MP/MP*
MPI/MPI*

Michel Goumi
Nicolas Jousse
Ivan Gozard
Bertrand Hauchecorne
Olivier Leuck

PRÉPAS SCIENCES

COLLECTION DIRIGÉE PAR **BERTRAND HAUCHECORNE**

MATHS

- Méthodologie et objectifs
- Cours résumé
- Méthodes
- Vrai/faux, erreurs classiques
- Exercices de base et d'approfondissement
- Sujets de concours (écrits, oraux)
- Exercices-type oraux
- Corrigés détaillés et commentés

5e édition

ellipses

Mathématiques
MP/MP*
MPI/MPI*

PRÉPAS SCIENCES

collection dirigée par Bertrand Hauchecorne

Mathématiques MP/MP* MPI/MPI*

5e édition

ouvrage coordonné par

Michel GOUMI
Ancien professeur au lycée E. Perrier (Tulle)

Nicolas JOUSSE
Professeur au lycée Michel Montaigne (Bordeaux)

Ivan GOZARD
Professeur au lycée Carnot (Dijon)

Bertrand HAUCHECORNE
Ancien professeur au lycée Pothier (Orléans)

Olivier LEUCK
Professeur au lycée R. Follereau (Belfort)

ellipses

Collection
PRÉPAS SCIENCES

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

Les notices culturelles « Un mathématicien » et « Un peu d'histoire » des pages de titre des chapitres ont été rédigées par Bertrand Hauchecorne.

Les macros de cet ouvrage ont été réalisées par Nicolas Nguyen en LaTeX.

ISBN 9782340-116344
Dépôt légal : juillet 2026

www.editions-ellipses.fr

Avant-propos

Réussir en classes préparatoires nécessite d'assimiler rapidement un grand nombre de connaissances, mais surtout de savoir les utiliser, à bon escient, et les rendre opérationnelles au moment opportun. Bien sûr, l'apprentissage du cours de votre professeur jour après jour est indispensable. Cependant, on constate que pour beaucoup, c'est loin d'être suffisant. Combien d'entre vous ont bien appris leur cours et pourtant se trouvent démunis lors d'un DS, et plus grave, le jour du concours.

Cette collection a été conçue pour répondre à cette difficulté. Suivant scrupuleusement le programme, chaque ouvrage est scindé en chapitres, dont chacun correspond, en gros, à une semaine de cours. Leur structure est identique pour chaque niveau, en mathématiques comme en physique ou chimie.

Le résumé de cours est là pour vous remettre en mémoire tous les résultats à connaître. Sa relecture est indispensable avant un DS, le passage d'une colle relative au thème traité et lors des révisions précédant les concours. Ils sont énoncés sans démonstration.

La partie « méthodes » vous initie aux techniques utiles pour résoudre les exercices classiques. Complément indispensable du cours, elle l'éclaire et l'illustre.

La partie « vrai/faux » vous permet de tester votre recul par rapport au programme et de remédier à quelques mauvais réflexes. Son corrigé est l'occasion de mettre en garde contre des **erreurs classiques**.

Les exercices sont incontournables pour assimiler le programme et pour répondre aux exigences du concours. Des **indications**, que les meilleurs pourront ignorer, permettront de répondre aux besoins de chacun, selon son niveau. Les **corrigés** sont rédigés avec soin et de manière exhaustive.

Du nouveau dans cette édition profondément refondue

- Une note méthodologique en début d'ouvrage, vous aide à aborder les concours dans les meilleures conditions.
- Des « exos-minutes » dans chaque chapitre, plutôt faciles à résoudre, vous permettent de tester vos réflexes en application directe du cours et une ou deux étoiles vous indiquent les exercices plus difficiles à résoudre.
- Dans chaque chapitre des exercices, particulièrement adaptés aux épreuves orales, repérés par un petit micro, vous entrainent à affronter avec succès les oraux.

Ainsi l'ouvrage de maths comme ceux de physique, de chimie et de sciences industrielles de l'ingénieur vous accompagneront tout au long de l'année et vous guideront dans votre cheminement vers **la réussite aux concours**.

Bertrand Hauchecorne

Sommaire

Méthodologie

Si vous tenez ce livre jaune entre vos mains, c'est que vous avez probablement été admis à passer en deuxième année de classes préparatoires aux grandes écoles : Félicitations ! Le nouvel objectif est maintenant d'intégrer l'école de vos rêves. Vous avez déjà acquis une belle expérience de travail en première année et elle vous sera très utile en deuxième année. Reste à réfléchir à la façon d'aborder les quelques mois qui arrivent.

Cette deuxième année sera rythmée par plusieurs échéances marquantes :

— Les épreuves écrites des concours étalées généralement sur les mois d'avril et mai ;

— Les résultats des épreuves écrites (admissibilités) au début du mois de juin ;

— les épreuves orales qui se tiennent de la fin du mois de juin jusqu'à fin juillet ;

— Les résultats des épreuves orales (admissions) à la toute fin du mois de juillet ;

— Les propositions des écoles durant tout le mois d'août.

C'est donc une très longue année qui vous attend, et afin que celle-ci se déroule dans les meilleurs conditions, il convient de mettre en place dès le mois de septembre une méthode de travail efficace et adaptée à vos objectifs. Nous vous proposons ici quelques éléments qui vous aideront à vous organiser en mathématiques, mais qui sont facilement transposables dans les autres matières scientifiques.

L'apprentissage du cours : C'est probablement la partie la plus importante, malheureusement trop souvent négligée par certains élèves. Le cours proposé par votre professeur devra être travaillé avec soin, et il sera d'autant plus facile de le faire que vous aurez été attentif pendant les séances en classe. Souvent, une seule lecture de ce cours ne suffira pas et il faudra y « repasser » plusieurs fois ! N'hésitez pas à vous réciter à haute voix les définitions et énoncés des théorèmes, et même à les écrire au brouillon pour être certain de bien les connaître. La partie **Résumé de cours** proposée dans ce livre, vous permettra, avant un DS, une khôlle ou avant les concours, de vous remettre en tête les notions les plus importantes. La partie **Vrai-Faux** sera aussi l'occasion de vous mettre en garde contre des erreurs classiques.

Le travail des exercices : une fois le cours correctement mémorisé, il convient de passer à la pratique. Là encore, les exercices sélectionnés par votre professeur devront vous servir de base de travail, surtout si vous les avez déjà préparés, voire si vous êtes passé au tableau devant toute la classe. Attention toutefois à ne pas vous contenter de « lire » un corrigé d'exercice : vous auriez la sensation de l'avoir compris mais les idées de départ ou les arguments utilisés ne resteraient pas forcément gravés dans votre esprit. Il faut donc impérativement se mettre dans une situation de recherche de ces exercices devant une feuille blanche. La partie

Méthodes et les **exercices classiques** seront de précieux alliés pour vous aider dans cet objectif. Commencez à les travailler, puis, si vous vous sentez complètement démuni, les indications pourront vous donner une idée pour démarrer. Une fois l'exercice terminé, comparez votre résultat avec le corrigé du livre pour vous assurer que votre raisonnement ou votre calcul est correct.

La recherche de problèmes : C'est la dernière étape, à ne réaliser qu'une fois les deux précédentes effectuées. En début d'année, vous pourrez vous contenter de « morceaux » de sujets

de concours car les problèmes complets pourraient traiter de chapitres que vous n'avez pas encore abordés. Là encore, vous ne tireriez aucun avantage à lire uniquement les corrigés : cela vous donnerait une impression trompeuse d'avoir compris et mémorisé les idées, alors qu'il faut travailler et bloquer sur certaines questions pour en tirer profit. Avant les écrits, vous pourrez enfin vous entraîner sur de vrais sujets à traiter en entier. Vous trouverez d'ailleurs, dans la partie **exercices** de ce livre, des extraits de sujets d'écrits.

La préparation aux oraux : En toute fin d'année, vous serez amené à passer des épreuves orales. Vous vous entraînerez toute l'année à l'aide des khôlles ou des oraux blancs proposés par votre professeur mais il sera important de vous y préparer également de votre côté. N'hésitez pas à solliciter vos camarades de classe et mettez vous dans la peau, l'espace de quelques instants, tantôt d'un examinateur exigeant en posant des questions ou des exercices, tantôt dans le rôle du candidat, en répondant à leurs questions. Là encore, les exercices classiques présents dans ce livre, dont certains ont d'ailleurs été récemment posés à l'oral, pourront vous servir de base pour cette mise en situation.

Conclusion : En suivant méthodiquement les quelques conseils précédents, nul doute que vous progresserez ! L'année sera longue et semée d'embûches ; vous passerez par des moments de doute et par d'autres phases d'euphorie. Mais soyez assuré qu'il en est de même pour tous les élèves qui préparent les concours. Restez donc persévérant et continuez à travailler régulièrement. La marche est haute, mais la satisfaction, une fois l'objectif atteint, sera très grande !

Épreuves écrites de mathématiques de la filière MP-MPI :

Concours	CCINP	Centrale(1)	Mines	X	ENS
Épreuves	2 × 4H00	2 × 4H00	3H00 + 4H00	2 × 4H00	2 × 4H00

Épreuves orales de mathématiques de la filière MP-MPI :

Concours	CCINP	Centrale(1)	Mines	Mines-Telecom	X	ENS
Épreuves	1H00	30' + 1H00	1H00	30'	2 × 50'	2 × 50'

(1) Les épreuves du concours Centrale sont susceptibles de changer à compter de la session 2026-2027 mais à ce jour, nous ne disposons pas de ces informations.

Chapitre 1
Groupes

UN MATHÉMATICIEN

Évariste Galois (1811-1832) s'intéresse très jeune aux mathématiques et lit avec passion les traités des plus grands savants. Il publie à dix-sept ans un article dans une prestigieuse revue et entre en 1829 à l'École normale supérieure.

Il meurt à vingt ans dans un duel qu'il savait perdu d'avance. Dans la nuit qui précède, il rédige ses découvertes sur l'impossibilité de résoudre par radicaux l'équation du cinquième degré ; on y trouve la genèse de la notion de groupe.

Un peu d'histoire

À la Renaissance, des mathématiciens italiens avaient trouvé les formules donnant les solutions d'une équation polynomiale de degré 3 et 4. Par la suite, les efforts de différents savants furent vains pour déterminer celles du cinquième degré. Joseph Lagrange ouvre la voie en étudiant les permutations des racines pour découvrir les propriétés qui permettaient que tout se passe bien en degré 3 et 4.

Reprenant les méthodes du savant français, Niels Abel démontre que l'équation du cinquième degré ne peut se résoudre par radicaux, c'est-à-dire qu'il n'existe pas de formule, comme pour le degré 2, donnant les solutions à l'aide des coefficients. Peu après, Évariste Galois donne les conditions nécessaires et suffisantes pour que cette résolution soit possible. Pour le faire, il introduit les groupes de permutations et pose les bases de la théorie des groupes.

Objectifs

les incontournables

- approfondir les points abordés en première année (axiomes de définition, exemples usuels, sous-groupe, morphisme de groupes, etc) ;
- savoir prouver qu'une partie d'un groupe en est un sous-groupe ;
- s'approprier les notions de partie génératrice, de générateur, de groupe monogène, de groupe cyclique et d'ordre d'une élément d'un groupe ;
- étudier le groupe $\big(\mathbb{Z}/n\mathbb{Z}, +\big)$, champ d'application privilégié des notions listées ci-dessus et de quelques autres ;
- revoir les connaissances acquises en première année sur les groupes symétriques et la notion de signature d'une permutation ;
- savoir déterminer l'ordre d'un élément d'un groupe.

et plus si affinités

- s'intéresser aux groupes classiques ;
- utiliser des notions de théorie des groupes pour prouver des résultats en algèbre, en géométrie...

Résumé de cours

Structure de groupe

Définition : *Un **groupe** est un ensemble G muni d'une loi de composition interne notée $*$ vérifiant les propriétés suivantes :*

– *La loi $*$ est associative, c'est-à-dire que : pour tous $a, b, c \in G$, on a : $a * (b * c) = (a * b) * c$.*

– *Elle est munie d'un élément neutre $e \in G$, c'est-à-dire qu'il existe un élément e qui vérifie : $a * e = e * a = a$ pour tout $a \in G$.*

– *Tout élément $x \in G$ possède un symétrique, c'est-à-dire qu'il existe $x' \in G$ tel que :*

$$x * x' = x' * x = e.$$

L'élément neutre d'un groupe est unique ; si x admet un symétrique, celui-ci est unique.

Théorème 1.1.— Groupe produit —. Étant donnés deux groupes $(G_1, *)$ et (G_2, Δ), on définit sur le produit cartésien $G = G_1 \times G_2$ l'opération : $(x_1, x_2)\Upsilon(y_1, y_2) = (x_1 * y_1, x_2 \Delta y_2)$.
L'opération Υ définit sur G une structure de groupe.
Par récurrence, on définit, plus généralement, le groupe produit d'une famille finie de groupes.

Définition : *Une partie H du groupe $(G, *)$ est un **sous-groupe** de G lorsqu'elle vérifie les assertions suivantes :*

i) H n'est pas vide ;

ii) H est stable pour $*$, c'est-à-dire : $\forall (x, y) \in H^2$, $x * y$ appartient à H ;

iii) le symétrique de tout élément de H est un élément de H.

Proposition 1.2.— H est un sous-groupe de G si, et seulement si, H contient l'élément neutre e et pour tout $(a, b) \in H \times H$, $a * b^{-1}$ appartient à H.

Remarque : Si H est un sous-groupe de G, alors la loi induite par $*$ sur H est une loi de composition interne, et H, muni de cette loi, est un groupe.

Lemme 1.3.— Toute intersection de sous-groupes de G est un sous-groupe de G.

Théorème-Définition 1.4.— Soit A une partie du groupe G. L'intersection de tous les sous-groupes de G contenant A est un sous-groupe. C'est le plus petit sous-groupe de G contenant A. Ce groupe s'appelle le ***sous-groupe engendré*** par A.

Définition : *Une partie X du groupe G en est une **partie génératrice** lorsque le sous-groupe engendré par X est égal à G.*

Théorème 1.5.— Sous-groupes de $\mathbb{Z}$ —. Les sous-groupes de $(\mathbb{Z}, +)$ sont les ensembles $n\mathbb{Z}$ pour $n \in \mathbb{Z}$.

Morphismes de groupes

Définition : *Soit $(G, *)$ et (G', Δ) deux groupes. On appelle **morphisme de groupes** de $(G, *)$ dans (G', Δ) une application f de G dans G' qui vérifie :*

$$\forall (a, b) \in G^2,\ f(a * b) = f(a) \Delta f(b).$$

Proposition 1.6.— Soit f un morphisme de groupes de $(G,*)$ dans (G',Δ). Notons e l'élément neutre de G et $e^{'}$ celui de $G^{'}$.

▸ Si H est un sous-groupe de G, $f(H)$ est un sous-groupe de G'. Si H' est un sous-groupe de G', $f^{-1}(H') = \{x \in G \mid f(x) \in H'\}$ est un sous-groupe de G.

▸ $f(G)$ est un sous-groupe de G, appelé ***image*** de f et noté Im f.
$f^{-1}(\{e'\}) = \{x \in G \mid f(x) = e'\}$ est un sous-groupe de G, appelé ***noyau*** de f et noté Ker f.

▸ f est surjectif si, et seulement si, Im $f = G'$. f est injectif si, et seulement si, Ker $f = \{e\}$.

Définition : *On appelle* ***isomorphisme de groupes*** *de* $(G,*)$ *sur* (G',Δ) *un morphisme de groupes bijectif.*

Proposition 1.7.— Si f est un isomorphisme de groupes de $(G,*)$ sur (G',Δ), sa bijection réciproque f^{-1} est un isomorphisme de groupes de (G',Δ) sur $(G,*)$.

■ Groupe $\mathbb{Z}/n\mathbb{Z}$

Définition : Congruence modulo n **—.** *Fixons un entier* $n \in \mathbb{N}$*; les entiers* $a \in \mathbb{Z}$ *et* $b \in \mathbb{Z}$ *sont dits* ***congrus modulo*** n *lorsque* $b - a \in n\mathbb{Z}$*. On note alors* $a\mathcal{R}_n b$ *ou* $a \equiv b\,[n]$.

Proposition 1.8.— La relation de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$.

Notation : *Dans la suite,* $\overline{k}$ *désigne la classe d'équivalence de* $k \in \mathbb{Z}$ *pour cette relation.*
On a donc : $\overline{0} = n\mathbb{Z}$, $\overline{1} = \{\ldots, 1-2n, 1-n, 1, n+1, 2n+1 \ldots\}$, *etc.*
L'ensemble des classes d'équivalence selon la relation de congruence modulo n *se note* $\mathbb{Z}/n\mathbb{Z}$.

Proposition 1.9.— Pour $n \in \mathbb{N}^*$ fixé, $\mathbb{Z}/n\mathbb{Z}$ est un ensemble fini de cardinal n :

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

Lemme 1.10.— Soit $(a, a', b, b') \in \mathbb{Z}^4$ avec $a \equiv a'\,[n]$ et $b \equiv b'\,[n]$, alors $(a+b) \equiv (a'+b')\,[n]$. On dit que la relation est *compatible* avec l'addition. On peut donc définir sur $\mathbb{Z}/n\mathbb{Z}$ l'opération :

$$u + v = \overline{a+b},\ \text{où } u = \overline{a} \text{ et } v = \overline{b}\ .$$

L'élément de $\mathbb{Z}/n\mathbb{Z}$ ainsi défini ne dépend pas des représentants choisis.

Théorème 1.11.— Muni de l'addition ainsi définie, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ est un groupe commutatif. L'application $\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}, z \longmapsto \overline{z}$ est un morphisme de groupes surjectif. On l'appelle le morphisme canonique, ou la surjection canonique, de $\mathbb{Z}$ vers $\mathbb{Z}/n\mathbb{Z}$.

■ Groupe engendré par un élément

Notation : *En général, la loi du groupe* G *est noté multiplicativement et sans symbole :* $ab = a*b$*; l'élément neutre se note* e *ou* $\mathbf{1}_G$*, le symétrique d'un élément* x *est noté* x^{-1}.

Lemme 1.12.— Soit $(G,.)$ un groupe et $a \in G$. Le sous-groupe engendré par a (ou par $\{a\}$) est :

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

Définition : *Un groupe G est dit* ***monogène*** *lorsqu'il est engendré par un seul élément. Tout élément qui l'engendre en est un* ***générateur****.*

Définition : *Un groupe* ***cyclique*** *est un groupe monogène fini, c'est-à-dire fini et engendré par un seul élément.*

Exemple : Le groupe additif $\mathbb{Z}/n\mathbb{Z}$ est cyclique engendré par $\overline{1}$ car $\overline{k} = k\,\overline{1} = \overline{1} + \overline{1} + \ldots + \overline{1}$ (k fois). Plus généralement :

Théorème 1.13.— Les générateurs du groupe additif $\mathbb{Z}/n\mathbb{Z}$ sont les $\overline{k}$ avec $k \wedge n = 1$.

Théorème 1.14.— Un groupe monogène infini est isomorphe à $\mathbb{Z}$.
Un groupe cyclique de cardinal n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Corollaire 1.15.— Le groupe $\mathbb{U}_n = \{e^{2ik\pi/n},\, 0 \leqslant k < n\}$ des racines n-ièmes de l'unité est engendré par $e^{2i\pi/n}$ puisque $e^{2ik\pi/n} = (e^{2i\pi/n})^k$. Il est donc isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

■ Ordre d'un élément d'un groupe

Définition : *Soit $(G, .)$ un groupe. On appelle* ***ordre*** *de l'élément x de G le cardinal du sous-groupe de G engendré par x.*

Théorème 1.16.— Si x est d'ordre fini d et si e est l'élément neutre de G, alors, pour n dans $\mathbb{Z}$, on a :

$$x^n = e \Longleftrightarrow d|n.$$

Théorème 1.17.— Si G est un groupe fini, alors tout élément de G est d'ordre fini, et son ordre divise Card (G).

■ Groupe symétrique

L'ensemble des bijections de l'ensemble $\{1, 2, \ldots, n\}$ est noté $\mathcal{S}_n$. Les éléments de $\mathcal{S}_n$ sont appelés ***permutations*** de $[\![1, n]\!]$.

Définition : Groupe symétrique —. *$\mathcal{S}_n$ muni de la loi $\circ$ de composition des applications est un groupe, en général non commutatif, appelé* ***groupe symétrique*** *d'ordre n.*

Notation : *La permutation σ de $[\![1, n]\!]$ est notée :* $\begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$.

Vocabulaire : ▸ *La composition de permutations est souvent notée par simple juxtaposition et on dit que c'est leur* ***produit****. Toutefois, cette opération n'est toujours pas commutative et $\sigma_1\sigma_2$ n'est pas égale, en général, à $\sigma_2\sigma_1$.*

▸ *Une permutation σ de $\mathcal{S}_n$ est un* ***cycle de longueur*** *k lorsqu'il existe k éléments deux à deux distincts $i_1, i_2, \ldots i_k$ de $[\![1, n]\!]$ tel que : $\sigma(i_1) = i_2, \sigma(i_2) = i_3, .., \sigma(i_{k-1}) = i_k, \sigma(i_k) = i_1$ et, pour tout $i \in [\![1, n]\!] \setminus \{i_1, i_2, \ldots, i_k\}$, $\sigma(i) = i$. On le note $\sigma = (i_1\, i_2\, \ldots\, i_k)$.*

▸ *Les cycles de longueur 2 sont appelés* ***transpositions****. Conformément à la notation définie ci-dessus, la transposition $\tau = (i, j)$ échange i et j et laisse les autres éléments de $[\![1, n]\!]$ invariants.*

Remarque : $\mathcal{S}_1$ est réduit à $\{\mathrm{Id}\}$, aussi, dans la suite de ce paragraphe, on suppose que $n \geqslant 2$.

Définition : *Le* ***support*** *d'une permutation $\sigma \in \mathcal{S}_n$ est $\{i \in [\![1, n]\!],\ \sigma(i) \neq i\}$.*

Remarque : Deux permutations de $\mathcal{S}_n$ de supports disjoints commutent.

Proposition 1.18.— Toute permutation de $\mathcal{S}_n$ se décompose en produits de cycles à supports disjoints. De plus, cette décomposition est unique à l'ordre près des termes.

Corollaire 1.19.— Les transpositions engendrent le groupe symétrique $\mathcal{S}_n$.

Il suffit de prouver que tout cycle se décompose en transpositions, cela découle de l'égalité :

$$(i_1\, i_2\, \ldots\, i_k) = (i_1\, i_2)(i_2\, i_3)\ldots(i_{k-1}\, i_k).$$

Soit $\sigma \in \mathcal{S}_n$ une permutation, il y a égalité entre les trois quantités suivantes :

1. $(-1)^T$, où T est le nombre de transpositions dans une décomposition de σ en un produit de transpositions.
2. $(-1)^I$, où I est le nombre d'inversions de σ, c'est-à-dire le nombre de couples (i, j) avec $i < j$ et $\sigma(i) > \sigma(j)$.
3. $\displaystyle\prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(i) - \sigma(j)}{i - j}$.

Cette quantité commune s'appelle ***signature de la permutation*** σ ; on la note $\varepsilon(\sigma)$.

Proposition 1.20.— La signature ε est l'unique morphisme de groupes de $\mathcal{S}_n$ dans $\{-1, 1\}$ envoyant toute transposition sur -1.

Exemple : Un cycle σ de longueur k est d'ordre k ($\sigma^k = \mathrm{Id}$) et a pour signature $(-1)^{k-1}$.

Méthodes

Comment montrer qu'un ensemble muni d'une loi de composition interne est un groupe

❑ **Méthode 1.1.—** Pour montrer que $(G, .)$ est un groupe, on peut :
- Utiliser la définition d'un groupe.
- Montrer que c'est un sous-groupe d'un groupe connu.

Mise en œuvre : exercice 1.4, **exercice 1.12**, **exercice 1.13**.

Remarques : • Avant d'utiliser la définition d'un groupe, regardez si l'ensemble étudié n'est pas inclus dans un groupe déjà connu. Ceci évite de démontrer l'associativité et de chercher un élément neutre.
• Parfois, l'ensemble étudié est composé de fonctions. Il est utile de se rappeler que l'ensemble des fonctions d'un ensemble quelconque dans un groupe $(G, *)$ est lui-même un groupe pour l'opération, encore notée $*$, définie par : $f * g : x \longmapsto f(x) * g(x)$.
• Les axiomes de groupe s'appliquent à une loi de composition interne. Ceci implique que, pour montrer que $(G, *)$ est un groupe, il faut d'abord vérifier la stabilité de la loi, c'est-à-dire que le produit de deux éléments de G est bien un élément de G.

Comment montrer qu'un sous-ensemble H d'un groupe G est un groupe

❑ **Méthode 1.2.—** Soit $(G, .)$ un groupe. Soit H une partie de G. Pour montrer que H est un sous-groupe de G, on peut :
- Utiliser la caractérisation des sous-groupes.
- Montrer que H est l'intersection d'une famille de sous-groupes.
- Montrer que H est l'image d'un groupe par un morphisme.
- Montrer que H est le noyau d'un morphisme de groupes (ou, plus généralement, l'image réciproque d'un sous-groupe par un morphisme).

Mise en œuvre : exercice 1.4, **exercice 1.2**, **exercice 1.12**.

Remarques : • Pour montrer que H est un sous-groupe de G en utilisant la caractérisation des sous-groupes, il faut montrer que :
1 - H n'est pas vide. En général, on justifie qu'il contient l'élément neutre de G.
2 - H est stable par la loi du groupe : c'est fondamental, ceci revient à montrer que la loi est une loi de composition interne pour H.
3 - Le symétrique de tout élément a de H est encore dans H. Souvent, on connaît déjà la forme de ce symétrique. Il suffit alors seulement de montrer qu'il est dans H.
• On peut condenser les deux assertions 2 et 3 en une seule propriété :

$$\forall (a, b) \in H^2,\ a * b^{-1} \in H.$$

Ceci peut faire gagner du temps. Il ne faut l'utiliser que si la forme du symétrique dans G est connue. Dans les autres cas, il est préférable de séparer la stabilité et l'existence du symétrique.

Exemple : *Soit E un espace vectoriel de dimension finie. Montrer que*
$$\mathrm{SL}(E) = \{f \in \mathscr{L}(E) \ / \ \det(f) = 1\}$$
est un sous-groupe de $(\mathrm{GL}(E), \circ)$.
On considère $\varphi : f \longmapsto \det(f)$. C'est un morphisme du groupe $\mathrm{GL}(E)$ dans $(\mathbb{K}^*, \times)$ car, pour tous $f, g \in \mathrm{GL}(E)$, $\det(f \circ g) = \det(f) \times \det(g)$. L'élément neutre de $(\mathbb{K}^*, \times)$ étant 1, $\mathrm{SL}(E)$ est le noyau de φ, c'est donc un sous-groupe de $(\mathrm{GL}(E), \circ)$.

Exemple : L'ensemble des fonctions continues, bornées de $\mathbb{R}$ dans lui-même est un groupe pour l'addition des fonctions, car c'est l'intersection de l'ensemble des fonctions continues et de celui des fonctions bornées qui sont, d'après le cours, des groupes.

■ Comment rechercher l'ordre d'un élément d'un groupe

❑ **Méthode 1.3.—** Soit G un groupe, noté multiplicativement, et soit $a \in G$. Pour déterminer l'ordre de l'élément a, on peut :

- Calculer les puissances successives de l'élément a jusqu'à l'obtention de l'élément neutre.
- Trouver une propriété qui montre qu'aucune puissance de a ne peut être le neutre.

Remarque : Si le groupe est fini, tout élément a un ordre fini qui divise l'ordre, c'est-à-dire le cardinal, du groupe.

Mise en œuvre : exercice 1.12, **exercice 1.15**.

Exemple : *Chercher l'ordre de chacun des éléments* $M = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$, $N = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$ et $P = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ *dans le groupe $GL_2(\mathbb{C})$ des matrices inversibles (2,2) à coefficients complexes.*
Le calcul de $M^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ montre que $M^3 \neq I_2$ et $M^4 = I_2$ donc l'ordre de M est 4.

Comme $\det(N) = -2$, on a : $\forall n \in \mathbb{N}^*$, $\det(N^n) = (-2)^n \neq 1$, donc N est d'ordre infini.
On obtient $P^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, et on montre par une récurrence facile que : $\forall n \in \mathbb{N}$, $P^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$.
Ainsi, pour tout $n > 0$, $P^n \neq I_2$, ce qui montre que P est d'ordre infini.

Exemple : *Soit $z = re^{2i\pi\theta} \in \mathbb{C}$ avec $r > 0$ et $\theta \in \mathbb{R}$. Chercher l'ordre de z dans le groupe $(\mathbb{C}^*, \times)$ des nombres complexes non nuls.*
– Si $r \neq 1$, alors, pour $n \geqslant 1$, $|z^n| = r^n \neq 1$ donc $z^n \neq 1$. Ainsi, l'ordre de z est infini.
– Si $r = 1$ alors $z^n = 1$ si, et seulement si, $n\theta \in \mathbb{Z}$. Si θ est irrationnel, ceci est impossible pour $n \neq 0$, donc z est d'ordre infini. Si θ est rationnel, $\theta = p/q$ avec $p \wedge q = 1$ et $q > 0$, alors q est le plus petit entier strictement positif tel que $q\theta \in \mathbb{Z}$. On en déduit que l'ordre de z est égal à q.

■ Calculs dans le groupe symétrique $\mathcal{S}_n$

❑ **Méthode 1.4.—** L'essentiel est de retenir les notations d'une permutation et d'un cycle (dont les transpositions), mais aussi de se souvenir que, bien que notée multiplicativement et appelée produit, la composition des permutations n'est pas, en général, commutative.

Mise en œuvre : de l'**exercice 1.15** à l'**exercice 1.17**.

Exemple : *Écrire les cycles* $(1\,2\,3)$ *et* $(1\,2\,3\,4)$ *comme produit de 2 et 3 transpositions respectivement.*

$(1\,2\,3) = (1\,2)(2\,3)$. En effet, on commence par appliquer la transposition de droite, $(2\,3)$: 1 est invariant, 2 et 3 sont échangés, puis celle de gauche qui laisse 3 invariant et échange 1 et 2. Au final, en composant, 1 a pour image 2, 2 a pour image 3 et 3 a pour image 1, tous les autres élément de $[\![1, n]\!]$ restant invariants, ce qui est bien la définition du cycle $(1\,2\,3)$.
De même, on vérifiera que : $(1\,2\,3\,4) = (1\,2)(2\,3)(3\,4)$.

Exemple : *Soit* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 7 & 6 & 8 & 4 & 9 & 2 & 1 \end{pmatrix}$. *Décomposer* σ *en produits de cycles à supports disjoints. Déterminer l'ordre de* σ*, c'est-à-dire le plus petit entier* $p \geqslant 1$ *tel que* $\sigma^p = \mathrm{Id}$*, et la signature de* σ*.*

Les supports des cycles recherchés étant disjoints, leur composition (ou produit) est commutative. On repère le cycle $c_1 = (1\,3\,7\,9)$, puis le cycle $c_2 = (2\,5\,8)$ et, enfin la transposition $\tau = (4\,6)$. $\sigma = c_1 c_2 \tau$, dans n'importe quel ordre.
L'ordre d'un cycle est sa longueur. Du fait de la commutativité de la composition des cycles à supports disjoints : $\forall\, k \geqslant 1$, $\sigma^k = c_1^k c_2^k \tau^k$ et $\sigma^k = \mathrm{Id}$ si, et seulement si, $c_1^k = c_2^k = \tau^k = \mathrm{Id}$, donc si, et seulement si, k est un multiple commun de 4, 3 et 2. Le plus petit d'entre eux est 12, qui est donc l'ordre de σ.
D'après l'exemple précédent, $c_1 = (1\,3)(3\,7)(7\,9)$, $c_2 = (2\,5)(5\,8)$, donc σ est le produit de 6 transpositions et sa signature est $(-1)^6 = +1$.
D'une autre manière, la signature est un morphisme du groupe $(\mathcal{S}_n, \circ)$ dans le groupe $\big(\{-1, 1\}, \times\big)$ et la signature d'un cycle de longueur k est $(-1)^{k-1}$. Donc :

$$\varepsilon(\sigma) = \varepsilon(c_1) \times \varepsilon(c_2) \times \varepsilon(\tau) = (-1)^3 \times (-1)^2 \times (-1)^1 = +1.$$

Vrai/Faux

	Vrai	Faux
1. Dans un groupe, l'égalité $xy = xz$ entraîne $y = z$.	☐	☐
2. Dans un groupe, tout élément est régulier ; en d'autres termes, on peut simplifier.	☐	☐
3. Soit E un espace vectoriel ; alors $(\mathscr{L}(E), \circ)$ est un groupe.	☐	☐
4. Le groupe produit $G = G_1 \times \cdots \times G_m$ est commutatif si, et seulement si, tous les groupes G_i, $1 \leqslant i \leqslant m$, sont commutatifs.	☐	☐
5. Les groupes $(\mathbb{R}, +)$ et $(\mathbb{R}^*, \times)$ sont isomorphes.	☐	☐
6. Les groupes $(\mathbb{R}, +)$ et $(\mathbb{R}_+^*, \times)$ sont isomorphes.	☐	☐
7. Un sous-groupe non réduit à $\{0\}$ de $(\mathbb{Z}, +)$ est isomorphe à $\mathbb{Z}$.	☐	☐
8. $\{-1, 1\}$ muni de la multiplication est un groupe isomorphe à $\mathbb{Z}/2\mathbb{Z}$.	☐	☐
9. Tout sous-groupe d'un groupe cyclique est cyclique.	☐	☐
10. Le seul élément d'ordre 1 d'un groupe est son élément neutre.	☐	☐
11. Tout groupe de cardinal 5 est commutatif.	☐	☐
12. Tout groupe de cardinal 6 est commutatif.	☐	☐
13. Si deux éléments d'un groupe G sont d'ordre fini, il en est de même de leur produit.	☐	☐
14. Dans un groupe d'ordre fini, tout élément est d'ordre fini.	☐	☐
15. Un groupe dans lequel tout élément est d'ordre fini est d'ordre fini.	☐	☐
16. La signature de $\sigma = (1\,3\,5)(5\,4\,3\,2)(5\,6\,7\,8)$ est $+1$.	☐	☐

Énoncé des exercices

Exos minutes

Exercice 1.1 : Pour tout $(x, y) \in \left(\mathbb{R}_+^*\right)^2$, on pose $x \star y = \sqrt{x^2 + y^2}$.
Est-ce $\left(\mathbb{R}_+^*, \star\right)$ est un groupe ?

Exercice 1.2 : Pour $x \in \mathbb{R}$, on note $M_x = \begin{pmatrix} 1 & 0 & 0 \\ x^2 & 1 & x \\ 2x & 0 & 1 \end{pmatrix}$. Soit $G = \{M_x,\, x \in \mathbb{R}\}$.
Montrer que G est un sous-groupe de $\mathrm{GL}_3(\mathbb{R})$, isomorphe à $(\mathbb{R}, +)$.

Exercice 1.3 : Déterminer tous les éléments de $\mathcal{S}_3$ et donner l'ordre de chacun d'entre eux.

Généralités

Exercice 1.4 : Montrer que l'ensemble G des matrices de la forme $\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}$ avec $x, y, z \in \mathbb{R}$ est un groupe pour le produit matriciel. Trouver le centre de ce groupe (c'est-à-dire le sous-groupe formé par l'ensemble des éléments qui commutent avec tous les autres).

Exercice 1.5 * : On considère un groupe $(G, *)$ d'élément neutre e dans lequel tout élément x vérifie $x * x = e$.

1. Montrer que G est commutatif.

2. Montrer que $H = (\mathbb{Z}/2\mathbb{Z})^n$ vérifie cette condition.

3. Donner un exemple infini de tel groupe.

D'après Mines-Ponts

Exercice 1.6 :** Soit G un ensemble muni d'une loi interne associative, notée ., ayant un neutre à gauche et pour laquelle tout élément admet un inverse à gauche. Montrer que $(G, .)$ est un groupe.

D'après École Polytechnique

Exercice 1.7 : Soit G un groupe. Un sous-groupe H de G est dit *distingué* lorsqu'il vérifie :

$$\forall g \in G,\, \forall h \in H,\, ghg^{-1} \in H.$$

1. Montrer que si G est commutatif, tout sous-groupe H de G est distingué.

2. Montrer que si φ est un morphisme de groupes de G dans G', $\mathrm{Ker}\,\varphi$ est un sous-groupe distingué de G. Plus généralement, montrer que : si H' est un sous-groupe distingué de G', $\varphi^{-1}(H')$ est un sous-groupe distingué de G.

3. Montrer que l'intersection d'une famille de sous-groupes distingués de G est un sous-groupe distingué de G.

4. Soit H et K deux sous-groupes de G. On suppose que H est distingué dans G. Montrer que $HK = \{xy,\, (x, y) \in H \times K\}$ est un sous-groupe de G.

■ Groupe engendré par un élément

Exercice 1.8 : **1.** Montrer que tout groupe à trois éléments est isomorphe à $\mathbb{Z}/3\mathbb{Z}$.
2. Montrer que tout groupe à quatre éléments est isomorphe soit à $\mathbb{Z}/4\mathbb{Z}$, soit à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercice 1.9 : Soit G un groupe cyclique de cardinal n engendré par a et $p \in \mathbb{N}^*$ un diviseur de n. Montrer qu'il existe un unique sous-groupe de cardinal p de G, et que ce sous-groupe est cyclique engendré par $a^{n/p}$.

Exercice 1.10* : Soit $(G, .)$ un groupe, H et K deux sous-groupes cycliques de G. Montrer que $H \cap K$ est cyclique.

D'après Centrale-Supélec

Exercice 1.11 : Soit G un sous-groupe fini de $\mathbb{C}^*$ pour la multiplication non réduit à $\{1\}$.
1. Montrer que tout élément de G a pour module 1.
2. Soit B l'ensemble des arguments des éléments de G choisis dans l'intervalle $[0, 2\pi[$,
et $\theta = \min(B \setminus \{0\})$.
Justifier l'existence de θ et montrer que $\theta = 2\pi/n$ pour un certain $n \in \mathbb{N}^*$.
3. Montrer que $\mathbb{U}_n \subset G$, puis que $\mathbb{U}_n = G$. Conclusion ?

Exercice 1.12 : On rappelle que $\mathrm{GL}_2(\mathbb{R})$ désigne l'ensemble des matrices carrées $(2, 2)$ de déterminant non nul et on note H l'ensemble des matrices carrées $(2, 2)$ à coefficients dans $\mathbb{Z}$ dont le déterminant vaut 1 ou -1.
1. Montrer que H est un groupe pour la multiplication.
2. On pose : $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$. Calculer l'ordre de A, de B, et de AB. Conclusion ?

Exercice 1.13 : On note G l'ensemble des rationnels de $[0, 1[$ muni de la loi notée $*$ suivante :
$x * y = x + y$ si $x + y < 1$ et $x * y = x + y - 1$ si $x + y \geqslant 1$.
1. Montrer que $(G, *)$ est un groupe commutatif.
2. Montrer que ce groupe est infini mais que tous ses éléments sont d'ordre fini.

Exercice 1.14 : Soit G un groupe. Si x est un élément d'ordre fini de G, on note $\omega(x)$ son ordre.
1. Soit $a \in G$ d'ordre fini et $m = \omega(a)$. Soit $k \in [\![0, m-1]\!]$. Soit $d = \mathrm{pgcd}(k, m)$ et $m' = m/d$. Montrer que $\omega(a^k) = \omega(a^d) = m'$.
2. Soit $a, b \in G$ tous deux d'ordre fini. On pose $m = \omega(a)$, $n = \omega(b)$. On suppose que a et b commutent entre eux et que $\mathrm{pgcd}(m, n) = 1$. Montrer que $\omega(ab) = mn$.

■ Groupe symétrique

Exercice 1.15 : Soit $(G, .)$ un groupe.
1. Montrer que si pour tous $a, b \in G$, on a : $a^2b^2 = (ab)^2$, alors G est commutatif.
2. Trouver deux éléments a et b du groupe $\mathcal{S}_3$ des bijections de $\{1, 2, 3\}$ dans lui-même tels que $a^2b^2 \neq (ab)^2$.

Exercice 1.16 : Montrer que l'ordre d'un élément du groupe symétrique $\mathcal{S}_5$ est un élément de $\{1, 2, 3, 4, 5, 6\}$. Pour chaque $k \in \{1, 2, 3, 4, 5, 6\}$, donner le nombre d'éléments d'ordre k.

Exercice 1.17* : Soit $(G,.)$ un groupe. Si $g \in G$, soit φ_g l'application de G dans G telle que :

$$\forall x \in G,\ \varphi_g(x) = gxg^{-1}.$$

1. Montrer que pour tout $g \in G$, φ_g est un automorphisme de G.

2. Montrer que l'application Φ qui à $g \in G$ associe φ_g est un morphisme de G dans le groupe $\mathrm{Aut}(G)$ des automorphismes de G. Quel est son noyau ?

3. Donner un exemple où Φ n'est pas surjectif.

4. Soit $n \in \mathbb{N}^*$ et $G = \mathcal{S}_n$. On note $\mathcal{A}_n$ le sous-groupe de G constitué des permutations paires. Montrer que $\mathcal{A}_n$ est stable par les φ_g.

5. On revient au cas général. On pose $\mathcal{G} = \mathrm{Aut}(G)$ et $\mathcal{H} = \mathrm{Im}\Phi$. Si $\delta \in \mathrm{Aut}(G)$, $\mathcal{H}$ est-il stable par φ_δ ?

D'après Centrale-Supélec

Indications

Ex. 1.2

On pourra commencer par calculer $M_x M_y$.

Ex. 1.4

Montrer que G est un sous-groupe du groupe $GL_3(\mathbb{R})$ des matrices inversibles $(3,3)$ à coefficients réels.

Ex. 1.8

On dressera la table de multiplication en notant e l'élément neutre et on regardera toutes les possibilités. On pourra de plus remarquer que chaque ligne et chaque colonne de la table contient chaque élément une fois et une seule (Justifiez pourquoi !). (Attention, c'est un groupe et non un sudoku !)

Ex. 1.9

Commencer par la partie existence : considérer le sous-groupe engendré par $a^{n/p}$.

Ex. 1.10

Si $H \cap K$ n'est pas réduit à l'élément neutre, considérer $E = \left\{ i \in [\![1, n-1]\!] \ / \ a^i \in H \cap K \right\}$ où a est un générateur de G.

Ex. 1.11

1. *Considérer le module de a^n.*

2. *Introduire n tel que $n\theta \leqslant 2\pi < (n+1)\theta$.*

3. *Montrer que $\mathbb{U}_n \subset G$. Puis essayer de considérer $b \in G$ avec $b \notin \mathbb{U}_n$.*

Ex. 1.12

1. *Montrer que H est un sous-groupe de $GL_2(\mathbb{R})$.*

Ex. 1.16

Chercher d'abord les cycles, puis les produits de cycles à supports disjoints.

Ex. 1.17

2. *On montrera que le noyau de Φ est le sous–groupe $Z(G) = \{g \in G \ / \forall h \in G,\ gh = hg\}$ de G constitué des éléments qui commutent avec tous les autres (on l'appelle le centre de G).*

3. *On pourra observer que $G \to G, x \longmapsto x^{-1}$ est toujours un automorphisme du groupe G.*

Corrigé des vrai/faux

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
V	V	F	V	F	V	V	V	V	V	V	F	F	V	F	V

1. Il suffit de multiplier par x^{-1} à gauche.
2. Il suffit de multiplier par l'élément symétrique.
3. Les applications linéaires non bijectives n'ont pas d'inverse. Pour avoir un groupe, il faut se restreindre à $\mathrm{GL}(E)$.
4. Clairement si tous les G_i sont commutatifs, G l'est. Pour la réciproque, observer que, pour tout i, l'application $x = (x_1, \ldots, x_m) \in G \longmapsto x_i \in G_i$ est un morphisme de groupes surjectif et que l'image par un tel morphisme d'un groupe commutatif est un groupe commutatif.
5. Dans $(\mathbb{R}, +)$, il n'y a aucun élément d'ordre 2, tandis que dans $(\mathbb{R}^*, \times)$, il y en a un (qui est -1).
6. La restriction à $]0, +\infty[$ de $x \longmapsto e^x$ est un isomorphisme de $(\mathbb{R}, +)$ dans $(\mathbb{R}_+^*, \times)$.
7. Un tel groupe est monogène et infini.
8. Si p est premier, tout groupe à p éléments est cyclique donc isomorphe à $\mathbb{Z}/p\mathbb{Z}$.
9. Voir **exercice 1.9**.
10. Évident.
11. Il est cyclique donc commutatif.
12. Le groupe symétrique $\mathcal{S}_3$ fournit un contre-exemple. Les transpositions $(1,2)$ et $(1,3)$ qui intervertissent respectivement 1 et 2 et 1 et 3 ne commutent pas puisque $(1,2) \circ (1,3) = (1,3,2)$ et $(1,3) \circ (1,2) = (1,2,3)$.
13. Voir **exercice 1.12**.
14. Vrai. De plus, l'ordre de tout élément divise l'ordre du groupe.
15. Voir **exercice 1.13**.
16. La signature est un morphisme du groupe $(\mathcal{S}_n, \circ)$ dans le groupe $\big(\{-1, 1\}, \times\big)$ et la signature d'un cycle de longueur k est $(-1)^{k-1}$. Donc : $\varepsilon(\sigma) = (-1)^2 \times (-1)^3 \times (-1)^3 = +1$.

Erreurs classiques

- Croire que le symétrique de xy est $x^{-1}y^{-1}$. Cette égalité n'a lieu que si x et y commutent entre eux. Le symétrique de xy est : $(xy)^{-1} = y^{-1}x^{-1}$.
- Croire que si a est un élément d'ordre fini k, alors toutes ses puissances successives ont le même ordre.
- Dans un groupe non commutatif, écrire $(ab)^p = a^p b^p$...

Corrigé des exercices

Exercice 1.1

$\forall (x,y) \in \left(\mathbb{R}_+^*\right)^2$, $\sqrt{x^2+y^2} > \sqrt{x^2} = x$: il n'existe donc aucun élément neutre pour la loi $\star \in \mathbb{R}_+^*$. $\left(\mathbb{R}_+^*, \star\right)$ n'est pas un groupe.

Exercice 1.2

Par un calcul facile, on obtient : $\forall (x,y) \in \mathbb{R}^2$, $M_x\ M_y = M_{x+y}$.
Comme $M_0 = I_3$, ceci entraîne : chaque matrice M_x est inversible, d'inverse M_{-x}. On peut donc déjà dire que G est un sous-groupe de $\mathrm{GL}_3(\mathbb{R})$. Ainsi, en introduisant $\phi : x \longmapsto M_x$, on a $\phi(x+y) = \phi(x)\phi(y)$ pour tout (x,y) de $\mathbb{R}^2$ et on peut dire que ϕ est un morphisme de $(\mathbb{R},+)$ vers $\mathrm{GL}_3(\mathbb{R})$, et par construction $G = \operatorname{Im}\phi$.
Soit $x \in \operatorname{Ker}\phi$, alors $M_x = I_3$ donc $x = 0$. Ceci montre l'injectivité de ϕ.
En conclusion : G est un sous-groupe de $\mathrm{GL}_3(\mathbb{R})$ et grâce à l'application ϕ, G est isomorphe à $(\mathbb{R},+)$.

Exercice 1.3

Les éléments de $\mathcal{S}_3$ sont au nombre de $6 = 3!$:

$$\sigma_1 = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = \mathrm{Id} \qquad \sigma_2 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = (2,3)$$

$$\sigma_3 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = (1,3) \qquad \sigma_4 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = (1,2)$$

$$\sigma_5 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = (1,2,3) \qquad \sigma_6 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = (1,3,2)$$

σ_1 est d'ordre 1, les transpositions σ_2, σ_3 et σ_4 sont d'ordre 2, les cycles σ_5 et σ_6 sont d'ordre 3.

Exercice 1.4

▷ Montrons que G est un sous-groupe de $\mathrm{GL}_3(\mathbb{R})$.
En prenant $x = y = z = 0$, on montre que $I_3 \in G$.
Soit $M = \begin{pmatrix}1&x&z\\0&1&y\\0&0&1\end{pmatrix}$ et $M' = \begin{pmatrix}1&x'&z'\\0&1&y'\\0&0&1\end{pmatrix}$.
Alors $MM' = \begin{pmatrix}1&x+x'&z+z'+xy'\\0&1&y+y'\\0&0&1\end{pmatrix} \in G$.
Le calcul précédent montre que si on pose $x' = -x$, $y' = -y$ et $z' = -z + xy$, alors $MM' = M'M = I_3$ donc $M' = M^{-1} \in G$.
Ainsi G est un sous-groupe de $\mathrm{GL}_3(\mathbb{R})$.

▷ Soit $M = \begin{pmatrix}1&x&z\\0&1&y\\0&0&1\end{pmatrix} \in G$. M est un élément du centre de G si, et seulement si, $MM' = M'M$ pour tout $M' \in G$.
Ceci équivaut à : $\forall (x',y',z') \in \mathbb{R}^3$, $x + x' = x' + x$, $y + y' = y' + y$ et $z + z' + xy' = z' + z + x'y$.

Corrigé

C'est-à-dire à : $xy' = x'y$ pour tout x' et tout y', ce qui n'a lieu que pour $x = 0$ et $y = 0$.
Ainsi le centre de G est l'ensemble des matrices de la forme :

$$\begin{pmatrix} 1 & 0 & z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, z \in \mathbb{R}.$$

Exercice 1.5

1. Soit $(x, y) \in G^2$. On a $(x * y) * (x * y) = e$ d'une part, et $(x * x) * (y * y) = e$ d'autre part, donc $x * y * x * y = x * x * y * y$.
Or, dans un groupe on peut simplifier (en multipliant par le symétrique). Il vient : $y * x = x * y$.
Ceci vaut pour tout $(x, y) \in G^2$. Le groupe G est donc commutatif.
2. $H = \mathbb{Z}/2\mathbb{Z}^n = \left\{\overline{0}, \overline{1}\right\}^n$, muni de l'addition des n-uplets, est un groupe pour lequel $(\overline{0}, \ldots, \overline{0})$ est l'élément neutre.
Soit $a = (a_1, a_2, \ldots, a_n) \in H$. Alors :

$$a + a = (a_1 + a_1, a_2 + a_2, \ldots, a_n + a_n) = (\overline{0}, \overline{0}, \ldots, \overline{0}),$$

car tout élément x de $\mathbb{Z}/2\mathbb{Z}$ vérifie $x + x = \overline{0}$.

$$H \text{ vérifie la condition.}$$

3. Soit X un ensemble infini et F l'ensemble des applications de X dans $\mathbb{Z}/2\mathbb{Z}$. On munit F de l'addition usuelle des applications, notée $+$:

- $\forall (f, g) \in F^2, \forall x \in X, (f + g)(x) = f(x) + g(x) \in \mathbb{Z}/2\mathbb{Z} : f + g \in F$;
- cette addition est associative ;
- $\tilde{0} : x \longmapsto \overline{0} \in F$ est bien neutre pour l'addition des applications de F ;
- f est son propre symétrique, puisque :
  $$\forall x \in X, (f + f)(x) = f(x) + f(x) = \overline{0} \text{ donc } f + f = \tilde{0}.$$
- F est infini, puisque $\varphi : x \longmapsto f_x$ définie par :
  $$\forall z \in X, f_x(z) = \begin{cases} \overline{1}, \text{ si } z = x \\ \overline{0}, \text{ sinon} \end{cases}$$
  est une injection de X dans F ($\varphi(x) = \varphi(y) \Longrightarrow x = y$), donc une bijection de X dans $\varphi(X)$: $\mathsf{Card}\ \left(\varphi(X)\right) = \mathsf{Card}\ (X)$. Or, $\varphi(X) \subset F$, donc :
  $$\mathsf{Card}\ (F) \geqslant \mathsf{Card}\ \left(\varphi(X)\right) = \mathsf{Card}\ (X).$$

$(F, +)$ est un groupe infini qui vérifie la propriété de l'énoncé.

Exercice 1.6

Notons e le neutre à gauche.
Soit $x \in G$. Considérons x' l'inverse à gauche de x, puis x'' celui de x'.
$x''x' = e$, donc $(x''x')x = ex = x$.
Or, par associativité, $(x''x')x = x''(x'x) = x''e$.
Donc (*) $x''e = x$.
Par conséquent : $xx' = (x''e)x'$.
Or, par associativité, $(x''e)x' = x''(ex') = x''x' = e$. Donc $xx' = e$.
Donc x est l'inverse à gauche de x', ou encore : $x'' = x$.
Reprenant (*), il vient, puisque $x'' = x$: $xe = x$. Ce raisonnement vaut pour tout $x \in G$. Donc e est neutre.
Pour tout $x \in G$, $x'x = e$ et $x''x' = e$ donc, puisque $x'' = x$, $x'x = xx' = e$, et x' est l'inverse de x.

En conclusion, la loi est associative, e est élément neutre et chaque élément de G possède un inverse. Ainsi, $(G,.)$ est un groupe.

Exercice 1.7

1. Supposons que G est commutatif.
Soit H un sous-groupe de G. Alors : $\forall g \in G, \forall h \in H, hg^{-1} = g^{-1}h$, donc $ghg^{-1} = gg^{-1}h = h$, donc $ghg^{-1} \in H$.
Ainsi H est distingué dans G.

2. Notons e' l'élément neutre de G'. On a :
$\forall g \in G, \forall h \in \operatorname{Ker}\varphi, \varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi\big(g^{-1}\big) = \varphi(g)e'(\varphi(g))^{-1} = e'$, donc $ghg^{-1} \in \operatorname{Ker}\varphi$.

✎ *φ est un morphisme de groupes.*

Ainsi $\operatorname{Ker}\varphi$ est distingué dans G.

Soit H' un sous-groupe distingué de G'. Alors :
$\forall g \in G, \forall h \in \varphi^{-1}(H'), \varphi(h) \in H'$ donc, comme H' est distingué dans G', $\varphi\big(ghg^{-1}\big) = \varphi(g)\varphi(h)\varphi\big(g^{-1}\big) = \varphi(g)\varphi(h)\big(\varphi(g)\big)^{-1} \in H'$, donc :
$ghg^{-1} \in \varphi^{-1}(H')$ et $\varphi^{-1}(H')$ est distingué dans G.

3. Soit $(H_i)_{i\in I}$ une famille de sous-groupes distingués de G et $H = \bigcap_{i\in I} H_i$.
Soit $h \in H$. Alors $\forall g \in G, \forall i \in I, ghg^{-1} \in H_i$ car $h \in H_i$ et H_i est distingué dans G, donc $\forall g \in G, ghg^{-1} \in H$.
Ainsi H est un sous-groupe distingué de G.

4. $e \in H$ et $e \in K$ donc $e = ee \in HK$.
Soit $x \in HK$ et $y \in HK$. Alors il existe $(a,b) \in H \times K$ et $(u,v) \in H \times K$ tel que $x = ab$ et $y = uv$.
On a donc : $xy = (ab)(uv) = a(bub^{-1})bv$.
Or comme $u \in H$ et H est distingué, $bub^{-1} \in H$. Donc, par stabilité de H, $a(bub^{-1}) \in H$.
D'autre part, comme $(b,v) \in K^2$ et K est un sous-groupe de G, $bv \in K$.
Donc $xy = (a(bub^{-1}))(bv) \in HK$.
$x^{-1} = (ab)^{-1} = b^{-1}a^{-1} = (b^{-1}a^{-1}b)b^{-1}$. Or $a \in H$ et H est un sous-groupe de G, donc $a^{-1} \in H$, donc, H étant distingué, $b^{-1}a^{-1}b = b^{-1}a^{-1}(b^{-1})^{-1} \in H$.
D'autre part, comme $b \in K$ et K est un sous-groupe de G, $b^{-1} \in K$.
Donc $x^{-1} = (b^{-1}a^{-1}b)b^{-1} \in HK$.
Ainsi HK est un sous-groupe de G.

Exercice 1.8

1. Soit $G = \{e,a,b\}$ tel que $(G,.)$ soit un groupe d'ordre 3 de neutre e. Un élément différent du neutre ne peut être d'ordre 2, il est donc d'ordre 3.
Peut-on avoir, par exemple, $a.a = a$? Si c'est le cas, $e = a.a.a = a.a$: a est d'ordre 2 et on sait que ce n'est pas possible. Donc $a.a = b$, puis $a.b = a.(a.a) = e$, ainsi $b = a^{-1}$, donc $a = b^{-1}$.

✎ *L'ordre de tout élément divise le cardinal du groupe, ici 3.*

L'application φ de G dans $\mathbb{Z}/3\mathbb{Z}$ définie par : $\varphi(e) = \overline{0}$, $\varphi(a) = \overline{1}$ et $\varphi(b) = \overline{2}$, est évidemment une bijection.
De plus, φ est aussi un morphisme de groupes :

- $\varphi(e.a) = \varphi(a) = \overline{0} + \varphi(a) = \varphi(e) + \varphi(a)$; *idem* en permutant e et a, puis en remplaçant a par b ;
- $\varphi(a.b) = \varphi(e) = \overline{0} = \overline{1} + \overline{2} = \varphi(a) + \varphi(b)$; *idem* en permutant q et b.

Le groupe G est donc isomorphe à $\mathbb{Z}/3\mathbb{Z}$.

2. Soit $G = \{e,a,b,c\}$ tel que $(G,.)$ soit un groupe d'ordre 4 de neutre e.

✎ *L'ordre de chaque élément divise 4.*

Corrigé

1. Supposons que G comporte un élément d'ordre 4, par exemple a, alors $a^2 \neq e$, $a^3 \neq e$ et $a^4 = e$, d'où $a^{-1} = a^3$. On ne peut avoir $a^2 = a$, car sinon, on aurait : $a^3 = a^2 = a$, puis $e = a^4 = a^3 = a^2 = a$, donc $a = e$, ce qui n'est pas possible, un groupe admettant un seul élément neutre. Ne pouvant avoir $a^2 = e$, on a donc $a^2 = b$ ou $a^2 = c$. Disons $a^2 = b$, d'où $a^4 = b^2 = e$: b est d'ordre 2 et $b^{-1} = b$. L'inverse de a, ne pouvant donc être b, est nécessairement c.
   On dresse la table de multiplication avec ces informations, en complétant avec la propriété de l'élément neutre. Ce qui donne :

	e	a	b	c
e	e	a	b	c
a	a	b		e
b	b		e	
c	c	e		

   $a \longmapsto ab$ et $a \longmapsto ba$ sont des bijections de G dans G, puisque b admet un inverse dans G. De ce fait, chaque ligne et chaque colonne de la table contient chaque élément de G une fois et une seule, d'où :

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

   φ de G dans $\mathbb{Z}/4\mathbb{Z}$ définie par : $\varphi(e) = \overline{0}$, $\varphi(a) = \overline{1}$, $\varphi(b) = \overline{2}$ et $\varphi(c) = \overline{3}$, est évidemment une bijection.
   Il est un peu fastidieux, mais très simple, de vérifier que :
   $\forall\,(x, y) \in G^2$, $\varphi(x.y) = \varphi(x) + \varphi(y)$.
   φ est un isomorphisme de groupes de G dans $\mathbb{Z}/4\mathbb{Z}$.
2. Supposons que G ne comporte aucun élément d'ordre 4, alors G ne peut être isomorphe à $\mathbb{Z}/4\mathbb{Z}$ qui en comporte un : $\overline{1}$. Les trois éléments non neutres sont donc d'ordre 2 : met l'élément neutre e sur la diagonale de la table de multiplication. Ce qui donne :

	e	a	b	c
e	e	a	b	c
a	a	e		
b	b		e	
c	c			e

   On termine comme ci-dessus :

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	a	b	e

Cette table se superpose avec celle de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

On peut faire correspondre a, b et c avec les trois éléments différents du neutre dans n'importe quel ordre.

Il reste à vérifier que l'on a bien un morphisme de groupes et on obtient un isomorphisme de groupes de G dans $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercice 1.9

▷ Pour $k \in \mathbb{Z}$, on a : $\left(a^{n/p}\right)^k = e \iff a^{nk/p} = e \iff n \mid \frac{n}{p}k \iff p \mid k$.

✎ $\frac{nk}{p}$ *est un entier divisible par* n*, donc* $\frac{k}{p}$ *est un entier.*

Donc $a^{n/p}$ est d'ordre p.

Ainsi le sous-groupe F engendré par $a^{n/p}$ est cyclique de cardinal p.

▷ Prouvons maintenant l'unicité. Soit H un sous-groupe de cardinal p de G. Puisque G est cyclique de cardinal n engendré par a, chaque élément de G s'écrit de façon unique sous la forme a^k où $0 \leqslant k < n$. Donc il existe une séquence strictement croissante $(k_1, \ldots, k_p)$ d'éléments de $[\![0, n-1]\!]$ telle que $H = \{a^{k_i},\ i \in [\![1, p]\!]\}$. Comme $e \in H$, $k_1 = 0$.

Comme $\mathsf{Card}\ (H) = p$, tout élément x de H vérifie $x^p = e$, donc pour chaque $i \in [\![1, p]\!]$, on a : $a^{k_i p} = e$, donc n divise $k_i p$, c'est-à-dire : il existe $q_i \in \mathbb{N}$ tel que $k_i = q_i \dfrac{n}{p}$.

Il vient : $0 = q_1 < q_2 < \ldots < q_p = \dfrac{pk_p}{n} < p$.

Par conséquent : $\forall i \in [\![1, p]\!]$, $q_i = i - 1$.

Ainsi $H = \left\{\left(a^{n/p}\right)^{i-1},\ i \in [\![1, p]\!]\right\}$, c'est-à-dire $H = F$.

▷ En conclusion : il existe un unique sous-groupe de cardinal p de G, c'est le sous-groupe cyclique engendré par $a^{n/p}$.

Exercice 1.10

Notons $n = \mathsf{Card}\ H$ et a un générateur de H. Alors : $H = \left\{a^i,\ 0 \leqslant i \leqslant n-1\right\}$.

$H \cap K$ est inclus dans H donc fini ; il reste à prouver qu'il est monogène. Si $H \cap K = \{e\}$, c'est clair. Supposons désormais que $H \cap K \neq \{e\}$. Alors $E = \left\{i \in [\![1, n-1]\!] \ /\ a^i \in H \cap K\right\}$ est non vide, donc E admet un minimum, disons p.

Comme $H \cap K$ est un sous-groupe de G, le sous-groupe de G engendré par a^p est inclus dans $H \cap K$.

Soit $x \in H \cap K$. Il existe $i \in [\![0, n-1]\!]$ tel que $x = a^i$. Effectuons la division euclidienne de i par p : il existe $(q, r) \in \mathbb{N}^2$ tel que $i = qp + r$ et $0 \leqslant r < p$. Comme a^i et a^p appartiennent à $H \cap K$, $a^r = a^i (a^p)^{-q} \in H \cap K$. Si $r \neq 0$, alors $r \in E$ et $r < p = \min E$: c'est absurde...

Ainsi $r = 0$, donc $i = qp$ et $x = a^i = (a^p)^q$.

Finalement $H \cap K$ est le sous-groupe de G engendré par a^p, il est monogène, donc cyclique.

Exercice 1.11

1. Soit $n \in \mathbb{N}^*$ l'ordre de l'élément a de G. Alors $|a|^n = 1$ donc $|a| = 1$.

2. $B \setminus \{0\}$ est une partie finie non vide de $\mathbb{R}^*$. Elle admet un plus petit élément, disons θ. Soit $a \in G$ d'argument θ. Alors : $a = e^{i\theta}$.

Posons $n = \left\lfloor \dfrac{2\pi}{\theta} \right\rfloor$, alors $n \in \mathbb{N}^*$ et $n\theta \leqslant 2\pi < (n+1)\theta$.

✎ $\lfloor x \rfloor$ *désigne la partie entière de* x*.*

Corrigé

Supposons que $n\theta < 2\pi$, alors $(n+1)\theta$ est un argument de a^{n+1} et $\varphi = (n+1)\theta - 2\pi$ en est un autre. Or $a^{n+1} \in G$ et $0 < \varphi < 2\pi$, donc $\varphi \in B$. Comme $\varphi < \theta$, ceci contredit la définition de θ. On en déduit que $n\theta = 2\pi$, soit $\theta = 2\pi/n$.

3. ▷ D'après le cours $a = e^{i\theta}$ engendre $\mathbb{U}_n$, donc $\mathbb{U}_n \subset G$.

▷ Soit $b \in G \setminus \{1\}$. Alors $b = e^{i\varphi}$ avec $\varphi \in B$. Il existe $p \in \mathbb{N}$ tel que $p\theta \leqslant \varphi < (p+1)\theta$. Si $p\theta < \varphi$, alors l'argument $\psi = \varphi - p\theta$ de $ba^{-p} \in G$ vérifie : $0 < \psi < \theta$. Ce qui contredit la définition de θ. On en déduit que $p\theta = \varphi$, puis que $b = a^p \in \mathbb{U}_n$.

Ainsi, on a : $G = \mathbb{U}_n$.

En conclusion : tout sous-groupe fini de $\mathbb{C}^*$ est cyclique.

Exercice 1.12

1. On sait que $\mathrm{GL}_2(\mathbb{R})$ est un groupe pour la multiplication. Montrons que H en est un sous-groupe.

– H contient la matrice identité I_2, il n'est donc pas vide.

Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $N = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ des éléments de H. $\mathbb{Z}$ étant un anneau, $MN = \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix} \in H$.

– De plus le déterminant de M valant ± 1, $M^{-1} = \pm \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in H$.

Ainsi H est un sous-groupe.

2. Par le calcul on a : $A^2 = -I_2$ donc $A^3 = -A$ puis $A^4 = I_2$; A est donc d'ordre 4.

Et $B^2 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$ puis $B^3 = I_2$; donc B est d'ordre 3.

On a : $AB = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$.

Par une récurrence facile, on montre que : $\forall n \in \mathbb{N}$, $(AB)^n = (-1)^n \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$.

On en déduit que l'ordre de AB est infini.

On en conclut que, dans un groupe non commutatif, le produit de deux éléments d'ordre fini n'est pas nécessairement d'ordre fini.

Exercice 1.13

1. Remarquons que $x * y = x + y - \lfloor x + y \rfloor$, où $\lfloor t \rfloor$ désigne la partie entière de t. On a donc : $(x * y) * z = (x * y) + z - \lfloor (x * y) + z \rfloor$

$= (x + y) - \lfloor x + y \rfloor + z - \lfloor x + y - \lfloor x + y \rfloor + z \rfloor$

$= x + y + z - \lfloor x + y + z \rfloor$

Si n est entier, $\lfloor a + n \rfloor = \lfloor a \rfloor + n$.

Comme $+$ est une loi associative, il en est de même de la loi $*$.

De plus $y * x = y + x - \lfloor y + x \rfloor = x + y - \lfloor x + y \rfloor = x * y$.

Ce qui montre la commutativité.

Pour tout $x \in [0, 1[$, $x * 0 = x$; donc 0 est élément neutre.

De plus, si $x \neq 0$, on a $x * (1 - x) = 1 - \lfloor 1 \rfloor = 0$; donc $1 - x$ est le symétrique de x. On remarque aussi que 0 est son propre symétrique.

En conclusion : $(G, *)$ est un groupe.

2. $G = [0, 1[\cap \mathbb{Q}$ est infini.

Soit x un élément non nul de G. Soit $x = \dfrac{p}{q}$ l'écriture irréductible de ce rationnel. Comme $0 < x < 1$, on a : $0 < p < q$.
Alors, on prouverait par récurrence que $x^{*q} = qx - \lfloor qx \rfloor = qx - p = 0$; donc x est d'ordre fini.
Ainsi tout élément de G est d'ordre fini.

✎ $x^{*q} = x * \ldots * x$ *(produit où x figure q fois).*

Exercice 1.14

1. ▷ Pour $z \in \mathbb{Z}$, on a : $\left(a^d\right)^z = a^{dz}$, donc :

$$\left(a^d\right)^z = e \iff a^{dz} = e \iff m|dz \iff m'|z.$$

Par conséquent, $\omega\left(a^d\right) = \min\{z \in \mathbb{N}^* \mid m'/z\} = m'$.
▷ Notons $k' = k/d$. Alors $k = k'd, m = m'd$ et $\text{pgcd}(k', m') = 1$.
Pour $z \in \mathbb{Z}$, on a : $\left(a^k\right)^z = a^{kz}$, donc :

$$\left(a^k\right)^z = e \iff a^{kz} = e \iff m|kz \iff m'd|dk'z \iff m'|k'z.$$

Évidemment, si $m'|z$, alors $m'|k'z$.
Réciproquement, si $m'|k'z$, alors, comme $\text{pgcd}(k', m') = 1$, le théorème de Gauss assure que $m'|z$.
Ainsi $\left(a^k\right)^z = e \iff m'|z$. Par conséquent, $\omega\left(a^k\right) = m'\omega(a^d)$.

✎ $\omega(a^d) = \min(\{z \in \mathbb{N}^* \ / \ \left(a^d\right)^z = e\})$.

2. Comme a et b commutent, pour tout $z \in \mathbb{Z}$, $(ab)^z = a^z b^z$.
$a^m = e$, donc $a^{mn} = (a^m)^n = e^n = e$, et $b^n = e$, donc $b^{mn} = (b^n)^m = e^m = e$; donc $(ab)^{mn} = a^{mn}b^{mn} = e$.
Ainsi $\omega(ab)|mn$.
Notons $w = \omega(ab)$.
$(ab)^w = e$, donc $(ab)^{wn} = ((ab)^w)^n = e^n = e$,
or $(ab)^{wn} = a^{wn}b^{wn} = a^{wn}(b^n)^w = a^{wn}e^w = a^{wn}$, donc $a^{wn} = e$.
Par conséquent $m = \omega(a)$ divise wn. Or m est premier avec n, donc, par le théorème de Gauss, m divise w.
De même, échangeant les rôles, on voit que $b^{wm} = e$, donc n divise w.
Ainsi $\text{ppcm}(m, n)$ divise w.
Or m et n sont premiers entre eux, donc $\text{ppcm}(m, n) = mn$ et mn divise w.
Finalement, $\omega(ab) = mn$.

Exercice 1.15

1. L'hypothèse nous donne $aabb = abab$.
Multipliant les deux membres de cette égalité à gauche par a^{-1} et à droite par b^{-1}, on obtient : $ab = ba$.
Ce résultat qui vaut pour tout $(a, b) \in G^2$ montre que G est commutatif.

2. Notons a la transposition $(1\ 2)$ ou $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$, et $b = (1\ 3)$ ou $\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$.
Alors $aabb$ est l'identité, tandis que, puisque ab est la permutation circulaire $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$, $abab$ est $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$, donc : $a^2b^2 \neq (ab)^2$.

✎ *La composition des éléments de $\mathcal{S}_n$ est souvent notée comme un produit, ce n'est pas pour autant que cette opération devient commutative !*

Exercice 1.16

Seule l'identité est d'ordre 1.
Pour $k \in \{2, 3, 4, 5\}$, un k-cycle est d'ordre k. Un k-cycle est défini par le choix de k éléments parmi 5. On peut alors opérer $(k-1)!$ permutations circulaires de ces k éléments (le premier est choisi arbitrairement, tout ordre sur les $k-1$ autres définit une permutation circulaire).

Corrigé

Il y a donc $\binom{5}{k}$ $(k-1)!$ k-cycles dans $\mathcal{S}_5$.

Il reste les produits de cycles à supports disjoints qui peuvent être, soit deux transpositions, soit une transposition et un 3-cycle.

Dans le premier cas, l'ordre est 2. Il y a 15 éléments de $\mathcal{S}_5$ de ce type (5 choix de l'élément invariant puis 3 choix de l'image d'un des 4 éléments choisis qui définit la permutation).

Dans le second cas l'ordre est le ppcm de 2 et 3 soit 6. Il y a $\binom{5}{2}\ \binom{5}{3} = 20$ éléments de ce type dans $\mathcal{S}_5$.

En définitive, il y a respectivement :

25 éléments d'ordre 2, 20 d'ordre 3, 30 d'ordre 4, 24 d'ordre 5 et 20 d'ordre 6.

En comptant l'identité, d'ordre 1, on obtient bien les $120 = 5!$ éléments de $\mathcal{S}_5$.

Exercice 1.17

1. $\forall (x,y) \in G^2$,

$\varphi_g(xy) = g(xy)g^{-1} = gx(g^{-1}g)yg^{-1} = (gxg^{-1})(gyg^{-1}) = \varphi_g(x)\varphi_g(y)$.

Ainsi φ_g est un endomorphisme de groupe de G.

Clairement $\varphi_g \circ \varphi_{g^{-1}} = \varphi_{g^{-1}} \circ \varphi_g = \mathrm{Id}_G$.

Donc φ_g est bijective et $(\varphi_g)^{-1} = \varphi_{g^{-1}}$.

En conclusion φ_g est un automorphisme de G.

2. ▷ Soit $(a,b) \in G^2$.

On a : $\forall x \in G$, $(\varphi_a \circ \varphi_b)(x) = \varphi_a(\varphi_b(x)) = a(bxb^{-1})a^{-1}$
$= (ab)x(b^{-1}a^{-1}) = (ab)x(ab)^{-1} = \varphi_{ab}(x)$.

Donc $\Phi(ab) = \varphi_{ab} = \varphi_a \circ \varphi_b = \Phi(a) \circ \Phi(b)$.

Ainsi Φ est un morphisme de G dans $\mathrm{Aut}(G)$.

▷ Pour $g \in G$, on a :

$g \in \mathrm{Ker}\,\Phi \iff \Phi(g) = \mathrm{Id}_G \iff \varphi_g = \mathrm{Id}_G$
$\iff (\forall x \in G,\ gxg^{-1} = x) \iff (\forall x \in G,\ gx = xg)$

Ainsi le noyau de Φ est le sous-groupe $Z(G) = \{g \in G \mid \forall h \in G,\ gh = hg\}$ de G constitué des éléments qui commutent avec tous les autres (on l'appelle le *centre* de G).

3. Si on prend pour G un groupe commutatif, alors on a $Z(G) = G$, donc, d'après ce qui précède, $\mathrm{Im}\Phi = \{\mathrm{Id}_G\}$; et par ailleurs, clairement, l'application $u : G \longrightarrow G, x \longmapsto x^{-1}$ est un automorphisme du groupe G.

Donc si G est un groupe commutatif dans lequel il existe au moins un élément x tel que $x \neq x^{-1}$, alors Φ n'est pas surjective. Par exemple, pour $n \geqslant 3$ et $G = \mathbb{Z}/n\mathbb{Z}$ (additif), Φ n'est pas surjective.

4. Notons ε la signature : c'est un morphisme de $\mathcal{S}_n$ dans $\mathbb{U}_2 = \{-1,1\}$, qui est commutatif.

Soit $g \in G$. $\forall x \in G$, $\varepsilon(\varphi_g(x)) = \varepsilon(gxg^{-1}) = \varepsilon(g)\varepsilon(x)(\varepsilon(g))^{-1} = \varepsilon(x)$.

Donc $\forall x \in \mathcal{A}_n$, $\varepsilon(\varphi_g(x)) = \varepsilon(x) = 1$ et $\varphi_g(x) \in \mathcal{A}_n$.

Ainsi $\mathcal{A}_n$ est stable par les φ_g.

5. Soit $h \in \mathcal{H}$. Il existe $g \in G$ tel que $h = \Phi(g)$.

Donc $\varphi_\delta(h) = \delta \circ h \circ \delta^{-1}$ vérifie : $\forall x \in G$,

$[\varphi_\delta(h)](x) = \delta(h(\delta^{-1}(x))) = \delta(g\delta^{-1}(x)g^{-1})$
$= \delta(g)\delta[\delta^{-1}(x)]\delta(g^{-1}) = \delta(g)x(\delta(g))^{-1}$.

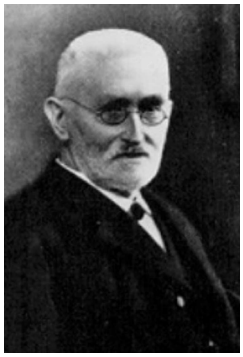
Donc $\varphi_\delta(h) = \Phi(\delta(g))$, donc $\varphi_\delta(h) \in \mathcal{H}$.

Ainsi $\mathcal{H}$ est stable par φ_δ.

Chapitre 2

Anneaux et corps

UN MATHÉMATICIEN



Richard Dedekind (1831-1916) suit à l'université de Göttingen les cours de Gauss et Dirichlet avant d'entamer une carrière universitaire. Son œuvre mathématique est immense. Il propose en 1871 une construction des nombres réels. Dedekind est également l'un des principaux fondateurs de la théorie des anneaux et des corps ; il introduit en 1879 la notion d'idéal. Avec Georg Cantor il concourt à l'émergence de la théorie des ensembles et la définition de la notion d'infini.

Un peu d'histoire

Les notions d'anneau et de corps se sont élaborées dans la deuxième moitié du XIX^{e} siècle. Avant de mourir tragiquement en duel, Galois avait ouvert la voie à l'adjonction de racines dans un ensemble de nombres afin de fournir des racines à des équations polynomiales. C'est en s'en inspirant que Leoplod Kronecker étudie en 1845 l'ensemble $\mathbb{Q}(\sqrt{2})$ puis généralise ce procédé de construction d'ensembles contenant les rationnels et stables par les opérations. Vers 1860, Ernst Kummer introduit les nombres algébriques définis comme racines d'équations polynomiales à coefficients entiers, qui possèdent également cette propriété de stabilité.

On doit à Richard Dedekind, en 1871, la première définition d'anneau et de corps, en tant que sous-ensemble des réels ou complexes. En 1893 Heinrich Weber donne une définition axiomatique équivalente à celle que nous connaissons.

Objectifs

les incontournables

- connaître les notions de première année : calcul dans un anneau, exemples usuels ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$), groupe des inversibles d'un anneau, anneau intègre, corps, sous-anneau, morphisme d'anneaux ;
- s'approprier la notion d'idéal, notion centrale de deuxième année ;
- savoir montrer qu'une partie d'un anneau est un sous-anneau, ou un idéal ;
- connaître la divisibilité dans un anneau commutatif intègre et le lien entre cette notion et la notion d'idéal ;
- savoir calculer modulo un entier fixé ;
- connaître l'anneau $\mathbb{Z}/n\mathbb{Z}$, en particulier ses éléments inversibles ;
- pratiquer l'arithmétique dans l'anneau des polynômes.

et plus si affinités

- connaître quelques anneaux et corps classiques ;
- maîtriser la notion d'idéal, opérer sur les idéaux.

Résumé de cours

Compléments sur les anneaux

Définition : *Un ensemble A, muni de deux lois de composition internes notées $+$ et $\times$ appelées respectivement addition et multiplication, est un* ***anneau*** *lorsque :*

i) $(A,+)$ *est un groupe commutatif.*

ii) La loi $\times$ *est associative.*

iii) La loi $\times$ *possède un élément neutre noté* $\mathbf{1}_A$*, différent du neutre additif* 0_A*.*

iv) La multiplication est distributive par rapport à l'addition, c'est-à-dire que pour tous a,b,c *dans* A *on a :* $a\times(b+c)=a\times b+a\times c$ *et* $(b+c)\times a=b\times a+c\times a$*.*

Si la loi $\times$ *est commutative, on dit que* A *est un anneau commutatif.*

Définition : *Soit* $\left(A_i,+_i,\times_i\right)_{1\leqslant i\leqslant n}$ *une famille finie d'anneaux. On munit l'ensemble produit* $A=\prod_{i=1}^{n}A_i$ *d'une structure d'anneau en posant :*

$$\forall\,(a,b)\in A^2,\ a+b=(a_i+_i b_i)_{1\leqslant i\leqslant n}\qquad a\times b=(a_i\times_i b_i)_{1\leqslant i\leqslant n}.$$

$(A,+,\times)$ *est un anneau, appelé* ***anneau-produit*** *des anneaux* $A_1,\ldots,A_n$*. On a :* $0_A=\left(0_{A_i}\right)_{1\leqslant i\leqslant n}$ *et* $\mathbf{1}_A=\left(\mathbf{1}_{A_i}\right)_{1\leqslant i\leqslant n}$*.*

Rappels rapides :

1. Un sous-anneau de A est une partie B de A qui contient $\mathbf{1}_A$ et vérifie : $\forall\,(x,y)\in B^2$, $x-y\in B$ et $x\times y\in B$.
2. Une application f de l'anneau $(A,+,\times)$ dans l'anneau $(B,\hat{+},*)$ est appelée un morphisme d'anneaux lorsqu'elle vérifie : $\forall\,(x,y)\in A^2$, $f(x+y)=f(x)\hat{+}f(y)$ et $f(x\times y)=f(x)*f(y)$, ainsi que $f(\mathbf{1}_A)=\mathbf{1}_B$.
3. L'image d'un sous-anneau par un morphisme d'anneau est un sous-anneau.
4. L'anneau A est intègre lorsque : $\forall(a,b)\in A^2$, $ab=0\Longrightarrow(a=0$ ou $b=0)$.
5. L'ensemble $\mathbb{U}(A)$ des éléments inversibles de A pour la multiplication est un groupe pour cette loi.

Définition : Corps —. *Un anneau commutatif dans lequel tout élément non nul possède un inverse s'appelle un* ***corps*** *commutatif.*

Idéaux d'un anneau commutatif

Dans cette partie, A et B désignent des anneaux **commutatifs**, leurs multiplications étant désormais notées par simple juxtaposition.

Définition : Idéaux —. *La partie I de A est un* ***idéal*** *de l'anneau A lorsqu'elle vérifie les deux assertions suivantes :*

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

ii) I *est* ***absorbant*** *: pour tout* $x\in I$ *et tout* $a\in A, xa\in I$*.*

Remarques : — Un idéal n'est pas, en général, un sous-anneau. Il est facile de vérifier que $2\mathbb{Z}$ est un idéal de $\mathbb{Z}$ et de constater que ce n'est pas un sous-anneau de $\mathbb{Z}$ puisqu'il ne contient pas 1.

— Un idéal qui contient un élément inversible est égal à l'anneau tout entier.

Exemple : $\{0_A\}$ et A sont des idéaux de A.

Proposition 2.1.— Caractérisation des idéaux —. Une partie I de l'anneau commutatif A est un idéal si, et seulement si :
i) I n'est pas vide ;
ii) I est stable pour $+$;
iii) pour tout $x \in I$ et tout $a \in A, xa \in I$.

Proposition 2.2.— Le noyau d'un morphisme ϕ de l'anneau A vers l'anneau B est un idéal de A.

Remarque : $\mathrm{Ker}\,\phi$ n'est pas, en général, un sous-anneau car $\phi(\mathbf{1}_A) = \mathbf{1}_B \neq 0_B : \mathbf{1}_A \notin \mathrm{Ker}\,(\phi)$.

Proposition 2.3.— Toute intersection d'idéaux est un idéal.

Remarque : Comme pour les groupes, on peut définir l'idéal engendré par une partie P de l'anneau A : c'est l'intersection de tous les idéaux contenant P, c'est donc le plus petit idéal contenant P.

Exemple : Étant donné deux idéaux I et J, le plus petit idéal contenant I et J, c'est-à-dire celui engendré par $I \cup J$, est $\{a + b,\, a \in I,\, b \in J\}$. Cet idéal est noté $I + J$.

Théorème 2.4.— Idéal engendré par un élément —. Soit x un élément fixé de l'anneau commutatif A. L'ensemble $\{xa,\, a \in A\}$ est l'idéal engendré par l'élément $x \in A$. C'est le plus petit idéal de A contenant x. On le note souvent xA ou (x).

Définition : Divisibilité dans un anneau commutatif intègre —. *Soit $(A, +, \times)$ un anneau commutatif intègre et $(a, b) \in A^2$. On dit que a **divise** b, ou que b est un **multiple** de a, s'il existe $c \in A$ tel que $b = ca$. Dans ce cas, on dit aussi que a est un **diviseur** de b et on note : $a \mid b$.*

Proposition 2.5.— Divisibilité et idéaux engendrés —. Avec les mêmes notations que ci-dessus :
$$a \text{ divise } b \iff bA \subset aA.$$

■ Idéaux de l'anneau commutatif intègre $\mathbb{Z}$

Théorème 2.6.— Idéaux de $\mathbb{Z}$ —. Les idéaux de $\mathbb{Z}$ sont les ensembles $n\mathbb{Z}$ pour $n \in \mathbb{Z}$. Tout sous-groupe de $(\mathbb{Z}, +)$ est donc un idéal.

Définition : PGCD de deux entiers —. *Le **PGCD** de deux entiers a et b est l'unique entier positif d tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. On note alors $d = a \wedge b$.*

Cette définition est équivalente à celle donnée en première année.

Définition : *Deux entiers a et b sont **premiers entre eux** si, et seulement si, $a \wedge b = 1$.*

Corollaire 2.7.— Relation de Bézout —. Soit $(a, b) \in \mathbb{Z}^2$ et $d \in \mathbb{N}$,
$$d = a \wedge b \iff \exists\,(u, v) \in \mathbb{Z}^2 \text{ tels que } au + bv = d.$$

Définition : PGCD de plusieurs entiers —. *Soit $(a_1, a_2, \ldots, a_n) \in \mathbb{Z}^n$. Le **PGCD** de $a_1, a_2, \ldots, a_n$*

est l'unique entier positif d tel que $\sum_{i=1}^{n} a_i\mathbb{Z} = d\mathbb{Z}$. *On note alors* $d = a_1 \wedge a_2 \wedge \ldots \wedge a_n$.

Définition : $a_1, a_2, \ldots, a_n$ *sont* ***premiers entre eux*** *si, et seulement si,* $a_1 \wedge a_2 \wedge \ldots \wedge a_n = 1$.

Faire la différence avec « $a_1, a_2, \ldots, a_n$ sont **deux à deux premiers entre eux** », propriété qui entraîne « $a_1, a_2, \ldots, a_n$ sont premiers entre eux », la réciproque étant fausse.

Corollaire 2.8.— Relation de Bézout —. Soit $(a_1, a_2, \ldots, a_n) \in \mathbb{Z}^n$ et $d \in \mathbb{N}$,

$$d = a_1 \wedge a_2 \wedge \ldots \wedge a_n \iff \exists\,(u_1, u_2, \ldots, u_n) \in \mathbb{Z}^n \text{ tels que } \sum_{i=1}^{n} a_i u_i = d.$$

■ Anneau $\mathbb{Z}/n\mathbb{Z}$

$\left(\mathbb{Z}/n\mathbb{Z}, +\right)$ a déjà été traité dans le chapitre précédent. Munissons maintenant $\mathbb{Z}/n\mathbb{Z}$ d'une multiplication.

Théorème 2.9.— Si $(a, a', b, b') \in \mathbb{Z}^4$ avec $a \equiv a'\,[n]$ et $b \equiv b'\,[n]$, alors $a \times b \equiv a' \times b'\,[n]$. La relation de congruence modulo n est compatible avec la multiplication.
On peut donc définir sur $\mathbb{Z}/n\mathbb{Z}$ l'opération : $\overline{a} \times \overline{b} = \overline{a \times b}$.
L'addition, déjà définie dans le chapitre précédent, et le produit ainsi défini ne dépendent pas des représentants choisis.
Pour $n \geqslant 2$, l'ensemble $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif.

- L'application σ_n de $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ qui envoie chaque $a \in \mathbb{Z}$ sur $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ est un morphisme d'anneaux surjectif. On l'appelle la surjection canonique.
- Une récurrence simple conduit à : $\forall\, k \in \mathbb{N}$, $\overline{a^k} = \overline{a}^k$.

Théorème 2.10.— L'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ est un groupe pour $\times$. Pour tout $k \in \mathbb{Z}$, $\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si, et seulement si, $k \wedge n = 1$.

Corollaire 2.11.— $\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est premier.

Remarque : Pour p premier, on note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$.

Théorème 2.12.— des restes chinois —. Soit m et n deux entiers naturels $\geqslant 2$, ***premiers entre eux***. $\overline{k}$, $\hat{k}$ et $\tilde{k}$ désignant respectivement les classes de congruence de k dans $\mathbb{Z}/mn\mathbb{Z}$, $\mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$, l'application $\left\{\begin{array}{ccc} \mathbb{Z}/mn\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ \overline{k} & \longmapsto & \left(\hat{k}, \tilde{k}\right) \end{array}\right.$ est bien définie et est un isomorphisme d'anneaux.

Ce résultat s'étend à plus de deux facteurs : si $(m_1, m_2, \ldots, m_n)$ est une famille d'entiers naturels ***deux à deux premiers entre eux***, alors, avec des notations similaires à ci-dessus, l'application $\left\{\begin{array}{ccc} \mathbb{Z}/(\prod_{i=1}^{n} m_i)\mathbb{Z} & \longrightarrow & \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_n\mathbb{Z} \\ \overline{k} & \longmapsto & \left(\hat{k}, \tilde{k}, \ldots, \check{k}\right) \end{array}\right.$, bien définie, est un isomorphisme d'anneaux.

Définition : Indicatrice d'Euler —. *On appelle* ***indicatrice d'Euler*** *l'application φ de $\mathbb{N}^*$ dans $\mathbb{N}^*$ définie par : $\varphi(1) = 1$ et, pour tout $n \geqslant 2$, $\varphi(n)$ est le nombre d'entiers $k \in \mathbb{N}$ tels que*
$$1 \leqslant k < n \text{ et } k \wedge n = 1.$$

Proposition 2.13.— Soit m et n deux entiers naturels non nuls et premiers entre eux. Alors :
$$\varphi(mn) = \varphi(m)\varphi(n)$$

Proposition 2.14.— Soit $n \geqslant 2$ un entier naturel. Soit $n = {p_1}^{\alpha_1} \dots {p_k}^{\alpha_k}$ (les p_i nombres premiers distincts, les $\alpha_i \in \mathbb{N}^*$) sa décomposition en produit de puissances de nombres premiers. Alors :
$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right).$$
En particulier, si p est premier et si $k \in \mathbb{N}^*$, alors, $\varphi(p^k) = p^k - p^{k-1}$.

Théorème 2.15.— d'Euler —. Soit $n \geqslant 2$ dans $\mathbb{N}$ et a un entier relatif premier avec n. Alors :
$$a^{\varphi(n)} \equiv 1\,[n].$$

Remarque : Si p est premier, $\varphi(p) = p - 1$. Le théorème d'Euler est une généralisation du petit théorème de Fermat :

Corollaire 2.16.— Petit théorème de Fermat —. Soit p un nombre premier. Soit a un entier relatif non divisible par p. Alors $a^{p-1} \equiv 1\,[p]$.

■ Anneau $\mathbb{K}[X]$

Dans cette partie, $\mathbb{K}$ désigne un sous-corps de $\mathbb{C}$.

Théorème 2.17.— Pour tout idéal I non nul de $\mathbb{K}[X]$, il existe un unique polynôme unitaire P qui engendre I. On a donc $I = (P) = \{PQ,\, Q \in K[X]\} = P\mathbb{K}[X]$.

Définition : PGCD —. *Soit $(P_1, \dots, P_n)$ un n-uplet de polynômes non tous nuls.*
L'unique polynôme unitaire engendrant l'idéal
$$(P_1) + \dots + (P_n) = \{\ U_1P_1 + \dots + U_nP_n,\ (P_1, \dots, P_n) \in \mathbb{K}[X]^n\ \}$$
s'appelle PGCD de $(P_1, \dots, P_n)$.
On convient que PGCD de $(0, \dots, 0)$ est 0.

Proposition 2.18.— Caractérisation du PGCD —. Un polynôme D est le PGCD de $(P_1, \dots, P_n)$ si, et seulement si :
1 - D est unitaire ;
2 - pour tout $i \in [\![1, n]\!]$, $D \mid P_i$;
3 - Pour tout polynôme R, ($\forall i \in [\![1, n]\!]$, $R \mid P_i$) entraîne $R \mid D$ (Tout polynôme divisant chacun des P_i divise D).

Définition : PPCM —. *Soit $(P_1, \dots, P_n)$ un n-uplet de polynômes tous non nuls.*
L'unique polynôme unitaire engendrant $(P_1) \cap \dots \cap (P_n)$ s'appelle le PPCM de $(P_1, \dots, P_n)$.
On convient que si l'un des P_i est nul, le PPCM de $(P_1, \dots, P_n)$ est 0.

Proposition 2.19.— Caractérisation du PPCM —. Un polynôme M est le PPCM de $(P_1, \dots, P_n)$ si, et seulement si :
1 - M est unitaire ;
2 - pour tout $i \in [\![1, n]\!]$, $P_i \mid M$;
3 - Pour tout polynôme R, $(\forall i \in [\![1, n]\!],\ P_i \mid R)$ entraîne $M \mid R$.

Définition : *$P_1, \dots, P_n$ sont premiers entre eux dans leur ensemble lorsque leur PGCD vaut* 1.

Théorème 2.20.— Identité de Bézout —. $P_1, \dots, P_n$ sont premiers entre eux dans leur ensemble si, et seulement s'il existe $(U_1, \dots, U_n) \in \mathbb{K}[X]^n$ tel que $U_1P_1 + \cdots + U_nP_n = 1$.

Théorème 2.21.— Théorème de Gauss —. Étant donné trois polynômes P, Q et R, si $P \mid QR$ et $P \wedge Q = 1$, alors $P \mid R$.

■ Polynôme irréductible

Dans ce paragraphe encore, $\mathbb{K}$ est un sous-corps de $\mathbb{C}$.

Définition : *Un polynôme P de $\mathbb{K}[X]$ est dit **irréductible** dans $\mathbb{K}[X]$ lorsque* $\deg P \geqslant 1$ *et les seuls diviseurs de P dans $\mathbb{K}[X]$ sont les polynômes de degré* 0 *et les λP, où $\lambda \in \mathbb{K}^*$.*

Théorème 2.22.— Décomposition en facteurs irréductibles —. Soit $P \in \mathbb{K}[X]$ de degré $\geqslant 1$.
Il existe $\lambda \in \mathbb{K}^*$, $k \in \mathbb{N}^*$, un k-uplet $(P_1, \dots, P_k)$ de polynômes unitaires irréductibles et $(n_1, \dots, n_k) \in (\mathbb{N}^*)^k$ tels que : $P = \lambda P_1^{n_1} \cdots P_k^{n_k}$.
λ est le coefficient dominant de P, et il y a unicité, à l'ordre près des facteurs, d'une telle décomposition.

Théorème 2.23.— de d'Alembert-Gauss —. Tout polynôme de $\mathbb{C}[X]$ non constant admet au moins une racine dans $\mathbb{C}$.

Proposition 2.24.— Polynômes irréductibles de $\mathbb{C}[X]$ —. Les éléments irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.

Proposition 2.25.— Polynômes irréductibles de $\mathbb{R}[X]$ —. Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 à discriminant strictement négatif (i.e. de la forme $aX^2 + bX + c$ où $(a, b, c) \in \mathbb{R}^* \times \mathbb{R}^2$ et $b^2 - 4ac < 0$).

■ Notion de K-algèbre

Dans cette section, K désigne un corps commutatif quelconque.

Définition : *On appelle K–**algèbre**, ou algèbre sur K, tout quadruplet $(A, +, \times, .)$ tel que :*
i) $(A, +, .)$ est un K-espace vectoriel ;
ii) $(A, +, \times)$ est un anneau ;
iii) $\forall \lambda \in K,\ \forall (a, b) \in A^2,\ (\lambda.a) \times b = a \times (\lambda.b) = \lambda.(a \times b)$.

Vocabulaire : ▸ *Une K-algèbre est dite de dimension finie lorsque le K-espace vectoriel sous-jacent est de dimension finie ; si tel est le cas, on appelle dimension de la K-algèbre la dimension du K-espace vectoriel sous-jacent.*

▸ *Une K-algèbre est dite commutative [resp. intègre] lorsque l'anneau $(A, +, \times)$ est commutatif [resp. intègre].*

Exemples : – Si I est un ensemble non vide, l'ensemble K^I des applications de I dans K, muni des lois usuelles, est une K-algèbre commutative.
– Si E est un K-espace vectoriel non réduit à $\{0\}$, $(\mathscr{L}(E), +, \circ, .)$ est une K-algèbre.
– L'ensemble $\mathscr{M}_n(K)$ des matrices carrées à n lignes à coefficients dans K est une K-algèbre, non commutative ni intègre si $n \geqslant 2$.

Définition : *Soit A une K-algèbre. On appelle **sous-algèbre de** A toute partie de A qui est à la fois un sous-espace vectoriel de A et un sous-anneau de A.*

Définition : *Soit A et B deux algèbres sur le même corps K. On appelle **morphisme d'algèbres** de A dans B toute application $f : A \longrightarrow B$ qui est à la fois un morphisme de K-espaces vectoriels et un morphisme d'anneaux de A dans B.*

Exemple : Soit $a \in \mathbb{K}$, l'application $\left\{ \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathbb{K} \\ P & \longmapsto & P(a) \end{array} \right.$ est un morphisme d'algèbre.

Proposition 2.26.— f est un morphisme d'algèbres de A dans B si, et seulement si, elle vérifie les trois propriétés :
- $\forall (\alpha, \beta) \in K^2$, $\forall (x, y) \in A^2$, $f(\alpha x + \beta y) = \alpha f(x) + \beta f(y)$ (c'est-à-dire : f est linéaire) ;
- $\forall (x, y) \in A^2$, $f(xy) = f(x)f(y)$;
- $f(\mathbf{1}_A) = \mathbf{1}_B$.

Méthodes

Comment montrer qu'un ensemble muni d'une loi de composition interne est un anneau

❑ **Méthode 2.1.—** Pour montrer que $(A, +, .)$ est un anneau, on peut :

- utiliser la définition d'un anneau ;
- montrer que c'est un sous-anneau d'un anneau ou d'un corps connu ;
- transporter une structure d'anneau par un morphisme (voir exemple ci-dessous).

Mise en œuvre : exercice 2.14, **exercice 2.16**.

Remarque : Se rappeler que l'ensemble des fonctions d'un ensemble quelconque dans un anneau $(A, +, .)$ est lui-même un anneau pour les opérations fonctionnelles définies par :

$$f + g : x \longmapsto f(x) + g(x) \text{ et } f \times g : x \longmapsto f(x).g(x).$$

Exemple : *On définit sur l'ensemble $\mathscr{P}(E)$ des parties de l'ensemble non vide E l'opération : $A\Delta B = (A \setminus B) \cup (B \setminus A)$ et l'opération $\cap$. Montrons que $(\mathscr{P}(E), \Delta, \cap)$ est un anneau.*

L'ensemble F des applications continues de E dans $\mathbb{Z}/2\mathbb{Z}$ est un anneau (cf. remarque précédente). Notons ψ l'application qui à $f \in F$ fait correspondre $\{x \in E \mid f(x) = \overline{1}\}$.
Alors $\psi(f+g) = \{x \in E \mid f(x)+g(x) = \overline{1}\}$. Or $f(x)+g(x) = \overline{1}$ équivaut à : ($f(x) = \overline{1}$ et $g(x) = \overline{0}$) ou ($f(x) = \overline{0}$ et $g(x) = \overline{1}$), soit à : $x \in \psi(f)\Delta\psi(g)$. On en déduit que $\psi(f + g) = \psi(f)\Delta\psi(g)$.
De même $\psi(f \times g) = \{x \in E \mid f(x)g(x) = \overline{1}\}$. Or $f(x)g(x) = \overline{1}$ équivaut à $f(x) = \overline{1}$ et $g(x) = \overline{1}$, soit à : $x \in \psi(f) \cap \psi(g)$. On en déduit que $\psi(f + g) = \psi(f) \cap \psi(g)$.
Il s'ensuit que ψ est un morphisme d'anneaux. Or ψ est bijective car pour tout $A \in \mathscr{P}(E)$, la fonction définie par : $f_A(x) = \overline{1}$ si $x \in A$ et $f(x) = \overline{0}$ sinon vérifie $\psi(f_A) = A$, et c'est clairement la seule.
Donc $\psi(F) = \mathscr{P}(E)$ est un anneau.

Comment montrer qu'un ensemble K est un corps

❑ **Méthode 2.2.—** Soit K un ensemble muni de deux lois de composition interne, $+$ et $\times$. Pour montrer que $(K, +, \times)$ est un corps, on peut :

- Montrer que K est un anneau commutatif dans lequel tout élément non nul est inversible.
- Montrer que K est un anneau et que l'ensemble $(K^*, \times)$ est un groupe pour la multiplication.
- Montrer que K est un sous-anneau d'un anneau connu A, que tout élément non nul de K est inversible dans A et que son inverse est dans K.

Mise en œuvre : exercice 2.12.

Exemple : *Notons* $K = \{a + b\sqrt{2},\ (a,b) \in \mathbb{Q}^2\}$. *Montrer que* K *est un sous-corps de* $\mathbb{R}$.

Il est aisé de montrer que K est un sous-anneau de $\mathbb{R}$.
Soit $x = a+b\sqrt{2} \neq 0$; alors x est inversible dans $\mathbb{R}$ et $\dfrac{1}{x} = \dfrac{a - b\sqrt{2}}{a^2 - 2b^2} = \dfrac{a}{a^2 - 2b^2} + \dfrac{-b}{a^2 - 2b^2}\ \sqrt{2} \in K$
car $\left(\dfrac{a}{a^2 - 2b^2}, \dfrac{-b}{a^2 - 2b^2}\right) \in \mathbb{Q}^2$.
Ainsi K est un sous-corps de $\mathbb{R}$.

■ Comment montrer qu'un ensemble muni d'une loi de composition interne est un sous-anneau

❑ **Méthode 2.3.—** Soit A un anneau. Soit B une partie de A. Pour montrer que B est un sous-anneau de A, on peut :

- Utiliser la caractérisation des sous-anneaux.
- Montrer que c'est l'image d'un sous-anneau par un morphisme.

Mise en œuvre : exercice 2.14, **exercice 2.16**.

■ Comment montrer qu'un sous-ensemble d'un anneau est un idéal

❑ **Méthode 2.4.—** Soit A un anneau. Soit I une partie de A.
Pour montrer que I est un idéal de A, on peut :

- Utiliser la caractérisation de la **proposition 2.1**.
- Montrer que c'est le noyau d'un morphisme d'anneaux.
- Montrer que c'est une intersection d'idéaux.
- Montrer que c'est l'idéal engendré par une partie.

Remarque : L'idéal engendré par une partie G de A est l'intersection de tous les idéaux de A qui contiennent G.

Mise en œuvre : exercice 2.15, **exercice 2.16**.

Exemple : *Montrer que l'ensemble des polynômes réels dont tous les coefficients sont nuls jusqu'au degré* $p-1$ *inclus est un idéal de* $\mathbb{R}[X]$.
C'est l'ensemble des polynômes divisibles par X^p, c'est donc $X^p\mathbb{R}[X]$, donc c'est l'idéal engendré par X^p.

Exemple : *Soit* $a \in \mathbb{C}$. *Montrer que* $I_a = \{P \in \mathbb{Q}[X] \ \mid \ P(a) = 0\}$ *est un idéal de* $\mathbb{Q}[X]$.
L'application $\phi_a : P \longmapsto P(a)$ est clairement un morphisme de l'anneau $\mathbb{Q}[X]$ vers $\mathbb{C}$, car $(P+Q)(a) = P(a) + Q(a)$ et $(PQ)(a) = P(a)Q(a)$ et $\phi_a(1) = 1$.
Or I_a est le noyau de ϕ_a, c'est donc un idéal de $\mathbb{Q}[X]$.

■ Comment manier les congruences modulo n

❑ **Méthode 2.5.—** Parmi les utilisations des congruences modulo n, on peut citer les trois suivantes, importantes :

- Recherche du reste de la division euclidienne par n.
- Résolution d'équations dans $\mathbb{Z}/n\mathbb{Z}$.
- Utilisation du théorème d'Euler (de Fermat si n est premier).

Mise en œuvre : exercice 2.5, **exercice 2.6**.

Exemple : *Déterminer le reste r de la division euclidienne de 9^{43} par 7.*
Comme $9 \equiv 2[7]$, $9^{43} \equiv 2^{43}[7]$: r est le reste de la division euclidienne de 2^{43} par 7. On cherche alors une puissance de 2 proche de 7. Comme $2^3 = 8 = 7+1$, on écrit $43 = 3\times14+1$ donc $2^{43} = (2^3)^{14}\times2$. Or $(2^3)^{14}$ est congru à 1 modulo 7, donc 2^{43} est congru à 2 modulo 7 . Finalement, $r = 2$.

Remarque : Si n est premier, $\mathbb{Z}/n\mathbb{Z}$ est un corps, donc les méthodes de résolution d'équations ou de systèmes sont analogues à celles vues dans $\mathbb{R}$ ou $\mathbb{C}$. Il suffit juste se rappeler que diviser par $\overline{k}$ revient à multiplier par son inverse dans $\mathbb{Z}/n\mathbb{Z}$. Ainsi, diviser par $\overline{5}$ dans $\mathbb{Z}/7\mathbb{Z}$, revient à multiplier par $\overline{3}$ car $\overline{5}\times\overline{3} = \overline{1}$.
Si n n'est pas premier, il existe des diviseurs de zéro et de nouvelles solutions peuvent apparaître. Faire attention au fait que l'égalité $(x-a)(x-b) = 0$ admet en général d'autres solutions que $x = a$ ou $x = b$, et que multiplier une équation par un élément non inversible ne donne pas une équation équivalente.

■ Applications du théorème des restes chinois et de l'indicatrice d'Euler

❑ **Méthode 2.6.— Résolution d'un système de congruences —.** Soit $n \geqslant 2$, $m_1, m_2, \ldots, m_n$ des entiers deux à deux premiers entre eux, pour résoudre le système de congruences :

$$\begin{cases} x & \equiv & x_1\,[m_1] \\ x & \equiv & x_2\,[m_2] \\ & \ldots & \\ x & \equiv & x_n\,[m_n] \end{cases}$$

on utilisera le théorème des restes chinois qui affirme que $(\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n})$ de $\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \ldots \times \mathbb{Z}/m_n\mathbb{Z}$ admet un unique antécédent $\overline{x}$ dans $\mathbb{Z}/M\mathbb{Z}$, où $M = \prod_{i=1}^{n} m_i$, par l'isomorphisme canonique entre ces ensembles.
Il s'agira donc de déterminer cet antécédent, puis de choisir, éventuellement, un représentant pertinent de cette classe d'équivalence modulo M.

Mise en œuvre : exercice 2.10.

Exemple : *Trouver le plus petit réel positif x vérifiant* $\begin{cases} x & \equiv & 3\,[17] \\ x & \equiv & 5\,[6] \end{cases}$.

Méthodes

6 et 17 sont bien premiers entre eux, le x cherché existe effectivement et est unique modulo $6 \times 17 = 102$.
On cherche x sous la forme : $x = 3 \times u + 5 \times v$, où u et v sont des entiers relatifs vérifiant :

$$\begin{cases} u \equiv 1\,[17] \text{ et } u \equiv 0\,[6] \\ v \equiv 0\,[17] \text{ et } v \equiv 1\,[6] \end{cases},$$

de manière à ce que les équations du système soient vérifiées.
Donc : $x = 3 \times 6 \times h + 5 \times 17 \times k$, où $(h, k) \in \mathbb{Z}^2$ tel que $6h \equiv 1\,[17]$ et $17k \equiv 1\,[6]$.
$17k \equiv 1\,[6] \iff (-1)k \equiv 1\,[6]$. $k = -1$ ou $k = 5$ conviennent.
$6h \equiv 1\,[17] \iff 6h \equiv 18\,[17]$. $h = 3$ convient.
$x = 3 \times 6 \times 3 + 5 \times 17 \times 5 = 479 \equiv 71\,[102]$. 71 est la solution du problème.

Exemple : *Résoudre* $\begin{cases} x \equiv 3\,[8] \\ x \equiv 7\,[12] \\ x \equiv 1\,[14] \end{cases}$.

8, 12 et 14 ne sont pas deux à deux premiers entre eux : le théorème des restes chinois ne s'applique plus. On peut sans doute s'y ramener.
$x \equiv 7\,[12] \Longrightarrow x \equiv 1\,[3]$ et $x \equiv 1\,[14] \Longrightarrow x \equiv 1\,[7]$.
8, 3 et 7 sont bien deux à deux premiers entre eux, le x cherché existe effectivement et est unique modulo $8 \times 3 \times 7 = 168$.
Comme précédemment, cherchons $x = 3 \times 3 \times 7 \times h + 1 \times 8 \times 7 \times k + 1 \times 8 \times 3 \times \ell$, où $(h, k, \ell) \in \mathbb{Z}^3$ tel que $21h \equiv 1\,[8]$, donc $5h \equiv 1\,[8]$, $56k \equiv 1\,[3]$, donc $2k \equiv 1\,[3]$ et $24\ell \equiv 1\,[7]$, donc $3\ell \equiv 1\,[7]$.
$h = 5$, $k = 2$ et $\ell = 5$ conviennent, donc $x = 63 \times 5 + 56 \times 2 + 24 \times 5 = 547 \equiv 43\,[168]$.
Réciproquement, on vérifie facilement que 43 vérifie le système et que 168 est congru à 0 modulo 8,12 et 14.

Les solutions sont les $43 + n \times 168$, $n \in \mathbb{Z}$.

❑ **Méthode 2.7.— Calcul d'inverse, calcul de reste.** $m_1, m_2, \ldots, m_p$ étant deux à deux premiers entre eux, si on note φ l'isomorphisme canonique de $\mathbb{Z}/(m_1 ... m_p)\mathbb{Z}$ dans $\mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_p\mathbb{Z}$, l'idée est de faire les calculs demandés sur $\varphi(n)$. Ils seront plus simples car modulo les m_i qui sont plus petits que le produit $m_1 \times \ldots \times m_p$.
Le prix à payer est la recherche un peu lourde, de l'antécédent de la solution trouvée par l'isomorphisme ϕ.

Exemple : *Calculer* $\overline{17}^{100}$ *dans* $\mathbb{Z}/360\mathbb{Z}$. *Calculer l'inverse de* $\overline{17}$ *dans* $\mathbb{Z}/360\mathbb{Z}$.

$360 = 2^3 \times 3^2 \times 5 = 8 \times 9 \times 5$, où 8, 9 et 5 sont deux à deux premiers entre eux. Soit φ l'isomorphisme d'anneaux canonique de $\mathbb{Z}/360\mathbb{Z}$ dans $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, $\varphi(\overline{17}) = (\overline{1}, \overline{-1}, \overline{2})$.
$\varphi\left(\overline{17}^{100}\right) = \left(\varphi(\overline{17})\right)^{100} = (\overline{1}^{100}, \overline{-1}^{100}, \overline{2}^{100}) = (\overline{1}, \overline{1}, \overline{1})$ (dans $\mathbb{Z}/5\mathbb{Z}$, $\overline{2}^{100} = \left(\overline{2}^4\right)^{25} = \overline{1}^{25} = \overline{1}$).
L'antécédent dans $\mathbb{Z}/360\mathbb{Z}$ de $(\overline{1}, \overline{1}, \overline{1})$ par φ est évidemment $\overline{1}$, donc, dans $\mathbb{Z}/360\mathbb{Z}$, $\overline{17}^{100} = \overline{1}$.

$\overline{17}$ admet bien un inverse dans $\mathbb{Z}/360\mathbb{Z}$, puisque $17 \wedge 360 = 1$. Pour le trouver, l'idée est la même, mais ce sera un peu plus fastidieux en terme de calcul.
$\varphi\left(\overline{17}^{-1}\right) = \left(\varphi(\overline{17})\right)^{-1} = (\overline{1}^{-1}, \overline{-1}^{-1}, \overline{2}^{-1}) = (\overline{1}, \overline{-1}, \overline{3})$ (dans $\mathbb{Z}/5\mathbb{Z}$, $\overline{2}^{-1} = \overline{3}$, car $6 \equiv 1\,[5]$).
Chercher l'antécédent x dans $\mathbb{Z}/360\mathbb{Z}$ de $(\overline{1}, \overline{-1}, \overline{3})$ par φ revient à résoudre le système de congruences $\begin{cases} x \equiv 1\,[8] \\ x \equiv -1\,[9] \\ x \equiv 3\,[5] \end{cases}$

Cherchons $x = 1 \times 9 \times 5 \times h + (-1) \times 8 \times 5 \times k + 3 \times 8 \times 9 \times \ell$, où $(h, k, \ell) \in \mathbb{Z}^3$ tel que $45h \equiv 1\,[8]$, donc $5h \equiv 1\,[8]$, $40k \equiv 1\,[9]$, donc $4k \equiv 1\,[9]$ et $72\ell \equiv 1\,[5]$, donc $2\ell \equiv 1\,[5]$.
$h = 5$, $k = 7$ et $\ell = 3$ conviennent, donc $x = 45 \times 5 - 40 \times 7 + 216 \times 3 = 593 \equiv 233\,[360]$.
L'inverse de $\overline{17}$ dans $\mathbb{Z}/360\mathbb{Z}$ est $\overline{233}$.

❑ **Méthode 2.8.— Utilisation de l'indicatrice d'Euler —.** Il faut simplement connaître sa définition et les propriétés listées par le programme : application multiplicative, expression à partir de la décomposition en facteurs premiers, théorème d'Euler et petit théorème de Fermat.

Mise en œuvre : exercice 2.3, **exercice 2.8**,**exercice 2.9**, **exercice 2.11**.

■ Comment montrer qu'un polynôme en divise un autre

❑ **Méthode 2.9.—** Soit P et Q deux éléments de $\mathbb{K}[X]$. Pour montrer que P divise Q, on peut :

- Raisonner à l'aide des racines.
- Utiliser le théorème de Gauss.

Remarque : Si le polynôme P est scindé à racines simples, P divise Q si, et seulement si, pour toute racine α de P, $Q(\alpha) = 0$.

Exemple : *Montrer que si d divise n, $n = pd$, alors $X^d - 1$ divise $X^n - 1$.*

Plaçons-nous dans $\mathbb{C}$. Soit $\zeta \in \mathbb{C}$ une racine de $X^d - 1$, alors $\zeta^d = 1$ donc $\zeta^n = (\zeta^d)^p = 1^p = 1$, donc ζ^d est racine de $X^n - 1$. Le résultat s'en déduit puisque $X^d - 1$ n'a que des racines simples qui sont les racines d-ièmes de l'unité.

Exemple : *Montrer que $P = X^2 + X + 1$ divise $Q = X^{3n} - 1$.*

Remarquons que les racines de P sont j et $\overline{j}$ avec $j = e^{2i\pi/3}$. P et Q étant à coefficients réels, si $P(\zeta) = 0$, alors $P(\overline{\zeta}) = \overline{P(\zeta)} = 0$. Il suffit donc de montrer que j est racine de Q ; ceci est vérifié car $j^{3n} = \left(j^3\right)^n = 1^n = 1$. Le résultat demandé s'en déduit.

Exemple : *Montrer que $X^2 + X + 1$ divise $X^4 + X^2 + 1$.*

Nous savons par l'exemple précédent que X^2+X+1 divise X^6-1. Or $X^6-1 = (X^2-1)(X^4+X^2+1)$. Or $X^2 + X + 1$ et $X^2 - 1$ sont premiers entre eux, car ils n'ont aucune racine complexe commune. Le théorème de Gauss permet d'affirmer que $X^2 + X + 1$ divise $X^4 + X^2 + 1$.

Vrai/Faux

	Vrai	Faux
1. Si A est un anneau, alors, pour tout $(a,b) \in A^2$, $(a+b)^2 = a^2 + 2ab + b^2$.	☐	☐
2. L'anneau-produit $A_1 \times \ldots \times A_n$ est commutatif si, et seulement si, $A_1, \ldots, A_n$ sont tous commutatifs.	☐	☐
3. Si a est un élément non nul de l'anneau A, alors : $a \times b = a \times c \Longrightarrow b = c$.	☐	☐
4. $\big(\mathscr{M}_n(\mathbb{K}), +, \times\big)$ est un anneau intègre.	☐	☐
5. $\mathbb{U}(A)$ est un sous-groupe additif de l'anneau A.	☐	☐
6. $\mathbb{U}(A)$ est un sous-groupe multiplicatif de l'anneau A.	☐	☐
7. Si A_1 et A_2 sont intègres, l'anneau produit $A_1 \times A_2$ est intègre.	☐	☐
8. Tout idéal d'un anneau est un sous-anneau.	☐	☐
9. Tout sous-anneau de A est un sous-groupe additif.	☐	☐
10. La seule partie de l'anneau A qui est à la fois un sous-anneau et un idéal est A lui-même.	☐	☐
11. Si l'anneau A est intègre, alors A est un corps.	☐	☐
12. Si n est premier, alors $\mathbb{Z}/n\mathbb{Z}$ est un corps.	☐	☐
13. A désigne $\mathbb{Z}$ ou $K[X]$. a et b sont premiers entre eux si, et seulement si, il existe $(u,v) \in A^2$ tel que $au + bv = 1$.	☐	☐
14. Tout polynôme de degré 1 est irréductible.	☐	☐
15. Un polynôme de degré trois est irréductible si, et seulement s'il n'a pas de racine.	☐	☐
16. Un polynôme de $\mathbb{R}[X]$ sans racine réelle est irréductible.	☐	☐
17. L'indicatrice d'Euler peut être définie par $\varphi(1) = 1$ et $\forall\, n \geqslant 2$, $\varphi(n) = \mathsf{Card}\ \big(\mathbb{U}(\mathbb{Z}/n\mathbb{Z})\big)$.	☐	☐
18. Si φ est l'indicatrice d'Euler, pour tout $n \geqslant 3$, $\varphi(n)$ est pair.	☐	☐

Énoncé des exercices

Exos minutes

Exercice 2.1 : Résoudre les équations suivantes dans $\mathbb{Z}/7\mathbb{Z}$:

$$x^2 - \overline{5}x + \overline{6} = \overline{0} \qquad \begin{cases} \overline{3}x + & \overline{2}y = & \overline{1} \\ x + & y = & \overline{5} \end{cases}$$

Exercice 2.2 : Quels sont les idéaux d'un corps $\mathbb{K}$?

Anneaux $\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$

Exercice 2.3 : Soit G un groupe cyclique multiplicatif d'ordre $n \in \mathbb{N}^*$, de générateur g.
1. Montrer que $x \in G$ est un générateur de G si, et seulement si, il existe un entier naturel a tel que $x^a = g$.
2. Montrer que, si $k \in [\![1, n-1]\!]$, g^k est un générateur de G si, et seulement si, k et n sont premiers entre eux. En déduire le nombre de générateurs de G.

Exercice 2.4 : On note p un nombre premier.
1. Montrer que pour tout $k \in [\![1, p-1]\!]$, p divise $\binom{p}{k}$.
2. On note $\mathbb{F}_p$ l'anneau $\mathbb{Z}/p\mathbb{Z}$, montrer que l'application de $\mathbb{F}_p$ dans $\mathbb{F}_p$ définie par $\phi : a \longmapsto a^p$ est un isomorphisme d'anneaux, puis que c'est l'identité.
3. Montrer que pour tout $x \in \mathbb{Z}$, $x^p \equiv x\,[p]$.
Ce résultat, vu en cours par une autre démarche, est le petit théorème de Fermat.

Exercice 2.5 : 1. Décomposer $a = 383838$ en produit de facteurs premiers.
2. En utilisant plusieurs fois le petit théorème de Fermat, montrer que pour tout $n \in \mathbb{N}$, $a = 383838$ divise $n^{37} - n$.

Exercice 2.6 : 1. Trouver le reste de la division de 17^{17} par 7.
2. Trouver le reste de la division de 4^{30} par 7.

Exercice 2.7 : Déterminer le groupe des inversibles de $\mathbb{Z}/8\mathbb{Z}$. Ce groupe est-il cyclique ?
D'après Mines-Ponts

Exercice 2.8 ** : Montrer qu'il existe un multiple de 23 qui ne s'écrit qu'avec des 1 en base 10.
D'après École Polytechnique

Exercice 2.9 : Trouver les trois derniers chiffres de 9^{1000}.

Exercice 2.10 : Résoudre $\begin{cases} x \equiv 3\,[17] \\ x \equiv 4\,[11] \\ x \equiv 5\,[6] \end{cases}$.