

Algèbre I — Master 1

Séance 1 — Révisions de théorie des groupes

Groupes quotients, actions, suites exactes et produits semi-directs

But de la séance. Revoir les constructions de théorie des groupes qui interviendront dans la suite du cours, notamment en théorie des modules et des représentations : noyaux et quotients, actions, orbites et stabilisateurs, suites exactes et extensions scindées.

Table des matières

1	Groupes, sous-groupes et morphismes	1
1.1	Groupes et exemples fondamentaux	1
1.2	Sous-groupes et générateurs	2
1.3	Morphismes, noyau et image	2
2	Sous-groupes normaux et quotients	3
2.1	Normalité	3
2.2	Le groupe quotient	3
2.3	Premier théorème d'isomorphisme	4
3	Actions de groupes	4
3.1	Définition et premiers exemples	4
3.2	Orbites et stabilisateurs	5
3.3	Conjugaison et équation des classes	5
3.4	Le lemme de Burnside	5
4	Quelques théorèmes sur les groupes finis	6
5	Suites exactes et produits semi-directs	6
5.1	Suites exactes courtes	6
5.2	Produit direct	7
5.3	Produit semi-direct	7
6	Des actions aux représentations	8
7	Compléments : séries de composition, résolubilité et nilpotence	8
7.1	Séries de composition et théorème de Jordan–Hölder	8
7.2	Groupes résolubles	9
7.3	Groupes nilpotents	9
	À retenir	9

1. Groupes, sous-groupes et morphismes

1.1. Groupes et exemples fondamentaux

Définition 1.1. Un *groupe* est un ensemble G muni d'une loi de composition

$$G \times G \longrightarrow G, \quad (g, h) \longmapsto gh,$$

qui est associative, possède un élément neutre e , et pour laquelle tout $g \in G$ possède un inverse g^{-1} . Le groupe est *abélien* si $gh = hg$ pour tous $g, h \in G$.

Les exemples suivants serviront tout au long du cours.

1. $(\mathbb{Z}, +)$ et ses quotients $\mathbb{Z}/n\mathbb{Z}$ sont des groupes abéliens.
2. Le groupe symétrique $\mathfrak{S}_n$ est le groupe des permutations de $\{1, \dots, n\}$. Il n'est pas abélien pour $n \geq 3$.
3. Si V est un espace vectoriel sur un corps $\mathbf{k}$, les automorphismes linéaires de V forment le groupe $\mathrm{GL}(V)$. Après le choix d'une base de V de dimension n , on obtient $\mathrm{GL}(V) \simeq \mathrm{GL}_n(\mathbf{k})$.
4. Si A est un anneau unitaire, l'ensemble $A^\times$ de ses éléments inversibles est un groupe pour la multiplication.
5. Plus généralement, dans toute catégorie, les automorphismes d'un objet X forment un groupe $\mathrm{Aut}(X)$.

Le dernier exemple donne un principe important : faire agir un groupe G sur un objet X revient à construire un morphisme $G \rightarrow \mathrm{Aut}(X)$, pour une notion d'automorphisme adaptée à la structure portée par X .

1.2. Sous-groupes et générateurs

Proposition 1.2 (Critère de sous-groupe). *Soit H une partie non vide d'un groupe G . Les conditions suivantes sont équivalentes :*

- (i) H est un sous-groupe de G ;
- (ii) pour tous $x, y \in H$, on a $xy^{-1} \in H$.

Démonstration. La première condition implique clairement la seconde. Réciproquement, choisissons $x \in H$. Alors $e = xx^{-1} \in H$. Pour $y \in H$, on obtient $y^{-1} = ey^{-1} \in H$, puis $xy = x(y^{-1})^{-1} \in H$ pour $x, y \in H$. $\square$

Si $S \subseteq G$, le *sous-groupe engendré* par S , noté $\langle S \rangle$, est le plus petit sous-groupe de G contenant S . Explicitement, ses éléments sont les produits finis

$$s_1^{\varepsilon_1} \cdots s_r^{\varepsilon_r}, \quad s_i \in S, \quad \varepsilon_i \in \{1, -1\}.$$

Un groupe engendré par un seul élément est dit *cyclique*. Tout groupe cyclique infini est isomorphe à $\mathbb{Z}$ et tout groupe cyclique fini d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Exemple 1.3. Le groupe $\mathfrak{S}_n$ est engendré par les transpositions adjacentes $(1\ 2), (2\ 3), \dots, (n-1\ n)$. Le groupe diédral des symétries d'un n -gone régulier est engendré par une rotation r et une réflexion s , avec la présentation

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

Ici, la notation D_{2n} indique que le groupe possède $2n$ éléments.

1.3. Morphismes, noyau et image

Définition 1.4. Un *morphisme de groupes* $f: G \rightarrow H$ est une application vérifiant $f(gg') = f(g)f(g')$. Son noyau et son image sont

$$\mathrm{Ker}(f) = \{g \in G \mid f(g) = e_H\}, \quad \mathrm{Im}(f) = \{f(g) \mid g \in G\}.$$

On a automatiquement $f(e_G) = e_H$ et $f(g^{-1}) = f(g)^{-1}$. Le noyau est un sous-groupe de G , l'image un sous-groupe de H , et

$$f \text{ est injectif} \iff \text{Ker}(f) = \{e_G\}, \quad f \text{ est surjectif} \iff \text{Im}(f) = H.$$

Exemple 1.5. 1. Le déterminant $\det: \text{GL}_n(\mathbf{k}) \rightarrow \mathbf{k}^\times$ est surjectif et son noyau est $\text{SL}_n(\mathbf{k})$.

2. La signature $\text{sgn}: \mathfrak{S}_n \rightarrow \{\pm 1\}$ a pour noyau le groupe alterné $\mathfrak{A}_n$.

3. La projection $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ a pour noyau $n\mathbb{Z}$.

2. Sous-groupes normaux et quotients

2.1. Normalité

Définition 2.1. Un sous-groupe $N \subseteq G$ est *normal*, ce que l'on note $N \trianglelefteq G$, si

$$gNg^{-1} = N \quad \text{pour tout } g \in G.$$

Cela équivaut à $gN = Ng$ pour tout $g \in G$.

Tout sous-groupe d'un groupe abélien est normal. Le centre

$$Z(G) = \{z \in G \mid zg = gz \text{ pour tout } g \in G\}$$

est normal dans G . En revanche, un sous-groupe quelconque n'est pas nécessairement normal : dans $\mathfrak{S}_3$, le sous-groupe engendré par $(1\ 2)$ ne l'est pas.

Proposition 2.2. *Le noyau d'un morphisme de groupes $f: G \rightarrow H$ est un sous-groupe normal de G .*

Démonstration. Si $n \in \text{Ker}(f)$ et $g \in G$, alors $f(gng^{-1}) = f(g)f(n)f(g)^{-1} = e_H$. Ainsi $g\text{Ker}(f)g^{-1} \subseteq \text{Ker}(f)$; l'inclusion inverse s'obtient en remplaçant g par g^{-1} . $\square$

2.2. Le groupe quotient

Soit $N \trianglelefteq G$. Sur l'ensemble des classes à gauche G/N , on définit

$$(gN)(hN) = ghN.$$

Cette loi est bien définie : si $g' = gn$ et $h' = hm$, avec $n, m \in N$, alors

$$g'h' = gnhm = gh(h^{-1}nh)m \in ghN,$$

car $h^{-1}nh \in N$. L'ensemble G/N devient ainsi un groupe et la projection canonique

$$\pi: G \longrightarrow G/N, \quad g \longmapsto gN,$$

est un morphisme surjectif de noyau N .

On obtient donc la caractérisation conceptuelle suivante : les sous-groupes normaux sont exactement les noyaux de morphismes de groupes.

Remarque 2.3. Pour un sous-groupe H non nécessairement normal, l'ensemble G/H des classes à gauche existe toujours et porte une action naturelle de G , mais il ne possède en général aucune structure naturelle de groupe.

2.3. Premier théorème d'isomorphisme

Théorème 2.4 (Premier théorème d'isomorphisme). Soit $f: G \rightarrow H$ un morphisme de groupes. L'application

$$\bar{f}: G/\text{Ker}(f) \longrightarrow \text{Im}(f), \quad g \text{Ker}(f) \longmapsto f(g),$$

est un isomorphisme. Ainsi

$$G/\text{Ker}(f) \simeq \text{Im}(f).$$

Démonstration. Si $g \text{Ker}(f) = g' \text{Ker}(f)$, alors $g'^{-1}g \in \text{Ker}(f)$, donc $f(g) = f(g')$: l'application est bien définie. C'est un morphisme, car $\bar{f}(gg' \text{Ker}(f)) = f(g)f(g')$. Elle est surjective par définition de l'image. Enfin, si $\bar{f}(g \text{Ker}(f)) = e_H$, alors $g \in \text{Ker}(f)$, donc la classe de g est la classe neutre : $\bar{f}$ est injective. $\square$

Exemple 2.5. On retrouve

$$\text{GL}_n(\mathbf{k})/\text{SL}_n(\mathbf{k}) \simeq \mathbf{k}^\times, \quad \mathfrak{S}_n/\mathfrak{A}_n \simeq \{\pm 1\} \quad (n \geq 2), \quad \mathbb{Z}/n\mathbb{Z} \simeq \text{Im}(\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}).$$

Exercice 2.6. Soient H, K deux sous-groupes d'un groupe G , avec $H \trianglelefteq G$. Montrer que $HK = \{hk \mid h \in H, k \in K\}$ est un sous-groupe de G , que $H \cap K \trianglelefteq K$, et construire un isomorphisme

$$K/(H \cap K) \simeq HK/H.$$

3. Actions de groupes

3.1. Définition et premiers exemples

Définition 3.1. Une *action à gauche* d'un groupe G sur un ensemble X est une application $G \times X \rightarrow X$, $(g, x) \mapsto g \cdot x$, telle que

$$e \cdot x = x, \quad (gh) \cdot x = g \cdot (h \cdot x).$$

De manière équivalente, c'est un morphisme

$$\rho: G \longrightarrow \text{Aut}(X), \quad g \longmapsto (x \mapsto g \cdot x).$$

Exemple 3.2. 1. G agit sur lui-même par translations à gauche : $g \cdot x = gx$. Cette action est transitive et libre.

2. G agit sur lui-même par conjugaison : $g \cdot x = gxg^{-1}$.

3. Si $H \subseteq G$, alors G agit sur G/H par $g \cdot (xH) = (gx)H$.

4. $\mathfrak{S}_n$ agit sur $\{1, \dots, n\}$ par permutation.

5. $\text{GL}(V)$ agit sur V , sur l'ensemble de ses sous-espaces, et sur les constructions tensorielles associées à V .

Une action est dite *transitive* si elle n'a qu'une orbite, et *libre* si $g \cdot x = x$ implique $g = e$. Elle est *fidèle* si le morphisme $G \rightarrow \text{Aut}(X)$ est injectif. Ces trois notions sont distinctes.

3.2. Orbites et stabilisateurs

Définition 3.3. Pour $x \in X$, l'orbite et le stabilisateur de x sont

$$G \cdot x = \{g \cdot x \mid g \in G\}, \quad G_x = \text{Stab}_G(x) = \{g \in G \mid g \cdot x = x\}.$$

Les orbites forment une partition de X . Le stabilisateur G_x est un sous-groupe de G ; si $y = g \cdot x$, alors $G_y = gG_xg^{-1}$.

Théorème 3.4 (Orbite–stabilisateur). Pour tout $x \in X$, l'application

$$G/G_x \longrightarrow G \cdot x, \quad gG_x \longmapsto g \cdot x,$$

est une bijection. Si G est fini, alors

$$|G \cdot x| = [G : G_x], \quad |G| = |G \cdot x| |G_x|.$$

Démonstration. Deux éléments $g, h \in G$ ont la même image si et seulement si $g \cdot x = h \cdot x$, c'est-à-dire si et seulement si $h^{-1}g \in G_x$, ou encore $gG_x = hG_x$. L'application induite est donc injective ; elle est surjective par définition de l'orbite. $\square$

Si G et X sont finis et si $x_1, \dots, x_r$ représentent les orbites,

$$|X| = \sum_{i=1}^r |G \cdot x_i| = \sum_{i=1}^r [G : G_{x_i}].$$

3.3. Conjugaison et équation des classes

Pour l'action de conjugaison de G sur lui-même, l'orbite de x est sa *classe de conjugaison* et son stabilisateur est le centralisateur

$$C_G(x) = \{g \in G \mid gx = xg\}.$$

La classe de conjugaison de x est donc en bijection avec $G/C_G(x)$. Les points fixes de l'action sont exactement les éléments du centre $Z(G)$.

Proposition 3.5 (Équation des classes). Si G est fini et si $x_1, \dots, x_r$ représentent les classes de conjugaison non centrales, alors

$$|G| = |Z(G)| + \sum_{i=1}^r [G : C_G(x_i)].$$

Corollaire 3.6. Tout groupe fini d'ordre p^n , où p est premier et $n \geq 1$, possède un centre non trivial.

Démonstration. Dans l'équation des classes, chaque indice $[G : C_G(x_i)]$ est une puissance de p strictement supérieure à 1, donc est divisible par p . Par conséquent, $|Z(G)|$ est divisible par p . $\square$

3.4. Le lemme de Burnside

La formule suivante sera utile pour les représentations de permutation.

Théorème 3.7 (Lemme de Burnside, ou formule de Cauchy–Frobenius). Si un groupe fini G agit sur un ensemble fini X , le nombre d'orbites est

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|, \quad X^g = \{x \in X \mid g \cdot x = x\}.$$

Démonstration. Comptons de deux manières l'ensemble $\{(g, x) \in G \times X \mid g \cdot x = x\}$. En fixant g , sa cardinalité vaut $\sum_x |X^g|$. En fixant x , elle vaut $\sum_g |G_x|$. Sur chaque orbite $\mathcal{O}$, le théorème orbite–stabilisateur donne $\sum_{x \in \mathcal{O}} |G_x| = |G|$. Le résultat s'ensuit. $\square$

4. Quelques théorèmes sur les groupes finis

Théorème 4.1 (Lagrange). *Si H est un sous-groupe d'un groupe fini G , alors*

$$|G| = [G : H]|H|.$$

En particulier, $|H|$ divise $|G|$, l'ordre de tout élément $g \in G$ divise $|G|$, et $g^{|G|} = e$.

Démonstration. Les classes à gauche de H partitionnent G et ont toutes $|H|$ éléments. $\square$

La réciproque de Lagrange est fautive en général : le fait qu'un entier d divise $|G|$ n'assure pas l'existence d'un sous-groupe d'ordre d . Les théorèmes suivants donnent cependant des résultats très forts pour les puissances de nombres premiers.

Théorème 4.2 (Cauchy). *Si un nombre premier p divise l'ordre d'un groupe fini G , alors G contient un élément d'ordre p .*

Théorème 4.3 (Sylow). *Écrivons $|G| = p^a m$, où p est premier et $p \nmid m$. Un sous-groupe d'ordre p^a est appelé un p -sous-groupe de Sylow. Alors :*

1. G possède au moins un p -Sylow ;
2. tous les p -Sylow sont conjugués ;
3. tout p -sous-groupe de G est contenu dans un p -Sylow ;
4. le nombre n_p des p -Sylow vérifie $n_p \equiv 1 \pmod{p}$ et $n_p \mid m$.

Exemple 4.4. Soit G un groupe d'ordre 15. On a $n_5 \mid 3$ et $n_5 \equiv 1 \pmod{5}$, donc $n_5 = 1$. L'unique 5-Sylow est normal dans G . De même, $n_3 \mid 5$ et $n_3 \equiv 1 \pmod{3}$, donc $n_3 \in \{1, 5\}$; la congruence exclut 5, et le 3-Sylow est également normal. On peut alors montrer que G est cyclique.

Remarque 4.5. Pour la suite du cours, on utilisera surtout les énoncés de Lagrange, Cauchy et Sylow, ainsi que les raisonnements par action qui les accompagnent.

5. Suites exactes et produits semi-directs

5.1. Suites exactes courtes

Définition 5.1. Une suite de morphismes de groupes

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{p} H \longrightarrow 1$$

est *exacte* si i est injectif, p est surjectif et $\text{Im}(i) = \text{Ker}(p)$. On l'appelle aussi une *extension de H par N* .

Après avoir identifié N à son image dans G , l'exactitude signifie que $N \trianglelefteq G$ et que $G/N \simeq H$. Par exemple,

$$1 \longrightarrow \text{SL}_n(\mathbf{k}) \longrightarrow \text{GL}_n(\mathbf{k}) \xrightarrow{\det} \mathbf{k}^\times \longrightarrow 1$$

et, pour $n \geq 2$,

$$1 \longrightarrow \mathfrak{A}_n \longrightarrow \mathfrak{S}_n \xrightarrow{\text{sgn}} \{\pm 1\} \longrightarrow 1$$

sont exactes.

Définition 5.2. Une *section* de p est un morphisme $s: H \rightarrow G$ tel que $p \circ s = \text{id}_H$. Si une telle section existe, l'extension est dite *scindée*.

Une section est nécessairement injective. Elle permet donc de voir H comme un sous-groupe de G , mais elle n'est en général ni unique ni normale.

5.2. Produit direct

Le produit direct $G \times H$ est muni de la loi $(g, h)(g', h') = (gg', hh')$. Il est caractérisé par la propriété universelle suivante : pour tout groupe K , la donnée d'un morphisme $u: K \rightarrow G \times H$ équivaut à la donnée du couple $(\text{pr}_G \circ u, \text{pr}_H \circ u)$ de morphismes $K \rightarrow G$ et $K \rightarrow H$.

On a une suite exacte scindée

$$1 \longrightarrow G \longrightarrow G \times H \longrightarrow H \longrightarrow 1.$$

Dans ce cas, les sous-groupes $G \times \{e\}$ et $\{e\} \times H$ commutent.

5.3. Produit semi-direct

Supposons donné un morphisme

$$\alpha: H \longrightarrow \text{Aut}(N),$$

c'est-à-dire une action de H sur le groupe N par automorphismes. Sur l'ensemble $N \times H$, posons

$$(n, h)(n', h') = (n \alpha(h)(n'), hh').$$

On obtient un groupe, appelé *produit semi-direct* de N par H et noté $N \rtimes_\alpha H$. Son élément neutre est (e_N, e_H) et

$$(n, h)^{-1} = (\alpha(h^{-1})(n^{-1}), h^{-1}).$$

Il existe une suite exacte scindée

$$1 \longrightarrow N \xrightarrow{n \mapsto (n, e_H)} N \rtimes_\alpha H \xrightarrow{(n, h) \mapsto h} H \longrightarrow 1,$$

dont une section est $h \mapsto (e_N, h)$.

Théorème 5.3. *Toute extension scindée*

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{p} H \longrightarrow 1$$

est isomorphe à un produit semi-direct $N \rtimes_\alpha H$.

Démonstration. Soit $s: H \rightarrow G$ une section. Après identification de N à $i(N)$, la conjugaison par $s(h)$ préserve $N = \text{Ker}(p)$ et définit

$$\alpha(h)(n) = s(h)ns(h)^{-1}.$$

Comme s est un morphisme, $\alpha: H \rightarrow \text{Aut}(N)$ est un morphisme. L'application

$$N \rtimes_\alpha H \longrightarrow G, \quad (n, h) \longmapsto ns(h),$$

est un morphisme. Elle est surjective, car $gs(p(g))^{-1} \in \text{Ker}(p) = N$. Elle est injective : si $ns(h) = e$, alors $h = p(ns(h)) = e_H$, puis $n = e_N$. $\square$

Exemple 5.4 (Groupe diédral). Le groupe $C_2 = \{1, \sigma\}$ agit sur $C_n = \langle r \rangle$ par inversion : $\sigma(r) = r^{-1}$. On obtient

$$D_{2n} \simeq C_n \rtimes C_2.$$

La relation $(e, \sigma)(r, e)(e, \sigma)^{-1} = (r^{-1}, e)$ est exactement la relation $srs = r^{-1}$ de la présentation précédente.

Exemple 5.5 (Groupe affine). Le groupe multiplicatif $\mathbf{k}^\times$ agit sur le groupe additif $(\mathbf{k}, +)$ par $a \cdot b = ab$. Le produit semi-direct $\mathbf{k} \rtimes \mathbf{k}^\times$ s'identifie au groupe des transformations affines de la droite

$$x \longmapsto ax + b, \quad a \in \mathbf{k}^\times, b \in \mathbf{k}.$$

La composition $(b, a)(b', a') = (b + ab', aa')$ retrouve la loi du produit semi-direct.

Remarque 5.6. Le produit semi-direct dépend de l'action α , et non seulement des deux groupes N et H . L'action triviale donne le produit direct $N \times H$.

6. Des actions aux représentations

Définition 6.1. Une *représentation linéaire* d'un groupe G sur un espace vectoriel V sur $\mathbf{k}$ est un morphisme

$$\rho: G \longrightarrow \mathrm{GL}(V).$$

Autrement dit, c'est une action de G sur V telle que chaque application $v \mapsto g \cdot v$ soit linéaire.

Le vocabulaire des actions se traduit ainsi :

- la représentation est *fidèle* si $\mathrm{Ker}(\rho) = \{e\}$;
- un sous-espace $W \subseteq V$ est une *sous-représentation* s'il est stable sous l'action de G ;
- une action de G sur un ensemble fini X fournit une représentation de permutation sur l'espace vectoriel $\mathbf{k}[X]$ de base $(e_x)_{x \in X}$, par $g \cdot e_x = e_{g \cdot x}$.

L'objet qui reliera la théorie des anneaux à celle des représentations est l'*algèbre de groupe* $\mathbf{k}[G]$. Une représentation de G sur un $\mathbf{k}$ -espace vectoriel sera exactement un $\mathbf{k}[G]$ -module. Cette équivalence sera étudiée dans la seconde partie du cours.

Enfin, si V est de dimension finie, le caractère de V est la fonction

$$\chi_V(g) = \mathrm{Tr}(\rho(g)).$$

Comme $\rho(hgh^{-1}) = \rho(h)\rho(g)\rho(h)^{-1}$, la trace montre déjà que χ_V est constante sur les classes de conjugaison.

7. Compléments : séries de composition, résolubilité et nilpotence

Cette section rassemble quelques notions structurelles importantes qui ne seront pas nécessaires à la progression principale du cours.

7.1. Séries de composition et théorème de Jordan–Hölder

Définition 7.1. Une *série de composition* d'un groupe G est une suite

$$\{e\} = G_r \trianglelefteq G_{r-1} \trianglelefteq \cdots \trianglelefteq G_1 \trianglelefteq G_0 = G$$

dans laquelle chaque G_{i+1} est normal dans G_i et chaque quotient G_i/G_{i+1} est simple. Ces quotients sont les *facteurs de composition* de la série.

Tout groupe fini non trivial admet une série de composition, par récurrence sur son ordre.

Théorème 7.2 (Jordan–Hölder). *Deux séries de composition d'un même groupe fini ont la même longueur et les mêmes facteurs de composition, à permutation et isomorphisme près.*

Ainsi, les facteurs simples jouent pour les groupes finis un rôle analogue à celui des facteurs premiers d'un entier. Le théorème n'affirme toutefois pas que le groupe est déterminé par ses facteurs de composition : la manière dont les extensions sont assemblées contient une information supplémentaire.

7.2. Groupes résolubles

Pour deux éléments $x, y \in G$, leur commutateur est $[x, y] = xyx^{-1}y^{-1}$. Le *sous-groupe dérivé* $[G, G]$ est le sous-groupe engendré par tous les commutateurs. Il est normal et le quotient

$$G^{\text{ab}} = G/[G, G]$$

est le plus grand quotient abélien de G : tout morphisme de G vers un groupe abélien se factorise de façon unique par G^{ab} .

On définit la série dérivée par

$$G^{(0)} = G, \quad G^{(i+1)} = [G^{(i)}, G^{(i)}].$$

Le groupe G est *résoluble* si $G^{(r)} = \{e\}$ pour un certain r . Équivalamment, G possède une suite subnormale dont les quotients successifs sont abéliens. Les groupes abéliens et les p -groupes finis sont résolubles ; $\mathfrak{S}_n$ est résoluble pour $n \leq 4$ et ne l'est pas pour $n \geq 5$.

7.3. Groupes nilpotents

Pour des sous-groupes $A, B \subseteq G$, on note $[A, B]$ le sous-groupe engendré par les commutateurs $[a, b]$. La série centrale descendante est définie par

$$\gamma_1(G) = G, \quad \gamma_{i+1}(G) = [G, \gamma_i(G)].$$

Le groupe G est *nilpotent* si $\gamma_{c+1}(G) = \{e\}$ pour un certain c ; le plus petit tel c est sa classe de nilpotence. Un groupe est abélien si et seulement s'il est nilpotent de classe au plus 1.

Tout groupe nilpotent est résoluble. Tout p -groupe fini est nilpotent ; plus précisément, un groupe fini est nilpotent si et seulement si tous ses sous-groupes de Sylow sont normaux, ou encore s'il est le produit direct de ses sous-groupes de Sylow.

Exemple 7.3. Le groupe D_8 est nilpotent, car c'est un 2-groupe fini. Le groupe $\mathfrak{S}_3$ est résoluble, puisque $\{e\} \trianglelefteq \mathfrak{A}_3 \trianglelefteq \mathfrak{S}_3$ a des quotients abéliens, mais il n'est pas nilpotent : ses 2-Sylow ne sont pas normaux.

À retenir

- Les sous-groupes normaux sont exactement les noyaux ; ils permettent de former les groupes quotients.
- Toute action transitive est isomorphe à l'action de G sur G/H pour le stabilisateur H d'un point.
- L'équation orbite–stabilisateur est le mécanisme commun à de nombreux arguments de dénombrement en théorie des groupes finis.
- Une suite exacte courte décrit un groupe comme une extension ; si elle est scindée, le groupe est un produit semi-direct.
- Une représentation linéaire est une action sur un espace vectoriel ; elle sera reformulée comme un module sur l'algèbre de groupe.
- Les facteurs de Jordan–Hölder mesurent les constituants simples ; la résolubilité et la nilpotence expriment l'existence de dévissages par groupes abéliens ou centraux.