Leçon 104. Groupes abéliens et non abéliens finis. Exemples et applications.

1. Ordre dans un groupes finis

1.1. Notion d'ordre

1. Définition. L'*ordre* d'un groupe fini G est son cardinal $|G|$ en tant qu'ensemble.
2. Exemple. Pour un entier $n \geqslant 1$, le groupe fini $\mathbf{Z}/n\mathbf{Z}$ est d'ordre n.
3. Théorème *(Lagrange)*. Soient G un groupe fini et $H \subset G$ un sous-groupe. Alors l'ordre du groupe H divise celui du groupe G.
4. Définition. Avec les mêmes notations, l'*indice* du sous-groupe H dans le groupe G est l'entier $[G : H] \coloneqq |G| \,/\, |H| \in \mathbf{N}^*$.
5. Exemple. Le sous-groupe $\mathfrak{A}_n$ est d'indice 2 dans le groupe $\mathfrak{S}_n$.
6. Proposition. Avec les mêmes notations, on a $[G : H] = |G/H|$.
7. Proposition. Un sous-groupe d'indice 2 est distingué.
8. Définition. Soit G un groupe. L'ordre d'un élément $g \in G$ est le cardinal du groupe $\langle g \rangle$, noté $\mathrm{o}(g) \in \mathbf{N}^* \cup \{+\infty\}$.
9. Exemple. Le neutre est toujours d'ordre 1. Pour $n \geqslant 2$, la permutation $(1\ 2) \in \mathfrak{S}_n$ est d'ordre 2.
10. Proposition. Soient G un groupe fini et $g \in G$ un élément. Alors
    - l'ordre de l'élément g est fini et divise l'ordre du groupe G, c'est-à-dire $\mathrm{o}(g) \mid |G|$.
    - $\mathrm{o}(g) = \min\{k \in \mathbf{N} \mid g^k = 1\}$;
    - pour tout entier $k \in \mathbf{N}$, on a $g^k = 1 \Leftrightarrow \mathrm{o}(g) \mid n$.
11. Corollaire. Soient G un groupe fini d'ordre $n \geqslant 1$ et $g \in G$ un élément quelconque. Alors $g^n = 1$.
12. Application *(petit théorème de Fermat)*. Pour tout nombre premier p et tout entier $a \in \mathbf{Z}^*$ tel que $p \nmid a$, on a $a^{p-1} \equiv 1 \mod p$.
13. Proposition. Soient G un groupe fini et $g, h \in G$ deux éléments commutant. Alors l'élément gh est d'ordre $\mathrm{ppcm}(\mathrm{o}(g), \mathrm{o}(h))$.

1.2. Action d'un groupe fini sur un ensemble fini

14. Définition. Soit G un groupe agissant sur un ensemble X. L'*orbite* d'un élément $x \in X$ est l'ensemble

$$\mathrm{Orb}_G(x) \coloneqq \{g \cdot x \mid g \in G\} \subset X$$

et son stabilisateur est l'ensemble

$$\mathrm{Stab}_G(x) \coloneqq \{g \in G \mid g \cdot x = x\} \subset G.$$

L'ensemble des orbites est noté G/X.
15. Exemple. En considérant l'action du groupe $\mathfrak{S}_3$ sur l'ensemble $\{1, 2, 3\}$, le stabilisateur de l'entier 1 est l'ensemble $\mathrm{Stab}_{\mathfrak{S}_3}(1) = \{\mathrm{Id}, (2\ 3)\}$ et son orbite est l'ensemble $\mathrm{Orb}_{\mathfrak{S}_3}(1) = \{1, 2, 3\}$.
16. Proposition. Les stabilisateurs sont des sous-groupes de G.
17. Proposition. Soit $x \in X$ un élément. Alors l'application

$$\begin{vmatrix} G/\mathrm{Stab}_G(x) \longrightarrow \mathrm{Orb}_G(x), \\ g\,\mathrm{Stab}_G(x) \longmapsto g \cdot x \end{vmatrix}$$

est une bijection.
18. Corollaire. Soit $x \in X$ un élément. Alors $|\mathrm{Orb}_G(x)| = [G : \mathrm{Stab}_G(x)]$. En particulier, si le groupe G est fini, alors

$$|\mathrm{Orb}_G(x)| = |G| \,/\, |\mathrm{Stab}_G(x)|.$$

19. Théorème *(équation aux classes)*. Soit G un groupe agissant sur ensemble fini X. Soit $\{x_1, \ldots, x_r\}$ un système de représentants des orbites. Alors

$$|X| = \sum_{i=1}^{r} \frac{|G|}{|\mathrm{Stab}_G(x_i)|}.$$

20. Remarque. Si l'action est transitive, alors $|X| = |G| \,/\, |\mathrm{Stab}_G(x)|$ avec $x \in X$.
21. Corollaire. Soit $\{x_1, \ldots, x_r\}$ un système de représentants des orbites non ponctuelles. Alors

$$|X| = |X^G| + \sum_{i=1}^{r} \frac{|G|}{|\mathrm{Stab}_G(x_i)|}.$$

22. Théorème *(Burnside)*. Soit G un groupe fini agissant sur un ensemble fini X. Pour un élément $g \in G$, on note

$$\mathrm{Fix}(g) \coloneqq \{x \in X \mid g \cdot x = x\}.$$

Alors le nombre d'orbites $t \geqslant 1$ vérifiant la relation

$$\sum_{g \in G} |\mathrm{Fix}(g)| = t\,|G|.$$

1.3. Les p-groupes et les théorèmes de Sylow

23. Définition. Soit p un nombre premier. Un *p-groupe* est un groupe fini dont le cardinal est une puissance de l'entier p.
24. Exemple. Le groupe diédral $\mathbf{D}_4$ d'ordre 4 est un 2-groupe.
25. Lemme. Soit G un p-groupe agissant sur un ensemble fini X. On note $X^G \subset X$ l'ensemble des points fixes sous cette action. Alors

$$|X^G| \equiv |X| \mod p.$$

26. Théorème *(Cauchy)*. Tout groupe fini d'ordre divisible par un nombre premier p admet un élément d'ordre p.
27. Proposition. Le centre d'un p-groupe non trivial est non trivial.
28. Définition. Soient G un groupe fini de cardinal n et p un diviseur premier de l'entier n. On note $n = p^\alpha m$ avec $p \nmid m$. Un *p-sous-groupe de Sylow* de G est un sous-groupe de cardinal p^α.
29. Exemple. Un p-sous-groupe de Sylow du groupe $\mathrm{GL}_n(\mathbf{F}_p)$ est le groupe des matrices triangulaires supérieures dont les coefficients de la diagonale valent 1.
30. Théorème *(Sylow)*. Soient G un groupe fini et p un diviseur de son ordre. Alors le groupe G contient au moins un p-sous-groupe de Sylow.
31. Théorème *(Sylow)*. Soient G un groupe fini de cardinal n et p un diviseur premier de l'entier n. On note $n = p^\alpha m$ avec $p \nmid m$. Alors

– pour tout sous-groupe $H \subset G$, il existe un p-sous-groupe de Sylow $S \subset G$ tel que $H \subset S$;
– les p-sous-groupes de Sylow sont conjugués ;
– le nombre de p-sous-groupes de Sylow vérifie $k \equiv 1 \mod p$ et $k \mid |G|$

32. Corollaire. Soit S un p-sous-groupe de Sylow de G. Alors il est distingué si et seulement s'il est l'unique p-sous-groupe de Sylow de G.

2. Les groupes abéliens finis

2.1. Cyclicité d'un groupe

33. Définition. Un groupe G est *monogène* s'il existe un élément $g \in G$ tel que $G = \langle g \rangle$. Dans ce cas, on dit que l'élément g est un *générateur* du groupe G. Un *groupe cyclique* est un groupe fini monogène.
34. Exemple. Le groupe $\mathbf{Z}/4\mathbf{Z}$ est cyclique et il est engendré par l'élément 1 ou 3. Le groupe $\mathbf{Z}$ est monogène mais non cyclique.
35. Proposition. Soit $n \geqslant 1$ un entier. Alors le groupe $\mathbf{Z}/n\mathbf{Z}$ est cyclique. Plus précisément, un élément $k \in \mathbf{Z}/n\mathbf{Z}$ le génère si et seulement si $n \wedge k = 1$.
36. Théorème. Tout groupe cyclique d'ordre n est isomorphe au groupe $\mathbf{Z}/n\mathbf{Z}$.
37. Exemple. Le groupe $\mathbf{U}_n \subset \mathbf{C}^\times$ des racines n-ième de l'unité est cyclique, il est donc isomorphe au groupe $\mathbf{Z}/n\mathbf{Z}$.
38. Corollaire. Deux groupes cycliques de même ordre sont isomorphes.
39. Corollaire. Soient G un groupe fini et $g \in G$ un élément. Alors $\langle g \rangle \simeq \mathbf{Z}/\mathrm{o}(g)\mathbf{Z}$.
40. Proposition. Un groupe fini d'ordre premier est cyclique.
41. Proposition. Tout sous-groupe d'un groupe cyclique est cyclique.

2.2. Le théorème de structure des groupes abéliens finis

42. Théorème *(de structure)*. Soit G un groupe abélien fini. Alors il existe un unique entier $r \geqslant 1$ et des uniques entiers $e_1, \dots, e_r \geqslant 1$ vérifiant

$$G \simeq \mathbf{Z}/e_1\mathbf{Z} \times \cdots \times \mathbf{Z}/e_r\mathbf{Z} \qquad \text{et} \qquad e_1 \mid \cdots \mid e_r. \tag{$*$}$$

43. Exemple. À isomorphisme près, il existe deux groupes d'ordre $60 = 2^2 \times 3 \times 5$.
44. Corollaire. Soient k un corps et $G \subset k^\times$ un sous-groupe fini. Alors ce dernier est cyclique.
45. Exemple. Le groupe $\mathbf{F}_q^\times$ est isomorphe au groupe $\mathbf{Z}/(q-1)\mathbf{Z}$.
46. Définition. L'*exposant* d'un groupe est le PPCM des ordres de ses éléments.
47. Corollaire. Soit G un groupe d'ordre e. On le décompose sous la forme $(*)$. Alors $e = e_r$ et le groupe G admet un élément d'ordre e.

3. Des groupes non abéliens finis remarquables

3.1. Le groupe symétrique

48. Proposition. Le groupe symétrique $\mathfrak{S}_n$ est d'ordre $n!$ et il n'est pas abélien lorsque $n > 2$. Il est engendré par
– soit les transpositions de $\mathfrak{S}_n$;
– soit les transpositions de la forme $(1\ i)$ avec $i \in \{2, \dots, n\}$;
– soit les transpositions de la forme $(i\ i+1)$ avec $i \in \{1, \dots, n-1\}$.

49. Proposition. L'action par translation sur un groupe G est fidèle et transitive. En particulier, elle donne un morphisme de groupes injectif $G \hookrightarrow \mathfrak{S}(G)$.
50. Théorème *(Cayley)*. Soit G un groupe fini d'ordre n. Alors il est isomorphe à un sous-groupe du groupe $\mathfrak{S}_n$.
51. Définition. Le *groupe alterné* est le groupe distingué $\mathfrak{A}_n < \mathfrak{S}_n$ défini comme étant le noyau du morphisme signature $\mathfrak{S}_n \longrightarrow \{\pm 1\}$
52. Lemme. Le groupe $\mathfrak{A}_5$ est simple.
53. Théorème. Lorsque $n \geqslant 5$, le groupe $\mathfrak{A}_n$ est simple.

3.2. Le groupe linéaire d'un espace vectoriel et ses sous-groupes

54. Définition. Soit E un k-espace vectoriel. Son *groupe linéaire* est le groupe $\mathrm{GL}(E)$ des automorphismes de l'espace E. Son *groupe spécial linéaire* est le noyau $\mathrm{SL}(E)$ du morphisme de groupes det : $\mathrm{GL}(E) \longrightarrow k^\times$.
55. Théorème. Le groupe $\mathrm{SL}(E)$ est engendré par les transvections.
56. Corollaire. Le groupe $\mathrm{GL}(E)$ est engendré par les transvections et dilatations.
57. Définition. Soit E un espace euclidien. Le *groupe orthogonal* de l'espace E est le sous-groupe $\mathrm{O}(E) < \mathrm{GL}(E)$ des isométries. Son *groupe spécial orthogonal* est le sous-groupe $\mathrm{SO}(E) \coloneqq \mathrm{SL}(E) \cap \mathrm{O}(E)$.
58. Théorème. Le groupe $\mathrm{O}(E)$ est engendré par les réflexions.
59. Corollaire. Le groupe $\mathrm{SO}(E)$ est engendré par les retournements.
60. Remarque. En introduisant les matrices de permutations, on obtient un morphisme injectif $\mathfrak{S}_n \hookrightarrow \mathrm{SO}(\mathbf{R}^n)$.

3.3. Les groupes d'isométries préservant un ensemble

61. Définition. Le *groupe diédral de degré n* est le groupe $\mathbf{D}_n$ des isométries préservant le polygone régulier $\mathscr{P}_n \subset \mathbf{R}^2$ à n sommets.
62. Remarque. Le groupe $\mathbf{D}_n$ agit naturellement sur le polygone $\mathscr{P}_n$ et.
63. Proposition. Le groupe $\mathbf{D}_n$ est d'ordre $2n$ et il est isomorphe au groupe

$$\langle r, s \mid r^n = e,\ s^2 = e,\ srs^{-1} = r^{-1} \rangle.$$

64. Proposition. Soit G un groupe. Alors les points suivants sont équivalents :
– le groupe G est isomorphe au groupe $\mathbf{D}_n$;
– il est engendré par deux éléments $a, b \in G$ tels que $\mathrm{o}(a) = \mathrm{o}(ab) = 2$ et $\mathrm{o}(b) = n$.

65. Définition. Soit $\mathscr{E}$ un espace affine. Une isométrie $\varphi \in \mathrm{Isom}(\mathscr{E})$ *stabilise* une partie $X \subset \mathscr{E}$ si $\varphi(X) \subset X$. On note $\mathrm{Isom}(X)$ le groupe des isométries de $\mathscr{E}$ stabilisant X ainsi que $\mathrm{Isom}^+(X)$ le groupe des isométries positives de $\mathscr{E}$ stabilisant X
66. Lemme. Soit $X \subset \mathscr{E}$. On suppose que la partie X est l'enveloppe convexe d'une partie $S \subset \mathscr{E}$ et que les points de S sont extrémaux. Alors toute isométrie stabilisant X stabilise S, c'est-à-dire $\mathrm{Isom}(X) = \mathrm{Isom}(S)$.
67. Théorème. Les groupes d'isométries du cube $C \subset \mathbf{R}^3$ sont

$$\mathrm{Isom}^+(C) \simeq \mathfrak{S}_4 \qquad \text{et} \qquad \mathrm{Isom}(C) \simeq \mathfrak{S}_4 \times \mathbf{Z}/2\mathbf{Z}.$$

[1] Josette Calais. *Éléments de théorie des groupes*. 3e édition. Presses Universitaires de France, 1998.
[2] Philippe Caldero et Jérôme Germoni. *Nouvelles histoires hédonistes de groupes et de géométries*. T. Tome second. Calvage & Mounet, 2018.
[3] Daniel Perrin. *Cours d'algèbre*. Ellipses, 1996.
[4] Felix Ulmer. *Théorie des groupes*. 2e édition. Ellipses, 2021.

- D1 -
- D2 -