GROUPES

STÉPHANE LAMY

Ces notes reprennent certains des points vus en cours (mais pas tous), ou apportent quelques compléments (Jordan-Hölder notamment).

Table des matières

1. Isomorphismes entre S_3 et ...

Proposition. *Les groupes* $\mathrm{GL}_2(\mathbb{F}_2)$ *et* S_3 *sont isomorphes.*

Démonstration. Chaque $A \in \mathrm{GL}_2(\mathbb{F}_2)$ correspond à une bijection linéaire de $(\mathbb{F}_2)^2$, et donc à une permutation des trois vecteurs non nuls $v_1 = (1,0)$, $v_2 = (0,1)$, $v_3 = (1,1)$. Autrement dit il existe $\sigma_A \in S_3$ tel que $A(v_i) = v_{\sigma_A(i)}$. L'application φ qui a $A \in \mathrm{GL}_2(\mathbb{F}_2)$ fait correspondre $\sigma_A \in S_3$ est un morphisme, et est injective car A est l'identité ssi elle fixe les deux vecteurs de la base v_1, v_2. φ est donc l'isomorphisme cherché. □

Proposition. *Les groupes* $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ *et* S_3 *sont isomorphes.*

Démonstration. Découle de la proposition précédente, en remarquant qu'un automorphisme du groupe additif $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est automatiquement un automorphisme de $\mathbb{F}_2$-espace vectoriel (pas beaucoup de scalaires dans $\mathbb{F}_2$...) □

Proposition. *Les groupes* $\mathrm{Aut}(S_3)$ *et* S_3 *sont isomorphes.*

Démonstration. L'application qui à σ fait correspondre l'automorphisme intérieur $\sigma' \mapsto \sigma\sigma'\sigma^{-1}$ est un morphisme injectif de S_3 dans $\mathrm{Aut}(S_3)$, car le centre de S_3 est trivial.

De plus $\varphi \in \mathrm{Aut}(S_3)$ est déterminé par l'image des générateurs (12) et (13). Il y a au plus six choix possibles (choisir deux parmi les trois éléments d'ordre 2 de S_3), donc en comparant les cardinaux on obtient que le morphisme ci-dessus est un isomorphisme. □

Proposition. *Un groupe* G *d'ordre 6 est isomorphe à* $\mathbb{Z}/6\mathbb{Z}$ *ou* S_3*.*

Démonstration. Soit G un groupe d'ordre 6, et $g \in G$ distinct de l'élément neutre. Par Lagrange, l'ordre de g est 2, 3 ou 6. Si G admet un élément d'ordre 6, il est cyclique et donc isomorphe à $\mathbb{Z}/6\mathbb{Z}$. Sinon, G n'admet que des éléments d'ordre 2 ou 3 à part le neutre. Il ne peut pas contenir deux éléments a, b d'ordre 2 tel que le produit ab soit aussi d'ordre 2, car alors $\{1, a, b, ab\}$ serait un sous-groupe, contradiction avec Lagrange. Donc G contient au moins un élément d'ordre 3, et comme les éléments d'ordre 3 arrivent par paire g, g^{-1}, il y en a au plus 4 dans G. Bilan : G contient un élément τ d'ordre 2, et un élément γ d'ordre 3. On a $G = \langle \tau, \gamma \rangle$, par Lagrange à nouveau. Les éléments τ et γ ne commutent pas, sinon $\tau\gamma$ serait d'ordre $\mathrm{PPCM}(2,3) = 6$ et on a exclu ce cas. Donc $\gamma\tau\gamma^{-1}$ est d'ordre 2 et distinct de τ, donc il y a exactement 2 éléments d'ordre 3 dans G qui sont τ et τ^{-1} (plus la place pour deux autres...). Finalement $\sigma\tau\sigma = \tau^{-1}$ (seul

Date: 2 novembre 2016.

élément d'ordre 3 distinct de τ), et cette identité permet de reconstruire entièrement la table de G, qui coïncide donc avec celle de S_3, via l'isomorphisme $\varphi(\tau) = (12)$ et $\varphi(\gamma) = (123)$. □

Remarque. Il n'est pas raisonnable de montrer la proposition précédente à l'aide des théorèmes de Sylow (adapter la taille de votre marteau à la taille du clou...). Bien avoir conscience que le "théorème" de Lagrange est essentiellement une trivialité. Les théorèmes de Sylow par contre, qui ne sont pas formellement au programme, sont une application un peu ardue de la notion d'action de groupes (qui elle est centrale dans le programme), et ne seront bienvenus que pour montrer des résultats un peu plus avancés, du genre "voici la liste des groupes d'ordre 12" ou "tout groupe simple d'ordre 60 est isomorphe à A_5".

2. Morphisme signature

Proposition. *Il existe un unique morphisme de groupes non trivial $S_n \to \mathbb{C}^*$. Ce morphisme, appelé le morphisme signature, est en fait à valeur dans $\{\pm 1\}$, et prend la valeur -1 sur toute transposition de S_n.*

Démonstration. Soit $\varphi\colon S_n \to \mathbb{C}^*$ un morphisme de groupes. Comme $\mathbb{C}^*$ est abélien, si σ_1, σ_2 sont deux éléments de S_n, on a $\varphi(\sigma_1\sigma_2\sigma_1^{-1}) = \varphi(\sigma_2)$.

Par ailleurs, si $\tau \in S_n$ est une transposition, on a

$$\varphi(\tau)^2 = \varphi(\tau^2) = \varphi(\mathrm{id}) = 1,$$

d'où $\varphi(\tau) = \pm 1$.

Les transpositions sont deux à deux conjuguées dans S_n, ainsi ou bien $\varphi(\tau) = 1$ pour toute transposition et φ est le morphisme trivial, ou bien $\varphi(\tau) = -1$ pour toute transposition comme annoncé.

Reste à voir qu'en posant $\varphi(\tau) = -1$ pour toute transposition on définit bien un morphisme. Une façon est de constater que la formule

$$\varphi(\sigma) := \prod_{i<j} \frac{\sigma(j) - \sigma(i)}{j - i}$$

définit un morphisme, et vaut -1 sur la transposition $(1\,2)$ (et donc sur toutes) :

$$\begin{aligned}
\varphi(\sigma \circ \sigma') &= \prod_{i<j} \frac{\sigma(\sigma'(j)) - \sigma(\sigma'(i))}{j - i} \frac{\sigma'(j) - \sigma'(i)}{\sigma'(j) - \sigma'(i)} \\
&= \left(\prod_{i<j} \frac{\sigma(\sigma'(j)) - \sigma(\sigma'(i))}{\sigma'(j) - \sigma'(i)} \right) \left(\prod_{i<j} \frac{\sigma'(j) - \sigma'(i)}{j - i} \right) \\
&= \varphi(\sigma)\varphi(\sigma'), c
\end{aligned}$$

et si $\tau = (1\,2)$, on a

$$\begin{aligned}
\varphi(\tau) &= \prod_{i<j} \frac{\tau(j) - \tau(i)}{j - i} \\
&= \frac{\tau(2) - \tau(1)}{2 - 1} \prod_{j\geq 3} \frac{\tau(j) - \tau(1)}{j - 1} \prod_{j\geq 3} \frac{\tau(j) - \tau(2)}{j - 2} \prod_{j>i\geq 3} \frac{\tau(j) - \tau(i)}{j - i} \\
&= \frac{1 - 2}{2 - 1} \prod_{j\geq 3} \frac{j - 2}{j - 1} \prod_{j\geq 3} \frac{j - 1}{j - 2} \prod_{j>i\geq 3} \frac{j - i}{j - i} \\
&= -1
\end{aligned}$$

□

3. S_4 comme groupe d'isométries

On peut voir le groupe symétrique S_4 comme le groupe des isométries de $\mathbb{R}^3$ préservant un tétraèdre régulier (action sur les 4 sommets, ou sur les 4 faces), ou comme le groupe des isométries directes préservant un cube (action sur les 4 grandes diagonales). C'est un bon exercice d'interpréter les propriétés abstraites que l'on connaît sur ce groupe en termes géométriques (classes de conjugaison, sous-groupes distingués...)

Lemme. *Le groupe S_4 contient six transpositions.*

Cube : Retournement d'axe par les milieux de deux arêtes opposées.

Tétraèdre : Symétrie de plan contenant une arête et le milieu de l'arête opposée.

Lemme. *Le groupe S_4 contient huit 3-cycles.*

Cube : Rotations d'axe l'une des 3 grandes diagonales.
Tétraèdre : Rotations d'axe passant par un sommet et le milieu de la face opposée.

Lemme. *Le groupe S_4 contient six 4-cycles.*

Cube : Rotations d'axe passant par les centres de deux faces opposées.
Tétraèdre : La moins évidente... En reliant les milieux de 4 des 6 arêtes on peut construire un carré (3 choix), la rotation d'un quart de tour de ce carré suivi de la symétrie par rapport au plan contenant le carré est l'un des 4-cycles cherchés.

Lemme. *Le groupe S_4 contient trois double-transpositions.*

Cube : Retournement d'axe passant par les centres de deux faces opposées.
Tétraèdre : Retournement d'axe passant par les milieux d'arêtes opposées.

Lemme. *Il existe un morphisme de S_4 vers S_3, dont le noyau est V_4.*

Cube : Agir sur les paires de faces opposées.
Tétraèdre : Agir sur les paires d'arêtes opposées.

Lemme. *Les 2-Sylow (d'ordre 8) de S_4 sont isomorphes au groupe diédral D_4, et sont au nombre de trois. Leur intersection est égal à V_4.*

Cube : Considérer les trois carrés obtenus en tranchant par un hyperplan médiateur à une arête.
Tétraèdre : Considérer les trois carrés obtenus en tranchant par un plan passant par les milieux de 4 arêtes .

Lemme. *Dans A_4 il y a 2 classes de conjugaison de 3-cycles.*

Cube : A_4 correspond au groupe préservant le coloriage en damier des sommets, les grandes diagonales peuvent alors être orientées (disons blanc vers noir), et les rotations tournent d'un tiers de tour dans le sens direct ou indirect. Note : en reliant les sommets d'une même couleur on obtient un tétraèdre, ce qui fait le lien avec l'autre point de vue.
Tétraèdre : A_4 correspond au groupe des isométries préservant l'orientation. On peut orienter les axes depuis un sommet vers le centre de la face opposée. Alors les rotations tournent d'un tiers de tour dans le sens direct ou indirect.

4. Le groupe de l'icosaèdre

Proposition. *Soit G un sous-groupe fini de $\mathrm{SO}_3(\mathbb{R})$ dont l'action sur les pôles comporte exactement trois orbites de cardinaux respectifs 30, 20 et 12, correspondant à des stabilisateurs d'ordre 2, 3 et 5. Alors G est le groupe des isométries directes préservant un icosaèdre régulier.*

Démonstration. Notons x l'un des pôles contenus dans l'orbite de cardinal 12, et notons $\mathcal{P}$ l'enveloppe convexe de $\mathrm{Orb}(x)$. Par définition G agit transitivement sur l'ensemble des 12 sommets de $\mathcal{P}$. Comme $\mathrm{Stab}(x)$ est d'ordre 5, il est cyclique, et donc il y a au moins 5 arêtes issues du sommet x. Mais par la formule d'Euler (portant sur les nombres S, A, F de sommets, d'arêtes et de faces de $\mathcal{P}$), on montre que la valence v_S des sommets est au plus 5 :

$$S - A + F = 2, \quad v_S \cdot S = 2A, \quad 3 \cdot F \leq 2A$$

implique

$$\frac{1}{v_S} + \frac{1}{3} \geq \frac{1}{2} + \frac{1}{A} \quad \Rightarrow \quad \frac{1}{v_S} > \frac{1}{6} \quad \Rightarrow \quad v_S < 6.$$

On en déduit que G agit transitivement sur les arêtes de $\mathcal{P}$. En effet si y est un sommet voisin de x, et x', y' deux autres sommets voisins de $\mathcal{P}$, on peut envoyer x sur x' par transitivité de l'action sur les sommets, puis y sur y' par transitivité de $\mathrm{Stab}(x)$ sur les voisins de x.

Le même raisonnement montre que G agit transitivement sur les faces, et même mieux, sur les drapeaux orientés : si y, z sont deux sommets voisins consécutif de x, et y', x', z' trois autres sommets consécutifs d'une face, on peut envoyer x' sur x, y' sur y, et donc z' sur z si les orientations coincidaient.

Finalement les formules ci-dessus donne que $A = 30$, $F = 20$ et la valence des faces vérifiant $v_F \cdot F = 2A$, ce sont des triangles équilatéraux, et finalement $\mathcal{P}$ est un icosaèdre régulier. □

5. Sylow

Référence : [Per96], [Ser78].

Soit G un groupe fini et p un nombre premier. Si $|G| = p^a m$ avec $p \wedge m = 1$, alors on appelle p-Sylow (abbréviation de p-sous-groupe de Sylow) tout sous-groupe $S \subset G$ de cardinal p^a.

Proposition. *Soit $S \subset G$ un p-Sylow, et $H \subset G$ un sous-groupe. Alors il existe $g \in G$ tel que $gSg^{-1} \cap H$ soit un p-Sylow de H.*

Démonstration. On note comme ci-dessus $|G| = p^a m$, et de même $|H| = p^b n$. On fait agir G (et donc également H) par translation sur l'ensemble X des classes à gauche de G modulo S. Noter que $g' \in \mathrm{Stab}(gS)$ équivaut à $g' \in gSg^{-1}$. Par ailleurs l'ensemble X est de cardinal m, qui n'est pas multiple de p. L'une des orbites Ω de X sous l'action de H est donc de cardinal non multiple de p. Soit $x = gS \in \Omega$. Le stabilisateur $\mathrm{Stab}(x)$ est de la forme $H \cap gSg^{-1}$, donc de cardinal p^c pour un certain $c \leq b$. Mais comme de plus $|\mathrm{Stab}(x)| \cdot |\Omega| = |H| = p^b n$ et $|\Omega| \wedge p = 1$, on a finalement $|\Omega| = n$ et $|\mathrm{Stab}(x)| = p^b$ comme attendu. □

Théorème. *Soit p un nombre premier. Tout groupe fini G dont le cardinal est un multiple de p admet un p-Sylow.*

Démonstration. L'idée est d'exhiber un plongement de G dans un groupe G' dont on sait qu'il contient un p-Sylow, afin d'appliquer la proposition.

Le rôle du groupe G' va être joué par un groupe linéaire $\mathrm{GL}_n(\mathbb{F}_p)$, où $\mathbb{F}_p$ est le corps à p éléments et n sera assez grand, disons le cardinal du groupe. En effet montrons que le sous-groupe $T \subset \mathrm{GL}_n(\mathbb{F}_p)$ des matrices triangulaires unipotentes (c'est-à-dire, avec des 1 sur la diagonale) supérieures est un p-Sylow. Le cardinal de $\mathrm{GL}_n(\mathbb{F}_p)$ est (compter les bases de $(\mathbb{F}_p)^n$) :

$$|\mathrm{GL}_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p)(p^n - p^2) \dots (p^n - p^{n-1}) = p^{1+2+\dots+(n-1)} m,$$

avec $m \wedge p = 1$. Or $p^{1+2+\dots+(n-1)}$ est le cardinal de T.

Par ailleurs tout groupe fini G se plonge dans un groupe symétrique S_n (faire agir G sur lui-même par translation, ce qui montre que $n = |G|$ convient). De plus le groupe symétrique S_n se plonge dans $\mathrm{GL}_n(\mathbf{k})$, pour tout corps $\mathbf{k}$. □

Une propriété des p-groupes :

Lemme. *Tout p-groupe (non trivial) admet un centre non trivial, et donc en particulier admet un élément central d'ordre p.*

Démonstration. On fait agir G sur lui-même par conjugaison. Les orbites sont ou bien de cardinal 1 (pour chaque élément du centre), ou bien de cardinal une puissance de p non égale à 1. En écrivant G comme une union d'orbites, on a donc $|Z(G)| \equiv 0 \mod p$, ce qui interdit à $Z(G)$ d'être trivial. □

Énoncés des "théorèmes de Sylow" :

Théorème. *Soit G un groupe de cardinal $p^a m$, avec p premier et $m \wedge p = 1$. Alors :*

1. *Pour tout $0 \leq b \leq a$, G admet un sous-groupe d'ordre p^b ;*
2. *Soit S un p-Sylow de G et H un p-sous-groupe de G, alors il existe $g \in G$ tel que $H \subset gSg^{-1}$. En particulier les p-Sylow sont deux à deux conjugués.*
3. *Le nombre de p-Sylow divise m est est congru à 1 modulo p.*

Démonstration. (1) Vu le théorème précédent, il suffit de le vérifier lorsque G est un p-groupe. C'est clair pour un groupe d'ordre 1 ou p ($a = 0$ ou 1), et on procède alors par récurrence sur l'ordre de G. On peut supposer $b \geq 1$, sinon c'est évident. Il existe un élément x d'ordre p dans le centre de G. Le quotient $G/\langle x \rangle$ admet un sous-groupe d'ordre p^{b-1}, qui provient d'un groupe d'ordre p^b dans G.

(2) La proposition donne l'existence de g tel que $gSg^{-1} \cap H = H$, ce qui équivaut à $H \subset gSg^{-1}$.

(3) On fait agir G par conjugaison sur l'ensemble X des p-Sylow de G. On vient de voir que cette action est transitive. Soit S un p-Sylow de G. On a donc

$$|\mathrm{Stab}(S)| \cdot |X| = p^a m,$$

et comme $S \subset \mathrm{Stab}(S)$ on a $p^a \mid |\mathrm{Stab}(S)|$, et donc $|X| \mid m$.

On restreint maintenant cette même action à S. Chaque orbite est ou bien un singleton, ou bien de cardinal une puissance de p. Chaque singleton correspond à un p-Sylow T qui est

normalisé par S, c'est-à-dire $sTs^{-1} = T$ pour tout $s \in S$. Considérons $H = \langle S, T\rangle \subset G$. Alors S, T sont des p-Sylow de H, et $T \lhd H$, on a donc $S = T$. Finalement, en écrivant X comme l'union des orbites sous l'action de S, on obtient que $|X|$ est congru à 1 (l'unique singleton) modulo p. □

6. Produits (semi-)directs

Commençons par une fausse piste. Si $H, K \subset G$ sont deux sous-groupes et que $(k, h) \mapsto kh$ définit une bijection du produit cartésien ensembliste $K \times_{\text{ens}} H$ vers G, on pourrait avoir envie de dire que G est le "produit" de ses sous-groupes K et H. C'est parfait d'un point de vue ensembliste, le problème est qu'une telle bijection n'explique pas comment relier la structure de groupe sur G à celle sur K et H.

La situation naturelle dans le contexte des groupes est plutôt la suivante : on a $K \lhd G$ distingué dans G, $H = G/K$ est le groupe quotient, et on se demande comment reconstruire G à partir de K et H. Par rapport à la fausse piste précédente, on a désymétrisé la situation :

- On a ajouté de l'information sur K (il est normal dans G) ;
- On a retiré de l'information sur H (ce n'est plus un sous-groupe de G).

Maintenant contemplons la définition suivante.

Définition. Soit G un groupe, $K \lhd G$ distingué et $H \subset G$ un sous-groupe. Si l'application $(k, h) \mapsto kh$ est une bijection de $K \times_{\text{ens}} H$ vers G, on dit que G est le produit semi-direct de K et H, et on note $G = K \rtimes H$.

Dans cette situation les éléments de H forment un système de représentants des classes modulo K, et H est isomorphe au quotient G/K.

D'autre part si $k_1, k_2 \in K$ et $h_1, h_2 \in H$, on a

$$(k_1h_1)(k_2h_2) = \underbrace{k_1h_1k_2h_1^{-1}}_{\in K}\underbrace{h_1h_2}_{\in H}.$$

Donnons un critère qui permet de vérifier que l'application dans la définition est une bijection (indépendamment du fait que ces sous-groupes soient distingués ou non) :

Lemme. *Soient K, H deux sous-groupes d'un groupe G. L'application $\varphi\colon (k, h) \mapsto kh$ est une bijection de $K \times_{ens} H$ vers G si et seulement si $KH = G$ et $K \cap H = \{1\}$.*

Démonstration. Par définition φ est surjective ssi $KH = G$.

Supposons φ injective. Soit $g \in K \cap H$. On a $g = \varphi(g, 1) = \varphi(1, g)$, par injectivité $(g, 1) = (1, g)$, et donc $g = 1$.

Réciproquement supposons $K \cap H = \{1\}$, et $\varphi(k_1, h_1) = \varphi(k_2, h_2)$. Alors $k_2^{-1}k_1 = h_2h_1^{-1}$ est un élément de $K \cap H$ donc est égal à 1, ce qui donne $k_1 = k_2$ et $h_1 = h_2$. Ainsi φ est injective. □

Reformulation en termes de suite exacte. Si $K \lhd G$ un sous-groupe distingué, on a la suite exacte

$$1 \to K \xrightarrow{i} G \xrightarrow{p} G/K \to 1.$$

S'il existe une section $s : G/K \to G$, c'est-à-dire un morphisme (forcément injectif) de groupe tel que $p \circ s = \mathrm{id}$, alors G est le produit semi-direct de K et $H = s(G/K)$.

On peut voir la notion de produit direct comme un cas particulier de la précédente.

Définition. Soit G un groupe, et $H, K \lhd G$ deux sous-groupes distingués. Si l'application $(k, h) \mapsto kh$ est une bijection de $K \times_{\text{ens}} H$ vers G (autrement dit si $KH = G$ et $K \cap H = \{1\}$), on dit que G est le produit direct ("interne", voir plus bas) de K et H, et on note $G = K \times H$.

Proposition. *Dans les conditions de la définition, pour tous $h \in H$, $k \in K$, on a $hk = kh$. En particulier la loi de groupe sur G est donnée par (pour tous $k_1, k_2 \in K$ et $h_1, h_2 \in H$) :*

$$(k_1h_1)(k_2h_2) = k_1k_2h_1h_2.$$

Démonstration. Il suffit d'écrire $hkh^{-1}k^{-1} = (\underbrace{hkh^{-1}}_{\in K})k^{-1} = h(\underbrace{kh^{-1}k^{-1}}_{\in H}) \in K \cap H$. □

Étant donnés deux groupes K et H (qui ne sont plus supposés sous-groupes d'un même groupe G ambiant), on peut construire le produit direct *externe* de K et H en munissant le produit cartésien ensembliste de la loi "multiplier facteur par facteur".

On obtient un groupe $G := K \times H$ qui contient $K \times_{\text{ens}} \{1\}$ et $\{1\} \times_{\text{ens}} H$ qui sont des sous-groupes isomorphes à K et H, et on a une structure de produit direct *interne*

$$G = (K \times_{\text{ens}} \{1\}) \times (\{1\} \times_{\text{ens}} H).$$

Il y a de même une notion de produit semi-direct *externe*, qui répond à la question "étant donnés K et H, comment construire un groupe G dans lequel se plongent K et H, de façon à ce que G soit produit semi-direct des ces copies de K et H" ? C'est plus compliqué, je ne l'aborde pas dans le cours (mais c'est indispensable je crois pour ceux qui veulent traiter en développement les groupes d'ordre pq, ou d'ordre 12).

Exemples. • $S_n = A_n \rtimes \mathbb{Z}/2\mathbb{Z}$, où $\mathbb{Z}/2\mathbb{Z}$ est identifié au sous-groupe de S_n engendré par une transposition (ou plus généralement par un élément d'ordre 2 de signature -1, par exemple une triple transposition. Beaucoup de choix possibles donc).

• $\mathbb{D}_n = \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$, où $\mathbb{Z}/2\mathbb{Z}$ est identifié au sous-groupe engendré par une symétrie axiale (la symétrie centrale appartient à $\mathbb{D}_n$ quand n est pair, mais ne convient pas car elle préserve l'orientation).

• $\mathrm{GL}_n(\mathbf{k}) = \mathrm{SL}_n(\mathbf{k}) \rtimes \mathbf{k}^\times$, où le groupe multiplicatif $\mathbf{k}^\times$ est identifié au groupe des matrices diagonales $\{\mathrm{diag}(a, 1, \dots, 1);\ a \in \mathbf{k}^\times\}$.

• Isom(tétraèdre) = Isom^+(tétraèdre) $\rtimes \mathbb{Z}/2\mathbb{Z}$ (c'est une interprétation géométrique de $S_4 = A_4 \rtimes \mathbb{Z}/2\mathbb{Z}$) ;

• Isom(cube) = Isom^+(cube) $\rtimes \mathbb{Z}/2\mathbb{Z}$ (en prenant une symétrie par rapport à un plan de symétrie pour générateur du groupe d'ordre 2), mais on peut également écrire Isom(cube) = Isom^+(cube) $\times \mathbb{Z}/2\mathbb{Z}$ (en prenant la symétrie centrale pour générateur du groupe d'ordre 2) ;

• Le groupe affine d'un espace de dimension n : $\mathrm{Aff}_n = \mathbf{k}^n \rtimes \mathrm{GL}_n(\mathbf{k})$, où le groupe additif $\mathbf{k}^n$ est identifié aux translations.

• A_5 contient A_4 et $\mathbb{Z}/5\mathbb{Z}$ comme sous-groupes, on a la bijection "fausse piste" $A_4 \times_{\text{ens}} \mathbb{Z}/5\mathbb{Z} \to A_5$, mais A_5 n'est certainement pas un produit semi-direct : il est simple, donc est considéré comme un "atome" (étymologiquement : "qu'on ne peut pas couper en parties plus petites").

7. Jordan-Hölder

Référence : [Ser78].

Rapport Jury 2015 (sur la leçon 103) : "*Il faut savoir pourquoi on s'intéresse particulièrement aux groupes simples*"...

Une filtration d'un groupe G est une suite finie de sous-groupes de G

$$\{1\} = G_0 \subsetneq G_1 \subsetneq \cdots \subsetneq G_n = G$$

avec G_{i-1} normal dans G_i pour tout $i = 1, \dots, n$. Une filtration où chacun des quotients G_i/G_{i-1} est simple est appelée une suite de Jordan-Hölder.

Proposition. *Tout groupe fini admet une suite de Jordan-Hölder.*

Démonstration. Le cas du groupe trivial ($n = 0$) est clair, tout comme celui d'un groupe simple ($n = 1$). Traitons maintenant le cas d'un groupe fini G qui est non simple et non trivial, en procédant par récurrence sur le cardinal de G. Soit $N \subsetneq G$ un sous-groupe normal propre maximal de G. Alors le quotient G/N est simple : en effet de manière générale les sous-groupes normaux d'un quotient G/N sont en bijection avec les sous-groupes normaux de G contenant N. Par hypothèse de récurrence N admet une suite de Jordan-Hölder $(N_i)_{i=0}^n$, et $N_0, \dots, N_{n-1}, N, G$ est alors une suite de Jordan-Hölder pour G. □

Théorème. *Soit G un groupe fini, et $(G_i)_{i=0}^n$ une suite de Jordan-Hölder de G. L'ensemble des quotients G_i/G_{i-1} (c'est-à-dire la suite des quotients à permutation des indices près) ne dépend que de G.*

Démonstration. Il s'agit de montrer que si S est un groupe fini simple fixé, le nombre $n(G, S)$ de quotient G_i/G_{i-1} isomorphes à S est (comme la notation l'anticipe) indépendant de la suite (G_i).

Comme dans la preuve de l'existence, les cas où G est trivial ou simple sont clairs, et on raisonne ensuite par récurrence sur le cardinal de G.

Soit $N \subsetneq G$ un sous-groupe normal propre de G (il ne semble pas y avoir d'avantage à prendre N maximal). La suite (G_i) induit des suites de Jordan-Hölder à la fois sur N et sur

G/N, en posant (remarquer que les G_iN forment une suite de sous-groupes de G contenant N) :

$$N_i := N \cap G_i, \quad (G/N)_i := (G_iN/N).$$

Ces groupes sont reliés par la suite exacte (les isomorphismes sont donnés par les théorèmes de Noether, rappelés juste après la preuve) :

$$1 \to N_i/N_{i-1} \simeq N_iG_{i-1}/G_{i-1} \to G_i/G_{i-1} \to (G_iN/N)/(G_{i-1}N/N) \simeq G_iN/G_{i-1}N \to 1.$$

Comme G_i/G_{i-1} est simple, dans cette suite exacte deux des groupes sont isomorphes et le troisième est trivial. On peut donc réaliser une partition $I_1 \cup I_2 = \{1, \dots, n\}$ de l'ensemble des indices de telle sorte que

- $i \in I_1$ si $N_i/N_{i-1} \simeq G_i/G_{i-1}$;
- $i \in I_2$ si $G_i/G_{i-1} \simeq (G/N)_i/(G/N)_{i-1}$.

En particulier N admet une suite de Jordan-Hölder indicée par I_1, et G/N une suite indicée par I_2. Par hypothèse de récurrence, $n(N, S)$ et $n(G/N, S)$ sont indépendants du choix d'une suite, et comme avec les suites ci-dessus on a par construction

$$n(G, S) = n(N, S) + n(G/N, S),$$

le nombre $n(G, S)$ est également indépendant du choix d'une suite. □

On a utilisé :

Théorème (Noether)**.**

(1) *Soit $N \lhd G$ et $H \subset G$, alors $H/(H \cap N) \simeq HN/N$.*

(2) *Soit $N \lhd G$, $M \lhd G$ avec $M \subset N$, alors $(G/M)/(N/M) \simeq G/N$.*

8. Groupes abéliens finis

Rappelons d'abord deux énoncés basiques :

Lemme. *Soit $a \in G$ un élément d'ordre mn, pour certains $m, n \geq 1$. Alors a^m est d'ordre n.*

Lemme. *Soit G abélien et a, b d'ordres finis premiers entre eux. Alors* ordre $ab =$ ordre a ordre b.

Démonstration. Soit $d =$ ordre ab, il s'agit de voir que ordre a ordre $b \mid d$, ce qui impliquera l'égalité. On a $1 = (ab)^d = a^db^d$, donc ordre $a^d =$ ordre b^d. Mais ces deux ordres sont des diviseurs respectifs de ordre a et ordre b qui sont premiers entre eux, donc ordre $a^d =$ ordre $b^d = 1$. Autrement dit ordre $a \mid d$ et ordre $b \mid d$, comme attendu. □

L'exposant d'un groupe fini G est défini comme le PPCM de l'ordre de tous les éléments de G.

Proposition. *Soit G un groupe abélien fini, et soit m le maximum parmi les ordres des éléments de G. Alors l'ordre de tout élément de G divise m, en particulier m est l'exposant de G.*

Démonstration. Soit $x \in G$ réalisant l'ordre maximal m, et supposons qu'il existe $y \in G$ dont l'ordre q ne divise pas m. Ceci implique qu'il existe un premier p et des entiers $b > a$ tels que

$$m = p^am' \quad \text{et} \quad q = p^bq',$$

avec m', n' premiers avec p. Alors par les lemmes ordre$(y^{q'}x^{p^a}) = p^bm' > m$, absurde. □

Corollaire. *Soit $\mathbf{k}$ un corps, et G un sous-groupe fini du groupe multiplicatif $\mathbf{k}^\times$. Alors G est cyclique. En particulier , pour tout premier p le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique.*

Démonstration. Soit $x \in G$ réalisant l'exposant m. Par la proposition tout élément y de G vérifie $y^m = 1$, de plus le polynôme $X^m - 1$ admet au plus m racines sur le corps $\mathbf{k}$. Mais on connaît déjà m racines de ce polynôme, à savoir $1, x, x^2, \dots, x^{m-1}$. Ainsi G est égal au groupe cyclique engendré par x. □

Proposition. *Soit G un groupe abélien fini et $x \in G$ réalisant l'exposant m de G. Alors il existe un sous-groupe K de G tel que*

$$G = K \times \langle x \rangle.$$

Démonstration. On cherche à construire K comme noyau d'un morphisme de G dans $\langle x\rangle$ qui envoie x sur x, cette dernière condition assurant que $K\cap\langle x\rangle=\{1\}$ et donc qu'on a bien une structure de produit direct pour G. Supposons un tel morphisme φ construit sur H contenant $\langle x\rangle$, et cherchons à étendre φ sur un sous-groupe $\langle y,H\rangle$ où $y\in G\setminus H$. L'existence de φ quand $H=\langle x\rangle$ est triviale et permet d'amorcer le raisonnement, et le φ cherché s'obtient en prenant une suite finie de telles extensions. Notons b l'ordre de y, et notons y^β un générateur de $\langle y\rangle\cap H$. Par définition b divise m, et β divise b. De plus il existe $\alpha\in\mathbb{N}$ tel que $\varphi(y^\beta)=x^\alpha$. Si on peut montrer que $\alpha=n\beta$ pour un certain $n\in\mathbb{N}$, on pourra prolonger φ à $\langle y,H\rangle$ en posant $\varphi(y)=x^n$ (si vous ressentez le besoin d'un argument formel ici, voir plus bas).

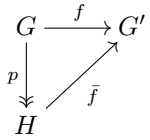
Écrivons $m=bb'$ et $b=\beta\beta'$. Alors $1=\varphi(y^{\beta\beta'})=x^{\alpha\beta'}$, donc $\alpha\beta'=km$ pour un certain $k\geq 1$. On obtient

$$\alpha\beta'=km=kb'b=kb'\beta'\beta \qquad \text{d'où} \qquad \alpha=kb'\beta$$

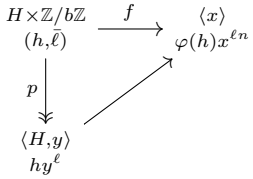
et $n=kb'$ est l'entier attendu. □

Dans la preuve on a utilisé implicitement le résultat général suivant de "factorisation" :

Lemme. *Si $f\colon G\to G'$ est un morphisme de groupe, et $p\colon G\twoheadrightarrow H$ est un morphisme surjectif, alors il existe $\bar f\colon H\to G'$ qui fasse commuter le diagramme suivant si et seulement si* $\ker p\subset\ker f$.



En effet dans le contexte de la preuve de la proposition on applique ce lemme au diagramme :



Théorème. *Soit G un groupe abélien fini (non trivial). Il existe une unique suite d'entiers $(a_i)_{i=1}^s$ tels que $a_{i+1}\mid a_i$ pour tout $i=1,\dots s-1$, $a_s\geq 2$, et*

$$G\simeq\mathbb{Z}/a_1\mathbb{Z}\times\cdots\times\mathbb{Z}/a_s\mathbb{Z}.$$

En particulier a_1 est l'exposant du groupe, et $\prod a_i$ est le cardinal du groupe.

Preuve de l'existence. Le résultat est clair pour G cyclique. Supposons maintenant G non cyclique, et raisonnons par récurrence sur $|G|$. Posons a_1 égal à l'exposant de G. Par la proposition, il existe K un sous-groupe de G tel que $G\simeq\mathbb{Z}/a_1\mathbb{Z}\times K$. De plus K est non trivial puisque G est supposé non cyclique. Par hypothèse de récurrence le groupe K admet une factorisation

$$K\simeq\mathbb{Z}/a_2\mathbb{Z}\times\cdots\times\mathbb{Z}/a_s\mathbb{Z},$$

où a_2 est l'exposant de K. Reste à remarquer que l'exposant d'un sous-groupe divise l'exposant du groupe ambiant, et donc $a_2\mid a_1$. □

Ce résultat d'existence peut s'exprimer avec le langage des représentations (cf [Colmez, p. 250-252], je compte le faire lors du cours d'avril) :

L'unicité est un peu plus délicate à obtenir (il n'est pas clair que le groupe K soit unique dans la preuve ci-dessus). Le moyen le plus rapide semble être de commencer par l'établir pour les p-groupes.

Pour alléger un peu l'écriture je note dans la suite $\mathbb{Z}/n$ au lieu de $\mathbb{Z}/n\mathbb{Z}$.

Lemme. *Soit G un p-groupe, et*

$$G\simeq\mathbb{Z}/p^{b_1}\times\cdots\times\mathbb{Z}/p^{b_s}$$

une factorisation donnée par le théorème. Alors les b_i sont uniquement déterminés par G.

Démonstration. Rappelons que p^{b_1} est l'exposant du groupe. Si $b_1=1$, le résultat est clair, et on raisonne maintenant par récurrence sur b_1. Considérons le sous-groupe $G^p:=\{g^p;\ g\in G\}$, on a

$$G^p\simeq\mathbb{Z}/p^{b_1-1}\times\cdots\times\mathbb{Z}/p^{b_s-1}.$$

Les $b_i-1\geq 1$ sont uniquement déterminés par hypothèse de récurrence, donc les $b_i\geq 2$, et finalement aussi les $b_i=1$ en comparant les cardinaux. □

Preuve de la partie "unicité" dans le théorème. Soit p un nombre premier divisant $|G|$, et S l'unique p-Sylow de G. Étant donnée une factorisation

$$G \simeq \mathbb{Z}/a_1 \times \cdots \times \mathbb{Z}/a_s,$$

notons b_i l'entier tel que $a_i = p^{b_i} n_i$ avec n_i premier avec p. Alors en considérant dans chaque $\mathbb{Z}/a_i$ l'unique sous-groupe d'ordre p^{b_i}, on obtient une factorisation :

$$S \simeq \mathbb{Z}/p^{b_1} \times \cdots \times \mathbb{Z}/p^{b_s}.$$

Par le lemme les b_i sont uniquement déterminés. Ainsi la puissance de p intervenant dans la factorisation de chaque a_i est uniquement déterminée, et ceci étant vrai pour tout premier p, les a_i eux-mêmes sont uniquement déterminés. □

On obtient au passage une autre façon de factoriser les groupes abéliens finis :

Proposition. *Soit G un groupe abélien fini de cardinal $|G| = p_1^{b_1} \dots p_r^{b_r}$. Notons S_i l'unique p_i-Sylow, pour chaque $i = 1, \dots, r$. Alors G est le produit direct de ses sous-groupes S_i :*

$$G = S_1 \times \cdots \times S_r.$$

En particulier G s'écrit de façon unique (à l'ordre des facteurs près bien sûr) comme un produit de groupes cycliques élémentaires :

$$G \simeq \prod_{j=1}^{r} \left(\mathbb{Z}/p_j^{b_{j,1}} \times \cdots \times \mathbb{Z}/p_j^{b_{j,s_j}} \right).$$

Démonstration. Montrons que le morphisme naturel

$$\varphi \colon (x_1, \dots, x_r) \in S_1 \times \cdots \times S_r \mapsto x_1 \dots x_r \in G$$

est injectif. Si $(x_1, \dots, x_r) \in \ker \varphi$ n'est pas l'élément neutre, notons j le plus petit indice tel que $x_j \neq 1$. On a $x_j x_{j+1} \dots x_r = 1$, donc x_j et $x_{j+1} \dots x_r$ sont de même ordre, mais ordre(x_j) est une puissance non trivial de p_j alors que ordre$(x_{j+1} \dots x_r)$ est de la forme $p_{j+1}^{c_{j+1}} \dots p_r^{c_r}$, contradiction.

Donc φ est un isomorphisme par égalité des cardinaux. Pour la dernière assertion, appliquer le théorème de factorisation à chaque S_i. □

Faisons un parallèle avec la théorie des réductions d'un endomorphisme. La proposition précédente correspond au point de vue "Jordan", alors que le théorème correspond au point de vue "Frobenius". Comme dans le contexte de l'algèbre linéaire, l'usage de diagramme de Young est un moyen agréable de coder les différentes possibilités, ou de passer d'un point de vue à l'autre.

Exemple. Donnons la liste des groupes abéliens d'ordre 72.

Il y a trois possibilités pour le 2-Sylow (d'ordre $8 = 2^3$) :

$\mathbb{Z}/8$ 

$\mathbb{Z}/4 \times \mathbb{Z}/2$ 

$\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$ 

Par ailleurs il y a deux possibilités pour le 3-Sylow (d'ordre $9 = 3^2$) :

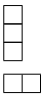
$\mathbb{Z}/9$ 

$\mathbb{Z}/3 \times \mathbb{Z}/3$

En combinant ces possibilités, on obtient donc six groupes abéliens d'ordre 72 à isomorphisme près.

$$\mathbb{Z}/72 \simeq \mathbb{Z}/8 \times \mathbb{Z}/9$$

$$\mathbb{Z}/24 \times \mathbb{Z}/3 \simeq \mathbb{Z}/8 \times \mathbb{Z}/3 \times \mathbb{Z}/3$$



$$\mathbb{Z}/36 \times \mathbb{Z}/2 \simeq \mathbb{Z}/4 \times \mathbb{Z}/2 \times \mathbb{Z}/9$$

$$\mathbb{Z}/12 \times \mathbb{Z}/6 \simeq \mathbb{Z}/4 \times \mathbb{Z}/2 \times \mathbb{Z}/3 \times \mathbb{Z}/3$$

$$\mathbb{Z}/18 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \simeq \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/9$$

$$\mathbb{Z}/6 \times \mathbb{Z}/6 \times \mathbb{Z}/2 \simeq \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/3 \times \mathbb{Z}/3$$

9. Dictionnaire entre groupes abéliens et endomorphismes

Référence : [BMP05].

On a observé des similitudes frappantes entre la théorie de la réduction des endomorphismes sur un $\mathbf{k}$-espace vectoriel, et la classification des groupes abéliens finis. Voici un dictionnaire entre les notions, sous forme de tableau à deux colonnes. La raison profonde de ce dictionnaire est que chacune des deux colonnes relève de la théorie des modules sur un anneau principal. Mais il n'y a pas besoin d'apprendre la théorie abstraite des modules pour commencer à apprécier les similitudes, ni pour chercher à allonger la liste...

Groupe abélien fini G	Espace vectoriel E muni d'un endomorphisme u
G est un $\mathbb{Z}$-module	E est un $\mathbf{k}[X]$-module
$n \cdot x := x^n$	$P(X) \cdot x := P(u)(x)$
Ordre de G	Polynôme caractéristique de u
Exposant de G	Polynôme minimal de u
Ordre d'un élément x	Polynôme minimal ponctuel en x
Diviseur p premier de $\lvert G\rvert$	Facteur $(X-\lambda)$ de χ_u
p-Sylow de G	Sous-espace caractéristique associé à λ
Sous-groupe des éléments d'ordre p	Sous-espace propre associé à λ
Factorisation $\mathbb{Z}/a_1 \times \cdots \times \mathbb{Z}/a_s$	Décomposition de Frobénius
Étude des p-groupes	Étude des endomorphismes nilpotents
Factorisation $\mathbb{Z}/p^{m_1} \times \cdots \times \mathbb{Z}/p^{m_r}$	Décomposition de Jordan d'une matrice nilpotente
Sous-groupe cyclique	Sous-espace u-cyclique

10. Automorphismes de $\mathbb{Z}/n\mathbb{Z}$

Référence : [Gui13, p. 29, mais attention aux fautes d'énoncés].

On rappelle d'abord le

Lemme. *Soit $a \in \mathbb{Z}$, et $n \geq 2$. Sont équivalents :*

(1) *a est premier avec n ;*

(2) *$\bar{a}$ est un inversible de l'anneau $\mathbb{Z}/n\mathbb{Z}$;*

(3) *$\bar{a}$ est un générateur du groupe additif $\mathbb{Z}/n\mathbb{Z}$.*

Démonstration. Dire que a est premier avec n équivaut à l'existence d'une relation de Bézout $au + nv = 1$, qui elle-même équivaut à l'existence d'une égalité $\bar{a}\bar{u} = \bar{1}$ dans $\mathbb{Z}/n\mathbb{Z}$. Quitte à ajouter un multiple de n à u, on peut supposer $u > 0$, et la dernière égalité équivaut à $\underbrace{\bar{a} + \bar{a} + \cdots + \bar{a}}_{u \text{ fois}} = \bar{1}$, c'est-à-dire à $\bar{1} \in \langle \bar{a} \rangle$, ou encore $\mathbb{Z}/n\mathbb{Z} = \langle \bar{a} \rangle$. □

On note $(\mathbb{Z}/n\mathbb{Z})^\times$ le groupe multiplicatif des inversibles dans l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Proposition. *Les groupes* $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ *et* $(\mathbb{Z}/n\mathbb{Z})^\times$ *sont isomorphes.*

Démonstration. Si $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$, l'application

$$\bar{u} \mapsto \bar{a}\bar{u}$$

est un automorphisme (de groupe additif) de $\mathbb{Z}/n\mathbb{Z}$: en effet par distributivité $\bar{a}(\bar{u}+\bar{v}) = \bar{a}\bar{u}+\bar{a}\bar{v}$.

Réciproquement, tout automorphisme $\varphi \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ envoie générateur sur générateur, en particulier $\varphi(\bar{1}) = \bar{a}$ est inversible par le lemme. De plus pour tout $\bar{u}$ avec $u > 0$, on a

$$\varphi(\bar{u}) = \underbrace{\varphi(\bar{1}) + \varphi(\bar{1}) + \cdots + \varphi(\bar{1})}_{u \text{ fois}} = \overline{ua},$$

ainsi φ est de la forme précédente. □

Pour la suite à nouveau j'allège l'écriture en notant $\mathbb{Z}/n$ au lieu de $\mathbb{Z}/n\mathbb{Z}$.

Par le théorème des restes chinois, si $n = p_1^{a_1} \dots p_r^{a_r}$, alors

$$(\mathbb{Z}/n)^\times \simeq (\mathbb{Z}/p_1^{a_1})^\times \times \cdots \times (\mathbb{Z}/p_r^{a_r})^\times.$$

On se ramène à montrer la proposition suivante (il faut aussi traiter le cas $p = 2$, voir plus bas) :

Proposition. *Soit* p *premier impair, et* $a \geq 1$. *Alors* $(\mathbb{Z}/p^a)^\times$ *est cyclique d'ordre* $p^{a-1}(p-1)$.

Démonstration. Tout d'abord l'ordre de $(\mathbb{Z}/p^a)^\times$ est $p^{a-1}(p-1) = p^a - p^{a-1}$: il y a p^a éléments dans $\mathbb{Z}/p^a$, et parmi les représentants $1, \dots, p^a$, les multiples de p sont au nombre de p^{a-1}.

Le groupe $(\mathbb{Z}/p^a)^\times$ contient un élément d'ordre $p-1$: prendre $x \in \mathbb{N}$ dont la classe engendre $(\mathbb{Z}/p)^\times$, son ordre dans $(\mathbb{Z}/p^a)^\times$ est $k(p-1)$ pour un certain $k \geq 1$, et x^k convient. On utilise ici le morphisme naturel d'anneau $\hat{y} \in \mathbb{Z}/p^a \mapsto \bar{y} \in \mathbb{Z}/p$, et le fait qu'il induit un morphisme de groupe $(\mathbb{Z}/p^a)^\times \to (\mathbb{Z}/p)^\times$.

Par ailleurs la classe de $1+p$ dans $(\mathbb{Z}/p^a\mathbb{Z})^\times$ est d'ordre p^{a-1}. Pour cela il suffit de montrer que pour tout $k \geq 0$, $(1+p)^{p^k} = 1 + qp^{k+1}$ avec $q \wedge p = 1$. Pour $k = 0$ c'est clair, pour $k = 1$ également en notant que tous les coefficients binomiaux $\frac{p!}{(p-i)!i!}$ sont multiples de p pour $p > i > 0$, et on obtient le résultat par récurrence sur k, en écrivant

$$(1 + qp^k)^p = 1 + qp^{k+1} + p^{k+2}(\dots)$$

Finalement la classe de $x^k(1+p)$ est le générateur cherché. □

Exemple. $(\mathbb{Z}/9)^\times$ contient $-\bar{1}$ qui est d'ordre $p-1 = 2$. Par ailleurs $1+p = 4$ est bien d'ordre 3. On obtient que $-\bar{4} = \bar{5}$ est un générateur de $(\mathbb{Z}/9)^\times$, qui est cyclique d'ordre 6. L'unique autre générateur est $\bar{2}$, qui est l'inverse de $\bar{5}$.

Ne pas confondre la proposition précédente avec la situation suivante (dont on a déjà vu la preuve, comme corollaire de la notion d'exposant d'un groupe) :

Proposition. *Soit* p *premier, et* $\mathbb{F}_{p^a}$ *un corps de cardinal* p^a. *Alors* $(\mathbb{F}_{p^a})^\times$ *est cyclique d'ordre* $p^a - 1$.

Exemple. $(\mathbb{F}_4)^\times$ est cyclique d'ordre 3 : si on utilise la représentation $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/(X^2+X+1)$, alors les classes de X et $X+1$ sont les deux générateurs. Par contre $(\mathbb{Z}/4)^\times$ est cyclique d'ordre 2, avec $\bar{3}$ comme unique élément non trivial.

Pour être complet, mentionnons rapidement le résultat analogue pour $p = 2$:

Proposition. [RW10, p. 16] *Pour tout* $k \geq 2$, *le groupe* $(\mathbb{Z}/2^k)^\times$ *est isomorphe à* $\mathbb{Z}/2 \times \mathbb{Z}/2^{k-2}$. *En particulier pour* $k \geq 3$ *ce n'est pas un groupe cyclique.*

Démonstration. Le groupe $(\mathbb{Z}/2^k)^\times$ est d'ordre 2^{k-1}. On cherche à montrer que $-\bar{1}$ et $\bar{5}$ engendrent $(\mathbb{Z}/2^k)^\times$, et donnent la structure de produit direct attendue.

Tout d'abord $\bar{5}$ est d'ordre 2^{k-2} dans $(\mathbb{Z}/2^k)^\times$: il suffit de montrer que pour tout $n \geq 0$ on a $5^{2^n} = 1 + q2^{n+2}$ avec q impair, ce qui se fait par une récurrence immédiate.

On en déduit que $\bar{5}$ engendre le noyau du morphisme $(\mathbb{Z}/2^k)^\times \to (\mathbb{Z}/4)^\times$, et comme $-\bar{1}$ n'est pas dans le noyau, on a la conclusion attendue. □

Remarque philosophique : le problème initial était de décrire les automorphismes du **groupe** $\mathbb{Z}/n\mathbb{Z}$, et on a obtenu une réponse en exploitant la structure d'**anneau** de $\mathbb{Z}/n\mathbb{Z}$. Donc ce paragraphe a toute sa place dans la leçon "Anneau $\mathbb{Z}/n\mathbb{Z}$", mais bien réaliser qu'on n'est pas en train de parler des automorphismes de l'anneau $\mathbb{Z}/n\mathbb{Z}$ (qui n'admet que l'automorphisme trivial...)

11. Un automorphisme non intérieur de S_6

Rappelons que si $H \subset G$ est un sous-groupe d'indice r, on obtient un morphisme de G dans S_r en faisant agir G sur les classes à gauche modulo H. Précisément, en notant $x_1H, \dots, x_rH$, les r classes à gauche, on associe une permutation $\sigma \in S_r$ à un élément $g \in G$ en posant

$$(gx_i)H = x_{\sigma(i)}H.$$

Noter que $i \mapsto \sigma(i)$ est bien une bijection, car l'inverse est donné par l'action de g^{-1}.

Lemme. *Soit $n \geq 5$. Si $H \subset S_n$ est un sous-groupe d'indice n agissant transitivement sur $\{1, \dots, n\}$, alors le morphisme $\psi \colon S_n \to S_n$ associé à l'action de S_n sur les classes de S_n modulo H est un automorphisme non intérieur.*

Démonstration. Considérons donc l'action

$$\begin{aligned} S_n \times S_n/H &\to S_n/H \\ g \quad , \ x_iH &\mapsto x_{\sigma(i)}H := (gx_i)H. \end{aligned}$$

Par définition, dire qu'un élément g est dans le noyau de ψ revient à dire

$$g \in \bigcap_{i=1}^{n} \mathrm{Stab}(x_iH).$$

En particulier $\ker\psi \subset H$, et comme H est d'indice $n \geq 3$, on a $\ker\psi = \{1\}$ (les seuls autres sous-groupes distingués de S_n sont d'indice 1 ou 2). Ainsi ψ est un automorphisme.

Si ψ était un automorphisme intérieur, alors $\psi(H)$ serait de la forme aHa^{-1} pour un certain $a \in S_n$ et donc agirait transitivement sur $\{1, \dots, n\}$. En effet si $i, j \in \{1, \dots, n\}$, il existe par hypothèse $h \in H$ tel que $h(a^{-1}(i)) = a^{-1}(j)$, donc aha^{-1} est un élément de aHa^{-1} qui envoie i sur j. Reste à remarquer que si $x_iH = H$ est la classe de l'élément neutre modulo H, alors $\psi(H)$ fixe i (car si $h \in H$, $hx_iH = hH = H = x_iH$), et donc n'agit pas transitivement. □

Bien sûr on sait par ailleurs que les hypothèses du lemme ne sont jamais satisfaites pour $n \neq 6$. Ceci dit il m'a semblé intéressant d'énoncer le lemme ainsi pour faire ressortir que les arguments sont indépendants d'une valeur particulière de n. Donnons maintenant la construction qui permet grâce au lemme de conclure à l'existence d'un automorphisme non intérieur dans S_6.

Proposition. *Il existe un sous-groupe $H \subset S_6$ d'indice 6, qui agit transitivement sur $\{1, \dots, 6\}$.*

Démonstration. On considère l'action de $\mathrm{GL}_2(\mathbb{F}_5)$ sur les six droites du plan $(\mathbb{F}_5)^2$. Cette action est transitive, et devient fidèle après quotient par le sous-groupe des homothéties, qui est d'ordre 4. Autrement dit cette action donne un morphisme injectif de $\mathrm{PGL}_2(\mathbb{F}_5)$ dans S_6, et l'image H de ce morphisme agit transitivement sur $\{1, \dots, 6\}$. L'ordre de $\mathrm{GL}_2(\mathbb{F}_5)$ est $24 \cdot 20 = 5! \cdot 4$, et donc

$$|H| = |\,\mathrm{PGL}_2(\mathbb{F}_5)| = 5!$$

Ainsi H est sous-groupe d'indice 6 dans S_6. □

Références

[BMP05] V. Beck, J. Malick, et G. Peyré. *Objectif agrégation*. H&K, 2005.

[Gui13] D. Guin. *Algèbre II : Anneaux, modules et algèbre multilinéaire*. EDP Sciences, 2013.

[Per96] D. Perrin. *Cours d'algèbre*. Ellipses, 1996.

[RW10] J.-P. Ramis et A. Warusfel. *Cours de mathématique vol.1 algèbre et géométrie*. De Boeck, 2010.

[Ser78] J.-P. Serre. Groupes finis. *arXiv:math/0503154*, 1978.