Examen du cours d'Algèbre 1, ENS Ulm, 18 Janvier 2022

Aucun document n'est autorisé. Temps de composition : 3h. On soignera la rédaction.

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 $n \geq 2$. En considérant l'action par translations de G sur G/H, montrer que $|G|$ divise $n!$.

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) En déduire que si $g, h \in \mathrm{A}_5$ sont d'ordres respectifs 3 et 5, alors g et h engendrent A_5.

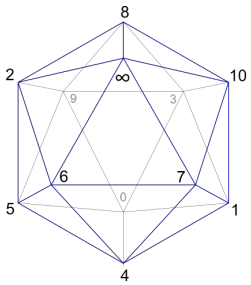
Soit H le sous-groupe de A_5 engendré par g et h. Par Lagrange, les ordres 3 et 5 de g et h divisent $|H|$. On a donc $15 \,|\, |H|$, et l'indice n de H dans G divise $60/15 = 4$. Comme A_5 est simple, le (i) affirme que l'on a soit $n = 1$ (i.e. $H = G$), soit $60 = |G| \,|\, 4! = 24$, ce qui est absurde.

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 $2 \cdot 6 \equiv 3 \cdot 4 \equiv 5 \cdot 9 \equiv 7 \cdot 8 \equiv 10^2 \equiv 1 \bmod 11$.

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) Conclure en contemplant l'icosaèdre suivant.



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. *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 $G \simeq \widetilde{\mathrm{A}_5}$* (Schur).

(i) Montrer que Z est inclus dans le centre de G.

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) 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 $\pi : G \to G/Z$.

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) (suite) En déduire $N \simeq \mathrm{A}_5$ et $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathrm{A}_5$.

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. $G \simeq Z \times N \simeq \mathbb{Z}/2\mathbb{Z} \times \mathrm{A}_5$.

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 $\mathrm{D}(G) = G$.

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) Montrer $r(G) \subset \mathrm{SL}_n(\mathbb{C})$.

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 suppose r irréductible. Montrer que l'on a $r(z) = 1_n$ ou $r(z) = -1_n$.

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 suppose* $r(z) = -1_n$. *Montrer* $n \equiv 0 \bmod 2$ *et que* r *est injective.*

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* $\{1\}$.

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* $\sum_{i\in I} (\dim U_i)^2 = |G| - |G/Z| = 60$.

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) *En déduire qu'il existe* $i \in I$ *avec* $\dim U_i = 2$.

D'après le (vii), on a $\dim U_i$ *pair pour tout* i. *On a aussi* $1 \leq \dim U_i^2 \leq 60$ *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) *Montrer que* G *est isomorphe à un sous-groupe fini de* $\mathrm{SL}_2(\mathbb{C})$.

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* $r(G) \subset \mathrm{SL}_2(\mathbb{Z})$ *par le (v) et* $G \simeq r(G)$ *par le (vii).*

(xi) *En déduire* $G \simeq \widetilde{\mathrm{A}_5}$. *On utilisera sans démonstration*[1] *le fait que tout sous-groupe fini de* $\mathrm{SL}_2(\mathbb{C})$ *est conjugué à un sous-groupe de* $\mathrm{Sp}(1)$.

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* $G \simeq \widetilde{A_5}$.

1. 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 $\mathrm{Sp}(1) = \mathrm{SU}(2)$.

(xii) (Application) En déduire $\mathrm{SL}_2(\mathbb{Z}/5\mathbb{Z}) \simeq \widetilde{\mathrm{A}_5}$.

D'après le cours, on a vu que pour p premier > 3, le centre Z de $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ est $\{\pm 1_2\} \simeq \mathbb{Z}/2\mathbb{Z}$ et que les seuls sous-groupes distingués de $G = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ 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. *Dans tout ce problème, p désigne un nombre premier. Soient G un sous-groupe de S_p avec $p \mid |G|$, et $0 \leq r < p$ 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.

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) Retrouver que le groupe $\mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$ est simple en le faisant agir sur $(\mathbb{Z}/2\mathbb{Z})^3 \smallsetminus \{0\}$.

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) 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. [2]

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 : 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.

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.

2. Le groupe M_{11} est le plus petit des groupes simples dits *sporadiques*.

(ii) *Montrer que le normalisateur de* $\langle c \rangle$ *dans* S_X *est* Aff_X.

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 : l'invariant r d'un sous-groupe transitif de S_p

Soit G *un sous-groupe de* S_p.

(i) *Montrer les équivalences entre :*

(a) p *divise* $|G|$,

(b) G *contient un* p*-cycle,*

(c) G *agit transitivement sur* $\{1, \dots, p\}$.

Montrons (a) $\Longrightarrow$ *(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)* $\Longrightarrow$ *(c) est claire. L'implication (c)* $\Longrightarrow$ *(a) vient de la formule orbite-stabilisateur (le cardinal de l'orbite d'un point est* p, *et divise* $|G|$.

On suppose désormais ces propriétés satisfaites. On note r_G *l'unique élément* $0 \leq r < p$ *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* $|G| = |\mathrm{N}_G(P)|\,\mathrm{n}_G$.

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) *Montrer* $|\mathrm{N}_G(P)| = p\,\mathrm{r}_G$ *et que* r_G *divise* $p - 1$.

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* $\mathrm{n_G} \equiv 1 \bmod p$ *par Sylow, on a* $q \equiv \mathrm{r}_G \bmod p$. *Comme* $1 \leq q \leq p - 1$ *on a* $\mathrm{r}_G = q$.

(iv) *On suppose* $\mathrm{r}_G = 1$. *Montrer que* G *possède exactement* n_G *éléments qui ne sont pas d'ordre* p.

Les p*-Sylows 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) *(suite) En considérant les stabilisateurs dans G des éléments de $\{1,\dots,p\}$, montrer $\mathrm{n}_G = 1$.*

Soit $i \in \{1,\dots,p\}$ 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 $\{1,\dots,p\}$, donc $G_i = \{1\}$, puis $\mathrm{n}_G = |G_i| = 1$.

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 $\{1,\dots,p\}$ sous l'action de N ont toutes même cardinal.*

L'orbite de $i \in \{1,\dots,p\}$ sous N est $Ni \subset \{1,\dots,p\}$. 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 $\{1,\dots,p\}$ 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 $\{1,\dots,p\}$, il pemute aussi transitivement les orbites sous N, qui ont donc toutes même cardinal.

(ii) *En déduire que p divise $|N|$.*

Les a N-orbites ont même cardinal, disons b, et forment une partition de $\{1,\dots,p\}$, 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) *Montrer $\mathrm{n}_N = \mathrm{n}_G$.*

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) *Montrer que r_N divise r_G.*

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) *Conclure.*

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 $\mathrm{r}_N = \mathrm{r}_G$. 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. *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.*

Par hypothèse, il existe $e_1, \dots, e_r \in M$ 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) *Soient $m \in M$ et $a \in \mathbb{Z}[i] \smallsetminus \{0\}$ avec $a\,m = 0$. Montrer $m = 0$.*

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 $\sum_{i=1}^{r} nx_i e_i = 0$ 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) *Conclure.*

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 $2s = r$.

(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*

$$u.u = v.v, \quad u.v = 0 \text{ et } L = \mathbb{Z}u + \mathbb{Z}v.$$

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 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 !