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 $n \geq 1$, 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 $n \geq 1$, $x^n = (x^{-1})^{-n}$ pour $n \leq -1$, 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 $n \geq 1$ 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 $n \geq 1$, 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 $H \leq G$ pour « H est un sous-groupe de G ». On a bien sur $\{1\} \leq G$ (sous-groupe *trivial*) et $G \leq G$ (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 $n \geq 1$, 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 $n \geq 1$, $g_1, g_2, \ldots, g_n \in X$ 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 $n \geq 0$ 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 $k^\times = k \setminus \{0\}$.*

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 :

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

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

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

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

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 $n \geq 2$ 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 $n \geq 3$. 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 $1 \leq k < n$, avec a (resp. b) un certain produit "dans l'ordre" des éléments x_i avec $i \leq k$ (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 $1 \leq k < n$, 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 $k \geq 2$, 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 $n \geq 1$, 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 $G \simeq G : \mathrm{id}_G$ 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 $n \geq 1$, 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