MATHS

MP/MP*-MPI/MPI*

Claude Deschamps | François Moulin | Yoann Gentric
Emmanuel Delsinne | François Lussier | Chloé Mullaert
Serge Nicolas | Jean Nougayrède | Claire Tête

MATHS

MP/MP*-MPI/MPI*

j'intègre

TOUT-EN-UN

6e édition

DUNOD

Couverture : création Hokus Pokus, adaptation Studio Dunod

11 rue Paul Bert, 92240 Malakoff
www.dunod.com
ISBN 978-2-10-084121-9

Table des matières

Pour Claude

Notre collègue et ami Claude Deschamps
est décédé le 11 mars 2022.

Difficile, Claude, de dissocier ton nom
de celui d'André Warusfel (« Warus »)
qui nous a quittés en 2016.

Vous avez tous les deux dirigé cette collection depuis 1997,
dans la lignée d'une longue série de livres,
dont le dernier avatar, qui porte ton nom,
« Ramis – Deschamps – Odoux », est encore utilisé de nos jours.

Sous votre houlette,
nous avons contribué à ces « Tout-en-un »
dont l'objectif est d'être des ouvrages de référence
pour tous les étudiants et dont le contenu,
accessible à tous, suit à la lettre le programme officiel.

Toute l'équipe de cet ouvrage,
dont certains membres ont été tes élèves,
tient à te rendre hommage en souvenir de tous ces moments
passés à chercher la rédaction idéale
pour transmettre aux étudiants
des notions mathématiques souvent délicates.

Avant-propos

Ce nouveau Tout-en-un de mathématiques vient répondre aux attentes des nouveaux programmes de classes préparatoires, entrés en vigueur en septembre 2021 pour la première année et en septembre 2022 pour la deuxième année. Il reprend l'ambition des précédentes éditions : faire tenir en un seul volume cours complet et exercices corrigés.

Ce volume MP - MPI se veut dans la continuité du volume MPSI - MP2I : lors de son élaboration, l'équipe d'auteurs ne s'est pas contentée d'adapter l'ancien livre au nouveau programme, mais a repensé chaque chapitre en profondeur, dans un souci permanent de clarté et de concision.

Il nous tient à cœur de préciser quelques éléments clés de la structure du livre.

- Plutôt que de faire figurer systématiquement, à la suite de l'énoncé d'une proposition ou d'un théorème, sa démonstration entièrement rédigée, nous préférons parfois donner un principe de démonstration (la démonstration complète étant alors reléguée en fin de chapitre). L'objectif est double :
  - rendre l'exposé du cours plus concis et plus facile à lire lorsque l'étudiant ne souhaite pas s'attarder sur les démonstrations ;
  - l'étudiant, ayant à sa disposition un principe de démonstration, peut soit (en cas de première lecture) tenter de réfléchir par lui-même à la manière d'élaborer la preuve complète, soit (en cas lecture ultérieure) se souvenir rapidement de cette preuve.
- Chaque chapitre se conclut par une série d'exercices permettant à l'étudiant de s'exercer. Chacun de ces exercices est entièrement corrigé.
  - Certains de ces exercices ont pour mission de faire appliquer de manière ciblée un théorème ou une méthode ; sous le numéro de l'exercice est alors indiqué le numéro de la page du cours associée. Inversement, ces exercices sont signalés dans la marge, à l'endroit concerné du cours.

    S'il n'est pas totalement indispensable de traiter ces exercices lors d'une première lecture du cours, leur lien étroit avec celui-ci les rend particulièrement intéressants pour assimiler les nouvelles notions et méthodes.
  - L'étudiant trouvera également des exercices d'entraînement un peu plus ambitieux, demandant plus de réflexion. Certains, plus difficiles, sont étoilés.

Bien entendu nous sommes à l'écoute de toute remarque dont les étudiants, nos collègues, tout lecteur… pourraient nous faire part (à l'adresse électronique suivante : `touten1maths@gmail.com`). Cela nous permettra, le cas échéant, de corriger certaines erreurs nous ayant échappé et surtout ce contact nous guidera pour une meilleure exploitation des choix pédagogiques que nous avons faits aujourd'hui dans cet ouvrage.

François Moulin et Yoann Gentric

« Mode d'emploi » d'un chapitre

Une introduction présente le sujet traité.

Compléments d'algèbre linéaire

Dans ce chapitre, E est un espace vectoriel sur un sous-corps $\mathbb{K}$ de $\mathbb{C}$ (on se limite en pratique au cas où $\mathbb{K}$ est égal à $\mathbb{R}$ ou $\mathbb{C}$).

Les encadrés correspondent soit à des théorèmes, propositions ou corollaires, qui partagent le même système de numérotation, soit à des définitions, qui ont leur propre numérotation.

Corollaire 46

Dans un groupe G fini de cardinal n, on a $\forall x \in G \quad x^n = e$.

Théorème 47 (Théorème d'Euler)

Soit $n \in \mathbb{N}^*$. Pour tout $a \in \mathbb{Z}$ premier avec n, on a $a^{\varphi(n)} \equiv 1\ [n]$.

Définition 7

Une **sous-algèbre** d'une algèbre A est un sous-espace vectoriel de A stable par multiplication et contenant 1_A.

La démonstration de chaque résultat encadré, lorsqu'elle ne suit pas directement celui-ci, est indiquée par un renvoi.

Proposition 4

Étant donné une partie X de A, il existe un plus petit idéal de A contenant X.

Démonstration page 26

Les points de méthode apparaissent sur fond grisé.

Point méthode Pour définir par $\overline{k} \mapsto \varphi(k)$ une application sur $\mathbb{Z}/n\mathbb{Z}$, on vérifiera bien que $\varphi(k)$ ne dépend que de la classe de congruence de k modulo n.

Les points auxquels il faut faire particulièrement attention sont signalés par un filet vertical sur la gauche.

> **Attention** La relation $a^n = e$ ne signifie pas que a est d'ordre n, mais seulement que son ordre divise n d'après la proposition suivante.

Des renvois vers des exercices peuvent apparaître en marge au sein du cours.

Exo 2.12

Définition 4

Un sous-espace vectoriel F de E est dit **stable** par u si $u(F) \subset F$.

Les exemples sont repérés par deux coins.

Ex. 48. Pour $n \in \mathbb{N}^*$, le groupe $\mathbb{U}_n$ des racines n-ièmes de l'unité est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Des exercices sont proposés en fin de chapitre, avec éventuellement un rappel du numéro de la page de cours où se trouve la notion dont l'exercice est une application.

S'entraîner et approfondir

Séries à valeurs dans un espace vectoriel de dimension finie

10.1 →424 Prouver la convergence et déterminer la somme de la série $\sum A^n$, où $A = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$.

Certains exercices bénéficient d'indications, et les plus difficiles sont étoilés.

⋆⋆ **12.30 Théorème de Bernstein**

Soit f une fonction de classe $\mathcal{C}^\infty$ sur un voisinage de 0 et telle que f ainsi que toutes ses dérivées soient positives sur ce voisinage. Montrer que f est développable en série entière.

Indication. *On pourra utiliser la formule de Taylor avec reste intégral.*

Tous les exercices sont entièrement corrigés.

Solutions des exercices

1.1 Soit A un anneau fini intègre et $a \in A$ non nul. L'application $x \mapsto ax$ de A dans A est injective par intégrité de A. Comme A est fini, elle est bijective, donc 1 admet un antécédent ce qui signifie qu'il existe $b \in A$ tel que $ab = 1$. Comme A est commutatif (puisqu'intègre), on a aussi $ba = 1$ et donc a est inversible.

Ainsi, A est un corps.

Chapitre 1 : Groupes, anneaux, arithmétique, algèbres

Groupes, anneaux, arithmétique, algèbres

Nous revenons dans ce chapitre sur les structures algébriques usuelles introduites en première année : groupes, anneaux et corps, notamment en vue de leur utilisation en arithmétique (dans $\mathbb{Z}$ et dans $\mathbb{K}[X]$) et nous les complétons par la notion d'*algèbre* dont deux exemples importants en algèbre linéaire (algèbres des endomorphismes et des matrices carrées) seront étudiés dans le chapitre de réduction des endomorphismes. Enfin, nous conclurons par des approfondissements sur les groupes.
Dans ce chapitre, nous supposons acquises les notions suivantes vues en première année :

- groupe, sous-groupe et morphisme de groupes,
- anneau et corps, sous-anneau et morphisme d'anneaux.

I Anneaux, arithmétique

1 Rappels et notations

- Dans un anneau A, le neutre pour l'addition est noté 0 (ou 0_A), le neutre pour la multiplication 1 (ou 1_A).
- L'anneau est commutatif si la multiplication est commutative (l'addition est commutative par définition).
- Un anneau A est **trivial** si $1_A = 0_A$; dans ce cas, A est réduit à cet unique élément (on dit aussi qu'il est **nul**).
- Un anneau A est intègre s'il est commutatif, non trivial, et s'il vérifie :

Exo 1.1

$$\forall (a,b) \in A^2 \quad ab = 0 \Longrightarrow (a = 0 \quad \text{ou} \quad b = 0)\,.$$

- Rappelons qu'un corps est un anneau commutatif non trivial dans lequel tout élément non nul est inversible.

2 Anneau produit

Soit $n \in \mathbb{N}^*$.

Proposition 1

Étant donné des anneaux $A_1, \dots, A_n$, les opérations terme à terme :

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n)$$

$$(a_1, \dots, a_n) \times (b_1, \dots, b_n) = (a_1 b_1, \dots, a_n b_n)$$

munissent le produit cartésien $A_1 \times \cdots \times A_n$ d'une structure d'anneau.

Démonstration. On sait déjà que $(A_1 \times \cdots \times A_n, +)$ est un groupe (groupe produit) de neutre $(0_{A_1}, \dots, 0_{A_n})$. On vérifie facilement que $(1_{A_1}, \dots, 1_{A_n})$ est neutre pour la multiplication. Enfin, les propriétés d'associativité et de distributivité se déduisent immédiatement des propriétés correspondantes des anneaux $(A_i, +, \times)$. □

Ex. 1. Si A est un anneau, alors A^n est un anneau, comme produit de n exemplaires de A. En particulier, $\mathbb{R}^n$ et $\mathbb{C}^n$ sont des anneaux.

Ex. 2. Dans un anneau produit $A_1 \times \cdots \times A_n$, les éléments inversibles sont les $(a_1, \dots, a_n)$, où a_i est inversible dans A_i pour tout i, avec alors $(a_1, \dots, a_n)^{-1} = (a_1^{-1}, \dots, a_n^{-1})$.

Exo 1.2

3 Idéaux d'un anneau commutatif

Soit A un anneau commutatif.

Définition 1 (Idéal d'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 stable par multiplication par tout élément de A, c'est-à-dire :

$$\forall x \in I \quad \forall a \in A \quad xa \in I.$$

Remarque Par commutativité de A, un idéal I de A vérifie aussi :

$$\forall x \in I \quad \forall a \in A \quad ax \in I.$$

Ex. 3. A et $\{0\}$ sont évidemment des idéaux de A, appelés **idéaux triviaux** de A.

Ex. 4. Soit X une partie de $\mathbb{R}$. L'ensemble des fonctions nulles en tout point de X est un idéal de $\mathcal{F}(\mathbb{R}, \mathbb{R})$.

Exo 1.3

Exo 1.4

Remarque
Si I est un idéal de A contenant 1, alors $\forall a \in A \quad a = a.1 \in I$, donc $I = A$.

Attention Soit B un anneau. Le **noyau** d'un morphisme d'anneaux de A dans B, c'est-à-dire son noyau en tant que morphisme de groupes de $(A,+)$ dans $(B,+)$ n'est pas un sous-anneau de $(A,+,\times)$ si B est non trivial puisqu'alors $\varphi(1_A) = 1_B \neq 0_B$ et donc que $1_A \notin \operatorname{Ker}\varphi$.
En revanche :

Proposition 2

Le noyau de tout morphisme d'anneaux φ de A dans un anneau B est un idéal de A.

Démonstration. C'est un sous-groupe de $(A,+)$ en tant que noyau d'un morphisme de groupes. Soit $x \in \operatorname{Ker}\varphi$ et $a \in A$. On a $\varphi(ax) = \varphi(a)\varphi(x) = \varphi(a) \times 0 = 0$. Donc $\operatorname{Ker}\varphi$ est un idéal de A. □

Idéal engendré par un élément

Proposition 3

Une intersection d'idéaux de A est un idéal de A.

Démonstration page 26

Proposition 4

Étant donné une partie X de A, il existe un plus petit idéal de A contenant X.

Démonstration page 26

Principe de démonstration. C'est l'intersection de tous les idéaux de A contenant X.

Terminologie

- On l'appelle **idéal** de A **engendré par X**.
- Si x est un élément de A, l'**idéal engendré par x** est, par définition, l'idéal engendré par $\{x\}$, c'est-à-dire le plus petit idéal de A contenant x.

Proposition 5 (Idéal engendré par un élément)

Exo 1.5

Soit $x \in A$. L'idéal engendré par x est $xA = \{xa \mid a \in A\}$.

Démonstration page 26

Proposition 6

L'idéal de A engendré par une partie finie $\{x_1, \ldots, x_k\}$ est :

$$x_1A + \cdots + x_kA = \{x_1a_1 + \cdots + x_ka_k \mid (a_1, \ldots, a_k) \in A^k\}.$$

C'est aussi le plus petit idéal de A contenant tous les idéaux $x_1A, \ldots, x_kA$.

Démonstration page 26

4 Divisibilité dans un anneau intègre

On suppose à partir de maintenant que A est un anneau intègre.

Définition 2

Soit $(x,y) \in A^2$. On dit que x **divise** y, ou que y est un **multiple** de x, s'il existe $z \in A$ tel que $y = xz$. On note alors $x \mid y$.

Terminologie

- Lorsque x divise y, on dit aussi que x est un **diviseur** de y ou que y est un **multiple** de x.
- Lorsque x non nul divise y, il y a, par intégrité de A, unicité de $z \in A$ tel que $y = xz$. Cet élément est alors appelé **quotient** de y par x.

Remarque Pour tout $(x, y) \in A^2$, on a $x \mid y \iff y \in xA$.

La relation de divisibilité est une relation réflexive et transitive, mais n'est en général ni symétrique ni antisymétrique (ce n'est donc ni une relation d'ordre, ni une relation d'équivalence).

Ex. 5. Les diviseurs de 1 sont les éléments inversibles.

Ex. 6. Tout élément de A divise 0, mais 0 ne divise que lui-même.

Ex. 7. Grâce à l'intégrité, on a, pour tout $a \neq 0$:

$$ax \mid ay \iff (\exists z \in A \quad ay = axz) \iff (\exists z \in A \quad y = xz) \iff x \mid y.$$

Lien avec les idéaux

La proposition suivante permet de ramener la notion de divisibilité à une relation d'ordre (inclusion sur les idéaux).

Proposition 7

On a, pour tout $(x, y) \in A^2$:

$$x \mid y \iff yA \subset xA.$$

Démonstration. Soit $(x, y) \in A^2$. Comme yA est le plus petit idéal de A contenant y et que xA est un idéal, l'inclusion $yA \subset xA$ est équivalente à $y \in xA$, c'est-à-dire à $x \mid y$. □

Remarque Deux éléments engendrent le même idéal si, et seulement s'ils se divisent mutuellement. On dit alors qu'ils sont **associés**.

Terminologie Les idéaux engendrés par un élément sont appelés **idéaux principaux**. L'exemple qui suit montre qu'il existe des idéaux non principaux.

Ex. 8. Considérons l'anneau $\mathbb{Z}[X]$ des polynômes à coefficients entiers et $I = 2\mathbb{Z}[X] + X\mathbb{Z}[X]$ l'idéal engendré par 2 et X. Supposons que I soit principal, c'est-à-dire qu'il existe un polynôme $P \in \mathbb{Z}[X]$ tel que $I = P\mathbb{Z}[X]$. Les inclusions $2\mathbb{Z}[X] \subset P\mathbb{Z}[X]$ et $X\mathbb{Z}[X] \subset P\mathbb{Z}[X]$ montrent alors, d'après la proposition 7, que P divise 2, donc qu'il est constant, et qu'il divise X, donc que son coefficient dominant est ± 1. Finalement, $P = \pm 1$ et il existe donc deux polynômes $(U, V) \in \mathbb{Z}[X]^2$ tels que $\pm 1 = 2U + XV$. En évaluant en 0, cela donne $2U(0) = \pm 1$, ce qui est absurde puisque $U(0) \in \mathbb{Z}$.
Donc I n'est pas principal.

Idéaux de $\mathbb{Z}$

Commençons par un résultat sur les sous-groupes de $\mathbb{Z}$.

Proposition 8

Les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$, pour $n \in \mathbb{N}$.

Démonstration page 26

Principe de démonstration. Si H est un sous-groupe non nul de $\mathbb{Z}$, on considère le plus petit élément n strictement positif de H et l'on utilise la division euclidienne par n pour montrer que tout élément de H est un multiple de n.

On en déduit que tous les idéaux de $\mathbb{Z}$ sont principaux :

Théorème 9

Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, pour $n \in \mathbb{N}$.

Démonstration.

- Pour tout $n \in \mathbb{N}$, l'ensemble $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ des multiples de n est un idéal de $\mathbb{Z}$: c'est l'idéal de $\mathbb{Z}$ engendré par n (cf. proposition 5 de la page 4).
- Réciproquement, un idéal étant en particulier un sous-groupe, il n'y en a pas d'autres d'après la proposition 8. □

Remarque Soit I un idéal de $\mathbb{Z}$. Il existe donc $n \in \mathbb{N}$ tel que $I = n\mathbb{Z}$.

- Si m est un entier relatif tel que $I = m\mathbb{Z}$, alors $n \in m\mathbb{Z}$ et $m \in n\mathbb{Z}$, donc $m \mid n$ et $n \mid m$, ce qui donne $m = \pm n$.
- Réciproquement, il est clair que $(-n)\mathbb{Z} = n\mathbb{Z}$.

On a ainsi montré l'unicité de $n \in \mathbb{N}$ tel que $I = n\mathbb{Z}$: on l'appelle **le générateur** de l'idéal I.

5 Retour sur le PGCD dans $\mathbb{Z}$

Soit $n \in \mathbb{N}^*$ et $a_1, \ldots, a_n$ des entiers relatifs. Nous avons vu à la proposition 6 de la page 4 que l'idéal de $\mathbb{Z}$ engendré par les éléments $a_1, \ldots, a_n$ était $I = a_1\mathbb{Z} + \cdots + a_n\mathbb{Z}$. Cela permet de donner une nouvelle définition du PGCD.

Proposition 10

Étant donné des entiers $a_1, \ldots, a_n$, il existe un unique entier naturel d tel que $d\mathbb{Z} = a_1\mathbb{Z} + \cdots + a_n\mathbb{Z}$. Pour tout $k \in \mathbb{Z}$, on a la relation :

$$k \mid d \iff \big(\forall i \in [\![1, n]\!] \quad k \mid a_i\big).$$

On l'appelle **PGCD** de $a_1, \ldots, a_n$ et l'on dispose de la **relation de Bézout** :

$$\exists (u_1, \ldots, u_n) \in \mathbb{Z}^n \quad d = a_1u_1 + \cdots + a_nu_n.$$

Démonstration.

- Considérons le générateur de l'idéal $a_1\mathbb{Z} + \cdots + a_n\mathbb{Z}$, c'est-à-dire l'unique $d \in \mathbb{N}$ tel que $d\mathbb{Z} = a_1\mathbb{Z} + \cdots + a_n\mathbb{Z}$ (cf. remarque de la présente page).

Ainsi, $d\mathbb{Z}$ est le plus petit idéal de $\mathbb{Z}$ contenant $\{a_1, \dots, a_n\}$ (proposition 6 de la page 4), donc pour tout $k \in \mathbb{Z}$, puisque $k\mathbb{Z}$ est un idéal de $\mathbb{Z}$:

$$\begin{aligned} k \mid d &\iff d\mathbb{Z} \subset k\mathbb{Z} \\ &\iff \forall i \in [\![1, n]\!] \quad a_i \in k\mathbb{Z} \\ &\iff \forall i \in [\![1, n]\!] \quad k \mid a_i. \end{aligned}$$

- Enfin, puisque $d \in d\mathbb{Z} = a_1\mathbb{Z} + \cdots + a_n\mathbb{Z}$, on a par définition :

$$\exists (u_1, \dots, u_n) \in \mathbb{Z}^n \quad d = a_1u_1 + \cdots + a_nu_n. \qquad \square$$

Remarques

- Les diviseurs communs à $a_1, \dots, a_n$ sont donc exactement les diviseurs de d.
- Lorsque d est non nul, c'est-à-dire lorsqu'au moins l'un des a_i est non nul, c'est donc le plus grand parmi tous les diviseurs positifs communs à $a_1, \dots, a_n$ (et même parmi tous les diviseurs communs à $a_1, \dots, a_n$).
- De la même façon, on pourrait définir le **PPCM** de $a_1, \dots, a_n$ comme le générateur m de l'idéal $a_1\mathbb{Z} \cap \cdots \cap a_n\mathbb{Z}$, de façon à avoir, pour tout $k \in \mathbb{Z}$, l'équivalence :

$$k \in m\mathbb{Z} \iff \big(\forall i \in [\![1, n]\!] \quad k \in a_i\mathbb{Z}\big).$$

C'est le plus petit des multiples positifs communs à $a_1, \dots, a_n$.

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

Congruences dans $\mathbb{Z}$

Soit n un entier naturel.

Rappels Nous avons vu en première année la relation de congruence modulo n définie par :

$$x \equiv y \ [n] \iff y - x \in n\mathbb{Z}.$$

Il s'agit une relation d'équivalence sur $\mathbb{Z}$ qui est compatible avec les opérations de $\mathbb{Z}$, c'est-à-dire qui vérifie :

$$\forall (x, y, x', y') \in \mathbb{Z}^4 \quad \left\{ \begin{array}{l} x \equiv x' \ [n] \\ y \equiv y' \ [n] \end{array} \right. \implies \left\{ \begin{array}{l} x + y \equiv x' + y' \ [n] \\ x \times y \equiv x' \times y' \ [n]. \end{array} \right.$$

Notation On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence pour cette relation. La classe d'un élément k de $\mathbb{Z}$ est souvent notée $\overline{k}$.

Ex. 9. La congruence modulo 0 est la relation d'égalité, donc $\mathbb{Z}/0\mathbb{Z} = \big\{\{k\} \mid k \in \mathbb{Z}\big\}$.

Ex. 10. Deux entiers quelconques sont évidemment congrus modulo 1, donc $\mathbb{Z}/1\mathbb{Z} = \{\overline{0}\}$.

Ex. 11. Modulo 2, il y a deux classes : celle des entiers pairs et celle des entiers impairs. Donc $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$.

Proposition 11

Pour $n \in \mathbb{N}^*$, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ a n éléments, et l'on a :

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

Démonstration page 27

Principe de démonstration. Utiliser la division euclidienne par n.

Ex. 12. Soit n et p deux entiers naturels non nuls. Pour $k \in \mathbb{Z}$, nous noterons $[k]_n$ et $[k]_p$ les classes de k respectivement modulo n et p.
Voyons à quelle condition on peut définir une application :

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \\ [k]_n & \longmapsto & [k]_p. \end{array}$$

- Si une telle application existe, comme $[n]_n = [0]_n$, on doit avoir $[n]_p = [0]_p$, soit $p \mid n$.
- Supposons réciproquement que p divise n. Alors si k et ℓ sont deux entiers tels que $[k]_n = [\ell]_n$, on a $n \mid k - \ell$, donc $p \mid k - \ell$, soit $[k]_p = [\ell]_p$. On peut donc bien définir l'application :

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \\ \alpha & \longmapsto & [k]_p \quad \text{où } k \in \alpha \end{array}$$

puisque la définition de l'image de α ne dépend que de α et non d'un de ses représentants.

Point méthode Pour définir par $\overline{k} \mapsto \varphi(k)$ une application sur $\mathbb{Z}/n\mathbb{Z}$, on vérifiera bien que $\varphi(k)$ ne dépend que de la classe de congruence de k modulo n.

Anneau $\mathbb{Z}/n\mathbb{Z}$

Proposition 12

Il existe sur $\mathbb{Z}/n\mathbb{Z}$ des lois, notées $+$ et $\times$ et appelées **lois quotient**, telles que :

1. $\forall (x, y) \in (\mathbb{Z}/n\mathbb{Z})^2 \quad \overline{x} + \overline{y} = \overline{x+y}$ et $\overline{x} \times \overline{y} = \overline{x \times y}$,
2. $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ soit un anneau commutatif d'éléments neutres $\overline{0}$ et $\overline{1}$,
3. la **projection canonique** $\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ x & \longmapsto & \overline{x} \end{array}$ soit un morphisme d'anneaux surjectif de noyau $n\mathbb{Z}$.

Démonstration page 27

Principe de démonstration. Pour α et β dans $\mathbb{Z}/n\mathbb{Z}$, on définit :

$$\alpha + \beta = \overline{x+y} \quad \text{et} \quad \alpha \times \beta = \overline{x \times y} \qquad \text{où} \qquad x \in \alpha \quad \text{et} \quad y \in \beta.$$

Il faut commencer par vérifier que $\overline{x+y}$ et $\overline{x \times y}$ ne dépendent que de α et β, et non des représentants x et y choisis, grâce à la compatibilité de la relation de congruence avec les lois de $\mathbb{Z}$.

Notation Le produit de deux éléments α et β de $\mathbb{Z}/n\mathbb{Z}$ est souvent noté $\alpha\beta$ plutôt que $\alpha \times \beta$.

Ex. 13. Écrivons les tables d'addition et de multiplication de $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$. Pour alléger les notations, nous écrirons $0, 1, 2, \ldots$ à la place de $\overline{0}, \overline{1}, \overline{2}, \ldots$

$\mathbb{Z}/5\mathbb{Z}$:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\mathbb{Z}/6\mathbb{Z}$:

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

On remarque que $\mathbb{Z}/5\mathbb{Z}$ est intègre puisque pour avoir $\alpha\beta = 0$ il est nécessaire d'avoir $\alpha = 0$ ou $\beta = 0$ (absence de 0 dans la portion entourée de pointillés).
En revanche, $\mathbb{Z}/6\mathbb{Z}$ est non intègre puisque, par exemple $\overline{2} \times \overline{3} = \overline{0}$.

Remarque On peut aussi prendre pour représentants des classes modulo $n \in \mathbb{N}^*$, n'importe quel n-uplet d'entiers consécutifs. Par exemple, pour étudier la multiplication sur $\mathbb{Z}/5\mathbb{Z}$, il pourra être intéressant d'écrire $\mathbb{Z}/5\mathbb{Z} = \{-\overline{2}, -\overline{1}, \overline{0}, \overline{1}, \overline{2}\}$.

Ex. 14. Pour résoudre l'équation $x^2 - \overline{1} = \overline{0}$ dans $\mathbb{Z}/12\mathbb{Z}$, il suffit de lister les carrés des éléments de $\mathbb{Z}/12\mathbb{Z}$ pour voir lesquels sont égaux à $\overline{1}$:

x	$\overline{0}$	$\pm\overline{1}$	$\pm\overline{2}$	$\pm\overline{3}$	$\pm\overline{4}$	$\pm\overline{5}$	$\overline{6}$
x^2	$\overline{0}$	$\overline{1}$	$\overline{4}$	$-\overline{3}$	$\overline{4}$	$\overline{1}$	$\overline{0}$

On en déduit que $x^2 - \overline{1} = \overline{0} \iff x \in \{-\overline{1}, \overline{1}, -\overline{5}, \overline{5}\}$.

Proposition 13 (Éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$)

La classe de $k \in \mathbb{Z}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si, et seulement si, k est premier avec n.

Démonstration page 27

Principe de démonstration. L'élément $\overline{k}$ de $\mathbb{Z}/n\mathbb{Z}$ est inversible si, et seulement s'il existe $(u, v) \in \mathbb{Z}^2$ tel que $ku + nv = 1$ et son inverse est alors $\overline{u}$.

Remarque Trouver l'inverse de $\overline{k}$ dans $\mathbb{Z}/n\mathbb{Z}$ revient à trouver l'inverse de k modulo n (voir le cours de première année). Rappelons (c'est d'ailleurs aussi ce qui a été fait dans la démonstration précédente) qu'il suffit pour cela de trouver un couple (u, v) tel que $ku + nv = 1$ (coefficients de Bézout). L'inverse de $\overline{k}$ est alors $\overline{u}$.

Ex. 15. Déterminons l'inverse de $\overline{13}$ dans $\mathbb{Z}/34\mathbb{Z}$.
On trouve, par exemple à l'aide de l'algorithme d'Euclide (voir le cours de première année), l'égalité de Bézout $5 \times 34 - 13 \times 13 = 1$, donc l'inverse de $\overline{13}$ est $-\overline{13} = \overline{21}$ dans $\mathbb{Z}/34\mathbb{Z}$.

Théorème 14

Soit $n \in \mathbb{N}^*$. Alors $\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est premier.

Démonstration page 27

Principe de démonstration.

- Si n est premier, tous les éléments de $[\![1, n-1]\!]$ sont premiers avec n, donc leur classe est inversible.
- Si $n = ab$, alors $\overline{a} \times \overline{b} = \overline{ab} = \overline{0}$, ce qui permet de montrer que $\mathbb{Z}/n\mathbb{Z}$ est non intègre si n n'est pas premier.

Notation Lorsque p est un nombre premier, le corps $\mathbb{Z}/p\mathbb{Z}$ est aussi noté $\mathbb{F}_p$.

7 Théorème chinois

On note ici $[k]_n$ la classe de l'entier k modulo un entier naturel non nul n.

Proposition 15

Soit n et m des entiers naturels premiers entre eux. Les anneaux $\mathbb{Z}/(nm)\mathbb{Z}$ et $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ sont isomorphes par le morphisme d'anneaux φ :

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

Démonstration page 28

Principe de démonstration. Pour la définition de φ, vérifier que le couple $\big([k]_n, [k]_m\big)$ ne dépend que de la classe de k modulo nm.

On démontre l'injectivité de φ et l'on conclut par cardinalité.

Le corollaire suivant n'est que la traduction en termes de congruence de la proposition 15.

Corollaire 16 (Théorème chinois)

Si n et m sont des entiers premiers entre eux, alors pour tout $(a, b) \in \mathbb{Z}^2$, il existe un entier k vérifiant le système :

$$\left\{ \begin{array}{l} k \equiv a \ [n] \\ k \equiv b \ [m] \end{array} \right. \qquad (S)$$

et les solutions de ce système sont exactement les entiers congrus à k modulo nm.

Le théorème chinois permet de ramener l'étude d'une équation sur $\mathbb{Z}/n\mathbb{Z}$ lorsque n n'est pas premier, à celle d'équations sur des anneaux plus simples.

Point méthode (pour obtenir une solution de (S)) À partir d'une relation de Bézout $mu + nv = 1$, on trouve deux entiers $k_1 = mu$ et $k_2 = nv$ vérifiant respectivement les systèmes de congruences :

$$\left\{ \begin{array}{l} k_1 \equiv 1 \ [n] \\ k_1 \equiv 0 \ [m] \end{array} \right. \qquad \text{et} \qquad \left\{ \begin{array}{l} k_2 \equiv 0 \ [n] \\ k_2 \equiv 1 \ [m] \end{array} \right.$$

et une solution du système (S) est alors $k = k_1 a + k_2 b$ (vérification immédiate en prenant les congruences modulo n et m).

Ex. 16. Trouvons les entiers k tels que $k^2+k+11 \equiv 0\ [143]$, c'est-à-dire tels que l'on ait simultanément $k^2+k+11 \equiv 0\ [11]$ et $k^2+k+11 \equiv 0\ [13]$.
Cela revient à résoudre l'équation $x^2+x+11=0$ dans $\mathbb{Z}/11\mathbb{Z}$ et dans $\mathbb{Z}/13\mathbb{Z}$. Pour chaque couple de solutions $\big([a]_{11},[b]_{13}\big)$, le point méthode précédent donne la classe modulo 143 correspondante.

- Dans $\mathbb{Z}/11\mathbb{Z}$, l'équation devient $x^2+x=0$, c'est-à-dire $x(x+1)=0$.
  Comme $\mathbb{Z}/11\mathbb{Z}$ est un corps, cela équivaut à $x=0$ ou $x=-1$.
- De même, dans $\mathbb{Z}/13\mathbb{Z}$, on obtient l'équation $x^2+x-2=0$, c'est-à-dire $(x-1)(x+2)=0$, ce qui donne, puisque $\mathbb{Z}/13\mathbb{Z}$ est un corps, les deux solutions $x=1$ ou $x=-2$.
- On a donc 4 solutions modulo 143 à l'équation initiale données, en reprenant les notations du corollaire 16 de la page précédente, par $a \in \{0,-1\}$ et $b=\{1,-2\}$.
- Une relation de Bézout entre 11 et 13 est $6\times 11-5\times 13=1$. Ainsi $k_1=-65$ vérifie $k_1\equiv 1\ [11]$ et $k_1\equiv 0\ [13]$. De même, $k_2=66$ vérifie $k_2\equiv 0\ [11]$ et $k_2\equiv 1\ [13]$.
- Pour chaque couple (a,b), la solution correspondante est ak_1+bk_2. Les résultats sont récapitulés dans le tableau ci-dessous :

a \ b	1	-2
0	66	11
-1	131	76

Remarque L'obtention d'une telle solution est non triviale, mais il est très facile de vérifier qu'elle est effectivement solution, ce qui permet de repérer une erreur de calcul éventuelle. Par exemple il est immédiat que 76 est bien congru à -1 modulo 11 et à -2 modulo 13.

Corollaire 17

Étant donné des entiers naturels $n_1,\dots,n_r$ premiers entre eux deux à deux, les anneaux $\mathbb{Z}/(n_1\cdots n_r)\mathbb{Z}$ et $(\mathbb{Z}/n_1\mathbb{Z})\times\cdots\times(\mathbb{Z}/n_r\mathbb{Z})$ sont isomorphes.

Démonstration. Par récurrence sur r, en remarquant que si $n_1,\dots,n_{r+1}$ sont premiers entre eux deux à deux, alors $n_1\cdots n_r$ et n_{r+1} sont premiers entre eux et $(\mathbb{Z}/n_1\mathbb{Z})\times\cdots\times(\mathbb{Z}/n_{r+1}\mathbb{Z})$ est isomorphe à $\big((\mathbb{Z}/n_1\mathbb{Z})\times\cdots\times(\mathbb{Z}/n_r\mathbb{Z})\big)\times(\mathbb{Z}/n_{r+1}\mathbb{Z})$. □

8 Indicatrice d'Euler

Définition 3

On appelle **indicatrice d'Euler** de $n\in\mathbb{N}^*$, et l'on note $\varphi(n)$, le cardinal de l'ensemble :

$$\big\{k\in[\![1,n]\!]\ :\ k\wedge n=1\big\}.$$

Remarques

- On a évidemment $\varphi(1)=1$.
- Pour $n\geqslant 2$, $\varphi(n)$ est aussi le nombre d'éléments de $[\![1,n-1]\!]$ premiers avec n.
- Dans tous les cas, c'est aussi le nombre d'éléments de $[\![0,n-1]\!]$ premiers avec n, donc également le nombre d'éléments inversibles dans l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Ex. 17. Pour tout $n \geqslant 2$, on a $\varphi(n) \leqslant n-1$ avec égalité si, et seulement si, n est premier. En effet, d'après les remarques précédentes, $\varphi(n)$ est le nombre d'éléments de $[\![1, n-1]\!]$ premiers avec n (d'où l'inégalité) et n est premier si, et seulement si, tous les éléments de $[\![1, n-1]\!]$ sont premiers avec n.

Exo 1.7

Lemme 18

Soit p un nombre premier. Pour tout $k \in \mathbb{N}^*$, on a $\varphi(p^k) = p^k - p^{k-1}$.

Démonstration. Les éléments qui sont non premiers avec p^k sont les multiples de p, c'est-à-dire $p, 2p, \ldots, (p^{k-1})p$ pour ceux qui sont dans $[\![1, p^k]\!]$. Il y en a donc p^{k-1}. □

Proposition 19

Étant donné des entiers naturels $n_1, \ldots, n_r$ premiers entre eux deux à deux, on a $\varphi(n_1 \cdots n_r) = \varphi(n_1) \cdots \varphi(n_r)$.

Démonstration page 28

Principe de démonstration. L'isomorphisme d'anneaux du corollaire 17 de la page précédente entre $\mathbb{Z}/(n_1 \cdots n_r)\mathbb{Z}$ et $(\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_r\mathbb{Z})$ induit une bijection entre leurs groupes des unités.

Corollaire 20

Si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, avec $p_1, \ldots, p_r$ des nombres premiers distincts deux à deux et $\alpha_1, \ldots, \alpha_r$ des entiers naturels non nuls, alors on a :

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

Démonstration. À l'aide du résultat précédent et du lemme 18, il vient :

$$\varphi(n) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_r^{\alpha_r}) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \cdots \left(p_r^{\alpha_r} - p_r^{\alpha_r - 1}\right),$$

ce qui donne le résultat après factorisation par $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. □

II Anneau des polynômes à une indéterminée

On considère ici un sous-corps $\mathbb{K}$ de $\mathbb{C}$. La structure d'anneau de $\mathbb{K}[X]$, étudiée en première année lorsque $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$, se définit de la même manière dans le cas général [1].

On conserve en particulier la notion de degré ainsi que ses propriétés qui permettent de montrer le résultat suivant.

Proposition 21

L'anneau $\mathbb{K}[X]$ est intègre.

Démonstration page 28

On conserve aussi le théorème de division euclidienne, dont la démonstration est exactement la même que celle qui a été faite en première année dans le cas de $\mathbb{R}$ ou de $\mathbb{C}$.

1. En fait, tout ce qui est fait ici est valable pour un corps quelconque, en particulier pour un corps fini $\mathbb{F}_p$, avec p premier.

Théorème 22

Soit A et B deux polynômes de $\mathbb{K}[X]$, avec $B \neq 0$.

Il existe un unique couple (Q, R) de polynômes de $\mathbb{K}[X]$ vérifiant :

$$A = BQ + R \qquad \text{et} \qquad \deg R < \deg B.$$

1 Propriétés arithmétiques élémentaires

Nous allons maintenant généraliser les propriétés arithmétiques de $\mathbb{K}[X]$ vues en première année lorsque $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$.

Ex. 18. Un polynôme B non nul divise $A \in \mathbb{K}[X]$ si, et seulement si, le reste de la division euclidienne de A par B est nul.

Ex. 19. Soit $\mathbb{K}'$ un sous-corps de $\mathbb{K}$ ainsi que A et B deux polynômes à coefficients dans $\mathbb{K}'$, avec B non nul. Montrons que le polynôme B divise A dans $\mathbb{K}'[X]$ si, et seulement s'il divise A dans $\mathbb{K}[X]$.

Il est évident que si B divise A dans $\mathbb{K}'[X]$, alors il divise A dans $\mathbb{K}[X]$. Réciproquement, supposons qu'il existe $C \in \mathbb{K}[X]$ tel que $A = BC$. La division euclidienne de A par B dans $\mathbb{K}'[X]$ s'écrit $A = BQ + R$, avec $(Q, R) \in \mathbb{K}'[X]^2$ et $\deg R < \deg B$. On dispose alors des deux égalités dans $\mathbb{K}[X]$:

$$A = BQ + R \quad \text{avec} \quad \deg R < \deg B \qquad \text{et} \qquad A = BC + 0 \quad \text{avec} \quad \deg 0 < \deg B$$

et l'unicité de la division euclidienne dans $\mathbb{K}[X]$ donne $R = 0$. Donc B divise A dans $\mathbb{K}'[X]$.

Inversibles

Proposition 23

Les éléments inversibles de $\mathbb{K}[X]$ sont les polynômes constants non nuls.

Démonstration page 28

Polynômes associés

Proposition 24

Soit A et B deux éléments de $\mathbb{K}[X]$. Les propriétés suivantes sont équivalentes :

(i) $A \mid B$ et $B \mid A$;

(ii) il existe $\lambda \in \mathbb{K}^*$ tel que $B = \lambda A$.

On dit alors que A et B sont **associés**.

Démonstration page 28

Ex. 20. 0 n'est associé qu'à lui-même.

Ex. 21. Les éléments inversibles de $\mathbb{K}[X]$ sont les associés de 1.

Ex. 22. Tout élément A non nul de $\mathbb{K}[X]$ est associé à un unique polynôme unitaire, obtenu en divisant A par son coefficient dominant.

Polynômes irréductibles

Définition 4

Un **polynôme irréductible** est un polynôme non constant dont les seuls diviseurs sont ses associés et les constantes non nulles.

Ex. 23. Tout polynôme de degré 1 est irréductible.

Proposition 25

Un élément $A \in \mathbb{K}[X]$ est irréductible si, et seulement si :

- A est non constant ;
- si $A = BC$, avec $(B, C) \in \mathbb{K}[X]^2$, alors B ou C est constant.

Démonstration page 29

Rappelons la caractérisation des irréductibles de $\mathbb{R}[X]$ et $\mathbb{C}[X]$.

Proposition 26 (Irréductibles de $\mathbb{R}[X]$ et $\mathbb{C}[X]$)

- Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.
- Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 dont le discriminant est strictement négatif.

Ex. 24. Un polynôme $P \in \mathbb{K}[X]$ de degré 2 ou 3 n'ayant aucune racine dans $\mathbb{K}$ est irréductible dans $\mathbb{K}[X]$.

En effet, s'il s'écrivait $P = AB$, avec A et B non constants, on aurait $\deg A \geqslant 1$, $\deg B \geqslant 1$ et $\deg A + \deg B = \deg P \leqslant 3$. L'un des deux polynômes A ou B serait donc de degré 1, donc aurait une racine dans $\mathbb{K}$, ce qui est impossible puisqu'il divise P qui n'a pas de racine dans $\mathbb{K}$.

Ex. 25. Montrons que $P = X^3 + X + 1$ est irréductible dans $\mathbb{Q}[X]$. Comme il est de degré 3, l'exemple précédent montre qu'il suffit de prouver qu'il n'a pas de racine dans $\mathbb{Q}$.

Supposons donc, par l'absurde, $P(p/q) = 0$ avec p et q deux entiers premiers entre eux et $q \neq 0$.

Exo 1.10

Alors $p^3 + pq^2 + q^3 = 0$, donc $q \mid p^3$ et $p \mid q^3$. On en déduit $p = \pm 1$ et $q = \pm 1$ puisque $p \wedge q = 1$. Ainsi, $p/q = \pm 1$, ce qui est contradictoire puisque $P(1) = 3 \neq 0$ et $P(-1) = -1 \neq 0$.

Polynômes premiers entre eux

Définition 5

Deux éléments de $\mathbb{K}[X]$ sont **premiers entre eux** si leurs seuls diviseurs communs sont les polynômes constants non nuls de $\mathbb{K}[X]$.

Ex. 26. Deux polynômes irréductibles non associés sont premiers entre eux. Considérons, en effet, deux polynômes irréductibles P et Q non premiers entre eux. Ils admettent alors un diviseur commun D non constant. Comme P et Q sont irréductibles, on en déduit que D est associé à P et à Q, donc que P et Q sont associés.

Plus généralement :

Proposition 27

Soit P un polynôme irréductible et A un polynôme quelconque. Alors P et A sont premiers entre eux si, et seulement si, P ne divise pas A.

Démonstration page 29

2 Utilisation des idéaux de $\mathbb{K}[X]$

Idéaux de $\mathbb{K}[X]$

Si B est un élément de $\mathbb{K}[X]$, la proposition 5 de la page 4 montre que :

$$B\mathbb{K}[X] = \{BQ \mid Q \in \mathbb{K}[X]\}$$

est un idéal de $\mathbb{K}[X]$: c'est l'idéal engendré par B.

Comme dans le cas de $\mathbb{Z}$, on obtient ainsi tous les idéaux de $\mathbb{K}[X]$.

Théorème 28

Les idéaux de $\mathbb{K}[X]$ sont les $B\mathbb{K}[X]$, pour $B \in \mathbb{K}[X]$.

Démonstration page 29

Principe de démonstration. Si I est un idéal non nul de $\mathbb{K}[X]$, on considère un élément B non nul de I de degré minimal et l'on utilise la division euclidienne par B pour montrer que tout élément de I est un multiple de B.

Ainsi, tout comme $\mathbb{Z}$, l'anneau $\mathbb{K}[X]$ a tous ses idéaux principaux (voir page 5). On dit que ce sont des **anneaux principaux**.

Grâce à cette propriété importante de $\mathbb{K}[X]$, nous allons pouvoir retrouver (et généraliser au cas d'un corps $\mathbb{K}$ quelconque) les propriétés arithmétiques de l'anneau $\mathbb{K}[X]$.

Lien avec la divisibilité

Rappelons (proposition 7 de la page 5) que la divisibilité se ramène à une inclusion d'idéaux :

$$\forall (A,B) \in \mathbb{K}[X]^2 \quad B \mid A \iff A\mathbb{K}[X] \subset B\mathbb{K}[X].$$

On en déduit, grâce à la proposition 24 de la page 13, que deux polynômes sont associés si, et seulement s'ils sont générateurs du même idéal.

Corollaire 29

Tout idéal I de $\mathbb{K}[X]$ est de la forme $A\mathbb{K}[X]$ pour un unique polynôme A nul ou unitaire. Ce polynôme A est appelé **le générateur** de I.

PGCD de polynômes

Soit $n \in \mathbb{N}^*$ et $A_1, \ldots, A_n$ des polynômes à coefficients dans $\mathbb{K}$. Nous avons vu à la proposition 6 de la page 4 que l'idéal de $\mathbb{K}[X]$ engendré par les éléments $A_1, \ldots, A_n$ était $I = A_1\mathbb{K}[X] + \cdots + A_n\mathbb{K}[X]$. Cela conduit à la définition :

Proposition 30 (Définition du PGCD)

Étant donné $A_1, \dots, A_n$ dans $\mathbb{K}[X]$, il existe un polynôme $D \in \mathbb{K}[X]$ tel que $D\mathbb{K}[X] = A_1\mathbb{K}[X] + \cdots + A_n\mathbb{K}[X]$. On a, pour tout $P \in \mathbb{K}[X]$:

$$P \mid D \iff \big(\forall i \in [\![1, n]\!] \quad P \mid A_i\big).$$

On dit que D est un **PGCD** de $A_1, \dots, A_n$ et l'on dispose de la **relation de Bézout** :

$$\exists (U_1, \dots, U_n) \in \mathbb{K}[X]^n \quad D = A_1U_1 + \cdots + A_nU_n.$$

Démonstration page 29

Remarques

- Les diviseurs communs à $A_1, \dots, A_n$ sont donc exactement les diviseurs de D.
- Ainsi, deux PGCD de $A_1, \dots, A_n$ se divisent mutuellement, donc sont associés.
- Lorsque D est non nul, c'est-à-dire lorsqu'au moins l'un des A_i est non nul, son degré est le plus grand parmi tous les degrés des diviseurs communs à $A_1, \dots, A_n$.
- Il y a unicité de D si on lui impose la condition supplémentaire d'être nul ou unitaire. On l'appelle *le* PGCD de $A_1, \dots, A_n$ et on le note $A_1 \wedge \cdots \wedge A_n$.
- De la même façon, on pourrait définir un **PPCM** de $A_1, \dots, A_n$ comme un générateur M de l'idéal $A_1\mathbb{K}[X] \cap \cdots \cap A_n\mathbb{K}[X]$, de façon à avoir, pour tout $P \in \mathbb{K}[X]$, l'équivalence :

$$P \in M\mathbb{K}[X] \iff \big(\forall i \in [\![1, n]\!] \quad P \in A_i\mathbb{K}[X]\big).$$

L'unique polynôme nul ou unitaire associé à M est appelé *le* PPCM de $A_1, \dots, A_n$.

Ex. 27. Deux polynômes A et B sont premiers entre eux si, et seulement si, $A \wedge B = 1$.

3 Théorème de Gauss et décomposition en produit d'irréductibles

Théorème 31 (Lemme de Gauss)

Soit A, B et C trois éléments de $\mathbb{K}[X]$.

Si A divise BC et si A est premier avec B, alors A divise C.

Démonstration page 29

Principe de démonstration. Multiplier par C une relation de Bézout $AU + BV = 1$.

Corollaire 32

Un polynôme est premier avec un produit si, et seulement s'il est premier avec chacun des facteurs.

Démonstration page 30

Théorème 33

Tout polynôme non constant de $\mathbb{K}[X]$ est produit d'irréductibles.

Démonstration page 30

Principe de démonstration. Récurrence forte sur le degré de P.

Notons $\mathcal{P}$ l'ensemble des polynômes irréductibles unitaires. Les éléments de $\mathcal{P}$ sont donc deux à deux non associés et tout polynôme irréductible est associé à un unique élément de $\mathcal{P}$.

Théorème 34

Tout polynôme A non nul de $\mathbb{K}[X]$ s'écrit de façon unique sous la forme :

$$A = \lambda \prod_{P \in \mathcal{P}} P^{\alpha_P}$$

où $\lambda \in \mathbb{K}^*$ et $(\alpha_P)_{P \in \mathcal{P}}$ est une famille presque nulle d'entiers naturels.

Démonstration page 30.

Point méthode Dans la pratique, on écrit la décomposition en produit d'irréductibles d'un polynôme A non nul sous l'une des formes :

- $A = \lambda P_1^{\alpha_1} \cdots P_k^{\alpha_k}$ où $k \in \mathbb{N}$, $\lambda \in \mathbb{K}^*$, $P_1, \ldots, P_k$ sont des éléments de $\mathcal{P}$ distincts deux à deux et $\alpha_1, \ldots, \alpha_k$ des entiers naturels non nuls ;
- $A = \lambda P_1^{\alpha_1} \cdots P_k^{\alpha_k}$ où $k \in \mathbb{N}$, $\lambda \in \mathbb{K}^*$, $P_1, \ldots, P_k$ sont des éléments de $\mathcal{P}$ distincts deux à deux et $\alpha_1, \ldots, \alpha_k$ des entiers naturels éventuellement nuls.

Avec la deuxième forme, on peut utiliser les mêmes irréductibles pour plusieurs éléments de $\mathbb{K}[X]$.

Ex. 28. Soit A et B deux éléments non nuls de $\mathbb{K}[X]$ décomposés sous la deuxième forme :

$$A = \lambda P_1^{\alpha_1} \cdots P_k^{\alpha_k} \qquad \text{et} \qquad B = \mu P_1^{\beta_1} \cdots P_k^{\beta_k}.$$

- $B \mid A$ si, et seulement si, $\forall i \in [\![1, k]\!] \quad \beta_i \leqslant \alpha_i$;
- le PGCD de A et B est $D = P_1^{\min(\alpha_1, \beta_1)} \cdots P_k^{\min(\alpha_k, \beta_k)}$;
- le PPCM de A et B est $M = P_1^{\max(\alpha_1, \beta_1)} \cdots P_k^{\max(\alpha_k, \beta_k)}$.

On a ainsi $AB = \lambda \mu DM$.

III Algèbres

Dans toute cette section, on suppose que $\mathbb{K}$ est un sous-corps de $\mathbb{C}$.

1 Structure d'algèbre

Définition 6

Une **algèbre** est un espace vectoriel A muni d'une structure d'anneau dont les deux multiplications (interne et externe) vérifient la propriété de compatibilité :

$$\forall (\lambda, x, y) \in \mathbb{K} \times A \times A \quad \lambda(x \times y) = (\lambda x) \times y = x \times (\lambda y). \qquad (*)$$

Lorsque le produit est commutatif, on dit que l'algèbre est **commutative**.

Remarques

- De même que pour les espaces vectoriels, on peut préciser « $\mathbb{K}$-algèbre » pour spécifier le corps de base.
- Comme dans un anneau, la multiplication interne sera souvent notée implicitement xy au lieu de $x \times y$.

Ex. 29. $\mathbb{K}$, $\mathbb{K}^{\mathbb{N}}$, $\mathcal{F}(X, \mathbb{K})$ (pour X un ensemble quelconque) constituent des $\mathbb{K}$-algèbres.

Ex. 30. $\mathbb{K}[X]$, $\mathbb{K}(X)$, et $\mathcal{M}_n(\mathbb{K})$ sont des $\mathbb{K}$-algèbres pour les lois usuelles, ainsi que $\mathcal{L}(E)$ (E étant un $\mathbb{K}$-espace vectoriel quelconque).

Proposition 35

Soit A un $\mathbb{K}$-espace vectoriel muni d'une multiplication interne $(x,y) \mapsto x \times y$.

Exo 1.13

Alors A est une $\mathbb{K}$-algèbre si, et seulement si, ce produit est bilinéaire, associatif et si A possède un élément neutre multiplicatif.

Démonstration. Il suffit de montrer que la bilinéarité du produit, c'est-à-dire les relations :

$$x \times (\lambda y + \mu z) = \lambda(x \times y) + \mu(x \times z) \qquad \text{et} \qquad (\lambda x + \mu y) \times z = \lambda(x \times z) + \mu(y \times z) \quad (**)$$

est équivalente à la distributivité et à la propriété $(*)$ de compatibilité.

- En supposant $(**)$, on obtient la distributivité en prenant $\lambda = \mu = 1$ et la relation $(*)$ en prenant $\mu = 0$.
- Supposons la distributivité et $(*)$. Alors, pour tout $(x,y,z) \in A^3$ et $(\lambda, \mu) \in \mathbb{K}^2$:

$$\begin{aligned} x \times (\lambda y + \mu z) &= x \times (\lambda y) + x \times (\mu z) \quad \text{par distributivité} \\ &= \lambda(x \times y) + \mu(x \times z) \quad \text{par la relation } (*) \end{aligned}$$

et de même pour la deuxième relation de $(**)$. □

Attention Comme c'est déjà le cas pour un anneau, une algèbre est **unitaire**, c'est-à-dire possède un élément neutre multiplicatif.

2 Sous-algèbres

Définition 7

Une **sous-algèbre** d'une algèbre A est un sous-espace vectoriel de A stable par multiplication et contenant 1_A.

Remarques

- Autrement dit, une sous-algèbre est une partie de A stable par combinaison linéaire, par multiplication et contenant l'élément neutre multiplicatif 1_A.
- Une sous-algèbre est naturellement munie d'une structure d'algèbre pour les lois induites.
- Dans la plupart des cas, on démontre qu'un ensemble est muni d'une structure d'algèbre en montrant que c'est une sous-algèbre d'une algèbre connue.

Ex. 31. Si A est une algèbre, alors $\mathrm{Vect}(1_A)$ est une sous-algèbre de A.

Ex. 32. L'ensemble des suites convergentes à termes dans $\mathbb{K}$ est une sous-algèbre de $\mathbb{K}^{\mathbb{N}}$.

Ex. 33. Si I est un intervalle de $\mathbb{R}$, $\mathcal{C}(I,\mathbb{R})$ est une sous-algèbre de $\mathcal{F}(I,\mathbb{R})$.

Ex. 34. Dans $\mathcal{M}_n(\mathbb{K})$, l'ensemble des matrices triangulaires supérieures est une sous-algèbre. De même pour les matrices triangulaires inférieures ou les matrices diagonales, mais pas pour les matrices symétriques lorsque $n \geqslant 2$ (un produit de deux matrices symétriques est symétrique si, et seulement si, elles commutent).