Sylvain Gugger
Gérard Rozsavolgyi
Laurent Pater
Henri Lemberg

PARCOURS PRÉPAS

MATHS MP/MP* MPI/MPI*

EDISCIENCE

Création de couverture : Studio graphique Dunod

11 rue Paul Bert, 92240 Malakoff
www.dunod.com
ISBN 978-2-10-084100-4

Avant-propos

Cet ouvrage s'adresse aux élèves de deuxième année de classe préparatoire MP-MPI. Il s'agit d'un complément à leur cours de mathématiques mettant l'accent sur les notions essentielles à connaître et les méthodes à maîtriser, et permettant de les mettre en œuvre par le biais d'exercices.
Le livre est divisé en quatre parties, quatorze chapitres et une section de sujets d'annales.

Chaque chapitre commence par une partie nommée *L'essentiel du cours*. On y présente tous les points les plus importants du cours (définitions, propositions, théorèmes, remarques) à la manière d'une fiche. Les preuves ne sont volontairement pas incluses pour se concentrer sur les résultats à connaître, mais peuvent être trouvées dans votre cours au besoin. La première chose à faire pour apprendre un chapitre donné est de retenir cette partie.
On trouve ensuite une partie nommée *Les méthodes à maîtriser*. Elle présente les méthodes en rapport avec le chapitre en cours qu'il faut absolument savoir mettre en pratique. Chaque méthode est illustrée par un exemple corrigé en détail, et comporte un renvoi vers les exercices qui l'utilisent. Il est très utile de refaire par soi-même les exemples de chaque méthode sur une feuille blanche lors des révisions du chapitre.

Si la méthode présentée est facilement programmable sur ordinateur, on trouvera ensuite un programme associé en langage Python.

Pour tester la connaissance du cours et des méthodes, chaque chapitre comporte ensuite une *Interro de cours*. Elle comporte généralement des questions de cours (énoncé d'une définition ou d'un théorème), des vrais/faux et des exemples d'application directe des méthodes. Cette partie permettra d'identifier rapidement les éventuelles lacunes sur le chapitre en cours.
La suite du chapitre est consacrée aux *Exercices*. On les a séparés en deux parties : dans la rubrique *S'entraîner*, on trouve un ensemble d'exercices couvrant tous les points du chapitre. Ce sont les plus faciles, en général, mais certaines méthodes étant plus difficiles à mettre en œuvre que d'autres, ils ne sont pas nécessairement de difficulté égale. La rubrique *Approfondir* contient d'autres exercices pour continuer de s'exercer, a priori un peu plus difficiles. Lorsque cela était possible, on a choisi des exercices proposés récemment à l'oral de concours d'entrée aux grandes écoles.
Enfin, la partie *Corrections* comporte les corrigés détaillés de l'interrogation de cours et des exercices.

La dernière partie de l'ouvrage est consacrée à des sujets d'annales d'écrits récemment posés aux concours d'entrée aux grandes écoles. On a cherché à rassembler une collection de sujets de difficulté moyenne couvrant l'ensemble du programme et illustrant les méthodes présentées dans cet ouvrage. Certaines parties ont été réécrites pour parfaitement correspondre au programme de la filière MP-MPI (lorsqu'il s'agit de sujets d'autres filières ou antérieurs à la réforme des programmes) et les erreurs d'énoncé ont été corrigées ou sont signalées par une note de bas de page.
Chaque sujet est corrigé de manière détaillée, avec des remarques signalant les questions les plus classiques ou les pièges à éviter.

Durant tout l'ouvrage, on a utilisé un certain nombre de pictogrammes :

pour attirer l'attention du lecteur sur un ou plusieurs points spécifiques.

pour signaler un piège ou une erreur à éviter.

pour mettre l’accent sur une bonne manière de rédiger.

Un grand merci tout particulier à Monsieur Jean-Marie Monier pour avoir relu en détail l’intégralité de l’ouvrage et pour ses nombreuses propositions de corrections, améliorations et conseils en tous genres ! Merci également à Caroline Kalla pour ses suggestions dans certains passages d’Algèbre.

Des vidéos pour vous aider à réussir en prépa

Pour réussir vos concours, vous devrez mettre en œuvre des compétences disciplinaires ***(hard skills)***, mais aussi des ***soft skills***, ces compétences transversales qui vous permettront de tenir le bon rythme. La collection ***Parcours Prépas*** vous offre six vidéos pour vous préparer à réussir dès la première année et faire la différence le jour J par la maîtrise de votre énergie (physique, émotionnelle, mentale), par l'entretien de votre motivation et par vos méthodes de travail.

*Tout d'abord deux vidéos méthodologiques d'**Alexis Brès**. Professeur agrégé de physique-chimie en MP2I (lycée Hoche, Versailles), il est aussi correcteur et concepteur de sujets pour la banque du concours e3a-Polytech ; ancien correcteur du concours d'entrée aux ENS. Auteur de L'Oral de physique aux concours des ENS et de Polytechnique (Dunod).*

http://dunod.link/jvy7mqd

Vidéo 1 : Apprendre à apprendre Comment mobiliser efficacement son cours ?

Comment apprendre un cours ? Comment savoir si on l'a vraiment compris ? Comment le mobiliser dans les TD et dans les épreuves ? Comment créer du lien entre les connaissances pour se forger une intuition de la solution et gagner un temps précieux ? Autant de questions-réponses abordées dans cette vidéo. Une méthodologie particulièrement adaptée à l'apprentissage des cours de physique, de mathématiques ou de sciences industrielles.

http://dunod.link/z0psk69

Vidéo 2 : Écrit, oral : aborder sereinement la résolution d'un problème

Si les exigences d'un sujet d'écrit et d'un oral peuvent sembler assez différentes, il existe des techniques communes pour aborder ces épreuves sans stress. Cette vidéo fournit :

- des techniques pour apprivoiser la résolution d'un problème de physique : modalités de décryptage du sujet et de mobilisation du cours ;
- des recommandations sur le fond et la forme pour gagner la confiance des correcteurs ;
- des tactiques cohérentes pour gagner des points ;
- des points de vigilance concernant la préparation des khôlles et des oraux.

*Ensuite quatre vidéos « soft skills » pour aborder la prépa comme le ferait un sportif de haut niveau. Ces vidéos ont été conçues par **Stéphane Fassetta**, fondateur de Syprium, coach professionnel, préparateur mental de sportifs de haut niveau, professeur d'aïkido. Auteur de Nos 8 profils énergétiques (InterÉditions).*

http://dunod.link/80x2gwu

Vidéo 3 : Les cinq piliers de l'énergie, ou comment réussir le marathon de la prépa ?

La prépa, c'est un peu comme le sport de haut niveau : plus le temps passe, plus le niveau ou les contraintes augmentent. Maîtriser son énergie, c'est donc faire un usage optimum de ses ressources pour tenir le rythme des deux années, s'adapter à la diversité des situations et réussir ses épreuves. Cette vidéo présente les dimensions de notre énergie et les cinq piliers pour l'entretenir. La capacité à se ressourcer sur ces cinq piliers est une compétence à développer dès votre arrivée en prépa.

Vidéo 4 : Gérer efficacement son temps en prépa

http://dunod.link/sicy8u3

En prépa, on manque toujours de temps. L'enjeu est donc de gérer efficacement cette ressource pour atteindre les objectifs de vos différentes échéances.

Cette vidéo fournit des repères pour :

- trouver sa propre organisation personnelle : techniques de planification, objectifs SMART... ;
- développer sa capacité d'attention, essentielle à la compréhension, à la mémorisation, à la gestion de la charge mentale et à votre avancement ;
- connaître ses propres biorythmes pour un apprentissage efficient, en capitalisant sur les acquis de la chronobiologie.

Vidéo 5 : Gérer son stress et développer la confiance en soi pour les concours

http://dunod.link/p5maym6

Comme dans le sport de haut niveau, la préparation d'un concours soumet votre énergie à rude épreuve. Si une certaine pression est stimulante pour doper ses performances, l'installation dans un stress chronique compromet à la fois votre santé et vos chances de réussite.

Cette vidéo permet :

- d'identifier les sources externes et internes de son propre stress ;
- de comprendre le rôle du stress comme mécanisme naturel d'adaptation de l'organisme face à une situation déstabilisante et/ou à fort enjeu ;
- d'apprendre à reconnaître certains symptômes physiques, émotionnels ou cognitifs du stress pour prévenir l'épuisement ;
- de connaître les possibilités de régulation physique et mentale du stress ;
- d'entretenir passionnément sa motivation pour préserver durablement la confiance en soi, quelles que soient vos contre-performances.

Vidéo 6 : Techniques respiratoires et de préparation mentale pour préparer les concours

http://dunod.link/vncd3c5

La capacité à se relaxer ou à récupérer quand il le faut est essentielle pour tenir le rythme de préparation d'un concours.

Grâce à cette vidéo :

- vous saurez mettre en œuvre différentes techniques respiratoires adaptées à la récupération et à la dynamisation ;
- vous disposerez de deux techniques de préparation mentale pour conserver un état d'esprit positif, limiter votre niveau de stress et améliorer vos capacités d'attention.

Table des matières

Partie 1 Algèbre

Partie 2 Topologie

Partie 3 Analyse réelle

Partie 4 Probabilités

Partie 1

Algèbre

CHAPITRE 1

Structures algébriques usuelles

L'essentiel du cours

1 Compléments sur les groupes

On ne rappelle ici que les définitions et les propriétés fondamentales du cours de première année. Pour approfondir ces rappels, se reporter au chapitre 7 de l'ouvrage MPSI.

Définition

On appelle **groupe** la donnée d'un ensemble G et d'une loi de composition interne $*$ vérifiant les propriétés suivantes

- $*$ est associative : $\forall (x, y, z) \in G^3$, $x * (y * z) = (x * y) * z$.
- $*$ admet un élément neutre : $\exists\, e \in G$, $\forall x \in G$, $x * e = e * x = x$.
- Tout élément de G admet un inverse pour $*$: $\forall x \in G$, $\exists y \in G$, $x * y = y * x = e$.

Si de plus la loi $*$ est commutative ($\forall (x, y) \in G^2$, $x * y = y * x$), on dit que le groupe $(G, *)$ est **abélien**.

- L'élément neutre de G est alors unique.
- Si $x \in G$, l'inverse de x dans G est unique. On le note x^{-1}.

Produit cartésien de groupes

Si $(G, *)$ et $(H, \times)$ sont deux groupes, on définit une loi de composition interne $\cdot$ sur $G \times H$ en posant

$$\forall ((x, y), (x', y')) \in (G \times H)^2, \quad (x, y).(x', y') = (x * x', y \times y').$$

L'ensemble $G \times H$ muni de la loi . est un groupe. Si de plus G et H sont abéliens, $G \times H$ est également abélien.

- On peut définir de même une loi de composition interne sur un produit de n groupes $G_1 \times \cdots \times G_n$, qui le munit d'une structure de groupe.
- Si $G_1 = \cdots = G_n = G$, on a ainsi muni G^n d'une structure de groupe.

Définition

Soit $(G, *)$ un groupe. On appelle **sous-groupe** de G une partie H de G telle que $(H, *)$ soit un groupe (où l'on note encore $*$ la loi de G restreinte à H^2).

Caractérisations des sous-groupes

Soit $(G, *)$ un groupe. Si H est une partie de G, les assertions suivantes sont équivalentes :
(1) H est un sous groupe de G.
(2) H est non vide, stable par la loi $*$ et par inverse, c'est-à-dire

$$\forall (x, y) \in H^2,\ x * y \in H \qquad \text{et} \qquad \forall x \in H,\ x^{-1} \in H.$$

(3) H est non vide et $\forall (x, y) \in H^2,\ x * y^{-1} \in H$.

⚠ Dans tous les cas, ne pas oublier de montrer que H est non vide (on montre généralement que e, le neutre de G, est dans H) en appliquant cette caractérisation.

Intersection de sous-groupes

Soient $(G, *)$ un groupe et $(H_i)_{i\in I}$ une famille de sous-groupes de G.
Alors l'intersection $\bigcap\limits_{i\in I} H_i$ est un sous-groupe de G.

Sous-groupe engendré

Soient $(G, *)$ un groupe et X une partie de G. Il existe un unique sous-groupe H contenant X tel que pour tout sous-groupe G' de G contenant X, $H \subset G'$.

Définition

On appelle **sous-groupe engendré** par X dans G l'unique sous-groupe décrit dans la proposition précédente.

Dans le cas où $X = \{x\}$, on parle plus simplement du sous-groupe engendré par x.

Sous-groupes de $\mathbb{Z}$

Les sous-groupes de $(\mathbb{Z}, +)$ sont les $a\mathbb{Z} = \{ak\,;\, k \in \mathbb{Z}\}$, avec $a \in \mathbb{N}$.

■ 2 Morphismes de groupes

Cette partie est au programme de première année. Voir le chapitre 7 de l'ouvrage MPSI. Nous rappellerons simplement ici quelques exemples classiques.

- La signature est un morphisme de groupes de $(S_n, \circ)$ dans $(\{\pm 1\}, \times)$.
- Si $\mathbb{K}$ est un sous-corps de $\mathbb{C}$ et E un $\mathbb{K}$-espace vectoriel, le déterminant est un morphisme de $(\mathrm{GL}(E), \circ)$ (ou de $(\mathrm{GL}_n(\mathbb{K}), \times)$) dans $(\mathbb{K}^*, \times)$.
- L'ensemble des automorphismes du groupe G est un groupe pour la loi $\circ$.

■ 3 Groupes monogènes et groupes cycliques

Dans cette partie n désigne un entier $\geqslant 2$.

Définition

- On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence de $\mathbb{Z}$ pour la relation de congruence modulo n.
- Si $x \in \mathbb{Z}$, on note souvent $\overline{x}$ sa classe d'équivalence pour la relation de congruence modulo n (qui est $\{x + kn\,;\, k \in \mathbb{Z}\}$). On dit que x est un **représentant** de $\overline{x}$.
- Si $(x, y) \in \mathbb{Z}^2$, on note $\boldsymbol{\overline{x} + \overline{y}}$ la classe d'équivalence $\overline{x + y}$.

Ceci définit une loi de composition interne $+$ sur $\mathbb{Z}/n\mathbb{Z}$, puisque $\overline{x + y}$ ne dépend pas du choix du représentant x de $\overline{x}$ et du représentant y de $\overline{y}$.

Il convient de ne pas confondre un élément x de $\mathbb{Z}$ avec sa classe $\overline{x}$ modulo n. Par exemple $\overline{x} = \overline{y}$ implique $x \equiv y\ \ [n]$, pas $x = y$.

Proposition

$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien.

Générateurs du groupe $\mathbb{Z}/n\mathbb{Z}$

Soit $x \in \mathbb{Z}$. Le groupe $\mathbb{Z}/n\mathbb{Z}$ est engendré par $\overline{x}$ si et seulement si x est premier avec n.

On dit alors que $\overline{x}$ **engendre** $\mathbb{Z}/n\mathbb{Z}$.

Définition

- On dit qu'un groupe G est **monogène** s'il est engendré par un singleton. Un élément $a \in G$ tel que G soit engendré par a est alors appelé **générateur** de G.
- On dit qu'un groupe G est **cyclique** s'il est monogène et fini.

Le groupe $\mathbb{U}_n$ des racines n-ièmes de l'unité est engendré par $e^{\frac{2i\pi}{n}}$ donc est cyclique.

Proposition

- Tout groupe monogène infini est isomorphe à $(\mathbb{Z}, +)$.
- Tout groupe cyclique de cardinal n est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

Intuitivement, cette proposition signifie qu'il n'existe qu'un (à isomorphisme près) groupe monogène infini, $\mathbb{Z}$ et qu'un groupe cyclique de cardinal n, $\mathbb{Z}/n\mathbb{Z}$.

4 Ordre d'un élément dans un groupe

Définition

• Un élément x d'un groupe G est dit **d'ordre fini** s'il existe $k \in \mathbb{N}^*$ tel que $x^k = e$ (neutre de G).
• On appelle alors **ordre** de x le plus petit entier $k \in \mathbb{N}^*$ tel que $x^k = e$.

Propriétés

- Si $x \in G$ est un élément d'ordre d, le groupe engendré par x dans G est de cardinal d.
- Si $x \in G$ est un élément d'ordre d, pour $n \in \mathbb{Z}$, on a $x^n = e$ si et seulement si $d \mid n$.

Proposition

Si G est un groupe fini, tout élément x de G est d'ordre fini divisant $|G|$.

5 Compléments sur les anneaux

On ne rappelle ici que les définitions et les propriétés fondamentales du cours de première année.
Pour approfondir ces rappels, se reporter au chapitre 7 de l'ouvrage MPSI.

Définition

On appelle **anneau** la donnée d'un ensemble A et de deux lois de composition interne $+$ et $\times$ vérifiant les propriétés suivantes :

- $(A, +)$ est un groupe abélien.
- $\times$ est associative.
- A admet un élément neutre pour la loi $\times$.
- $\times$ est distributive sur $+$ à gauche et à droite :

$$\forall (x, y, z) \in A^3,\ x \times (y + z) = x \times y + x \times z \text{ et } (x + y) \times z = x \times z + y \times z.$$

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

Produit cartésien d'anneaux

Si $(A_1, +, \times)$ et $(A_2, +, \times)$ sont deux anneaux, on définit deux lois de composition interne sur $A_1 \times A_2$ en posant pour tout $((x, y), (x', y')) \in (A \times B)^2$,

$$(x, y) + (x', y') = (x + x', y + y') \qquad \text{et} \qquad (x, y) \times (x', y') = (x \times x', y \times y').$$

L'ensemble $A \times B$ muni de ces deux lois est un anneau.
Si de plus A_1 et A_2 sont commutatifs, $A_1 \times A_2$ est également commutatif.

• On peut définir de même une loi de composition interne sur un produit de n anneaux $A_1 \times \cdots \times A_n$, qui le munit d'une structure d'anneau.
• Si $A_1 = \cdots = A_n = A$, on a ainsi muni A^n d'une structure d'anneau.

Définition

Soit $(A, +, \times)$ un anneau. On dit que B, une partie de A, est un **sous-anneau** de A si
- $1_A \in B$ (1_A étant le neutre de A pour la loi $\times$).
- $\forall (x, y) \in B^2$, $x - y \in B$ et $x \times y \in B$.

Ici, en plus de supposer B non vide, il faut vraiment montrer que $1_A \in B$ (aucun autre point de la définition ne permet de l'obtenir).

Proposition

Muni des lois $+$ et $\times$ induites par celles de A, un sous-anneau de A est un anneau.

Définition

Soient $(A, +, \times)$ et $(B, +, \times)$ deux anneaux. On dit que l'application $f : A \to B$ est un **morphisme d'anneaux** si $f(1_A) = 1_B$ et

$$\forall (x, y) \in A^2, \quad f(x + y) = f(x) + f(y) \quad \text{et} \quad f(x \times y) = f(x) \times f(y).$$

En particulier, un morphisme d'anneaux est un morphisme de groupes (pour la loi $+$). On peut donc définir son image et son noyau et utiliser la caractérisation de l'injectivité vue en MPSI.

Images et images réciproques de structures par un morphisme

Soit $f : A \to B$ un morphisme de l'anneau $(A, +, \times)$ dans l'anneau $(B, +, \times)$.
- Si A_1 est un sous-anneau de A, $f(A_1)$ est un sous-anneau de B.
- Si B_1 est un sous-anneau de B, $f^{-1}(B_1)$ est un sous-anneau de A.

On en déduit que $\mathrm{Im}(f)$ est un sous-anneau de B, mais attention, $\mathrm{Ker}(f)$ n'est pas en général un sous-anneau de A (il ne contient pas 1_A).

Définition

On dit que $f : A \to B$ est un **isomorphisme d'anneaux** si c'est un morphisme d'anneaux bijectif.

Opérations sur les morphismes d'anneaux

Soient $(A, +, \times)$, $(B, +, \times)$ et $(C, +, \times)$ trois anneaux.
- Si $f : A \to B$ et $g : B \to C$ sont des morphismes d'anneaux, $g \circ f$ est un morphisme d'anneaux.
- Si $f : A \to B$ est un isomorphisme d'anneaux, f^{-1} est un isomorphisme d'anneaux.

Définition

Soit $(A, +, \times)$ un anneau commutatif. On dit qu'une partie I de A est un **idéal** de A si
- I est un sous-groupe de $(A, +)$.
- I est absorbant pour $\times$: $\forall (x, y) \in A \times I,\ x \times y \in I$.

Exemples d'idéaux

- Si $f : (A, +, \times) \to (B, +, \times)$ est un morphisme d'anneaux, $\mathrm{Ker}(f)$ est un idéal de A.
- Les idéaux de $\mathbb{Z}$ sont les $a\mathbb{Z} = \{an\,;\, n \in \mathbb{Z}\}$, $a \in \mathbb{N}$.
- Si A est un anneau et si $a \in A$, l'ensemble $aA = \{ab\,;\, b \in A\}$ est un idéal de A.

Définition

On dit qu'un anneau $(A, +, \times)$ est **intègre** si

$$\forall (a, b) \in A^2,\ a \times b = 0 \Rightarrow (a = 0 \text{ ou } b = 0).$$

Proposition

Si $(A, +, \times)$ est un anneau intègre, et si $(a, b, c) \in A^3$ vérifie $a \times b = a \times c$ avec $a \neq 0$, alors $b = c$.

⚠ On ne peut pas simplifier par a si $a \neq 0$ lorsque A n'est pas intègre (comme dans $\mathscr{M}_n(\mathbb{K})$ par exemple).

Définition

Si $(A, +, \times)$ est un anneau commutatif intègre, on dit que a **divise** b et on note $a|b$ s'il existe $c \in A$ tel que $b = ac$.

Proposition

Pour des éléments a et b de l'anneau A, a divise b si et seulement si $bA \subset aA$.

Définition

Soit $(A, +, \times)$ un anneau commutatif intègre. Pour tout $a \in A$, l'ensemble $aA = \{ax\,;\ x \in A\}$ est un idéal de A, noté (a) et appelé idéal principal **engendré** par a. Lorsque dans un anneau A, tous les idéaux sont principaux (engendrés par un seul élément), on dit que A est un **anneau principal** . Si a et b sont deux éléments de A, l'idéal engendré par a, b est noté (a, b).

PGCD

On note A^* l'ensemble des éléments de A différents de e. Soit A un anneau principal (donc intègre). Pour toute famille $(a_1, a_2, \ldots, a_n)$ d'éléments de A^*, il existe un élément δ de A^* tel que l'idéal engendré par les a_i soit égal à celui engendré par δ : $(a_1, a_2, \cdots, a_n) = (\delta)$. On a donc :

$$\delta = \sum_{k=1}^{n} u_k a_k$$

où les u_i sont des éléments de A et δ un pgcd de $a_1, a_2, \ldots, a_n$. On retrouve ici la relation de Bezout (vue en première année dans $\mathbb{Z}$ et ci-dessous dans $\mathbb{K}[X]$).

• Pour assurer une unicité du PGCD, on peut choisir dans $\mathbb{Z}$ un générateur positif, et dans $\mathbb{K}[X]$, un générateur unitaire.
• La notion d'anneau principal n'est pas explicitement au programme, mais elle permet d'utiliser un langage plus structurant et quitte à redéfinir le terme, cela ne pose pas de problème.
• Tous les idéaux de $\mathbb{Z}$ et de $\mathbb{K}[X]$ sont des idéaux principaux (déjà vu pour $\mathbb{Z}$ et cf ci-dessous pour $\mathbb{K}[X]$), assurant ainsi que $\mathbb{Z}$ et $\mathbb{K}[X]$ sont des anneaux principaux.

Définition

Un **corps** est la donnée d'un ensemble $\mathbb{K}$ et deux lois de composition interne $+$ et $\times$ telles que
- $(\mathbb{K}, +, \times)$ est un anneau commutatif.
- Tout élément non nul de $\mathbb{K}$ est inversible pour la loi $\times$.

Un corps est anneau intègre.

Définition

Soit $(\mathbb{K}, +, \times)$ un corps. On dit que $\mathbb{L}$, une partie de $\mathbb{K}$, est un **sous-corps** de $\mathbb{K}$ si
- $\mathbb{L}$ contient un élément non nul.
- $\forall (x, y) \in \mathbb{K}^2$, $x - y \in \mathbb{K}$, $x \times y \in \mathbb{K}$ et $x^{-1} \in \mathbb{K}$.

• Pour montrer que $\mathbb{L}$ contient un élément non nul, on vérifie généralement que $1_{\mathbb{K}} \in \mathbb{L}$.
• Toutes les notions étudiées l'année dernière en algèbre linéaire avec $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ peuvent être étendues au cas où $\mathbb{K}$ est un sous-corps de $\mathbb{C}$.

6 L'anneau $\mathbb{Z}/n\mathbb{Z}$

Dans cette partie n désigne un entier $\geqslant 2$.

Définition

Si $(x, y) \in \mathbb{Z}^2$, on note $\overline{\boldsymbol{x}} \times \overline{\boldsymbol{y}}$ la classe d'équivalence $\overline{x \times y}$ modulo n.

Ceci définit une loi de composition interne $\times$ sur $\mathbb{Z}/n\mathbb{Z}$, puisque $\overline{x \times y}$ ne dépend pas du choix du représentant x de $\overline{x}$ et du représentant y de $\overline{y}$.

Proposition

- L'ensemble $\mathbb{Z}/n\mathbb{Z}$ muni des lois $+$ et $\times$ est un anneau commutatif.
- $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps si et seulement si n est premier. On le note alors $\mathbb{F}_n$.

$\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre en général (il est intègre si et seulement si n est premier).

Proposition

Un élément $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si x est premier avec n.

Définition

On appelle **fonction indicatrice d'Euler** la fonction φ qui à $n \geqslant 2$ associe le cardinal de l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Théorème chinois

Soient m et n deux entiers premiers entre eux. L'application

$$f : \mathbb{Z}/(mn)\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \quad \overline{x}^{mn} \mapsto (\overline{x}^{m}, \overline{x}^{n})$$

est un isomorphisme d'anneaux (où $\overline{x}^{p}$ désigne la classe de x modulo p).

En particulier f induit un isomorphisme de groupes entre $(\mathbb{Z}/(mn)\mathbb{Z})^*$ et $(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$, ce qui montre que $\varphi(mn) = \varphi(m)\varphi(n)$.

Théorème chinois étendu

Soient $n_1 n_2 \dots n_k$ des entiers premiers entre eux et n le PPCM (et produit) des $(n_i)_{1 \leqslant i \leqslant n}$. L'application

$$\Phi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}, \quad \overline{x}^{n} \mapsto (\overline{x}^{n_1}, \overline{x}^{n_2} \dots, \overline{x}^{n_k})$$

est un isomorphisme d'anneaux (où $\overline{x}^{p}$ désigne la classe de x modulo p).

Corollaires

Soit $n \geqslant 2$, et $n = p_1^{n_1} \times \cdots \times p_k^{n_k}$ la décomposition en facteurs premiers de n. Alors

$$\varphi(n) = \prod_{i=1}^{k}(p_i^{n_i} - p_i^{n_i-1}) = n\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^{k}(p_i - 1)\,p_i^{n_i-1}.$$

Théorème d'Euler

Si $a \in \mathbb{Z}$ est premier avec n, on a $a^{\varphi(n)} \equiv 1 \ [n]$.

Ce théorème constitue une généralisation du théorème de Fermat vu en première année, puisque $\varphi(p) = p - 1$ si p est premier.

7 Anneaux de polynômes

Le cours de première année sur les anneaux (chapitre 7 de l'ouvrage MPSI) se généralise sans peine au cas où $\mathbb{K}$ est un sous-corps de $\mathbb{C}$.

Proposition

- $\mathbb{K}[X]$ est un anneau intègre.
- Les idéaux de $\mathbb{K}[X]$ sont les $P\mathbb{K}[X] = \{PQ\,;\, Q \in \mathbb{K}[X]\}$, avec $P \in \mathbb{K}[X]$. (Tous les idéaux sont principaux dans $\mathbb{K}[X]$)

Définition

- Si P et $Q \in \mathbb{K}[X]$ sont non tous deux nuls on dit que R est le **PGCD** de P et Q si R est unitaire, et si c'est un diviseur commun à P et Q de degré maximal. On le note $P \wedge Q$.
- On appelle **PGCD** de $P_1, \ldots, P_n$ le polynôme R unitaire qui est un diviseur commun à $P_1, \ldots, P_n$ de degré maximal.

Contrairement au cas des entiers, deux polynômes admettent a priori une infinité de PGCD : si R en est un, tous les λR, $\lambda \in \mathbb{K}^*$ en sont. On choisit de ne garder que le PGCD unitaire.

Relation de Bézout

- Soit $(P, Q) \in \mathbb{K}[X]^2 \backslash \{(0, 0)\}$. $\exists (U, V) \in \mathbb{K}[X]^2$, $PU + QV = P \wedge Q$.
- Si D est le PGCD de $P_1, \ldots, P_n$, il existe $(U_1, \ldots, U_n) \in \mathbb{K}[X]^n$ tel que

$$P_1U_1 + \cdots + P_nU_n = D.$$

Théorème de Bezout

Soit $(A, B) \in \mathbb{K}[X]^2$, alors A et B sont premiers entre eux si et seulement si

$$\exists (U, V) \in \mathbb{K}[X]^2,\ AU + BV = 1.$$

Théorème de Gauss

Soit $(A, B, C) \in \mathbb{K}[X]^3$. Si $A|BC$ et si A est premier avec B, alors $A|C$.

Définition

On dit que $P \in \mathbb{K}[X]$ est **irréductible** si P est non constant et si tout diviseur Q de P est constant ou associé à P ($P|Q$ ou $Q|p$, voir chapitre 9 du MPSI).

- Comme vu en première année, les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.
- Comme vu en première année, les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 de discriminant < 0.

La notion d'irréductibilité dépend du corps $\mathbb{K}$ choisi. Si l'on change $\mathbb{K}$, l'ensemble des polynômes irréductibles change aussi.

Décomposition en facteurs irréductibles

Soit $P \in \mathbb{K}[X]$ non nul. Il existe une unique (à l'ordre des facteurs près) décomposition de P sous la forme $P = \lambda \prod_{k=1}^{r} P_k^{\alpha_k}$, où $\lambda \in \mathbb{K}^*$ est le coefficient dominant de P, et où $P_1, \ldots, P_r$ sont des polynômes irréductibles unitaires deux à deux distincts de $\mathbb{K}[X]$, $\alpha_1, \ldots, \alpha_r$ des entiers naturels non nuls.

Il s'agit de la généralisation de la factorisation dans $\mathbb{C}[X]$ ou dans $\mathbb{R}[X]$ d'un polynôme.

■ 8 Algèbres

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

Définition

Soit A un ensemble muni de deux lois de composition interne + et $\times$, et d'une loi de composition externe $\cdot$ de $\mathbb{K} \times A$ dans A. On dit que $(A, +, \times, .)$ est une $\mathbb{K}$-**algèbre** si

- $(A, +, \times)$ est un anneau.
- $(A, +, .)$ est un $\mathbb{K}$-espace vectoriel.
- $\forall(\lambda, x, y) \in \mathbb{K} \times A^2$, $\lambda.(x \times y) = (\lambda.x) \times y = x \times (\lambda.y)$.

La troisième propriété est appelée propriété d'entrelacement. Elle permet de s'assurer de la compatibilité de . et $\times$.

Exemples d'algèbres

$\mathbb{K}[X]$, $\mathscr{L}(E)$ (où E est un $\mathbb{K}$-espace vectoriel), $\mathscr{M}_n(\mathbb{K})$ et $\mathscr{F}(X, \mathbb{K})$ (où X est un ensemble quelconque) munies de leurs opérations usuelles sont des $\mathbb{K}$-algèbres.

Définition

Soit A une $\mathbb{K}$-algèbre. On dit que B, une partie de A, est une **sous-algèbre** de A si c'est un sous-espace vectoriel de A et un sous-anneau de A.

Le fait de montrer que B est un sous-espace vectoriel de A montre que pour $(x, y) \in B^2$, $x - y \in B$. Il n'y a donc que la stabilité par produit et le fait que $1_A \in B$ à montrer dans B sous-anneau de A.

Proposition

Muni des lois induites par celles de A, une sous-algèbre de A est une $\mathbb{K}$-algèbre.

Définition

Soient $(A, +, \times, .)$ et $(B, +, \times, .)$ deux $\mathbb{K}$-algèbres. On dit que $f : A \to B$ est un **morphisme de $\mathbb{K}$-algèbres** si f est un morphisme d'anneaux linéaire.

Le fait de montrer que f est linéaire montre que pour $(x, y) \in A^2$, $f(x+y) = f(x)+f(y)$. Il n'y a donc que la compatibilité avec le produit et le fait que $f(1_A) = 1_B$ à montrer dans f morphisme d'anneaux.

Les méthodes à maîtriser

Méthode 1.1 : Savoir montrer qu'un ensemble muni d'une loi est un groupe

Lorsqu'on doit montrer que $(G, *)$ est un groupe, on commence par regarder si la loi $*$ est la même que celle d'un exemple usuel $(H, *)$ avec $G \subset H$. Dans ce cas, on montre que G est un sous-groupe de H.

Exemple d'application

Soit $n \in \mathbb{Z}$. Montrer que $n\mathbb{Z}$, l'ensemble des multiples de n, est un groupe pour la loi $+$.

Comme $(\mathbb{Z}, +)$ est un groupe usuel, et comme $n\mathbb{Z} \subset \mathbb{Z}$, on montre que $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.
$0 = 0 \times n$ est un multiple de n, donc $0 \in n\mathbb{Z}$ et donc $n\mathbb{Z} \neq \varnothing$.
Soit $(x, y) \in (n\mathbb{Z})^2$, alors on a $(k, l) \in \mathbb{Z}^2$ tel que $x = nk$ et $y = nl$, puis $x - y = nk - nl = n(k - l)$ est un multiple de n. Ainsi $x - y \in n\mathbb{Z}$.
En conclusion, $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$, donc un groupe pour la loi $+$.

- Lorsque ce n'est pas évident, il faut bien vérifier que $G \subset H$.
- Exceptionnellement, on peut être amené à vérifier les trois points de la définition d'un groupe.

Voir exercices **1.1** et **1.2**.

Méthode 1.2 : Savoir montrer qu'un ensemble muni de deux lois est un anneau ou un corps

Lorsqu'on doit montrer que $(A, +, \times)$ est un anneau (ou un corps), on commence par regarder si les lois $+$ et $\times$ sont les mêmes que celles d'un exemple usuel $(B, +, \times)$ avec $A \subset B$. Dans ce cas, on montre que A est un sous-anneau (ou un sous-corps) de B.
Sinon, on vérifie les points de la définition d'un anneau (ou d'un corps).

Exemple d'application

Montrer que $A = \{x + y\sqrt{2}\,;\,(x, y) \in \mathbb{Q}^2\}$ est un corps (pour les lois $+$ et $\times$ usuelles).

Comme $A \subset \mathbb{R}$, il suffit de montrer que A est un sous-corps de $\mathbb{R}$.
On a d'abord $1 = 1 + 0 \times \sqrt{2} \in A$, puis soit $(x, y) \in A^2$, alors on a $(p, q, r, s) \in \mathbb{Q}^4$ tels que $x = p + q\sqrt{2}$ et $y = r + s\sqrt{2}$. Par suite $x - y = (p - r) + (q - s)\sqrt{2} \in A$ (puisque $p - r$ et $q - s \in \mathbb{Q}$) et

$$x \times y = pr + qr\sqrt{2} + ps\sqrt{2} + 2qs = (pr + 2qs) + (qr + ps)\sqrt{2} \in A$$

puisque $pr + 2qs$ et $qr + ps \in \mathbb{Q}$.
Enfin, si $x \neq 0$, on a $p - q\sqrt{2} \neq 0$ (car $\sqrt{2}$ est irrationnel) donc

$$x^{-1} = \frac{p - q\sqrt{2}}{x(p - q\sqrt{2})} = \frac{p - q\sqrt{2}}{p^2 - 2q^2} = \frac{p}{p^2 - 2q^2} - \frac{q}{p^2 - 2q^2}\sqrt{2} \in A.$$

Ainsi A est un sous-corps de $\mathbb{R}$, donc est un corps.

Plus rarement, on peut être amené à vérifier les points de la définition d'un anneau (ou d'un corps).Voir la Méthode 7.3 de l'ouvrage MPSI.

Voir exercices **1.5** et **1.14**.

Méthode 1.3 : Savoir montrer qu'une application est un morphisme

Pour montrer qu'une application $f : G \to H$ entre deux groupes (resp. anneaux) est un morphisme, on se contente de vérifier la définition. Dans la définition d'un morphisme d'anneaux, attention à ne pas oublier la condition $f(1_A) = 1_B$.

Exemple d'application

Soient $n \in \mathbb{N}^*$ et $P \in \mathrm{GL}_n(\mathbb{R})$. Montrer que $f : \mathscr{M}_n(\mathbb{R}) \to \mathscr{M}_n(\mathbb{R})$, $M \mapsto P^{-1}MP$ est un morphisme d'anneaux.

Observons tout d'abord que $f(I_n) = P^{-1}I_nP = P^{-1}P = I_n$ et ensuite que si $(M, N) \in \mathscr{M}_n(\mathbb{R})^2$, on a :

$$f(M+N) = P^{-1}(M+N)P = P^{-1}MP + P^{-1}NP = f(M) + f(N)$$

$$\text{et} \qquad f(MN) = P^{-1}MNP = P^{-1}MPP^{-1}NP = f(M)f(N)$$

donc f est un morphisme d'anneaux.

Voir exercices **1.1**,**1.2** et **1.4**.

Méthode 1.4 : Savoir déterminer l'ordre d'un élément dans un groupe

Dans un groupe $(G, \times)$, un élément x est d'ordre fini s'il existe $n \in \mathbb{N}^*$ tel que $x^n = e$ (le neutre de G). On détermine ensuite l'ordre de x en trouvant le plus petit entier n vérifiant cette propriété.

Exemple d'application

Déterminer l'ordre de $\overline{x}$ dans $(\mathbb{Z}/n\mathbb{Z}, +)$ (avec $n \geqslant 2$).

Soit $x \in \mathbb{Z}$. Pour $d \in \mathbb{N}$, la puissance d-ième de $\overline{x}$ pour la loi $+$ est $d\overline{x} = \overline{dx}$. On a $\overline{dx} = \overline{0}$ (le neutre de $\mathbb{Z}/n\mathbb{Z}$ pour $+$) si et seulement si $dx \equiv 0 \ [n]$ i.e. $n|dx$. Ainsi $n\overline{x} = \overline{0}$ et $\overline{x}$ est d'ordre fini.
On cherche ensuite le plus entier $d \in \mathbb{N}^*$ tel que $n|dx$. Notons $l = n \wedge x$, alors $x = lm$, avec $m \in \mathbb{Z}$ premier avec n. Ainsi $n|dx = dlm$ si et seulement si n divise dl (par le théorème de Gauss), ce qui équivaut à $\dfrac{n}{l}$ divise d. Le plus petit entier d non nul vérifiant cela est $d = \dfrac{n}{l}$. Ainsi $\overline{x}$ est d'ordre $\dfrac{n}{l} = \dfrac{n}{n \wedge x}$.

⚠ Vérifier que $x^d = e$ ne suffit pas pour montrer que x est un élément d'ordre d. Il faut vérifier que d est le plus petit entier non nul vérifiant cette propriété.

Voir exercices **1.3** et **1.11**.

Méthode 1.5 : Savoir résoudre un système de congruences

Lorsqu'on a à résoudre un système de la forme $\begin{cases} x \equiv a \ [m] \\ x \equiv b \ [n] \end{cases}$ avec $(a, b) \in \mathbb{Z}^2$, m et n deux entiers premiers entre eux, on sait d'après le théorème chinois qu'il existe au moins une solution $x \in \mathbb{Z}$, unique modulo mn.
Si l'on trouve une solution particulière x_0, les solutions sont donc les $x_0 + kmn$, $k \in \mathbb{Z}$. Pour trouver une solution particulière x_0, on part d'une relation de Bezout $mu + nv = 1$ (avec $(u, v) \in \mathbb{Z}$). On a alors $c = mu$ qui vérifie $c \equiv 0 \ [m]$ et $c \equiv 1 \ [n]$, pendant que $d = nv$ vérifie $d \equiv 1 \ [m]$ et $d \equiv 0 \ [n]$. Ainsi $x_0 = ad + bc$ est une solution particulière.

Exemple d'application

Résoudre le système $\begin{cases} \boldsymbol{x \equiv 2 \ [5]} \\ \boldsymbol{x \equiv 3 \ [7]} \end{cases}$

Comme 5 et 7 sont premiers entre eux, le système admet au moins une solution $x \in \mathbb{Z}$, unique modulo 35, par le théorème chinois.
$3 \times 5 - 2 \times 7 = 1$ est une relation de Bezout évidente entre 5 et 7 (si on ne la voit pas, on applique l'algorithme d'Euclide étendu pour la trouver) donc $c = 15$ vérifie $c \equiv 1 \ [7]$ et $c \equiv 0 \ [5]$, $d = -14$ vérifie $d \equiv 0 \ [7]$ et $d \equiv 1 \ [5]$. Par suite $x_0 = 2d + 3c = -28 + 45 = 17$ est solution du système.
Les solutions du système sont les $17 + 35k$, $k \in \mathbb{Z}$.

➔ Voir exercice **1.8**.

Méthode 1.6 : Savoir calculer un PGCD de deux polynômes

Pour calculer un PGCD de deux polynômes non tous deux nuls A et B, on utilise l'algorithme d'Euclide.

1. Si A (resp. B) est nul, un PGCD de A et B est égal à B (resp. A). Sinon, on pose $A_0 = A$ et $A_1 = B$, ou l'inverse, de sorte que $\deg(A_0) \geqslant \deg(A_1)$.
2. Tant que A_{n+1} est non nul, on pose A_{n+2} le reste dans la division euclidienne de A_n par A_{n+1}.
3. Le PGCD de A et B est le dernier reste non nul.

Ainsi on pose A_2 le reste dans la division euclidienne de A_0 par A_1, puis A_3 le reste dans la division euclidienne de A_1 par A_2, et ainsi de suite jusqu'à obtenir un reste nul.
À chaque étape, on peut choisir de poser un polynôme associé au reste (et pas le reste lui-même) si cela simplifie les calculs.

Exemple d'application

Calculer un PGCD de $\boldsymbol{A = X^5 + 2X^4 + 2X^3 - 2X^2 + X + 4}$ et $\boldsymbol{B = X^3 - X^2 + 2}$.

On pose $A_0 = A$ et $A_1 = B$. La division euclidienne de A_0 par A_1 est

$$A_0 = A_1(X^2 + 3X + 5) + (X^2 - 5X - 6).$$

On pose donc $A_2 = X^2 - 5X - 6$. La division euclidienne de A_1 par A_2 est

$$A_1 = A_2(X + 4) + 26X + 26.$$

On pose donc $A_3 = X + 1$ (associé au reste, mais unitaire). La division euclidienne de A_2 par A_3 est $A_2 = (X - 6)A_3 + 0$.
Le PGCD de A et B est donc $A_3 = X + 1$, unitaire et associé au dernier reste non nul.

Lors du calcul du PGCD par l'algorithme d'Euclide, on peut à toute étape changer le reste obtenu en un polynôme associé si cela simplifie les calculs.

Voir exercice **1.9**.

Pour faire des calculs sur les polynômes avec Python, on utilise le sous-module `Polynomial` du module `numpy.polynomial`. On construit alors un objet de type `Polynomial` en donnant la liste des coefficients (du plus petit degré au plus haut) en argument de la commande `Polynomial`. Si `A` est un tel objet, `A.coef` donne la liste des coefficients de `A`, `A.degree()` son degré. Le produit ou la somme de deux polynômes se fait avec les commandes + et ∗. Les commandes // et `%` donnent le quotient et le reste dans la division euclidienne. Le programme Python suivant calcule le pgcd des polynômes A et B en suivant l'algorithme d'Euclide.

```python
from numpy.polynomial import Polynomial
def pgcd(A,B):
    if A.degree() < B.degree():
        (A,B) = (B,A)
    while B != Polynomial([0]):
        (A,B) = (B,A % B)
    if A != Polynomial([0]):
        A = A / A.coef[A.degree()]
    return A
```

Méthode 1.7 : Savoir calculer une relation de Bezout entre polynômes

Pour trouver une relation de Bezout entre deux polynômes A et B, on applique l'algorithme d'Euclide étendu : on applique l'algorithme d'Euclide à A et B, auquel on ajoute les étapes suivantes

1. Lorsqu'on pose $A_0 = A$ et $A_1 = B$ (ou $A_0 = B$ et $A_1 = A$), on ajoute $U_0 = 1$, $U_1 = 0$, et $V_0 = 0$, $V_1 = 1$ (ou $U_0 = 0$, $U_1 = 1$ et $V_0 = 1$, $V_1 = 0$) de sorte que $AU_0 + BV_0 = A_0$ et $AU_1 + BV_1 = A_1$.

2. À l'étape $n+1$, on effectue la division euclidienne de A_n par A_{n+1} et on note A_{n+2} le reste. On a donc $Q_n \in K[X]$ tel que $A_n = Q_nA_{n+1} + A_{n+2}$. On a construit U_n,U_{n+1} et V_n, V_{n+1} de sorte que $AU_n + BV_n = A_n$ et $AU_{n+1} + BV_{n+1} = A_{n+1}$, donc on a

$$\begin{aligned} A_{n+2} &= A_n - Q_nA_{n+1} = AU_n + BV_n - Q_n(AU_{n+1} + BV_{n+1}) \\ &= A(U_n - Q_nU_{n+1}) + B(V_n - Q_nV_{n+1}) \end{aligned}$$

et on pose $U_{n+2} = U_n - Q_nU_{n+1}$ et $V_{n+2} = V_n - Q_nV_{n+1}$.

3. À la fin de l'algorithme d'Euclide, lorsqu'on obtient A_k le PGCD, on a construit U_k et V_k tels que $AU_k + BV_k = A_k$, donc on a une relation de Bezout.

Exemple d'application

Donner une relation de Bezout entre $A = X^5 + 2X^4 + 2X^3 - 2X^2 + X + 4$ et $B = X^3 - X^2 + 2$.

On pose $A_0 = A$ et $A_1 = B$, $U_0 = 1$, $U_1 = 0$, $V_0 = 0$ et $V_1 = 1$ (de sorte que $AU_0 + BV_0 = A_0$ et $AU_1 + BV_1 = A_1$). La division euclidienne de A_0 par A_1 est

$$A_0 = A_1(X^2 + 3X + 5) + (X^2 - 5X - 6).$$

On pose donc $A_2 = X^2 - 5X - 6$. On a alors

$$\begin{aligned} A_2 &= A_0 - A_1(X^2 + 3X + 5) = AU_0 + BV_0 - (AU_1 + BV_1)(X^2 + 3X + 5) \\ &= A(U_0 - (X^2 + 3X + 5)U_1) + B(V_0 - (X^2 + 3X + 5)V_1). \end{aligned}$$

On pose donc $U_2 = U_0 - (X^2 + 3X + 5)U_1 = 1$ et $V_2 = V_0 - (X^2 + 3X + 5)V_1 = -X^2 - 3X - 5$.
La division euclidienne de A_1 par A_2 est $A_1 = A_2(X + 4) + 26X + 26$. On pose donc $A_3 = 26X + 26$ et on a

$$A_3 = A_1 - A_2(X + 4) = AU_1 + BV_1 - (AU_2 + BV_2)(X + 4) = A(U_1 - (X + 4)U_2) + B(V_1 - (X + 4)V_2).$$

On pose donc $U_3 = U_1 - (X + 4)U_2 = -X - 4$ et

$$V_3 = V_1 - (X + 4)V_2 = 1 - (-X^2 - 3X - 5)(X + 4) = X^3 + 7X^2 + 17X + 21.$$

La division euclidienne de A_2 par A_3 est $A_2 = \dfrac{1}{26}(X - 6)A_3 + 0$.

Le PGCD de A et B est donc $\dfrac{1}{26}A_3 = X + 1$, et une relation de Bezout est

$$\frac{1}{26}(-X - 4)A + \frac{1}{26}(X^3 + 7X^2 + 17X + 21)B = X + 1.$$

Voir exercice **1.9**.

Toujours avec le module *numpy*, le programme suivant calcule une relation de Bezout entre A et B.

```
from numpy.polynomial import Polynomial
def bezout(A,B):
    if A.degree() < B.degree():
        (A,B) = (B,A)
    U0 = Polynomial([1])
     U1 = Polynomial([0])
     V0 = Polynomial([0])
     V1 = Polynomial([1])
     while B != Polynomial([0]):
         Q = A // B
         (U0,U1) = (U1, U0 - U1 * Q)
         (V0,V1) = (V1, V0 - V1 * Q)
         (A,B) = (B,A\% B)
     if A != Polynomial([0]):
         coeffdom = A.coef[A.degree()]
         U0 = U0 / coeffdom
         V0 = V0 / coeffdom
     return (U0,V0)
```

Interro de cours

1. Rappeler la définition d'un groupe.
2. Montrer que A, l'ensemble des automorphismes d'un groupe G (i.e. des isomorphismes de groupe de G dans G), muni de la loi $\circ$, est un groupe.
3. Montrer que l'ensemble des nombres dyadiques $H = \{n2^{-p} ; (n, p) \in \mathbb{Z} \times \mathbb{N}\}$ muni des lois usuelles est un anneau. Est-ce un corps ?
4. Justifier si les applications suivantes sont des morphismes de groupe ou d'anneaux pour les lois usuelles.
   (a) $f : \mathbb{C} \to \mathbb{R}$, $x \mapsto |x|$.
   (b) $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $x \mapsto \overline{x}$.
   (c) $f : \mathbb{R} \mapsto \mathscr{M}_2(\mathbb{R})$, $x \mapsto \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}$.
   (d) $f : \mathbb{R}^2 \mapsto \mathscr{M}_2(\mathbb{R})$, $(x, y) \mapsto \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$.
5. Soient $\mathbb{K}$ et $\mathbb{L}$ deux corps, $f : \mathbb{K} \to \mathbb{L}$ un morphisme d'anneaux. Montrer que f est injectif.
6. Donner l'ordre de $z = e^{\frac{2ik\pi}{n}}$ dans le groupe $(\mathbb{C}^*, \times)$ (avec $k \in \mathbb{Z}$, $n \in \mathbb{N}^*$).
7. Déterminer (et justifier) si les énoncés suivants sont vrais ou faux :
   (a) Tout élément de $\mathbb{Z}/n\mathbb{Z}$ est d'ordre fini divisant n pour la loi $+$.
   (b) Tout élément inversible de $\mathbb{Z}/n\mathbb{Z}$ est d'ordre fini divisant n pour la loi $\times$.
   (c) L'anneau $\mathbb{Z}/n\mathbb{Z}$ est commutatif.
   (d) L'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre.
8. Résoudre le système $\begin{cases} x \equiv 2 \ [3] \\ x \equiv 4 \ [5] \end{cases}$.
9. Rappeler la définition de $\varphi(n)$ pour $n \in \mathbb{N}^*$, et donner son expression en fonction de n.
10. Donner le PGCD et une relation de Bezout entre $A = X^3 + X^2 + X - 3$ et $B = X^2 - 3X + 2$.
11. Déterminer (et justifier) si les énoncés suivants sont vrais ou faux :
    (a) Si $(P, Q) \in \mathbb{K}[X]^2 \backslash \{(0, 0)\}$, on a un unique $(U, V) \in \mathbb{K}[X]^2$ tel que $PU + QV = P \wedge Q$.
    (b) Si P et Q sont premiers entre eux et divisent R, $PQ|R$.
    (c) Un polynôme irréductible de degré $\geqslant 2$ dans $\mathbb{K}[X]$ n'admet pas de racine dans $\mathbb{K}$.
    (d) Un polynôme n'admettant pas de racine dans $\mathbb{K}$ est irréductible dans $\mathbb{K}[X]$.
12. Donner la définition et quatre exemples de $\mathbb{K}$-algèbres.

Exercices

■ S'entraîner

Exercice 1.1

Soit G un groupe, pour $a \in G$, on note $f_a : G \to G$, $x \mapsto axa^{-1}$.

1. Montrer que f_a est un isomorphisme de G dans G.
2. Montrer que $\mathrm{Int}(G) = \{f_a\,;\, a \in G\}$, muni de la composition, est un groupe.
3. Montrer que $\varphi : G \to \mathrm{Int}(G)$, $a \mapsto f_a$ est un morphisme de groupes. Quel est son noyau ?

Exercice 1.2

Soit $a \in \mathbb{R}_+^*$. Pour $h \in \mathbb{R}$, on pose $A(h) = \begin{pmatrix} a^h & 0 & 0 \\ 0 & 1 & h \\ 0 & 0 & 1 \end{pmatrix}$ et on note $E = \{A(h)\,;\, h \in \mathbb{R}\}$.

1. Montrer que E est un groupe pour le produit matriciel.
2. Montrer que E est isomorphe à $(\mathbb{R}, +)$

Exercice 1.3

On se donne $n \in \mathbb{N}^*$ et on rappelle que $\mathbb{U}_n$ est l'ensemble des racines n-ièmes de l'unité.

1. Écrire un programme Python prenant en entrée un entier n et renvoyant $\varphi(n)$.
2. Écrire un programme Python prenant en entrée un entier n et renvoyant $\sum\limits_{d|n} \varphi(d)$.
3. Pour $k \in \mathbb{Z}$, déterminer l'ordre de $z = \mathrm{e}^{\frac{2ik\pi}{n}}$ dans $\mathbb{U}_n$.
4. Si $d|n$, combien $\mathbb{U}_n$ a-t-il d'éléments d'ordre d ?
5. En déduire que $\sum\limits_{d|n} \varphi(d) = n$.

Exercice 1.4

Soient G un groupe cyclique engendré par a, d'ordre n, G' un groupe et $a' \in G'$.

1. Montrer qu'il existe un morphisme $f : G \to G'$ tel que $f(a) = a'$ si et seulement si a' est d'ordre fini divisant n. Justifier que ce morphisme est alors unique.
2. Déterminer tous les morphismes de groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$ dans $(\mathbb{Z}, +)$, $(\mathbb{C}^*, \times)$ et $(\mathbb{Z}/m\mathbb{Z}, +)$ ($m \in \mathbb{N}^*$).

Exercice 1.5

Pour $d \in \mathbb{N}$, on note $A_d = \{(x, y) \in \mathbb{Z}^2\,;\, d|(y - x)\}$.

1. Montrer que pour $d \in \mathbb{N}$, A_d est un sous-anneau de $\mathbb{Z}^2$.
2. Réciproquement si A est un sous-anneau de $\mathbb{Z}^2$, montrer que $H = \{x \in \mathbb{Z}\,;\, (x, 0) \in A\}$ est un sous-groupe de $\mathbb{Z}$, et en déduire qu'il existe $d \in \mathbb{N}$ tel que $A = A_d$.

Exercice 1.6

Soit $(A, +, \times)$ un anneau commutatif. On dit qu'un idéal de A est premier si pour tout $(x, y) \in A^2$ vérifiant $xy \in I$, on a $x \in I$ ou $y \in I$.

1. Quels sont les idéaux premiers de $\mathbb{Z}$?
2. Quels sont les idéaux premiers de $\mathbb{K}[X]$?
3. Soient J et K deux idéaux de A, I un idéal premier tel que $J \cap K = I$. Montrer que $J = I$ ou $K = I$.
4. On suppose que tout idéal de A est premier. Montrer que A est intègre puis montrer que A est un corps (on pourra considérer a^2A, avec $a \in A\backslash\{0\}$, pour montrer ce dernier point).

Exercice 1.7

Soit p un nombre premier impair.

1. Déterminer le nombre de carrés dans $\mathbb{Z}/p\mathbb{Z}$.
2. Montrer que $(p-1)! \equiv -1 \ [p]$.
3. Déduire des questions précédentes que -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $p \equiv 1 \ [4]$.

Exercice 1.8

Résoudre les systèmes de congruence suivants.

1. $\begin{cases} x \equiv 2 \ [3] \\ x \equiv 3 \ [7] \end{cases}$ **2.** $\begin{cases} 2x + 1 \equiv 2 \ [5] \\ 3x - 1 \equiv 3 \ [7] \end{cases}$ **3.** $\begin{cases} 5x + 2 \equiv 1 \ [6] \\ 7x + 1 \equiv 4 \ [13] \end{cases}$

Exercice 1.9

Donner le PGCD de chacun des couples de polynômes suivants, ainsi qu'une relation de Bezout.

1. $A = X^4 + X^3 - 2X + 1$ et $B = X^2 + X + 1$.
2. $A = X^4 - 2X^3 + X^2 - 3X + 2$ et $B = X^3 - 3X^2 + X + 2$.
3. $A = X^3 + X + 1$ et $B = X^2 - X + 1$.

■ Approfondir

Exercice 1.10

Soit $n \in \mathbb{N}$ tel que $n \geqslant 3$.

On note $\mathscr{A}_n$ le sous-groupe de S_n composé des éléments de signature 1.

1. Si $(a, b, c, d) \in [\![1, n]\!]^4$ est tel que a, b, c et d sont deux à deux distincts, calculer $(a\ b\ c) \circ (b\ c\ d)$.
2. Montrer que $\mathscr{A}_n$ est engendré par les 3-cycles.

Exercice 1.11

Soit G un groupe abélien fini.

1. Soient x et y des éléments de G d'ordre p et q respectivement. Si p et q sont premiers entre eux, montrer que xy est d'ordre pq.
2. En déduire qu'il existe $x \in G$ dont l'ordre est le ppcm des ordres des éléments de G.

Exercice 1.12

Soit A un anneau commutatif et I un idéal de A. On note $\sqrt{I} = \{x \in A\,;\, \exists n \in \mathbb{N}\,;\, x^n \in I\}$.

1. Montrer que $\sqrt{I}$ est un idéal de A.
2. Montrer que $\sqrt{\sqrt{I}} = \sqrt{I}$.
3. Si $A = \mathbb{Z}$ et $I = 2023\mathbb{Z}$, trouver $\sqrt{I}$.

Exercice 1.13

Soit p un nombre premier impair. On considère $(a, b, c) \in \mathbb{Z}^3$ tel que $\overline{a} \neq \overline{0}$.

1. Montrer que l'équation $\overline{a}x^2 + \overline{b}x + \overline{c} = \overline{0}$ admet des solutions dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $\Delta = \overline{b^2 - 4ac}$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$.
2. Discuter le nombre de solutions, et donner leur expression suivant la valeur de Δ.
3. Résoudre dans $\mathbb{Z}/7\mathbb{Z}$ les équations $x^2 + \overline{5}x + \overline{1} = \overline{0}$ et $x^2 + \overline{2}x + \overline{4} = \overline{0}$.

Exercice 1.14

Si $\mathbb{K}$ est un sous-corps de $\mathbb{C}$ et si $a \in \mathbb{C}$, on note $\mathbb{K}[a] = \{P(a)\,;\, P \in \mathbb{K}[X]\}$.

1. Montrer que $\mathbb{K}[a]$ est un anneau pour les lois usuelles.
2. S'il existe $P \in \mathbb{K}[X]\backslash\{0\}$ tel que $P(a) = 0$, montrer que $\{Q \in \mathbb{K}[X]\,;\, Q(a) = 0\}$ est de la forme $R\mathbb{K}[X]$ avec R un polynôme irréductible. En déduire que $\mathbb{K}[a]$ est un corps.
3. Montrer que si $\mathbb{K}[a]$ est un corps, on a $P \in \mathbb{K}[X]\backslash\{0\}$ tel que $P(a) = 0$.

Exercice 1.15

On note $\mathbb{Z}[X]$ l'ensemble des polynômes à coefficients entiers, et si $P \in \mathbb{Z}[X]$, on note $c(P)$ le pgcd des coefficients de P.

1. Soit $(P, Q) \in \mathbb{Z}[X]^2$, avec $c(P) = 1$. On considère p un diviseur premier de $c(PQ)$. Montrer que p divise tous les coefficients de Q.
2. Montrer que pour tout $(P, Q) \in \mathbb{Z}[X]^2$, $c(PQ) = c(P)c(Q)$.
3. Montrer que si P est irréductible dans $\mathbb{Z}[X]$ (tout diviseur de P dans $\mathbb{Z}[X]$ est constant ou associé à P), alors P est irréductible dans $\mathbb{Q}[X]$.
4. Soient $a_1, \ldots, a_n \in \mathbb{Z}$ deux à deux distincts. Montrer que $P = (X - a_1)\ldots(X - a_n) - 1$ est irréductible dans $\mathbb{Q}[X]$.

Exercice 1.16

Soit $\mathbb{K}$ une $\mathbb{R}$-algèbre intègre de dimension finie $n \geqslant 2$.
On assimile tout élément x de $\mathbb{R}$ à l'élément $x.1$ de $\mathbb{K}$.

1. Montrer que tout élément non nul de $\mathbb{K}$ est inversible.
2. Si $a \in \mathbb{K}\backslash\mathbb{R}$, montrer que $(1, a)$ est libre mais que $(1, a, a^2)$ est liée. On pourra commencer par trouver $P \in \mathbb{R}[X]$ tel que $P(a) = 0$.
3. Montrer qu'il existe $i \in \mathbb{K}$ vérifiant $i^2 = -1$.
4. Si $\mathbb{K}$ est commutative, montrer que $\mathbb{K}$ est isomorphe à $\mathbb{C}$.