Algèbre Abstraite I

Groupes et Anneaux

Notes de Cours — Licence L2

1er mars 2026

Table des matières

Préface

L'algèbre abstraite, telle que nous la connaissons aujourd'hui, est le fruit d'une longue maturation intellectuelle qui s'étend sur plus de deux siècles. Ses origines se trouvent dans des questions très concrètes : la résolution d'équations polynomiales par radicaux, l'étude des symétries de figures géométriques, et l'arithmétique des nombres entiers.

C'est Joseph-Louis **Lagrange** qui, dans ses *Réflexions sur la résolution algébrique des équations* (1770–1771), mit en évidence pour la première fois le rôle des permutations des racines d'un polynôme dans la compréhension de sa résolubilité. En étudiant systématiquement les « résolvantes » associées aux équations de degré 3 et 4, Lagrange identifia un phénomène fondamental : le nombre de valeurs distinctes prises par une fonction rationnelle des racines, lorsqu'on permute celles-ci, divise le nombre total de permutations. Ce résultat, ancêtre du théorème qui porte aujourd'hui son nom, allait devenir la pierre angulaire de la théorie des groupes.

Niels Henrik **Abel** (1824) démontra l'impossibilité de résoudre par radicaux l'équation générale de degré ≥ 5, puis Évariste **Galois**, dans ses écrits tragiquement brefs (1831–1832), accomplit le pas décisif : il associa à toute équation polynomiale un *groupe* de permutations — le groupe de Galois — et montra que la résolubilité par radicaux équivaut à une propriété purement algébrique de ce groupe (sa résolubilité). Ce faisant, Galois inventa simultanément la notion de groupe, celle de sous-groupe distingué, et celle de groupe quotient, anticipant de plusieurs décennies le développement formel de ces concepts.

Au cours du XIXe siècle, Augustin-Louis **Cauchy** systématisa la théorie des permutations, Arthur **Cayley** proposa la définition abstraite d'un groupe (1854), et Camille **Jordan** publia son *Traité des substitutions et des équations algébriques* (1870), premier ouvrage de synthèse sur la théorie des groupes. Parallèlement, Richard **Dedekind** introduisit les notions d'idéal et de module, jetant les bases de l'algèbre commutative moderne.

Le XXe siècle vit l'avènement de l'algèbre abstraite proprement dite. Emmy **Noether**, dans ses travaux fondateurs des années 1920, démontra que la bonne façon d'étudier les structures algébriques consiste à se concentrer sur les *morphismes* — les applications qui préservent la structure — plutôt que sur les éléments individuels. Son approche, systématisée par Emil **Artin** et Bartel Leendert **van der Waerden** dans le célèbre traité *Moderne Algebra* (1930–1931), donna naissance au point de vue qui domine l'algèbre contemporaine : l'étude des structures (groupes, anneaux, corps, modules) et des applications qui les relient (homomorphismes, isomorphismes).

Pourquoi l'abstraction ? Le lecteur pourrait légitimement se demander pourquoi nous étudions des « groupes » et des « anneaux » en toute généralité, plutôt que de nous contenter des exemples concrets ($\mathbb{Z}$, $\mathbb{R}$, les matrices, les permutations). La réponse est triple :

(i) *Unification.* Un même théorème, démontré une fois dans le cadre abstrait, s'applique

simultanément à une multitude de situations concrètes. Le théorème de Lagrange, par exemple, donne d'un seul coup le petit théorème de Fermat, le théorème d'Euler, et des contraintes sur l'ordre des éléments de tout groupe fini.

(ii) *Clarification.* L'abstraction permet d'identifier précisément quelles hypothèses sont nécessaires pour chaque résultat, séparant l'essentiel de l'accessoire.

(iii) *Découverte.* Le cadre abstrait suggère des constructions (produits, quotients, extensions) et des questions (classification, simplicité, représentation) qui n'auraient pas émergé naturellement dans un cadre concret.

Le fil conducteur de ce cours est l'idée noethérienne que *comprendre une structure algébrique, c'est comprendre ses morphismes.* Nous étudierons chaque structure (groupe, anneau, idéal, corps) en mettant systématiquement l'accent sur les homomorphismes, les sous-structures, les quotients, et les théorèmes d'isomorphisme qui les relient. Les diagrammes commutatifs, omniprésents dans ce texte, sont l'expression visuelle de cette philosophie.

Ce premier volume couvre la théorie des groupes (chapitres 1 à 5) et l'introduction aux anneaux et corps (chapitres 6 à 8). Il est destiné aux étudiants de deuxième année de licence (L2) et suppose acquises les notions de base de la théorie des ensembles, des applications, et des relations d'équivalence.

Notations

Notation	Signification
$\mathbb{N}$	Ensemble des entiers naturels $\{0, 1, 2, \ldots\}$
$\mathbb{Z}$	Anneau des entiers relatifs
$\mathbb{Q}$	Corps des nombres rationnels
$\mathbb{R}$	Corps des nombres réels
$\mathbb{C}$	Corps des nombres complexes
$\mathbb{F}_q$	Corps fini à q éléments
$\mathbb{Z}/n\mathbb{Z}$	Anneau (ou groupe) des entiers modulo n
$(\mathbb{Z}/n\mathbb{Z})^\times$	Groupe des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$
$\lvert G\rvert$	Ordre (cardinal) du groupe G
$\mathrm{ord}(g)$	Ordre de l'élément g dans un groupe
$\langle g\rangle$	Sous-groupe engendré par g
$\langle S\rangle$	Sous-groupe engendré par le sous-ensemble S
$H \leq G$	H est un sous-groupe de G
$H \trianglelefteq G$	H est un sous-groupe distingué de G
$[G : H]$	Indice de H dans G
G/N	Groupe quotient de G par N
$G \times H$	Produit direct de G et H
$G \simeq H$	G est isomorphe à H
$\mathrm{GL}_n(K)$	Groupe linéaire général d'ordre n sur K
$\mathrm{SL}_n(K)$	Groupe spécial linéaire d'ordre n sur K
S_n	Groupe symétrique sur n éléments
A_n	Groupe alterné sur n éléments
D_n	Groupe diédral d'ordre $2n$
Q_8	Groupe des quaternions
V_4	Groupe de Klein à quatre éléments
$Z(G)$	Centre du groupe G
$[G, G]$	Sous-groupe dérivé (des commutateurs) de G
$\mathrm{Aut}(G)$	Groupe des automorphismes de G
$\mathrm{Inn}(G)$	Groupe des automorphismes intérieurs de G
$\mathrm{Hom}(G, H)$	Ensemble des homomorphismes de G dans H
$\mathrm{Ker}(f)$	Noyau de l'homomorphisme f
$\mathrm{Im}(f)$	Image de l'homomorphisme f
Id	Application identité
$\mathrm{car}(A)$	Caractéristique de l'anneau A
$\mathrm{pgcd}(a, b)$	Plus grand commun diviseur
$\mathrm{ppcm}(a, b)$	Plus petit commun multiple

Chapitre 1

Groupes : définitions, exemples et premières propriétés

1.1 Introduction historique

La notion de *groupe* est l'une des plus fécondes de l'ensemble des mathématiques. Elle naît de l'observation que de nombreux objets mathématiques possèdent des *symétries*, et que l'ensemble de ces symétries, muni de la composition, obéit à des lois algébriques remarquablement simples et universelles.

Historiquement, les groupes apparaissent sous trois formes :

(a) **Les groupes de permutations.** Lagrange (1770) étudia les permutations des racines d'un polynôme ; Cauchy (1815, 1844) systématisa la théorie des substitutions ; Cayley (1854) montra que tout groupe (abstrait) est isomorphe à un sous-groupe d'un groupe de permutations (théorème de Cayley).

(b) **Les groupes de symétries géométriques.** Les symétries d'un polygone régulier forment un *groupe diédral* ; celles d'un polyèdre régulier, un sous-groupe de $\mathrm{GL}_3(\mathbb{R})$. Klein (1872), dans son *Programme d'Erlangen*, proposa de *définir* une géométrie par son groupe de transformations.

(c) **Les groupes de nombres.** L'ensemble $\mathbb{Z}$ muni de l'addition, le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$, le groupe multiplicatif $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$: autant d'exemples issus de l'arithmétique et de l'analyse.

L'abstraction consiste à dégager les propriétés communes à tous ces exemples et à les prendre comme *axiomes*.

1.2 Loi de composition interne

Définition 1.1 (Loi de composition interne)**.** Soit E un ensemble non vide. Une *loi de composition interne* (ou *opération binaire interne*) sur E est une application

$$\star : E \times E \longrightarrow E, \qquad (a, b) \longmapsto a \star b.$$

Remarque 1.1. La condition essentielle est que $a \star b \in E$ pour tous $a, b \in E$: on dit que E est *stable* (ou *fermé*) pour $\star$.

Exemple 1.1 (Exemples de lois de composition interne)**.** (i) L'addition $+$ et la multiplication $\times$ sont des lois de composition internes sur $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

(ii) La soustraction $-$ est une loi de composition interne sur $\mathbb{Z}$, mais *pas* sur $\mathbb{N}$ (car $2-5=-3\notin\mathbb{N}$).

(iii) La composition des applications $\circ$ est une loi de composition interne sur l'ensemble des bijections d'un ensemble E dans lui-même.

(iv) La multiplication matricielle est une loi de composition interne sur $M_n(K)$, l'ensemble des matrices carrées d'ordre n à coefficients dans un corps K.

1.3 Définition d'un groupe

Définition 1.2 (Groupe)**.** Un *groupe* est un couple $(G,\star)$ où G est un ensemble non vide et $\star$ est une loi de composition interne sur G vérifiant les axiomes suivants :

(G1) Associativité. Pour tous $a,b,c\in G$:

$$(a\star b)\star c=a\star(b\star c).$$

(G2) Élément neutre. Il existe un élément $e\in G$ tel que, pour tout $a\in G$:

$$e\star a=a\star e=a.$$

(G3) Symétrique. Pour tout $a\in G$, il existe un élément $a'\in G$ tel que :

$$a\star a'=a'\star a=e.$$

On note usuellement $a'=a^{-1}$ (notation multiplicative) ou $a'=-a$ (notation additive).

Remarque 1.2. Certains auteurs incluent explicitement la stabilité (le fait que $\star$ soit une loi de composition interne sur G) comme axiome **(G0)**, ce qui donne quatre axiomes. Dans notre formulation, la stabilité fait partie de la définition de ń loi de composition interne ż.

1.4 Premières propriétés

Théorème 1.1 (Unicité de l'élément neutre)**.** Soit $(G,\star)$ un groupe. L'élément neutre est unique.

Démonstration. Supposons que e et e' soient deux éléments neutres de G. Alors :

$$e=e\star e'=e',$$

la première égalité provenant du fait que e' est neutre (donc $e\star e'=e$) et la seconde du fait que e est neutre (donc $e\star e'=e'$). Ainsi $e=e'$. □

Théorème 1.2 (Unicité de l'inverse)**.** Soit $(G, \star)$ un groupe et $a \in G$. L'inverse de a est unique.

Démonstration. Supposons que b et c soient deux inverses de a, c'est-à-dire $a \star b = b \star a = e$ et $a \star c = c \star a = e$. Alors :

$$b = b \star e = b \star (a \star c) = (b \star a) \star c = e \star c = c.$$

Donc $b = c$. □

Théorème 1.3 (Inverse d'un produit)**.** Soit $(G, \star)$ un groupe et $a, b \in G$. Alors :

$$(a \star b)^{-1} = b^{-1} \star a^{-1}.$$

Démonstration. Il suffit de vérifier que $b^{-1} \star a^{-1}$ satisfait la définition de l'inverse de $a \star b$. On calcule :

$$(a \star b) \star (b^{-1} \star a^{-1}) = a \star (b \star b^{-1}) \star a^{-1} = a \star e \star a^{-1} = a \star a^{-1} = e.$$

De même :

$$(b^{-1} \star a^{-1}) \star (a \star b) = b^{-1} \star (a^{-1} \star a) \star b = b^{-1} \star e \star b = b^{-1} \star b = e.$$

Par unicité de l'inverse (théorème 1.2), on conclut $(a \star b)^{-1} = b^{-1} \star a^{-1}$. □

Proposition 1.1 (Régularité)**.** Soit $(G, \star)$ un groupe et $a, b, c \in G$.

(i) Si $a \star b = a \star c$, alors $b = c$ (régularité à gauche).

(ii) Si $b \star a = c \star a$, alors $b = c$ (régularité à droite).

Démonstration. (i) Si $a \star b = a \star c$, on compose à gauche par a^{-1} :

$$a^{-1} \star (a \star b) = a^{-1} \star (a \star c) \implies (a^{-1} \star a) \star b = (a^{-1} \star a) \star c \implies e \star b = e \star c \implies b = c.$$

La preuve de (ii) est analogue, en composant à droite par a^{-1}. □

Proposition 1.2 (Involutivité de l'inversion)**.** Soit $(G, \star)$ un groupe et $a \in G$. Alors $(a^{-1})^{-1} = a$.

Démonstration. Par définition, $a^{-1} \star a = a \star a^{-1} = e$. Cela signifie que a est un inverse de a^{-1}. Par unicité de l'inverse, $(a^{-1})^{-1} = a$. □

1.5 Groupes abéliens

Définition 1.3 (Groupe abélien)**.** Un groupe $(G, \star)$ est dit *abélien* (ou *commutatif*) si, pour tous $a, b \in G$:

$$a \star b = b \star a.$$

Remarque 1.3. Le nom ń abélien ż est un hommage à Niels Henrik Abel. Par convention, les groupes abéliens sont souvent notés additivement $(G, +)$, l'élément neutre étant noté 0 et l'inverse de a étant noté $-a$.

1.6 Exemples fondamentaux

Exemple 1.2 (Le groupe $(\mathbb{Z}, +)$)**.** L'ensemble $\mathbb{Z}$ des entiers relatifs, muni de l'addition, est un groupe abélien. L'élément neutre est 0 ; l'inverse de $n \in \mathbb{Z}$ est $-n$.

Exemple 1.3 (Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$)**.** Pour tout entier $n \geq 1$, l'ensemble $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ muni de l'addition modulo n est un groupe abélien fini d'ordre n. L'élément neutre est $\bar{0}$; l'inverse de $\bar{k}$ est $\overline{n-k}$.

Exemple 1.4 (Le groupe $(\mathbb{R}^*, \times)$)**.** L'ensemble $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ muni de la multiplication est un groupe abélien. L'élément neutre est 1 ; l'inverse de a est $1/a$. On note que $\mathbb{R}$ tout entier ne forme *pas* un groupe pour la multiplication, car 0 n'a pas d'inverse.

Exemple 1.5 (Le groupe linéaire $\mathrm{GL}_n(\mathbb{R})$)**.** L'ensemble $\mathrm{GL}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det(A) \neq 0\}$ des matrices inversibles d'ordre n, muni du produit matriciel, est un groupe. L'élément neutre est la matrice identité I_n ; l'inverse de A est la matrice inverse A^{-1}. Ce groupe est **non abélien** dès que $n \geq 2$.

Exemple 1.6 (Le groupe spécial linéaire $\mathrm{SL}_n(\mathbb{R})$)**.** L'ensemble $\mathrm{SL}_n(\mathbb{R}) = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid \det(A) = 1\}$ est un groupe pour le produit matriciel. En effet, si $\det(A) = \det(B) = 1$, alors $\det(AB) = \det(A)\det(B) = 1$ et $\det(A^{-1}) = 1/\det(A) = 1$.

Exemple 1.7 (Le groupe symétrique S_n)**.** Soit $E = \{1, 2, \ldots, n\}$. L'ensemble S_n de toutes les bijections de E dans E (appelées *permutations*) muni de la composition est un groupe d'ordre $n!$. L'élément neutre est l'identité Id_E ; l'inverse d'une permutation σ est la permutation réciproque σ^{-1}. Le groupe S_n est non abélien dès que $n \geq 3$.

Exemple 1.8 (Le groupe diédral D_n)**.** Le *groupe diédral* D_n est le groupe des isométries du plan qui préservent un polygone régulier à n côtés. Il contient n rotations (d'angles $2k\pi/n$, pour $k = 0, 1, \ldots, n-1$) et n réflexions, soit $2n$ éléments au total. On écrit :

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

où r désigne la rotation d'angle $2\pi/n$ et s une réflexion. Le groupe D_n est non abélien pour $n \geq 3$.

Exemple 1.9 (Le groupe des quaternions Q_8)**.** Le *groupe des quaternions* est le groupe d'ordre 8 :

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$$

avec les relations $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$, $ji = -k$, $kj = -i$,

$ik = -j$. C'est un groupe non abélien. Il fournit un exemple important d'un groupe dont tous les sous-groupes sont distingués (on dit que Q_8 est un groupe *hamiltonien*).

Exemple 1.10 (Le groupe de Klein V_4)**.** Le *groupe de Klein* (ou *Vierergruppe*) est le groupe abélien d'ordre 4 :

$$V_4 = \{e, a, b, c\} \quad \text{avec} \quad a^2 = b^2 = c^2 = e, \quad ab = c, \quad bc = a, \quad ac = b.$$

On peut le réaliser comme $V_4 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, ou comme le sous-groupe $\{\mathrm{Id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ de S_4.

1.7 Groupes cycliques

Définition 1.4 (Groupe monogène, groupe cyclique)**.** Un groupe G est dit *monogène* s'il existe un élément $g \in G$ tel que $G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$. Un groupe monogène fini est appelé *cyclique*. Par abus courant, on qualifie aussi de cyclique tout groupe monogène (fini ou infini). L'élément g est appelé un *générateur* de G.

Exemple 1.11.
(i) $(\mathbb{Z}, +)$ est un groupe cyclique (infini) engendré par 1 (ou par -1).
(ii) $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique d'ordre n, engendré par $\bar{1}$.
(iii) Le groupe des racines n-ièmes de l'unité $\mu_n = \{e^{2ik\pi/n} \mid k = 0, \ldots, n-1\} \subset \mathbb{C}^*$ est un groupe cyclique d'ordre n, engendré par $e^{2i\pi/n}$.

Théorème 1.4 (Classification des groupes cycliques)**.** Tout groupe cyclique est isomorphe soit à $\mathbb{Z}$ (s'il est infini), soit à $\mathbb{Z}/n\mathbb{Z}$ pour un certain $n \geq 1$ (s'il est fini d'ordre n).

Démonstration. Soit $G = \langle g \rangle$ un groupe cyclique et considérons l'application

$$\varphi : \mathbb{Z} \longrightarrow G, \qquad n \longmapsto g^n.$$

C'est un homomorphisme de groupes : $\varphi(m+n) = g^{m+n} = g^m \cdot g^n = \varphi(m) \cdot \varphi(n)$. De plus, φ est surjective puisque $G = \langle g \rangle$.

Posons $K = \mathrm{Ker}(\varphi) = \{n \in \mathbb{Z} \mid g^n = e\}$. C'est un sous-groupe de $\mathbb{Z}$. Or, tout sous-groupe de $\mathbb{Z}$ est de la forme $d\mathbb{Z}$ pour un certain $d \geq 0$ (cf. exercice 1.1).

Cas 1 : $K = \{0\}$, c'est-à-dire $d = 0$. Alors φ est injective, donc bijective, et $G \simeq \mathbb{Z}$.

Cas 2 : $K = d\mathbb{Z}$ avec $d \geq 1$. Par le théorème d'isomorphisme (que nous admettrons ici et démontrerons au chapitre 3), on a :

$$G \simeq \mathbb{Z}/K = \mathbb{Z}/d\mathbb{Z}.$$

De plus, $|G| = |\mathbb{Z}/d\mathbb{Z}| = d$, donc $d = n$ si G est d'ordre n. Ainsi $G \simeq \mathbb{Z}/n\mathbb{Z}$. □

1.8 Ordre d'un élément

Définition 1.5 (Ordre d'un élément)**.** Soit $(G, \cdot)$ un groupe et $g \in G$. L'*ordre* de g, noté $\mathrm{ord}(g)$, est le plus petit entier $n \geq 1$ tel que $g^n = e$, s'il existe. Si aucun tel entier n'existe, on dit que g est d'*ordre infini* et on pose $\mathrm{ord}(g) = +\infty$.

Définition 1.6 (Ordre d'un groupe)**.** L'*ordre* d'un groupe G, noté $|G|$, est le cardinal de G.

Proposition 1.3. Soit G un groupe et $g \in G$. Alors $\mathrm{ord}(g) = |\langle g \rangle|$.

Démonstration. Si $\mathrm{ord}(g) = +\infty$, les éléments g^k $(k \in \mathbb{Z})$ sont tous distincts (sinon $g^{k-l} = e$ pour $k \neq l$, contredisant l'hypothèse), donc $\langle g \rangle$ est infini.

Si $\mathrm{ord}(g) = n < +\infty$, montrons que $\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$, ce qui donnera $|\langle g \rangle| = n$. Tout élément de $\langle g \rangle$ s'écrit g^k pour un certain $k \in \mathbb{Z}$. Par division euclidienne, $k = nq + r$ avec $0 \leq r < n$, d'où $g^k = g^{nq+r} = (g^n)^q \cdot g^r = e^q \cdot g^r = g^r$. Donc $\langle g \rangle \subseteq \{e, g, \ldots, g^{n-1}\}$. De plus, ces n éléments sont distincts : si $g^i = g^j$ avec $0 \leq i < j < n$, alors $g^{j-i} = e$ avec $0 < j - i < n$, contredisant la minimalité de n. □

Proposition 1.4. Soit $g \in G$ un élément d'ordre fini n. Alors $g^k = e$ si et seulement si $n \mid k$.

Démonstration. Si $n \mid k$, alors $k = nq$ et $g^k = (g^n)^q = e^q = e$. Réciproquement, si $g^k = e$, écrivons $k = nq + r$ avec $0 \leq r < n$. Alors $g^r = g^{k-nq} = g^k \cdot (g^n)^{-q} = e \cdot e = e$. Par minimalité de n, on a $r = 0$, donc $n \mid k$. □

1.9 Tables de Cayley

La *table de Cayley* d'un groupe fini $G = \{g_1, \ldots, g_n\}$ est le tableau dont l'entrée à la ligne i et à la colonne j est le produit $g_i \star g_j$.

Exemple 1.12 (Table de Cayley de $\mathbb{Z}/4\mathbb{Z}$)**.**

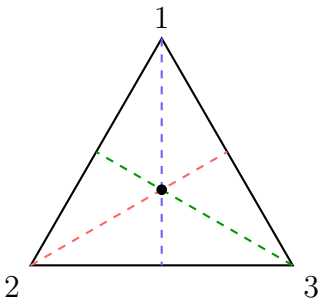
$+$	$\overline{0.7}$	$\overline{0.7}$	$\overline{0.7}$	$\overline{0.7}$
$\overline{0.0}$	$\overline{0.0}$	$\overline{0.0}$	$\overline{0.0}$	$\overline{0.0}$
-1.0	1.0	-1.0	-1.0	-1.0
-2.0	2.0	-2.0	-2.0	-2.0
-3.0	3.0	-3.0	-3.0	-3.0

·	0.7	0.7	0.7	0.7
0.0	0.0	0.0	0.0	0.0
−1.0	1.0	−1.0	−1.0	−1.0
−2.0	2.0	−2.0	−2.0	−2.0
−3.0	3.0	−3.0	−3.0	−3.0

Exemple 1.13 (Table de Cayley du groupe de Klein V_4).

1.10 Symétries des polygones

1.10.1 Symétries du triangle — le groupe D_3



r : rotation de 120

s : réflexion

$D_3 = \{e, r, r^2, s, sr, sr^2\}$

$|D_3| = 6$

Les éléments de D_3 sont :

— $e = \mathrm{Id}$: l'identité,

— r : rotation de $2\pi/3$ (sens trigonométrique),

— r^2 : rotation de $4\pi/3$,

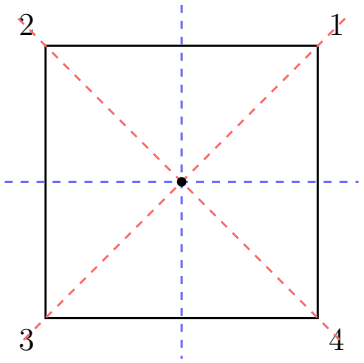
— s : réflexion par rapport à l'axe passant par le sommet 1,

— sr : réflexion par rapport à l'axe passant par le sommet 3,

— sr^2 : réflexion par rapport à l'axe passant par le sommet 2.

Les relations fondamentales sont $r^3 = e$, $s^2 = e$ et $srs = r^{-1}$ (c'est-à-dire $sr = r^{-1}s = r^2 s$). On remarque que $D_3 \simeq S_3$ (puisque le groupe a 6 éléments et opère fidèlement sur les trois sommets).

1.10.2 Symétries du carré — le groupe D_4



r : rotation de 90

4 rotations : e, r, r^2, r^3

4 réflexions : s, sr, sr^2, sr^3

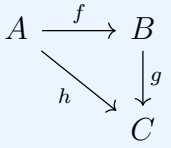
$|D_4| = 8$

Le groupe $D_4 = \langle r, s \mid r^4 = s^2 = e,\ srs = r^{-1} \rangle$ est d'ordre 8. Il est non abélien et possède une structure remarquablement riche pour un groupe si petit : il a 10 sous-groupes, dont 3 sont distingués.

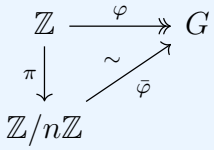
1.11 Diagrammes commutatifs

Les *diagrammes commutatifs* constituent un outil fondamental en algèbre. Un diagramme d'ensembles (ou de groupes) et d'applications (ou d'homomorphismes) est dit *commutatif* si, pour tout couple de chemins reliant deux mêmes sommets, les applications composées correspondantes sont égales.

Exemple 1.14. Le diagramme suivant exprime que $h = g \circ f$:



Exemple 1.15. Le diagramme commutatif suivant résume la situation de la classification des groupes cycliques. Si $G = \langle g \rangle$ est cyclique d'ordre n, alors :



où $\varphi(k) = g^k$, π est la projection canonique, et $\bar{\varphi}$ est l'isomorphisme induit.

1.12 Produit direct de groupes

Définition 1.7 (Produit direct)**.** Soient $(G, \cdot_G)$ et $(H, \cdot_H)$ deux groupes. Le *produit direct* $G \times H$ est l'ensemble $\{(g, h) \mid g \in G,\ h \in H\}$ muni de la loi :

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \cdot_G g_2,\ h_1 \cdot_H h_2).$$

Proposition 1.5. Le produit direct $G \times H$ est un groupe, d'élément neutre (e_G, e_H) et d'inverses $(g, h)^{-1} = (g^{-1}, h^{-1})$. Si G et H sont finis, alors $|G \times H| = |G| \cdot |H|$.

Démonstration. L'associativité découle composante par composante de celle de G et de H. On vérifie immédiatement que (e_G, e_H) est neutre et que (g^{-1}, h^{-1}) est l'inverse de (g, h). Enfin, $|G \times H| = |G| \cdot |H|$ résulte du principe de dénombrement des paires. □

Remarque 1.4. La construction se généralise à un nombre fini quelconque de facteurs : $G_1 \times G_2 \times \cdots \times G_k$.

Exemple 1.16. (i) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq V_4$ (groupe de Klein).

(ii) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z}$ (car $\gcd(2,3) = 1$).

(iii) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \not\simeq \mathbb{Z}/4\mathbb{Z}$ (le premier n'a aucun élément d'ordre 4).

1.13 Exercices

Exercice 1.1 (Sous-groupes de $\mathbb{Z}$)**.** Montrer que tout sous-groupe de $(\mathbb{Z}, +)$ est de la forme $n\mathbb{Z}$ pour un certain $n \in \mathbb{N}$. [*Indication : considérer le plus petit élément strictement positif, s'il existe.*]

Exercice 1.2 (Ordre dans $\mathbb{Z}/n\mathbb{Z}$)**.** Soit $n \geq 1$ et $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$. Montrer que $\mathrm{ord}(\bar{k}) = n/\gcd(k,n)$. En déduire que $\bar{k}$ engendre $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $\gcd(k,n) = 1$.

Exercice 1.3 (Groupe d'ordre 2)**.** Soit G un groupe tel que $g^2 = e$ pour tout $g \in G$. Montrer que G est abélien.

Exercice 1.4 (Centre de $\mathrm{GL}_n(\mathbb{R})$)**.** Montrer que $Z(\mathrm{GL}_n(\mathbb{R})) = \{\lambda I_n \mid \lambda \in \mathbb{R}^*\}$, l'ensemble des matrices scalaires inversibles.

Exercice 1.5 (Le groupe S_3)**.** Écrire les 6 éléments de S_3 en notation cyclique. Calculer la table de Cayley de S_3. Identifier tous les sous-groupes de S_3 et dessiner le diagramme de Hasse correspondant.

Exercice 1.6 (Groupe des quaternions)**.** Écrire la table de Cayley complète de Q_8. Déterminer le centre $Z(Q_8)$ et l'ordre de chaque élément.

Exercice 1.7 (Produit direct et cyclicité)**.** Soient $m, n \geq 1$. Montrer que $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est cyclique si et seulement si $\gcd(m,n) = 1$. [*Indication : considérer l'ordre de* $(\bar{1}, \bar{1})$.]

Exercice 1.8 (Groupe diédral D_n)**.** Soit $n \geq 3$.

(a) Montrer que $D_n = \{e, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$ et que $|D_n| = 2n$.

(b) Montrer que $r^k s = sr^{-k}$ pour tout $k \in \mathbb{Z}$.

(c) Déterminer le centre $Z(D_n)$.

(d) Montrer que D_n est isomorphe à un sous-groupe de S_n.

Exercice 1.9 (Sous-groupe engendré)**.** Soit G un groupe et $S \subseteq G$ une partie non vide. Montrer que le sous-groupe engendré par S est :

$$\langle S \rangle = \bigcap_{\substack{H \leq G \\ S \subseteq H}} H = \{s_1^{\varepsilon_1} s_2^{\varepsilon_2} \cdots s_k^{\varepsilon_k} \mid k \geq 0,\ s_i \in S,\ \varepsilon_i \in \{-1, 1\}\}.$$

Exercice 1.10 (Automorphismes de $\mathbb{Z}/n\mathbb{Z}$)**.** Montrer que $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$. En déduire que $|\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})| = \varphi(n)$, où φ désigne la fonction indicatrice d'Euler.

Exercice 1.11 (Application : petit théorème de Fermat *(difficile)*)**.** Soit p un nombre premier et $a \in \mathbb{Z}$ tel que $p \nmid a$.

(a) Montrer que $(\mathbb{Z}/p\mathbb{Z})^\times$ est un groupe d'ordre $p-1$.

(b) En utilisant le théorème de Lagrange (chapitre 2), montrer que $a^{p-1} \equiv 1 \pmod{p}$.

(c) En déduire que $a^p \equiv a \pmod{p}$ pour tout $a \in \mathbb{Z}$.

Exercice 1.12 (Commutateur)**.** Soient G un groupe et $a, b \in G$. Le *commutateur* de a et b est $[a,b] = aba^{-1}b^{-1}$.

(a) Montrer que $ab = ba[a,b]^{-1}$... Non : montrer que $ab = ba \cdot [a,b]$ si et seulement si $[a,b] = e$, c'est-à-dire si et seulement si a et b commutent.

(b) Montrer que $[a,b]^{-1} = [b,a]$.

(c) Calculer quelques commutateurs dans S_3 et dans D_4.

Résumé du chapitre 1. Un *groupe* $(G, \star)$ est un ensemble muni d'une loi associative possédant un élément neutre et des inverses. Les exemples fondamentaux comprennent $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{R}^*$, GL_n, S_n, D_n, Q_8, V_4. Tout groupe cyclique est isomorphe à $\mathbb{Z}$ ou à $\mathbb{Z}/n\mathbb{Z}$. L'ordre d'un élément g est le cardinal du sous-groupe $\langle g \rangle$. Le produit direct $G \times H$ est un groupe d'ordre $|G| \cdot |H|$.

Chapitre 2

Sous-groupes, sous-groupes distingués et quotients

2.1 Introduction

L'étude d'un groupe G passe de manière essentielle par celle de ses *sous-groupes*. Tout comme un espace vectoriel est analysé à travers ses sous-espaces, un groupe est compris à travers ses sous-groupes et les relations qu'ils entretiennent entre eux. Le théorème central de ce chapitre — le théorème de Lagrange — relie l'ordre d'un sous-groupe à l'ordre du groupe ambiant et constitue l'un des résultats les plus fondamentaux de toute la théorie des groupes.

Le passage au quotient, qui nécessite la notion de sous-groupe *distingué*, fournit un mécanisme de construction de nouveaux groupes à partir d'anciens, et se révèle indispensable pour la compréhension structurelle des groupes.

2.2 Sous-groupes

Définition 2.1 (Sous-groupe)**.** Soit $(G, \cdot)$ un groupe. Un sous-ensemble $H \subseteq G$ est un *sous-groupe* de G si $(H, \cdot)$ est lui-même un groupe (pour la loi induite). On note $H \leq G$.

Théorème 2.1 (Critère de sous-groupe — forme condensée)**.** Soit G un groupe et $H \subseteq G$ une partie non vide. Les conditions suivantes sont équivalentes :

(i) H est un sous-groupe de G.

(ii) Pour tous $a, b \in H$, on a $ab^{-1} \in H$.

(iii) H est non vide, et pour tous $a, b \in H$, on a $ab \in H$ et $a^{-1} \in H$.

Démonstration. **(i) $\Rightarrow$ (ii).** Si $H \leq G$ et $a, b \in H$, alors $b^{-1} \in H$ (car H est un groupe) et $ab^{-1} \in H$ (par stabilité).

(ii) $\Rightarrow$ (iii). Supposons (ii). Puisque $H \neq \varnothing$, prenons un élément $a \in H$. Alors $e = aa^{-1} \in H$ (en prenant $b = a$). Pour tout $b \in H$, on a $b^{-1} = eb^{-1} \in H$ (en prenant $a = e$). Enfin, pour $a, b \in H$, comme $b^{-1} \in H$, on obtient $ab = a(b^{-1})^{-1} \in H$ (en appliquant (ii) avec a et b^{-1}).

(iii) ⇒ (i). Si (iii) est vérifiée, alors H est stable par la loi de G et par passage à l'inverse. L'associativité est héritée de G. L'existence de l'élément neutre : pour $a \in H$, on a $a^{-1} \in H$ puis $e = a \cdot a^{-1} \in H$. Donc $(H, \cdot)$ est un groupe. □

Remarque 2.1 (Sous-groupes triviaux)**.** Tout groupe G possède au moins deux sous-groupes : le sous-groupe *trivial* $\{e\}$ et G lui-même. Un sous-groupe H tel que $\{e\} \subsetneq H \subsetneq G$ est dit *propre*.

Corollaire 2.1 (Critère de sous-groupe fini)**.** Si G est un groupe et $H \subseteq G$ est une partie **finie** et non vide, stable par la loi de G (c'est-à-dire $ab \in H$ pour tous $a, b \in H$), alors H est un sous-groupe de G.

Démonstration. Il suffit de vérifier que H contient les inverses. Soit $a \in H$. Si $a = e$, alors $a^{-1} = e \in H$. Sinon, considérons les éléments $a, a^2, a^3, \ldots$ Par stabilité, tous ces éléments appartiennent à H. Puisque H est fini, il existe $i < j$ tels que $a^i = a^j$, d'où $a^{j-i} = e$ par régularité. Posons $n = j - i \geq 1$. Alors $a^{-1} = a^{n-1} \in H$ (car $n - 1 \geq 0$ et $a^0 = e \in H$, $a^k \in H$ par stabilité). □

2.3 Exemples de sous-groupes

Exemple 2.1 (Sous-groupes de $(\mathbb{Z}, +)$)**.** Les sous-groupes de $(\mathbb{Z}, +)$ sont exactement les ensembles $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ pour $n \in \mathbb{N}$ (cf. exercice 1.1). En particulier, tout sous-groupe de $\mathbb{Z}$ est cyclique.

Exemple 2.2 (SL_n dans GL_n)**.** Le groupe spécial linéaire $\mathrm{SL}_n(K)$ est un sous-groupe de $\mathrm{GL}_n(K)$: il est non vide ($I_n \in \mathrm{SL}_n(K)$), et pour $A, B \in \mathrm{SL}_n(K)$, on a $\det(AB^{-1}) = \det(A)/\det(B) = 1/1 = 1$, donc $AB^{-1} \in \mathrm{SL}_n(K)$.

Exemple 2.3 (A_n dans S_n)**.** Le *groupe alterné* A_n est l'ensemble des permutations paires de S_n, c'est-à-dire les permutations pouvant s'écrire comme produit d'un nombre pair de transpositions. C'est un sous-groupe de S_n d'ordre $n!/2$ (pour $n \geq 2$).

Exemple 2.4 (Intersection de sous-groupes)**.** Si $(H_i)_{i \in I}$ est une famille de sous-groupes de G, alors $\bigcap_{i \in I} H_i$ est un sous-groupe de G. En effet, l'intersection est non vide (elle contient e) et, pour $a, b \in \bigcap H_i$, on a $ab^{-1} \in H_i$ pour tout i (car chaque H_i est un sous-groupe), donc $ab^{-1} \in \bigcap H_i$.

Remarque 2.2. La *réunion* de deux sous-groupes n'est en général *pas* un sous-groupe. Par exemple, $2\mathbb{Z} \cup 3\mathbb{Z}$ n'est pas un sous-groupe de $\mathbb{Z}$ (car $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$).

2.4 Théorème de Lagrange

Le théorème de Lagrange est l'un des résultats les plus importants de la théorie des groupes finis. Sa démonstration repose sur la notion de *classe latérale*.

Définition 2.2 (Classes latérales)**.** Soient G un groupe et $H \leq G$. Pour $g \in G$, on définit :

- la *classe latérale à gauche* de g modulo H : $gH = \{gh \mid h \in H\}$,
- la *classe latérale à droite* de g modulo H : $Hg = \{hg \mid h \in H\}$.

Lemme 2.1. Soient G un groupe et $H \leq G$. Pour tous $a, b \in G$:

(i) $aH = bH$ si et seulement si $b^{-1}a \in H$.

(ii) Les classes latérales à gauche forment une partition de G.

(iii) Toutes les classes latérales à gauche ont le même cardinal : $|aH| = |H|$.

Démonstration. **(i)** On a $aH = bH$ si et seulement si $a \in bH$ (car $a = ae \in aH$), ce qui équivaut à l'existence de $h \in H$ tel que $a = bh$, soit $b^{-1}a = h \in H$.

(ii) Définissons la relation $\sim$ sur G par $a \sim b \Leftrightarrow aH = bH$, c'est-à-dire $b^{-1}a \in H$ d'après (i). Montrons que $\sim$ est une relation d'équivalence :

- *Réflexivité :* $a^{-1}a = e \in H$.
- *Symétrie :* si $b^{-1}a \in H$, alors $a^{-1}b = (b^{-1}a)^{-1} \in H$.
- *Transitivité :* si $b^{-1}a \in H$ et $c^{-1}b \in H$, alors $c^{-1}a = (c^{-1}b)(b^{-1}a) \in H$.

Les classes latérales à gauche sont les classes d'équivalence de $\sim$, elles forment donc une partition de G.

(iii) L'application $\psi : H \to aH$ définie par $\psi(h) = ah$ est bijective. En effet, elle est surjective par définition de aH, et injective car $ah_1 = ah_2$ implique $h_1 = h_2$ (régularité à gauche). Donc $|aH| = |H|$. □

Définition 2.3 (Indice)**.** L'*indice* de H dans G, noté $[G : H]$, est le nombre de classes latérales à gauche de H dans G :

$$[G : H] = |G/H| \quad \text{(ici, } G/H \text{ désigne l'ensemble des classes } gH\text{)}.$$

Théorème 2.2 (Théorème de Lagrange)**.** Soit G un groupe fini et $H \leq G$. Alors :

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

En particulier, $|H|$ divise $|G|$.

Démonstration. Par le lemme 2.1, les classes latérales à gauche $g_1H, g_2H, \ldots, g_kH$ (où $k = [G : H]$) forment une partition de G en k parties disjointes, chacune de cardinal $|H|$. Par conséquent :

$$|G| = \sum_{i=1}^{k} |g_iH| = \sum_{i=1}^{k} |H| = k \cdot |H| = [G : H] \cdot |H|.$$ □

Corollaire 2.2 (L'ordre d'un élément divise l'ordre du groupe)**.** Soit G un groupe fini et $g \in G$. Alors $\mathrm{ord}(g)$ divise $|G|$. En particulier, $g^{|G|} = e$.

Démonstration. On a $\text{ord}(g) = |\langle g \rangle|$ (proposition 1.3) et $\langle g \rangle \leq G$. Par le théorème de Lagrange, $|\langle g \rangle|$ divise $|G|$. Donc $\text{ord}(g)$ divise $|G|$. De plus, $|G| = \text{ord}(g) \cdot q$ pour un certain q, d'où $g^{|G|} = (g^{\text{ord}(g)})^q = e^q = e$. □

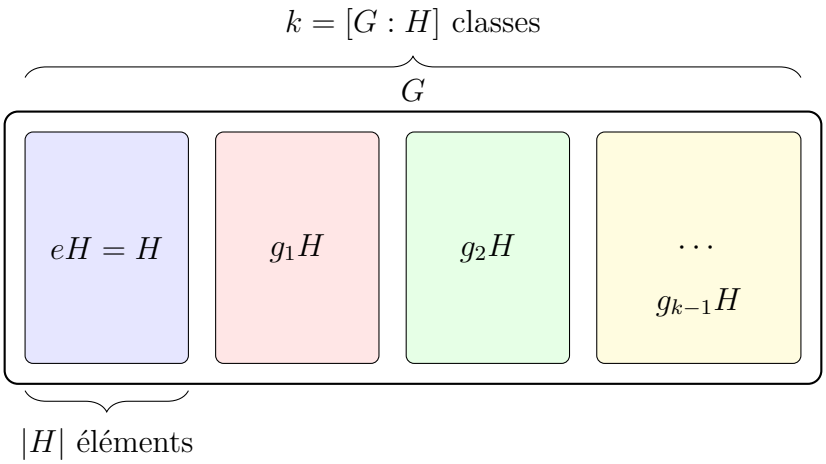
Corollaire 2.3 (Groupes d'ordre premier)**.** Si G est un groupe d'ordre premier p, alors G est cyclique, isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Démonstration. Puisque $|G| = p > 1$, il existe $g \in G$ avec $g \neq e$. Alors $\text{ord}(g) > 1$ et $\text{ord}(g)$ divise p (corollaire 2.2). Comme p est premier, $\text{ord}(g) = p = |G|$. Donc $\langle g \rangle = G$: le groupe G est cyclique d'ordre p, isomorphe à $\mathbb{Z}/p\mathbb{Z}$ par le théorème 1.4. □

Remarque 2.3 (Réciproque fausse)**.** La réciproque du théorème de Lagrange est fausse : si d divise $|G|$, il n'existe pas nécessairement de sous-groupe d'ordre d. Par exemple, A_4 (d'ordre 12) ne possède pas de sous-groupe d'ordre 6.

2.5 Classes latérales : visualisation

La partition de G en classes latérales de H se visualise comme suit :



On a donc $|G| = k \cdot |H|$, la formule du théorème de Lagrange.

2.6 Sous-groupes distingués

Définition 2.4 (Sous-groupe distingué)**.** Un sous-groupe N de G est dit *distingué* (ou *normal*, ou *invariant*) dans G, et on note $N \trianglelefteq G$, si pour tout $g \in G$:

$$gNg^{-1} = N,$$

c'est-à-dire $gNg^{-1} \subseteq N$ (ce qui suffit, voir ci-dessous).

Théorème 2.3 (Caractérisations des sous-groupes distingués)**.** Soit G un groupe et $N \leq G$. Les conditions suivantes sont équivalentes :

(i) $N \trianglelefteq G$.

(ii) Pour tout $g \in G$, $gNg^{-1} \subseteq N$.

(iii) Pour tout $g \in G$, $gN = Ng$ (les classes à gauche et à droite coïncident).

(iv) Pour tout $g \in G$ et tout $n \in N$, on a $gng^{-1} \in N$.

Démonstration. **(i) ⇔ (ii).** L'implication (i) ⇒ (ii) est triviale. Pour la réciproque, supposons $gNg^{-1} \subseteq N$ pour tout g. En appliquant cela à g^{-1}, on obtient $g^{-1}Ng \subseteq N$, soit $N \subseteq gNg^{-1}$. D'où $gNg^{-1} = N$.

(i) ⇔ (iii). On a $gN = Ng$ si et seulement si $gNg^{-1} = N$ (en multipliant à droite par g^{-1}, respectivement par g).

(ii) ⇔ (iv). La condition $gNg^{-1} \subseteq N$ signifie exactement que pour tout $n \in N$, $gng^{-1} \in N$. □

Remarque 2.4. Si G est abélien, alors *tout* sous-groupe de G est distingué, car $gng^{-1} = n \in N$ pour tout $g \in G$ et $n \in N$.

Exemple 2.5 (Sous-groupes distingués)**.** (i) $\{e\}$ et G sont toujours distingués dans G.

(ii) $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ (puisque $\mathbb{Z}$ est abélien).

(iii) $\mathrm{SL}_n(K) \trianglelefteq \mathrm{GL}_n(K)$, car pour $A \in \mathrm{GL}_n(K)$ et $M \in \mathrm{SL}_n(K)$, $\det(AMA^{-1}) = \det(M) = 1$.

(iv) $A_n \trianglelefteq S_n$, car A_n est le noyau du morphisme signature $\varepsilon : S_n \to \{-1, +1\}$.

(v) Dans S_3, le sous-groupe $\langle (1\ 2\ 3) \rangle = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$ (d'ordre 3) est distingué, mais les sous-groupes d'ordre 2 (engendrés par les transpositions) ne le sont pas.

2.7 Groupe quotient

Définition 2.5 (Ensemble quotient)**.** Soit G un groupe et $N \trianglelefteq G$. L'*ensemble quotient* G/N est l'ensemble des classes latérales à gauche :

$$G/N = \{gN \mid g \in G\}.$$

Théorème 2.4 (Groupe quotient)**.** Soit G un groupe et $N \trianglelefteq G$. La loi :

$$(aN) \cdot (bN) = (ab)N$$

est bien définie sur G/N et munit G/N d'une structure de groupe. L'élément neutre est $eN = N$ et l'inverse de aN est $a^{-1}N$. L'ordre de G/N est $[G : N]$.

Démonstration. **Bonne définition.** C'est le point crucial. Supposons $aN = a'N$ et $bN = b'N$; il faut montrer que $(ab)N = (a'b')N$. Par hypothèse, il existe $n_1, n_2 \in N$ tels que $a' = an_1$ et $b' = bn_2$. Alors :

$$a'b' = an_1 \cdot bn_2 = a \cdot (n_1 b) \cdot n_2.$$

Or $n_1 b = b(b^{-1} n_1 b)$. Puisque N est distingué dans G, on a $b^{-1} n_1 b \in N$; notons $n_3 = b^{-1} n_1 b \in N$. Donc :

$$a'b' = ab \cdot n_3 n_2,$$

et $n_3 n_2 \in N$ car N est un sous-groupe. Ainsi $a'b' \in (ab)N$, c'est-à-dire $(a'b')N = (ab)N$.

Associativité. Pour $a, b, c \in G$:

$$((aN)(bN))(cN) = (ab)N \cdot cN = ((ab)c)N = (a(bc))N = aN \cdot (bc)N = (aN)((bN)(cN)).$$

Élément neutre. $N \cdot aN = (ea)N = aN$ et $aN \cdot N = (ae)N = aN$, donc $N = eN$ est neutre.

Inverses. $(aN)(a^{-1}N) = (aa^{-1})N = eN = N$ et de même $(a^{-1}N)(aN) = N$. Donc l'inverse de aN est $a^{-1}N$. □

Remarque 2.5. La condition $N \trianglelefteq G$ est **indispensable** pour que la loi sur G/N soit bien définie. Si $H \leq G$ n'est pas distingué, l'ensemble G/H n'a pas de structure naturelle de groupe.

Définition 2.6 (Projection canonique)**.** L'application

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

est un homomorphisme surjectif de groupes, appelé *projection canonique* (ou *surjection canonique*). Son noyau est $\mathrm{Ker}(\pi) = N$.

Le diagramme commutatif suivant résume la situation :

$$G \xrightarrow{\ \pi\ } G/N$$

Exemple 2.6 (Quotients classiques)**.** (i) $\mathbb{Z}/n\mathbb{Z}$ est le quotient du groupe $(\mathbb{Z}, +)$ par le sous-groupe $n\mathbb{Z}$. Les classes sont $\bar{0}, \bar{1}, \ldots, \overline{n-1}$.

(ii) $\mathrm{GL}_n(K)/\mathrm{SL}_n(K) \simeq K^*$. En effet, le morphisme det : $\mathrm{GL}_n(K) \to K^*$ est surjectif et a pour noyau $\mathrm{SL}_n(K)$.

(iii) $S_n/A_n \simeq \mathbb{Z}/2\mathbb{Z}$. Le morphisme signature $\varepsilon : S_n \to \{-1, +1\} \simeq \mathbb{Z}/2\mathbb{Z}$ est surjectif de noyau A_n.

2.8 Centre d'un groupe

Définition 2.7 (Centre)**.** Le *centre* d'un groupe G, noté $Z(G)$, est l'ensemble des éléments qui commutent avec tous les éléments de G :

$$Z(G) = \{z \in G \mid \forall g \in G,\ zg = gz\}.$$

Proposition 2.1. Le centre $Z(G)$ est un sous-groupe distingué abélien de G. De plus, G est abélien si et seulement si $Z(G) = G$.

Démonstration. **Sous-groupe :** $e \in Z(G)$ (donc $Z(G) \neq \varnothing$). Si $a, b \in Z(G)$, alors pour tout $g \in G$, $(ab^{-1})g = a(b^{-1}g) = a(gb^{-1}) = (ag)b^{-1} = (ga)b^{-1} = g(ab^{-1})$. (On utilise le fait que b^{-1} commute avec g si b le fait : $b^{-1}g = b^{-1}g(bb^{-1}) = b^{-1}(gb)b^{-1} = b^{-1}(bg)b^{-1} = gb^{-1}$.) Donc $ab^{-1} \in Z(G)$.

Distingué : pour $g \in G$ et $z \in Z(G)$, on a $gzg^{-1} = zgg^{-1} = z \in Z(G)$.

Abélien : si $a, b \in Z(G)$, alors $ab = ba$ par définition.

Enfin, $Z(G) = G$ si et seulement si tout élément commute avec tout autre, soit G abélien. □

Exemple 2.7. (i) $Z(S_n) = \{e\}$ pour $n \geq 3$.

(ii) $Z(\mathrm{GL}_n(K)) = \{\lambda I_n \mid \lambda \in K^*\}$ (les matrices scalaires).

(iii) $Z(D_n) = \{e\}$ si n est impair, $Z(D_n) = \{e, r^{n/2}\}$ si n est pair.

(iv) $Z(Q_8) = \{1, -1\}$.

2.9 Sous-groupe dérivé

Définition 2.8 (Commutateur, sous-groupe dérivé)**.** Soit G un groupe. Le *commutateur* de $a, b \in G$ est $[a, b] = aba^{-1}b^{-1}$. Le *sous-groupe dérivé* (ou *groupe des commutateurs*) de G est :

$$[G, G] = \langle\, [a, b] \mid a, b \in G \,\rangle,$$

le sous-groupe engendré par l'ensemble de tous les commutateurs.

Remarque 2.6. L'ensemble $\{[a, b] \mid a, b \in G\}$ n'est en général *pas* un sous-groupe ; il faut prendre le sous-groupe engendré.

Proposition 2.2. Le sous-groupe dérivé $[G, G]$ est un sous-groupe distingué de G, et le quotient $G/[G, G]$ est abélien. De plus, si $N \trianglelefteq G$ et G/N est abélien, alors $[G, G] \subseteq N$.

Démonstration. **Distingué :** pour $g \in G$ et $a, b \in G$, on a :

$$g[a, b]g^{-1} = g(aba^{-1}b^{-1})g^{-1} = (gag^{-1})(gbg^{-1})(ga^{-1}g^{-1})(gb^{-1}g^{-1}) = [gag^{-1}, gbg^{-1}].$$

Donc $g[a, b]g^{-1}$ est un commutateur, et par conséquent $g[G, G]g^{-1} \subseteq [G, G]$.

$G/[G, G]$ **est abélien :** soient $a, b \in G$. Dans $G/[G, G]$, on a :

$$(a[G, G])(b[G, G]) = ab[G, G] \quad \text{et} \quad (b[G, G])(a[G, G]) = ba[G, G].$$

Or $ab(ba)^{-1} = aba^{-1}b^{-1} = [a, b] \in [G, G]$, donc $ab[G, G] = ba[G, G]$.

Minimalité : si $N \trianglelefteq G$ et G/N est abélien, alors pour tous $a, b \in G$, $aN \cdot bN = bN \cdot aN$, soit $(ab)N = (ba)N$, d'où $a^{-1}b^{-1}ab \in N$, c'est-à-dire $[a^{-1}, b^{-1}] \in N$. Comme N contient tous les commutateurs et est un sous-groupe, $[G, G] \subseteq N$. □

2.10 Groupes simples

Définition 2.9 (Groupe simple)**.** Un groupe G est dit *simple* s'il est non trivial ($|G| > 1$) et si ses seuls sous-groupes distingués sont $\{e\}$ et G.

Exemple 2.8. (i) Tout groupe d'ordre premier p est simple (car il n'a aucun sous-groupe propre, par Lagrange).

(ii) Le groupe alterné A_n est simple pour $n \geq 5$ (théorème classique).

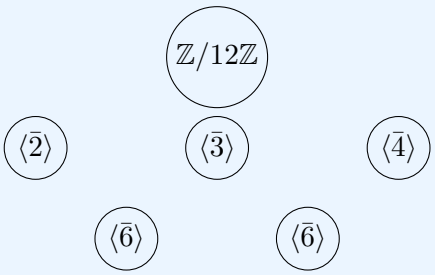
(iii) A_4 n'est pas simple : il contient le sous-groupe distingué $V_4 = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.

Théorème 2.5 (Simplicité de A_n pour $n \geq 5$)**.** Pour tout $n \geq 5$, le groupe alterné A_n est simple.

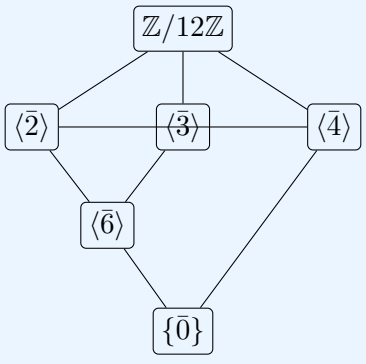
La démonstration de ce théorème sera donnée au chapitre 4, après l'étude des actions de groupes.

2.11 Treillis de sous-groupes

Le *treillis* (ou *diagramme de Hasse*) des sous-groupes d'un groupe G est le diagramme dans lequel chaque sous-groupe est un sommet, et on relie H à K par un trait si $H \subsetneq K$ et s'il n'existe pas de sous-groupe strictement intermédiaire.

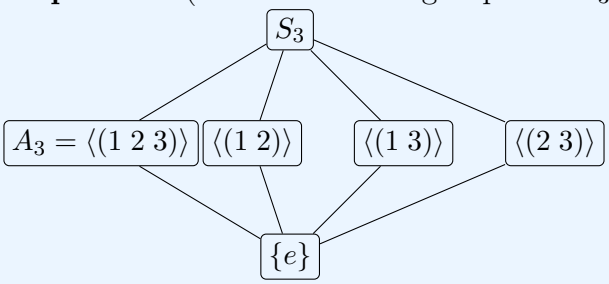


Exemple 2.9 (Treillis des sous-groupes de $\mathbb{Z}/12\mathbb{Z}$)**.**
Précisons : les sous-groupes de $\mathbb{Z}/12\mathbb{Z}$ sont $\langle\bar{d}\rangle$ pour $d \mid 12$, soit $d \in \{1, 2, 3, 4, 6, 12\}$:



où $\langle\bar{2}\rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\}$ (ordre 6), $\langle\bar{3}\rangle = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$ (ordre 4), $\langle\bar{4}\rangle = \{\bar{0}, \bar{4}, \bar{8}\}$ (ordre 3), $\langle\bar{6}\rangle = \{\bar{0}, \bar{6}\}$ (ordre 2). Tous sont distingués puisque $\mathbb{Z}/12\mathbb{Z}$ est abélien.

Exemple 2.10 (Treillis des sous-groupes de S_3)**.**



Le sous-groupe A_3 est le seul sous-groupe distingué propre de S_3.

2.12 Exercices

Exercice 2.1 (Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$)**.** Montrer que les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont exactement les $\langle \bar{d} \rangle$ pour d diviseur de n. En déduire que $\mathbb{Z}/n\mathbb{Z}$ a exactement autant de sous-groupes que de diviseurs de n.

Exercice 2.2 (Sous-groupes de D_4)**.** Déterminer tous les sous-groupes de D_4. Lesquels sont distingués ? Dessiner le treillis des sous-groupes.

Exercice 2.3 (Indice 2 implique distingué)**.** Montrer que tout sous-groupe d'indice 2 est distingué. [*Indication : il n'y a que deux classes latérales.*]

Exercice 2.4 (Centre et quotient)**.** Soit G un groupe. Montrer que si $G/Z(G)$ est cyclique, alors G est abélien. [*Indication : écrire* $G/Z(G) = \langle gZ(G) \rangle$ *et montrer que deux éléments quelconques de* G *commutent.*]

Exercice 2.5 (Commutateur dans S_n)**.** Montrer que $[S_n, S_n] = A_n$ pour $n \geq 2$. [*Indication : montrer que tout* 3*-cycle est un commutateur.*]

Exercice 2.6 (Sous-groupes du groupe de Klein)**.** Déterminer tous les sous-groupes de V_4. Montrer qu'ils sont tous distingués. Calculer les groupes quotients correspondants.

Exercice 2.7 (Intersection de sous-groupes distingués)**.** Soient $N_1, N_2 \trianglelefteq G$. Montrer que $N_1 \cap N_2 \trianglelefteq G$.

Exercice 2.8 (Produit de sous-groupes)**.** Soient $H, K \leq G$. On pose $HK = \{hk \mid h \in H, k \in K\}$.

(a) Montrer que HK est un sous-groupe de G si et seulement si $HK = KH$.

(b) Montrer que si $H \trianglelefteq G$ ou $K \trianglelefteq G$, alors HK est un sous-groupe de G.

(c) Si H et K sont finis, montrer que $|HK| = |H||K|/|H \cap K|$.

Exercice 2.9 (Noyau et sous-groupe distingué)**.** Soit $f : G \to H$ un homomorphisme de groupes. Montrer que $\mathrm{Ker}(f) \trianglelefteq G$.

Exercice 2.10 (Quotients de $\mathbb{Z}$)**.** (a) Montrer que $\mathbb{Z}/n\mathbb{Z}$ est un groupe cyclique d'ordre n en utilisant la définition du groupe quotient.

(b) Déterminer tous les homomorphismes de groupes $\mathbb{Z}/12\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$.

Exercice 2.11 (Correspondance de sous-groupes *(difficile)*)**.** Soit $N \trianglelefteq G$ et $\pi : G \to G/N$ la projection canonique. Montrer qu'il existe une bijection croissante :

$$\{H \leq G \mid N \subseteq H\} \longleftrightarrow \{K \leq G/N\}$$

donnée par $H \mapsto H/N = \pi(H)$ et $K \mapsto \pi^{-1}(K)$. De plus, $H \trianglelefteq G$ si et seulement si $H/N \trianglelefteq G/N$.

Exercice 2.12 (Groupes d'ordre p^2 *(difficile)*)**.** Soit p un nombre premier. Montrer que tout groupe d'ordre p^2 est abélien. [*Indication : montrer d'abord que* $Z(G) \neq \{e\}$ *en utilisant l'équation des classes (chapitre 4), puis appliquer l'exercice 2.4.*]

Résumé du chapitre 2. Un *sous-groupe* $H \leq G$ satisfait le critère $ab^{-1} \in H$ pour tous $a, b \in H$. Le *théorème de Lagrange* affirme que $|H|$ divise $|G|$ (en particulier, $\mathrm{ord}(g)$ divise $|G|$). Un sous-groupe est *distingué* ($N \trianglelefteq G$) si $gNg^{-1} = N$ pour tout g, ce qui permet de construire le *groupe quotient* G/N avec la loi $(aN)(bN) = (ab)N$. Le *centre* $Z(G)$ et le *sous-groupe dérivé* $[G, G]$ sont des sous-groupes distingués fondamentaux. Un groupe est *simple* s'il n'a pas de sous-groupe distingué propre non trivial ; A_n est simple pour $n \geq 5$.

Chapitre 3

Homomorphismes et théorèmes d'isomorphisme

Introduction

Dans les chapitres précédents, nous avons construit un répertoire de groupes et de sous-groupes, et nous avons appris à fabriquer de nouveaux groupes par quotient. Mais comment *comparer* deux groupes ? Quand peut-on affirmer que deux groupes, présentés de manières très différentes, sont en réalité « le même » objet algébrique ?

La réponse réside dans la notion d'*homomorphisme* : une application entre deux groupes qui *respecte la structure*, c'est-à-dire qui envoie le produit sur le produit. Les homomorphismes sont les « bonnes » applications en théorie des groupes, de la même façon que les applications linéaires sont les « bonnes » applications en algèbre linéaire, et les applications continues en topologie.

Ce chapitre culmine avec les *théorèmes d'isomorphisme*, qui relient noyaux, images, sous-groupes distingués et quotients dans un cadre à la fois élégant et puissant. Ces théorèmes constituent l'outil fondamental pour l'étude structurelle des groupes.

3.1 Homomorphismes de groupes

3.1.1 Définition et premières propriétés

Définition 3.1 (Homomorphisme de groupes)**.** Soient $(G, \cdot)$ et $(H, *)$ deux groupes. Un *homomorphisme de groupes* est une application $f : G \to H$ telle que

$$\forall\, a, b \in G, \quad f(a \cdot b) = f(a) * f(b).$$

Proposition 3.1 (Propriétés élémentaires)**.** Soit $f : G \to H$ un homomorphisme de groupes. Alors :

(i) $f(e_G) = e_H$;

(ii) $\forall\, a \in G, \quad f(a^{-1}) = f(a)^{-1}$;

(iii) $\forall\, a \in G,\ \forall\, n \in \mathbb{Z}, \quad f(a^n) = f(a)^n$.

Démonstration. **(i)** On a $f(e_G) = f(e_G \cdot e_G) = f(e_G) * f(e_G)$. En multipliant les deux membres à gauche par $f(e_G)^{-1}$, on obtient $e_H = f(e_G)$.

(ii) Soit $a \in G$. Alors

$$f(a) * f(a^{-1}) = f(a \cdot a^{-1}) = f(e_G) = e_H.$$

De même, $f(a^{-1}) * f(a) = e_H$. Par unicité de l'inverse dans H, on conclut $f(a^{-1}) = f(a)^{-1}$.

(iii) Pour $n \geq 1$, on procède par récurrence. Le cas $n = 0$ découle de (i) et le cas $n < 0$ se ramène au cas positif par (ii). □

Remarque 3.1. La composée de deux homomorphismes de groupes est un homomorphisme de groupes : si $f\colon G \to H$ et $g\colon H \to K$ sont des homomorphismes, alors $g \circ f\colon G \to K$ est un homomorphisme. En effet, pour tous $a, b \in G$,

$$(g \circ f)(ab) = g(f(ab)) = g(f(a)f(b)) = g(f(a))\, g(f(b)) = (g \circ f)(a)\, (g \circ f)(b).$$

3.1.2 Noyau et image

Définition 3.2 (Noyau et image)**.** Soit $f\colon G \to H$ un homomorphisme de groupes. On définit :

(i) le *noyau* de f : $\operatorname{Ker} f = \{g \in G \mid f(g) = e_H\}$;

(ii) l'*image* de f : $\operatorname{Im} f = \{f(g) \mid g \in G\} = f(G)$.

Théorème 3.1 (Le noyau est distingué)**.** Soit $f\colon G \to H$ un homomorphisme de groupes. Alors $\operatorname{Ker} f$ est un sous-groupe distingué de G, c'est-à-dire $\operatorname{Ker} f \trianglelefteq G$.

Démonstration. Sous-groupe. L'élément e_G appartient à $\operatorname{Ker} f$ car $f(e_G) = e_H$ (proposition 3.1). Si $a, b \in \operatorname{Ker} f$, alors

$$f(ab^{-1}) = f(a)\, f(b^{-1}) = f(a)\, f(b)^{-1} = e_H \cdot e_H^{-1} = e_H,$$

donc $ab^{-1} \in \operatorname{Ker} f$. Par le critère du sous-groupe, $\operatorname{Ker} f \leq G$.

Distingué. Soit $g \in G$ et $k \in \operatorname{Ker} f$. Alors

$$f(gkg^{-1}) = f(g)\, f(k)\, f(g^{-1}) = f(g) \cdot e_H \cdot f(g)^{-1} = e_H.$$

Donc $gkg^{-1} \in \operatorname{Ker} f$ pour tout $g \in G$, ce qui montre que $\operatorname{Ker} f \trianglelefteq G$. □

Théorème 3.2 (L'image est un sous-groupe)**.** Soit $f\colon G \to H$ un homomorphisme de groupes. Alors $\operatorname{Im} f$ est un sous-groupe de H.

Démonstration. L'image est non vide car $e_H = f(e_G) \in \operatorname{Im} f$. Soient $h_1, h_2 \in \operatorname{Im} f$; il existe $g_1, g_2 \in G$ tels que $h_i = f(g_i)$. Alors

$$h_1 h_2^{-1} = f(g_1)\, f(g_2)^{-1} = f(g_1)\, f(g_2^{-1}) = f(g_1 g_2^{-1}) \in \operatorname{Im} f.$$

Par le critère du sous-groupe, $\operatorname{Im} f \leq H$. □

Proposition 3.2 (Injectivité et noyau)**.** Soit $f\colon G \to H$ un homomorphisme. Alors

$$f \text{ est injectif} \iff \operatorname{Ker} f = \{e_G\}.$$

Démonstration. ($\Rightarrow$) Si f est injectif et $g \in \operatorname{Ker} f$, alors $f(g) = e_H = f(e_G)$, d'où $g = e_G$.
($\Leftarrow$) Si $\operatorname{Ker} f = \{e_G\}$ et $f(a) = f(b)$, alors $f(ab^{-1}) = f(a)f(b)^{-1} = e_H$, d'où $ab^{-1} \in \operatorname{Ker} f = \{e_G\}$, soit $a = b$. □

3.1.3 Types d'homomorphismes

Définition 3.3 (Types d'homomorphismes)**.** Soit $f\colon G \to H$ un homomorphisme de groupes.

- f est un *monomorphisme* si f est injectif.
- f est un *épimorphisme* si f est surjectif.
- f est un *isomorphisme* si f est bijectif. On écrit alors $G \cong H$.
- f est un *endomorphisme* si $H = G$ (homomorphisme d'un groupe dans lui-même).
- f est un *automorphisme* si f est un endomorphisme bijectif.

Remarque 3.2. Si $f\colon G \to H$ est un isomorphisme, alors $f^{-1}\colon H \to G$ est aussi un isomorphisme. En effet, si $h_1, h_2 \in H$, posons $g_i = f^{-1}(h_i)$; alors $f(g_1g_2) = h_1h_2$, d'où $f^{-1}(h_1h_2) = g_1g_2 = f^{-1}(h_1)f^{-1}(h_2)$.

3.1.4 Exemples fondamentaux

Exemple 3.1 (Déterminant)**.** L'application $\det\colon \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$ est un homomorphisme de groupes (le groupe $\mathrm{GL}_n(\mathbb{R})$ étant muni de la multiplication matricielle et $\mathbb{R}^*$ de la multiplication usuelle). En effet, $\det(AB) = \det(A)\det(B)$. On a

$$\operatorname{Ker}(\det) = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid \det(A) = 1\} = \mathrm{SL}_n(\mathbb{R}),$$

et $\operatorname{Im}(\det) = \mathbb{R}^*$ (l'application est surjective). Le théorème 3.1 redonne le fait classique que $\mathrm{SL}_n(\mathbb{R}) \trianglelefteq \mathrm{GL}_n(\mathbb{R})$.

Exemple 3.2 (Signature)**.** L'application signature $\varepsilon\colon \mathrm{Sym}_n \to \{+1, -1\}$ est un homomorphisme de groupes surjectif (pour $n \geq 2$). Son noyau est le groupe alterné : $\operatorname{Ker}\varepsilon = \mathrm{Alt}_n \trianglelefteq \mathrm{Sym}_n$. Par le premier théorème d'isomorphisme (théorème 3.3), $\mathrm{Sym}_n / \mathrm{Alt}_n \cong \{+1, -1\} \cong \mathbb{Z}/2\mathbb{Z}$.

Exemple 3.3 (Exponentielle)**.** L'application $\exp\colon (\mathbb{R}, +) \to (\mathbb{R}_+^*, \times)$ est un isomorphisme de groupes. En effet, $\exp(x+y) = \exp(x) \cdot \exp(y)$ et exp est bijective de $\mathbb{R}$ sur $\mathbb{R}_+^*$ (son inverse étant le logarithme népérien).

Exemple 3.4 (Projection canonique)**.** Soit $N \trianglelefteq G$. La *projection canonique* $\pi\colon G \to G/N$ définie par $\pi(g) = gN$ est un épimorphisme de groupes. En effet,

$$\pi(ab) = (ab)N = (aN)(bN) = \pi(a)\pi(b),$$

et π est clairement surjective. De plus, $\operatorname{Ker}\pi = N$.

3.2 Théorèmes d'isomorphisme

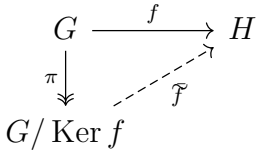
Les théorèmes d'isomorphisme constituent le cœur de l'algèbre des groupes. Ils établissent des liens profonds entre noyaux, images, sous-groupes distingués et quotients.

3.2.1 Premier théorème d'isomorphisme

Théorème 3.3 (Premier théorème d'isomorphisme)**.** Soit $f\colon G \to H$ un homomorphisme de groupes. Alors il existe un unique isomorphisme $\bar{f}\colon G/\operatorname{Ker} f \xrightarrow{\sim} \operatorname{Im} f$ tel que $\bar{f}(g \operatorname{Ker} f) = f(g)$ pour tout $g \in G$. Autrement dit,

$$G/\operatorname{Ker} f \;\cong\; \operatorname{Im} f.$$

Le diagramme commutatif suivant résume la situation :



où $\pi\colon G \to G/\operatorname{Ker} f$ désigne la projection canonique.

Démonstration. Posons $N = \operatorname{Ker} f$ et définissons $\bar{f}\colon G/N \to H$ par $\bar{f}(gN) = f(g)$.

Bonne définition. Si $gN = g'N$, alors $g'^{-1}g \in N = \operatorname{Ker} f$, d'où $f(g'^{-1}g) = e_H$, c'est-à-dire $f(g') = f(g)$. Donc $\bar{f}(gN) = \bar{f}(g'N)$.

Homomorphisme. Pour $gN, g'N \in G/N$,

$$\bar{f}(gN \cdot g'N) = \bar{f}((gg')N) = f(gg') = f(g)f(g') = \bar{f}(gN)\,\bar{f}(g'N).$$

Injectivité. Si $\bar{f}(gN) = e_H$, alors $f(g) = e_H$, d'où $g \in \operatorname{Ker} f = N$, soit $gN = N = e_{G/N}$. Donc $\operatorname{Ker}\bar{f} = \{N\}$, et $\bar{f}$ est injectif par la proposition 3.2.

Surjectivité sur $\operatorname{Im} f$. Par construction, $\operatorname{Im}\bar{f} = \{f(g) \mid g \in G\} = \operatorname{Im} f$.

Unicité. Si $\tilde{f}\colon G/N \to \operatorname{Im} f$ est un autre isomorphisme tel que $\tilde{f} \circ \pi = f$, alors pour tout $g \in G$, $\tilde{f}(gN) = \tilde{f}(\pi(g)) = f(g) = \bar{f}(gN)$, donc $\tilde{f} = \bar{f}$. □

Corollaire 3.1. Si $f\colon G \to H$ est un épimorphisme (homomorphisme surjectif), alors $G/\operatorname{Ker} f \cong H$.

Démonstration. Si f est surjectif, alors $\operatorname{Im} f = H$, et le théorème 3.3 donne $G/\operatorname{Ker} f \cong H$. □

Exemple 3.5. L'application $f\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ définie par $f(k) = \bar{k}$ est un épimorphisme de $(\mathbb{Z}, +)$ sur $(\mathbb{Z}/n\mathbb{Z}, +)$ dont le noyau est $n\mathbb{Z}$. Le premier théorème d'isomorphisme redonne $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$ (tautologiquement, mais cela illustre le mécanisme).

3.2.2 Deuxième théorème d'isomorphisme

Théorème 3.4 (Deuxième théorème d'isomorphisme)**.** Soient G un groupe, $H \leq G$ un sous-groupe et $N \trianglelefteq G$ un sous-groupe distingué. Alors :

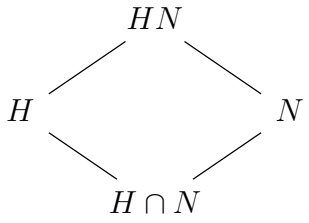
(i) $HN = \{hn \mid h \in H,\ n \in N\}$ est un sous-groupe de G ;

(ii) $H \cap N \trianglelefteq H$;

(iii) $N \trianglelefteq HN$;

(iv) $HN/N \ \cong\ H/(H \cap N)$.

Ce théorème est parfois appelé le *théorème du parallélogramme* ou *du diamant*, en raison du diagramme suivant :



Démonstration. **(i)** Puisque $N \trianglelefteq G$, pour tout $h \in H$ et $n \in N$, on a $hn = h \cdot n \cdot h^{-1} \cdot h = n'h$ pour un certain $n' \in N$ (car $hNh^{-1} = N$). Plus précisément, HN est non vide (il contient e), et si $h_1n_1,\ h_2n_2 \in HN$, alors

$$(h_1n_1)(h_2n_2)^{-1} = h_1n_1n_2^{-1}h_2^{-1} = h_1h_2^{-1} \cdot (h_2n_1n_2^{-1}h_2^{-1}).$$

Or $h_1h_2^{-1} \in H$ et $h_2n_1n_2^{-1}h_2^{-1} \in N$ (car $N \trianglelefteq G$), donc $(h_1n_1)(h_2n_2)^{-1} \in HN$. Par le critère du sous-groupe, $HN \leq G$.

(ii) Soit $h \in H$ et $x \in H \cap N$. Alors $hxh^{-1} \in H$ (car H est un sous-groupe) et $hxh^{-1} \in N$ (car $N \trianglelefteq G$). Donc $hxh^{-1} \in H \cap N$, ce qui montre $H \cap N \trianglelefteq H$.

(iii) Puisque $N \trianglelefteq G$ et $N \subseteq HN \leq G$, on a $N \trianglelefteq HN$.

(iv) Définissons $\varphi\colon H \to HN/N$ par $\varphi(h) = hN$. Vérifions que φ est un homomorphisme surjectif de noyau $H \cap N$.

Homomorphisme. $\varphi(h_1h_2) = (h_1h_2)N = (h_1N)(h_2N) = \varphi(h_1)\varphi(h_2)$.

Surjectivité. Tout élément de HN/N est de la forme $(hn)N = hN = \varphi(h)$ pour $h \in H$, $n \in N$.

Noyau. $h \in \operatorname{Ker}\varphi \iff hN = N \iff h \in N$. Puisque $h \in H$, on obtient $\operatorname{Ker}\varphi = H \cap N$.

Par le premier théorème d'isomorphisme (théorème 3.3),

$$H/(H \cap N) = H/\operatorname{Ker}\varphi \ \cong\ \operatorname{Im}\varphi = HN/N. \qquad \square$$

3.2.3 Troisième théorème d'isomorphisme

Théorème 3.5 (Troisième théorème d'isomorphisme)**.** Soient $N \trianglelefteq G$ et $H \trianglelefteq G$ avec $N \subseteq H$. Alors $H/N \trianglelefteq G/N$ et

$$(G/N)\big/(H/N) \;\cong\; G/H.$$

$$\begin{array}{ccc} G & \xrightarrow{\pi_H} & G/H \\ {\scriptstyle \pi_N}\downarrow & & \uparrow{\scriptstyle \sim} \\ G/N & \xrightarrow[\bar{\pi}]{} & (G/N)/(H/N) \end{array}$$

Démonstration. $H/N \trianglelefteq G/N$. Soit $gN \in G/N$ et $hN \in H/N$. Alors

$$(gN)(hN)(gN)^{-1} = (ghg^{-1})N.$$

Puisque $H \trianglelefteq G$, on a $ghg^{-1} \in H$, donc $(ghg^{-1})N \in H/N$. Ainsi $H/N \trianglelefteq G/N$.

Isomorphisme. Définissons $\varphi\colon G/N \to G/H$ par $\varphi(gN) = gH$.
Bonne définition. Si $gN = g'N$, alors $g'^{-1}g \in N \subseteq H$, d'où $gH = g'H$.
Homomorphisme. $\varphi(gN \cdot g'N) = \varphi((gg')N) = (gg')H = (gH)(g'H) = \varphi(gN)\,\varphi(g'N)$.
Surjectivité. Pour tout $gH \in G/H$, on a $\varphi(gN) = gH$.
Noyau. $gN \in \operatorname{Ker}\varphi \iff gH = H \iff g \in H \iff gN \in H/N$. Donc $\operatorname{Ker}\varphi = H/N$.

Par le premier théorème d'isomorphisme, $(G/N)/(H/N) = (G/N)/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi = G/H$. □

3.2.4 Théorème de correspondance

Théorème 3.6 (Théorème de correspondance)**.** Soit $N \trianglelefteq G$ et $\pi\colon G \to G/N$ la projection canonique. L'application

$$\Phi\colon \{H \leq G \mid N \subseteq H\} \to \{K \leq G/N\}, \qquad H \mapsto H/N = \pi(H),$$

est une bijection, dont l'inverse est $K \mapsto \pi^{-1}(K)$. De plus :

(i) $H_1 \subseteq H_2 \iff H_1/N \subseteq H_2/N$;
(ii) $H \trianglelefteq G \iff H/N \trianglelefteq G/N$;
(iii) $[G : H] = [G/N : H/N]$.

$$\left\{\begin{smallmatrix} H \leq G \\ N \subseteq H \end{smallmatrix}\right\} \underset{\pi^{-1}}{\overset{\Phi}{\rightleftarrows}} \{K \leq G/N\}$$

Démonstration. Φ *est bien définie.* Si $N \subseteq H \leq G$, alors $H/N = \pi(H)$ est un sous-groupe de G/N car π est un homomorphisme et l'image d'un sous-groupe par un homomorphisme est un sous-groupe.

π^{-1} est l'inverse. Pour $K \leq G/N$, posons $H = \pi^{-1}(K)$. Alors H est un sous-groupe de G contenant N (car $\pi(n) = N \in K$ pour tout $n \in N$). On a $\pi(H) = K$ (surjectivité de π sur K), donc $\Phi(\pi^{-1}(K)) = K$.

Inversement, si $N \subseteq H \leq G$, montrons que $\pi^{-1}(\pi(H)) = H$. L'inclusion $H \subseteq \pi^{-1}(\pi(H))$ est évidente. Pour l'autre sens, si $g \in \pi^{-1}(\pi(H))$, alors $gN = hN$ pour un $h \in H$, d'où $g \in hN \subseteq H$ (car $N \subseteq H$).

(i) $H_1 \subseteq H_2 \Rightarrow H_1/N \subseteq H_2/N$ est clair. Réciproquement, si $H_1/N \subseteq H_2/N$ et $h \in H_1$, alors $hN \in H_1/N \subseteq H_2/N$, donc $h \in \pi^{-1}(H_2/N) = H_2$.

(ii) On a vu dans la preuve du théorème 3.5 que si $H \trianglelefteq G$ et $N \subseteq H$, alors $H/N \trianglelefteq G/N$. Réciproquement, si $H/N \trianglelefteq G/N$, alors pour tout $g \in G$ et $h \in H$, $(gN)(hN)(gN)^{-1} = (ghg^{-1})N \in H/N$, d'où $ghg^{-1} \in H$, soit $H \trianglelefteq G$.

(iii) La bijection Φ induit une bijection entre les classes à gauche de H dans G et celles de H/N dans G/N par $gH \mapsto (gN)(H/N)$. □

3.3 Automorphismes

Définition 3.4 (Groupe des automorphismes)**.** Soit G un groupe. L'ensemble $\mathrm{Aut}(G)$ de tous les automorphismes de G, muni de la composition, est un groupe appelé le *groupe des automorphismes* de G.

Définition 3.5 (Automorphisme intérieur)**.** Pour $g \in G$, l'application $\iota_g \colon G \to G$ définie par $\iota_g(x) = gxg^{-1}$ est un automorphisme de G appelé *automorphisme intérieur* défini par g. L'ensemble $\mathrm{Inn}(G) = \{\iota_g \mid g \in G\}$ est le *groupe des automorphismes intérieurs*.

Théorème 3.7. Soit G un groupe. Alors :

(i) $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$;

(ii) $\mathrm{Inn}(G) \cong G/Z(G)$, où $Z(G)$ désigne le centre de G.

Démonstration. **(ii)** Définissons $\Phi \colon G \to \mathrm{Aut}(G)$ par $\Phi(g) = \iota_g$. C'est un homomorphisme car

$$\Phi(gh)(x) = (gh)x(gh)^{-1} = g(hxh^{-1})g^{-1} = \iota_g(\iota_h(x)) = (\iota_g \circ \iota_h)(x) = (\Phi(g) \circ \Phi(h))(x).$$

Le noyau de Φ est $\ker \Phi = \{g \in G \mid \iota_g = \mathrm{Id}_G\} = \{g \in G \mid gxg^{-1} = x,\ \forall x \in G\} = Z(G)$. L'image de Φ est $\mathrm{Inn}(G)$ par définition. Le premier théorème d'isomorphisme donne alors $G/Z(G) \cong \mathrm{Inn}(G)$.

(i) Pour montrer que $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$, soit $\varphi \in \mathrm{Aut}(G)$ et $\iota_g \in \mathrm{Inn}(G)$. Pour tout $x \in G$,

$$(\varphi \circ \iota_g \circ \varphi^{-1})(x) = \varphi(g\,\varphi^{-1}(x)\,g^{-1}) = \varphi(g) \cdot x \cdot \varphi(g)^{-1} = \iota_{\varphi(g)}(x).$$

Donc $\varphi \circ \iota_g \circ \varphi^{-1} = \iota_{\varphi(g)} \in \mathrm{Inn}(G)$. □

Exemple 3.6. Pour $n \geq 1$, un automorphisme φ de $\mathbb{Z}/n\mathbb{Z}$ est entièrement déterminé par $\varphi(\bar{1})$, et $\varphi(\bar{1})$ doit être un générateur de $\mathbb{Z}/n\mathbb{Z}$. Les générateurs de $\mathbb{Z}/n\mathbb{Z}$ sont les $\bar{k}$ avec $\gcd(k, n) = 1$, donc

$$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \;\cong\; (\mathbb{Z}/n\mathbb{Z})^*,$$

le groupe des unités de l'anneau $\mathbb{Z}/n\mathbb{Z}$, qui est d'ordre $\varphi(n)$ (indicatrice d'Euler).

Exemple 3.7. On a $\mathrm{Aut}(\mathrm{Sym}_3) \cong \mathrm{Inn}(\mathrm{Sym}_3) \cong \mathrm{Sym}_3 / Z(\mathrm{Sym}_3) \cong \mathrm{Sym}_3$, car $Z(\mathrm{Sym}_3) = \{e\}$ (le centre du groupe symétrique Sym_n est trivial pour $n \geq 3$).

3.4 Exercices

Exercice 3.1 ($\star$)**.** Soit $f\colon G \to H$ un homomorphisme de groupes. Montrer que si G est abélien et f est surjectif, alors H est abélien.

Exercice 3.2 ($\star$)**.** Soit $f\colon G \to H$ un homomorphisme de groupes et $g \in G$ d'ordre fini n. Montrer que $\mathrm{ord}(f(g))$ divise n. Montrer de plus que si f est injectif, alors $\mathrm{ord}(f(g)) = n$.

Exercice 3.3 ($\star$)**.** Soit $f\colon G \to H$ un homomorphisme de groupes finis. Montrer que $|G| = |\operatorname{Ker} f| \cdot |\operatorname{Im} f|$.

Exercice 3.4 ($\star$)**.** Montrer que tout homomorphisme $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ est déterminé par $f(\bar{1})$, et que $f(\bar{1}) = \bar{k}$ définit un homomorphisme si et seulement si $m \mid kn$.

Exercice 3.5 ($\star\star$)**.** Soit $f\colon G \to H$ un homomorphisme et $K \leq H$. Montrer que $f^{-1}(K) \leq G$. Montrer que si $K \trianglelefteq H$, alors $f^{-1}(K) \trianglelefteq G$.

Exercice 3.6 ($\star\star$)**.** Soient G et H deux groupes. Montrer que $G \times H/(G \times \{e_H\}) \cong H$ en utilisant le premier théorème d'isomorphisme.

Exercice 3.7 ($\star\star$)**.** Soient $m, n \geq 2$ des entiers tels que $\gcd(m, n) = 1$. Montrer que $\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) \cong \mathrm{Aut}(\mathbb{Z}/m\mathbb{Z}) \times \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$. *(Indication : utiliser le fait que $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.)*

Exercice 3.8 ($\star\star$)**.** Soit $G = \mathbb{Z}/12\mathbb{Z}$. Déterminer tous les sous-groupes de G et vérifier le théorème de correspondance pour $N = \langle \bar{4} \rangle$.

Exercice 3.9 ($\star\star$)**.** Soit $G = \mathbb{Z}$, $N = 6\mathbb{Z}$ et $H = 2\mathbb{Z}$. On a $N \subseteq H \subseteq G$ et $N, H \trianglelefteq G$. Vérifier que $(G/N)/(H/N) \cong G/H$ en identifiant explicitement les deux membres.

Exercice 3.10 ($\star\star\star$)**.** Soit $V_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ le groupe de Klein. Montrer que $\mathrm{Aut}(V_4) \cong \mathrm{Sym}_3$. *(Indication : V_4 possède exactement trois éléments d'ordre 2, et tout automorphisme permute ces trois éléments.)*

Exercice 3.11 ($\star\star\star$)**.** Montrer que si $G/Z(G)$ est cyclique, alors G est abélien. En déduire que $\mathrm{Inn}(G)$ ne peut jamais être cyclique non trivial.

Résumé du chapitre 3

Concepts clés.

- Un **homomorphisme** $f\colon G \to H$ vérifie $f(ab) = f(a)f(b)$; il préserve le neutre et les inverses.
- $\mathrm{Ker}\, f \trianglelefteq G$ et $\mathrm{Im}\, f \leq H$. L'injectivité équivaut à $\mathrm{Ker}\, f = \{e\}$.
- **1er théorème d'iso.** : $G/\mathrm{Ker}\, f \cong \mathrm{Im}\, f$.
- **2e théorème d'iso.** : si $H \leq G$ et $N \trianglelefteq G$, alors $HN/N \cong H/(H \cap N)$.
- **3e théorème d'iso.** : si $N \subseteq H \trianglelefteq G$, alors $(G/N)/(H/N) \cong G/H$.
- **Correspondance** : les sous-groupes de G/N sont en bijection avec les sous-groupes de G contenant N.
- $\mathrm{Inn}(G) \cong G/Z(G)$ et $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

Chapitre 4

Actions de groupes et théorèmes de Sylow

Introduction

L'idée de *groupe* est née historiquement de l'étude des symétries : symétries d'une équation polynomiale (Galois), symétries d'une figure géométrique (Klein), transformations d'un espace (Lie). Dans chacun de ces contextes, un groupe *agit* sur un ensemble — sur les racines d'un polynôme, sur les sommets d'un polyèdre, sur les points d'un espace.

La formalisation de cette idée — celle d'*action de groupe* — est l'un des outils les plus puissants de l'algèbre. Elle permet de transformer des questions abstraites sur la structure interne d'un groupe en des questions concrètes de combinatoire (compter des orbites, des points fixes, etc.), et réciproquement.

Ce chapitre développe la théorie des actions de groupes, en commençant par la formule orbite-stabilisateur et l'équation aux classes. Nous en déduisons des résultats structurels importants (théorème de Cauchy, p-groupes) avant de culminer avec les *théorèmes de Sylow*, qui constituent l'un des sommets de la théorie des groupes finis.

4.1 Actions de groupes

4.1.1 Définition et exemples

Définition 4.1 (Action de groupe)**.** Soit G un groupe et X un ensemble non vide. Une *action* (à gauche) de G sur X est une application $G \times X \to X$, notée $(g, x) \mapsto g \cdot x$, satisfaisant :

(A1) $e \cdot x = x$ pour tout $x \in X$;

(A2) $g \cdot (h \cdot x) = (gh) \cdot x$ pour tous $g, h \in G$ et $x \in X$.

On dit alors que G *agit sur* X, ou que X est un G*-ensemble*.

Proposition 4.1 (Formulation comme homomorphisme)**.** Se donner une action de G sur X équivaut à se donner un homomorphisme de groupes $\rho \colon G \to \mathrm{Sym}(X)$, où $\mathrm{Sym}(X)$ désigne le groupe des bijections de X sur lui-même.

Démonstration. Étant donné une action $G \times X \to X$, pour chaque $g \in G$, l'application $\sigma_g \colon X \to X$ définie par $\sigma_g(x) = g \cdot x$ est une bijection de X (d'inverse $\sigma_{g^{-1}}$), et l'application $\rho \colon g \mapsto \sigma_g$ est un homomorphisme de G dans $\mathrm{Sym}(X)$ car $\sigma_{gh} = \sigma_g \circ \sigma_h$ (axiome (A2)).

Réciproquement, un homomorphisme $\rho \colon G \to \mathrm{Sym}(X)$ définit une action par $g \cdot x = \rho(g)(x)$. □

Définition 4.2 (Noyau d'une action)**.** Le *noyau* de l'action est $\operatorname{Ker}\rho = \{g \in G \mid g \cdot x = x,\ \forall x \in X\}$. L'action est dite *fidèle* si $\operatorname{Ker}\rho = \{e\}$.

Exemple 4.1. Tout groupe G agit sur lui-même par *translation à gauche* : $g \cdot x = gx$. Cette action est fidèle. L'homomorphisme associé $\rho \colon G \to \mathrm{Sym}(G)$ est injectif ; c'est le *théorème de Cayley* : tout groupe est isomorphe à un sous-groupe d'un groupe symétrique.

Exemple 4.2. Tout groupe G agit sur lui-même par *conjugaison* : $g \cdot x = gxg^{-1}$. Le noyau de cette action est le centre $Z(G)$.

Exemple 4.3. Le groupe G agit par conjugaison sur l'ensemble de ses sous-groupes : $g \cdot H = gHg^{-1}$. Le stabilisateur d'un sous-groupe H sous cette action est le *normalisateur* $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$.

4.1.2 Orbites et stabilisateurs

Définition 4.3 (Orbite et stabilisateur)**.** Soit G un groupe agissant sur un ensemble X et soit $x \in X$.

- L'*orbite* de x est $\mathrm{Orb}_G(x) = G \cdot x = \{g \cdot x \mid g \in G\}$.
- Le *stabilisateur* de x est $\mathrm{Stab}_G(x) = G_x = \{g \in G \mid g \cdot x = x\}$.

Proposition 4.2. Pour tout $x \in X$, le stabilisateur $\mathrm{Stab}_G(x)$ est un sous-groupe de G.

Démonstration. On a $e \cdot x = x$, donc $e \in \mathrm{Stab}_G(x)$. Si $g, h \in \mathrm{Stab}_G(x)$, alors $(gh^{-1}) \cdot x = g \cdot (h^{-1} \cdot x) = g \cdot x = x$ (car $h^{-1} \cdot x = x$ puisque $h \cdot x = x$). Donc $\mathrm{Stab}_G(x) \leq G$. □

Remarque 4.1. La relation « x et y sont dans la même orbite » (c'est-à-dire $\exists\, g \in G,\ y = g \cdot x$) est une relation d'équivalence sur X. Les orbites forment donc une *partition* de X. Si l'on note X/G l'ensemble des orbites, on a $X = \bigsqcup_{\mathcal{O} \in X/G} \mathcal{O}$.

4.1.3 Formule orbite-stabilisateur

Théorème 4.1 (Formule orbite-stabilisateur)**.** Soit G un groupe fini agissant sur un ensemble X et soit $x \in X$. Alors

$$|\mathrm{Orb}_G(x)| = [G : \mathrm{Stab}_G(x)] = \frac{|G|}{|\mathrm{Stab}_G(x)|}.$$

Démonstration. Posons $S = \mathrm{Stab}_G(x)$ et considérons l'application

$$\Phi \colon G/S \to \mathrm{Orb}_G(x), \qquad gS \mapsto g \cdot x.$$

Bonne définition. Si $gS = g'S$, alors $g'^{-1}g \in S$, d'où $(g'^{-1}g) \cdot x = x$, soit $g \cdot x = g' \cdot x$. Donc $\Phi(gS) = \Phi(g'S)$.

Injectivité. Si $g \cdot x = g' \cdot x$, alors $(g'^{-1}g) \cdot x = x$, d'où $g'^{-1}g \in S$, soit $gS = g'S$.

Surjectivité. Par définition de l'orbite, tout élément de $\mathrm{Orb}_G(x)$ est de la forme $g \cdot x = \Phi(gS)$.

Ainsi Φ est une bijection entre G/S et $\mathrm{Orb}_G(x)$, d'où $|\mathrm{Orb}_G(x)| = |G/S| = [G : S]$. □

Corollaire 4.1. Si G est fini, alors $|\mathrm{Orb}_G(x)|$ divise $|G|$ pour tout $x \in X$.

4.2 Équation aux classes

Théorème 4.2 (Équation aux classes)**.** Soit G un groupe fini agissant sur un ensemble fini X. Soient $x_1, \ldots, x_r$ des représentants des orbites distinctes. Alors

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

Démonstration. Les orbites forment une partition de X (remarque 4.1), donc $|X| = \sum_{i=1}^{r} |\mathrm{Orb}_G(x_i)|$. Le théorème orbite-stabilisateur 4.1 donne $|\mathrm{Orb}_G(x_i)| = [G : \mathrm{Stab}_G(x_i)]$. □

Remarque 4.2. Notons $X^G = \{x \in X \mid g \cdot x = x,\ \forall g \in G\}$ l'ensemble des *points fixes* de l'action. Un point x est fixe si et seulement si $\mathrm{Orb}_G(x) = \{x\}$. En séparant les orbites de cardinal 1 (les points fixes) des autres, l'équation aux classes s'écrit :

$$|X| = |X^G| + \sum_{\substack{i=1 \\ |\mathrm{Orb}_G(x_i)|>1}}^{r} [G : \mathrm{Stab}_G(x_i)].$$

4.2.1 Lemme de Burnside

Théorème 4.3 (Lemme de Burnside)**.** Soit G un groupe fini agissant sur un ensemble fini X. Le nombre d'orbites de cette action est

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|,$$

où $X^g = \{x \in X \mid g \cdot x = x\}$ désigne l'ensemble des points fixés par g.

Démonstration. Considérons l'ensemble $\Omega = \{(g, x) \in G \times X \mid g \cdot x = x\}$ et comptons $|\Omega|$ de deux manières.

En sommant sur g. $|\Omega| = \sum_{g \in G} |X^g|$.

En sommant sur x. $|\Omega| = \sum_{x \in X} |\mathrm{Stab}_G(x)|$. Or, par le théorème orbite-stabilisateur, $|\mathrm{Stab}_G(x)| = |G|/|\mathrm{Orb}_G(x)|$. Donc

$$|\Omega| = \sum_{x \in X} \frac{|G|}{|\mathrm{Orb}_G(x)|} = |G| \sum_{x \in X} \frac{1}{|\mathrm{Orb}_G(x)|}.$$

Or, pour chaque orbite $\mathcal{O}$, $\sum_{x \in \mathcal{O}} \frac{1}{|\mathcal{O}|} = 1$, donc

$$\sum_{x \in X} \frac{1}{|\mathrm{Orb}_G(x)|} = |X/G|.$$

En égalant les deux expressions de $|\Omega|$, $\sum_{g \in G} |X^g| = |G| \cdot |X/G|$, d'où le résultat. □

Exemple 4.4 (Comptage de colliers)**.** Combien y a-t-il de colliers distincts formés de 4 perles, chacune pouvant être de 3 couleurs, si deux colliers sont considérés identiques lorsqu'on peut passer de l'un à l'autre par rotation ?
Le groupe agissant est $G = \mathbb{Z}/4\mathbb{Z}$ (rotations) et $X = \{1, 2, 3\}^4$ (coloriages). On a $|X| = 81$ et $|G| = 4$.

- $g = \bar{0}$ (identité) : $|X^g| = 81$;
- $g = \bar{1}$ (rotation de 90) : toutes les perles doivent être de même couleur, $|X^g| = 3$;
- $g = \bar{2}$ (rotation de 180) : perles opposées de même couleur, $|X^g| = 3^2 = 9$;
- $g = \bar{3}$ (rotation de 270) : comme $\bar{1}$, $|X^g| = 3$.

Par Burnside, le nombre de colliers est $\frac{1}{4}(81 + 3 + 9 + 3) = \frac{96}{4} = 24$.

4.3 Conjugaison et équation aux classes d'un groupe

Définition 4.4 (Classes de conjugaison)**.** Soit G un groupe. Deux éléments $x, y \in G$ sont dits *conjugués* s'il existe $g \in G$ tel que $y = gxg^{-1}$. Les orbites de l'action de G sur lui-même par conjugaison sont les *classes de conjugaison* de G. La classe de x est notée $\mathrm{Cl}(x)$.

Définition 4.5 (Centralisateur)**.** Le *centralisateur* d'un élément $x \in G$ est $C_G(x) = \{g \in G \mid gxg^{-1} = x\} = \mathrm{Stab}_G(x)$ pour l'action par conjugaison.

Proposition 4.3 (Équation aux classes d'un groupe)**.** Soit G un groupe fini. Soient $x_1, \ldots, x_r$ des représentants des classes de conjugaison non centrales ($|\mathrm{Cl}(x_i)| > 1$).

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

Démonstration. C'est un cas particulier de l'équation aux classes (théorème 4.2) appliquée à l'action de G sur lui-même par conjugaison. Les points fixes sont exactement les éléments du centre : $x \in G^G \iff gxg^{-1} = x$ pour tout $g \in G \iff x \in Z(G)$. □

4.3.1 Applications aux p-groupes

Définition 4.6 (p-groupe)**.** Soit p un nombre premier. Un groupe fini G est un *p-groupe* si $|G| = p^k$ pour un entier $k \geq 0$.

Théorème 4.4 (Centre d'un p-groupe)**.** Soit p un nombre premier et G un p-groupe non trivial ($|G| = p^k$, $k \geq 1$). Alors $Z(G) \neq \{e\}$.

Démonstration. Appliquons l'équation aux classes de la proposition 4.3 :
$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(x_i)].$$
Pour chaque i, $[G : C_G(x_i)] = |\mathrm{Cl}(x_i)| > 1$, et $[G : C_G(x_i)]$ divise $|G| = p^k$, donc $p \mid [G : C_G(x_i)]$. Ainsi p divise $\sum_{i=1}^{r} [G : C_G(x_i)]$ et p divise $|G|$, d'où p divise $|Z(G)|$. En particulier, $|Z(G)| \geq p > 1$. □

Théorème 4.5 (Groupes d'ordre p^2)**.** Tout groupe d'ordre p^2 (p premier) est abélien.

Démonstration. Soit $|G| = p^2$. Par le théorème 4.4, $Z(G) \neq \{e\}$, donc $|Z(G)| \in \{p, p^2\}$ (car $|Z(G)|$ divise $|G| = p^2$ et $|Z(G)| > 1$).

Si $|Z(G)| = p^2$, alors $G = Z(G)$ et G est abélien.

Supposons $|Z(G)| = p$. Alors $|G/Z(G)| = p^2/p = p$, donc $G/Z(G)$ est cyclique (tout groupe d'ordre premier est cyclique). Mais si $G/Z(G)$ est cyclique, alors G est abélien (cf. exercice 3.11), ce qui contredit $|Z(G)| = p < p^2$. Donc ce cas est impossible. □

4.4 Théorème de Cauchy

Théorème 4.6 (Théorème de Cauchy)**.** Soit G un groupe fini et p un nombre premier divisant $|G|$. Alors G possède un élément d'ordre p.

Démonstration. On procède par récurrence forte sur $|G|$.

Base. Si $|G| = 1$, aucun premier ne divise $|G|$, donc l'énoncé est trivialement vrai.

Étape de récurrence. Soit $|G| > 1$ et supposons le résultat vrai pour tout groupe d'ordre strictement inférieur à $|G|$. Considérons l'équation aux classes (proposition 4.3) :
$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(x_i)].$$

Cas 1. Il existe i tel que $p \nmid [G : C_G(x_i)]$. Puisque $p \mid |G|$ et $|G| = [G : C_G(x_i)] \cdot |C_G(x_i)|$, on a $p \mid |C_G(x_i)|$. Or $C_G(x_i) \neq G$ (car $|\mathrm{Cl}(x_i)| > 1$, donc $x_i \notin Z(G)$), d'où $|C_G(x_i)| < |G|$. Par hypothèse de récurrence, $C_G(x_i)$ possède un élément d'ordre p, qui est aussi un élément de G d'ordre p.

Cas 2. Pour tout i, $p \mid [G : C_G(x_i)]$. Alors p divise $\sum_i [G : C_G(x_i)]$, et puisque $p \mid |G|$, on déduit $p \mid |Z(G)|$. Comme $Z(G)$ est abélien, on peut l'écrire (par le théorème des groupes abéliens finis) comme un produit de groupes cycliques. Puisque $p \mid |Z(G)|$, au moins un de ces facteurs cycliques est d'ordre divisible par p. Si $\mathbb{Z}/m\mathbb{Z}$ est un tel facteur avec $p \mid m$, alors $\mathbb{Z}/m\mathbb{Z}$ contient un élément d'ordre p (l'élément $\overline{m/p}$). Cet élément est un élément d'ordre p dans G. □

Remarque 4.3. On peut donner une preuve plus élémentaire qui ne fait pas appel au théorème de structure des groupes abéliens finis. Si $Z(G)$ est abélien et $p \mid |Z(G)|$, il suffit de prendre un élément $a \in Z(G)$ d'ordre $n > 1$. Si $p \mid n$, alors $a^{n/p}$ est d'ordre p. Sinon, considérer le quotient $Z(G)/\langle a \rangle$ et raisonner par récurrence sur l'ordre.

4.5 Sous-groupes de Sylow

Définition 4.7 (Sous-groupe de Sylow)**.** Soit G un groupe fini d'ordre $|G| = p^k m$ avec p premier et $\gcd(p, m) = 1$ (c'est-à-dire p^k est la plus grande puissance de p divisant $|G|$). Un *p-sous-groupe de Sylow* (ou simplement *Sylow p-sous-groupe*) de G est un sous-groupe d'ordre p^k. On note $\mathrm{Syl}_p(G)$ l'ensemble des Sylow p-sous-groupes de G et $n_p = |\mathrm{Syl}_p(G)|$ leur nombre.

4.5.1 Premier théorème de Sylow

Théorème 4.7 (Premier théorème de Sylow)**.** Soit G un groupe fini et p un nombre premier. Si p^k divise $|G|$, alors G possède un sous-groupe d'ordre p^k. En particulier, les Sylow p-sous-groupes existent.

Démonstration. On procède par récurrence forte sur $|G|$. Le résultat est trivial pour $|G| = 1$.

Supposons $|G| > 1$ et le résultat vrai pour tout groupe d'ordre strictement inférieur.

Cas 1 : $p \mid |Z(G)|$. Par le théorème de Cauchy (théorème 4.6), $Z(G)$ possède un élément a d'ordre p. Posons $N = \langle a \rangle \trianglelefteq G$ (car $a \in Z(G)$). Le quotient G/N est d'ordre $|G|/p$ et p^{k-1} divise $|G/N|$. Par hypothèse de récurrence, G/N possède un sous-groupe $\bar{H}$ d'ordre p^{k-1}. Par le théorème de correspondance (théorème 3.6), $\bar{H} = H/N$ pour un sous-groupe H de G contenant N, et $|H| = |\bar{H}| \cdot |N| = p^{k-1} \cdot p = p^k$.

Cas 2 : $p \nmid |Z(G)|$. Considérons l'équation aux classes : $|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(x_i)]$. Puisque $p \mid |G|$ et $p \nmid |Z(G)|$, il existe un i tel que $p \nmid [G : C_G(x_i)]$. Posons $C = C_G(x_i)$; c'est un sous-groupe propre de G ($|\mathrm{Cl}(x_i)| > 1$). Comme $|G| = |C| \cdot [G : C]$ et $p^k \mid |G|$ mais $p \nmid [G : C]$, on a $p^k \mid |C|$. Par hypothèse de récurrence (car $|C| < |G|$), C possède un sous-groupe d'ordre p^k, qui est aussi un sous-groupe de G d'ordre p^k. □

4.5.2 Deuxième théorème de Sylow

Lemme 4.1. Soit P un p-groupe agissant sur un ensemble fini X. Alors $|X| \equiv |X^P| \pmod{p}$, où $X^P = \{x \in X \mid g \cdot x = x,\ \forall g \in P\}$ est l'ensemble des points fixes.

Démonstration. Par l'équation aux classes, $|X| = |X^P| + \sum_j |\mathrm{Orb}_P(x_j)|$, où la somme porte sur les orbites de cardinal > 1. Pour chacune, $|\mathrm{Orb}_P(x_j)| = [P : \mathrm{Stab}_P(x_j)]$ divise $|P| = p^k$, et $|\mathrm{Orb}_P(x_j)| > 1$, donc $p \mid |\mathrm{Orb}_P(x_j)|$. D'où $|X| \equiv |X^P| \pmod{p}$. □

Théorème 4.8 (Deuxième théorème de Sylow)**.** Soit G un groupe fini et p un nombre premier. Tous les Sylow p-sous-groupes de G sont conjugués : si P et Q sont deux Sylow p-sous-groupes, il existe $g \in G$ tel que $Q = gPg^{-1}$.

Démonstration. Soit P un Sylow p-sous-groupe de G et posons $\Sigma = \{gPg^{-1} \mid g \in G\}$ l'ensemble des conjugués de P (qui sont tous des Sylow p-sous-groupes de G). Nous devons montrer que tout Sylow p-sous-groupe Q appartient à Σ.

Faisons agir Q sur Σ par conjugaison : $q \cdot (gPg^{-1}) = (qg)P(qg)^{-1}$. Par le lemme 4.1, $|\Sigma| \equiv |\Sigma^Q| \pmod{p}$.

Un élément $gPg^{-1} \in \Sigma$ est fixé par Q si et seulement si $Q \subseteq N_G(gPg^{-1})$, le normalisateur de gPg^{-1}. Si $gPg^{-1} \in \Sigma^Q$, alors Q et gPg^{-1} sont tous deux des Sylow p-sous-groupes du groupe $N_G(gPg^{-1})$, et $gPg^{-1} \trianglelefteq N_G(gPg^{-1})$. Considérons le quotient $N_G(gPg^{-1})/(gPg^{-1})$. L'image de Q dans ce quotient est $Q(gPg^{-1})/(gPg^{-1})$, qui est un p-groupe par le deuxième théorème d'isomorphisme (théorème 3.4). Mais l'ordre de ce quotient divise $[N_G(gPg^{-1}) : gPg^{-1}]$, qui n'est pas divisible par p (car gPg^{-1} est déjà un Sylow p-sous-groupe). Donc $Q(gPg^{-1})/(gPg^{-1})$ est trivial, d'où $Q \subseteq gPg^{-1}$. Comme $|Q| = |gPg^{-1}| = p^k$, on conclut $Q = gPg^{-1}$.

Ainsi, $\Sigma^Q = \{gPg^{-1}\}$ tel que $Q = gPg^{-1}$, donc $|\Sigma^Q| = 1$. En particulier $Q \in \Sigma$. □

4.5.3 Troisième théorème de Sylow

Théorème 4.9 (Troisième théorème de Sylow)**.** Soit G un groupe fini d'ordre $|G| = p^k m$ avec $\gcd(p, m) = 1$. Alors :

(i) $n_p \equiv 1 \pmod{p}$;

(ii) n_p divise $m = |G|/p^k$.

Démonstration. **(i)** Soit P un Sylow p-sous-groupe et $\Sigma = \mathrm{Syl}_p(G)$. Par le deuxième théorème de Sylow (théorème 4.8), Σ est l'orbite de P sous l'action de G par conjugaison, donc $n_p = |\Sigma|$.

Faisons agir P sur Σ par conjugaison. Par le lemme 4.1, $|\Sigma| \equiv |\Sigma^P| \pmod{p}$. Dans la preuve du théorème 4.8, nous avons montré que si $Q \in \Sigma$ est fixé par un Sylow p-sous-groupe, alors Q coïncide avec ce sous-groupe. Donc $\Sigma^P = \{P\}$, d'où $|\Sigma^P| = 1$ et $n_p \equiv 1 \pmod{p}$.

(ii) Le groupe G agit transitivement sur Σ par conjugaison (théorème 4.8), donc $n_p = |\Sigma| = [G : N_G(P)]$, où $N_G(P)$ est le normalisateur de P dans G. Puisque $P \leq N_G(P)$,

on a $p^k \mid |N_G(P)|$, d'où

$$n_p = \frac{|G|}{|N_G(P)|} \;\middle|\; \frac{|G|}{p^k} = m. \qquad \square$$

4.6 Applications des théorèmes de Sylow

4.6.1 Groupes d'ordre pq

Proposition 4.4 (Groupes d'ordre pq)**.** Soient $p < q$ deux nombres premiers tels que $q \not\equiv 1 \pmod{p}$. Alors tout groupe d'ordre pq est cyclique.

Démonstration. Soit $|G| = pq$. Par le troisième théorème de Sylow (théorème 4.9) :

- $n_q \mid p$ et $n_q \equiv 1 \pmod{q}$. Donc $n_q \in \{1, p\}$. Puisque $p < q$, $p \not\equiv 1 \pmod{q}$, donc $n_q = 1$.
- $n_p \mid q$ et $n_p \equiv 1 \pmod{p}$. Donc $n_p \in \{1, q\}$. Puisque $q \not\equiv 1 \pmod{p}$, on a $n_p = 1$.

Soient P et Q les uniques Sylow p- et q-sous-groupes. Ils sont distingués ($n_p = n_q = 1$), d'ordres p et q respectivement (donc cycliques). De plus, $P \cap Q = \{e\}$ (car $\gcd(p, q) = 1$) et $|PQ| = |P| \cdot |Q|/|P \cap Q| = pq = |G|$, donc $G = PQ$. Comme P et Q sont distingués et $P \cap Q = \{e\}$, on a $G \cong P \times Q \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$. $\square$

Corollaire 4.2. Tout groupe d'ordre 15 est cyclique.

Démonstration. $15 = 3 \times 5$. On a $p = 3$, $q = 5$ et $q = 5 \not\equiv 1 \pmod{3}$. La proposition 4.4 s'applique. $\square$

4.6.2 Groupes d'ordre 12

Proposition 4.5. Il n'existe pas de groupe simple d'ordre 12.

Démonstration. Soit G un groupe d'ordre $12 = 2^2 \cdot 3$.

Par le troisième théorème de Sylow, $n_3 \mid 4$ et $n_3 \equiv 1 \pmod{3}$, donc $n_3 \in \{1, 4\}$.

Cas 1 : $n_3 = 1$. L'unique Sylow 3-sous-groupe est distingué, donc G n'est pas simple.

Cas 2 : $n_3 = 4$. G agit par conjugaison sur $\mathrm{Syl}_3(G)$ (qui a 4 éléments), ce qui définit un homomorphisme $\varphi\colon G \to \mathrm{Sym}_4$. Le noyau $\ker\varphi \trianglelefteq G$. Puisque l'action est transitive sur $\mathrm{Syl}_3(G)$, φ n'est pas triviale, donc $\ker\varphi \neq G$.

Si $\ker\varphi = \{e\}$, alors G s'injecte dans Sym_4 ($|G| = 12$ divise $|\mathrm{Sym}_4| = 24$). Les 4 Sylow 3-sous-groupes fournissent $4 \times 2 = 8$ éléments d'ordre 3. Il reste $12 - 8 = 4$ éléments dans G, qui doivent constituer un unique Sylow 2-sous-groupe (d'ordre 4). Ce Sylow 2-sous-groupe est alors distingué, et G n'est pas simple.

Si $\{e\} \subsetneq \ker\varphi \subsetneq G$, alors G possède un sous-groupe distingué non trivial, et n'est pas simple.

Dans tous les cas, G n'est pas simple. $\square$

4.6.3 Diagramme de sous-groupes

Le diagramme suivant illustre le treillis des sous-groupes d'un groupe G d'ordre 12 avec $n_3 = 1$ et $n_2 = 1$ (cas $G \cong \mathbb{Z}/12\mathbb{Z}$), en mettant en évidence les Sylow sous-groupes.

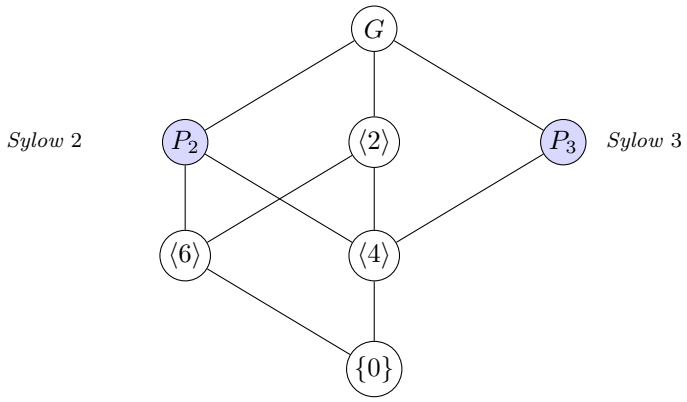


FIGURE 4.1 – Treillis des sous-groupes de $\mathbb{Z}/12\mathbb{Z}$, avec les Sylow sous-groupes en bleu.

4.7 Exercices

Exercice 4.1 ($\star$)**.** Vérifier que l'action de Sym_3 sur $\{1, 2, 3\}$ par permutation naturelle satisfait les axiomes (A1) et (A2). Déterminer l'orbite et le stabilisateur de chaque élément.

Exercice 4.2 ($\star$)**.** Le groupe diédral D_4 (d'ordre 8) agit sur les sommets d'un carré. Déterminer toutes les orbites et tous les stabilisateurs. Vérifier la formule orbite-stabilisateur.

Exercice 4.3 ($\star$)**.** Déterminer les classes de conjugaison de Sym_3 et vérifier l'équation aux classes.

Exercice 4.4 ($\star$)**.** Déterminer le centre du groupe diédral D_n pour tout $n \geq 3$.

Exercice 4.5 ($\star\star$)**.** De combien de manières peut-on colorier les faces d'un cube avec k couleurs, si deux coloriages sont considérés identiques lorsqu'on peut passer de l'un à l'autre par une rotation ? *(Le groupe des rotations du cube est isomorphe à* Sym_4*, d'ordre* 24*.)*

Exercice 4.6 ($\star\star$)**.** Soit G un p-groupe d'ordre p^n ($n \geq 1$). Montrer que G possède un sous-groupe distingué d'ordre p^k pour tout $0 \leq k \leq n$. *(Raisonner par récurrence en utilisant le fait que* $Z(G) \neq \{e\}$*.)*

Exercice 4.7 ($\star\star$)**.** Soit G un groupe fini et P un Sylow p-sous-groupe de G. Montrer que $N_G(N_G(P)) = N_G(P)$.

Exercice 4.8 ($\star\star$)**.** Montrer que si $n_p = 1$, alors l'unique Sylow p-sous-groupe est distingué dans G.

Exercice 4.9 ($\star\star$)**.** Déterminer les possibilités pour n_3 et n_7 dans un groupe d'ordre 21. En déduire que tout groupe d'ordre 21 possède un unique Sylow 7-sous-groupe, qui est distingué.

Exercice 4.10 ($\star\star\star$)**.** Montrer qu'il n'existe pas de groupe simple d'ordre 36. *(Considérer n_3 et raisonner comme dans la proposition 4.5.)*

Exercice 4.11 ($\star\star\star$)**.** Soient $p < q$ deux nombres premiers. Classifier (à isomorphisme près) les groupes d'ordre p^2q lorsque $q \not\equiv 1 \pmod{p}$ et $q \not\equiv 1 \pmod{p^2}$.

Exercice 4.12 ($\star\star\star$)**.** Soit G un groupe fini et p un premier tel que $n_p > 1$. Montrer qu'il existe deux Sylow p-sous-groupes distincts P_1, P_2 tels que $P_1 \cap P_2$ est le plus grand p-sous-groupe distingué de G contenu dans tout Sylow p-sous-groupe, c'est-à-dire $P_1 \cap P_2 = O_p(G) := \bigcap_{P \in \mathrm{Syl}_p(G)} P$.

Exercice 4.13 ($\star\star\star$)**.** Soit G un groupe simple d'ordre 60. Montrer que $G \cong \mathrm{Alt}_5$. *(Montrer que $n_5 = 6$, puis que l'action de G sur $\mathrm{Syl}_5(G)$ donne un monomorphisme $G \hookrightarrow \mathrm{Sym}_6$ dont l'image est contenue dans Alt_6.)*

Résumé du chapitre 4

Concepts clés.

- Une **action** de G sur X est un homomorphisme $G \to \mathrm{Sym}(X)$.
- **Orbite-stabilisateur** : $|\mathrm{Orb}(x)| = [G : \mathrm{Stab}(x)]$.
- **Équation aux classes** : $|X| = |X^G| + \sum [G : \mathrm{Stab}(x_i)]$.
- **Burnside** : $|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$.
- Le **centre d'un p-groupe** non trivial est non trivial.
- Tout groupe d'ordre p^2 est **abélien**.
- **Cauchy** : si $p \mid |G|$, il existe un élément d'ordre p.
- **Sylow 1** : les Sylow p-sous-groupes existent.
- **Sylow 2** : ils sont tous conjugués.
- **Sylow 3** : $n_p \equiv 1 \pmod{p}$ et $n_p \mid |G|/p^k$.

Chapitre 5

Anneaux — Définitions, exemples, idéaux

Introduction

L'étude des anneaux trouve son origine dans les travaux de Dedekind, qui introduisit la notion d'*ordre* dans les corps de nombres algébriques pour comprendre la factorisation des entiers dans des extensions de $\mathbb{Z}$. Hilbert systématisa l'usage du mot *Zahlring* (anneau de nombres) dans son *Zahlbericht* (1897), et c'est Noether qui, dans les années 1920, dégagea la théorie abstraite des anneaux et de leurs idéaux dans toute sa généralité, posant les fondements de l'algèbre commutative moderne.

Le passage du groupe à l'anneau enrichit considérablement la structure : on dispose désormais de *deux* opérations, l'addition et la multiplication, liées par la distributivité. Cette structure apparaît naturellement dans $\mathbb{Z}$, dans les anneaux de polynômes $K[X]$, dans les anneaux de matrices $M_n(K)$, et dans bien d'autres contextes. Le présent chapitre introduit les définitions fondamentales, étudie les premières propriétés, puis développe la théorie des idéaux.

5.1 Définition d'un anneau

Définition 5.1 (Anneau)**.** Un *anneau* est un triplet $(A, +, \cdot)$ où A est un ensemble muni de deux lois de composition internes vérifiant :

(A1) $(A, +)$ est un groupe abélien, d'élément neutre noté 0_A (ou simplement 0).

(A2) La multiplication est associative : $\forall\, a, b, c \in A,\ (a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(A3) Il existe un élément $1_A \in A$ (ou simplement 1), appelé *élément unité*, tel que $\forall\, a \in A,\ 1_A \cdot a = a \cdot 1_A = a$.

(A4) La multiplication est distributive par rapport à l'addition :

$$\forall\, a, b, c \in A, \quad a(b + c) = ab + ac \quad \text{et} \quad (a + b)c = ac + bc.$$

Si de plus la multiplication est commutative, on dit que A est un *anneau commutatif*.

Remarque 5.1 (Convention)**.** Dans cet ouvrage, sauf mention explicite du contraire, tous les anneaux possèdent un élément unité 1_A, et les morphismes d'anneaux respectent l'unité (cf. la section 5.5). Cette convention suit l'usage de Bourbaki.

Remarque 5.2 (Anneau trivial)**.** Si $1_A = 0_A$, alors pour tout $a \in A$, $a = 1_A \cdot a = 0_A \cdot a = 0_A$ (cf. la proposition 5.1), d'où $A = \{0\}$. On appelle cet anneau l'*anneau trivial* ou *anneau nul*.

5.2 Propriétés élémentaires

Proposition 5.1 (Propriétés élémentaires d'un anneau)**.** Soit $(A, +, \cdot)$ un anneau. Pour tous $a, b \in A$:

(i) $0 \cdot a = a \cdot 0 = 0$ (0 est *absorbant*).

(ii) $(-1) \cdot a = a \cdot (-1) = -a$.

(iii) $(-a)(-b) = ab$.

(iv) $\Big(\sum_{i=1}^{m} a_i\Big)\Big(\sum_{j=1}^{n} b_j\Big) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_i b_j$.

Démonstration. (i) On a $0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a$ par distributivité. En ajoutant $-(0 \cdot a)$ des deux côtés, on obtient $0 = 0 \cdot a$. La relation $a \cdot 0 = 0$ se démontre de manière symétrique.

(ii) On calcule $(-1) \cdot a + a = (-1) \cdot a + 1 \cdot a = (-1+1) \cdot a = 0 \cdot a = 0$ par (i). Donc $(-1) \cdot a = -a$. L'égalité $a \cdot (-1) = -a$ s'obtient de façon analogue.

(iii) $(-a)(-b) = (-1 \cdot a)(-1 \cdot b) = (-1)(-1) \cdot ab$. Or $(-1)(-1) + (-1) = (-1)((-1) + 1) = (-1) \cdot 0 = 0$, donc $(-1)(-1) = 1$. D'où $(-a)(-b) = ab$.

(iv) Par récurrence sur m et n, en utilisant la distributivité à chaque étape. □

5.3 Exemples fondamentaux

Exemple 5.1 (Anneaux classiques)**.** Les ensembles suivants, munis de l'addition et de la multiplication usuelles, sont des anneaux commutatifs unitaires :

(a) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

(b) $\mathbb{Z}/n\mathbb{Z}$ pour tout entier $n \geqslant 1$.

(c) L'anneau des entiers de Gauss $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$.

(d) Pour $d \in \mathbb{Z}$ sans facteur carré, $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$.

Exemple 5.2 (Anneau de polynômes)**.** Soit A un anneau commutatif. L'*anneau de polynômes* $A[X]$ est l'ensemble des suites $(a_n)_{n \geqslant 0}$ d'éléments de A, presque toutes nulles, muni de l'addition terme à terme et du produit de Cauchy :

$$\Big(\sum_{k} a_k X^k\Big)\Big(\sum_{k} b_k X^k\Big) = \sum_{k}\Big(\sum_{i+j=k} a_i b_j\Big) X^k.$$

On note $\deg(P)$ le degré d'un polynôme non nul P. Par convention, $\deg(0) = -\infty$.

Exemple 5.3 (Anneau de séries formelles)**.** Soit A un anneau commutatif. L'anneau $A[[X]]$ des *séries formelles* à coefficients dans A est défini comme l'ensemble des suites $(a_n)_{n\geqslant 0}$ d'éléments de A (sans condition de support fini), muni des mêmes opérations que $A[X]$. L'anneau $A[X]$ est un sous-anneau de $A[[X]]$.

Exemple 5.4 (Anneau de matrices)**.** Soit A un anneau et $n \geqslant 1$. L'ensemble $M_n(A)$ des matrices carrées $n \times n$ à coefficients dans A, muni de l'addition et de la multiplication matricielles, est un anneau unitaire d'élément unité I_n. Pour $n \geqslant 2$, cet anneau est *non commutatif*.

Exemple 5.5 (Anneau de groupe)**.** Soit A un anneau commutatif et G un groupe (fini pour simplifier). L'*anneau de groupe* $A[G]$ est le A-module libre de base G, c'est-à-dire l'ensemble des sommes formelles $\sum_{g\in G} a_g\, g$ avec $a_g \in A$, muni de la multiplication :

$$\Big(\sum_{g\in G} a_g\, g\Big)\Big(\sum_{h\in G} b_h\, h\Big) = \sum_{g,h\in G} a_g b_h\, (gh).$$

C'est un anneau unitaire (d'unité $1_A \cdot e_G$), commutatif si et seulement si G est abélien.

5.4 Diviseurs de zéro, intégrité, éléments inversibles

Définition 5.2 (Diviseur de zéro)**.** Soit A un anneau. Un élément $a \in A \setminus \{0\}$ est un *diviseur de zéro* (à gauche) s'il existe $b \in A \setminus \{0\}$ tel que $ab = 0$. On définit de même les diviseurs de zéro à droite.

Définition 5.3 (Anneau intègre)**.** Un anneau commutatif unitaire A est *intègre* (ou est un *domaine d'intégrité*) si $A \neq \{0\}$ et s'il ne possède aucun diviseur de zéro, c'est-à-dire :

$$\forall\, a, b \in A, \quad ab = 0 \implies a = 0 \text{ ou } b = 0.$$

Exemple 5.6. Les anneaux $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $K[X]$ (où K est un corps), $\mathbb{Z}[i]$ sont intègres. L'anneau $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre car $\bar{2} \cdot \bar{3} = \bar{0}$.

Définition 5.4 (Élément inversible, groupe des unités)**.** Soit A un anneau. Un élément $a \in A$ est *inversible* (ou est une *unité*) s'il existe $b \in A$ tel que $ab = ba = 1$. L'ensemble des éléments inversibles de A est noté $A^\times$ ou $U(A)$; c'est un groupe pour la multiplication, appelé le *groupe des unités* de A.

Exemple 5.7 (Groupes des unités)**.** (a) $U(\mathbb{Z}) = \{-1, 1\}$.
(b) $U(\mathbb{Z}/n\mathbb{Z}) = \{\bar{a} \mid \operatorname{pgcd}(a, n) = 1\} = (\mathbb{Z}/n\mathbb{Z})^\times$.

(c) $U(K[X]) = K^\times = K \setminus \{0\}$ pour tout corps K.
(d) $U(M_n(K)) = \mathrm{GL}_n(K)$.
(e) $U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$.
(f) $U(K[[X]]) = \{f \in K[[X]] \mid f(0) \neq 0\}$.

Proposition 5.2. Soit A un anneau et $a \in U(A)$. Alors a n'est pas un diviseur de zéro.

Démonstration. Supposons $ab = 0$ avec $a \in U(A)$. Alors $b = 1 \cdot b = (a^{-1}a)b = a^{-1}(ab) = a^{-1} \cdot 0 = 0$. Donc a n'est pas un diviseur de zéro. □

5.5 Sous-anneaux et morphismes d'anneaux

Définition 5.5 (Sous-anneau)**.** Soit A un anneau. Un sous-ensemble $B \subseteq A$ est un *sous-anneau* de A si :

(i) $1_A \in B$.
(ii) B est stable par soustraction : $\forall\, a, b \in B,\ a - b \in B$.
(iii) B est stable par multiplication : $\forall\, a, b \in B,\ ab \in B$.

Définition 5.6 (Morphisme d'anneaux)**.** Soient A et B deux anneaux. Une application $\varphi\colon A \to B$ est un *morphisme d'anneaux* si :

(i) $\varphi(a + a') = \varphi(a) + \varphi(a')$ pour tous $a, a' \in A$.
(ii) $\varphi(a \cdot a') = \varphi(a) \cdot \varphi(a')$ pour tous $a, a' \in A$.
(iii) $\varphi(1_A) = 1_B$.

Le *noyau* est $\mathrm{Ker}(\varphi) = \varphi^{-1}(\{0_B\})$ et l'*image* est $\mathrm{Im}(\varphi) = \varphi(A)$.

Proposition 5.3. Soit $\varphi\colon A \to B$ un morphisme d'anneaux.

(i) $\mathrm{Im}(\varphi)$ est un sous-anneau de B.
(ii) $\mathrm{Ker}(\varphi)$ est un idéal bilatère de A (cf. définition 5.7).
(iii) φ est injectif si et seulement si $\mathrm{Ker}(\varphi) = \{0\}$.

Démonstration. (i) L'image contient $\varphi(1_A) = 1_B$, et elle est stable par soustraction et multiplication par fonctorialité de φ.

(ii) Le noyau $I = \mathrm{Ker}(\varphi)$ est un sous-groupe de $(A, +)$ car φ est un morphisme de groupes additifs. Soient $a \in A$ et $x \in I$. Alors $\varphi(ax) = \varphi(a)\varphi(x) = \varphi(a) \cdot 0 = 0$, donc $ax \in I$. De même $xa \in I$. Ainsi I est un idéal bilatère.

(iii) Si φ est injectif, le seul antécédent de 0 est 0, donc $\mathrm{Ker}(\varphi) = \{0\}$. Réciproquement, si $\mathrm{Ker}(\varphi) = \{0\}$ et $\varphi(a) = \varphi(a')$, alors $\varphi(a - a') = 0$, d'où $a - a' \in \mathrm{Ker}(\varphi) = \{0\}$ et $a = a'$. □

5.6 Idéaux

Définition 5.7 (Idéal bilatère)**.** Soit A un anneau. Un sous-ensemble $I \subseteq A$ est un *idéal à gauche* de A si :

(i) $(I, +)$ est un sous-groupe de $(A, +)$.

(ii) $\forall\, a \in A,\ \forall\, x \in I,\ ax \in I$.

On définit de même un *idéal à droite* en remplaçant (ii) par $xa \in I$. Un idéal est dit *bilatère* s'il est à la fois à gauche et à droite. Dans un anneau commutatif, ces trois notions coïncident ; on parle alors simplement d'*idéal*.

Remarque 5.3. En pratique, pour vérifier que I est un idéal d'un anneau commutatif A, il suffit de montrer que :

(a) $I \neq \varnothing$ (par exemple $0 \in I$).

(b) $\forall\, x, y \in I,\ x - y \in I$.

(c) $\forall\, a \in A,\ \forall\, x \in I,\ ax \in I$.

Définition 5.8 (Idéal principal)**.** Soit A un anneau commutatif et $a \in A$. L'*idéal principal engendré par* a est :

$$(a) = aA = \{ax \mid x \in A\}.$$

Un idéal I de A est dit *principal* s'il existe $a \in A$ tel que $I = (a)$.

Définition 5.9 (Idéal engendré)**.** Soit A un anneau commutatif et $S \subseteq A$. L'*idéal engendré par* S, noté (S), est le plus petit idéal de A contenant S :

$$(S) = \bigcap_{\substack{I \text{ idéal de } A \\ S \subseteq I}} I = \Big\{ \sum_{i=1}^{n} a_i s_i \;\Big|\; n \geqslant 0,\ a_i \in A,\ s_i \in S \Big\}.$$

Pour un nombre fini de générateurs, on note $(a_1, \ldots, a_k) = a_1 A + \cdots + a_k A$.

Exemple 5.8 (Idéaux de $\mathbb{Z}$)**.** Tout idéal de $\mathbb{Z}$ est principal : si I est un idéal non nul de $\mathbb{Z}$, soit d le plus petit élément strictement positif de I. Par division euclidienne, tout élément de I est un multiple de d, d'où $I = d\mathbb{Z} = (d)$.

Exemple 5.9 (Idéaux de $K[X]$)**.** De même, tout idéal de $K[X]$ (K corps) est principal. Si $I \neq \{0\}$, le polynôme unitaire de degré minimal dans I engendre I (par division euclidienne).

5.7 Opérations sur les idéaux

Proposition 5.4 (Opérations sur les idéaux)**.** Soient I et J deux idéaux d'un anneau commutatif A.

(i) L'*intersection* $I \cap J$ est un idéal de A.

(ii) La *somme* $I + J = \{a + b \mid a \in I,\ b \in J\}$ est un idéal de A ; c'est le plus petit idéal contenant I et J.

(iii) Le *produit* $IJ = \left\{\sum_{k=1}^{n} a_k b_k \mid n \geqslant 1,\ a_k \in I,\ b_k \in J\right\}$ est un idéal de A, et $IJ \subseteq I \cap J$.

Démonstration. (i) L'intersection de sous-groupes est un sous-groupe, et si $a \in A$, $x \in I \cap J$, alors $ax \in I$ et $ax \in J$, donc $ax \in I \cap J$.

(ii) La somme $I+J$ contient $0 = 0+0$. Si $a+b$, $a'+b' \in I+J$ avec $a, a' \in I$ et $b, b' \in J$, alors $(a+b)-(a'+b') = (a-a')+(b-b') \in I+J$. Pour $c \in A$, $c(a+b) = ca+cb \in I+J$.

(iii) Vérifions que IJ est un idéal. La stabilité par addition résulte de la définition (on concatène les sommes). Pour $c \in A$ et $\sum a_k b_k \in IJ$, on a $c\sum a_k b_k = \sum (ca_k) b_k \in IJ$ car $ca_k \in I$. Enfin, si $x \in IJ$, $x = \sum a_k b_k$ avec $a_k b_k \in I$ (car I est un idéal et $b_k \in A$) et $a_k b_k \in J$ de même, donc $x \in I \cap J$. □

Exemple 5.10. Dans $\mathbb{Z}$: $(m) + (n) = (\mathrm{pgcd}(m,n))$, $\quad (m) \cap (n) = (\mathrm{ppcm}(m,n))$, $(m)(n) = (mn)$.

5.8 Idéaux premiers et idéaux maximaux

Définition 5.10 (Idéal premier)**.** Un idéal $\mathfrak{p}$ d'un anneau commutatif A est *premier* si $\mathfrak{p} \neq A$ et :

$$\forall\, a, b \in A, \quad ab \in \mathfrak{p} \implies a \in \mathfrak{p} \text{ ou } b \in \mathfrak{p}.$$

Définition 5.11 (Idéal maximal)**.** Un idéal $\mathfrak{m}$ d'un anneau commutatif A est *maximal* si $\mathfrak{m} \neq A$ et si les seuls idéaux contenant $\mathfrak{m}$ sont $\mathfrak{m}$ et A :

$$\forall\, I \text{ idéal de } A, \quad \mathfrak{m} \subseteq I \subseteq A \implies I = \mathfrak{m} \text{ ou } I = A.$$

Théorème 5.1 (Caractérisation des idéaux premiers)**.** Soit A un anneau commutatif et $\mathfrak{p}$ un idéal de A. Alors :

$$\mathfrak{p} \text{ est premier} \iff A/\mathfrak{p} \text{ est intègre.}$$

Démonstration. ($\Rightarrow$) Supposons $\mathfrak{p}$ premier. Comme $\mathfrak{p} \neq A$, on a $A/\mathfrak{p} \neq \{0\}$. Soient $\bar{a}, \bar{b} \in A/\mathfrak{p}$ tels que $\bar{a}\bar{b} = \bar{0}$, c'est-à-dire $ab \in \mathfrak{p}$. Comme $\mathfrak{p}$ est premier, $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$, c'est-à-dire $\bar{a} = \bar{0}$ ou $\bar{b} = \bar{0}$. Donc $A/\mathfrak{p}$ est intègre.

($\Leftarrow$) Supposons $A/\mathfrak{p}$ intègre. En particulier $A/\mathfrak{p} \neq \{0\}$, donc $\mathfrak{p} \neq A$. Si $ab \in \mathfrak{p}$, alors $\bar{a}\bar{b} = \overline{ab} = \bar{0}$ dans $A/\mathfrak{p}$. Par intégrité, $\bar{a} = \bar{0}$ ou $\bar{b} = \bar{0}$, c'est-à-dire $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$. Donc $\mathfrak{p}$ est premier. □

Théorème 5.2 (Caractérisation des idéaux maximaux)**.** Soit A un anneau commutatif et $\mathfrak{m}$ un idéal de A. Alors :

$$\mathfrak{m} \text{ est maximal} \iff A/\mathfrak{m} \text{ est un corps.}$$

Démonstration. ($\Rightarrow$) Supposons $\mathfrak{m}$ maximal. Comme $\mathfrak{m} \neq A$, l'anneau quotient $A/\mathfrak{m}$ est non nul. Soit $\bar{a} \in A/\mathfrak{m}$, $\bar{a} \neq \bar{0}$, c'est-à-dire $a \notin \mathfrak{m}$. Considérons l'idéal $\mathfrak{m} + (a)$. Comme $a \notin \mathfrak{m}$, on a $\mathfrak{m} \subsetneq \mathfrak{m} + (a)$. Par maximalité, $\mathfrak{m} + (a) = A$. Il existe donc $m \in \mathfrak{m}$ et $b \in A$ tels que $m + ab = 1$. En passant au quotient, $\bar{a}\bar{b} = \bar{1}$, ce qui montre que $\bar{a}$ est inversible. Ainsi $A/\mathfrak{m}$ est un corps.

($\Leftarrow$) Supposons que $A/\mathfrak{m}$ est un corps. En particulier $A/\mathfrak{m} \neq \{0\}$, donc $\mathfrak{m} \neq A$. Soit I un idéal de A tel que $\mathfrak{m} \subsetneq I$. Il existe $a \in I \setminus \mathfrak{m}$, donc $\bar{a} \neq \bar{0}$ dans $A/\mathfrak{m}$. Comme $A/\mathfrak{m}$ est un corps, il existe $\bar{b}$ tel que $\bar{a}\bar{b} = \bar{1}$, c'est-à-dire $ab - 1 \in \mathfrak{m} \subseteq I$. Comme $a \in I$ et $ab \in I$, on obtient $1 = ab - (ab - 1) \in I$, d'où $I = A$. Ainsi $\mathfrak{m}$ est maximal. □

Corollaire 5.1 (Maximal implique premier)**.** Tout idéal maximal est premier.

Démonstration. Si $\mathfrak{m}$ est maximal, alors $A/\mathfrak{m}$ est un corps par le théorème 5.2. Or tout corps est intègre (un élément non nul est inversible, donc n'est pas diviseur de zéro par la proposition 5.2). Donc $A/\mathfrak{m}$ est intègre, et $\mathfrak{m}$ est premier par le théorème 5.1. □

Remarque 5.4. La réciproque est fausse en général : l'idéal (0) de $\mathbb{Z}$ est premier (car $\mathbb{Z}$ est intègre) mais n'est pas maximal (il est strictement contenu dans (2), par exemple).

Exemple 5.11 (Idéaux de $\mathbb{Z}/n\mathbb{Z}$)**.** Les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont de la forme $d\mathbb{Z}/n\mathbb{Z}$ où $d \mid n$. L'idéal $d\mathbb{Z}/n\mathbb{Z}$ est premier (resp. maximal) si et seulement si d est un nombre premier divisant n (auquel cas il est aussi maximal, car $(\mathbb{Z}/n\mathbb{Z})/(d\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/d\mathbb{Z}$ est un corps).

5.9 Treillis des idéaux de $\mathbb{Z}/12\mathbb{Z}$

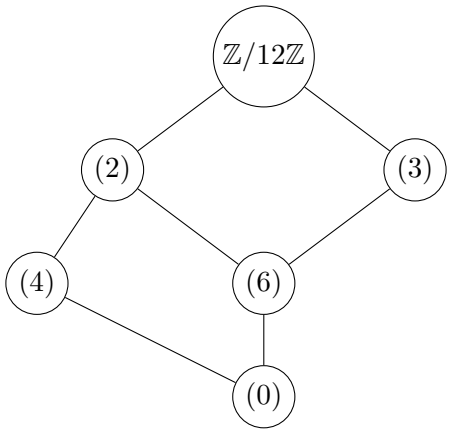


FIGURE 5.1 – Treillis des idéaux de $\mathbb{Z}/12\mathbb{Z}$. Les idéaux maximaux sont (2) et (3).

5.10 Exercices

Exercice 5.1. Montrer que dans un anneau A, l'élément unité est unique.

Exercice 5.2. Montrer que $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{R}$. Déterminer $U(\mathbb{Z}[\sqrt{2}])$.

Exercice 5.3. Soit A un anneau commutatif. Montrer que A est intègre si et seulement si pour tous $a, b, c \in A$ avec $a \neq 0$, l'égalité $ab = ac$ entraîne $b = c$ (propriété de simplification).

Exercice 5.4. Trouver tous les diviseurs de zéro dans $\mathbb{Z}/12\mathbb{Z}$.

Exercice 5.5. Soit A un anneau fini intègre. Montrer que A est un corps. *Indication : considérer l'application $x \mapsto ax$ pour $a \neq 0$.*

Exercice 5.6. Un élément a d'un anneau A est dit *nilpotent* s'il existe $n \geqslant 1$ tel que $a^n = 0$. Montrer que si a est nilpotent, alors $1 - a$ est inversible. *Indication : série géométrique finie.*

Exercice 5.7. Soit $\varphi\colon A \to B$ un morphisme d'anneaux. Montrer que si $\mathfrak{p}$ est un idéal premier de B, alors $\varphi^{-1}(\mathfrak{p})$ est un idéal premier de A.

Exercice 5.8. Montrer que l'intersection d'une famille quelconque d'idéaux est un idéal. L'union de deux idéaux est-elle toujours un idéal ?

Exercice 5.9. Déterminer tous les idéaux premiers et maximaux de $\mathbb{Z}/30\mathbb{Z}$.

Exercice 5.10. Soit A un anneau commutatif. Montrer que l'ensemble des éléments nilpotents de A, noté $\mathfrak{N}(A)$, est un idéal de A (le *nilradical*).

Exercice 5.11. Soit K un corps. Montrer que $K[X]/(X^2)$ est un anneau local (un seul idéal maximal). Déterminer les éléments inversibles et les éléments nilpotents.

Résumé du chapitre 5

- Un *anneau* $(A, +, \cdot)$ est un groupe abélien pour l'addition, muni d'une multiplication associative, unitaire et distributive.
- Un *anneau intègre* est un anneau commutatif non nul sans diviseurs de zéro. Le *groupe des unités* $U(A)$ est le groupe des éléments inversibles.
- Un *idéal* I d'un anneau commutatif A est un sous-groupe additif stable par multiplication par les éléments de A. Un idéal *principal* est engendré par un seul élément.
- Un idéal $\mathfrak{p}$ est *premier* si et seulement si $A/\mathfrak{p}$ est intègre. Un idéal $\mathfrak{m}$ est *maximal* si et seulement si $A/\mathfrak{m}$ est un corps.

— Tout idéal maximal est premier. La réciproque est fausse en général.

Chapitre 6

Anneaux quotients, domaines d'intégrité, corps de fractions

Introduction

Le passage au quotient, que nous avons rencontré dans le cadre des groupes, se transpose naturellement aux anneaux : pour former l'anneau quotient A/I, il faut et il suffit que I soit un idéal bilatère. Ce chapitre développe cette construction, établit les théorèmes d'isomorphisme pour les anneaux, puis étudie le théorème des restes chinois. Nous examinons ensuite la notion de caractéristique et construisons, pour tout anneau intègre, son corps de fractions — la plus petite extension dans laquelle tout élément non nul devient inversible.

6.1 Anneau quotient

Théorème 6.1 (Construction de l'anneau quotient)**.** Soit A un anneau (commutatif) et I un idéal de A. L'ensemble quotient $A/I = \{\bar{a} = a + I \mid a \in A\}$, muni des opérations :

$$\bar{a} + \bar{b} = \overline{a+b}, \qquad \bar{a} \cdot \bar{b} = \overline{ab},$$

est un anneau (commutatif), d'élément neutre additif $\bar{0}$ et d'élément unité $\bar{1}$. La surjection canonique $\pi \colon A \twoheadrightarrow A/I$, $a \mapsto \bar{a}$, est un morphisme d'anneaux de noyau I.

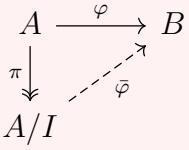
Démonstration. Il faut d'abord vérifier que la multiplication est *bien définie*. Soient $a, a', b, b' \in A$ tels que $\bar{a} = \bar{a}'$ et $\bar{b} = \bar{b}'$, c'est-à-dire $a - a' \in I$ et $b - b' \in I$. Alors :

$$ab - a'b' = ab - a'b + a'b - a'b' = (a - a')b + a'(b - b').$$

Comme I est un idéal, $(a - a')b \in I$ et $a'(b - b') \in I$, donc $ab - a'b' \in I$, c'est-à-dire $\overline{ab} = \overline{a'b'}$.

La vérification des axiomes d'anneau pour A/I est immédiate, car chaque axiome dans A/I se déduit de l'axiome correspondant dans A par passage au quotient. Enfin, π est clairement un morphisme d'anneaux surjectif, et $\operatorname{Ker}(\pi) = \{a \in A \mid \bar{a} = \bar{0}\} = I$. □

Théorème 6.2 (Propriété universelle du quotient)**.** Soient A un anneau, I un idéal de A et $\varphi\colon A \to B$ un morphisme d'anneaux tel que $I \subseteq \mathrm{Ker}(\varphi)$. Il existe un unique morphisme d'anneaux $\bar{\varphi}\colon A/I \to B$ tel que $\bar{\varphi} \circ \pi = \varphi$:



De plus, $\bar{\varphi}$ est injectif si et seulement si $I = \mathrm{Ker}(\varphi)$, et surjectif si et seulement si φ est surjectif.

Démonstration. Posons $\bar{\varphi}(\bar{a}) = \varphi(a)$. Cette définition est licite : si $\bar{a} = \bar{a}'$, alors $a - a' \in I \subseteq \mathrm{Ker}(\varphi)$, donc $\varphi(a) = \varphi(a')$. La vérification que $\bar{\varphi}$ est un morphisme d'anneaux est immédiate. L'unicité découle de la surjectivité de π.

On a $\mathrm{Ker}(\bar{\varphi}) = \{\bar{a} \mid \varphi(a) = 0\} = \mathrm{Ker}(\varphi)/I$. Donc $\bar{\varphi}$ est injectif si et seulement si $\mathrm{Ker}(\varphi) = I$. La surjectivité de $\bar{\varphi}$ équivaut clairement à celle de φ. □

6.2 Théorèmes d'isomorphisme pour les anneaux

Théorème 6.3 (Premier théorème d'isomorphisme)**.** Soit $\varphi\colon A \to B$ un morphisme d'anneaux. Alors :

$$A/\mathrm{Ker}(\varphi) \simeq \mathrm{Im}(\varphi).$$

Démonstration. On applique le théorème 6.2 avec $I = \mathrm{Ker}(\varphi)$. Le morphisme induit $\bar{\varphi}\colon A/\mathrm{Ker}(\varphi) \to B$ est injectif (car $I = \mathrm{Ker}(\varphi)$) et son image est $\mathrm{Im}(\varphi)$. □

Théorème 6.4 (Deuxième théorème d'isomorphisme)**.** Soit A un anneau commutatif, I et J des idéaux de A avec $I \subseteq J$. Alors J/I est un idéal de A/I et :

$$(A/I)/(J/I) \simeq A/J.$$

Démonstration. Considérons le morphisme composé $A \xrightarrow{\pi_I} A/I \xrightarrow{\pi_{J/I}} (A/I)/(J/I)$. C'est un morphisme d'anneaux surjectif de noyau J. Par le premier théorème d'isomorphisme, $(A/I)/(J/I) \simeq A/J$. □

Théorème 6.5 (Troisième théorème d'isomorphisme)**.** Soit A un anneau commutatif, I un idéal de A et B un sous-anneau de A. Alors $I \cap B$ est un idéal de B, $B + I$ est un sous-anneau de A contenant I comme idéal, et :

$$B/(I \cap B) \simeq (B + I)/I.$$

Démonstration. Le morphisme $B \hookrightarrow A \xrightarrow{\pi} A/I$ a pour noyau $B \cap I$ et pour image $\{b + I \mid b \in B\} = (B + I)/I$. On conclut par le premier théorème d'isomorphisme. □

6.3 Théorème des restes chinois

Théorème 6.6 (Théorème des restes chinois)**.** Soient $m, n \geqslant 1$ des entiers tels que $\operatorname{pgcd}(m, n) = 1$. Alors :

$$\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Démonstration. Considérons le morphisme d'anneaux :

$$\varphi\colon \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \qquad a \longmapsto (\bar{a}_m, \bar{a}_n),$$

où $\bar{a}_m$ désigne la classe de a modulo m.

Noyau. On a $a \in \operatorname{Ker}(\varphi)$ si et seulement si $m \mid a$ et $n \mid a$. Comme $\operatorname{pgcd}(m, n) = 1$, cela équivaut à $mn \mid a$, d'où $\operatorname{Ker}(\varphi) = mn\mathbb{Z}$.

Surjectivité. Comme $\operatorname{pgcd}(m, n) = 1$, il existe $u, v \in \mathbb{Z}$ tels que $um + vn = 1$ (identité de Bézout). Pour tout $(\bar{r}_m, \bar{s}_n) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, posons $a = s \cdot um + r \cdot vn$. Alors :

$$a \equiv r \cdot vn \equiv r \cdot (1 - um) \equiv r \pmod{m}, \qquad a \equiv s \cdot um \equiv s \cdot (1 - vn) \equiv s \pmod{n}.$$

Donc $\varphi(a) = (\bar{r}_m, \bar{s}_n)$, et φ est surjectif.

Par le premier théorème d'isomorphisme (théorème 6.3) :

$$\mathbb{Z}/mn\mathbb{Z} = \mathbb{Z}/\operatorname{Ker}(\varphi) \simeq \operatorname{Im}(\varphi) = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}. \qquad \square$$

Théorème 6.7 (Théorème des restes chinois — version générale)**.** Soit A un anneau commutatif et $I_1, \ldots, I_k$ des idéaux de A deux à deux *comaximaux*, c'est-à-dire $I_i + I_j = A$ pour $i \neq j$. Alors :

$$A \Big/ \bigcap_{i=1}^{k} I_i \;\simeq\; \prod_{i=1}^{k} A/I_i,$$

et de plus $\bigcap_{i=1}^{k} I_i = I_1 I_2 \cdots I_k$.

Démonstration. Le morphisme canonique $\varphi\colon A \to \prod_{i=1}^{k} A/I_i$, $a \mapsto (\bar{a}_1, \ldots, \bar{a}_k)$, a pour noyau $\bigcap_i I_i$. Montrons la surjectivité par récurrence sur k.

Pour $k = 2$: comme $I_1 + I_2 = A$, il existe $a_1 \in I_1$, $a_2 \in I_2$ avec $a_1 + a_2 = 1$. L'élément $e_1 = a_2$ satisfait $e_1 \equiv 1 \pmod{I_1}$ et $e_1 \equiv 0 \pmod{I_2}$ (car $e_1 = 1 - a_1$ et $a_1 \in I_1$; et $e_1 = a_2 \in I_2$). Corrigeons : $e_1 = a_2 \in I_2$ donc $e_1 \equiv 0 \pmod{I_2}$, et $e_1 = 1 - a_1$ avec $a_1 \in I_1$ donc $e_1 \equiv 1 \pmod{I_1}$. De même $e_2 = a_1$ satisfait $e_2 \equiv 0 \pmod{I_1}$ et $e_2 \equiv 1 \pmod{I_2}$. Pour $(r_1, r_2) \in A/I_1 \times A/I_2$, l'élément $x = r_1 e_1 + r_2 e_2$ satisfait $\varphi(x) = (r_1, r_2)$.

Montrons aussi que $I_1 \cap I_2 = I_1 I_2$. On a toujours $I_1 I_2 \subseteq I_1 \cap I_2$. Réciproquement, si $x \in I_1 \cap I_2$, alors $x = x \cdot 1 = x(a_1 + a_2) = xa_1 + xa_2$. Or $xa_1 \in I_2 I_1$ (car $x \in I_2$) et $xa_2 \in I_1 I_2$ (car $x \in I_1$), donc $x \in I_1 I_2$.

Le cas général $k \geqslant 3$ se traite par récurrence en montrant que I_1 et $I_2 \cdots I_k$ sont comaximaux (exercice). $\square$

6.4 Anneau intègre et caractéristique

Proposition 6.1 (Propriété de simplification)**.** Soit A un anneau commutatif. Alors A est intègre si et seulement si pour tous $a, b, c \in A$ avec $a \neq 0$:

$$ab = ac \implies b = c.$$

Démonstration. ($\Rightarrow$) $ab = ac \implies a(b-c) = 0 \implies b - c = 0$ (car $a \neq 0$ et A intègre).
($\Leftarrow$) Si $ab = 0$ avec $a \neq 0$, alors $ab = a \cdot 0$, d'où $b = 0$ par simplification. □

Définition 6.1 (Caractéristique)**.** Soit A un anneau. La *caractéristique* de A, notée $\mathrm{car}(A)$, est l'ordre de 1_A dans le groupe additif $(A, +)$: c'est le plus petit entier $n \geqslant 1$ tel que $n \cdot 1_A = 0$, ou 0 si aucun tel entier n'existe.
De manière équivalente, l'unique morphisme d'anneaux $\mathbb{Z} \to A$, $n \mapsto n \cdot 1_A$, a pour noyau $\mathrm{car}(A) \cdot \mathbb{Z}$.

Proposition 6.2. La caractéristique d'un anneau intègre est 0 ou un nombre premier.

Démonstration. Soit A intègre avec $\mathrm{car}(A) = n > 0$. Supposons $n = ab$ avec $1 < a, b < n$. Alors $0 = n \cdot 1_A = (a \cdot 1_A)(b \cdot 1_A)$ dans A. Par intégrité, $a \cdot 1_A = 0$ ou $b \cdot 1_A = 0$, ce qui contredit la minimalité de n. Donc n est premier. □

6.5 Corps de fractions

6.5.1 Construction

Théorème 6.8 (Corps de fractions)**.** Soit A un anneau commutatif intègre. Il existe un corps K, unique à isomorphisme unique près, et un morphisme injectif d'anneaux $\iota \colon A \hookrightarrow K$, tels que tout élément de K s'écrive $\iota(a) \cdot \iota(b)^{-1}$ avec $a \in A$, $b \in A \setminus \{0\}$. Le corps K est appelé le *corps de fractions* de A et noté $\mathrm{Frac}(A)$.

Démonstration. Construction. Posons $S = A \times (A \setminus \{0\})$ et définissons sur S la relation :

$$(a, b) \sim (c, d) \iff ad = bc.$$

Étape 1 : $\sim$ est une relation d'équivalence. La réflexivité ($ab = ba$) et la symétrie sont claires. Pour la transitivité, supposons $(a, b) \sim (c, d)$ et $(c, d) \sim (e, f)$, c'est-à-dire $ad = bc$ et $cf = de$. Alors :

$$adf = bcf = bde, \quad \text{d'où} \quad d(af - be) = 0.$$

Comme $d \neq 0$ et A intègre, $af = be$, c'est-à-dire $(a, b) \sim (e, f)$.

Notons $\dfrac{a}{b}$ la classe de (a, b) et $K = S/\!\sim$.

Étape 2 : opérations sur K. Définissons :

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Notons que $bd \neq 0$ par intégrité de A.

Étape 3 : bonne définition. Vérifions pour la multiplication. Soient $(a,b) \sim (a',b')$ et $(c,d) \sim (c',d')$, c'est-à-dire $ab' = a'b$ et $cd' = c'd$. Alors :

$$(ac)(b'd') = (ab')(cd') = (a'b)(c'd) = (a'c')(bd),$$

donc $(ac, bd) \sim (a'c', b'd')$. La vérification pour l'addition est analogue : $(ad+bc)(b'd') = adb'd' + bcb'd' = a'dbd' + b \cdot c'd \cdot b' \cdot 1$. Développons plus soigneusement :

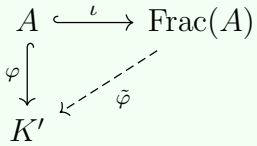
$$\begin{aligned}(ad+bc)(b'd') &= adb'd' + bcb'd' \\ (a'd'+b'c')(bd) &= a'd'bd + b'c'bd.\end{aligned}$$

Or $ab' = a'b$ donne $adb'd' = a'bdd' = a'd'bd$, et $cd' = c'd$ donne $bcb'd' = bb'cd' = bb'c'd = b'c'bd$. Donc les deux expressions sont égales.

Étape 4 : K est un corps. L'élément neutre additif est $\frac{0}{1}$, l'opposé de $\frac{a}{b}$ est $\frac{-a}{b}$, et l'élément unité est $\frac{1}{1}$. La vérification de l'associativité, de la commutativité et de la distributivité est directe (et fastidieuse). Si $\frac{a}{b} \neq \frac{0}{1}$, c'est-à-dire $a \neq 0$, alors $\frac{b}{a} \in K$ et $\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{1}{1}$. Donc tout élément non nul est inversible : K est un corps.

Étape 5 : plongement de A dans K. Le morphisme $\iota \colon A \to K$, $a \mapsto \frac{a}{1}$, est un morphisme d'anneaux injectif. En effet, $\frac{a}{1} = \frac{0}{1}$ si et seulement si $a \cdot 1 = 0 \cdot 1$, c'est-à-dire $a = 0$. □

Proposition 6.3 (Propriété universelle du corps de fractions)**.** Soit A un anneau intègre et $\iota \colon A \hookrightarrow \mathrm{Frac}(A)$ le plongement canonique. Pour tout morphisme injectif d'anneaux $\varphi \colon A \hookrightarrow K'$ où K' est un corps, il existe un unique morphisme d'anneaux $\tilde{\varphi} \colon \mathrm{Frac}(A) \to K'$ tel que $\tilde{\varphi} \circ \iota = \varphi$:



Démonstration. Posons $\tilde{\varphi}\left(\frac{a}{b}\right) = \varphi(a) \cdot \varphi(b)^{-1}$. Comme φ est injectif et $b \neq 0$, on a $\varphi(b) \neq 0$, donc $\varphi(b)^{-1}$ existe dans le corps K'.

Bonne définition. Si $\frac{a}{b} = \frac{c}{d}$, alors $ad = bc$, d'où $\varphi(a)\varphi(d) = \varphi(b)\varphi(c)$, d'où $\varphi(a)\varphi(b)^{-1} = \varphi(c)\varphi(d)^{-1}$ (en multipliant à droite par $\varphi(d)^{-1}$ et à gauche par $\varphi(b)^{-1}$).

La vérification que $\tilde{\varphi}$ est un morphisme d'anneaux est directe. L'unicité résulte du fait que tout élément de $\mathrm{Frac}(A)$ s'écrit $\iota(a)\iota(b)^{-1}$, et un morphisme d'anneaux préserve les inverses. □

Exemple 6.1 (Corps de fractions classiques)**.** (a) $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$.

(b) $\mathrm{Frac}(K[X]) = K(X)$, le corps des fractions rationnelles à coefficients dans K.

(c) $\mathrm{Frac}(\mathbb{Z}[i]) = \mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\} = \mathbb{Q}(i)$.

6.6 Exercices

Exercice 6.1. Montrer que $\mathbb{Z}[i]/(1+i) \simeq \mathbb{Z}/2\mathbb{Z}$. *Indication : utiliser le morphisme* $\mathbb{Z} \to \mathbb{Z}[i]/(1+i)$.

Exercice 6.2. Montrer que si p est premier, l'anneau $\mathbb{Z}/p\mathbb{Z}$ n'a aucun idéal non trivial.

Exercice 6.3. Soit K un corps et $a \in K$. Montrer que l'application d'évaluation $\mathrm{ev}_a \colon K[X] \to K$, $P \mapsto P(a)$, est un morphisme d'anneaux surjectif de noyau $(X-a)$. En déduire que $K[X]/(X-a) \simeq K$.

Exercice 6.4. Montrer que $\mathbb{R}[X]/(X^2+1) \simeq \mathbb{C}$.

Exercice 6.5. Appliquer le théorème des restes chinois pour décrire la structure de $\mathbb{Z}/60\mathbb{Z}$ comme produit d'anneaux.

Exercice 6.6. Soit A un anneau intègre de caractéristique $p > 0$. Montrer que l'application de Frobenius $F \colon A \to A$, $a \mapsto a^p$, est un morphisme d'anneaux injectif.

Exercice 6.7. Construire le corps de fractions de $\mathbb{Z}[\sqrt{-3}]$ et le décrire explicitement.

Exercice 6.8. Montrer que dans un anneau intègre, la caractéristique est 0 ou un nombre premier (redemonstration directe, sans utiliser la proposition 6.2).

Exercice 6.9. Soient I, J des idéaux d'un anneau commutatif A avec $I + J = A$. Montrer que $I^m + J^n = A$ pour tous $m, n \geqslant 1$.

Exercice 6.10. Soit $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ la décomposition de n en facteurs premiers. Montrer que :

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}.$$

En déduire l'expression de $\varphi(n)$ (indicatrice d'Euler).

Exercice 6.11. Montrer que l'anneau $\mathbb{Z}[\sqrt{-5}]$ est intègre. Déterminer son corps de fractions.

Résumé du chapitre 6

- L'anneau quotient A/I est bien défini lorsque I est un idéal, et la surjection canonique $\pi \colon A \to A/I$ vérifie une propriété universelle.
- Les théorèmes d'isomorphisme pour les anneaux sont les analogues exacts de ceux pour les groupes.
- Le théorème des restes chinois : si $\mathrm{pgcd}(m,n) = 1$, alors $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.
- La caractéristique d'un anneau intègre est 0 ou un nombre premier.

— Pour tout anneau intègre A, le corps de fractions $\mathrm{Frac}(A)$ est le plus petit corps contenant A. Sa construction repose sur des classes d'équivalence de couples (a, b) avec $b \neq 0$.

Chapitre 7

Anneaux principaux, euclidiens et factoriels

Introduction

L'un des résultats les plus fondamentaux de l'arithmétique élémentaire est le *théorème fondamental de l'arithmétique* : tout entier $n \geqslant 2$ se décompose de manière essentiellement unique en produit de nombres premiers. Ce résultat, tenu pour évident pendant des siècles, s'est révélé d'une subtilité inattendue lorsque les mathématiciens ont cherché à l'étendre à d'autres anneaux. Kummer et Dedekind ont découvert que la factorisation unique peut *échouer* dans certains anneaux d'entiers algébriques, ce qui a conduit à l'invention des idéaux et, ultimement, à la théorie que nous développons ici.

Ce chapitre classifie les anneaux intègres selon la qualité de leur arithmétique : anneaux euclidiens, principaux, factoriels. Nous établissons les implications :

$$\text{corps} \subset \text{euclidien} \subset \text{principal} \subset \text{factoriel} \subset \text{intègre}$$

et démontrons que chaque inclusion est stricte.

7.1 Divisibilité dans un anneau intègre

Définition 7.1 (Divisibilité, éléments associés)**.** Soit A un anneau commutatif intègre et $a, b \in A$.

(i) On dit que a *divise* b (noté $a \mid b$) s'il existe $c \in A$ tel que $b = ac$.

(ii) Les éléments a et b sont *associés* (noté $a \sim b$) s'il existe $u \in U(A)$ tel que $b = ua$, ce qui équivaut à $a \mid b$ et $b \mid a$.

Remarque 7.1. Dans un anneau commutatif intègre A, on a $a \mid b \iff (b) \subseteq (a)$, et $a \sim b \iff (a) = (b)$.

Définition 7.2 (Élément irréductible)**.** Soit A un anneau intègre. Un élément $p \in A$ est *irréductible* si :

(i) $p \neq 0$ et $p \notin U(A)$.

(ii) Si $p = ab$, alors $a \in U(A)$ ou $b \in U(A)$.

Définition 7.3 (Élément premier)**.** Soit A un anneau intègre. Un élément $p \in A$ est *premier* si :

(i) $p \neq 0$ et $p \notin U(A)$.

(ii) Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$.

De manière équivalente, p est premier si et seulement si l'idéal (p) est un idéal premier non nul de A.

Lemme 7.1 (Premier implique irréductible)**.** Dans tout anneau intègre, un élément premier est irréductible.

Démonstration. Soit p premier dans un anneau intègre A. Supposons $p = ab$. Alors $p \mid ab$, donc $p \mid a$ ou $p \mid b$.

Cas 1 : $p \mid a$. Il existe $c \in A$ tel que $a = pc$. Alors $p = ab = pcb$, d'où $p(1 - cb) = 0$. Comme $p \neq 0$ et A intègre, $cb = 1$, donc $b \in U(A)$.

Cas 2 : $p \mid b$. Par un argument symétrique, $a \in U(A)$.

Dans les deux cas, $a \in U(A)$ ou $b \in U(A)$, donc p est irréductible. □

Remarque 7.2. La réciproque est fausse en général. Dans $\mathbb{Z}[\sqrt{-5}]$, l'élément 2 est irréductible mais pas premier : on a $2 \mid 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, mais $2 \nmid (1 + \sqrt{-5})$ et $2 \nmid (1 - \sqrt{-5})$.

7.2 Anneaux principaux

Définition 7.4 (Anneau principal)**.** Un anneau commutatif intègre A est un *anneau principal* (ou un *domaine d'idéaux principaux*, abrégé en PID) si tout idéal de A est principal, c'est-à-dire si pour tout idéal I de A, il existe $a \in A$ tel que $I = (a)$.

Exemple 7.1. Les anneaux $\mathbb{Z}$ et $K[X]$ (pour K corps) sont des anneaux principaux (exemples 5.8 et 5.9).

Théorème 7.1 (Dans un PID, irréductible $\iff$ premier)**.** Soit A un anneau principal et $p \in A$. Alors :

$$p \text{ est irréductible} \iff p \text{ est premier.}$$

Démonstration. ($\Leftarrow$) C'est le lemme 7.1, valable dans tout anneau intègre.

($\Rightarrow$) Soit p irréductible et supposons $p \mid ab$. Comme A est principal, l'idéal (p, a) est principal : il existe $d \in A$ tel que $(p, a) = (d)$. En particulier $d \mid p$, donc $p = du$ avec $u \in A$.

Comme p est irréductible, $d \in U(A)$ ou $u \in U(A)$.

Cas 1 : $u \in U(A)$, c'est-à-dire $d \sim p$. Alors $(d) = (p)$, donc $a \in (p)$, c'est-à-dire $p \mid a$.

Cas 2 : $d \in U(A)$. Alors $(d) = A$, donc $(p, a) = A$. Il existe $x, y \in A$ tels que $px + ay = 1$. En multipliant par b : $pbx + aby = b$. Or $p \mid ab$ donne $p \mid aby$, et $p \mid pbx$. Donc $p \mid b$.

Dans les deux cas, $p \mid a$ ou $p \mid b$, donc p est premier. □

7.3 Anneaux euclidiens

Définition 7.5 (Anneau euclidien)**.** Un anneau commutatif intègre A est *euclidien* s'il existe une application $v \colon A \setminus \{0\} \to \mathbb{N}$ (appelée *stathme* ou *fonction euclidienne*) telle que pour tous $a \in A$ et $b \in A \setminus \{0\}$, il existe $q, r \in A$ vérifiant :

$$a = bq + r, \qquad r = 0 \text{ ou } v(r) < v(b).$$

Théorème 7.2 (Euclidien implique principal)**.** Tout anneau euclidien est un anneau principal.

Démonstration. Soit A un anneau euclidien de stathme v et I un idéal non nul de A. Choisissons $b \in I \setminus \{0\}$ tel que $v(b)$ soit minimal parmi les valeurs de v sur $I \setminus \{0\}$. Montrons que $I = (b)$.

L'inclusion $(b) \subseteq I$ est claire car $b \in I$ et I est un idéal. Réciproquement, soit $a \in I$. Par division euclidienne, il existe $q, r \in A$ tels que $a = bq + r$ avec $r = 0$ ou $v(r) < v(b)$. Or $r = a - bq \in I$ (car $a \in I$ et $bq \in I$). Si $r \neq 0$, alors $v(r) < v(b)$, ce qui contredit la minimalité de $v(b)$ dans $I \setminus \{0\}$. Donc $r = 0$ et $a = bq \in (b)$.

Ainsi $I = (b)$ est principal. □

Exemple 7.2 (Anneaux euclidiens classiques)**.**
(a) $\mathbb{Z}$ est euclidien pour le stathme $v(n) = |n|$.
(b) $K[X]$ (K corps) est euclidien pour le stathme $v(P) = \deg(P)$.
(c) Les entiers de Gauss $\mathbb{Z}[i]$ sont euclidiens pour le stathme $v(a + bi) = a^2 + b^2$ (la norme).

Théorème 7.3 ($\mathbb{Z}[i]$ est euclidien)**.** L'anneau $\mathbb{Z}[i]$ est euclidien pour le stathme $N \colon \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N}^*$ défini par $N(a + bi) = a^2 + b^2$.

Démonstration. Notons d'abord que N est *multiplicative* : $N(\alpha\beta) = N(\alpha)N(\beta)$ pour tous $\alpha, \beta \in \mathbb{Z}[i]$ (vérification directe par calcul).

Soient $\alpha, \beta \in \mathbb{Z}[i]$ avec $\beta \neq 0$. Considérons le quotient $\alpha/\beta \in \mathbb{Q}(i)$:

$$\frac{\alpha}{\beta} = \frac{\alpha\bar{\beta}}{|\beta|^2} = u + vi$$

avec $u, v \in \mathbb{Q}$. Choisissons $p, q \in \mathbb{Z}$ tels que $|u - p| \leqslant \frac{1}{2}$ et $|v - q| \leqslant \frac{1}{2}$. Posons $\gamma = p + qi \in \mathbb{Z}[i]$ et $\rho = \alpha - \beta\gamma \in \mathbb{Z}[i]$. Alors :

$$\frac{\rho}{\beta} = \frac{\alpha}{\beta} - \gamma = (u - p) + (v - q)i.$$

Par conséquent :

$$N(\rho) = N(\beta) \cdot N\left(\frac{\rho}{\beta}\right) = N(\beta)\big((u-p)^2 + (v-q)^2\big) \leqslant N(\beta)\left(\frac{1}{4} + \frac{1}{4}\right) = \frac{N(\beta)}{2} < N(\beta).$$

Donc $\alpha = \beta\gamma + \rho$ avec $\rho = 0$ ou $N(\rho) < N(\beta)$, ce qui montre que $\mathbb{Z}[i]$ est euclidien. □

7.4 Échec de la factorisation unique : $\mathbb{Z}[\sqrt{-5}]$

Proposition 7.1. L'anneau $\mathbb{Z}[\sqrt{-5}]$ n'est pas factoriel.

Démonstration. Considérons la norme $N\colon \mathbb{Z}[\sqrt{-5}] \to \mathbb{N}$ définie par $N(a + b\sqrt{-5}) = a^2 + 5b^2$. Cette norme est multiplicative : $N(\alpha\beta) = N(\alpha)N(\beta)$.

Étape 1 : les éléments 2, 3, $1 + \sqrt{-5}$, $1 - \sqrt{-5}$ *sont irréductibles.*

Pour 2 : $N(2) = 4$. Si $2 = \alpha\beta$, alors $N(\alpha)N(\beta) = 4$. Les diviseurs possibles de 4 dans $\mathbb{N}$ sont $1, 2, 4$. Or $N(a+b\sqrt{-5}) = 2$ exigerait $a^2+5b^2 = 2$, ce qui n'a aucune solution dans $\mathbb{Z}$ (si $b \neq 0$, $a^2+5b^2 \geqslant 5$; si $b = 0$, $a^2 = 2$ est impossible dans $\mathbb{Z}$). Donc dans la décomposition $2 = \alpha\beta$, l'un des facteurs a norme 1 (donc est une unité, car $U(\mathbb{Z}[\sqrt{-5}]) = \{\pm 1\}$ puisque $a^2 + 5b^2 = 1$ impose $b = 0$, $a = \pm 1$). Ainsi 2 est irréductible.

Le même argument s'applique à 3 ($N(3) = 9$, et $a^2 + 5b^2 = 3$ n'a pas de solution) et à $1 \pm \sqrt{-5}$ ($N(1 \pm \sqrt{-5}) = 6$, et $a^2 + 5b^2 = 2$ ou 3 n'a pas de solution).

Étape 2 : deux factorisations distinctes de 6.

On a :

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Ce sont deux factorisations en irréductibles. Elles sont essentiellement distinctes car 2 n'est pas associé à 3, $1 + \sqrt{-5}$ ou $1 - \sqrt{-5}$ (les seules unités sont ± 1, et par exemple $2 \neq \pm(1 + \sqrt{-5})$).

Ainsi la factorisation n'est pas unique : $\mathbb{Z}[\sqrt{-5}]$ n'est pas factoriel. □

7.5 Anneaux factoriels

Définition 7.6 (Anneau factoriel)**.** Un anneau commutatif intègre A est *factoriel* (ou est un *domaine de factorisation unique*, abrégé en UFD) si :

(F1) **Existence** : tout élément $a \in A \setminus (\{0\} \cup U(A))$ s'écrit comme un produit fini d'éléments irréductibles : $a = p_1 p_2 \cdots p_n$.

(F2) **Unicité** : si $p_1 \cdots p_m = q_1 \cdots q_n$ sont deux factorisations en irréductibles, alors $m = n$ et, quitte à réordonner, $p_i \sim q_i$ pour tout i.

Théorème 7.4 (PID implique UFD)**.** Tout anneau principal est factoriel.

Démonstration. Soit A un anneau principal. Nous devons démontrer l'existence et l'unicité de la factorisation.

Existence de la factorisation. Supposons par l'absurde qu'il existe un élément $a \in A \setminus (\{0\} \cup U(A))$ qui ne s'écrit pas comme produit d'irréductibles. Comme a n'est pas

irréductible, on peut écrire $a = a_1 b_1$ avec $a_1, b_1 \notin U(A)$ et $a_1, b_1 \neq 0$. Au moins l'un des deux, disons a_1, ne s'écrit pas comme produit d'irréductibles (sinon $a = a_1 b_1$ serait un tel produit). De plus, $(a) \subsetneq (a_1)$ car $a_1 \mid a$ mais $a_1 \nmid a$ impliquerait $b_1 \in U(A)$, contradiction. Corrigeons : on a $(a) \subsetneq (a_1)$ car $a = a_1 b_1 \in (a_1)$ donc $(a) \subseteq (a_1)$, et si $(a) = (a_1)$, alors $a_1 = au$ pour un $u \in A$, d'où $a = a_1 b_1 = a u b_1$, donc $u b_1 = 1$, c'est-à-dire $b_1 \in U(A)$, contradiction.

En itérant, on construit une chaîne strictement croissante d'idéaux :

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots$$

Posons $J = \bigcup_{n \geqslant 0} (a_n)$ (avec $a_0 = a$). Alors J est un idéal de A : si $x, y \in J$, il existe n tel que $x, y \in (a_n)$, donc $x - y \in (a_n) \subseteq J$; et si $c \in A$, $cx \in (a_n) \subseteq J$. Comme A est principal, $J = (d)$ pour un $d \in A$. Or $d \in J$, donc $d \in (a_N)$ pour un certain N, d'où $(d) \subseteq (a_N)$. Mais $(a_N) \subseteq J = (d)$, donc $(a_N) = (d) = J$. Cela entraîne $(a_{N+1}) \subseteq J = (a_N)$, ce qui contredit $(a_N) \subsetneq (a_{N+1})$.

Cette contradiction prouve que tout élément non nul et non inversible admet une décomposition en produit d'irréductibles.

Unicité de la factorisation. Soient $p_1 \cdots p_m = q_1 \cdots q_n$ deux factorisations en irréductibles. Comme A est principal, tout irréductible est premier (théorème 7.1). Procédons par récurrence sur m.

Cas $m = 1$: $p_1 = q_1 \cdots q_n$. Comme p_1 est irréductible, $n = 1$ et $p_1 = q_1$ (ils sont associés car le quotient est une unité, mais ici l'égalité directe donne $p_1 \sim q_1$).

Pas de récurrence : supposons le résultat vrai pour $m-1$. L'élément p_1 divise $q_1 \cdots q_n$. Comme p_1 est premier, il divise l'un des q_j. Quitte à réordonner, $p_1 \mid q_1$. Comme q_1 est irréductible et $p_1 \notin U(A)$, on a $q_1 = u p_1$ avec $u \in U(A)$, c'est-à-dire $p_1 \sim q_1$.

Alors $p_1 p_2 \cdots p_m = u p_1 q_2 \cdots q_n$. Par simplification (l'anneau est intègre), $p_2 \cdots p_m = u q_2 \cdots q_n$. En remplaçant q_2 par $u q_2$ (qui est encore irréductible et associé à q_2), on obtient une factorisation $p_2 \cdots p_m = q_2' q_3 \cdots q_n$ en $m-1$ et $n-1$ irréductibles. Par hypothèse de récurrence, $m - 1 = n - 1$ et, quitte à réordonner, $p_i \sim q_i$ pour $i \geqslant 2$. Donc $m = n$ et $p_i \sim q_i$ pour tout i. □

7.6 Lemme de Gauss et polynômes sur un UFD

Définition 7.7 (Contenu d'un polynôme)**.** Soit A un anneau factoriel et $f = a_0 + a_1 X + \cdots + a_n X^n \in A[X]$ un polynôme non nul. Le *contenu* de f, noté $c(f)$, est le pgcd des coefficients $a_0, a_1, \ldots, a_n$ (défini à association près). Le polynôme f est dit *primitif* si $c(f) \sim 1$, c'est-à-dire si les coefficients de f sont premiers entre eux dans leur ensemble.

Lemme 7.2 (Lemme de Gauss)**.** Soit A un anneau factoriel et $f, g \in A[X]$ deux polynômes non nuls. Alors :

$$c(fg) \sim c(f) \cdot c(g).$$

En particulier, le produit de deux polynômes primitifs est primitif.

Démonstration. En écrivant $f = c(f) f_0$ et $g = c(g) g_0$ avec f_0, g_0 primitifs, on a $fg = c(f)c(g) f_0 g_0$. Il suffit donc de montrer que si f et g sont primitifs, alors fg est primitif.

Supposons par l'absurde que fg n'est pas primitif. Alors il existe un élément irréductible $p \in A$ qui divise tous les coefficients de fg. Comme A est factoriel (et en particulier un anneau intègre), l'idéal (p) est premier (car dans un UFD, tout irréductible est premier — ce que nous montrerons ci-dessous, ou utilisons directement le fait que A est un UFD). Considérons la réduction modulo p : $\bar{f}, \bar{g} \in (A/(p))[X]$, avec $\bar{f}\bar{g} = \bar{0}$.

Comme p est premier, $A/(p)$ est intègre, donc $(A/(p))[X]$ est intègre. Ainsi $\bar{f} = \bar{0}$ ou $\bar{g} = \bar{0}$, c'est-à-dire p divise tous les coefficients de f ou de g. Cela contredit le fait que f et g sont primitifs. □

Remarque 7.3. Dans un anneau factoriel, tout élément irréductible est premier. En effet, soit p irréductible et $p \mid ab$, disons $pc = ab$. En décomposant a, b, c en irréductibles et par unicité de la factorisation, p apparaît parmi les facteurs irréductibles de ab, donc parmi ceux de a ou de b, c'est-à-dire $p \mid a$ ou $p \mid b$.

Théorème 7.5 (A UFD implique $A[X]$ UFD)**.** Si A est un anneau factoriel, alors $A[X]$ est un anneau factoriel.

Esquisse de preuve. Notons $K = \mathrm{Frac}(A)$. Comme K est un corps, $K[X]$ est euclidien, donc factoriel.

Existence. Soit $f \in A[X]$ non nul, non inversible. On écrit $f = c(f) \cdot f_0$ avec f_0 primitif. Le facteur $c(f) \in A$ se décompose en irréductibles de A (qui restent irréductibles dans $A[X]$). Pour f_0, on le factorise dans $K[X]$ en irréductibles ; par le lemme de Gauss, on ramène ces facteurs à des polynômes primitifs de $A[X]$, qui sont irréductibles dans $A[X]$.

Unicité. Si $p_1 \cdots p_m = q_1 \cdots q_n$ dans $A[X]$, on sépare les facteurs constants (irréductibles de A) des facteurs de degré $\geqslant 1$. L'unicité pour les facteurs constants provient de celle dans A ; pour les facteurs de degré $\geqslant 1$, on passe dans $K[X]$ et on utilise l'unicité dans $K[X]$ combinée au lemme de Gauss. □

7.7 Hiérarchie des anneaux

Le diagramme suivant résume les inclusions entre les différentes classes d'anneaux étudiées :

7.8 Contre-exemple : PID non euclidien

Théorème 7.6. L'anneau $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ est un anneau principal qui n'est pas euclidien.

Remarque 7.4. La preuve que cet anneau est principal mais non euclidien est non triviale. La principalité découle de la théorie des formes quadratiques binaires : le nombre de classes de l'ordre $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ (qui est l'anneau des entiers de $\mathbb{Q}(\sqrt{-19})$) est 1, ce qui signifie que tout idéal est principal. Pour la non-existence d'un stathme euclidien, on montre qu'il n'existe pas de "plus petit élément non inversible au sens de tout stathme possible". Nous renvoyons à [1] ou [4] pour les détails.

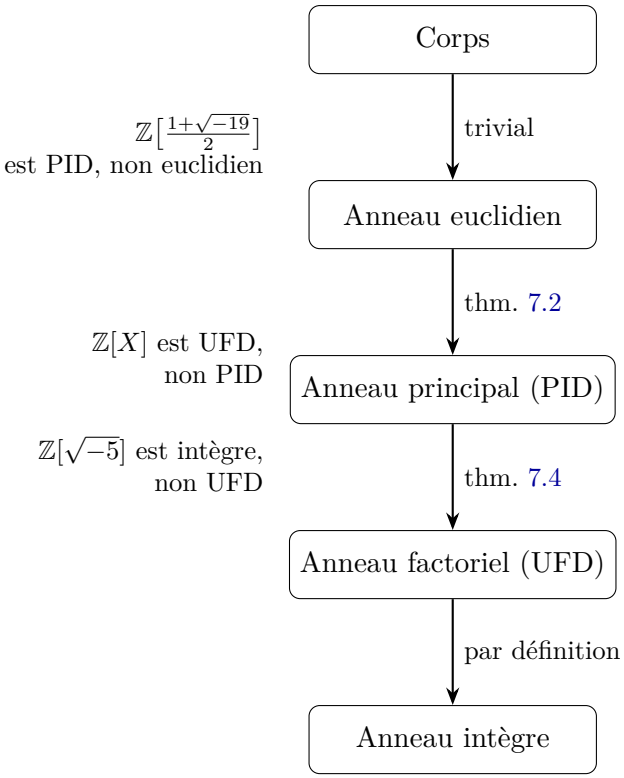


FIGURE 7.1 – Hiérarchie des anneaux commutatifs intègres. Chaque inclusion est stricte.

7.9 Critère d'irréductibilité d'Eisenstein

Théorème 7.7 (Critère d'Eisenstein)**.** Soit A un anneau factoriel et $f = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in A[X]$ un polynôme de degré $n \geqslant 1$. S'il existe un élément irréductible $p \in A$ tel que :

(i) $p \nmid a_n$,

(ii) $p \mid a_i$ pour tout $0 \leqslant i \leqslant n-1$,

(iii) $p^2 \nmid a_0$,

alors f est irréductible dans $A[X]$ (et dans $K[X]$ si f est primitif, où $K = \mathrm{Frac}(A)$).

Démonstration. Supposons par l'absurde que $f = gh$ dans $A[X]$ avec $\deg(g) = r \geqslant 1$ et $\deg(h) = s \geqslant 1$, $r + s = n$. Écrivons $g = b_r X^r + \cdots + b_0$ et $h = c_s X^s + \cdots + c_0$. Alors $a_0 = b_0 c_0$ et $a_n = b_r c_s$.

Réduisons modulo p. Les conditions (i) et (ii) donnent $\bar{f} = \bar{a}_n X^n$ dans $(A/(p))[X]$. Comme p est irréductible dans l'UFD A, l'idéal (p) est premier, et $A/(p)$ est intègre. De $\bar{f} = \bar{g}\bar{h}$, on déduit $\bar{a}_n X^n = \bar{g} \cdot \bar{h}$ dans l'anneau intègre $(A/(p))[X]$.

Par unicité de la factorisation dans $(A/(p))[X]$ (c'est un domaine intègre, et X est irréductible — en fait, on utilise simplement que $(A/(p))[X]$ est intègre et que X^n ne se factorise qu'en puissances de X à unité près), on obtient $\bar{g} = \bar{b}_r X^r$ et $\bar{h} = \bar{c}_s X^s$. En particulier, $\bar{b}_0 = 0$ et $\bar{c}_0 = 0$, c'est-à-dire $p \mid b_0$ et $p \mid c_0$. Mais alors $p^2 \mid b_0 c_0 = a_0$, ce qui contredit (iii). □

Exemple 7.3. Le polynôme cyclotomique $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$ est irréductible sur $\mathbb{Z}$ pour p premier. En effet, le changement de variable $Y = X - 1$ donne :

$$\Phi_p(Y+1) = \frac{(Y+1)^p - 1}{Y} = Y^{p-1} + \binom{p}{1} Y^{p-2} + \cdots + \binom{p}{p-2} Y + p.$$

Le critère d'Eisenstein s'applique avec l'irréductible p : le coefficient dominant est 1 ($p \nmid 1$), tous les autres coefficients sont divisibles par p ($p \mid \binom{p}{k}$ pour $1 \leqslant k \leqslant p-1$), et le terme constant est p ($p^2 \nmid p$). Donc $\Phi_p(Y+1)$ est irréductible dans $\mathbb{Z}[Y]$, et par conséquent $\Phi_p(X)$ est irréductible dans $\mathbb{Z}[X]$.

7.10 Exercices

Exercice 7.1. Déterminer les éléments inversibles et les éléments irréductibles de $\mathbb{Z}[i]$.

Exercice 7.2. Montrer que $\mathbb{Z}[\sqrt{-3}]$ n'est pas factoriel. *Indication : considérer* $4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$.

Exercice 7.3. Montrer que dans un anneau principal, tout idéal premier non nul est maximal.

Exercice 7.4. Soit K un corps. Montrer que $K[X, Y]$ n'est pas un anneau principal. *Indication : considérer l'idéal* (X, Y).

Exercice 7.5. Appliquer le critère d'Eisenstein pour montrer que $X^4 + 2X^3 + 6X + 3$ est irréductible dans $\mathbb{Z}[X]$.

Exercice 7.6. Soit p un nombre premier et $p \equiv 1 \pmod 4$. Montrer qu'il existe $a, b \in \mathbb{Z}$ tels que $p = a^2 + b^2$. *Indication : utiliser le fait que* -1 *est un carré modulo* p*, puis travailler dans* $\mathbb{Z}[i]$ *qui est principal.*

Exercice 7.7. Montrer que $X^2 + Y^2 - 1$ est irréductible dans $\mathbb{R}[X, Y]$.

Exercice 7.8. Soit A un anneau principal et $a, b \in A$. Montrer qu'il existe $d = \operatorname{pgcd}(a, b)$ et qu'on peut écrire $d = ua + vb$ pour certains $u, v \in A$ (identité de Bézout).

Exercice 7.9. Montrer que $\mathbb{Z}[X]$ est factoriel mais n'est pas principal. *Indication : pour la non-principalité, considérer l'idéal* $(2, X)$.

Exercice 7.10. Soit A un anneau factoriel. Montrer que $a \in A$ est irréductible si et seulement si l'idéal (a) est maximal parmi les idéaux principaux propres de A.

Exercice 7.11. Factoriser $X^4 - 1$ dans $\mathbb{Z}[X]$, dans $\mathbb{Q}[X]$, dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$.

Exercice 7.12. Montrer que pour tout entier $n \geqslant 2$, le polynôme $f(X) = X^n - 2$ est irréductible dans $\mathbb{Z}[X]$. En déduire que $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$.

Exercice 7.13. Un anneau commutatif A est dit *noethérien* si toute suite croissante d'idéaux $I_1 \subseteq I_2 \subseteq \cdots$ est stationnaire. Montrer que tout anneau principal est noethérien. Donner un exemple d'anneau noethérien qui n'est pas principal.

Résumé du chapitre 7

— Dans un anneau intègre, tout élément premier est irréductible. La réciproque est vraie dans les anneaux principaux et les anneaux factoriels, mais fausse en général.

— Un anneau *euclidien* possède une division euclidienne. Tout anneau euclidien est principal (les idéaux sont engendrés par leurs éléments de stathme minimal).

— Un anneau *principal* (PID) est un anneau intègre dont tout idéal est principal. Tout PID est factoriel (argument par chaînes ascendantes pour l'existence, et primalité des irréductibles pour l'unicité).

— Un anneau *factoriel* (UFD) possède la factorisation unique en irréductibles. Le lemme de Gauss montre que A UFD entraîne $A[X]$ UFD.

— Hiérarchie stricte : corps $\subsetneq$ euclidien $\subsetneq$ PID $\subsetneq$ UFD $\subsetneq$ intègre.

— Le critère d'Eisenstein fournit une condition suffisante d'irréductibilité dans $A[X]$ pour A factoriel.

Bibliographie

[1] Dummit, D. S. et Foote, R. M., *Abstract Algebra*, 3e édition, John Wiley & Sons, Hoboken, 2004.

[2] Lang, S., *Algebra*, 3e édition, Graduate Texts in Mathematics **211**, Springer-Verlag, New York, 2002.

[3] Artin, M., *Algebra*, 2e édition, Pearson, Boston, 2011.

[4] Jacobson, N., *Basic Algebra I*, 2e édition, W. H. Freeman and Company, New York, 1985.

[5] Bourbaki, N., *Algèbre*, Chapitres 1 à 3, Springer-Verlag, Berlin, 2007 (réimpression).

[6] Perrin, D., *Algèbre : cours de mathématiques de première année*, Ellipses, Paris, 1996.

Index