UNIVERSITÉ MOHAMMED V
FACULTÉ DES SCIENCES DE RABAT
Département de Mathématiques

Licence 1 – Sciences Mathématiques

Algèbre II

CHAPITRE 1

Structures algébriques

Groupes, morphismes et anneaux

Prof. Mohamed Najib LAATABI

Toute remarque de votre part est la bienvenue.
Si vous identifiez une erreur, veuillez la signaler.

najib.laatabi@um5r.ac.ma

mohamednajiblaatabi.com

Année universitaire : **2025–2026**

Table des matières

Notations et mode d'emploi **ii**

1 Structures algébriques **1**

1.1 Lois de composition interne 1
1.2 Groupes : définition et règles de calcul 3
1.3 Sous-groupes et sous-groupes engendrés 4
1.4 Morphismes de groupes 6
1.5 Ordre d'un élément et groupes cycliques 7
1.6 Classes modulo un sous-groupe et théorème de Lagrange 10
1.7 Le groupe des permutations 11
1.8 Complément : groupes quotients et factorisation 13
1.9 Complément : actions de groupes 15
1.10 Anneaux et règles de calcul 16
1.11 Éléments inversibles, anneaux intègres et corps 18
1.12 Sous-structures et morphismes d'anneaux 20
1.13 L'anneau des classes modulo n 22

Bibliographie **25**

Notations et mode d'emploi

Notation	Signification
$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	Entiers naturels (avec 0), entiers relatifs, rationnels, réels, complexes.
e_G, x^{-1}	Élément neutre de G ; inverse de x dans un groupe.
$H \leq G$	H est un sous-groupe de G.
$\langle S \rangle$, $\langle a \rangle$	Sous-groupe engendré par une partie S, ou par un élément a.
$\lvert G \rvert$, $\mathrm{ord}(a)$	Cardinal (ordre) de G ; ordre de l'élément a.
$\ker f$, $\mathrm{Im}\, f$	Noyau et image d'un morphisme.
gH, $[G : H]$	Classe à gauche ; nombre de classes à gauche modulo H.
$H \trianglelefteq G$	H est un sous-groupe distingué de G.
S_n, A_n	Groupe symétrique ; groupe alterné.
$\overline{a}$, $\mathbb{Z}/n\mathbb{Z}$	Classe de a modulo n ; ensemble des classes.
0_A, 1_A	Neutres de l'addition et de la multiplication dans un anneau.
$A^\times = U(A)$	Groupe des éléments inversibles de l'anneau A.
$\mathbb{F}_p$	Corps $\mathbb{Z}/p\mathbb{Z}$, lorsque p est premier.
$\varphi(n)$	Indicatrice d'Euler.

Chapitre

1 Structures algébriques

Additionner des entiers, multiplier des nombres complexes ou composer des permutations sont des opérations différentes. Elles obéissent pourtant à des règles communes. Une **structure algébrique** permet d'isoler ces règles et de démontrer une seule fois les résultats qui en découlent.

Ce chapitre construit progressivement les notions de groupe et d'anneau. La progression reprend les thèmes des fiches fournies et s'appuie sur le résumé de Bordeaux [1]. Le cours Exo7 [2] fournit une lecture complémentaire de première année ; Godement [3] permet d'approfondir.

Objectifs du chapitre

Reconnaître une structure ; vérifier un sous-groupe ou un sous-anneau ; utiliser un morphisme, son noyau et son image ; calculer l'ordre d'un élément ; appliquer Lagrange ; travailler dans $\mathbb{Z}/n\mathbb{Z}$; distinguer anneau, anneau intègre et corps.

1.1 Lois de composition interne

1.1.1 Définition et premières propriétés

Définition 1.1.1: Loi interne

Une **loi de composition interne** sur un ensemble E est une application

$$\star : E \times E \longrightarrow E, \qquad (x, y) \longmapsto x \star y.$$

Le résultat $x \star y$ doit être défini de manière unique et appartenir à E.

Exemple 1: Le choix de l'ensemble est essentiel

L'addition est une loi interne sur $\mathbb{N}$, $\mathbb{Z}$ et $\mathbb{R}$. La soustraction est interne sur $\mathbb{Z}$, mais pas sur $\mathbb{N}$, puisque $2 - 5 \notin \mathbb{N}$. La division n'est pas une loi interne sur $\mathbb{R}$ car on ne peut pas diviser par 0 ; elle est interne sur $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$. La composition est une loi interne sur l'ensemble des applications de E dans E.

Définition 1.1.2: Associativité, commutativité, élément neutre

Une loi $\star$ sur E est :

— **associative** si $(x \star y) \star z = x \star (y \star z)$ pour tous $x, y, z \in E$;

— **commutative** si $x \star y = y \star x$ pour tous $x, y \in E$.

Un élément $e \in E$ est **neutre** si $e \star x = x \star e = x$ pour tout $x \in E$. Si un neutre existe, y est un **symétrique** de x si $x \star y = y \star x = e$. En notation multiplicative, on parle d'**inverse** ; en notation additive, d'**opposé**.

Proposition 1.1.1: Unicité

Le neutre, s'il existe, est unique. Pour une loi associative possédant un neutre, le symétrique d'un élément, s'il existe, est unique.

Démonstration. Si e et e' sont neutres, alors $e = e \star e' = e'$. Si y et z sont deux symétriques de x, l'associativité donne

$$y = y \star e = y \star (x \star z) = (y \star x) \star z = e \star z = z.$$

■

Remarque 1: Ne pas confondre les propriétés

La soustraction sur $\mathbb{Z}$ n'est ni commutative ni associative : $(5-3)-1 = 1$, tandis que $5-(3-1) = 3$. La composition des applications est associative, mais elle n'est généralement pas commutative. L'associativité autorise à supprimer les parenthèses ; elle n'autorise pas à changer l'ordre des facteurs.

1.1.2 Parties stables et lois induites

Définition 1.1.3: Stabilité

Une partie $A \subset E$ est **stable** par $\star$ si $x \star y \in A$ pour tous $x, y \in A$. La restriction de $\star$ à $A \times A$ est alors une loi interne sur A, appelée loi induite.

Par exemple, $2\mathbb{Z}$ est stable par l'addition, tandis que l'ensemble des entiers impairs ne l'est pas. Une propriété comme l'associativité passe automatiquement à une loi induite. La présence du neutre et des inverses doit, elle, être vérifiée.

1.2 Groupes : définition et règles de calcul

1.2.1 La structure de groupe

Définition 1.2.1: Groupe et groupe abélien

Un **groupe** est un ensemble G muni d'une loi interne $\star$ telle que :

1. la loi est associative ;
2. il existe un neutre e_G ;
3. chaque élément de G possède un symétrique.

Si la loi est aussi commutative, le groupe est dit **abélien**. Le cardinal d'un groupe fini est appelé son **ordre** et se note $|G|$.

Exemple 2: Exemples fondamentaux

— $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ et $(\mathbb{C},+)$ sont abéliens, de neutre 0 ; l'opposé de x est $-x$.

— $(\mathbb{Q}^*,\times)$, $(\mathbb{R}^*,\times)$ et $(\mathbb{C}^*,\times)$ sont abéliens, de neutre 1 ; l'inverse est $1/x$.

— L'ensemble $\mathcal{B}(E)$ des bijections de E dans lui-même est un groupe pour la composition : le neutre est id_E et l'inverse est la bijection réciproque.

— $(\mathbb{N},+)$ n'est pas un groupe : 1 n'a pas d'opposé dans $\mathbb{N}$. $(\mathbb{Z}\setminus\{0\},\times)$ n'est pas un groupe : 2 n'y a pas d'inverse.

1.2.2 Simplification et résolution des équations

Dans la suite, une loi de groupe sera souvent notée multiplicativement : xy au lieu de $x\star y$, et e au lieu de e_G.

Proposition 1.2.1: Calcul dans un groupe

Pour tous $a,b,x,y\in G$:

1. $e^{-1}=e$, $(x^{-1})^{-1}=x$ et $(xy)^{-1}=y^{-1}x^{-1}$;
2. $ax=ay\Rightarrow x=y$ et $xa=ya\Rightarrow x=y$;
3. $ax=b$ admet l'unique solution $x=a^{-1}b$; $xa=b$ admet l'unique solution $x=ba^{-1}$.

Démonstration. Les deux premières égalités de 1 résultent de l'unicité de l'inverse. Pour la troisième, on vérifie

$$(xy)(y^{-1}x^{-1})=x(yy^{-1})x^{-1}=e,\qquad (y^{-1}x^{-1})(xy)=e.$$

Si $ax=ay$, multiplier à gauche par a^{-1} donne $x=y$; la preuve à droite est analogue. Enfin, $ax=b$ implique $x=a^{-1}b$ et cette valeur vérifie l'équation. L'autre équation se traite en multipliant à droite. ■

Remarque 2: L'ordre des facteurs

Dans un groupe non abélien, on ne peut pas remplacer $a^{-1}b$ par ba^{-1}. De même, l'inverse d'un produit s'obtient en inversant *et en renversant* l'ordre des facteurs.

1.2.3 Puissances et groupe produit

Pour $a \in G$, on pose $a^0 = e$, $a^n = \underbrace{a \cdots a}_{n \text{ facteurs}}$ si $n \geq 1$, et $a^{-n} = (a^{-1})^n$. Alors, pour tous $m, n \in \mathbb{Z}$,

$$a^{m+n} = a^m a^n, \qquad (a^m)^n = a^{mn}.$$

Pour les exposants positifs, ces identités résultent de l'associativité et d'une récurrence ; pour les exposants négatifs, on utilise l'inverse et la simplification. En notation additive, a^n est remplacé par na.

Proposition 1.2.2: Produit de groupes

Si G et H sont des groupes, alors $G \times H$, muni de

$$(g, h)(g', h') = (gg', hh'),$$

est un groupe de neutre (e_G, e_H) et d'inverse $(g, h)^{-1} = (g^{-1}, h^{-1})$. Il est abélien si et seulement si G et H le sont.

Démonstration. L'associativité, le neutre et les inverses se vérifient dans chaque composante. Si les facteurs sont abéliens, les produits de couples commutent. Réciproquement, la commutativité des couples (g, e_H) impose celle de G, et celle des couples (e_G, h) impose celle de H. ■

1.3 Sous-groupes et sous-groupes engendrés

1.3.1 Un critère pratique

Définition 1.3.1: Sous-groupe

Une partie H d'un groupe G est un **sous-groupe**, noté $H \leq G$, si elle contient e_G, est stable par produit et est stable par passage à l'inverse. Avec la loi induite, H est lui-même un groupe.

Théorème 1.3.1: Critère de sous-groupe

Une partie $H \subset G$ est un sous-groupe si et seulement si

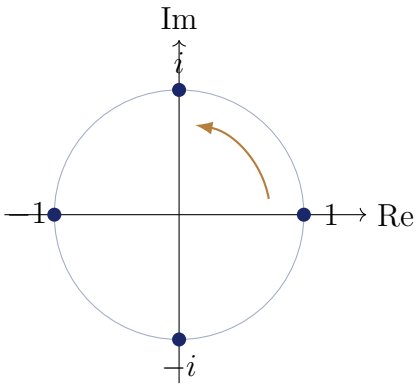
$$H \neq \varnothing \quad \text{et} \quad \forall x, y \in H, \quad xy^{-1} \in H.$$

Pour un groupe additif, le second test devient $x - y \in H$.

Démonstration. Un sous-groupe satisfait le critère par stabilité. Réciproquement, choisissons $h \in H$. Le test avec $x = y = h$ donne $e \in H$. Puis, avec $x = e$ et $y \in H$, il donne $y^{-1} \in H$. Enfin, si $x, y \in H$, alors $y^{-1} \in H$ et le test appliqué à (x, y^{-1}) donne $x(y^{-1})^{-1} = xy \in H$. ■

Exemple 3: Racines de l'unité

Pour $n \geq 1$, posons $U_n = \{z \in \mathbb{C} : z^n = 1\}$. On a $1 \in U_n$, et si $z, w \in U_n$, alors $w \neq 0$ et $(zw^{-1})^n = z^n / w^n = 1$. Ainsi $U_n \leq \mathbb{C}^*$. En particulier, $U_4 = \{1, i, -1, -i\}$.



Multiplier par i
fait tourner d'un quart de tour.

FIGURE 1.1 – Le groupe U_4 : la multiplication devient une composition de rotations.

1.3.2 Les sous-groupes de $(\mathbb{Z}, +)$

Théorème 1.3.2: Classification des sous-groupes de $\mathbb{Z}$

Pour tout sous-groupe H de $(\mathbb{Z}, +)$, il existe un unique $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$. On convient que $0\mathbb{Z} = \{0\}$.

Démonstration. Si $H = \{0\}$, on prend $n = 0$. Sinon, H contient un entier non nul et son opposé, donc un entier strictement positif. Soit n le plus petit entier strictement positif de H. Comme H est un groupe, tous les multiples de n sont dans H : $n\mathbb{Z} \subset H$. Pour $a \in H$, effectuons la division euclidienne $a = qn + r$, $0 \leq r < n$. Alors $r = a - qn \in H$. La minimalité de n impose $r = 0$; ainsi $a \in n\mathbb{Z}$. Donc $H = n\mathbb{Z}$. Si $H \neq \{0\}$, n est déterminé comme son plus petit élément positif, ce qui prouve l'unicité ; le cas nul est immédiat. ■

1.3.3 Intersection, réunion et génération

Proposition 1.3.1: Intersection de sous-groupes

L'intersection d'une famille non vide de sous-groupes de G est un sous-groupe.

Démonstration. Le neutre appartient à tous les sous-groupes. Si x et y appartiennent à l'intersection, xy^{-1} appartient à chacun d'eux, donc à l'intersection. ■

Remarque 3: La réunion n'est pas toujours un sous-groupe

Dans $\mathbb{Z}$, les ensembles $2\mathbb{Z}$ et $3\mathbb{Z}$ sont des sous-groupes, mais leur réunion ne l'est pas : elle contient 2 et 3, sans contenir $2+3 = 5$. Plus généralement, $H \cup K$ est un sous-groupe si et seulement si $H \subset K$ ou $K \subset H$. En effet, si aucune inclusion n'a lieu, choisir $h \in H \setminus K$ et $k \in K \setminus H$. Le produit hk ne peut appartenir ni à H (sinon $k \in H$), ni à K (sinon $h \in K$).

Définition 1.3.2: Sous-groupe engendré

Pour $S \subset G$, le sous-groupe $\langle S \rangle$ est l'intersection de tous les sous-groupes de G contenant S. C'est le plus petit sous-groupe contenant S. Pour $S = \{a\}$, on écrit $\langle a \rangle$.

Proposition 1.3.2: Description par des produits

Le sous-groupe $\langle S\rangle$ est constitué des produits finis $s_1^{\varepsilon_1}\cdots s_r^{\varepsilon_r}$, avec $r \geq 0$, $s_j \in S$ et $\varepsilon_j \in \{-1, 1\}$. Le produit vide ($r = 0$) vaut e. En particulier, $\langle\varnothing\rangle = \{e\}$ et

$$\langle a\rangle = \{a^k : k \in \mathbb{Z}\}.$$

Démonstration. L'ensemble des produits décrits contient e et S. Il est stable par produit, par concaténation, et par inverse, en renversant l'ordre et les signes des exposants. C'est donc un sous-groupe contenant S. Inversement, tout sous-groupe contenant S contient ces produits, ce qui prouve la minimalité. ■

Exemple 4: Un calcul dans $\mathbb{Z}$

Le sous-groupe engendré par 8 et 12 est $4\mathbb{Z}$. Toute combinaison $8u + 12v$ est multiple de 4, et $4 = 12 - 8$ appartient au sous-groupe engendré. Les deux inclusions sont donc établies.

1.4 Morphismes de groupes

1.4.1 Définition, exemples et composition

Définition 1.4.1: Morphisme et isomorphisme

Une application $f : G \to H$ entre deux groupes est un **morphisme** si

$$\forall x, y \in G, \qquad f(xy) = f(x)f(y).$$

Un morphisme bijectif est un **isomorphisme**. On écrit alors $G \simeq H$. Un morphisme de G dans lui-même est un endomorphisme ; s'il est bijectif, c'est un automorphisme.

Exemple 5: Respecter les lois indiquées

L'application $\exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \times)$ est un isomorphisme car $e^{x+y} = e^x e^y$ et l'exponentielle est bijective ; sa réciproque est ln. Pour un entier m, $f : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$, $f(k) = mk$, est un morphisme. En revanche, $k \mapsto k + 1$ n'est pas un morphisme additif, puisque $f(0) = 1 \neq 0$.

Proposition 1.4.1: Propriétés automatiques

Si $f : G \to H$ est un morphisme, alors

$$f(e_G) = e_H, \qquad f(x^{-1}) = f(x)^{-1}, \qquad f(x^n) = f(x)^n \quad (n \in \mathbb{Z}).$$

La composée de deux morphismes est un morphisme. La réciproque d'un isomorphisme est un isomorphisme.

Démonstration. De $f(e_G) = f(e_G)^2$, la simplification donne $f(e_G) = e_H$. Puis $f(x)f(x^{-1}) = f(e_G) = e_H$ et, dans l'autre sens, le produit vaut aussi e_H ; l'unicité de l'inverse donne la deuxième égalité. La troisième se prouve par récurrence pour $n \geq 0$, puis par passage à l'inverse. Si $g : H \to K$ est un morphisme, $(g \circ f)(xy) = g(f(x)f(y)) = (g \circ f)(x)(g \circ f)(y)$.

Enfin, si f est bijectif et si $u = f(x)$, $v = f(y)$, alors $f^{-1}(uv) = f^{-1}(f(xy)) = xy = f^{-1}(u)f^{-1}(v)$. ■

1.4.2 Images, images réciproques, noyau

Proposition 1.4.2: Transport des sous-groupes

Si $f : G \to H$ est un morphisme, $K \leq G$ et $L \leq H$, alors $f(K) \leq H$ et $f^{-1}(L) \leq G$.

Démonstration. L'image contient $e_H = f(e_G)$. Pour $u = f(x)$ et $v = f(y)$, avec $x, y \in K$, on a $uv^{-1} = f(xy^{-1}) \in f(K)$. L'image réciproque contient e_G. Si $x, y \in f^{-1}(L)$, alors $f(xy^{-1}) = f(x)f(y)^{-1} \in L$, donc $xy^{-1} \in f^{-1}(L)$. Dans les deux cas, on applique le critère de sous-groupe. ■

Définition 1.4.2: Noyau et image

Pour un morphisme $f : G \to H$, on pose

$$\ker f = \{x \in G : f(x) = e_H\}, \qquad \operatorname{Im} f = f(G) = \{f(x) : x \in G\}.$$

Le noyau est un sous-groupe de G ; l'image est un sous-groupe de H.

Ces deux affirmations résultent de la proposition précédente, avec $L = \{e_H\}$ et $K = G$.

Théorème 1.4.1: Injectivité et surjectivité

Pour un morphisme $f : G \to H$,

$$f \text{ injectif} \iff \ker f = \{e_G\}, \qquad f \text{ surjectif} \iff \operatorname{Im} f = H.$$

Démonstration. Si f est injectif et $f(x) = e_H = f(e_G)$, alors $x = e_G$. Réciproquement, si le noyau est réduit au neutre, $f(x) = f(y)$ implique $f(xy^{-1}) = e_H$, donc $xy^{-1} = e_G$ et $x = y$. L'équivalence concernant la surjectivité est sa définition. ■

Exemple 6: Le noyau peut être grand

Pour $f : (\mathbb{R}, +) \to (\mathbb{C}^*, \times)$, $f(t) = e^{2\pi i t}$, on a $\ker f = \mathbb{Z}$ et $\operatorname{Im} f = \{z \in \mathbb{C} : |z| = 1\}$. Le morphisme n'est ni injectif, ni surjectif sur $\mathbb{C}^*$; il est surjectif sur le cercle unité si l'on choisit celui-ci comme ensemble d'arrivée.

1.5 Ordre d'un élément et groupes cycliques

1.5.1 Quand les puissances recommencent-elles ?

Définition 1.5.1: Ordre d'un élément

L'élément $a \in G$ est d'**ordre fini** s'il existe un entier $n \geq 1$ tel que $a^n = e$. Le plus petit de ces entiers est $\operatorname{ord}(a)$. Si aucun entier positif ne convient, a est d'ordre infini.

Proposition 1.5.1: Caractérisation et cardinal

Si a est d'ordre n, alors pour tout $k \in \mathbb{Z}$,

$$a^k = e \iff n \mid k, \qquad \langle a \rangle = \{e, a, \dots, a^{n-1}\}, \quad |\langle a \rangle| = n.$$

Si a est d'ordre infini, ses puissances entières sont deux à deux distinctes.

Démonstration. Écrivons $k = qn + r$, avec $0 \leq r < n$. Alors $a^k = a^r$. Si $a^k = e$, la minimalité de n impose $r = 0$. La réciproque est immédiate. Toutes les puissances se ramènent donc aux n puissances indiquées. Si $a^i = a^j$ pour $0 \leq i < j < n$, on aurait $a^{j-i} = e$, contradiction. Enfin, dans le cas infini, une égalité $a^i = a^j$ avec $i < j$ fournirait justement une puissance positive égale au neutre. ■

Définition 1.5.2: Groupe monogène et groupe cyclique

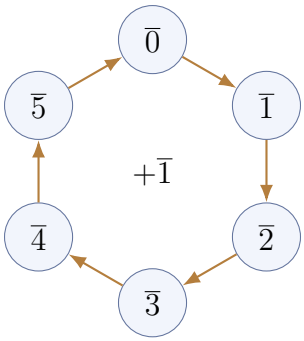
Un groupe G est **monogène** s'il existe a tel que $G = \langle a \rangle$. Il est **cyclique** s'il est monogène et fini. Un groupe monogène est abélien, puisque $a^m a^n = a^{m+n} = a^n a^m$.

1.5.2 Le groupe additif des classes modulo n

Pour $n \geq 1$, la relation $a \equiv b \pmod{n}$ signifie $n \mid (a - b)$. Elle est réflexive, symétrique et transitive : c'est une relation d'équivalence. La classe de a est $\overline{a} = a + n\mathbb{Z}$; l'ensemble des classes est $\mathbb{Z}/n\mathbb{Z}$. Par division euclidienne,

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}.$$

On définit $\overline{a} + \overline{b} = \overline{a+b}$. Cette loi ne dépend pas des représentants : si $a - a'$ et $b - b'$ sont multiples de n, leur somme l'est aussi. Elle fait de $\mathbb{Z}/n\mathbb{Z}$ un groupe abélien, de neutre $\overline{0}$ et d'opposé $-\overline{a} = \overline{-a}$. Ce groupe est cyclique, engendré par $\overline{1}$.



Six additions successives ramènent à $\overline{0}$.

FIGURE 1.2 – Le groupe $\mathbb{Z}/6\mathbb{Z}$ comme un parcours cyclique.

Théorème 1.5.1: Classification des groupes monogènes

Si $G = \langle a \rangle$, alors :

— si a est d'ordre infini, $G \simeq (\mathbb{Z}, +)$;

— si a est d'ordre n, $G \simeq (\mathbb{Z}/n\mathbb{Z}, +)$.

Démonstration. Dans le cas infini, $k \mapsto a^k$ est un morphisme surjectif et les puissances sont distinctes, donc il est bijectif. Dans le cas fini, $\overline{k} \mapsto a^k$ est bien défini puisque deux représentants diffèrent d'un multiple de n. C'est un morphisme surjectif, et $a^k = e$ équivaut à $\overline{k} = \overline{0}$; il est donc injectif. ■

1.5.3 Ordre d'une puissance et générateurs

Théorème 1.5.2: Ordre de a^r

Si a est d'ordre fini n et $r \in \mathbb{Z}$, alors

$$\boxed{\operatorname{ord}(a^r) = \frac{n}{\operatorname{pgcd}(n, r)}.}$$

Ainsi a^r engendre $\langle a \rangle$ si et seulement si $\operatorname{pgcd}(n, r) = 1$.

Démonstration. Posons $d = \operatorname{pgcd}(n, r)$, $n = dn_0$ et $r = dr_0$, où $\operatorname{pgcd}(n_0, r_0) = 1$. Pour $k \geq 1$,

$$(a^r)^k = e \iff n \mid rk \iff n_0 \mid r_0 k \iff n_0 \mid k,$$

la dernière équivalence résultant du lemme de Gauss. Le plus petit k est n_0. Le sous-groupe engendré par a^r coïncide avec celui de a exactement lorsqu'il a le même cardinal n, donc lorsque $d = 1$. ■

Exemple 7: Générateurs et racines de l'unité

Dans $\mathbb{Z}/12\mathbb{Z}$, les générateurs sont $\overline{1}, \overline{5}, \overline{7}, \overline{11}$, et $\operatorname{ord}(\overline{8}) = 12/\operatorname{pgcd}(12, 8) = 3$. Pour $\omega = e^{2\pi i/n}$, les solutions de $z^n = 1$ sont les ω^k, $0 \leq k < n$; ainsi $U_n = \langle \omega \rangle$ et ω^r est générateur exactement lorsque $\operatorname{pgcd}(n, r) = 1$.

Si $G = \langle a \rangle$ est infini, seuls a et a^{-1} sont générateurs : l'isomorphisme avec $\mathbb{Z}$ ramène la question à $r\mathbb{Z} = \mathbb{Z}$, équivalente à $r = \pm 1$.

Théorème 1.5.3: Sous-groupes d'un groupe monogène

Tout sous-groupe d'un groupe monogène est monogène. Si $G = \langle a \rangle$ est d'ordre n, il existe, pour chaque diviseur positif d de n, un unique sous-groupe d'ordre d, à savoir $\left\langle a^{n/d} \right\rangle$.

Démonstration. Soit $H \leq \langle a \rangle$. L'ensemble $E = \{k \in \mathbb{Z} : a^k \in H\}$ est un sous-groupe de $\mathbb{Z}$, donc $E = m\mathbb{Z}$ pour un $m \geq 0$. Par définition de E, $H = \langle a^m \rangle$. Si a est d'ordre n, alors $n \in E$, donc $m \geq 1$ et $m \mid n$. L'ordre de a^m vaut n/m. Avoir $|H| = d$ impose $m = n/d$, d'où l'unicité. Réciproquement, la formule de l'ordre montre que $\left\langle a^{n/d} \right\rangle$ a bien d éléments. ■

1.6 Classes modulo un sous-groupe et théorème de Lagrange

1.6.1 Découper un groupe en classes

Définition 1.6.1: Classe à gauche et indice

Pour $H \leq G$ et $g \in G$, on pose $gH = \{gh : h \in H\}$. L'ensemble de ces classes à gauche se note G/H. Le nombre de classes, lorsqu'il est fini, est l'**indice** $[G : H]$. À ce stade, G/H est un ensemble ; aucune loi de groupe n'y est encore supposée.

Proposition 1.6.1: Partition et égalité des cardinaux

Les classes à gauche forment une partition de G et chaque classe est en bijection avec H.

Démonstration. Tout $g \in G$ appartient à gH, puisque $e \in H$. Si $xH \cap yH \neq \varnothing$, écrivons $xh = yk$ avec $h, k \in H$. Alors $x = y(kh^{-1})$, donc $xH \subset yH$; en échangeant x et y, on obtient l'égalité. Deux classes sont donc égales ou disjointes. Enfin, $h \mapsto gh$ est une bijection de H sur gH, de réciproque $u \mapsto g^{-1}u$. ■

Théorème 1.6.1: Lagrange

Si G est fini et $H \leq G$, alors

$$\boxed{|G| = [G : H]\,|H|.}$$

En particulier, l'ordre d'un sous-groupe divise l'ordre du groupe.

Démonstration. La partition précédente possède $[G : H]$ classes, chacune de cardinal $|H|$. Il suffit d'additionner leurs cardinaux. ■

Exemple 8: Une partition de $\mathbb{Z}/12\mathbb{Z}$

Le sous-groupe $H = \langle \overline{4} \rangle = \{\overline{0}, \overline{4}, \overline{8}\}$ a quatre classes, chacune de cardinal 3 :

$$\begin{array}{c|ccc} H & \overline{0} & \overline{4} & \overline{8} \\ \overline{1}+H & \overline{1} & \overline{5} & \overline{9} \\ \overline{2}+H & \overline{2} & \overline{6} & \overline{10} \\ \overline{3}+H & \overline{3} & \overline{7} & \overline{11} \end{array} \qquad 12 = 4 \times 3.$$

Corollaire 1.6.1: Ordres des éléments

Si G est fini et $a \in G$, alors $\mathrm{ord}(a) \mid |G|$ et $a^{|G|} = e$. Tout groupe d'ordre premier est cyclique.

Démonstration. Les puissances de a ne peuvent être toutes distinctes dans un groupe fini ; a est donc d'ordre fini. Appliquer Lagrange à $\langle a \rangle$ donne $\mathrm{ord}(a) \mid |G|$, puis $a^{|G|} = e$. Si $|G| = p$ est premier, choisir $a \neq e$. Son ordre est un diviseur de p différent de 1, donc vaut p. Ainsi $\langle a \rangle = G$. ■

Remarque 4: Ce que Lagrange ne dit pas

Si d divise $|G|$, Lagrange ne garantit pas l'existence d'un élément d'ordre d. Par exemple, dans $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, les trois éléments non nuls ont ordre 2 : aucun n'a ordre 4, bien que le groupe ait quatre éléments.

1.7 Le groupe des permutations

1.7.1 Permutations et cycles

Définition 1.7.1: Groupe symétrique

Pour $n \geq 1$, S_n est l'ensemble des bijections de $\{1, \ldots, n\}$ sur lui-même, muni de la composition. C'est un groupe d'ordre $n!$. Une permutation peut s'écrire

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

Dans $\sigma\tau$, on applique d'abord τ, puis σ.

Le cardinal $n!$ se justifie en choisissant successivement les images : n choix pour la première, $n-1$ pour la deuxième, jusqu'à un choix pour la dernière.

Définition 1.7.2: Cycle et transposition

Si $a_1, \ldots, a_r$ sont distincts, le cycle $(a_1\ a_2\ \cdots\ a_r)$ envoie a_1 sur a_2, puis a_2 sur a_3, jusqu'à a_r sur a_1, et fixe tous les autres éléments. Un cycle de longueur 2 est une **transposition**.

Exemple 9: La composition ne commute pas

Dans S_3, posons $\sigma = (1\ 2)$ et $\tau = (2\ 3)$. Alors $\sigma\tau = (1\ 2\ 3)$ tandis que $\tau\sigma = (1\ 3\ 2)$. Par exemple, $(\sigma\tau)(1) = 2$ et $(\tau\sigma)(1) = 3$. Ainsi S_3 n'est pas abélien. Le même exemple, en fixant les autres éléments, montre que S_n n'est pas abélien pour $n \geq 3$.

Théorème 1.7.1: Décomposition en cycles disjoints

Toute permutation est un produit de cycles à supports disjoints. Cette décomposition est unique à l'ordre des cycles et à la rotation de l'écriture de chaque cycle près, une fois les points fixes omis.

Démonstration. Partons d'un élément a. La suite $a, \sigma(a), \sigma^2(a), \ldots$ rencontre une valeur déjà vue. Comme σ est bijective, la première répétition ramène à a : si $\sigma^i(a) = \sigma^j(a)$ avec $i < j$, on peut simplifier pour obtenir $a = \sigma^{j-i}(a)$. On obtient un cycle. Si des éléments restent, on recommence avec l'un d'eux. Les ensembles parcourus sont disjoints, et la procédure s'arrête puisque l'ensemble est fini. Les cycles ainsi obtenus reproduisent σ sur chaque élément. Ils sont imposés par les itérations de σ, ce qui prouve l'unicité. ■

Proposition 1.7.1: Ordre d'une permutation

Un cycle de longueur r a pour ordre r. Si les cycles disjoints de σ ont pour longueurs $r_1, \dots, r_k$, alors

$$\operatorname{ord}(\sigma) = \operatorname{ppcm}(r_1, \dots, r_k).$$

Démonstration. Sur un cycle de longueur r, il faut un nombre de pas multiple de r pour ramener chaque élément à sa place. Les cycles disjoints agissent sur des ensembles indépendants et commutent. Ainsi $\sigma^m = \mathrm{id}$ exactement lorsque chaque r_j divise m ; le plus petit tel entier est leur ppcm. ■

Exemple 10: Calculer sans multiplier de grandes tables

Pour

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 6 & 2 & 4 \end{pmatrix}, \qquad \sigma = (1\ 3)(2\ 5)(4\ 6).$$

Les trois cycles ont longueur 2, donc σ a ordre 2. Pour $\tau = (1\ 2\ 3)(4\ 5)$ dans S_5, l'ordre est $\operatorname{ppcm}(3, 2) = 6$.

1.7.2 Signature et groupe alterné

Chaque cycle se décompose en transpositions :

$$(a_1\ a_2\ \cdots\ a_r) = (a_1\ a_r)(a_1\ a_{r-1}) \cdots (a_1\ a_2).$$

Pour vérifier cette égalité, on suit l'image de chaque a_j de droite à gauche. La décomposition en cycles montre donc que toute permutation est un produit de transpositions. Leur nombre dépend de la décomposition, mais sa parité ne dépend pas du choix.

Définition 1.7.3: Signature

Une **inversion** de $\sigma \in S_n$ est un couple (i, j) tel que $i < j$ et $\sigma(i) > \sigma(j)$. Si $I(\sigma)$ est le nombre d'inversions, on pose $\operatorname{sgn}(\sigma) = (-1)^{I(\sigma)}$. La permutation est **paire** si sa signature vaut 1, **impaire** sinon.

Théorème 1.7.2: Propriétés de la signature

L'application $\operatorname{sgn} : S_n \to \{1, -1\}$ est un morphisme :

$$\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau).$$

Une transposition a signature -1 ; un cycle de longueur r a signature $(-1)^{r-1}$. L'ensemble $A_n = \ker(\operatorname{sgn})$ est un sous-groupe de S_n, appelé groupe alterné. Pour $n \geq 2$, $|A_n| = n!/2$.

Démonstration. Notons $s_i = (i\ i+1)$. Multiplier σ à droite par s_i échange deux entrées voisines de la liste $\sigma(1), \dots, \sigma(n)$. Leur ordre mutuel est renversé, tandis que le nombre total de comparaisons avec toute autre entrée est inchangé. Ainsi le nombre d'inversions varie de 1 ou de -1, et la signature change de signe.

Toute liste permutée peut être triée par échanges d'entrées voisines : si elle n'est pas croissante, elle possède une descente voisine, dont l'échange diminue le nombre d'inversions. On peut donc écrire toute τ comme un produit $s_{i_1} \cdots s_{i_m}$. En partant de l'identité, on obtient $\operatorname{sgn}(\tau) =$

$(-1)^m$; en partant de σ, on obtient $\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)(-1)^m$. Cela prouve la propriété de morphisme.

Pour $a < b$, la transposition $(a\ b)$ s'écrit $s_a s_{a+1} \cdots s_{b-1} s_{b-2} \cdots s_a$, produit de $2(b-a)-1$ transpositions voisines. Sa signature vaut donc -1. La décomposition d'un cycle en $r-1$ transpositions donne sa signature. Le noyau est un sous-groupe. Enfin, pour $n \geq 2$, multiplier par $(1\ 2)$ donne une bijection entre permutations paires et impaires ; elles sont en nombres égaux parmi les $n!$ permutations. ■

Exemple 11: Signature d'un produit de cycles

Pour $\sigma = (1\ 2\ 3\ 4)(5\ 6\ 7)$ dans S_7, $\operatorname{sgn}(\sigma) = (-1)^3(-1)^2 = -1$ et $\operatorname{ord}(\sigma) = \operatorname{ppcm}(4,3) = 12$. La signature et l'ordre répondent à deux questions différentes.

1.8 Complément : groupes quotients et factorisation

1.8.1 Sous-groupes distingués

Le groupe additif $\mathbb{Z}/n\mathbb{Z}$ possède une loi qui ne dépend pas du représentant choisi. Pour reproduire cette construction dans un groupe non abélien, il faut une condition supplémentaire.

Définition 1.8.1: Sous-groupe distingué

Un sous-groupe $H \leq G$ est **distingué**, ou normal, si

$$\forall g \in G, \qquad gHg^{-1} = H.$$

On note $H \trianglelefteq G$. Cette condition équivaut à $gH = Hg$ pour tout g.

L'équivalence s'obtient en multipliant l'égalité d'ensembles à droite par g ou par g^{-1}. Il suffit aussi de vérifier $gHg^{-1} \subset H$ pour tout g : l'inclusion appliquée à g^{-1} donne l'inclusion réciproque.

Proposition 1.8.1: Exemples et noyaux

Tout sous-groupe d'un groupe abélien est distingué. Le noyau d'un morphisme de groupes est toujours distingué dans son groupe de départ.

Démonstration. Dans un groupe abélien, $ghg^{-1} = h$. Si $h \in \ker f$, alors $f(ghg^{-1}) = f(g)ef(g)^{-1} = e$; ainsi $g(\ker f)g^{-1} \subset \ker f$ pour tout g, ce qui suffit. ■

Exemple 12: Un sous-groupe non distingué

Dans S_3, $H = \{\mathrm{id}, (1\ 2)\}$ n'est pas distingué : pour $g = (1\ 2\ 3)$, on a $g(1\ 2)g^{-1} = (2\ 3) \notin H$. En revanche, A_3 est distingué car c'est le noyau de la signature.

1.8.2 Construction du groupe quotient

Théorème 1.8.1: Loi sur les classes

Si $H \trianglelefteq G$, la formule

$$(xH)(yH) = (xy)H$$

définit une loi de groupe sur G/H. Son neutre est H et l'inverse de xH est $x^{-1}H$. La projection $\pi : G \to G/H$, $\pi(x) = xH$, est un morphisme surjectif de noyau H.

Démonstration. Le point essentiel est l'indépendance des représentants. Si $x' = xh$ et $y' = yk$, avec $h, k \in H$, alors

$$x'y' = xhyk = xy\underbrace{(y^{-1}hy)}_{\in H}k,$$

donc $(x'y')H = (xy)H$. L'associativité vient de celle de G. Les égalités $HxH = xH$ et $(xH)(x^{-1}H) = H$ donnent le neutre et les inverses. La formule du produit exprime précisément que π est un morphisme. Il est surjectif par définition des classes, et $xH = H$ équivaut à $x \in H$. ■

Remarque 5: Pourquoi la condition est nécessaire

Si la projection vers les classes était un morphisme pour une certaine loi de groupe, son noyau serait H ; le résultat précédent sur les noyaux imposerait donc que H soit distingué. On ne peut pas multiplier arbitrairement les classes modulo un sous-groupe quelconque.

1.8.3 Théorème de factorisation

Théorème 1.8.2: Factorisation et premier isomorphisme

Soient $f : G \to K$ un morphisme et $H \trianglelefteq G$ avec $H \subset \ker f$. Il existe un unique morphisme $\widetilde{f} : G/H \to K$ tel que $f = \widetilde{f} \circ \pi$. Il est donné par $\widetilde{f}(xH) = f(x)$. En particulier,

$$\boxed{G/\ker f \simeq \operatorname{Im} f.}$$

Démonstration. Si $xH = yH$, alors $x = yh$ pour un $h \in H$, donc $f(x) = f(y)f(h) = f(y)$. La formule est bien définie. Elle respecte les produits et vérifie $f = \widetilde{f} \circ \pi$; la surjectivité de π impose l'unicité. Pour $H = \ker f$, une classe xH appartient au noyau de $\widetilde{f}$ exactement lorsque $x \in \ker f = H$, donc lorsque $xH = H$. Le morphisme induit est injectif et son image est $\operatorname{Im} f$, d'où l'isomorphisme. ■

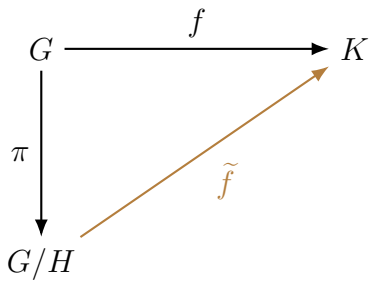


FIGURE 1.3 – Factoriser : deux chemins donnent la même application f.

Exemple 13: Le cercle unité comme quotient

Pour $f(t) = e^{2\pi it}$, défini sur $(\mathbb{R}, +)$, le noyau est $\mathbb{Z}$ et l'image est le cercle unité U. Le théorème donne $\mathbb{R}/\mathbb{Z} \simeq U$. Deux réels représentent le même point du cercle exactement lorsqu'ils diffèrent d'un entier.

1.9 Complément : actions de groupes

1.9.1 Orbites et stabilisateurs

Définition 1.9.1: Action d'un groupe

Une action à gauche d'un groupe G sur un ensemble X est une application $(g, x) \mapsto g \cdot x$ de $G \times X$ dans X telle que

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

L'**orbite** de x est $G{\cdot}x = \{g{\cdot}x : g \in G\}$. Le **stabilisateur** de x est $G_x = \{g \in G : g{\cdot}x = x\}$.

Exemple 14: Faire agir des transformations

Le groupe S_n agit sur $\{1, \dots, n\}$ par $\sigma \cdot j = \sigma(j)$. Le groupe des rotations d'un triangle équilatéral agit sur ses trois sommets. Dans ce dernier cas, les trois sommets forment une même orbite ; seul l'élément neutre fixe un sommet donné.

Proposition 1.9.1: Partition en orbites

Les orbites forment une partition de X et $G_x \leq G$ pour tout $x \in X$.

Démonstration. La relation « $y = g \cdot x$ pour un $g \in G$ » est réflexive grâce à e, symétrique grâce à g^{-1}, et transitive grâce au produit. Ses classes sont exactement les orbites. Le stabilisateur contient e. Si g, h fixent x, alors h^{-1} fixe x (appliquer h^{-1} à $h \cdot x = x$), et $(gh^{-1}) \cdot x = g \cdot x = x$. Le critère de sous-groupe s'applique. ■

Théorème 1.9.1: Formule orbite-stabilisateur

Si G est fini, alors

$$|G \cdot x| = [G : G_x] = \frac{|G|}{|G_x|}.$$

Si X est fini et si $x_1, \dots, x_r$ représentent ses orbites, alors

$$|X| = \sum_{j=1}^{r} |G \cdot x_j|.$$

Démonstration. L'application $gG_x \mapsto g \cdot x$ est bien définie : si $g = hk$ avec $k \in G_x$, alors $g \cdot x = h \cdot x$. Elle est surjective par définition de l'orbite et injective car $g \cdot x = h \cdot x$ équivaut à $h^{-1}g \in G_x$, donc à $gG_x = hG_x$. La première formule résulte de cette bijection et de Lagrange. La seconde vient de la partition en orbites. ■

1.9.2 Une application : le théorème de Cauchy

Théorème 1.9.2: Cauchy

Si un nombre premier p divise l'ordre d'un groupe fini G, alors G possède un élément d'ordre p.

Démonstration. Posons $N = |G|$ et

$$X = \{(x_1, \dots, x_p) \in G^p : x_1 x_2 \cdots x_p = e\}.$$

Les $p-1$ premières coordonnées sont arbitraires et la dernière est imposée, donc $|X| = N^{p-1}$. La rotation $\rho(x_1, \dots, x_p) = (x_2, \dots, x_p, x_1)$ préserve X : si $x_1 \cdots x_p = e$, alors $x_2 \cdots x_p x_1 = x_1^{-1}(x_1 \cdots x_p)x_1 = e$. Comme $\rho^p = \mathrm{id}$, les rotations définissent une action de $\mathbb{Z}/p\mathbb{Z}$ sur X. Par la formule orbite-stabilisateur, chaque orbite a cardinal 1 ou p.

Les orbites réduites à un point correspondent aux tuples $(a, \dots, a)$ avec $a^p = e$. Si m est le nombre de ces éléments a, la partition donne $|X| \equiv m \pmod p$. Or $p \mid N$, donc $p \mid N^{p-1}$ et $p \mid m$. Comme $a = e$ est une solution, $m \geq 1$, donc $m \geq p$. Il existe ainsi $a \neq e$ avec $a^p = e$. Son ordre divise p et n'est pas 1 ; il vaut donc p. ■

Les compléments sur les quotients et les actions expliquent plusieurs résultats du document de Bordeaux. La suite revient aux structures portant deux lois, au cœur de la seconde fiche fournie.

1.10 Anneaux et règles de calcul

1.10.1 Deux lois compatibles

Définition 1.10.1: Anneau unitaire et anneau commutatif

Un **anneau unitaire** $(A, +, \times)$ est un ensemble muni de deux lois internes vérifiant :

1. $(A, +)$ est un groupe abélien, de neutre 0_A ;
2. la multiplication est associative et possède un neutre 1_A ;
3. les deux distributivités sont satisfaites :

$$x(y+z) = xy + xz, \qquad (x+y)z = xz + yz.$$

L'anneau est **commutatif** si $xy = yx$ pour tous $x, y \in A$. Dans ce cours, « anneau » signifie toujours « anneau unitaire ».

Remarque 6: Deux neutres, deux rôles

Tout élément de A possède un opposé pour l'addition. La définition n'exige pas que tout élément non nul ait un inverse pour la multiplication. On autorise l'anneau nul $A = \{0\}$, où $0_A = 1_A$; les notions de corps et d'anneau intègre excluront ce cas.

Exemple 15: Des anneaux familiers

Les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, munis de leurs opérations usuelles, sont des anneaux commutatifs. Si E est un ensemble non vide, l'ensemble des fonctions $E \to \mathbb{R}$ est un anneau commutatif pour les opérations point par point : $(f+g)(x) = f(x)+g(x)$ et $(fg)(x) = f(x)g(x)$. Les neutres sont les fonctions constantes 0 et 1 ; les axiomes se vérifient en chaque point de E.

Exemple 16: Un anneau non commutatif

L'ensemble $M_2(\mathbb{R})$ des matrices réelles de taille 2 est un anneau pour l'addition et la multiplication matricielles. Ses neutres sont la matrice nulle et I_2. Avec

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},$$

on a

$$AB = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = BA.$$

Les deux distributivités sont donc nécessaires dans la définition générale : on ne peut pas passer de l'une à l'autre en échangeant les facteurs.

1.10.2 Zéro, opposés et distributivité

Proposition 1.10.1: Identités élémentaires dans un anneau

Pour tous $x, y \in A$,

$$x0_A = 0_A x = 0_A, \qquad x(-y) = (-x)y = -(xy), \qquad (-x)(-y) = xy.$$

De plus, $0_A = 1_A$ si et seulement si A est l'anneau nul.

Démonstration. La distributivité donne $x0_A = x(0_A + 0_A) = x0_A + x0_A$; la simplification dans le groupe additif donne $x0_A = 0_A$. L'autre égalité se prouve de même. Puis $xy + x(-y) = x(y-y) = 0_A$, donc $x(-y)$ est l'opposé de xy. La preuve de $(-x)y = -(xy)$ est analogue ; en appliquant ces identités deux fois, on obtient $(-x)(-y) = xy$. Enfin, si $0_A = 1_A$, tout x vérifie $x = x1_A = x0_A = 0_A$. La réciproque est immédiate. ■

Remarque 7: Développer sans commuter

Dans tout anneau,

$$(a+b)^2 = a^2 + ab + ba + b^2.$$

On ne peut remplacer $ab + ba$ par $2ab$ que si $ab = ba$. De même, $(ab)^n = a^n b^n$ est garanti lorsque a et b commutent ; ce n'est pas une règle générale des anneaux.

1.10.3 Binôme de Newton et différence de puissances

Théorème 1.10.1: Formules pour deux éléments qui commutent

Si $a, b \in A$ vérifient $ab = ba$, alors pour tout entier $n \geq 0$,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

Pour $n \geq 1$,

$$a^n - b^n = (a-b) \sum_{k=0}^{n-1} a^{n-1-k} b^k.$$

Un coefficient entier désigne ici une addition répétée dans le groupe $(A, +)$.

Démonstration. La formule du binôme est vraie pour $n = 0$. Supposons-la vraie au rang n et multiplions par $a + b$. Comme a et b commutent, on peut regrouper les termes de même puissance : le coefficient de $a^{n+1-k}b^k$ devient $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$, avec les termes extrêmes égaux à 1. Cela prouve la récurrence. Pour la seconde formule, développons :

$$(a-b) \sum_{k=0}^{n-1} a^{n-1-k} b^k = \sum_{k=0}^{n-1} a^{n-k} b^k - \sum_{k=0}^{n-1} a^{n-1-k} b^{k+1}.$$

Les termes intermédiaires se compensent ; il reste $a^n - b^n$. ■

1.11 Éléments inversibles, anneaux intègres et corps

1.11.1 Le groupe des unités

Définition 1.11.1: Élément inversible

Un élément $a \in A$ est **inversible** s'il existe $b \in A$ tel que $ab = ba = 1_A$. On note $A^\times$, ou $U(A)$, l'ensemble des inversibles.

Proposition 1.11.1: Les unités forment un groupe

La multiplication fait de $A^\times$ un groupe de neutre 1_A. Si a, b sont inversibles, alors $(ab)^{-1} = b^{-1}a^{-1}$.

Démonstration. Le neutre est inversible. Si a, b le sont, les produits $(ab)(b^{-1}a^{-1})$ et $(b^{-1}a^{-1})(ab)$ valent 1_A. Le produit ab est donc inversible. Si $a \in A^\times$, son inverse est lui-même inversible, d'inverse a. L'associativité est héritée de l'anneau. ■

Exemple 17: Être non nul ne suffit pas

$\mathbb{Z}^\times = \{-1, 1\}$: si $ab = 1$ avec $a, b \in \mathbb{Z}$, alors $|a| = |b| = 1$. En revanche, $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$, et de même pour $\mathbb{R}$ et $\mathbb{C}$. Dans $M_2(\mathbb{R})$, les unités sont les matrices inversibles, formant le groupe $\mathrm{GL}_2(\mathbb{R})$.

Remarque 8: Inverse à gauche et inverse à droite

Dans un anneau non commutatif, la définition exige les deux égalités. Si b est un inverse à gauche de a et c un inverse à droite, alors $b = b(ac) = (ba)c = c$. La présence des deux inverses garantit donc qu'ils coïncident.

1.11.2 Diviseurs de zéro et intégrité

Définition 1.11.2: Anneau intègre

Un anneau **intègre** est un anneau commutatif, non nul, tel que

$$ab = 0_A \quad \Longrightarrow \quad a = 0_A \text{ ou } b = 0_A.$$

Dans un anneau commutatif, un élément $a \neq 0_A$ est un **diviseur de zéro** s'il existe $b \neq 0_A$ avec $ab = 0_A$.

Proposition 1.11.2: Simplification dans un anneau intègre

Dans un anneau intègre, si $a \neq 0$ et $ab = ac$, alors $b = c$. Réciproquement, un anneau commutatif non nul dans lequel on peut simplifier par tout facteur non nul est intègre.

Démonstration. L'égalité $ab = ac$ donne $a(b-c) = 0$. L'intégrité et $a \neq 0$ imposent $b-c = 0$. Réciproquement, si $ab = 0$ et $a \neq 0$, écrire $ab = a0$ puis simplifier donne $b = 0$. ■

Exemple 18: Un produit nul avec deux facteurs non nuls

L'anneau $\mathbb{Z}$ est intègre. L'anneau produit $\mathbb{R} \times \mathbb{R}$, avec les opérations composante par composante, ne l'est pas : $(1,0)(0,1) = (0,0)$. Dans l'anneau des matrices de l'exemple précédent, $A \neq 0$ mais $A^2 = 0$. On voit pourquoi la simplification multiplicative ne découle pas des seuls axiomes d'un anneau.

1.11.3 Corps et anneaux intègres finis

Définition 1.11.3: Corps commutatif

Un **corps** est un anneau commutatif K tel que $0_K \neq 1_K$ et

$$K^\times = K \setminus \{0_K\}.$$

Ainsi tout élément non nul possède un inverse multiplicatif.

Proposition 1.11.3: Un corps est intègre

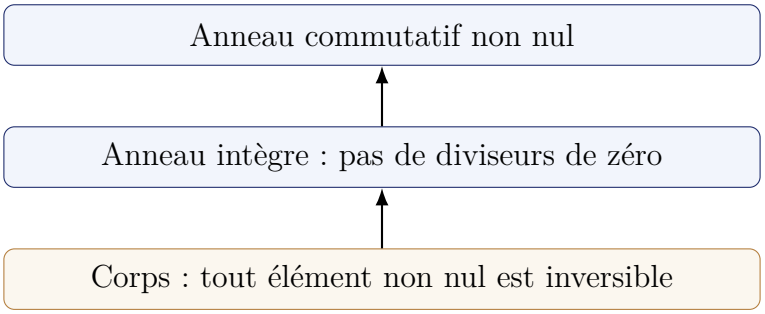
Tout corps est un anneau intègre. La réciproque est fausse en général.

Démonstration. Si $ab = 0$ et $a \neq 0$, multiplier par a^{-1} donne $b = 0$. Pour la réciproque, $\mathbb{Z}$ est intègre mais n'est pas un corps, car 2 n'y est pas inversible. ■

Théorème 1.11.1: Un anneau intègre fini est un corps

Tout anneau intègre ayant un nombre fini d'éléments est un corps.

Démonstration. Fixons $a \neq 0$ et considérons $m_a : A \to A$, $x \mapsto ax$. L'intégrité rend m_a injective. Une application injective d'un ensemble fini dans lui-même est surjective ; il existe donc $b \in A$ tel que $ab = 1_A$. La commutativité donne aussi $ba = 1_A$. Tout élément non nul est inversible. ■



Les flèches remontent vers une structure moins contraignante.
Pour un anneau fini, l'intégrité implique aussi la propriété de corps.

FIGURE 1.4 – Distinguer les hypothèses : $\mathbb{Z}$ est intègre ; dans $\mathbb{Q}$, tout rationnel non nul est inversible.

1.12 Sous-structures et morphismes d'anneaux

1.12.1 Critère de sous-anneau

Définition 1.12.1: Sous-anneau unitaire

Une partie B d'un anneau A est un **sous-anneau** si

$$1_A \in B, \qquad \forall x, y \in B, \quad x - y \in B \text{ et } xy \in B.$$

Elle est alors un anneau pour les lois induites, avec les mêmes neutres que A.

Démonstration. La partie B est non vide et stable par différence, donc est un sous-groupe de $(A, +)$. Elle contient ainsi 0_A et tous les opposés. La stabilité par multiplication, la présence de 1_A et les propriétés héritées de A donnent les autres axiomes. ■

Exemple 19: Les entiers de Gauss

L'ensemble $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{C}$. Il contient 1, est stable par différence, et

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i \in \mathbb{Z}[i].$$

En revanche, $2\mathbb{Z}$ n'est pas un sous-anneau unitaire de $\mathbb{Z}$ selon notre convention, car $1 \notin 2\mathbb{Z}$, même s'il est stable par différence et par produit.

1.12.2 Sous-corps

Définition 1.12.2: Sous-corps

Une partie L d'un corps K est un **sous-corps** si elle contient 1_K, est stable par différence et par multiplication, et vérifie $x^{-1} \in L$ pour tout $x \in L \setminus \{0\}$.

Les axiomes du corps se transmettent alors à L. Par exemple, $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ sont des inclusions de sous-corps.

Exemple 20: Le corps $\mathbb{Q}(\sqrt{2})$

Posons $L = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. Cet ensemble contient 1 et est stable par différence et par produit. Si $a + b\sqrt{2} \neq 0$, alors

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} \in L.$$

Le dénominateur ne s'annule pas : si $b \neq 0$ et $a^2 = 2b^2$, alors $(a/b)^2 = 2$, ce qui contredit l'irrationalité de $\sqrt{2}$; si $b = 0$, on a $a \neq 0$. Ainsi L est un sous-corps de $\mathbb{R}$.

1.12.3 Morphismes unitaires

Définition 1.12.3: Morphisme d'anneaux

Une application $f : A \to B$ est un **morphisme d'anneaux** si, pour tous $x, y \in A$,

$$f(x + y) = f(x) + f(y), \quad f(xy) = f(x)f(y), \quad f(1_A) = 1_B.$$

Si elle est bijective, c'est un isomorphisme d'anneaux. On pose $\ker f = \{x \in A : f(x) = 0_B\}$ et $\operatorname{Im} f = f(A)$.

Proposition 1.12.1: Propriétés et transport des structures

Un morphisme d'anneaux vérifie $f(0_A) = 0_B$ et $f(-x) = -f(x)$. Il est injectif si et seulement si $\ker f = \{0_A\}$. Il envoie les inversibles sur des inversibles et $f(u^{-1}) = f(u)^{-1}$ pour $u \in A^\times$. L'image d'un sous-anneau et l'image réciproque d'un sous-anneau sont des sous-anneaux.

Démonstration. Les premières propriétés et le critère d'injectivité sont ceux du morphisme additif sous-jacent. Si $uu^{-1} = u^{-1}u = 1_A$, leurs images donnent $f(u)f(u^{-1}) = f(u^{-1})f(u) = 1_B$. L'image d'un sous-anneau contient $1_B = f(1_A)$; la conservation des différences et des produits assure les stabilités. Pour une image réciproque, 1_A y appartient et les mêmes identités établissent les deux stabilités. ■

Remarque 9: Le noyau n'est généralement pas un sous-anneau unitaire

Si B n'est pas l'anneau nul, $f(1_A) = 1_B \neq 0_B$; ainsi $1_A \notin \ker f$. Le noyau est bien un sous-groupe additif, mais ne satisfait pas notre convention de sous-anneau contenant l'unité. Aucune structure supplémentaire sur le noyau n'est nécessaire pour ce chapitre.

Exemple 21: Conjugaison complexe

L'application $z \mapsto \overline{z}$ de $\mathbb{C}$ dans $\mathbb{C}$ conserve l'addition, la multiplication et 1. Elle est sa propre réciproque : c'est un automorphisme d'anneaux, et même de corps.

Corollaire 1.12.1: Un morphisme de corps est injectif

Tout morphisme unitaire $f : K \to L$ entre deux corps est injectif.

Démonstration. Si $x \neq 0$ appartenait au noyau, on aurait $1_L = f(xx^{-1}) = f(x)f(x^{-1}) = 0_L$, contradiction. Le noyau est donc réduit à 0, d'où l'injectivité. ■

1.13 L'anneau des classes modulo n

1.13.1 Construction et éléments inversibles

Dans cette section, $n \geq 2$. On conserve l'addition déjà définie sur $\mathbb{Z}/n\mathbb{Z}$ et l'on pose

$$\overline{a}\,\overline{b} = \overline{ab}.$$

Cette multiplication est bien définie : si $a - a'$ et $b - b'$ sont multiples de n, alors $ab - a'b' = a(b - b') + (a - a')b'$ est multiple de n. L'associativité, la commutativité et les distributivités sont héritées de $\mathbb{Z}$. Le neutre multiplicatif est $\overline{1}$. La projection $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $a \mapsto \overline{a}$, est un morphisme d'anneaux.

Théorème 1.13.1: Inversibilité modulo n

Pour $a \in \mathbb{Z}$, les trois assertions suivantes sont équivalentes :

1. $\overline{a}$ est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$;
2. $\operatorname{pgcd}(a, n) = 1$;
3. $\overline{a}$ engendre le groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$.

Démonstration. La classe $\overline{a}$ est inversible si et seulement s'il existe $b \in \mathbb{Z}$ tel que $ab \equiv 1 \pmod{n}$, c'est-à-dire s'il existe $b, q \in \mathbb{Z}$ avec $ab + nq = 1$. Par Bézout, cela équivaut à $\operatorname{pgcd}(a, n) = 1$. Enfin, $\overline{a}$ engendre le groupe additif si et seulement si $\overline{1}$ est un multiple entier de $\overline{a}$, donc s'il existe b tel que $b\overline{a} = \overline{1}$, ce qui est la même congruence. ■

Exemple 22: Trouver un inverse avec Bézout

Dans $\mathbb{Z}/26\mathbb{Z}$, 7 est premier à 26. L'égalité $15 \times 7 - 4 \times 26 = 1$ montre que $\overline{7}^{-1} = \overline{15}$. En revanche, $\overline{6}$ n'est pas inversible car $\operatorname{pgcd}(6, 26) = 2$; on observe d'ailleurs $\overline{6}\,\overline{13} = \overline{0}$ avec deux facteurs non nuls.

Théorème 1.13.2: Quand $\mathbb{Z}/n\mathbb{Z}$ est-il un corps ?

Pour $n \geq 2$,

$$\boxed{\mathbb{Z}/n\mathbb{Z} \text{ est un corps} \iff \mathbb{Z}/n\mathbb{Z} \text{ est intègre} \iff n \text{ est premier.}}$$

Si p est premier, ce corps se note $\mathbb{F}_p$.

Démonstration. Un corps est intègre. Si n n'est pas premier, on peut écrire $n = ab$ avec $1 < a, b < n$. Les classes $\overline{a}$ et $\overline{b}$ sont non nulles mais leur produit est nul ; l'anneau n'est donc pas intègre. Enfin, si $n = p$ est premier, chaque $a \in \{1, \dots, p-1\}$ est premier à p. Toutes les classes non nulles sont alors inversibles, donc $\mathbb{Z}/p\mathbb{Z}$ est un corps. ■

Exemple 23: Deux structures sur le même ensemble

Dans $\mathbb{Z}/5\mathbb{Z}$, le groupe additif est d'ordre 5, de neutre $\overline{0}$. Le groupe multiplicatif $\mathbb{F}_5^\times$ est d'ordre 4, de neutre $\overline{1}$. On a $\overline{2}^2 = \overline{4}$, $\overline{2}^3 = \overline{3}$, $\overline{2}^4 = \overline{1}$: $\overline{2}$ engendre le groupe multiplicatif. Il faut toujours préciser la loi lorsque l'on parle d'ordre ou de générateur.

1.13.2 Théorème chinois des restes

Théorème 1.13.3: Théorème chinois

Soient $m, n \geq 2$ premiers entre eux. L'application

$$\Phi : \mathbb{Z}/(mn)\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \qquad \overline{a}^{(mn)} \longmapsto (\overline{a}^{(m)}, \overline{a}^{(n)})$$

est un isomorphisme d'anneaux. En particulier, pour tous entiers r, s, le système $x \equiv r \pmod m$, $x \equiv s \pmod n$ a une unique solution modulo mn.

Démonstration. Changer a d'un multiple de mn ne change aucune des deux classes : Φ est bien définie. Elle conserve les deux opérations et l'unité. Si $\Phi(\overline{a}) = 0$, alors $m \mid a$ et $n \mid a$. Comme m, n sont premiers entre eux, $mn \mid a$; le noyau est donc nul et Φ est injective. Les deux ensembles ayant mn éléments, elle est bijective.

On peut aussi construire la solution. Soient $u, v \in \mathbb{Z}$ tels que $um + vn = 1$. L'entier $x = rvn + sum$ vérifie $x \equiv r \pmod m$ et $x \equiv s \pmod n$. Deux solutions ont une différence divisible par m et par n, donc par mn. ■

Exemple 24: Résoudre deux congruences

Pour $x \equiv 2 \pmod 3$ et $x \equiv 3 \pmod 5$, écrivons $2 \times 3 - 1 \times 5 = 1$. La construction précédente donne $x = 2(-1)5 + 3(2)3 = 8$. Toutes les solutions sont donc $x \equiv 8 \pmod{15}$.

1.13.3 Indicatrice d'Euler

Définition 1.13.1: Fonction φ

Pour $n \geq 2$, on pose

$$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times| = |\{a \in \{1, \dots, n\} : \operatorname{pgcd}(a, n) = 1\}|.$$

On pose par convention $\varphi(1) = 1$.

Proposition 1.13.1: Calcul de l'indicatrice

Si p est premier et $k \geq 1$, alors $\varphi(p^k) = p^k - p^{k-1}$. Si $m, n \geq 1$ sont premiers entre eux, alors $\varphi(mn) = \varphi(m)\varphi(n)$. Par conséquent, pour $n \geq 2$,

$$\boxed{\varphi(n) = n \prod_{p \mid n,\ p \text{ premier}} \left(1 - \frac{1}{p}\right).}$$

Démonstration. Un entier est premier à p^k exactement lorsqu'il n'est pas multiple de p. Parmi les entiers de 1 à p^k, il y a p^{k-1} multiples de p, d'où la première formule. Dans un produit d'anneaux, (a, b) est inversible si et seulement si a et b le sont : l'inverse est alors (a^{-1}, b^{-1}). Le théorème chinois identifie donc les unités modulo mn aux couples d'unités modulo m et modulo n. En prenant les cardinaux, on obtient la multiplicativité pour $m, n \geq 2$; les cas où l'un vaut 1 sont immédiats. On applique enfin ces deux formules à la décomposition $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. ■

Théorème 1.13.4: Euler et petit théorème de Fermat

Si $n \geq 2$ et $\operatorname{pgcd}(a, n) = 1$, alors

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

En particulier, si p est premier et $p \nmid a$, alors $a^{p-1} \equiv 1 \pmod{p}$. Pour tout entier a, on a aussi $a^p \equiv a \pmod{p}$.

Démonstration. La classe $\overline{a}$ appartient au groupe fini $(\mathbb{Z}/n\mathbb{Z})^\times$, de cardinal $\varphi(n)$. Le corollaire de Lagrange donne $\overline{a}^{\varphi(n)} = \overline{1}$. Pour $n = p$ premier, $\varphi(p) = p - 1$, d'où la première formule de Fermat. Multiplier par a donne $a^p \equiv a$ lorsque $p \nmid a$. Si $p \mid a$, les deux membres sont nuls modulo p. ■

Exemple 25: Réduire un grand exposant

On a $\varphi(15) = 15(1 - 1/3)(1 - 1/5) = 8$ et $\operatorname{pgcd}(2, 15) = 1$. Comme $100 = 12 \times 8 + 4$,

$$2^{100} \equiv (2^8)^{12} 2^4 \equiv 16 \equiv 1 \pmod{15}.$$

L'hypothèse de coprimalité est indispensable : on ne peut pas appliquer Euler à $a = 3$ modulo 15.

Bibliographie

[1] **Université de Bordeaux.** *Structures algébriques 1 : résumé de cours*. Licence de Sciences, Technologies, Santé, document de cours, sans date indiquée. Chapitres 1 à 5 : groupes, permutations, morphismes, actions et anneaux.

https://www.math.u-bordeaux.fr/~rcoulang/n1ma4w11/stalg1web.pdf.

Usage : document fourni comme support ; les preuves laissées en exercice dans ce résumé sont développées ici pour les résultats retenus.

[2] **Collectif Exo7.** *Algèbre – Cours de mathématiques, première année*. Livre librement accessible sur le site Exo7.

https://exo7.emath.fr/cours/livre-algebre-1.pdf.

Usage : lecture complémentaire pour les groupes, les morphismes, les congruences et les exemples élémentaires.

[3] **Roger Godement.** *Cours d'algèbre*, 3e édition, Hermann.

https://www.editions-hermann.fr/livre/cours-d-algebre-roger-godement.

Usage : ouvrage de référence pour approfondir les structures algébriques et pratiquer des démonstrations plus exigeantes.