Vincent Rohart

Toutes les maths en MP/MPI

et un peu plus en MP* /MPI*

MP/MP*
MPI/MPI*

- Cours complet avec démonstrations détaillées
- Compléments « étoilés » pour MP*
- 437 exercices avec corrigés détaillés : du basique à l'incontournable
- Méthodes, bilans, erreurs fréquentes, astuces

ellipses

Références sciences

Toutes les maths en MP/MPI

et un peu plus en MP*/MPI*

- Cours complet avec démonstrations détaillées
- Compléments « étoilés » pour MP*
- 437 exercices avec corrigés détaillés : du basique à l'incontournable
- Méthodes, bilans, erreurs fréquentes, astuces

MP/MP*
MPI/MPI*

Vincent Rohart

ellipses

Collection Références sciences

dirigée par Paul de Laboulaye
paul.delaboulaye@editions-ellipses.fr

Retrouvez tous les livres de la collection et des extraits sur www.editions-ellipses.fr

ISBN 9782340-069688

8/10 rue la Quintinie 75015 Paris

www.editions-ellipses.fr

*À mon ancien élève, Nicolas Chatain de Chastaing (*1997-2018*).*

Avant-propos

Les classes de seconde année des classes préparatoires scientifiques, traditionnellement appelées *Mathématiques Spéciales*, connaissent en septembre 2022 un « toilettage » de leur programme, après une réforme plus conséquente en 2014. Cet ouvrage se propose de mettre à jour le cours et les exercices de la filière MP (et de la nouvelle MPI) et leurs versions étoilées, en y apportant des conseils pour les épreuves écrites et orales que *vous* allez passer à la fin de l'année. J'ai donc rassemblé au fil de ces nombreuses pages les trucs et astuces mais aussi les pièges que j'ai pu recenser grâce à mon expérience de correcteur des épreuves écrites, et examinateur aux épreuves orales d'une grande école, dite du « groupe A », que la déontologie m'interdit de nommer.

Comme pour le précédent ouvrage de la même collection *Les Mathématiques dévoilées en MPSI* paru en 2014, je me suis efforcé de placer chaque chapitre dans son contexte historique pour que le lecteur puisse apprécier comment les Mathématiques se sont construites. D'autre part, il me semble important qu'un étudiant de MP/MPI aille au-delà de l'apprentissage brut des définitions et des théorèmes : leur histoire, ce pourquoi on les a découverts, leur donne tout leur sens.

En plus de ça, le lecteur trouvera

— un bilan par chapitre sur ce qu'il faut retenir,
— une liste d'erreurs fréquentes, des pièges classiques à éviter,
— des recettes de cuisine pour épater vos examinateurs pour un oral presque parfait,
— des exercices classés : basiques, grands classiques, plus techniques. Les exercices plus difficiles sont signalés par un $(*)$ et sont issus des oraux de concours plus exigeants.
— leurs corrections (souvent détaillées, parfois synthétiques) rassemblées en fin d'ouvrage afin que vous ne soyez pas trop tentés de les regarder (on vous connaît...)

Pour satisfaire les appétits et exigences de tout le monde, de nombreux chapitres comporteront un ou plusieurs compléments « étoilés », pour les étudiants de MP*/MPI* afin de mieux se préparer aux concours les plus difficiles : X et ENS. Attention toutefois de ne pas tomber dans le côté obscur du hors programme ! À ce propos, démystifions ce fameux corpus de connaissances noires, qui tente tellement d'étudiants.

— Quand le programme signale *non exigible*, il sera impossible d'attendre de vous que vous connaissiez ce résultat. Cela ne veut pas dire que le thème ne peut être abordé : il suffit de tout définir et de guider.
— Le *hors programme* quant à lui est plus tranché : aucune évaluation ne peut porter dessus. Toutefois, les concours les plus élitistes font souvent fi de cette subtilité et l'assimilent souvent à du *non exigible*.
— Il n'est jamais reproché à un candidat d'avoir des connaissances mathématiques avancées. En revanche, il faut maîtriser ce que l'on dit, et ne pas faire « pschiiit » à la moindre question portant sur ce que vous prononcez.
— De toute façon, on vous évaluera non pas sur le résultat, mais sur la façon avec laquelle vous y arrivez. Si la question demande de démontrer telle chose avec l'inégalité de Schwarz, il faut utiliser l'inégalité de Schwarz, sinon vous ne répondez pas à la question, peu importe si la théorie des espaces de Machin-Truc de troisième espèce trivialise la question.

En somme, s'il est bon d'avoir de la culture mathématique, si elle peut vous aiguiller intelligemment dans les exercices et vous donner du recul, elle n'est en aucune circonstance une sorte de passe-droit vous évitant de répondre aux questions posées.

Remerciements

Je remercie à nouveau les éditions ELLIPSES pour leur confiance, particulièrement Monsieur Paul de Laboulaye qui m'a motivé une cinquième fois alors que je m'étais promis d'arrêter.

En plus de LaTeX, j'ai eu besoin d'une kyrielle de « packages » pour écrire ce livre, dont `bclogo` de Maxime Chupin et Patrick Fradin : merci pour leur travail ! Les figures ont été réalisées avec PSTRICKS, GEOGEBRA, parfois MAPLE 2020 et même OPEN OFFICE ! Les illustrations (de mathématiciens par exemple) sont toutes libres de droit.

Merci à Michel Cognet qui me permet d'interroger dans sa classe de MP*1 au lycée Saint-Louis (Paris) depuis de longues années, pour ses précieux conseils,

et bien sûr merci à mes élèves qui par leur intérêt, leurs questions et leur fraîcheur d'esprit rendent passionnant le métier consistant à transmettre les Mathématiques.

Pour la relecture, je remercie Mikaël Falconet pour ses conseils en Probabilités et surtout Jean-Louis Cornou pour son colossal travail, toujours précis et avisé. S'il reste des coquilles c'est donc uniquement de ma faute. Je tiens à jour un *erratum* en ligne sur

`http://vrohart.e-monsite.com/`

dans le menu `Documents divers`. Vous pouvez aussi me contacter *via* ce site (dans l'onglet `Contact`) pour me signaler vos trouvailles en matière de coquille. Je vous en saurai le meilleur gré du monde en implorant votre indulgence.

Choix personnels

— J'ai fait le choix d'écrire « soit x et y deux réels » et non « soient x et y deux réels ». Ce n'est pas choquant : on écrit bien
  — « vive les vacances ! » et non « vivent les vacances ! »,
  — « Étant donné deux fonctions » et non « étant données deux fonctions ».
  Je précise toutefois que la forme « soient deux réels » est tolérée.
— Les ensembles usuels de nombres seront notés $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, et non $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ comme le veut la norme typographique officielle.
— Je ne parle pas de la formule du binôme *de Newton*, parce qu'elle est connue en Chine depuis au moins le X$^{\text{e}}$ siècle, et que l'arrière arrière arrière grand-père de Newton était loin d'être né. [1]
— Je mets des majuscules aux disciplines : « le Calcul intégral » (mais « un calcul intégral permet de déterminer une aire »), la Géométrie euclidienne (mais « la géométrie d'un domaine du plan »), etc.

1. Cela dit, le théorème de Pythagore n'a pas non plus été trouvé par Pythagore...

Symboles utilisés dans ce cours

	Définition.
	Théorème, lemme ou corollaire.
	Mise en garde d'une erreur fréquente.
	Recette de cuisine à aller chercher en fin de chapitre.
	Remarque historique ou culturelle.
(∗)	Résultat dépassant le cadre du programme, ou exercice ardu.
✓	Savoir-faire fondamental (en fin de chapitre).
♠	Chose à ne surtout pas faire (en fin de chapitre).
□	Fin de démonstration (introduit par Paul Halmos (1916-2006)).

$\mathrm{Com}(\mathrm{M})$	Comatrice de la matrice carrée M.
$\partial_i f$ ou $\frac{\partial f}{\partial x_i}$	Dérivée partielle i^{e} de f.
$d(x, \mathrm{A})$	Distance d'un point x à une partie A.
$\mathscr{D}_n(\mathbb{K})$	Ensemble des matrices diagonalisables sur $\mathbb{K}$.
$\mathscr{L}_p(\mathrm{E}^p, \mathrm{F})$	Espace des applications p-linéaires de E^p dans F.
$\mathcal{S}(\mathrm{E})$	Espace des endomorphismes autoadjoints de E.
$\ell^1(\mathrm{I}, \mathbb{K})$	Espace des familles sommables indexées par I.
$\mathscr{L}^1(\mathrm{I}, \mathbb{K})/\mathscr{L}^1_c(\mathrm{I}, \mathbb{K})$	Espace des fonctions [cpm/continues] intégrables.
$\mathscr{L}^2(\mathrm{I}, \mathbb{K})/\mathscr{L}^2_c(\mathrm{I}, \mathbb{K})$	Espace des fonctions [cpm/continues] de carré intégrable.
$\mathscr{M}_{n,p}(\mathbb{K})$, $\mathscr{M}_n(\mathbb{K})$	Espace des matrices de format (n, p), de format (n, n).
$\mathcal{S}_n(\mathbb{K}), \mathcal{A}_n(\mathbb{K})$	Espace des matrices symétriques, antisymétriques.
$\ell^1_{\mathscr{T},\mathbb{P}}(\Omega, \mathbb{R})$	Espace des VARD admettant une espérance.
$\ell^2_{\mathscr{T},\mathbb{P}}(\Omega, \mathbb{R})$	Espace des VARD admettant une variance.
$\mathbb{E}(\mathrm{X}), \mathbb{V}(\mathrm{X})$	Espérance, variance de la VARD X.
$\mathrm{Fr}(\mathrm{X})$	Frontière d'une partie X d'un espace normé.
$\overrightarrow{\nabla} f(a)$	Gradient de f en a.
$\mathfrak{A}_n$ ou A_n	Groupe alterné.
$\mathfrak{S}_{\mathrm{X}}$ ou S_{X}	Groupe des bijections de X sur X.
$\mathbb{U}$, $\mathbb{U}_n$	Groupe des complexes de module 1, des racines n^{e} de 1.
$\mathrm{GL}_n(\mathbb{R})$, $\mathrm{GL}(\mathrm{E})$	Groupe général linéaire.
$\mathrm{O}_n(\mathbb{R})$, $\mathrm{O}(\mathrm{E})$	Groupe orthogonal.
$\mathrm{SL}_n(\mathbb{R})$, $\mathrm{SL}(\mathrm{E})$	Groupe spécial linéaire.
$\mathrm{SO}_n(\mathbb{R})$, $\mathrm{SO}(\mathrm{E})$	Groupe spécial orthogonal.
$\mathrm{Ann}_{\mathbb{K}}(u)$	Idéal annulateur de u.
$\mathring{\mathrm{X}}$ / $\overline{\mathrm{X}}$	Intérieur / adhérence d'une partie X d'un espace normé.
$\mathfrak{R}$	Isomorphisme de Riesz d'un espace euclidien.
$\mathrm{J}_f(a)$ / $\mathrm{H}_f(a)$	Matrice jacobienne / hessienne de f en a.
$\lvert\!\lvert\!\lvert \cdot \rvert\!\rvert\!\rvert$	Norme subordonnée.
$\mathrm{A}^{\perp}$	Orthogonal d'une partie A.
π_u, χ_u	Polynôme minimal/caractéristique de u.
$\mathbb{P}_{\mathrm{B}}(\mathrm{A})$ ou $\mathbb{P}(\mathrm{A} \mid \mathrm{B})$	Probabilité conditionnelle.
ε_σ ou $\varepsilon(\sigma)$	Signature de la permutation σ de $[\![1, n]\!]$.
$\mathrm{N}_\lambda(u)$ / $\mathrm{E}_\lambda(u)$	Sous-espace caractéristique / propre de u.
$\mathrm{tr}(\mathrm{M})$ / $\det(\mathrm{M})$	Trace / déterminant de la matrice carrée M.
$\mathrm{M}^{\intercal}$	Transposée de la matrice M (anciennement ${}^{\mathrm{t}}\mathrm{M}$).
$\mathrm{X} \rightsquigarrow \mathscr{L}$	La variable aléatoire X suit la loi $\mathscr{L}$.

Abréviations usuelles

§	Paragraphe.
àpdcr	À partir d'un certain rang.
ACV	(Série) absolument convergente.
BON(D)	Base orthonormale (directe)
cf.	Se reporter à (*confere* en latin).
chap.	Chapitre.
CL, CLC	Combinaison linéaire, combinaison linéaire convexe.
CNS	Condition nécessaire et suffisante.
Coeff.	Coefficient
cpm	Continue par morceaux.
CV, CVA, CVS	Converge, absolument, simplement.
CVU, CVN	Converge uniformément, normalement.
DV, DVG	Diverge, diverge grossièrement.
DL	Développement limité.
EDLk	Équation différentielle linéaire d'ordre k.
ev	Espace vectoriel.
EVN	Espace vectoriel normé.
HR	Hypothèse de récurrence.
i.e. / c.-à-d.	C'est-à-dire (*id est* en latin).
iid	Indépendantes et identiquement distribuées.
ipp	Intégration par parties.
récip.	Réciproquement.
resp.	Respectivement.
sev	Sous-espace vectoriel.
ssi	Si et seulement si.
STP	Série à termes positifs.
TAF / IAF	Théorème/inégalité des accroissements finis.
TFCI	Théorème fondamental du Calcul intégral.
t.q.	Tel que.
TLM	Théorème de la limite monotone.
TVI	Théorème des valeurs intermédiaires.
VA(R)D	Variable aléatoire (réelle) discrète.

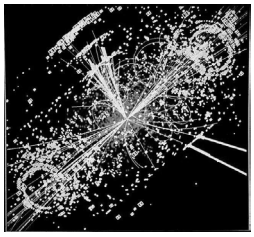
Table des matières

Chapitre 1

Des structures algébriques

Pourquoi autant généraliser, pourquoi dégager la notion de groupe, d'anneau, de corps ? Certainement pas pour le plaisir de manipuler un vocabulaire fleuri et abstrait, mais pour unifier de nombreuses situations très semblables, se réalisant dans des contextes différents. L'intérêt est double : ne pas refaire plusieurs fois la même chose, mais surtout pouvoir généraliser certains concepts et en découvrir de nouveaux.

Évariste Galois
(1811-1832)



Mise en évidence
du boson de Higgs

Le cube
de Ernő Rubik

C'est en cherchant à résoudre « par des formules » les équations polynomiales (le cas du degré 2 est étudié en Première avec la célèbre expression $\frac{-b\pm\sqrt{\Delta}}{2a}$*) que le jeune mathématicien français Évariste Galois, au destin tragique, remarqua une propriété importante de l'ensemble des permutations des racines d'un polynôme. La notion de groupe est née, mais il a fallu attendre de nombreuses années avant d'en obtenir une définition axiomatisée.*

Bien plus proche de nous, la théorie des groupes a permis de soupçonner l'existence de particules élémentaires, tel le célèbre boson de Higgs H^0*, mis en évidence en* 2013*. Pour les amateurs de casse-têtes, signalons enfin que la résolution du* Rubik's cube *regorge d'automorphismes de groupes finis !*

1 Structure de groupe

Si X est un ensemble (disons non vide), on ne peut qu'en admirer les éléments, et rien d'autre. L'Algèbre a pour but « d'habiller » X en lui donnant une structure afin de mettre en jeu ses éléments les uns avec les autres. Le lecteur sait depuis l'année dernière :

- qu'une structure de groupe sur X consiste à munir X d'une loi interne ayant certaines propriétés (rappelées dans cette section).
- qu'une structure d'espace vectoriel sur X consiste à munir X d'une loi interne $+$ et d'une loi externe $\cdot$.
- qu'une structure d'ensemble ordonné sur X consiste à munir X d'une relation d'ordre $\prec$.
- etc.

Plus généralement, si $\mathscr{F}$ est une famille (souvent finie) de lois internes, externes, de relations binaires (par exemple de relations d'ordre), on dit que le couple $(X, \mathscr{F})$ est un *magma* et que $\mathscr{F}$ est une *structure algébrique* sur X.

1.1 Groupes et sous-groupes

Définition 1

Un *groupe* est un couple $(G, \star)$, où G est un ensemble non vide et $\star$ une loi interne associative, possédant un élément neutre et dans lequel tout élément admet un symétrique.
Si en plus $\star$ est commutative, on dit que le groupe est *abélien* (ou *commutatif*).

Notations usuelles.

- L'élément neutre, qui est unique, se note souvent e ou e_G (si l'on veut être précis en cas de plusieurs groupes).
- Quant au symétrique d'un élément g, qui est unique lui aussi, on le note souvent g^{-1}.
- Le symbole $+$ pour la loi interne $\star$ est réservé pour certaines lois commutatives. Le neutre est alors noté 0_G ou simplement 0 et le symétrique d'un élément g se note $-g$ plutôt que g^{-1}, et s'appelle *l'opposé* de g. L'élément $g + (-h)$ se note de façon plus concise $g - h$.

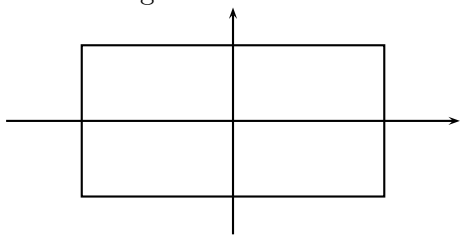
Exemples.

— $(\mathbb{R}, +)$ est un groupe abélien. Il en est de même de $(\mathbb{C}, +)$, de $(\mathbb{Z}, +)$, mais pas de $(\mathbb{N}, +)$ car 2, par exemple, n'a pas de symétrique.

— $(\mathbb{R}^*, \times)$ est un groupe abélien, tout comme $(\mathbb{R}_+^*, \times)$ et $(\mathbb{C}^*, \times)$, mais pas $(\mathbb{Z}^*, \times)$ car 2, par exemple, n'a pas de symétrique (on dit *inverse* quand la loi est $\times$).

- Si X est un ensemble quelconque, on note[1] $\mathfrak{S}_X$ l'ensemble des bijections de X sur X : c'est un groupe si on le munit de la loi de composition $\circ$. Ici, le symétrique d'une bijection $\sigma : X \to X$ est sa bijection réciproque σ^{-1}. $(\mathfrak{S}_X, \circ)$ est le *groupe symétrique de* X. On montre facilement que $\mathfrak{S}_X$ n'est pas abélien dès que X a au moins trois éléments. Le lecteur sait sûrement que si $n \in \mathbb{N}^*$, il est d'usage de noter $\mathfrak{S}_n$ au lieu de $\mathfrak{S}_{[\![1,n]\!]}$.

— *(Extrait de CentraleSupélec).* Considérons l'ensemble $\mathfrak{K}$ des isométries de $\mathbb{R}^2$ laissant invariant le rectangle $[-2, 2] \times [-1, 1]$. Nous dénombrons quatre éléments dans $\mathfrak{K}$: l'identité, la symétrie s_1 d'axe (Ox), celle, notée s_2 d'axe (Oy) et la symétrie r de centre O, qui n'est autre que la rotation d'angle π.



$\circ$	Id	s_1	s_2	r
Id	Id	s_1	s_2	r
s_1	s_1	Id	r	s_2
s_2	s_2	r	Id	s_1
r	r	s_2	s_1	Id

On dit que $\mathfrak{K}$ est le *stabilisateur* du rectangle. Pour la loi $\circ$ de composition, $\mathfrak{K}$ est un groupe. La table de la loi de ce groupe est donnée ci-dessus. On constate que $(\mathfrak{K}, \circ)$ est abélien : c'est le *groupe de Klein*.

En guise d'exercice, le lecteur est invité à montrer que l'ensemble noté $\mathfrak{D}_4$ laissant invariant un *carré* possède huit éléments et n'est pas commutatif : c'est le *groupe diédral d'indice 4*.

Définition 2

Soit $n \in \mathbb{N}^*$ et $(G_1, \star_1), \ldots, (G_n, \star_n)$ des groupes. Sur le produit cartésien $G_1 \times \ldots \times G_n$, on définit *la loi produit* $\star$ par

$$(g_1, \ldots, g_n) \star (h_1, \ldots, h_n) = (g_1 \star_1 h_1, \ldots, g_n \star_n h_n)$$

pour tous $g_1, h_1 \in G_1, \ldots g_n, h_n \in G_n$.

1. La lettre $\mathfrak{S}$ est un S en gothique allemand (écriture *Fraktur*). Les Allemands ont beaucoup contribué à l'évolution de l'Algèbre au XIX^e siècle, et ont laissé leur marque jusqu'aux noms de certains théorèmes : *Nullstellensatz* de Hilbert, *Hauptidealsatz* de Krauss, etc. Le lecteur connaît certainement la notation Ker désignant le noyau d'une application linéaire : lui-même vient de l'allemand *das Kern*.

Théorème 1 *(groupe produit)*
La loi $\star$ définie ci-dessus est une loi de groupe sur $\mathrm{G}_1 \times \ldots \times \mathrm{G}_n$. On dit que $(\mathrm{G}_1 \times \ldots \times \mathrm{G}_n, \star)$ est le *groupe produit* des groupes $(\mathrm{G}_1, \star_1), \ldots, (\mathrm{G}_n, \star_n)$.

Preuve. L'associativité est évidente. Le neutre est $(e_1, \ldots, e_n)$, où e_i désigne le neutre de $(\mathrm{G}_i, \star_i)$, et le symétrique de $(g_1, \ldots, g_n)$ est $(g_1^{-1}, \ldots, g_n^{-1})$. □

Définition 3

Soit $(\mathrm{G}, \star)$ un groupe. On appelle *sous-groupe* de $(\mathrm{G}, \star)$ toute partie H de G qui est stable par $\star$ et qui est un groupe pour la loi induite correspondante.

Dire que H est stable par $\star$ signifie que $h \star h' \in \mathrm{H}$ à chaque fois que $h, h' \in \mathrm{H}$. Ainsi, la loi $\star$ induit, par restriction, une loi interne sur H.

Théorème 2 *(caractérisation des sous-groupes)*
Soit $(\mathrm{G}, \star)$ un groupe. Une partie H de G en est un sous-groupe si et seulement si

1. La partie H n'est pas vide (en pratique on montre $e_\mathrm{G} \in \mathrm{H}$)
2. pour tous $g, h \in \mathrm{H}$, $g \star h^{-1} \in \mathrm{H}$.

Preuve. Ne pose aucun problème. Cf. cours de 1re année au besoin. □

PIÈGE !

Dans le cas d'un groupe dont la loi est notée additivement, comme par exemple $(\mathbb{Z}, +)$, la condition 2 s'écrit

$$\forall g, h \in \mathrm{H}, \quad g - h \in \mathrm{H}.$$

Théorème 3 *(sous-groupes de $(\mathbb{Z}, +)$)*
Les sous-groupes de $(\mathbb{Z}, +)$ sont exactement les parties de $\mathbb{Z}$ de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$.

Preuve. Il est clair que si $n \in \mathbb{N}$, alors $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$: utiliser la caractérisation des sous-groupes.

Réciproquement, soit H un sous-groupe de $(\mathbb{Z}, +)$. Si $H = \{0\}$, alors $H = 0\mathbb{Z}$. Sinon, il existe $x \in H \setminus \{0\}$. Si $x < 0$, alors $-x \in H$: dans tous les cas $H \cap \mathbb{N}^* \neq \varnothing$. D'après la propriété fondamentale de $\mathbb{N}$, on peut considérer $n = \min(H \cap \mathbb{N}^*)$.

Il est clair que $n\mathbb{Z} \subset H$, mais inversement, si $h \in H$, faisons la division euclidienne de h par n (licite car $n \neq 0$) : $h = nq + r$ avec $q \in \mathbb{Z}$ et $r \in [\![0, n-1]\!]$. Puisque H est un sous-groupe, $r = h - qn \in H$. Si jamais r était non nul, il serait un élément de $H \cap \mathbb{N}^*$ encore plus petit que $n = \min(H \cap \mathbb{N}^*)$, ce qui n'est pas possible. Ainsi, $r = 0$, ce qui prouve que $h = nq \in n\mathbb{Z}$ et donc que $H \subset n\mathbb{Z}$. □

Remarque. Cf. exercice 6 pour la description des sous-groupes de $(\mathbb{R}, +)$.

1.2 Sous-groupe engendré par une partie

☆ **Théorème 1** *(intersection de sous-groupes)*
Soit $(H_i)_{i\in I}$ une famille (quelconque) de sous-groupes d'un même groupe $(G, \star)$. L'intersection $\bigcap_{i\in I} H_i = \{g \in G \mid \forall i \in I,\ g \in H_i\}$ est un sous-groupe de $(G, \star)$.

Une famille $(H_i)_{i\in I}$ de sous-groupes indexée par un ensemble I, est la donnée, pour chaque $i \in I$, d'un sous-groupe H_i. Formellement, c'est donc une application $i \mapsto H_i$ de I vers l'ensemble des sous-groupes de $(G, \star)$.

Preuve. Notons H cette intersection. Puisque $e \in H_i$ pour tout $i \in I$, $e \in H$, ce qui prouve que H n'est pas vide. Soit de plus $g, h \in H$ et soit $i \in I$ quelconque. Puisque $h \in H_i$ et que H_i est un sous-groupe, on a $h^{-1} \in H_i$. Comme $g \in H_i$, on peut alors dire que $g \star h^{-1} \in H_i$. Puisque i est quelconque, cela montre que $g \star h^{-1} \in H$. D'après la caractérisation des sous-groupes, H est bien un sous-groupe de $(G, \star)$. □

☆ **Corollaire**
Soit $(G, \star)$ un groupe et A une partie quelconque de G (même vide). Il existe un plus petit (au sens de $\subset$) sous-groupe de $(G, \star)$ contenant A.

Preuve. Considérons l'ensemble I de tous les sous-groupes de $(G, \star)$ contenant A et considérons $\bigcap_{H\in I} H$: c'est un sous-groupe de $(G, \star)$ d'après le théorème précédent et il contient A puisque si $a \in A$, alors $a \in H$ pour tout $H \in I$. Par construction, il est inclus dans tout sous-groupe contenant A, c'est donc bien le plus petit de tous ces sous-groupes. □

Définition

Le plus petit (au sens de l'inclusion) sous-groupe contenant la partie A s'appelle *le sous-groupe engendré par* A. On le note $\langle \mathrm{A} \rangle$ ou parfois $\mathrm{gr}(\mathrm{A})$.

Par exemple, $\langle \varnothing \rangle = \{e_\mathrm{G}\}$.

Théorème 2 *(description de $\langle \mathrm{A} \rangle$)*
Soit $(\mathrm{G}, \star)$ un groupe et A une partie de G. Le sous-groupe $\langle \mathrm{A} \rangle$ engendré par A est constitué des éléments de G de la forme

$$a_1^{\varepsilon_1} \star \ldots \star a_n^{\varepsilon_n},$$

avec $n \in \mathbb{N}$, $a_1, \ldots, a_n \in \mathrm{A}$ et $\varepsilon_1, \ldots, \varepsilon_n \in \{-1, 1\}$ quelconques, et la convention que cet élément désigne e_G si $n = 0$.

Preuve. L'ensemble E des éléments décrits ci-dessus est un sous-groupe de G : il contient e_G, il est stable par produit (évident) et l'inverse de $a_1^{\varepsilon_1} \star \ldots \star a_n^{\varepsilon_n}$ est $a_n^{-\varepsilon_n} \star \ldots \star a_1^{-\varepsilon_1}$ (attention à l'ordre !), qui est bien de la forme décrite. Ce sous-groupe contient bien sûr A (prendre $n = 1$ et $\varepsilon_1 = 1$). De plus si, H est un sous-groupe contenant A, il contient tous les éléments de la forme $a_1^{\varepsilon_1} \star \ldots \star a_n^{\varepsilon_n}$, donc $\mathrm{E} \subset \mathrm{H}$. Cela prouve que $\mathrm{E} = \langle \mathrm{A} \rangle$. □

Cas particulier. Si $(\mathrm{G}, +)$ est commutatif, $\langle \mathrm{A} \rangle$ est l'ensemble des éléments de G de la forme

$$\lambda_1 a_1 + \ldots + \lambda_n a_n$$

avec $n \in \mathbb{N}$, $\lambda_1, \ldots, \lambda_n \in \mathbb{Z}$ et $a_1, \ldots, a_n \in \mathrm{A}$. Il est possible alors d'imiter les notations de l'Algèbre linéaire et de noter $\mathrm{Vect}_\mathbb{Z}(a_1, \ldots, a_n)$ l'ensemble de ces éléments, alors appelées *combinaisons linéaires entières*. Cette remarque donne peut-être envie au lecteur de voir un groupe abélien comme un « $\mathbb{Z}$-espace vectoriel » [2] : ceci est le début d'une longue et riche histoire...

Exemple 1. Dans le groupe $(\mathbb{Z}, +)$, la partie $\{1\}$ est génératrice : $\mathbb{Z} = \langle 1 \rangle$ (notation fréquente, en lieu et place de $\langle \{1\} \rangle$).

Exemple 2. L'ensemble $\mathfrak{T}_n$ des transpositions de $[\![1, n]\!]$ engendre le groupe symétrique $(\mathfrak{S}_n, \circ)$ (cf. cours de 1re année). On peut même faire mieux : si $\tau_{a,b}$ désigne la transposition échangeant uniquement a et b (deux éléments distincts dans $[\![1, n]\!]$), alors $\mathfrak{S}_n = \langle \tau_{1,2}, \tau_{2,3}, \ldots, \tau_{n-1,n} \rangle$.

2. On parle plutôt de $\mathbb{Z}$-*module* au lieu de « $\mathbb{Z}$-espace vectoriel » et on note $\mathrm{Mod}_\mathbb{Z}(a_1, \ldots, a_n)$ au lieu de $\mathrm{Vect}_\mathbb{Z}(a_1, \ldots, a_n)$.

Exemple 3. Le groupe $(\mathbb{Q},+)$ n'est pas engendré par un nombre fini d'éléments. En effet, soit $q_1,\dots,q_n$ des rationnels non nuls. Pour tout $i\in[\![1,n]\!]$, notons $\frac{a_i}{b_i}$ la forme irréductible de q_i et posons $\mathrm{D}=\mathrm{ppcm}(b_1,\dots,b_n)$. Un élément de $\langle q_1,\dots,q_n\rangle$ est de la forme

$$\lambda_1 q_1+\ldots+\lambda_n q_n,\quad \text{avec } \lambda_1,\dots,\lambda_n\in\mathbb{Z}.$$

Un tel rationnel s'écrit donc $\frac{c}{\mathrm{D}}$ avec $c\in\mathbb{Z}$. Puisque D ne possède qu'un nombre fini de diviseurs, on peut considérer un entier $\mathrm{N}\in\mathbb{N}^*$ qui n'est pas un diviseur de D. La fraction $\frac{1}{\mathrm{N}}$ ne saurait donc être de la forme $\frac{c}{\mathrm{D}}$, ce qui prouve que $\langle q_1,\dots,q_n\rangle\neq\mathbb{Q}$.

☆ **Théorème 3** *(pgcd et ppcm dans $\mathbb{Z}$)*
Soit a,b dans $\mathbb{Z}$. Alors $a\mathbb{Z}+b\mathbb{Z}$ est le sous-groupe engendré par a et b. De plus,

$$a\mathbb{Z}+b\mathbb{Z}=\mathrm{pgcd}(a,b)\mathbb{Z}\quad\text{et}\quad a\mathbb{Z}\cap b\mathbb{Z}=\mathrm{ppcm}(a,b)\mathbb{Z}.$$

Notation.

- Il est fréquent de noter $a\wedge b$ le PGCD de a et b, et $a\vee b$ leur PPCM [3].
- Il est possible de noter $\mathrm{Vect}_{\mathbb{Z}}(a,b)$ au lieu de $a\mathbb{Z}+b\mathbb{Z}$: c'est l'ensemble des entiers de la forme $au+bv$ (avec $u,v\in\mathbb{Z}$).

Preuve. Le fait que $\langle a,b\rangle=a\mathbb{Z}+b\mathbb{Z}$ est une conséquence du théorème 2. Puisque $a\mathbb{Z}+b\mathbb{Z}$ et $a\mathbb{Z}\cap b\mathbb{Z}$ sont des sous-groupes de $(\mathbb{Z},+)$, on peut écrire $a\mathbb{Z}+b\mathbb{Z}=d\mathbb{Z}$ et $a\mathbb{Z}\cap b\mathbb{Z}=m\mathbb{Z}$ avec $d,m\in\mathbb{N}$.

Ensuite, $\mathrm{pgcd}(a,b)$ divise à la fois a et b, donc $\mathrm{pgcd}(a,b)\mathbb{Z}$ est un sous-groupe contenant a et b, et comme $d\mathbb{Z}$ est le plus petit des sous-groupes à contenir a et b, on a $d\mathbb{Z}\subset\mathrm{pgcd}(a,b)\mathbb{Z}$. Inversement, le théorème de Bézout assure [4] le fait que $\mathrm{pgcd}(a,b)\in a\mathbb{Z}+b\mathbb{Z}$, et donc que $\mathrm{pgcd}(a,b)\mathbb{Z}\subset d\mathbb{Z}$.

Enfin, puisque $\mathrm{ppcm}(a,b)$ est à la fois un multiple de a et b : $\mathrm{ppcm}(a,b)\mathbb{Z}\subset m\mathbb{Z}$. Inversement, en supposant que $a\neq0$ et $b\neq0$ (sinon le résultat est évident), on a $\mathrm{ppcm}(a,b)\neq0$. La division euclidienne de m par $\mathrm{ppcm}(a,b)$ donne $m=\mathrm{ppcm}(a,b)q+r$ avec $0\leqslant r<\mathrm{ppcm}(a,b)$. Mais r est alors la différence de deux multiples communs de a et b, donc en est un aussi. Puisque $\mathrm{ppcm}(a,b)$ est par définition le plus petit non nul d'entre eux, on a nécessairement $r=0$. Cela prouve que $m\in\mathrm{ppcm}(a,b)\mathbb{Z}$ et donc que $m\mathbb{Z}\subset\mathrm{pgcd}(a,b)\mathbb{Z}$. □

3. L'explication est la suivante. Dans un ensemble ordonné $(\mathrm{E},\prec)$ (cf. cours de 1re année), on note $a\wedge b$ la borne inférieure, si elle existe, de la paire $\{a,b\}$. Dans $(\mathbb{N},\leqslant)$, $a\wedge b$ est donc $\min(a,b)$. Mais dans $(\mathbb{N},|)$ (relation de divisibilité), $a\wedge b$ est le plus grand des minorants de $\{a,b\}$, c'est-à-dire le plus grand des entiers m tels que $m\mid a$ et $m\mid b$: c'est $\mathrm{pgcd}(a,b)$. Notons que dans $(\mathscr{P}(\mathrm{X}),\subset)$, $\mathrm{A}\wedge\mathrm{B}$ n'est autre que $\mathrm{A}\cap\mathrm{B}$, ce qui explique la notation $\wedge$.

4. Précisément, on peut écrire $a=a'\mathrm{pgcd}(a,b)$ et $b=b'\mathrm{pgcd}(a,b)$ avec a',b' premiers entre eux. Le théorème de Bézout nous dit qu'il existe $u,v\in\mathbb{Z}$ tels que $a'u+b'v=1$. En multipliant tout par $\mathrm{pgcd}(a,b)$, on obtient $\mathrm{pgcd}(a,b)=au+bv\in a\mathbb{Z}+b\mathbb{Z}$.

1.3 Morphismes de groupes

Tout comme pour les espaces vectoriels, si on dispose d'une application d'un groupe vers un autre, il est naturel de ne s'intéresser qu'aux applications qui « respectent » les lois de ces groupes.

Définition 1

Soit $(\mathrm{G}, \star)$ et $(\mathrm{H}, \intercal)$ deux groupes. On appelle *morphisme de groupes* de $(\mathrm{G}, \star)$ vers $(\mathrm{H}, \intercal)$ toute application $f : \mathrm{G} \to \mathrm{H}$ telle que

$$\forall x, y \in \mathrm{G}, \quad f(x \star y) = f(x) \intercal f(y).$$

On dit aussi *homomorphisme* au lieu de *morphisme*. L'ensemble des morphismes de groupes de $(\mathrm{G}, \star)$ vers $(\mathrm{H}, \intercal)$ se note $\mathrm{Hom}((\mathrm{G}, \star), (\mathrm{H}, \intercal))$ ou simplement $\mathrm{Hom}(\mathrm{G}, \mathrm{H})$ s'il n'y a pas d'ambiguïté.

Exemple 1. L'application exponentielle (réelle) est un morphisme de groupes de $(\mathbb{R}, +)$ vers $(\mathbb{R}_+^*, \times)$. L'exponentielle complexe, quant à elle, en est un de $(\mathbb{C}, +)$ vers $(\mathbb{C}^*, \times)$.

Exemple 2. Le logarithme népérien est un morphisme de groupes de $(\mathbb{R}_+^*, \times)$ vers $(\mathbb{R}, +)$.

Exemple 3. La fonction carré est un morphisme de $(\mathbb{R}^*, \times)$ vers lui-même.

Exemple 4. La signature ε est un morphisme de groupes de $(\mathfrak{S}_n, \circ)$ vers $(\{-1, 1\}, \times)$. Rappelons que pour $\sigma \in \mathfrak{S}_n$, une définition possible de $\varepsilon(\sigma)$ est $(-1)^{\mathrm{I}(\sigma)}$ où $\mathrm{I}(\sigma)$ est le nombre d'inversions que présente σ. On appelle ainsi tout couple $(i, j) \in [\![1, n]\!]^2$ tel que $i < j$ et $\sigma(i) > \sigma(j)$. On démontre[5] alors que

$$\varepsilon(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(j) - \sigma(i)}{j - i},$$

ce qui permet d'établir que $\varepsilon(\sigma \circ \tau) = \varepsilon(\sigma) \times \varepsilon(\tau)$ pour tous $\sigma, \tau \in \mathfrak{S}_n$.

Exemple 5. L'application $\vartheta \mapsto \mathrm{R}_\vartheta$ où $\mathrm{R}_\vartheta = \begin{pmatrix} \cos\vartheta & -\sin\vartheta \\ \sin\vartheta & \cos\vartheta \end{pmatrix}$ (matrice de rotation) est un morphisme du groupe $(\mathbb{R}, +)$ dans le groupe spécial orthogonal $(\mathrm{SO}_2(\mathbb{R}), \times)$. En effet, $\mathrm{R}_{\vartheta+\vartheta'} = \mathrm{R}_\vartheta \times \mathrm{R}_{\vartheta'}$ (composer deux rotations c'est ajouter leurs angles !). Il est même surjectif.

5. Cf. par exemple *Les Mathématiques dévoilées*, du même auteur.

Théorème 1 *(propriétés des morphismes)*
Soit f un morphisme de groupes de $(\mathrm{G}, \star)$ vers $(\mathrm{H}, \intercal)$.

1. Si on note e_G et e_H les neutres de ces groupes, alors $f(e_\mathrm{G}) = e_\mathrm{H}$.
2. Pour tout $g \in \mathrm{G}$, $f(g^{-1}) = f(g)^{-1}$.

Preuve. 1. Écrivons $f(e_\mathrm{G}) = f(e_\mathrm{G} \star e_\mathrm{G}) = f(e_\mathrm{G}) \intercal f(e_\mathrm{G})$. En composant à droite (par exemple) par $f(e_\mathrm{G})^{-1}$, on obtient donc $e_\mathrm{H} = f(e_\mathrm{G})$.

2. Remarquons que $f(g) \intercal f(g^{-1}) = f(g \star g^{-1}) = f(e_\mathrm{G}) = e_\mathrm{H}$ d'après ce qui précède. De même, $f(g^{-1}) \intercal f(g) = f(e_\mathrm{G}) = e_\mathrm{H}$. Cela montre que le symétrique de $f(g)$ est $f(g^{-1})$. □

Si $f : \mathrm{X} \to \mathrm{Y}$ est une application, et si $\mathrm{A} \subset \mathrm{X}$ et $\mathrm{B} \subset \mathrm{Y}$, on rappelle que l'on note $f\langle \mathrm{A} \rangle$ l'ensemble des images des éléments de A et $f^{-1}\langle \mathrm{B} \rangle$ l'ensemble des antécédents des éléments de B.

Théorème 2 *(images directes et réciproques)*
Soit f un morphisme de groupes de $(\mathrm{G}, \star)$ vers $(\mathrm{H}, \intercal)$.

1. Si G' est un sous-groupe de $(\mathrm{G}, \star)$, l'image directe $f\langle \mathrm{G}' \rangle$ est un sous-groupe de $(\mathrm{H}, \intercal)$.
2. Si H' est un sous-groupe de $(\mathrm{H}, \intercal)$, l'image réciproque $f^{-1}\langle \mathrm{H}' \rangle$ est un sous-groupe de $(\mathrm{G}, \star)$.

Preuve. 1. Soit $g, h \in f\langle \mathrm{G}' \rangle$. On peut écrire $g = f(x)$ et $h = f(y)$ avec $x, y \in \mathrm{G}'$. On a alors $g \intercal h^{-1} = f(x) \intercal f(y^{-1}) = f(x \star y^{-1})$, ce qui montre que $g \intercal h^{-1} \in \mathrm{G}'$. On conclut d'après la caractérisation des sous-groupes.

2. Soit $g, h \in f^{-1}\langle \mathrm{H}' \rangle$. On a donc $f(g) \in \mathrm{H}'$ et $f(h) \in \mathrm{H}'$, de sorte que $f(g \star h^{-1})$ vaut $f(g) \intercal f(h^{-1}) \in \mathrm{H}'$ car H' est un sous-groupe. On conclut par la même caractérisation. □

Définition 2

Soit f un morphisme de groupes de $(\mathrm{G}, \star)$ vers $(\mathrm{H}, \intercal)$.

- On appelle *image de* f, le sous-groupe $f\langle \mathrm{G} \rangle$, noté $\mathrm{Im}(f)$, de $(\mathrm{H}, \intercal)$.
- On appelle *noyau de* f, le sous-groupe $f^{-1}\langle \{e_\mathrm{H}\} \rangle$, noté $\mathrm{Ker}(f)$, de $(\mathrm{G}, \star)$.

Évidemment, un morphisme $f : \mathrm{G} \to \mathrm{H}$ est surjectif si et seulement si $\mathrm{Im}(f) = \mathrm{H}$: c'est la définition de la surjectivité. De façon duale, on a la caractérisation suivante de l'injectivité.

☆ **Théorème 3** *(caractérisation de l'injectivité)*
Soit f un morphisme de groupes de $(\mathrm{G}, \star)$ vers $(\mathrm{H}, \intercal)$.
Alors f est injectif si et seulement si $\mathrm{Ker}(f) = \{e_{\mathrm{G}}\}$.

Preuve. Si f est injectif, l'équation $f(x) = e_{\mathrm{H}}$ s'écrit $f(x) = f(e_{\mathrm{G}})$ et n'a donc qu'une seule solution : e_{G}. Cela montre que $\mathrm{Ker}(f) = \{e_{\mathrm{G}}\}$.

Réciproquement, supposons que $\mathrm{Ker}(f) = \{e_{\mathrm{G}}\}$. Si $x, y \in \mathrm{G}$ sont tels que $f(x) = f(y)$, on a $f(x) \intercal f(y)^{-1} = e_{\mathrm{H}}$, ou encore $f(x \star y^{-1}) = e_{\mathrm{H}}$, ce qui entraîne par hypothèse $x \star y^{-1} = e_{\mathrm{G}}$, ou encore $x = y$. Ainsi, f est injectif. □

Exemple de référence 1. L'application $\begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C}^* \\ z & \longmapsto & \mathrm{e}^z \end{array}$ est un morphisme du groupe $(\mathbb{C}, +)$ dans $(\mathbb{C}^*, \times)$. Étant surjectif, son image est $\mathbb{C}^*$, mais son noyau est $2\mathrm{i}\pi\mathbb{Z}$ car le lecteur sait depuis la 1re année que

$$\forall z, z' \in \mathbb{C}, \quad \mathrm{e}^z = \mathrm{e}^{z'} \iff \exists k \in \mathbb{Z},\ z = z' + 2\mathrm{i}k\pi.$$

À l'inverse, l'exponentielle réelle $\begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R}^* \\ x & \longmapsto & \mathrm{e}^x \end{array}$ est un morphisme de groupes de $(\mathbb{R}, +)$ dans $(\mathbb{R}^*, \times)$ qui est injectif mais dont l'image est $\mathbb{R}_+^*$.

Exemple de référence 2. Le noyau de $\varepsilon : \mathfrak{S}_n \to \{-1, 1\}$ est l'ensemble des *permutations paires*. On le note $\mathfrak{A}_n$: c'est le *groupe alterné d'indice n*.

☆ **Théorème 4** *(composée de morphismes de groupes)*
La composée de deux morphismes de groupes est un morphisme de groupes.

Preuve. Considérons $(\mathrm{G}, \star)$, $(\mathrm{H}, \intercal)$ et $(\mathrm{K}, \diamond)$ trois groupes, et $f : \mathrm{G} \to \mathrm{H}$, $g : \mathrm{H} \to \mathrm{K}$ deux morphismes de groupes. Pour tous $x, y \in \mathrm{G}$ on a

$$g \circ f(x \star y) = g(f(x \star y)) = g(f(x) \intercal f(y)) = g(f(x)) \diamond g(f(y)) = \Big[g \circ f(x)\Big] \diamond \Big[g \circ f(y)\Big].$$

ce qui prouve que $g \circ f : \mathrm{G} \to \mathrm{K}$ est un morphisme de groupes. □

☆ **Corollaire** *(isomorphisme de groupes)*
Si un morphisme de groupes est bijectif, sa réciproque est aussi un morphisme de groupes.

Preuve. Soit f un morphisme de groupes bijectif, de $(\mathrm{G},\star)$ sur $(\mathrm{H},\intercal)$. Pour tous $x,y\in\mathrm{H}$, on peut écrire $x=f(f^{-1}(x))$ et $y=f(f^{-1}(y))$, donc

$$f^{-1}(x\intercal y)=f^{-1}\Big(f(f^{-1}(x))\intercal f(f^{-1}(y))\Big)=f^{-1}\Big(f\Big[f^{-1}(x)\star f^{-1}(y)\Big]\Big).$$

qui vaut $f^{-1}(x)\star f^{-1}(y)$ puisque $f^{-1}\circ f=\mathrm{Id}_{\mathrm{G}}$, ce qui montre que f^{-1} est un morphisme de groupes, de $(\mathrm{H},\intercal)$ sur $(\mathrm{G},\star)$. □

Vocabulaire. On adopte les mêmes racines grecques[6] qu'en Algèbre linéaire :

- Un morphisme d'un groupe dans lui-même s'appelle un *endomorphisme* de groupes.
- Un morphisme bijectif s'appelle un *isomorphisme* de groupes.
- Un endomorphisme bijectif s'appelle un *automorphisme* de groupes.

Quand il existe au moins un isomorphisme d'un groupe sur un autre, on dit que ces deux groupes sont *isomorphes*. Ils ont alors les mêmes propriétés algébriques (si l'un est commutatif, l'autre aussi, etc.) de sorte qu'il n'y a aucun moyen de les distinguer du point de vue de la théorie des groupes.

Exemple 1. Les groupes $(\mathbb{R},+)$ et $(\mathbb{R}_+^*,\times)$ sont isomorphes car exp est un isomorphisme de $(\mathbb{R},+)$ sur $(\mathbb{R}_+^*,\times)$. L'isomorphisme réciproque est ln.

Exemple 2. Les groupes $(\mathbb{R},+)$ et $(\mathbb{R}^*,\times)$ ne sont pas isomorphes. En effet, imaginons un instant que f soit un isomorphisme de $(\mathbb{R}^*,\times)$ sur $(\mathbb{R},+)$ et considérons l'équation $x^2=1$ dans $\mathbb{R}^*$. Puisque f est bijective, cette équation équivaut à $f(x^2)=f(1)$, soit à $2f(x)=0$ car f envoie neutre sur neutre, c'est-à-dire $f(1)=0$. Mais l'équation $x^2=1$ admet deux solutions, tandis que $2f(x)=0$ en admet qu'une seule : $f(x)=0$, soit $x=1$. On trouve ainsi une absurdité.

☆ **Théorème 5** *(le groupe* $\mathrm{Aut}(\mathrm{G})$*)*
Si $(\mathrm{G},\star)$ est un groupe, l'ensemble $\mathrm{Aut}(\mathrm{G})$ des automorphismes de groupes de $(\mathrm{G},\star)$ est lui-même un groupe pour la loi de composition $\circ$.

Preuve. $\mathrm{Aut}(\mathrm{G})$ est en fait un sous-groupe de $(\mathfrak{S}_{\mathrm{G}},\circ)$ (le groupe de toutes les bijections de G sur G) : facile grâce à la caractérisation des sous-groupes. □

6. En grec, ἔνδον : à l'intérieur, ἴσος : égal et αὐτός : lui-même. Pour le lecteur amateur de vocabulaire savant, un morphisme injectif s'appelle un *monomorphisme* tandis qu'un morphisme surjectif est un *épimorphisme* (ἐπί : sur).

1.4 Les groupes cycliques $(\mathbb{Z}/n\mathbb{Z}, +)$

Motivation. S'il est 11 heures et que l'on doit se rendre à un rendez-vous dans 3 heures, nous devrons y être à $11 + 3 = 14$ heures, ou encore à 2 heures. On est donc tenté de définir une nouvelle opération, encore notée $+$, pour laquelle $11 + 3 = 2$: c'est *l'addition modulo 12*. Il se trouve que cette nouvelle addition est une loi de groupe.

Rappel.
Soit $n \in \mathbb{N}$. La relation binaire $\equiv_n$ sur $\mathbb{Z}$ définie par $a \equiv_n b$ si et seulement si $a - b \in n\mathbb{Z}$ est une relation d'équivalence : c'est la *congruence modulo n*. On note aussi $a \equiv b\ [n]$. La classe d'équivalence de l'entier k se notera $\bar{k}$, $\dot{k}$ ou parfois $[k]_n$.

- Si $n = 0$, on obtient la relation d'égalité. Il y a donc une infinité de classes d'équivalence : les $\{n\}$ avec $n \in \mathbb{Z}$.
- Si $n \in \mathbb{N}^*$, il y a exactement n classes d'équivalences : $\bar{0}, \bar{1}, \ldots, \overline{n-1}$.

Notation. L'ensemble $\{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ des classes d'équivalence de la relation $\equiv_n$ se note $\mathbb{Z}/n\mathbb{Z}$ (lire « $\mathbb{Z}$ sur $n\mathbb{Z}$ »). Ses éléments sont *les entiers modulo n*.

Remarque 1. Si $n = 0$, alors $\mathbb{Z}/0\mathbb{Z} = \{\{k\} \mid k \in \mathbb{Z}\}$. L'ensemble $\mathbb{Z}/0\mathbb{Z}$ est donc en bijection avec $\mathbb{Z}$, *via* $k \mapsto \{k\}$.

Remarque 2. Si $n = 1$, l'ensemble $\mathbb{Z}/\mathbb{Z}$ est un singleton : $\{\bar{0}\}$. En effet, la relation d'équivalence modulo 1 est la relation triviale, c'est-à-dire celle où tout le monde est équivalent à tout le monde !

Théorème 1 *(structure de groupe sur $\mathbb{Z}/n\mathbb{Z}$)*
Soit $n \in \mathbb{N}^*$. Il existe une et une seule loi de groupe, encore notée $+$, sur $\mathbb{Z}/n\mathbb{Z}$ pour laquelle l'application $k \mapsto \bar{k}$ soit un morphisme de groupes, c'est-à-dire telle que

$$\forall k, \ell \in \mathbb{Z}, \quad \overline{k + \ell} = \bar{k} + \bar{\ell}.$$

Preuve. *Analyse.* Si une telle loi de groupe existe, elle est forcément unique puisque si $x, y \in \mathbb{Z}/n\mathbb{Z}$, il existe $k, \ell \in \mathbb{Z}$ tels que $x = \bar{k}$ et $y = \bar{\ell}$ et on impose à $x + y$ de valoir $\overline{k + \ell}$.

Synthèse. Cette relation définit correctement une loi interne car si $\bar{k} = \bar{k}'$ et $\bar{\ell} = \bar{\ell}'$, on aura $k - k' \in n\mathbb{Z}$ et $\ell - \ell' \in n\mathbb{Z}$, donc en ajoutant, $(k + \ell) - (k' + \ell') \in n\mathbb{Z}$, ce qui montre que $\overline{k + \ell} = \overline{k' + \ell'}$. Ainsi, la classe $\overline{k + \ell}$ ne dépend bien que des classes $\bar{k}$ et $\bar{\ell}$ et non du choix de représentants particuliers. Cette loi est bien une loi de groupe. Elle est associative car pour tous $k, \ell, m \in \mathbb{Z}$,

$$(\bar{k} + \bar{\ell}) + \bar{m} = \overline{k + \ell} + \bar{m} = \overline{k + \ell + m} = \bar{k} + \overline{\ell + m} = \bar{k} + (\bar{\ell} + \bar{m}).$$

Il est clair que $\bar{0}$ le neutre et que si $k \in \mathbb{Z}$, le symétrique de $\bar{k}$ est $\overline{-k}$. □

Exemple. La table de la loi + dans $\mathbb{Z}/_{4\mathbb{Z}}$ est :

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

.

☆ **Théorème 2** *(règle de calcul dans $\mathbb{Z}/_{n\mathbb{Z}}$)*
Soit $n \in \mathbb{N}^*$. Pour tout $\bar{k} \in \mathbb{Z}/_{n\mathbb{Z}}$ (avec $k \in \mathbb{Z}$) et $p \in \mathbb{Z}$,

$$p \cdot \bar{k} = \overline{pk},$$

où $p \cdot \bar{k}$ est bien sûr défini comme étant $\bar{k} + \ldots + \bar{k}$ (p fois) si $p > 0$, 0 si $p = 0$ et $\overline{-k} + \ldots + \overline{-k}$ ($-p$ fois) si $p < 0$.

Preuve. Résulte du fait que $f : x \mapsto \bar{x}$ est un morphisme de groupes. Précisément, $\bar{k} + \bar{k} = f(k) + f(k) = f(k+k) = \overline{2k}$, puis par récurrence, $pf(k) = f(pk)$ pour tout $p \in \mathbb{N}^*$. Si $p < 0$, $f(pk) + f((-p)k) = f(pk - pk) = f(0) = \bar{0}$, donc $f(pk) = -f(pk)$, ce qui donne le résultat voulu. □

1.5 Groupes monogènes et cycliques

La notion de groupe engendré $\langle \mathrm{A} \rangle$ par une partie A a été définie au § 1.2. Si A est un singleton $\{x\}$, on notera $\langle x \rangle$ au lieu de $\langle \{x\} \rangle$. Le théorème qui suit est un cas particulier de la description de $\langle \mathrm{A} \rangle$ vue au § 1.2.

☆ **Théorème 1** *(description de $\langle x \rangle$)*
Soit $(\mathrm{G}, \star)$ un groupe et $x \in \mathrm{G}$. Les éléments du sous-groupe engendré par x sont les éléments de G de la forme x^n avec $n \in \mathbb{Z}$ quelconque :

$$\langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}.$$

Un tel sous-groupe est nécessairement abélien.

Remarque. En notation additive, $\langle x \rangle = \{nx \mid n \in \mathbb{Z}\}$.

Définition 1

Soit $(G, \star)$ un groupe.

- On dit que $(G, \star)$ est un *groupe monogène* quand il existe $x \in G$ tel que $G = \langle x \rangle$.
- Un tel élément x est appelé un *générateur* de $(G, \star)$.
- Un *groupe cyclique* est un groupe monogène fini.

Exemple fondamental n°1. Le groupe $(\mathbb{Z}, +)$ est monogène car engendré par 1 (mais aussi par -1). Il n'est toutefois pas cyclique car il n'est pas fini. On note que les seuls générateurs de $(\mathbb{Z}, +)$ sont 1 et -1.

Exemple fondamental n°2. Le groupe $(\mathbb{Z}/_{n\mathbb{Z}}, +)$ (avec $n \in \mathbb{N}^*$) est engendré par $\bar{1}$. En effet, si $x \in \mathbb{Z}/_{n\mathbb{Z}}$, alors $x = \bar{k}$ avec $k \in [\![1, n]\!]$, et $\bar{k} = \bar{1} + \ldots + \bar{1}$ (k fois), donc $x = k \cdot \bar{1}$. Ainsi, $(\mathbb{Z}/_{n\mathbb{Z}}, +)$ est un groupe cyclique.

Contrairement à $\mathbb{Z}$, $\mathbb{Z}/_{n\mathbb{Z}}$ possède de nombreux générateurs. Le théorème suivant les décrit tous.

Théorème 2 *(générateurs de $(\mathbb{Z}/_{n\mathbb{Z}}, +)$)*
Soit $n \in \mathbb{N}^*$. Les générateurs du groupe cyclique $(\mathbb{Z}/_{n\mathbb{Z}}, +)$ sont les $\bar{k}$ avec $k \in [\![0, n-1]\!]$ premier avec n.

Preuve. Soit $k \in [\![0, n-1]\!]$ tel que $\bar{k}$ engendre $\mathbb{Z}/_{n\mathbb{Z}}$. En particulier, $\bar{1}$ peut s'écrire $\bar{1} = u\bar{k} = \overline{uk}$ avec $u \in \mathbb{Z}$. Cela signifie que $1 = uk + vn$ avec $v \in \mathbb{Z}$. Si d est un diviseur positif commun de k et de n, alors d divise 1, donc $d = 1$. Ainsi, $\text{pgcd}(k, n) = 1$, c'est-à-dire k et n sont premiers entre eux.

Inversement, si k et n sont premiers entre eux, le théorème de Bézout nous assure l'existence d'un couple $(u, v) \in \mathbb{Z}^2$ tel que $ku + nv = 1$, si bien que $\overline{ku} + \bar{0} = \bar{1}$. Si maintenant $\bar{c}$ est un élément quelconque de $\mathbb{Z}/_{n\mathbb{Z}}$, alors $\bar{c} = c \cdot \bar{1} = c\overline{u}\overline{k}$, ce qui prouve que $\bar{k}$ engendre $\mathbb{Z}/_{n\mathbb{Z}}$. □

Exemple. Le groupe $(\mathbb{Z}/_{12\mathbb{Z}}, +)$ possède quatre générateurs : $\bar{1}$, $\bar{5}$, $\bar{7}$ et $\bar{11}$. Sur les figures ci-dessus, on met en évidence le caractère générateur de $\bar{1}$ et $\bar{7}$, et au contraire le fait que $\bar{4}$ n'engendre qu'un sous-groupe ayant 3 éléments.

Le théorème suivant classifie définitivement tous les groupes monogènes et nous informe que les deux exemples fondamentaux précédents sont les seuls cas possibles, à isomorphisme près.

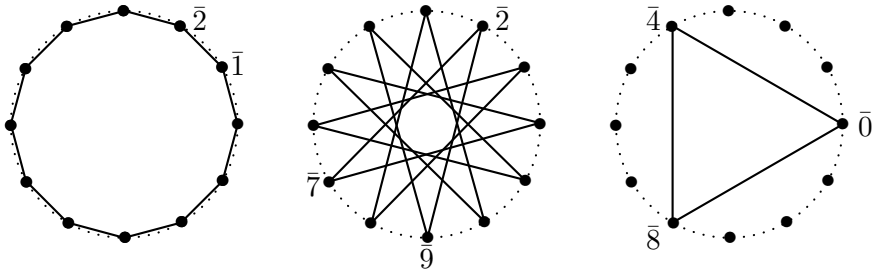


FIGURE 1.1 – Le groupe $\mathbb{Z}/12\mathbb{Z}$: $\bar{1}$ et $\bar{7}$ sont générateurs, mais pas $\bar{4}$.

☆ **Théorème 3** *(description des groupes monogènes)*
Un groupe monogène est ou bien isomorphe à $(\mathbb{Z}, +)$ s'il est infini, ou bien isomorphe à $(\mathbb{Z}/_{n\mathbb{Z}}, +)$ s'il est fini de cardinal n.

Ainsi, le seul groupe cyclique possédant n éléments est, à isomorphisme près, $(\mathbb{Z}/_{n\mathbb{Z}}, +)$.

Preuve. Soit $(\mathrm{G}, \star)$ un groupe monogène. Notons x un de ses générateurs, c'est-à-dire un élément $x \in \mathrm{G}$ tel que $\mathrm{G} = \langle x \rangle$. Considérons alors l'application

$$f : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathrm{G} \\ k & \longmapsto & x^k. \end{array}$$

Cette application f est surjective par construction, et est un morphisme de groupes car $x^{k+k'} = x^k \star x^{k'}$.

• Si f est injective, alors f est un isomorphisme de $(\mathbb{Z}, +)$ sur $(\mathrm{G}, \star)$, et en particulier, G est infini.

• Sinon, $\mathrm{Ker}(f)$ est un sous-groupe de $(\mathbb{Z}, +)$ non réduit à $\{0\}$, donc $\mathrm{Ker}(f) = n\mathbb{Z}$ avec $n \in \mathbb{N}^*$. Définissons $\hat{f} : \mathbb{Z}/_{n\mathbb{Z}} \to \mathrm{G}$ par

$$\hat{f}(\bar{k}) = f(k)$$

pour tout $k \in \mathbb{Z}$, où $\bar{k}$ désigne la classe modulo n de k. Cette application est correctement définie car si $\bar{k} = \bar{\ell}$, alors $k - \ell = nd$ avec $d \in \mathbb{Z}$, donc $x^{k-\ell} = (x^n)^d = e_{\mathrm{G}}^d = e_{\mathrm{G}}$ (ceci car $n \in \mathrm{Ker}(f) = n\mathbb{Z}$). On a donc $f(k) = f(\ell)$, ce qui montre que $\hat{f}(\bar{k})$ ne dépend que de $\bar{k}$ et non du choix d'un des représentants de cette classe d'équivalence.

L'application $\hat{f}$ est surjective, car si $g \in \mathrm{G}$, $g = x^k = f(k)$ pour un certain $k \in \mathbb{Z}$ (n'oublions pas que x est un générateur de G) et donc $g = \hat{f}(\bar{k})$. Mais l'application $\hat{f}$ est aussi injective car si $\hat{f}(\bar{k}) = e_{\mathrm{G}}$, pour un certain $k \in \mathbb{Z}$, on aura $f(k) = e_{\mathrm{G}}$, c'est-à-dire $k \in n\mathbb{Z}$, autrement dit, $\bar{k} = \bar{0}$.

En conclusion, $\hat{f}$ est un isomorphisme de $(\mathbb{Z}/_{n\mathbb{Z}}, +)$ sur $(\mathrm{G}, \star)$ et en particulier G est fini et possède n éléments. □

On rappelle que si $n \in \mathbb{N}^*$, $\mathbb{U}_n$ désigne le groupe des racines n-ièmes de l'unité, c'est-à-dire les $z \in \mathbb{C}$ tels que $z^n = 1$.

☆ Corollaire
Pour tout $n \in \mathbb{N}^*$, les groupes $(\mathbb{Z}/_{n\mathbb{Z}}, +)$ et $(\mathbb{U}_n, \times)$ sont isomorphes.

Preuve. Il suffit de montrer que $(\mathbb{U}_n, \times)$ est cyclique. C'est le cas car ce groupe est fini (possède n éléments) et est engendré par $\omega = \mathrm{e}^{\frac{2\mathrm{i}\pi}{n}}$: en effet, $z \in \mathbb{U}_n$, z s'écrit $r\mathrm{e}^{\mathrm{i}\vartheta}$ avec $r > 0$ et $\vartheta \in \mathbb{R}$. Le fait que z^n entraîne $r = 1$ et $n\vartheta \equiv 0\ [2\pi]$, soit $z = \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}k} = \omega^k$ avec $k \in \mathbb{Z}$. □

D'après la preuve précédente, on peut même affirmer qu'un isomorphisme de $\mathbb{Z}/_{n\mathbb{Z}}$ sur $\mathbb{U}_n$ est $\bar{k} \mapsto \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}k}$, application correctement définie car $\mathrm{e}^{\mathrm{i}\frac{2\pi}{n}k}$ ne dépend que de $\bar{k}$, et non du choix d'un représentant de la classe d'équivalence $\bar{k}$.

Conséquence. Les générateurs de $(\mathbb{U}_n, \times)$ sont les $\mathrm{e}^{\mathrm{i}\frac{2\pi}{n}k}$ où $k \in [\![0, n-1]\!]$ est premier avec n : ce sont les *racines primitives n-ièmes de l'unité*.

Définition 2
Si $n \in \mathbb{N}^*$, on note $\varphi(n)$ le nombre d'entiers $k \in [\![0, n-1]\!]$ premiers avec n. L'application $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ s'appelle *l'indicatrice d'Euler*.

Ainsi, $\varphi(n)$ est le nombre de générateurs d'un groupe cyclique ayant n éléments. Nous verrons au § 2.3 comment calculer $\varphi(n)$ grâce à la décomposition de n en facteurs premiers.

Exemple de groupe abélien non cyclique. Le groupe $(\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}, +)$ n'est pas cyclique. En effet, posons $e = (\bar{0}, \bar{0})$ son élément neutre, et $a = (\bar{0}, \bar{1})$, $b = (\bar{1}, \bar{0})$ et $c = (\bar{1}, \bar{1})$. La table du groupe produit $(\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}, +)$ est

$+$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

.

Le lecteur remarquera que c'est la table du groupe de Klein $(\mathfrak{K}, \circ)$ qui stabilise un rectangle (exemple page 3). On constate que tout élément $x \neq e$ vérifie $2x = e$: il n'existe donc pas de générateur. En revanche, on peut remarquer que $\langle a, b\rangle = \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$.

Le lecteur remarquera qu'au contraire, le groupe produit $\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{3\mathbb{Z}}$ est cyclique. En effet, $g = (\bar{1}, \dot{1})$ est générateur puisque

$$2g = (\bar{0}, \dot{2}), \quad 3g = (\bar{1}, \dot{0}), \quad 4g = (\bar{0}, \dot{1}), \quad 5g = (\bar{1}, \dot{2})$$

ce qui montre que $\{(\bar{0}, \dot{0}), g, 2g, \ldots, 5g\} = \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{3\mathbb{Z}}$.

1.6 Ordre d'un élément dans un groupe

Définition

Soit $(\mathrm{G}, \star)$ un groupe et $x \in \mathrm{G}$. On dit que x *est d'ordre fini* si le sous-groupe $\langle x \rangle$ qu'il engendre possède un nombre fini d'éléments.
Ce nombre, qui est un entier naturel non nul, s'appelle alors *l'ordre* de x et se note $\mathrm{ord}(x)$ ou $\omega(x)$.

Remarque. Si $(\mathrm{G}, \star)$ est un groupe, on dit que G est *l'ensemble sous-jacent* à ce groupe. Si cet ensemble est fini, son cardinal s'appelle *l'ordre* du groupe $(\mathrm{G}, \star)$. Toutefois, on fera l'abus répandu de parler du *cardinal* du groupe $(\mathrm{G}, \star)$ pour parler de $\mathrm{Card}(\mathrm{G})$.

Rappel.

Si x est un élément d'ordre d de G, l'application $f : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathrm{G} \\ k & \longmapsto & x^k. \end{array}$ est un morphisme de groupes, avec $\mathrm{Im}(f) = \langle x \rangle$ et $\mathrm{Ker}(f) = d\mathbb{Z}$ (cf. preuve du théorème 3 du § précédent). De plus l'application $\hat{f} : \bar{k} \mapsto x^k$ est correctement définie et est un isomorphisme de $\mathbb{Z}/_{d\mathbb{Z}}$ sur $\langle x \rangle$.

Théorème 1

Si x est d'ordre fini $d \in \mathbb{N}^*$ dans le groupe $(\mathrm{G}, \star)$, alors

$$\langle x \rangle = \{e, x, x^2, \ldots, x^{d-1}\},$$

où e désigne le neutre de $(\mathrm{G}, \star)$. De plus, $\mathrm{ord}(x)$ est le plus petit entier $n \in \mathbb{N}^*$ tel que $x^n = e$.

Remarque. En notation additive, $\langle x \rangle = \{0, x, 2x, \ldots, (d-1)x\}$.

Preuve. Avec les notations du rappel, puisque $\mathbb{Z}/_{d\mathbb{Z}} = \{\bar{0}, \bar{1}, \ldots, \overline{d-1}\}$, on en déduit que $\langle x \rangle = \{\hat{f}(\bar{0}), \hat{f}(\bar{1}), \ldots, \hat{f}(\overline{d-1})\} = \{e, x, x^2, \ldots, x^{d-1}\}$. On a aussi $x^d = \hat{f}(\overline{d}) = \hat{f}(\bar{0}) = e$ et si $0 \leqslant k < d$, alors $x^k = \hat{f}(\bar{k}) \neq e$ car $\bar{k} \neq \bar{0}$ et $\hat{f}$ est injective. □

☆ Corollaire
Soit x un élément d'ordre d dans un groupe $(\mathrm{G}, \star)$ de neutre e. Alors pour tout $n \in \mathbb{Z}$,

$$x^n = e \iff d \mid n.$$

Preuve. L'application $\hat{f} : \bar{k} \mapsto x^k$ est une bijection de $\mathbb{Z}/_{d\mathbb{Z}}$ sur $\langle x \rangle$, donc $x^n = e$ équivaut à $(\hat{f})^{-1}(x^n) = (\hat{f})^{-1}(e)$, c'est-à-dire à $\bar{n} = \bar{0}$ ou encore à $n \equiv 0\ [d]$. □

☆ Théorème 2
Soit $(\mathrm{G}, \star)$ un groupe fini.
L'ordre d'un élément de G divise Card(G). En particulier, pour tout $x \in \mathrm{G}$, $x^{\mathrm{Card(G)}} = e$.

Preuve. *Cas où* G *est abélien.* Notons $g_1, \ldots, g_n$ les éléments de G. Soit x un élément particulier de G ($x = g_i$ pour un certain i) et d son ordre. L'application $a \mapsto x \star a$ est une bijection de G sur G (car x est inversible) donc

$$g_1 \star \ldots \star g_n = (x \star g_1) \star \ldots \star (x \star g_n).$$

Puisque $\star$ est commutative, $(x \star g_1) \star \ldots \star (x \star g_n) = x^n \star (g_1 \star \ldots \star g_n)$. Si on note π le composé de tous les éléments de G, on a donc $\pi = x^n \star \pi$, et donc $x^n = e$ en simplifiant. En vertu du corollaire précédent, $d \mid n$.

Cas où G *est non abélien (preuve non exigible).* Soit $g \in \mathrm{G}$. Notons d son ordre. On considère la relation binaire $\mathscr{R}_g$ définie par

$$\forall x, y \in \mathrm{G}, \quad x \mathscr{R}_g y \iff x^{-1} y \in \langle g \rangle.$$

On vérifie sans mal que $\mathscr{R}_g$ est une relation d'équivalence sur G. La classe $[x]$ d'un élément x de G est

$$\{y \in \mathrm{G} \mid \exists k \in \mathbb{Z},\ y = xg^n\} = \{x, xg, xg^2, \ldots, xg^{d-1}\}.$$

Cette classe contient d éléments : en effet, si $xg^k = xg^\ell$ avec $k, \ell \in [\![0, d-1]\!]$, alors $g^{k-\ell} = e$, donc $|k - \ell|$ divise d, ce qui n'est possible que si $k = \ell$ puisque $|k - \ell| < d$. Comme pour toute relation d'équivalence, G est partitionné par ses classes d'équivalence. Si N désigne le nombre de classes d'équivalence, on a donc $\mathrm{G} = \bigcup_{i=1}^{\mathrm{N}} [x_i]$ avec $x_1, \ldots, x_{\mathrm{N}} \in \mathrm{G}$. Ainsi,

$$\mathrm{Card(G)} = \sum_{i=1}^{\mathrm{N}} \mathrm{Card}([x_i]) = \sum_{i=1}^{\mathrm{N}} d = \mathrm{N}d$$

ce qui montre bien que d divise Card(G). □

Remarque $(*)$**.** Le lecteur adaptera sans aucun problème la preuve du cas non abélien (non exigible) à un sous-groupe quelconque H de G, pas nécessairement un sous-groupe monogène $\langle g \rangle$. Il considèrera la relation binaire $\mathscr{R}_{\mathrm{H}}$ définie par $x \mathscr{R}_{\mathrm{H}} y \iff x^{-1} y \in \mathrm{H}$ et montrera que la classe de x est $x\mathrm{H} = \{xh \mid h \in \mathrm{H}\}$, qui a le même cardinal que H. Il établira donc le *théorème de Lagrange* (qui n'est pas écrit au programme officiel) :

Dans un groupe fini de cardinal n, abélien ou non, le cardinal d'un sous-groupe quelconque divise n.

Par exemple, $(\mathfrak{S}_3, \circ)$, groupe de cardinal 6, ne possède pas de sous-groupe à 4 éléments, ni à 5 éléments.

Corollaire 2
Tout groupe de cardinal un nombre premier est nécessairement cyclique. De plus, tout élément différent du neutre en est un générateur.

Preuve. Soit $(\mathrm{G}, \star)$ un groupe dont le cardinal, noté p, est un nombre premier. Si $g \in \mathrm{G} \setminus \{e\}$ (possible car $p \geqslant 2$), alors $\mathrm{ord}(g) > 1$ et $\mathrm{ord}(g)$ divise p d'après le théorème précédent. Puisque p est premier, $\mathrm{ord}(g) = p$, ce qui signifie que $\langle g \rangle$ est une partie de cardinal p de l'ensemble G : on a donc $\langle g \rangle = \mathrm{G}$. □

PIÈGE !
La réciproque est évidemment fausse : $(\mathbb{Z}/_{4\mathbb{Z}}, +)$ est cyclique, pourtant 4 n'est pas premier.

Théorème 3 *(hors programme, mais classique)*
Soit x et y des éléments d'ordre fini d'un groupe $(\mathrm{G}, \star)$. On suppose que

1. les éléments x et y commutent : $x \star y = y \star x$,
2. leurs ordres sont premiers entre eux : $\mathrm{pgcd}(\mathrm{ord}(x), \mathrm{ord}(y)) = 1$.

Alors $\mathrm{ord}(x \star y) = \mathrm{ord}(x)\mathrm{ord}(y)$.

Preuve. Notons m et n les ordres de x et y respectivement et notons d celui de $x \star y$. Puisque x et y commutent, $(x \star y)^{mn} = x^{mn} \star y^{mn} = (x^m)^n \star (y^n)^m = e \star e = e$, ce qui prouve déjà que $d \mid mn$ (corollaire du théorème 1).

Ensuite, puisque $(x \star y)^d = e$ et que x et y commutent, on a $x^d \star y^d = e$, soit $x^d = y^{-d}$. Ainsi,

$$x^{nd} = (x^d)^n = (y^{-d})^n = (y^n)^{-d} = e^{-d} = e,$$

donc $m \mid nd$ et comme m et n sont premiers entre eux on en déduit que $m \mid d$ (c'est le lemme de Gauss). De la même façon, $n \mid d$. La propriété fondamentale des PPCM implique que $\mathrm{ppcm}(m, n) \mid d$, c'est-à-dire $mn \mid d$ (car m et n sont premiers entre eux). Finalement, $mn = d$. □

2 Structures d'anneaux et de corps

2.1 Généralités

Définition 1

On appelle *anneau* tout triplet $(\mathrm{A}, +, \times)$ où A est un ensemble non vide, et où $+$ et $\times$ sont deux lois internes sur A telles que

- $(\mathrm{A}, +)$ soit un groupe commutatif, dont le neutre est traditionnellement noté 0_A,
- $\times$ est associative,
- $\times$ possède un élément neutre, traditionnellement noté 1_A,
- $\times$ est distributive sur $+$ c'est-à-dire

$$\forall x, y, z \in \mathrm{A}, \quad \begin{cases} x \times (y+z) &= (x \times y) \ + \ (x \times z), \\ (y+z) \times x &= (y \times x) \ + \ (z \times x). \end{cases}$$

Si $\times$ est en plus commutative, on dit que l'anneau $(\mathrm{A}, +, \times)$ est *commutatif*. Il est d'usage de noter xy au lieu de $x \times y$.

Si $n \in \mathbb{Z}$ et $a \in \mathrm{A}$, on définit $n \cdot a$ (aussi noté na, mais pas $n \times a$ cependant) de façon naturelle. Si $n \in \mathbb{N}$, on définit aussi a^n (par convention $a^0 = 1_\mathrm{A}$).

Exemples de référence.

- Tout singleton $\mathrm{A} = \{a\}$ est muni d'une unique structure d'anneau en posant $a + a = a$ et $a \times a = a$. Tout anneau de cette forme est appelé *anneau nul*. Dans un tel anneau, on notera que l'on a $0_\mathrm{A} = 1_\mathrm{A}$.
- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ munis des lois usuelles sont des anneaux commutatifs.
- Si $(\mathrm{A}, +, \times)$ est un anneau commutatif, l'ensemble $\mathrm{A}[\mathrm{X}]$ des polynômes à coefficients dans A est un anneau commutatif.
- Si $n \in \mathbb{N}^*$, et si $(\mathrm{A}, +, \times)$ est un anneau commutatif, l'ensemble $\mathscr{M}_n(\mathrm{A})$ des matrices carrées de taille n à coefficients dans A est un anneau pour l'addition et la multiplication matricielles, non commutatif si $n > 1$.
- Si E est un espace vectoriel, l'ensemble $\mathscr{L}(\mathrm{E})$ des endomorphismes de E est un anneau pour $+$ et $\circ$, non commutatif dès que $\dim(\mathrm{E}) > 1$.
- Si X est un ensemble et A un anneau, l'ensemble $\mathscr{F}(\mathrm{X}, \mathrm{A})$ (aussi noté A^X) des applications de X dans A est un anneau pour l'addition et la multiplication des fonctions. Si A est commutatif, $\mathscr{F}(\mathrm{X}, \mathrm{A})$ l'est aussi.

Théorème 1 *(règles de calcul)*
Soit $(\mathrm{A}, +, \times)$ un anneau. Pour tous $a, b \in \mathrm{A}$ et $n \in \mathbb{Z}$,

- $a \times 0_\mathrm{A} = 0_\mathrm{A} \times a = 0_\mathrm{A}$ (on dit que 0_A est *absorbant*).
- $(-a) \times b = a \times (-b) = -(a \times b)$ et $(-a) \times (-b) = a \times b$.
- $(n \cdot a) \times b = a \times (n \cdot b) = n \cdot (a \times b)$.
- Si en plus a et b commutent (c'est-à-dire $ab = ba$), alors

  (i) $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot a^k b^{n-k}$ (formule du binôme),

  (ii) $a^{n+1} - b^{n+1} = (a-b) \sum_{k=0}^{n} a^k b^{n-k}$ (identité de Bernoulli),

Preuve. Cf. cours de 1re année. □

Théorème 2 *(groupe des inversibles d'un anneau)*
Soit $(\mathrm{A}, +, \times)$ un anneau. Les éléments inversibles de A, c'est-à-dire les $x \in \mathrm{A}$ tels qu'il existe $y \in \mathrm{A}$ vérifiant $xy = yx = 1_\mathrm{A}$, forment un groupe pour $\times$.

Il est d'usage de noter $\mathrm{A}^\times$ ou parfois $\mathcal{U}_\mathrm{A}$ l'ensemble des inversibles de l'anneau A. La notation $\mathcal{U}_\mathrm{A}$ s'explique du fait que les inversibles d'un anneau ont anciennement été appelés les *unités* de cet anneau.

Exemples. $\mathbb{Z}^\times = \{-1, 1\}$, $\mathbb{R}^\times = \mathbb{R}^*$, $\mathbb{C}[\mathrm{X}]^\times = \mathbb{C}^*$ et $\mathscr{M}_n(\mathbb{R})^\times = \mathrm{GL}_n(\mathbb{R})$.

Preuve. Premièrement $\mathrm{A}^\times$ contient 1_A. Ensuite, si x et y sont dans $\mathrm{A}^\times$, alors xy aussi car $y^{-1}x^{-1}$ est son inverse. À ce stade $\times$ est une loi interne sur $\mathrm{A}^\times$. Elle est évidemment associative. Ensuite si $x \in \mathrm{A}^\times$, $x^{-1} \in \mathrm{A}^\times$, car son inverse est x. □

Définition 2

On dit qu'un anneau $(\mathrm{A}, +, \times)$ est *intègre* quand il est commutatif, non nul (c'est-à-dire $1_\mathrm{A} \neq 0_\mathrm{A}$) et que pour tous $a, b \in \mathrm{A}$,

$$a \times b = 0_\mathrm{A} \quad \Longrightarrow \quad \Big[a = 0_\mathrm{A} \ \text{ ou } \ b = 0_\mathrm{A}\Big].$$

Exemple 1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des anneaux intègres. Il en va de même de $\mathrm{A}[\mathrm{X}]$ où A est un anneau intègre.

Exemple 2. L'anneau $\mathcal{F}(\mathbb{R},\mathbb{R})$ des fonctions de $\mathbb{R}$ dans $\mathbb{R}$ n'est pas intègre : ni $\mathbb{1}_{\mathbb{R}_+}$ ni $\mathbb{1}_{\mathbb{R}_-^*}$ ne sont nulles, mais leur produit l'est.

☆ **Théorème 3** *(produit fini d'anneaux)*
Soit $n \in \mathbb{N}^*$ et $\mathrm{A}_1, \ldots, \mathrm{A}_n$ des anneaux. On munit l'ensemble $\mathrm{A}_1 \times \ldots \times \mathrm{A}_n$, aussi noté $\prod_{i=1}^{n} \mathrm{A}_i$, d'une structure d'anneau en posant,

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n),$$

$$(x_1, \ldots, x_n) \times (y_1, \ldots, y_n) = (x_1 \times y_1, \ldots, x_n \times y_n).$$

Muni de ces lois, $\mathrm{A}_1 \times \ldots \times \mathrm{A}_n$ s'appelle *l'anneau produit* de $\mathrm{A}_1, \ldots, \mathrm{A}_n$.

Preuve. Sans difficulté. Le neutre de $+$ est $(0_{\mathrm{A}_1}, \ldots, 0_{\mathrm{A}_n})$ et celui de $\times$ est $(1_{\mathrm{A}_1}, \ldots, 1_{\mathrm{A}_n})$. □

Remarque. Dès que $n > 1$, un produit d'anneaux, même intègres, n'est pas intègre. En effet, $(0,1) \times (1,0) = (0,0)$.

Définition 3

Soit $(\mathrm{A}, +, \times)$ un anneau, et soit $\mathrm{B} \subset \mathrm{A}$ une partie de A. On dit que B est un *sous-anneau* de $(\mathrm{A}, +, \times)$ quand

1. B est un sous-groupe de $(\mathrm{A}, +)$ (ce qui force à avoir $0_{\mathrm{A}} \in \mathrm{B}$),
2. $1_{\mathrm{A}} \in \mathrm{B}$,
3. B est stable par $\times$, c'est-à-dire $\forall b, b' \in \mathrm{B},\ b \times b' \in \mathrm{B}$.

On vérifie sans mal que pour les lois $+$ et $\times$ restreintes à B, B est alors un anneau, avec $0_{\mathrm{B}} = 0_{\mathrm{A}}$ et $1_{\mathrm{B}} = 1_{\mathrm{A}}$.

Exemples

- Si $n \in \mathbb{N}$ est tel que $n \neq 1$, l'ensemble $n\mathbb{Z}$ n'est pas un sous-anneau de $(\mathbb{Z}, +, \times)$ bien qu'il soit un sous-groupe de $(\mathbb{Z}, +)$ et stable par $\times$: il ne contient pas 1.
- Les ensembles $\mathcal{T}_n^+(\mathbb{R})$ et $\mathcal{T}_n^-(\mathbb{R})$ des matrices triangulaires supérieures, resp. inférieures, sont des sous-anneaux de $(\mathcal{M}_n(\mathbb{R}), +, \times)$.
- Pour tout $k \in \mathbb{N} \cup \{\infty\}$, $\mathcal{C}^k(\mathrm{I}, \mathbb{C})$ (où I est un intervalle de longueur non nulle) est un sous-anneau de $\mathcal{F}(\mathrm{I}, \mathbb{C})$.

Définition 4

Soit $(\mathrm{A}, +, \times)$ et $(\mathrm{B}, +, \times)$ deux anneaux. On appelle *morphisme d'anneaux* de A dans B toute application $f : \mathrm{A} \to \mathrm{B}$ telle que pour tout $(a, b) \in \mathrm{A}^2$,

$$f(a+b) = f(a) + f(b), \quad f(a \times b) = f(a) \times f(b), \quad f(1_\mathrm{A}) = 1_\mathrm{B}.$$

Quand f est bijective, on parle *d'isomorphisme d'anneaux*.

PIÈGE !

L'égalité $f(0_\mathrm{A}) = 0_\mathrm{B}$ est automatique : elle résulte du fait que f est un morphisme de groupes de $(\mathrm{A}, +)$ dans $(\mathrm{B}, +)$. En revanche, la condition $f(1_\mathrm{A}) = 1_\mathrm{B}$ est indépendante du fait que $\forall a, b \in \mathrm{A},\ f(a \times b) = f(a) \times f(b)$.

Propriétés faciles.

- Si $a \in \mathrm{A}$ est inversible alors $f(a)$ aussi et $f(a)^{-1} = f(a^{-1})$.
- Si f est un isomorphisme d'anneaux de A sur B, sa réciproque f^{-1} en est un de B sur A.
- La composée de deux morphismes d'anneaux en est un aussi.

Théorème 4

1. Quels que soient les anneaux A et B, $(\mathrm{A} \times \mathrm{B})^\times = \mathrm{A}^\times \times \mathrm{B}^\times$.
2. Si A et B sont deux anneaux isomorphes, les groupes $\mathrm{A}^\times$ et $\mathrm{B}^\times$ sont isomorphes.

Preuve. 1. Soit $a \in \mathrm{A}$ et $b \in \mathrm{B}$. Dire que (a, b) est inversible, c'est dire qu'il existe $(a', b') \in \mathrm{A} \times \mathrm{B}$ tel que $(a, b) \times (a', b') = (1_\mathrm{A}, 1_\mathrm{B}) = (a', b') \times (a, b)$, c'est donc dire que $(aa', bb') = (1_\mathrm{A}, 1_\mathrm{B}) = (a'a, b'b)$, c'est-à-dire $(a, b) \in \mathrm{A}^\times \times \mathrm{B}^\times$.

2. Soit $f : \mathrm{A} \to \mathrm{B}$ un isomorphisme d'anneaux : il envoie $\mathrm{A}^\times$ dans $\mathrm{B}^\times$ (cf. propriétés faciles ci-dessus) et on peut donc considérer l'application induite $\tilde{f} : \mathrm{A}^\times \to \mathrm{B}^\times$ définie par $\tilde{f}(a) = f(a)$ pour tout $a \in \mathrm{A}^\times$. C'est un morphisme de groupes (car f respecte $\times$, donc $\tilde{f}$ aussi), injectif (car f l'est déjà). Enfin, si $b \in \mathrm{B}^\times$, posons $a = f^{-1}(b)$: cet élément est dans $\mathrm{A}^\times$, car son inverse est $f^{-1}(b^{-1})$. Par construction $\tilde{f}(a) = b$, donc $\tilde{f}$ est surjectif. □

Définition 5

On appelle *corps* tout anneau commutatif non nul (c'est-à-dire ayant au moins deux éléments), tel que tout élément non nul est inversible.
Un *sous-corps* d'un corps, est un sous-anneau du corps en question : c'est lui-même un corps pour les lois induites par restriction.

Ainsi, si $(\mathrm{K}, +, \times)$ est un corps alors $\mathrm{K}^\times = \mathrm{K}^*$. Un corps est un cas particulier d'anneau intègre puisque la relation $xy = 0$ entraîne, si $x \neq 0$, $x^{-1}xy = x^{-1}0 = 0$, soit $y = 0$.

Exemple 1. $\mathbb{Q}, \mathbb{R}$ sont des sous-corps de $\mathbb{C}$ (pour les opérations usuelles), mais $\mathbb{Z}$ n'en est pas un, bien qu'étant intègre.

Exemple 2. L'ensemble $\mathrm{K}(\mathrm{X})$ des fractions rationnelles sur un corps K est un corps (cf. cours de MPSI), mais pas $\mathrm{K}[\mathrm{X}]$, qui n'est qu'un anneau intègre.

Exemple 3. L'ensemble $\mathbb{Q}(\sqrt{2})$ des réels de la forme $a + b\sqrt{2}$ avec $a, b \in \mathbb{Q}$ est un sous-corps de $\mathbb{R}$. En effet, remarquons déjà que pour tous $a, b \in \mathbb{Q}$, $a + b\sqrt{2} = 0 \iff a = b = 0$ (car $\sqrt{2}$ est irrationnel). Cela étant dit, si $a + b\sqrt{2} \neq 0$, alors $a - b\sqrt{2} \neq 0$ d'après ce que l'on vient de dire et

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = a' + b'\sqrt{2}$$

avec $a' = \frac{a}{a^2-2b^2} \in \mathbb{Q}$ et $b' = \frac{-b}{a^2-2b^2} \in \mathbb{Q}$, si bien que $a + b\sqrt{2}$ est inversible dans $\mathbb{Q}(\sqrt{2})$.

Théorème 5

Soit $f : \mathrm{K} \to \mathrm{A}$ un morphisme d'anneaux. Si K est un corps et A n'est pas réduit à $\{0_\mathrm{A}\}$, alors f est nécessairement injectif.

Preuve. Montrons que $\mathrm{Ker}(f) = \{0_\mathrm{K}\}$. Soit $x \in \mathrm{K}$ tel que $f(x) = 0_\mathrm{A}$. Si x n'était pas nul, on pourrait considérer son inverse (car K est un corps), et $f(xx^{-1}) = f(1_\mathrm{K}) = 1_\mathrm{A}$. Or $f(xx^{-1}) = f(x)f(x^{-1}) = 0_\mathrm{A} \times f(x^{-1}) = 0_\mathrm{A}$. On a donc $0_\mathrm{A} = 1_\mathrm{A}$: absurde car $\mathrm{A} \neq \{0_\mathrm{A}\}$. □

2.2 Idéaux d'un anneau commutatif

Motivation. Si $f : \mathrm{A} \to \mathrm{B}$ est un morphisme d'anneaux, son image $\mathrm{Im}(f)$ est un sous-anneau de B. En revanche, son noyau $\{x \in \mathrm{A} \mid f(x) = 0_\mathrm{B}\}$ **n'est pas** un sous-anneau de A : il ne contient pas 1_A (sauf bien sûr dans le cas

exceptionnel de l'anneau nul où $1_A = 0_A$). Cependant, $\mathrm{Ker}(f)$ est un sous-groupe de $(A, +)$ qui, à défaut de contenir 1_A, jouit d'une propriété plus forte que la stabilité par $\times$:

$$\forall x \in \mathrm{Ker}(f),\ \boxed{\forall a \in A},\quad xa \in \mathrm{Ker}(f).$$

En effet, $f(xa) = f(x)f(a) = 0_B \times f(a) = 0_B$. On dit que $\mathrm{Ker}(f)$ est *absorbant*.

Définition 1

Soit $(A, +, \times)$ un anneau commutatif. Une partie I de A est appelée *idéal* de l'anneau $(A, +, \times)$ quand

1. I est un sous-groupe de $(A, +)$,
2. I est absorbant, c'est-à-dire $\forall i \in I,\ \forall a \in A,\ i \times a \in I$, ce que l'on écrit plus rapidement $IA \subset I$.

Remarque 1. Si I est un idéal de l'anneau $(A, +, \times)$ et si I contient 1_A alors nécessairement $I = A$. Plus généralement, si I contient ne serait-ce qu'un élément inversible x, alors $I = A$, car alors $xx^{-1} = 1_A \in I$.

Remarque 2. Les idéaux d'un corps $(K, +, \times)$ sont en conséquence réduits aux idéaux triviaux : $\{0_K\}$ et K.

Remarque 3. Les noyaux des morphismes d'anneaux sont des idéaux de l'anneau de départ (très important).

Remarque $(*)$**.** Si $(A, +, \times)$ n'est pas commutatif, on distingue les *idéaux à gauche*, c'est-à-dire ceux vérifiant $AI \subset I$ des *idéaux à droite* qui vérifient quant à eux $IA \subset I$. Un idéal à la fois à gauche et à droite est qualifié de *bilatère*.

Théorème 1 *(idéaux de $\mathbb{Z}$)*
Les idéaux de l'anneau $(\mathbb{Z}, +, \times)$ sont les parties de $\mathbb{Z}$ de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$.

Preuve. Les sous-groupes de $(\mathbb{Z}, +)$ sont les parties de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$ (cf. théorème 3 du § 1.1, page 4). Le fait que ces parties soient absorbantes est immédiat. □

Théorème 2 *(idéaux de K[X])*
Soit K un corps. Les idéaux de l'anneau $(K[X], +, \times)$ sont les parties de K[X] de la forme $PK[X] = \{PQ \mid Q \in K[X]\}$ avec $P \in K[X]$.

Preuve. Sensiblement la même[7] que pour $\mathbb{Z}$. Tout d'abord, les parties de la forme PK[X] sont des idéaux (vérification facile). Inversement, si I est un idéal de K[X], que l'on suppose non réduit à $\{0\}$, considérons

$$\mathscr{D} = \{\deg(A) \mid A \in I \setminus \{0\}\}$$

qui est une partie non vide de $\mathbb{N}$, et qui admet donc un élément minimal d. On peut donc considérer $P \in I \setminus \{0\}$ tel que $\deg(P) = d$. Si $A \in I$ est quelconque, la division euclidienne de A par P s'écrit $A = PQ + R$ avec $Q, R \in K[X]$ et $\deg(R) < d$. Puisque I est un idéal, $R = Q - AP \in I$, ce qui force R à être nul, sans quoi $\deg(R)$ serait un élément de $\mathscr{D}$ plus petit que $\min(\mathscr{D})$. En conclusion, $A = PQ \in PK[X]$ et comme A est quelconque dans I, $I \subset PK[X]$. L'inclusion réciproque est évidente par définition d'un idéal. □

Vocabulaire. Un anneau commutatif A est dit *principal* quand ses idéaux sont tous principaux, c'est-à-dire de la forme $a\mathrm{A}$ avec $a \in \mathrm{A}$: on vient donc de montrer que $\mathbb{Z}$ et K[X], si K est corps, sont des anneaux principaux.

PIÈGE !

Si K n'est pas un corps, l'anneau K[X] n'est pas principal : cf. exercice.

Définition 2

Soit $(\mathrm{A}, +, \times)$ un anneau commutatif et soit a et b deux éléments de A. On dit que a divise b, et on note $a \mid b$, quand il existe $c \in \mathrm{A}$ tel que $b = ac$, autrement dit quand b est un multiple de a.

Ainsi, $a \mid b \iff b\mathrm{A} \subset a\mathrm{A}$: la notion d'idéal sert à traduire la divisibilité dans un anneau commutatif.

Définition 3

Lorsque $a\mathrm{A} = b\mathrm{A}$, on dit que a et b sont *associés* : $a \mid b$ et $b \mid a$.

Théorème 2 *(éléments associés)*

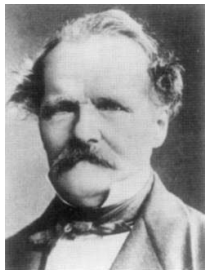
Soit $(\mathrm{A}, +, \times)$ un anneau commutatif.

1. La relation « être associés » est une relation d'équivalence sur A.
2. Si l'anneau est en plus intègre, a et b sont associés si et seulement s'il existe un élément inversible u tel que $a = ub$.

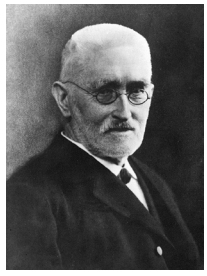
7. $\mathbb{Z}$ et $\mathbb{K}[X]$ sont deux proches cousins dans la grande famille des anneaux : ils possèdent tous deux un outil redoutable appelé *division euclidienne*.

Preuve. 1. est facile. Pour 2., si $a = ub$ avec u inversible, alors $b = u^{-1}a$, ce qui prouve que $b \mid a$ et $a \mid b$. Réciproquement, si $b \mid a$ et $a \mid b$, alors $a = ub$ et $b = va$ avec $u, v \in \mathrm{A}$, donc $a = uva$ ou encore $a(uv - 1_\mathrm{A}) = 0_\mathrm{A}$. Si l'anneau est intègre, $a = 0_\mathrm{A}$ (dans ce cas $b = ay = 0_\mathrm{A}$ aussi) ou $uv = 1_\mathrm{A}$, ce qui force u (et v) à être inversible. □

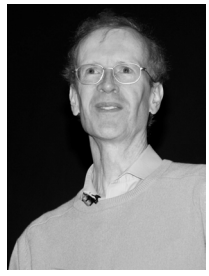
Le terme *idéal* peut paraître incongru. En quoi un idéal est-il *idéal* ? Ce mot a été introduit au XIX^e siècle par le mathématicien allemand E. Kummer qui cherchait à imiter la décomposition en facteurs irréductibles, bien connue dans $\mathbb{Z}$ ou $\mathbb{K}[X]$, dans certains anneaux centraux dans la résolution de la célèbre équation de Fermat « $x^n + y^n = z^n$ ». Malheureusement, une telle décomposition n'était pas possible, et Kummer montra que ces « nombres idéaux » pouvant se décomposer en facteurs irréductibles n'existaient pas toujours. Plus tard, R. Dedekind prouva que dans une large classe d'anneaux qui portent aujourd'hui son nom, ce ne sont pas les éléments qui se décomposent, mais certains sous-groupes additifs : les idéaux tels qu'on les a présentés dans ce cours. Le lecteur aura donc compris qu'il existe des *idéaux premiers*, et que ceux-ci servent à décomposer tout idéal non nul... Ces concepts ont permis des avancées spectaculaires en Arithmétique, notamment dans la résolution, achevée depuis 1994, de l'équation de Fermat par Andrew Wiles.



Ernest KUMMER
(1810-1893)



Richard DEDEKIND
(1831-1916)



Andrew WILES
(1953-)

2.3 Les anneaux de congruence $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

On enrichit ici la structure du groupe $(\mathbb{Z}/_{n\mathbb{Z}}, +)$ en lui conférant une structure d'anneau.

☆ **Théorème 1** *(multiplication sur $\mathbb{Z}/_{n\mathbb{Z}}$)*
Soit $n \in \mathbb{N}^*$.
Il existe une et une seule loi interne, encore notée $\times$, sur $\mathbb{Z}/_{n\mathbb{Z}}$ pour laquelle

l'application $\begin{array}{ccc}\mathbb{Z} & \longrightarrow & \mathbb{Z}/_{n\mathbb{Z}} \\ k & \longmapsto & \bar{k}\end{array}$ vérifie

$$\forall k, \ell \in \mathbb{Z}, \quad \overline{k \times \ell} = \bar{k} \times \bar{\ell}.$$

De plus, $(\mathbb{Z}/_{n\mathbb{Z}}, +, \times)$ est un anneau commutatif, dont l'unité est $\bar{1}$.

Preuve. On sait déjà que $k \mapsto \bar{k}$ est un morphisme de groupes et que pour tous entiers $k, \ell \in \mathbb{Z}$, $\overline{k\ell} = k\bar{\ell}$.

Analyse. Supposons trouvée une telle loi $\times$. Si on impose la condition de l'énoncé, il n'y a pas de choix possible : si x et y sont deux éléments de $\mathbb{Z}/_{n\mathbb{Z}}$, on peut les écrire $x = \bar{k}$ et $y = \bar{\ell}$ avec $k, \ell \in \mathbb{Z}$ et nécessairement, $x \times y$ ne peut être égal qu'à $\overline{k\ell}$.

Synthèse. Il faut vérifier que cette définition est cohérente (on dit aussi bien fondée) en prouvant que $\overline{k\ell}$ ne dépend effectivement que de x et de y, et non de k et de ℓ. Pour ce faire, considérons k, k', ℓ, ℓ' dans $\mathbb{Z}$ tels que $\bar{k} = \bar{k}'$ et $\bar{\ell} = \bar{\ell}'$. On a alors

$$\overline{k\ell} - \overline{k'\ell'} = \overline{k\ell - k'\ell'} = \overline{k\ell - k'\ell + k'\ell - k'\ell'} = \overline{(k-k')\ell} + \overline{k'(\ell - \ell')} = \ell\bar{0} + k'\bar{0} = \bar{0}.$$

On a bien prouvé que $\overline{k\ell} = \overline{k'\ell'}$.

Cette loi interne $\times$ est alors commutative car $\overline{k\ell} = \overline{\ell k}$, et $\bar{1}$ en est le neutre puisque $\bar{k} \times \bar{1} = \overline{k \times 1} = \bar{k}$. De plus, $\times$ est associative car $\bar{k} \times (\bar{\ell} \times \bar{m}) = \bar{k} \times \overline{\ell m} = \overline{k\ell m} = (\bar{k} \times \bar{\ell}) \times \bar{m}$. Enfin $\times$ est distributive sur $+$ car $\bar{k} \times (\bar{\ell} + \bar{m}) = \bar{k} \times (\overline{\ell + m}) = \overline{k(\ell + m)} = \overline{k\ell + km}$ qui n'est autre que $(\bar{k} \times \bar{\ell}) + (\bar{k} \times \bar{m})$. En conclusion, $(\mathbb{Z}/_{n\mathbb{Z}}, +, \times)$ est un anneau commutatif. □

☆ **Théorème 2** *(éléments inversibles de $\mathbb{Z}/_{n\mathbb{Z}}$)*
Soit $n \in \mathbb{N}^*$. Les éléments inversibles de l'anneau $(\mathbb{Z}/_{n\mathbb{Z}}, +, \times)$ sont les classes $\bar{k}$ avec $k \in [\![0, n-1]\!]$ premiers avec n.

Ce sont donc exactement les générateurs du groupe cyclique $(\mathbb{Z}/_{n\mathbb{Z}}, +)$, et leur nombre est par définition $\varphi(n)$ (indicatrice d'Euler).

Preuve. Soit $x \in \mathbb{Z}/_{n\mathbb{Z}}$. On peut écrire $x = \bar{k}$ avec $k \in \mathbb{Z}$. Dire que x est inversible c'est dire qu'il existe $\ell \in \mathbb{Z}$ tel que $\bar{k} \times \bar{\ell} = \bar{1}$, c'est-à-dire $\overline{k\ell} = \bar{1}$. C'est donc équivalent à dire que $k\ell - 1 = np$ avec $p \in \mathbb{Z}$. En vertu du théorème de Bézout, la relation $k\ell - np = 1$ est équivalente à dire que $\text{pgcd}(k, n) = 1$, c'est-à-dire k et n sont premiers entre eux. □

☆ **Corollaire 1**
Soit $n \in \mathbb{N}^*$. L'anneau $(\mathbb{Z}/_{n\mathbb{Z}}, +, \times)$ est un corps si et seulement si n est premier.

Preuve. Si n est premier, alors $n \geqslant 2$ et tous les entiers k entre 1 et $n-1$ sont premiers avec n (car les seuls entiers qui ne sont pas premiers avec un nombre premier sont ses multiples). Ainsi, $\bar{1}, \bar{2}, \ldots, \overline{n-1}$ sont inversibles dans $\mathbb{Z}/n\mathbb{Z}$, et ce dernier est donc bien un corps.

Si l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps, il possède au moins deux éléments, donc $n \geqslant 2$. Supposons que $n = a \times b$ avec $1 \leqslant a, b \leqslant n$. La relation $\bar{a} \times \bar{b} = \bar{0}$ entraîne donc $\bar{a} = \bar{0}$ ou $\bar{b} = \bar{0}$, c'est-à-dire $a = n$ ou $b = n$. N'ayant que des diviseurs triviaux, n est premier. □

Notation. Si p est un nombre premier, le corps $\mathbb{Z}/p\mathbb{Z}$ se note plutôt $\mathbb{F}_p$. La lettre F vient de l'anglais *field*, traduction de *corps* (commutatif).

☆ **Corollaire 2** *(théorème d'Euler)*
Soit $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$. Si a est premier avec n, alors $a^{\varphi(n)} \equiv 1\ [n]$.

Preuve. Si a est premier avec n, sa classe $\bar{a}$ est un élément du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ qui possède $\varphi(n)$ éléments. On sait alors que $\bar{a}^{\varphi(n)} = \bar{1}$, c'est-à-dire $a^{\varphi(n)} \equiv 1\ [n]$. □

Cas particulier. Si p est un nombre premier, $\varphi(p) = p - 1$ car les seuls entiers n'étant pas premiers avec p sont les multiples de p. Ainsi, pour tout a non multiple de p, $a^{p-1} \equiv 1\ [p]$: ce résultat est connu sous le nom de (petit) théorème de Fermat.

☆ **Théorème 3** *(des restes chinois)*
Soit $m, n \in \mathbb{N}^*$ deux entiers. Si $\text{pgcd}(m, n) = 1$, alors l'application

$$\begin{array}{ccc} \mathbb{Z}/mn\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ [k]_{mn} & \longmapsto & ([k]_m\ ,\ [k]_n) \end{array}$$

est correctement définie, et est un isomorphisme d'anneaux, où pour tout $p \in \mathbb{N}$, on a noté $[k]_p$ la classe d'équivalence modulo p d'un entier k.

Preuve. L'application est correctement définie : si $[k]_{mn} = [k']_{mn}$ avec $k, k' \in \mathbb{Z}$, alors $k = k' + mnq$ avec $q \in \mathbb{Z}$. Donc $[k]_m = [k']_m + [0]_m = [k']_m$, et de même $[k]_n = [k']_n$. Cela montre que les classes $[k]_m$ et $[k]_n$ ne dépendent que de la classe $[k]_{mn}$ et non de k.

L'application est un morphisme d'anneaux. En effet, les applications $k \mapsto [k]_x$ sont toutes des morphismes d'anneaux, quel que soit l'entier x.

L'application est injective car si $([k]_m, [k]_n) = ([0]_m, [0]_n)$, alors $k \in m\mathbb{Z} \cap n\mathbb{Z}$. On sait que $m\mathbb{Z} \cap n\mathbb{Z} = \text{ppcm}(m, n)\mathbb{Z} = mn\mathbb{Z}$. Ainsi, $[k]_{mn} = [0]_{mn}$, ce qui prouve l'injectivité. Enfin, les ensembles finis $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ ont même cardinal, mn, donc la surjectivité est garantie. □