Leçon 104 : Groupes finis, exemples et applications

astrid.thollet

February 2026

1 Définitions et propriétés

Soit $(G, \cdot)$ un groupe, on appellera G ce même groupe, et on notera 1 son neutre. Pour $x, y \in G$on notera $xy = x \cdot y$ et $x^n = x \cdot x \cdot \cdots \cdot x$ (n fois) avec la convention $x^0 = 1$.

1.1 Ordre

Définition 1 (Ordre d'un groupe)**.** *On appelle l'ordre de $(G, \cdot)$ le cardinal de G (fini ou infini)*

Exemple 2. $\{1\}$ *est l'unique groupe d'ordre* 1 *à isomorphisme près (groupe trivial).*
$\{1, y\}$ *avec* $y^2 = 1$ *est l'unique groupe d'ordre* 2 *à isomorphisme près.*

Exemple 3 (Groupe symétrique)**.** *Soit X un ensemble, on note S_X l'ensemble des bijections de X vers X (permutations de X), muni de la loi de composition $\circ$ des applications. C'est une groupe, qu'on appelle "Groupe symétrique de X", de neutre Id_X. L'inverse d'une bijection σ^{-1} est sa bijection réciproque σ^{-1}.*
Dans le cas $X = \{1, \ldots, n\}$ avec $n \in \mathbb{N}^*$ on le note S_n et on a $|S_n| = n!$.

Exemple 4 (Groupe linéaire)**.** *Soit V un $\mathbb{R}$espace vectoriel de dimension non nulle, l'ensemble des applications k-linéaires bijectives de V (automorphismes de V) muni de la loi $\circ$ de composition des applications est un groupe appelé groupe linéaire de V, noté $GL(V)$.*
Il est d'ordre infini.

Proposition 5. *Soit $f : G \to G'$ un morphisme de groupes, alors les fibres non vides sont en bijection ensembliste avec* $\ker f$*. En particulier :*

1. *f est injective si et seulement si* $\ker f = \{1\}$
2. *Si G est fini, on a* $|G| = |Imf| \times |\ker f|$.

Proposition 6 (Cayley)**.** *Tout groupe d'ordre fini n est isomorphe à un sous-groupe de S_n.*

Définition 7 (Ordre d'un élément)**.** *Soit $g \in G$. On considère le morphisme surjectif $\varphi : \mathbb{Z} \to < g >$, $m \mapsto g^m$.*

1. *Si φ est injectif, on dit que g est d'ordre infini.*
2.

Si φ n'est pas injectif, on dit que g est d'ordre fini et on appelle ordre de g l'unique entier $d \geq 1$ tel que $\ker \varphi = d\mathbb{Z}$.
De manière équivalente, $d = \min\{n \in \mathbb{N}^*, g^n = 1\}$.

Proposition 8. *Si $g \in G$ d'ordre fini d, $< g >$ est isomorphe à $\mathbb{Z}/d\mathbb{Z}$.*

Proposition 9. *(Isomorphisme chinois) Soient $n, m \in \mathbb{Z}$ premiers entre eux, $\phi : \mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}), k \mapsto (k \ mod\ n, k \ mod\ m)$ définit par passage au quotient un isomorphisme d'anneaux $(\mathbb{Z}/nm\mathbb{Z}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$.*

1.2 Théorème de Lagrange

Théorème 10 (Lagrange)**.** *Si H est un sous-groupe de G et $q : G \to G/H$ l'application de passage au quotient. Les fibres de q sont en bijection avec H. En particulier, si deux des trois ensembles G, H et G/H sont finis, le troisième l'est aussi et on a $|G| = |H| \times [G : H]$.*

Proposition 11 (Corollaires - Théorèmes de Lagrange)**.**

1. *Si H est un sous-groupe de G alors $|H|$ divise $|G|$.*
2. *Si G est fini et si $g \in G$ alors $g^{|G|} = 1$*

Proposition 12 (Corollaire)**.** *Tout groupe d'ordre premier p est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.*

1.3 Groupes abéliens finis

Théorème 13 (Théorème de structure des groupes abéliens finis)**.** *Soit G un groupe abélien fini non trivial. Il existe un unique entier $n \geq 1$ et des uniques entiers $a_1, \ldots, a_n > 1$ tels que $a_1 | a_2 | \ldots a_n$ vérifiant*

$$G \simeq \prod_{i=1}^{n} \mathbb{Z}/a_i\mathbb{Z}.$$

Les a_i s'appellent les diviseurs élémentaires de G

Exemple 14. *Les groupes abéliens de cardinal 8 sont, à isomorphisme près, $\mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ et $(\mathbb{Z}/2\mathbb{Z})^3$.*

Exemple 15. *Soit $G = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$.*
Ses diviseurs élémentaires sont 2 et 30 et par isomorphismes chinois on a $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$.

2 Les groupes symétrique et alterné

2.1 Le groupe symétrique

Soit $n \geq 1$ un entier.

Définition 16. *Soit $\sigma \in S_n$. On note Fix$\sigma = \{i \in \{1, \ldots, n\}, \sigma(i) = i\}$(points fixes de σ) et Suppσ son complémentaires (support de σ).*

Proposition 17. *Deux permutations à supports disjoints commutent.*

Définition 18. *Si $2 \leq k \leq n$ un entier, on appelle k-cycle (ou cycle de longueur k) une permutation σ telle que :*

1. *$|Supp\ \sigma| = k$,*
2. *Il existe une énumération Supp $\sigma = \{i_1, \ldots, i_k\}$ qui vérifie $\forall m \in \{1, \ldots, k-1\}$, $\sigma(i_k) = \sigma(i_{k+1})$ et $\sigma(i_k) = i_1$.*

On appelle tout cycle de longueur 2 une transposition.

Proposition 19. *Soit $k \in \{2, \dots, n\}$, un k-cycle est d'ordre k.*
Les k-cycles sont conjugués.

Proposition 20 (Décomposition en cycles d'une permutation)**.** *Soit $\sigma \in S_n$, il existe unique famille de cycles $\{c_i\}$ à supports disjoints telle que $\sigma = \Pi c_i$.*
En particulier, les cycles engendrent S_n.

Exemple 21. *On a la décomposition en cycles suivante :* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 8 & 6 & 1 & 3 & 4 & 7 & 2 \end{pmatrix} = (1\,5\,3\,6\,4)(2\,8)$.

Proposition 22. *Soit $\sigma \in S_n$ décomposée en cycles $\sigma = \Pi c_i$, alors l'ordre de σ est le ppcm des longueurs des c_i.*

Proposition 23. *Les transposition engendrent S_n.*

2.2 Le groupe alterné

Définition 24 (Signature)**.** *On définit la signature d'une permutation $\sigma \in S_n$ par*

$$\varepsilon(\sigma) = \prod_{\{i,j\} \in \{1,\dots,n\}^2} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

Proposition 25. *La signature est un morphisme de groupes $\varepsilon : S_n \to \{-1, 1\}$.*
Pour toute transposition τ on a $\varepsilon(\tau) = -1$.

Définition 26. *On définit le groupe alterné $A_n = \ker \varepsilon$ (sous-groupe des permutations paires).*

Proposition 27. *A_n est distingué, et si $n \geq 2$ on a $|A_n| = \frac{n!}{2}$.*

[Début DEV 1]

Proposition 28. *Les produits de deux transpositions engendrent A_n.*
Les 3-cycles engendrent A_n.

Proposition 29. *On a $A_1 = A_2 = \{1\}$ et $A_3 \simeq \mathbb{Z}/3/Z$.*
A_4 n'est pas simple.
Pour $n \geq 5$, A_n est simple.

[Fin DEV 1]

3 Sous-groupes finis de $O(3)$ et $SO(3)$

On fixe E_3 un espace euclidien de dimension 3, et on considère les polyèdres convexes (bornés) réguliers (solides de Platon) centrés en 0.

Définition 30. *Soit P un tel polyèdre, on note $Iso(P) = \{g \in O(E_3), g(P) = P\}$.*
On note $\mathcal{S}$ l'ensemble de ses sommets, $\mathcal{A}$ celui de ses arrêtes et $\mathcal{F}$ l'ensemble de ses faces.

Proposition 31. *L'action de $Iso(P)$ est fidèle sur $\mathcal{S}$.*

(Début DEV 2 - Solides de Platon)

Proposition 32. *Soit T le tétraèdre régulier, on a $Iso(T) \simeq S_4$ et $Iso^+(T) \simeq A_4$.*

Proposition 33. *Soit C le cube, on a $Iso^+(C) \simeq S_4$ et $Iso^+ \times \{-1, +1\} \simeq Iso(C)$.*

Proposition 34 (Dualité entre O et C)**.** *Soit O l'octaèdre régulier, on a $Iso(O) = Iso(C)$.*

Proposition 35. *Soit D le dodécaèdre régulier, on a $Iso^+(D) \simeq A_5$ et $Iso(D) = \{-1, +1\} \times Iso^+(D)$*

Proposition 36. *([Dualité entre I et D] Soit I l'icosaèdre réguliers, on a $Iso(I) = Iso(D)$.*

(Fin DEV 2)

Théorème 37 (Klein)**.** *Les sous-groupes finis de $SO(3)$ sont, à conjugaison près, les groupes évoqués ci-dessus.*
Autrement dit : tout sous-groupe fini de $SO(3)$ est soit cyclique, soit un groupe de Klein (isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$), soit dihédral (isomorphe à) soit isomorphe à A_4, S_4 ou A_5.