivons la présentation du cours de Serre de la démonstration du théorème de Hall. Nous aurons besoin du lemme suivant :

Lemme 9.5. *Soient G un groupe fini, et A et B deux sous-groupes de G d'indices premiers entre eux. On a $G = AB$ et $[A : A \cap B] = [G : B]$.*

Démonstration — En effet, par Lagrange l'indice $[G : A \cap B]$ est divisible par $[G : A]$ et $[G : B]$, et donc par leur produit $[G : A][G : B]$ sous l'hypothèse de l'énoncé. Regardons l'action naturelle de A par translations à gauche sur G/B. Le stabilisateur de $\{B\} \in G/B$ est $A \cap B$. Mais toujours par Lagrange on a

$$|A/A \cap B| = |A|/|A \cap B| = [G : A \cap B]/[G : A] = |G/B|.$$

Cela démontre d'abord la formule de l'énoncé, et aussi que la A-orbite de $\{B\}$ est tout G/B, *i.e.* $G = AB$. □

Nous aurons aussi besoin du critère suivant de résolubilité.

PROPOSITION 9.6. (Wielandt) *Soit G un groupe fini. On suppose que G possède trois sous-groupes résolubles d'indices 2 à 2 premiers entre eux. Alors G est résoluble.*

DÉMONSTRATION — On raisonne par récurrence sur $|G|$. Soient H_1, H_2, H_3 les trois sous-groupes de l'énoncé. On peut supposer $H_1 \neq \{1\}$, car sinon $H_2 = H_3 = G$ est résoluble. Par un argument déjà vu dans le premier paragraphe de la démonstration du Théorème 4.1 Chap. 6, comme H_1 est résoluble il existe un nombre premier p tel que H_1 possède un sous-groupe abélien p-élementaire non trivial et distingué A. Comme H_2 et H_3 ont des indices premiers entre eux, on peut supposer quitte à les échanger que p ne divise par $[G : H_2]$. Ainsi, H_2 contient un p-Sylow S de G.

Par Sylow, il existe $g \in G$ tel que $g^{-1}Ag \subset S$. Par le Lemme 9.5 on a $G = H_1H_2$. Comme A est distingué dans H_1, tout conjugué de A (par un élément de G) est donc de la forme $h^{-1}Ah$ avec $h \in H_2$. On a vu qu'il existe un tel conjugué dans S, donc dans H_2. Tous les conjugés de A sont donc inclus dans H_2. Soit B le sous-groupe de G engendré par les gAg^{-1} avec $g \in G$. Il est non trivial, distingué dans G, et inclus dans H_2, donc résoluble. Pour des raisons générales, l'image H_i' de H_i dans le groupe quotient G/B est d'indice divisant $[G : H_i]$, et les H_i' sont résolubles. Par récurrence, G/B est résoluble, ainsi donc que G. □

DÉMONSTRATION — (du Théorème de Hall) Pour $p \in \Pi(G)$, appelons *p-complément* de G un π-sous groupe avec $\pi = \Pi(G) \smallsetminus \{p\}$. Démontrons, par récurrence sur $|G|$, que si G possède un p-complément pour tout $p \in \Pi(G)$ alors G est résoluble. Cet énoncé entraîne manifestement le Théorème de Hall. Pour la même raison que ci-dessus, il est clair pour $|\Pi(G)| = 1$, et résulte du théorème de Burnside pour $|\Pi(G)| = 2$.

On suppose donc que $\Pi(G)$ possède au moins 3 éléments distincts p_1, p_2, p_3, et on choisit H_1, H_2 et H_3 des p_i-compléments de G (ils existent par hypothèse). On a en particulier $|H_i| < |G|$ pour tout i. D'après Wieldandt (Prop. 9.6), il suffit de voir que chacun des H_i satisfait l'hypothèse de récurrence. Soient $p \in \Pi(H_i)$ et soit H un p-complément de G. On a $p \neq p_i$ par définition de H_i. Comme $[G : H_i]$ (une puissance de p_i) et $[G : H]$ (une puissance de p) sont premiers entre eux, on a $[H_i : H \cap H_i] = [G : H]$ par le Lemme 9.5, et $H \cap H_i$ est un p-complément de H_i. □

Terminons, comme promis, par une démonstration relativement élémentaire du Lemme 9.3. Il sera commode de dégager d'abord les deux énoncés suivants.

LEMME 9.7. *Soient $x_1, \ldots, x_n$ et $y_1, \ldots, y_m$ dans $\mathbb{C}$. On suppose que les polynômes $\prod_{i=1}^n (X - x_i)$ et $\prod_{j=1}^m (X - y_j)$ sont dans $\mathbb{Q}[X]$. Alors on a aussi*

$$\prod_{1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant m} (X - x_i - y_j) \ \in \ \mathbb{Q}[X].$$

DÉMONSTRATION — Pour tout $P \in \mathbb{Q}[X]$, on a $\prod_{i=1}^n P(X - x_i) \in \mathbb{Q}[X]$. En effet, le polynôme $\prod_{i=1}^n P(X - X_i) \in \mathbb{Q}[X][X_1, \ldots, X_n]$ est symétrique en les X_i, et donc ses coefficients en X sont des polynômes à coefficients rationnels en les polynômes symétriques élémentaires en les X_k. Mais les polynômes symétriques élémentaires en les x_i sont dans $\mathbb{Q}$ par hypothèse. On conclut en posant $P = \prod_{j=1}^m (X - y_j)$. □

Soit $x \in \mathbb{C}$. On dit que x est *algébrique* s'il existe $P \in \mathbb{Q}[X]$ non nul avec $P(x) = 0$, ou autrement si $\mathrm{I}_x := \{P \in \mathbb{Q}[X] \mid P(x) = 0\}$ est $\neq \{0\}$. Observons que I_x est un idéal de $\mathbb{Q}[X]$ (*idéal annulateur de* x), de sorte que s'il est non nul il est principal de la forme (Π_x) pour un unique polynôme unitaire $\Pi_x \in \mathbb{Q}[X]$, appelé *polynôme minimal* du nombre algébrique x. C'est donc aussi le polynôme unitaire de plus petit degré de $\mathbb{Q}[X]$ annulant x.

Lemme 9.8. *Soit $x \in \mathbb{C}$ algébrique. On a $x \in \overline{\mathbb{Z}}$ si, et seulement si, $\Pi_x \in \mathbb{Z}[X]$.*

Démonstration — La condition est trivialement suffisante. Supposons donc $x \in \overline{\mathbb{Z}}$. Par hypothèse, il existe $P \in \mathbb{Z}[X]$ unitaire avec $P(x) = 0$. On a donc $P \in \mathrm{I}_x$, puis $\Pi_x \mid P$ dans $\mathbb{Q}[X]$. En particulier, toute y de Π_x dans $\mathbb{C}$ est racine de P, et donc dans $\overline{\mathbb{Z}}$. Comme $\overline{\mathbb{Z}}$ est un sous-anneau de $\mathbb{C}$ par la Proposition 6.3, on en déduit $\Pi_x \in \overline{\mathbb{Z}}[X]$, et on conclut car on a $\overline{\mathbb{Z}}[X] \cap \mathbb{Q}[X] = \mathbb{Z}[X]$ par la Proposition 6.2. $\square$

Démonstration — (du Lemme 9.3) Choisissons $N \geqslant 1$ assez grand de sorte que l'on ait $\lambda_i^N = 1$ pour tout $1 \leqslant i \leqslant n$. Posons $z = \frac{1}{n}(\lambda_1 + \cdots + \lambda_n)$. Chaque λ_i/n est algébrique, car annulé par $(nX)^N - 1$. Par le Lemme 9.7, le polynôme

$$P(X) = \prod_{\zeta_1, \zeta_2, \ldots, \zeta_n \in \mu_N} (X - \frac{\zeta_1 + \zeta_2 + \cdots + \zeta_n}{n}) \tag{78}$$

est dans $\mathbb{Q}[X]$ et annule z. En particulier, z est algébrique. Comme on a $z \neq 0$ par hypothèse, on a $\Pi_z(0) \neq 0$ sinon Π_z/X serait dans I_z et de degré $< \deg \Pi_z$. Mais comme z est dans $\overline{\mathbb{Z}}$, on a aussi $\Pi_z \in \mathbb{Z}[X]$ d'après le Lemme 9.8, et donc au final

$$\Pi_z(0) \in \mathbb{Z} \smallsetminus \{0\}. \tag{79}$$

On vu $P \in \mathrm{I}_z = (\Pi_z)$ et donc toute racine z' de Π_z dans $\mathbb{C}$ est de la forme $\frac{1}{n}(\sum_{i=1}^n \lambda_i')$ avec les $\lambda_i' \in \mu_N$ pour tout $i = 1, \ldots, n$. Toute racine de Π_z dans $\mathbb{C}$ est donc de module $\leqslant \frac{1+\cdots+1}{n} = 1$. Mais le produit de ces racines est de norme $\geqslant 1$ par (79), de sorte que chacune est de norme 1, et en particulier $|z| = 1$. Le cas d'égalité de l'inégalité triangulaire dans $\mathbb{C}$ implique que les λ_i sont tous positivement proportionnels, et donc égaux car ils sont de même module 1, ce que l'on voulait démontrer. $\square$

10. Exercices

EXERCICE 9.1. *Soient k un corps et G un groupe fini agissant 2-transitivement sur l'ensemble fini X, avec $|G| \in k^\times$. On se propose de décomposer en irréductibles la représentation de permutation de G sur $V = k\,X$. On pose*

$$D = k \sum_{x\in X} \mathrm{e}_x \ \text{ et } \ H = \{\sum_{x\in X} \lambda_x\,\mathrm{e}_x \in k\,X \mid \sum_{x\in X} \lambda_x = 0\}.$$

Ce sont deux sous-modules de V.

(i) Montrer que V possède un unique sous-module D de dimension 1.

(ii) Déterminer, pour tout $x \in X$, le sous-espace des invariants V^{G_x}.

(iii) Montrer que l'entier $|X|(|X|-1)$ est non nul dans k.

(iv) En déduire que H est irréductible.

(v) Conclure.

EXERCICE 9.2. *Soit V un $k[G]$-module semi-simple de dimension 2.*

(i) Montrer que si V est réductible si, et seulement si, $\rho_V(G)$ est un sous-groupe abélien de $\mathrm{GL}(V)$.

(ii) Donner des contre-exemples avec V non semi-simple ou $\dim V > 2$.

EXERCICE 9.3. *Montrer que si G est fini non trivial alors le $k[G]$-module $k\,G$ est monogène, mais pas irréductible.*

EXERCICE 9.4. *Soit G un sous-groupe de $\mathrm{SO}(3)$ et $V = \mathbb{R}^3$ le $\mathbb{R}[G]$-module naturellement associé.*

(i) Montrer que V est réductible si, et seulement si, G est conjugué à un sous-groupe de $\mathrm{O}(2)$ (plongé dans $\mathrm{SO}(3)$ de manière habituelle).

(ii) En déduire que si G est fini, alors V est irréductible si, et seulement si, G est isomorphe à A_4, S_4 ou A_5.

EXERCICE 9.5. *Soit k un corps et G un groupe fini. On se propose de montrer qu'à isomorphisme près, il n'existe qu'un nombre fini de $k[G]$-modules irréductibles.*[7] *On fixe $S_1, \ldots, S_n$ des $k[G]$-modules irréductibles deux à deux non isomorphes, on pose $M = S_1 \oplus \cdots \oplus S_n$, on choisit $v_i \in S_i$ non nul pour tout i et on pose*

$$v = v_1 + \cdots + v_n \in M.$$

(i) Montrer que $k[G]v$ est un sous-module semi-simple de M.

(ii) En considérant les composantes isotypiques de M, montrer $k[G]v = M$.

(iii) Montrer $\dim_k M \leqslant |G|$.

(iv) Conclure.

EXERCICE 9.6. *Soient G un p-groupe fini et $k = \mathbb{Z}/p\mathbb{Z}$. Montrer que toute représentation k-linéaire irréductible de G est de dimension 1 et triviale.*

7. Dans cet exercice, on ne fait pas d'hypothèse sur le corps k.

Exercice 9.7. *Soit V un $k[G]$-module de dimension finie. Montrer que V est irréductible si, et seulement si, son dual $V^\vee$ l'est.*

Exercice 9.8. *Soient k un corps infini, $G = \mathrm{GL}_2(k)$ et $V = k^2$ le $k[G]$-module naturellement associé. On note $\mathrm{Pol}(V)$ la k-algèbre des fonctions polynomiales $f : k^2 \to k$, c'est-à-dire de la forme $(x, y) \mapsto F(x, y)$ avec $F \in k[X, Y]$.*[8] *On considère la représentation k-linéaire de G sur $\mathrm{Pol}(V)$ définie par $(g, f) \mapsto f \circ g^{-1}$. On a donc*

$$(g.f)(x, y) = f(ax + by, cx + dy)$$

pour tout $f \in \mathrm{Pol}(V)$ et $g^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G$. Pour $d \geqslant 0$ entier, on note $\mathrm{Pol}_d(V) \subset \mathrm{Pol}(V)$ le sous-espace des fonctions homogènes de degré d.

(i) Montrer que $\mathrm{Pol}_d(V)$ est un sous-$k[G]$-module de $\mathrm{Pol}(V)$ de dimension $d+1$, et que l'on a une décomposition en somme directe $\mathrm{Pol}(V) = \bigoplus_{d\geqslant 0} \mathrm{Pol}_d(V)$.

On suppose d'abord k de caractéristique nulle et $d \geqslant 0$. On se propose de montrer que $\mathrm{Pol}_d(V)$ est irréductible. On fixe $W \subset \mathrm{Pol}_d(V)$ un sous-module non nul.

(ii) En considérant l'action du sous-groupe de G constitué des matrices diagonales, montrer que si W contient le polynome $\sum_{i=0}^{d} \lambda_i x^i y^{d+1-i}$, et si $\lambda_i \neq 0$, alors W contient le monôme $x^i y^{d+1-i}$.

(iii) En considérant l'action de $\mathrm{U}_2(k) \subset G$, montrer que W contient x^d.

(iv) Conclure.

On suppose enfin k de caractéristique $p > 0$.

(v) Montrer que $\mathrm{Pol}_d(V)$ est irréductible pour $0 \leqslant d < p$.

(vi) Montrer que $\mathrm{Pol}_p(V)$ n'est pas semi-simple.

Exercice 9.9. (Torsion par un automorphisme) *Soient G un groupe, V un $k[G]$-module, et $\phi \in \mathrm{Aut}(G)$.*

(i) Montrer que $(g, v) \mapsto \phi(g).v$ définit une représentation de G sur V. On la note V^ϕ.

(ii) On suppose V de dimension finie. Exprimer χ_{V^ϕ} en fonction de χ_V.

(iii) On suppose ϕ intérieur, montrer $V^\phi \simeq V$.

(iv) (suite) Donner un contre-exemple si ϕ n'est pas intérieur.

Exercice 9.10. *Montrer que si G est fini non trivial alors le $k[G]$-module $k[G]$ est monogène, mais pas irréductible.*

Exercice 9.11. *Soit V un $k[G]$-module semi-simple. Montrer que tout quotient de V est semi-simple.*

---

8. Comme k est infini, on sait que l'application naturelle $k[X, Y] \to \mathrm{Pol}(V)$, $F \mapsto ((x, y) \mapsto F(x, y))$, est bijective.

Exercice 9.12. (Socle d'un $k[G]$-module) *Soit V un $k[G]$-module (que l'on pourra supposer de dimension finie). Notons* $\operatorname{Soc} V \subset V$ *la somme de tous les sous-modules irréductibles de V (socle de V).*

(i) Montrer que $\operatorname{Soc} V$ *est le plus grand sous-module semisimple de V.*

(ii) On suppose $G = \mathrm{S}_n$ et que $V = k^n$ est la représentation de permutation associée à l'action standard de G sur $\{1, \ldots, n\}$. Déterminer $\operatorname{Soc} V$.

Soit A un anneau et M un A-module. On dit que M est simple on a $M \neq \{0\}$ et si les seuls sous-modules de M sont $\{0\}$ et M.

Exercice 9.13. *(Lemme de Schur, version 2) Montrer que si M est un A-module simple, alors l'anneau* $\operatorname{End}_A(M)$ *des endomorphismes A-linéaires de M est un anneau à division.*

Exercice 9.14. *Soit M un A-module de type fini non nul.*

(i) Montrer que M possède un sous-module $N \subsetneq M$ maximal pour l'inclusion.

(ii) Montrer que M possède admet quotient qui est un A-module simple.

Un A-module M est dit semi-simple si on peut écrire $M = \oplus_{i \in I} M_i$ où les M_i, avec $i \in I$, sont des sous-modules simples de M.

Exercice 9.15. *(Modules semisimples) Soient A un anneau et M un A-module. Monter l'équivalence entre :*

(a) M est semi-simple.

(b) M est somme de sous-modules simples.

(c) Pour tout sous-module N de M, il existe un sous-module N' de M tel que $M = N \oplus N'$.

(d) Tout sous-module de M est semisimple.

Un $\mathbb{C}[G]$-module V est dit *fidèle* si la représentation associée $\rho_V : G \to \mathrm{GL}(V)$ est injective, autrement dit si l'action de G sur V associée est fidèle.

Exercice 9.16. *Soient G un groupe fini, V un $\mathbb{C}[G]$-module de dimension finie et $\rho_V : G \to \mathrm{GL}(V)$ le morphisme associé.*

(i) Montrer que pour $g \in G$, on a $\chi_V(g) = \dim V \iff \rho_V(g) = \mathrm{id}_V$. En déduire que $\{g \in G \ \chi_V(g) = \chi(1)\}$ est un sous-groupe distingué de G.

(ii) Montrer que V est fidèle $\iff$ on a $\chi_V(g) \neq \chi_V(1)$ pour tout $g \neq 1$.

(iii) Réciproquement, montrer que pour tout sous-groupe distingué N de G, il existe un caractère χ de G avec $N = \{g \in G \mid \chi(g) = \chi(1)\}$.

Exercice 9.17. *Soient G un groupe fini, ainsi que U et V deux $\mathbb{C}[G]$-modules de dimension finie. On suppose V fidèle et U irréductible, et on s'intéresse à la suite des entiers $\langle \chi_U, \chi_V^n \rangle$ avec $n \geqslant 0$. On note $Z \subset G$ le sous-groupe des éléments $z \in G$ tels que z agit par une homothétie sur V, dont on notera $\omega_V(z)$ le rapport.*

(i) Montrer $Z \subset \mathrm{Z}(G)$ et que $\omega_V : Z \to \mathbb{C}^\times$ est un morphisme de groupes.

(ii) Montrer qu'il existe un morphisme de groupes $\omega_U : Z \to \mathbb{C}^\times$ *tel que tout* $z \in Z$ *agit dans* U *comme l'homothétie de rapport* $\omega_U(z)$.

(iii) Soit $n \in \mathbb{N}$ *tel que* $\omega_V^n \neq \omega_U$. *Montrer* $\langle \chi_U, \chi_V^n \rangle = 0$.

On pose $N = \{n \in \mathbb{Z} \mid \omega_V^n = \omega_U\}$ *et on suppose désormais qu'il n'est pas vide. On considère la série formelle* $f = \sum_{n \geqslant 0} \langle \chi_U, \chi_V^n \rangle z^n \in \mathbb{C}[[z]]$.

(iv) Montrer que N *est de la forme* $n_0 + m\mathbb{Z}$ *pour certains* $n_0, m \in \mathbb{Z}$.

(v) Montrer la formule $f = \frac{1}{|G|} \sum_{g \in G} \frac{\chi_U(g)}{1 - \chi_V(g) z}$.

(vi) En déduire qu'il existe un réel $0 < r < \dim V$ *tel que pour* $n \in N \cap \mathbb{N}$ *on ait*

$$\langle \chi_U, \chi_V^n \rangle = (\dim V)^n \frac{|Z|}{|G|} \dim U + \mathrm{O}(r^n), \quad n \to +\infty.$$

Exercice 9.18. *Soit* G *un groupe fini.*

(i) On fait agit G *sur* G *par conjugaison et on note* V *la représentation de permutation associée. Déterminer* χ_V.

(ii) En déduire que la somme de chaque ligne de la table des caractères de G *est un entier* $\geqslant 0$.

Exercice 9.19. *Déterminer la table des caractères de* H_8.

Exercice 9.20. *Déterminer la table des caractères de* D_8.

Exercice 9.21. *Soit* $n \geqslant 3$ *un entier. On se propose de déterminer la table des caractères de* D_{2n}.

(i) Montrer que D_{2n} *a* 2 *ou* 4 *caractères de degré* 1, *selon la parité de* n, *et les déterminer.*

(ii) Montrer que pour $\zeta \in \mu_n$, *il existe un unique représentation* $\rho_\zeta : \mathrm{D}_{2n} \to \mathrm{GL}_2(\mathbb{C})$ *vérifiant* $\rho_\zeta(c) = \begin{bmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{bmatrix}$ *et* $\rho_\zeta(\tau) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.

(ii) Montrer $\rho_\zeta \simeq \rho_\mu$ *si, et seulement si,* $\zeta = \mu$ *ou* $\zeta = \mu^{-1}$.

(iii) À quelle condition sur ζ *la représentation* ρ_ζ *est-elle irréductible ?*

(vii) Conclure.

L'exercice suivant fait référence au Problème 1 de l'examen partiel 2021 (Appendice B).

Exercice 9.22. *Soient* X, Y, Z *"les" trois* S_4*-ensembles transitifs à* 6*-éléments deux à deux non isomorphes. En utilisant la table des caractères de* S_4, *décomposer en irréductibles les représentations de permutation* $\mathbb{C}X$, $\mathbb{C}Y$ *et* $\mathbb{C}Z$.

Exercice 9.23. *Soit* G *un groupe fini. Montrer l'équivalence entre :*

(a) Tout élément g *de* G *est conjugué à* g^{-1}.

(b) Tout caractère de G *est à valeurs réelles.*

EXERCICE 9.24. *(Burnside) Soit G un groupe d'ordre impair. Montrer que le seul caractère irréductible à valeurs réelles de G est le caractère trivial.*

EXERCICE 9.25. (Caractères de degré 1) *Soit G un groupe fini d'abélianisé $G_{\mathrm{ab}} = G/\mathrm{D}(G)$. Montrer que les caractères de degré 1 de G sont exactement les $|G_{\mathrm{ab}}|$-morphismes $\chi \circ \pi$ avec $\chi \in \widehat{G_{\mathrm{ab}}}$ et $\pi : G \to G_{\mathrm{ab}}$ la projection canonique.*

EXERCICE 9.26. (Torsion par un caractère de degré 1) *Soit $\rho : G \to \mathrm{GL}(V)$ une représentation $\mathbb{C}$-linéaire de dimension finie de G sur V et $\eta \in \widehat{G}$.*

(i) Vérifier $\rho_\eta(g) := \eta(g)\rho(g)$ est une autre représentation $\mathbb{C}$-linéaire de G sur V.

(ii) Montrer que ρ_η est irréductible si, et seulement si, ρ l'est.

(iii) Déterminer le caractère de ρ_η et retrouver le (ii).

(iv) Donner un exemple avec $\eta \neq 1$ et ρ_η isomorphe à ρ, et un autre avec ρ_η non isomorphe à ρ.

EXERCICE 9.27. (Restriction de représentations) *Soit $\rho : G \to \mathrm{GL}(V)$ une représentation $\mathbb{C}$-linéaire de G sur V, et $f : G' \to G$ un morphisme de groupes.*

(i) Vérifier que $\rho' := \rho \circ f$ est une représentation $\mathbb{C}$-linéaire de H sur V, dite restriction à G' de ρ (via f).

(ii) On supposer (V, ρ) irréductible et f surjective. Montrer que (V, ρ') est irréductible.

(iii) Déterminer $\chi_{\rho'}$ en fonction de χ_ρ.

EXERCICE 9.28. *Déterminer les tables des caractères de $\widetilde{\mathrm{A}_4}$, $\widetilde{\mathrm{S}_4}$ et $\widetilde{\mathrm{A}_5}$.*

EXERCICE 9.29. *Soient G un groupe fini et H un sous-groupe de G d'indice n.*

(i) Montrer que la représentation régulière $\mathbb{C}G$ de G, restreinte à H, est isomorphe à $(\mathbb{C}H)^{\oplus n}$.

(ii) Soit $f : \mathbb{C}[X_G] \to \mathbb{C}[X_H]$ le morphisme de $\mathbb{C}$-algèbres envoyant X_g sur 0 pour $g \notin H$. Montrer $f(\det G) = (\det H)^n$.

EXERCICE 9.30. *Factoriser* $\det \mathrm{H}_8$ *en irréductibles dans* $\mathbb{C}[X_{\mathrm{H}_8}]$.

EXERCICE 9.31. *Soit G un groupe fini et p un nombre premier.*

(i) Montrer $\det G \in \mathbb{Z}[\mathrm{X}_G]$.

(ii) On suppose que G est un p-groupe. Montrer $\det G \equiv (\sum_{g \in G} X_g)^{|G|} \bmod p\mathbb{Z}[\mathrm{X}_G]$.

EXERCICE 9.32. (Irréductibilité du déterminant) *Soit A un anneau commutatif intègre.*

(i) Soit $\pi \in A$ irréductible. Montrer que π est irréductible dans $A[X]$.

(ii) Soient $n \geqslant 2$ et $f_1, \ldots, f_n$ des éléments de A premiers entre eux. Montrer que $f_1X_1 + f_2X_2 + \cdots + f_nX_n$ est irréductible dans $A[X_1, \ldots, X_n]$.

(iii) En déduire que $\det(X_{i,j})_{1\leqslant i,j\leqslant n}$ est irréductible dans $\mathbb{C}[\{X_{i,j} \mid 1 \leqslant i, j \leqslant n\}]$.

Exercice 9.33. (Lois bilinéaires définies sur une base) *Soient k un corps, V un k-espace vectoriel et $\{e_i\}_{i\in I}$ une base de V. Une loi de composition $f : V \times V \to V$ qui est dite k-bilinéaire, si pour tout $x \in V$, les applications $V \to V$, $v \mapsto f(v, x)$ et $v \mapsto f(x, v)$, sont k-linéaires.*

(i) Fixons, pour tout $(i, j) \in I \times I$, un élément $v_{i,j}$ de V. Montrer qu'il existe une et une seule loi de composition k-bilinéaire $f : V \times V \to V$ telle que $f(e_i, e_j) = v_{i,j}$ pour tous $i, j \in I$.

On fixe désormais une loi de composition $f : V \times V \to V$ qui est k-bilinéaire.

(ii) Montrer que f est commutative si, et seulement si, on a $f(e_i, e_j) = f(e_j, e_i)$ pour tout $i, j \in I$.

(iii) Montrer que $e \in V$ est un élément neutre de f si, et seulement si, on a $f(e, e_i) = f(e_i, e) = e$ pour tout $i \in I$.

(iv) Montrer que f est associative si, et seulement si, on a

$$f(f(e_i, e_j), e_k) = f(e_i, f(e_j, e_k)), \quad \forall i, j, k \in I.$$

Annexe A

Corrections des exercices

Exercices du chapitre 1

Exercice 1.1. L'ensemble $\mathscr{E}$ des relations d'équivalence sur X est un sous-ensemble de $\mathrm{P}(X \times X)$. Il est stable par intersections quelconques. Pour le (i), définir R' comme l'intersection des éléments de $\mathscr{E}$ contenant R. Pour le (ii), vérifier que la relation donnée est d'équivalence, contient R, et est incluse dans toute relation d'équivalence contenant R.

Exercice 1.2. (i) On suppose $f^{p^m} = \mathrm{id}_X$. Soit $x \in X$ et $d = |[x]|$. Il suffit de montrer $d = p^k$ avec $0 \leqslant k \leqslant m$. D'après le cours, on sait que d est le plus petit entier $\geqslant 1$ vérifiant $f^d(x) = x$. Le pgcd de d et p^m est de la forme p^k pour un certain $0 \leqslant k \leqslant m$. On a donc $a, b \in \mathbb{Z}$ avec $ad + bp^m = p^k$ par Bezout, puis $f^{ad} = f^{p^k}$ et donc $f^{p^k}(x) = x$ puis $d = p^k$ par minimalité de d.

(ii) On peut avoir $|X| = p + p^m$ avec un cycle de longueur p et un autre de longueur p^m ; le nombre de points fixes est 0, mais il n'est pas congru à $|X| \bmod p^m$ si $m > 1$.

Exercice 1.3. (i) Soit X l'ensemble des partitions de $I = \{1, \ldots, n\} \coprod \mathbb{Z}/p\mathbb{Z}$. Soit f l'application de l'énoncé. C'est une bijection de I, mais elle induit aussi une bijection F de X, envoyant $I = \coprod_i I_i$ sur $I = \coprod_i f(I_i)$. On a $f^p = \mathrm{id}_I$ et $F^p = \mathrm{id}_X$. On a donc $\mathrm{B}_{n+p} = |X| \equiv |\mathrm{Fix}\, X| \bmod p$. Soit I une partition fixe par F, et I_0 la partie de I contenant $0 \in \mathbb{Z}/p\mathbb{Z}$. On va d'abord montrer que l'on a soit $I_0 \supset \mathbb{Z}/p\mathbb{Z}$, soit $I_0 = \{0\}$. En effet, deux parties de la forme $I_j := f^j(I_0)$ avec $j \in \mathbb{Z}$ sont soit égales soit disjointes par hypothèse. Ainsi, si I_0 rencontre $\{1, \ldots, n\}$, donc contient un point fixe de f, on a nécessairement $f(I_0) = I_0$ et donc $I_0 \supset \mathbb{Z}/p\mathbb{Z}$. Sinon, on a $I_0 \subset \mathbb{Z}/p\mathbb{Z}$ et donc les parties de la forme I_j forment une partition de $\mathbb{Z}/p\mathbb{Z}$ en sous-ensembles de même cardinal $|I_0|$. Le nombre n de ces parties distinctes vérifie donc $n|I_0| = p$, ce qui force $|I_0| = 1$ ou p, *i.e.* $I_0 = \{0\}$ ou $I_0 = \mathbb{Z}/p\mathbb{Z}$. Au final, F a deux types de points fixes dans X : (a) les partitions telles que la partie contenant 0 contient tout $\mathbb{Z}/p\mathbb{Z}$: il y a trivialement B_{n+1} telles partitions (on identifie $\mathbb{Z}/p\mathbb{Z}$ à un point !), (b) les partitions de la forme $P \coprod \coprod_{x \in \mathbb{Z}/p\mathbb{Z}} \{x\}$ avec P une partition de $\{1, \ldots, n\}$: il y en a B_n.

(ii) On procède de la même manière en considérant $I = \{1, \ldots, n\} \coprod \mathbb{Z}/p^m\mathbb{Z}$ et la bijection qui vaut identité sur $\{1, \ldots, n\}$ et $x \mapsto x + 1$ sur $\mathbb{Z}/p^m\mathbb{Z}$. On observera d'abord qu'il existe exactement $m + 1$ partitions de $\mathbb{Z}/p^m\mathbb{Z}$ invariantes par $x \mapsto x + 1$, à savoir les partitions dont l'une des parties est $p^i\mathbb{Z}/p^m\mathbb{Z}$ pour $0 \leqslant i \leqslant m$ (et les autres sont les $x + p^i\mathbb{Z}/p^m\mathbb{Z}$ avec $x = 0, \ldots, p^i - 1$). On appliquera l'Exercice 1.2.

Exercice 1.5. (i) Soit $E \subset \mathbb{Q}$ non vide. Notons q_E le plus petit entier $q \geqslant 1$ tel qu'il existe un élément de E de la forme p/q avec $p \in \mathbb{Z}$. Parmi les éléments de E de la forme p/q_E avec $p \in \mathbb{Z}$, il existe un unique élément $e \in E$ avec $|e|$ minimal, et avec $e \geqslant 0$ dans le cas $\pm e \in E$. On pose $\tau(E) = e$. On a $\tau(E) \in E$, de sorte que τ est une fonction de choix sur $\mathbb{Q}$. Considérons maintenant le cas de $\mathbb{Q}^2$. On fixe τ une fonction de choix sur $\mathbb{Q}$, par exemple celle construite ci-dessus. Soit $E \subset \mathbb{Q}^2$ non vide. Soit E' son image dans $\mathbb{Q}$ par $\mathbb{Q}^2 \to \mathbb{Q}, (x, y) \mapsto x$. Soit $E'' \subset \mathbb{Q}$ l'unique partie telle que $E \cap (\tau(E') \times \mathbb{Q}) = \tau(E') \times E''$. Alors $E \mapsto (\tau(E'), \tau(E''))$ est une fonction de choix sur $\mathbb{Q}^2$.

(ii) Soit τ une fonction de choix sur $\mathbb{Q}^2$. Si U est un ouvert non vide de $\mathbb{R}^2$, alors $U \cap \mathbb{Q}^2$ est non vide par densité de $\mathbb{Q}^2$ dans $\mathbb{R}^2$, et on a $\tau(U \cap \mathbb{Q}^2) \in U$. Ainsi, $U \mapsto \tau(U \cap \mathbb{Q}^2)$ convient.

Considérons le (iii). Soit F est un fermé non vide de $\mathbb{C}$. Si $0 \in F$ on pose $\tau(F) = 0$. Sinon, un argument de compacité montre qu'il existe un plus petit réel $r_F > 0$ tel que F contienne un élément de module r_F. Un autre argument de compacité montre qu'il existe un plus petit réel $\theta_F \in [0, 2\pi]$ tel que $r_F e^{i\theta_F} \in F$. Alors $\tau(F) = r_F e^{i\theta_F}$ est dans F.

Supposons enfin donnée une fonction de choix τ sur les parties dénombrables non vides de $\mathbb{R}$ (plutôt que de $\mathbb{R}^2$, pour simplifier). Soit $\sim$ la relation d'équivalence de Vitali sur $\mathbb{R}$: $x \sim y$ si, et seulement si, $x - y \in \mathbb{Q}$. Ses classes d'équivalence sont dénombrables et denses dans $\mathbb{R}$. La fonction τ permet donc de définir l'ensemble $V = \{\tau(C \cap [0,1]) \,|\, C \in \mathbb{R}/\sim\} \subset [0,1]$ (*ensemble de Vitali*). Rappelons, suivant Vitali, pourquoi V n'est pas Lebesgue-mesurable. On a $[0,1] \subset \coprod_{x \in [-1,1] \cap \mathbb{Q}} (x + V) \subset [-1, 2]$, la réunion du milieu étant dénombrable et disjointe. Si V était mesurable, il serait de mesure nulle par la seconde inclusion, ce qui contredirait la première. Ainsi, d'après l'énoncé admis de Solovay, l'axiome du choix est nécessaire pour définir τ.

Exercice 1.6. Pour le (i), s'il existe $x \in X$ avec $d(x, a) \geqslant \epsilon$ pour tout $a \in A$, alors $A \cup \{x\}$ serait ϵ-séparée, et contenant strictement A, contredisant la maximalité de A. Pour le (ii), soit A une partie ϵ-séparée de X. Soit $\mathscr{B}$ l'ensemble des parties ϵ-séparées de X contenant A, ordonné par l'inclusion. Vérifions qu'il est inductif. Si $\{B_i\}$ est une famille totalement ordonnée d'éléments de $\mathscr{A}$ alors on constate $B = \cup_i B_i \in \mathscr{B}$. En effet, deux éléments distincts b, b' de B sont dans un même B_i, et vérifient donc $d(b, b') \geqslant \epsilon$. On a bien sur $A \subset B_i \subset B$ pour tout i. On conclut par Zorn.

Exercice 1.7. Le (i) est une vérification immédiate. Pour le (ii), si $A \subset X \times Y$ est non vide, un élément (x, y) de A d'abscisse x minimale (existe car X bien ordonné), et de coordonnée y minimale telle que $(x, y) \in A$ (existe car $\{x\} \times Y$ est bien ordonné), convient. Pour le (iii), considérons l'ensemble lexicographiquement ordonné $\mathbb{N} \times \{0, 1\}$. On a $(0,0) < (0,1) < (1,0) < (1,1) < (2,0) < (2,1) < \cdots$. On constate qu'il est isomorphe à $\mathbb{N}$ via $(n, e) \mapsto 2n + e$. En revanche, $\{0,1\} \times \mathbb{N}$ n'est pas isomorphe à $\mathbb{N}$, car la suite des $(0, n)$ y est strictement croissante, et majorée par $(1, 0)$.

Exercice 1.8. (i) S'il existe une injection $j : A \to B$, alors j induit une bijection entre A et $A' = j(A) \subset B$. Quitte à remplacer A par A', on peut donc supposer $A \subset B$. Pour le (ii), écrivons $B = A \coprod C$. Supposons qu'il existe $x, y \in C$, et $m \geqslant n \geqslant 0$, avec $i^m(x) = i^n(y)$. On a $i^n(i^{m-n}(x)) = i^n(y)$, puis $i^{m-n}(x) = y$ car i^n est injective. Si $m - n > 0$ on a $i^{m-n}(x) \subset i(B) \subset A$, contredisant $y \in C = B \smallsetminus A$. On a donc $m = n$, puis $x = y$. Le (iii) est évident.

Exercice 1.9. (i) Si f admet une rétraction $r : Y \to X$, la relation $r \circ f = \mathrm{id}_X$ montre que f est injective et r est surjective. Supposons réciproquement f injective. Fixons $x_0 \in X$. Pour $y \in Y$, on pose $r(y) = x_0$ si $y \notin f(X)$, et si $y \in f(X)$ on définit $r(y)$ comme étant l'unique élément $x \in X$ tel que $f(x) = y$. On a clairement $r \circ f = \mathrm{id}_X$.

(ii) Si on a une injection $f : A \to B$, toute rétraction r de f est une surjection $B \to A$. Si on a une surjection $f : A \to B$, toute section s de f (donnée par AC) est une injection $A \to B$ (car f est une retraction de s !).

Exercice 1.10. (i) Il faut voir qu'une partie infinie $A \subset \mathbb{N}$ est en bijection avec $\mathbb{N}$. On définit pour cela par récurrence une suite $\{a_n\}_{n \geqslant 0}$ d'éléments de A, et $A_n = \{a_0, \ldots, a_n\} \subset A$, en posant $a_0 = \min(A)$ et $a_n = \min A \smallsetminus A_{n-1}$. La suite a_n est strictement croissante et on a $A \cap \{0, \ldots, n\} \subset A_n$: l'application $n \mapsto a_n, \mathbb{N} \to A$, est bijective.

Pour le (ii), si $\mathbb{N}$ se surjecte sur A et A se surjecte sur B alors $\mathbb{N}$ se surjecte sur B. Pour le (iii), il suffit de voir par (ii) que $\mathbb{N} \times \mathbb{N}$ est dénombrable. Mais $(a, b) \mapsto 2^a 3^b$ est une injection de $\mathbb{N} \times \mathbb{N}$ dans $\mathbb{N}$. Pour le (iv), on choisit une surjection $\varphi_n : \mathbb{N} \to A_n$. Alors $\mathbb{N} \times \mathbb{N} \to \cup_n A_n, (m, n) \mapsto \varphi_n(m)$, est surjective.

Exercice 1.11. (i) On a clairement $[0, 1] \hookrightarrow \mathbb{R}$ et aussi $\mathbb{R} \hookrightarrow [0, 1]$ (considérer par exemple $\frac{1}{2} + \frac{1}{\pi}\arctan$), donc $\mathbb{R} \sim [0, 1]$ par Cantor-Bernstein. De plus $\{0, 1\}^{\mathbb{N}}$ s'injecte dans $[0, 1[$ par $(\epsilon_i) \mapsto \sum_{i=0}^{\infty} \frac{\epsilon_i}{3^i}$. Enfin, $\{0, 1\}^{\mathbb{N}}$ se surjecte sur $[0, 1[$ par $(\epsilon_i) \mapsto \sum_{i=0}^{\infty} \frac{\epsilon_i}{2^i}$. On a donc $\{0, 1\}^{\mathbb{N}} \sim [0, 1[$ par Cantor-Bernstein. On a bien sûr $[0, 1[\sim [0, 1]$ car $\mathbb{N} \sim \mathbb{N} \smallsetminus \{0\}$ et $\mathbb{N} \hookrightarrow [0, 1]$.

Pour le (ii), on observe que si $\{e_n\}_{n \geqslant 0}$ est une suite d'éléments de $\{0, 1\}^{\mathbb{N}}$, alors la suite $f = (f_n)$ définie par $f_n = 1 - (e_n)_n$ est dans $\{0, 1\}^{\mathbb{N}}$, mais est distincte de tous les e_n. Pour le (iii), on a vu $\mathbb{R} \sim \{0, 1\}^{\mathbb{N}}$ et $\mathbb{N} \sim \mathbb{N} \times \mathbb{N}$, donc $\mathbb{R} \sim \{0, 1\}^{\mathbb{N} \times \mathbb{N}} \sim\sim (\{0, 1\}^{\mathbb{N}})^{\mathbb{N}}$. Mais il est clair que l'on a $\{0, 1\}^{\mathbb{N}} \hookrightarrow \mathbb{N}^{\mathbb{N}}$ et $\mathbb{N} \hookrightarrow \mathbb{R} \sim \{0, 1\}^{\mathbb{N}}$, d'où $\mathbb{R} \sim \mathbb{N}^{\mathbb{N}}$.

Exercice 1.12. Pour le (i), on regarde l'ensemble $\mathscr{E}$ des couples (B, P) avec $B \subset A$ et $P \subset \mathrm{P}(B)$ une partition de B en sous-ensembles infinis dénombrables. On ordonne $\mathscr{E}$ par $(B, P) \leqslant (C, Q)$ si et seulement si on a $B \subset C$ et $P \subset Q$ (en particulier, B est réunion de parties dans Q). Cet ordre est (trivialement !) inductif. Détaillons tout de même l'argument. Soit (B_i, P_i) une partie totalement ordonnée de $\mathscr{E}$. On pose $B = \cup_i B_i$ et $P = \cup_i P_i$. Vérifions que l'on a $(B, P) \in \mathscr{E}$. On a $B_i = \coprod_{E \in P_i} E$ et donc $B = \cup_{E \in P} E$. Soient E, F distincts dans P, disons $E \in P_i$ et $F \in P_j$. Comme (B_i, P_i) est totalement ordonnée, on peut supposer $(B_i, P_i) \leqslant (B_j, P_j)$. En particulier, on a E, F dans P_j, et donc $E \cap F = \varnothing$, ce qui conclut.

Par Zorn, il existe (B, P) maximal dans $(\mathscr{E}, \leqslant)$. Regardons $A \smallsetminus B$. S'il est infini, alors il existe une partie $C \subset A \smallsetminus B$ avec $C \sim \mathbb{N}$. Mézalor on a $B' = B \coprod C \subset A$, et $P' = P \cup \{C\}$ est une partition de B' vérifiant $(B, P) \leqslant (B', C')$. C'est absurde par maximalité. On en déduit que $F := A \smallsetminus B$ est fini. Mais comme A est infini, B est infini et on peut l'écrire $B = E \coprod B''$ pour un certain $E \sim \mathbb{N}$ appartenant à P. On a alors $A = (E \coprod F) \coprod B'$, $E \coprod F \sim \mathbb{N}$, et B' est réunion disjointe de parties infinies dénombrables, à savoir les $E' \in P'$ tels que $E' \neq E$. Cela prouve le (i).

Montrons le (ii). Par le (i) on peut écrire $A = \coprod_{i \in I} A_i$ avec $A_i \sim \mathbb{N}$ pour tout $\in I$. Soit $\varphi_i : \mathbb{N} \to A_i$ une bijection. L'application $I \times \mathbb{N} \to A, (i, n) \mapsto \varphi_i(n)$ est donc bijective. On a montré $A \sim I \times \mathbb{N}$. On a alors $A \times \mathbb{N} \sim (I \times \mathbb{N}) \times \mathbb{N} \sim I \times (\mathbb{N} \times \mathbb{N}) \sim I \times \mathbb{N} \sim A$. Pour $n \geqslant 1$, on a aussi les injections $A \hookrightarrow A \times \{1, \ldots, n\} \hookrightarrow A \times \mathbb{N} \sim A$, et donc $A \sim A \times \{1, \ldots, n\}$.

Exercice 1.13. On note $\mathscr{E}$ l'ensemble de l'énoncé. On l'ordonne par $(X, f) \leqslant (Y, g)$ si, et seulement si, on a $X \subset Y$ et $g_{|X} = f$. L'ensemble ordonné $(\mathscr{E}, \leqslant)$ est inductif. En effet, si $\{(X_i, f_i)\}$ en est une famille totalement ordonnée, l'ensemble $X := \cup_i X_i$, et l'application $f : X \to B$ (bien) définie par $f(x) = f_i(x)$ pour $x \in X_i$, vérifie $(X, f) \in \mathscr{E}$ et $(X_i, f_i) \leqslant (X, f)$ pour tout i. Par Zorn, on peut donc considérer $(X, f) \in \mathscr{E}$ maximal. Par construction, on a $X \subset A$ et $f : X \hookrightarrow B$. Si on a $X = A$ ou $f(X) = B$, on a respectivement $A \hookrightarrow B$ ou $B \hookrightarrow A$, et on a gagné. C'est toujours le cas. En effet, s'il existe $a \in A \smallsetminus X$ et $b \in B \smallsetminus f(X)$, on peut considérer $X' = X \cup \{a\}$ et définir $f' : X' \to B$ par $f'(x') = f(x)$ pour $x \in X$, et $f(a) = b$. On a clairement $(X', f') \in \mathscr{E}$ et $(X, f) \leqslant (X', f')$, contredisant la maximalité de (X, f).

Exercice 1.14. Par hypothèse on a $A \twoheadrightarrow B$. Comme $X = A \cup B$ est infini, A l'est aussi. Mais par l'Exercice 1.12 on a $A \sim A \times \{1, 2\} \sim A \coprod A \twoheadrightarrow A \cup A = X$, et clairement $A \hookrightarrow X$, donc $A \sim X$.

Exercice 1.15. (i) On a $Y \times Y = (X \times X) \coprod Z$ avec $Z = (X \times X') \coprod (X' \times X) \coprod (X' \times X')$. Il suffit donc de montrer $X' \sim Z$. Mais on a $X' \sim X$ et $X \times X \sim X$ par hypothèse, et donc $Z \sim X \times X \times \{1,2,3\} \sim X \times \{1,2,3\} \sim X \sim X'$ par l'Exercice 1.12.

Pour le (ii), notons $\mathscr{E}$ l'ensemble des couples (A, f) en question. On l'ordonne par $(A, f) \leqslant (B, g)$ si, et seulement si, $A \subset B$, $g(A \times A) \subset A$ et $g_{|A \times A} = f$. On vérifie immédiatement que $(\mathscr{E}, \leqslant)$ est inductif. Soit (A, f) un élément maximal. On a en particulier $A \sim A \times A$. Écrivons $X = A \coprod C$. Si on a $C \hookrightarrow A$, on a vu à l'exercice précédent que l'on a $X \sim A$, et donc $X \times X \sim A \times A \sim A \sim X$. Sinon, on a $A \hookrightarrow C$, et donc $A' \subset X \smallsetminus A$ avec $A' \sim A$. Mais le (i) montre que l'on peut trouver $(A \coprod A', g)$ dans $\mathscr{E}$ avec $(A, f) \leqslant (A \coprod A', g)$ une contradiction car $A \subsetneq A \coprod A'$.

Exercice 1.16. Pour $n \geqslant 1$ entier, notons $\mathrm{P}(X)_n \subset \mathrm{P}(X)$ l'ensemble des parties non vides à $\leqslant n$ éléments de X. On a $\mathrm{P}(X)_m \subset \mathrm{P}(X)_n$ pour $m \leqslant n$, et une bijection $X \hookrightarrow \mathrm{P}(X)_1, x \mapsto \{x\}$. On a donc $X \hookrightarrow \mathrm{P}_f(X)$, et par Cantor-Bernstein il s'agit de montrer que l'on a $\mathrm{P}_f(X) \hookrightarrow X$. Comme X est infini, l'ensemble $\mathrm{P}'_f(X) = \mathrm{P}_f(X) \smallsetminus \{\varnothing\}$ des parties finies non vides de X vérifie $\mathrm{P}'_f(X) \sim \mathrm{P}_f(X)$, il suffit donc de montrer $X \twoheadrightarrow \mathrm{P}'_f(X)$.

Pour $n \geqslant 1$, l'application $X^n \to \mathrm{P}(X)_n, (x_1, \ldots, x_n) \mapsto \{x_1, \ldots, x_n\}$, est surjective. On a donc une surjection $X \sim X^n \twoheadrightarrow \mathrm{P}(X)_n$ par l'Exercice 1.15. Notons la f_n. On aussi $\mathrm{P}'_f(X) = \cup_{n \geqslant 1} \mathrm{P}(X)_n$, et donc une surjection $X \times \mathbb{N} \twoheadrightarrow \mathrm{P}'_f(X)$, $(x, n) \mapsto f_n(x)$. Mais on a vu $X \times \mathbb{N} \sim X$ à l'Exercice 1.12, ce qui conclut.

Exercice 1.17 . (i) Soient $j \in J$ et V_j le sous-espace vectoriel de V engendré par les f_i avec $i \neq j$. On a $j \notin J_i$ si et seulement si $e_i \in V_j$, car f est une base. Ainsi, si j n'est dans aucun J_i, $i \in I$, on a $e_i \in V_j$ pour tout i, et donc $V = V_j$ car e est génératrice. Mais f étant une base, on a aussi $f_j \notin V_j$: une contradiction. Pour le (ii), on constate que comme J_i est fini, on a une surjection $\varphi_i : \mathbb{N} \to J_i$, puis une surjection $\mathbb{N} \times I \to J, (n, i) \mapsto \varphi_i(n)$. Si I est infini, on a vu $\mathbb{N} \times I \sim I$, et donc $I \twoheadrightarrow J$, puis $J \hookrightarrow I$. Si I est fini, alors V est de dimension finie et on sait $I \sim J$. Pour le (iii), on a $I \hookrightarrow J$ et $J \hookrightarrow I$ par symétrie, et donc $I \sim J$ par Cantor-Bernstein.

Exercice 1.18. On a $V \sim k^{(I)}$ comme e est une base. Posons $W = k^{(I)}$. Pour $n \geqslant 1$, notons $\mathscr{I}_n$ l'ensemble des parties à $\leqslant n$ éléments de I. On note aussi $W_n \subset W$ le sous-ensemble des éléments (x_i) tels que $x_i = 0$ pour tout i sauf au plus n d'entre eux. On a $W = \cup_{n \geqslant 1} W_n$. Noter que l'application $k^\times \times I \to k^{(I)}, (x, i) \mapsto (0, .., 0, x, 0, ...)$, le x étant à la place i, est une bijection $k^\times \times I \twoheadrightarrow W_1 \smallsetminus \{0\}$. On a donc $W_1 \sim W_1 \smallsetminus \{0\} \sim k^\times \times I$. Mais comme $\{0, 1\} \times I \sim I$, on a aussi $k^\times \times I \sim k \times I$. On a donc montré $W_1 \sim k \times I$. Il suffit donc de montrer $W_n \sim k \times I$ pour tout $n \geqslant 1$. En effet, on aura alors

$$k \times I \sim W_1 \hookrightarrow W \hookrightarrow k \times I \times \mathbb{N} \sim k \times I,$$

puis $W \sim k \times I$ (Exercice 1.12 et Cantor-Bernstein). Fixons $n \geqslant 1$. Comme on a $W_1 \subset W_n$, il ne reste qu'à montrer $k \times I \twoheadrightarrow W_n$. Notons $\mathscr{J}_n$ l'ensemble des parties non vides de I à $\leqslant n$ éléments, ainsi que Σ_n l'ensemble des couples (J, φ) avec $J \in \mathscr{J}_n$ et $\varphi : \{1, \ldots, |J|\} \to J$ une bijection. On a une surjection naturelle $k^n \times \Sigma_n \to W_n$, envoyant $((x_1, \ldots, x_n), (J, \varphi))$ sur l'élément w vérifiant $w_j = x_{\varphi^{-1}(j)}$ pour tout $j \in J$, et $w_j = 0$ pour $j \notin J$. On a $\mathscr{J}_n \sim I$ par l'Exercice 1.16, car I est infini. La surjection $\Sigma_n \to \mathscr{J}_n, (J, \varphi) \mapsto J$, étant à fibres finies et non vides, on a aussi $\mathscr{J}_n \hookrightarrow \Sigma_n \hookrightarrow \mathbb{N} \times \mathscr{J}_n$, et donc $\mathscr{J}_n \sim \Sigma_n$ (Exercice 1.12 et Cantor-Bernstein), puis $\Sigma_n \sim I$. Il ne reste qu'à montrer que l'on a $k^n \times I \sim k \times I$. C'est clair si k est infini, car on a alors $k^n \sim k$. Si k est fini, c'est vrai aussi, car on a même $k \times I \sim I$. Cela termine la démonstration du (i). Pour le (ii), on constate que si on a $Y \hookrightarrow X$ avec X infini et Y non vide, alors on a $X \hookrightarrow Y \times X \hookrightarrow X \times X \sim X$, et donc $Y \times X \sim X$.

Exercices du chapitre 2

Exercice 2.1. (i) Soit M régulier et $x \in M$. Par hypothèse, l'application $M \to M, m \mapsto xm$, est injective. Si M est fini, elle est donc aussi surjective. En particulier, pour tout $x \in M$ il existe $y \in M$ tel que $xy = 1$ (*tout $x \in M$ admet un inverse à droite*). Il reste à voir que ce y vérifie aussi $yx = 1$. On constate que l'élément $e = yx$ vérifie $e^2 = yxyx = y1x = e$ (*idempotent*). Mais si f désigne un inverse à droite de e, on a alors $e = e^2 f = ef = 1$, et donc $yx = 1$.

Le (ii) est une conséquence du (i) appliqué à $M = A^\times$ (l'argument est même un peu plus simple, car la régularité vaut des deux côtés dans ce cas particulier). Montrons le (iii). Il faut voir que si H est non vide et stable par produits, alors c'est un sous-groupe. Il existe $h \in H$. Comme G est fini, on a $h^n = 1$ pour un certain entier $n > 0$, et donc $h^{-1} = h^{n-1}$ est dans H, puis $h^n = 1$ est dans H.

Exercice 2.2. (i) Observons que f_i est un cycle de longueur $n-i$ sur $\{i, i+1, \ldots, n-1\}$, et que l'on a $f_i^i(\{0, 1, \ldots, n\}) \subset \{i, i+1, \ldots, n-1\}$. On en déduit $f_i^n = f_i^{n-i} f_i^i = f_i^i$, puis $M_i = \{f_i^k \mid 0 \leqslant k < n\}$. De plus, les éléments f_i^k avec $k = 0, \ldots, n-1$ sont distincts, car on a $f_i^k(0) = k$. On a montré $|M_i| = n$.

(ii) Si M est un monoide, posons $M(n) = \{m^k \mid m \in M \smallsetminus \{1\}, k \geqslant n\}$. On constate que l'on a $M_i(n) = \{f_i^k \mid k \geqslant i\}$, et donc $|M_i(n)| = n - i$. Mais tout isomorphisme $M \to N$ induit une bijection $M(n) \sim N(n)$. Ainsi, si on a $M_i \simeq M_j$, on a $n - i = n - j$, puis $i = j$.

(iii) Supposons $M = \langle x \rangle$ et $|M| = n$. Les éléments $1, x, x^2, \ldots, x^{n-1}$ sont distincts. En effet, si on a $x^j = x^i$ avec $0 \leqslant i < j \leqslant n-1$, une récurrence immédiate montre que pour tout entier $n \geqslant i$, l'élément x^n est de la forme x^m avec $i \leqslant m < j$. En particulier, on a $|M| \leqslant i + j - i \leqslant j < n$, une contradiction. On a donc $M = \{x^i \mid 0 \leqslant i < n\}$. Ainsi, il existe un unique entier $0 \leqslant i < n$ avec $x^n = x^i$. Il ne serait pas difficile de vérifier à la main qu'il existe un (unique) isomorphisme $M \to M_i$ envoyant x sur f_i. On peut aussi procéder comme suit. Pour tout monoïde M, on dispose d'un morphisme naturel *à la Cayley* de M dans $(M^M, \circ)$, à savoir $m \mapsto \mathrm{L}_m$ avec $\mathrm{L}_m(n) = mn$. Il est injectif, car on a $\mathrm{L}_m(1) = m$. Il identifie donc M à un sous-monoide de M^M. Revenons à $M = \langle x \rangle$ comme ci-dessus et identifions l'ensemble M à $\{0, 1, \ldots, n-1\}$ via $j \mapsto x^j$, de sorte que M^M s'identifie à $\mathrm{F}(n)$. On constate que L_x n'est rien d'autre que la fonction f_i. Ainsi, on a construit un morphisme injectif $M \to \mathrm{F}(n)$ d'image M_i, donc un isomorphisme $M \simeq M_i$. À isomorphisme près, les n monoïdes monogènes sont donc les M_i, $0 \leqslant i < n$.

Exercice 2.3. (i) Soit M un monoïde de cardinal 2. On a $M = \{1, x\}$ avec $x \neq 1$. Si $x^2 = 1$, alors M est un groupe d'ordre 2, isomorphe à $(\mathbb{Z}/2\mathbb{Z}, +)$. Si $x^2 = x$, on constate que la bijection $(\mathbb{Z}/2\mathbb{Z}, \times) \to M$ envoyant 1 sur 1 et 0 sur x est un morphisme de monoïde.

(ii) Soit M de cardinal 3 non monogène. Soit $x \in M$ avec $x \neq 1$. On a $x^2 \in \{1, x\}$. Soit y l'unique élément tel que l'on ait $M = \{1, x, y\}$. Supposons d'abord $x^2 = 1$, *i.e.* x inversible d'inverse x. Vérifions $xy = y = yx$. En effet, $xy = 1$ implique $y = x$ (absurde), de même pour $yx = 1$, $xy = x$ implique $y = 1$ (absurde) et de même pour $yx = x$. On constate alors que la bijection $(\mathbb{Z}/3\mathbb{Z}, \times) \to M$ envoyant 1 sur 1, -1 sur x, et 0 sur y est un morphisme de monoïde ! Cela montre aussi qu'un tel M existe, car $M = (\mathbb{Z}/3\mathbb{Z}, \times)$ a les propriétés requises. Dans le dernier cas, on a donc $x^2 = x$ pour tout $x \neq 1$, et même $x^2 = x$ pour tout x.

(iii) Supposons donc $M = \{1, x, y\}$ de cardinal 3 avec $x^2 = x$ et $y^2 = y$. On a $xy \neq 1$, car $xy = 1$ implique par exemple $x = x^2 y = xy = 1$. On a donc $\{xy, yx\} \subset \{x, y\}$, et il y a au plus 4 cas. Soit $xy = x$ et $yx = y$. Dans ce cas, on constate que l'on a $ab = a$ pour tout $a, b \in M$ avec $a, b \neq 1$. Soit $xy = y$ et $yx = x$. Dans ce cas, on constate que l'on a $ab = b$ pour tout $a, b \in M$ avec $a, b \neq 1$. Soit $xy = x$ et $yx = x$, ou $xy = y$ et $yx = y$.

Ces deux cas sont isomorphes comme on le voit en échangeant x et y. Les 3 cas ci-dessus ne sont pas isomorphes entre eux s'ils existent, par les constatations. Il y a donc au plus 3 tels monoïdes. Pour voir que ces 3 cas existent, on peut continuer l'analyse synthèse et voir que par le morphisme de Cayley $M \to (M^M, \circ), m \mapsto \mathrm{L}_m$, ces trois monoïdes se plongent dans F(3) (exercice précédent) s'ils existent. On a tout fait pour qu'il soit aisé de les réaliser concrètement dans F(3) : nous laissons cette vérification au lecteur.

Exercice 2.4. Soient $1_\star$ et $1_\circ$ les neutres de $(X, \star)$ et $(X, \circ)$. On a $1_\star = 1_\star \star 1_\star = (1_\star \circ 1_\circ) \star (1_\circ \circ 1_\star) = (1_\star \star 1_\circ) \circ (1_\circ \star 1_\star) = 1_\circ \circ 1_\circ = 1_\circ$. On pose $1 = 1_\star = 1_\circ$. Pour $x, y \in X$ on a $x \star y = (x \circ 1) \star (1 \circ y) = (x \star 1) \circ (1 \star y) = x \circ y$: les deux lois sont égales, on les note $xy = x \star y = x \circ y$. On a donc $(xy)(zt) = (xz)(yt)$ pour tout $x, y, z, t \in X$. Pour $z = 1$, c'est l'associativité. Pour $x = t = 1$, c'est la commutativité. (Ce lemme est moins futile qu'il n'en a l'air, et sert par exemple en topologie algébrique !)

Exercice 2.5. (i) Fixons $r \in \mathbb{Z}$. Par Bezout, il existe $(a, b) \in \mathbb{Z}^2$ avec $r = am + bn$. On peut toujours ajouter ou soustraire à (a, b) le couple $(n, -m)$ et préserver cette égalité, de sorte que l'on peut supposer $0 \leqslant b < m$. Si on a une autre écriture $am + bn = a'm + b'n$ on a $(a' - a)m = (b - b')n$ et donc, comme m et n sont premiers entre eux, $a \equiv a' \bmod n$ et $b \equiv b' \bmod m$. Si on a $0 \leqslant b, b' < m$, cela force $b = b'$, puis $a = a'$.

Montrons le (ii). Si on a $r = am + bn$ avec $a, b \geqslant 0$, observons que quitte à ajouter $(n, -m)$ à (a, b) on peut supposer $0 \leqslant b < m$. Autrement dit, $\mathbb{N}n + \mathbb{N}m$ est l'ensemble des $am + bn$ avec $a \geqslant 0$ et $0 \leqslant b < m$. Par le (i), les entiers non de cette forme sont les $am + bn$ avec $a < 0$ et $0 \leqslant b < m$. Le plus grand d'entre eux s'obtient pour $a = -1$ et $b = m - 1$: c'est $-m + (m - 1)n = mn - n - m$.

Pour le (iii), notons d_i le pgcd de $(m_1, \ldots, m_i)$, pour $1 \leqslant i \leqslant n$. On a $d_{i+1} = \mathrm{pgcd}(d_i, m_{i+1})$ pour $i < n$, et $d_n = 1$. Observons que pour $a, b \in \mathbb{N}$, de pgcd d, alors on a $a\mathbb{N} + b\mathbb{N} = d(a'\mathbb{N} + b'\mathbb{N})$ avec $a = a'd$ et $b = b'd$, et donc $a\mathbb{N} + b\mathbb{N}$ contient tous les multiples de d assez grands par le (ii). Ainsi, $m_1\mathbb{N} + m_2\mathbb{N}$ contient un entier de la forme $d_2 s_2$ avec s_2 premier avec m_3. Le pgcd de $d_2 s_2$ et m_3 est d_3. Ensuite, $d_2 s_2 \mathbb{N} + m_3\mathbb{N}$ contient un entier de la forme $d_3 s_3$ avec s_3 premier à m_4, etc... À la $n-1$-ème étape, on a construit un sous-monoïde $d_{n-1}s_{n-1}\mathbb{N} + m_n\mathbb{N} \subset m_1\mathbb{N} + m_2\mathbb{N} + \cdots + m_n\mathbb{N}$, avec s_{n-1} premier à m_n, et donc $\mathrm{pgcd}(d_{n-1}s_{n-1}, m_n) = d_n = 1$, ce qui conclut.

Montron le (iv). Notons $F(z) \in \mathbb{C}(z)$ la fraction rationnelle de l'énoncé. On a $F(z) = \sum_{k \geqslant 0} f_k z^k$ pour $|z| < 1$ et on veut montrer $f_k \neq 0$ pour tout k assez grand. Le complexe $z = 1$ est un pôle d'ordre n de $F(z)$, et les autres pôles sont des racines de l'unité $\neq 1$, et sont (en tant que pôle) d'ordre $\leqslant n$. On constate que comme les m_i sont premiers entre eux, ces pôles $\neq 1$ sont d'ordre $< n$. Mais pour $n \geqslant 1$ on a $1/(1-z)^n = \sum_{k \geqslant 0} p_k(n)\, z^k$ avec $p_k(n) = (k+1)(k+2)\cdots(k+n-1)$ (et $p_k(1) = 1$). On a $p_k(n) = k^{n-1} + \mathrm{O}(k^{n-2})$ pour $k \to \infty$. Décomposons $F(z)$ en éléments simples. Il y a un terme en $c/(1-z)^n$, avec $c = \lim_{z \to 1}(z-1)^n F(z) = 1/(m_1 \cdots m_n)$. Les autres termes sont de la forme $d/(1-\zeta z)^{n'}$ avec $n' < n$ et $|\zeta| = 1$. On en déduit $f_k = ck^{n-1} + \mathrm{O}(k^{n-2})$ où $c = 1/(m_1 \ldots m_n)$ (c'est vrai aussi pour $n = 1$, car on a alors $m_1 = 1$ et $f_k = 1$ pour tout $k \geqslant 0$).

Exercice 2.6. (i) Soit $M \subset \mathbb{N}$ un sous-monoïde. Si M contient r et $r + 1$ (premiers entre eux), alors il est primitif. Réciproquement, si le pgcd d'une famille infinie éléments $x_1, x_2, \ldots, x_n, \ldots,$ (disons non nuls) vaut 1, c'est que le pgcd de $x_1, \ldots, x_n$ vaut 1 pour n assez grand. En effet, si on pose $d_i = \mathrm{pgcd}(x_1, \ldots, x_i)$, on a $d_{i+1} = \mathrm{pgcd}(d_i, x_{i+1})$ et donc $d_{i+1} \mid d_i$. Ainsi, la suite des entiers $d_i \geqslant 1$ est décroissante, et donc est constante égale à un certain entier d pour n assez grand. Par définition, d divise tous les x_i. On a donc $d = 1$, ce qui conclut. On conclut par le (i) par le point (iii) de l'exercice précédent.

(ii) Soit M un sous-monoïde de $\mathbb{N}$. On peut supposer $M \neq \{0\}$. Notons $d \geqslant 1$ le pgcd des éléments de M. On a $M \subset d\mathbb{N}$, et quitte à remplacer M par $\frac{1}{d}M$, on peut supposer $d = 1$.

Si $m_1, \ldots, m_n$ sont dans M et premiers entre eux, on a vu que $\mathbb{N}m_1 + \mathbb{N}m_2 + \cdots + \mathbb{N}m_n \subset M$ contient tous les entiers plus grand qu'un certain entier r. Soient N l'ensemble fini des entiers qui sont à la fois dans M et $< r$. Il est clair que M est engendré par N et par les m_i (un nombre fini d'éléments).

(iii) Soient M_1 et M_2 deux sous-monoïdes de $\mathbb{N}$, ainsi que $f : M_1 \to M_2$ un morphisme de monoïdes. Si M_1 est primitif, le sous-groupe de $\mathbb{Z}$ engendré par M_1 est $\mathbb{Z}$. Tout $x \in \mathbb{Z}$ s'écrit donc $x = m - n$ avec $m, n \in M_1$. On constate que $f(m) - f(n) \in \mathbb{Z}$ ne dépend pas de l'écriture choisie de x. En effet, si on a $m - n = m' - n'$ avec m, m', n, n' dans M_1, alors on a $m + n' = m' + n$ dans M_1, puis $f(m) + f(n') = f(m') + f(n)$ car f morphisme, puis $f(m) - f(n) = f(m') - f(n')$. Il existe donc une unique application $f' : \mathbb{Z} \to \mathbb{Z}$ vérifiant $f'(m) = f(m)$ pour $m \in M_2$, et $f'(m - n) = f(m) - f(n)$ pour tout $m, n \in M_2$. Un tel f' est manifestement un morphisme de groupes. Posons $d = f'(1)$: on a alors $f'(n) = nd$ pour tout $n \in \mathbb{Z}$, et donc $f(M_1) \subset d\mathbb{Z}$. Supposant maintenant $f(M_1) = M_2$ et M_2 primitif, on a $d = \pm 1$, puis $d = 1$ car M_2 est dans $\mathbb{N}$. On a donc $f = \mathrm{id}$ et $M_1 = M_2$.

(iv) Les sous-monoïdes primitifs $M_n := n\mathbb{N} + (n+1)\mathbb{N}$ de $\mathbb{N}$ sont distincts car le plus petit élément non nul de M_n est n. Ces monoïdes sont donc non isomorphes par le (iii).

Exercice 2.7. (i) Soit $f : X \to X$ vue comme élément de M. Alors f est inversible à droite si, et seulement si, elle admet une section, et on a vu que c'est équivalent à f surjective. De même, f est inversible à gauche si, et seulement si, elle admet une retraction (Exercice 1.9 Chap. 1), ce qui est équivalent à f injective.

(ii) Si X est infini, on a $X \sim X \coprod \{0\} \sim X \coprod \mathbb{N}$, et donc il existe une surjection $f : X \to X$ possédant une fibre infinie en un point x_0. Une telle f admet une infinité de sections. De même, il existe une injection $f : X \to X$ avec $X \smallsetminus f(X)$ infini. Une telle f admet une infinité de rétractions.

(iii) Soit $m \in M$. Supposons que l'on a $x, y \in M$ avec $mx = 1$ et $ym = 1$. Alors par associativité on a $y = y(mx) = (ym)x = x$.

(iv) Soit $e : X \to X$. On a $e^2 = e$ si, et seulement si, $e(e(x)) = e(x)$ pour tout $x \in X$ (on dit alors que e est *idempotent*). Il est donc équivalent de demander que e vaut l'identité sur $\mathrm{Im}\, e$ (c'est l'analogue ensembliste des projecteurs). Supposons $e^2 = e$ et soit $f : X \to X$. On a $ef = f$ si, et seulement si, $\mathrm{Im}\, f \subset \mathrm{Im}\, e$. On a $fe = f$ si, et seulement si, f est constante sur les fibres de e.

(v) On a $emen = e(men)$ donc $eM \subset M$ est stable par produits. La loi induite est bien sûr associative car celle de M l'est. On a $e = e.1 \in eM$. Pour $x = em$ avec $m \in M$, on constate $ex = eem = em = x$. Réciproquement, si $x = ex$ on a $x \in eM$. On a donc $eM = \{m \in M \mid em = m\}$. Si eM a un élément neutre, il est donc nécessairement égal à e. De plus, e est neutre si, et seulement si on a $me = m$ pour tout $m \in eM$, *i.e.* si toute fonction $X \to \mathrm{Im}\, e$ est constante sur les fibres de e par le (iv). Si $|\mathrm{Im} e| = 1$, toute telle fonction est constante, donc convient. Si e est surjective, c'est l'identité par (iv), et les fibres de e sont des singletons, donc tout f convient. Dans le cas restant, il existe a, b, c distincts dans X avec $\{a, b\} \in \mathrm{Im}\, e$ et $c \notin \mathrm{Im}\, e$. On peut même supposer $b = e(c)$. Soit $f : X \to X$ la fonction définie par $f(c) = a$ et $f(x) = b$ pour $x \neq c$. On a bien $\mathrm{Im}\, f \subset \mathrm{Im}\, e$ mais f n'est pas constante sur $e^{-1}(b) \supset \{c, b\}$.

Exercice 2.8. (i) On a $(h, k)(h', k') = (hh', kk')$ dans le groupe $H \times K$ par définition de la loi de groupe produit. Ainsi, f est un morphisme de groupes si, et seulement si, pour tout $h, h' \in H$ et tout $k, k' \in K$ on a $hh'kk' = hkh'k'$. Il est équivalent de demander que pour tout $h \in H$ et tout $k \in K$ on a $hk = kh$. (Autrement dit tout élément de H commute avec tout élément de K. Attention, les sous-groupes H et K ne sont pas nécessairement commutatifs).

(ii) Vérifions que f est injective si, et seulement si, on a $H \cap K = \{1\}$. En effet, si $x \in H \cap K$ est non trivial, on a $(1, x) \neq (x, 1)$ et $f(1, x) = f(x, 1) = x$, donc f est non injective. Réciproquement, supposons $H \cap K = \{1\}$. Alors $hk = h'k'$ avec $h, h' \in H$ et $k, k' \in K$ implique $h^{-1}h' = k(k')^{-1} \in H \cap K = \{1\}$, et donc $h = h'$ et $k = k'$: f est injective.

(iii) L'application f est surjective si, et seulement si, on a $G = HK$.

(iv) C'est la concaténation des conditions (i), (ii), (iii) : $hk = kh$ pour tout $(h, k) \in H \times K$, $H \cap K = \{1\}$ et $G = HK$.

Exercice 2.9. (i) Comme dans l'exercice précédent, on regarde l'application $f : H \times K \to HK$, $(h, k) \mapsto hk$. Elle est surjective par construction, et il suffit pour conclure de montrer que toutes ses fibres ont même cardinal $|H \cap K|$. Fixons $(h, k) \in H \times K$. Supposons que $(h', k') \in H \times K$ vérifie $h'k' = hk$. Alors l'élément $z := h^{-1}h' = k(k')^{-1}$ est dans $H \cap K$, et on a $(h', k') = (hz, z^{-1}k)$. Récipoquement, pour tout $z \in H \cap K$, l'élément $(h', k') = (hz, z^{-1}k)$ vérifie $h'k' = hzz^{-1}k = hk$. Ainsi, la fibre de f au dessus de $f(h, k) = hk$ est constitué des $|H \cap K|$ éléments de la forme $(hz, z^{-1}k)$ avec $z \in H \cap K$, ce qui conclut.

(ii) Le groupe $H \cap K$ est un sous-groupe de H et de K, donc par Lagrange son cardinal divise $|H|$ et $|K|$, puis $|H \cap K| = 1$. On conclut par le (i).

Exercice 2.10. (i) Supposons que HK est un sous-groupe. Il est alors stable par la bijection $x \mapsto x^{-1}$, donc on a $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$. Réciproquement, si $HK = KH$ le même calcul montre que HK est stable par inversion. Il contient $1 = 1.1$, et il est stable par produit car $HKHK = HHKK = HK$.

(ii) Supposons que dans le groupe G on a deux éléments s et t d'ordre 2 qui ne commutent pas. Par exemple, on peut prendre $G = \mathrm{O}(2)$ et deux reflexions d'axes distincts et non perpendiculaires. On pose $H = \langle s \rangle$ et $K = \langle t \rangle$. Alors on a $HK = \{1, s, t, st\} \neq KH = \{1, t, s, ts\}$.

(iii) Si H est distingué dans G on a $Hk = kH$ pour tout k dans K, et en particulier, $HK = KH$.

Exercice 2.11. Soient $h \in H$ et $k \in K$. On regarde l'élément

$$hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} = k(hk^{-1}h^{-1}).$$

La première écriture montre qu'il est dans K (qui est distingué), et la seconde qu'il est dans H (idem). Il est donc dans $H \cap K = \{1\}$. On a donc $hkh^{-1}k^{-1} = 1$ puis $hk = kh$. On conclut par le (iv) de l'Exercice 2.8.

Exercice 2.12. (i) Vrai. On a $G = G^{-1} = (HK)^{-1} = K^{-1}H^{-1} = KH$.

(ii) Vrai. Rappelons que pour $g \in G$, on dispose d'un automorphisme $\mathrm{int}_g : G \to G, x \mapsto gxg^{-1}$. Il suffit de montrer que l'on a $G = gKg^{-1}H$ pour tout $g \in G$, par le (i). Mais tout $g \in G$ s'écrit $g = hk$ avec $h \in H$ et $k \in K$. Utilisant $kKk^{-1} = K$ et $hHh^{-1} = H$ on constate $gKg^{-1}H = hkKk^{-1}h^{-1}H = hKh^{-1}H = h(KH)h^{-1} = hGh^{-1} = G$.

(iii) Faux. Soit $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $H = \langle (1, 0) \rangle$, $K = \langle (0, 1) \rangle$ et $L = \langle (1, 1) \rangle$. On a $G = H + K = H + L$, $H \cap K = H \cap L = \{0\}$, mais $K \neq L$.

Exercice 2.13. Toutes les vérifications sont triviales.

Exercice 2.14. (i) Toute application $f : S \to H \times K$, s'écrit de manière unique sous la forme $f(x) = (a(x), b(x))$ avec $a : S \to H$ et $b : S \to K$ (quelconques). Par définition du groupe produit, f est un morphisme de groupes si, et seulement si, a et b en sont. Pour S fini on a donc $|\mathrm{Hom}(S, G \times H)| = |\mathrm{Hom}(S, G)||\mathrm{Hom}(S, H)|$, et de même$|\mathrm{Hom}(S, G \times K)| = |\mathrm{Hom}(S, G)||\mathrm{Hom}(S, K)|$. Mais on a aussi $|\mathrm{Hom}(S, G \times H)| = |\mathrm{Hom}(S, G \times K)|$ car on

a $G \times H \simeq G \times K$ par hypothèse. Comme $|\mathrm{Hom}(S, G)|$ est fini non nul (considérer le morphisme trivial !), cela montre le (i).

(ii) Par récurrence sur $|S|$. Tout morphisme $f : S \to H$ admet un noyau, qui est un sous-groupe distingué Q de S, et le morphisme f est injectif si et seulement si on a $Q = 1$. Le nombre de morphismes $S \to H$ de noyau Q est, par propriété universelle du groupe quotient, $|\mathrm{inj}(S/Q, H)|$. La même chose vaut pour les morphismes $S \to K$ de noyau Q. Mais on a $|\mathrm{inj}(S/Q, H)| = |\mathrm{inj}(S/Q, K)|$ par récurrence quand $Q \neq 1$, et $|\mathrm{Hom}(S, H)| = |\mathrm{Hom}(S, K)|$ d'après le (i). On a donc aussi $|\mathrm{inj}(S/Q, H)| = |\mathrm{inj}(S/Q, K)|$ pour $Q = 1$.

(iii) On a $|\mathrm{inj}(H, H)| \geqslant 1$ (l'identité !). Par le (ii) pour $S = H$ on en déduit l'existence d'un morphisme injectif $H \to K$. C'est un isomorphisme, car on a $|H| = |K|$.

(iv) Posons $G = (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$. On a $\mathbb{N} \coprod \{\bullet\} \sim \mathbb{N}$, et donc un isomorphisme $G \times \mathbb{Z}/2\mathbb{Z} \simeq (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$. On a même $\mathbb{N} \coprod \mathbb{N} \sim \mathbb{N}$, et donc $G \times G \simeq G$.

Exercice 2.15. On voit $(\mathbb{Z}/2\mathbb{Z})^X$ comme l'ensemble des fonctions $X \to \mathbb{Z}/2\mathbb{Z}$. C'est un anneau pour les lois $+$ et $\cdot$ évidentes, issues de l'anneau $(\mathbb{Z}/2\mathbb{Z}, +, \cdot)$. Pour $A \subset X$ on note $1_A \subset (\mathbb{Z}/2\mathbb{Z})^X$ la fonction caractéristique de A. On constate $1_A 1_B = 1_{A \cap B}$ et $1_A + 1_B = 1_{A \Delta B}$. Ainsi, $A \mapsto 1_A$ est une bijection $\mathrm{P}(X) \to (\mathbb{Z}/2\mathbb{Z})^X$ qui définit à la fois un morphisme $(\mathrm{P}(X), \Delta) \to ((\mathbb{Z}/2\mathbb{Z})^X, +)$ et un morphisme $(\mathrm{P}(X), \cap) \to ((\mathbb{Z}/2\mathbb{Z})^X, \cdot)$. On conclut par transport de structure que $(\mathrm{P}(X), \Delta, \cap)$ est un anneau isomorphe à $(\mathbb{Z}/2\mathbb{Z})^X$.

Exercice 2.16. Montrons le (i). Soient x et y deux points fixes distincts de f. On veut montrer que la droite (x, y) est constituée de point fixes de f. Comme la distance d de E est euclidienne, pour tout point z de cette droite, si on pose $a = \mathrm{d}(z, x)$ et $b = \mathrm{d}(z, y)$, alors z est l'unique point de E à distance a de x et à distance b de y (cas d'égalité de l'inégalité triangulaire). Mais on a $a = \mathrm{d}(x, z) = \mathrm{d}(f(x), f(z)) = \mathrm{d}(x, f(z))$ et $b = \mathrm{d}(y, z) = \mathrm{d}(f(y), f(z) = \mathrm{d}(y, f(z))$, et donc $z = f(z)$.

Montrons le (ii) par récurrence descendante sur l'entier p (qui est $\geqslant 0$). On a $p = n$ si, et seulement si, $f = \mathrm{id}_E$, et on convient naturellement dans ce cas que f est produit de 0 reflexions. Si $p < n$, il existe $x \in E - 0$ avec $f(x) \neq x$. Soit H l'hyperplan médiateur du segment $[x, f(x)]$. On a $\mathrm{s}_H(f(x)) = x$ et H contient manifestement $\mathrm{Fix}(f)$: pour $z \in \mathrm{Fix}(f)$ on a $\mathrm{d}(z, x) = \mathrm{d}(f(z), f(x)) = \mathrm{d}(z, f(x))$. Mézalor l'isométrie $g = \mathrm{s}_H \circ f$ vérifie $\mathrm{Fix}(g) \supsetneq \mathrm{Fix}(f)$ et donc on a $p' = \dim \mathrm{Fix}(g) \geqslant p + 1$ (cela colle avec notre convention $p = -1$ si $\mathrm{Fix}(f)$ est vide). Par hypothèse de récurrence, g est produit d'au plus $n - p' \leqslant n - p - 1$ réflexions, et donc $f = \mathrm{s}_H^{-1} \circ g = \mathrm{s}_H \circ g$ est produit d'au plus $n - p$ réflexions. Cela termine la preuve du (ii). Le (iii) en découle car le fait d'être affine est stable par composition, et les réflexions sont affines.

Exercice 2.17. Par définition, les réflexions affines de $\mathbb{R}$ sont les $\mathrm{s}_a(x) = a - x$, où $a \in \mathbb{R}$, ce qui répond à (i). On sait que toute isométrie affine de $\mathbb{R}$ est produit de 0, 1 ou 2 réflexions affines. C'est donc respectivement soit $\mathrm{id}_{\mathbb{R}}$, soit s_a avec $a \in \mathbb{R}$, soit de la forme $\mathrm{s}_a \circ \mathrm{s}_b(x) = a - (b - x) = a - b + x$ avec $a, b \in \mathbb{R}$, *i.e.* une translation de vecteur $a - b$. On a montré le (ii). Pour $v \in \mathbb{R}$ on note τ_v la translation de vecteur v, *i.e.* $\tau_v(x) = x + v$. Les translations forment un sous-groupe $H \subset \mathrm{Iso}(1)$ isomorphe à $\mathbb{R}$: c'est l'image du morphisme injectif $\mathbb{R} \to \mathrm{Iso}(1), v \mapsto \tau_v$. Fixons arbitrairement $a \in \mathbb{R}$ et posons $K = \langle \mathrm{s}_a \rangle \simeq \mathbb{Z}/2\mathbb{Z}$. En fait, K coincide avec le sous-groupe K' des $f \in \mathrm{Iso}(1)$ vérifiant $f(a/2) = a/2$. Par exemple, K' ne contient aucune translation non triviale, et on a $s_b \in K'$ si et seulement si $b = a$. On a trivialement $K' \cap H = \{1\}$ et aussi $\mathrm{Iso}(1) = HK'$. En effet, pour $f \in \mathrm{Iso}(1)$, f envoit $a/2$ sur un réel b, et on a $\tau_v \circ f \in K'$ pour $v = a/2 - b$, et donc $f \in HK'$. Cela montre la première assertion du (iii). Pour la seconde c'est non, car $\mathrm{Iso}(1)$ n'est pas commutatif : on a $\mathrm{s}_0 \circ \tau_v = \tau_{-v} \circ \mathrm{s}_0$ pour tout $v \in \mathbb{R}$.

Exercice 2.18. Pour le (i), le sous-groupe μ de $\mathbb{C}^\times$ constitué des racines de l'unité d'ordre arbitraire, *i.e.* $\mu = \cup_{n\geqslant 1}\mu_n$, convient. Un autre exemple est $G = (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$, dont tous les éléments sont d'ordre 1 ou 2. Pour le (ii), on peut regarder les réflexions $\mathrm{s}_0(x) = -x$ et $\mathrm{s}_1(x) = 1 - x$ dans $\mathrm{Iso}(1)$ (exercice précédent). Elles sont d'ordre 2, mais $\mathrm{s}_0 \circ \mathrm{s}_1$ est la translation $x \mapsto x + 1$, qui est d'ordre infini. Un autre exemple du même type est obtenu en considérant deux réflexions orthogonales s et t du le plan euclidien. On a $s^2 = t^2 = 1$, et st est la rotation d'angle le double de l'angle $\pi\theta$ entre les deux axes. Ainsi, st est d'ordre fini si, et seulement si, $\theta \in \mathbb{Q}$.

Exercice 2.19. Pour le (i), on remarque que comme on a $d_i x_i = 0$ dans G pour $i = 1, \ldots, n$, on dispose d'un morphisme bien défini $f : \prod_{i=1}^n (\mathbb{Z}/d_i\mathbb{Z}) \to G, (\overline{m_i}) \mapsto \sum_{i=1}^n m_i x_i$. Il est surjectif car les x_i engendrent G. On a donc

$$d_1 d_2 \cdots d_n = |\prod_{i=1}^n (\mathbb{Z}/d_i\mathbb{Z})| = |\mathrm{Im}\, f|\,|\ker f| = |G||\ker f|,$$

et donc $|G|$ divise $d_1 d_2 \cdots d_n$. Pour le (ii), on constate que si p divise $|G|$, il divise l'un des d_i, disons $d_i = pm_i$, et donc $m_i x_i$ est d'ordre $d_i/m_i = p$.

Exercice 2.20. (i) Que A soit d'ordre a est clair. Pour le B, l'observation donnée montre que le polynôme caractéristique de B est $(X - \zeta_b)(X - \zeta_b^{-1})$. On a $\zeta_b \neq \zeta_b^{-1}$ car $b > 2$. Ainsi, B est diagonalisable de valeurs propres ζ_b et ζ_b^{-1}, et donc conjuguée à la matrice diagonale $\mathrm{diag}(\zeta_b, \zeta_b^{-1})$, manifestement d'ordre b.

(ii) Un calcul immédiat montre $\mathrm{trace}\, A\, B_t = (\zeta_a - \zeta_a^{-1})t + \zeta_a^{-1}\zeta_b + \zeta_a^{-1}\zeta_b^{-1}$.

(iii) La trace ci-dessus est de la forme $\alpha t + \beta$ avec $\alpha \neq 0$ (car $a > 2$). Pour t bien choisi elle vaut donc $\zeta_c + \zeta_c^{-1}$. Pour un tel t, la matrice $A\, B_t$ (de déterminant 1) est de trace $\zeta_c + \zeta_c^{-1}$, donc d'ordre c par l'observation et le même argument qu'au (i) (il utilise $c > 2$). Pour un t bien choisi, on a $|\mathrm{trace}\, A\, B_t| > 2$, et donc $A\, B_t$ est d'ordre infini (les valeurs propres d'un $M \in \mathrm{GL}_n(\mathbb{C})$ d'ordre fini sont des racines de l'unité).

(iv) En effet, si $p \equiv 1 \bmod abc$, le groupe cyclique $(\mathbb{Z}/p\mathbb{Z})^\times$, qui est d'ordre $p - 1$, contient des éléments d'ordre a, b et c, que l'on note encore ζ_a, ζ_b et ζ_c. L'argument précédent fonctionne alors verbatim dans $G = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$.

(v) Soit m impair avec $h^m = 1$. On a $\det gh = \det g \det h$, $\det g = \pm 1$ et $(\det h)^m = 1$. Si $\det g = -1$, on en déduit que $\det gh$ est d'ordre pair, et donc gh est d'ordre pair. Si $\det g = 1$, comme g est diagonalisable de valeurs propres ± 1, la seule possibilité est $g = -1_2$. Mais dans ce cas g est central, et donc on a $(gh)^{2m} = 1_2$ et $(gh)^m = -1_2$, et gh est d'ordre pair. Cela montre que l'on ne peut pas d'affranchir des hypothèses $a, b, c \geqslant 3$ par cette méthode.

(vi) Observons que le seul élément d'ordre 2 de $\mathrm{SL}_2(k)$, quand k est un corps de caractéristique $\neq k$, est -1_2. En effet, si on a $g^2 = 1$ alors $X^2 - 1 = (X - 1)(X + 1)$ annule g et est à racines simples, donc g est conjugué dans $\mathrm{GL}_2(k)$ à $\mathrm{diag}(\pm 1, \pm 1)$. Mais $\det g = 1$ montre que ces deux signes sont les mêmes, et $g \neq 1$ conclut l'observation.

Fixons a, b, c des entiers $\geqslant 2$. Supposons que l'on a un groupe G possédant un unique élément z d'ordre 2, que z est dans le centre de G (en fait, c'est automatique), et que l'on a $g, h \in G$ avec g d'ordre $2a$, h d'ordre $2b$ et gh d'ordre $2c$. Soit $Z = \langle z \rangle$. C'est un sous-groupe distingué de G car z est central. Notons g' et h' les images de g et h dans le groupe quotient $G' = G/Z$. On observe que l'on a $g^a = z$, $h^b = z$ et $(gh)^c = z$, car ces trois éléments sont d'ordre 2. On en déduit aisément que g', h' et $g'h'$ sont d'ordre respectifs a, b et c dans G' : ce que l'on cherchait à démontrer.

Exercice 2.21. (i) Deux morphismes $f, f' : G \to H$ qui coïncident sur le générateur g de G sont égaux, donc ev_g est injective. Soit $x \in H$, avec en outre $x^N = 1$ si g est d'ordre

$N \geqslant 1$. Montrons qu'il existe un morphisme $f : G \to H$ tel que $f(g^n) = x^n$ pour tout $n \in \mathbb{Z}$. Il est nécessairement unique s'il existe par ce que l'on vient de voir. Il est bien défini car si on a $g^n = g^m$ dans G alors on a $n = m$ si g est d'ordre infini (et donc $x^n = x^m$), et $n \equiv m \bmod N$ si g est d'ordre $N \geqslant 1$, et donc encore $x^n = x^m$ car $x^N = 1$.

(ii) Par définition, quand G et H sont des groupes quelconques avec H abélien la loi de groupes que l'on met sur $\mathrm{Hom}(G, H)$ est $(f, f') \mapsto ff'$ avec $(ff')(x) := f(x)f'(x)$. Noter que l'on a bien $ff' \in \mathrm{Hom}(G, H)$ car pour tout $x, y \in G$ on a $f(y)f'(x) = f'(x)f(y)$ puis

$$(ff')(xy) = f(xy)f'(xy) = f(x)f(y)f'(x)f'(y) = f(x)f'(x)f(y)f'(y) = (ff')(x)(ff')(y),$$

On conclut car pour G monogène engendré par g, et $f, f' \in \mathrm{Hom}(G, H)$, on a trivialement

$$\mathrm{ev}_g(ff') = (ff')(g) = f(g)f'(g) = \mathrm{ev}_g(f)\mathrm{ev}_g(f').$$

Exercice 2.37. Montrons le (i). Soit P le produit de tous les éléments de $(\mathbb{Z}/p\mathbb{Z})^\times$. On a $P \equiv (p-1)! \bmod p$. Regardons l'involution $f : x \mapsto a/x$ de $(\mathbb{Z}/p\mathbb{Z})^\times$ (noter $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$). Pour $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ tel que $\{x, a/x\}$ a deux éléments, on a $x \cdot a/x = a$. Sinon, on a $x^2 = a$. Si a n'est pas un carré, cela ne se produit pas, et donc en regroupant dans P les paires $\{x, a/x\}$ on a $P \equiv a^{\frac{p-1}{2}} \bmod p$. Si a est un carré, c'est le carré de deux éléments distincts u et $-u$ (car $p \neq 2$) et donc f a deux uniques points fixes, u et $-u$, et $\frac{p-3}{2}$ paires échangées. On a donc $P \equiv -u^2 a^{\frac{p-3}{2}} \equiv -a^{\frac{p-1}{2}}$. Dans tous les cas on a bien $(p-1)! \equiv P \equiv -(\frac{a}{p})a^{\frac{p-1}{2}}$. Pour $a = 1$, on retrouve $(p-1)! \equiv -1 \bmod p$. On en déduit alors $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}}$, puis la multiplicativité est immédiate car $(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}}$. On a montré le (ii).

Exercice 2.38. Montrons le (i). On a la congruence classique $(p-1)! \equiv -1 \bmod p$, vue par exemple à l'exercice précédent. On a aussi $(p-1)! = \prod_{i=1}^{(p-1)/2} i(p-i) \equiv x^2(-1)^{\frac{p-1}{2}} \bmod p$, où $x := (\frac{p-1}{2})!$. Pour $p \equiv 1 \bmod 4$, on a donc $x^2 \equiv -1 \bmod p$.

Montrons le (ii). On peut supposer $p > 3$. La relation de l'énoncé n'est autre que l'identité $4(X^2 + X + 1) = (2X + 1)^2 + 3$. Ainsi, -3 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si, et seulement si, $X^2 + X + 1$ a une racine dans $\mathbb{Z}/p\mathbb{Z}$. Mais on a $X^3 - 1 = (X - 1)(X^2 + X + 1)$ dans $(\mathbb{Z}/p\mathbb{Z})[X]$ et 1 n'est pas racine de $X^2 + X + 1$ dans $\mathbb{Z}/p\mathbb{Z}$ pour $p \neq 3$. On en déduit que $X^2 + X + 1$ a une racine dans $\mathbb{Z}/p\mathbb{Z}$ si, et seulement si, $(\mathbb{Z}/p\mathbb{Z})^\times$ a un élément d'ordre 3. Utilisant soit le fait que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique (Gauss), soit le lemme de Cauchy, c'est équivalent à $p \equiv 1 \bmod 3$.

Montrons le (iii). Par multiplicativité du symbole de Legendre, on a $(\frac{3}{p}) = (\frac{-3}{p})(\frac{-1}{p})$. Pour $p \equiv 1 \bmod 12$, ce signe vaut $1.1 = 1$, pour $p \equiv 5 \bmod 12$ il vaut $1 \cdot -1 = -1$, pour $p \equiv 7 \bmod 12$ il vaut $-1 \cdot 1 = -1$, et pour $p \equiv -1 \bmod 12$ il vaut $-1 \cdot -1 = 1$. On en déduit $(\frac{3}{p}) = 1$ si, et seulement si, $p \equiv \pm 1 \bmod 12$.

Montrons le (iv). Si $p \equiv 1 \bmod 8$, par Gauss il existe $\xi \in (\mathbb{Z}/p\mathbb{Z})^\times$ d'ordre 8. On a $\xi^8 = 1$ et $\xi^4 \neq 1$, donc $\xi^4 = -1$, puis $\xi^{-2} = -\xi^2$, et donc $(\xi + \xi^{-1})^2 = 2$. Ainsi, 2 est un carré dans $\mathbb{Z}/p\mathbb{Z}$.

Montrons le (v). Soit F un corps de cardinal p^2 contenant $\mathbb{Z}/p\mathbb{Z}$ comme dans l'énoncé. Par Gauss, le groupe $F^\times$ est cyclique d'ordre $p^2 - 1$. On a toujours $p^2 \equiv 1 \bmod 8$, et donc il existe un élément ξ d'ordre 8 dans $F^\times$. L'élément $u = \xi + \xi^{-1} \in F$ est de carré 2, car on a $\xi^2 = -\xi^{-2}$. Les deux racines de $X^2 - 2$ dans F sont donc $\pm u$. En particulier, 2 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si, et seulement si, on a $u \in \mathbb{Z}/p\mathbb{Z}$. Mais $\mathbb{Z}/p\mathbb{Z}$ est exactement l'ensemble des racines du polynôme $X^p - X$ dans F (une inclusion est évidente, et ce polynôme a au plus p racines). Il ne reste qu'à comparer $u^p = (\xi + \xi^{-1})^p = \xi^p + \xi^{-p}$ (car F est de carctéristique p) avec u. Si $p \equiv \pm 1 \bmod 8$, on a $\xi^p = \xi$ ou ξ^{-1}, et donc $u^p = u$, *i.e.* $u \in \mathbb{Z}/p\mathbb{Z}$, et donc 2 est un carré modulo p. Si $p \equiv \pm 3 \bmod 8$, on a $\xi^p = \xi^{\pm 3} = -\xi^{\pm 1}$, puis $u^p = -u \neq u$ et donc $u \notin \mathbb{Z}/p\mathbb{Z}$: 2 n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$.

Exercice 2.22. Soit H un sous-groupe de G. Alors $I = \cap_{g\in G} gHg^{-1}$ est un sous-groupe distingué de G. Supposons H d'indice fini, disons $G = \coprod_{i=1}^{n} g_i H$ avec les g_i dans G. On constate alors $gHg^{-1} = g_i H g_i^{-1}$ pour $g \in g_i H$, et donc $I = \cap_{i=1}^{n} g_i H g_i^{-1}$. On conclut par le (iii) de l'exercice précédent.

Exercice 2.23. Appliquons le théorème de Lagrange dans le groupe G/H (de cardinal n). Pour tout $g \in G$ on a $H = (gH)^n = g^n H$, et donc $g^n \in H$.

Exercice2.36. (i) L'inversion $x \mapsto x^{-1}, G \to G$, étant bijective, on a $|T^{-1}| = |T|$. Soit $g \in G$. En utilisant la bijectivité des applications $x \mapsto x^{-1}$ et $x \mapsto gx$, de G dans G, on a $|gT^{-1}| = |T^{-1}| = |T|$. Comme $|S| + |T| > |G|$, les parties gT^{-1} et S ne sont pas disjointes dans G, donc il existe $s \in S$ et $t \in T$ avsc $gt^{-1} = s$, puis $g = st$.

(ii) On se place dans le groupe *additif* $G = \mathbb{Z}/p\mathbb{Z}$. On prend $S = \{ax^2 \mid x \in \mathbb{Z}/p\mathbb{Z}\}$ et $T = \{bx^2 \mid x \in \mathbb{Z}/p\mathbb{Z}\}$. Pour $p = 2$ on a $|S| = |T| = 2$ et pour $p > 2$ on a $|S| = |T| = 1 + \frac{p-1}{2} > p/2$ car il y a $\frac{p-1}{2}$ carrés non nuls dans $(\mathbb{Z}/p\mathbb{Z})^\times$.

(iii) On suppose que G possède un sous-groupe S (distingué) d'indice 2, par exemple $G = \mathbb{Z}/n\mathbb{Z}$ avec n pair. On a $SS = S \neq G$ et $|S| + |S| = |G|$.

Exercice 2.25. (i) Soit une famille $\{x_i\}_{i\in I}$ d'éléments de G telle que $G = \coprod_{i\in I} x_i B$. On a $I \sim G/B$. Soit de même une famille $\{y_j\}_{j\in J}$ d'éléments de B avec $B = \coprod_{j\in J} y_j A$. On a clairement $G = \bigcup_{(i,j)\in I\times J} x_i y_j A$. On vérifie immédiatement que cette réunion est disjointe, ce qui montre que l'on a des bijections $G/A \sim I \times J \sim G/B \times B/A$.

(ii) On regarde l'application $f : A \to AB/B, a \mapsto aB$. Elle est surjective par définition. Si on a deux éléments a, a' de A avec $a \sim_{A\cap B} a'$, *i.e.* $a' = ab$ avec $b \in A \cap B$, alors on a $f(a') = a'B = abB = aB = f(a)$. Ainsi, f se factorise en une application $f' : A/A \cap B \to AB/B, aA \cap B \mapsto aB$. Cette application f' est encore clairement surjective. Elle est aussi injective : si on a $aB = a'B$, alors $a' \in aB$, puis $a' = ab$ avec $b \in B$, et même $b = a'a^{-1} \in A \cap B$. On a donc $aA \cap B = a'A \cap B$. On a montré que f' est bijective.

(iii) Soit $C = A \cap B$. Par le (ii), on a $A/C \sim AB/B \hookrightarrow G/B$, donc C est d'indice fini dans A. On a alors $|G/C| = |G/A|\,|A/C|$ par le (i), donc C est d'indice fini dans G.

(iv) Posons $C = A \cap B$. Par (iii) et (i) on a $|G/C| = |G/A|\,|A/C| = |G/B|\,|B/C|$. Comme $|G/A|$ et $|G/B|$ sont premiers entre eux, $|G/B|$ divise $|A/C|$. Mais on a aussi $A/C \sim AB/B \hookrightarrow G/B$ par (ii), donc on a $AB/B = G/B$, ou ce qui revient au même, $G = AB$.

Exercice 2.27. Pour le (i) on suppose $G/\mathrm{Z}(G)$ monogène engendré par $x\mathrm{Z}(G)$. On en déduit que pour tout $g \in G$, alors $g\mathrm{Z}(G)$ est de la forme $x^n\mathrm{Z}(G)$ pour $n \in \mathbb{Z}$. En particulier, G est engendré par x et $\mathrm{Z}(G)$. Comme x commute avec $\mathrm{Z}(G)$ et lui-même, cela entraîne $x \in \mathrm{Z}(G)$, puis $G = \mathrm{Z}(G)$ est abélien.

Pour $G = \mathrm{H}_8$, on a $\mathrm{Z}(G) = \{\pm 1\}$, puis $G/\mathrm{Z}(G)$ est d'ordre 4 engendré par les images i et j de I et J, qui vérifient $i^2 = j^2 = 1$ et $ij = ji$. On a donc $G/\mathrm{Z}(G) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (bien non monogène).

Exercice 2.28. Si on a $\mathrm{Aut}(G) = 1$, les automorphismes intérieurs de G sont triviaux, *i.e* $gxg^{-1} = x$ pour tout $g \in G$ et $x \in G$. Ainsi, G est abélien. Dans ce cas, l'application $g \mapsto g^{-1}$ est aussi un automorphisme. On a donc $g = g^{-1}$ pour tour $g \in G$, *i.e.* $g^2 = 1$. Cela montre que G est un $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel de manière naturelle (voir la discussion des p-groupes abéliens élémentaires au Chapitre 3), puis $G \simeq (\mathbb{Z}/2\mathbb{Z})^{(I)}$ en en considérant une base indexée par un certain ensemble I. Si on a $|I| \geqslant 2$, on peut écrire $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times H$. Mais l'application $(x, y, h) \mapsto (x + y, y, h)$ est un automorphisme non trivial de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times H$ (de carré identité) : absurde. On a donc $|I| \leqslant 1$, *i.e.* $|G| \leqslant 2$.

Exercice 2.30. Pour $\lambda \in \mathbb{Q}$ on pose $u(\lambda) = \begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Q})$. On a $u(\lambda)u(\lambda') = u(\lambda + \lambda')$, donc l'application $\mathbb{Q} \to \mathrm{GL}_2(\mathbb{Q}), \lambda \mapsto u(\lambda)$, est donc un morphisme de groupes. Il est injectif, et induit donc un isomorphisme $\mathbb{Z} \xrightarrow{\sim} u(\mathbb{Z}) = H$. On a

$$g\, u(\lambda)\, g^{-1} \;=\; u(2\lambda), \text{ pour } \lambda \in \mathbb{Q},$$

et donc $gHg^{-1} = u(2\mathbb{Z}) \subsetneq u(\mathbb{Z}) = H$. On a montré le (i). On constate que H' est le sous-groupe constitué des $u(\lambda)$ avec λ de la forme $n/2^m$ pour $n \in \mathbb{Z}$ et $m \geqslant 0$. C'est le plus petit sous-groupe de $\mathrm{GL}_2(\mathbb{Q})$ contenant $H = u(\mathbb{Z})$ et stable par $x \mapsto g^{-1}xg$.

Exercice 2.31. Regardons l'application $f : \prod_i G_i \to \prod_i G_i/H_i, (g_i) \mapsto (g_iH_i)$, Elle est clairement surjective, et un morphisme de groupes. Son noyau est l'ensemble des $(g_i) \in \prod_i G_i$ vérifiant $g_iH_i = H_i$ pour tout i, c'est-à-dire $g_i \in H_i$. On a donc $\ker f = \prod_i H_i$. Ainsi, ce dernier est distingué (ce qui justifie le (i)) et on conclut le (ii) par $G/\ker f \simeq \mathrm{Im} f$.

Exercice 2.40. Si p et q sont premiers impairs, la relation d'Eisenstein montre $(\frac{p}{q})\,((\frac{q}{p}) = (-1)^s$ où s est le nombre de points à coordonnées entières à l'intérieur du rectangle OP'S'Q'. En effet, les seuls points à coordonnées entières sur la diagonale $y = qx/p$ du rectangle OPSQ sont O et S car p et q sont premiers entre eux. On conclut le (i) car on a $s = \frac{p-1}{2}\frac{q-1}{2}$.

Montrons la relation d'Eisenstein. Comme q est premier à p, la multiplication par q est injective dans $\mathbb{Z}/p\mathbb{Z}$; on a donc $|R| = |X| = \frac{p-1}{2}$. Pour montrer le (ii) il suffit alors de voir que l'application de l'énoncé est injective. Soient $r, r' \in R$ de parités différentes et avec $r + r' = p$. On écrit $r \equiv qx \bmod p$ et $r' \equiv qx' \bmod p$ pour $x, x' \in X$. Il vient $x + x' \equiv 0 \bmod p$ car q est premier à p, puis $x + x' = p$, ce qui est absurde modulo 2.

Le (ii) entraîne $\prod_{x\in X} x \equiv \prod_{r\in R}(-1)^r r \bmod p$. Le (iii) s'en déduit car on a $\prod_{r\in R} r \equiv q^{\frac{p-1}{2}} \prod_{x\in X} x \bmod p$ (le produit sur X est non nul car p est premier).

Le (iv) est immédiat car x est pair et p est impair. On a déjà observé que la droite $y = qx/p$ ne contient aucun point (x, y) avec $y \in \mathbb{Z}$ et $x \in X$ car q est premier à p, on a donc $f = \sum_{x\in X}[qx/p]$ en dénombrant abscisse par abscisse, ce qui prouve le (v) d'après le (iv).

Pour le (vi), on raisonne abscisse par abscisse en observant qu'il y a $q - 1$ entiers compris strictement entre 0 et q, et $q - 1 \equiv 0 \bmod 2$. La symétrie $(x, y) \mapsto (p - x, q - y)$ identifie les points à coordonnées entières et d'abscisse paire intérieurs au triangle S'SQ", aux points à coordonnées entières et d'abscisse impaire intérieurs au triangle OP'S'.

Le (vii) se déduit alors de (v) et (vi). Le premier point du (viii) découle du (v) pour $q = 2$. Si $n \in \mathbb{Z}$ est un entier impair, notons $f(n)$ le nombre d'entiers pairs compris entre $n/2$ et n. On a $f(1) = 0$, $f(3) = 1$, $f(5) = 1$ et $f(7) = 2$. On observe de plus $f(n + 8) = f(n) + 2$. A insi, on a $f(n) \equiv \frac{n^2-1}{8} \bmod 2$.

Exercices du chapitre 3

Exercice 3.1. Observons d'abord que pour une suite d'entiers a_1, a_2, $\ldots$, a_n on a

$$a_1 \mid a_2 \mid \cdots \mid a_n \quad \Leftrightarrow \mathrm{v}_p(a_1) \leqslant \mathrm{v}_p(a_2) \leqslant \cdots \leqslant \mathrm{v}_p(a_n) \ \text{ pour tout } p \text{ premier},$$

où v_p désigne la valuation p-adique. Revenons au problème. On a $2025 = 3^4 5^2$. Les facteurs invariants possibles d'un groupe abélien d'ordre 5^2 sont $(5,5)$ et (5^2). Les facteurs invariants possibles d'un groupe abélien d'ordre 3^4 sont $(3,3,3,3)$, $(3,3,3^2)$, $(3,3^3)$, $(3^2,3^2)$ et (3^4). Les facteurs invariants possibles d'un groupe abélien d'ordre 2025 sont donc $(3,3,3\cdot 5,3\cdot 5)$, $(3,3\cdot 5,3^2\cdot 5)$, $(3\cdot 5,3^3\cdot 5)$, $(3^2\cdot 5,3^2\cdot 5)$, $(5,3^4\cdot 5)$, $(3,3,3,3\cdot 5^2)$, $(3,3,3^2\cdot 5^2)$, $(3,3^3\cdot 5^2)$, $(3^2,3^2\cdot 5^2)$ et $(3^4\cdot 5^2)$. Autrement dit, ce sont exactement

$$(3,3,15,15),(3,15,15),(3,15,45),(15,135),(45,45),(5,405),(3,3,3,75),(3,3,225),(3,675),(2025).$$

En particulier, il y a exactement 10 groupes abéliens non isomorphes d'ordre 2025.

Exercice 3.2. Soit $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Observons que les éléments d'ordre 4 de G sont $(0,\pm 1)$ et $(1,\pm 1)$. Les deux premiers (inverses l'un de l'autre) engendrent le même sous-groupe $H_1 = \{0\} \times \mathbb{Z}/4\mathbb{Z}$, et les deux second engendrent de même un même sous-groupe $\simeq \mathbb{Z}/4\mathbb{Z}$, à savoir $H_2 = \{(n \bmod 2, n \bmod 4) \mid n \in \mathbb{Z}\} \subset G$. Soit H un sous-groupe de G, que l'on peut supposer $\neq G$, donc d'ordre divisant 4. Si H contient un élément d'ordre 4, alors H contient le groupe cyclique engendré par cet élément, et coïncide donc avec H_1 ou H_2 pour des raisons de cardinalité. Sinon, tout élément h de H vérifie $2h = 0$, et donc H est inclus dans le sous-groupe $H_3 = \{(x,y) \mid x \in \mathbb{Z}/2\mathbb{Z}, y \in 2\mathbb{Z}/4\mathbb{Z}\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Mais H_2 est un 2-groupe abélien élémentaire, donc un $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel de dimension 2, et ses sous-groupes sont ses sous-espaces. Il a donc H_2 lui-même, ses trois droites, engendrées respectivement par $(1,0)$, $(0,2)$ et $(1,2)$, et le groupe trivial $\{0\}$. Le groupe G a donc exactement $1+3+4 = 8$ sous-groupes.

Exercice 3.3. Un tel groupe G est d'ordre 16. Comme on le suppose abélien, il est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^4$, $(\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ ou $\mathbb{Z}/16\mathbb{Z}$. Mais G n'a pas d'élément d'ordre 8. En effet, pour tout $g \in G$ on a $g^2 = 1$ dans G/H, donc $g^2 \in H$, puis $(g^2)^2 = g^4 = 1$ car $h^2 = 1$ pour tout $h \in H$. Cela élimine $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ et $G \simeq \mathbb{Z}/16\mathbb{Z}$. Les autres cas sont possibles : pour $G = (\mathbb{Z}/2\mathbb{Z})^4$ on peut prendre $H = \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\{0\}\times\{0\}$, pour $G = (\mathbb{Z}/2\mathbb{Z})^2\times\mathbb{Z}/4\mathbb{Z}$ on peut prendre $H = \mathbb{Z}/2\mathbb{Z}\times\{0\}\times 2\mathbb{Z}/4\mathbb{Z}$, et pour $G = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ on peut prendre $H = 2\mathbb{Z}/4\mathbb{Z} \times 2\mathbb{Z}/4\mathbb{Z}$.

Exercice 3.4. (i) On note G additivement. On a clairement $G[a] \subset G[b]$ si $a|b$. On a donc $G[n]$ et $G[m]$ inclus dans $G[mn]$. Par Bezout, on a u, v dans $\mathbb{Z}$ avec $1 = un + vm$. Supposons $x \in G$ avec $nx = 0$ et $mx = 0$. On en déduit $x = unx + vmx = 0$. On a donc $G[n] \cap G[m] = \{0\}$. De plus, pour tout x dans G on a $x = unx + vmx$. Si x est dans $G[mn]$, on a alors $nx \in G[m]$ et $mx \in G[n]$, puis $x \in G[m] + G[n]$. On a monté $G[mn] = G[m] \oplus G[n]$. Pour le (ii), imiter la démonstration de l'Exercice 3.1.

Exercice 3.5. Soient $a_1, \ldots, a_n$ les facteurs invariants de G. Soit d un diviseur de G. En utilisant la première observation de la solution de l'Exercice 3.1 il n'est pas difficile de voir que l'on peut trouver, pour tout $i = 1, \ldots, n$, un diviseur d_i de a_i, tels que $d = d_1 d_2 \cdots d_n$. On a $G \simeq \prod_i C_i$ avec C_i cyclique d'ordre a_i. On sait que C_i a un sous-groupe (cyclique) D_i d'ordre d_i. On en déduit que le sous-groupe $\prod_i D_i$ convient.

Exercice 3.6. Si G est abélien p-élémentaire, on a vu que G est un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel $G^\sharp$ de manière naturelle. Il est équivalent de se donner un automorphisme de G et un automorphisme de cet espace vectoriel $G^\sharp$. On a donc $\mathrm{Aut}(G) = \mathrm{GL}(G^\sharp) \simeq \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$. Les sous-groupes caractéristiques de G sont les sous-espaces vectoriels de $G^\sharp$ stables par toute application linéaire inversible : ce sont donc $\{0\}$ et $G^\sharp$.

Exercice 3.7. Supposons $g^2 = 1$ pour tout $g \in G$, *i.e.* $g^{-1} = g$ pour tout $g \in G$. Pour $g, h \in G$ on a $gh = g^{-1}h^{-1} = (hg)^{-1} = hg$. Donc G est commutatif : il est abélien 2-élémentaire. On conclut par le cours.

Exercice 3.8. (i) On sait que si k est un corps et $N \in \mathrm{M}_n(k)$ est nilpotente, on a $N^n = 0$. On en déduit que pour $p \geqslant n$ et $N \in \mathrm{M}_n(\mathbb{Z}/p\mathbb{Z})$ on a $(1+N)^p = 1 + N^p = 1$. Pour le (ii), on prend $G = \mathrm{U}_3(\mathbb{Z}/p\mathbb{Z})$ et $p \geqslant 3$. On a $|G| = p^3$, et même

$$|\mathrm{U}_n(\mathbb{Z}/p\mathbb{Z})| = p^{1+2+\cdots+n-1} = p^{\frac{n(n-1)}{2}}$$

pour tout $n \geqslant 1$. On a $g^p = 1$ pour tout $g \in G$ par le (i). Il est facile de voir que $\mathrm{U}_3(k)$ n'est jamais commutatif (pour k un corps), et même que le centre de $\mathrm{U}_n(k)$ est constitué des matrices $(m_{i,j}) \in \mathrm{U}_n(k)$ avec $m_{i,j} = 0$ pour tout $i \leqslant j$ vérifiant soit $i > 1$, soit $j < n$.

Exercice 3.9. (a) Faux : $\{2, 3\}$ est une famille génératrice minimale de $\mathbb{Z}$, mais elle n'est pas libre car on a $3 \cdot 2 - 2 \cdot 3 = 0$.

(b) Faux : $\{2\}$ est une famille libre maximale non génératrice de $\mathbb{Z}$. En effet, pour tout $a, b \in \mathbb{Z}$ on a $ba - ab = 0$, donc les familles libres de $\mathbb{Z}$ ont au plus un élément.

(c) Vrai. On a vu en cours qu'un groupe abélien de type fini sans torsion est libre.

(d) Vrai (plus difficile). Si $e_1, \ldots, e_n$ est une famille libre de G, regardons $H = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \cdots \oplus \mathbb{Z}e_n$. Aucun élément non nul de H n'est d'ordre fini : on a donc $H \cap G_{\mathrm{tor}} = \{0\}$. On en déduit que les images des e_i dans G/G_{tor} forment encore une famille libre de G/G_{tor}. Mais on a $G/G_{\mathrm{tor}} \simeq \mathbb{Z}^m$ où m est le rang de G. Il ne reste qu'à montrer qu'une famille libre $f_1, \ldots, f_n$ de $\mathbb{Z}^m$ a au plus m éléments. Pour cela, on voit $\mathbb{Z}^m$ comme inclus dans $\mathbb{Q}^m$. On constate que les f_i sont $\mathbb{Q}$-linéairement indépendants. En effet, si on a $\sum_{i=1}^n \lambda_i f_i = 0$ avec $\lambda_i \in \mathbb{Q}$, on écrit $\lambda_i = p_i/q$ avec $q \geqslant 1$ et les p_i dans $\mathbb{Z}$, on en déduit en multipliant par q que l'on a $\sum_{i=1}^n p_i f_i = 0$. Par $\mathbb{Z}$-liberté des f_i on a donc $p_i = 0$ pour tout i, puis $\lambda_i = 0$ pour tout i. Mais dans le $\mathbb{Q}$-espace vectoriel $\mathbb{Q}^m$, les familles $\mathbb{Q}$-libres ont au plus m éléments. On a donc $n \leqslant m$.

(e) Faux. Soient $p_1, \ldots, p_n$ des nombres premiers distincts. On pose $q_i = \prod_{j \neq i} p_j$. Alors les q_i sont premiers entre eux dans leur ensemble, mais aucun sous-ensemble strict des q_i n'a cette propriété. Ainsi, $q_1, \ldots, q_n$ est une famille génératrice minimale de $\mathbb{Z}$.

(f) Faux : $\{1\}$ et $\{2, 3\}$ sont deux familles génératrices minimales de $\mathbb{Z}/6\mathbb{Z}$.

Exercice 3.10. Supposons que $h_1, \ldots, h_m$ engendrent H et que $x_1H, \ldots, x_nH$ engendrent G/H, avec $x_i \in G$. Alors $\{x_1, \ldots, x_n, h_1, \ldots, h_m\}$ engendre G. En effet, soit $\pi : G \to G/H$ la projection canonique. Pour $g \in G$, $\pi(g)$ est un certain mot en les x_iH et les $(x_iH)^{-1} = x_i^{-1}H$. Soit $g' \in \langle x_1, \ldots, x_n \rangle$ ce même mot, mais en les x_i et les $x_i^{\pm 1}$. On a donc $\pi(g') = \pi(g)$. Mais alors $(g')^{-1}g$ est dans $H = \langle h_1, \ldots, h_m \rangle$. On a donc montré $G \subset \langle x_1, \ldots, x_n \rangle \langle h_1, \ldots, h_m \rangle$.

Exercice 3.11. (i) C'est le cas $G = \mathbb{Z}g$ monogène (disons non nul). Considérons

$$\varphi : \mathbb{Z} \to G, m \mapsto mg.$$

C'est un morphisme surjectif. Si H est un sous-groupe de G, on a $H = \varphi(\varphi^{-1}(H))$ et $\varphi^{-1}(H)$ est un sous-groupe de $\mathbb{Z}$. On a donc $\varphi^{-1}(H) = d\mathbb{Z}$ pour un certain $d \geqslant 0$, puis $H = \varphi(d\mathbb{Z}) = \mathbb{Z}dg$ est monogène, et donc $\min(H) \leqslant 1 = \min(G)$.

(ii) Posons $n = \min(G)$ et choisissons $g_1, \ldots, g_n$ des générateurs de G. On pose $g = g_1$. Alors $G' = G/\langle g \rangle$ est engendré par les images $g_i\langle g \rangle$ des g_i dans G'. Mais comme celle de g_1 est triviale, G' est engendré par les $g_i\langle g \rangle$ avec $i > 1$. On a donc $\min(G') \leqslant n-1 < \min(G)$.

(iii) On raisonne par récurrence sur $\min(G)$, le cas $\min(G) = 0$ étant évident. Supposons $\min(G) \geqslant 1$. Regardons le morphisme $H \to G'$ de l'énoncé. Soient H' son image et $H'' = H \cap \langle g \rangle$ son noyau. Par l'exercice précédent, on a $\min(H) \leqslant \min(H') + \min(H'')$.

Par le (i), on a $\min(H'') \leqslant 1$ car $H'' \subset \mathbb{Z}g$. Par récurrence et le (ii), on a $\min(H') \leqslant \min(G') < \min(G)$. On a donc $\min(H) \leqslant \min(G)$.

(iv) Un sous-groupe H de $\mathbb{Z}^n$ vérifie $\min(H) \leqslant n$ par ce que l'on a montré. Il est donc de type fini. Il est aussi sans torsion. Il est donc libre par le cours, *i.e.* $H \simeq \mathbb{Z}^m$. On conclut car $\min(\mathbb{Z}^m) = m$.

Exercice 3.12. Notons a et b les matrices respectives de l'énoncé, et $G = \langle a, b\rangle$. On a

$$a^{-n}ba^n = \begin{bmatrix} 1 & \frac{1}{2^n} \\ 0 & 1 \end{bmatrix}.$$

On en déduit que G contient toutes les matrices de la forme $\mathrm{m}(x) := \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$ avec x dans

$$\mathbb{Z}[1/2] = \{m/2^n \mid m \in \mathbb{Z},\ n \geqslant 0\}.$$

Mais ces matrices forment un sous-groupe de G isomorphe à $(\mathbb{Z}[1/2], +)$, via $x \mapsto \mathrm{m}(x)$, et ce dernier est un sous-groupe de $\mathbb{Q}$ qui n'est pas de type fini (*dénominateurs non bornés*).

Exercice 3.13. On sait que le groupe $H = (\mathbb{Z}/2\mathbb{Z})^3$ vérifie $\min(H) = 3$. Mais par Cayley, ce groupe est isomorphe à un sous-groupe de $G = \mathrm{S}_8$. Mais nous verrons bientôt que pour $n > 2$, le groupe S_n est non abélien et engendré par $(1\,2)$ et $(1\,2\,3\,\ldots\,n)$, donc $\min(\mathrm{S}_n) = 2$.

Exercice 3.15. (i) est une vérification immédiate. Montrons (ii). Posons $n = |G|$. On a $g^n = 1$ pour tout $g \in G$ par Lagrange. Comme $X^n - 1$ est à racines simples dans $\mathbb{C}[X]$, chaque endomorphisme $g \in G$ est diagonalisable (de valeurs propres des racines n-èmes de l'unité). Comme G est commutatif, ses éléments sont codiagonalisables. Soit $v \in V - \{0\}$ un vecteur propre commun : pour tout $g \in G$ il existe $\lambda_g \in \mathbb{C}^\times$ avec $gv = \lambda_g v$. On a d'une part $g'(gv) = g'(\lambda_g v) = \lambda_g g'v = \lambda_g \lambda'_g v$, et d'autre part $g'(gv) = (g'g)(v) = \lambda_{gg'}v$, donc $\lambda_{gg'} = \lambda_g\lambda'_g$ pour tout $g, g' \in G$ (comme $v \neq 0$). Ainsi, $\chi(g) := \lambda_g$ définit un élément χ de $\widehat{G}$, et on a $v \in V_\chi$. On a donc $V = \sum_\chi V_\chi$ par codiagonalisabilité. Reste à voir que la somme est directe. Supposons que l'on a $v_1 + \cdots + v_n = 0$ avec $v_i \neq 0$, $v_i \in V_{\chi_i}$, $\chi_i \neq \chi_j$ pour $i \neq j$, et n minimal. On a clairement $n > 1$. En appliquant $g \in G$ à $v_1 + \cdots + v_n = 0$ on a $\sum_i \chi_i(g)v_i = 0$, puis $\sum_i(\chi_i(g) - \chi_1(g))v_i = 0$. Par minimalité de n, on a donc $\chi_i(g) = \chi_1(g)$ pour tout g, *i.e.* $\chi_i = \chi_1$, une contradiction.

Exercice 3.16. (i) Soit χ un caractère de $G_1 \times G_2$. On définit $\chi_1 : G_1 \to \mathbb{C}^\times$ et $\chi_2 : G_2 \to \mathbb{C}^\times$ par $\chi_1(g) = \chi(g, 1)$ et $\chi_2(g) = \chi(1, g)$. Ce sont deux caractères. On a donc défini une application $\widehat{G_1 \times G_2} \to \widehat{G_1} \times \widehat{G_2}$, $\chi \mapsto (\chi_1, \chi_2)$. C'est clairement un morphisme de groupes. La formule $\chi(g_1, g_2) = \chi((g_1, 1)(1, g_2)) = \chi(g_1, 1)\chi(1, g_2) = \chi_1(g_1)\chi_2(g_2)$ montre qu'il est injectif. Il est surjectif, car si $\psi_i : G_i \to \mathbb{C}^\times$ sont des caractères pour $i = 1, 2$, alors $\chi(g_1, g_2) := \psi_1(g_1)\psi_2(g_2)$ est un caractère de $G_1 \times G_2$ avec $\chi_i = \psi_i$ pour $i = 1, 2$.

(ii) Soit G un groupe abélien fini. On sait qu'il existe un isomorphisme $G \simeq \prod_{i=1}^n \mathbb{Z}/a_i\mathbb{Z}$ avec $a_1, \ldots, a_n$ des entiers $\geqslant 1$. On a donc $\widehat{G} \simeq \prod_{i=1}^n \widehat{\mathbb{Z}/a_i\mathbb{Z}}$ par le (i). Mais on a vu en cours que pour $m \geqslant 1$ on a $\widehat{\mathbb{Z}/m\mathbb{Z}} \simeq \mu_m \simeq \mathbb{Z}/m\mathbb{Z}$. On a donc bien $\widehat{G} \simeq G$.

Exercice 3.17. (i) Dire que ι_G est injective signifie que pour tout $g \neq 1$, il existe $\chi \in \widehat{G}$ tel que $\chi(g) \neq 1$. Fixons donc $g \neq 1$. L'étude des caractères d'un groupe cyclique montre qu'il existe $\psi : \langle g\rangle \to \mathbb{C}^\times$ avec $\psi(g) \neq 1$. On conclut en considérant un prolongement χ de ψ à G tout entier. L'injectivité de ι_G entraîne sa bijectivité, car on a $|\widehat{\widehat{G}}| = |\widehat{G}| = |G|$.

(ii) La bijectivité de ι montre que les caractères de $\widehat{G}$ sont les $\chi \mapsto \chi(g)$ avec $g \in G$. Les relations d'orthogonalité s'écrivent donc $\frac{1}{|G|}\sum_{\chi \in \widehat{G}} \chi(g)\overline{\chi}(h) = 0$ pour $h \neq g$, 1 pour $h = g$.

Exercice 3.18. (i) G est un 2-groupe abélien élémentaire, ou ce qui revient au même, un $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel de dimension 2. Pour tout $v \in G$ non nul, il existe une unique forme linéaire $v^* : G \to \mathbb{Z}/2\mathbb{Z}$ qui vaut 0 sur v et qui est non nulle. En effet, v^* vaut automatiquement 1 sur les deux autres vecteurs non nuls, qui sont de la forme w et $w + v$. On définit aussi 0^* comme étant la forme linéaire nulle sur G. On constate que $G \to \mathrm{Hom}(G, \mathbb{Z}/2\mathbb{Z}), v \mapsto v^*$ est un isomorphisme de $\mathbb{Z}/2\mathbb{Z}$-espace vectoriels. En effet, seule la linéarité est non évidente, mais pour $u, v \in G$ on a bien $(u + v)^\star = u^* + v^*$: c'est clair si $u = v$, et si $u \neq v$ c'est vrai aussi car on a $u^*(v) = v^*(u) = 1$ (!). Ainsi, l'application $G \to \widehat{G}, u \mapsto (-1)^{u^*}$ est un isomorphisme de groupes. Je le qualifierais de naturel car on n'a utilisé aucun choix particulier pour le définir.

(ii) L'existence de χ_g est du cours. Un φ comme dans l'énoncé est unique, car c'est un morphisme et qu'il est donné sur un générateur de G. Soit g un générateur du groupe cyclique G (d'ordre n). Pour tout $k \in (\mathbb{Z}/n\mathbb{Z})^*$, on sait que g^k est encore un générateur de G, on a donc d'une part $\varphi(g^k) = \chi_{g^k}$ et d'autre part $\varphi(g^k) = \varphi(g)^k = (\chi_g)^k$ (car φ est un morphisme). En évaluant ces égalités en l'élément g^k, on a donc $\varphi(g^k)(g^k) = \chi_{g^k}(g^k) = e^{2i\pi/n}$ et $\varphi(g^k)(g^k) = (\chi_g(g^k))^k = \chi_g(g)^{k^2} = e^{2i\pi k^2/n}$, ce qui conclut.

(iii) On a donc $k^2 \equiv 1 \bmod n$ pour tout k premier à n. Ainsi, $(\mathbb{Z}/n\mathbb{Z})^\times$ est un 2-groupe abélien élémentaire. En particulier, l'indicatrice d'Euler $\varphi(n)$ est une puissance de 2, ce qui force $n = 2^m$ ou $n = 3 \cdot 2^m$ avec $m \geqslant 0$. Mais alors 5 est premier à n, et $5^2 \equiv 1 \bmod n$, donc n divise $25 - 1 = 24$.

(iv) Supposons donc G cyclique d'ordre n avec $n \mid 24$. Fixons un générateur g de G. Pour $k, k' \in \mathbb{Z}$ on définit $\varphi(g^k) \in \widehat{G}$ par $\varphi(g^k)(g^{k'}) = e^{2i\pi kk'/n}$. On constate que c'est bien défini (le résultat ne dépend que de $k \bmod n$ et $k' \bmod n$). Par définition, on a $\varphi(g^k g^q) = \varphi(g^{k+q})$: φ est un morphisme $G \to \widehat{G}$. De plus, caractère le $\varphi(g^k)$ de G vaut $e^{2i\pi k^2/n}$ en g^k. On conclut car pour $n|24$, on a $k^2 \equiv 1 \bmod n$ pour tout k premier à n. (C'est la réciproque de l'observation du (ii), plus facile.)

Exercice 3.19 (i) (C'est assez tautologique mais on vérifie quand même les détails) Vérifions la bilinéarité de b_f. Fixons $g \in G$. L'application $h \mapsto \mathrm{b}_f(g, h) = f(g)(h), G \to \mathbb{C}^\times$ est un morphisme : c'est le caractère $f(g)$. L'application $h \mapsto \mathrm{b}_f(h, g) = f(h)(g)$ est aussi un morphisme car f est un morphisme de groupes. Donc $f \mapsto \mathrm{b}_f$ est bien définie (c'est même un morphisme de groupes si l'on munit $\mathrm{Bil}(G)$ de la loi évidente). Elle est trivialement injective. Elle est aussi surjective car pour $b \in \mathrm{Bil}(G)$, posant $f(g)(h) = b(g, h)$ alors $g \mapsto f(g)$ est un morphisme $G \to \widehat{G}$ vérifiant $b = \mathrm{b}_f$.

(ii) Il est équivalent de dire que f est injective, et que b_f est non dégénérée à droite. Comme $\widehat{G}$ et G ont même cardinal, f est injective si et seulement si f est bijective. Cela montre $(a) \iff (b)$. On dispose aussi du morphisme $f' : G \to \widehat{G}$, $g \mapsto (h \mapsto f(h)(g) = \mathrm{b}_f(h, g))$. Il est injectif si, et seulement si, b_f est non dégénéré à gauche. Le noyau de f' est l'ensemble des éléments $g \in G$ tels que $f(h)(g) = 1$ pour tout $h \in G$. S'il possède un élément non trivial g, cela veut dire que tout les caractères dans $f(G)$ sont triviaux sur h. Mais par prolongement des caractères il existe $\chi \in \widehat{G}$ tel que $\chi(h) \neq 1$, donc f n'est pas surjective. Cela montre $(a) \implies (c)$. Enfin, si f' est injective, elle est surjective, donc tout caractère de G est de la forme $h \mapsto f(h)(g)$ pour un certain $g \in G$. Comme tous ces caractères sont triviaux sur $\ker f$, cela entraîne que f est injective, donc bijective.

Exercice 3.20. (i) f est naturel si, et seulement si, pour tout $g \in G$ on a $f(\alpha(g)) = f(g) \circ \alpha^{-1}$, soit encore si pour tout g et h dans G on a $f(\alpha(g))(h) = f(g)(\alpha^{-1}(h))$, *i.e.* $\mathrm{b}_f(\alpha(g), h) = \mathrm{b}_f(g, \alpha^{-1}(h))$, et on conclut par la bijection $h \mapsto \alpha(h)$.

(ii) Pour le (iv), l'isomorphisme construit satisfait par définition $\mathrm{b}_f(g^a, g^b) = e^{2i\pi ab/n}$. Mais comme G est cyclique d'ordre n, on sait que $(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(G), k \mapsto (x \mapsto x^k)$,

est un isomorphisme. On conclut car pour tout $k \in (\mathbb{Z}/n\mathbb{Z})^\times$ on a $k^2 \equiv 1 \bmod n$ et donc $\mathrm{b}_f(g^{ak}, g^{bk}) = e^{2i\pi k^2 ab/n} = \mathrm{b}_f(g^a, g^b)$. Considérons maintenant l'exemple du (i). On rappelle que l'on voit G comme un $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel de dimension 2. On a $\mathrm{b}_f(u, v) = (-1)^{u^*(v)}$ par définition. On constate que la forme $\mathbb{Z}/2\mathbb{Z}$-bilinéaire $(u, v) \mapsto u^*(v) \in \mathbb{Z}/2\mathbb{Z}$ est alternée et non nulle. Comme on est sur $(\mathbb{Z}/2\mathbb{Z})^2$, il n'y a qu'une seule telle forme, qui coincide nécessairement avec le déterminant (dans n'importe quelle base) ! On a $\mathrm{Aut}(G) \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$, donc tout automorphisme α de G vérifie bien $\mathrm{b}_f(\alpha(g), \alpha(h)) = \det(\alpha)\mathrm{b}_f(g, h) = \mathrm{b}_f(g, h)$.

(iii) Supposons que f est un isomorphisme naturel entre G et son dual. Soit $k \in \mathbb{Z}$ premier à l'exposant e de G. Alors $x \mapsto kx$ est un automorphisme de G. On en déduit $k^2x = x$ pour tout x dans G. En effet, soit on applique directement la définition d'isomorphisme naturel $G \to \widehat{G}$ à cet automorphisme, soit on écrit $\mathrm{b}_f(kx, ky) = \mathrm{b}_f(x, y)$ pour tout $x, y \in G$, puis $\mathrm{b}_f(kx, y)^k = \mathrm{b}_f(k^2x, y) = \mathrm{b}_f(x, y)$ pour tout x, y dans G, et on conclut par non dégénérescence de b_f. On en déduit que l'exposant e de G vérifie $k^2 \equiv 1 \bmod e$ pour tout k premier à e, donc e divise 24.

(iv) On a $G = G[n] \oplus G[m]$ (voir l'Exercice 3.4). L'application naturelle $\widehat{G} \to \widehat{G[n]} \times \widehat{G[m]}, \chi \mapsto (\chi_{|G[n]}, \chi_{|G[m]})$, est bijective par l'argument de l'Exercice 3.16. De plus, on sait que si G' est un autre groupe abélien, tout (iso-)morphisme $G \to G'$ induit par restriction à $G[n]$ un (iso-)morphisme $G[n] \to G'[n]$ (idem avec n remplacé par m, bien entendu). Ainsi, l'application $\mathrm{Aut}(G) \to \mathrm{Aut}(G[n]) \times \mathrm{Aut}(G[m]), \varphi \mapsto (\varphi_{|G[n]}, \varphi_{|G[m]})$, est bijective. De même, l'application naturelle $\mathrm{Hom}(G, \widehat{G}) \to \mathrm{Hom}(G[n], \widehat{G[n]}) \times \mathrm{Hom}(G[m], \widehat{G[m]})$ est bijective. Le résultat en découle.

(v) Tout élément c de G s'écrit de manière unique $c = c_1 + \cdots + c_n$ avec $c_i \in C_i$. Fixons $1 \leqslant i \leqslant n$. L'application $\alpha_i : G \mapsto G$ envoyant $c \in G$ sur l'unique élément c' tel que $c'_i = -c_i$ et $c'_j = c_j$ pour $j \neq i$ est clairement un automorphisme de G (*inversion à la place* i). Pour $j \neq i$, on a donc $f(x_i, x_j) = f(\alpha_i(x_i), \alpha_i(x_j)) = f(-x_i, x_j) = f(x_i, x_j)^{-1}$, puis $f(x_i, x_j)^2 = 1$.

(vi) Comme $e_i \,|\, e_n$ pour $i < n$, il existe un morphisme de groupes $C_n \to C_i$ envoyant x_n sur x_i. Notons $\beta_i : G \to G$ l'application envoyant $c = \sum_{i=1}^n c_i$ sur l'unique élément c' vérifiant $c'_j = c_j$ pour $j < n$, et $c'_n = c_n + \varphi(c_n)$. C'est clairement un morphisme de groupes, manifestement injectif, donc bijectif : c'est un automorphisme (c'est une *transvection* !). Il vérifie $\beta_i(x_j) = x_j$ pour $j < n$ et $\beta_i(x_n) = x_n + x_i$. On a donc, toujours pour $j < n$,

$$f(x_j, x_n) = f(\beta_i(x_j), \beta_i(x_n)) = f(x_j, x_n + x_i) = f(x_j, x_n)f(x_j, x_i),$$

puis $f(x_j, x_i) = 1$.

(vii) Si $e_1 = 2$, on peut trouver un morphisme de groupes $C_1 \to C_n$ envoyant x_1 sur l'élément y (car $2y = 0$). En procédant comme au (vi), il existe donc un automorphisme γ de G envoyant x_1 sur $x_1 + y$, et x_i sur x_i pour $i > 1$. On a $f(x_1, x_n) = f(\gamma(x_1), \gamma(x_n)) = f(x_1 + y, x_n) = f(x_1, x_n)f(y, x_n)$ puis $f(y, x_n) = 1$.

(viii) Si b est non dégénérée, alors G est naturellement isomorphe à son dual par le (i) et l'Exercice 3.19, et donc l'exposant e_n de G divise 24 par le (iii).

(ix) Pour $i < n$, on a $f(x_i, x_j) = \pm 1$ pour tout j par les (v) et (vi). On a donc $1 = f(2x_i, x_j) = f(x_i, x_j)^2$ pour tout j, puis $f(2x_i, g) = 1$ pour tout g dans G, et donc $2x_i = 0$ car f est non dégénérée. Cela montre $e_i = 2$ pour $i < n$ (et donc e_n est pair.) Supposons $n > 2$. Alors l'un au moins des trois éléments $f(x_1, x_n), f(x_2, x_n)$ et $f(x_1 + x_2, x_n) = f(x_1, x_n)f(x_2, x_n)$ vaut 1, car $f(x_i, x_n) = \pm 1$ par (v). Soit $u \in \{x_1, x_2, x_1 + x_2\}$ avec $f(u, x_n) = 1$. Le (vi) montre alors $f(u, x_i) = 1$ pour tout i, puis $u = 0$ par non dégénérescence : absurde. Si on a $n \equiv 0 \bmod 4$, alors y est un carré dans C_n, et donc

$f(x_i, y) = 1$ pour $i < n$ par le (v). Mais on a aussi $f(x_n, y) = 1$ par le (vii), et donc $y = 0$ par non dégénérescence. Absurde.

(x) Supposons G isomorphe à son dual. Si G est cyclique, il est d'ordre divisant 24 par le (iii), et réciproquement on a vu que les groupes cycliques d'un tel ordre conviennent. Supposons G non cyclique. La question (ix) montre que ses facteurs invariants sont $(2, e)$ avec $e|24$ et e non multiple de 4. On a donc soit $e = 2$ et $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, soit $e = 6$ et $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Autrement dit, on a $G[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $G[3] \simeq \mathbb{Z}/3\mathbb{Z}$. Ces exemples conviennent par le (ii) et (iv).

Exercice 3.21. L'application de l'énoncé est un morphisme de groupes. Il suffit de voir que son noyau est trivial. Soit $g \in G$ non trivial. Si g est d'ordre fini, on peut trouver un caractère χ du groupe cyclique $\langle g \rangle$ avec $\chi(g) \neq 1$ par le cours. Si g est d'ordre infini, c'est aussi vrai, et même plus facile : pour n'importe quel $x \in \mathbb{C}^\times$, $\chi(g^k) := x^k$ définit un caractère de $\langle g \rangle$, avec $\chi(g) \neq 1$ dès que $x \neq 1$. Comme $\mathbb{C}^\times$ est divisible, on peut prolonger χ en un caractère de G : l'application de l'énoncé est injective. Cela prouve le (i). Pour le (ii), on observe que si D est divisible, il en va de même du groupe produit D^I pour tout ensemble I.

Exercice 3.22. Pour tout entier $n \geqslant 1$, le morphisme $x \mapsto nx$ est bijectif. Pour $\lambda \in \mathbb{Q}$ et $x \in G$, il y a alors un sens à considérer "λx" dans G. Pour le voir, observons que si on a $p/q = p'/q'$ dans $\mathbb{Q}$, avec p, p', q, q' dans $\mathbb{Z}$ et $q, q' \geqslant 1$, et si y et y' sont les uniques éléments de G vérifiant $qy = px$ et $q'y = p'x$, alors $y = y'$. En effet, on a $pq' = qp'$ puis

$$qq'y' = qp'x = q'px = q'qy,$$

et donc $y = y'$ par bijectivité de la multiplication par qq' dans G. Au final, pour tout $\lambda \in \mathbb{Q}$ et tout $x \in G$, il existe un unique élément que l'on notera $\lambda x \in G$ tel que pour toute écriture $\lambda = p/q$ avec $p, q \in \mathbb{Z}$ et $q \geqslant 1$ on ait $q\lambda x = px$. Il est alors trivial de vérifier que $\mathbb{Q} \times G \to G, (\lambda, x) \mapsto \lambda x$, est une structure de $\mathbb{Q}$-espace vectoriel sur G dont le groupe abélien sous-jacent est G. Le (i) s'en déduit en considérant une base de ce $\mathbb{Q}$-espace vectoriel. Pour le (ii), on applique l'Exercice 1.18 Chap. 1.

Exercice 3.23. (i) Montrons $A_{\mathrm{tor}} = \prod'_p \mathbb{Z}/p\mathbb{Z}$ (produit restreint). Autrement dit, un élément $x = (x_p)$ avec $x_p \in \mathbb{Z}/p\mathbb{Z}$ est d'ordre fini si, et seulement si, on a $x_p = 0$ pour tout p assez grand. En effet, si $x_p = 0$ pour $p \geqslant N$, et si on pose $n = \prod_{p \leqslant N}$, on a $nx = (nx_p) = 0$. Réciproquement, si on a $n \geqslant 1$ et $nx = 0$, alors on a $nx_p = 0$ pour tout p. Comme n est inversible dans l'anneau $\mathbb{Z}/p\mathbb{Z}$ pour $p > n$, on a donc $x_p = 0$ pour $p > n$.

(ii) Soit n un entier $\geqslant 1$. Vérifions que la multiplication par $n : A/A_{\mathrm{tor}} \to A/A_{\mathrm{tor}}, x + A_{\mathrm{tor}} \mapsto nx + \mathrm{A}_{\mathrm{tor}}$, est surjective. Soit $x \in A$. Comme la multiplication par n est surjective sur $\mathbb{Z}/p\mathbb{Z}$ pour tout $p > n$, il existe $y \in A$ tel que $y_p = nx_p$ pour $p > n$. Mézalor $y - nx$ a toutes ses p-coordonnées nulles pour $p > n$, et donc $y - nx \in A_{\mathrm{tor}}$ par le (i).

(iii) Pout tout groupe abélien G, le groupe G/G_{tor} est sans torsion. En effet, soient $\pi : G \to G/G_{\mathrm{tor}}$ la projection canonique et $x \in G/G_{\mathrm{tor}}$ de torsion. Il existe $n \geqslant 1$ avec $x^n = 1$ dans G/G_{tor}. Soit $y \in G$ avec $\pi(y) = x$. On a $1 = x^n = \pi(y^n)$ donc $y^n \in \ker \pi = G_{\mathrm{tor}}$. Ainsi, il existe $m \geqslant 1$ avec $(y^n)^m = 1$. Mais alors $y^{nm} = 1$ avec $nm \geqslant 1$ et donc $y \in G_{\mathrm{tor}}$ et $x = \pi(y) = 1$. Ainsi, $G = A/A_{\mathrm{tor}}$ est sans torsion, et divisible par le (ii). Autrement dit, il est uniquement divisible : les applications $G \to G, x \mapsto x^n$, sont bijectives pour $n \geqslant 1$. Par l'Exercice 3.22, on a donc $G \simeq \mathbb{Q}^{(I)}$ pour un certain ensemble I, avec en outre $I \sim G$ si G est indénombrable. La projection sur une coordonnée répond à la question.

(iv) On utilise les exercices sur la cardinalité du Chapitre 1. On a $\{0, 1\}^{\mathbb{N}}$ qui s'injecte dans A, et A qui s'injecte dans $\mathbb{N}^{\mathbb{N}}$. Mais $\{0, 1\}^{\mathbb{N}}$ et $\mathbb{N}^{\mathbb{N}}$ sont tous deux équipotents à $\mathbb{R}$ (Cantor, Exercice 1.11 Chap. 1.). On a donc $A \sim \mathbb{R}$ par Cantor-Bernstein. Mais A_{tor} est dénombrable : c'est une réunion dénombrable d'ensemble finis (par exemple des

$\prod_{p\leqslant n}\mathbb{Z}/p\mathbb{Z}\times\{0\}$ pour $n\geqslant 1$). Par Lagrange, on a aussi $A\sim A/A_{\mathrm{tor}}\times A_{\mathrm{tor}}$, et donc $\mathbb{R}\sim A/A_{\mathrm{tor}}\times\mathbb{N}$. On en déduit d'abord que A/A_{tor} est infini, puis $A/A_{\mathrm{tor}}\times\mathbb{N}\sim A/A_{\mathrm{tor}}$, et donc $A/A_{\mathrm{tor}}\sim\mathbb{R}$. Comme $\mathbb{R}$ est indénombrable, on a donc $A/A_{\mathrm{tor}}\simeq\mathbb{Q}^{(I)}$ avec $I\sim\mathbb{R}$.

Exercice 3.25. (i) Le fait que $\mathbb{Z}_p$ est un sous-groupe découle de ce que l'application naturelle (bien définie) $f_n:\mathbb{Z}/p^{n+1}\mathbb{Z}\to\mathbb{Z}/p^n\mathbb{Z},\ x \bmod p^{n+1}\mapsto x \bmod p^n$, est un morphisme de groupes. Le fait que $\mathbb{Z}_p\to\mathbb{Z}/p^n\mathbb{Z},(x_n)\mapsto x_n$, est un morphisme de groupes est évident (définition d'un groupe produit). Il est surjectif, car pour tout $y\in\mathbb{Z}$, l'élément (y_m) avec $y_m:=y \bmod p^m$ est dans $\mathbb{Z}_p$, et sa composante $y_n\in\mathbb{Z}/p^n\mathbb{Z}$ est arbitraire.

(ii) Comme au (iv) ci-dessus on a $\{0,1\}^n\hookrightarrow\mathbb{Z}_p\hookrightarrow\mathbb{N}^{\mathbb{N}}$ et donc $\mathbb{Z}_p$ est équipotent à $\mathbb{R}$ par Cantor-Bernstein.

(iii) Soit $(x_n)\in\mathbb{Z}_p$ non nul. Il existe $N\geqslant 1$ tel que $x_N\neq 0$. On peut donc écrire $x_N\in p^v(\mathbb{Z}/p^N\mathbb{Z})^\times$ avec $0\leqslant v<N$. Mais pour $M\geqslant N$, l'élément x_N est image de x_M par la projection naturelle $\mathbb{Z}/p^M\mathbb{Z}\to\mathbb{Z}/p^N\mathbb{Z}$. On a donc aussi $x_M\in p^v(\mathbb{Z}/p^M\mathbb{Z})^\times$. L'ordre de x_M dans $\mathbb{Z}/p^M\mathbb{Z}$ est donc p^{M-v}. Cet ordre tend vers l'infini avec M. Ainsi, il n'existe aucun entier $m\geqslant 1$ tel que $m(x_n)=(mx_n)=0$.

(iv) Soit χ un caractère de μ_{p^∞}. Sa restriction au groupe cyclique μ_{p^n} vérifie donc $\chi(e^{2i\pi/p^n})=e^{2i\pi k_n/p^n}$ pour un certain $k_n\in\mathbb{Z}$, uniquement déterminé modulo p^n. En appliquant χ à l'égalité $(e^{2i\pi/p^{n+1}})^p=e^{2i\pi/p^n}$ on déduit $e^{2i\pi k_{n+1}/p^n}=e^{2i\pi k_n/p^n}$, ou ce qui revient au même, $k_{n+1}\equiv k_n \bmod p^n$. Ainsi, $k(\chi):=(k_n)$ est dans $\mathbb{Z}_p$.

(v) On a défini ci-dessus une application $\widehat{\mu_{p^\infty}}\to\mathbb{Z}_p,\ \chi\mapsto k(\chi)$. C'est un morphisme de groupes : on a $k(\chi)+k(\psi)=k(\chi\psi)$. Il est clairement injectif puisqu'on a $\chi(e^{2i\pi/p^n})=1$ si, et seulement si, $k_n\equiv 0 \bmod p^n$. Il ne reste donc qu'à justifier sa surjectivité. Soit $k=(k_n)$ un entier p-adique. On définit un caractère χ_n du groupe cyclique $\mu_{p^n}=\langle e^{2i\pi/p^n}\rangle$ en posant $\chi(e^{2i\pi/p^n})=e^{2i\pi k_n/p^n}$. Observons que l'on a $(\chi_m)_{|\mu_{p^n}}=\chi_n$ pour $m\geqslant n$. En effet :

$$\chi_m(e^{2i\pi/p^n})=\chi_m(e^{2i\pi/p^m})^{p^{m-n}}=e^{2i\pi k_m/p^n}=e^{2i\pi k_n/p^n},$$

la dernière égalité venant de $k_m\equiv k_n \bmod p^n$. Ainsi, pour $x\in\mu_{p^\infty}$, $\chi_n(x)$ est bien défini et indépendant de n dès que n est assez grand de sorte que $x\in\mu_{p^n}$: on le note $\chi(x)$. On a $\chi(xy)=\chi(x)\chi(y)$ car x,y et xy sont dans un même μ_{p^n} pour n assez grand, et l'égalité vaut alors pour χ remplacé par χ_n. Par définition, on a $\chi_{|\mu_{p^n}}=\chi_n$, et donc $k(\chi)=(k_n)$.

Exercice 3.27 (i) On a $\mathrm{J}(\chi,\chi^{-1})=\sum_{x\in\mathbb{Z}/p\mathbb{Z}\smallsetminus\{1\}}\chi(\frac{x}{1-x})$. Regardons l'application

$$\mathbb{Z}/p\mathbb{Z}\smallsetminus\{1\}\to\mathbb{Z}/p\mathbb{Z},\ x\mapsto x/(1-x).$$

Elle est injective, car c'est $x\mapsto -1+1/(1-x)$. Elle ne prend pas la valeur -1. Elle définit donc une bijection $\mathbb{Z}/p\mathbb{Z}\smallsetminus\{1\}\to\mathbb{Z}/p\mathbb{Z}\smallsetminus\{-1\}$. On a donc $\mathrm{J}(\chi,\chi^{-1})=-\chi(-1)+\sum_{x\in\mathbb{Z}/p\mathbb{Z}}\chi(x)=-\chi(-1)$, car on sait que la somme est nulle pour $\chi\neq 1$.

(ii) On a $|C|=\sum_{a+b=1}\mathrm{N}(x^2=a\alpha^{-1})\mathrm{N}(y^2=b\beta^{-1})$, puis par le cours

$$|C|=\sum_{a+b=1}(1+(\frac{a\alpha^{-1}}{p}))(1+(\frac{b\beta^{-1}}{p}))=\sum_{a+b=1}(1+(\frac{\alpha}{p})(\frac{a}{p})+(\frac{\beta}{p})(\frac{b}{p})+(\frac{\alpha\beta}{p})(\frac{a}{p})(\frac{b}{p})).$$

Mais on a $\sum_{a+b}1=p$ et $\sum_a(\frac{a}{p})=0$, puis $|S|=p+(\frac{\alpha\beta}{p})\mathrm{J}(\lambda,\lambda)$, et on conclut par le (i).

(iii) On fixe u non carré dans $(\mathbb{Z}/p\mathbb{Z})^\times$. Un élément de $\mathbb{Z}/p\mathbb{Z}$ est non carré si, et seulement si, il est de la forme uy^2 avec $y\neq 0$. On regarde donc l'équation $x^2+1=uy^2$, soit $x^2-uy^2=1$. Cette équation a $p-(\frac{u}{p})=p+1$ solutions (x,y) dans $(\mathbb{Z}/p\mathbb{Z})^2$ par le (ii). L'application associant à une solution (x,y) l'élément $x^2\in(\mathbb{Z}/p\mathbb{Z})^\times$ se surjecte sur l'ensemble à dénombrer. Ses fibres ont 4 éléments, sauf pour $x^2=-1$, auquel cas les deux

antécédents sont $(\pm x, 0)$. Le nombre cherché est donc $(p+1)/4$, sauf si -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$, auquel cas c'est $(p-1)/4$.

Exercice 3.28. On a vu en cours $|\mathrm{S}_p| \equiv 1 \bmod 2$ et $|\mathrm{S}_p| \equiv -1 \bmod 3$, autrement dit $|\mathrm{S}_p| \equiv -1 \bmod 6$ (Bezout). Il s'agit donc de montrer $|\mathrm{S}_p| \equiv -1 \bmod 4$, et aussi que $|\mathrm{S}_p| \equiv -1 \bmod 8$ implique $p \equiv 1 \bmod 4$. Mais d'après le théorème de Gauss vu en cours on a aussi $|\mathrm{S}_p| = p + 2A$ avec $p = A^2 + 3B^2$. En regardant modulo 4 et en se rappelant $p \neq 2$, on constate que l'on a soit A pair, B impair et $p \equiv -1 \bmod 4$, soit A impair, B pair et $p \equiv 1 \bmod 4$. Dans les deux cas on constate $p + 2A \equiv -1 \bmod 4$, et donc $|\mathrm{S}_p| \equiv -1 \bmod 4$. Enfin, si on a $p + 2A \equiv -1 \bmod 8$, on en déduit $A^2 + 3B^2 + 2A + 1 \equiv 0 \bmod 8$, puis $(A+1)^2 \equiv -3B^2 \bmod 8$. Si B est impair, on a $(A+1)^2 \equiv -3 \bmod 8$, ce qui est absurde, donc B est pair, *i.e.* $p \equiv 1 \bmod 4$.

Exercice 3.29. Pour tout entier $n \geqslant 1$, le nombre u_n de solutions dans $(\mathbb{Z}/p\mathbb{Z})^2$ de $y^2 = x^n + 1$ s'ecrit $u_n = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \mathrm{N}(y^2 = x^n + 1) = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} (1 + (\frac{x^n+1}{p})) = p + v_n$ où $v_n = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} (\frac{x^n+1}{p})$ est la somme de l'énoncé. On a $u_2 = p - 1$ par l'Exercice 3.27 (ii), donc $v_2 = u_2 - p = -1$, ce qui répond à la question (i). On a $u_3 = p + 2A$ comme dans le Théorème de Gauss vu en cours, donc $v_3 = 2A$, ce qui répond à la question (ii). Enfin, pour répondre à la question (iii) on écrit par le cours

$$u_n = \sum_{a+b=1} \mathrm{N}(y^2 = a)\mathrm{N}(x^n = -b) = \sum_{a+b=1} (1 + \lambda(a))(\sum_{\chi} \chi(-b)),$$

la somme portant sur les m caractères de $(\mathbb{Z}/p\mathbb{Z})^\times$ vérifiant $\chi^m = 1$. Mais on a $\mathrm{J}(1, \chi) = \mathrm{J}(\chi, 1) = 0$ pour $\chi \neq 1$. On a donc $v_n = u_n - p = \sum_{\chi \neq 1 \,|\, \chi^m = 1} \chi(-1)\mathrm{J}(\lambda, \chi)$. Si m est impair, aucun des $m-1$ caractères $\chi \neq 1$ vérifiant $\chi^m = 1$ n'est l'inverse de λ (*i.e.* égal à λ), de sorte que l'on a $\lambda\chi \neq 1$ et $|\mathrm{J}(c, \chi)| = \sqrt{p}$ par le cours. Si m est pair, un seul des $m-1$ caractères $\chi \neq 1$ vérifiant $\chi^m = 1$ est égal à $\lambda^{-1} = \lambda$, et pour $\chi = \lambda$ on a $\mathrm{J}(\chi, \lambda) = \mathrm{J}(\lambda, \lambda^{-1}) = \pm 1$ par l'Exercice 3.27 (i). Cela conclut la démonstration.

Exercice 3.30. (i) On a $G^2 = \mathrm{J}(c, c)\mathrm{G}(c^2)$ car $c^2 \neq 1$. Par la Formule (17) Chap. 3, et $c^2 = c^{-1} = \overline{c}$, on a aussi $\mathrm{G}(c^2) = c(-1)\overline{G}$. Mais on a $c(-1) = c((-1)^3) = c(-1)^3 = 1$, donc $\mathrm{G}(c^2) = \overline{G}$. On conclut par la relation $\overline{G}G = p$.

(ii) On a $J = a + bj$ avec $a, b \in \mathbb{Z}$ et $j = e^{2i\pi/3}$, donc $J + \overline{J} = a + a - b = 2a - b$. On a aussi par le cours $p = |J|^2 = a^2 - ab + b^2$, donc $4p = (2a - b)^2 + 3b^2$.

(iii) En utilisant $\sum_{x \in (\mathbb{Z}/p\mathbb{Z})^\star} \zeta^x = -1$, ainsi qu'un changement de variable $x \mapsto -x$ dans $\overline{G}$, et encore $c(-1) = 1$, on trouve $-1 + G + \overline{G} = \sum_{x \in (\mathbb{Z}/p\mathbb{Z})^\times} (c(x) + \overline{c(x)} + 1)\, \zeta^x$. Si x n'est pas un cube, on a $c(x) + \overline{c(x)} + 1 = 0$ car $c(x) = j$ ou j^2. Si x est un cube, on a $c(x) + \overline{c(x)} + 1 = 3$, et comme x est le cube d'exactement 3 éléments on a aussi $-1 + G + \overline{G} = \sum_{x \in (\mathbb{Z}/p\mathbb{Z})^\times} \zeta^{x^3}$. Le terme de droite étant réel, on peut y remplacer ζ^{x^3} par sa partie réelle $\cos(2\pi x^3/p)$, et on conclut.

(iv) On a $(G + \overline{G})^3 = G^3 + \overline{G^3} + 3G\overline{G}(G + \overline{G})$, avec $G^3 + \overline{G^3} = p(J + \overline{J}) = pA$ par le (i) et (ii), et aussi $G\overline{G} = p$, de sorte que $x = G + \overline{G}$ vérifie $x^3 = pA + 3px$. Le polynôme $X^3 - 3pX - pA$ a trois racines réelles car son discriminant $-4(-3p)^3 - 27p^2A^2 = 27p^2(4p - A^2) = 3^4p^2B^2$ est > 0 (c'est même un carré !).

Exercice 3.31. (i) Soit $\mathrm{C}_p \subset (\mathbb{Z}/p\mathbb{Z})^\times$ le sous-groupe des carrés. On suppose $p \equiv 3 \bmod 4$, et donc $-1 \notin \mathrm{C}_p$. Le morphisme $\mathrm{C}_p \to \mathrm{C}_p, x \mapsto x^2$, est alors de noyau trivial : il est donc bijectif. Ainsi, on a $\mathrm{T}_p \sim \{(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2 \,|\, y^2 + x^2 = 1\}$. On est dans le cas $\alpha = \beta = 1$ de l'Exercice 3.27. On a donc $|\mathrm{T}_p| = p + 1$ car $(\frac{-1}{p}) = -1$.

(ii) On suppose $p \equiv 1 \bmod 4$. On sait qu'il existe un élément $i \in \mathbb{Z}/p\mathbb{Z}$ avec $i^2 = -1$. L'idée est d'exploiter le fait que les deux bijections $\alpha(x, y) = (x, -y)$ et $\beta(x, y) = (ix, y)$ de

$(\mathbb{Z}/p\mathbb{Z})^2$ préservent T_p. En anticipant un peu sur la suite du cours on peut procéder comme suit. Soit G le sous-groupe de $\mathrm{S}_{(\mathbb{Z}/p\mathbb{Z})^2}$ engendré par α et β. On vérifie aisément que ce groupe est d'ordre 8 (en fait, isomorphe à D_8). Son action naturelle sur $(\mathbb{Z}/p\mathbb{Z})^2$ préserve le sous-ensemble T_p. L'orbite d'une solution $(x,y) \in \mathrm{T}_p$ est l'ensemble des $(ux, \pm y)$ avec $u = \pm 1$ ou $\pm i$. Pour $(x,y) \neq 0$, cette orbite a 8 éléments. Pour $y = 0$, la seule possibilité est $x = \pm 1$, et $\{(1,0),(-1,0)\}$ est une orbite à 2 éléments. Enfin, pour $x = 0$, la seule possibilité est $y = \pm 1, \pm i$, et $\{(0,\pm 1),(0,\pm i)\}$ est une orbite à 4 éléments. Écrivant T_p comme réunion disjointe de ses G-orbites on a $|\mathrm{T}_p| \equiv 2 + 4 \bmod 8$.

(iii) On fixe g un générateur du groupe cyclique $(\mathbb{Z}/p\mathbb{Z})^\times$. Comme $p \equiv 1 \bmod 4$, on sait par le cours qu'il existe exactement 4 caractères $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \to \mu_4$ avec $\chi^4 = 1$, uniquement déterminés par l'élément $\chi(g) \in \mu_4$. On note c le tel que χ vérifiant $\chi(g) = i$ (il dépend du choix de g). Les 4 caractères précédents sont donc $1, c, c^2 = \lambda$ (le symbole de Legendre) et $c^3 = c^{-1}$. Par la méthode de Weil, on trouve en procédant comme dans le cours $|\mathrm{T}_p| = p + \mathrm{J}(\lambda, c) + \mathrm{J}(\lambda,\lambda) + \overline{\mathrm{J}(\lambda, c)}$. On a $\mathrm{J}(\lambda,\lambda) = -1$ par l'Exercice 3.27 (i). On constate aussi que $\mathrm{J}(\Lambda, c)$ est de la forme $a + bi$ avec $a, b \in \mathbb{Z}$. Et donc $|\mathrm{T}_p = p - 1 + 2a$. La congruence du (ii) donne $p - 1 + 2a \equiv 6 \bmod 8$, puis $a \equiv -\frac{p+1}{2} \bmod 4$. En particulier, a est impair car $p \equiv 1 \bmod 4$. Comme on a $\lambda c = c^3 \neq 1$, le cours donne $a^2 + b^2 = |\mathrm{J}(\lambda, c)|^2 = p$. Comme a est impair, on a b pair.

Exercice 3.32. (i) Fixons $a \leqslant k \leqslant b - 1$ un entier. On applique le théorème de convergence de Dirichlet (en analyse de Fourier) à la fonction 1-périodique nulle aux entiers et coïncidant avec f sur $]k, k+1[$, et en un point dans $\mathbb{Z}$. On en déduit

$$\frac{1}{2}(f(k) + f(k+1)) = \lim_{A\to\infty} \sum_{n=-A}^{A} \int_k^{k+1} f(t) e^{2i\pi nt} dt =: \sum_{n\in\mathbb{Z}} \int_k^{k+1} f(t) e^{2i\pi nt} dt.$$

On conclut en sommant cette identité pour $k = a, \ldots, b-1$. Bien noter que la sommation dans l'énoncé (et donc la somme sur $\mathbb{Z}$ de droite) est à prendre au sens de la limite ci-dessus. Pour le (ii), on applique le (i) à la fonction $f(t) = e^{2i\pi t^2/N}$ sur le segment $[0, N]$. Le terme de gauche est G_N. Par changement de variables $u = t + \frac{nN}{2}$, on a aussi

$$\int_0^N f(t) e^{2i\pi nt} dt \;=\; i^{-n^2 N} \int_{\frac{nN}{2}}^{\frac{(n+2)N}{2}} e^{\frac{2i\pi u^2}{N}} du \;=\; i^{-n^2 N}\, N^{1/2} \int_{\frac{n}{2}}^{\frac{n}{2}+1} e^{2i\pi u^2} du.$$

Le (ii) s'en déduit en séparant les n pairs et impairs. Pour le (iii), On en déduit d'abord $I = (1-i)^{-1} = \frac{1+i}{2}$ en prenant $N = 1$, car dans ce cas on a $\mathrm{G}_1 = 1$, et on conclut par le (ii).

Exercice 3.33. (i) On suppose ici plus généralement que p, q sont des entiers $\geqslant 1$ premiers entre eux. Posons $\zeta = e^{\frac{2i\pi}{pq}}$. En développant, $\mathrm{G}_{p,q}\mathrm{G}_{q,p}$ est la somme, sur tous les couples $(\overline{a}, \overline{b}) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, des $\zeta^{a^2q^2 + b^2p^2}$. Mais on constate $a^2q^2 + b^2p^2 \equiv (aq + bp)^2 \equiv 0 \bmod pq$. Il suffit donc de voir que l'application $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/pq\mathbb{Z}, (\overline{a}, \overline{b}) \mapsto aq + bp$, qui est bien définie et un morphisme, est bijective. Il suffit de voir qu'elle est injective, mais si on a $aq + bp \equiv 0 \mod pq$, on a $aq \equiv 0 \bmod p$ et $bp \equiv 0 \bmod q$, et comme p et q sont premiers entre eux, on a bien$a \equiv 0 \bmod p$ et $b \equiv 0 \bmod q$.

(ii) Si p divise a, on a $\mathrm{G}_{p,a} = 0$ et $(\frac{a}{p}) = 0$. On suppose a premier à p. Si $a \equiv u^2 \bmod p$, le changement de variable bijectif $\overline{k} \mapsto \overline{ku}$ dans $\mathbb{Z}/p\mathbb{Z}$ montre $\mathrm{G}_{p,a} = \mathrm{G}_{p,1} = \mathrm{G}_p$. Posons $\zeta = e^{2i\pi/p}$ et notons C_p l'ensemble des carrés de $(\mathbb{Z}/p\mathbb{Z})^\times$. Si a n'est pas un carré, l'ensemble N_p des non carrés dans $(\mathbb{Z}/p\mathbb{Z})^\times$ est $\mathrm{N}_p = a\mathrm{C}_p$. Comme tout carré non nul est le carré d'exactement 2 éléments, on a $-1 = \sum_{k\in(\mathbb{Z}/p\mathbb{Z})^\times} \zeta^k = \sum_{k\in\mathrm{C}_p} \zeta^k + \zeta^{ak} = \frac{1}{2}(\mathrm{G}_p - 1) + \frac{1}{2}(\mathrm{G}_{p,a} - 1)$, puis $\mathrm{G}_{p,a} = -\mathrm{G}_p$. On a bien montré $\mathrm{G}_{p,a} = (\frac{a}{p})\,\mathrm{G}_p$.

(iii) Par le (i) et le (ii) on a $\mathrm{G}_{pq} = (\frac{p}{q})(\frac{q}{p})\mathrm{G}_p\mathrm{G}_q$. Mais pour $N \geqslant 1$ impair, on a vu à l'exercice précédent que l'on a $\mathrm{G}_N = \epsilon_N N^{1/2}$, avec $\epsilon_N = 1$ pour $N \equiv 1 \bmod 4$ et $\epsilon_N = i$ pour $N \equiv 3 \bmod 4$. On en déduit

$$(\frac{p}{q})(\frac{q}{p}) = \epsilon_p\epsilon_q/\epsilon_{pq}.$$

Pour $p \equiv 1 \bmod 4$, on a $q \equiv pq \equiv 3 \bmod 4$ et donc $\epsilon_p\epsilon_q/\epsilon_{pq} = 1$, mais on a aussi $(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = (-1)^{\text{pair}} = 1$. De même bien sûr pour $q \equiv 1 \bmod 4$. Enfin, pour $p \equiv q \equiv 3 \bmod 4$, et donc $pq \equiv 1 \bmod 4$, on a $\epsilon_p\epsilon_q/\epsilon_{pq} = i \cdot i/1 = -1$, et aussi $(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = (-1)^{\text{impair}} = -1$. On a montré $(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ dans tous les cas.

(iv) Le premier point du est un cas particulier du (i) tel qu'on l'a rédigé. Pour le second , posons $\zeta = e^{2i\pi/8}$. Pour $k \in \mathbb{Z}/8\mathbb{Z}$, on a $k^2 \equiv 1 \bmod 8$ si k est impair, $k^2 \equiv 4 \bmod 8$ si $k \equiv \pm 2 \bmod 8$, et $k^2 \equiv 0 \bmod 8$ pour $k \equiv 0 \bmod 4$. On a donc $\mathrm{G}_{8,p} = 4\zeta^p + 2\,(-1)^p + 2 = 4\zeta^p$.

(v) Le (ii) pour $a = 8$ montre $\mathrm{G}_{p,8} = (\frac{8}{p})\mathrm{G}_p$. Mais on a $(\frac{8}{p}) = (\frac{2}{p})^3 = (\frac{2}{p})$, et donc $\mathrm{G}_{p,8} = (\frac{2}{p})\mathrm{G}_p$. On a vu à l'exercice précédent que l'on a $\mathrm{G}_p = \epsilon_p p^{1/2}$ et $\mathrm{G}_{8p} = (1+i)(8p)^{1/2} = 4\zeta\sqrt{p}$. La formule $\mathrm{G}_{8,p}\mathrm{G}_{p,8} = \mathrm{G}_{8p}$ s'écrit donc $4\,\zeta^p\,(\frac{2}{p})\,\epsilon_p = 4\,\zeta$, puis $(\frac{2}{p}) = \zeta^{1-p}/\epsilon_p$. Pour $p \equiv 1, 3, -3, -1 \bmod 8$, ce symbole de Legendre vaut donc respectivement $1, -1, -1$ et 1, et coïncide avec $(-1)^{\frac{p^2-1}{8}}$.

Exercice 3.34. (i) Évident. (ii) Soit $f \in \mathrm{L}^2(G)$. On a $\widehat{f}(\chi) = \sum_{g\in G} f(g)\overline{\chi(g)}$. Notons $\mathrm{ev}_g : \widehat{G} \to \mathbb{C}^\times$ le caractère $\chi \mapsto \chi(g)$. On a donc, pour tout $g \in G$,

$$\widehat{(\widehat{f})} \circ \iota_G(g) = \widehat{(\widehat{f})}(\mathrm{ev}_g) = \sum_{\psi\in\widehat{G}} \widehat{f}(\psi)\overline{\psi(g)} = \sum_{h\in G, \psi\in\widehat{G}} f(h)\psi(h^{-1})\overline{\psi(g)} = f(g^{-1})$$

où on a utilisé $\overline{\psi(h)} = \psi(h^{-1})$ et le (ii) de l'Exercice 3.17.

Exercice 3.35. (i) Tout est immédiat sauf l'associativité de $\star$. Mais on a

$$(f \star f'') \star f''(g) = \sum_{a,b|ab=g} (f \star f')(a)f''(b) = \sum_{a,b,c|abc=g} f(a)f'(b)f''(c) = f \star (f'' \star f'')(g).$$

Pour le (ii) on observe $f \star \chi(g) = \sum_{a\in G} f(a)\chi(a^{-1}g) = \chi(g)\widehat{f}(\chi)$. Par associativité et (ii), on en déduit le (iii) : $\widehat{f \star f'}(\chi)\,\chi = f \star f' \star \chi = f \star (\widehat{f'}(\chi)\chi) = \widehat{f'}(\chi) f \star \chi = \widehat{f'}(\chi)\widehat{f}(\chi)\chi$.

Exercices du chapitre 4

Exercice 4.1. Soit σ dans le centre de S_n. Écrivons que σ commute à la transposition $(i\,j)$. On a $(i\,j) = \sigma(i\,j)\sigma^{-1} = (\sigma(i)\,\sigma(j))$, *i.e.* $\sigma(\{i,j\}) = \{i,j\}$. Ainsi, si σ préserve toutes les parties à 2 éléments de $\{1,\dots,n\}$. Comme on a $n \geqslant 3$, pour tout $i \in \{1,\dots,n\}$ on peut trouver $j,k \in \{1,\dots,n\}$ avec i,j,k distincts. On a alors $\{i\} = \{i,j\} \cap \{i,k\}$ puis $\sigma(i) = i$: σ est l'identité.

Exercice 4.2. (i) Un morphisme de groupes $f : G \to G'$ *avec* G' *abélien* est constant sur les classes de conjugaison de G : si on a $g,x \in G$ alors $f(gxg^{-1}) = f(g)f(x)f(g)^{-1} = f(g)f(g)^{-1}f(x) = f(x)$. Comme deux transpositions sont conjuguées dans S_n, tout morphisme $\mathrm{S}_n \to \{\pm 1\}$ prend la même valeur $\epsilon \in \{\pm 1\}$ sur chaque transposition. Comme les transpositions engendrent S_n, il y a donc au plus deux morphismes $\mathrm{S}_n \to \{\pm 1\}$. Pour $\epsilon = 1$, le morphisme est nécessairement trivial (et existe bien !). Pour $\epsilon = -1$, il existe encore : c'est la signature.

(ii) Pour tout sous-groupe H d'indice 2 d'un groupe G on a vu en cours qu'il existe un morphisme $G \to \{\pm 1\}$ de noyau H. En effet, on sait que H est distingué, et on regarde alors la composée de la projection canonique $G \to G/H$ et de l'unique isomorphisme $G/H \simeq \{\pm 1\}$. Comme il n'y a qu'un morphisme non trivial $\mathrm{S}_n \to \{\pm 1\}$ par le (i), à savoir la signature, A_n est le seul sous-groupe d'indice 2 de S_n.

Exercice 4.5. (i) Soit $f : \mathrm{A}_n \to \{\pm 1\}$ un morphisme. On sait que A_n est engendré par les 3-cycles. Il suffit donc de montrer que si c est un 3-cycle on a $f(c) = 1$. Mais on a $f(c^3) = f(c)^3 = 1$ et donc $f(c) = 1$ car $f(c) = \pm 1$. (Plus généralement, si on a un morphisme $f : G \to G'$ et $g \in G$ tels que l'ordre de g est premier à $|G'|$, alors on a $f(g) = 1$.)

(ii) On a $|\mathrm{A}_4| = 12$. Si A_4 admet un sous-groupe H d'ordre 6, ce sous-groupe est donc d'indice 2, puis le noyau d'un morphisme surjectif $\mathrm{A}_4 \to \{\pm 1\}$. Il n'y a pas de tel morphisme par le (i). C'est le contre-exemple à la réciproque naive du théorème de Lagrange évoqué après le Corollaire 4.7 Chap. 2.

Exercice 4.6. Soit H le sous-groupe de A_n engendré par les $(i\ i+1\ i+2)$ avec $1 \leqslant i < n-1$. On veut montrer $H = \mathrm{A}_n$. Il suffit de voir que tous les 3-cycles sont dans H, car ces derniers engendrent A_n par le cours. C'est clair pour $n = 1,2,3$. Noter $(i\,j\,k)^{-1} = (j\,i\,k)$. Pour $n = 4$, on a $(1\,2\,3)(3\,2\,4) = (1\,2\,4) \in H$ et $(1\,3\,4) = (2\,3\,4)(1\,2\,3)(2\,3\,4)^{-1}$. Les 8 3-cycles sont bien dans H. Pour $n \geqslant 4$, on déduit du cas $n = 4$ que H contient toutes les permutations paires à support dans $\{i, i+1, i+2, i+3\}$, pour tout $1 \leqslant i \leqslant n-3$. Si $(i\,j\,k)$ est dans H, on a aussi $\sigma(i\ j\ k)\sigma^{-1} = (\sigma(i)\,\sigma(j)\,\sigma(k))$ pour tout $\sigma \in H$. On en déduit successivement que H contient tous les $(i\,i+1\,k)$ avec $i+2 \leqslant k \leqslant n$, puis que H contient tous les (i,j,k) avec $i < j < k$.

(Pour ce type d'arguments, il est souvent plus pratique d'utiliser l'Exercice 4.23. Concrètement, on aurait d'abord pu vérifier que H agit 3-transitivement sur $\{1,\dots,n\}$ pour $n \geqslant 5$ (clair par récurrence), puis conclure en disant que H contient un 3-cycle, et donc tous les 3-cycles par conjugaison et 3-transitivité.)

Exercice 4.7. Quitte à conjuguer c (i.e. à renuméroter les entiers de 1 à n), on peut supposer $c = (1\,2\,3\,\dots\,m)$. Pour k divisant m, on constate alors que c^k est le produit des m/k-cycles $(i\ i{+}k\ i{+}2k\ \cdots\ i{+}(m{-}1)/k)$ avec $i = 1,\dots,k$. (Ces cycles sont bien disjoints : les entiers dans leur support sont $\equiv i \bmod k$). Pour k général on écrit $c^k = (c^d)^{k/d}$. Les cycles de c^d sont de longueur m/d comme on l'a vu, et on a k/d premier à d.

On est donc ramené au cas où k est premier avec m, et il faut voir que c^k est un m-cycle, *i.e.* que $\langle c^k \rangle$ permute transitivement $\{1,\dots,m\}$. Mais par Bezout il existe $q \in \mathbb{Z}$

avec $kq \equiv 1 \bmod m$. On a alors $(c^k)^q = c$, et donc $\langle c^k \rangle = \langle c \rangle$ permute transitivement $\{1, \ldots, m\}$.

Exercice 4.10. (i) L'ordre d'un élément est le ppcm des longueurs des cycles de sa décomposition en cycles. Si c'est p, c'est que tous ses cycles sont de longueur p. Comme on est dans S_p, l'unique possibilité est que ce soit un p-cycle.

(ii) Il existe $1 \leqslant i < p$ tel que $\sigma^i(1) = 2$. Comme p est premier, i est premier à p, et donc $c := \sigma^i$ est un p-cycle par l'exercice précédent (voir le second paragraphe du corrigé). Par définition, on a $c(1) = 2$. Enfin, les p éléments $\sigma^j(1)$ avec $j = 0, \ldots, p-1$ sont $\{1, \ldots, p\}$ car c est un cycle, de sorte que l'application $\{0, 1, \ldots, p-1\} \to \{1, 2, \ldots, p\}$ envoyant j sur $c^j(1)$ est bijective. Il y a donc un unique j tel que $\sigma^j(1) = 2$.

(iii) Par les (i) et (ii), tout sous-groupe H d'ordre p est engendré par un unique p-cycle de la forme $(1\,2\,a_3\,a_4\,\ldots\,a_p)$, avec $\{a_3, a_4, \ldots, a_p\} = \{3, 4, \ldots, p\}$. Il y a $(p-2)!$ tels éléments.

Exercice 4.8. (i) Soit H le sous-groupe engendré par la transposition t et le p-cycle c. On veut montrer $H = \mathrm{S}_p$. Quitte à conjuguer à H (= renuméroter), on peut supposer $t = (1\,2)$. Par le (ii) de l'exercice précédent, il existe $1 \leqslant i < p$ tel que $c^i = (1\,2\,a_3\,\ldots a_p) \in H$ avec $\{a_3, a_4, \ldots, a_p\} = \{3, 4, \ldots, p\}$. On a alors $\gamma := tc = (1\,2)(1\,2\,a_3\,\ldots a_p) = (2\,a_3\,\ldots a_p) \in H$, puis $\gamma^i t \gamma^{-i} = (1\,a_{i+1}) \in H$ pour $1 \leqslant i < p$, et donc $(1\,i) \in H$ pour tout $i = 2, \ldots, p$. Enfin, pour $1 < i < j$ on en déduit $(i\,j) = (1\,i)(1\,j)(1\,i)^{-1} \in H$: le groupe H contient toutes les transpositions, c'est S_p.

(ii) Pour $p = 4$, les éléments $c = (1\,2\,3\,4)$ et $t = (1\,3)$ n'engendrent pas S_4. En effet, on a $tct^{-1} = (3\,2\,1\,4) = c^{-1}$, de sorte que tout élément de $\langle c, t \rangle$ est de la forme $t^k c^q$ avec $0 \leqslant k \leqslant 1$ et $0 \leqslant q \leqslant 3$: il y a un plus 8 tels éléments.

Exercice 4.3. Comme G contient une transposition par hypothèse, on a $n \geqslant 2$, et de même on a $n \geqslant 3$ dans la question (ii).

(i) La condition suffisante est claire car S_n agit 2-transitivement sur $\{1, \ldots, n\}$. Réciproquement, fixons $i < j$ avec $(i\,j) \in G$. Pour $g \in G$ on a $g(i\,j)g^{-1} = (g(i)\,g(j))$. Si G agit 2-transitivement sur $\{1, \ldots, n\}$, on a donc $(k\,l) \in G$ pour tout $k < l$, puis G contient toutes les transpositions, et on a $G = \mathrm{S}_n$.

(ii) Le groupe G agit transitivement sur $\{1, \ldots, n\}$ car il contient un n-cyclique. Pour voir qu'il agit 2-transitivement, il suffit de voir que pour un certain $i \in \{1, \ldots, n\}$ le stabilisateur G_i de i dans G agit transitivement sur $\{1, \ldots, \hat{i}, \ldots, n\}$. C'est clair si on prend pour i le point fixe d'un $n-1$-cycle dans G.

Exercice 4.4. Pour montrer l'indication, on raisonne par récurrence sur $r := |X|$ et on note $H(x_1, \ldots, x_n) \subset S_X$ le sous-groupe engendré par les $t_i := (x_i\ x_{i+1})$. Le résultat est évident pour $r \leqslant 2$. Écrivons $X = Y \cup \{x_n\}$ avec $Y = \{x_1, \ldots, x_{n-1}\}$. Par récurrence, on a $H(x_1, \ldots, x_{n-1}) = \mathrm{S}_Y$. Si on a $X = Y$, on a gagné. Sinon, x_n n'est pas dans Y et on identifie S_Y au sous-groupe de S_X fixant x_n. Pour $\sigma \in \mathrm{S}_Y$ on a $\sigma\, t_r\, \sigma^{-1} = (\sigma(x_r)\,\sigma(x_{r+1}))$. On en déduit que $H(x_1, \ldots, x_n)$ contient tous les $(x\,x')$ avec $x, x' \in X$, et donc $H(x_1, \ldots, x_n) = \mathrm{S}_X$.

Supposons que le graphe $\mathscr{G}$ n'est pas connexe. Il existe donc une partition $S = S_1 \coprod S_2$ telle que toute arète de $\mathscr{G}$ est incluse dans S_1 ou dans S_2. Par définition de $\mathscr{G}$ on constate que toute transpositions dans T préserve S_1 et S_2. On en déduit que le groupe $\langle T \rangle$ préserve aussi S_1 et S_2. Il n'agit donc pas transitivement sur $\{1, \ldots, n\}$, et donc $\langle T \rangle \neq \mathrm{S}_n$.

Supposons enfin que $\mathscr{G}$ est connexe...

Exercice 4.9. Soit H le sous-groupe de S_n engendré par $c := (1\,2\,\cdots\,n)$ et la transposition $(i\,j)$. Notons d le pgcd de n et $|j-i|$. Montrons d'abord que $H = \mathrm{S}_n$ entraîne $d = 1$. Observons pour cela que si l'on a $1 \leqslant a, b \leqslant n$ avec $a \equiv b \bmod d$, alors pour tout $\sigma \in H$ on a $\sigma(a) \equiv \sigma(b) \bmod d$. En effet, c'est vrai pour $\sigma = c, c^{-1}$ et $\sigma = (i\,j)$, et on conclut par définition de H. Autrement dit, les parties de $\{1, \ldots, n\}$ de la forme $P_i := (i + d\mathbb{Z}) \cap \{1, \ldots, n\}$ avec $i \in \mathbb{Z}$ sont préservées dans leur ensemble par H. Noter

$$\coprod_{i=1}^{d} P_i = \{1, \ldots, n\} \quad \text{et} \quad |P_i| = n/d, \ \ \forall i \in \mathbb{Z}.$$

Supposant $H = \mathrm{S}_n$, le groupe H agit 2-transitivement sur $\{1, \ldots, n\}$ et on a donc soit $d = 1$ et $|P_i| = n$, soit $d = n$ et $|P_i| = 1$. Le second cas est exclus car d divise $i - j$ et $|i - j| < n$.

Supposons réciproquement $d = 1$. Regardons les transpositions dans H de la forme $c^k(i\,j)c^{-k} = (i + k \ \ j + k)$, avec $k \in \mathbb{Z}$, et identifions pour simplifier $\{1, \ldots, n\}$ avec $\mathbb{Z}/n\mathbb{Z}$. Posant $s = j - i$, ces transpositions contiennent notamment

$$(0\ s), \ \ (s\ 2s), \ \ \ldots, \ \ (ks\ (k+1)s), \ \ \forall k \in \mathbb{Z}.$$

Mais comme s est dans $(\mathbb{Z}/n\mathbb{Z})^\times$ par hypothèse, tout élément de $\mathbb{Z}/n\mathbb{Z}$ est de la forme ks pour $k \in \mathbb{Z}$ bien choisi. Ainsi, le graphe de sommets $\mathbb{Z}/n\mathbb{Z}$ et dont les arêtes sont les $\{ks, \ (k+1)s\}$ avec $k \in \mathbb{Z}$, est connexe (tout point est relié à 0). On conclut par Exercice **??** (vi).

Exercice 4.12. (i) Soit H le sous-groupe des permutations de S_n à support dans le complémentaire T de S. L'application $H \to \mathrm{S}_T, \sigma \mapsto \sigma_{|T}$, est un isomorphisme. Les éléments de $\langle c \rangle$ sont à support dans S. On a donc $H \cap \langle c \rangle = 1$ et $hg = gh$ pour tout $h \in H$ et tout $g \in \langle c \rangle$. En particulier, on a $\langle c \rangle H \subset C$. Reste à voir $C = \langle c \rangle H$. Écrivons $c = (i_1, \ldots, i_k)$ et considérons $\sigma \in C$. L'identité

$$\sigma(i_1\, i_2\, \ldots\, i_k)\sigma^{-1} = (\sigma(i_1)\, \sigma(i_2)\, \ldots\, \sigma(i_k)) = (i_1\, i_2\, \ldots\, i_k)$$

montre que σ préserve S (et donc T), et aussi que si l'on a $\sigma(i_1) = i_1$ alors $\sigma_{|S} = \mathrm{id}_S$. Mais on a $\sigma(i_1) = c^q(i_1)$ pour un certain q car σ préserve S. On a donc $c^{-q}\sigma \in C$ et $c^{-q}\sigma(i_1) = i_1$, et donc $c^{-q}\sigma$ préserve S et y vaut l'identité : c'est un élément de H. On a montré $\sigma \in \langle c \rangle H$.

(ii) D'après le (i), le centralisateur de $(1\,2)$ est $\langle (1\,2), (3\,4) \rangle = \{1, (1\,2), (3\,4), (1\,2)\,(3\,4)\}$. Il est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$. De même, celui de $(1\,2\,3)$ est $\langle (1\,2\,3) \rangle \simeq \mathbb{Z}/3\mathbb{Z}$, et celui de $(1\,2\,3\,4)$ est $\langle (1\,2\,3\,4) \rangle \simeq \mathbb{Z}/4\mathbb{Z}$. Reste à déterminer le centralisateur C de la double transposition $d = (1\,2)(3\,4)$. Un élément $\sigma \in \mathrm{S}_4$ est dans C si, et seulement si, on a $(1\,2)(3\,4) = \sigma d \sigma^{-1} = (\sigma(1)\,\sigma(2))(\sigma(3)\,\sigma(4))$. Il y a donc exactement deux cas. Soit on a $\sigma(\{1,2\}) = \{1,2\}$ et $\sigma(\{3,4\}) = \{3,4\}$, ce qui équivaut à dire que σ est dans le sous-groupe $H := \langle (1\,2), (3\,4) \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Soit on a $\sigma(\{1,2\}) = \{3,4\}$ et $\sigma(\{3,4\}) = \{1,2\}$, ce qui revient aussi à dire que l'élément $(1\,3)(2\,4)\sigma$ est dans H. On en déduit $C = \langle (1\,2), (3\,4), (1\,3)(2\,4) \rangle$. En fait, on a $(1\,2)(1\,3)(2\,4) = (1\,3\,2\,4) \in C$, $(1\,3\,2\,4)^2 = (1\,2)(3\,4)$, et $(1\,2)(3\,4)(1\,3)(2\,4) = (1\,4)(2\,3)$. On en déduit $C = \langle (1\,4)(2\,3), (1\,3\,2\,4) \rangle$: c'est aussi le conjugué par $(2\,3)$ du groupe diédral $\mathrm{D}_8 \subset \mathrm{S}_4$ du cours. En particulier, on a $C \simeq \mathrm{D}_8$.

Exercice 4.14. (i) Pour $i = j$ on a $s_i^2 = 1$. Mais si on a $s_i^2 = s_j^2 = 1$, les relations $s_i s_j s_i s_j = 1$ et $s_i s_j s_i s_j s_i s_j = 1$ s'écrivent respectivement $s_i s_j = s_j s_i$ et $s_i s_j s_i = s_j s_i s_j$.

(ii) On raisonne par récurrence sur n. Le cas $n = 1$ est trivial, car on a $G = \{1, s_1\}$. On suppose $n > 1$. Soit $g \in G$. Utilisant $s_n^2 = 1$ on peut écrire

$$g \ = \ h_1\, s_n\, h_2\, s_n\, \cdots\, s_n\, h_k, \tag{80}$$

pour un certain $k \geqslant 1$ et des éléments $h_1, \dots, h_k$ dans $H := \langle s_1, \dots, s_{n-1} \rangle$. Si on a $k = 1$, alors g est dans H, et il n'y a rien à démontrer. Sinon, l'élément h_2 s'écrit par récurrence $h_2 = s_i\, s_{i+1} \cdots s_{n-1}\, h_2'$ avec $1 \leqslant i \leqslant n$ et $h_2' \in \langle s_1, \dots, s_{n-2} \rangle$. Supposons d'abord $k > 2$. Comme s_n commute aux s_i avec $i < n-1$ par hypothèse, on a donc

$$s_n\, h_2\, s_n \;=\; s_i\, s_{i+1} \cdots s_n\, s_{n-1}\, s_n\, h_2'.$$

La relation de tresse permet de remplacer $s_n\, s_{n-1}\, s_n$ par $s_{n-1}\, s_n\, s_{n-1}$. Le nombre k d'occurences de s_n dans l'écriture (80) de g a donc chuté de 1. Par récurrence sur k, on peut donc supposer $k = 2$, *i.e.* $g = h_1\, s_n\, h_2$. Écrivons $h_1 = s_j\, s_{j+1} \cdots s_{n-1}\, h_1'$ avec $1 \leqslant j \leqslant n$ et $h_1' \in \langle s_1, \dots, s_{n-2} \rangle$. Comme s_n commute aux s_j avec $j < n-1$ on a donc

$$g \;=\; h_1\, s_n\, h_2 \;=\; s_j\, s_{j+1} \cdots s_{n-1}\, s_n\, h_1'\, h_2 \;=\; f_j\, h_1'\, h_2 \;\in\; f_j H.$$

(iii) On raisonne par récurence sur n. C'est évident pour $n = 1$ car alors $G = \{1, s_1\}$ est de cardinal $\leqslant 2$. Le sous-groupe H de G engendré par les s_i avec $i < n$ satisfait l'hypothèse de récurrence, et donc vérifie $|H| \leqslant n!$. On a donc $|G| \leqslant (n+1)n! = (n+1)!$ par le (ii).

(iv) On constate que les n transpositions $t_i := (i\ i+1)$ de S_{n+1}, avec $1 \leqslant i \leqslant n$, satisfont $(t_i\, t_j)^2 = 1$ pour $i = j$ et $|i - j| > 1$, et que l'élément $t_i\, t_{i+1} = (i\ i+1\ i+2)$, pour $i < n$, vérifie aussi $(t_i\, t_{i+1})^3 = 1$. Soit Γ le groupe de droite défini par les générateurs s_i avec $1 \leqslant i \leqslant n$, et les relations $(s_i\, s_j)^{m_{i,j}} = 1$ pour tout $1 \leqslant i \leqslant j \leqslant n$. Par la propriété universelle de Γ, on a un unique morphisme de groupes

$$f : \Gamma \to \mathrm{S}_{n+1}$$

vérifiant $f(s_i) = t_i$ pour tout $i = 1, \dots, n$. Mais les t_i engendrent S_{n+1} par le cours, donc f est surjectif. On a aussi $|\Gamma| \leqslant (n+1)!$ par le (iii). Le morphisme f est donc un isomorphisme.

Exercice 4.15. (i) Si la case vide est déplacée horizontalement pour passer de E à F, ou plus généralement en suivant le serpent, on a $\mathrm{s}(E) = \mathrm{s}(F)$ et donc $\sigma(F) = \sigma(E)$. Sinon nous allons voir que $\sigma(E)^{-1}\sigma(F)$ est un cycle de longueur $3, 5$ ou 7 qui ne dépend pas de E. En effet, supposons par exemple que la case vide se trouve à la i-ème case de la deuxième ligne et monte verticalement en première ligne. Écrivons $\mathrm{s}(E) = (x_1, x_2, x_3, x_4, x_5, x_6, x_7, \dots)$. Alors selon que l'on a $i = 1, 2, 3$, l'élément $\mathrm{s}(F)$ vaut $(x_2, x_3, x_4, x_5, x_6, x_7, x_1, \dots)$, $(x_1, x_3, x_4, x_5, x_6, x_2, x_7, \dots)$ et $(x_1, x_2, x_4, x_5, x_3, x_6, x_7, \dots)$ respectivement. On constate donc que l'on a $\sigma(F) = \sigma(E) \circ \sigma_i$ avec

$$\sigma_1 = (1\,2\,3\,4\,5\,6\,7),\ \ \sigma_2 = (2\,3\,4\,5\,6)\ \text{ et }\ \sigma_3 = (3\,4\,5).$$

En étudiant de même la montée de la case vide en partant des lignes 3 et 4, on trouve les permutations suivantes (conjuguées de celles ci-dessus par $x \mapsto x+4$ et $x \mapsto x+8$) :

$$(7\,8\,9),\ (6\,7\,8\,9\ 10),\ (5\,6\,7\,8\,9\ 10\ 11),\ (9\,10\ 11\ 12\ 13\ 14\ 15),\ (10\ 11\ 12\ 13\ 14)\ \text{ et }\ (11\ 12\ 13).$$

Bien entendu, lorsque l'on descend la case vide au lieu de la monter, on obtient les cycles inverses à ceux ci-dessus.

(ii) Soient $E = E_1, \dots, E_n = F$ une suite d'états du taquin obtenus par mouvements élémentaires successifs. On a

$$\sigma(E)^{-1}\sigma(F) = (\sigma(E_1)^{-1}\sigma(E_2))\,(\sigma(E_2)^{-1}\sigma(E_3))\,\dots(\sigma(E_{n-1})^{-1}\sigma(F)). \tag{81}$$

Ainsi, on constate que $\sigma(E)^{-1}\sigma(F)$ est un produit de $n-1$ éléments parmi les 9 cycles ci-dessus et leurs inverses. Comme tous ces cycles sont de longueur impaire, il est dans A_{15}. Si le taquin A donné était dans $\mathscr{E}$ on aurait donc $\sigma(E_0)^{-1}\sigma(A) = (13\ \ 14) \in \mathrm{A}_{15}$, une contradiction.

(iii) La Formule (81) et le (i) montrent que l'ensemble G de l'énoncé est un sous-groupe de S_{15} inclus dans A_{15}. Mieux, c'est le sous-groupe de A_{15} engendré par les 9 cycles indiqués plus haut. On constate que G agit 3-transitivement sur $\{1, \dots, 15\}$. En effet, la transitivité est claire rien que grâce aux trois 7-cycles. La transitivité du stabilisateur G_1

sur $\{2,\dots,15\}$ est aussi claire à cause de $(2\,3\,4\,5\,6)$, $(5\,6\,7\,8\,9\ 10\ 11)$ et $(9\,10\ 11\ 12\ 13\ 14\ 15)$. Enfin, la transitivité du stabilisateur $(G_1)_2$ sur $\{3,\dots,15\}$ est encore claire à cause de $(3\,4\,5)$, $(5\,6\,7\,8\,9\ 10\ 11)$ et $(9\,10\ 11\ 12\ 13\ 14\ 15)$. On conclut par l'Exercice 4.23. Comme G contient le 3-cycle $(3\,4\,5)$, il contient par conjugaison tous les $(\sigma(3)\,\sigma(4)\,\sigma(5))$ avec $\sigma \in G$ et donc tous les 3-cycles par 3-transitivité de G. On a montré $G = \mathrm{A}_{15}$.

(iv) On a $\sigma(C)^{-1}\sigma(B) = (13\ \ 14)$ donc un seul de B ou C est un état du jeu de Taquin par le (iii). On a $\mathrm{s}(B) = (1\,2\,3\,7\,6\,5\,4\,8\,9\,10\,11\,15\,14\,13\,12)$, et donc on constate

$$\sigma(E_0)^{-1}\sigma(B) = \begin{bmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,9\ 10\ 11\ 12\ 13\ 14\ 15 \\ 1\,2\,3\,6\,7\,8\,4\,5\,9\ 10\ 11\ 13\ 14\ 15\ 12 \end{bmatrix},$$

qui vaut aussi $(4\,6\,8\,5\,7)(12\,13\,14\,15)$. Il n'est pas dans A_{15} : c'est le C qui est un état du taquin.

(v) Il est clair que l'on a $\mathrm{s}(F) = \mathrm{s}(F')$ si, et seulement si, F' est obtenu à partir de F et d'un déplacement de la case vide le long du serpent. Il y a donc exactement 16 tels F' à F donné. Il est équivalent de se donner $\mathrm{s}(F)$ et $\sigma(F)$, ou encore son translaté $\sigma(E_0)^{-1}\sigma(F)$. L'application $\mathscr{E} \to G, F \mapsto \sigma(E_0)^{-1}\sigma(F)$, est donc injective, et toutes ses fibres ont 16 éléments. On en déduit $|\mathscr{E}| = 16|\mathrm{A}_{15}| = 16!/2$.

Exercice 4.16. (i) L'élément $f^{-1} \circ \sigma \circ f$ est une bijection de $\{1,\dots,n\}$ (composée de 3 bijections), *i.e.* dans S_n. Il y a donc un sens à considérer sa signature. Changer f en une autre bijection f' revient à écrire $f = f' \circ g$ avec $g \in \mathrm{S}_n$. On a alors $(f')^{-1} \circ \sigma \circ f' = g^{-1}(f^{-1} \circ \sigma \circ f)g$. On conclut car deux éléments conjugués de S_n ont même signature (voir par exemple le corrigé de la question (i) de l'Exercice 4.2).

(ii) Pour vérifier le (ii), on choisit un f et on utilise simplement $f^{-1} \circ \sigma\sigma' \circ f = (f^{-1} \circ \sigma \circ f)(f^{-1} \circ \sigma' \circ f)$ et le fait que la signature est un morphisme sur S_n. On définit bien sûr le groupe A_X comme le noyau de la signature.

(iii) On peut par exemple écrire $\tau = t_1 t_2 \dots t_r$ où les t_i sont des transvections de Y. On constate alors que l'on a $\sigma = t'_1 t'_2 \dots t'_r$ où t'_i est l'unique transposition de X à support dans Y et coïncidant avec t_i sur Y. On a bient $\epsilon(\tau) = (-1)^r = \epsilon(\sigma)$.

Exercice 4.17. Soit $f : G \to \mathrm{S}_G, g \mapsto \mathrm{m}_g$, le morphisme donné par l'action de Cayley. En le composant avec la signature $\epsilon : \mathrm{S}_G \to \{\pm 1\}$, on en déduit un morphisme $\epsilon \circ f : G \to \{\pm 1\}$. Comme G est simple, ce morphisme est soit trivial, soit injectif, et ce dernier cas ne se produit que si on a $|G| \leqslant 2$. On suppose désormais $|G| > 2$, et donc $\epsilon \circ f = 1$.

Pour $g \in G$, regardons la décomposition en cycles de la bijection $\mathrm{m}_g : G \to G, h \mapsto gh$. Pour cela, on introduit l'ordre d de g, ainsi que des représentants $h_1,\dots,h_n \in G$ de $\langle g\rangle\backslash G$ (classes à droite). Tout $h \in G$ s'écrit de manière unique sous la forme $g^i h_j$ avec $1 \leqslant j \leqslant n$ et $0 \leqslant i < d$, et on a $dn = |G|$. On en déduit que m_g est un produit de n d-cycles à supports disjoints. Sa signature $\epsilon(\mathrm{m}_g)$ vaut donc $(-1)^{(d-1)n}$.

Supposons maintenant $|G|$ pair, et par Cauchy, que l'on a choisi $g \in G$ d'ordre $d = 2$. On a $\epsilon(\mathrm{m}_g) = (-1)^n = 1$, et donc $n = |G|/2$ est pair, et $|G| \equiv 0 \bmod 4$.

Exercice 4.11. (i) On pose $G = \mathrm{A}_4$ et $K = \mathrm{K}_4$. On a $K \lhd G$. Soit H le sous-groupe $\langle (1\,2)(3\,4)\rangle$ de K_4. C'est un sous-groupe d'ordre 2 et distingué dans K_4, ce dernier étant abélien. Mais il n'est pas distingué dans A_4, car $(1\,2\,3)(1\,2)(3\,4)(1\,2\,3)^{-1} = (2\,3)(1\,4) \notin H$.

(ii) Soit $g \in G$. Alors l'automorphisme $\alpha := \mathrm{int}_g$ de G vérifie $\alpha(K) = K$ car K est distingué dans G, de sorte que l'on a $\alpha_{|K} \in \mathrm{Aut}(K)$. Comme H est caractéristique dans K, on a $\alpha_{|K}(H) = H$, i.e. $gHg^{-1} = H$. On a montré que H est distingué dans G.

Exercice 4.13. (i) Supposons que σ possède un cycle c de cardinal pair. Alors $\tau = c$ convient. Supposons que σ possède deux cycles de même cardinal m impair, disons $(i_1\, i_2\, \dots\, i_m)$ et $(j_1\, j_2\, \dots\, j_m)$. Alors $\tau = (i_1\, j_1)(i_2\, j_2)\dots(i_m\, j_m)$ est de signature $(-1)^m = 1$ et vérifie $\tau\sigma\tau^{-1} = \sigma$. Si σ a deux points fixes i et j alors $\tau = (i\, j)$ convient aussi. Supposons enfin $\sigma = c_1 c_2 \cdots c_r$ avec les c_i de longueur impaires distinctes, et au plus un point fixe. Soient C le centralisateur de σ dans S_n et $\tau \in C$. On sait que les cycles de $\tau\sigma\tau^{-1} = \sigma$ sont les $\tau c_i \tau^{-1}$. Par unicité des longueurs des cycles, on a donc $\tau c_i \tau^{-1} = c_i$ pour tout i. En particulier, τ préserve le support S_i de chaque c_i, ainsi que l'éventuel point fixe de σ. Quitte à multiplier τ par un élément du sous-groupe $H = \langle c_1, c_2, \dots, c_r\rangle \subset C$, on peut supposer que τ admet un point fixe dans chacun des S_i. La formule $\tau c_i \tau^{-1} = c_i$ montre alors $\tau_{|S_i} = \mathrm{id}_{S_i}$, puis $\tau = 1$. On a montré $C = H$. On conclut car $\varepsilon(c_i) = 1$ pour tout i, et donc $\varepsilon(C) = \{1\}$.

(ii) Supposons $\sigma \in \mathrm{A}_n$ non spécial. Soit $\tau \in \mathrm{S}_n$ avec $\tau\sigma = \sigma\tau$ et $\varepsilon(\tau) = -1$. Pour tout $g \in \mathrm{S}_n \smallsetminus \mathrm{A}_n$ on a $g\sigma g^{-1} = g\tau\sigma(g\tau)^{-1}$ avec $g\tau \in \mathrm{A}_n$. L'inclusion évidente $\mathrm{Conj}_{\mathrm{A}_n}(\sigma) \subset \mathrm{Conj}_{\mathrm{S}_n}(\sigma)$ est donc une égalité.

(iii) Supposons $\sigma \in \mathrm{A}_n$ spécial et fixons $s \in \mathrm{S}_n \smallsetminus \mathrm{A}_n$. On a $\mathrm{S}_n = \mathrm{A}_n \coprod \mathrm{A}_n s$ car A_n est d'indice 2 dans S_n. On en déduit que pour $g \in \mathrm{S}_n \smallsetminus \mathrm{A}_n$, on a $g = hs$ pour un certain $h \in \mathrm{A}_n$, puis $g\sigma g^{-1} = hs\sigma s^{-1}h^{-1}$. Cela montre $\mathrm{Conj}_{\mathrm{S}_n}(\sigma) = \mathrm{Conj}_{\mathrm{A}_n}(\sigma) \cup \mathrm{Conj}_{\mathrm{A}_n}(s\sigma s^{-1})$. Supposons enfin que l'on a $g\sigma g^{-1} = hs\sigma s^{-1}h^{-1}$ avec g, h dans A_n. Alors l'élément $s^{-1}h^{-1}g \in \mathrm{S}_n$ commute avec σ et il est de signature -1 : absurde.

(iv) Par le cours, des représentants des classes de conjugaison de S_4 incluses dans A_4 sont $1, (1\,2)(3\,4), (1\,2\,3)$. Les éléments 1 et $(1\,2)(3\,4)$ sont non spéciaux dans S_4, mais $(1\,2\,3)$ y est spécial. Des représentants des classes de conjugaison de A_4 sont donc $1, (1\,2)(3\,4), (1\,2\,3)$ et $(2\,1\,3)$ (on a pris $s = (1\,2)$). De même, des représentants des classes de conjugaison de S_5 incluses dans A_5 sont $1, (1\,2)(3\,4), (1\,2\,3)$ et $(1\,2\,3\,4\,5)$. Les éléments $1, (1\,2)(3\,4), (1\,2\,3)$ sont non spéciaux dans S_5, mais $(1\,2\,3\,4\,5)$ y est spécial. Des représentants des classes de conjugaison de A_4 sont donc $1, (1\,2)(3\,4), (1\,2\,3), (1\,2\,3\,4\,5)$ et $(2\,1\,3\,4\,5)$.

Exercice 4.18. On suppose que G agit transitivement sur X, avec $|X| = n$ et G fini.

(i) Soit $x \in X$. On a $\mathrm{O}_x = X$ car l'action est transitive. On a donc $|G| = |X||\mathrm{G}_x|$ par la formule orbite-stabilisateur, puis n divise $|G|$.

(ii) Par hypothèse, le morphisme $\mathrm{m} : G \to \mathrm{S}_X$ associé à l'action est injectif. On a $G \simeq \mathrm{m}(G)$, $\mathrm{m}(G)$ sous-groupe de S_X, et $\mathrm{S}_X \simeq \mathrm{S}_n$. On a donc $|G| \,|\, n!$ par Lagrange.

(iii) Soient $x_1, \dots, x_r$ des représentants des orbites de G dans X. On a donc $|X| = \sum_{i=1}^r |\mathrm{O}_{x_i}|$ par l'équation aux classes. Mais on a $G_x = \{1\}$ pour tout $x \in X$ par hypothèse, et donc $|G| = |\mathrm{O}_x|$ par la formule orbite-stabilisateur, puis $|X| = r|G|$.

Exercice 4.19. (i) On peut supposer $G = \mu_n$. Soit d un diviseur de n. On fait agir G sur μ_d par $G \times \mu_d \to \mu_d, (g, x) \mapsto g^{n/d}x$. C'est clairement une action transitive. On aurait aussi pu utiliser le point de vue $\mathbb{Z}/n\mathbb{Z}$, et observer que $\mathbb{Z}/n\mathbb{Z}$ agit sur $\mathbb{Z}/d\mathbb{Z}$ par $(\overline{m}, \overline{x}) \mapsto \overline{m + x}$.

(ii) On sait que deux actions transitives de G sont isomorphes si, et seulement si, elles ont un stabilisateur en commun. Mais on sait aussi que les sous-groupes du groupe cyclique μ_n sont les μ_d avec $d \,|\, n$. Le stabilisateur de 1 dans l'action ci-dessus est $\mu_{n/d}$. Cela conclut.

Exercice 4.20. Pour $n \geqslant 2$, on a une action transitive de S_n sur l'ensemble à 2 éléments $\{\pm 1\}$ donnée par $(\sigma, u) \mapsto \epsilon(\sigma)u$. (On peut bien sur transporter cette action en une action sur $\{1, 2\}$.) Ainsi, comme le souligne l'énoncé, on dispose d'une action transitive de S_3 sur $1, 2, 3$ et 6 éléments. Pour voir que ce sont les seuls, il suffit de voir d'après le cours que tout sous-groupe de S_3 est le stabilisateur d'un point dans une de ces 4 actions.

Soit donc H un sous-groupe de S_3. Si on a $H = \{1\}$, c'est le stabilisateur de n'importe quel point de l'action de Cayley (qui est libre). Si on a $H = \mathrm{S}_3$, c'est le stabilisateur de l'unique point de l'action triviale. Sinon, on a $|H| = 2$ ou $|H| = 3$ par Lagrange. Si on a $|H| = 3$, la seule possibilité est $H = \langle(1\,2\,3)\rangle = \mathrm{A}_3$: c'est le stabilisateur d'un point quelconque dans l'action sur $\{\pm 1\}$. Enfin si on a $|H| = 2$, alors H est engendré par une transposition $(i\,j)$, et si k est tel que $\{1, 2, 3\} = \{i, j, k\}$, alors H s'identifie au stabilisateur de $\{k\}$ dans l'action naturelle sur $\{1, 2, 3\}$.

Exercice 4.21. (i) L'action de Cayley étant libre et transitive, l'image de l'action de Cayley de S_3 convient. On peut par exemple nommer respectivement a, b, c, d, e, f les éléments 1, $(1\,2)$, $(2\,3)$, $(1\,3)$, $(1\,2\,3)$, $(1\,3\,2)$ de S_3. Le morphisme de Cayley $\mathrm{S}_3 \to \mathrm{S}_X, g \mapsto \mathrm{L}_g$, avec $X = \mathrm{S}_3 = \{a, b, c, d, e, f\}$, vérifie alors

$$\mathrm{L}_1 = 1,\ \mathrm{L}_{(1\,2)} = (a\,b)(c\,e)(d\,f),\ \mathrm{L}_{(2\,3)} = (a\,c)(b\,f)(d\,e),\ \mathrm{L}_{(1\,3)} = (a\,d)(b\,e)(c\,f),$$

$$\mathrm{L}_{(1\,2\,3)} = (a\,e\,f)(b\,d\,c) \ \text{ et } \ \mathrm{L}_{(1\,3\,2)} = (a\,f\,e)(b\,c\,d).$$

(ii) On procède de même que ci-dessus pour H_8. (iii) Supposons que S_n possède un sous-groupe isomorphe à H_8, ou ce qui revient au même, que l'on dispose d'une action fidèle de H_8 sur $X = \{1, \ldots, n\}$. Soient $x \in X$ et O_x son orbite sous H_8. Si le stabilisateur de x est trivial, on a $|\mathrm{O}_x| = |\mathrm{H}_8| = 8$ par la formule orbite-stabilisateur, et donc $n = |X| \geqslant |\mathrm{O}_x| = 8$, ce qui conclut. On peut donc supposer que le stabilisateur de chaque $x \in X$ est non trivial dans H_8. Mais on constate sur la description des sous-groupes de H_8 que tout sous-groupe non trivial contient -1. On en déduit que -1 agit trivialement sur X, contredisant le caractère fidèle de l'action de H_8 sur X.

Exercice 4.22. (i) En effet, G_x stabilise l'ensemble $Y = X \smallsetminus \{x\}$ qui a $p-1$ éléments. Toute orbite O_y de G_x dans Y est de cardinal $1 \leqslant d \leqslant p-1$. On a $d \mid |G_x|$ par la formule orbite-stabilisateur, et donc $d \mid |G|$ (Lagrange). Cela montre $d = 1$ par hypothèse sur p, donc $\mathrm{O}_y = \{y\}$: l'action est triviale.

(ii) Soit H un sous-groupe d'indice p dans G. On fait agir G par translations sur $X = G/H$, qui a p éléments. Le stabilisateur de H est H lui-même. Par le (i), il agit trivialement sur G/H : on a donc $H \subset \mathrm{Stab}_G(gH) = gHg^{-1}$ pour tout $g \in G$, puis $H \lhd G$.

Exercice 4.23. (i) Posons $Y = X \smallsetminus \{x\}$. Alors G_x agit naturellement sur Y. On a clairement $|X| \geqslant k+1 \iff |Y| \geqslant k$. Supposons que G agit $k+1$-transitivement sur X. Alors G agit transitivement sur X. Soient $(x_1, \ldots, x_k)$ et $(y_1, \ldots, y_k)$ deux k-uples d'éléments distincts de Y. Alors $(x, x_1, \ldots, x_k)$ et $(x, y_1, \ldots, y_k)$ sont des $k+1$-uples d'éléments distincts de X. Par $k+1$-transitivité de l'action de G, il existe $g \in G$ avec $g(x) = x$ et $g(x_i) = y_i$ pour $i = 1, \ldots, k$. On a donc $g \in G_x$, et G_x est bien k-transitif sur Y. Réciproquement supposons que G agit transitivement sur X, et que G_x agit k-transitivement sur Y. Soient $(x_1, \ldots, x_{k+1})$ et $(y_1, \ldots, y_{k+1})$ des $k+1$-uples d'éléments distincts dans X. Par transitivité de G sur X, il existe $g, h \in G$ tels que $g(x_1) = x$ et $h(y_1) = x$. Les k-uples $(g(x_2), \ldots, g(x_{k+1}))$ et $(h(y_2), \ldots, h(x_{k+1}))$ sont bien constitués d'éléments distincts de Y. Par k-transitivité de G_x sur Y, il existe $\sigma \in G_x$ vérifiant $\sigma(g(x_i)) = h(y_i)$ pour tout $2 \leqslant i \leqslant k+1$. Ainsi, l'élément $h^{-1}\sigma g$ envoie x_i sur y_i pour $2 \leqslant i \leqslant k+1$, et aussi pour $i = 1$.

(ii) On a $|G| = |X||G_x|$ car G agit transitivement sur X, par la formule orbite stabilisateur. On raisonne par récurrence sur k. Le cas $k = 1$ est simplement la formule que l'on vient d'écrire. Pour $k > 1$ on sait que G_x agit $k-1$ transitivement sur $Y = X \smallsetminus \{x\}$, et donc $|G_x|$ est multiple de $|Y|(|Y|-1)\cdots(|Y|-k+2)$. On conclut par $|G| = |X||G_x|$ et $|Y| = |X| - 1$.

(iii) Le fait que S_n et A_n agissent respectivement n-transitivement et $n-2$ transitivement sur $\{1, \ldots, n\}$ est du cours. Réciproquement, si $G \subset \mathrm{S}_n$ agit $n-2$ transitivement

sur $\{1,\dots,n\}$ on a $\frac{n!}{2}$ divise $|G|$ par le (ii). On en déduit que G est d'indice 1 ou 2. Mais on a vu à l'Exercice 4.2 que A_n est l'unique sous-groupe d'indice 2 de S_n.

Exercice 4.24. (i) On pose $c = (1\,2\,3\,4\,5)$, $t = (1\,2)(3\,6)(5\,4)$. L'orbite de 6 sous l'action de G contient $3 = t(6)$, puis $\{1,2,3,4,5\} = \{c^i(3) \mid i \in \mathbb{Z}\}$, ainsi bien sûr que 6 : l'action en question de G est donc transitive. Pour montrer qu'elle est 2-transitive, on utilise le (i) de l'exercice précédent. Il suffit de voir que G_6 agit transitivement sur $\{1,2,3,4,5\}$, mais c'est clair car on a $c \in \mathrm{G}_6$. On constate enfin que l'on a

$$c\,t = (1\,2\,3\,4\,5)\,(1\,2)(3\,6)(5\,4) = (1\,3\,6\,4).$$

Mais toujours par le (i) de l'exercice précédent, l'action de G est 3-transitive si, et seulement si, celle de $G_2 \cap G_5$ est transitive sur $\{1,3,4,6\}$. On conclut car on vient de voir $(1\,3\,6\,4) \in G_2 \cap G_5$.

(ii) On a donc $|G|$ divisible par $6 \cdot 5 \cdot 4 = 120$ par le (ii) de l'exercice précédent. Mais on a construit dans le cours un morphisme $f : \mathrm{S}_5 \to \mathrm{S}_X$ avec $X = \{a,b,c,d,e,f\}$ envoyant $(1\,2)$ sur $(a\,d)(b\,c)(e\,f)$ et $(1\,2\,3\,4\,5)$ sur (b,c,d,e,f). Identifiant X à $\{1,\dots,6\}$ en envoyant respectivement a,b,c,d,e,f sur $6,1,2,3,4,5$, et donc S_X à S_6, on a alors $t = f((1\,2))$ et $c = f((1\,2\,3\,4\,5))$. On a donc $G \subset f(\mathrm{S}_5)$. Mais on a à la fois $|f(\mathrm{S}_5)|\,|\ker f| = |\mathrm{S}_5| = 120$ et $|G| \geqslant 120$. Cela montre $\ker f = \{1\}$ et $G = f(\mathrm{S}_5) \simeq \mathrm{S}_5$.

Exercice 4.25. (i) Les égalités données se vérifie immédiatement en appliquant l'algorithme donnant la décomposition en cycle d'une permutation. Étant donné la notation pour les types discutée en cours, les éléments a, b, b^2a, $[a,b]$ et aba sont respectivement de type 11, $1^3\,4^2$, $1^2\,3^3$, $1\,5^2$ et $1\,2\,8$.

(ii) Comme $G := \mathrm{M}_{11}$ possède un 11-cycle, il agit transitivement sur $E = \{1,2,\dots,11\}$. On va appliquer de nombreuses fois le critère de multiple transitivité de l'Exercice 4.23 (i). Observons que si G possède un élément g ayant un point fixe x dans E, alors pour tout $y \in E$, il existe $h \in G$ de même type que g, et avec en outre $h(y) = y$. En effet, comme G agit transitivement sur E, il existe $\sigma \in G$ avec $\sigma(x) = y$, et $h = \sigma g \sigma^{-1}$ convient. On déduit de cela que pour tout $x \in E$, le stabilisateur G_x de x dans G, qui agit naturellement sur $E' = E \smallsetminus \{x\}$, possède des éléments de type $1^2\,4^2$, $1\,3^3$, 5^2 et $2\,8$ vus dans $\mathrm{S}_{E'}$. La présence de $2\,8$ et 5^2 par exemple montre que G_x agit transitivement sur E'. Rappliquant l'observation ci-dessus à G_x agissant sur E', on en déduit que pour tout $y \in E'$, $(G_x)_y = G_x \cap G_y$ possède des éléments de types $1\,4^2$ et 3^3 vus comme éléments de $\mathrm{S}_{E''}$ avec $E'' = E \smallsetminus \{x,y\}$. Cela force la transitivité de $(G_x)_y$ sur E''. C'est assez clair ! On peut dire qu'une orbite de ce dernier doit être de cardinal à la fois multiple de 3, et égal à 1, 4, $1+4$, $4+4$ ou $1+4+4$. La seule possibilité est le cardinal 9.

(iii) On a vu que G agit 3-transitivement sur E. En particulier, il permute transitivement les parties à 3 éléments de E. Soit F une telle partie. Noter que G_F préserve F et son complémentaire $E \smallsetminus F$, mais que G_F n'agit pas nécessairement trivialement sur F. D'après le (i), observons que G_F contient des éléments de type 4^2, $1^2\,3^2$ et 8 vus comme éléments de $\mathrm{S}_{E \smallsetminus F}$ (c'est une variante de l'observation du (ii)). Il suffit de voir que si G possède un élément g ayant une partie stable $S \subset E$ à 3 él'ements, alors il existe $h \in G_F$ tel que $h_{|F}$ a même type que $g_{|S}$ et $h_{|E \smallsetminus F}$ a même type que $g_{|E \smallsetminus S}$. Mais comme G agit permute transitivement les parties à 3 éléments de E, il existe $\sigma \in G$ avec $\sigma(S) = F$, et $h = \sigma g \sigma^{-1}$ convient. Cela conclut l'observation. Comme G_F possède un élément qui agit comme un 8-cycle sur $E \smallsetminus F$, il agit bien transitivement sur $E \smallsetminus F$, puis transitivement sur les parties à 4 éléments de E.

(iv) et (v) Comme G agit transitivement sur les parties à 4 éléments de E, l'argument ci-dessus et le (i) montrent que G_F contient des éléments de type $1\,3$ et 4 vus comme permutations de F. Il reste à voir qu'un sous-groupe H de S_4 engendré par un 4-cycle

et un 3 cycle est S_4. On peut le faire à la main, ou observer que le cardinal de H serait multiple de $3 \cdot 4 = 12$ par Lagrange, donc H serait d'indice 1 ou 2. Mais A_4 est l'unique sous-groupe d'ordre 12 de S_4 (Exercice 4.2), et H contient un 4-cycle, non dans A_4, on a donc bien $H = \mathrm{S}_4$.

(vi) La seconde assertion découle de la première et du (ii) de l'Exercice 4.23. Pour la première, soient (x_1, x_2, x_3, x_4) et (y_1, y_2, y_3, y_4) des 4-uples d'éléments distincts de E. On pose $X = \{x_1, x_2, x_3, x_4\}$ et $Y = \{y_1, y_2, y_3, y_4\}$. Par le (iii), il existe $g \in \mathrm{M}_{11}$ avec $g(X) = Y$. Posons $x'_i = g(x_i)$ pour tout $1 \leqslant i \leqslant 4$. Par le (iv), il existe $h \in \mathrm{G}_Y$ avec $h(x'_i) = y_i$ pour tout $1 \leqslant i \leqslant 4$. L'élément $gh \in G$ envoie bien x_i sur y_i pour tout $1 \leqslant i \leqslant 4$.

Exercice 4.26. (i) On a $Hn = nn^{-1}Hn = nH$ pour tour $n \in N$, puis $gHn = gnH$ pour tout $g \in G$ et $n \in N$. La multiplication à droite par $n \in N$ dans $\mathrm{P}(G)$ préserve donc G/H. Elle est bijective d'inverse la multiplication à droite par n^{-1}. C'est trivialement un isomorphisme de $(G/H, \bullet)$: on a $g' \bullet (gHn) = (g' \bullet gH)n = g'gHn$ pour tout $g, g' \in G$ (les multiplications à droite et à gauche commutent...).

(ii) L'application $N \times G/H \to G/H, (n, gH) \mapsto gHn^{-1}$, définit manifestement une action de N sur G/H, et donc un morphisme associé $f : N \to \mathrm{S}_{G/H}$. Notons $A \subset \mathrm{S}_{G/H}$ le sous-groupe des automorphismes de $(G/H, \bullet)$. On a vérifié au (i) que l'on a $f(N) \subset A$. Remarquons que $\ker f$ est le sous-groupe des $n \in N$ vérifiant $gHn = gH$ pour tout $g \in G$, ce qui équivaut à $n \in H$, on a donc $\ker f = H$. Choisissons enfin $\varphi \in A$. On a $\varphi(gH) = g\varphi(H)$ pour tout $g \in G$. Soit $n \in G$ tel que $\varphi(H) = nH$. On a donc $nH = \varphi(H) = \varphi(hH) = h\varphi(H) = hnH$ pour tout $h \in H$. Cela implique $n^{-1}Hn \subset H$. En considérant de même $\varphi^{-1} \in A$, qui envoie nH sur H et donc H sur $n^{-1}H$, on a l'inclusion dans l'autre sens $nHn^{-1} \subset H$, puis $nHn^{-1} = H$. On a montré $n \in N$, puis $\varphi(H) = Hn$, $\varphi(gH) = gHn$, et donc $\varphi = f(n)$. Ainsi, f induit un isomorphisme $N/H \xrightarrow{\sim} A$.

Exercice 4.27. (i) Soit $x \in X$. On a $\mathrm{O}_x = \{g \bullet x \mid g \in G\}$. Comme on a $f(g \bullet x) = g \star f(x)$ pour $g \in G$, on a donc $f(\mathrm{O}_x) = \{g \star f(x) \mid g \in G\} = \mathrm{O}_{f(x)}$. Ainsi, $f(X_i)$ est une G-orbite dans Y : c'est Y_j pour un unique $j \in J$.

(ii) La restriction f_i de f à X_i définit donc une bijection $X_i \to Y_j$ où $j = \varphi(i)$. On a $f_i(g \bullet x) = f(g \bullet x) = g \star f(x) = g \star f_i(x)$ pour $x \in X_i$, donc f_i est un isomorphisme entre $(X_i, \bullet)$ et $(Y_j, \star)$. L'action de G sur X_i (resp. Y_j) est transitive car X_i (resp. Y_j) est une G-orbite. Comme f est surjective la fonction $\varphi : I \to J$ l'est aussi. Vérifions qu'elle est injective. Supposons $i, i' \in I$ distincts. On a $X_i \cap X_{i'} = \varnothing$ et donc on a $f(X_i) \cap f(X_{i'}) = \varnothing$ car f est injective, cela conclut.

(iii) Réciproquement, supposons donnés une bijection $\varphi : I \to J$, et pour tout $i \in I$ un isomorphisme d'actions $f_i : X_i \xrightarrow{\sim} Y_{\varphi(i)}$. On définit $f : X \to Y$ par $f(x) = f_i(x)$ où i est l'unique élément de I tel que x est dans X_i. C'est clairement un isomorphisme d'actions car les f_i en sont.

Exercice 4.28. (i) Quitte à échanger i et j on peut supposer que l'on a $g^{i+1} = hg^ih^{-1}$ avec $h \in G$. On en déduit $g = g^{-i}\, h\, g^i\, h^{-1} = [g^{-j}, h]$.

(ii) Écrivons $g^i = h\, g^j\, h^{-1}$ avec $h \in G$. On a $g^{i-j} = [g^{-j}, h] \in \mathrm{D}(G)$. Soit $k \in \mathbb{Z}$ tel que $k(i-j) \equiv 1 \bmod n$. On a donc $g = (g^{i-j})^k \in \mathrm{D}(G)$.

Exercice 4.29. Soit $\pi : G \to G/\mathrm{D}(G)$ le morphisme canonique. Le groupe $G/\mathrm{D}(G)$ étant commutatif, tous ses sous-groupes sont distingués. Mais tout sous-groupe de G contenant $\mathrm{D}(G)$ est de la forme $\pi^{-1}(H)$ avec H sous-groupe de $G/\mathrm{D}(G)$, d'après le cours. On conclut car l'image inverse d'un sous-groupe distingué par un morphisme de groupes est encore distingué.

Exercice 4.30. Pour le (i), ce sont des vérifications triviales. Par exemple, on a $[x, yz] = xyzx^{-1}(yz)^{-1} = (xyx^{-1}y^{-1})y(xzx^{-1}z^{-1})y^{-1} = [x, y]\ {}^{y}[x, z]$. Pour le (ii), on a $[x, y^{n+1}] = [x, y^n y] = [x, y^n]\ {}^{y^n}[x, y]$ par le (i), et on conclut par récurrence sur n.

Exercice 4.31. (i) Le groupe $Z = \{\pm 1\}$ est central donc distingué dans H_8. La relation $[I, J] = IJI^{-1}J^{-1} = -1$ montre $-1 \in \mathrm{D}(H_8)$, donc $Z \subset \mathrm{D}(\mathrm{H}_8)$, et aussi que H_8/Z est commutatif, car il est engendré par les classe de I et J qui commutent modulo Z. On a donc $\mathrm{D}(\mathrm{H}_8) \subset Z$ puis $\mathrm{D}(\mathrm{H}_8) = Z$. On en déduit $\mathrm{H}_8/\mathrm{D}(\mathrm{H}_8) = \mathrm{H}_8/\{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(ii) Posons $G = \mathrm{D}_{2n}$. On a $G = \langle c, \tau \rangle$ comme dans le cours, avec $\tau c = c^{-1}\tau$. Le sous-groupe $C := \langle c \rangle$ est distingué et d'indice 2 dans G. On a donc $G/C \simeq \mathbb{Z}/2\mathbb{Z}$ (abélien) et donc $\mathrm{D}(G) \subset C$. D'autre part, on a aussi $\tau c \tau^{-1} c^{-1} = c^{-2} \in \mathrm{D}(G)$. Notons C' le sous-groupe de C engendré par c^2. On a montré $C' \subset \mathrm{D}(G)$. Si n est impair, on a $C' = C$ et donc $C = \mathrm{D}(G)$ et $G/\mathrm{D}(G) \simeq \mathbb{Z}/2\mathbb{Z}$. Si n est pair, alors C' est d'ordre $n/2$ et distingué dans G, car c^2 commute avec c et vérifie $\tau c^2 \tau^{-1} = c^{-2} \in C'$. Ainsi, G/C' est d'ordre 4, engendré par les images de c et τ. Mais on a $c^2 \in C'$, $\tau^2 \in C'$ et $[\tau, c] = c^{-2} \in C'$, on a donc $G/C' \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Comme G/C' est abélien on a $\mathrm{D}(G) \subset C'$, puis $\mathrm{D}(G) = C'$ et $G/\mathrm{D}(G) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercice 4.33. C'est un fait général que pour $\dim V \geqslant 2$, le groupe $\mathrm{GL}(V)$ agit 2-transitivement sur $\mathbb{P}(V)$. En effet, on a d'abord clairement $|\mathrm{P}(V)| > 2$. De plus, soient (D_1, D_2) et (D'_1, D'_2) deux couples de droites distinctes de V. Fixons $e_i \in D_i$ et $f_i \in D'_i$ des vecteurs non nuls. Alors e_1, e_2 est libre, ainsi que f'_1, f'_2. On peut donc les compléter en des bases respectives $\{e_i\}_{1 \leqslant i \leqslant n}$ et $\{f_i\}_{1 \leqslant i \leqslant n}$ de V, avec $n = \dim V$. Il existe un unique $g \in \mathrm{GL}(V)$ avec $g(e_i) = f_i$ pour tout i. Il vérifie $g(D_1) = D'_1$ et $g(D_2) = D'_2$.

Supposons maintenant V de dimension 2. Fixons $\{e_1, e_2\}$ une base de V et posons $L_1 = ke_1$, $L_2 = ke_2$ et $L_3 = k(e_1 + e_2)$. Soit $G \subset \mathrm{GL}(V)$ le sous-groupe des éléments g tels que $g(L_1) = L_1$ et $g(L_2) = L_2$. Par l'Exercice 4.23 (i), il suffit de montrer que l'action naturelle de G sur $X = \mathbb{P}(V) \smallsetminus \{L_1, L_2\}$ est transitive. Mais toute droite D de V distincte de L_1 et L_2 est engendrée par un (unique) vecteur de la forme $e_1 + \lambda e_2$ avec $\lambda \neq 0$. Soit $g \in \mathrm{GL}(V)$ l'unique élément avec $g(e_1) = e_1$ et $g(e_2) = \lambda e_2$. On a $g \in G$ et $g(L_3) = D$. Ainsi, X est l'orbite de L_3 sous G.

Exercice 4.34. (i) Ce sont des opérations élémentaires sur les lignes et les colonnes. Pour i, j notons $\mathrm{E}_{i,j} \in \mathrm{M}_n(k)$ la matrice élémentaire d'indice (i, j) égal à 1 et d'indice (p, q) nul pour $(p, q) \neq (i, j)$. Pour $i < j$, on a $\mathrm{e}_{i,j}(x) = 1_n + x\mathrm{E}_{i,j}$ dans $\mathrm{M}_n(k)$. Notons que pour i fixé, les $\mathrm{e}_{i,j}(x)$ avec $j > 1$ et $x \in k$ commutent deux à deux. Si $m = (m_{i,j}) \in \mathrm{U}_n(k)$, on constate que la matrice $m \prod_{j=2}^{n} \mathrm{e}_{1,j}(-m_{1,j})$ a sa première ligne nulle hors du coefficient diagonal (et même tous ses autres coefficients identiques à ceux de m). On conclut en raisonnant par récurrence dans le bloc $(n-1) \times (n-1)$.

(ii) Pour $i < j$ on a $\mathrm{e}_{i,j}(0) = 1$ et $\mathrm{e}_{i,j}(x)\mathrm{e}_{i,j}(y) = \mathrm{e}_{i,j}(x + y)$. En particulier, l'ensemble $Z \subset \mathrm{U}_n(k)$ des $\mathrm{e}_{1,n}(x)$, $x \in k$, est un sous-groupe de $\mathrm{U}_n(k)$ (isomorphe à $(k, +)$). Pour tout $t \in \mathrm{T}_n(k)$ on constate dans $\mathrm{M}_n(k)$ les égalités

$$t\,\mathrm{e}_{1,n}(x) = t + t_{1,1}x\,\mathrm{E}_{1,n} \quad \text{et} \quad \mathrm{e}_{1,n}(x)\,t = t + t_{n,n}x\,\mathrm{E}_{1,n}. \tag{82}$$

En particulier, Z est dans le centre de $\mathrm{U}_n(k)$. Montrons que le sous-groupe C des éléments de $\mathrm{T}_n(k)$ qui commute à tous les éléments de $\mathrm{U}_n(k)$ est $k^\times Z$. On a déjà vu $C \supset k^\times Z$. Réciproquement fixons $g \in C$. Écrivons matriciellement $g\ \mathrm{e}_{i,j} = \mathrm{e}_{j,i}\ g$ pour $i < j$. On en déduit $g_{i,i} = g_{j,j}$ et $g_{k,i} = 0$ pour $1 \leqslant k < i$ et $g_{j,k} = 0$ pour $j < k \leqslant n$. Cela conclut. De $C = k^\times Z$ on déduit $\mathrm{Z}(\mathrm{U}(k)) = Z$ et par la formule (82), $\mathrm{Z}(\mathrm{T}_n(k)) = k^\times$.

Exercice 4.35. (i) On a $(\mathbb{Z}/2\mathbb{Z})^\times = \{1\}$ et donc $\mathrm{T}_n(\mathbb{Z}/2\mathbb{Z}) = \mathrm{U}_n(\mathbb{Z}/2\mathbb{Z})$. Pour $n \geqslant 1$, on a toujours un morphisme surjectif $\mathrm{U}_n(k) \to k^{n-1}$ donné par la surdiagonale, et donc $\mathrm{D}(\mathrm{U}_n(k) \subsetneq \mathrm{U}_n(k)$ pour $n > 1$. On en déduit $\mathrm{D}(\mathrm{T}_n(\mathbb{Z}/2)) \subsetneq \mathrm{U}_n(\mathbb{Z}/2\mathbb{Z})$. Supposons

maintenant $k \neq \mathbb{Z}/2\mathbb{Z}$. Soient $1 \leqslant i < j \leqslant n$ et $x \in k$. Par le (i) de l'exercice précédent, il suffit de montrer $\mathrm{e}_{i,j}(x) \in \mathrm{D}(\mathrm{T}_n(k))$. Soit $t = \mathrm{diag}(t_1, \ldots, t_n)$ une matrice diagonale. Mais on constate

$$[t, \mathrm{e}_{i,j}(x) = t\mathrm{e}_{i,j}(x)t^{-1}\mathrm{e}_{i,j}(-x) = \mathrm{e}_{i,j}(t_i t_j^{-1}x)\mathrm{e}_{i,j}(-x) = \mathrm{e}_{i,j}((t_i t_j^{-1} - 1)x) \in \mathrm{D}(\mathrm{T}_n(k))$$

Comme $k \neq \mathbb{Z}/2\mathbb{Z}$, il existe $u \in k \smallsetminus \{0, 1\}$ et donc on peut choisir t avec $t_j = 1$ et $t_i = u$. On conclut car l'application $k \mapsto k, x \mapsto (u-1)x$ est bijective.

(ii) C'est un simple calcul à partir de $\mathrm{E}_{i,j}\mathrm{E}_{k,l} = \delta_{j,k}\mathrm{E}_{i,l}$ et de

$$[\mathrm{e}_{i,i+2^m}, \mathrm{e}_{i+2^m,i+2^{m+1}}] = (1 + \mathrm{E}_{i,i+2^m})(1 + \mathrm{E}_{i+2^m,i+2^{m+1}})(1 - \mathrm{E}_{i,i+2^m})(1 - \mathrm{E}_{i+2^m,i+2^{m+1}}).$$

(iii) On raisonne par récurrence sur $m \geqslant 0$ (le cas $m = 0$ est évident). On peut supposer $j = i + 2^{m+1} \leqslant n$. On a $\mathrm{e}_{i,i+2^m}$ et $\mathrm{e}_{i+2^m,i+2^{m+1}} \in \mathrm{D}^m(\mathrm{U}_n(k))$ par hypothèse de récurrence, puis $\mathrm{e}_{i,j} \in \mathrm{D}^{m+1}(\mathrm{U}_n(k))$ par le (ii).

(iv) On suppose $n \geqslant 2$. Soit m le plus grand entier tel que $1 + 2^m \leqslant n$. On a $\mathrm{e}_{1,1+2^m} \in \mathrm{D}^m(\mathrm{U}_n(k))$ par le (iii), et donc $\mathrm{D}^m(\mathrm{U}_n(k)) \neq \{1\}$. On en déduit que la classe c de résolubilité de $\mathrm{U}_n(k)$ est $\geqslant 1 + m$. Par définition, on a $m = \lfloor \log_2(n-1) \rfloor$. Par le cours (démonstration de la Proposition 6.13), on a aussi $c \leqslant \lceil \log_2(n) \rceil$. Pour conclure il suffit d'observer l'égalité $1 + \lfloor \log_2(n-1) \rfloor = \lceil \log_2(n) \rceil$. En effet, si on a $n = 2^k$ avec $k \geqslant 1$, alors on a $2^{k-1} < n - 1 < 2^k$ et donc l'égalité s'écrit $1 + k - 1 = k$. L'autre situation est $2^{k-1} < n < 2^k$, et donc $2^{k-1} \leqslant n - 1 < 2^k$, et l'égalité s'écrit encore $1 + k - 1 = k$.

Exercice 4.36. (i) L'action naturelle de $\mathrm{GL}(V)$ sur $\mathscr{F}$ sous-entendue dans l'énoncé est bien sûr $(g, (V_i)) \mapsto (g(V_i))$. Elle est bien définie car on a $\dim g(V_i) = \dim V_i$ et $V_i \subset V_j \implies g(V_i) \subset g(V_j)$. C'est manifestement une action. Montrons qu'elle est transitive. Soient $V_0 \subset V_1 \subset \cdots \subset V_n = V$ et $W_0 \subset W_1 \subset \cdots \subset W_n = V$ deux drapeaux de V. Par récurrence sur i, et par le théorème de la base incomplète, on peut trouver une base $e_1, \ldots, e_n$ de V telle que $V_i = \sum_{j=1}^{i} k\, e_j$ pour tout $i = 1, \ldots, n$. De même, on peut trouver une base $f_1, \ldots, f_n$ de V telle que $W_i = \sum_{j=1}^{i} k\, f_j$ pour tout $i = 1, \ldots, n$. Soit $g \in \mathrm{GL}(V)$ l'unique élément vérifiant $g(e_i) = f_i$ pour $i = 1, \ldots, n$. On a $g(V_i) = W_i$ pour tout i : l'action de l'énoncé est transitive.

(ii) Le stabilisateur du drapeau standard est par définition $\mathrm{T}_n(k)$. Montrons (iii). Un sous-groupe $G \subset \mathrm{GL}(V)$ préserve un drapeau $d = (V_i)$ si, et seulement si, il est inclus dans le stabilisateur $\mathrm{Stab}_{\mathrm{GL}(V)}(d)$ de ce drapeau. Mais par le (i) tout drapeau d s'écrit $d = p(s)$ où $s \in \mathscr{F}$ est le drapeau standard, et p est un certain élément de $\mathrm{GL}(V)$. Mais on a $\mathrm{Stab}_{\mathrm{GL}(V)}(d) = p\,\mathrm{Stab}_{\mathrm{GL}(V)}(s)\,p^{-1} = p\,\mathrm{T}_n(k)\,p^{-1}$ par le principe de conjugaison et le (ii). Cela conclut le (iii).

Exercice 4.37. (i) On pose $H = \mathrm{GL}_n(\mathbb{C})$. C'est à la fois un groupe et un ouvert du $\mathbb{C}$-espace vectoriel de dimension finie $\mathrm{M}_n(\mathbb{C})$, ce qui lui confère une structure d'espace topologique. Observons que la multiplication $H \times H \to H, (x, y) \mapsto xy$, et l'inversion $H \to H, x \mapsto x^{-1}$, sont toutes les deux continues : la première est polynomiale, et pour la seconde utiliser $x^{-1} = {}^{\mathrm{t}}\mathrm{Co}(x)(\det x)^{-1}$ et la continuité et non annulation du déterminant. (On dit que H est un *groupe topologique*). Il découle de ces observations que si X et Y sont des parties connexes de H, il en va de même de X^{-1} (image de X par l'inversion) et de XY (image du connexe $X \times Y$ par la multiplication). Si en outre X contient 1, alors on a $1 \in X^n$ pour tout $n \in \mathbb{Z}$ puis $X^n \cap X^m \neq \varnothing$, et donc $\langle X \rangle = \cup_{n \in \mathbb{Z}} X^n$ est connexe. On a montré que *le sous-groupe engendré par une partie connexe contenant* 1 *de* $\mathrm{GL}_n(\mathbb{C})$ est connexe. Considérons enfin G comme dans l'énoncé. L'ensemble des commutateurs $C = \{[x, y] \mid (x, y) \in G \times G\}$ est une partie connexe de G, comme image du connexe $G \times G$ par l'application continue $H \times H \to H, (x, y) \mapsto xyx^{-1}y^{-1}$. Ainsi, C est un connexe contenant 1, et donc $\mathrm{D}(G) = \langle C \rangle$ est connexe.

(ii) Pour $g, h \in \mathrm{GL}_n(\mathbb{C})$ on a $\det([g,h]) = [\det(g), \det(h)] = 1$ car $\mathbb{C}^\times$ est commutatif. Montrons le (iii). Si $\mathrm{D}(G)$ est constitué d'homothéties, alors ces homothéties sont de rapport $\lambda \in \mathbb{C}^\times$ avec $\lambda^n = 1$ par le (ii). Mais par le (i) $\mathrm{D}(G)$ est connexe. Le seul sous-groupe connexe de $\mathbb{C}^\times$ inclus dans μ_n est $\{1\}$. On a donc $\mathrm{D}(G) = 1$, c'est-à-dire G abélien. Les éléments de G sont trigonalisables et commutent : ils sont donc co-trigonalisables par un exercice classique.

(iv) Choisissons une base $e = (e_1, \ldots, e_n)$ de $\mathbb{C}^n$ telle que $e_1, \ldots, e_m$ est une base de W. Par hypothèse on a $1 \leqslant m = \dim W < n$. De plus, pour tout $g \in G$ on a

$$\mathrm{Mat}_e g = \begin{bmatrix} A(g) & B(g) \\ 0 & C(g) \end{bmatrix} \text{ avec } A(g) \in \mathrm{GL}_m(\mathbb{C}) \text{ et } B(g) \in \mathrm{GL}_{n-m}(\mathbb{C}).$$

Les applications $A : G \to \mathrm{GL}_r(\mathbb{C}), g \mapsto A(g)$, et $B : G \to \mathrm{GL}_{n-m}(\mathbb{C}), g \mapsto B(g)$, sont des morphismes de groupes, et sont manifestement continues. Ainsi, les groupes images $A(G)$ et $B(G)$ sont connexes (images continues d'un connexe) et quotients de G, donc résolubles et de classe respective $a, b \leqslant r$. On a $m + a < n + r$ et $m - n + b < n + r$. Par récurrence, $A(G)$ et $B(G)$ sont donc co-trigonalisables. Quitte à changer de base e, cela montre que l'on peut supposer que $A(G)$ et $B(G)$ sont triangulaires supérieurs dans la base e, ainsi donc que G.

(v) La classe de résolubilité de $\mathrm{D}(G)$ est $r - 1$, et $\mathrm{D}(G)$ est connexe par le (i). Par hypothèse de récurrence, $\mathrm{D}(G)$ est co-trigonalisable. En particulier, il existe une droite $D \subset V$ stable par tout élément de $\mathrm{D}(G)$. Soit e une base de D, *i.e.* $D = \mathbb{C}e$. Pour tout $g \in \mathrm{D}(G)$, il existe un unique $\lambda_g \in \mathbb{C}^\times$ tel que $g(e) = \lambda_g e$. On a donc $\lambda_{gh} e = gh(e) = g(h(e)) = \lambda_h g(e) = \lambda_g \lambda_h e$, puis $\chi(g) := \lambda_g$ définit un caractère de $\mathrm{D}(G)$. On a $e \in V_\chi$, et donc $\chi \in S$.

(vi) Soit $X \subset S$ de cardinal non nul et minimal tel qu'il existe une relation $0 = \sum_{\chi \in X} v_\chi$ avec v_χ non nul et dans V_χ pour tout $\chi \in X$. Soient $\alpha \in X$ et $g \in G$. Appliquant $\alpha(g)\mathrm{id} - g$ à cette relation on trouve $0 = \sum_{\chi \in X} (\alpha(g) - \chi(g)) v_\chi$. Le coefficient $\alpha(g) - \chi(g)$ est nul pour $\alpha = \chi$, et donc on a $\alpha(g) = \chi(g)$ pour tout $\chi \in X$ et tout $g \in G$ par minimalité de la relation. Cela montre $X = \{\alpha\}$, puis $0 = v_\alpha$, une contradiction.

(vii) La somme des V_χ étant directe par le (vi) on a $n \geqslant \dim V = \sum_{\chi \in S} \dim V_\chi$. Mais on a $\dim V_\chi \geqslant 1$ pour $\chi \in S$ par définition de S. On a donc $|S| \leqslant n$.

(viii) On sait que $\mathrm{D}(G)$ est distingué dans G, donc pour $g \in G$ la restriction de int_g à $\mathrm{D}(G)$ est un automorphisme de $\mathrm{D}(G)$. Pour $\chi \in \mathscr{C}$ on constate que l'on a ${}^g\chi = \chi \circ \mathrm{int}_{g^{-1}}$: c'est donc bien un élément de $\mathscr{C}$. De plus, on a $\chi^1 = \chi$ et ${}^g({}^h\chi)(x) = {}^h\chi(g^{-1}xg) = \chi(h^{-1}g^{-1}xgh) = \chi((gh)^{-1}x(gh)) = {}^{gh}\chi(x)$ pour $g, h \in G$ et $x \in \mathrm{D}(G)$. Ainsi, $G \times \mathscr{C} \to \mathscr{C}, (g, \chi) \mapsto {}^g\chi$, est une action de G sur $\mathscr{C}$.

Si on a $v \in V_\chi$ et $g \in G$, on a $g(v) \in V_{{}^g\chi}$. En effet, pour $h \in \mathrm{D}(G)$ et $g \in G$ on a $g^{-1}hg \in \mathrm{D}(G)$ et donc $hgv = g(g^{-1}hg)v = g\chi(g^{-1}hg)v = {}^g\chi(h)gv$. On a donc montré $g(V_\chi) \subset V_{{}^g\chi}$ pour tout $g \in G$ et tout $\chi \in \mathscr{C}$. Appliquant ceci à g^{-1} et ${}^g\chi$, on a l'égalité de l'énoncé.

(ix) Fixons $\chi \in S$. La dernière assertion du (viii) montre que pour $g \in G$ on a ${}^g\chi \in S$. Comme S est fini, l'ensemble des ${}^g\chi$ est donc fini. En particulier, pour $h \in \mathrm{D}(G)$ donné et $v \in V_\chi$, l'application $G \to \mathbb{C}^\times, g \mapsto \chi(ghg^{-1})$, est d'image finie. Admettons temporairement que l'application $\chi : \mathrm{D}(G) \to \mathbb{C}^\times, x \mapsto \chi(x)$, est continue. Comme G est connexe, l'application ci-dessus est alors constante. On en déduit ${}^g\chi = \chi$, ce qui était demandé. Vérifions enfin la continuité de χ. Pour tout $v \in \mathbb{C}^n$, l'application $G \to \mathbb{C}^n$, $g \mapsto g(v)$, est continue, et si on choisit $v \in V_\chi$ non nul, elle coïncide avec $g \mapsto \chi(g)v$ sur $\mathrm{D}(G)$.

(x) Par le (v) on a $S \neq \emptyset$. Fixons donc $\chi \in S$. Soit $g \in G$. Par le (ix), on a ${}^g\chi = \chi$, et donc $g(V_\chi) = V_\chi$ par le (ii). On en déduit que G stabilise V_χ. Par le (iv), on conclut si $\dim V_\chi < n$. Mais si $V_\chi = V$, alors $\mathrm{D}(G)$ agit par homothéties sur V, et on conclut encore par le (iii).

(xi) Le sous-groupe $\mathrm{H}_8 \subset \mathrm{GL}_2(\mathbb{C})$ est résoluble mais pas co-trigonalisable. En effet, les seules droites stables de $I = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$ sont $\mathbb{C}\epsilon_1$ et $\mathbb{C}\epsilon_2$, mais aucune des deux n'est stable par J.

Exercice 4.38. Pour $m, m' \in \mathbb{Z}/n\mathbb{Z}$ et $k, k' \in \mathbb{Z}/2\mathbb{Z}$ on a dans le groupe G_s la relation $(m', k')(m, k) = (m' + s^{k'}m, k' + k)$. Ainsi, (m, k) est dans le centre de G_s si, et seulement si, on a $sm = m$. Soit H_s le sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ défini par $H = \{m \in \mathbb{Z}/n\mathbb{Z} \mid sm = m\}$. On a montré $\mathrm{Z}(G_s) \simeq H_s \times \mathbb{Z}/2\mathbb{Z}$ (groupe produit).

Notons s_p et $s_q \in \{\pm 1\}$ les signes tels que $s \equiv s_p \bmod p$ et $s \equiv s_q \bmod q$. L'isomorphisme chinois identifie H_s au sous-groupe des $(x, y) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ vérifiant $s_p x = x$ et $s_q y = y$. Pour l impair et $x \in \mathbb{Z}/l\mathbb{Z}$, on a $-x = x \iff x = 0$. On en déduit

$$H_{-1} = 0, \;\; H_1 \simeq \mathbb{Z}/pq\mathbb{Z}, \;\; H_a \simeq \mathbb{Z}/p\mathbb{Z} \;\text{ et }\; H_b \simeq \mathbb{Z}/q\mathbb{Z}.$$

Ainsi, pour $s = -1, 1, a$ et b respectivement, le centre de G_s est cyclique d'ordre $2, 2pq, 2p$ et $2q$ respectivement.

Exercice 4.39. Soit $a \in \mathrm{Aut}(G)$. Considérons le morphisme de groupes $\alpha : \mathbb{Z} \to \mathrm{Aut}(G), n \mapsto a^n$. On pose $G' = G \rtimes_\alpha \mathbb{Z}$. On a un morphisme injectif $f : G \to G', g \mapsto (g, 0)$. Soit $x = (0, 1) \in G'$. On conclut car pour $g \in G$ on a

$$xf(g)x^{-1} = (0, 1) \star_\alpha (g, 0) \star_\alpha (0, -1) = (a(g), 1) \star_\alpha (0, -1) = (a(g), 0) = f(a(g)).$$

Exercice 4.40. (i) Par Cauchy, G possède un élément x d'ordre p, et un élément y d'ordre q. On pose $P = \langle x \rangle$ et $Q = \langle y \rangle$. Comme Q est d'indice p, le plus petit facteur premier de $|G|$, alors il est distingué par le Lemme de Ore (Exercice 4.22).

(ii) Le sous-groupe $P \cap Q$ est un sous-groupe de P et de Q, d'ordres premiers entre eux, et donc $P \cap Q = \{1\}$ par Lagrange. On a aussi $|G| = pq = |P||Q|$. On sait donc que Q et P sont complémentaire. Comme Q est distingué, on a donc $G = Q \rtimes P$ (produit semi-direct interne) et un morphisme $\alpha : P \to \mathrm{Aut}(Q), p \mapsto \mathrm{int}_{p|Q}$. Comme Q est cyclique d'ordre q, on sait que l'on a $\mathrm{Aut}(Q) \simeq (\mathbb{Z}/q\mathbb{Z})^\times$, puis $|\mathrm{Aut}(Q)| = q - 1$ car q est premier. Tout morphisme $f : G \to G'$ avec G et G' finis de cardinaux premiers entre eux étant trivial, on a donc $\alpha = 1$ si p ne divise pas $q - 1$. Dans ce cas, on a donc $xy = yx$, et donc xy est d'ordre pq car p et q sont premiers entre eux, puis $G = \langle xy \rangle$ est cyclique d'ordre pq.

(iii) On suppose désormais $p \,|\, |\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})| = q - 1$. Dans ce cas $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ possède un élément c d'ordre p. Concrètement, il existe un élément $u \in (\mathbb{Z}/q\mathbb{Z})^\times$ d'ordre p et on a $c(m) = um$ pour $m \in \mathbb{Z}/q\mathbb{Z}$. Il existe donc un morphisme injectif $\beta : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ avec $\beta_{\overline{1}} = c$, i.e. $\beta_{\overline{1}}(m) = um$. Le groupe $\Gamma_{p,q} = \mathbb{Z}/q\mathbb{Z} \rtimes_\beta \mathbb{Z}/p\mathbb{Z}$ convient. En effet, il n'est pas commutatif car c n'est pas l'identité : on a $(0, 1) \star_\beta (m, 0) \star_\beta (0, 1)^{-1} = (c(m), 0)$ pour tout $x \in \mathbb{Z}/q\mathbb{Z}$.

(iv) On raffine l'analyse du (ii). On a $G = Q \rtimes P$ et $\alpha : P \to \mathrm{Aut}(Q), p \mapsto \alpha_p$, le morphisme associé. Si $\alpha = 1$ on conclut $G \simeq \mathbb{Z}/pq\mathbb{Z}$ comme au (ii), donc on peut supposer $\alpha \neq 1$. On rappelle l'isomorphisme $(\mathbb{Z}/q\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Aut}(Q), k \mapsto \varphi_k$, défini par $\varphi_k(g) = g^k$. Comme $(\mathbb{Z}/q\mathbb{Z})^\times$ est cyclique d'ordre $q - 1 \equiv 0 \bmod p$, il a un unique sous-groupe d'ordre p, nécessairement cyclique. En particulier, si $u \in (\mathbb{Z}/q\mathbb{Z})^\times$ est l'élément d'ordre p choisi au (ii), les autres sont les u^k avec $k \in (\mathbb{Z}/p\mathbb{Z})^\times$.

Comme α est non trivial et $P = \langle y \rangle$, l'automorphisme $\alpha_y \in \mathrm{Aut}(Q)$ est d'ordre p. On a donc $\alpha_y = \varphi_{u^k}$ pour un certain $k \in (\mathbb{Z}/p\mathbb{Z})^\times$. Soit q l'inverse de k dans $\mathbb{Z}/p\mathbb{Z}$. On a alors $\alpha_{y^q} = \varphi_{u^{kq}} = \varphi_u$. Ainsi, quitte à remplacer le générateur y de P par y^q (un autre générateur), on peut supposer que l'on a $\alpha_y = \varphi_u$. Suivont maintenant les isomorphismes : on a des isomorphismes $a : \mathbb{Z}/p\mathbb{Z} \xrightarrow{\sim} P$, $m \mapsto x^m$, $b : \mathbb{Z}/q\mathbb{Z} \xrightarrow{\sim} Q$, $m \mapsto y^m$, et donc $G = Q \rtimes P \simeq \mathbb{Z}/p\mathbb{Z} \rtimes_{\alpha'} \mathbb{Z}/2\mathbb{Z}$ d'après la Proposition 7.8, avec pour $m \in \mathbb{Z}/p\mathbb{Z}$ la formule

$$\alpha'_{\bar{1}}(m) = (a^{-1}\alpha_y a)(m) = a^{-1}(\alpha_\tau(x^m)) = a^{-1}(x^{um}) = um.$$

On a donc $\alpha' = \beta$ (notation du (iii)), et on a montré $G \simeq \Gamma_{p,q}$.

(v) On considère $u \in (\mathbb{Z}/p\mathbb{Z})^\times$ d'ordre p comme au (iii). Soit Q le sous-groupe de $\mathrm{GL}_p(\mathbb{C})$ constitué des matrices diagonales de la forme

$$\mathrm{d}(\zeta) := \mathrm{diag}(\zeta, \zeta^u, \zeta^{u^2}, \ldots, \zeta^{u^{p-1}}) \text{ avec } \zeta \in \mu_q.$$

Il est cyclique d'ordre q engendré par $\mathrm{d}(e^{2i\pi/q})$. Notons $\epsilon_1, \ldots, \epsilon_p$ la base canonique de $\mathbb{C}^p$ et $\sigma \in \mathrm{GL}_p(\mathbb{C})$ la matrice de permutation circulaire définie par $\sigma(e_i) = e_{i+1}$ pour $i < p$ et $\sigma(e_p) = e_1$. On constate que l'on a $\sigma^{-1}\mathrm{d}(\zeta)\sigma = \mathrm{d}(\zeta^u)$. Cela montre que le sous-groupe G de $\mathrm{GL}_p(\mathbb{C})$ engendré par Q et $P = \langle \sigma \rangle$ (cyclique d'ordre p) s'écrit ausi $G = QP$, et comme on a $Q \cap P = \{1\}$, qu'il est d'ordre pq. Il est non commutatif par la formule ci-dessus. Il est donc isomorphe à $\Gamma_{p,q}$ d'après le (iv).

Exercice 4.41. Si D_{2m} possède un sous-groupe d'ordre $2n$, on a $2n \mid 2m$ par Lagrange, puis $n | m$. Supposons donc réciproquement $n \,|\, m$. Par définition, on a $\mathrm{D}_{2m} = \langle c, \tau \rangle$ avec c d'ordre m, τ d'ordre 2 et $\tau c \tau^{-1} = c^{-1}$. L'élément $d := c^{m/n}$ est donc d'ordre n, et il vérifie encore $\tau d \tau^{-1} = (\tau c \tau^{-1})^{m/n} = (c^{-1})^{m/n} = d^{-1}$. Posant $D = \langle d \rangle$ et $K = \langle \tau \langle$ on en déduit que $H := DK$ est un sous-groupe de D_{2m} qui est produit semi-direct interne de $K \simeq \mathbb{Z}/2\mathbb{Z}$ par $D \simeq \mathbb{Z}/n\mathbb{Z}$, et ce pour l'action d'inversion de $K \simeq \mathbb{Z}/2\mathbb{Z}$ sur D. Par la remarque précédent l'exercice (Exemple 4.41), on en déduit $H \simeq \mathrm{D}_{2n}$.

Exercice 4.42. On note G_n le groupe défini par générateurs et relations dans l'énoncé.

(Cas $n = 1$) On a $G_1 = \langle s, t \rangle$ avec $st = 1$ et $s^2 = 1$, donc $s = t$, puis $G_1 = \langle s \rangle = \{1, s\}$ est de cardinal $\leqslant 2$. Par la propriété universelle de G_1, il existe un unique morphisme de groupes $f_1 : G_1 \to \{\pm 1\}$ vérifiant $f(s) = f(t) = -1$, car $-1 \cdot -1 = 1$. Le morphisme f_1 est clairement surjectif. Comme on a $|G_1| \leqslant 2 = |\{\pm 1\}|$, c'est un isomorphisme.

(Cas $n = 2$) On a $G_2 = \langle s, t \rangle$ avec $s^2 = t^2 = 1$ et $st = ts$. On en déduit $G_2 = \{1, s, t, st\}$ puis $|G_2| \leqslant 4$. Par la propriété universelle de G_2, il existe un unique morphisme de groupes $f_2 : G_2 \to \{\pm 1\} \times \{\pm 1\}$ vérifiant $f(s) = (-1, 1)$ et $f(t) = (1, -1)$ car $\{\pm 1\} \times \{\pm 1\}$ est commutatif d'exposant 2. Le morphisme f_2 est clairement surjectif. Comme on a $|G_2| \leqslant 4 = |\{\pm 1\}^2|$, c'est un isomorphisme.

(Cas $n > 2$) On a $G_2 = \langle s, t \rangle$ avec $s^2 = t^2 = 1$ et $(st)^n = 1$. On en déduit

$$G_2 = \{1, s, t, st, ts, sts, tst, stst, tsts, \ldots, (st)^{n-1}, (ts)^{n-1}\}$$

et en particulier $|G_2| \leqslant 2n$. On rappelle que D_{2n} est le sous-groupe de S_n engendré par $\sigma = (1\,2\,\ldots\,n)$ et $\tau = (1\,n)(2\,n{-}1)\cdots$. On constate que l'on a $\sigma\tau = (2\,n)\,(3\,n{-}1)\,(4\;n{-}2)\,\ldots$. On a donc $\tau^2 = 1$, $(\sigma\tau)^2 = 1$ et $(\sigma\tau\tau)^n = 1$. Par la propriété universelle de G_n, il existe donc un unique morphisme de groupes $f_n : G_n \to \mathrm{D}_{2n}$ vérifiant $f(s) = \sigma\tau$ et $f(t) = \tau$. Il est surjectif par $\mathrm{Im}\, f_n$ contient $\langle \tau, \sigma \rangle = \mathrm{D}_{2n}$. On a vu $|\mathrm{D}_{2n}| = 2n$ en cours, et $|G_n| \leqslant 2n$ ci-dessus. On en déduit que f_n est un isomorphisme.

Exercice 4.43. (i) Dans le groupe G_n, on a $(v, \sigma)(v', \sigma') = (v + \sigma(v'), \sigma\sigma')$, et $\sigma((v_i)) = (v_{\sigma^{-1}(i)})$. Si (v, σ) est dans le centre de G_n, on constate donc que σ est dans le centre de S_n, *i.e.* $\sigma = 1$ d'après l'Exercice 4.1. Comme on a $(v', \sigma') = (v', 1)(0, \sigma')$, l'élément $(v, 1)$ est dans le centre de G_n si, et seulement si, il commute à tous les $(v', 1)$ et les $(0, \sigma')$. Mais on

a $(v,1)(v',1) = (v+v',1) = (v',1)(v,1)$, donc la première condition est automatique. Pour la seconde, on a $(0,\sigma')(v,1)(0,\sigma'^{-1}) = (\sigma'(v),1)$. Ainsi, (v,σ) est dans le centre de G_n si, et seulement si, on a $\sigma = 1$ et toutes les coordonnées de v sont égales, i.e. $v \in \langle e\rangle = \{0,e\}$. Le centre de G_n est donc $\langle e\rangle \times 1 \simeq \mathbb{Z}/2\mathbb{Z}$.

(ii) Le sous-groupe $\langle e\rangle \subset (\mathbb{Z}/2\mathbb{Z})^n$ est bien stable par S_n. Soit V comme dans l'énoncé avec V non inclus dans $\langle e\rangle$. Il existe $v \in V$ et $i \neq j$ tels que $v_i = 1$ et $v_j = 0$. En considérant $(i\,j)v - v \in V$. On en déduit $\epsilon_i - \epsilon_j \in V$, où $\epsilon_1, \ldots, \epsilon_n$ est la base canonique de $(\mathbb{Z}/2\mathbb{Z})^n$. Mais on a $\sigma(\epsilon_i - \epsilon_j) = \epsilon_{\sigma(i)} - \epsilon_{\sigma(j)}$, et comme S_n permute transitivement sur les parties à 2 éléments de $\{1,2,\ldots,n\}$ on a $\epsilon_i - \epsilon_j \in V$ pour tout $1 \leqslant i \neq j \leqslant n$. Cela montre $V \supset \mathrm{H}_n$.

(iii) Notons que φ est un morphisme de groupes, et qu'elle vérifie $\varphi(\sigma(v)) = \varphi(v)$ pour tout $v \in (\mathbb{Z}/2\mathbb{Z})^n$ et tout $\sigma \in \mathrm{S}_n$. Soit $f(v,\sigma) := (\varphi(v),\sigma)$ l'application de l'énoncé. On a donc

$$f((v,\sigma)(v',\sigma')) = f(v+\sigma(v'),\sigma\sigma') = (\varphi(v)+\varphi(v'),\sigma\sigma') = (\varphi(v),\sigma)(\varphi(v'),\sigma').$$

(iv) Comme $f : G_n \to \mathbb{Z}/2\mathbb{Z} \times \mathrm{S}_n$ est un morphisme surjectif, on a

$$f(\mathrm{D}(G_n)) = \mathrm{D}(\mathbb{Z}/2\mathbb{Z} \times \mathrm{S}_n) = \{0\} \times \mathrm{A}_n.$$

On a utilisé $\mathrm{D}(\mathrm{S}_n) = \mathrm{A}_n$, et le fait immédiat $\mathrm{D}(G \times G') = \mathrm{D}(G) \times \mathrm{D}(G')$. Tout $g \in \mathrm{D}(G_n)$ s'écrit donc $(v,\sigma) = (v,1)(0,\sigma)$ avec $v \in \mathrm{H}_n$ et $\sigma \in \mathrm{A}_n$. Comme réciproquement l'injection canonique $\mathrm{S}_n \to G_n, \sigma \mapsto (0,\sigma)$, est un morphisme de groupes, on a aussi $\{0\} \times \mathrm{A}_n \subset \mathrm{D}(G_n)$. On en déduit que (v,σ) est dans $\mathrm{D}(G_n)$ si, et seulement si, $\sigma \in \mathrm{A}_n$, $v \in \mathrm{H}_n$ et $(v,1) \in \mathrm{D}(G_n)$. Notons $V \subset \mathrm{H}_n$ le sous-ensemble des v tels que $(v,1) \in \mathrm{D}(G_n)$. C'est clairement un sous-groupe, et il est stable par S_n car $\mathrm{D}(G_n)$ est distingué dans G_n et on a $(0,\sigma)(v,1)(0,\sigma)^{-1} = (\sigma(v),1)$. D'après le (ii), on a donc soit $V \subset \langle e\rangle$, soit $V = \mathrm{H}_n$. Mais pour $v \in (\mathbb{Z}/2\mathbb{Z})^n$ et $\sigma \in \mathrm{S}_n$ on a la formule

$$[(v,1),(0,\sigma)] = (v,1)(0,\sigma)(-v,1)(0,\sigma^{-1}) = (v-\sigma(v),1).$$

Prenant $v = (1,0,\ldots,0)$ et $\sigma = (1\,2)$ on obtient $\epsilon_1 - \epsilon_2 \in V$. On a donc $V \neq \{0\}$. Pour $n = 2$ on a $\langle e\rangle = \mathrm{H}_2$, et on conclut. Pour $n > 2$ on a $\epsilon_1 - \varepsilon_2 \notin \langle e\rangle$, et donc $V = \mathrm{H}_n$.

(v) On a une suite exacte courte $1 \to (\mathbb{Z}/2\mathbb{Z})^n \to G_n \to \mathrm{S}_n \to 1$. Le groupe $(\mathbb{Z}/2\mathbb{Z})^n$ est abélien donc résoluble. D'après le cours, G_n est résoluble si, et seulement si, S_n l'est, *i.e.* $n \leqslant 4$.

(vi) Observons d'abord que l'on a $\sigma(\mathrm{H}_n) \subset H_n$ pour tout $\sigma \in \mathrm{S}_n$. Ainsi, le groupe $G'_n := \mathrm{H}_n \rtimes_\alpha \mathrm{S}_n$ a bien un sens, et c'est un sous-groupe de G_n. De plus, l'application $G'_n \times H_n \to H_n, ((v,\sigma),w) \mapsto v+\sigma(w)$, est bien définie. C'est une action car on a $(v,\sigma)(v',\sigma') = (v+\sigma(v'),\sigma\sigma')$ dans G'_n, et on a bien $v+\sigma(v'+\sigma'(w)) = v+\sigma(v')+\sigma\sigma(w')$ dans H_n. Montrons que cette action est fidèle. Soit $(v,\sigma) \in G'_n$ avec $v+\sigma(w) = w$ pour tout $w \in H_n$. Pour $w = v$ on a $\sigma(v) = 0$, puis $v = \sigma^{-1}\sigma(v) = 0$, et donc $\sigma(w) = w$ pour tout $w \in H_n$. Appliquée à $w = \epsilon_i + \epsilon_j \in \mathrm{H}_n$ pour $1 \leqslant i < j \leqslant n$, on en déduit que σ préserve $\{i,j\}$ pour tout $i \neq j$. Pour $n > 2$, cela implique $\sigma = 1$.

(vii) Soit $X = H_3$. On a $|X| = 4$ et le groupe G'_3 agit fidèlement sur X par le (vi), le morphisme associé $G'_3 \to \mathrm{S}_X \simeq \mathrm{S}_4$ est donc injectif. Mais on a $|G'_3| = |X||\mathrm{S}_3| = 4 \cdot 6 = 24$: c'est un isomorphisme.

Exercices du chapitre 5

Exercice 5.2. (i) On a $\varphi > 1$. Pour voir que les 12 faces sont équilatérales il suffit de montrer que la largeur commune des trois rectangles, à savoir 2, coïncide avec celle du segment AB avec $A = (\varphi, 0, 1)$ (un sommet du rectangle vert foncé) et $B = (0, 1, \varphi)$ (un sommet du rectangle violet). Mais on a $AB^2 = \varphi^2 + 1 + (\varphi - 1)^2 = 2 - 2\varphi + 2\varphi^2$, et donc $AB = 2$ si, et seulement si, $\varphi^2 = \varphi + 1$. L'unique solution > 1 de cette équation est bien le nombre d'or $\frac{1+\sqrt{5}}{2}$.

(ii) Le centre d'une face (un triangle équilatéral) est l'isobarycentre de ses sommets. Le centre de la face F supérieure est donc

$$\frac{1}{3}((\varphi, 0, 1) + (0, 1, \varphi) + (0, -1, \varphi)) = \frac{1}{3}(\varphi, 0, \varphi^3)$$

en notant $\varphi^3 = \varphi(1+\varphi) = 1+2\varphi$. De même le centre de la face adjacente à F et contenant $(1, \varphi, 0)$ est $\frac{1}{3}((\varphi, 0, 1)+(1, \varphi, 0)+(0, 1, \varphi)) = \frac{1}{3}(\varphi^2, \varphi^2, \varphi^2)$ Par construction, le sous-groupe $G \subset \mathrm{O}(3)$ constitué des permutations circulaires (ou triviales) des coordonnées et des changements de signes (qui est d'ordre 24) est un sous-groupe du groupe des isométries de I. Il permute donc ses 20 faces, et donc leurs centres. L'orbite par G de $\frac{1}{3}(\varphi, 0, \varphi^3)$ a clairement $3{\cdot}4 = 12$ points, et celle de $\frac{1}{3}(\varphi^2, \varphi^2, \varphi^2)$ en a $2^3 = 8$. On conclut par $8+12 = 20$.

Exercice 5.3. (i) L'angle au sommet d'un polygone régulier à $n \geqslant 3$ côtés est $\pi - 2\pi/n$. La somme des angles entre les f demi-droites consécutives est 2π. On a donc $2\pi > (\pi - 2\pi/n)f$ puis $1/2 < 1/f + 1/n$.

(ii) Comme on a $f \geqslant 3$ et $1/3 + 1/6 = 9/18 = 1/2$, on a $3 \leqslant n \leqslant 5$, et de même $3 \leqslant f \leqslant 5$, et aussi $f = 3$ ou $n = 3$ car $1/4 + 1/4 = 1/2$. Les seules solutions sont donc $(n, f) = (3, 3), (3, 4), (4, 3), (3, 5), (5, 3)$. Soit P un polyèdre convexe possédant un sommet S appartenant à exactement f faces que l'on suppose être des polygones réguliers à n côtés. Soit H un plan affine avec $H \cap P = \{S\}$. Considérons la projection orthogonale $p : \mathbb{R}^3 \to H$. Les n arêtes de P de sommets S, et dans l'une des f faces contenant P, sont envoyés sur des segments de H satisfaisant les hypothèses de l'exercice. On est donc dans l'un des 5 cas de couples (n, f) ci-dessus. Si P est régulier, c'est donc manifestement (?) un tétraèdre, un octaèdre, un cube, un dodécaèdre ou un icosaèdre.

Exercice 5.5. Le groupe $\mathbb{Z}/2\mathbb{Z}$ est le groupe de symétries d'un parallélogramme centré en 0 non losange, et le groupe trivial est le groupe de symétries de tout quadrilatère suffisamment quelconque. On suppose donc $n \geqslant 3$.

Soient $\mathscr{P}_n \subset E$ un polygone régulier à n côtés de centre 0, S_n l'ensemble des sommets de $\mathscr{P}_n$, S'_n une petite rotation non triviale de S_n et $r > 1$ un réel assez proche de 1. Soit P_n l'enveloppe convexe de $\Sigma_n = S_n \cup rS'_n$. C'est un polygone régulier à $2n$ côtés de sommets Σ_n. Le groupe $G \simeq \mathbb{Z}/n\mathbb{Z}$ des rotations d'angle dans $\frac{2\pi}{n}\mathbb{Z}$ préserve clairement P_n. Réciproquement, une isométrie de P_n préserve ses sommets Σ_n ainsi que S_n et rS'_n, car pour $x \in S_n$ et $y \in rS'_n$ on a $||x|| \neq ||y||$. Mais on sait que $\mathrm{Iso}(\mathscr{P}_n)$ est un groupe diédral d'ordre $2n$, constitué de G et de n réflexions orthogonales fixant soit le milieu d'une arête de $\mathscr{P}_n$, soit deux sommets opposés de $\mathscr{P}_n$. Mais par choix de S'_n, une telle réflexion ne préserve pas S_n. On a donc bien $\mathrm{Iso}(P_n) = G$.

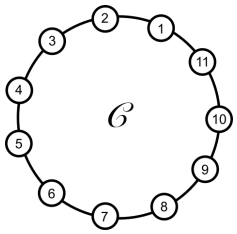
Exercice 5.6. Les éléments non triviaux de A_5 sont soit des 3-cycles, soit des 5-cycles, soit des doubles transpositions. Les sous-groupes cycliques de A_5 sont donc $\simeq \mathbb{Z}/n\mathbb{Z}$ avec $n = 1, 2, 3, 5$. Un sous-groupe fini G de A_5 se plonge dans $\mathrm{SO}(3)$. Il est donc dans la liste du théorème de Klein. S'il est réductible, il est soit cyclique, et ce cas vient d'être traité, soit diédral, soit $\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Si on a $G \simeq \mathrm{D}_{2m}$, avec donc $m \geqslant 3$, on a $m = 3$ ou 5 car G contient un élément d'ordre $m \geqslant 3$. Réciproquement, on constate que D_{10} est dans A_5 (et plus généralement, D_{2n} est dans A_n pour $n \equiv 0, 1 \bmod 4$). De plus, le sous-groupe

de A_5 préservant $\{1,2,3\}$ est isomorphe à $\mathrm{S}_3 \simeq \mathrm{D}_6$, et le groupe A_4 se plonge clairement dans A_5, ainsi donc au passage que son sous-groupe K_4. On peut donc supposer que G est irréductible, et isomorphe à S_4. Mais c'est impossible par Lagrange car 24 ne divise pas 60.

Exercice 5.7. (i) Le groupe G a $2m$ éléments, dont m rotations, et donc m réflexions. Si m est pair, on a $\mathscr{P}_m = -\mathscr{P}_m$, et les $m/2$ réflexions d'axe passant par deux sommets opposés sont conjuguées par la formule $gs_Hg^{-1} = s_{g(H)}$, car G agit transitivement sur les sommets. Les $m/2$ autres réflexions ont un axe reliant les milieux de deux côtés opposés. Pour la même raison, elles sont conjuguées entre elles, mais pas aux $m/2$ précédentes car aucune isométrie de $\mathscr{P}_m$ n'envoie un sommet sur le milieu d'un côté. Enfin si m est impair, il y a m droites reliant un sommet de $\mathscr{P}_m$ au milieu du côté opposé, permutées transitivement par G. Les m réflexions associées forment donc une unique classe de conjugaison de G.

(ii) Il suffit de prendre pour s la réflexion fixant un sommet S et t celle fixant le milieu d'une arête contenant S. L'angle entre les axes de ces deux réflexions est $\frac{1}{2}\frac{2\pi}{m}$, donc st est la rotation d'angle $\pm\frac{2\pi}{m}$. Comme G est d'ordre $2m$, on a bien $G = \langle s, t\rangle$.

Exercice 5.8. Supposons fixé un collier $\mathscr{C}$ possédant $2+3+6=11$ emplacements de perles numérotés circulairement de 1 à 11.



Notons X l'ensemble de tous les remplissages possibles de ces 11 emplacements avec en tout 2 perles violettes, 3 rouges et 6 bleues. On peut définir rigoureusement X comme un sous-ensemble de l'ensemble des 3^{11} fonctions $\{1,2,\ldots,11\} \to \{\text{bleu}, \text{rouge}, \text{violet}\}$. On a $|X| = \binom{11}{2}\binom{9}{3} = 4620$. Le groupe S_{11} agit naturellement sur X par précomposition à la source des fonctions. On sait que le groupe des rotations spatiales de $\mathscr{C}$ s'identifie au sous-groupe diédral D_{22} du groupe S_{11} des permutations des 11 emplacements. Il agit donc aussi naturellement sur X, et la question de l'énoncé est de déterminer le nombre N d'orbites de cette action. D'après Burnside-Frobenius, N est le nombre moyen de points fixes d'un élément de D_{22} agissant sur X. Le groupe D_{22} a trois types d'éléments :

– Le neutre 1. Il agit bien sûr sur X avec $|X|$ points fixes.

– 10 éléments d'ordre 11 (les c^i avec $0 < i < 11$). Un éléments d'ordre 11 de S_{11} est un 11-cycle. Un remplissage de $\mathscr{C}$ fixé par un 11-cycle doit donc avoir toutes ses perles de couleurs identiques, et un tel remplissage n'est pas dans X. Ainsi, les 10 éléments d'ordre 11 de D_{22} n'ont aucun point fixe dans X.

– 11 éléments d'ordre 2 possédant un unique point fixe dans $\{1,2,\ldots,11\}$ (les conjugués de τ). Fixons $s \in \mathrm{S}_{11}$ d'ordre 2 et possèdant un unique point fixe. Déterminons le nombre de remplissages de $\mathscr{C}$ dans X et invariants par s. La seule couleur présente en nombre impaire (en l'occurence, 3) étant le rouge, la perle fixée par s doit être rouge, et toutes les autres viennent par paires monochromes préservées par s. Parmi ces 5 paires, une est violette, une est rouge et les 3 autres sont bleues. Il y a donc exactement $5\cdot 4 = 20$ éléments de X fixés par s.

On a donc $N = \frac{1}{|\mathrm{D}_{22}|}(|X| + 10\cdot 0 + 11\cdot 20) = \frac{1}{22}(4620+220) = 220$ colliers possibles.

Exercice 5.9. (i) L'action de G sur X ayant une seule orbite, on a $1 = \frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}\, g|$ par Burnside-Frobenius. Mais $g = 1$ a $|X| \geqslant 2$ points fixes. Ainsi, si les éléments non triviaux de G ont tous au moins un point fixe on aurait $1 \geqslant \frac{1}{|G|}(2 + |G| - 1) > 1$, une contradiction.

(ii) On applique la question précédente à $X = G/H$, pour l'action (transitive) par translations. On a bien $|X| \geqslant 2$ par l'hypothèse $H \neq G$. Il existe donc $\gamma \in G$ qui ne stabilise aucun gH avec $g \in G$. Mais le stabilisateur de gH pour l'action par translations est gHg^{-1}, on a donc $\gamma \in G \smallsetminus \cup_{g\in G} gHg^{-1}$.

(iii) Si H contient un représentant de chaque classe de conjugaison de G, on a $G \subset \cup_{g\in G} gHg^{-1}$, et donc $H = G$ par la question (ii).

(iv) Le groupe infini $G = \mathrm{SO}(3)$ agit transitivement sur la sphère S^2. Par Euler, tout $g \in G$ admet deux points fixes dans S^2. Fixons $x_0 \in \mathrm{S}^2$, de stabilisateur $T := G_{x_0}$ (un sous-groupe isomorphe à S^1). Pour $g \in G$, le stabilisateur du point gx_0 est gTg^{-1}, et on a donc $G = \cup_{g\in G} gTg^{-1}$. Ainsi le sous-groupe T (commutatif!) contient un représentant de chaque classe de conjugaison de G. On a bien sûr $T \neq G$.

Exercice 5.10. Écrivons $X = \coprod_{i=1}^{r} \Omega_i$ comme réunion disjointe des orbites Ω_i sous l'action de G. Par la formule de Burnside-Frobenius et l'hypothèse (b), on a

$$r = \frac{1}{|G|}(|X| + h), \tag{83}$$

où h est le nombre d'éléments de G distincts de 1 et ayant exactement 1 point fixe dans X. On a bien sûr $h < |G|$. De plus, comme on a $|G_x| \geqslant 2$ pour tout $x \in X$ par l'hypoth ese (a), on a aussi $|\Omega_i| \leqslant |G|/2$ pour tout i par la formule orbite-stabilisateur, puis $|X| \leqslant r|G|/2$. L'égalité (83) montre donc $r < r/2 + 1$, puis $r < 2$ et $r = 1$.

Exercice 5.11. On se place dans l'espace euclidien standard $E = \mathbb{R}^n$, et on identifie $\mathrm{O}(E)$ à $\mathrm{O}(n)$ comme d'habitude (matrice dans la base canonique).

(i) Un élément g du centre de $\mathrm{O}(E)$ commute avec toutes les réflexions de E. On a donc $g\,\mathrm{s}_H\,g^{-1} = \mathrm{s}_{g(H)} = \mathrm{s}_H$, puis $g(H) = H$ (car on a $\mathrm{s}_H = \mathrm{s}_{H'} \iff H = H'$) pour tout hyperplan $H \in E$. On en déduit que g préserve toutes les droites de E (orthogonaux des hyperplans). Il est classique (et vu en cours) qu'alors g est une homothétie, puis $g = \pm\mathrm{id}_E$ car g est dans $\mathrm{O}(E)$. On en déduit $\mathrm{Z}(\mathrm{O}(n)) = \{\pm 1_n\}$.

(ii) Le morphisme det de $\mathrm{O}(E)$ vers le groupe abélien $\{\pm 1\}$ montre $\mathrm{D}(\mathrm{O}(E)) \subset \mathrm{SO}(E)$. Montrons l'inclusion réciproque. Pour $g \in \mathrm{O}(E)$ et $H \subset E$ un hyperplan on a $[g, s_H] = s_{g(H)}s_H$. Mais $\mathrm{O}(E)$ permute transitivement les hyperplans de E, car il permute transitivement les vecteurs de norme 1. On en déduit que le produit de deux réflexions est dans $\mathrm{D}(\mathrm{O}(E))$. Comme les produits de deux réflexions engendrent $\mathrm{SO}(E)$ par Cartan-Dieudonné, on a montré $\mathrm{SO}(E) = \mathrm{D}(\mathrm{O}(E))$.

(iii) Considérons l'application $f : \mathrm{O}(E) \to \mathrm{O}(E) \times \{\pm 1\}, g \mapsto ((\det g)g, \det g)$. On constate que c'est un morphisme de groupes injectif et d'image contenant $\mathrm{SO}(E) \times \{1\}$. Si n est impair on a $\det -\mathrm{id}_E = -1$ et donc f induit un isomorphisme $\mathrm{O}(E) \xrightarrow{\sim} \mathrm{SO}(E) \times \{\pm 1\}$. Si n est pair, on n'a pas $\mathrm{O}(n) \simeq \mathrm{SO}(n) \times \{\pm 1\}$, car le centre de $\mathrm{SO}(n) \times \{\pm 1\}$ contient les 4 éléments $(\pm 1_n, \pm 1)$, et celui de $\mathrm{O}(n)$ est d'ordre 2 par le (i).

Exercice 5.12. On pose $E = \mathbb{R}^n$ et on identifie encore $\mathrm{O}(E)$ à $\mathrm{O}(n)$ comme dans l'exercice précédent.

(i) Pour tout plan P de E il existe un unique élément $r_P \in \mathrm{O}(E)$. qui vaut l'identité sur P et $-\mathrm{id}$ sur $P^\perp$. C'est l'unique retournement fixant $P^\perp$. On a $r_P \in \mathrm{SO}(E)$, et pour $g \in \mathrm{O}(E)$ on a $gr_Pg^{-1} = r_{g(P)}$. On notera $R(E) \subset \mathrm{SO}(E)$ le sous-ensemble des retournements de E, *i.e.* des r_P avec P un plan de E. Pour voir $\langle R(E)\rangle = \mathrm{SO}(E)$, il suffit de voir que le

groupe de gauche contient les produits de deux réflexions par Cartan-Dieudonné. Soient s_1 et s_2 deux réflexions de E d'hyperplans H_1 et H_2. Supposons d'abord $\dim E = 3$. Pour tout plan P de E on a alors $-r_P = \mathrm{s}_P$ (une réflexion). On a donc $s_1 s_2 = (-s_1)(-s_2) \in \langle R(E) \rangle$. Retournons au cas général $\dim E \geqslant 3$. Le cas $\dim E = 3$ appliqué à tous les sous-espaces de dimension 3 de E montre que $\langle R(E) \rangle$ contient tous les éléments $g \in \mathrm{SO}(E)$ dont les points fixes sont de codimension $\leqslant 3$. On conclut car $s_1 s_2$ fixe $H_1 \cap H_2$ qui est de codimension $\leqslant 2$.

(ii) Pour $n \leqslant 2$ alors $\mathrm{SO}(E)$ est commutatif. On a donc $\mathrm{Z}(\mathrm{SO}(E)) = \mathrm{SO}(E)$ et $\mathrm{D}(\mathrm{SO}(E)) = \{1\}$. On suppose donc $n \geqslant 3$. Un élément $g \in \mathrm{Z}(\mathrm{SO}(E))$ commute à tous les r_P, et donc stabilise tous les plans P de E. Comme on a $\dim E > 2$, toute droite de E est intersection de deux plans. Ainsi, g préserve toutes les droites, puis g est une homothétie, $g = \pm \mathrm{id}_E$, puis $g = \mathrm{id}_E$ si n est impair. On a donc $\mathrm{Z}(\mathrm{SO}(E)) = 1$ pour n impair, $\mathrm{Z}(\mathrm{SO}(E)) = \{\pm \mathrm{id}_E\}$ pour n pair.

Montrons enfin $\mathrm{D}(\mathrm{SO}(E)) = \mathrm{SO}(E)$. Le même argument qu'au (i) montre que l'on peut supposer $n = \dim E = 3$. Mais pour $g \in \mathrm{SO}(E)$ et $r_P \in R(E)$ on a $[g, r_P] = r_{g(P)} r_P = (-r_{g(P)})(-r_P) = s_{g(P)} s_P \in \mathrm{D}(\mathrm{SO}(E))$. Comme $\mathrm{SO}(E)$ agit transitivement sur les plans de E, on en déduit que $\mathrm{D}(\mathrm{SO}(E))$ contient tous les produits de deux réflexions, puis $\mathrm{SO}(E)$.

Exercice 5.13. Soit G un sous-groupe de $\mathrm{SO}(2)$ et $h \in \mathrm{O}(2)$. Si h est dans $\mathrm{SO}(2)$ on a $hGh^{-1} = G$ car $\mathrm{SO}(2)$ est commutatif. Si non, h est une réflexion et on a $hrh^{-1} = r^{-1}$ pour tout $r \in \mathrm{SO}(2)$. On a donc encore $hGh^{-1} = G^{-1} = G$. On a montré que tout sous-groupe de $\mathrm{SO}(2)$ est distingué dans $\mathrm{O}(2)$.

Il reste à voir que si un sous-groupe $G \subset \mathrm{O}(2)$ est distingué et contient une réflexion s, alors on a $G = \mathrm{O}(2)$. Mais alors G contient les rsr^{-1} avec $r \in \mathrm{SO}(2)$, et donc toutes les réflexions, puis toutes les rotations (produits de deux réflexions).

Exercice 5.14. (i) La matrice d'une rotation plane d'angle θ est

$$\mathrm{R}_\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

dans une base orthonormée, de sorte que sa trace est $2\cos\theta$. Par Euler, toute rotation g de $\mathrm{SO}(3)$ fixe une droite, et donc induit une rotation d'un certain angle θ dans le plan orthogonal. Ainsi, g est conjuguée à

$$\mathrm{m}(\theta) := \begin{bmatrix} 1 & 0 \\ 0 & \mathrm{R}_\theta \end{bmatrix}.$$

dans $\mathrm{O}(3)$, et même dans $\mathrm{SO}(3)$ car $\det -1_3 = -1$, et sa trace est $1 + 2\cos\theta$.

(ii) La trace est invariante par conjugaison. Réciproquement, on a $\operatorname{tr} \mathrm{m}(\theta) = \operatorname{tr} \mathrm{m}(\theta')$ si, et seulement si, $\theta \equiv \pm\theta' \bmod 2\mathbb{Z}$. On conclut car $\mathrm{m}(\theta)$ est conjuguée à $\mathrm{m}(-\theta)$ dans $\mathrm{SO}(3)$ (conjuguer par la matrice diagonale $\mathrm{diag}(-1, -1, 1)$).

(iii) On a $\operatorname{tr} \mathrm{m}(\theta) = 3$ si et seulement si $\theta \in 2\pi\mathbb{Z}$, *i.e.* $\mathrm{m}(\theta) = 1_3$. On peut aussi utiliser le (ii).

(iv) Comme H est distingué dans G, on sait par le (ii) et l'hypothèse que H contient tous les $\mathrm{m}(\theta)$ avec $|\theta| < \epsilon$ pour un certain $\epsilon > 0$ (par exemple vérifiant $1 + 2\cos\epsilon > x$), et il faut voir par le (ii) encore qu'il contient tous les $\mathrm{m}(\theta)$ avec $\theta \in \mathbb{R}$. Pour tout entier $n \geqslant 1$ et $|\theta| < \epsilon$, le sous-groupe H contient $\mathrm{m}(\theta)^n = \mathrm{m}(n\theta)$, et on conclut car on a $\cup_{n \geqslant 1}]-n\epsilon, n\epsilon[= \mathbb{R}$.

(iv) Fixons $h \in H \smallsetminus \{1\}$. Pour tout $g \in \mathrm{SO}(3)$, on a $[g, h] = (ghg^{-1})h^{-1} \in H$ car H est distingué. Considérons l'application $f : \mathrm{SO}(3) \to [-1, 3], g \mapsto \operatorname{tr}[g, h]$, est continue. Comme $\mathrm{SO}(3)$ est connexe son image est un connexe de $[-1, 3]$, donc un intervalle. Elle contient $f(1) = 3$. Mieux, $[g, h]$ est de trace 3 si, et seulement si, on a $[g, h] = 1$ par le

(iii), *i.e.* si g commute avec h. Comme le centre de $\mathrm{SO}(3)$ est 1, h est $\neq 1$ par hypothèse, on a $]x,3] \subset \mathrm{Im} f$ pour un certain $x < 3$. On a montré $\mathrm{tr}\, H \supset]x,3]$, et on conclut par le (iii).

Exercice 5.15. (i) Montrons que les seuls sous-groupes distingués de $\mathrm{Sp}(1)$ sont 1, $\{\pm 1\}$ et $\mathrm{Sp}(1)$ (ces sous-groupes le sont clairement). On sait qu'il existe un morphisme $\pi : \mathrm{Sp}(1) \to \mathrm{SO}(3)$ qui est surjectif de noyau $\{\pm 1\}$. Si G est un sous-groupe distingué de $\mathrm{Sp}(1)$, alors $\pi(G)$ est distingué dans $\mathrm{SO}(3)$. C'est donc $\{1\}$ ou $\mathrm{SO}(3)$ par l'Exercice 5.14. Mais $\pi(G) = \{1\}$ entraîne bien $G \subset \{\pm 1\}$. Sinon il existe $q \in G$ tel que $\pi(q)$ est d'ordre 2 dans $\mathrm{SO}(3)$. On a donc $q^2 = \pm 1$. Mais $q^2 = 1$ implique $q = \pm 1$ dans le corps gauche $\mathbb{H}$, et donc $\pi(q) = 1$. On a donc $q^2 = -1$, et donc $-1 \in G$, puis $G = \mathrm{Sp}(1)$ car $\pi(G) = \mathrm{SO}(3)$.

(ii) Posons $\Gamma = \mathrm{Sp}(1) \times \mathrm{Sp}(1)$. Ce groupe a deux sous-groupes distingués naturels $\simeq \mathrm{Sp}(1)$ qui sont $\Gamma_1 = \mathrm{Sp}(1) \times \{1\}$ et $\Gamma_2 = \{1\} \times \mathrm{Sp}(1)$. On sait qu'il existe un morphisme $\pi : \Gamma \to \mathrm{SO}(4)$ surjectif et de noyau $\{(1,1),(-1,-1)\}$. Nous allons voir que les sous-groupes distingués de $\mathrm{SO}(4)$ sont $1, \{\pm 1\}, \pi(\Gamma_1), \pi(\Gamma_2)$ et $\mathrm{SO}(4)$. Mais les sous-groupes distingués de $\mathrm{SO}(4)$ sont exactement les $\pi(G)$ avec G un sous-groupe distingué de Γ contenant $(-1,-1)$. Soit G un tel sous-groupe. Il suffit donc de voir que l'on a soit $G \subset Z$ (et donc $\pi(G) \subset \pi(Z) = \{\pm 1\}$), soit $G = Z\Gamma_i$ (et donc $\pi(G) = \pi(\Gamma_i)$ car $\pi(Z) \subset \pi(\Gamma_i)$), soit $G = \Gamma$ (et donc $\pi(G) = \mathrm{SO}(4)$). Mais $G_i := G \cap \Gamma_i$ est distingué dans Γ_i. Par le (i) on a donc $G_i \subset \{\pm 1\}$ ou $G_i = \Gamma_i$. Supposons $G_1 = \Gamma_1$, le cas $G_2 = \Gamma_2$ est similaire. La relation $\Gamma = \Gamma_1\Gamma_2$ entraîne alors $G = \Gamma_1 G_2$, puis soit $G = \Gamma_1 Z$ car $(-1,-1) \in G$ (cas $G_2 \subset \{\pm 1\}$) soit $G = \Gamma$ (cas $G_2 = \Gamma_2$). Dans le cas restant, on a G_1 et G_2 inclus dans $\{\pm 1\}$ et donc $G \subset Z$.

Exercice 5.16. Cet exercice est à comparer à la preuve du cours montrant la simplicité de A_n à partir de celle de A_5.

(i) On pose $E = \mathbb{R}^{2n+1}$ et on identifie $\mathrm{SO}(2n+1)$ à $\mathrm{SO}(E)$ comme d'habitude. Soit G un sous-groupe distingué non trivial de $\mathrm{SO}(E)$. On va montrer $G = \mathrm{SO}(E)$. Par l'Exercice 5.12, il suffit de voir que G contient un retournement. Soit F un sous-espace de E de dimension k. On a $\mathrm{S}(F) \simeq \mathrm{SO}(k)$ et $G \cap \mathrm{S}(F)$ est distingué dans $\mathrm{S}(F)$. Comme $\mathrm{SO}(3)$ est simple, il suffit de trouver F de dimension 3 tel que $G \cap \mathrm{S}(F)$ est non trivial. Cela impliquera $G \cap \mathrm{S}(F) = \mathrm{S}(F)$, et donc que G contient un retournement.

Soit $g \in G \smallsetminus \{1\}$ (et donc aussi $g \neq -1$ car $-1 \notin \mathrm{SO}(2n+1)$). Alors on a g n'est pas dans le centre de $\mathrm{O}(E)$ par l'Exercice 5.11. Ainsi, il existe une doite $D \subset E$ avec $s(D) \neq D$. Posant $H = D^\perp$, on a donc $g\mathrm{s}_H \neq \mathrm{s}_H g$. Le commutateur $[g, \mathrm{s}_H] = [g, -\mathrm{s}_H]$ est donc non trivial. Mais comme $\dim E$ est impaire, on a $-\mathrm{s}_H \in \mathrm{SO}(E)$, et comme G est distingué dans $\mathrm{SO}(E)$, on a donc $[g, \mathrm{s}_H] \in G$. Mais on a aussi $[g, \mathrm{s}_H] = g\mathrm{s}_H g^{-1}\mathrm{s}_H = \mathrm{s}_{g(H)}\mathrm{s}_H$. C'est un élément non trivial de $\mathrm{S}(F)$ pour $F = g(D) + D$, qui est de dimension 2. Il est donc aussi dans $\mathrm{S}(F)$ pour tout sous-espace F contenant $g(D) + D$. Il suffit donc de considérer un tel F de dimension 3.

(ii) On suppose maintenant $E = \mathbb{R}^{2n+2}$ avec $n > 1$, et G distingué dans $\mathrm{SO}(E)$ non trivial. Soit g dans G différent de ± 1. Il existe donc un plan P de E avec $[g, r_P] \neq 1$ par l'Exercice 5.12. Mais on a d'une part $[g, r_P] = g(r_P g^{-1} r_P^{-1}) \in G$ car G est distingué, et aussi $[g, r_P] = r_{g(P)} r_P \in \mathrm{S}(F)$ avec $F = P + g(P^\perp)$, qui est de dimension $\geqslant 4$. Considérant un sous-espace F' de dimension 5 arbitraire contenant F, on a alors $[g, r_P] \in G \cap \mathrm{S}(F')$ et donc $G \cap \mathrm{S}(F') \neq \{1\}$. Mais on a $\mathrm{S}(F') \simeq \mathrm{SO}(5)$ et $G \cap \mathrm{S}(F')$ distingué non trivial dans $\mathrm{S}(F')$, donc $G \cap \mathrm{S}(F') = \mathrm{S}(F')$. En particulier, G contient des retournements, et donc $G = \mathrm{SO}(E)$ par l'Exercice 5.12 (i).

Exercice 5.18. (i) Si B est un bloc, alors B est non vide, ainsi donc que les $g(B)$. Si on a $g(B) \cap g'(B) \neq \varnothing$ pour $g, g' \in G$ alors $g^{-1}g'(B) \cap B$ est non vide. On a donc $g^{-1}g'(B) = B$ car B est un bloc, puis $g(B) = g'(B)$. Comme l'action de G sur X est transitive, on a

aussi $X = \cup_{g\in G} g(B)$. On a bien montré que les $g(B)$, avec $g \in G$, forment une partition de X. La réciproque est triviale.

(ii) Soit B un bloc et $b \in B$. Pour $g \in G_b$ on a $g(b) = b$ et donc $b \in g(B) \cap B$, puis $g(B) = B$ car B est un bloc.

(iii) Observer que si l'action de G sur X est libre, on a $G_x = \{1\}$ pour tout $x \in X$. Ainsi, tous les sous-ensembles non vide $B \subset X$ sont trivialement équilibrés. Considérons $X = G$ pour l'action de Cayley pour fixer les idées. Notons B un bloc contenant 1, fixons $g, h \in B$. On a $g^{-1}.g = 1 \in B \cap g^{-1}(B)$ donc $g^{-1}(B) = B$ puis $g^{-1}.1 = g^{-1} \in B$. On a aussi $hg.g^{-1} = h \in B \cap hg(B)$ donc $B = hg(B)$ puis $gh.1 = hg \in B$. Ainsi, B est un sous-groupe de G. On obtient donc un contre-exemple en choisissant pour B une partie de G contenant 1 mais qui n'est pas un sous-groupe. C'est possible dès que $|G| > 2$.

(iv) Soient N un sous-groupe distingué de G, $x \in G$ et $B = Nx$ l'orbite de x sous N. Soit $g \in G$. On constate $gNx = gNg^{-1}gx = Ngx$ car N est distingué dans G, et Ngx est l'orbite de $gx \in X$ sous N. On conclut car on sait que les orbites de X sous l'action de N forment une partition de X.

Exercice 5.19. (i) Supposons $n = 3$ pour commencer. Soit $B \subset \mathrm{S}^2$ une partie équilibée possédant deux éléments x, y avec $y \notin \{x, -x\}$. Si $r_\theta \in \mathrm{SO}(3)$ est désigne rotation d'axe y et d'angle $\pm\theta$, on a $r_\theta(x) \in B$ par hypothèse. Nous en déduisons deux choses.

(a) il existe des éléments de $B \smallsetminus \{x\}$ aussi proches que l'on veut de x (prendre des θ très petits).

(b) le cercle de S^2 passant par y et orthogonal à x est inclus dans B.

Ceci étant dit, notons $\mathscr{C}_z$ le grand cercle (ou *équateur*) de S^2 orthogonal à $z \in \mathrm{S}^2$. Ainsi, si on a $B \cap \mathscr{C}_x \neq \emptyset$, on en déduit $\mathscr{C}_x \subset B$ par (b), puis $\mathscr{C}_z \subset B$ pour tout $z \in \mathscr{C}_x$ encore par (b) car $\mathscr{C}_x \cap \mathscr{C}_z$ est non vide, et on conclut car on a alors

$$\mathrm{S}^2 = \cup_{z\in\mathscr{C}_x} \mathscr{C}_z \subset B.$$

Posons $x_0 = x$. Il suffit donc de montrer $B \cap \mathscr{C}_{x_0} \neq \emptyset$. Par (a), il existe $x_1 \in B \smallsetminus \{x_0\}$ assez proche de x_0 de sorte que la longueur ℓ de l'arc (x_0x_1) soit $< \pi/2$ (cette condition sera suffisante mais il sera plus clair d'imaginer ℓ très petite). Soit $\mathscr{C} \subset \mathrm{S}^2$ le grand cercle passant par x_0 et x_1. Le cercle de S^2 de centre x_1 et passant par x_0 est inclus dans B par (b), et il coupe $\mathscr{C}$ en deux points x_0, x_2. On construit ainsi de proche en proche une suite de points $x_0, x_1, x_2, \ldots, x_n$ de $B \cap \mathscr{C}$, avec $(x_0x_n) \subset \mathscr{C}$ de longueur $n\ell$ et (x_ix_{i+1}) de longueur ℓ. Soit $n > 0$ le plus petit entier tel que la longueur de $(x\, x_{n+1})$ est $\geqslant \pi/2$. Alors $(x_nx_{n+1}) \cap \mathscr{C}_x$ est non vide. On peut supposer $x_n, x_{n+1} \notin \mathscr{C}_x$ (sinon on a gagné). Mais alors le cercle de centre x_n et de rayon ℓ rencontre $\mathscr{C}_x$ car $\ell < \pi/2$, puis $B \cap \mathscr{C}_x \neq \emptyset$ par (b).

(ii) Pour $n \geqslant 1$ on note $C_n \subset \mathrm{SO}(2)$ le sous-groupe cyclique d'ordre n. C'est un sous-groupe distingué de $\mathrm{SO}(2)$ car ce dernier est abélien. Ses orbites dans S^1 sont donc des blocs pour l'action de $\mathrm{SO}(2)$ sur S^1 par l'Exercice 5.18 (iv). Une telle orbite a n éléments (sommets d'un polygone régulier du plan à n côtés).

Exercice 5.20. (i) D'après l'Exercice 5.18 (iv), les orbites de S^2 sous H sont des blocs pour l'action de $\mathrm{SO}(3)$. Par ce même exercice assertion (ii), ce sont des parties équilibrées. Par l'Exercice 5.19, chaque orbite de S^2 sous H est donc soit de la forme $\{x\}$, soit de la forme $\{x, -x\}$, soit S^2. Dans ce dernier cas on conclut, et sinon pour tout $h \in H$ on a $h(x) = \pm x$ pour tout $x \in \mathrm{S}^2$. On sait qu'un tel h est une homothétie, puis $h = \pm\mathrm{id}$, et donc $h = 1$ car $\det -1_3 = -1$. C'est une contradiction car H est non trivial.

(ii) Soit s_P la réflexion orthogonal d'hyperplan $P \subset \mathbb{R}^3$. On a $-\mathrm{s}_P \in \mathrm{SO}(3)$, puis

$$[h, -\mathrm{s}_P] = g\mathrm{s}_P g^{-1}\mathrm{s}_P = \mathrm{s}_{h(P)}\mathrm{s}_P$$

pour tout $h \in H$. Comme H est distingué dans $\mathrm{SO}(3)$ on a $[h, -\mathrm{s}_P] \in H$ pour tout plan P et $h \in H$. Mais H agit transitivement sur S^2 par le (i), donc sur les plans de $\mathbb{R}^3$ (considérer un vecteur orthogonal). La formule ci-dessus montre que H contient tous les produits de deux réflexions. On a donc $H = \mathrm{SO}(3)$ par Cartan-Dieudonné.

Exercice 5.28. On voit $\mathbb{H}$ comme espace euclidien muni de n. On a vu en cours $q \in \mathscr{I} \iff q \in \mathbb{H}^0$ et $\mathrm{n}(q) = 1$. (i) Soient q et q' deux éléments de $\mathscr{I}$, *i.e.* de la sphère unité de $\mathbb{H}^0$, il existe $u \in \mathrm{SO}(\mathbb{H}^0)$ avec $u(q) = q'$. D'après le cours, u est de la forme $h \mapsto xhx^{-1}$ pour un certain $x \in \mathrm{Sp}(1)$. On a donc $q' = xqx^{-1}$, comme demandé. (Voir l'exercice suivant pour une généralisation de cet argument).

(ii) Comme indiqué, $\mathbb{C}_q$ est un sous-corps de $\mathbb{H}$ de dimension 2 sur $\mathbb{R}$ (isomorphe à $\mathbb{C}$!). (En particulier, il est commutatif). On peut donc voir $\mathbb{H}$ comme $\mathbb{C}_q$-espace vectoriel. On constate que si $a, b \in \mathbb{H}$ est $\mathbb{C}_q$-libre, alors a, qa, b, qb est $\mathbb{R}$-libre, donc $\mathbb{H}$ est un $\mathbb{C}_q$-espace vectoriel de dimension 2. Écrivons $\mathbb{H} = \mathbb{C}_q + \mathbb{C}_q h$ pour un certain $h \in \mathbb{H}$, en complément la famille libre $\{1\}$. Si $A \subset \mathbb{H}$ contient strictement $\mathbb{C}_q$, il va contenir qh pour un certain $q \in \mathbb{C}_q$ non nul, donc inversible, puis $h \in A$ et $\mathbb{C}_q + \mathbb{C}_q = \mathbb{H} \subset A$.

(iii) On a $q^2 - aq + b = 0$ avec $a, b \in \mathbb{R}$ par Cayley-Hamilton. On a donc $(q - a/2)^2 = -b + a^2/4$. Si $-b + a^2/4$ est $\geqslant 0$, on a $(q - a/2)^2 = u^2$ avec $u \in \mathbb{R}$, puis $(q - a/2 - u)(q - a/2 + u) = 0$ dans $\mathbb{H}$ et donc $q = a/2 \pm u \in \mathbb{R}$, en contradiction avec l'énoncé. On a donc $(q - a/2)^2 = -u^2$ avec $u \in \mathbb{R}^\times$, et donc $q' = \frac{1}{u}(q - a/2) \in \mathbb{C}_q$ vérifiant $q'^2 = -1$, puis évidemment $\mathbb{C}_{q'} = \mathbb{R} + \mathbb{R}q' = \mathbb{R} + \mathbb{R}q$.

(v) Si A est une sous-algèbre de $\mathbb{H}$, on a $\mathbb{R} \subset A$ par définition. Si $\mathbb{R} \subsetneq A$, il existe $q \in \mathscr{I}$ avec $\mathbb{C}_q \subset A$ par le (iii). Par le (ii) on a soit $A = \mathbb{H}$, soit $A = \mathbb{C}_q$. Les $\mathbb{C}_q$ sont conjuguées par le (i).

Exercice 5.29. D'abord, on a $\mathrm{t}(xqx^{-1}) = \mathrm{t}(x^{-1}xq) = \mathrm{t}(q)$ car on a $\mathrm{trace} AB = \mathrm{trace}\, BA$ pour A, B dans $\mathrm{M}_2(\mathbb{C})$. Réciproquement, supposons $q, q' \in \mathrm{Sp}(1)$ et $\mathrm{t}(q) = \mathrm{t}(q')$. Dans l'espace euclidien $(\mathbb{H}, \mathrm{n})$, de produit scalaire $x.y = \mathrm{tr}(x^*y)$, on a donc $1.q = 1.q'$. Ainsi, il existe $u \in \mathrm{O}(\mathbb{H})$ vérifiant $u(1) = 1$ et $u(q) = q'$. Quitte à modifier u par un élément de $\mathrm{O}(\mathbb{H})$ fixant 1, q et de déterminant -1, on peut supposer $u \in \mathrm{SO}(\mathbb{H})$). Mais alors on $\mathrm{a}u(x) = axb^{-1}$ pour certains $a, b \in \mathrm{Sp}(1)$ par le cours, puis $u(1) = ab^{-1} = 1$ donc $a = b$, et donc $u(q) = aqa^{-1} = q'$.

Exercice 5.30. Pour $1 \leqslant k \leqslant m/2$, on considère le polynôme suivant dans $\mathbb{R}[X]$

$$P_{k/m}(X) = (X - e^{2ik\pi/m})(X - e^{-2ik\pi/m}) = X^2 - 2\cos(2k\pi/m)X + 1.$$

Le polynôme $X^m - 1$ est produit de $X - 1$ et des $P_{k/m}$ dans $\mathbb{R}[X]$, avec $1 \leqslant k < m/2$, ainsi que de $X + 1$ si m est pair. Ainsi, pour $q \neq \pm 1$, on a $q^m = 1$ si, et seulement si, il existe $0 < k/m < 1/2$ avec $P_{k/m}(q) = 0$, car $\mathbb{H}$ est un corps gauche.

Soit $q \in \mathrm{Sp}(1)$, de polynôme caractéristique $\chi_q = X^2 - \mathrm{t}(q)\, X + 1$. Sous l'hypothèse de l'énoncé, on a $\chi_q = P_{k/m}$, et donc le théorème de Cayley-Hamilton montre $P_{k/m}(q) = 0$, et q est d'ordre m. Réciproquement, si on a $P_{k/m}(q) = 0$ le polynôme minimal de q dans $\mathbb{R}[X]$ divise $P_{k/m}$, et est donc égal à $P_{k/m}$ car ce dernier est irréductible. Mais il divise aussi χ_q par Cayley-Hamilton, et on a donc $\chi_q = P_{k/m}$. (Une démonstration alternative aurait été d'utiliser l'exercice précédent).

Exercice 5.35. Il est évident que G_B est un sous-groupe de G.

(i) Si B est un bloc, on a vu que B est équilibré à l'Exercice 5.18, ce qui signifie $G_x \subset G_B$ pour tout $x \in B$. Soient $b, b' \in B$. Par transitivité de l'action de G sur X, il existe $g \in G$ avec $gb = b'$. Mais alors $gB \cap B$ est non vide, et donc $g(B) = B$ car B est un bloc, puis $g \in G_B$. On a montré que G_B agit transitivement sur B.

(ii) Montrons que $B = Hx$ est un bloc pour l'action de G sur X. Si on a $ghx = h'x$ pour $g \in G$ et $h, h' \in H$, alors constate que l'on a $(h')^{-1}gh \in G_x$, puis $g \in h'G_xh^{-1} \in H$ car G_x est inclus dans H. On en déduit $gB = gHx = Hx = B$: on a montré que B est un bloc. L'inclusion $H \subset G_B$ est évidente, et l'analyse juste faite montre $G_B \subset H$.

(iii) Notons $\mathscr{B}_x$ l'ensemble des blocs de X contenant x et $\mathscr{G}_x$ l'ensemble des sous-groupes de G contenant G_x. D'après le (ii), on a une application bien définie $\beta : \mathscr{G}_x \to \mathscr{B}_x,\ H \mapsto Hx$. D'après le (i), on a une application bien définie $\gamma : \mathscr{B}_x \mapsto \mathscr{G}_x, B \mapsto G_B$. Ces applications sont manifestement croissantes pour l'inclusion. Pour $H \in \mathscr{G}_x$ on a $\gamma \circ \beta(H) = G_{Hx} = H$, par le (ii). On a aussi $\beta \circ \gamma(B) = G_Bx = B$ car G_B agit transitivement sur B par le (i). Ainsi, β et γ sont inverses l'une de l'autre.

Exercice 5.36. (i) Soit B un bloc et $b \in B$. On a vu $G_b \subset G_B$. Mais G_b agit transitivement sur $X \smallsetminus \{b\}$ par l'hypothèse de 2-transitivité. Ainsi, on a soit $B = \{b\}$, soit $B = X$: l'action est primitive.

(ii) Comme N agit non trivialement, il existe $x \in X$ avec $|Nx| > 1$. Mais Nx est un bloc par la question (iv) de l'Exercice 5.18. On a donc $Nx = X$ par primitivité, et donc N agit transitivement sur X.

(iii) C'est verbatim la démonstration du cours à ceci près qu'on utilise le (ii) au lieu de la 2-transitivité pour assurer que si N agit non trivialement sur X alors il agit transitivement.

(iv) Supposons que G agit transitivement sur X et fixons $x \in X$. D'après la dernière question de l'Exercice 5.35, G_x est un sous-groupe maximal si et seulement si les deux seuls blocs de X contenant x sont $\{x\}$ (cas $H = G_x$) et X (cas $H = G$). Si l'action est primitive, on en déduit donc que G_x est maximal. Réciproquement supposons G_x maximal. Soit B un bloc de X. Alors les $g(B)$ avec $g \in G$ sont clairement aussi des blocs de X. Comme l'action est transitive l'un deux contient x. On a donc $g(B) = \{x\}$ ou $g(B) = X$. Dans le second cas on a $B = X$, et dans le premier on a $B = \{g^{-1}x\}$: l'action est primitive.

(v) Soient $x \in X$, $Y = X \smallsetminus \{x\}$ et $g \in G \smallsetminus G_x$. On a $g(x) \neq x$, et donc $g(x) \in Y$. On sait que G agit 2-transitivement sur X, si et seulement si G_x agit transitivement sur Y (Exercice 4.23 (i)). Supposons que G_x agit transitivement sur Y. Pour $h \in G \smallsetminus G_x$, l'élément $h(x) \in Y$ est de la forme $kg(x)$ pour un certain $k \in G_x$. On a donc $g^{-1}k^{-1}h(x) = x$ puis $g^{-1}k^{-1}h \in G_x$ et donc $h \in G_xgG_x$. On a montré $G = G_x \cup G_xgG_x$. Supposons réciproquement $G = G_x \cup G_xgG_x$. Comme G agit transitivement sur X, on a

$$X = Gx = G_x\,x \cup G_x\,g\,G_x\,x = \{x\} \cup G_x\,g(x).$$

Noter qu'un élément de la forme $hg(x)$ avec $h \in G_x$ ne peut être égal à x, sinon on aurait $g(x) = h^{-1}(x) = x$, absurde. On en déduit $Y = G_xg(x)$, et donc que G_x agit transitivement sur Y.

Exercice 5.37. On rappelle $n \geqslant 3$.

(i) Notons $\mathscr{C}_n$ l'ensemble des couples (I, J) constitués de deux parties $I, J \subset \{1, \ldots, n\}$ avec $|I| = |J| = 2$ et $I \neq J$. Le groupe S_n agit sur $\mathscr{C}_n$ via $(\sigma, (I, J)) \mapsto (\sigma(I), \sigma(J))$. Dire que S_n agit 2-transitivement sur X_n est équivalent à dire qu'il agit transitivement sur $\mathscr{C}_n$. Mais il y a deux "types" d'éléments de $\mathscr{C}_n$: les couples (I, J) avec $I \cap J = \varnothing$ et ceux avec $|I \cap J| = 1$. Le premier type n'existe que pour $n \geqslant 4$ car on doit avoir $4 = |I| + |J| \leqslant n$, et le second existe pour tout $n \geqslant 3$. Si (I, J) et d'un type, et pour $\sigma \in \mathrm{S}_n$, alors $(\sigma(I), \sigma(J))$ est clairement du même type. Ainsi, pour que S_n agisse 2-transitivement sur X_n il faut que l'on ait $n = 3$. Pour $n = 3$, X_3 est en bijection avec $\{1, 2, 3\}$ par passage au complémentaire, et l'action de S_3 sur X_3 est équivalente à celle sur $\{1, 2, 3\}$, qui est 3-transitive comme on le sait.

(ii) Pour $n = 4$, observons que les parties à deux éléments de X_4 de la forme $\{I, I^c\}$, avec I^c le complémentaire de I dans $\{1, 2, 3, 4\}$, sont des blocs non triviaux. En effet, ces parties sont deux à deux disjointes dans X_4, et permutées par S_4. Ainsi, l'action n'est pas primitive pour $n = 4$. Elle est 2-transitive donc primitive pour $n = 3$.

Supposons $n > 4$. Soit $B \subset X_4$ une partie équilibrée de cardinal > 1. Pour $\{i, j\} \in B$, alors B est stable par le stabilisateur de $\{i, j\}$ dans S_n, qui est un groupe $\simeq \mathrm{S}_2 \times \mathrm{S}_{n-2}$ agissant à la fois transitivement sur $\{i, j\}$ et $n-2$ transitivement sur son complémentaire (et ce indépendamment). Ainsi, si B contient un élément I avec $|I| = 2$ et $I \cap \{i, j\} = \varnothing$ (resp. $|I \cap \{i, j\}| = 1$), il contient toutes les telles parties. Mais pour $n \geqslant 5$, le complémentaire d'une partie à 2 éléments de $\{1, \ldots, n\}$ contient deux parties à deux éléments distinctes et d'intersection non triviale. Ainsi, B contient toujours deux parties à 2 éléments de $\{1, \ldots, n\}$ qui sont distinctes d'intersection non triviale, disons $\{1, 2\}$ et $\{2, 3\}$ quitte à renuméroter. Il contient ensuite $\{1, 3\}$, les $\{1, i\}$ avec $i > 1$, les $\{2, i\}$ avec $i > 2$, puis tous les $\{i, j\}$ avec $i \neq j$. On a montré $B = X_n$: l'action est primitive.

(iii) On suppose $n > 4$. On a vu que S_n agit primitivement sur X_n. Le stabilisateur dans S_n de l'élément $\{1, 2\} \in X_n$ est $\mathrm{S}_2 \times \mathrm{S}_{n-2}$. Il contient $A := \mathrm{S}_2 \times 1$ comme sous-groupe abélien distingué, engendré par la transposition $(1\,2)$, et on sait que les conjugués de $(1\,2)$ dans S_n engendent S_n. D'après le critère d'Iwasawa (version du (iii) de l'Exercice 5.36), un sous-groupe distingué de S_n contient soit $\mathrm{D}(\mathrm{S}_n) = \mathrm{A}_n$ (ce point était facile dans le cours), soit est inclus dans le noyau de l'action de S_n sur X_n. Mais cette action est fidèle, car un $\sigma \in \mathrm{S}_n$ stabilisant $\{i, j\}$ et $\{i, k\}$ pour tous i, j, k distincts fixe tout $i \in \{1, \ldots, n\}$.

Exercice 5.43. (i) On a $|\mathrm{A}_8| = 8!/2$. D'autre part, si k est un corps à q éléments on a $|\mathrm{SL}_3(k)| = q^3(q^3 - 1)(q^2 - 1)$ et $|\mu_3(k)| = (3, q - 1)$. Pour $q = 4$ on a donc

$$|\mathrm{PSL}_3(\mathbb{F}_4)| = \frac{1}{3} \cdot 4^3 \cdot (4^3 - 1) \cdot (4^2 - 1) = 4^4 \cdot 7 \cdot 9 \cdot 5 = 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 = \frac{8!}{2}.$$

(ii) Soit $g \in \mathrm{SL}_3(\mathbb{F}_4)$ avec $g^2 = 1$. On a $(g-1)^2 = 0$ dans $\mathrm{M}_3(\mathbb{F}_4)$ car on a $2g = 0$. On en déduit $\{0\} \subsetneq \mathrm{Im}(g-1) \subset \ker g - 1$, puis par le théorème du rang que l'on a $\dim \ker(g-1) = 2$. Ainsi g est une transvection. Mais toutes les transvections sont conjuguées dans $\mathrm{SL}_3(k)$. Il ne reste qu'à vérifier sur une seule transvection qu'elle est d'ordre 2 pour en déduire que les éléments d'ordre 2 de $\mathrm{SL}_3(\mathbb{F}_4)$ forment une unique classe de conjugaison. On conclut car on a par exemple $(1_3 + \mathrm{E}_{2,3})^2 = 1_3 + 2\mathrm{E}_{2,3} = 1_3$ dans $\mathrm{M}_3(\mathbb{F}_4)$ car on a $2x = 0$ pour tout $x \in \mathbb{F}_4$.

(iii) Posons $f : \mathrm{SL}_3(\mathbb{F}_4) \to \mathrm{PSL}_3(\mathbb{F}_4)$ la projection canonique. On a $\ker f = \mu_3(\mathbb{F}_4) = \mathbb{F}_4^\times \simeq \mathbb{Z}/3\mathbb{Z}$. Notons A (resp. B) l'ensemble des éléments d'ordre 2 de $\mathrm{SL}_3(\mathbb{F}_4)$ (resp. $\mathrm{PSL}_3(\mathbb{F}_4)$). Aucun élément de $\ker f$ n'est d'ordre 2. Ainsi, pour $g \in A$ on a $f(g)^2 = 1$ et $f(g) \neq 1$, et donc $f(g) \in B$. Vérifions que l'application $f_{|A} : A \to B, a \mapsto f(a)$, bien définie, est bijective. Si on a $g, h \in A$ avec $f(g) = f(h)$, on a donc $g = \lambda h$ pour un $\lambda \in \mathbb{F}_4^\times$. Mézalor on a $g = g^3 = \lambda^3 h^3 = 1 \cdot h$, puis $g = h$. Ainsi, $f_{|A}$ est injective. Reste à voir sa surjectivité. Soit $g \in B$. Par surjectivité de f il existe $h \in \mathrm{SL}_3(\mathbb{Z}/2\mathbb{Z})$ avec $f(h) = g$. On a $h^6 = 1$, donc l'ordre de h divise 6. Mais on a $f(h^3) = g^3 = g \neq 1$, donc l'ordre de h est 2 ou 6. Dans le premier cas on a $h \in A$ et on a gagné. Dans le second, on a $h^3 \in A$ et $f(h^3) = g$: on a aussi gagné.

(iv) Comme A est l'ensemble des conjugués d'un certain $a \in A$ par le (ii), et comme on a $f(gag^{-1}) = f(g)f(a)f(g)^{-1}$ car f est un morphisme, on déduit du (iii) que tous les éléments d'ordre 2 de $\mathrm{PSL}_3(\mathbb{F}_4)$ sont conjugués. Si on avait $\mathrm{A}_8 \simeq \mathrm{PSL}_2(\mathbb{F}_4)$, alors A_8 n'aurait qu'une classe de conjugaison d'éléments d'ordre 2. Mais les éléments $(1\,2)(3\,4)$ et $(1\,2)(3\,4)(5\,6)(7\,8)$ sont d'ordre 2, dans A_8, et non conjugués dans S_8.

Exercices du chapitre 6

Exercice 6.1. (i) Comme P est non trivial, son centre Z est non trivial par le cours. Ainsi, Z possède un élément d'ordre p. En effet, cela découle immédiatement de Cauchy, ou même plus simplement de ce que si on a $x \in Z \smallsetminus \{1\}$, alors x est d'orde p^m avec $m > 0$, et donc $x^{p^{m-1}} \in Z$ est d'ordre p. Au final, le sous-groupe $H := \langle x \rangle$ est d'ordre p, inclus dans Z, et donc distingué dans G.

(ii) On raisonne par récurrence sur n. C'est trivial pour $n \leqslant 1$. Soit C un sous-groupe distingué d'ordre p de P. Un tel C existe par le (i). Le groupe quotient P/C est un p-groupe d'ordre $|P|/p = p^{n-1}$. Par récurrence, il contient des sous-groupes distingués Q_i avec $|Q_i| = p^i$ pour $i < n$ et $Q_i \subset Q_{i+1}$ pour $i < n-1$. En utilisant la bijection croissante entre sous-groupes (distingués) de P/C et sous-groupes (distingués) de P contenant C, chaque Q_i s'écrit P_{i+1}/C où P_{i+1} est un sous-groupe distingué de P contenant C, et avec $P_i \subset P_{i+1}$ pour $1 \leqslant i < n$. On a bien sûr $|P_{i+1}| = |C||Q_i| = p^{1+i}$. On conclut en posant $P_0 = \{1\}$.

Exercice 6.2. (i) Soient P un p-groupe et M un sous-groupe maximal de P (ce qui force $P \neq 1$). On montre que M est distingué d'indice p par récurrence sur $|P|$. C'est évident si on a $|P| = p$, car alors on a $M = \{1\}$. Soit C un sous-groupe central d'ordre p de P (Exercice 6.1 (i)). Si C est inclus dans M alors M/C est un sous-groupe maximal de P/C, donc distingué dans P/C et d'indice p par hypothèse de récurrence, et donc $M = \pi^{-1}(M/C)$ est aussi distingué dans P et d'indice p. Sinon on a $C \cap M = \{1\}$ et $MC = P$, avec C central, donc $P = C \times M$ (produit direct interne). Mais dans ce cas, M est manifestement encore distingué dans P, et d'indice p.

(ii) Dans D_8, les 5 éléments d'ordre 2 sont $c^2 = (1\,3)(2\,4)$, $\tau = (1\,4)(2\,3)$, $c\tau c^{-1} = (2\,1)(3\,4)$, $c\tau = (2\,4)$ et $\tau c = (3\,1)$. Seul $\langle c^2 \rangle$ est distingué (en fait, il est central).

Exercice 6.3. On pose $G = \mathrm{GL}_n(k)$, $T = \mathrm{T}_n(k)$ et $U = \mathrm{U}_n(k)$. On note aussi $\epsilon_1, \ldots, \epsilon_n$ la base canonique de k^n, et $F_i = \mathrm{vect}_k(\epsilon_1, \ldots, \epsilon_i)$.

(i) On a un morphisme surjectif naturel $\mathrm{diag} : T \to (k^\times)^n$ de noyau U, c'est pourquoi U est distingué dans T, et on a donc $T \subset \mathrm{N}_G(U)$. Réciproquement, soit $g \in \mathrm{N}_G(U)$. On a $u(F_i) = F_i$ pour tout $u \in U$ et tout i, et donc $u(g(F_i)) = g(F_i)$ pour tout $u \in U$ et tout i. Cela implique $g \in \mathrm{T}_n(k)$. Une manière de le voir est de considérer l'élément $X \in \mathrm{M}_n(k)$ envoyant ϵ_i sur ϵ_{i-1} pour $i > 1$, et ϵ_1 sur 0. L'élément $u = 1 + X \in U$ a pour unique sous-espace stable de dimension i le sous-espace F_i. En effet, si E_i est un tel sous-espace, on a $X_{|E_i}$ nilpotent, donc $X^i(E_i) = 0$, puis $E_i \subset \ker X^i$, mais ce dernier est égal à F_i, et donc $E_i = F_i$ pour des raisons de dimension. Appliqué à $E_i = g(F_i)$, on a montré $g(F_i) = F_i$.

(ii) Soit $g \in G$ normalisant $\mathrm{T}_n(k)$. On voit comme ci-dessus $t(g(F_i)) = g(F_i)$ pour tout $t \in \mathrm{T}_n(k)$, et appliqué à $t = 1 + X$ comme ci-dessus on a encore $g \in \mathrm{T}_n(k)$.

Exercice 6.4. (i) Un groupe d'ordre p^n avec p premier possède au moins un sous-groupe d'ordre p^i pour tout $0 \leqslant i \leqslant n$ d'après l'Exercice 6.1. Ainsi, G possède un sous-groupe H d'ordre p^2. Un tel sous-groupe est nécessairement distingué d'après l'Exercice 6.2, ou encore d'après le Lemme de Ore (Exercice 4.22). Mais on sait qu'un groupe d'ordre p^2 est abélien d'après le cours. Par hypothèse, on a $g^p = 1$ pour tout $g \in G$, et donc H est abélien p-élémentaire. On a donc $H \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

(ii) Soit $g \in \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ vérifiant $g^p = 1$. On a $(g-1)^p = 0$ dans $\mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$ car $p \mid \mathrm{C}_p^k$ pour $k = 1, \ldots, p-1$. On en déduit que $g - 1$ est nilpotente. On a donc $(g-1)^2 = 0$. Mais $g - 1$ n'est pas nul car g est d'ordre $p > 1$, donc $g - 1$ est d'indice de nilpotence 1, et donc conjuguée à $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ dans $\mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$.

(iii) Soit $H \subset G$ le sous-groupe défini au (i). Soit $g \in G \smallsetminus H$. On a $g \neq 1$, donc g est d'ordre p car G est d'exposant p. On a $\langle g \rangle \cap H = \{1\}$(car $g \notin H$ et p est premier), donc $|\langle g \rangle H| = pp^2 = p^3$, puis $K := \langle g \rangle$ est un complément de H. Comme H est distingué, G est produit semi-direct interne de $K \simeq \mathbb{Z}/p\mathbb{Z}$ par $H \simeq (\mathbb{Z}/p\mathbb{Z})^2$. Considérons, comme toujours en situation de produit semi-direct interne, le morphisme de conjugaison

$$\alpha : K \to \mathrm{Aut}(H), k \mapsto \alpha_k, \text{ avec } \alpha_k(h) := \mathrm{int}_k(h) = khk^{-1} \text{ pour } h \in H.$$

On a $(\alpha_g)^p = \alpha_{g^p} = \mathrm{id}_H$ et donc α_g est un automorphisme de H d'ordre divisant p. Si on a $\alpha_g = \mathrm{id}_H$ alors $ghg^{-1} = h$ pour tout $h \in G$ et donc G est commutatif : absurde. Donc α_g est un élément d'ordre p de $\mathrm{Aut}(H) \simeq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. Dans une $\mathbb{Z}/p\mathbb{Z}$-base bien choisie du groupe abélien p-élémentaire $H \simeq (\mathbb{Z}/p\mathbb{Z})^2$, cet automorphisme a pour matrice t, par le (ii). Autrement dit, pour un isomorphisme $a : (\mathbb{Z}/p\mathbb{Z})^2 \xrightarrow{\sim} H$ bien choisi, on a $a^{-1} \circ \alpha_g \circ a = t$. On fixe l'isomorphisme $b : \mathbb{Z}/p\mathbb{Z} \to \langle g \rangle, \overline{k} \mapsto g^k$. Par suivi des isomorphismes (Proposition 7.8 Chap. 5), on a donc bien un isomorphisme

$$G \simeq (\mathbb{Z}/p\mathbb{Z})^2 \rtimes_{\alpha'} \mathbb{Z}/p\mathbb{Z},$$

avec $\alpha' : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^2) = \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ défini par $\alpha'(\overline{1}) = a^{-1} \circ \alpha_g \circ a = t$.

(iv) Le (iii) montre que tout groupe non abélien abélien d'ordre p^3 et d'exposant p est isomorphe au groupe $\Gamma := (\mathbb{Z}/p\mathbb{Z})^2 \rtimes_{\alpha'} \mathbb{Z}/p\mathbb{Z}$ avec α' comme ci-dessus. À isomorphisme près, il y a donc au plus un tel groupe d'ordre p^3. Mais par l'exercice 3.8 Chap. 3, le groupe $\mathrm{U}_3(\mathbb{Z}/p\mathbb{Z})$ convient. Cela termine la démonstration. On a montré au passage que Γ, qui est clairement d'ordre p^3 et non abélien (car $\alpha' \neq 1$), est d'exposant p. Cela peut bien sûr se vérifier directement !

Exercice 6.5. (i) Pour tout $x \in G$ on a $x^{p^3} = 1$ par Lagrange. Mais G n'est pas d'exposant p par hypothèse, donc il existe $x \in G$ d'ordre p^2 ou p^3. Comme G n'est pas abélien (donc non cyclique), un tel x est d'ordre p^2. Le sous-groupe H qu'il engendre est d'incide p dans G donc distingué d'après l'Exercice 6.2, ou encore d'après le Lemme de Ore (Exercice 4.22).

(ii) Soient $g \in G \smallsetminus H$ et $K = \langle g \rangle$. Le groupe H étant distingué d'indice p on a d'une part $G/H \simeq \mathbb{Z}/p\mathbb{Z}$ et donc $g^p \in H$, et d'autre part $G = HK$ car H est maximal. Toutefois, on ne sait pas si on a $H \cap K = \{1\}$ ou non, ou ce qui revient au même, si on a $g^p = 1$ ou non. Quoiqu'il en soit, comme H est distingué on dispose d'un morphisme de groupes $\alpha : G \to \mathrm{Aut}(H), h \mapsto (\mathrm{int}_g)_{|H}$. L'identité $g^p \in H$ et la commutativité de H montrent $\alpha(g)^p = \alpha(g^p) = \mathrm{id}_H$. Mais G n'étant pas commutatif, on a aussi $\alpha(g) \neq \mathrm{id}_H$. On en déduit que $\alpha(g)$ est un automorphisme de H d'ordre p. Mais H est cyclique d'ordre p^2, et donc on sait d'après le cours que tout automorphisme de H est de la forme $\varphi_k(h) = h^k$ avec $k \in (\mathbb{Z}/p^2\mathbb{Z})^\times$, et mieux, que l'application $(\mathbb{Z}/p^2\mathbb{Z})^\times \to \mathrm{Aut}(H), \overline{k} \mapsto \varphi_k$, est un isomorphisme de groupes. On a donc $\alpha(g) = \varphi_k$ pour un unique $k \in (\mathbb{Z}/p^2\mathbb{Z})^\times$ d'ordre p. Toujours par le cours sur les groupes cycliques, pour tout $q \in \mathbb{Z}$ premier à p, l'élément g^q engendre encore K, c'est pourquoi nous pouvons remplacer g par g^q si nécessaire sans changer la situation. Ainsi, quitte à remplacer g par g^{p-1}, et donc k par k^{p-1}, on peut supposer que $k \equiv 1 \bmod p$. Mais alors on a $k \equiv 1 + pu \bmod p^2$ avec $u \neq 0 \bmod p$. Quitte à remplacer en sus g par g^q avec $qu \equiv 1 \bmod p$, on peut supposer que l'on a $k \equiv 1+p \bmod p^2$. Autrement dit, on a $ghg^{-1} = h^{1+p}$ pour tout $h \in H$.

(iii) Soit $h \in H$. Pour $i \geqslant 1$ on a l'identité

$$(hg)^i = h\, ghg^{-1}\, g^2hg^{-2} \cdots g^{i-1}hg^{1-i}\, g^i.$$

On a aussi $g^ihg^{-i} = h^{(1+p)^i}$ par le (ii), ainsi que la congruence

$$\sum_{i=0}^{p-1}(1+p)^i \equiv p + (\sum_{i=0}^{p-1} i)\, p \equiv \frac{p(p+1)}{2} \bmod p^2.$$

On a déjà vu que l'on a $g^p \in H$. Comme G n'est pas abélien, g est d'ordre p ou p^2 (mais pas p^3), de sorte que $g^p \in H$ est d'ordre 1 ou p. Fixons γ un générateur de H. On a $g^p = \gamma^k$ pour un certain $k \equiv 0 \bmod p$. D'autre part, la formule ci-dessus montre

$$(\gamma^q\, g)^p = \gamma^{qp(p+1)/2+k} \quad \text{pour tout } q \in \mathbb{Z}.$$

On cherche $q \in \mathbb{Z}$ tel que $q\,p(p+1)/2 + k \equiv 0 \bmod p^2$. Comme on a $p > 2$ et $k \equiv 0 \bmod p$, il est équivalent de demander $q(p+1)/2 + \frac{k}{p} \equiv 0 \bmod p$. Cette équation a une unique solution $\overline{q} \in \mathbb{Z}/p\mathbb{Z}$ car $(p+1)/2 \equiv -1/2$ est non nul modulo $p > 2$. On pose $h = \gamma^q$.

(iv) On remplace g par hg, qui a même classe dans G/H mais qui a la propriété que $\langle hg \rangle \simeq \mathbb{Z}/p\mathbb{Z}$ est un complément de H. Posant $K' = \langle hg \rangle$, le groupe G est produit semi-direct interne de K' par H. On a encore $\alpha(hg) = \alpha(h)\alpha(g) = 1 \cdot \alpha(g) = \alpha(g) = (x \mapsto x^{(1+p)})$. On conclut par un simple suivi des isomorphismes, comme dans la question (iii) de l'exercice précédent. Il est clair que le produit semi-direct en question est d'ordre p^3, non abélien, et contient un élément d'ordre p^2.

Exercice 6.6. Il y a exactement 2 groupes non abéliens d'ordre p^3 à isomorphisme près. En effet, pour $p = 2$ on a vu en cours qu'il n'y a que H_8 et D_8. Pour $p > 2$, il y en a un et un seul d'exposant p d'après l'exercice 6.4, à savoir le groupe d'Heisenberg fini $\mathrm{U}_3(\mathbb{Z}/p\mathbb{Z})$, ainsi qu'un et un seul d'exposant $> p$ d'après l'exercice 6.5, à savoir le produit semi-direct du (iv) de ce même exercice.

Il faut bien noter que l'on a utilisé $p = 2$ au (iii) de l'Exercice 6.4 ci-dessus. En effet, l'énoncé est inexact pour $p = 2$: le groupe H_8 est d'ordre 8, d'exposant 4, non abélien, mais n'est pas un produit semi-direct de $\mathbb{Z}/2\mathbb{Z}$ par $\mathbb{Z}/4\mathbb{Z}$ (les 3 sous-groupes d'ordre 4 n'ont pas de complément).

Exercice 6.7. Comme une action transitive est par définition sur un ensemble non vide, on a $|G| > 1$.

(i) Pour tout automorphisme α de G, et tout $g \in G$, alors $\alpha(g)$ et g ont même ordre. Par hypothèse, tous les éléments de $G \smallsetminus \{1\}$ ont donc même ordre. Mais l'un d'eux est d'ordre premier p, soit par Cauchy en considérant p premier divisant $|G|$, soit en prenant un élément non trivial arbitraire et en l'élevant à une puissance convenable.

(ii) On sait que tout élément de G est d'ordre 1 ou p par le (i). Par Cauchy, on en déduit que G est un p-groupe. Mais le centre $\mathrm{Z}(G)$ de G est non trivial d'après le cours. Comme $\mathrm{Z}(G)$ est clairement stable par tout automorphisme de G, l'hypothèse sur G montre donc $G = \mathrm{Z}(G)$: c'est un groupe abélien.

(iii) Ainsi, G est un p-groupe abélien élémentaire, et donc isomorphe à $(\mathbb{Z}/p\mathbb{Z})^n$ pour un certain $n \geqslant 1$. Réciproquement un tel groupe convient. En effet, pour tout corps k, le groupe $\mathrm{GL}_n(k)$ agit transitivement sur $k^n \smallsetminus \{0\}$, et on a $\mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^n) \supset \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ (c'est même une égalité).

Exercice 6.8. (i) Si on a $p \neq 2$, alors n et $2n$ ont même valuation en p. Comme D_{2n} possède un sous-groupe cyclique C d'ordre n, les p-Sylow de C (il n'y en a en fait qu'un seul cas C est cyclique) sont des p-Sylow de D_{2n}, et sont donc cyclique.

(ii) Écrivons $2n = 2^k m$ avec m impair. Les 2-Sylow de S sont d'ordre 2^k. Mais D_{2n} contient un sous-groupe isomorphe à D_{2^k} par l'Exercice 4.41. Un tel sous-groupe est donc un 2-Sylow de D_{2n}, et on a donc $S \simeq \mathrm{D}_{2^k}$ par conjugaison des 2-Sylow.

Exercice 6.9. (i) Pour $n < p^2$ la valuation en p de $n!$ est $[n/p]$ (partie entière de n/p). Autrement dit, c'est le plus grand entier $0 \leqslant k$ tel que $kp \leqslant n$. Pour $1 \leqslant i \leqslant k$, notons c_i un p-cycle quelconque de S_n de support $\{(i-1)p + j \mid 1 \leqslant j \leqslant p\}$. Ce sont donc k p-cycles à supports disjoints. Ils engendrent donc un groupe abélien p-élémentaire P, et forment

même une $\mathbb{Z}/p\mathbb{Z}$-base de ce dernier (ils sont libres car les supports sont disjoints), de sorte que l'on a $P \simeq (\mathbb{Z}/p\mathbb{Z})^k$. Pour des raisons de cardinalité, P est un p-Sylow de S_n.

(ii) Le groupe S_n s'identifie naturellement au sous-groupe H des $\sigma \in \mathrm{S}_{n+1}$ vérifiant $\sigma(n+1) = n+1$. On a $|\mathrm{S}_{n+1}| = (n+1)|\mathrm{S}_n|$. Ainsi, si p ne divise pas $n+1$, tout p-Sylow de H est un p-Sylow de S_{n+1}. On conclut par conjugaison (et donc isomorphie !) des p-Sylow de S_{n+1}.

Exercice 6.10. On rappelle que les p-Sylow d'un groupe fini G sont tous conjugués, donc isomorphes. On ne considère bien sûr que les premiers $p \leqslant n$ et on notera $\mathrm{Syl}_{p,n}$ un p-Sylow de S_n. D'après l'Exercice 6.9 assertions (i) et (ii), on a $\mathrm{Syl}_{p,n} \simeq \mathbb{Z}/p\mathbb{Z}$ pour $p \leqslant n < 2p$ (facile !), $\mathrm{Syl}_{p,n} \simeq (\mathbb{Z}/p\mathbb{Z})^2$ pour $2p \leqslant n < 3p$ et $p \neq 2$ (idem !), et $\mathrm{Syl}_{p,n} \simeq \mathrm{Syl}_{p,n+1}$ pour p ne divisant pas $n+1$. On raisonne au cas par cas.

Pour $n = 2$, on a clairement $\mathrm{Syl}_{2,2} = \mathrm{S}_2 \simeq \mathbb{Z}/2\mathbb{Z}$.

Pour $n = 3$, on a $\mathrm{Syl}_{2,3} \simeq \mathrm{Syl}_{2,2} \simeq \mathbb{Z}/2\mathbb{Z}$ et $\mathrm{Syl}_{3,3} \simeq \mathbb{Z}/3\mathbb{Z}$.

Pour $n = 4$, on a $\mathrm{Syl}_{3,4} \simeq \mathrm{Syl}_{3,3} \simeq \mathbb{Z}/3\mathbb{Z}$. On a $|\mathrm{S}_4| = 24 = 3 \cdot 8$, donc $|\mathrm{Syl}_{2,4}| = 8$. Mais comme D_4 est un sous-groupe d'ordre 8 de S_4 on a $\mathrm{Syl}_{2,4} \simeq \mathrm{D}_4$.

Pour $n = 5$, on a $\mathrm{Syl}_{5,5} \simeq \mathbb{Z}/5\mathbb{Z}$, et pour $p = 2, 3$, $\mathrm{Syl}_{p,5} \simeq \mathrm{Syl}_{p,4}$, déjà décrits.

Pour $n = 6$, on a $\mathrm{Syl}_{5,6} \simeq \mathrm{Syl}_{5,5} \simeq \mathbb{Z}/5\mathbb{Z}$ et $\mathrm{Syl}_{3,6} \simeq (\mathbb{Z}/3\mathbb{Z})^2$. On a aussi $|\mathrm{S}_6| = 620 = 2^4 \cdot 3^2 \cdot 5$, donc $|\mathrm{Syl}_{2,6}| = 16$, et il reste donc à trouver un sous-groupe d'ordre 16 de S_6. Mais $\mathrm{S}_4 \times \mathrm{S}_2$ s'identifie au sous-groupe de S_6 préservant $\{5, 6\}$, et contient $\mathrm{D}_8 \times \mathrm{S}_2$ d'ordre 16. On a donc $\mathrm{Syl}_{2,6} \simeq \mathrm{D}_8 \times \mathbb{Z}/2\mathbb{Z}$.

Pour $n = 7$, on a $\mathrm{Syl}_{7,7} \simeq \mathbb{Z}/7\mathbb{Z}$ et $\mathrm{Syl}_{p,7} \simeq \mathrm{Syl}_{p,6}$ pour $p = 2, 3, 5$.

On considère enfin le cas $n = 8$. Pour $p = 3, 5, 7$ on a $\mathrm{Syl}_{p,8} \simeq \mathrm{Syl}_{p,7}$, déjà déterminé. On a $|\mathrm{S}_8| = 2^7 \cdot 3^2 \cdot 5 \cdot 7$ et donc $|\mathrm{Syl}_{2,8}| = 2^7$. Le sous-groupe de S_8 préservant $\{1, 2, 3, 4\}$ (et donc $\{5, 6, 7, 8\}$) est naturellement isomorphe à $\mathrm{S}_4 \times \mathrm{S}_4$. On obtient donc un sous-groupe d'ordre 2^6 de S_8 en considérant $\mathrm{D}_8 \times \mathrm{D}_8$. Concrètement, on peut prendre par exemple

$$D = \langle (1\,2\,3\,4), (5\,6\,7\,8), (1\,4)(2\,3), (5\,8)(6\,7) \rangle \simeq \mathrm{D}_8 \times \mathrm{D}_8.$$

Ce n'est pas tout-à-fait un 2-Sylow car son ordre est $2^6 < 2^7$. Mais on constate qu'il est normalisé par l'involution

$$\tau = (1\,5)(2\,6)(3\,7)(4\,8).$$

En effet, la conjugaison par τ échange $(1\,2\,3\,4)$ et $(5\,6\,7\,8)$, ainsi que $(1\,4)(2\,3)$ et $(5\,8)(6\,7)$. On en déduit que le groupe $S := \langle D, \tau \rangle$ vérifie $S = D\langle \tau \rangle$. Comme τ n'est pas dans D (ce dernier préserve $\{1, 2, 3, 4\}$), on a que $\langle \tau \rangle$ est un complément de D dans S, et donc $|S| = 2^7$: c'est un 2-Sylow de S_8. Par suivi des isomorphismes, on a

$$\mathrm{Syl}_{2,8} \simeq S \simeq (\mathrm{D}_8 \times \mathrm{D}_8) \rtimes_\alpha \mathbb{Z}/2\mathbb{Z}$$

où $\alpha : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathrm{D}_8 \times \mathrm{D}_8)$ est le morphisme envoyant $\overline{1}$ sur l'automorphisme $(x, y) \mapsto (y, x)$ de $\mathrm{D}_8 \times \mathrm{D}_8$.

Exercice 6.11. Les p-Sylow de S_{p^2} sont d'ordre p^m avec $m = \mathrm{v}_p(\mathrm{S}_{p^2}) = p + 1$. Pour $i = 0, \ldots, p-1$, on considère le p-cycle

$$\mathrm{c}_i = (ip+1 \;\; ip+2 \;\; \ldots \;\; ip+p) \;\in\; \mathrm{S}_{p^2}.$$

Ces p permutations sont des p-cycles sont à supports disjoints. En particulier, elles commutent deux à deux, et par unicité de la décomposition en cycles, engendrent un sous-groupe $H_1 = \langle \mathrm{c}_1, \ldots, \mathrm{c}_p \rangle$ de S_{p^2} isomorphe à $(\mathbb{Z}/p\mathbb{Z})^p$. On a $|H_1| = p^p < p^{p+1}$ donc H_1 est encore p fois trop petit.

Considérons enfin l'élément $\tau \in \mathrm{S}_{p^2}$ défini par $\tau(i) \equiv i + p \bmod p^2$ pour tout i. C'est un produit de p cycles de longueur p à supports disjoints, vérifiant $\tau \mathrm{c}_i \tau^{-1} = \mathrm{c}_{i+1}$, les

indices étant pris modulo p. En particulier, τ normalise H_1, et on a $\langle\tau\rangle \cap H_1 = \{1\}$, car les éléments de H_1 préservent tous $\{1, \ldots, p\}$, alors que 1 est le seul élément de $\langle\tau\rangle$ avec cette propriété. On en déduit que $H_2 = H_1\langle\tau\rangle$ est un sous-groupe d'ordre p^{p+1} de S_{p^2}. C'est donc un p-Sylow de S_{p^2}, produit semi-direct interne de $\langle\tau\rangle$ et H_1, et on conclut manifestement par suivi des isomorphismes.

Exercice 6.12. On pose $G = \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$. Observer que l'on a $\gcd(q-1, q+1) = 2$ si 1 pour $q = 2$, et $\gcd(q-1, q+1) = 2$ pour $q > 2$. En particulier, pour $p > 2$ on a exclusivement $p \mid q-1$ ou $p \mid q+1$, de sorte que l'on a $\mathrm{v}_p(|G|) = 2\alpha$ pour $p \mid q-1$ et $\mathrm{v}_p(|G|) = \beta$ pour $p \mid q+1$.

(i) Le sous-groupe des matrices diagonales est isomorphes à $(\mathbb{Z}/q\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$. De plus le groupe $(\mathbb{Z}/q\mathbb{Z})^\times$ est cyclique d'ordre $q-1$ d'après Gauss. Il contient donc un sous-groupe cyclique d'ordre p^α. Ainsi, G contient un sous-groupe diagonal isomorphe à $\mathbb{Z}/p^\alpha\mathbb{Z} \times \mathbb{Z}/p^\alpha\mathbb{Z}$. Par le premier paragraphe ci-dessus, c'est un p-Sylow, et il est donc isomorphe (même conjugué) à S.

(ii) On a vu à l'exercice **??** que G contient un sous-groupe cyclique C d'ordre q^2-1, dont la valuation en p est $\beta = \mathrm{v}_p(|G|)$. Ainsi, le sous-groupe cyclique d'ordre p^β de C est un p-Sylow de G, et donc isomorphe à S.

(iii) On suppose $p = 2$. On a donc $\alpha, \beta \geqslant 1$, $q > 2$, et $\gcd(q-1, q+1) = 2$, de sorte que l'on a soit $\alpha = 1$, soit $\beta = 1$. Supposons d'abord $\beta = 1$. D'après l'Exercice 5.44, le normalisateur dans G du sous-groupe $T \simeq (\mathbb{Z}/q\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$ des matrices diagonales est le groupe $N = T\langle w\rangle$ avec $w = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Il est isomorphe à $N' = (\mathbb{Z}/q\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$ avec $\varphi_{\overline{1}}(x, y) = (y, x)$. On constate $\mathrm{v}_2(|N|) = 2\alpha + 1 = \mathrm{v}_2(|G|)$ de sorte que les 2-Sylow de N sont des 2-Sylow de G, et donc isomorphes à S. Mais si D désigne l'unique 2-Sylow de $(\mathbb{Z}/q\mathbb{Z})^\times$ (cyclique d'ordre 2^α), alors $D \times D$ est l'unique 2-Sylow de $(\mathbb{Z}/q\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$, et il est stable par $(x, y) \mapsto (y, x)$, de sorte que $(D \times D) \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$ est un 2-Sylow de $N' \simeq N$, et donc isomorphe à S.

Supposons maintenant $\alpha = 1$, et donc $\mathrm{v}_2(|G|) = 2\alpha + \beta = 2 + \beta$. On a vu à l'exercice **??** que G possède un sous-groupe H isomorphe à D_{2n} avec $n := q^2 - 1 = (q-1)(q+1)$. Mais on a alors $\mathrm{v}_2(|H|) = \mathrm{v}_2(2n) = 1 + \alpha + \beta = 2 + \beta = \mathrm{v}_2(|G|)$. Ainsi, tout 2-Sylow de D_{2n} est un 2-Sylow de G, et donc isomorphe à S. On conclut par l'Exercice 6.8 (ii).

Exercice 6.13. (i) On raisonne dans l'anneau $\mathbb{Z}/p\mathbb{Z}[X]$. L'identité $(1+X)^p = 1 + X^p$ montre $(1+X)^{p^\alpha n} = (1 + X^{p^\alpha})^n$. En identifiant les coefficients en X^{p^α} on en déduit $\binom{p^\alpha n}{p^\alpha} \equiv n \bmod p$, et on conclut car on a $n \not\equiv 0 \bmod p$.

(ii) Soit $\mathscr{E}$ l'ensemble des parties à p^α éléments de G. On fait agit G sur $\mathscr{E}$ par $(g, X) \mapsto gX$. Fixons $X \in \mathscr{E}$, une partie à p^α éléments de G. Son stabilisateur dans G est

$$G_X = \{g \in G \mid gX = X\}.$$

En particulier, $X \subset G$ est une réunion de classes à droite de G_X dans G, et on a

$$X = \coprod_{i=1}^{n_X} G_X\, x_i,$$

pour certains représentants $x_i \in X$ en nombre n_X, et on a $|G_X|\, n_X = |X| = p^\alpha$. D'autre part, on a montré $|\mathscr{E}| \not\equiv 0 \bmod p$ au (i). On en déduit par équation aux classes qu'il existe une G-orbite dans $\mathscr{E}$ de cardinal premier à p, et donc un $X \in \mathscr{E}$ avec $\mathrm{v}_p(|G_X|) = \mathrm{v}_p(|G|) = \alpha$ (Formule orbite-stabilisateur). Pour un tel X, on nécessairement $n_X = 1$ et $|G_X| = p^\alpha$, et donc G_X est un p-Sylow de G.

Exercice 6.15. (i) Seule l'inclusion $\subset$ est non triviale. Soient $H = \mathrm{N}_G(P)$ et $g \in G$ avec $gHg^{-1} = H$. On a $P \subset H \subset G$. Alors gPg^{-1} est un p-Sylow de G, et donc de H. Par

conjugaison des p-Sylow dans H, il existe $h \in H$ tel que $gPg^{-1} = hPh^{-1}$. On en déduit $h^{-1}g \in \mathrm{N}_G(P) = H$, et donc $g \in H$. (On a répété l'argument de Frattini, que l'on aurait d'ailleurs pu appliquer directement au groupe $\mathrm{N}_G(H)$ et à son sous-groupe distingué H).

(ii) On rappelle que pour toute partie $A \subset G$, $\mathrm{C}_G(A)$ est le sous-groupe des $g \in G$ tels que $ga = ag$ pour tout $a \in A$. Soient $x, y \in \mathrm{C}_G(P)$, ainsi que $g \in G$ vérifiant $y = gxg^{-1}$. On a $P \subset \mathrm{C}_G(x) \cap \mathrm{C}_G(y)$ par hypothèse. On a aussi $\mathrm{C}_G(y) = g\,\mathrm{C}_G(x)\,g^{-1}$ en appliquant int_g. On en déduit que P et $g^{-1}Pg$ sont dans $\mathrm{C}_G(x)$. Mais ce sont des p-Sylow de G, et donc de $\mathrm{C}_G(x)$. Ils sont donc conjugués dans $\mathrm{C}_G(x)$: il existe $h \in \mathrm{C}_G(x)$ tel que $g^{-1}Pg = hPh^{-1}$. On a donc $gh \in \mathrm{N}_G(P)$, et $y = gxg^{-1} = ghxh^{-1}g^{-1}$ utilisant $h \in \mathrm{C}_G(x)$.

Exercice 6.16. (i) Par Cauchy, G possède un sous-groupe cyclique H d'ordre q. Comme H est d'indice p, le plus petit diviseur premier de $|G|$, le Lemme de Ore (Exercice 4.22) montre que H est distingué dans G. Cela montre le (i). Donnons une seconde démonstration utilisant les théorèmes de Sylow. On a $\mathrm{n}_q(G) \mid p$ et $\mathrm{n}_q(G) \equiv 1 \bmod q$. On a $p \not\equiv 1 \bmod q$ car $p < q$, donc $\mathrm{n}_q(P) = 1$ et G possède un unique q-Sylow. Il est donc distingué, et cyclique d'ordre q car $\mathrm{v}_q(|G|) = 1$.

(ii) Soit K un sous-groupe d'ordre p de G (il en existe par Cauchy ou Sylow). Pour des raisons de cardinalité (Exercice 2.9), on a $G = HK$ avec $H \cap K = \{1\}$. Ainsi, G est produit semi-direct interne de K par H. Considérons le morphisme de groupes habituel dans cette situation $\alpha : K \to \mathrm{Aut}(H)$, $k \mapsto (h \mapsto khk^{-1})$. Comme H est cyclique d'ordre q on sait que l'on a $\mathrm{Aut}(H) \simeq (\mathbb{Z}/q\mathbb{Z})^\times$, et en particulier $|\mathrm{Aut}(H)| = q - 1$ car q est premier. Sous l'hypothèse $q \not\equiv 1 \bmod p$, les cardinaux $|K|$ et $|\mathrm{Aut}(H)|$ sont premiers entre eux, et donc le morphisme α est trivial (i.e. $khk^{-1} = h$ pour tout $h \in H$ et tout $k \in K$). Le produit semi-direct est donc direct, et on a un isomorphisme

$$G \simeq H \times K \simeq \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}/pq\mathbb{Z}$$

(le dernier isomorphisme étant l'isomorphisme chinois).

(iii) On suppose désormais $q \equiv 1 \bmod p$. Le groupe $(\mathbb{Z}/q\mathbb{Z})^\times$ étant d'ordre $q-1$ (Gauss), il admet un élément ζ d'ordre p que l'on fixe. Mieux, comme $(\mathbb{Z}/q\mathbb{Z})^\times$ est cyclique, il admet un unique sous-groupe d'ordre p, à savoir $\langle\zeta\rangle$ (ou encore les p racines du polynome $X^p - 1$ dans $(\mathbb{Z}/q\mathbb{Z})[X]$). Regardons encore $\alpha : K \to \mathrm{Aut}(H)$ comme ci-dessus. Si α est trivial, le raisonnement précédent s'applique et montre $G \simeq \mathbb{Z}/pq\mathbb{Z}$. Supposons α non trivial, et donc injectif car $|K|$ est premier. Dans ce cas, $\alpha(K)$ est un sous-groupe d'ordre p de $\mathrm{Aut}(H)$: c'est donc $\langle\zeta\rangle$ par la remarque précédente. Ainsi, $x := \alpha^{-1}(\zeta)$ est un générateur de K vérifiant $xhx^{-1} = h^\zeta$ pour tout $h \in H$. Identifions K à $\mathbb{Z}/p\mathbb{Z}$ en envoyant x sur $\overline{1}$, et H à $\mathbb{Z}/q\mathbb{Z}$ arbitrairement. Par suivi des isomorphismes, on a montré $G \simeq G_\zeta$. Comme G_ζ est non commutatif, on a en outre G_ζ non isomorphe à $\mathbb{Z}/pq\mathbb{Z}$.

Exercice 6.17. (i) Les p-Sylow de G sont cycliques d'ordre p. Chacun p-Sylow contient donc $p-1$ éléments d'ordre p (tous sauf le neutre). Réciproquement, chaque élément d'ordre p engendre un unique p-Sylow de G. Il y a donc $\mathrm{n}_p(G)(p-1)$ éléments d'ordre p dans G.

(ii) Soit S l'ensemble des éléments de G qui ne sont pas d'ordre p. Par le (i), on a $|G| = |S| + \mathrm{n}_p(G)(p-1)$ puis $|S| = pm - (p-1)m = m$. Mais tout q Sylow est d'ordre m et inclus dans S. Ainsi, S est en fait l'unique q-Sylow de G, et $\mathrm{n}_q(G) = 1$.

(iii) Si G est simple, on a $\mathrm{n}_p(G) > 1$ et $\mathrm{n}_q(G) > 1$. Par Sylow, on a donc $\mathrm{n}_q(G) = p$ et $\mathrm{n}_p(G) = q$ ou q^2. Mais $\mathrm{n}_p(G) = q^2$ implique $\mathrm{n}_q(G) = 1$ par le (ii), une contradiction. On a donc $\mathrm{n}_q(G) = p$. Mais on a aussi les congruences $\mathrm{n}_q(G) \equiv 1 \bmod q$ et $\mathrm{n}_p(G) \equiv 1 \bmod p$, et donc $p \equiv 1 \bmod q$ et $q \equiv 1 \bmod p$. C'est absurde, car ces congruences impliquent $p > q$ et $q > p$.

(iv) Par Sylow, on a $\mathrm{n}_p(G) \mid qr$ et $\mathrm{n}_p(G) \equiv 1 \bmod p$. Par le (i) on sait que G contient $(p-1)\mathrm{n}_p(G)$ éléments d'ordre p. Idem en échangeant les rôles de p, q et r. En comptant

les éléments de G d'ordre premier ou 1 on a donc l'inégalité

$$(p-1)\mathrm{n}_p(G) + (q-1)\mathrm{n}_q(G) + (r-1)\mathrm{n}_r(G) < |G| = pqr. \tag{84}$$

On suppose par l'absurde $\mathrm{n}_p(G), \mathrm{n}_q(G)$ et $\mathrm{n}_r(G)$ tous > 1. Par la congruence de Sylow, ils sont alors $\geqslant 1+p, 1+q$ et $1+r$ respectivement. Quitte à renommer p, q, et r on peut supposer $p > q > r$. On en déduit que $\mathrm{n}_p(G) \in \{q, r, qr\}$ ne peut pas être q ou r : c'est donc qr. L'inégalité (84) montre alors $(q-1)\mathrm{n}_q(G) + (r-1)\mathrm{n}_r(G) < qr$ puis $q^2 - qr + r^2 < 2$. Mais on a $4(q^2 - qr + r^2) = (2q-r)^2 + 3r^2$, et $(2q-r)^2 + 3r^2 < 8$ force $r < 2$: absurde.

Exercice 6.18. (i) On peut supposer G non trivial. Si G est un p-groupe, on sait que son centre est non trivial. S'il est simple, il est donc abélien et isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Si on a $|G| = pq$, $|G| = p^2q$ ou $|G| = pqr$ avec p, q, r premiers distincts, on a vu aux Exercices 6.16 et 6.17 que G possède un sous-groupe de Sylow adéquat qui est distingué. En particulier, G n'est pas simple.

(ii) On raisonne par récurrence sur $|G|$ (évident pour $|G| = 1$). Si G est cyclique d'ordre premier, il est résoluble. Sinon, il n'est pas simple par le (i), et donc possède un sous-groupe distingué $H \subset G$ avec $H \neq 1, G$. Mais on a $|H||G/H| = |G|$ donc $|H|$ et $|G/H|$ sont $< |G|$ et encore produits d'au plus 3 nombres premiers, et donc résolubles par hypothèse de récurrence. On en déduit que G est résoluble par le cours.

Exercice 6.19. Pour le (i), voir le corrigé de la question (i) du Problème 1 de l'Examen 2022-2023. Pour le (ii), on rappelle que $\mathrm{n}_p(G)$ est l'indice de $\mathrm{N}_G(P)$ dans G. On a donc soit $\mathrm{n}_p(G) = 1$, soit $|G| \mid \mathrm{n}_p(G)!$ par le (i). Mais si $\mathrm{n}_p(G) = 1$, l'unique p-Sylow de G est distingué, donc égal à G, et G est un p-groupe simple, donc cyclique d'ordre p.

Exercice 6.20. (i) Écrivons $|G| = \prod_{i=1}^r p_i^{\alpha_i}$ avec les p_i premiers distincts et croissants. D'après l'Exercice 6.18, on a $\sum_{i=1}^r \alpha_i \geqslant 4$. On sait aussi que G n'est pas un p-groupe, donc on a $r > 1$. On a enfin $|G| \leqslant 60$ et $3^4 > 60$, puis $p_1 = 2$. On a $2 \cdot 3^3 = 54$ qui convient, et $2 \cdot 3^2 \cdot 5 > 60$, donc supposant $|G| \neq 54$ on a $\alpha_1 \geqslant 2$. Ainsi, $|G|/4$ est $\leqslant 15$ et produit d'au moins deux nombres premiers, dont au moins un impair. Les seules possibilités pour $|G|/4$ sont donc $6, 9, 10, 12, 14$ et 15.

(ii) Si on a $|G| = 24$, alors on a $\mathrm{n}_2(G) > 1$ car G est simple, puis $\mathrm{n}_2(G) = 3$, ce qui est absurde car $24 > 3!$ (Exercice 6.19). De même, on exclut $|G| = 36$ car $\mathrm{n}_3(G) = 1$ ou 4 sont impossibles ($36 > 4!$), et $|G| = 48$ car $\mathrm{n}_2(G) = 1$ ou 3 sont impossibles. Pour $|G| = 40$ c'est plus simple car on a $\mathrm{n}_5(G) = 1$, ainsi que pour $|G| = 54 = 2 \cdot 3^3$ car on a $\mathrm{n}_3(G) = 1$.

(iii) D'après le cours, il ne reste qu'à éliminer $|G| = 56$. Supposons donc $|G| = 56 = 2^3 \cdot 7$. On a $\mathrm{n}_7(G) \mid 8$ et $\mathrm{n}_7(G) \equiv 1 \bmod 7$, donc $\mathrm{n}_7(G) = 8$. Mais cela implique $\mathrm{n}_2(G) = 1$ par le (ii) de l'Exercice 6.17 : une contradiction.

Exercice 6.21. Soient G d'ordre 12, D un 2-Sylow de G et T un 3-Sylow de G. On a $G \simeq \mathbb{Z}/3\mathbb{Z}$ et $|D| = 4$. On sait qu'un groupe d'ordre 4 est abélien (car d'ordre p^2 !) et donc que l'on a $D \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ou $D \simeq \mathbb{Z}/4\mathbb{Z}$. Par l'Exercice 6.17, soit D, soit T est distingué dans G. Par l'Exercice 2.9, D et T sont compléments l'un de l'autre, et donc on a soit $D \lhd G$ et $G \simeq D \rtimes T$, soit $T \lhd G$ et $G \simeq T \rtimes D$ (produits semi-directs internes). On suppose en outre G non abélien : comme T et D sont abéliens, cela implique que G n'est pas produit direct de T et D.

Supposons d'abord D distingué dans G, et regardons le morphisme $\alpha : T \to \mathrm{Aut}(D), t \mapsto \alpha_t$, avec $\alpha_t(d) = tdt^{-1}$ pour $d \in D$. Comme G n'est pas produit direct, α est non trivial, *i.e.* $\alpha(T)$ est un sous-groupe d'ordre 3 de $\mathrm{Aut}(D)$. Cela montre que D n'est pas cyclique d'ordre 4, sans quoi on aurait $\mathrm{Aut}(D) \simeq (\mathbb{Z}/4\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}$. On a donc $D \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, et $\alpha(T)$ est un sous-groupe d'ordre 3 de $\mathrm{Aut}(D) \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \simeq \mathrm{S}_3$. Mais à conjugaison près, il y a un unique élément d'ordre 3 dans $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ (ou dans S_3 !), à savoir $u = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$

et son inverse (qui est aussi sa transposée !). On peut donc trouver une $\mathbb{Z}/2\mathbb{Z}$-base e, f du 2-groupe abélien élémentaire D, et un générateur g de T, tels que $\mathrm{Mat}_{e,f}\,\alpha_g = u$. Ainsi, considérons l'isomorphisme $b : \mathbb{Z}/3\mathbb{Z} \xrightarrow{\sim} T$ envoyant 1 sur g, et l'isomorphisme $a : (\mathbb{Z}/2\mathbb{Z})^2 \xrightarrow{\sim} D$ envoyant $(1,0)$ sur e et $(0,1)$ sur f. Par suivi des isomorphismes, on a

$$G \simeq (\mathbb{Z}/2\mathbb{Z})^2 \rtimes_{\alpha'} \mathbb{Z}/3\mathbb{Z}$$

avec $\alpha'_{\overline{1}} = u$. En particulier, il y a au plus un tel groupe G. Mais le groupe $G = \mathrm{A}_4$ convient (on a $D = \mathrm{K}_4$). On a donc $G \simeq \mathrm{A}_4$.

Supposons maintenant T distingué dans G, et regardons le morphisme $\alpha : D \to \mathrm{Aut}(T), d \mapsto \alpha_d$, avec $\alpha_d(t) = dtd^{-1}$ pour $t \in T$. Comme G n'est pas produit direct, α est non trivial, *i.e.* $\alpha(D)$ est un sous-groupe non trivial de $\mathrm{Aut}(T) \simeq (\mathbb{Z}/3\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}$. Autrement dit, il existe $x \in D$ vérifiant $\alpha_x(t) = t^{-1}$ pour tout $t \in T$ (l'unique automorphisme d'ordre 2 d'un groupe d'ordre 3). Comme $d \mapsto \alpha_d$ est un morphisme de groupes, x n'est pas un carré dans D. Cela montre que si on a $D \simeq \mathbb{Z}/4\mathbb{Z}$ alors x engendre D. Dans ce cas, un suivi des isomorphismes montre

$$G \simeq \mathbb{Z}/3\mathbb{Z} \rtimes_{\alpha'} \mathbb{Z}/4\mathbb{Z}, \;\; \alpha'_{\overline{1}}(t) = -t.$$

Le groupe G est donc uniquement déterminé à isomorphisme près, et il y a donc au plus un groupe non abélien d'ordre 12 ayant un 3-Sylow distingué et un 2-Sylow cyclique. Le groupe $\widetilde{\mathrm{D}_6}$ a cette propriété. En effet, il se surjecte sur $\mathrm{D}_6 \simeq \mathrm{S}_3$, de sorte qu'il est non abélien, et il a un unique élément d'ordre 2, de sorte que ses 2-Sylow sont cycliques, et aussi non distingués car ceux de son quotient S_3 sont non distingués.

Dans le cas restant, T est distingué dans G et on a $D \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Soit $y \in D$ tel que $\alpha_y = 1$. On a y d'ordre 2, $y \neq x$, et donc $\{x, y\}$ est une $\mathbb{Z}/2\mathbb{Z}$-base de $D^\sharp \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. On constate que $\langle y \rangle$ est dans le centre de G, et que $\langle x \rangle T$ en est un complément, de sorte que l'on a un produit direct interne $G \simeq \mathbb{Z}/2\mathbb{Z} \times H$ avec $H = \langle x \rangle T$ non abélien d'ordre 6, donc isomorphe à S_3.

Le groupe D_{12} admet un sous-groupe cyclique et distingué d'ordre 6, donc aussi un sous-groupe cyclique distingué d'ordre 3 (rotations d'ordre $\mid 3$), et son 2-Sylow est $\simeq \mathrm{D}_4 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (Exercice 6.8, c'est aussi le sous-groupe engendré par deux réflexions orthogonales d'un pentagone régulier). Il est donc isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathrm{S}_3$.

Exercice 6.22. (i) Soit G non abélien d'ordre pq^2. On rappelle que tous les q-Sylow de G sont conjugués, donc isomorphes. Comme ils sont d'ordre q^2, ils sont soit $\simeq \mathbb{Z}/q^2\mathbb{Z}$, soit $\simeq (\mathbb{Z}/q\mathbb{Z})^2$. Enfin, si l'un d'eux est distingué, ils le sont tous, car en fait il n'y en a qu'un. Soient P un p-Sylow de G et Q un q-Sylow de G. On a vu à l'Exercice 6.17 (iii) que soit P, soit Q est distingué dans G. Pour justifier le (i), il ne reste donc qu'à montrer que ces deux cas sont exclusifs. En effet, on a $G = PQ$ et $P \cap Q = \{1\}$ par l'Exercice 2.9. Si P et Q étaient distingués on aurait un produit direct $G = P \times Q$ par l'Exercice 2.11, et G serait abélien car P et Q le sont.

(ii) On écrit encore $G = PQ$ comme ci-dessus et on suppose P distingué. On a donc un produit semi-direct interne de Q par $P \simeq \mathbb{Z}/p\mathbb{Z}$. Pour qu'un tel produit semi-direct soit non abélien, il faut que le morphisme naturel $Q \to \mathrm{Aut}(P) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ soit non trivial, et donc que q divise $p-1$. Si c'est le cas, fixons un élément $\zeta \in (\mathbb{Z}/p\mathbb{Z})^\times$ d'ordre q. Notons G_n le produit semi-direct $\mathbb{Z}/p\mathbb{Z} \rtimes_\alpha \mathbb{Z}/q^n\mathbb{Z}$ défini par $\alpha : \mathbb{Z}/q^n\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ envoyant $\overline{1}$ sur $x \mapsto \zeta x$. En raisonnant comme dans l'Exercice 6.21, on voit que l'on a soit $G \simeq \mathrm{G}_2$ (cas Q cyclique), soit $G \simeq \mathbb{Z}/q\mathbb{Z} \times G_1$ (cas Q non cyclique). Réciproquement, G_2 et $\mathbb{Z}/q\mathbb{Z} \times G_1$ sont bien d'ordre pq^2, non abéliens, et non isomorphes, le premier ayant un q-Sylow cyclique, et l'autre isomorphe à $(\mathbb{Z}/q\mathbb{Z})^2$.

(iii) On écrit encore $G = PQ$ comme ci-dessus et on suppose maintenant $Q \simeq \mathbb{Z}/q^2\mathbb{Z}$ distingué, de sorte que G est produit semi-direct interne de $P \simeq \mathbb{Z}/p\mathbb{Z}$ par $Q \simeq \mathbb{Z}/q^2\mathbb{Z}$.

Pour qu'un tel produit semi-direct soit non abélien, il faut que le morphisme naturel $P \to \mathrm{Aut}(Q)$ soit non trivial. On sait que $\mathrm{Aut}(\mathbb{Z}/q^2\mathbb{Z}) \simeq (\mathbb{Z}/q^2\mathbb{Z})^\times$ est d'ordre $\varphi(q^2) = q(q-1)$. Ainsi, il existe un morphisme non trivial $\mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q^2\mathbb{Z})$ si, et seulement si p divise $q-1$. Supposons donc $q \equiv 1 \bmod p$. On sait que $(\mathbb{Z}/q^2\mathbb{Z})^\times$ est cyclique (Corollaire 5.9 Chap. 2) et donc possède un unique sous-groupe d'ordre p. Fixons $\zeta \in (\mathbb{Z}/q^2\mathbb{Z})^\times$ d'ordre p. Un générateur convenable de P agit donc comme $g \mapsto g^\zeta$ par conjugaison sur Q. Ainsi, par suivi des isomorphismes on a $G \simeq \mathbb{Z}/q^2\mathbb{Z} \rtimes_\alpha \mathbb{Z}/p\mathbb{Z}$ avec $\alpha_{\overline{1}}(x) = \zeta x$, comme unique possibilité pour G. Réciproquement, ce groupe convient, et on a donc $\mathrm{b}(p,q) = 1$.

(iv) On suppose maintenant Q distingué et $Q \simeq (\mathbb{Z}/q\mathbb{Z})^2$. Comme Q est abélien distingué, le morphisme $f : G \to \mathrm{Aut}(Q), g \mapsto (q \mapsto gqg^{-1})$, est trivial sur Q, et donc a pour image le sous-groupe $f(G) = f(P) \simeq \mathbb{Z}/p\mathbb{Z}$ de $\mathrm{Aut}(Q)$. Le choix d'une base de $Q^\sharp$ identifie $f(G)$ à un sous-groupe H de $\mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$, et changer de base de Q revient à conjuguer H par un élément de $\mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$, de sorte que le groupe G définit une unique classe de conjugaison de sous-groupes d'ordre p de H. Enfin, par suivi des isomorphismes, G s'identifie au produit semi-direct naturel

$$G_H := (\mathbb{Z}/q\mathbb{Z})^2 \rtimes_\alpha H,$$

avec $\alpha_h(x) = h(x)$ pour $h \in H$ et $x \in (\mathbb{Z}/q\mathbb{Z})^2$. Réciproquement, si $H \subset \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$ est un sous-groupe quelconque d'ordre p. Le groupe G_H ci-dessus est d'ordre pq^2, ayant $\{0\} \times (\mathbb{Z}/q\mathbb{Z})^2$ pour unique q-Sylow, et tel que le sous-groupe d'ordre p de $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})^2$ naturellement associé, et via l'identification naturelle $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})^2 = \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$, est H par construction. Cela conclut.

(v) Supposons d'abord $q = 2$, et donc $p > 2$. On a $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \simeq \mathrm{S}_3$. On en déduit $\mathrm{c}(3,2) = 1$ (il y a même un unique sous-groupe d'ordre 3) et $\mathrm{c}(p,2) = 0$ pour $p > 3$. Supposons maintenant $p = 2$, et donc $q > 2$. Un élément d'ordre 2 dans $\mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$ est annulé par $X^2 - 1 = (X-1)(X+1) \in \mathbb{Z}/q\mathbb{Z}[X]$ qui est scindé à racines distinctes (car $-1 \neq 1$!). Il est donc conjugé à $\mathrm{diag}(1,-1)$ ou à $\mathrm{diag}(-1,-1)$ (exclusivement), et on a $\mathrm{c}(2,q) = 2$.

(vi) Par le (iii), Cauchy et Lagrange on a

$$\mathrm{c}(p,q) \neq 0 \iff p \mid |\mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})| = q(q-1)(q+1) \iff q \equiv \pm 1 \bmod p.$$

Noter que comme on a $p > 2$, on ne peut pas avoir à la fois p divisant $q+1$ et $q-1$.

Supposons d'abord $p \mid q-1$. On a dit que $(\mathbb{Z}/q\mathbb{Z})^\times$ a un sous-groupe d'ordre p, et donc $X^p - 1$ est scindé à racines distinctes dans $\mathbb{Z}/q\mathbb{Z}[X]$. Ainsi, un sous-groupe H d'ordre p est engendré par un élément h diagonalisable. Fixons $\zeta \in (\mathbb{Z}/q\mathbb{Z})^\times$ d'ordre p, et pour $i \in \mathbb{Z}/q\mathbb{Z}$, posons $h_i = \mathrm{diag}(\zeta, \zeta^i)$ et $H_i = \langle h_i \rangle$. On vient de montrer que H est conjugué à l'un des H_i. Reste à voir à quelle condition on a H_i conjugué à H_j. Le groupe H_0 est le seul à avoir un générateur possédant la valeur propre 1, et donc H_i n'est pas conjugué à H_0 pour $i \neq 0$. De plus, dans H_i avec $i \neq 0$, les seuls éléments possédant la valeur propre ζ sont h_i et $\mathrm{diag}(\zeta^j, \zeta)$ où j est l'inverse de i dans $(\mathbb{Z}/p\mathbb{Z})^\times$. Pour i, j non nuls, on a donc H_i conjugué à H_j si, et seulement si, $ij = 1$. On conclut car le nombre d'orbites de $x \mapsto x^{-1}$ sur $(\mathbb{Z}/q\mathbb{Z})^\times$ est $1 + 1 + \frac{p-3}{2} = \frac{p+1}{2}$ car $p > 2$ (on a $q > 2$ et les points fixes sont 1 et -1).

Supposons enfin $p \mid q+1$. D'après l'Exercice 6.12, et utilisant $p > 2$, on sait que les p-Sylow de $\mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$ sont cycliques. En particulier, chaque p-Sylow de $\mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$ possède un et un seul sous-groupe d'ordre p. Mais on sait aussi que tout sous-groupe d'ordre p est inclus dans un p-Sylow, de sorte que par conjugaison des p-Sylow, deux sous-groupes d'ordre p quelconque de $\mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$ sont conjugués,[1] et on a $\mathrm{c}(p,q) = 1$.

1. Un autre point de vue, plus naturel avec le recul mais prématuré à ce stade du cursus, consisterait à utiliser que $\mathrm{M}_2(\mathbb{Z}/q\mathbb{Z})$ contient une unique classe de $\mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$-conjugaison de sous-corps de cardinal q^2, et d'utiliser que le groupe mutliplicatif d'un tel corps est cyclique par Gauss

Exercice 6.23. (i) Si x, y et z sont d'ordres respectifs p, q et r (Cauchy), alors xyz est d'ordre pqr si G est abélien.

(ii) Le nombre de r-Sylow d'un tel groupe est $\equiv 1 \bmod r$ et divise p ou $q < r$, c'est donc 1.

(iii) D'après l'Exercice 6.17 (iv), G possède un sous-groupe de Sylow S distingué. Par le théorème de Schur-Zassenhaus, S possède un complément K. Si on a $|S| = r$, c'est gagné. Supposons $|S| = p$ ou q, et donc $|K| = pr$ ou qr. Par le (ii), K admet un r-Sylow distingué R. Considérons morphisme de conjugaison $\varphi : R \to \mathrm{Aut}(S)$, $g \mapsto (s \mapsto gsg^{-1})$. On a $\mathrm{Aut}(S) \simeq (\mathbb{Z}/|S|\mathbb{Z})^\times$, d'ordre $|S| - 1 > r$. Ainsi, φ est trivial, et donc S commute à R. Ainsi, le normalisateur de R dans G contient S et K, ainsi donc que $G = SK$, et K est distingué dans G.

(iv) Par le (iii), si G est non abélien d'ordre pq, G est produit semi-direct interne de K par R avec $|R| = r$ et $|K| = pq$. Par l'Exercice 6.16, on sait que l'on a soit $K \simeq \mathbb{Z}/pq\mathbb{Z}$, soit $p \mid q-1$ et $K \simeq \mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$, un produit semi-direct supposé *non trivial*, mais qu'il est inutile de préciser davantage, car il n'en existe qu'un à isomorphisme près par cet exercice.

Supposons d'abord $K \simeq \mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$. On a donc $K = QP$ avec Q son q-Sylow distingué et P un p-Sylow. Un morphisme $f : K \to (\mathbb{Z}/r\mathbb{Z})^\times$ est nécessairement trivial sur Q. En effet, f ne peut pas être injectif sinon K serait abélien, et $\ker f = P$ entraînerait P distingué dans K puis $K \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ par l'Exercice 2.11. On a donc $q \mid \ker f$, puis $Q \subset \ker f$, *i.e.* f se factorise par $K/Q \simeq \mathbb{Z}/p\mathbb{Z}$. On a donc soit $f(K) = 1$ et $G = \mathbb{Z}/r\mathbb{Z} \times H$ (produit direct), soit $f(K)$ est l'unique sous-groupe d'ordre p de $\mathrm{Aut}(\mathbb{Z}/r\mathbb{Z}) \simeq (\mathbb{Z}/r\mathbb{Z})^\times$. Ce dernier cas est possible si, et seulement si, on a $p \mid r-1$. Il conduit à un produit semi-direct unique à isomorphisme près que l'on note $\mathbb{Z}/r\mathbb{Z} \rtimes (\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z})$. En effet, pour justifier l'unicité fixons $\zeta \in (\mathbb{Z}/r\mathbb{Z})^\times$ d'ordre p. Il existe $x \in P$ tel que $f(x) = \zeta$. On identifie P à $\mathbb{Z}/p\mathbb{Z}$ en faisant correspondre x et $\overline{1}$. Par suivi des isomorphismes, on a identifié G à $\mathbb{Z}/r\mathbb{Z} \rtimes_\alpha (\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z})$ où α est l'unique morphisme $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z} \to (\mathbb{Z}/r\mathbb{Z})^\times$ trivial sur $\mathbb{Z}/q\mathbb{Z} \times \{0\}$ et envoyant $(0, \overline{1})$ sur ζ.

Supposons maintenant $H \simeq \mathbb{Z}/pq\mathbb{Z}$. On a donc $H = Q \times P$ (produit direct) avec Q, P les uniques q et p-Sylow de G. Pour $n \mid pq$ et $n \mid r-1$, il existe à isomorphisme près un unique produit semi-direct $\mathbb{Z}/r\mathbb{Z} \rtimes_n \mathbb{Z}/pq\mathbb{Z}$ tel que le morphisme correspondant $\mathbb{Z}/pq\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/r\mathbb{Z})$ a pour image l'unique sous-groupe cyclique d'ordre n de $\mathrm{Aut}(\mathbb{Z}/r\mathbb{Z}) \simeq (\mathbb{Z}/r\mathbb{Z})^\times$. Ces assertions d'unicité découlent d'un simple suivi d'isomorphismes sans doute maitrisé par le lecteur s'il s'est aventuré jusque là !

Exercice 6.24. Dans la table on constate que l'on a $\mathrm{N}(n) = 1$ si, et seulement si, $n = pq$ avec p et q premiers et $p \mid q-1$. Tous ces cas sont donc expliqués par l'Exercice 6.16.

Dans tous les cas $\mathrm{N}(n) = 2, 3$ ou 5 on a $n = pqr$ avec p, q, r premiers. On a vu en effet qu'il y a exactement deux groupes non abéliens d'ordre p^3 pour p premier (Exercice 6.6) donc le cas $p = q = r$ donne bien $\mathrm{N}(n) = 2$. Les cas $n = pq^2$ avec $q \neq p$ sont aussi tous expliqués par l'Exercice 6.22. Les deux cas avec p, q, r distincts sont $30 = 2 \cdot 3 \cdot 5$ et $42 = 2 \cdot 3 \cdot 7$. Mais on a $\mathrm{N}(30) = 3$ par l'Exercice 6.16 car on a $2 \mid 3-1$, $2 \mid 5-1$ et $3 \nmid 5-1$. De plus, on a aussi $\mathrm{N}(42) = 5$ car on a $2 \mid 3-1$, $2 \mid 5-1$ et $3 \mid 7-1$

Exercice 6.25. (i) Pour $g \in G$ et $x \in X$ fixés, on a par définitions

$$g\,\widehat{x} \;=\; \widehat{gx}\,h'_{g,x} \;=\; \widetilde{gx}\,h_{gx}\,h'_{g,x} = g\,\widetilde{x}\,h_{g,x}^{-1}\,h_{gx}\,h'_{g,x} \;=\; g\,\widehat{x}\,h_x^{-1}\,h_{g,x}^{-1}\,h_{gx}\,h'_{g,x}.$$

(d'ordre $q^2 - 1$). L'idée est qu'à isomorphisme près, il n'y a qu'un corps fini de cardinal q^2, disons $\mathbb{F}_{q^2}$, et qu'une structure de $\mathbb{F}_{q^2}$-espace vectoriel sur le groupe abélien $(\mathbb{Z}/q\mathbb{Z})^2$.

On en déduit $1 = h_x^{-1}\, h_{g,x}^{-1}\, h_{gx}\, h'_{g,x}$, qui est la formule de l'énoncé. Pour le (ii) fixons $g \in G$. Dans le groupe abélien H_{ab} on a par le (i)

$$\prod_{x\in X} h_{gx} \equiv (\prod_{x\in X} h'_{g,x})\,(\prod_{x\in X} h_x)\,(\prod_{x\in X} h_{gx})^{-1} \equiv \prod_{x\in X} h'_{g,x},$$

car $x \mapsto gx$ étant une bijection de X on a $\prod_{x\in X} h_{gx} \equiv \prod_{x\in X} h_x$. Ainsi, $\mathrm{Ver}(g)$ ne dépend pas du choix de $x \mapsto \widetilde{x}$. Pour le (iii) on a

$$gg'\,\widehat{x} \;=\; \widehat{gg'x}\, h_{gg',x} \;\text{ et }\; gg'\,\widehat{x} \;=\; g\,\widehat{g'x}\, h_{g',x} \;=\; \widehat{gg'x}\, h_{g,g'x},$$

puis la relation de l'énoncé. Pour le (iv) fixons $g, g' \in G$. Comme H_{ab} est abélien on a

$$\mathrm{Ver}(gg') = \prod_{x\in X} h_{gg',x} = (\prod_{x\in X} h_{g,g'x})\mathrm{Ver}(g')$$

par le (iii). On a aussi $\prod_{x\in X} h_{g,g'x} = \prod_{x\in X} h_{g,x} = \mathrm{Ver}(g)$ par la bijection $X \to X, x \mapsto g'x$.

Exercice 6.26. (i) Par définition, Ω_i est une orbite de $\langle g\rangle$ et contient l'élément g_iH. Pour ne pas avoir à distinguer les cas où le groupe monogène $\langle g\rangle$ est cyclique ou infini, il sera plus commode de faire agir le groupe $\mathbb{Z}$ sur $X = G/H$ par $(n, x) \mapsto g^n x$. Ses orbites sont bien sur toujours les Ω_i. Le stabilisateur S_i de $g_iH \in \Omega_i$ dans $\mathbb{Z}$ vérifie donc $\mathbb{Z}/S \sim \Omega_i$ (formule orbite-stabilisateur). Ainsi, S_i est non nul, et donc de la forme $d_i\mathbb{Z}$ où d_i est le plus petit entier $n \geqslant 1$ avec $g^n g_i H = g_i H$, soit encore $g_i^{-1} g^n g_i \in H$, puis $d_i = |\mathbb{Z}/S| = |\Omega_i| = n_i$. De plus, les n_i éléments de Ω_i sont les $g^n g_i H$ avec $1 \leqslant n \leqslant n_i$. On choisit enfin pour représentants de X les éléments $x_{n,i} := g^n g_i$ avec $1 \leqslant n \leqslant n_i$. On peut calculer $\mathrm{Ver}(g)$ à l'aide de ce système de représentants par l'Exercice 6.25 (ii). On a $gx_{n,i} = x_{n+1,i}$ pour $n < n_i$, *autrement dit le* $h_{g,x_{n,i}}$ *vaut* 1, et

$$gx_{n_i,g} \;=\; g^{n_i+1} g_i \;=\; g g_i g_i^{-1} g^{n_i} g_i \;=\; x_{1,i}\, g_i^{-1} g^{n_i} g_i$$

et donc $h_{g,x_{n_i,i}} = g_i^{-1} g^n g_i \in H$. On a donc bien $\mathrm{Ver}(g) \equiv \prod_i g_i^{-1} g^{n_i} g_i$. Pour le (ii), on a $g_i^{-1} g^{n_i} g_i \equiv g^{n_i}$ dans G_{ab}, et donc

$$\mathrm{Res}(\mathrm{Ver}(g)) \equiv \prod_i g^{n_i} = g^{\sum_i \Omega_i} = g^{|G/H|}.$$

Dans le cas G abélien on a $G = G_{\mathrm{ab}}$ et $H = H_{\mathrm{ab}}$ et on conclut par le (ii).

Exercice 6.27. (i) D'après le cours, on a $\mathrm{D}(\mathrm{S}_n) = \mathrm{A}_n$, et donc $(\mathrm{S}_n)_{\mathrm{ab}} \simeq \mathbb{Z}/2\mathbb{Z}$. On peut aussi raisonner directement de la manière suivante. On sait que S_n est engendré par les transpositions. Ainsi, son quotient $(\mathrm{S}_n)_{\mathrm{ab}}$ a la même propriété. Mais comme deux transpositions sont conjuguées dans S_n, elles ont même image dans $(\mathrm{S}_n)_{\mathrm{ab}}$. On en déduit que $(\mathrm{S}_n)_{\mathrm{ab}}$ est engendré par la classe de $(1\,2)$, et donc qu'il est donc soit trivial, soit $\simeq \mathbb{Z}/2\mathbb{Z}$. Il n'est pas trivial car la signature se factorise en un morphisme surjectif $(\mathrm{S}_n)_{\mathrm{ab}} \to \{\pm 1\}$.

(ii) Le morphisme $\mathrm{Res} : (\mathrm{S}_n)_{\mathrm{ab}} \to (\mathrm{S}_{n+1})_{\mathrm{ab}}$ envoie évidemment la classe de $(1\,2)$ sur celle de $(1\,2)$. D'après le (i), c'est donc un isomorphisme $\mathbb{Z}/2\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z}$.

(iii) Comme $\mathrm{Res} : (\mathrm{S}_n)_{\mathrm{ab}} \to (\mathrm{S}_{n+1})_{\mathrm{ab}}$ est un isomorphisme, il suffit de voir que $\mathrm{Res} \circ \mathrm{Ver} : (\mathrm{S}_{n+1})_{\mathrm{ab}} \to (\mathrm{S}_{n+1})_{\mathrm{ab}}$ est un isomorphisme pour n pair, nul pour n impair. Mais par l'Exercice 6.26 (ii), c'est l'endomorphisme $g \mapsto g^{n+1}$ d'un groupe d'ordre 2. Cela conclut.

Exercice 6.28. (i) Les éléments g^n et $h\, g^n\, h^{-1}$ sont dans P et manifestement conjugués dans G. Comme P est abélien, il est inclus dans son centralisateur. Par l'Exercice 6.15 (ii), g^n et $h\, g^n\, h^{-1}$ sont donc conjugués dans $\mathrm{N}_G(P)$. Ainsi, il existe $k \in \mathrm{N}_G(P)$ vérifiant $kg^nk^{-1} = h\, g^n\, h^{-1}$. Comme $g^n \in P$ est dans le centre de $\mathrm{N}_G(P)$ par l'hypothèse de l'exercice, on a $kg^nk^{-1} = g^n$, ce qui conclut.

Le (ii) est une conséquence directe du (i) de l'Exercice 6.26. Montrons le (iii). Posons $\varphi = \mathrm{Ver}_{|P} : P \to P$. On a $\varphi(g) = g^{|G/P|}$ par le (ii). C'est un morphisme de groupes

(simplement car P abélien), qui est injectif par Lagrange car $|G/P|$ est premier à $|P|$, et donc bijectif. Soit $N = \ker \mathrm{Ver}$, c'est un sous-groupe distingué de G. Les remarques juste faites montrent que N est un complément de P. En effet, on a d'une part $N \cap P = \ker \varphi = \{1\}$. D'autre part, soit $g \in G$. On a $\mathrm{Ver}(g) = \mathrm{Ver}(p)$ pour un certain $p \in P$ par surjectivité de φ, puis $gp^{-1} \in N$ et $g \in NP$. (On aurait aussi pu dire que φ^{-1} est une section de groupes de Ver).

Exercice 6.29. (i) Soit N le normalisateur de P dans G. Considérons le morphisme $\varphi : N \to \mathrm{Aut}(P), n \mapsto (\mathrm{int}_n)_{|P}$. Il est trivial sur P car P est abélien, et il se factorise donc en un morphisme $\overline{\varphi} : N/P \to \mathrm{Aut}(P), nP \mapsto (\mathrm{int}_n)_{|P}$. On a $P \simeq \mathbb{Z}/p^m\mathbb{Z}$ pour un certain $m \geqslant 1$, et donc $\mathrm{Aut}(P) \simeq (\mathbb{Z}/p^m\mathbb{Z})^\times$ est d'ordre $\varphi(p^m) = p^{m-1}(p-1)$. Mais $|N/P|$ a tous ses facteurs premiers $> p$ par hypothèse. Il est donc premier à $|\mathrm{Aut}(P)|$, de sorte que tout morphisme $N/P \to \mathrm{Aut}(P)$ est trivial par Lagrange. Ainsi, $\overline{\varphi}$, puis φ, est trivial. Mais cela veut dire que P est dans le centre de N. Par Burnside (Exercice 6.28), P a un complément distingué dans G.

(ii) On a cette fois-ci $\mathrm{Aut}(P) \simeq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ de cardinal $p(p-1)^2(p+1)$. On conclut de la même manière sauf si $|N|/|P|$ a un diviseur premier ℓ divisant $p+1$. On aurait $\ell > p$ par hypothèse de minimalité de p, et aussi $\ell \leqslant p+1$, et donc $\ell = p+1$, $p = 2$ et $\ell = 3$.

(iii) Supposons G simple non abélien. Le sous-groupe P n'a pas de complément N distingué car sinon on aurait $N = \{1\}$ par simplicité de G, puis $G = P$, puis G abélien car le centre d'un p-groupe est non trivial (et donc $G \simeq \mathbb{Z}/p\mathbb{Z}$). Supposons que p^3 ne divise pas $|G|$. On a donc $|P| = p$ ou $|P| = p^2$. Cela montre que soit P est cyclique, soit $P \simeq (\mathbb{Z}/p\mathbb{Z})^2$. Par le (i), on est donc dans ce second cas. Par le (ii), on a $p = 2$ et $3 \mid |G|$, puis $2^2 \cdot 3 = 12$ divise $|G|$.

Exercices du chapitre 7

Exercice : 7.1. Les irréductibles de $\mathbb{Z}[i]$ sont de norme 2 (pour $1+i$), ou p premier $\equiv 1 \bmod 4$ (pour π et $\overline{\pi}$ dans l'écriture $p = \pi\overline{\pi}$), ou p^2 avec $p \equiv 3 \bmod 4$. On a donc une bonne idée de la factorisation en irréductibles d'un $z \in \mathbb{Z}[i]$ en factorisant d'abord $\mathrm{N}(z)$ dans $\mathbb{Z}$.

On a $-3+15i = 3(-1+5i)$ et $\mathrm{N}(-1+5i) = 1+25 = 26 = 2\cdot 13$. On sait que $1+i$ doit diviser $-1+5i$, et c'est bien le cas

$$\frac{-1+5i}{1+i} = \frac{1}{2}(-1+5i)(1-i) = \frac{1}{2}(4-6i) = 2-3i.$$

De plus $2-3i$ est irréductible (de norme 13), on a donc la décomposition en irréductibles $-3+15i = 2(1+i)(2-3i)$.

De même, on a $\mathrm{N}(4+7i) = 16+49 = 65 = 5\cdot 13$. On a $5 = 1^2+2^2 = (1+2i)(1-2i)$, et les deux irréductibles de $\mathbb{Z}[i]$ de norme 5 sont donc les associés de $1\pm 2i$. Un seul des deux divise $4+7i$. On a en effet

$$\frac{4+7i}{1+2i} = \frac{1}{5}(4+7i)(1-2i) = \frac{1}{5}(18-i), \text{ et}$$

$$\frac{4+7i}{1-2i} = \frac{1}{5}(4+7i)(1+2i) = \frac{1}{5}(-10+15i) = -2+3i.$$

On a donc la décomposition en irréductibles $4+7i = (1-2i)(-2+3i)$ dans $\mathbb{Z}[i]$. On aurait pu éviter tout calcul en observant que l'on a $4+7i \equiv -1+2i \bmod 5\mathbb{Z}[i]$, et donc c'est $1-2i$ qui divise $4+7i$ (car il divise 5).

Exercice 7.2. On va montrer que la seule solution est $(x,y) = (1,0)$. Soit $(x,y) \in \mathbb{Z}^2$ avec $y^2 = x^3-1$. On a dans $\mathbb{Z}[i]$ la relation $x^3 = y^2+1 = (y-i)(y+i)$. Vérifions que $y-i$ et $y+i$ sont premiers entre eux dans $\mathbb{Z}[i]$.

Sinon, il existe un irréductible π de $\mathbb{Z}[i]$ divisant $y+i$ et $y-i$. On a alors $\pi \mid (y+i)-(y-i) = 2i$, donc π divise 2, puis $\pi \sim 1+i$ car on a $2 = -i(1+i)^2$. Mais alors π divise $y^2+1 = x^3$, et $2 = \mathrm{N}(\pi)$ divise x^6, et x est pair. C'est absurde car alors on a $y^2 \equiv -1 \bmod 4$.

Comme $\mathbb{Z}[i]$ est factoriel, on en déduit que l'on a $y+i = uz^3$ avec $z \in \mathbb{Z}[i]$ et $u \in \mathbb{Z}[i]^\times$. On a $u = (u^{-1})^3$, puis $y+i = (uz)^3$. Écrivons $uz = a+bi$ avec $a,b \in \mathbb{Z}$. On a donc

$$y+i \;=\; (a+bi)^3 \;=\; (a^3-3ab^2)+(3ba^2-b^2)i,$$

puis $1 = b(3a^2-b^2)$. Cela entraîne $b = \pm 1$, puis $3a^2 = 1+b$, $b = -1$, $a = 0$, $y = 0$ puis $x = 1$.

Exercice 7.3. Montrons le (i). Comme $\mathbb{Z}[i]$ a pour $\mathbb{Z}$-base $1, i$, le groupe abélien sous-jacent à $(2+2i)$ est engendré par $2+2i$ et $i(2+2i) = -2+2i$, ou ce qui revient au même par 4 et $2+2i$. Ces éléments sont $\mathbb{R}$-linéairement indépendants, donc $\mathbb{Z}$-libres.

Comme $1, 1+i$ est une $\mathbb{Z}$-base de $\mathbb{Z}[i]$, et comme $c+d(1+i)$ est dans $(2+2i)$ si, et seulement si, on a $c \equiv 0 \bmod 4$ et $d \equiv 0 \bmod 2$ par le (i), on en déduit que le morphisme de groupes additifs $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}[i]/(2+2i), (\overline{a},\overline{b}) \mapsto \overline{c+d(1+i)}$, clairement bien défini et surjectif, est un isomorphisme. Pour la condition demandée dans l'énoncé, on écrit $a+bi = a-b+b(1+i)$ et on a donc $b \equiv 0 \bmod 2$ et $a-b \equiv 3 \bmod 4$.

Pour le (iii), on renvoie au Complément 9 pour la structure d'anneau quotient, et on note $f : \mathbb{Z}[i] \to A$ la projection canonique (un morphisme d'anneaux). Posons $\epsilon = f(1+i)$. On a $i(2+2i) = (1+i)^3$ dans $\mathbb{Z}[i]$, et donc $\epsilon^3 = 0$ en appliquant f. On a aussi $(1+i)\mathbb{Z}[i] = 2\mathbb{Z}+(1+i)\mathbb{Z}$, et donc ϵA est l'ensemble des classes des $c+d(1+i)$ avec c pair. Il y a 4 tels éléments, tous non inversibles car $\epsilon^3 = 0$. Les 4 éléments restants sont ± 1 et $\pm 1+\epsilon \equiv \pm i$.

Montrons enfin le (iv). Soit π un irréductible de $\mathbb{Z}[i]$ non associé à $1+i$. On sait alors qu'il est premier à $1+i$, et donc par Bezout qu'il existe $u, v \in \mathbb{Z}[i]$ avec $u\pi + v(1+i) = 1$. En appliquant f on en déduit que $f(\pi)$ est inversible dans A. D'après le (iv), il existe une unique unité u de $\mathbb{Z}[i]$ tel que $f(u\pi) = f(u)f(\pi) \equiv 1 \bmod (2+2i)$ (noter que l'on a $3 \equiv -1$ dans A). Ainsi, $u\pi$ est l'unique associé de π qui est congru à 3 modulo $(2+2i)$.

Exercice 7.4. (i) Soit $n \in \mathbb{Z}$ et $(a,b) \in \mathbb{Z}^2$. On a $(a,b) \in \Sigma_n \iff n = \mathrm{N}(a+bi)$. Mais tout élément de $\mathbb{Z}[i]$ est produit d'une unité, de norme 1, et d'iréductibles, de norme 2, p premier $\equiv 1 \bmod 4$, ou p^2 avec p premier $\equiv 3 \bmod 4$. On en déduit que si σ_n est non vide alors pour tout premier $p \equiv 3 \bmod 4$ dans $\mathbb{Z}$ on a $\mathrm{v}_p(n)$ pair. Réciproquement, cette condition implique bien que n est somme de deux carrés. En effet, le produit de deux sommes de deux carrés est une somme de deux carré par la formule $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$, de plus 2, les $p \equiv 1 \bmod 4$, et les p^2 avec $p \equiv 3 \bmod 4$, sont tous sommes de deux carrés (évident pour 2 et p^2, du cours pour les $p \equiv 1 \bmod 4$).

(ii) Pour $n \geqslant 1$ donné, le nombre $|\Sigma_n|$ d'éléments de $\mathbb{Z}[i]$ de norme n est de la forme $4a_n$ avec $a_n \geqslant 0$, à cause des 4 unités de $\mathbb{Z}[i]$. En utilisant que $\mathbb{Z}[i]$ est factoriel, la multiplicativité de la norme, et que la norme de chacun de ses irréductibles est une puissance d'un nombre premier, on constate que pour m et n premiers entre eux, et $z \in \Sigma_{mn}$, il existe une décomposirion $z = z_1 z_2$, avec z_1 et z_2 uniques modulo les unités, vérifiant $z_1 \in \Sigma_m$ et $z_2 \in \Sigma_n$. En particulier, on a $a_{mn} = a_m a_n$.

Pour $m, n \geqslant 1$ premiers entre eux, tout diviseur d de mn s'écrit de manière unique sous la forme ab avec $a|m$ et $b|n$. Regardant les restes modulo 4, on constate donc $\sigma_1(mn) = \sigma_1(m)\sigma_1(n) + \sigma_3(m)\sigma_3(n)$ et $\sigma_3(mn) = \sigma_1(m)\sigma_3(n) + \sigma_3(n)\sigma_1(n)$. Autrement dit, la fonction $n \mapsto b_n = \sigma_1(n) - \sigma_3(n)$ est multiplicative.

(iii) Il suffit donc de vérifier $a_n = b_n$ pour n une puissance d'un nombre premier.

– Les éléments de $\mathbb{Z}[i]$ de norme 2^k sont les $u(1+i)^k$ avec u unité, car l'unique irréductible (modulo unités) de norme une puissance de 2 est $1+i$, de norme 2. On a donc $a_{2^k} = 1$ pour tout $k \geqslant 0$. On a aussi $\sigma_1(2^k) = 1$ et $\sigma_3(2^k) = 0$, donc $b_{2^k} = 1$.

– Pour $p \equiv 1 \bmod 4$, disons $p = \pi\overline{\pi}$, les éléments de $\mathbb{Z}[i]$ de norme p^k sont les $u\pi^a\overline{\pi}^b$ avec u unité et $a+b = k$, car les uniques irréductibles (modulo unités) de norme une puissance de p sont π et $\overline{\pi}$, de norme p. On a donc $a_{p^k} = k+1$. On a aussi $\sigma_1(p^k) = k+1$ et $\sigma_3(p^k) = 0$, donc $b_{p^k} = k+1$.

– Pour $p \equiv 3 \bmod 4$, les éléments de $\mathbb{Z}[i]$ de norme p^k sont les $up^{k/2}$ avec u unité si k est pair, et il n'y en a pas si k est impair, car l'unique irréductible (modulo unités) de norme une puissance de p est p, de norme p^2. On a donc $a_{p^k} = 1$ ou 0 selon que k est pair ou impair. Pour k pair, on a $\sigma_1(p^k) = 1 + k/2$ et $\sigma_3(p^k) = k/2$. Pour k impair, on a $\sigma_1(p^k) = \sigma_3(p^k) = (1+k)/2$. On a toujours $a_{p^k} = b_{p^k}$.

Exercice 7.5. (i) On a vu en cours que $\mathbb{Z}[\sqrt{-3}]$ est non factoriel, donc non principal, en examinant l'identité $2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})$. De même, $\mathbb{Z}[\sqrt{-4}] = \mathbb{Z} + 2\mathbb{Z}i$ est non factoriel à cause de l'identité $2 \cdot 2 = -(2i)(2i)$. En effet, $\mathbb{Z}[\sqrt{-4}]$ n'a pas d'élément de norme ± 2, puisque $x^2 + 4y^2 = \pm 2$ n'a aucune solution $x, y \in \mathbb{Z}$. Cela montre que ± 2 et $\pm 2i$ sont irréductibles. Ils sont non associés (!) car les inversibles de $\mathbb{Z}[2i]$ sont ± 1 (bien noter que $\pm i$ n'est pas dans $\mathbb{Z}[2i]$!).

(ii) L'équation $x^2 - dy^2 \leqslant 4$ avec $x, y \in \mathbb{Z}$ implique bien $y = 0$ et $x = 1$ ou 2.

(iii) On a clairement $\mathbb{Z}[\sqrt{d}] = \mathbb{Z} + \mathbb{Z}\alpha$. Ainsi, l'idéal $(2, \alpha) = 2(\mathbb{Z} + \alpha\mathbb{Z}) + \alpha(\mathbb{Z} + \alpha\mathbb{Z})$ est engendré comme groupe abélien par $2, \alpha, 2\alpha$ et α^2. Mais les éléments 2α et α^2 sont dans $2\mathbb{Z} + \alpha\mathbb{Z}$ (si d est pair on a $\alpha^2 = d$, et si d est impair on a $\alpha^2 = d - 1 + 2(1+\sqrt{d})$). On a donc bien $(2, \alpha) = 2\mathbb{Z} + \alpha\mathbb{Z}$.

(vi) On déduit du (iii) que l'on a $(2,\alpha) \neq \mathbb{Z}[\sqrt{d}]$, car 1 n'est pas de la forme $2n+\alpha m$ avec $m,n \in \mathbb{Z}$ (on aurait $m=0$). Ainsi, si on suppose $(2,\alpha)=(z)$ avec $z \in \mathbb{Z}[\sqrt{d}]$ on a $\mathrm{N}(z)>1$. Mais on a aussi $z|2$ car $2 \in (z)$, et donc $\mathrm{N}(z) \,|\, \mathrm{N}(2)=4$ dans $\mathbb{Z}$. D'après le (ii), cela implique $z=\pm 2$. Mais on a aussi $z|\,\alpha$ car $\alpha \in (z)$. Mais il est clair que 2 ne divise pas α (les multiples de 2 dans $\mathbb{Z}+\mathbb{Z}\alpha$ ont leurs coefficients en 1 et α qui sont des entiers pairs).

Exercice 7.6. (i) Soit $z \in I$ non nul. On constate $\mathrm{N}(z)=\overline{z}z \in I$. Mais $\mathrm{N}(z)$ est un entier non nul.

(ii) Comme on a $\mathbb{Z}[\sqrt{d}] \simeq \mathbb{Z}^2$, on a aussi $\mathbb{Z}[\sqrt{d}]/n\mathbb{Z}[\sqrt{d}] \simeq (\mathbb{Z}/n\mathbb{Z})^2$. En particulier, c'est un groupe fini, et il n'a donc qu'un nombre fini de sous-groupes. On conclut car les sous-groupes de $\mathbb{Z}[\sqrt{d}]/n\mathbb{Z}[\sqrt{d}]$ sont en bijection naturelle avec ceux de $\mathbb{Z}[\sqrt{d}]$ contenant $n\mathbb{Z}[\sqrt{d}]$ (dont les idéaux contenant n font partie).

(iii) Soit I un idéal non nul de A. On a vu que I contient $(n)=nA$ pour un certain entier $n \geqslant 1$. Observons que les sous-groupes de $\mathbb{Z}^2$ contenant $n\mathbb{Z}^2$ sont clairement de type fini, engendrés par $(n,0)$, $(0,n)$ et par un sous-ensemble de l'ensemble fini des (a,b) avec $0 \leqslant a,b<n$. On en déduit que tout idéal de A (isomorphe à $\mathbb{Z}^2$ comme groupe abélien) est finiment engendré comme groupe abélien, et donc *a fortiori* de type fini comme idéal. On a $nA \subset I$ et nA d'indice fini dans A, donc I est d'indice fini dans A (en clair, on a une surjection $A/nA \to A/I$).

(iv) On peut supposer $\mathrm{N}(z)$ non nul. On a $z \in zA$ donc $\mathrm{N}(z) \in zA$ et on a vu qu'il n'y a qu'un nombre fini d'ideaux de A contenant $\mathrm{N}(z)$.

Exercice 7.7. (i) C'est l'argument classique dû à Dirichlet. On regarde les $N+1$ éléments $k\alpha-[k\alpha]$ de $[0,1[$, avec $0 \leqslant k \leqslant N$. Consirérant la partition de $[0,1[$ en les N parties $[q/N,(q+1)/N[$ avec $0 \leqslant q<N$, on en déduit qu'il existe $0 \leqslant i<j \leqslant N$ avec $|(j\alpha-[j\alpha])-(i\alpha-[i\alpha])|<1/N$. Posons $q=j-i$ et $p=[j\alpha]-[i\alpha]$, on a $1 \leqslant q<N$ et $|p-q\alpha|<1/N$.

(ii) On choisit $p_n \in \mathbb{Z}$ et $1 \leqslant q_n$ avec $|p_n-q_n\sqrt{d}|<1/n$ et $1 \leqslant q_n \leqslant n$. On a donc $|p_n|<1/n+|q_n|\sqrt{d} \leqslant 1/n+n\sqrt{d}$ puis $|\mathrm{N}(p_n-q_n\sqrt{d})|<1/n(1/n+n\sqrt{d})<1+\sqrt{d}$. On conclut en posant $x_n=p_n-q_n\sqrt{d}$ (nécessairement non nul car $q_n \neq 0$).

(iii) Comme l'ensemble des $\mathrm{N}(x_n)$ est fini (des entiers bornés), quitte à extraire (x_n) on peut supposer qu'il existe $k \in \mathbb{Z}$ avec $\mathrm{N}(x_n)=k$ pour tout n et $x_n \to 0$. De même, comme on a $\mathbb{Z}[\sqrt{d}]/k\mathbb{Z}[\sqrt{d}]=\mathbb{Z}/k\mathbb{Z}\overline{1} \oplus \mathbb{Z}/k\mathbb{Z}\overline{\sqrt{d}}$, un ensemble fini, on peut supposer que $x_n \bmod k\mathbb{Z}[\sqrt{d}]$ est constante. Comme $k\mathbb{Z}[\sqrt{d}]$ est un idéal de $\mathbb{Z}[\sqrt{d}]$, on peut multiplier les congruences, et on en déduit que la classe $x_m\overline{x_n} \bmod k\mathbb{Z}[\sqrt{d}]$ ne dépend pas de $n,m \geqslant 1$. Pour $m=n$ on a $x_n\overline{x_n}=\mathrm{N}(x_n)=k \equiv 0 \bmod k\mathbb{Z}[\sqrt{d}]$. On a donc $x_m\overline{x_n} \in k\mathbb{Z}[\sqrt{d}]$ pour tout $m,n \geqslant 1$.

(iv) Posons $x_m\overline{x_n}=ky_{m,n}$ pour un certain $y_{m,n} \in \mathbb{Z}[\sqrt{d}]$. En prenant la norme on a $k^2=\mathrm{N}(x_m)\mathrm{N}(x_n)=k^2\mathrm{N}(y_{m,n})$, puis $y_{m,n} \in \mathbb{Z}[\sqrt{d}]^\times$ pour tout m,n. On a $y_{m,n} \to 0$ et $y_{m,n} \neq 0$, on a donc construit une infinité d'unités.

Exercice 7.8. (i) Soit $M=\begin{bmatrix} a & c \\ b & d \end{bmatrix}$ la matrice dont les colonnes sont les deux vecteurs donnés. Son déterminant est $ad-bc$, non nul par hypothèse. Soit $G \subset \mathbb{Z}^2$ le sous-groupe engendré par (a,b) et (c,d). On veut montrer qu'il est d'indice fini $|\det M|$. Pour $P \in \mathrm{GL}_2(\mathbb{Z})=\mathrm{Aut}(\mathbb{Z}^2)$, $P(G)$ a même indice que G dans $\mathbb{Z}^2$. Il est engendré par les deux colonnes de PM, qui est de déterminant $\det P \det M=\pm\det M$. On peut donc à loisir multiplier à gauche M par des éléments de $\mathrm{GL}_2(\mathbb{Z})$. En utilisant des transvections standards, on peut remplacer (a,b) par (a,b') (resp. (a',b)) où b' est le reste de la division

euclidienne de b par a (resp. de a par b). Après un nombre fini d'itérations, on se ramène donc au cas $a = 0$ ou $b = 0$. Par symétrie, on peut donc supposer $b = 0$, et on a $ad \neq 0$. Mais le sous-groupe H de $\mathbb{Z}^2$ engendré par $(1, 0)$ et (c, d) est d'indice $|d|$ dans $\mathbb{Z}^2$, car c'est le noyau de $(x, y) \mapsto y \bmod d$, et G est d'indice $|a|$ dans H, car c'est le noyau de $x(1, 0) + y(c, d) \mapsto x \bmod a$. Ainsi, G est bien d'indice $|ad|$ dans $\mathbb{Z}^2$.

(ii) Le groupe abélien A est libre de rang 2 engendré par 1 et $\sqrt{d}$. Écrivons $z = a+b\sqrt{d}$ avec $a, b \in \mathbb{Z}$. Le sous-groupe Az de A est engendré par $z = a + b\sqrt{d}$ et $z\sqrt{d} = bd + a\sqrt{d}$. Mais le sous-groupe de $\mathbb{Z}^2$ engendré par (a, b) et (bd, a) est d'indice fini égal à $a^2 - db^2 \neq 0$ par le (i). On conclut car $\mathrm{N}(z) = a^2 - db^2$.

Exercice 7.9. (i) Si on a $I = xA$ avec $x \neq 0$ alors on a clairement $I \sim A$. Réciproquement, si on a $aI = bA$ avec a, b non nuls, on a $b \in aI \subset aA$ et donc $b = ac$ pour un certain $c \in A$, puis $aI = acA$, et comme A est intègre, $I = cA$ est principal.

(ii) On a toujours $[A] \in \mathrm{Cl}(A)$, et par le (i) A est principal si, et seulement si, on a $\mathrm{Cl}(A) = \{[A]\}$.

Exercice 7.10. (i) Si la largueur du rectangle est 1, les disques roses sont de rayon 1 et centrés aux sommets du rectangle, les disques oranges sont de rayon 1/2. La longueur du rectangle est donc $\sqrt{3}/2 + 1 + \sqrt{3}/2 = 1 + \sqrt{3}$. Cela conclut.

(ii) On a $3 < 2\sqrt{3}$ et donc $\sqrt{|d|} \leqslant \sqrt{7} < 1 + \sqrt{3}$. On pose $z = a/b$. Par le (i), il existe $q \in A$ avec soit $\mathrm{N}(a/b - q) < 1$, soit $\mathrm{N}(a/b - q/2) < 1/4$. On a $\mathrm{N}(r) < \mathrm{N}(b)$ avec $r = a - qb$ dans le premier cas, et $r = 2a - qb$ dans le second.

(iii) On choisit $z \in I$ non nul et avec $\mathrm{N}(z)$ minimal. On a $Az \subset I$ car I est un idéal. Soit $a \in I$ non nul. Par le (ii), on peut écrire soit $a = qz + r$, soit $2a = qz + r$, avec $\mathrm{N}(r) < \mathrm{N}(z)$. On a $r \in I$ et donc $r = 0$ dans les deux cas, par choix de z. On a donc $z \mid 2a$ dans les deux cas, puis $2I \subset Az$. On a montré $zA \subset I \subset \frac{1}{2}zA$. En multipliant ces inclusions par l'élément $\frac{2}{z} \in \mathbb{Q}[\sqrt{d}]^\times$, elles s'écrivent aussi $2A \subset I' \subset A$ avec $I' = \frac{2}{z}I$, qui est donc un idéal non nul de A. Il vérifie $zI' = 2I$: il est équivalent à I.

(iv) Soit I un idéal de A contenant $2A$. On a $A = \mathbb{Z} \oplus \mathbb{Z}\alpha$. Le groupe quotient $A/2A \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ a donc pour représentants $0, 1, \alpha, \alpha + 1$. Si I contient 1 on a $I = A$. Si I contient α on a $J \subset I$, puis $I = J$ ou $I = A$ car J est d'indice 2. Enfin, si I contient $\alpha + 1$, alors I contient aussi $\alpha(\alpha + 1) = \alpha^2 + \alpha$. Si d est pair on a $\alpha^2 = d \in 2\mathbb{Z} \subset I$, donc I contient α, puis $1 = 1 + \alpha - \alpha$, et donc $I = A$. De même, si d est impair on a $\alpha^2 = 2\alpha + d - 1$ et donc $\alpha(\alpha + 1) + \alpha = 3\alpha + d - 1 \in \alpha + 2A$, et donc $\alpha \in I$ puis encore $1 \in I$ et donc $I = A$.

(v) D'après (iii) et (iv), tout idéal non nul de A est équivalent à $2A$, J ou A. Comme A et $2A$ sont principaux, on a $\mathrm{Cl}(A) = \{[A], [J]\}$. On en déduit que l'idéal J est principal si, et seulement si, A est principal, par l'Exercice 7.9. On a vu que J n'est pas principal pour $d < -4$ dans l'Exercice 7.5. Pour $d = -3$, on a vu que A est non factoriel en cours, donc non principal, donc J est non principal aussi dans ce cas.

Exercice 7.11. (i) On a $j^2 + j + 1 = 0$, donc $j^2 = -j - 1$, ce qui implique que $\mathbb{Z}[j]$ est un sous-anneau de $\mathbb{C}$. On observera que pour $z \in \mathbb{Z}[j]$, on a $\overline{z} \in \mathbb{Z}[j]$ (conjugaison complexe) car $\overline{j} = j^2 = -j - 1$.

(ii) On a $j^3 = 1$ donc les 6 éléments donnés sont dans $\mathbb{Z}[j]^\times$. Réciproquement, si on a $\alpha\beta = 1$ avec α, β dans $\mathbb{Z}[j]$, alors on a $|\alpha|^2|\beta|^2 = 1$ avec $|\alpha|^2, |\beta|^2 \in \mathbb{Z}$ par la formule ci-dessus, puis donc $|\alpha|^2 = 1$. Posons $\alpha = a+bj$ avec $a, b \in \mathbb{Z}$. Cela s'écrit aussi $a^2-ab+b^2 = 1$, et en multipliant par 4, $(2a - b)^2 + 3b^2 = 4$. Les seules solutions ce cette équation sont $(a, b) = (\pm 1, 0)$, $(a, b) = (0, \pm 1)$ et $(a, b) = \pm(1, 1)$, qui sont les 6 solutions déjà trouvées.

(iii) En raisonnant comme dans le cours, il suffit de montrer que pour tout $z \in \mathbb{C}$ il existe $q \in \mathbb{Z}[j]$ tel que $|z-q|^2 < 1$. Posons $z = a + bj$, $u, v \in \mathbb{Z}$ et $q = u + vj$. On a

$$4|z-q|^2 = (2(a-u) - (b-v))^2 + 3(b-v)^2.$$

On peut choisir $v \in \mathbb{Z}$ tel que $|b-v| \leqslant 1/2$, puis $u \in \mathbb{Z}$ tel que $|2a - (b-v) - 2u| \leqslant 1$. On a alors bien $4|z-q|^2 \leqslant 1 + 3/4 < 4$.

(iv) On a montré que $\mathbb{Z}[j]$ est euclidien, donc principal et factoriel. Soit $p \equiv 1 \bmod 3$ un nombre premier. On sait que $(\mathbb{Z}/p\mathbb{Z})^\times$ a un élément d'ordre 3 (Gauss ou Cauchy), de sorte que le polynôme $X^3 - 1 = (X-1)(X^2+X+1)$ a une racine $\neq 1$ dans $\mathbb{Z}/p\mathbb{Z}$. Ainsi, il existe un entier $n \in \mathbb{Z}$ tel que $n^2+n+1 \equiv 0 \bmod p$. Mézalor p divise $n^2+n+1 = (n-j)(n-j^2)$ dans $\mathbb{Z}[j]$. Si p était irréductible, donc premier, il diviserait $n+j$ ou $n+j^2$: absurde car le coefficient en j de $n+j$ et $n+j^2$ est ± 1, qui n'est pas multiple de p dans $\mathbb{Z}$. Ainsi, p est réductible, et s'écrit donc $\alpha\beta$ avec $|\alpha|^2, |\beta|^2 > 1$ par le (ii). De $p^2 = |\alpha|^2|\beta|^2$, et $|\alpha|^2, |\beta|^2 \in \mathbb{Z}$, on déduit $p = |\alpha|^2$. On a donc $p = \alpha\overline{\alpha}$ pour un certain $\alpha \in \mathbb{Z}[j]$. Écrivons $\alpha = a + bj$ avec $a, b \in \mathbb{Z}$, et donc $p = a^2 - ab + b^2$. Les associés de α sont

$$a+bj, -a-bj, -b+(a-b)j, b-(a-b)j, -(a-b)-aj \text{ et } (a-b)+aj.$$

On a aussi $\overline{\alpha} = (a-b) - jb$. Il n'est pas dans la liste ci-dessus ! En effet, sinon on aurait soit $b = -b = 0$, soit $b = 2a$, soit $a = 2b$, soit $b = \pm a$, et tous ces cas sont exclus par $a^2 - ab + b^2 = p$ (premier impair).

(v) Comme dans le cours, $\mathbb{Z}[j]$ étant factoriel il y a exactement $6 + 6 = 12$ éléments de $\mathbb{Z}[j]$ de norme p, à savoir les $u\alpha$ et les $u\overline{\alpha}$ avec $u \in \mathbb{Z}[j]^\times$.

(vi) Si on a $p = a^2 - ab + b^2$ avec $(a, b) \in \mathbb{Z}$. On a vu que les 12 écritures possibles sont obtenues en remplaçant (a, b) par les 6 couples suivants et leurs opposés :

$$(a,b),\ (-b, a-b), (a-b, a), (a-b, -b), (b, a) \text{ et } (-a, b-a).$$

Les couples (c, d) avec $p = c^2 + 3d^2$ correspondent bijectivement aux (a, b) avec $p = a^2 - ab + b^2$ et b pair, via $(c, d) = (a - b/2, b/2)$, via l'identité

$$a^2 - ab + b^2 = (a - b/2)^2 + 3(b/2)^2.$$

De plus, si on a (a, b) avec $p = a^2 - ab + b^2$, alors a ou b est impair. En considérant (a, b), (b, a) et $(-b, a-b)$ on constate que l'un au moins des couples ci-dessus à sa seconde coordonnée paire. Quitte à prendre ce couple pour couple (a, b) de départ, on peut donc supposer b pair et a impair. On constate alors que parmi les 6 couples ci-dessus, seuls (a, b) et $(a-b, -b)$ ont leur seconde coordonnée paire. Ajoutant leurs opposés, les 4 uniques couples (c, d) avec $p = c^2 + 3d^2$ sont donc $\pm(a - b/2, b/2)$ et $\pm(a - b/2, -b/2)$. Autrement dit, si (c, d) est l'une de ces 4 écritures, les autres sont $(\pm c, \pm d)$: c'est l'assertion d'unicité cherchée.

Exercice 7.12. (i) On démontre comme pour $\mathbb{Z}[\sqrt{d}]$ que les unités de A_d sont ses éléments de norme ± 1. On a

$$4(x^2 + xy + \frac{1-d}{4}y^2) = (2x+y)^2 - dy^2.$$

Pour $d < -3$ et $x, y \in \mathbb{Z}$, le terme de droite est égal à 4 si, et seulement si, $y = 0$ et $x = \pm 1$. Cela prouve exactement $\mathrm{A}_d^\times = \{\pm 1\}$ dans ce cas. Pour $d = -3$, on a aussi $\pm(1, 1)$ et $\pm(0, 1)$ comme on l'a déjà vu dans l'Exercice 7.11, ce qui donne $\mathrm{A}_{-3} = \mu_6$.

(ii) Les démonstrations sont les même verbatim. Vérifions par exemple $|A/zA| = |\mathrm{N}(z)|$ pour $A = \mathrm{A}_d$ et $z \in \mathrm{A}_d$ non nul. Le groupe abélien A est libre de rang 2 engendré par 1 et τ_d. Écrivons $z = a + b\tau_d$ avec $a, b \in \mathbb{Z}$. Le sous-groupe Az de A est engendré par $z = a + b\tau_d$ et $z\tau_d = a\tau_d + b(\tau_d + \frac{d-1}{4}) = b\frac{d-1}{4} + (a+b)\tau_d$. Mais le sous-groupe de $\mathbb{Z}^2$ engendré par (a, b) et $(b\frac{d-1}{4}, a+b)$ est d'indice fini égal à $|a(a+b) + b^2\frac{1-d}{4}|$ par le (i) de l'Exercice 7.8, car on a $\mathrm{N}(z) = a^2 + ab + \frac{1-d}{4}b^2 \neq 0$.

Exercice 7.13. C'est la même démonstration que pour la question (iii) de l'Exercice 7.11. On utilise au final que l'on a $1 + \frac{|d|}{4} < 4$ pour $|d| = 3, 7, 11$.

Exercice 7.14. (i) La méthode est la même que dans l'Exercice 7.10. Pour changer, on procède algébriquement plutôt que géométriquement. Soit $z \in \mathbb{C}$. Montrons qu' il existe $u, v \in \mathbb{Z}$ tel que l'on a soit $|z - (u + \alpha v)|^2 < 1$, soit $|z - (u + \alpha v)/2|^2 < 1/4$. Écrivons $z = x + y\,\alpha$ avec $x, y \in \mathbb{R}$. On a

$$|z - (u + \alpha v)|^2 = \frac{1}{4}\left(2(x - u) + (y - v))^2 + 19(y - v)^2\right).$$

Posons $r = \sqrt{\frac{3}{19}}$ (on a $r \simeq 0.397$). Supposons d'abord qu'il existe $v \in \mathbb{Z}$ tel que $|y - v| < r$. On peut bien sûr choisir $u \in \mathbb{Z}$ avec $|2x + (y - v) - 2u| \leqslant 1$, et on a alors

$$|z - (u + \alpha v)|^2 \leqslant \frac{1}{4}(1 + 19r^2) < 1.$$

(Cela explique bien sûr le choix de r). Sinon, la distance de y à $1/2 + \mathbb{Z}$ est $\leqslant s$ avec $s := 1/2 - r \simeq 0.103$. On peut donc trouver $v \in \mathbb{Z}$ avec $|y - v/2| \leqslant s$ et $u \in \mathbb{Z}$ tel que $|2(x - u/2) + (y - v/2)| \leqslant 1/2$, de sorte que l'on a

$$|z - (u + \alpha v)/2|^2 = \frac{1}{4}\left(2(x - u/2) + (y - v/2))^2 + 19(y - v/2)^2\right) \leqslant \frac{1}{4}\left(\frac{1}{4} + 19s^2\right).$$

On conclut car on a $1/4 + 19s^2 \simeq 0.26 < 1$.

(ii) Posons $\alpha = \tau_{-19}$ et $A = \mathrm{A}_{-19} = \mathbb{Z} \oplus \mathbb{Z}\alpha$. Alors $A/2A$ a pour représentants $0, 1, \alpha$ et $1 + \alpha$. Mais on a $\alpha^2 - \alpha + 5 = 0$, et donc $\alpha(1 + \alpha) = -5 \in 1 + 2A$. Ainsi, si I est un idéal de A contenant $2A$, on a soit $I = 2A$, soit $1 \in I$, et donc $I = A$.

(iii) Le même argument que dans l'Exercice 7.10 montre, à partir du (i), que tout idéal non nul de A est équivalent à un idéal contenant $2A$, *i.e.* à A ou à $2A$. Donc tout idéal est équivalent à un idéal principal, *i.e.* est principal.

Exercice 7.15. (i) Par hypothèse, on a $\{0\} \cup A^\times \subsetneq A$. On peut donc trouver $z \in A$ non nul, et non unité, tel que l'entier $\varphi(z)$ est minimal. Soit $a \in A$. Comme A est euclidien pour φ, on peut écrire $a = qx + r$ avec soit $r = 0$, soit $r \neq 0$ et $\varphi(r) < \varphi(x)$. Dans le second cas, on en déduit que r est une unité. On a montré que $\{0\} \cup A^\times$ contient des représentants de A/xA.

(ii) Pour $d < 0$ et $x, y \in \mathbb{Z}$, on a $4\mathrm{N}(x + y\tau_d) = (2x - y)^2 + |d|y^2$. On cherche à savoir quand cette quantité peut être égale à $2.4 = 8$ ou $3.4 = 12$. Pour $|d| > 11$ et $d \equiv 1 \bmod 4$, et donc $|d| \geqslant 15$, cela force $y = 0$, et il n'y a pas de solution car ni 8 ni 12 n'est un carré.

(iii) Pour $d < -3$ on a aussi $|\mathrm{A}_d^\times| = 2$. On en déduit que si x est comme au (i), on a A/xA de cardinal $1, 2$ ou 3. Mais $A = xA$ est impossible car x n'est pas une unité, on a donc $|A/xA| = 2$ ou 3. Mais d'après l'exercice 7.12 (ii) on a $|A/xA| = |\mathrm{N}(x)|$, ce qui contredit le (ii).

Exercice 7.25. (i) On a $\varphi(n) \leqslant |n|$ pour tout $n \in \mathbb{Z}$. Pour $m, n \in \mathbb{Z}$ avec $n \neq 0$, la division euclidienne de m par n sécrit $m = qn + r$ avec $0 \leqslant r < |n|$. Cela conclut si n est pair. Si n est impair, disons $|n| = 2k + 1$, on constate que quitte à remplacer q par $q \pm 1$ et r par $r - |n|$ si nécessaire, on peut supposer $|r| \leqslant k$, et donc $\varphi(r) \leqslant |r| \leqslant k = \varphi(n)$.

(ii) On pose $\varphi(2) = x$ avec $x \geqslant 2$. Pour $m, n \in \mathbb{Z}$ avec $n \neq 0$, la division euclidienne de m par n sécrit $m = qn + r$ avec $0 \leqslant r < |n|$. Si on a $n = 2$, alors $0 \leqslant r \leqslant 1$ et donc $\varphi(r) = r < 2 \leqslant \varphi(x)$. On suppose donc $n \neq 2$, en particulier $\varphi(n) = |n|$. Si on a $r \neq 2$, ou $r = 2$ et $|n| > x$, on a bien $\varphi(r) < \varphi(n)$. Dans le cas restant on a $r = 2$ et $3 \leqslant |n| \leqslant x$. Mais alors l'égalité $m = (q \pm 1)n + 2 - |n|$, et l'inégalité $2 - x \leqslant 2 - |n| \leqslant -1$ montre $\varphi(2 - |n|) = |n| - 2 < \varphi(n) = |n|$.

Exercice 7.27. (i) On constate que l'on a $\mathrm{E}_n(\mathbb{Z}) = \{k \in \mathbb{Z} \mid 0 < |k| < 2^n\}$. En effet, c'est clair pour $n = 0$. De plus, pour $m \in \mathbb{Z}$ on constate que $\mathbb{Z}/m\mathbb{Z}$ est recouvert par les classes des entiers $\pm k$ avec $|k| < 2^n$ si, et seulement si, on a $0 < |m| < 2^{n+1}$, et on conclut par récurrence. Enfin, pour $m \in \mathbb{Z}$ non nul on a montré que $\upsilon(m)$ est le plus petit entier n tel que $|m| < 2^{n+1}$. Autrement dit, $\upsilon(m)$ vaut le nombre de chiffres de m dans son écriture en base 2, moins 1.

(ii) Par division euclidienne, on constate par récurrence sur $n > 0$ que $\mathrm{E}_n(k[X])$ est l'ensemble des polynômes non nuls et de degré $\leqslant n$ dans $k[X]$. On a donc $\nu = \deg$.

(iii) On a $x \in \mathrm{E}_1(A) \iff Ax = A \iff x \sim 1 \iff x \in A^\times$. On a clairement $\mathrm{E}_0(A) \subset \mathrm{E}_1(A)$ et $\mathrm{E}_1(A) = A^\times \subset \mathrm{E}_2(A)$. Mais pour $X, Y \subset A$ avec $X \subset Y$, et $a \in A$, alors $aA + X = A$ implique évidemment $aA + Y = A$. On en déduit $\mathrm{E}_n(A) \subset \mathrm{E}_{n+1}(A)$ pour tout $n \geqslant 0$ par récurrence sur n.

(iv) Soit $a \in A$ non nul avec $\varphi(a) \leqslant n$. Il suffit de montrer que l'on a $\upsilon(a) \leqslant n$, *i.e.* $a \in \mathrm{E}_{n+1}(A)$. On procède par récurrence sur $n \geqslant 0$. Supposons $n = 0$. Par euclidianité et $\varphi(a) = 0$, on a $1 = aq + r$ avec $r = 0$, donc $a \in A^\times = \mathrm{E}_1(A)$ par le (i). Pour n général, on constate par euclidianité que A/aA est recouvert par les classes de 0 et des $b \in A$ non nuls avec $\varphi(b) < \varphi(a) \leqslant n$. Par récurrence et le (iv), un tel b est dans $\mathrm{E}_n(A)$, ce qui montre bien que a est dans $\mathrm{E}_{n+1}(A)$.

(v) Supposons enfin $A = \mathrm{Eucl}(A) \cup \{0\}$, de sorte que υ est bien définie sur $A \smallsetminus \{0\}$. Soient $a, b \in A$ avec $b \neq 0$. Posons $n = \nu(b)$. On a $b \in \mathrm{E}_{n+1}(A)$ donc la classe de a dans A/bA est soit nulle, soit celle d'un certain $r \in \mathrm{E}_n(A)$. Autrement dit, on a $a - r \in bA$ avec soit $r = 0$, soit $\upsilon(r) < n = \upsilon(b)$.

Annexe B

Sujets d'examens et corrigés

1. Examen partiel 2021-2022

Problème 1. *On s'intéresse aux actions transitives de* S_4 *sur un ensemble à* 6 *éléments. On note* X *l'ensemble des parties à* 2 *éléments de* $\{1,2,3,4\}$*, et* Y *l'ensemble des* 4*-cycles dans* S_4*.*

(i) Montrer $|X| = |Y| = 6$*.*

(ii) Montrer que l'action naturelle de S_4 *sur* X *est transitive. Pour* $i \neq j$ *dans* $\{1,2,3,4\}$*, lister les éléments du stabilisateur de l'élément* $\{i,j\}$ *de* X*.*

(iii) Montrer que l'action par conjugaison de S_4 *sur* Y *est transitive, puis que le stabilisateur d'un* 4*-cycle* $c \in Y$ *est* $\langle c \rangle$ *(le sous-groupe engendré par* c*).*

(iv) Montrer que ces actions de S_4 *sur* X *et* Y *sont fidèles.*

(v) Montrer qu'il existe une action transitive de S_3 *sur un ensemble* Z *à* 6 *éléments, et décrire ses stabilisateurs.*

(vi) (suite) En déduire une action transitive de S_4 *sur* Z*, dont les stabilisateurs sont tous égaux au sous-groupe* K_4 *de* S_4*.*

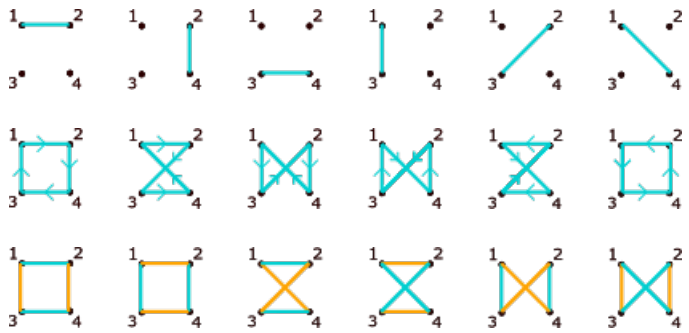
(vii) Rappeler pourquoi tout groupe d'ordre 4 *est isomorphe à* $\mathbb{Z}/4\mathbb{Z}$ *ou à* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$*.*

(viii) Déterminer le commutant dans S_4 *(ou « centralisateur ») de la transposition* $(i\,j)$*.*

(ix) Soit $H \subset \mathrm{S}_4$ *un sous-groupe d'ordre* 4*. Montrer que soit* H *est le stabilisateur d'un point de* X*, soit* H *est le stabilisateur d'un point de* Y*, soit* H *est le sous-groupe* K_4 *de* S_4*.*

(x) En déduire qu'à isomorphisme près, il existe exactement 3 *actions transitives de* S_4 *sur des ensembles à* 6 *éléments.*

(xi) Faire correspondre ces trois actions aux dessins ci-dessous.



(xii) (Bonus) Identifions S_4 *au sous-groupe de* S_5 *fixant l'élément* 5*. Est-ce que la restriction à* S_4 *de l'action exotique de* S_5 *est transitive ? Si oui, l'identifier à l'une des* 3 *actions ci-dessus.*

Les terminologies suivantes seront utilisées dans les problèmes ci-dessous. Soit H un sous-groupe d'un groupe G. On dira que H est *strict* si on a $H \neq G$. On dira que H est

maximal s'il est strict, et si les seuls sous-groupes de G contenant H sont G et H. Dans un groupe fini, tout sous-groupe strict est inclus dans un sous-groupe maximal (pourquoi ?). On rappelle enfin les notations $\mathrm{N}_G(H) = \{g \in G \mid gHg^{-1} = H\}$ (le *normalisateur de H dans G*) et $\mathrm{Z}(G) = \{h \in G \mid hg = gh,\ \forall g \in G\}$ (le *centre de G*).

Problème 2. (Non simplicité d'un groupe non abélien minimal) *Soit G un groupe fini non abélien dont tous les sous-groupes stricts sont abéliens. On se propose de montrer que G n'est pas simple.*

On suppose par l'absurde que G est simple. On note $\mathscr{M}$ l'ensemble des sous-groupes maximaux de G.

(i) Soient A et B deux sous-groupes stricts de G, montrer que $\mathrm{N}_G(A \cap B)$ contient A et B.

(ii) En déduire que pour $A, B \in \mathscr{M}$ avec $A \neq B$, on a $A \cap B = \{1\}$.

(iii) Montrer que $(g, A) \mapsto gAg^{-1}$ définit une action de G sur $\mathscr{M}$.

(iv) Montrer que l'orbite de $A \in \mathscr{M}$ est de cardinal $|G|/|A|$.

(v) Pour $A \in \mathscr{M}$, on pose $\mathscr{C}(A) = \bigcup_{g \in G} gAg^{-1}$. Montrer $|\mathscr{C}(A)| = 1 + \frac{|G|}{|A|}(|A| - 1)$.

(vi) (suite) En déduire $1 + \frac{|G|}{2} \leqslant |\mathscr{C}(A)| < |G|$.

(vii) Montrer que pour $A, B \in \mathscr{M}$, avec B non inclus dans $\mathscr{C}(A)$, on a $\mathscr{C}(A) \cap \mathscr{C}(B) = \{1\}$.

(viii) Conclure.

Problème 3. *Soit $n \geqslant 1$ un entier. On se propose de démontrer l'équivalence entre les deux propriétés suivantes :* (a) *tout groupe d'ordre n est cyclique,* (b) *n est premier à son indicatrice d'Euler $\varphi(n)$.*

(i) Montrer que l'on a $(n, \varphi(n)) = 1$ si, et seulement si, n est un produit de nombres premiers distincts $p_1, \ldots, p_r$ avec $p_i \nmid p_j - 1$ pour $i \neq j$.

(ii) On suppose $p^2 \mid n$ avec p premier. Montrer qu'il existe un groupe non cyclique d'ordre n.

(iii) Soient p et q premiers avec $p \mid q-1$. Montrer qu'il existe un morphisme non trivial $\mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$.

(iv) (suite) En déduire qu'il existe un groupe non abélien d'ordre pq.

(v) (suite) En déduire que pour tout $r \geqslant 1$, il existe un groupe non abélien d'ordre pqr.

(vi) Démontrer (a) $\Longrightarrow$ (b).

(vii) Montrer qu'un groupe abélien d'ordre $p_1 p_2 \cdots p_r$, avec les p_i premiers distincts, est cyclique.

(viii) Soit f un morphisme entre deux groupes finis de cardinaux premiers entre eux. Montrer que f est le morphisme trivial.

On va montrer (b) $\Longrightarrow$ (a) par récurrence sur n. On suppose donc $(n, \varphi(n)) = 1$, et que tout groupe d'ordre $d < n$, avec $(d, \varphi(d)) = 1$, est cyclique. Soit G un groupe fini d'ordre n.

(i) Montrer que soit G n'est pas simple, soit G est abélien (utiliser le résultat du Problème 2).

(ii) Soit H un sous-groupe distingué strict de G. En considérant un morphisme $G \to \mathrm{Aut}(H)$ approprié, montrer $H \subset \mathrm{Z}(G)$.

(iii) En déduire que $G/\mathrm{Z}(G)$ est cyclique.

(iv) Démontrer (b) $\Longrightarrow$ (a).

(v) (Application) *Montrer qu'un groupe d'ordre* 255 *est cyclique.*

(vi) (Devinette) *Quels sont les entiers n tels que tout groupe d'ordre n est abélien ?*

2. Examen partiel 2022-2023

Problème 1. *Soit $n \geqslant 3$ un entier. On se propose dans ce problème de montrer que tous les automorphismes du groupe S_n sont intérieurs, sauf dans le cas $n = 6$. Une suite de r transpositions $t_1, \ldots, t_r$ de S_n sera dite* alignée *si on a $t_i\, t_j = t_j\, t_i$ pour $|j - i| > 1$, et $t_i\, t_{i+1} \neq t_{i+1}\, t_i$ pour $1 \leqslant i < r$.*

(i) Soient t et t' deux transpositions distinctes dans S_n, de supports respectifs T et T'. Vérifier que l'on a $t\,t' \neq t'\,t$ si, et seulement si, $|T \cap T'| = 1$.

(ii) Donner un exemple d'une suite alignée de $n - 1$ transpositions engendrant S_n.

(iii) On suppose que $t_1, \ldots, t_r$ est une suite alignée de r transpositions distinctes de S_n. Montrer qu'il existe $a_1, a_2, \ldots, a_{r+1}$ distincts dans $\{1, \ldots, n\}$ avec $t_i = (a_i\ a_{i+1})$ pour tout $i = 1, \ldots, r$.

(iv) Soit f un automorphisme de S_n. On suppose qu'il existe une transposition t telle que $f(t)$ est une transposition. Montrer que pour toute transposition s, alors $f(s)$ est une transposition.

(v) (suite) Montrer que f est un automorphisme intérieur.

On rappelle que le centralisateur d'un élément $\sigma \in \mathrm{S}_n$ est le sous-groupe $\mathrm{C}(\sigma) = \{\tau \in \mathrm{S}_n \mid \sigma\tau = \tau\sigma\}$.

(vi) On suppose que $t \in \mathrm{S}_n$ est une transposition. Montrer $\mathrm{C}(t) \simeq \mathrm{S}_2 \times \mathrm{S}_{n-2}$.

(vii) Soit $s \in \mathrm{S}_n$ un élément d'ordre 2. Montrer qu'il existe un unique entier $1 \leqslant k \leqslant n/2$, tel que s est produit de k transpositions $s_1, \ldots, s_k$ à supports disjoints.

(viii) (suite) Soit $D = \langle s_1, \ldots, s_k \rangle$. Montrer que D est un sous-groupe de $\mathrm{C}(s)$ isomorphe à $(\mathbb{Z}/2\mathbb{Z})^k$.

(ix) (suite) Montrer que D est distingué dans $\mathrm{C}(s)$.

(x) On suppose $n = 4$ et $s = (a\,b)(c\,d)$ avec $\{a, b, c, d\} = \{1, 2, 3, 4\}$. Montrer $|\mathrm{C}(s)| > 4$.

(xi) On suppose que $\mathbb{Z}/2\mathbb{Z} \times \mathrm{S}_m$ a un sous-groupe distingué isomorphe à $(\mathbb{Z}/2\mathbb{Z})^k$ avec $k \geqslant 2$ et $m \geqslant 3$. Montrer $m = 4$. On pourra considérer la projection naturelle $\mathbb{Z}/2\mathbb{Z} \times \mathrm{S}_m \to \mathrm{S}_m$.

(xii) En déduire que pour $n \neq 6$, tout automorphisme de S_n est intérieur.

Dans les trois questions suivantes, on étudie le cas $n = 6$.

(xiii) Montrer qu'il existe un sous-groupe H de S_6 qui est isomorphe à S_5, et dont l'action naturelle sur $\{1, 2, \ldots, 6\}$ est transitive.

(xiv) (suite) En considérant l'action par translations de S_6 sur l'ensemble S_6/H, montrer qu'il existe un isomorphisme $f : \mathrm{S}_6 \to \mathrm{S}_6$ vérifiant $f(H) \subset \{\sigma \in \mathrm{S}_6 \mid \sigma(1) = 1\}$.

(xv) (suite) Montrer que f n'est pas intérieur.

On note $\operatorname{Int} \mathrm{S}_n \subset \operatorname{Aut} \mathrm{S}_n$ le sous-ensemble des automorphismes intérieurs. Pour $k = 1, 2, 3$ on note aussi T_k le sous-ensemble de S_6 constitué des produits de k transpositions à supports disjoints.

(xvi) Montrer que $\operatorname{Int} \mathrm{S}_n$ est un sous-groupe distingué de $\operatorname{Aut} \mathrm{S}_n$, et qu'il est isomorphe à S_n.

(xvii) Déterminer $|T_k|$ pour $k = 1$, 2 et 3.

(xviii) En déduire que pour $f \in \mathrm{Aut}\,\mathrm{S}_6$ *non intérieur on a* $f(T_2) = T_2$, $f(T_1) = T_3$ *et* $f(T_3) = T_1$.

(xix) Démontrer $\mathrm{Aut}\,\mathrm{S}_6/\mathrm{Int}\,\mathrm{S}_6 \simeq \mathbb{Z}/2\mathbb{Z}$.

PROBLÈME 2. *Soit* p *un nombre premier* <u>*impair*</u>. *On se propose de classifier, à isomorphisme près, les groupes d'ordre* $4p$. *On commence par quelques questions préliminaires.*

(i) Déterminer, à isomorphisme près, les groupes abéliens d'ordre $4p$.

(ii) Montrer que tout groupe d'ordre 4 *est isomorphe à* $\mathbb{Z}/4\mathbb{Z}$ *ou à* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(iii) Soient G *un groupe d'ordre* mn *avec* $(m, n) = 1$ *et* N *un sous-groupe distingué de* G *d'ordre* n. *Montrer que* N *est l'unique sous-groupe de* G *d'ordre* n. *On pourra considérer la projection canonique* $G \to G/N$.

(iv) Montrer que tout groupe d'ordre $2p$ *contient un unique sous-groupe d'ordre* p.

Dans les questions (v) à (viii) qui suivent, on suppose que G *est un groupe d'ordre* $4p$ *ne possèdant pas de sous-groupe distingué d'ordre* p. *On veut montrer* $p = 3$ *et* $G \simeq \mathrm{A}_4$. *Pour cela, on fixe* $x \in G$ *d'ordre* p *(on justifiera son existence) et on note* $C \subset G$ *la classe de conjugaison de* x.

(v) Montrer $|C| \neq 1$ *et* $|C| \mid 4$.

(vi) Montrer que G *ne possède pas de sous-groupe d'ordre* $2p$.

(vii) En déduire $|C| = 4$ *et que l'action de* G *par conjugaison sur* C *est fidèle.*

(viii) Conclure.

On suppose désormais que G *est un groupe* <u>*non abélien*</u> *d'ordre* $4p$, *et que* P *est un sous-groupe distingué d'ordre* p *de* G. *On fixe aussi un sous-groupe* Q *de* G *d'ordre* 4 *(on justifiera son existence).*

(ix) Montrer que Q *est un complément de* P *et que* $Q \to \mathrm{Aut}(P), q \mapsto (\mathrm{int}_q)_{|P}$, *est un morphisme de groupes bien défini et non trivial.*

(x) Soit V *un groupe abélien* 2*-élémentaire d'ordre* 4, C *un groupe cyclique, et* $f : V \to C$ *un morphisme de groupes. Montrer qu'il existe une base* v, w *de* $V^\sharp$ *avec* $f(v) = 1$.

(xi) On suppose $Q \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. *Montrer que l'on a* $G \simeq \mathbb{Z}/2\mathbb{Z} \times H$ *pour un certain groupe* H, *puis que l'on a un isomorphisme* $H \simeq \mathrm{D}_{2p}$.

On suppose finalement $Q \simeq \mathbb{Z}/4\mathbb{Z}$, *et dans les questions (xii) à (xiv) on suppose en outre* $p \equiv 3 \bmod 4$.

(xii) Montrer qu'il existe un unique morphisme non trivial $\alpha : \mathbb{Z}/4\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$.

(xiii) Montrer $G \simeq \mathbb{Z}/p\mathbb{Z} \rtimes_\alpha \mathbb{Z}/4\mathbb{Z}$.

(xiv) En déduire que tout groupe non abélien d'ordre $4p$ *est isomorphe à un, et un seul, des groupes*

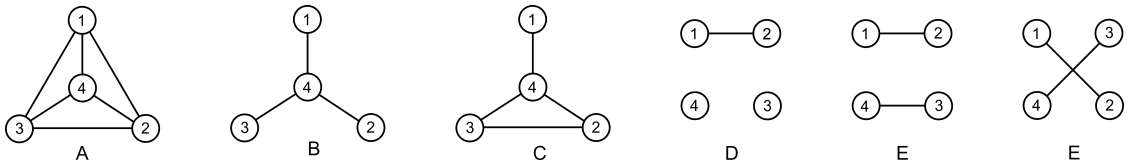
$$\mathbb{Z}/2\mathbb{Z} \times \mathrm{D}_{2p}, \quad \mathbb{Z}/p\mathbb{Z} \rtimes_\alpha \mathbb{Z}/4\mathbb{Z}, \quad \mathrm{A}_4 \ \ (\text{cas } p = 3).$$

(xv) On suppose enfin $p \equiv 1 \bmod 4$. *Comment la classification du (xiv) est-elle modifiée ?*

(xvi) (Bonus) Lequel des groupes ci-dessus est isomorphe à D_{4p} *?*

3. Examen partiel 2023-2024

Problème 1. *Soit $n \geqslant 1$ un entier. Nous appellerons n-*graphe *la donnée d'un sous-ensemble $\Gamma \subset \mathrm{P}(\{1,\dots,n\})$ constitué de parties à 2 éléments de $\{1,\dots,n\}$. Ces parties seront aussi appelées* arètes *du graphe Γ. Par exemple, les six figures suivantes définissent*[1] *cinq 4-graphes (les deux derniers étant égaux), dans lesquels les arètes sont représentées par des traits :*



Soit Γ un n-graphe. Pour $i \in \{1,\dots,n\}$ on pose $\mathrm{V}_\Gamma(i) = \{j \in \{1,\dots,n\} \mid \{i,j\} \in \Gamma\}$ (ensemble des voisins *de i dans Γ) et $\mathrm{v}_\Gamma(i) = |\mathrm{V}_\Gamma(i)|$. Enfin, on définit le* groupe de symétries de Γ *comme étant*

$$\mathrm{G}(\Gamma) := \{g \in \mathrm{S}_n \mid \forall i,j \in \{1,\dots,n\},\ \{i,j\} \in \Gamma \implies \{g(i),g(j)\} \in \Gamma\}.$$

(i) Vérifier que $\mathrm{G}(\Gamma)$ est bien un sous-groupe de S_n.

(ii) Soient $i \in \{1,\dots,n\}$ et $g \in \mathrm{G}(\Gamma)$. Vérifier $g(\mathrm{V}_\Gamma(i)) = \mathrm{V}_\Gamma(g(i))$ et $\mathrm{v}_\Gamma(i) = \mathrm{v}_\Gamma(g(i))$.

(iii) Pour chacun des cinq 4-graphes Γ ci-dessus, donner sans démonstration un groupe isomorphe à $\mathrm{G}(\Gamma)$ dans la liste suivante :

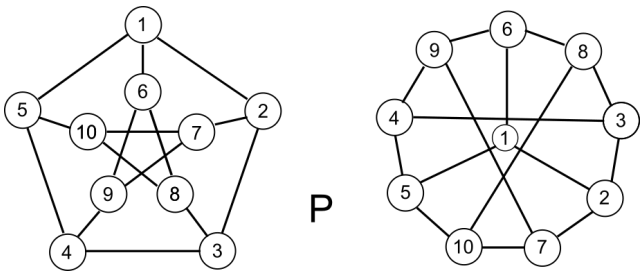
$$1,\ \mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/3\mathbb{Z},\ \mathbb{Z}/4\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z},\ \mathrm{S}_3,\ \mathrm{D}_8,\ \mathrm{H}_8,\ \mathrm{S}_4.$$

(iv) (suite) Pour deux graphes Γ de votre choix parmi ces cinq, justifier votre réponse. On pourra expliciter la fonction $\mathrm{v}_\Gamma : \{1,2,3,4\} \to \mathbb{N}$ et lister les éléments de $\mathrm{G}(\Gamma)$.

Dans la suite du problème, on s'intéresse au graphe de Petersen. *C'est le 10-graphe* P *défini par*

$$\mathrm{P} = \{\{1,2\},\{2,3\},\{3,4\},\{4,5\},\{1,5\},\{6,8\},\{8,10\},\{7,10\},\{7,9\},\{6,9\},\{1,6\},\{2,7\},\{3,8\},\{4,9\},\{5,10\}\}.$$

Les deux figures suivantes en donnent deux représentations :



On se propose de montrer que l'on a $\mathrm{G}(\mathrm{P}) \simeq \mathrm{S}_5$. Comme tout sous-groupe de S_{10}, le groupe $\mathrm{G}(\mathrm{P})$ agit naturellement sur $\{1,\dots,10\}$. Pour $I \subset \{1,\dots,n\}$ on pose $\mathrm{G}(\mathrm{P})_I = \{g \in \mathrm{G}(\mathrm{P}) \mid g(i) = i,\ \forall i \in I\}$.

(v) À l'aide des figures, donner un élément d'ordre 3 et un élément d'ordre 5 dans $\mathrm{G}(\mathrm{P})$.

(vi) Montrer que $\mathrm{G}(\mathrm{P})$ agit transitivement sur $\{1,\dots,10\}$.

(vii) Montrer que $\mathrm{G}(\mathrm{P})_{\{1,2,5,6\}}$ est engendré par l'élément $(3\,7)(4\,10)(8\,9)$.

---

1. Concrètement, il faut comprendre $\mathrm{A} = \{\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\}\}$, $\mathrm{B} = \{\{1,4\},\{2,4\},\{3,4\}\}$, $\mathrm{C} = \{\{1,4\},\{2,4\},\{2,3\},\{3,4\}\}$, $\mathrm{D} = \{\{1,2\}\}$ et $\mathrm{E} = \{\{1,2\},\{3,4\}\}$.

(viii) Montrer que l'on a une suite exacte courte $1 \to \mathrm{G(P)}_{\{1,2,5,6\}} \to \mathrm{G(P)}_{\{1\}} \to \mathrm{S}_{\{2,5,6\}} \to 1$.

(ix) En déduire $|\mathrm{G(P)}| = 120$.

Appelons tétrade *de* P *tout sous-ensemble* $T \subset \{1, 2, \ldots, 10\}$ *avec* $|T| = 4$ *et vérifiant* $\forall i, j \in T$, $\{i,\ j\} \notin \mathrm{P}$ *(autrement dit,* T *ne contient pas de couple de voisins dans* P*).*

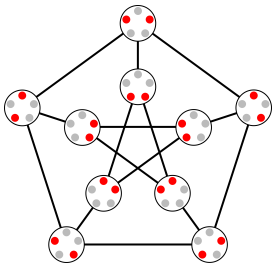
(x) Vérifier qu'il existe exactement deux tétrades T *et* T' *contenant* 1*, et que l'on a* $T \cap T' = \{1\}$.

(xi) En déduire que P *contient exactement* 5 *tétrades.*

(xii) Montrer qu'il existe un morphisme de groupes injectif $\mathrm{G(P)} \longrightarrow \mathrm{S}_5$.

(xiii) Conclure.

(xiv) Démontrer l'existence d'un morphisme injectif $\mathrm{S}_5 \to \mathrm{G(P)}$ *sans utiliser les questions précédentes, mais en contemplant l'égalité* $\binom{5}{2} = 10$ *et la figure suivante :*



Problème 2. (Le théorème de Miller-Moreno) *Un groupe* G *sera dit* sous-cyclique *si tout sous-groupe strict*[2] *de* G *est cyclique. On se propose de montrer le théorème suivant, dû à Miller et Moreno : si* G *est un groupe fini sous-cyclique, alors soit* G *est isomorphe à l'un des groupes*

$$\mathbb{Z}/n\mathbb{Z} \ \ (n \geqslant 1), \ \ \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \ \ (p \text{ premier}), \ \ \mathrm{H}_8,$$

soit on a $G \simeq \mathbb{Z}/p\mathbb{Z} \rtimes_\alpha \mathbb{Z}/q^n\mathbb{Z}$ *avec* $n \geqslant 1$, p *et* q *premiers vérifiant* $q \,|\, p-1$, *et* α *bien choisi.*

Partie I : Le cas des groupes abéliens

(i) Rappeler brièvement pourquoi tout groupe cyclique est sous-cyclique.

(ii) Montrer que pour p *premier, le groupe* $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ *est sous-cyclique et non cyclique.*

(iii) Montrer que si G *est un groupe abélien fini non cyclique, il existe un nombre premier* p *tel que* G *contienne un sous-groupe isomorphe à* $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

(iv) En déduire une classification, à isomorphisme près, des groupes abéliens finis sous-cycliques.

Partie II : Quelques propriétés des groupes sous-abéliens

Un groupe G *sera dit* sous-abélien *si tout sous-groupe strict de* G *est abélien.*

(i) Soient G *un groupe sous-abélien et* H *un sous-groupe distingué de* G. *Montrer que les groupes* H *et* G/H *sont sous-abéliens.*

(ii) Montrer que tout groupe abélien fini non trivial possède un sous-groupe d'indice premier.

2. Un sous-groupe H d'un groupe G est dit strict si on a $H \neq G$.

(iii) On admet qu'un groupe sous-abélien fini non abélien n'est pas simple.[3] *En déduire que tout groupe sous-abélien fini non trivial possède un sous-groupe distingué d'indice premier.*

On se propose maintenant de démontrer que si G est un groupe sous-abélien fini non abélien, il existe deux sous-groupes P et Q de G tels que : (a) $G = PQ$, (b) P *est distingué dans G et d'ordre p^m avec p premier et $m \geqslant 0$, et* (c) Q *est d'ordre q^n avec q premier $\neq p$ et $n \geqslant 1$.*

(iv) Soient H un groupe abélien fini et $n \geqslant 1$. Montrer que $H[n] = \{h \in H \mid h^n = 1\}$ est un sous- groupe caractéristique de H, et que tout nombre premier divisant $|H[n]|$ divise l'entier n.

(v) (suite) On suppose $|H| = ab$ avec a et b premiers entre eux, et pose $A = H[a]$ et $B = H[b]$. Montrer $H = AB$ et $A \cap B = \{1\}$, puis $|A| = a$ et $|B| = b$.

(vi) Soient A et B deux sous-groupes finis d'un groupe G avec $A \lhd G$. Montrer que AB est un sous-groupe de G d'ordre divisant $|A|\,|B|$.

(vii) Soient G un groupe et H un sous-groupe distingué de G d'indice premier q. Montrer qu'il existe $z \in G$ d'ordre une puissance de q et vérifiant $G = H\langle z\rangle$. On pourra considérer la projection canonique $G \to G/H$.

(viii) (suite) On suppose en outre G sous-abélien. Montrer que l'on a $G = H'Q$ avec H' un sous-groupe abélien distingué de G d'ordre premier à q, et Q un sous-groupe de G d'ordre q^n avec $n \geqslant 1$.

(ix) Conclure.

Partie III : Les groupes de Miller-Moreno

Dans cette partie, on s'intéresse aux groupes finis sous-cycliques G non abéliens tels que $|G|$ admette au moins deux diviseurs premiers distincts (« groupes de Miller-Moreno »). Soit G un tel groupe.

(i) Montrer qu'il existe des éléments x et y de G d'ordres respectifs p^m et q^n, avec p, q premiers distincts, m, n entiers $\geqslant 1$ et $G = \langle x\rangle\langle y\rangle$, ainsi que $k \in \mathbb{Z}$ avec $yxy^{-1} = x^k$ et $k \not\equiv 1 \bmod p^m$.

(ii) Montrer $x\,y^q = y^q\,x$ et $x^p\,y = y\,x^p$. On pourra considérer $\langle x\rangle\langle y^q\rangle$ et $\langle x^p\rangle\langle y\rangle$.

(iii) En déduire $k^q \equiv 1 \bmod p^m$ et $k \equiv 1 \bmod p^{m-1}$.

(iv) Montrer $m = 1$ et $q \mid p-1$. On rappelle, pour $r \in p\mathbb{Z}$, la congruence $(1+r)^p \equiv 1 \bmod pr$.

(v) Montrer qu'il existe un morphisme de groupes $\alpha : \mathbb{Z}/q^n\mathbb{Z} \to \operatorname{Aut}\mathbb{Z}/p\mathbb{Z}$ envoyant $\overline{1}$ sur $z \mapsto \overline{k}z$.

(vi) En déduire $G \simeq \mathbb{Z}/p\mathbb{Z} \rtimes_\alpha \mathbb{Z}/q^n\mathbb{Z}$.

(vii) Réciproquement, montrer que pour p et q premiers avec $q \mid p-1$, et $n \geqslant 1$, il existe un morphisme $\beta : \mathbb{Z}/q^n\mathbb{Z} \to \operatorname{Aut}\mathbb{Z}/p\mathbb{Z}$ tel que $\mathbb{Z}/p\mathbb{Z} \rtimes_\beta \mathbb{Z}/q^n\mathbb{Z}$ est sous-cyclique et non abélien.

Partie IV : (Bonus) le cas des p-groupes

On suppose enfin que G est un groupe sous-cyclique non abélien d'ordre p^n avec p premier et $n \geqslant 2$. On se donne un sous-groupe distingué $H = \langle x\rangle$ d'ordre p^{n-1}, et on fixe $y \in G \smallsetminus H$.

(i) Montrer $y^p \in \langle x^p\rangle$ et $y\,x^p = x^p\,y$.

3. Ce résultat, admis dans tout le problème, avait fait l'objet du second problème du partiel 2021-2022.

(ii) Montrer $yxy^{-1} = x^k$ *avec* $k \in \mathbb{Z}$, $k \equiv 1 \bmod p^{n-2}$ *et* $n \geqslant 3$.

(iii) Montrer que quitte à remplacer y *par* $x^i y$ *pour* $i \in \mathbb{Z}$ *bien choisi, on peut supposer* $y^{2p} = 1$.

(iv) En considérant le sous-groupe $\langle t, y\rangle$ *de* G *avec* $t = x^{p^{n-2}}$, *montrer* $p = 2$ *et* $y^2 = t$.

(v) En déduire $G \simeq \mathrm{H}_8$, *puis terminer la démonstration du théorème de Miller-Moreno.*

4. Examen 2021-2022

Aucun document n'est autorisé. Temps de composition : 3h. Il n'est pas du tout nécessaire de traiter toutes les questions pour avoir le maximum des points. On soignera la rédaction.

Problème 1. (Sommes de carrés, suivant Hurwitz et Eckmann) *On se propose de démontrer, que si l'on a une identité remarquable dans* $\mathbb{R}[x_1, \ldots, x_n, y_1, \ldots, y_n]$ *de la forme*

$$(x_1^2 + x_2^2 + \cdots + x_n^2)(y_1^2 + y_2^2 + \cdots + y_n^2) = z_1^2 + z_2^2 + \cdots + z_n^2,$$

où les z_k *sont combinaisons* $\mathbb{R}$*-linéaires des* $x_i y_j$, *alors on a* $n = 1, 2, 4$ *ou* 8 (Théorème de Hurwitz).

Partie 1

Soient m, n *des entiers* > 1 *avec* m *impair, ainsi que* $g_1, \ldots, g_m$ *des éléments de* $\mathrm{GL}_n(\mathbb{C})$ *vérifiant*[4]

$$(*) \qquad g_i^2 = -1_n \text{ pour tout } i, \text{ et } g_i g_j = -g_j g_i \text{ pour tout } i \neq j.$$

On se propose dans cette partie de démontrer la congruence $n \equiv 0 \bmod 2^{\frac{m-1}{2}}$. *Pour cela, on note* G *le sous-groupe de* $\mathrm{GL}_n(\mathbb{C})$ *engendré par les* g_i, *avec* $i = 1, \ldots, m$. *Nous allons commencer par déterminer* $|G|$, *le centre* Z *de* G, *ainsi que le groupe dérivé* $\mathrm{D}(G)$ *de* G. *Pour* $I \subset \{1, \ldots, m\}$, *disons* $I = \{i_1, \ldots, i_k\}$ *avec* $i_1 < i_2 < \cdots < i_k$, *on pose* $g_I = g_{i_1} g_{i_2} \ldots g_{i_k} \in G$, *avec la convention* $g_\varnothing = 1_n$. *On pose enfin* $\eta = g_{\{1,\ldots,m\}} = g_1 g_2 \cdots g_m \in G$. *On écrira « $a = \pm b$ » pour « $a = b$ ou $a = -b$ ».*

(i) Donner un exemple d'éléments g_1, g_2, g_3 *(cas* $m = 3$*) satisfaisant les relations* $(*)$ *pour* $n = 2$.

(ii) Soient $I, J \subset \{1, \ldots, m\}$, *justifier brièvement l'égalité* $g_I g_J = \pm g_K$ *avec* $K = (I \cup J) \smallsetminus (I \cap J)$.

(iii) En déduire $G = \{\pm g_I \mid I \subset \{1, \ldots, m\}\}$ *et* $g^2 = \pm 1_n$ *pour tout* $g \in G$.

(iv) Soit $I \subset \{1, \ldots, m\}$. *Montrer que l'on a* $g_i\, g_I\, g_i^{-1} = (-1)^{|I|} \epsilon g_I$ *avec* $\epsilon = 1$ *si* $i \notin I$, *et* $\epsilon = -1$ *sinon.*

(v) (suite) En déduire que si $g = \pm g_I$, *alors la classe de conjugaison de* g *dans* G *est* $\{g, -g\}$, *sauf si* $|I| = 0$ *ou* $|I| = m$, *auquel cas on a* $g \in Z$.

(vi) Montrer $Z = \{\pm 1_n, \pm\eta\}$, *puis* $|Z| = 2$ *ou* $|Z| = 4$, *selon que l'on a* $\eta = \pm 1_n$ *ou non.*[5]

(vii) Montrer $|G| = 2^{m-1}|Z|$. *On pourra montrer que tout élément de* G *s'écrit de manière unique sous la forme* $z g_I$ *avec* $z \in Z$ *et* $I \subset \{1, \ldots, m-1\}$.

(viii) Montrer que G *a exactement* $|Z| + \frac{|G|-|Z|}{2} = 2^{m-2}|Z| + \frac{|Z|}{2}$ *classes de conjugaison.*

(ix) Montrer $\mathrm{D}(G) = \{\pm 1_n\}$.

4. Bien entendu, 1_n désigne ici la matrice identité de $\mathrm{M}_n(\mathbb{C})$.

5. En fait, les deux cas peuvent se produire en général, donc on n'essaiera pas de montrer qu'on est dans un cas ou l'autre.

(x) En déduire qu'il existe exactement $|G|/2 = 2^{m-2}|Z|$ *morphismes de groupes* $G \to \mathbb{C}^\times$.

(xi) Montrer que l'unique solution de l'équation $2^m = a^2 + b^2$ *avec* a, b *entiers* $\geqslant 1$ *est* $a = b = 2^{\frac{m-1}{2}}$.

(xii) Montrer qu'à isomorphisme près, G *possède* $|Z|/2$ *représentations* $\mathbb{C}$*-linéaires irréductibles de dimension* > 1*, et qu'elles sont de dimension* $2^{\frac{m-1}{2}}$ *(on commencera par traiter le cas* $|Z| = 2$*).*

(xiii) Montrer que la représentation naturelle de G *sur* $\mathbb{C}^n$ *n'a aucune droite stable par* G.

(xiv) Montrer que l'on a $2^{\frac{m-1}{2}} \mid n$.

Partie 2

Soit E *un espace euclidien de dimension* $n > 1$*, de norme euclidienne notée* $||.||$*. On suppose qu'il existe une application* $\mathbb{R}$*-bilinéaire* $E \times E \to E$*,* $(x, y) \mapsto x \star y$*, telle que pour tout* $x, y \in E$ *on ait*

$$||x \star y||^2 = ||x||^2\, ||y||^2.$$

On se propose de montrer que l'on a $n = 2, 4$ *ou* 8*. On fixe une base orthonormée* $\varepsilon_1, \ldots, \varepsilon_n$ *de* E.

(i) Donner un exemple pour $n = 2$ *et pour* $n = 4$*. (Bonus : une idée dans le cas* $n = 8$ *?)*

(ii) Pour $x \in E$ *on note* $\mathrm{m}_x : E \to E$ *l'application linéaire* $y \mapsto x \star y$*, et* $\mathrm{M}(x) \in \mathrm{M}_n(\mathbb{R})$ *la matrice de* m_x *dans la base des* ε_i*. Montrer* ${}^{\mathrm{t}}\mathrm{M}(x)\,\mathrm{M}(x) = ||x||^2\, 1_n$ *pour tout* $x \in E$.

(iii) En déduire $\mathrm{M}(\varepsilon_i) \in \mathrm{O}(n)$ *pour tout* $i = 1, \ldots, n$*, et* ${}^{\mathrm{t}}\mathrm{M}(\varepsilon_i)\mathrm{M}(\varepsilon_j) + {}^{\mathrm{t}}\mathrm{M}(\varepsilon_j)\mathrm{M}(\varepsilon_i) = 0$ *pour* $i \neq j$.

(iv) On pose $g_i = \mathrm{M}(\varepsilon_i)\,{}^{\mathrm{t}}\mathrm{M}(\varepsilon_n) \in \mathrm{O}(n)$*. Vérifier, pour tout* $1 \leqslant i \neq j \leqslant n-1$*, les relations*

$$g_i^2 = -1_n \text{ et } g_i g_j = -g_j g_i.$$

(v) Montrer que n *est pair.*

(vi) Conclure, et expliquer pourquoi nous avons bien résolu la question initiale !

Problème 2. (Une caractérisation de $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$, suivant Zassenhaus)

Soit p *un nombre premier. Un théorème de Zassenhauss affirme que si* G *est un sous-groupe d'ordre* $p^3 - p = p(p-1)(p+1)$ *de* S_{p+1} *agissant transitivement sur* $\{1, 2, \ldots, p+1\}$*, alors* G *est isomorphe au groupe* $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$*. Dans la première partie, on se propose de démontrer ce résultat sous l'hypothèse supplémentaire* $p \equiv 3 \bmod 4$*. Dans la seconde partie, indépendante, nous en donnons une application.*

Partie 1

Soit p *un nombre premier. On considère l'ensemble*[6] $X = \mathbb{Z}/p\mathbb{Z} \coprod \{\infty\}$*, qui a* $p+1$ *éléments. On rappelle que le groupe* $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ *s'identifie naturellement au sous-groupe* $\mathscr{H}_X \subset \mathrm{S}_X$ *des homographies de* X*, c'est-à-dire des bijections de* X *de la forme*

$$x \mapsto \frac{ax+b}{cx+d}, \quad \text{avec} \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}).$$

6. Cet ensemble est aussi noté $\widehat{\mathbb{Z}/p\mathbb{Z}}$ dans le cours, où on l'a identifié à la droite projective $\mathrm{P}^1(\mathbb{Z}/p\mathbb{Z})$.

On note aussi $\mathrm{Aff}_X \subset \mathscr{H}_X$ *le sous-groupe des homographies* g *telles que* $g(\infty) = \infty$, *i.e. de la forme* $g(x) = ax + b$, *avec* $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ *et* $b \in \mathbb{Z}/p\mathbb{Z}$ *(homographies « affines »).*

(i) Rappeler pourquoi on a $|\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})| = p^3 - p$.

(ii) Montrer que $\mathscr{H}_X$ *est engendré par l'homographie* $x \mapsto 1/x$ *et son sous-groupe* Aff_X.

(iii) Montrer que Aff_X *agit* 2*-transitivement sur* $\mathbb{Z}/p\mathbb{Z}$.

Soit G *un sous-groupe de* S_X *de cardinal* $p^3 - p$ *et agissant transitivement sur* X. *On veut montrer qu'il existe* $\sigma \in \mathrm{S}_X$ *tel que* $\sigma G \sigma^{-1} = \mathscr{H}_X$. *On note* $\alpha \in \mathrm{Aff}_X$ *la translation* $x \mapsto x + 1$.

(iv) Montrer que G *possède un* p*-cycle.*

(v) En déduire qu'il existe $\sigma \in \mathrm{S}_X$ *tel que* $\sigma G \sigma^{-1}$ *contient* α, *puis que l'on peut supposer* $\alpha \in G$.

On suppose désormais $\alpha \in G$. *On veut montrer* $G = \mathscr{H}_X$. *On note* $G_\infty \subset G$ *le stabilisateur de* $\infty \in X$ *dans* G.

(vi) Monter $|G_\infty| = p^2 - p$.

(vii) Montrer que $P = \langle \alpha \rangle$ *est l'unique sous-groupe d'ordre* p *de* G_∞, *puis que l'on a* $P \lhd G_\infty$.

(viii) En déduire que pour tout $g \in G_\infty$, *il existe un entier* $1 \leqslant a < p$ *tel que* $g\alpha = \alpha^a g$.

(ix) Montrer $G_\infty \subset \mathrm{Aff}_X$, *puis* $G_\infty = \mathrm{Aff}_X$.

(x) En déduire que G *agit* 3*-transitivement sur* X.

(xi) Montrer que si $g \in G$ *fixe* 3 *points distincts dans* X, *alors* $g = 1$ *(on se ramenera au cas* $g \in G_\infty$*).*

On pose $C = \{g \in G_\infty \mid g(0) = 0\}$ *et* $C' = \{g \in \mathrm{S}_X \mid gc = cg \ \forall c \in C\}$ *(centralisateur de* C *dans* S_X*). On fixe* $\gamma \in G$ *tel que* $\gamma(0) = \infty$, $\gamma(1) = 1$ *et* $\gamma(\infty) = 0$ *(on justifiera l'existence de* γ*).*

(xii) Montrer que C *est cyclique d'ordre* $p-1$, *et qu'il est engendré par un* $(p-1)$*-cycle.*

(xiii) En déduire que C' *est engendré par* C *et la transposition* $(0\,\infty)$.

(xiv) Montrer que si G *contient une transposition, ou si* $p \leqslant 3$, *on a* $G = \mathrm{S}_X = \mathscr{H}_X$.

On suppose donc désormais $(0\,\infty) \notin G$ *et* $p > 3$.

(xv) Montrer $C' \cap G = C$.

(xvi) Montrer que $\mathrm{int}_\gamma : G \to G, g \mapsto \gamma g \gamma^{-1}$, *induit un automorphisme d'ordre* 2 *de* C.

(xvii) Montrer qu'il existe un entier $1 < n < p-1$ *avec* $n^2 \equiv 1 \bmod p-1$ *et* $\gamma c \gamma^{-1} = c^n$ *pour tout* $c \in C$.

(xviii) (suite) Montrer $\gamma(x) = x^n$ *pour tout* $x \in (\mathbb{Z}/p\mathbb{Z})^\times \subset X$.

(xix) (suite) En considérant les point fixes de γ *dans* X, *montrer* $n \equiv -1 \bmod \frac{p-1}{2}$.

(xx) (suite) On suppose enfin $p \equiv 3 \bmod 4$. *Montrer* $n \equiv -1 \bmod p - 1$.

(xxi) En déduire que si $p \equiv 3 \bmod 4$, *on a* $G = \mathscr{H}_X$.

Partie 2

Dans cette seconde partie, indépendante, nous donnons des applications du résultat principal de la Partie 1 *(que l'on pourra donc admettre). On suppose d'abord que* G *est un groupe d'ordre* $p^3 - p$, *avec* p *premier, et que* G *ne possède pas de sous-groupe distingué* H *non trivial avec* $|H| \mid p^2 - p$. *On note* X *l'ensemble des sous-groupes d'ordre* p *de* G, *et on fait agir* G *sur* X *par conjugaison.*

(i) Soit $d \geqslant 1$ un diviseur de $p^2 - 1$ avec $d \equiv 1 \bmod p$. Montrer $d = 1$ ou $d = p + 1$.

(ii) En déduire $|X| = p + 1$.

(iii) Montrer que l'action de G sur X est transitive et fidèle.

(iv) On suppose $p \equiv 3 \bmod 4$. Montrer que l'on a un isomorphisme $G \simeq \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$.

On considère enfin les groupes $H = \mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$ et $G = H \rtimes_\psi \mathbb{Z}/2\mathbb{Z}$, où $\psi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(H)$ est le morphisme envoyant l'élément non trivial de $\mathbb{Z}/2\mathbb{Z}$ sur l'automorphisme $h \mapsto {}^{\mathrm{t}}h^{-1}$ de H (d'ordre 2).

(v) Rappeler pourquoi H est un groupe simple, et montrer $|H| = 168$.

(vi) Montrer qu'il n'existe aucun élément $M \in \mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$ tel que ${}^{\mathrm{t}}hMh = M$ pour tout $h \in \mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$.

(vii) En déduire que G ne possède pas de sous-groupe distingué d'ordre 2.

(viii) Montrer que les seuls sous-groupes distingués de G sont $\{1\}$, G et $H \times \{\overline{0}\} \simeq H$.

(ix) En déduire $G \simeq \mathrm{PGL}_2(\mathbb{Z}/7\mathbb{Z})$, puis $H \simeq \mathrm{PSL}_2(\mathbb{Z}/7\mathbb{Z})$.

5. Examen 2022-2023

Problème 1. *On veut montrer que $\mathrm{PGL}_2(\mathbb{Z}/11\mathbb{Z})$ possède un sous-groupe isomorphe à A_5* (Galois).

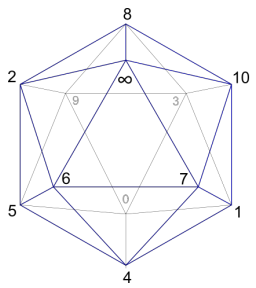
(i) Soit G un groupe simple possédant un sous-groupe H d'indice n avec $n \geqslant 2$. En considérant l'action par translations de G sur G/H, montrer que $|G|$ divise $n!$.

(ii) En déduire que si $g, h \in \mathrm{A}_5$ sont d'ordres respectifs 3 et 5, alors g et h engendrent A_5.

On pose $X := \mathbb{Z}/11\mathbb{Z} \coprod \{\infty\}$ et on rappelle que $\mathrm{PGL}_2(\mathbb{Z}/11\mathbb{Z})$ s'identifie naturellement au sous-groupe de S_X constitué des homographies de X.

(iii) Donner la décomposition en cycles de l'homographie $x \mapsto \frac{7x+1}{x+5}$ vue comme bijection de X. On donne les congruences $2 \cdot 6 \equiv 3 \cdot 4 \equiv 5 \cdot 9 \equiv 7 \cdot 8 \equiv 10^2 \equiv 1 \bmod 11$.

(iv) Conclure en contemplant l'icosaèdre suivant.



Problème 2. *Soit G un groupe possédant un sous-groupe distingué Z vérifiant $Z \simeq \mathbb{Z}/2\mathbb{Z}$ et $G/Z \simeq \mathrm{A}_5$. On se propose de montrer que l'on a soit $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathrm{A}_5$, soit*[7] *$G \simeq \widetilde{\mathrm{A}_5}$* (Schur).

(i) Montrer que Z est inclus dans le centre de G.

7. On rappelle que $\widetilde{\mathrm{A}_5}$ est un sous-groupe de $\mathrm{Sp}(1)$ contenant $\{\pm 1\}$ et dont l'image dans le groupe quotient $\mathrm{Sp}(1)/\{\pm 1\} \simeq \mathrm{SO}(3)$ est isomorphe à A_5. Dans ce problème, le groupe $\widetilde{\mathrm{A}_5}$ n'interviendra qu'à la question *(xi)*.

(ii) On suppose que G possède un sous-groupe distingué N distinct de $\{1\}$, Z et G. Montrer que N est un complément de Z dans G. On pourra considérer la projection canonique $\pi : G \to G/Z$.

(iii) (suite) En déduire $N \simeq \mathrm{A}_5$ et $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathrm{A}_5$.

On suppose désormais que les seuls sous-groupes distingués de G sont $\{1\}$, Z et G. On note z l'unique élément non trivial de Z et on fixe $r : G \to \mathrm{GL}_n(\mathbb{C})$ une représentation de G.

(iv) Montrer $\mathrm{D}(G) = G$.

(v) Montrer $r(G) \subset \mathrm{SL}_n(\mathbb{C})$.

(vi) On suppose r irréductible. Montrer que l'on a $r(z) = 1_n$ ou $r(z) = -1_n$.

(vii) On suppose $r(z) = -1_n$. Montrer $n \equiv 0 \bmod 2$ et que r est injective.

On choisit un ensemble de représentants $\{U_i\}_{i\in I}$ des classes d'isomorphisme de $\mathbb{C}[G]$-modules irréductibles dans lesquels z n'agit pas par l'identité.

(viii) Montrer $\sum_{i\in I} (\dim U_i)^2 = |G| - |G/Z| = 60$.

(ix) En déduire qu'il existe $i \in I$ avec $\dim U_i = 2$.

(x) Montrer que G est isomorphe à un sous-groupe fini de $\mathrm{SL}_2(\mathbb{C})$.

(xi) En déduire $G \simeq \widetilde{\mathrm{A}_5}$. On utilisera sans démonstration le fait que tout sous-groupe fini de $\mathrm{SL}_2(\mathbb{C})$ est conjugué à un sous-groupe de $\mathrm{Sp}(1)$.

(xii) (Application) Montrer $\mathrm{SL}_2(\mathbb{Z}/5\mathbb{Z}) \simeq \widetilde{\mathrm{A}_5}$.

Problème 3. *Dans tout ce problème, p désigne un nombre premier. Soient G un sous-groupe de S_p avec $p \mid |G|$, et $0 \leqslant r < p$ l'unique entier tel que $\frac{|G|}{p} \equiv r \bmod p$. On se propose de montrer que si r est premier, et si on a $|G| \neq pr$, alors le groupe G est simple (« critère de simplicité de Chapman ») .*

Partie 1 : applications

Dans cette partie, on admet le critère de simplicité de Chapman et on en donne trois applications.

(i) Retrouver que le groupe A_5 est simple.

(ii) Retrouver que le groupe $\mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$ est simple en le faisant agir sur $(\mathbb{Z}/2\mathbb{Z})^3 \smallsetminus \{0\}$.

(iii) Le groupe M_{11} est un sous-groupe de S_{11} construit par E. Mathieu en 1861. On admet que son action naturelle sur $\{1, \ldots, 11\}$ est 4-transitive, et que le seul élément de M_{11} fixant 4 points dans $\{1, \ldots, 11\}$ est l'identité. Déterminer $|\mathrm{M}_{11}|$ et montrer que M_{11} est simple. [8]

Partie 2 : préliminaires sur S_p

On pose $X = \mathbb{Z}/p\mathbb{Z}$ et on note Aff_X le sous-ensemble de S_X constitué des bijections de la forme $x \mapsto ax + b$ avec $a, b \in \mathbb{Z}/p\mathbb{Z}$. On note enfin $c \in \mathrm{Aff}_X$ la bijection $x \mapsto x + 1$.

(i) Vérifier que Aff_X est un sous-groupe de S_X et donner son ordre.

(ii) Montrer que le normalisateur de $\langle c \rangle$ dans S_X est Aff_X.

Partie 3 : l'invariant r d'un sous-groupe transitif de S_p

Soit G un sous-groupe de S_p.

8. Le groupe M_{11} est le plus petit des groupes simples dits *sporadiques*.

(i) Montrer les équivalences entre :

(a) p divise $|G|$,

(b) G contient un p-cycle,

(c) G agit transitivement sur $\{1, \ldots, p\}$.

On suppose désormais ces propriétés satisfaites. On note r_G l'unique élément $0 \leqslant r < p$ tel que $\frac{|G|}{p} \equiv r \bmod p$. On fixe P un p-Sylow de G, $\mathrm{N}_G(P)$ le normalisateur de P dans G, et on note n_G le nombre des p-Sylow de G.

(ii) Rappeler pourquoi on a $|P| = p$ et $|G| = |\mathrm{N}_G(P)|\,\mathrm{n}_G$.

(iii) Montrer $|\mathrm{N}_G(P)| = p\,\mathrm{r}_G$ et que r_G divise $p-1$.

(iv) On suppose $\mathrm{r}_G = 1$. Montrer que G possède exactement n_G éléments qui ne sont pas d'ordre p.

(v) (suite) En considérant les stabilisateurs dans G des éléments de $\{1, \ldots, p\}$, montrer $\mathrm{n}_G = 1$.

Partie 4 : démonstration du théorème

Soient G un sous-groupe de S_p avec r_G premier et $\mathrm{n}_G > 1$, et N un sous-groupe distingué non trivial de G.

(i) Montrer que les orbites de $\{1, \ldots, p\}$ sous l'action de N ont toutes même cardinal.

(ii) En déduire que p divise $|N|$.

(iii) Montrer $\mathrm{n}_N = \mathrm{n}_G$.

(iv) Montrer que r_N divise r_G.

(v) Conclure.

Problème 4. *Soit M un $\mathbb{Z}[i]$-module dont le groupe abélien sous-jacent est libre de rang fini r. On se propose d'abord de montrer que r est pair et que le $\mathbb{Z}[i]$-module M est libre de rang $r/2$.*

(i) Montrer que M est de type fini.

(ii) Soient $m \in M$ et $a \in \mathbb{Z}[i] \smallsetminus \{0\}$ avec $a\,m = 0$. Montrer $m = 0$.

(iii) Conclure.

(Application) *On se place dans un plan euclidien P, de produit scalaire $(x, y) \mapsto x.y$, et on se donne L un réseau de P, c'est-à-dire un sous-groupe additif engendré par une $\mathbb{R}$-base de P.*

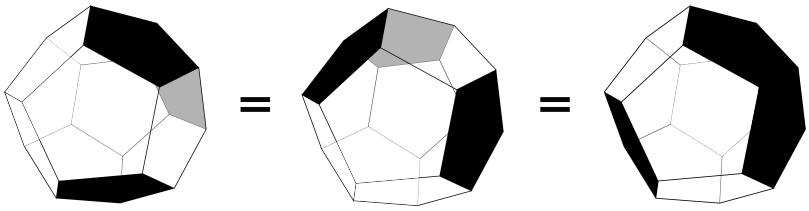
(iv) On suppose que L est stable par la rotation d'angle $\pi/2$. Montrer qu'il existe $u, v \in P$ avec

$$u.u = v.v, \;\; u.v = 0 \;\text{ et }\; L = \mathbb{Z}u + \mathbb{Z}v.$$

6. Examen 2023-2014

Problème 1. (Dodécaèdres noirs et blancs) *Soit* D *un dodécaèdre régulier. On se propose de déterminer le nombre de façons de colorier chaque face de* D *en noir ou en blanc, sachant que l'on identifie deux coloriages s'ils se déduisent l'un de l'autre par une rotation de* D.

(i) Déterminer le nombre de 3-cycles, de doubles-transpositions, et de 5-cycles, dans A_5.



Soit G un groupe agissant sur un ensemble fini X, et soit E un ensemble fini de cardinal m. Pour $g \in G$ et $\phi : X \to E$, on définit $g.\phi : X \to E$ par la formule $(g.\phi)(x) = \phi(g^{-1}x)$.

(ii) Vérifier que $(g, \phi) \mapsto g.\phi$ est une action de G sur l'ensemble E^X.

(iii) Soit $g \in G$. Montrer que le nombre de points fixes de g dans E^X est de la forme $m^{\mathrm{r}_X(g)}$, où $\mathrm{r}_X(g)$ est un entier que l'on exprimera en fonction du type de la décomposition en cycles de g sur X.

On suppose désormais que G est le groupe des isométries directes d'un dodécaèdre régulier, et que X est l'ensemble des 12 faces de ce dodécaèdre, muni de l'action naturelle de G.

(iv) Soit $g \in G \smallsetminus \{1\}$ possédant un point fixe dans X. Justifier brièvement pourquoi g est d'ordre 5 et possède exactement deux points fixes dans X.

(v) En déduire que l'action de G sur E^X a exactement $\frac{1}{60}(m^{12} + 15\,m^6 + 44\,m^4)$ orbites.

(vi) Conclure.

Problème 2. (Groupes auto-transitifs et critère de simplicité de Rotman) *On commence par une question préliminaire. Soit G un groupe agissant k-transitivement*[9] *sur un ensemble X, avec $k \geqslant 2$, et soit $x \in X$.*

(o) Vérifier que G_x agit $(k-1)$-transitivement sur $X \smallsetminus \{x\}$.

Partie I : groupes auto-transitifs

On s'intéresse aux groupes finis G tels que l'action naturelle du groupe $\mathrm{Aut}\, G$ sur l'ensemble $G \smallsetminus \{1\}$, $(\alpha, g) \mapsto \alpha(g)$, est transitive. Dans les questions (i) à (iii) on fixe un tel groupe $G \neq \{1\}$, et on choisit un nombre premier p divisant $|G|$.

(i) Montrer que tout élément non trivial de G est d'ordre p.

(ii) Montrer $\mathrm{Z}(G) = G$.

(iii) En déduire que l'on a $G \simeq (\mathbb{Z}/p\mathbb{Z})^n$ avec $n \geqslant 1$.

(iv) Réciproquement, montrer que pour p premier et $n \geqslant 1$, le groupe $(\mathbb{Z}/p\mathbb{Z})^n$ a la propriété requise.

On se donne enfin un entier $k \geqslant 2$ et un groupe fini G tels que l'action naturelle de $\mathrm{Aut}\, G$ sur $G \smallsetminus \{1\}$ est k-transitive.

(v) On suppose $k = 2$. Montrer que l'on a soit $G \simeq \mathbb{Z}/3\mathbb{Z}$, soit $G \simeq (\mathbb{Z}/2\mathbb{Z})^n$ et $n \geqslant 2$.

(vi) On suppose $k \geqslant 3$. Montrer $k = 3$ et $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Partie II : le critère de simplicité de Rotman

Soit G un groupe fini agissant fidèlement et k-transitivement sur un ensemble fini X, avec $k \geqslant 2$. Supposons qu'il existe $x \in X$ tel que le groupe G_x est simple. Suivant J. Rotman, nous allons démontrer que l'une des assertions suivantes est satisfaite :

9. On rappelle que notre convention est que si un groupe agit k-transitivement sur un ensemble X alors on a $|X| \geqslant k$.

(a) *G est simple,*

(b) *on a $k = 3$ et, soit $|X| = 3$ et $G = \mathrm{S}_X$, soit $|X|$ est une puissance de 2,*

(c) *on a $k = 2$ et $|X|$ est une puissance d'un nombre premier.*

On fixe $x_0 \in X$ tel que G_{x_0} est simple. Soit N un sous-groupe distingué de G avec $N \neq \{1\}$ et $N \neq G$.

(i) Montrer que N agit transitivement X. On pourra considérer $x \in X$ tel que $|Nx| > 1$ et montrer $X = Nx$.

(ii) Montrer $N \cap G_{x_0} = \{1\}$.

(iii) Vérifier que l'application $N \smallsetminus \{1\} \longrightarrow X \smallsetminus \{x_0\}, n \mapsto nx_0$, est bien définie et bijective.

(iv) En déduire que l'action par conjugaison de G_{x_0} sur $N \smallsetminus \{1\}$ est $(k-1)$-transitive.

(v) Conclure.

Partie III : deux applications du critère de Rotman

(i) Montrer que la simplicité de A_5 entraîne celle de A_n pour $n \geqslant 6$.

É. Mathieu a construit un sous-groupe G de S_{24} agissant 5-transitivement sur $\{1, 2, \ldots, 24\}$ et vérifiant $G_1 \cap G_2 \cap G_3 \simeq \mathrm{PSL}_3(\mathbb{F}_4)$, où G_i désigne le stabilisateur dans G de l'élément $i \in \{1, 2, \ldots, 24\}$ et $\mathbb{F}_4$ est un corps à 4 éléments. On note respectivement M_{24}, M_{23} et M_{22} les groupes G, G_1 et $G_1 \cap G_2$.

(ii) Montrer que M_{22}, M_{23} et M_{24} sont simples. [10]

Soient K un corps, V un K-espace vectoriel de dimension finie et u un endomorphisme de V. On rappelle que V_u désigne le $K[X]$-module de K-espace vectoriel sous-jacent V et vérifiant $Xv = u(v)$ pour tout $v \in V$. On note ${}^{\mathrm{t}}u$ l'endomorphisme du dual V^* de V défini par ${}^{\mathrm{t}}u(\varphi) = \varphi \circ u$ pour tout $\varphi \in V^*$ (*transposée* de u).

Problème 3. (Dualité, et actions non isomorphes de représentations de permutation associées isomorphes) *Soient K un corps, V un K-espace vectoriel de dimension finie $n \geqslant 1$, u un endomorphisme de V. On se propose d'abord de montrer que les $K[X]$-modules V_u et $(V^*)_{{}^{\mathrm{t}}u}$ sont isomorphes.*

(i) On suppose que le $K[X]$-module V_u est isomorphe à $K[X]/(P)$ avec $P \in K[X]$ unitaire. Montrer qu'il existe $v \in V$ tel que $v, Xv, X^2v, \ldots, X^{n-1}v$ est une base de V, et aussi $Pv = 0$.

(ii) (suite) Montrer que le $K[X]$-module $(V^*)_{{}^{\mathrm{t}}u}$ est monogène, et $P\psi = 0$ pour tout $\psi \in V^*$. On pourra considérer une forme linéaire ϕ sur V vérifiant $\phi(X^i v) = 0$ pour $0 \leqslant i < n-1$, et $\phi(X^{n-1}v) = 1$.

(iii) (suite) En déduire un isomorphisme de $K[X]$-modules $(V^*)_{{}^{\mathrm{t}}u} \simeq K[X]/(P)$.

(iv) On suppose $V = \oplus_{i=1}^r V_i$ avec $V_i \subset V$ un sous-espace vectoriel stable par u pour tout $i = 1, \ldots, r$, et on pose $u_i = u_{|V_i}$. Vérifier que l'on a un isomorphisme de $K[X]$-modules $\oplus_{i=1}^r (V_i^*)_{{}^{\mathrm{t}}u_i} \simeq (V^*)_{{}^{\mathrm{t}}u}$.

(v) Conclure.

(vi) (Application) Montrer que toute matrice dans $\mathrm{M}_n(K)$ est semblable à sa transposée.

On suppose désormais que K est un corps fini. On note X l'ensemble des droites vectorielles de K^n et Y celui des hyperplans de K^n. Ces deux ensembles sont munis d'une action naturelle du groupe $G = \mathrm{GL}_n(K)$.

10. Ce sont les trois plus gros groupes simples sporadiques découverts par Mathieu.

(vii) Montrer que tout $g \in G$ a le même nombre de points fixes dans X et dans Y.

(viii) En déduire que les $\mathbb{C}[G]$-modules $\mathbb{C}X$ et $\mathbb{C}Y$ sont isomorphes.

(ix) Montrer que toutefois, les actions de G sur X et sur Y ne sont pas isomorphes pour $n \geqslant 3$.

Problème 4. (Groupes de l'année) *On se propose de montrer qu'à isomorphisme près, il existe exactement 6 groupes d'ordre $2024 = 2^3 \cdot 11 \cdot 23$ possédant un élément d'ordre 8. Soit*[11] *G un groupe d'ordre 2024.*

(i) Montrer que G possède un unique sous-groupe distingué V d'ordre 23.

(ii) En déduire que G possède un sous-groupe Q d'ordre 88, puis que l'on a $G = V \rtimes Q$.

(iii) Montrer que Q possède un unique sous-groupe distingué O d'ordre 11.

(iv) En déduire $Q = O \rtimes H$ pour tout 2-Sylow H de Q.

(v) Montrer que le groupe $\operatorname{Aut} O$ est cyclique d'ordre 10, et a un unique élément d'ordre 2, à savoir $x \mapsto x^{-1}$. Montrer que le groupe $\operatorname{Aut} V$ possède exactement 4 sous-groupes, cycliques et engendrés par les automorphismes $v \mapsto v^i$ avec $i \in \{1, -1, 2, -2\}$. On donne la congruence $2^{11} \equiv 1 \bmod 23$.

On suppose désormais que G possède un élément d'ordre 8, et on fixe un 2-Sylow H de Q.

(vi) Montrer $H \simeq \mathbb{Z}/8\mathbb{Z}$.

On fixe dans ce qui suit un générateur h de H.

(vii) En considérant un morphisme de groupes $H \to \operatorname{Aut} O$ bien choisi, montrer que soit Q est abélien, soit on a $hxh^{-1} = x^{-1}$ pour tout $x \in O$.

(viii) Montrer que si Q est abélien, il est cyclique.

(ix) On suppose Q cyclique. Montrer qu'il existe un générateur g de Q, et $i \in \{1, -1, 2, -2\}$, tels que pour tout $v \in V$ on a $gvg^{-1} = v^i$.

(x) On suppose Q non cyclique. Montrer qu'il existe $i \in \{1, -1\}$ tel que pour tout $v \in V$, et tout $x \in O$, on a $hvh^{-1} = v^i$ et $xvx^{-1} = v$.

(xi) Conclure.

7. Corrigé du partiel 2021-2022

Problème 1. (i) On a $|X| = \binom{4}{2} = 6$. Un 4-cycle dans S_4 s'écrit de manière unique sous la forme $(1\,a\,b\,c)$ avec $\{a, b, c\} = \{2, 3, 4\}$. Il en a donc $|Y| = 3! = 6$.

(ii) L'action de $G = \mathrm{S}_4$ sur $\{1, 2, 3, 4\}$ est 2-transitive, donc celle sur X est transitive. Un élément $\sigma \in \mathrm{S}_4$ fixe $x = \{i, j\}$ ssi on a $\sigma(\{i, j\}) = \{i, j\}$. On note les deux autres élément de $\{1, 2, 3, 4\}$ par k et l. On a donc manifestement $G_x = \{1, (i\,j), (k\,l), (i\,j)(k\,l)\}$. On peut aussi dire que l'inclusion $\supset$ est claire et que pour $x \in X$ on a $|G_x| = |G|/|\mathrm{O}_x| = |G|/|X| = 24/6 = 4$.

(iii) On sait que le conjugué d'un k-cycle est un k-cycle, et que deux k-cycles de S_n sont conjugués (par k-transitivité), donc l'action par conjugaison de S_4 sur Y est bien définie et transitive. Le raisonnement ci-dessus montre que pour $c \in Y$ on a $|G_c| = 4$. On conclut car on a $ccc^{-1} = c$, et donc $\langle c \rangle \subset G_c$.

11. On utilisera la lettre V pour rappeler Vingt-trois, Q pour Quatre-vingt-huit, O pour Onze et H pour huit.

(iv) Vu la description des G_x pour $x \in X$, il est clair qu'aucun élément non trivial de S_4 n'est dans $G_{\{i,j\}}$ pour toute partie à 2 éléments $\{i,j\} \in X$. Par exemple, pour i,j,k distincts on a $G_{\{i,j\}} \cap G_{\{i,k\}} = \{1\}$. De même, pour $c = (i\,j\,k\,l) \in Y$ on a $G_c = \{1, (i\,j\,k\,l), (i\,k)(j\,l), (i\,l\,k\,l)\}$ et donc $G_c \cap G_{c'} = \{1\}$ avec $c' = (i\,j\,l\,k)$.

(v) L'action de $G = \mathrm{S}_3$ sur $Z = G$ (lui-même) par translations à gauche convient (action de Cayley). Elle est bien transitive car pour $g, g' \in G$, on a $g' = (g'g^{-1})g$. Ses stabilisateurs sont triviaux car pour $h \in G$, on a $gh = h$ si, et seulement si, $g = 1$.

(vi) On a un morphisme surjectif $f : \mathrm{S}_4 \to \mathrm{S}_3$ de noyau K_4. On en déduit que $(g,z) \mapsto f(g)z, \mathrm{S}_4 \times Z \to Z$, est une action transitive de S_4 sur l'ensemble à 6 éléments S_3. L'élément $g \in \mathrm{S}_4$ stabilise $z \in Z$ si, et seulement si, $f(g) \in \mathrm{S}_3$ stabilise z, et donc $f(g) = 1$ par la question précédente.

(vii) Si G est d'ordre 4 alors soit G a un élément d'ordre 4, et donc $G \simeq \mathbb{Z}/4\mathbb{Z}$, soit tout élément de G est d'ordre 1 ou 2 (Lagrange). Mais $g^2 = 1$ pour tout $g \in G$ implique G abélien car alors $[g,h] = ghgh = (gh)^2 = 1$ pour tout g,h. Dans ce cas, G est un groupe abélien 2-élémentaire, et donc $\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(viii) Un élément $\sigma \in \mathrm{S}_4$ commute avec la transposition $(i\,j)$ si et seulement si on a $(\sigma(i)\,\sigma(i)) = \sigma(i\,j)\sigma^{-1} = (i\,j)$, ou ce qui revient au même, si et seulement si $\sigma(\{i,j\}) = \{i,j\}$. Le commutant cherché est donc $G_{\{i,j\}}$.

(ix) Si H est cyclique d'ordre 4, il est engendré par un élément d'ordre 4 dans S_4. Vu les types possibles d'éléments (4, 3 + 1, 2 + 2, 2 + 1 + 1, 1 + 1 + 1 + 1), les éléments d'ordre 4 de S_4 sont les 4-cycles. On a donc $H = G_c$ pour un $c \in Y$ d'après la question (ii). Sinon H ne contient que des éléments d'ordre 1 ou 2 et on a $H \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Un élément d'ordre 2 de S_4 est soit une transposition, soit une double-transposition. Si H ne contient aucune transposition, on a nécessairement $H = \mathrm{K}_4 = \{1, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$. Si H contient $(i\,j)$, on a H inclus dans le commutant de $(i\,j)$ (car H est commutatif), puis $H = G_{(i\,j)}$ par la question précédente.

(x) Une action transitive de $G = \mathrm{S}_4$ sur un ensemble à 6 éléments a ses stabilisateurs qui sont des sous-groupes d'ordre $|G|/6 = 4$. De plus, par un résultat du cours, deux actions transitives de G sont isomorphes si, et seulement si, elles possèdent un stabilisateur en commun. La question précédente, ainsi que (ii), (iii) et (vi), montrent donc que tout action de G sur un ensemble à 6 éléments est isomorphe à X, Y ou Z. Ces actions sont non isomorphes entre elles car les stabilisateurs de X, Y et Z sont tous différents : ceux de Y contiennent un 4-cycle, ceux de X une transposition, et ceux non triviaux de Z uniquement des double-transpositions.

(xi) La première ligne représente les parties à 2 éléments de $\{1,2,3,4\}$: c'est X. La seconde représente les 4-cycles de S_4, c'est Y. La troisième ligne définit manifestement une action transitive de S_4 telle que les doubles transpositions agissent trivialement, c'est donc l'action de noyau K_4.

(xii) Soit H le stabilisateur dans S_4 du pentagone P contenant le 5-cycle $(1\,2\,3\,4\,5)$ (sans poisson dans l'illustration du cours). C'est l'ensemble des $\sigma \in \mathrm{S}_4$ tels que $(\sigma(1)\,\sigma(2)\,\sigma(3)\,\sigma(4)\,5)$ est l'un des quatre 5-cycles de $\langle(1\,2\,3\,4\,5)\rangle$. Le cycle $(1\,2\,3\,4\,5)$ correspond à $\sigma = \mathrm{id}$, le cycle $(4\,3\,2\,1\,5)$ à $\sigma = (1\,4)(3\,2)$, le cycle $(3\,1\,4\,2\,5)$ à $\sigma = (1\,3\,4\,2)$, et le cycle $(2\,4\,1\,3\,5)$ à $\sigma = (1\,2\,4\,3)$. En particulier, H est d'ordre 4, donc l'orbite du pentagone P a $6 = 24/4$ éléments : l'action est transitive. On a reconnu que H est le stabilisateur du 4-cycle $(1\,2\,4\,3)$ dans Y. C'est donc l'action du milieu.

Problème 2. (i) Le groupe $A \cap B$ est inclus dans A, qui est abélien car A est strict, donc on a $A \cap B \lhd A$, *i.e.* $A \subset \mathrm{N}_G(A \cap B)$. Par symétrie on a aussi $B \subset \mathrm{N}_G(A \cap B)$.

(ii) Le sous-groupe engendré par A et B est $\neq A$, sinon $B \subset A$ puis $B = A$ par maximalité de B. Il est donc alors égal à G par maximalité de A. On a donc $\mathrm{N}_G(A \cap B) = G$ par le (i), *i.e.* $A \cap B$ est distingué dans G. Comme $A \cap B \subset A \neq G$, on a $A \cap B = \{1\}$ car G est simple.

(iii) L'application int_g est un automorphisme du groupe G, elle envoit donc sous-groupe maximal sur sous-groupe maximal. La vérification que c'est une action est immédiate.

(iv) Par la formule orbite-stabilisateur, il suffit de montrer que le stabilisateur de A est A. Mais par définition c'est $\mathrm{N}_G(A)$, et on a $A \subset \mathrm{N}_G(A)$. Comme A est maximal, on a soit $A = \mathrm{N}_G(A)$, soit $\mathrm{N}_G(A) = G$ *i.e.* $A \lhd G$. Dans ce second cas, on a $A = \{1\}$ car G est simple. Mais $\{1\}$ n'est pas maximal, car pour $x \in G \neq \{1\}$ on a $\{1\} \subsetneq x \subsetneq G$ (la seconde inclusion est stricte car G n'est pas abélien). (Il faut faire attention à ce que $\mathbb{Z}/p\mathbb{Z}$ est simple et abélien !).

(v) Par le (iv), dans cette réunion il y a $|G|/|A|$ conjugués distincts de A. Ces conjugués sont isomorphes entre eux, donc ont même cardinal $|A|$. Les intersections 2 à 2 sont triviales d'après le (ii). Comptant l'élément neutre à part, et pour chacun de ces conjugués les $|A| - 1$ éléments non triviaux, on obtient la formule de l'énoncé.

(vi) Pour $n = |G|$ et $a = |A|$ on a $1 + \frac{n}{a}(a-1) = n + 1 - n/a$ avec $a|n$ et $n > a$, d'où $n/a \geqslant 2$ et $|\mathscr{C}(A)| < n$. On a déjà vu que $\{1\}$ n'est pas maximal plus haut. On en déduit $a \geqslant 2$, puis $\frac{n}{a}(a-1) = n(1-1/a) \geqslant \frac{n}{2}$.

(vii) Si B n'est pas inclus dans $\mathscr{C}(A)$, on a en particulier $B \neq gAg^{-1}$ pour tout $g \in G$, puis $hBh^{-1} \neq gAg^{-1}$ pour tout $h, g \in G$, ce qui implique $hBh^{-1} \cap gAg^{-1} = \{1\}$ par le (ii). Le résultat s'en déduit.

(viii) On sait que $\mathscr{M}$ est non vide (on a $G \neq \{1\}$, donc on peut considérer un sous-groupe maximal contenant 1). Soit $A \in \mathscr{M}$. On a $\mathscr{C}(A) \neq G$ par le (vi). Soit $g \notin \mathscr{C}(A)$. On a $\langle g \rangle \neq G$ car G n'est pas abélien. Ainsi, $\langle g \rangle$ s'inclut dans un sous-groupe maximal B, et on a $g \in B \smallsetminus \mathscr{C}(A)$. On a donc $|\mathscr{C}(A) \cup \mathscr{C}(B)| - 1 = |\mathscr{C}(A)| - 1 + |\mathscr{C}(B)| - 1$ par le (vii), mais cette quantité est $\geqslant |G| > |G| - 1$ par le (vi) : une contradiction.

Problème 3. Partie I

(i) C'est la formule $\varphi(\prod_i p_i^{m_i}) = \prod_i p_i^{m_i - 1}(p_i - 1)$.

(ii) Si on a $n = p^2 m$, le groupe $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, d'ordre n, n'est pas cyclique, car il contient $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \{0\} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ qui n'est pas cyclique (son min est 2).

(iii) On a $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \simeq (\mathbb{Z}/q\mathbb{Z})^\times$, qui est d'ordre $q-1$. Par Gauss ou Cauchy, $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ admet donc un élément d'ordre p, disons τ. Le morphisme $\mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}), \overline{k} \mapsto \tau^k$, est alors bien défini et non trivial.

(iv) Soit $\varphi : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ un morphisme non trivial, *i.e.* $\tau = \varphi(\overline{1})$ est un automorphisme non trivial de $\mathbb{Z}/q\mathbb{Z}$. On pose $G = \mathbb{Z}/q\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z}$. Soit $x \in \mathbb{Z}/q\mathbb{Z}$ tel que $\tau(x) \neq x$. Alors les éléments $a = (x, 0)$ et $b = (0, \overline{1})$ ne commutent pas : on a $ab = (x, \overline{1})$ et $ba = (\tau(x), \overline{1})$. (Plus généralement, $A \rtimes_\psi B$ est abélien si, et seulement si, A et B sont abéliens et ψ est trivial.)

(v) Si G est non abélien d'ordre m, alors $G \times \mathbb{Z}/r\mathbb{Z}$ est non abélien d'ordre mr (il contient le groupe $G \times \{0\}$ qui est isomorphe à G).

(vi) Supposons que tout groupe d'ordre n est cyclique. Le (ii) montre que n est sans facteur carré. Le (iv) montre que si $pq|n$ alors p ne divise pas $q - 1$. Le (i) conclut $(n, \varphi(n)) = 1$.

(vii) Par Cauchy il existe x_i dans G d'ordre p_i. Les p_i sont deux à deux premiers entre eux. Le groupe G est commutatif. Par un lemme du cours (Cauchy encore !) le produit des x_i est d'ordre $p_1 p_2 \dots p_r$, donc G est cyclique.

(viii) Soit $f : G \to G'$ avec $a = |G|$ premier à $b = |G'|$. On a $\operatorname{Im} f$ sous-groupe de G', donc $|\operatorname{Im} f|$ divise b. On a $|\operatorname{Im} f||\ker f| = |G|$ donc $|\operatorname{Im} f|$ divise a. On a $(a, b) = 1$ donc $|\operatorname{Im} f| = 1$, *i.e.* f est trivial.

Partie II

(i) Par Lagrange, un sous-groupe strict H de G est d'ordre $d < n$ avec $d|n$. Mais par le (i) un tel d vérifie $(d, \varphi(d)) = 1$. Donc H est cyclique par hypothèse de récurrence, donc abélien. Par le Problème 2, G n'est donc pas simple, ou il est abélien.

(ii) On sait que $G \to \operatorname{Aut}(G), g \mapsto \operatorname{int}_g$, est un morphisme de groupes. Comme H est distingué dans G, il est stable par int_g pour tout $g \in G$. On en déduit que $f : G \to \operatorname{Aut}(H), g \mapsto (\operatorname{int}_g)_{|H}$, est un morphisme de groupes. Mais on a vu ci-dessus $H \simeq \mathbb{Z}/d\mathbb{Z}$ avec $d|n$ et $d < n$ car H est strict. On a donc $\operatorname{Aut}(H) \simeq \operatorname{Aut}(\mathbb{Z}/d\mathbb{Z})(\simeq \mathbb{Z}/d\mathbb{Z})^\times$. Ainsi, G est de cardinal n et $\operatorname{Aut}(H)$ de cardinal $\varphi(d)$, qui est premier à n par le (i). Donc le morphisme f est trivial par le (viii). Cela veut dire que $\operatorname{int}_g(h) = ghg^{-1} = h$ pour tout $g \in G$ et $h \in H$: on a $H \subset \mathrm{Z}(G)$.

(iii) C'est évident si G est abélien. Sinon G n'est pas simple, et donc $\mathrm{Z}(G)$ non trivial par la question précédente. Ainsi, le groupe $G/\mathrm{Z}(G)$ est d'ordre $d|n$ avec $d < n$. Un tel d vérifie $(d, \varphi(d)) = 1$ par le (i) : le groupe $G/\mathrm{Z}(G)$ est donc cyclique par hypothèse de récurrence.

(iv) Par l'Exercice 2.27 Chap. 2 (i), on sait que $G/\mathrm{Z}(G)$ monogène implique G abélien. Mais par le (vii) Partie 1, G est alors cyclique, ce qu'il fallait démontrer.

(v) On a $255 = 5 \cdot 51 = 3 \cdot 5 \cdot 17$ et $\varphi(255) = 2 \cdot 4 \cdot 16$ premier à 255.

(vi) Ce sont les entiers de la forme $n = \prod_i p_i^{\alpha_i}$ avec $\alpha_i \leqslant 2$ pour tout i, et p_i ne divise pas $p_j^{\alpha_i} - 1$ pour $i \neq j$. La démonstration n'était pas demandée ! Montrons simplement que si tout groupe d'ordre n est abélien alors n est de la forme indiquée (l'autre sens, plus difficile, est démontré dans le Complément §7 Chap. 6). Soit p un nombre premier. Le sous-groupe des unipotents supérieurs de $\mathrm{GL}_3(\mathbb{Z}/p\mathbb{Z})$ est non commutatif d'ordre p^3. Ainsi, si p^3 divise n il existe un groupe non abélien d'ordre n (considérer le produit direct avec un groupe cyclique d'ordre n/p^3). Soient p, q premiers distincts avec $pq|n$. On a déjà vu que pour $p \mid q - 1$, il existe un groupe non abélien d'ordre n. Supposons donc que $p^2 q$ divise n. Si $q \mid p^2 - 1$ il existe un groupe non abélien d'ordre $p^2 q$ (et donc un groupe non abélien d'ordre n). En effet, on a $\operatorname{Aut}((\mathbb{Z}/p\mathbb{Z})^2) \simeq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ d'ordre $(p^2 - 1)(p^2 - p) = p(p^2 - 1)(p - 1)$, donc on peut trouver un morphisme non trivial $\varphi : \mathbb{Z}/q\mathbb{Z} \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, et le groupe $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes_\varphi \mathbb{Z}/q\mathbb{Z}$ fait l'affaire.

8. Corrigé du partiel 2022-2023

Problème 1. (i) On a $T \neq T'$ car t et t' sont distinctes. Il y a deux cas. Soit $T \cap T' = \varnothing$, auquel cas $tt' = t't$ car deux permutations à supports disjoints commutent. Soit $|T \cap T'| = 1$, et donc $T = \{a, b\}$ et $T' = \{a, c\}$ avec a, b, c distincts. Dans ce cas, on a $tt' = (a\,b)(a\,c) = (a\,c\,b)$ et $t't = (a\,c)(a\,b) = (a\,b\,c)$, et donc tt' et $t't$ diffèrent sur a.

(ii) On pose $t_i = (i\ i+1)$. Par le (i) c'est une suite alignée. Par le cours, elle engendre S_n.

(iii) Par récurrence sur r. Il n'y a rien à montrer pour $r = 1$, et pour $r = 2$ c'est le (i) car t_1 et t_2 ne commutent pas. On suppose $r \geqslant 3$. Soient $a_1, a_2, \ldots, a_r$ distincts avec $t_i = (a_i\ a_{i+1})$ pour tout $i = 1, \ldots, r-1$. Par hypothèse et $r \geqslant 3$, t_r commute avec $t_1, \ldots, t_{r-2}$, et donc le support de t_r ne contient aucun des a_i avec $1 \leqslant i \leqslant r-1$ par le (i). Toujours par hypothèse, t_r ne commute pas avec t_{r-1}, donc le support de t_r contient soit a_r, soit a_{r-1}, par le (i). Mais on a vu qu'il ne contient pas a_{r-1}. Le support de t_r est donc de la forme $\{a_r, x\}$ avec $x \neq a_i$ pour tout $i \leqslant r$. On pose $a_{r+1} = x$.

(iv) Soit s une transposition dans S_n. Comme les transpositions sont conjuguées dans S_n, il existe $\sigma \in \mathrm{S}_n$ avec $s = \sigma t \sigma^{-1}$. On en déduit $f(s) = f(\sigma) f(t) f(\sigma)^{-1}$. Comme $f(t)$ est une transposition, l'élément $f(s)$ qui lui est conjugué en est aussi une.

(v) On pose $s_i = (i\ i{+}1)$ pour $1 \leqslant i < n$. On a $s_i s_j = s_j s_i$ si, et seulement si, $|i-j| > 1$ par le (ii). Par le (vi), $t_i := f(s_i)$ est une transposition pour tout $1 \leqslant i < n$. Comme f est bijective, on a $t_i t_j = f(s_i s_j) = f(s_i s_j) = t_j t_i$ si, et seulement si, $|i-j| > 1$. Par le (iii), il existe n éléments distincts a_1, a_2, $\ldots$, a_n de $\{1, \ldots, n\}$ avec $t_i = (a_i\, a_{i+1})$ pour $i = 1, \ldots, r$. Ainsi, l'application $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}, i \mapsto a_i$, est dans S_n. Par la formule de conjugaison des cycles, on a $f(s_i) = \sigma s_i \sigma^{-1}$. Comme les s_i engendrent S_n, on constate $f = \mathrm{int}_\sigma$.

(vi) On suppose $t = (a\, b)$. Soit $\sigma \in \mathrm{S}_n$. On a $\sigma t \sigma^{-1} = (\sigma(a)\, \sigma(b))$. On en déduit que $\sigma t \sigma^{-1} = t$ si, et seulement si, $\sigma(\{a, b\}) = \{a, b\}$. Un tel σ préserve automatiquement le complémentaire I de $\{a, b\}$ dans $\{1, \ldots, n\}$. L'application $\mathrm{C}(t) \to \mathrm{S}_{\{a,b\}} \times \mathrm{S}_I, \sigma \mapsto (\sigma_{|\{a,b\}}, \sigma_I)$, est donc bijective. On conclut car c'est un morphisme de groupes et on a $\mathrm{S}_{\{a,b\}} \simeq \mathrm{S}_2$, ainsi que $\mathrm{S}_I \simeq \mathrm{S}_{n-2}$.

(vii) L'ordre d'une permutation est le ppcm des longueurs des cycles de sa décomposition en cycles. Si ce ppcm est 2, c'est que tous ces cycles sont de longueur 2 (et qu'il y en a au moins 1).

(viii) On a clairement $D \subset \mathrm{C}(s)$. Comme les s_i commutent et sont de carré 1, le groupe D est abélien 2-élémentaire. C'est donc un $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel. Les t_i en constituent une base. En effet, ils sont générateurs par définition. Supposons que l'on a une relation $\prod_{i \in I} t_i = \mathrm{id}$ avec $I \subset \{1, \ldots, k\}$. Cela force $I = \varnothing$ car les t_i sont a supports disjoints.

(ix) Pour $\sigma \in \mathrm{C}(s)$ on a $s = \sigma s \sigma^{-1} = (\sigma s_1 \sigma^{-1})(\sigma s_2 \sigma^{-1}) \cdots (\sigma s_n \sigma^{-1})$ et les $\sigma s_i \sigma^{-1}$ sont des transpositions à supports disjoints (images des supports des s_i par σ, par le cours). Par unicité de la décomposition en cycles, les ensembles des s_i et des $\sigma s_i \sigma^{-1}$ coïncident. On a donc $\sigma D \sigma^{-1} = \langle \sigma s_1 \sigma^{-1}, \ldots, \sigma s_k \sigma^{-1} \rangle = D$.

(x) On a $s \in \mathrm{K}_4$. Comme K_4 est abélien, on a donc $\mathrm{K}_4 \subset \mathrm{C}(s)$. On conclut car $s_1 \in \mathrm{C}(s) \smallsetminus \mathrm{K}_4$.

(xi) Regardons le morphisme surjectif $f : \mathbb{Z}/2\mathbb{Z} \times \mathrm{S}_m \to \mathrm{S}_m$. Soit H un sous-groupe distingué de $\mathbb{Z}/2\mathbb{Z} \times \mathrm{S}_m$ isomorphe à $(\mathbb{Z}/2\mathbb{Z})^k$. Comme f est surjectif, le sous-groupe $H' = f(H)$ est distingué dans S_m. Par le cours, c'est donc $\{1\}$, A_n, S_n, ou le sous-groupe K_4 dans le cas particulier $m = 4$. Mais on a $H \cap \ker f \subset \mathbb{Z}/2\mathbb{Z} \times \{0\}$, et donc $|H \cap \ker f| = 1$ ou 2. On en déduit que $H' \simeq H/(H \cap \ker f)$ est d'ordre 2^k ou 2^{k-1}, et donc $H' \neq \{1\}$. Pour $m \geqslant 3$, cela exclut S_m et A_m (leurs ordres sont multiples de 3). La seule possibilité est donc $m = 4$ et $H' = \mathrm{K}_4$.

(xii) Soit f un automorphisme de S_n. Soit t une transposition. Comme f est un isomorphisme, l'élément $s = f(t) \in \mathrm{S}_n$ est d'ordre 2. Par le (vii), s est un produit de k transpositions à supports disjoints par le (vii). On va montrer que pour $n \neq 6$ on a nécessairement $k = 1$, ce qui concluera par le (iv) et (v).

Noter que f induit aussi un isomorphisme $\mathrm{C}(t) \xrightarrow{\sim} \mathrm{C}(s)$, car pour $\tau \in \mathrm{S}_n$ on a $\tau t = t\tau \iff f(\tau) s = s f(\tau)$. Par le (vii), on a $\mathrm{C}(t) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathrm{S}_{n-2}$, et on

sait aussi que $\mathrm{C}(t) \simeq \mathrm{C}(s)$ possède un sous-groupe distingué isomorphe à $(\mathbb{Z}/2\mathbb{Z})^k$. Supposant $k \geqslant 2$, le (xi) montre $m = n-2 = 2$ ou $m = n-2 = 4$. On peut donc supposer $n = 4$ et $k = 2$. Mais dans ce cas on a $|\mathrm{C}(t)| = 4$ et $|\mathrm{C}(s)| > 4$ par le (x) : une contradiction.

(xii) On rappelle que l'action de S_5 sur les 6 pentagones mystiques est transitive. Numérotant arbitrairement ces 6 pentagones, on en déduit un morphisme de groupes $f : \mathrm{S}_5 \to \mathrm{S}_6$ dont l'image H agit transitivement sur $\{1, \dots, 6\}$. D'après le cours on sait qu'une action transitive de S_n sur $m > 2$ éléments avec $n > 4$ est fidèle (car les sous-groupes distingués d'un tel S_n sont $1, \mathrm{A}_n$ et S_n). On en déduit que f induit un isomorphisme $\mathrm{S}_5 \simeq H$.

(xiii) (proche d'un argument vu en TD) Soient $G = \mathrm{S}_6$ et $X = G/H$ (ensemble des classes à gauche). On a $|H| = 5!$ et donc $|X| = |G|/|H| = 6!/5! = 6$. Le groupe G agit transitivement par translations sur l'ensemble X. D'après le cours, on sait qu'une action transitive de S_n sur $m > 2$ éléments avec $n > 4$ est fidèle. Le groupe $G = \mathrm{S}_6$ agit donc fidèlement sur X. Le sous-groupe $H \subset G$ fixe le point $H \in X$. Numérotons les éléments de X en attribuant à $H \in X$ le numéro 1, et arbitrairement les 5 autres. Le morphisme associé à l'action induit alors un morphisme injectif $f : \mathrm{S}_6 \to \mathrm{S}_6$ avec $f(H) \subset \{\sigma \in \mathrm{S}_6 \,|\, \sigma(1) = 1\}$. Mais f est bijectif, car injectif d'un semble fini dans lui-même : c'est un automorphisme de S_6.

(xiv) Notons Γ_i le stabilisateur dans S_6 de l'élément i de $\{1, \dots, 6\}$ pour l'action naturelle. On a $f(H) \subset \Gamma_1$ par le (xiii). Supposons $f = \mathrm{int}_\tau$ avec $\tau \in \mathrm{S}_6$. On en déduit $\tau H \tau^{-1} \subset \Gamma_1$ puis $H \subset \tau^{-1}\Gamma_1\tau = \Gamma_j$ avec $j := \tau^{-1}(1)$ (principe de conjugaison). Ainsi, H fixe l'élément $j \in \{1, \dots, 6\}$ pour l'action naturelle, et n'agit donc pas transitivement sur ce dernier.

(xv) Considérons l'application $f : \mathrm{S}_n \to \mathrm{Aut}\,\mathrm{S}_n$, $\sigma \mapsto \mathrm{int}_\sigma$. On a $\mathrm{int}_\sigma \circ \mathrm{int}_{\sigma'} = \mathrm{int}_{\sigma\sigma'}$ pour tout $\sigma, \sigma' \in \mathrm{S}_n$: l'application f est un morphisme de groupes. Son image $\mathrm{Int}\,\mathrm{S}_n$ est donc un sous-groupe de $\mathrm{Aut}\,\mathrm{S}_n$. La formule $g \circ \mathrm{int}_\sigma \circ g^{-1} = \mathrm{int}_{g(\sigma)}$ pour $\sigma \in \mathrm{S}_n$ et $g \in \mathrm{Aut}\mathrm{S}_n$ montre qu'il est distingué. Il ne reste qu'à vérifier que l'on a $\ker f = \{1\}$, c'est à dire que le centre de S_n est trivial. (Jusqu'ici, l'argument a déjà été vu en TD). Soit σ dans le centre de S_n. On a $\sigma(i\,j)\sigma^{-1} = (\sigma(i)\,\sigma(j)) = (i\,j)$ pour tout $i < j$, et donc σ préserve tous les couples $\{i, j\}$ avec $i \neq j$. Comme $n > 2$ cela montre $\sigma = 1$.

(xvi) Par unicité de la décomposition en cycles on a

$$|T_1| = \binom{6}{2} = 15, \quad |T_2| = \frac{1}{2!} \cdot \binom{6}{2} \cdot \binom{4}{2} = 45 \text{ et } |T_3| = \frac{1}{3!} \cdot \binom{6}{2} \cdot \binom{4}{2} \cdot \binom{2}{2} = 15.$$

(xvii) Pour k fixé, les éléments de T_k sont conjugués d'après le cours. On en déduit que pour tout i, il existe j tel que $f(T_i) \subset T_j$. Comme f est injective, on a forcément $f(T_2) = T_2$ par le (xvi), puis soit $f(T_1) = T_1$ et $f(T_3) = T_3$, soit $f(T_1) = T_3$ et $f(T_3) = T_1$. Dans le premier cas, f est intérieur par le (iv)-(v).

(xviii) Si f et g sont deux automorphismes de S_6 non intérieurs, on a $f \circ g(T_1) = f(g(T_1)) = f(T_3) = T_1$ d'après le (xvi), et donc $f \circ g$ est intérieur. Comme f^{-1} est aussi non intérieur, on en déduit $g \in f\,\mathrm{Int}\,\mathrm{S}_6$.

Problème 2. (i) Soient $a_1, \dots, a_n$ les facteurs invariants d'un tel groupe. On a $1 < a_1 \,|\, a_2 \,|\, \cdots \,|\, a_n$ et $4p = a_1 \dots a_n$. Comme $4p$ est sans facteur cube, on a $n \leqslant 2$, et comme p^2 ne divise pas $4p$ car p est impair, on a que p ne divise pas a_1. Les seules possibilités sont donc $n = 1$ et $a_1 = 4p$, ou $n = 2$ et $(a_1, a_2) = (2, 2p)$. Par le cours, il y a donc exactement deux groupes abéliens d'ordre p à isomorphisme près, à savoir $\mathbb{Z}/4p\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2p\mathbb{Z}$.

(ii) Soit Q d'ordre 4 non cyclique. On a $x^2 = 1$, et donc $x^{-1} = x$, pour tout $x \in Q$. On sait qu'un tel Q est abélien car on a $xy = x^{-1}y^{-1} = (yx)^{-1} = yx$. Il est donc abélien élémentaire, isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$.

(iii) Soit N' un sous-groupe de G d'ordre n. Regardons la projection canonique $\pi : G \to G/N$. Pour $x \in N'$ on a $x^n = 1$ par Lagrange, et donc $\pi(x)^n = 1$. Mais on a aussi $m = |G/N|$ et donc $\pi(x)^m = 1$ par Largrange. Ainsi, l'ordre de $\pi(x)$ divise n et m : c'est donc 1, puis $\pi(x) = 1$. On a montré $\pi(N') = 1$, et donc $N' \subset N$, puis $N' = N$.

(iv) Un groupe G d'ordre $2p$ contient un sous-groupe P d'ordre p par Cauchy. Il est d'indice 2 donc distingué. On a p impair, donc P est l'unique sous-groupe d'ordre p de G par le (iii).

(v) On a $x \in C$ et donc $|C| = 1$ si et seulement si, $\sigma x \sigma^{-1} = x$ pour tout $\sigma \in G$. Cela implique $\langle x \rangle \lhd G$ (et même que x est central). La formule orbite stabilisateur pour l'action de conjugaison de G sur C montre $4p = |G| = |C||G_x|$ où $G_x = \{g \in G \mid gx = xg\}$ est le centralisateur de x dans G. C'est un sous-groupe de G contenant $\langle x \rangle$. On a donc $p \mid |G_x|$ puis $|C| \mid 4$.

(vi) Soit H un sous-groupe distingué de G d'ordre $2p$. Alors H est d'indice 2 dans G, donc distingué dans G. Mais H est d'ordre $2p$, donc possède un unique sous-groupe d'ordre p, disons P, par le (iv). Pour $g \in G$, on a donc $gPg^{-1} \subset gHg^{-1} = H$, et donc $gPg^{-1} = P$ par l'unicité susmentionnée, car on a $|gPg^{-1}| = |P|$ (image de P par une bijection).

(vii) Revenans à la preuve du (ii), on a $|G_x| \neq 2p$ par le (vi), et on a vu $p \mid |G_x|$, on a donc soit $|G_x| = p$ et $|C| = 4$, soit $|G_x| = 4p$ et $|C| = 1$. Ce dernier cas est exclus par le (v). On a donc $|C| = 4$, et le noyau de l'action K de G sur C vérifie $K \subset G_x$ et $K \lhd G$. On a donc $|K| \mid |G_x| = p$ (Lagrange), puis $K = 1$ car G n'a pas de sous-groupe distingué d'ordre p.

(viii) Par le (vii), on a un morphisme injectif $G \to \mathrm{S}_4$. On a donc $4p = |G| \mid |\mathrm{S}_4| = 24$. On en déduit $p = 3$, $|G| = 12$. Un sous-groupe d'indice 2 de S_4 est forcément distingué, et égal à A_4 par le cours (ou plus généralement car le seul sous-groupe d'indice 2 de S_n est A_n, par un argument vu en TD).

(ix) Le sous-groupe $P \cap Q$ est trivial car son ordre divise $4 = |Q|$ et $p = |P|$ (Lagrange). On a $|P||Q| = 4p = |G|$. On en déduit que P et Q sont complément l'un de l'autre. Le morphisme de l'énoncé est bien défini car P est distingué dans G. Si ce morphisme est trivial, on a $pq = qp$ pour tout $p \in P$ et $q \in Q$. Mais P est abélien (car cyclique) et Q est aussi abélien par le (ii). Comme $G = PQ$ on aurait alors G abélien : absurde.

(x) Comme C est cyclique, il a au plus un élément d'ordre 2. Comme on a $v^2 = 1$ pour tout $v \in V$, et donc $f(v)^2 = 1$, on en déduit $|f(V)| \leqslant 2$. On en déduit que $\ker f$ est non trivial. On choisit v non nul dans $\ker f$, et on la complète en une base du $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel v, w de W pour répondre à la question.

(xi) On applique la question précédente à $V = Q$ et au morphisme $f : Q \to \mathrm{Aut}(P)$. C'est possible car on sait que l'on a $\mathrm{Aut}(P) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ et que ce dernier est cyclique par Gauss. Ainsi, il existe une base v, w de $Q^\sharp$ telle que $vxv^{-1} = x$ pour tout $x \in P$. Comme v et w commutent, le (ix) montre que v est dans le centre de G.

Posons $D = \langle v \rangle \simeq \mathbb{Z}/2\mathbb{Z}$ et $H = P\langle w \rangle$. Comme P est distingué dans G, H est un sous-groupe de G. Par le (ix), on a $|H| = 2p$ et $D \cap H = \{1\}$. On a vu que l'on a $dh = hd$ pour tout $d \in D$ et $h \in H$. Ainsi, G est produit direct interne de D et H. On a donc $G \simeq D \times H$. Le groupe H est d'ordre $2p$, et non abélien sinon G serait abélien. On sait par le cours que cela entraîne $H \simeq \mathrm{D}_{2p}$.

(xii) Soit g un générateur de $\mathbb{Z}/4\mathbb{Z}$. Se donner un morphisme $\mathbb{Z}/4\mathbb{Z} \to \operatorname{Aut}\mathbb{Z}/p\mathbb{Z}$ est la même chose que se donner l'image du générateur g, qui peut être n'importe quel élément $a \in \operatorname{Aut}\mathbb{Z}/p\mathbb{Z}$ vérifiant $a^4 = 1$ (propriété universelle du groupe quotient $\mathbb{Z}/4\mathbb{Z}$). On sait que tout automorphisme de $\mathbb{Z}/p\mathbb{Z}$ est de la forme $\varphi_k : x \mapsto kx$, avec $k \in (\mathbb{Z}/p\mathbb{Z})^\times$. On a $\varphi_k^4 = \varphi_{k^4} = 1$ si, et seulement si, $k^4 = 1$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$. Mais $(\mathbb{Z}/p\mathbb{Z})^\times$ n'a pas d'élément d'ordre 4, car sinon on aurait $4 \mid p-1$ par Lagrange. On a donc $k^4 = 1$ si, et seulement si, $k^2 = 1$, ou ce qui revient au même, $k = \pm 1$. L'unique morphisme non trivial $\mathbb{Z}/4\mathbb{Z} \to \operatorname{Aut}\mathbb{Z}/p\mathbb{Z}$ est donc celui envoyant g sur φ_{-1} (i.e. $x \mapsto -x$).

(xiii) On sait que G est produit semi-direct interne de P par Q par le (ix), pour un morphisme non trivial $Q \to \operatorname{Aut}P$. On a donc $G \simeq \mathbb{Z}/p\mathbb{Z} \rtimes_\beta \mathbb{Z}/4\mathbb{Z}$ avec $\beta : \mathbb{Z}/4\mathbb{Z} \to \operatorname{Aut}(\mathbb{Z}/p\mathbb{Z})$, et sans suivre précisément les isomorphismes choisis $P \simeq \mathbb{Z}/p\mathbb{Z}$ et $Q \simeq \mathbb{Z}/4\mathbb{Z}$ on sait que β est non trivial. On a donc $\beta = \alpha$ par le (xiii).

(xiv) Soit G un groupe non abélien d'ordre $4p$. On a montré que si G n'a pas de sous-groupe distingué d'ordre p, alors on a $p = 3$ et $G \simeq \mathrm{A}_4$ au (viii). Réciproquement, A_4 est bien d'ordre 12 et sans sous-groupe d'ordre 3 distingué.

On a aussi montré que si G a un sous-groupe distingué P d'ordre p, alors ce sous-groupe est unique par le (iii), que tout 2-Sylow Q de G est un complément de P par (ix), et qu'en particulier un tel Q est isomorphe à G/P. On a vu au (ii) qu'on a soit $Q \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, auquel cas on a $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathrm{D}_{2p}$ par le (xi), soit $Q \simeq \mathbb{Z}/4\mathbb{Z}$, auquel cas on a $G \simeq \mathbb{Z}/p\mathbb{Z} \rtimes_\alpha \mathbb{Z}/4\mathbb{Z}$ par le (xiii). On conclut car il est clair que $\mathbb{Z}/2\mathbb{Z} \times \mathrm{D}_{2p}$ possède $0 \times C$ pour sous-groupe distingué d'ordre p et pour complément $\mathbb{Z}/2\mathbb{Z} \times \langle \tau \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, et que $\mathbb{Z}/p\mathbb{Z} \rtimes_\alpha \mathbb{Z}/4\mathbb{Z}$ possède $\mathbb{Z}/p\mathbb{Z} \times \{0\}$ pour sous-groupe distingué d'ordre p et pour complément $\{0\} \times \mathbb{Z}4\mathbb{Z} \simeq \mathbb{Z}/4\mathbb{Z}$.

(xv) Pour $p \equiv 1 \bmod 4$, il existe exactement 4 élément $k \in (\mathbb{Z}/p\mathbb{Z})^\times$ tels que $k^4 = 1$, à savoir ± 1, et $\pm i$ avec $i^2 = -1$. L'argument du (xii) montre qu'il existe alors deux autres morphismes non triviaux $\beta_1, \beta_2 : \mathbb{Z}/4\mathbb{Z} \to \operatorname{Aut}(\mathbb{Z}/p\mathbb{Z})$, l'un envoyant le générateur g sur φ_i, et l'autre g sur $\varphi_{-i} = \varphi_i^{-1}$. L'argument du (iii) montre qu'une possibilité supplémentaire est que l'un des deux générateurs g de Q satisfait $ghg^{-1} = h^i$ pour tout $h \in P$ (l'autre générateur g^{-1} satisfaisant alors $g^{-1}hg = h^{-i}$). Par suivi des isomorphismes, on en déduit $G \simeq \mathbb{Z}/p\mathbb{Z} \rtimes_{\beta_1} \mathbb{Z}/4\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \rtimes_{\beta_2} \mathbb{Z}/4\mathbb{Z}$. C'est l'unique groupe à ajouter à la liste. Il admet un (unique) sous-groupe distingué P d'ordre p avec un groupe $\simeq \mathbb{Z}/4\mathbb{Z}$ pour complément, mais il n'est pas isomorphe à $G' = \mathbb{Z}/p\mathbb{Z} \rtimes_\alpha \mathbb{Z}/4\mathbb{Z}$. En effet, l'image de $G \to \operatorname{Aut}(P)$ contient un élément d'ordre 4, et pas celle de $G' \to \operatorname{Aut}(P)$.

(xvi) Soient $G = \mathrm{D}_{4p}$, $c = (1\,2\,\ldots\,2p)$ et $\tau = (1\ 2p)(2\ 2p-1)\cdots(p\ p+1)$. On sait que le sous-groupe $C = \langle c \rangle$ de G est distingué d'ordre $2p$ et $\tau c = c^{-1}\tau$. L'unique sous-groupe d'ordre p de C, engendré par c^2, est aussi distingué dans G. Mais C contient l'élément c^p qui est d'ordre 2. On a donc $\tau c^p = c^{-p}\tau = c^p\tau$. Ainsi, τ et c^p engendrent un sous-groupe de G isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. D'après le (xi) on a donc $\mathrm{D}_{4p} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathrm{D}_{2p}$.

9. Corrigé du partiel 2023-2024

Problème 1. (i) On a clairement $1 \in \mathrm{G}(\Gamma)$. Soient $g, h \in \mathrm{G}(\Gamma)$. Pour $\{i,j\} \in \Gamma$, on a $\{h(i), h(j)\} \in \Gamma$ car $h \in \mathrm{G}(\Gamma)$, puis $\{g(h(i)), g(h(j))\} = \{gh(i), gh(j)\} \in \Gamma$ car $g \in \mathrm{G}(\Gamma)$, et donc $gh \in \mathrm{G}(\Gamma)$. Reste à voir $g^{-1} \in \mathrm{G}(\Gamma)$. Méthode 1. Observer $g^{-1} = g^{n-1}$ avec $n = \operatorname{ord} g \geqslant 1$, et donc $g^{-1} \in \mathrm{G}(\Gamma)$ par ce qui a déjà été montré. Méthode 2. L'application $\Gamma \to \Gamma, X \mapsto g(X)$, est bien définie pour $g \in \mathrm{G}(\Gamma)$, et injective car $g(X) = g(Y)$ implique $X = Y$ en appliquant $g^{-1} \in \mathrm{S}_n$. Comme Γ est fini, elle est bijective, et donc $g(\Gamma) = \Gamma$, puis $g^{-1}(\Gamma) = \Gamma$.

(ii) Pour $j \in \mathrm{V}_\Gamma(i)$ on a $\{g(i), g(j)\} \in \Gamma$ et donc $g(j) \in \mathrm{V}_\Gamma(g(i))$. On en déduit $g(\mathrm{V}_\Gamma(i)) \subset \mathrm{V}_\Gamma(g(i))$. Appliqué à $g^{-1} \in \mathrm{G}(\Gamma)$, on a aussi $g^{-1}(\mathrm{V}_\Gamma(g(i)) \subset \mathrm{V}_\Gamma(g^{-1}g(i)) = \mathrm{V}_\Gamma(i)$, puis l'autre inclusion $\mathrm{V}_\Gamma(g(i)) \subset g(\mathrm{V}_\Gamma(i))$. On conclut en prenant le cardinal.

(iii) On a $\mathrm{G(A)} = \mathrm{S}_4$, $\mathrm{G(B)} \simeq \mathrm{S}_3$, $\mathrm{G(C)} \simeq \mathbb{Z}/2\mathbb{Z}$, $\mathrm{G(D)} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $\mathrm{G(E)} \simeq \mathrm{D}_8$.

(iv) (A) Le graphe A contient tous les $\{i, j\}$ avec $1 \leqslant i < j \leqslant 4$. On a donc $\mathrm{G}(\Gamma) = \mathrm{S}_4$.

(B) On a $\mathrm{v_B}(i) = 1$ pour $i = 1, 2, 3$ et $\mathrm{v_B}(4) = 3$. Par le (ii), pour $g \in \mathrm{G(B)}$ on a donc $g(4) = 4$ et $g(\{1, 2, 3\}) = \{1, 2, 3\})$. Comme n'importe quelle permutation $\sigma \in \mathrm{S}_4$ fixant 4 permute $\{1, 4\}$, $\{2, 4\}$ et $\{3, 4\}$, on constate que G est l'ensemble des $\sigma \in \mathrm{S}_4$ avec $\sigma(4) = 4$. Il est naturellement isomorphe à S_3. Par exemple, l'application $\mathrm{G}(B) \to \mathrm{S}_{\{1,2,3\}}, \sigma \mapsto \sigma_{|\{1,2,3\}}$, est un morphisme bijectif.

(C) On a $\mathrm{v_C}(1) = 1$, $\mathrm{v_C}(4) = 3$ et $\mathrm{v_C}(i) = 2$ pour $i = 2, 3$ D'après le (ii), G(C) fixe 1, 4, et préserve $\{2, 3\}$. Ses seuls éléments possibles sont donc 1 et $(2\,3)$, qui conviennent manifestement. On a donc $\mathrm{G(C)} = \langle (2\,3) \rangle \simeq \mathbb{Z}/2\mathbb{Z}$.

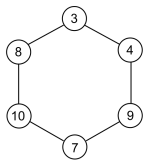
(D) Pour le graphe $\mathrm{D} = \{\{1, 2\}\}$ on a $g \in \mathrm{G(D)} \iff \{g(1), g(2)\} = \{1, 2\}$. On a donc $\mathrm{G(D)} = \{1, (12), (34), (12)(34)\}$. Ce groupe est isomorphe au groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. En effet, l'application $\mathrm{G(D)} \to \mathrm{S}_{\{1,2\}} \times \mathrm{S}_{\{3,4\}}, g \mapsto (g_{|\{1,2\}}, g_{|\{3,4\}})$, est un morphisme bijectif, et on a $\mathrm{S}_X \simeq \mathbb{Z}/2\mathbb{Z}$ pour $|X| = 2$.

(E) Plus difficile car on a $\mathrm{v}_\Gamma(i) = 2$ pour tout i. Par définition, on a $g \in \mathrm{G(E)} \iff g$ préserve ou échange $\{1, 2\}$ et $\{3, 4\}$. Le sous-groupe des $g \in \mathrm{G(E)}$ préservant $\{1, 2\}$ est le groupe G(D) déterminé ci-dessus. On a donc $\mathrm{G(E)} = \mathrm{G(D)} \cup (1\,4)(2\,3)\mathrm{G(D)}$, puis $|\mathrm{G(E)}| = 8$. On reconnaît que G(E) est un conjugué de D_8 dans S_4 : les éléments $(1\,3\,2\,4)$ et $(1\,4)(2\,3)$ sont dans G(E) et l'engendrent pour des raisons de cardinal.

(v) La figure de gauche étant invariante par la rotation centrale d'angle $2\pi/5$ (sens horaire), on constate que l'élément $c = (1\,2\,3\,4\,5)(6\,7\,8\,9\,10)$ est dans G(P). Il est d'ordre 5. En considérant de même, la rotation centrale d'angle $2\pi/3$ de la figure de droite, l'élément $t = (2\,5\,6)(3\,10\,9)(8\,7\,4)$ est dans G(P) et il est d'ordre 3.

(vi) Regardons l'orbite de 1 sous G(P). Elle contient les $c^i(1)$, $i \in \mathbb{Z}$, et donc $1, 2, 3, 4, 5$. Elle contient donc aussi $t(5) = 6$, puis les $c^j(6)$, $j \in \mathbb{Z}$, *i.e.* $6, 7, 8, 9, 10$. On a montré $\mathrm{O}_1 = \{1, \ldots, 10\}$: l'action est transitive.

(vii) L'élément $d := (3\,7)(4\,10)(8\,9)$ fixe $1, 2, 5, 6$, $\{1, 2\}$, $\{1, 5\}$, $\{1, 6\}$, et permute $\{5, 4\}$ et $\{5, 10\}$, $\{6, 8\}$ et $\{6, 9\}$, et $\{2, 3\}$ et $\{2, 7\}$. Les 6 arètes restantes forment le "sous-graphe" dont d est la symétrie centrale, ce qui montre $d \in \mathrm{G(P)}$. Réciproquement,



soit $g \in \mathrm{G(P)}_{\{1,2,5,6\}}$. Par le (ii), g permute les 3 voisins $1, 4, 10$ de $5 = g(5)$, et comme il fixe 1, on a $g(\{4, 10\}) = \{4, 10\}$. Quitte à remplacer g par dg on peut supposer $g(4) = 4$ et $g(10) = 10$. Comme 3 et l'unique voisin commun à 2 et 4, on a alors $g(3) = 3$, et on constate de même que g fixe 9 (unique voisin de 4 et 6), 8 (unique voisin de 3 et 10) et 7 (unique voisin de 2 et 10). On a donc $g = 1$, puis $\mathrm{G(P)}_{\{1,2,5,6\}} = \{1, d\}$.

(viii) Par la question (ii), le groupe $\mathrm{G(P)}_{\{1\}}$ agit naturellement sur l'ensemble $\{2, 5, 6\}$ des voisins de 1, ce qui définit donc un morphisme $f : \mathrm{G(P)}_{\{1\}} \to \mathrm{S}_{\{2,5,6\}}$. Par définition, on a $\ker f = \mathrm{G(P)}_{\{1,2,5,6\}}$. Il ne reste qu'à montrer que f est surjective. Mais on a vu $f(t) = (2\,5\,6)$. En considérant la symétrive verticale s de la figure de

droite, on a aussi $s \in \mathrm{G(P)}$ et $s = (8\,9)(3\,4)(2\,5)(7\,10)$, et donc $f(s) = (2\,5)$. On conclut car $(2\,5)$ et $(2\,5\,6)$ engendrent $\mathrm{S}_{\{2,5,6\}}$.

(ix) Par la formule orbite-stabilisateur, on a $|\mathrm{G(P)}| = |\mathrm{G(P)}_{\{1\}}||\mathrm{O}_1|$. On a vu $|\mathrm{O}_1| = 10$ au (vi). On a aussi $|\mathrm{G(P)}_{\{1\}}| = |\mathrm{Im}\, f||\ker f|$ avec $|\mathrm{Im}\, f| = |\mathrm{S}_3| = 6$ par le (viii) et $|\ker f| = |\mathrm{G(P)}_{\{1,2,5,6\}}| = 2$ par le (vii). On a donc bien $|\mathrm{G(P)}| = 10 \cdot 6 \cdot 2 = 120$.

(x) Soit T une tétrade contenant 1. Elle ne contient donc aucun voisin de 1 (*i.e.* 2, 5 et 6), et encore 3 éléments parmi $\{8, 3, 9, 4, 7, 10\}$. Comme $\{8, 3\}$, $\{9, 4\}$ et $\{7, 10\}$ sont dans P, T contient un et un seul élément de chacune de ces 3 paires. Si T contient 8, elle ne contient pas son voisin 10, et donc 7, et donc pas 9, et donc 4 : on a $T = \{1, 8, 7, 4\}$, qui convient bien. Dans l'autre cas, on a de même $T' = \{1, 3, 9, 10\}$. On a bien $T \cap T' = \{1\}$.

(xi) Le groupe G(P) préserve l'ensemble $\mathscr{T}$ des tétrades. Comme il agit transitivement sur $\{1, \ldots, 10\}$, on déduit du (viii) que tout $i \in \{1, \ldots, 10\}$ est dans exactement 2 tétrades. Il y a donc exactement $2 \cdot 10 = 20$ paires (T, i) avec $T \in \mathscr{T}$ et $i \in \{1, \ldots, 10\}$. Comme chaque tétrade a 4 éléments, on a donc aussi $20 = |\mathscr{T}| \cdot 4$, ce qui conclut.

(xii) Le groupe G(P) agit naturellement sur l'ensemble des parties à 4 éléments de $\{1, \ldots, 10\}$ en préservant les 5 tétrades. Soit $\varphi : \mathrm{G(P)} \to \mathrm{S}_{\mathscr{T}}$ le morphisme associé. Soit $i \in \{1, \ldots, 10\}$. Par le (vi) et le (x), il existe exactement deux tétrades T_i et T_i' contenant i, avec en outre $T_i \cap T_i' = \{i\}$. Pour $g \in \ker \varphi$, on a $g(T_i) = T_i$ et $g(T_i') = T_i'$, et donc $g(i) = i$, pour tout i, et donc $g = 1$. On conclut en composant φ avec un isomorphisme $\mathrm{S}_{\mathscr{T}} \simeq \mathrm{S}_5$.

(xiii) On a vu $|\mathrm{G(P)}| = 120 = |\mathrm{S}_5|$ au (ix), donc le morphisme injectif du (xii) est un isomorphisme.

(xiv) Soit C un ensemble a 5 éléments (« 5 points gris ») et D l'ensemble des parties à 2 éléments de C (« 2 points rouges parmi les 5 »). On a $|D| = \binom{5}{2} = 10$. Superposant la figure de l'énoncé et la figure gauche de P, on constate (Oh !) une bijection $b : D \xrightarrow{\sim} \{1, 2, \ldots, 10\}$ telle que

$$\forall X, Y \in D \text{ avec } X \neq Y, \text{ on a } X \cap Y = \varnothing \iff \{b(X), b(Y)\} \in \mathrm{P}.$$

Le groupe S_C agit naturellement sur D, donc sur $\{1, \ldots, 10\}$ via b. Le morphisme induit $\psi : \mathrm{S}_C \to \mathrm{S}_{10}$ a son image dans G(P), car pour $\sigma \in \mathrm{S}_C$ et $X, Y \subset C$, on a $X \cap Y = \varnothing \iff \sigma(X) \cap \sigma(Y) = \varnothing$. Pour conclure l'assertion d'injectivité, il suffit donc de voir que S_C agit fidèlement sur D. Supposons que $\sigma \in \mathrm{S}_C$ préserve toutes les parties à deux éléments de C. Soit $i \in C$. Choisissons $j, k \in C$ distincts et distincts de i. On a $\sigma(\{i, j\}) = \{i, j\}$, $\sigma(\{i, k\}) = \{i, k\}$, donc $\sigma(i) \in \{i, j\} \cap \{i, k\} = \{i\}$.

Problème 2. Partie I : Le cas des groupes abéliens

(i) D'après le cours, si G est cyclique d'ordre n engendré par g, les sous-groupes de G sont les $G^{(d)} = \langle g^d \rangle$ avec d divisant n. Ce groupe $G^{(d)}$ est cyclique d'ordre n/d.

(ii) Un groupe d'ordre p^2 avec p premier est sous-cyclique. En effet, si H est un sous-groupe strict de G on a $H = \{1\}$ ou $|H| = p$ par Lagrange, et donc H cyclique d'ordre p (cours). Le groupe (additif) $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ n'est pas cyclique, car on a $px = 0$ pour tout $x \in G$, et donc ses éléments sont d'ordre $\leqslant p$.

(iii) Par le théorème de structure on a un isomorphisme $f : G \xrightarrow{\sim} \mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \cdots \mathbb{Z}/a_n\mathbb{Z}$ avec $a_1|a_2|\cdots|a_n$ et $a_1 > 1$. Comme G n'est pas cyclique, on a $n \geqslant 2$. Soit p premier divisant a_1, et donc a_2. Pour $i = 1, 2$ le groupe cyclique $\mathbb{Z}/a_i\mathbb{Z}$ contient un sous-groupe cyclique C_i d'ordre p, engendré par la classe de a_i/p. Le sous-groupe $H = C_1 \times C_2 \times \{0\}^{n-2}$ de $\mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \cdots \mathbb{Z}/a_n\mathbb{Z}$ est isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, et $f^{-1}(H)$ convient.

(iv) Ce sont les groupes cycliques et ceux isomorphes à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ avec p premier. En effet, ces groupes conviennent par (i) et (ii). Réciproquement, si G est abélien sous-cyclique non cyclique, il contient un sous-groupe H avec $H \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Ce groupe est non cyclique par le (ii), donc non strict, i.e. $H = G$.

Partie II : Quelques propriétés des groupes sous-abéliens

(i) Un sous-groupe strict de H est un sous-groupe strict de G, donc abélien, et H est sous-abélien. Soit $\pi : G \to G/H$ la projection canonique (un morphisme de groupes). Si K est un sous-groupe strict de G/H alors par le cours $\pi^{-1}K$ est un sous-groupe strict de G, donc abélien, et on a $\pi(\pi^{-1}K) = K$. Comme l'image d'un groupe abélien par un morphisme de groupes est abélien, donc K est abélien.

(ii) Par le théorème de structure on a un isomorphisme $f : G \xrightarrow{\sim} G'$ avec $G' = \mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}$, $a_1|a_2|\cdots|a_n$, $n \geqslant 1$ et $a_1 > 1$. Soit p premier divisant a_1. Le groupe cyclique $\mathbb{Z}/a_1\mathbb{Z}$ possède un sous-groupe cyclique C d'ordre a_1/p (engendré par p). Ainsi, $H := C \times \mathbb{Z}/a_2\mathbb{Z} \times \cdots \mathbb{Z}/a_n\mathbb{Z}$ est un sous-groupe d'ordre $|G|/p$ de G', et le sous-groupe $f^{-1}(H)$ de G convient.

(iii) Soit G sous-abélien fini non trivial. On procède par récurrence sur $|G|$, le cas $|G| = 1$ étant vide. Si G est abélien, on conclut par le (ii). Sinon, par le résultat admis G possède un sous-groupe distingué H avec $\{1\} \neq H \neq G$. Par le (i), le groupe G/H est sous-abélien, et on a $1 < |G/H| = |G|/|H| < |G|$. Ainsi, G/H admet un sous-groupe distingué K d'indice premier p. Considérons le morphisme surjectif $\pi : G \to G/H$, dont les fibres sont de cardinal $|H|$. Par le cours, on a $\pi^{-1}(K) \lhd G$ et $|\pi^{-1}(K)| = |H||K| = |H|\frac{1}{p}|G/H| = |G|/p$.

(iv) Soit $\alpha \in \operatorname{Aut} H$ et $h \in H[n]$. On a $h^n = 1$ donc $1 = \alpha(h^n) = \alpha(h)^n$ puis $\alpha(h) \in H[n]$. Cela montre que $H[n]$ est caractéristique dans H. Soit p premier divisant $|H[n]|$. Par Cauchy, il existe $h \in H[n]$ d'ordre p. Mais alors $h^n = 1$ implique $p \mid n$.

(v) Par Bezout, il existe $u, v \in \mathbb{Z}$ avec $1 = au + bv$. Pour $h \in H$ on a donc $h = (h^b)^v(h^a)^u$. On en déduit d'abord $A \cap B = \{1\}$ car $h^a = h^b = 1$ implique $h = 1$. On en déduit aussi $H = AB$ car par Lagrange, on a $h^b \in H[a]$ et $h^a \in H[b]$. Ainsi, A et B sont complémentaires dans H, et donc $|H| = |A||B|$. Par le (v), les diviseurs premiers de $|A|$ (resp. $|B|$) divisent a (resp. b), on a donc nécessairement $|A| = a$ et $|B| = b$.

(vi) On a $1 = 1.1 \in AB$, $AB = BA$ car A est distingué dans H, et donc $ABAB = AABB = AB$, puis $(AB)^{-1} = (BA)^{-1} = A^{-1}B^{-1} = AB$. Ainsi, AB est un sous-groupe de H. D'après le cours, son ordre est $\frac{|A||B|}{|A \cap B|}$, donc divise $|A||B|$.

(vii) Par hypothèse, le groupe G/H est cyclique d'ordre premier q. Soit $z \in G$ tel que $\pi(z)$ est générateur de G/H. Écrivons $d = \operatorname{ord} z = q^n k$ avec k premier à q et $n \geqslant 0$. Alors $\pi(z^k) = \pi(z)^k$ engendre G/H (car k est premier à q) et z^k est d'ordre $d/k = q^n$. Ainsi, pour tout $g \in G$ il existe $j \in \mathbb{Z}$ avec $\pi(g) = \pi(z)^j$, puis $gz^{-j} \in H$, et donc $g \in H\langle z\rangle$. On a montré $G = H\langle z\rangle$.

(viii) Écrivons $|H| = aq^m$ avec a premier à q. Par le (v) on a $H = H[a]\,H[q^m]$ avec $|H[a]| = a$ et $|H[q^m]| = q^m$. On pose $H' = H[a]$ et $Q = H[q^m]\langle z\rangle$. Par le (vii) on a $G = H\langle z\rangle = H'Q$. Par le (iv), les $H[n]$ sont distingués dans G car on a $H \lhd G$ et $H[n]$ caractéristique dans H. Par le (vi), on a $|Q| = q^n$ avec $n \geqslant 0$. On a $n \geqslant 1$ car $z \in Q$ est non trivial (car non dans H).

(ix) Soit G sous-abélien fini non abélien. Partons de l'écriture $G = H'Q$ donnée par (iii) et (viii). Si $|H'|$ n'est pas une puissance d'un nombre premier, on peut écrire $|H'| = ab$ avec $a, b > 1$ premiers entre eux. On a vu $H' = AB$ avec $A = H'[a]$ d'ordre a et $B = H'[b]$ d'ordre b. D'après le (vi), AQ et BQ sont des sous-groupes

stricts de G, donc abéliens. Cela implique que les éléments de A, B et Q commutent deux à deux, puis que $G = ABQ$ est abélien.

Partie III : Les groupes de Miller-Moreno

(i) D'après le (ix) de la partie II, on a $G = PQ$ avec P sous-groupe distingué d'ordre p^m, Q sous-groupe d'ordre q^n, p, q premiers distincts et $n \geqslant 1$. On a $P \cap Q = \{1\}$ par Lagrange et donc $|G| = p^m q^n$, puis $m \geqslant 1$ par hypothèse. Comme G est sous-cyclique, on a $P = \langle x \rangle$, $Q = \langle y \rangle$. Enfin, comme P est distingué, on a $yxy^{-1} \in \langle x \rangle$. On a donc $yxy^{-1} = x^k$ pour un certain $k \in \mathbb{Z}$. On a $k \not\equiv 1 \bmod p^m$ sinon x et y commutent et G est abélien.

(ii) Le sous-groupe $P^{(p)} = \langle x^p \rangle$ de P est d'ordre p^{m-1} et distingué dans G car $yx^p y^{-1} = (x^p)^k$, ainsi $P^{(p)}Q$ est d'ordre divisant $p^{m-1}q^n$ par la partie II (vi), donc strict. Il est donc cyclique, en particulier abélien, et donc y et x^p commutent. De même, $PQ^{(q)}$ est un sous-groupe strict de G, donc abélien, et y^q et x commutent.

(iii) Par le (i) et (ii) on a $x = y^q x y^{-q} = y(y(...(yxy^{-1})...)y^{-1})y^{-1} = x^{k^q}$, puis $k^q \equiv 1 \bmod p^m$ car x est d'ordre p^m. De même, on a $x^p = yx^p y^{-1} = (yxy^{-1})^p = x^{kp}$, donc $kp \equiv p \bmod p^m$, puis $k \equiv 1 \bmod p^{m-1}$.

(iv) Si on a $m > 1$ alors $k \equiv 1 \bmod p^{m-1}$ implique $k^p \equiv 1 \bmod p^m$ par le rappel. Ainsi, l'ordre de k modulo p^m divise p et q : c'est donc 1 et on a $k \equiv 1 \bmod p^m$, en contradiction avec le (i). On a montré $m = 1$ et que l'ordre de $k \bmod p$ est q. On a donc $q \mid p - 1 = |(\mathbb{Z}/p\mathbb{Z})^\times|$.

(v) Soit a l'automorphisme de $\mathbb{Z}/p\mathbb{Z}$ défini par $a(z) = \overline{k}z$ pour $z \in \mathbb{Z}/p\mathbb{Z}$. On a $a^q = \mathrm{id}$ car $k^q \equiv 1 \bmod p$. On a un morphisme de groupes $f : \mathbb{Z} \to \operatorname{Aut} \mathbb{Z}/p\mathbb{Z}, i \mapsto \alpha^i$. On a $f(q^n) = a^{q^n} = 1$ car $a^q = 1$. Par propriété universelle des groupes quotients, f se factorise en un morphisme de groupes $\alpha : \mathbb{Z}/q^n\mathbb{Z} \to (\mathbb{Z}/p\mathbb{Z})^\times$ vérifiant $\alpha(\overline{i}) = a^i$ pour tout $i \in \mathbb{Z}$.

(vi) Le groupe G est produit semi-direct interne de Q par P (question (i)). Soit $a : \mathbb{Z}/p\mathbb{Z} \to P$ et $b : \mathbb{Z}/q^m\mathbb{Z} \to Q$ les isomorphismes envoyant respectivement $\overline{1}$ sur x et $\overline{1}$ sur y. On a $yxy^{-1} = x^k$ et donc $a \circ \mathrm{int}_{b(\overline{1})} \circ a^{-1} = \alpha(\overline{1})$. Par suivi des isomorphismes a et b on a donc $G \simeq \mathbb{Z}/p\mathbb{Z} \rtimes_\alpha \mathbb{Z}/q^n\mathbb{Z}$.

(vii) Par hypothèse, et Gauss ou Cauchy, il existe $k \in \mathbb{Z}$ tel que $\overline{k}$ est d'ordre q dans $(\mathbb{Z}/p\mathbb{Z})^\times$. On peut donc définir un morphisme $\beta : \mathbb{Z}/q^n\mathbb{Z} \to \operatorname{Aut} \mathbb{Z}/p\mathbb{Z}$ comme au (v), envoyant $\overline{1}$ sur $\overline{k}$. On pose $G = \mathbb{Z}/p\mathbb{Z} \rtimes_\beta \mathbb{Z}/q^n\mathbb{Z}$. Par construction, on a $G = PQ$ avec $P = \langle x \rangle$ distingué d'ordre p, $Q = \langle y \rangle$ d'ordre q^n, et $yxy^{-1} = x^k$. Comme $k \not\equiv 1 \bmod p$, x et y ne commutent pas : G n'est pas abélien. Montrons qu'il est sous-cyclique.

Soit $\pi : G \to G/P$ la projection canonique. Elle induit un isomorphisme $Q \simeq G/P$ (cyclique d'ordre q^m). Soit H un sous-groupe strict de G. Si on a $H \cap P = \{1\}$ on a $H \simeq \pi(H)$, et $\pi(H)$ est cyclique car sous-groupe du groupe cyclique G/P. Sinon, on a $P \subset H$ cap $|P|$ est premier, et $\pi(H)$ est un sous-groupe strict du groupe cyclique G/P (d'ordre q^n), donc inclus dans $(G/P)^{(q)}$. Mais alors H est inclus dans $\pi^{-1}((G/P)^{(q)}) = \langle x, y^q \rangle$. Mais on a $y^q x y^{-q} = x^{k^q} = x$, donc x et y^q commutent. Comme ils sont d'ordre p et q^{n-1}, le sous-groupe engendré $\langle x, y^q \rangle$ est cyclique d'ordre pq^{n-1} engendré par xy (Cauchy), donc H est cyclique.

Partie IV : (Bonus) le cas des p-groupes

(i) Comme H est d'indice p dans G on a $y^p \in H$. Mais tout élément de H est soit d'ordre p^{n-1} (= générateur), soit engendre un sous-groupe strict, de la forme $\langle x^{p^i} \rangle$ avec $1 \leqslant i \leqslant n-1$, et en particulier est inclus dans $\langle x^p \rangle$. Mais y^p n'est pas

d'ordre p^{n-1}, sinon y serait d'ordre p^n et G serait cyclique. Enfin, le sous-groupe $\langle x^p, y\rangle = \cup_{i=0}^{p-1} y^i\langle x^p\rangle$ est d'ordre $\leqslant pp^{n-2}$, donc strict, puis cyclique et donc abélien.

(ii) On a $\langle x\rangle \lhd G$ donc il existe $k \in \mathbb{Z}$ avec $yxy^{-1} = k$. Par le (i) on a $yx^p = x^py$ et $y^px = xy^p$. Comme au (iii) partie III cela implique $k \equiv 1 \bmod p^{n-2}$ et $k^p \equiv 1 \bmod p^{n-1}$. Pour $n = 2$ cette seconde congruence implique $k \equiv 1 \bmod p^{n-1}$ donc G commutatif : absurde.

(iii) La seule chose supposée sur $y \in G$ est $y \notin \langle x\rangle$, ce qui est encore le cas pour x^iy pour tout $i \in \mathbb{Z}$. On a $k = 1 + up^{n-2}$ avec $u \in \mathbb{Z}$ et $y^p = x^{pv}$ avec $v \in \mathbb{Z}$ par le (i). Pour $i \in \mathbb{Z}$ on a

$$(x^iy)^{2p} = x^i(yx^iy^{-1})(y^2x^iy^{-2})\cdots(y^{2p-1}x^iy^{-q+1})y^{2p} = x^{(\sum_{j=0}^{2p-1} ik^j)+2v}.$$

On a $k^j \equiv 1 + ju \bmod p^{n-1}$ et $\sum_{j=0}^{2p-1} j = p(2p-1)$, donc $\sum_{j=0}^{2p-1} k^j \equiv 2p \bmod p^{n-1}$. On a donc $(x^{-v}y)^{2p} = 1$.

(iv) Par le (i) le sous-groupe $K := \langle t, y\rangle$ est abélien. Il est donc strict (car G non abélien), donc cyclique, et annulé par $2p$. Comme $t \in K$ est d'ordre p, on a soit $K = \langle t\rangle$ et $|K| = p$, soit K d'ordre $2p$. Le premier cas est exclus car il entraîne $y \in \langle x\rangle$. Dans le second cas, on a $2p \,|\, p^n$ par Lagrange, et puis $p = 2$, $K = \langle y\rangle$ d'ordre 4 et $y^2 = t$.

(v) Soit $z = x^{2^{n-3}}$. On a z d'ordre 4, $z^2 = t = y^2$ et $yzy^{-1} = z^k$ avec $k \equiv \pm 1 \bmod 4$. Le cas $k \equiv 1 \bmod 4$ implique que $M := \langle z, y\rangle$ est commutatif, donc strict et cyclique, et d'exposant 4, donc cyclique d'ordre 4, puis $M = \langle x\rangle = \langle y\rangle$: absurde. On a donc $yzy^{-1} = z^{-1}$, M non commutatif, puis $M = G$. On a reconnu le groupe H_8 (envoyer I sur z et J sur y).

10. Corrigé de l'examen 2021-2022

Problème 1. Partie 1

(i) On pose $g_1 = \mathrm{I}$, $g_2 = \mathrm{J}$ et $g_3 = \mathrm{K}$ (quaternions). On a $G = \mathrm{H}_8$, $\eta = \mathrm{IJK} = -1_2$ et $n = 2^{\frac{m-1}{2}}$.

(ii) En utilisant les relations données, on constate que l'on a $g_Ig_i = \pm g_{I'}$ avec $I' = I \smallsetminus \{i\}$ ou $J = I \cup \{i\}$, selon que l'on a $i \in I$ ou non. La formule de l'énoncé pour g_Ig_J s'en déduit par récurrence sur $|J|$.

(iii) Le (ii) montre $g_I^2 = \pm 1_n$ pour $J = I$, donc $g_I^{-1} = \pm g_I$, puis que $X = \{\pm g_I\}$ est un sous-groupe de G contenant les g_i : c'est donc G.

(iv) On a $g_i(g_{i_1}\cdots g_{i_k})g_i^{-1} = (g_ig_{i_1}g_i^{-1})(g_ig_{i_2}g_i^{-1})\cdots(g_ig_{i_k}g_i^{-1})$. On conclut car pour tout $1 \leqslant s \leqslant k$ on a $g_ig_{i_s}g_i^{-1} = -g_{i_s}$ si $i \neq i_s$, $+g_i$ sinon.

(v) On a clairement $\pm 1_n = \pm g_\varnothing \in Z$. Comme m est impair, le (iv) montre que pour tout $i = 1, \ldots, m$ on a $g_i\eta = (-1)^{m-1}\eta g_i = \eta g_i$. On a donc aussi $\pm\eta \in Z$. Supposons maintenant $0 < |I| < m$. Le (iv) montre que $g_igg_i^{-1} = \pm g$, avec des signes opposés selon que l'on choisit i dans I ou non. Les deux cas se produisent comme $0 < |I| < m$. On en déduit que la classe de conjugaison de g contient $\pm g$. Mais en itérant le (iv) on a $g_Jgg_J^{-1} = \pm g$ pour tout J, donc cette classe de conjugaison est exactement $\{g, -g\}$.

(vi) La question précédente et (iii) montrent $Z = \{\pm 1_n, \pm\eta\}$. On a clairement $|Z| = 2$ si $\eta = \pm 1_n$. Sinon, les 4 éléments $\pm 1_n, \pm\eta$ sont distincts, et donc $|Z| = 4$.

(vii) Pour l'existence, il suffit d'observer que si $g = \pm g_I$ avec $I \subset \{1, \ldots, m\}$ et $m \in I$, alors $\eta g = \pm g_{I'}$ avec $I' \subset \{1, \ldots, m-1\}$ par le (ii), puis $g = \pm\eta g_{I'}$. Montrons l'unicité. Supposons $zg_I = z'g_J$ avec $z, z' \in Z$ et $I, J \subset \{1, \ldots, m-1\}$. On a alors $z^{-1}z' = g_Jg_I^{-1} \in Z$. Mais $g_Jg_I^{-1} = \pm g_Jg_I$ est de la forme $\pm g_K$ avec $K = (I \cup J) \smallsetminus (I \cap J)$. Le (iv) montre donc que l'on a $K = \{1, \ldots, m\}$ ou $K = \varnothing$. Le

premier cas est impossible car on a $m \notin K$. On a donc $K = \varnothing$, *i.e.* $I = J$, puis $z = z'$.

(viii) Tout élément $h \in Z$ est sa propre classe de conjugaison : on a $ghg^{-1} = h$ pour tout $g \in G$. Et si $\pm h$ n'est pas dans Z on a vu au (iv) que sa classe de conjugaison est $\{h, -h\}$. Le nombre total de classes de conjugaison est donc bien $|Z| + \frac{|G|-|Z|}{2} = \frac{|Z|}{2} + \frac{|G|}{2}$. On conclut car on a vu $|G| = 2^{m-1}|Z|$.

(ix) On a $-1_n = g_1 g_2 g_1^{-1} g_2^{-1}$ (on utilise ici $m > 1$) donc -1_n est dans $\mathrm{D}(G)$. Soit $g = \pm g_I$ et $h \in G$. Par le (v) on a $hgh^{-1} = \pm g$, et donc $[h, g] = \pm 1_n$. On a bien montré $\mathrm{D}(G) = \{\pm 1_n\}$.

(x) Tout morphisme de groupes $G \to \mathbb{C}^\times$ est trivial sur $\mathrm{D}(G)$ car $\mathbb{C}^\times$ est abélien. Par la propriété universelle du quotient, c'est la même chose de se donner un morphisme de groupes $G \to \mathbb{C}^\times$ et un morphisme de groupes $G/\mathrm{D}(G) \to \mathbb{C}^\times$. Mais $G/\mathrm{D}(G)$ est abélien, donc il a exactement $|G/\mathrm{D}(G)|$ tels morphismes, par un théorème du cours. On conclut car on a $|G/\mathrm{D}(G)| = |G|/2$.

(xi) Si on a $2^m = a^2 + b^2$ avec m impair, on a a et b pairs par réduction modulo 4, puis $a = 2a'$, $b = 2b'$ et $2^{m-2} = (a')^2 + (b')^2$ et on conclut par récurrence sur m.

(xii) Montrer qu'à isomorphisme près, G possède $|Z|/2$ représentations $\mathbb{C}$-linéaires irréductibles de dimension > 1, et qu'elles sont de dimension $2^{\frac{m-1}{2}}$ (on traitera d'abord le cas $|Z| = 2$).

Supposons d'abord $|Z| = 2$ comme indiqué. On a alors $|G| = 2^m$ par (vii) et G possède $2^{m-1} + 1$ classes de conjugaison par (viii). D'après Frobenius, on sait que G possède $2^{m-1}+1$ représentations $\mathbb{C}$-linéaires irréductibles non isomorphes. Par le (x), il y en a 2^{m-1} de degré 1. Il n'en reste donc qu'une seule, disons de degré d (en fait, avec $d > 1$). Mais toujours par Frobenius, on sait que la somme des carrés des degrés des dimensions irréductibles vaut $|G|$. On a donc $|G| = 2^m = 2^{m-1} \cdot 1^2 + d^2$, puis $d = 2^{(m-1)/2}$.

Supposons maintenant $|Z| = 4$. On a cette fois-ci $|G| = 2^{m+1}$ par (vii), G a $2^m + 2$ représentations irréductibles non isomorphes par (viii), dont 2^m de degré 1 par (x), il en reste donc 2 de degré $a, b > 1$ à déterminer. Mais on a $2^{m+1} = 2^m.1^2 + a^2 + b^2 + 1^2$, et donc $a^2 + b^2 = 2^m$, puis $a = b = 2^{\frac{m-1}{2}}$ par le (xi).

(xiii) Soit $D \subset \mathbb{C}^n$ une droite G-stable. Soit $\lambda_i \in \mathbb{C}^\times$ la valeurs propre de $g_i \in \mathrm{GL}_n(\mathbb{C})$ sur la droite de D. La relation $g_i g_j = -g_j g_i$ pour $i \neq j$ (et deux tels indices existent car $m > 1$) montre $\lambda_i \lambda_j = -\lambda_j \lambda_i$, ce qui est absurde dans $\mathbb{C}^\times$.

(xiv) D'après Maschke, il existe une décomposition $\mathbb{C}^n = \oplus_{k=1}^s U_k$ où les U_k sont des sous-espaces vectoriels de $\mathbb{C}^n$ qui sont G-stables et irréductibles comme représentation de G. On a $\dim U_k > 1$ pour tout k par le (xi), et donc $\dim U_k \equiv 0 \bmod 2^{\frac{m-1}{2}}$ par le (xiii). On en déduit que $n = \dim \mathbb{C}^n = \sum_k \dim U_k$ est multiple de $2^{\frac{m-1}{2}}$.

Partie 2

(i) Pour $n = 2$, on peut prendre $E = \mathbb{C}$ muni de sa norme euclidienne $z \mapsto |z|^2$ et $\star$ la multiplication usuelle dans $\mathbb{C}$. Pour $n = 4$, on peut prendre $E = \mathbb{H}$ muni de sa norme n, et $\star$ la multiplication sur les quaternions (l'hypothèse est satisfaite par multiplicativité de la norme). Pour $n = 8$, il faudrait considérer les octonions de Cayley et Graves, dont la norme est aussi euclidienne et multiplcative.

(ii) C'est clair pour $x = 0$ donc on suppose $x \neq 0$. Par hypothèse, m_x est une similitude orthogonale de rapport $||x||^2$, ce qui conclut. On peut aussi dire que si $||x|| = 1$ alors on a $\mathrm{m}_x \in \mathrm{O}(E)$, donc $\mathrm{M}(x) \in \mathrm{O}(n)$. Pour $||x|| = \lambda > 0$, on a $\mathrm{m}_{x/\lambda} = \frac{1}{\lambda}\mathrm{m}_x$ par bilinéarité de $\star$, et donc $\frac{1}{||x||}\mathrm{M}(x) \in \mathrm{O}(n)$.

(iii) On a $||\varepsilon_i|| = 1$ donc $\mathrm{M}(\varepsilon_i) \in \mathrm{O}(n)$ par la question précédente. Pour $x = \varepsilon_i + \varepsilon_j$ avec $i \neq j$, on a $||x||^2 = 2$, mais aussi $\mathrm{M}(\varepsilon_i + \varepsilon_j) = \mathrm{M}(\varepsilon_i) + \mathrm{M}(\varepsilon_i)$ par linéarité de $x \mapsto \mathrm{m}_x$. En appliquant la question précédente à $\varepsilon_i, \varepsilon_j$ et $\varepsilon_i + \varepsilon_j$, on trouve la formule annoncée.

(iv) C'est un calcul direct à partir de la question précédente : pour $i, j < n$ on a

$$g_i g_j = \mathrm{M}(\varepsilon_i)\,{}^{\mathrm{t}}\mathrm{M}(\varepsilon_n)\mathrm{M}(\varepsilon_j)\,{}^{\mathrm{t}}\mathrm{M}(\varepsilon_n) =$$
$$-\mathrm{M}(\varepsilon_i){}^{\mathrm{t}}\mathrm{M}(\varepsilon_j)\mathrm{M}(\varepsilon_n)\,{}^{\mathrm{t}}\mathrm{M}(\varepsilon_n) = -\mathrm{M}(\varepsilon_i){}^{\mathrm{t}}\mathrm{M}(\varepsilon_j) = -\mathrm{M}(\varepsilon_i)\mathrm{M}(\varepsilon_j)^{-1}.$$

On a donc $g_i^2 = -1_n$. Pour $i \neq j$, on a par le (iii) l'égalité

$$\mathrm{M}(\varepsilon_i)^{-1}\mathrm{M}(\varepsilon_j) = -\mathrm{M}(\varepsilon_j)^{-1}\mathrm{M}(\varepsilon_i),$$

qui s'écrit aussi $\mathrm{M}(\varepsilon_j)\mathrm{M}(\varepsilon_i)^{-1} = -\mathrm{M}(\varepsilon_i)\mathrm{M}(\varepsilon_j)^{-1}$, et donc $g_i g_j = -g_j g_i$.

(v) On a $g_i^2 = -1_n$ avec $g_i \in \mathrm{O}_n(\mathbb{R})$. On en déduit $1 = (\det g_i)^2 = (-1)^n$, puis n pair.

(vi) On peut supposer $n > 2$. On est dans la situation de la Partie 1 avec $m = n - 1$, qui est impair par la question (v). On en déduit que $2^{\frac{n-2}{2}}$ divise n, et en particulier l'inégalité $2^{\frac{n}{2}} \leqslant 2n$. On a égalité pour $n = 8$, mais la suite $x_n = 2^{\frac{n}{2}}$ croît plus vite que $y_n = 2n$ pour $n \geqslant 8$: on a $x_{n+1}/x_n = \sqrt{2}$ et $y_{n+1}/y_n \leqslant 1 + 1/8 < \sqrt{2}$. On a donc $n \leqslant 8$. Le cas $n = 6$ est exclus car $2^2 = 4$ ne divise pas 6. On a bien répondu à la question initiale : si on a $z_k \in \mathbb{R}[x_1, \ldots, x_n, y_1, \ldots, y_n]$ pour $k = 1, \ldots, n$ comme dans la partie 1, la formule $(x_i) \star (y_i) = (z_k(x_1, \ldots, x_n, y_1, \ldots, y_n))$ définit une loi de composition sur l'espace euclidien standard $\mathbb{R}^n$. Elle est $\mathbb{R}$-bilinéaire car les z_k ne contiennent que des monômes de la forme $x_i y_j$, et elle vérifie $||x \star y||^2 = ||x||^2 ||y||^2$ par l'identité remarquable.

Problème 2. Partie 1

(i) Comme on l'a vu en cours, le nombre de bases du $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel $(\mathbb{Z}/p\mathbb{Z})^2$ est $|\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})| = (p^2 - 1)(p^2 - p)$. On conclut car $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ est par définition le quotient du groupe $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ par son centre $(\mathbb{Z}/p\mathbb{Z})^\times$, d'ordre $p - 1$.

(ii) Soit H le sous-groupe de $\mathscr{H}_X$ engendré par Aff_X et l'homographie $g(x) = 1/x$. Soit $f \in \mathscr{H}_X$. Si on a $f(\infty) = \infty$ alors $f \in \mathrm{Aff}_X \subset H$. Sinon, on a $f(\infty) = k$ avec $k \in \mathbb{Z}/p\mathbb{Z}$. Soit $t \in \mathrm{Aff}_X$ l'homographie $t(x) = x - k$. Alors $g\,t\,f$ envoie ∞ sur ∞, et donc $g\,t\,f \in H$, puis $t\,f \in H$ car $g^{-1} \in H$, puis $f \in H$ car $t^{-1} \in H$.

(iii) (Rappel : Un groupe G agit k-transitivement sur un ensemble X si on a $|X| \geqslant k$ et si G agit transitivement sur l'ensemble Y des k-uples de la forme $(x_1, x_2, \ldots, x_k)$, où les x_i sont distincts et dans X. Il suffit de montrer que la G-orbite d'un k-uple donné est tout Y.) On a bien $|\mathbb{Z}/p\mathbb{Z}| = p \geqslant 2$. Pour montrer la 2-transitivité de Aff_X sur $\mathbb{Z}/p\mathbb{Z}$, il suffit donc de voir que si u et v sont deux éléments distincts de $\mathbb{Z}/p\mathbb{Z}$, il existe $h \in \mathrm{Aff}_X$ tel que $h(0) = u$ et $h(1) = v$. Mais $h(x) := (v - u)x + u$ convient.

(iv) On a $p \mid |G|$, donc G possède un élément g d'ordre p par Cauchy. On sait que l'ordre d'une permutation dans un groupe symétrique est le ppcm des longueurs de ses cycles. Ainsi, une permutation d'ordre premier p est un produit de p-cycles à supports disjoints. Comme on a $|X| = p + 1 < 2p$, la seule possibilité est que g soit un p-cycle.

(v) On constate que α est le p-cycle $(0\,1\,2\,\ldots\,p-1)$. Soit $g \in G$ un p-cycle (question (iv)). Comme deux p-cycles sont conjugués dans S_X, on en déduit qu'il existe $\sigma \in \mathrm{S}_X$ tel que $\sigma g \sigma^{-1} = \alpha$. Le conjugué $\sigma G \sigma^{-1}$ a même cardinal que G, contient α, et agit transitivement sur X (si g envoit $\sigma^{-1}(x)$ sur $\sigma^{-1}(y)$, alors $\sigma g \sigma^{-1}$ envoit x sur y).

(vi) Comme G agit transitivement sur X, la formule orbite stabilisateur montre $|G| = |G_\infty||X|$, et donc $|G_\infty| = (p^3 - p)/(p+1) = p^2 - p$.

(vii) Comme $|G_\infty| = p(p-1)$, les sous-groupes d'ordre p de G_∞, comme le sous-groupe P, sont ses p-Sylow. D'après les théorèmes de Sylow, le nombre de p-Sylow de G_∞ est un diviseur d de $p-1$ qui vérifie $d \equiv 1 \bmod p$. On a donc soit $d = 1$, soit $d \geqslant p+1$: absurde. Ainsi, G_∞ possède un unique p-Sylow, qui comme on le sait est alors distingué (il est égal à ses conjugués).

(viii) Soit $g \in G_\infty$. On a vu que $\langle \alpha \rangle$ est distingué dans G_∞. On a donc $g\alpha g^{-1} = \alpha^a$ avec $0 \leqslant a < p$. Mais $a = 0$ est impossible, sinon on aurait $g\alpha g^{-1} = 1$ puis $\alpha = 1$: absurde.

(ix) Soit $g \in G_\infty$. On a vu qu'il existe un entier $1 \leqslant a < p$ avec $g\alpha = \alpha^a g$. Cela sécrit aussi $g(x+1) = g(x) + a$ pour tout $x \in \mathbb{Z}/p\mathbb{Z}$. Posons $b = g(0) \in \mathbb{Z}/p\mathbb{Z}$. On a donc $g(1) = a + b$, $g(2) = g(1) + a = 2a + b$, et par récurrence immédiate, $g(x) = ax + b$ pour tout $x \in \mathbb{Z}/p\mathbb{Z}$. On a montré $g \in \mathrm{Aff}_X$. L'égalité $G_\infty = \mathrm{Aff}_X$ en découle car $|G_\infty| = |\mathrm{Aff}_X| = p^2 - p$ (question (vi)).

(x) On a $|X| = p + 1 \geqslant 3$. Il faut montrer que pour tout x, y, z distincts dans X, il existe g dans G tel que $(g(0), g(1), g(\infty)) = (x, y, z)$. Comme G agit transitivement sur X, on peut trouver $h \in G$ avec $h(z) = \infty$. Quitte à remplacer (x, y, z) par $(h(x), h(y), h(z))$, ce qui est loisible, on peut donc suppser $z = \infty$. Mais alors on conclut par 2-transitivité de $G_\infty = \mathrm{Aff}_X$ sur $\mathbb{Z}/p\mathbb{Z}$ (question (iii)).

(xi) Soit $g \in G$ fixant 3 points distincts x, y, z de X. On veut montrer $g = 1$. Quitte à remplacer g par hgh^{-1} avec $h \in G$, qui fixe $h(x), h(y), h(z)$ et qui est trivial si et seulement si g l'est, on peut supposer $(x, y, z) = (0, 1, \infty)$ par ce qu'on vient de démontrer. Mais alors on a $g \in G_\infty = \mathrm{Aff}_X$, et donc $g(x) = ax+b$, puis $b = g(0) = 0$ (car g fixe 0) et enfin $a = g(1) = 1$ (car g fixe 1), donc $g = 1$.

(xii) On a démontré $G_\infty = \mathrm{Aff}_X$ (question (ix)). Ainsi, C est l'ensemble des homographies de la forme $m_a(z) = az$ avec $a \in (\mathbb{Z}/p\mathbb{Z})^\star$. L'application $a \mapsto \mathrm{m}_a, (\mathbb{Z}/p\mathbb{Z})^\times \to C$, est manifestement un isomorphisme de groupes. D'après le théorème de Gauss, on en déduit que $C \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p-1$. Soit g un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$. Alors $\mathrm{m}_g \in C$ est le $p-1$-cycle $(1\, g\, g^2, \dots\, g^{p-1})$.

(xiii) Comme C fixe 0 et ∞, et C est commutatif, on a $C \subset C'$ et $(0\,\infty) \in C'$. Supposons réciproquement g est dans C'. Écrivons $C = \langle c \rangle$ avec c un $p-1$ cycle. Comme g commute à c, il préserve l'ensemble des points fixes de c, qui sont $\{0, \infty\}$. Quitte à multiplier g par (0∞), on peut donc supposer que g fixe 0 et ∞. Si $c = (i_1, \dots, i_{p-1})$ on a aussi $c = gcg^{-1} = (g(i_1), g(i_2), \dots, g(i_{p-1}))$. Mais quitte à remplacer g par gc^k avec $k \in \mathbb{Z}$, on peut supposer $g(i_1) = i_1$, mais alors on a aussi $g(i_k) = i_k$ pour tout $k > 1$, puis $g = 1$.

(xiv) Si G contient une transposition, il contient tous ses conjugués, et donc toutes les transpositions par 2-transitivité de G sur X. On a donc $G = \mathrm{S}_X$. On conclut car on a $|G| = |\mathscr{H}_X| = |\mathrm{S}_X|$ si, et seulement si, $(p-1)p(p+1) = (p+1)!$, *i.e.* $p - 2 \leqslant 1$.

(xv) En effet, on a $C \subset C' \cap G$. Réciproquement, comme $(0\,\infty)$ et C commutent, un élément de C' non dans C est de la forme $(0\,\infty)c$ avec $c \in C$. Ainsi, si un tel élément est dans G, on a $(0\,\infty) \in G$, une contradiction.

(xvi) Pour $c \in C$ on a $c(0) = 0$ et $c(\infty) = \infty$, donc $\gamma c \gamma^{-1}$ fixe aussi 0 et ∞. Ainsi, l'automorphisme int_γ de G préserve C. Il est non trivial car sinon on aurait $\gamma \in C' \cap G = C$: absurde car γ ne fixe pas ∞. Enfin, l'élément γ^2 fixe 0 et ∞, donc est dans C, qui est commutatif, et donc $(\mathrm{int}_\gamma)^2 = \mathrm{int}_{\gamma^2}$ est l'identité de C.

(xvii) Comme C est cyclique d'ordre $p-1$, tout automorphisme de C est de la forme $c \mapsto c^n$ avec $n \in (\mathbb{Z}/(p-1)\mathbb{Z})^\times$, d'après un théorème du cours. S'il est d'ordre 2, on

a $c^{n^2} = c$ pour tout c dans C, et donc $n^2 \equiv 1 \bmod p-1$ en considérant un élément c d'ordre $p-1$ dans C. De plus, s'il est non trivial on a $n \not\equiv 1 \bmod p-1$.

(xviii) On a $\gamma c = c^n \gamma$. Soit g un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$. Cette identité appliquée à $c = \mathrm{m}_g$ s'écrit $\gamma(gx) = g^n\gamma(x)$ pour tout $x \in (\mathbb{Z}/p\mathbb{Z})^\times$. On en déduit $\gamma(g^k) = g^{nk}\gamma(1)$ pour tout $k \in \mathbb{Z}$. Mais on a $\gamma(1) = 1$ par hypothèse. On a donc $\gamma(x) = x^n$ pour tout $x \in (\mathbb{Z}/p\mathbb{Z})^\times$.

(xix) Comme $\gamma \neq 1$, on sait que γ a au plus 2 points fixes dans $(\mathbb{Z}/p\mathbb{Z})^\times$. Ces points fixes sont nécessairement 1 et -1 (noter $p > 2$ et donc n impair). On en déduit que le noyau de l'application $\mathbb{Z}/(p-1)\mathbb{Z} \to \mathbb{Z}/(p-1)\mathbb{Z}, k \mapsto (n-1)k$ est $\{0, \frac{p-1}{2}\}$. Cela implique que $\frac{n-1}{2}$ et premier avec $\frac{p-1}{2}$. Mais $\frac{p-1}{2}$ divise $\frac{n^2-1}{2} = \frac{n-1}{2}(n+1)$, et on conclut.

(xx) On a n impair car $n^2 \equiv 1 \bmod p-1$. Par le (xix), on a soit $n \equiv -1 \bmod p-1$, soit $n \equiv \frac{p-1}{2} - 1 = \frac{p-3}{2} \bmod p-1$. Ce second cas est exclus car n est pair.

(xxi) On a montré $\gamma(x) = 1/x$. Comme γ et $\mathrm{Aff}_X = G_\infty$ sont dans G, on a $\mathscr{H}_X \subset G$ par la question (ii), puis égalité pour des raisons de cardinal.

Partie 2

(i) On a $p^2 - 1 = dd'$ avec $d, d' \geqslant 1$ et $d \equiv 1 \bmod p$, et donc $d' \equiv -1 \bmod p$. On en déduit $d' \geqslant p-1$. Si $d > 1$, on a $d \geqslant p+1$ et la seule possibilité est donc $d = p+1$ et $d' = 1$.

(ii) Les sous-groupes d'ordre p de G sont ses p-Sylow car on a $|G| = p(p^2-1)$. Leur nombre d est un diviseur de p^2-1 par les théorèmes de Sylow, avec en outre $d \equiv 1 \bmod p$. On a donc $d = 1$ ou $d = p+1$ par le (i). Si $d = 1$, alors l'unique p-Sylow P de G est distingué, et de cardinal $p \mid p^2 - p$: absurde.

(iii) On sait que les p-Sylow de G sont conjugués, donc l'action de G sur X est transitive. Son noyau est un sous-groupe distingué de G inclus dans le stabilisateur d'un point de X, qui est d'ordre $|G|/|X| = p^2 - p$ par transitivité et formule orbite stabilisateur. Cela contredit l'hypothèse sur G par Lagrange.

(iv) Le morphisme $G \to \mathrm{S}_X$ associé à l'action étant injectif, G est isomorphe à un sous-groupe de $\mathrm{S}_X \simeq \mathrm{S}_{p+1}$ agissant transitivement sur X, et d'ordre $p^3 - p$. Il est donc isomorphe à $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ par le théorème de Zassenhaus.

(v) On sait que $\mathrm{PSL}_3(\mathbb{Z}/2\mathbb{Z})$ est simple par le cours. Mais on a $\mathrm{SL}_3(\mathbb{Z}/2\mathbb{Z}) = \mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$ car $(\mathbb{Z}/2\mathbb{Z})^\times = \{1\}$, et pour la même raison le centre de ce groupe est trivial, donc on a $G \simeq \mathrm{PSL}_3(\mathbb{Z}/2\mathbb{Z}) \simeq \mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$. On sait que son cardinal est $(2^3-1)(2^3-2)(2^3-2^2) = 7 \cdot 6 \cdot 4 = 168$.

(vi) (Une preuve parmi d'autres) Un tel $M = (m_{i,j})$ commute à toutes les matrices de permutation $\mathrm{S}_3 \subset \mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$. Comme on a $\sigma(m_{i,j})\sigma^{-1} = (m_{\sigma(i),\sigma(j)})$, et que S_3 est 2-transitif, on en déduit que tous les $m_{i,i}$ sont égaux (à 0 ou 1) et de même que tous les autres coefficients sont égaux (à 0 ou 1). L'inversibilité de M implique alors $M = 1_3$, et donc ${}^t hh = 1_3$ pour tout $h \in \mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$. C'est faux pour une transvection standard.

(vii) Soit $N \subset G$ un sous-groupe distingué et d'ordre 2. Alors N n'est pas inclus dans le sous-groupe $H \subset G$, qui est simple. Donc N est engendré par un élément de la forme $g = (M, \overline{1})$ avec $M \in H$. On a nécessairement $hgh^{-1} = g$ pour tout h dans G. Utilisons simplement $(h, 0)g = g(h, 0)$ pour tout h dans H. On trouve $hM = M{}^t h^{-1}$ pour tout h dans H, une contradiction par la question (vi).

(viii) On rappelle qu'on a une suite exacte naturelle $1 \to H \to G \to \mathbb{Z}/2\mathbb{Z} \to 1$. En particulier, H est distingué (et d'indice 2) dans G. Soit N un sous-groupe distingué quelconque de G. Alors $N \cap H$ est distingué dans H, qui est simple. On a donc $N \cap H = \{1\}$ ou $H \supset N$. Dans le second cas, on a $N = G$ ou $N = H$ car H est

d'indice 2. Dans le premier cas la projection $N \to \mathbb{Z}/2\mathbb{Z}$ est injective, donc $|N| \leqslant 2$, et on conclut par le (vii).

(ix) On a $|G| = 2.|H| = 2.168 = 336 = 7^3 - 7$ avec $7 \equiv 3 \bmod 4$ premier. De plus, G n'a pas de sous-groupe distingué d'ordre divisant $7^2 - 7 = 42$ par le (viii). On a donc $G \simeq \mathrm{PGL}_2(\mathbb{Z}/7\mathbb{Z})$ par le (iv). Le sous-groupe distingué $\mathrm{PSL}_2(\mathbb{Z}/7\mathbb{Z})$ d'indice 2 de $\mathrm{PGL}_2(\mathbb{Z}/7\mathbb{Z})$ est donc isomorphe à un sous-groupe distingué d'indice 2 de G, *i.e. à* H.

11. Corrigé de l'examen 2022-2023

Problème 1. (i) Soit $X = G/H$. On a $|X| = n$ et l'action en question fournit un morphisme de groupes $f : G \to \mathrm{S}_X$. Son noyau est un sous-groupe distingué de G, donc égal à 1 où à G. Dans ce second cas, G agit trivialement sur X. Mais comme l'action de G sur X est transitive, cela force $|X| = n = 1$: une contradiction. Ainsi, f est injective, et donc G est isomorphe au sous-groupe $f(G)$ de $\mathrm{S}_X \simeq \mathrm{S}_n$. Par Lagrange, on a donc $|G| = |f(G)| \mid n! = |\mathrm{S}_n|$.

(ii) Soit H le sous-groupe de A_5 engendré par g et h. Par Lagrange, les ordres 3 et 5 de g et h divisent $|H|$. On a donc $15 \,|\, |H|$, et l'indice n de H dans G divise $60/15 = 4$. Comme A_5 est simple, le (i) affirme que l'on a soit $n = 1$ (i.e. $H = G$), soit $60 = |G| \,|\, 4! = 24$, ce qui est absurde.

(iii) Soit f l'homographie en question. On a $f(0) = 1/5 = 9$, $f(9) = 9/3 = 3$ et $f(3) = 0/8 = 0$, d'où le cycle $(0\,9\,3)$. On a $f(1) = 8/6 = 8 \cdot 2 = 5$, $f(5) = 3/10 = 3 \cdot 10 = 8$ et $f(8) = 2/2 = 1$, d'où le cycle $(1\,5\,8)$. On a $f(2) = 4/7 = 4 \cdot 8 = 10$, $f(10) = 5/4 = 5 \cdot 3 = 4$ et $f(4) = 7/9 = 7 \cdot 5 = 2$, d'où le cycle $(2\,10\,4)$. Enfin, on a $f(6) = \infty$, $f(\infty) = 7$ et $f(7) = 6/1 = 6$, d'où le cycle $(6\,\infty\,7)$. La décomposition en cycles de f est donc $(\infty\,7\,6)(2\,10\,4)(1\,5\,8)(9\,3\,0)$.

(iv) Soit G le groupe des isométries directes de l'icosaèdre régulier I du dessin. On sait par le cours que l'on a $G \simeq \mathrm{A}_5$. On sait aussi que G agit naturellement sur les 12 sommets, que l'on numérote par X comme dans le dessin, et que cette action est fidèle.

Soit h la rotation de I d'angle $2\pi/5$ d'axe $(0\ \infty)$ (dans le sens envoyant 1 sur 4). C'est un élément d'ordre 5, qui en tant que permutation de X a pour décomposition en cycles manifeste $(1\,4\,5\,9\,3)\,(2\,8\,10\,7\,6)$. On constate que c'est l'homographie $x \mapsto 4x$ (!).

Soit g la rotation de I d'angle $2\pi/3$ et fixant le centre la face $6\,7\,\infty$. C'est un élément d'ordre 3 de G, qui en tant que permutation de X a pour décomposition en cycles manifeste $(\infty\,7\,6)(2\,10\,4)(1\,5\,8)(9\,3\,0)$. On reconnaît l'homographie $x \mapsto \frac{7x+1}{x+5}$ grâce à la question (iii).

On sait que g et h engendrent $G \simeq \mathrm{A}_5$ par le (ii). De plus, ils agissent par homographies sur X par ce que l'on vient de voir. Ainsi, le morphisme naturel $G \to \mathrm{S}_X$ défini par l'action de G sur les sommets de I a son image image incluse dans le sous-groupe $\mathrm{PGL}_2(\mathbb{Z}/11\mathbb{Z}) \subset \mathrm{S}_X$. On a déjà dit qu'il est injectif car l'action de G sur les sommets de I est fidèle.

Problème 2. (i) Écrivons $Z = \{1, z\}$. Soit $g \in G$. Comme Z est distingué dans G on a $gzg^{-1} = 1$ ou $gzg^{-1} = z$. Le première possibilité est absure car elle implique $z = 1$.

(ii) Comme π est surjectif, $\pi(N)$ est un sous-groupe distingué de G/Z. Mais G/Z est simple, car isomorphe à A_5. On a donc $\pi(N) = G/Z$ ou $\pi(N) = \{1\}$. Dans le second cas, on a $N \subset Z$, et donc $N = \{1\}$ ou $N = Z$: absurde. On est donc dans

le premier cas. On a montré $G = NZ$. Si on a $N \cap Z = Z$ alors Z est inclus dans N et donc $G = N$. On a donc $N \cap Z = \{1\}$ car Z est d'ordre 2.

(iii) La restriction $\pi_{|N} : N \to G/Z$ est un isomorphisme par le (ii). On a donc $N \simeq G/Z \simeq \mathrm{A}_5$. De plus, comme Z est dans le centre de G par le (i), on a $nz = zn$ pour tout $n \in N$ et $z \in Z$. Ainsi, G est produit direct interne de Z et N, *i.e.* $G \simeq Z \times N \simeq \mathbb{Z}/2\mathbb{Z} \times \mathrm{A}_5$.

(iv) Comme π est surjectif, on a $\pi(\mathrm{D}(G)) = \mathrm{D}(G/Z)$, et ce dernier vaut G/Z car on sait que l'on a $\mathrm{D}(\mathrm{A}_5) = \mathrm{A}_5$. On sait aussi que $\mathrm{D}(G)$ est distingué dans G. On a donc $\mathrm{D}(G) \subset Z$ ou $\mathrm{D}(G) = G$ par hypothèse. Mais $\mathrm{D}(G) \subset Z$ implique $\pi(\mathrm{D}(G)) = 1$, une contradiction.

(v) On regarde le morphisme de groupes composé $\det \circ r : G \to \mathbb{C}^\times, g \mapsto \det r(g)$. Comme $\mathbb{C}^\times$ est abélien, il est trivial sur les commutateurs de G, et donc sur le sous-groupe $\mathrm{D}(G)$ qu'ils engendrent. Mais on a $\mathrm{D}(G) = G$, et donc $\det \circ r = 1$.

(vi) On sait que z est dans le centre de G par le (i). Ainsi, $r(z) \in \mathrm{GL}_n(\mathbb{C})$ commute à tous le $r(G)$. Autrement dit, c'est un endomorphisme $\mathbb{C}[G]$-linéaire du $\mathbb{C}[G]$-module $\mathbb{C}^n$ défini par la représentation r. Ce module est irréductible, donc $r(z)$ est une homothétie par le Lemme de Schur. On a $r(z^2) = r(z)^2 = 1$, donc cette homothétie est de rapport ± 1.

(vii) On a vu $\det r(z) = 1$, donc $(-1)^n = 1$, *i.e.* n est pair. Soit N le noyau de r, c'est un sous-groupe distingué de G. Il ne contient pas z, donc ce n'est ni Z, ni G. Par hypothèse sur G, c'est donc $\{1\}$.

(viii) Notons U'_j avec $j \in J$ des représentants des classes d'isomorphisme de $\mathbb{C}[G]$-modules de G dans lesquels z agit par l'identité. D'après le (vi), tout $\mathbb{C}[G]$-module irréductible de G est isomorphe à un et un seul des U_i ou des U'_j. Par Frobenius, on a donc

$$|G| = \sum_{i \in I} (\dim U_i)^2 + \sum_{j \in J} (\dim U'_j)^2.$$

Mais par la propriété universelle du quotient, il est équivalent de se donner une représentation ρ de G avec $\rho(z) = 1$ (*i.e.* $\rho(Z) = \{1\}$) et une représentation ρ' du groupe quotient G/Z, le lien entre les deux étant donné par la formule $\rho'(gZ) = \rho(g)$. On constate que ρ est irréductible si, et seulement si ρ' l'est, car ces deux représentations ont même sous-groupe image. Ainsi, les U'_j sont aussi des représentants des classes d'isomorphisme de $\mathbb{C}[G/Z]$-modules irréductibles. Par Frobenius encore, on a donc $\sum_{j \in J} (\dim U'_j)^2 = |G/Z|$. On conclut car on a $60 = |\mathrm{A}_5| = |G/Z| = |G|/2$.

(ix) D'après le (vii), on a $\dim U_i$ pair pour tout i. On a aussi $1 \leqslant (\dim U_i)^2 \leqslant 60$ par le (viii). On a donc $\dim U_i = 2, 4, 6$ pour tout i. Supposons que 2 n'apparaît pas, et que 4 et 6 apparaissent a et b fois respectivement. On a donc $60 = 16a + 36b$ par le (viii), puis $15 = 4a + 9b$, ce qui est impossible avec $a, b \in \mathbb{N}$.

(x) Soit i tel que $\dim U_i = 2$. Le morphisme ρ_{U_i} considéré dans une base arbitraire de U_i fournit un morphisme $r : G \to \mathrm{GL}_2(\mathbb{C})$ associé avec $r(z) = -1_2$. On a $r(G) \subset \mathrm{SL}_2(\mathbb{C})$ par le (v) et $G \simeq r(G)$ par le (vii).

(xi) Justifions d'abord ce que l'on demandait d'admettre. Soit $H \subset \mathrm{GL}_2(\mathbb{C})$ un sous-groupe fini. D'après l'astuce unitaire de Weyl dans le cas hermitien, H est conjugué à un sous-groupe H' du groupe unitaire $\mathrm{U}(2)$. Si on a en outre $\det h = 1$ pour tout $h \in H$, on a $H' \subset \mathrm{SU}(2)$. Mais on a $\mathrm{Sp}(1) = \mathrm{SU}(2)$.

Revenons à la question. Quitte à remplacer G par un sous-groupe de $\mathrm{Sp}(1)$ qui lui est isomorphe comme suggéré, on peut supposer $G \subset \mathrm{Sp}(1)$. Comme -1 est l'unique élément d'ordre 2 de $\mathrm{Sp}(1)$, on a alors $z = -1$. Considérons le morphisme surjectif du cours $f : \mathrm{Sp}(1) \to \mathrm{SO}(3)$ de noyau $\{\pm 1\} = Z$. On a donc $f(G) \simeq$

$G/Z \simeq \mathrm{A}_5$. On rappelle que tous les sous-groupes Γ de $\mathrm{SO}(3)$ isomorphes à A_5 sont conjugués, chacun d'entre eux étant le groupe des rotations d'un icosaèdre régulier et centré en 0 de l'espace. On rappelle aussi que leurs images inverses $f^{-1}(\Gamma)$ (des sous-groupes de $\mathrm{Sp}(1)$, $f^{-1}(\Gamma)$ étant le groupe binaire de l'icosaèdre définissant Γ) sont donc aussi conjugués dans $\mathrm{Sp}(1)$, donc isomorphes entre eux, et que l'un quelconque d'entre eux a été noté $\widetilde{\mathrm{A}_5}$. Comme G est l'une de ces images inverses, on a bien $G \simeq \widetilde{A_5}$.

(xii) D'après le cours, on a vu que pour p premier > 3, le centre Z de $G := \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ est $\{\pm 1_2\} \simeq \mathbb{Z}/2\mathbb{Z}$ et que les seuls sous-groupes distingués de G sont $\{1\}$, G et Z. On conclut car on a aussi vu que pour $p = 5$ que le groupe $\mathrm{PSL}_2(\mathbb{Z}/5\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}/5\mathbb{Z})/Z$, simple d'ordre $\frac{5^3-5}{2} = 60$, est miraculeusement isomorphe à A_5.

Problème 3. Partie 1

(i) On prend $p = 5$ et $G = \mathrm{A}_5$. On a $|G| = 60 = 5 \cdot 12$ avec $12 \equiv 2 \bmod 5$, donc $r = 2$ et $|G| > 5.2$.

(ii) Par le cours on a $|\mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})| = (2^3-1)(2^3-2)(2^3-2^2) = 7\cdot 6\cdot 4 = 168$. Ce groupe agit naturellement sur $(\mathbb{Z}/2\mathbb{Z})^3$ en fixant 0, et donc sur $X = (\mathbb{Z}/2\mathbb{Z})^3 \smallsetminus \{0\}$. Cette action est trivialement fidèle. Ainsi, $\mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$ est isomorphe à un sous-groupe G de $\mathrm{S}_X \simeq \mathrm{S}_7$. On prend $p = 7$. On a $|G| = 168 = 7 \cdot 24$ avec $24 \equiv 3 \bmod 7$, donc $r = 3$ est premier, et $168 > 7 \cdot 3$, donc G est simple.

(iii) Soit G un groupe fini agissant k-transitivement sur l'ensemble fini X de cardinal n. Pour $x \in X$, alors on a d'une part $|G| = n\,|G_x|$ (formule orbite-stabilisateur) et d'autre part que G_x agit $k-1$ transitivement sur $X \smallsetminus \{x\}$. Ainsi, si on choisit k points distincts $x_1, \ldots, x_k$ dans X, on a

$$|G| \;=\; n\,(n-1)\,\cdots\,(n-k+1)\;|G_{x_1} \cap G_{x_2} \cap \cdots G_{x_k}|$$

(cet argument a été vu en TD). Si en outre le seul élément de G fixant k points de X est 1, on a $G_{x_1} \cap G_{x_2} \cap \cdots G_{x_k} = 1$ puis $|G| = \frac{n!}{(n-k)!}$. Pour $G = \mathrm{M}_{11}$ on trouve $|G| = \frac{11!}{7!} = 11 \cdot 10 \cdot 9 \cdot 8$. Pour $p = 11$, on a $10 \cdot 9 \cdot 8 \equiv -1 \cdot -2 \cdot -3 \equiv 5 \bmod 11$, donc $r = 5$. On a $|G| > 5.11$, donc G est simple.

Partie 2

(i) L'application affine $x \mapsto ax + b$ est bijective si, et seulement si, on a $a \neq 0$. On a donc $|\mathrm{Aff}_X| = (p-1)p$, car il y a p choix pour b, $p-1$ pour a. On a $a(a'x + b') + b = aa'x + ab' + b$ donc la composée de deux applications affines est affine. L'identité est affine. Pour $a \neq 0$, l'inverse de $x \mapsto ax + b$ est $x \mapsto a^{-1}(x - b)$, qui est affine.

(ii) Pour $k \in \mathbb{Z}$, on a $c^k(x) = x + k$. Soit $\sigma \in \mathrm{S}_X$ normalisant $\langle c \rangle$. On a donc $\sigma c \sigma^{-1} = c^k$ pour un certain $k \in \mathbb{Z}$. L'entier k est premier à p car sinon on a $c^k = 1$ ce qui contredit la bijectivité de la conjugaison par σ dans S_X (automorphisme intérieur). La relation $\sigma c = c^k \sigma$ s'écrit $\sigma(x+1) = \sigma(x) + k$ pour tout $x \in X$. Posons $b = \sigma(0) \in X$. On a $\sigma(1) = b + k$, $\sigma(2) = b + 2k$, ..., et par récurrence immédiate, $\sigma(x) = kx + b$. Cela montre $\sigma \in \mathrm{Aff}_X$. Réciroquement, si $\sigma(x) = ax + b$ avec $a \in \mathbb{Z}$ premier à p, on a $\sigma(x+1) = \sigma(x) + a$ et donc $\sigma c \sigma^{-1} = c^a$.

Partie 3

(i) Montrons (a) $\implies$ (b). Si p divise $|G|$ alors par Cauchy, G contient un élément d'ordre p. Un élément d'ordre p dans S_n est un produit de p-cycles à supports

disjoints, car l'ordre est le ppcm des longueurs des cycles. Pour $n = p$, c'est nécessairement un p-cycle. L'implication (b) $\implies$ (c) est claire. L'implication (c) $\implies$ (a) vient de la formule orbite-stabilisateur (le cardinal de l'orbite d'un point est p, et divise $|G|$.

(ii) La plus grande puissance de p divisant $|\mathrm{S}_p| = p!$ est p. La plus grande puissance de p divisant $|G|$ est donc aussi p par Lagrange.

Soit S l'ensemble des p-Sylow de G. On a $|S| = \mathrm{n}_G$ par définition. Le groupe G agit sur S par conjugaison, et cette action est transitive par Sylow. L'orbite de $P \in S$ est donc S tout entier, et son stabilisateur est $\mathrm{N}_G(P)$. On a donc $|G| = |S|\,|\mathrm{N}_G(P)|$ avec $|S| = \mathrm{n}_G$.

(iii) On a $P = \langle c \rangle$ avec c un certain p-cycle, par le (i). Par la Partie 2 (i) et (ii) , on sait que le normalisateur N de P dans S_p est de cardinal $p(p-1)$. Comme on a $P \subset \mathrm{N}_G(P) \subset N$, on a $|\mathrm{N}_G(P)| = pq$ avec $q \,|\, p-1$ par Lagrange. Mais on a aussi $|G| = |\mathrm{N}_G(P)|\mathrm{n}_G = p\,q\,\mathrm{n}_G$ et donc $|G|/p = q\,\mathrm{n}_G$. Comme $\mathrm{n}_\mathrm{G} \equiv 1 \bmod p$ par Sylow, on a $q \equiv \mathrm{r}_G \bmod p$. Comme $1 \leqslant q \leqslant p-1$ on a $\mathrm{r}_G = q$.

(iv) Les p-Sylow de G sont ses sous-groupes d'ordre p par le (ii). Chacun d'eux possède exactement $p-1$ éléments d'ordre p. De plus, tout élément d'ordre p appartient à un seul p-Sylow de G, à savoir le sous-groupe qu'il engendre. Il y a donc $(p-1)\mathrm{n}_G$ éléments d'ordre p dans G. Comme on a $|G| = p\mathrm{n}_G$ par l'hypothèse $\mathrm{r}_G = 1$, il y a exactement n_G éléments qui ne sont pas d'ordre p.

(v) Soit $i \in \{1, \ldots, p\}$ un point et $G_i \subset G$ son stabilisateur. On a $|G| = p|G_i|$ par la formule orbite stabilisateur, donc $|G_i| = \mathrm{n}_G$. Mais tout élément de G_i est d'ordre premier à p (car ce n'est pas un p-cycle, ou encore car G_i est isomorphe à un sous-groupe de S_{p-1} qui est d'ordre premier à p). Par le (iv), G_i est donc égal à l'ensemble E des éléments de G d'ordre $\neq p$. Cet ensemble E ne dépend pas de i, donc on a $G_i = G_j$ pour tout i, j. Ainsi, un élément de G_i fixe tous les points de $\{1, \ldots, p\}$, donc $G_i = \{1\}$, puis $\mathrm{n}_G = |G_i| = 1$.

Partie 4

(i) L'orbite de $i \in \{1, \ldots, p\}$ sous N est $Ni \subset \{1, \ldots, p\}$. Pour $g \in G$ on a $gNi = gNg^{-1}g(i) = Ng(i)$: c'est l'orbite de $g(i)$. Autrement dit, l'a bijection g de $\{1, \ldots, p\}$ envoit la N-orbite Ni de i sur celle $Ng(i)$ de $g(i)$. En particulier on a $|Ni| = |Ng(i)|$. Comme G agit transitivement sur $\{1, \ldots, p\}$, il pemute aussi transitivement les orbites sous N, qui ont donc toutes même cardinal.

(ii) Les a N-orbites ont même cardinal, disons b, et forment une partition de $\{1, \ldots, p\}$, on a donc $p = ab$. Comme p est premier, on a soit $b = 1$ et $a = p$, soit $b = p$ et $a = 1$. Dans le premier cas, il y a p-orbites qui sont des singletons : N fixe chaque point, et donc $N = \{1\}$, ce qui est contraire à l'hypothèse. On a donc une seule orbite, à p-éléments : l'action est transitive.

(iii) On a $p \,|\, |N|$. Appliquant la Partie 3 (i) à N et G, on sait que les p-Sylow de N sont d'ordre p, tout comme ceux de G, de sorte que tout p-Sylow de N est un p-Sylow de G. Soit Q un p-Sylow de N, il en existe par Sylow ou Cauchy. Soit P un p-Sylow de G. Par Sylow, on sait que l'on a $P = gQg^{-1}$ pour un certain $g \in G$. Mais alors $P = gQg^{-1}$ est inclus dans $gNg^{-1} = N$, car N est distingué dans G. Ainsi, G et N ont exactement les mêmes p-Sylow, et donc $\mathrm{n}_N = \mathrm{n}_G$.

(iv) Soit P un p-Sylow de N, et donc de G. On a $\mathrm{N}_N(P) \subset \mathrm{N}_G(P)$. Par Lagrange et la Partie 3 (iii), on a donc $p\mathrm{r}_N \,|\, p\,\mathrm{r}_G$, puis $\mathrm{r}_N \,|\, \mathrm{r}_G$.

(v) Si r_G est premier, on a $\mathrm{r}_N = 1$ ou $\mathrm{r}_N = \mathrm{r}_G$ par le (iv). Mais on a déjà vu $\mathrm{n}_N = \mathrm{n}_G$ (question (iii)). Par hypothèse on a $\mathrm{n}_G \neq 1$, et donc $\mathrm{r}_N = \mathrm{r}_G$ par le (v) de la Partie 3 appliqué à N. Mais on a aussi $|G| = p\mathrm{n}_G\mathrm{r}_G$ et $|N| = p\mathrm{n}_N\mathrm{r}_N$ (Partie II questions

(ii) et (iii)). Ainsi, on a $|G| = |N|$, et donc $N = G$ car $N \subset G$. On a montré que le seul sous-groupe distingué non trivial de G est G : le groupe G est simple.

Problème 4. (i) Par hypothèse, il existe $e_1, \ldots, e_r \in M$ tels que $M = \oplus_{i=1}^r \mathbb{Z}e_i$. Utilisant simplement l'inclusion $\mathbb{Z} \subset \mathbb{Z}[i]$, on en déduit $M = \sum_{i=1}^r \mathbb{Z}[i]e_i$.

(ii) On a $\overline{a}(am) = (\overline{a}a)m = \mathrm{N}(a)m$ avec $\mathrm{N}(a) \in \mathbb{Z}_{>0}$. Mais le groupe abélien sous-jacent à M est sans torsion car il est libre : si on a $n\sum_{i=1}^r x_i e_i = 0$ on a $\sum_{i=1}^r n x_i e_i = 0$ puis $nx_i = 0$ pour tout i car les e_i sont $\mathbb{Z}$-libres, et donc soit $n = 0$, soit $x_i = 0$ pour tout i. Ainsi, on a $\mathrm{N}(a) = 0$ ou $m = 0$. Mais $\mathrm{N}(a) = 0 = a\overline{a}$ implique $a = 0$.

(iii) On sait que l'anneau $A := \mathbb{Z}[i]$ est principal. Le A-module M est de type fini par le (i). Par le théorème de structure des modules de type fini sur un anneau principal, on peut écrire $M = N \oplus N'$ avec $N \simeq A^s$ (libre d'un certain rang $s \in \mathbb{N}$), et N' isomorphe à une somme finie de A/a_iA avec $a_i \in A$ non nuls. On en déduit que tout élément de N' est annulé par le produit (fini, non nul) des a_i (car A est commutatif...). Par le (ii), cela montre $N' = 0$, et donc que $M = N$ est libre de rang s. Mais le groupe abélien sous-jacent à $A = \mathbb{Z}[i]$ est libre de rang 2 sur $\mathbb{Z}$. Ainsi, le groupe abélien sous-jacent à $M = N \simeq A^s$ est libre de rang $2s$ sur $\mathbb{Z}$. On a donc $2s = r$.

(iv) Soit $R \in \mathrm{O}(P)$ la rotation en question d'angle $\pi/2$. On a $R^2 = -\mathrm{id}_P$. On considère alors l'application $\mathbb{Z}[i] \times L \to L$, $(a + bi, v) \mapsto (a\mathrm{id}_P + bR)(v) = av + bR(v)$. Cette application est bien définie car $1, i$ est une $\mathbb{Z}$-base de $\mathbb{Z}[i]$. On vérifie immédiatement que[12] c'est une structure de $\mathbb{Z}[i]$-module sur L car on a $R^2 = -\mathrm{id}_P$ et $i^2 = -1$. Le groupe abélien sous-jacent est L par construction, qui est libre de rang 2. Par le (iii), le $\mathbb{Z}[i]$-module L est donc libre de rang 1. En particulier, il existe $u \in L$ tel que $L = \mathbb{Z}[i]u = \mathbb{Z}u + \mathbb{Z}R(u)$. Alors $v = R(u)$ convient !

12. Corrigé de l'examen 2023-2024

Problème 1. (i) Il y a $\binom{5}{2} \cdot 2 = 20$ 3-cycles : $\binom{5}{2}$ possibilités pour les deux points fixes, et il y a deux trois-cycles dans S_3. De même, il y a $5 \cdot 3 = 15$ doubles-transpositions : 5 possibilités pour le point fixe, et il y a 3 doubles-transpositions dans S_4 (ou K_4). Enfin, tout 5-cycle s'écrit de manière unique sous la forme $(1\,a\,b\,c\,d)$ avec $\{a, b, c, d\} = \{2, 3, 4, 5\}$, il y en a donc $4! = 24$.

(ii) Soient $\phi \in E^X$ et $x \in X$. On a $(1.\phi)(x) = \phi(x)$ et donc $1.\phi = \phi$. Pour $g, h \in G$, on a $(g.(h.\phi))(x) = (h.\phi)(g^{-1}x) = \phi(h^{-1}(g^{-1}x) = \phi((gh)^{-1}x) = ((gh).\phi)(x)$ et donc $g.(h.\phi) = (gh).\phi$.

(iii) La fonction $\phi : X \to E$ est fixe par $g \in G$, si et seulement si, on a $\phi(g^{-1}x) = \phi(x)$ pour tout $x \in X$, ou ce qui revient même, $\phi(gx) = \phi(x)$ pour tout x dans X (changement de variables $x \mapsto gx$). Autrement dit, il faut et suffit que ϕ soit constante sur les orbites de l'action de $\langle g \rangle$ sur X, c'est-à-dire sur les cycles intervenant dans la décomposition en cycles de g sur X. Il y a $|E| = m$ valeurs de ϕ possibles sur chaque cycles, et sur chaque point fixe. Ainsi g a m^r points fixes dans E^X, avec $r := \mathrm{r}_X(g)$ le nombre de cycles de G sur X, incluant les points fixes (« cycles de longueur 1 »).

(iv) Prenons l'origine de l'espace au centre O du dodécaèdre donné D. On sait alors que G est un sous-groupe de $\mathrm{SO}(3)$ permutant les sommets de D. Si $g \in G$ fixe une face F, il fixe donc le centre C de cette face, qui est l'isobarycentre des sommets. Il fixe aussi la face $-F$ et son centre $-C$. Comme un élément non trivial de $\mathrm{SO}(3)$ n'a

12. On aurait aussi pu simplement dire que l'on peut supposer $P = \mathbb{C}$ (muni de la norme euclidienne $z \mapsto |z|$, qui est un $\mathbb{Z}[i]$-module de manière évidente, et que par hypothèse L en est un sous-module.

qu'une droite fixe, et que $-F$ est la seule de D face parallèle à F, g fixe exactement deux faces et a donc 2 points fixes dans X. Comme g induit une isométrie directe du pentagone régulier F, c'est une rotation de ce pentagone, nécessairement d'ordre 5 par le cours.

(v) On applique la formule de Burnside-Frobenius à cette action. Par le (iii), le nombre d'orbites est $\frac{1}{|G|}\sum_{g\in G} m^{\mathrm{r}_X(g)}$. On sait que l'on a $G \simeq \mathrm{A}_5$, donc $|G| = 60$. D'après le (i), le groupe G a 15 éléments d'ordre 2, 20 éléments d'ordre 3 et 24 éléments d'ordre 5 (avec le neutre cela fait bien $1+15+30+24 = 60$). On a $\mathrm{r}_X(1) = |X| = 12$. Par le (iv), les éléments $g \in G$ d'ordre $p = 2$ ou 3 sont sans points fixes sur X, et donc de décomposition en cycles de type $p+p+..+p = 12$: on a $\mathrm{r}_X(g) = 12/2 = 6$ pour g d'ordre 2, $\mathrm{r}_X(g) = 12/3 = 4$ pour g d'ordre 3. Enfin, pour $g \in G$ d'ordre 5, l'unique décomposition en cycles possible sur X est de type $5+5+1+1 = 12$ par le (iv), donc on a $\mathrm{r}_X(g) = 4$. Au final, on a 1 fois $\mathrm{r}_X(g) = 12$, 15 fois $\mathrm{r}_X(g) = 6$, et $20 + 24 = 44$ fois $\mathrm{r}_X(g) = 4$.

(vi) Un coloriage en Noir ou Blanc des faces de D est une fonction $f : X \to \{N, B\}$. Par définition, deux coloriages f, f' sont considérés équivalents si et seulement s'il existe $g \in G$ avec $g.f = f'$. Le nombre de coloriages en Noir ou Blanc non équivalents de D est donc la quantité du (v) pour $E = \{N, B\}$, i.e. $m = 2$, puis $\frac{2^4}{60}(2^8 + 15 \cdot 2^2 + 44) = \frac{4}{15}(256 + 60 + 44) = \frac{4\cdot 360}{15} = 4 \cdot 24 = 96$.

Problème 2. (o) C'est le (i) de l'exercice corrigé 4.23.

Partie I : groupes auto-transitifs

(i) D'après Cauchy, il existe un élément $g \in G$ d'ordre p. Soit $h \in G \smallsetminus \{1\}$. Par hypothèse, il existe $\alpha \in \mathrm{Aut}\, G$ avec $\alpha(g) = h$. Comme h est un isomorphisme $G \to G$, h et g ont même ordre p.

(ii) Le groupe G est un p-groupe. En effet, si on a ℓ premier divisant $|G|$, alors g possède un élément d'ordre ℓ par Cauchy, et donc $\ell = p$ par le (i). On sait que le centre d'un p-groupe non trivial est non trivial, donc $\mathrm{Z}(G)$ est non trivial. Fixons $x \in \mathrm{Z}(G)$ non trivial. Soit $g \in G \smallsetminus \{1\}$. Montrons $g \in \mathrm{Z}(G)$. Par hypothèse il existe $\alpha \in \mathrm{Aut}G$ avec $g = \alpha(x)$. Soit $h \in G$, comme α est bijectif il existe $y \in G$ avec $\alpha(y) = h$, puis $gh = \alpha(x)\alpha(y) = \alpha(xy) = \alpha(yx) = \alpha(y)\alpha(x) = hg$, et $g \in \mathrm{Z}(G)$.

(iii) Par (i) et (ii), le groupe G est abélien p-élémentaire, on conclut par le cours.

(iv) On sait que le groupe $G = (\mathbb{Z}/p\mathbb{Z})^n$ est canoniquement un espace vectoriel $G^\sharp$ sur $\mathbb{Z}/p\mathbb{Z}$, et qu'une application $G \to G$ est un morphisme si, et seulement si, elle est $\mathbb{Z}/p\mathbb{Z}$-linéaire. Le groupe $\mathrm{Aut}\, G$ coïncide avec le groupe $\mathrm{GL}(G^\sharp)$ des bijections $\mathbb{Z}/p\mathbb{Z}$-linéaires de $G^\sharp$. Mais si V est un espace vectoriel de dimension finie (disons) sur un corps K, et si v et w sont deux vecteurs non nuls, on peut toujours trouver $g \in \mathrm{GL}(V)$ avec $g(v) = w$: compléter v en une base $v_1 = v, v_2, ..., v_n$, et w en une base $w_1 = w, w_2, \ldots, w_n$, et considérer l'unique g envoyant v_i sur w_i pour $i = 1, \ldots, n$.

(v) L'hypothèse sur G et $k \geqslant 1$ implique que $\mathrm{Aut}\, G$ agit transitivement $G \smallsetminus \{1\}$, donc on a $G \simeq (\mathbb{Z}/p\mathbb{Z})^n$ par le (iii). On a vu au (iv) que G peut être vu naturellement comme un K-espace vectoriel V de dimension n sur le corps $K = \mathbb{Z}/p\mathbb{Z}$, et qu'alors on a $\mathrm{Aut}\, G = \mathrm{GL}(V)$. Par hypothèse, le groupe $\mathrm{GL}(V)$ agit 2-transitivement sur $V \smallsetminus \{0\}$. Soit $v \in V$ non nul. Alors $\mathrm{GL}(V)_v$ agit transitivement sur $V\backslash\{0, v\}$ par le (o). Mais $\mathrm{GL}(V)_v$ préserve la droite Kv et agit trivialement sur cette droite par linéarité. On en déduit que si $Kv \smallsetminus \{0, v\}$ est non vide, i.e. $p = |K| > 2$, alors on a $V = Kv$ et $|Kv| = 3 = p$. Sinon, c'est que l'on a $Kv = \{0, v\}$ et donc $|K| = p = 2$. Dans ce cas, la convention $|G - \{1\}| \geqslant 2$ force $n \geqslant 1$.

(vi) On a $k \leqslant |G| - 1$ par convention, en particulier donc $|G| \geqslant 4$. Par le (v), et reprenant les notations ci-dessus, G est le groupe additif d'un espace vectoriel V de dimension $n \geqslant 2$ sur $K = \mathbb{Z}/2\mathbb{Z}$, et on sait $\operatorname{Aut} G = \mathrm{GL}(V)$. Soient $e_1, \ldots, e_n$ une base de V. Alors $\mathrm{GL}(V)_{e_1} \cap \mathrm{GL}(V)_{e_2}$ agit transitivement sur $V \smallsetminus \{0, e_1, e_2\}$ par le (o). Mais il fixe l'élément $e_1 + e_2$. On a donc $V = \{0, e_1, e_2, e_1 + e_2\}$, puis $n = 2$ et $k \leqslant 3$.

Partie II : le critère de simplicité de Rotman

(i) Si[13] on a $Nx = \{x\}$ pour tout $x \in X$ alors N agit trivialement sur X, et donc $N = \{1\}$ car l'action de G est supposée fidèle sur X. Donc il existe x tel que $|Nx| > 1$. Vérifions que le sous-ensemble $Nx \subset X$ est stable par G. En effet, pour $g \in G$ on a $gNx = gNg^{-1}x = Nx$ car N est distingué dans G. Mais G_x agit transitivement sur $Y := X \smallsetminus \{x\}$ par le (o), et on a $Nx \cap Y \neq \varnothing$ car $|Nx| > 1$, donc $X \smallsetminus \{x\} \subset Nx$, puis $X = Nx$.

(ii) Comme N est distingué dans G, on constate que $N \cap G_{x_0}$ est distingué dans G_{x_0}. Mais ce dernier est simple par hypothèse, on a donc soit $N \cap G_{x_0} = \{1\}$, soit $N \cap G_{x_0} = G_{x_0}$. Dans ce second cas, on a $G_{x_0} \subset N$. Montrons $N = G$. Soit $g \in G$. On a $gx_0 = nx_0$ pour un certain $n \in N$ par le (i), puis $n^{-1}g \in G_{x_0}$, et donc $g \in nG_{x_0} \in N$.

(iii) L'application est bien définie par le (ii). Elle est surjective par le (i). Enfin, si on a $nx_0 = mx_0$ avec $n, m \in N$, on a $m^{-1}n \in G_{x_0} \cap N = \{1\}$ (par le (ii)), donc $m = n$: l'application est injective.

(iv) L'application $f : N \smallsetminus \{1\} \longrightarrow X \smallsetminus \{x_0\}, n \mapsto nx_0$ est bijective par le (iii). Le groupe G_{x_0} agit naturellement sur $X \smallsetminus \{x_0\}$. Faisons-le aussi agir par conjugaison sur $N \smallsetminus \{1\}$. On constate que f définit un isomorphisme entre ces deux actions. En effet, pour $n \in N \smallsetminus \{1\}$ et $g \in G$ on a $f(gng^{-1}) = gng^{-1}x_0 = gnx_0 = g.f(n)$ car $gx_0 = x_0$. Ainsi, comme l'action de G_{x_0} sur $X \smallsetminus \{x_0\}$ est $(k-1)$-transitive (par le (o)), il en va de même de celle par conjugaison de G_{x_0} sur $N \smallsetminus \{1\}$.

(v) Supposant G non simple, on dispose d'un groupe N comme ci-dessus. L'action par conjugaison de G_{x_0} sur N définit un morphisme $G_{x_0} \to \operatorname{Aut} N$, dont l'image agit $k-1$ transitivement sur $N - \{1\}$ par le (iv). En particulier, $\operatorname{Aut} N$ agit $k-1$-transitivement sur $N - \{1\}$. On a aussi $|N| = |X|$ par la question (iii). D'après le (vi) partie I, on a $k - 1 \leqslant 3$, *i.e.* $k \leqslant 4$, et dans le cas $k = 4$ on a $N \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Dans ce second cas on a $|X| = 4$, puis par 4-transitivité de $G \subset \mathrm{S}_X$, $G = \mathrm{S}_X$, ce qui est absurde car alors $G_{x_0} \simeq \mathrm{S}_3$ n'est pas simple. Si on a $k = 3$, le (v) de la partie I montre que soit $|X| = |N|$ est une puissance de 2, soit on a $|N| = |X| = 3$. Dans ce dernier cas on a nécessairement $G = \mathrm{S}_X$ par 3-transitivité. Dans le cas restant $k = 2$, la question (iii) partie I montre $|X| = |N| = p^n$ avec p premier : on est dans le cas (c).

Partie III : deux applications du critère de Rotman

(i) Par récurrence sur $n \geqslant 5$. C'est l'hypothèse pour $n = 5$. Pour $n > 5$ on regarde l'action naturelle de A_n sur $\{1, \ldots, n\}$. On sait qu'elle est $n - 2$ transitive. Le stabilisateur du point n est A_{n-1} qui est simple par récurrence. Comme $n - 2 > 3$, le critère de Rotman affirme que A_n est simple.

(ii) Par le (o), M_{22} agit 3-transitivement sur l'ensemble $\{3, 4, \ldots, 24\}$ à 22 éléments, et le stabilisateur de 3 est $\mathrm{PSL}_3(\mathbb{F}_4)$, dont on sait qu'il est simple par le cours. Comme 22 n'est pas une puissance de 2, le critère de Rotman assure que M_{22} est simple. Ensuite, M_{23} agit 4-transivement sur l'ensemble $\{2, 3, \ldots, 24\}$ à 23 éléments, et le

13. Ce qui suit est le même argument que dans le début de la preuve du critère d'Iwasawa.

stabilisateur de $\{2\}$ est le groupe simple M_{22}, donc M_{23} est simple par Rotman. On conclut de même la simplicité de M_{24} à partir de celle de M_{23}.

Problème 3. (i) Par unicité du reste de la division euclidienne d'un polynôme par P, le $K[X]$-module $K[X]/(P)$ a pour K-base les classes de 1, X, $\ldots$, X^{n-1}. Soit $f : K[X]/(P) \to V_u$ un isomorphisme $K[X]$-linéaire. On pose $v = f(\overline{1})$. Alors f est K-linéaire, et envoie la base $\overline{X^i} = X^i.\overline{1}$, avec $i = 0, \ldots, n-1$, sur la base des $f(X^i.\overline{1}) = X^i f(\overline{1}) = X^i v$, avec $i = 0, \ldots, n-1$. On a $Pv = Pf(\overline{1}) = f(P\overline{1}) = f(\overline{P}) = f(0) = 0$.

(ii) Pour $i = 0, \ldots, n-1$ on pose $e_i = X^i v$. Les e_i forment une base de V par le (i). Il y a donc un sens à définir une telle ϕ. Écrivons $P = X^n + \sum_{i=0}^{n-1} a_i X^i$ avec les a_i dans K. Notons e_i^* la base duale des e_i ; on a d'abord $\phi = e_{n-1}^*$. Pour $i = 1, \ldots, n-1$ on constate $X^i\phi = e_{n-i-1}^* +$ une combinaison linéaire de e_j^* avec $n-i \leqslant j \leqslant n-1$. En effet, pour $j \leqslant n-i-1$ on a $(X^i\phi)(e_j) = \phi(X^i e_j) = \phi(X^{i+j}v)$ qui vaut 1 pour $i+j = n-1$, 0 pour $i+j < n-1$. On en déduit que $\phi, X\phi, \ldots, X^i\phi$ est une base de V^* (système triangulaire par rapport à la base $e_{n-1}^*, e_{n-2}^*, \ldots, e_1^*, e_0^*$). Enfin, pour $\phi \in V^*$ et $w \in W$ on a $(P\phi)(w) = \phi(Pw) = \phi(0) = 0$.

(iii) On regarde l'application $f : K[X] \to (V^*)_{{}^t u}, Q \mapsto Q\phi$. Elle est manifestement $K[X]$-linéaire, surjective par le (ii). Son noyau est un idéal de $K[X]$ contenant (P) donc principal de la forme (Π) pour un Π unitaire dans $K[X]$ divisant P. Mais f induit un isomorphisme $K[X]/(\Pi) \to (V^*)_{{}^t u}$, de sorte que le membre de gauche est de dimension $\deg \Pi = \dim V^* = \dim V = \deg P$, puis $\Pi = P$.

(iv) On considère l'application K-linéaire $f : V^* \to \oplus_{i=1}^r V_i^*$, $\varphi \mapsto \sum_{i=1}^r \phi_{|V_i}$. Elle est injective entre deux espaces de même dimension par $V = \oplus_{i=1}^r V_i$, donc bijective. Comme on a $u(V_i) \subset V_i$, on a aussi $\phi_{|V_i} \circ u = \phi_{|V_i} \circ u_i$, est donc f est $K[X]$-linéaire $(V^*)_{{}^t u} \to \oplus_{i=1}^r (V_i^*)_{{}^t u_i}$.

(v) Par le théorème de structure des $K[X]$-modules de dimension finie, on sait que le $K[X]$-module V_u s'écrit $V_u = \oplus_{i=1}^r V_i$, où pour tout $i = 1, \ldots, r$ V_i est un sous-module isomorphe à $K[X]/(P_i)$ avec $P_i \in K[X]$ unitaire. Par définition, on a $V_i = (V_i)_{u_i}$ avec $u_i = u_{|V_i}$ et un léger abus de language. Par le (iii) on a $(V_i)^*_{{}^t u_i} \simeq V_i$ pour tout i, et par le (iv) on a $(V^*)_{{}^t u} \simeq \oplus_{i=1}^r (V_i)^*_{{}^t u_i}$. Cela conclut.

(vi) Soient $u \in \mathrm{End}_K(V)$ et $e_1, \ldots, e_n$ une base V. Notons $U = (u_{i,j}) \in \mathrm{M}_n(K)$ la matrice de u dans cette base : pour $1 \leqslant j \leqslant n$ on a $u(e_j) = \sum_{i=1}^n u_{i,j} e_i$. Soit $e_1^*, \ldots, e_n^*$ la base duale de V. On constate que l'on a ${}^t u(e_j^*)(e_i) = e_j^*(u(e_i)) = u_{j,i}$, autrement dit la matrice de ${}^t u$ dans cette base duale est ${}^t U$. Le (v) affirme donc exactement que U et ${}^t U$ sont semblables.

(vii) Le nombre de points fixes de g dans X est le nombre de droites de $V = K^n$ stables par g. Le nombre de points fixes de g dans Y est le nombre d'hyperplans de V stables par g, ou ce qui revient au même, le nombre de droites de V^* stables par ${}^t g$. Mais les $K[X]$-modules V_g et $(V^*)_{{}^t g}$ étant isomorphes par (v), il existe une bijection K-linéaire $f : V \to V^*$ vérifiant $f \circ g = {}^t g \circ f$. Cette bijection induit une bijection entre les droites propres de g dans V et celles de ${}^t g$ dans V^*.

(viii) On sait que si G agit sur un ensemble fini E, et si $\mathbb{C}E$ est le $\mathbb{C}[G]$-module de permutation associé, alors pour tout $g \in G$, le nombre de points fixes de g dans E coïncide avec $\chi_{\mathbb{C}E}(g)$. On applique ceci à $E = X$ et $E = Y$. Par le (vii), on a donc l'égalité de caractères $\chi_{\mathbb{C}X} = \chi_{\mathbb{C}Y}$. Par le cours, on en déduit que les représentations $\mathbb{C}X$ et $\mathbb{C}Y$ sont isomorphes.

(ix) On sait que deux actions équivalentes possèdent un stabilisateur en commun. Ainsi, si les actions sur X et Y sont équivalentes, il existe une droite D de $V = K^n$

et un hyperplan $H \subset V$ tels que le stabilisateur respectifs de D et H dans $\mathrm{GL}(V)$ coïncident. Il suffit donc de trouver $g \in \mathrm{GL}(V)$ vérifiant $g(H) = H$ et $g(D) \neq D$. Si $D \cap H = \{0\}$, on peut trouver une base $e_1, \cdots, e_n$ de V avec $e_1, \ldots, e_{n-1} \in H$ et $e_n \in D$. L'élément g défini par $g(e_i) = e_i$ pour $i < n$, et $g(e_n) = e_n + e_{n-1}$ convient. Si $D \subset H$, on peut trouver une base $e_1, \cdots, e_n$ de V avec $e_1, \ldots, e_{n-1} \in H$ et $e_1 \in D$. L'élément g défini par $g(e_1) = e_2$, $g(e_2) = e_1$, et $g(e_i) = e_i$ pour $3 \leqslant i \leqslant n$ convient et existe car $n \geqslant 3$.

Problème 4. (i) Les sous-groupes d'ordre 23 de G sont ses 23-Sylow. Par Sylow, leur nombre $\mathrm{n}_{23}(G)$ est $\equiv 1 \bmod 23$ et divise $2^3 \cdot 11$. Les diviseurs > 23 de $2^3 \cdot 11$ sont $4 \cdot 11 = 44 \equiv -2 \bmod 23$ et $8 \cdot 11 = 88 \equiv -4 \bmod 23$. Donc G a un unique sous-groupe d'ordre 23, alors nécessairement distingué.

(ii) On a $|G| = 23 \cdot 88$ avec $23 \wedge 88 = 1$, et G a un sous-groupe distingué V d'ordre 23. D'après le théorème de Schur-Zassenhaus, V a un sous-groupe Q d'ordre 88 dans G. Par la remarque dans le cours suivant l'énoncé du théorème de Schur-Zassenhaus, un tel sous-groupe est un complément de V dans G. Ainsi, G est produit semi-direct interne de Q par V.

(iii) On a $|Q| = 2^3 \cdot 11$. Par Sylow, on a $\mathrm{n}_{11}(Q) \equiv 1 \bmod 11$ et $\mathrm{n}_{11}(Q) \mid 8$. On en déduit que Q possède un unique sous-groupe O d'ordre 11, nécesairement distingué.

(iv) Si H est un 2-Sylow de Q, on a $|H| = 8$, puis nécessairement $H \cap O = \{1\}$ par Lagrange, et donc $|OH| = |O||H| = |Q|$ par le cours, et donc H est un complément de O et on est dans une situation de produit semi-direct interne $Q = O \rtimes H$.

(v) D'après le cours, si C est cyclique d'ordre p, alors $\varphi_C : (\mathbb{Z}/p\mathbb{Z})^\times \to \operatorname{Aut} C, \bar{i} \mapsto (x \mapsto x^i)$, est un isomorphisme de groupes. Si p est premier, $\operatorname{Aut} C \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ est donc cyclique d'ordre $p-1$, d'après Gauss. En particulier, $\operatorname{Aut} C$ a un unique élément d'ordre 2, égal à $x \mapsto x^{-1}$ (i.e. $\varphi_C(-1)$), car -1 est l'élément d'ordre 2 de $(\mathbb{Z}/p\mathbb{Z})^\times$. Cela montre la première assertion ($C = O$, $p = 11$). Un groupe cyclique d'ordre 22 a un unique sous-groupe d'ordre d pour chaque diviseur d de 22, i.e. $d = 1, 2, 11, 22$. On conclut car $1, -1, 2$ et -2 sont d'ordre respectifs 1, 2, 11 (par la donnée) et 22 (par Cauchy) dans $(\mathbb{Z}/23\mathbb{Z})^\times$.

(vi) Les 2-Sylow de G sont ses sous-groupes d'ordre 8. Ils sont tous conjugués dans G par Sylow, et en particulier tous isomorphes. Si G possède élément d'ordre 8, *i.e. un sous-groupe cyclique d'ordre* 8, tous ses sous-groupes d'ordre 8 sont donc cycliques. Donc $H \leqslant Q \leqslant G$ est cyclique.

(vii) L'action de H par conjugaison sur le sous-groupe distingué O de Q définit un morphisme de groupes $f : H \to \operatorname{Aut} O, g \mapsto (x \mapsto gxg^{-1})$. Par le (v), on sait que $\operatorname{Aut} O$ est cyclique d'ordre 10 et a $x \mapsto x^{-1}$ pour seul élément d'ordre 2. L'image $f(H) = \langle f(h) \rangle$ est un sous-groupe d'ordre divisant $|H| = 2^8$ et $|\operatorname{Aut} O| = 10$, il est donc d'ordre 1 ou 2, et $f(h)$ est donc d'ordre 1 ou 2. On a donc soir $f(h) = 1$, et $Q = O\langle h \rangle$ est abélien, soit $f(h)$ est $x \mapsto x^{-1}$.

(viii) Le groupe Q est d'ordre 11, donc cyclique, disons engendré par g. Comme g et h commutent, gh est d'ordre $11 \cdot 8 = 88$ dans Q par Cauchy.

(ix) On regarde l'action de Q par conjugaison sur le sous-groupe distingué V de G, qui est un morphisme $f : Q \to \operatorname{Aut} V, g \mapsto (v \mapsto gvg^{-1})$. La question (vii) conclut si on observe que si on a un morphisme surjectif $\varphi : C \to C'$ entre groupes cycliques, tout générateur de C' est image d'un générateur de C. En effet, si g est un générateur de C, $\varphi(g)$ engendre C'. Tout autre générateur de C' est de la forme $\varphi(g)^k$ avec $k \wedge |C'| = 1$. Par Bézout, on peut trouver $k' \in \mathbb{Z}$ avec $k' \equiv k \bmod |C'|$ et $k' \equiv 1 \bmod p$ pour tout premier p divisant $|C|$ mais pas $|C'|$. Un tel k' vérifie $k' \wedge |C| = 1$, et le générateur $g^{k'}$ de C convient.

(x) On regarde encore l'action par conjugaison $f : Q \to \operatorname{Aut} V$ de Q sur V (comme au (viii)). L'élément $f(h)$ est d'ordre 1 ou 2, donc $f(h) = \mathrm{id}$ ou $f(h)$ est $v \mapsto v^{-1}$. Pour $x \in O$ on a $f(x)^{11} = 1$. On a aussi $f(hxh^{-1}) = f(h)f(x)f(h)^{-1} = f(x)$ car $\operatorname{Aut} V$ commutatif, et $f(hxh^{-1}) = f(x^{-1}) = f(x)^{-1}$, donc $f(x)^2 = 1$. Donc $f(x)$ est d'ordre 1, *i.e.* $f(x) = 1$.

(xi) Remarquons que G étant donné, V est l'unique sous-groupe distingué d'ordre 23 de G (donc canonique) et Q étant choisi, la décomposition $G = V \rtimes Q$ montre $G/V \simeq Q$, donc la classe d'isomorphisme de Q est ne dépend que de celle de G. De plus, l'image du morphisme naturel défini par conjugaison $G \to \operatorname{Aut} V$ (trivial sur V) est aussi bien défini à isomorphisme près : on la note I. En particulier, $|I|$ est ne dépend également que de la classe d'isomorphisme de G.

Pour $i = 1, -1, 2, -2$, notons $\varphi_i : \mathbb{Z}/88\mathbb{Z} \to \operatorname{Aut} \mathbb{Z}/23\mathbb{Z}$ le morphisme envoyant $\overline{1}$ sur l'automorphisme $x \mapsto ix$ (bien défini car $\overline{i} \in (\mathbb{Z}/23\mathbb{Z})^\times$ est d'ordre 1, 2, 11, 22 respectivement) et posons $G_i = \mathbb{Z}/23\mathbb{Z} \rtimes_{\varphi_i} \mathbb{Z}/88\mathbb{Z}$. Dans ces 4 cas, I est d'ordre 1, 2, 11 et 22 respectivement : les groupes G_i sont 2 à 2 non isomorphes. Si le groupe Q est abélien, donc cyclique par le (viii), alors d'après (ii) et (xi), on a $G \simeq G_i$ pour $i \in \{1, -1, 2, -2\}$.

Dans le cas restant, Q est isomorphe au groupe $Q_0 := \mathbb{Z}/11\mathbb{Z} \rtimes_\varphi \mathbb{Z}/8\mathbb{Z}$ avec $\varphi : \mathbb{Z}/8\mathbb{Z} \to \operatorname{Aut} \mathbb{Z}/11\mathbb{Z}$ envoyant $\overline{1}$ sur $x \mapsto -x$, d'après le (vii). Posons $G_0 = \mathbb{Z}/23\mathbb{Z} \rtimes_\psi Q_0$ où $\psi : Q_0 \to \operatorname{Aut} \mathbb{Z}/23\mathbb{Z}$ est le morphisme obtenu en composant la projection canonique $Q_0 \to \mathbb{Z}/8\mathbb{Z}$ et le morphisme $\mathbb{Z}/8\mathbb{Z} \to \operatorname{Aut} \mathbb{Z}/23\mathbb{Z}$ envoyant $\overline{1}$ sur $x \mapsto -x$. D'après (ii) et (x), on a soit $G \simeq \mathbb{Z}/23\mathbb{Z} \times Q_0$, soit $G \simeq G_0$. Ces deux groupes ne sont pas isomorphes : pour le premier on a $|I| = 1$, et pour le second $|I| = 2$. On a bien trouvé $4 + 2 = 6$ possibilités pour G.

Bibliographie

[AlBe95] J. Alperin & R. Bell, *Groups and representations*, Springer GTM 162 (1995).

[Ber90] M. Berger, *Géométrie*, tomes I et II, 2ème Ed. Nathan (1990).

[Che15] G. Chenevier, *Introduction aux formes modulaires*, mini-cours à l'École Normale Supérieure (2015).

[Che19] G. Chenevier, *Théorie algébrique des nombres*, cours à l'École Polytechnique (2019).

[Che22] G. Chenevier, *Sur un énoncé de la lettre de Galois à Chevalier*, à paraître à l'Enseignement Mathématiques (2023).

[CoSl89] J. Conway & N. Sloane, *Sphere Packings, Lattices and Groups* (1989).

[CoSm03] J. Conway & D. Smith, *On Quaternions and Octonions*, A. K. Peters, CRC Press (2003).

[ATLAS85] J. Conway, R. Curtis, S. Norton, R. Parker & R. Wilson, *ATLAS of finite groups*, Clarendon Press, Oxford (1985).

[Cox43] H. Coxeter, *Regular Polytopes*, Dover (1943).

[Dou05] R. & A. Douady, *Algèbre et théories galoisiennes*, Cassini (2005).

[Kle84] F. Klein, *Lectures on the Icosahedron and the solution of the Fifth Degree* (1884).

[Lan94] S. Lang, *Algebra*, 3eme Ed. Addison Wesley (1994).

[IrRo72] K. Ireland & M. Rosen, *A classical introduction to modern number theory*, Springer GTM 84 (1972).

[Per96] D. Perrin, *Cours d'algèbre*, Ellipses (1996).

[Ser70] J.-P. Serre, *Cours d'arithmétique*, P.U.F. (1970).

[Ser78] J.-P. Serre, *Groupes finis*, cours à l'École Normale Supérieure de Jeunes Filles (1978/1979).

[Ser78] J.-P. Serre, *Représentations linéaires des groupes finis*, Hermann (1978).

[StTa87] I. Stewart & D. Tall, *Algebraic Number Theory*, Chapman and Hall, 2ème Ed. (1987).