Leçon 104 : Groupes finis. Exemples et applications.

1 Généralités et groupes abéliens

1.1 Définitions et propriétés

Définition 1. Un groupe $(G, \cdot)$ est un ensemble G muni d'une application $\cdot : G \times G \to G$ associative, possédant un neutre e et dont tout élément est inversible. Il est dit fini lorsque G est fini.
Le cardinal d'un groupe fini est appelé ordre de G, noté $|G|$ ou $\#G$. L'ordre d'un élément $g \in G$ noté $o(g)$ est le plus petit entier tel que $g^n = e$, c'est aussi l'ordre du plus petit sous groupe engendré par g.

Corollaire 2. *Les assertions suivantes sont équivalentes :*

1. $g \in G$ *est d'ordre* n *;*
2. $g^n = e$ *et* $g^k \neq e$ *pour tout* $1 < k < n$ *;*
3. $g^k = e$ *si et seulement si* k *est multiple de* n*.*

A présent on considère $(G, \cdot)$ un groupe fini d'ordre n.

Définition 3. Soit H un sous groupe de G et $a \in H$, l'ensemble des classes à gauche de a est le sous ensemble aH. Les classes à gauche forment une partition de G dont l'ensemble est noté G/H dont le cardinal est appelé indice H dans G et noté $[G : H]$.

Théorème 4. *(Lagrange) Si* H *sous groupe de* G*, alors l'ordre de* H *et l'indice de* H *dans* G *divisent l'ordre de* G*. Plus précisément* $|G| = |H|\,[G : H]$*. En particulier l'ordre d'un élément divise l'ordre de* G*.*

Corollaire 5. *Un groupe* G *d'ordre* p *premier est cyclique et ses seuls sous groupes sont* G *et* $\{e\}$*.*

Proposition 6. *Tout groupe non abélien fini engendré par deux éléments d'ordre 2 est isomorphe à un groupe diédral* D_n *pour un* $n \geqslant 3$*.*

Lemme 7. *Soient* $a, b \in G$ *d'ordre respectifs* α *et* β*, alors si* $pgcd(\alpha, \beta) = 1$ *alors* $o(ab) = o(a)o(b)$*.*

1.2 Actions de groupe

Dans cette partie on considère X un ensemble.

Définition 8. — On dit que G opère sur X lorsqu'on a une application $. : G \times X \to X$; $(g, x) \mapsto g.x$ vérifiant :$\forall g, g' \in G, \forall x \in X, g.(g'.x) = (gg').x$ et $\forall x \in X, 1.x = x$. C'est équivalent au fait de se donner un morphisme $\varphi : G \to \mathcal{S}(X)$, on pose alors $g.x = \varphi(g)(x)$.

— On dit que G opère transitivement sur X lorsque $\forall x \in X, \forall y \in X, \exists g \in G, g.x = y$.

— On appelle stabilisateur de $x \in X$ l'ensemble $Stab_G(x) = \{g \in G \mid g.x = x\}$. On appelle orbite de x sous G le sous ensemble $\Omega(x) = \{g.x \mid g \in G\}$.

— On dit que G opère librement lorsque $Stab_G(x) = \{e\}$ pour tout $x \in X$ et qu'il opère transitivement lorsque $\Omega(x) = X$, il n'y a qu'une seule orbite.

Exemple 9. G agit sur lui même par translation à gauche avec $G \times G \to G$; $(g, h) \mapsto gh$. Cette action est fidèle et transitive.

Théorème 10. *(Cayley) Tout groupe fini* G *d'ordre* n *est isomorphe à un sous groupe transitif de* $\mathcal{S}_n$*.*

Exemple 11. G agit sur lui même par conjugaison avec $G \times G \to G$; $(g, h) \mapsto ghg^{-1}$. Cette action n'est jamais libre.

2 Groupes cycliques

2.1 Généralités

Définition 12. Un groupe fini G est cyclique lorsqu'il existe $g \in G$ qui engendre G.

Théorème 13. *Un groupe fini d'ordre* n *est isomorphe au groupe* $(\mathbb{Z}/n\mathbb{Z}, +)$*.*

Théorème 14. *Si $G = \langle g \rangle$ cyclique d'ordre n alors ses générateurs sont les g^k avec $pgcd(k, n) = 1$.*

Théorème 15. *Tout groupe de cardinal premier est cyclique (donc isomorphe à $\mathbb{Z}/p\mathbb{Z}$).*

Théorème 16. *Un groupe commutatif d'ordre pq où p et q sont premiers distincts, est cyclique.*

Corollaire 17. *Si $p \geqslant 2$ premier et G un p-groupe opérant sur un ensemble X fini, alors $\left|X^G\right| \equiv |X| \mod p$*

Corollaire 18. *Soit G un groupe fini qui opère sur lui même par conjugaison, en notant $\Omega(x_1), \ldots, \Omega(x_r)$ toutes les orbites 2 à 2 distinctes, on a :*

$$|G| = |Z(G)| + \sum_{\substack{i=1 \\ |\Omega(x_i)|\geqslant 2}}^{r} |\Omega(x_i)| = |Z(G)| + \sum_{\substack{i=1 \\ |\Omega(x_i)|\geqslant 2}}^{r} \frac{|G|}{|Stab(x_i)|}$$

Théorème 19. *Pour tout nombre premier p, le centre d'un p-groupe n'est pas réduit à $\{1\}$.*

Théorème 20. *Tout groupe d'ordre p^2 avec p premier est commutatif. Il est isomorphe soit à $\mathbb{Z}/p^2\mathbb{Z}$ soit à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.*

Proposition 21. *Soit p premier impair, si G groupe d'ordre $2p$ alors G est isomorphe soit à $\mathbb{Z}/2p\mathbb{Z}$ soit à D_{2p}.*

2.2 Classification des groupes

Définition 22. On appelle exposant de G l'entier $e(G) = \max_{g\in G} \{o(g)\} = \text{ppcm}(o(g) \mid g \in G)$.

Théorème 23. *(Chinois) Les ensembles $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/nm\mathbb{Z}$ sont isomorphes si et seulement si n et m sont premiers entre eux.*

Exemple 24. Les ensembles $(\mathbb{Z}/2\mathbb{Z})^2$ et $\mathbb{Z}/4\mathbb{Z}$ ne sont pas isomorphes.

Théorème 25. *(Kronecker) Pour tout groupe fini G d'ordre supérieur à 2, il existe une unique suite d'entier $(d_1, \ldots, d_r)$ avec $d_1 \geqslant 2$ et $d_1|d_2|\ldots|d_{r-1}|dr$ tels que G soit isomorphe au produit $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$.*

3 Groupes non abéliens

3.1 Groupe symétrique et alterné

Définition 26. Le groupe $\mathcal{S}(E)$ des bijections de E sur lui même est appelé groupe des permutations de E.

Remarque 27. Pour $E = \{1, \ldots, n\}$ on note $\mathcal{S}_n = \mathcal{S}(E)$ appelé groupe symétrique à n éléments.

Théorème 28. *Toute permutation $\sigma \in \mathcal{S}(E)$ se décompose en produit de transpositions.*

Lemme 29. *$\mathcal{S}_n$ est engendré par les $n-1$ transpositions $(1\ k)$ où $2 \leqslant k \leqslant n$.*

Lemme 30. *$\mathcal{S}_n$ est engendré par les $n-1$ transpositions $(k\ k+1)$ où $1 \leqslant k \leqslant n-1$.*

Lemme 31. *$\mathcal{S}_n$ est engendré par $(1\ 2)$ et $(1\ 2\ \ldots n)$.*

Définition 32. On dit qu'une permutation $\sigma \in \mathcal{S}(E)$ est paire (resp impaire) lorsque $\varepsilon(\sigma) = 1$ (resp $\varepsilon(\sigma) = -1$.

Définition 33. Le groupe alterné $\mathcal{A}(E)$ est le sous ensemble de $\mathcal{S}(E)$ formé des permutations paires.

Théorème 34. *Le sous groupe $\mathcal{A}(E)$ est un sous groupe normal du groupe $\mathcal{S}(E)$.*

Proposition 35. *Pour tout $n \in \mathbb{N}^*$, $\mathcal{A}_n$ est un sous groupe d'indice 2 de $\mathcal{S}_n$ et on a $|\mathcal{A}_n| = \frac{n!}{2}$.*

Lemme 36. *Le produit de 2 transpositions est un produit de 3-cycles. Précisément pour $x, y, z, t \in E$ distincts on a : $(x\ y)(x\ z) = (x\ z\ y)$ et $(x\ y)(z\ t) = (x\ y\ z)(y\ z\ t)$.*

Théorème 37. *Pour $n \geqslant 3$, $\mathcal{A}(E)$ est engendré par les 3-cycles.*

Théorème 38. *Pour $n \geqslant 5$ les sous groupes normaux de $\mathcal{S}(E)$ sont $\{Id\}, \mathcal{A}(E)$ et $\mathcal{S}(E)$.*

Théorème 39. *Pour $n = 3$ ou $n \geqslant 5$ le groupe $\mathcal{A}(E)$ est simple.*

3.2 Groupe linéaire

Définition 40. Le groupe linéaire de E un $\mathbb{K}$ espace vectoriel de dimension n noté $GL(E)$ est l'ensemble des inversibles de l'anneau $\mathcal{L}(E)$ des $\mathbb{K}$ -automorphismes de E.

Proposition 41. *Une matrice est diagonalisable (resp trigonalisable) si et seulement si son orbite pour cette action contient une matrice diagonale (resp triangulaire supérieure).*

Proposition 42. *Soit $u \in \mathcal{L}(E)$, u est nilpotente si et seulement si pour tout $k \in \{1, \dots, n\}$ $tr(u^k) = 0$.*

Lemme 43. *Soient G un sous groupe de $GL(E)$, F le sous espace vectoriel engendré par G, $\mathcal{B} = (u_1, \dots, u_p)$ une base de F extraite de G et $\varphi : G \to \mathbb{K}^p$; $u \mapsto (tr(u \circ u_1), \dots, tr(u \circ u_p))$.*
Si $u, v \in G$ sont tels que $\varphi(u) = \varphi(v)$ alors l'application $u \circ v^{-1} - Id$ est nilpotent.
Si tous les éléments de G sont diagonalisables alors φ est injective.

Théorème 44. *(Burnside) Soit G un sous groupe de $GL(E)$, on a les équivalences suivantes :*

1. *G est fini*
2. *G est d'exposant fini*
3. *$tr(G)$ est fini et tous ses éléments sont diagonalisables.*

Dev 1 : An est simple 36,37 et 39
Dev 2 : Classification des groupes d'ordre p^2 17, 18,19 et 20
Dev 3 : Critère de nilpotence et Burnside 42, 43 et 44

Références

[PER96] Daniel PERRIN : Cours d'algèbre. Ellipses, 1996.

[ROM17] JeanÉtienne ROMBALDI : Mathématiques pour l'Agrégation : Algèbre géométrie. De Boeck Superieur, 2017.

[ULM12] Félix ULMER : Théorie des groupes. Ellipses, 2012.

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 $\mathcal{S}_n$, 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 $\mathcal{S}_4, \mathcal{A}_4, \mathcal{S}_\triangledown$ 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.