Leçon 104 : Groupes finis. Exemples et applications.

Mathieu Alix

Jeudi 1 Mai 2025

1 Rapport du Jury

« Cette leçon est particulièrement vaste et il convient de faire des choix, qui devront pouvoir être justifiés. La notion d'ordre (d'un groupe, d'un élément et d'un sous-groupe) est très importante dans cette leçon ; le théorème de Lagrange est incontournable. Le théorème de structure des groupes abéliens finis doit figurer dans cette leçon. Sa démonstration est techniquement exigeante, mais il faut que l'énoncé soit bien compris, en particulier le sens précis de la clause d'unicité, et être capable de l'appliquer dans des cas particuliers.

Il est souhaitable de présenter des exemples de groupes finis particulièrement utiles comme les groupes $\mathbb{Z}/n\mathbb{Z}$ et S_n, en en maîtrisant les propriétés élémentaires (générateurs, classes de conjugaison, etc.). Il est important de connaître les groupes d'ordre premier ainsi que les groupes d'ordre inférieur à 8.

Des exemples de groupes finis issus de domaines autres que la théorie des groupes doivent figurer en bonne place dans cette leçon. L'étude des groupes d'isométries laissant fixe un polygone (ou un polyèdre) régulier peut être opportunément exploitée sous cet intitulé. Afin d'illustrer leur présentation, les candidates et candidats peuvent aussi s'intéresser à des groupes d'automorphismes ou étudier les groupes de symétries A_4, S_4, A_5 et relier sur ces exemples géométrie et algèbre.

Pour aller plus loin, les candidates et candidats peuvent s'attarder sur la dualité dans les groupes abéliens finis. Comme application, la cyclicité du groupe multiplicatif d'un corps fini est tout à fait adaptée. Il est possible d'explorer des représentations de groupes, de donner des exemples de caractères, additifs ou multiplicatifs dans le cadre des corps finis. Il est aussi possible de s'intéresser aux sommes de Gauss. Les candidates et candidats peuvent ensuite introduire la transformée de Fourier discrète, qui pourra être vue comme son analogue analytique, avec ses formules d'inversion, sa formule de Plancherel. Ainsi, la leçon peut mener à introduire la transformée de Fourier rapide sur un groupe abélien dont l'ordre est une puissance de 2 ainsi que des applications à la multiplication d'entiers, de polynômes et éventuellement au décodage de codes via la transformée de Hadamard. »

2 Questions classiques

1. Donner un exemple de groupe toujours abélien ?

Solution: Les groupes d'ordre p^2, voir [ROM] pour une preuve.

2. Quel est l'ordre de $\overline{9}$ dans $(\mathbb{Z}/12\mathbb{Z}, +)$?

Solution: On est sur la loi de groupe additive, alors on vérifie que :

$$2 \times \overline{9} = \overline{6}, 3 \times \overline{9} = \overline{3}, 4 \times \overline{9} = \overline{0}$$

$\overline{9}$ est donc d'ordre 4.

3. Déterminer les générateurs du groupe additif $\mathbb{Z}/12\mathbb{Z}$ et ceux du groupe multiplicatif $\mathbb{U}_{18}$.

Solution: Les deux groupes sont cycliques engendrés respectivement par $\overline{1}$ et $\zeta = e^{\frac{2i\pi}{18}} = e^{\frac{i\pi}{9}}$. Les générateurs de $\mathbb{Z}/12\mathbb{Z}$ sont donc les $\overline{k}$ tel que $pgcd(12, k) = 1$, soit : $\overline{1}, \overline{5}, \overline{7}, \overline{11}$ et ceux de $\mathbb{U}_{18}$ sont $\zeta, \zeta^5, \zeta^7, \zeta^{11}, \zeta^{13}, \zeta^{17}$.

4. Déterminer les éléments d'ordre 6 dans $\mathbb{U}_{30}$.

Solution: Le groupe $G = \mathbb{U}_{30}$ est cyclique engendré par $\zeta = e^{\frac{i\pi}{15}}$, il existe donc un unique sous groupe $H = \langle \zeta^{\frac{30}{6}} \rangle = \langle \zeta^5 \rangle$ d'ordre 6 de G. Tous les éléments d'ordre 6 se trouvent dans H qui admet $\varphi(6) = 2$ générateurs. Il n'y a donc que deux éléments d'ordre 6 qui sont ζ^5 et ζ^{25}.

5. Soient $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 6 & 7 & 1 & 2 & 4 \end{pmatrix}$

   (a) Décomposer σ en produit de cycles à supports disjoints. puis en transpositions.

   (b) Donner la signature de σ.

   (c) Calculer σ^{2001}.

Solution:

(a) On trouve $\sigma = (1\,3\,6\,2\,5) \circ (4\,7) = (1\,3) \circ (3\,6) \circ (6\,2) \circ (2\,5) \circ (4\;\;7)$

(b) La signature du 5 cycle est $(-1)^{5-1} = 1$ et celle de la transposition est (-1), donc la signature de σ est $1 \times (-1) = -1$. (On peut aussi le trouver avec les transpositions car on a 5 transpositions.

(c) De la décomposition en cycles à supports disjoints, on tire que l'ordre de σ vaut le ppcm de 2 et 5 soit 10, ainsi $\sigma^{10} = Id$. Ainsi $\sigma^{2001} = \sigma^{10 \times 200 + 1} = (\sigma^{10})^{200} \circ \sigma = \sigma$.

6. Quel est le plus petit entier n tel qu'il existe un groupe non-commutatif de cardinal n ?

Solution: Notons pour $n = 6$ que $(S_3, \circ)$ est un groupe non commutatif à 6 éléments. Un groupe à $n = 1$ élément est évidemment commutatif. Pour $n = 2, 3, 5$, les éléments vérifient

$x^n = e$ et comme n est premier, un élément autre que e de ce groupe est un élément d'ordre n et donc le groupe est cyclique engendré par cet élément, donc commutatif. Pour $n = 4$, s'il y a un élément d'ordre 4, celui-ci est cyclique donc comme précédemment. Sinon, tous les éléments du groupe vérifient $x^2 = e$. Il est alors classique de vérifier que le groupe est commutatif.

7. Déterminer les groupes abéliens d'ordre 15 à isomorphisme près.

Solution: On a $15 = 3 \times 5$, donc le seul facteur invariant possible d'un groupe abélien d'ordre 15 est 15. Ainsi $\mathbb{Z}/15\mathbb{Z}$ est le seul groupe abélien d'ordre 15.

8. Déterminer les groupes abéliens d'ordre 48 à isomorphisme près.

Solution:

$$\begin{aligned} 48 &= 2^4 \times 3 \text{ et le groupe est } \mathbb{Z}/48\mathbb{Z} \\ &= 2 \times (2^3 \times 3) \text{ et le groupe est } \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z} \\ &= 2^2 \times (2^2 \times 3) \text{ et le groupe est } \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \\ &= (2) \times (2) \times (2^2 \times 3) \text{ et le groupe est } (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/12\mathbb{Z} \\ &= (2) \times (2) \times (2) \times (2 \times 3) \text{ et le groupe est } (\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/6\mathbb{Z} \end{aligned}$$

9. Soit G un groupe d'ordre 33 agissant sur un ensemble X de cardinal 19. Montrer qu'il existe une orbite de cardinal 1.

Solution: Utiliser la formule des classes. Supposons par l'absurde qu'il n'existe pas d'orbite de cardinal 1 (i.e. il n'y a pas de point fixe sous l'action de G). Alors pour tout $x \in X \mathrm{Stab}(x) \neq G$. La formule des classes implique donc qu'on peut écrire 19 sous la forme $19 = 33a + 11b + 3c$ avec $(a, b, c) \in \mathbb{N}$. Nécessairement, $a = 0$, $b = 1$ ou $b = 0$. Si $b = 1$ alors $8 = 3c$ ce qui est impossible, et si $b = 0$ alors $19 = 3c$ impossible aussi.

10. Montrer qu'un groupe d'ordre 200 n'est pas simple.

Solution: Soit G un groupe d'ordre 200. Notons que $200 = 2^3 \times 5^2$. D'après les Théorèmes de Sylow le nombre de 5-Sylow de G est congru à 1 modulo 5 et divise $2^3 = 8$ donc vaut 1. L'unique 5-Sylow de G est donc nécessairement distingué dans G ; en particulier G n'est pas simple.

11. Montrer qu'un groupe d'ordre pq, où p et q sont premiers et distincts, ne peut être simple.

Solution: Soit G un groupe d'ordre pq. Quitte à renommer p et q nous pouvons supposer que $p > q$. Soit n_p le nombre de p-Sylow de G. Les théorèmes de Sylow assurent que $n_p = 1$

mod $[p]$ et n_p divise q, autrement dit que $n_p = 1 \mod [p]$ et $n_p \in \{1, q\}$. Mais comme $p > q$, $q \neq 1 \mod [p]$. Par suite $n_p = 1$, *i.e*, il y a un seul p-Sylow dans G qui est un sous-groupe d'ordre p distingué dans G et propre. Il s'en suit que G n'est pas simple.

3 Question plus exotique ?

1. Soit G un groupe admettant un nombre fini de sous-groupes.
   (a) Démontrer que tout élément de G est d'ordre fini.
   (b) En déduire que G est fini.

Solution:

(a) Supposons que G admette un élément x d'ordre infini et notons H le sous-groupe engendré par x. Alors H est isomorphe à $(\mathbb{Z}, +)$ qui contient une infinité de sous-groupes. On en déduit que H et donc G contiennent aussi une infinité de sous-groupes ce qui est absurde.

(b) Pour $x \in G$, notons H_x le sous-groupe engendré par x. Alors on a $G = \bigcup_{x \in G} H_x$, mais puisque G contient seulement un nombre fini de sous-groupe, il n'y a qu'un nombre fini de H_x différents, que l'on note $H_{x_1}, \ldots, H_{x_p}$, d'où $G = \bigcup_{i=1}^{p} H_{x_i}$. Or chacun des H_{x_i} est fini d'après la question précédente. Donc G est fini.

2. On suppose qu'il existe un groupe simple G d'ordre 180.
   (a) Monter que le nombre de 5-Sylow est 36.
   (b) Montrer que le nombre de 3-Sylow est 10.
   (c) Montrer que si H et K sont deux 3-Sylow de G dont l'intersection est non-triviale, alors le centralisateur d'un élément $g \neq e_G$ de $H \cap K$ est d'ordre 18.
   (d) En déduire que l'intersection de deux 3-Sylow distincts de G est triviale.
   (e) Conclure qu'il n'existe pas de groupe simple d'ordre 180.

Solution: On commence par se rappeler que $180 = 2^2 \times 3^2 \times 5$

(a) Pour tout p premier divisant $|G|$, on note n_p le nombre de p-Sylow de G. Les théorèmes de Sylow assurent que $n_5 | 36$ et $n_5 = 1 \mod [5]$. Cela implique que $n_5 = 1, 6$ ou 36. Comme G est simple, le cas $n_5 = 1$ est impossible (sinon le 5-Sylow sertait distingué dans G), donc $n_5 = 6$ ou 36. Supposons que $n_5 = 6$, alors l'action transitive de G par conjugaison sur l'ensemble de ses 5-Sylow induit un morphisme non trivial $G \to S_6$. Comme G est simple, ce morphisme est injectif. Comme le morphisme de signature à nécessairement un noyau trivial, on voit que G est un sous-groupe de A_6. En calculant les cardinaux, on observe que G est un sous-groupe d'indice 2 dans A_6, il est donc distingué et non trivial, ce qui contredit la simplicité de A_6. Cela assure donc que $n_5 = 36$.

(b) Comme précédemment $n_3|20$ et $n_3 = 1 \mod [3]$, cela implique comme G est simple que $n_3 = 4$ ou $n_3 = 10$. Si on avait $n_3 = 4$, on en déduire comme en (a) un morphisme injectif de G dans S_4, ce qui est impossible car le cardinal de G est strictement supérieur à celui de S_4, donc $n_3 = 10$.

(c) Soit $g \in H \cap K$ qu'on suppose être différent de e_G et on note $Z := \{x \in G, xg = gx\}$ le centralisateur de g dans G. Puisqu'un groupe d'ordre $9 = 3^2$ est abélien, on voit que Z contient H et K. On a donc nécessairement que $|Z| \in \{18, 36, 45, 90\}$. Or l'action (transitive) de G sur G/Z induit un morphisme injectif de G vers $S(G/Z)$, et donc par cardinalité, on a nécessairement que $|Z| = 18$.

(d) N et K sont des 3-Sylow de Z et un groupe d'ordre 18 admet un unique 3-Sylow, donc $N = K$, ce qui est une contradiction. Ainsi finalement $N \cap K = \{e_G\}$.

(e) Finalement G admet 10 3-Sylow dont les intersections deux à deux sont triviales. Par conséquent, il y a dans 6 exactement $10 \times 8 = 80$ éléments $\neq e_G$ d'ordre divisant 9. Or la question (a) assure que G contient $36 \times 4 = 144$ éléments d'ordre 5. Donc G possède au moins $144 + 80 = 224$ éléments ce qui est contradictoire.

3. Soit $G = GL_2(\mathbb{Z}/2\mathbb{Z})$ le groupe des matrices inversibles 2×2 à coefficients dans $\mathbb{Z}/2\mathbb{Z}$.
   (a) Quel est l'ordre de G ?
   (b) Soit E un espace vectoriel de dimension 2 sur $\mathbb{F}_2$. Définir une action non triviale de G sur E.
   (c) En déduire que G est isomorphe à S_3.

Solution: Dans toute cette solution, je fais le choix d'omettre de mettre des barres sur les $0, 1$ mais il faut avoir conscience que ceux sont les classes qui sont prises.

(a) Les éléments de G sont les matrices inversibles dans $\mathbb{Z}/2\mathbb{Z}$, en voici la liste :

$$\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix} \quad \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix} \quad \begin{pmatrix}1 & 1\\0 & 1\end{pmatrix} \quad \begin{pmatrix}1 & 0\\1 & 1\end{pmatrix} \quad \begin{pmatrix}1 & 1\\1 & 0\end{pmatrix} \quad \begin{pmatrix}0 & 1\\1 & 1\end{pmatrix}$$

Ainsi G est un groupe d'ordre 6

(b) À chaque base (v, w) de l'espace vectoriel E correspond une action de G sur E : pour $g \in G$ et $u \in E$, on définit $g \cdot u \in E$ comme étant l'image du vecteur u par l'application linéaire de matrice g dans la base (v, w).

(c) Fixons une base de E et considérons l'action correspondante de G sur E. Pour tout $g \in G$, l'application $\varphi_g : u \mapsto g \cdot u$ est définie par les images des vecteurs non-nuls de E ; en effet, le vecteur nul a toujours pour image lui-même.

Ainsi, à tout élément de G est associée une permutation de $E\backslash\{0\}$. Or E compte $2^2 = 4$ éléments. Soient v_1, v_2 et v_3 les trois vecteurs non-nuls de E. Alors

$$g \mapsto ((v_1, v_2, v_3) \mapsto (g \cdot v_1, g \cdot v_2, g \cdot v_3))$$

définit un morphisme de groupes de G dans S_3. Ce morphisme est injectif. Par suite G est isomorphe à un sous-groupe de S_3. Puis que G et S_3 ont même ordre, G est isomorphe à S_3.

4. Soient G un groupe d'ordre $n \geq 2$ et $\varphi : g \in G \mapsto (\varphi(g) : h \mapsto g \cdot h)$ l'injection de G dans $S(G)$.
   (a) Montrer que pour tout $g \in G \setminus \{1\}$, la permutation $\varphi(g)$ se décompose en produit de cycles tous de longueur égale à l'ordre $\theta(g)$ de g dans G.
   (b) En déduire la signature de $\varphi(g)$ pour tout $g \in G$.
   (c) En déduire que, si G est un groupe d'ordre impair, il est alors isomorphe à un sous-groupe du groupe alterné $\mathcal{A}(G)$.

Solution: Notons $G = \{1, g_1, \ldots, g_{n-1}\}$.

(a) Pour $g = 1$, on a $\varphi(1) = Id$. Pour g d'ordre $m \geq 2$, en notant $r = [G, \langle g \rangle]$ l'indice de $H = \langle g \rangle$ dans G, on a $H\backslash G = \{H, Hg_1, \ldots, Hg_{r-1}\}$ (classes à droite modulo H) et la partition $G = H \cup Hg_1 \cup \cdots \cup Hg_{r-1}$, donc $\varphi(g)$ est la permutation :

$$\begin{pmatrix} 1 & \ldots & g^{m-1} & g_1 & \ldots & g^{m-1}g_1 & \ldots & g_{r-1} & \ldots & g^{m-1}g_{r-1} \\ g & \ldots & 1 & gg_1 & \ldots & g_1 & \ldots & gg_{r-1} & \ldots & g_{r-1} \end{pmatrix}$$

qui est égale à $(1, g, \ldots, g^{m-1}) \circ (g_1, gg_1 \ldots, g^{m-1}g_1) \circ \cdots \circ (g_{r-1}, gg_{r-1}, \ldots, g^{m-1}g_{r-1})$ produit de r cycles de longueur m.

(b) Il en suite que pour g qui n'est pas le neutre d'ordre $m \geq 2$, la signature de $\varphi(g)$ est

$$\varepsilon(\varphi(g)) = (-1)^{r(m-1)} = (-1)^{[G,\langle g \rangle](\theta(g)-1)}$$

On remarque que ce résultat est encore valable pour $g = 1$.

(c) Si $n = |G|$ est d'ordre impair, alors $\theta(g)$ est impair pour tout $g \in G$ puisque il divise n et donc $\varepsilon(\varphi(g)) = 1$. Ainsi $\varphi(G)$ est un sous-groupe du groupe alterné $\mathcal{A}(G)$.

5. (Jury d'agreg) Considérons E un ensemble fini de cardinal n non multiple de p premier et σ une permutation d'ordre p. Montrer que σ a un point fixe.

Solution: Écrivons $\sigma = \gamma_1 \circ \cdots \circ \gamma_r$ sa décomposition en cycle à support disjoint. L'ordre de σ est le ppcm des ordres des cycles à support disjoint. Or l'ordre de σ vaut p, donc tout les cycles sont d'ordre soit p, soit 1. Supposons par l'absurde, que tous les cycles soient d'ordre p, alors en faisant agit $\langle \sigma \rangle$ sur E, par l'équation aux classes :

$$|E| = \sum_{w \in \Omega} |w| \text{ où } \Omega \text{ est un système de représentant des orbites}$$

Or chaque γ_i fournit une orbite de $\langle \sigma \rangle$, donc $n = |E| = \sum_{i=1}^{r} |\gamma_i| = p \times k$ ce qui est absurde car n n'est pas un multiple de p. Ainsi, il existe un cycle d'ordre 1 donc un point fixe.