# Mathématiques
## tout-en-un

j'intègre

TOUT-EN UN

# MP|MP*

**C. Deschamps, F. Moulin, A. Warusfel**
N. Cleirec, Y. Gentric, F. Lussier,
C. Mullaert, S. Nicolas, M. Volker

# Mathématiques tout-en-un

DUNOD

Conception et création de couverture : Atelier 3+



© Dunod, 2016
5 rue Laromiguière, 75005 Paris
www.dunod.com
ISBN 978-2-10-071361-5

# Préface

La réforme du lycée, qui a suivi celle du collège, s'est achevée en 2012, avec la mise en œuvre des nouvelles classes de terminale. Depuis septembre 2013, les étudiants qui entreprennent des études en classes préparatoires, ont bénéficié, durant leur scolarité au collège et au lycée, de programmes rénovés, en particulier en mathématiques. Afin d'assurer une continuité, de nouveaux programmes de classes préparatoires étaient donc indispensables.
En mathématiques, en 1995, lors de la mise en place des programmes de l'époque, les Éditions Dunod nous avaient confié la tâche de fournir aux étudiants des ouvrages de référence clairs et précis complétant le cours, irremplaçable, du professeur. Nous avions alors tenté un pari : faire tenir exposés et exercices, avec corrigés, en un seul volume, le premier « tout-en-un » (depuis très largement imité), qui a remporté un grand succès.
En septembre 2013 ont été mis en place de nouveaux programmes des classes préparatoires et, avec une équipe partiellement renouvelée et de grande qualité, nous avons récidivé : deux ouvrages « tout en un » (MPSI et PCSI-PTSI) proposent, aux étudiants de première année, un cours en conformité avec le texte, mais aussi avec l'esprit, du nouveau programme des classes préparatoires.
Aujourd'hui ce nouveau « tout en un » MP prolonge, pour la seconde année, l'ouvrage MPSI et il conserve l'ambition, en mettant en œuvre de nouvelles méthodes d'acquisition des connaissances, de proposer à l'étudiant une démarche pour s'approprier les théories du programme, théories indispensables tant aux mathématiques qu'aux autres disciplines.

En pratique, dans chaque chapitre :

- De très nombreux exemples, souvent simples et issus de connaissances du lycée ou du programme de première année, illustrent chaque définition et permettent à l'étudiant de s'approprier cette nouvelle notion.
- Les propositions et théorèmes sont énoncés et suivis immédiatement d'exemples élémentaires d'applications. En outre, leurs démonstrations sont l'occasion d'un travail personnel de l'étudiant. Nous avons choisi de ne pas faire figurer systématiquement, à la suite des énoncés, la rédaction complète de ces démonstrations mais plutôt d'indiquer à l'étudiant le principe de celles-ci avec les éléments qui lui permettront de la construire par lui-même et ainsi de mieux s'approprier la propriété. Évidemment, guidé par un renvoi précis en fin du chapitre, il pourra ensuite consulter la démonstration complète et vérifier ou compléter son travail personnel.

- Lorsque plusieurs preuves étaient possibles, nous avons choisi de ne pas privilégier systématiquement la plus courte, souvent au profit de constructions explicites. C'est volontaire ; durant leurs études au lycée nos étudiants n'ont en général pas construit les objets mathématiques qu'ils ont utilisés : ils se sont contentés d'en admettre les propriétés. Or construire un objet, comme le fait un artisan, c'est se l'approprier, connaître parfaitement ses propriétés et les limites de ces propriétés.
- Dans chaque chapitre, l'étudiant trouvera, pour illustrer immédiatement l'usage des propositions et théorèmes, de très nombreux exercices simples qu'il doit évidemment chercher au fur et à mesure de son apprentissage et dont il pourra consulter une solution en fin de chapitre afin de vérifier son propre travail.
- Régulièrement l'étudiant trouvera des « point méthode » qui, pour une situation donnée, lui offrent une ou deux possibilités d'approche de la résolution de son problème. Évidemment il trouvera après ce « point méthode » exemples et exercices l'illustrant.
- À l'issue de chaque chapitre, figurent des exercices plus ambitieux, demandant plus de réflexion, à chercher une fois le chapitre totalement maitrisé. Certains plus difficiles sont signalés par des étoiles ; les solutions détaillées de tous ces exercices complémentaires sont données.
- Enfin les étudiants de classes préparatoires de seconde année sont candidats aux concours des grandes écoles. Nous avons réunis des exercices posés aux premiers oraux portant sur les nouveaux programmes : l'étudiant trouvera des exercices posés aux oraux des concours 2015. Les chercher (et les résoudre) sera pour lui un excellent entraînement.
- Bien entendu nous sommes très intéressés par toute remarque que les étudiants, nos collègues, tout lecteur... seraient amenés à nous communiquer. 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.

Un grand merci à tous les auteurs de cet ouvrage d'avoir mené à terme ce travail de longue haleine.

Claude Deschamps et François Moulin

*Nathalie tu nous manques !*

*Notre collègue et amie Nathalie Cleirec*
*nous a quittés le 17 novembre 2015.*
*Enseignante de grande qualité,*
*elle était très attachée à ses étudiants*
*et faisait tout pour leur réussite.*

*Toute l'équipe de cet ouvrage*
*se souvient de sa gentillesse et de son travail :*
*une participation active aux réunions du groupe*
*et une rédaction remarquable des chapitres*
*dont elle avait la responsabilité.*

# Table des matières

# Chapitre 1 : Groupes, anneaux, arithmétique, algèbres

# Groupes, anneaux, arithmétique, algèbres


Nous revenons dans ce chapitre sur les structures algébriques usuelles vues en première année : groupes, anneaux et corps, notamment en vue de leur utilisation en arithmétique (sur $\mathbb{Z}$ et sur $\mathbb{K}[X]$).
Nous finirons par la notion d'*algèbre*, très présente en analyse, et dont les applications en algèbre linéaire seront étudiées dans le chapitre de réduction des endomorphismes.
Dans ce chapitre, nous supposons acquises les notions de groupe, de sous-groupe, d'anneaux et de corps vues en première année.

# I Anneaux et corps

## 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.
- Rappelons que, par définition, un corps est un anneau commutatif non trivial dans lequel tout élément non nul est inversible.

## 2 Anneaux intègres

**Définition 1**

Un anneau **intègre** est un anneau $A$ *commutatif non trivial* qui vérifie :

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

**Exemples**

1. $\mathbb{Z}$ est un anneau intègre.
2. Tout corps est un anneau intègre.

p.35 **Exercice 1** Donner un exemple d'anneau commutatif non trivial et non intègre.

**Point méthode**

Dans un anneau $A$ intègre tout élément $a$ non nul est **régulier** pour la multiplication, c'est-à-dire vérifie :

$$\forall (x,y) \in A^2 \quad a\,x = a\,y \Longrightarrow x = y.$$

**Exemple** Tout anneau fini intègre est un corps.
En effet, soit $A$ un anneau fini intègre et $a \in A$ non nul. L'application $x \mapsto a\,x$ de $A$ dans $A$ est injective par régularité 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 $a\,b = 1$. Comme $A$ est commutatif (puisqu'intègre), on a aussi $b\,a = 1$ et $a$ est inversible.

p.35 **Exercice 2** Montrer que dans l'anneau des fonctions continues de $\mathbb{R}$ dans $\mathbb{R}$, toute fonction polynomiale non nulle est régulière.

## 3 Sous-anneaux — sous-corps

**Définition 2**

Un **sous-anneau** d'un anneau $A$ est un sous-groupe additif de $A$ stable par multiplication et contenant $1_A$.

**Point méthode**

Pour montrer qu'une partie d'un anneau $A$ est un sous-anneau de $A$, il suffit de vérifier qu'elle est stable par les deux lois de $A$ par passage à l'opposé, et qu'elle contient l'élément neutre multiplicatif $1_A$.

En effet, il ne manque que la présence de l'élément neutre $0_A$, que l'on obtient par différence : $0_A = 1_A - 1_A$.

**Définition 3**

Un sous-corps d'un corps $\mathbb{K}$ est un sous-anneau de $\mathbb{K}$ qui est un corps.

**Exemples**

1. $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$.
2. L'ensemble des matrices triangulaires supérieures d'ordre $n$ est un sous-anneau de $\mathcal{M}_n(\mathbb{K})$.
3. $\mathbb{Z} + i\,\mathbb{Z}$ est un sous-anneau de $\mathbb{C}$.
4. $\mathbb{Q}$ et $\mathbb{R}$ sont des sous-corps de $\mathbb{C}$.

**Proposition 1**

Si $B$ est un sous-anneau de $A$ et $C$ un sous-anneau de $B$, alors $C$ est un sous-anneau de $A$.

**Démonstration.**

C'est immédiat à partir de la caractérisation donnée dans le point méthode ci-dessus. □

**Attention**

- La définition d'un sous-anneau impose qu'il contienne $1_A$. Cette vérification est indispensable car elle n'est pas une conséquence des autres axiomes comme le montrent les exemples de l'ensemble des matrices triangulaires supérieures strictes de $\mathcal{M}_n(\mathbb{K})$, ou plus simplement $\{0_A\}$ lorsque $A$ est un anneau non trivial.
- Ce même exemple $\{0_A\}$ montre que, contrairement à ce qui se passe pour les sous-groupes, une partie d'un anneau $A$ stable par les lois de $A$ et qui, munie des lois induites, est un anneau, n'est pas nécessairement un sous-anneau de $A$ (les deux éléments neutres multiplicatifs peuvent être différents). Voir aussi l'exercice 1.1 de la page 51.

## 4 Morphismes d'anneaux

**Définition 4**

Soit $A$ et $B$ deux anneaux. On dit qu'une application $\varphi : A \to B$ est un **morphisme d'anneaux** si elle vérifie :

$$\begin{aligned} &\forall (a,b) \in A^2 \quad \varphi(a+b) = \varphi(a) + \varphi(b) \\ &\forall (a,b) \in A^2 \quad \varphi(a\,b) = \varphi(a)\,\varphi(b) \\ &\qquad\qquad\quad \varphi(1_A) = 1_B. \end{aligned}$$

**Remarques**

- La première des conditions ci-dessus est en fait la définition d'un morphisme de groupes de $(A,+)$ dans $(B,+)$ (voir page 21). Un morphisme d'anneaux est donc en particulier un morphisme de groupes.
- Un morphisme d'anneaux $\varphi$ de $A$ dans $B$ vérifie l'égalité $\varphi(0) = 0$.

  En effet :

  $$\varphi(0) = \varphi(0+0) = \varphi(0) + \varphi(0)$$

  et en ajoutant $-\varphi(0)$ des deux côtés, on obtient $0 = \varphi(0)$. Alors, si $x \in A$, on a $\varphi(x) + \varphi(-x) = \varphi(0) = 0$ ce qui montre que $\varphi(-x) = -\varphi(x)$.

  Ce sont également des propriétés générales des morphismes de groupes.

**Attention** En revanche, l'égalité $\varphi(1) = 1$ de la définition précédente n'est pas une conséquence des autres axiomes comme le montre l'exemple de la fonction nulle lorsque $B \neq \{0\}$.

**Définition 5**

Un **isomorphisme d'anneaux** est un morphisme d'anneaux bijectif.

**Proposition 2**

Si $\varphi$ est un isomorphisme d'anneaux, alors $\varphi^{-1}$ est également un isomorphisme d'anneaux.

Démonstration page 35

**Proposition 3**

Soit $f$ un morphisme d'anneaux de $A$ dans $B$.

1. L'image par $f$ de tout sous-anneau de $A$ est un sous-anneau de $B$.
2. L'image réciproque par $f$ de tout sous-anneau de $B$ est un sous-anneau de $A$.

Démonstration page 35

**Exemple** Soit $f : A \to B$ un morphisme d'anneaux.
L'**image** de $f$ est le sous-anneau $f(A)$ de $B$.
Évidemment, $f$ est surjectif si, et seulement si, son image est égale à $B$.

**Définition 6 (Noyau)**

Le **noyau** d'un morphisme d'anneaux $f : A \to B$ est :

$$\operatorname{Ker} f = \{x \in A \mid f(x) = 0_B\}.$$

p.35

**Exercice 3** Montrer qu'un morphisme d'anneaux est injectif si, et seulement si, son noyau est réduit à $\{0\}$.

**Attention** Le noyau d'un morphisme d'anneaux n'est pas en général un sous-anneau (voir ci-dessous la notion d'idéal) comme le montre l'exercice suivant.

p.36

**Exercice 4** Montrer que le noyau d'un morphisme d'anneaux $f : A \to B$ est un sous-anneau de $A$ si, et seulement si, $B$ est trivial.

# 5 Anneaux produit

Étant donné des anneaux $A_1, \dots, A_n$, on munit le produit cartésien $A_1 \times \cdots \times A_n$ d'une structure d'anneau par opérations terme à terme :

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

Les deux éléments neutres sont naturellement $(0_{A_1}, \dots, 0_{A_n})$ et $(1_{A_1}, \dots, 1_{A_n})$.

p.36

**Exercice 5**

1. Écrire de même l'opposé d'un élément du produit cartésien.
2. Quels sont les inversibles d'un anneau produit ?
3. À quelle condition l'anneau produit $A \times B$ est-il un corps ?
4. À quelle condition l'anneau produit $A \times B$ est-il intègre ?

# 6 Idéaux d'un anneau commutatif

## Introduction

Si $\varphi$ est un morphisme d'anneaux de $A$ dans $B$, l'image de $\varphi$ est un sous-anneau de $B$ mais son noyau n'est pas un sous-anneau de $A$, sauf si $B$ est trivial (voir l'exercice 4 de la page précédente).
Mais $\operatorname{Ker}\varphi$ est un sous-groupe de $(A, +)$ qui possède la propriété suivante :

$$\forall x \in \operatorname{Ker}\varphi \quad \forall a \in A \quad (a\,x, x\,a) \in (\operatorname{Ker}\varphi)^2$$

puisque si $x \in \operatorname{Ker}\varphi$ et $a \in A$, on a $\varphi(a\,x) = \varphi(a)\,\varphi(x) = \varphi(a) \times 0 = 0$ et de même pour $\varphi(x\,a)$.
Cela caractérise la notion d'**idéal bilatère**.
Conformément au programme, on se place dans toute la suite dans le cadre des anneaux commutatifs.

**Définition 7 (Idéal d'un anneau commutatif)**

Soit $A$ 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 :

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

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

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

**Exemples**

1. Nous venons de voir que le noyau d'un morphisme d'anneaux de $A$ (commutatif) dans $B$ est un idéal de $A$.
2. Si $A$ est un anneau commutatif, alors $A$ et $\{0\}$ sont évidemment des idéaux de $A$.
3. L'ensemble des fonctions nulles sur une partie $X$ de $\mathbb{R}$ est un idéal de $\mathcal{F}(\mathbb{R},\mathbb{R})$.

p.36

**Exercice 6** Montrer que les suites réelles convergeant vers 0 constituent un idéal de l'anneau des suites réelles bornées.

S'agit-il d'un idéal de l'anneau de toutes les suites réelles ?

**Remarque** Soit $I$ un idéal de $A$ contenant 1.
Alors, pour tout $a \in A$, on a $a = a.1 \in I$, donc $I = A$.

p.37

**Exercice 7**

1. Montrer plus généralement qu'un idéal contenant un élément inversible de $A$ est égal à $A$.
2. Quels sont les idéaux d'un corps ?

## Opérations sur les idéaux

Soit $A$ un anneau commutatif.

**Proposition 4**

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

Démonstration page 37

p.37

**Exercice 8** Étant donné une partie $X$ de $A$, montrer qu'il existe un plus petit idéal de $A$ contenant $X$.

On l'appelle **idéal de $A$ engendré par $X$**.

**Exemple : idéal engendré par un élément** Soit $x \in A$. Décrivons l'idéal engendré par $x$, c'est-à-dire par $\{x\}$ (*cf.* exercice précédent). Par définition, pour tout idéal $I$ contenant $x$ et pour tout $a \in A$, on a $a\,x \in I$, donc $I$ contient $x\,A = \{x\,a\,;\ a \in A\}$. Montrons que $x\,A$ est le plus petit idéal de $A$ contenant $x$.

- Il contient $0 = x \times 0$ et il est stable par $+$ et $-$ puisque pour tout $(a,b) \in A$ :

$$x\,a + x\,b = x\,(a+b) \in x\,A \qquad \text{et} \qquad -(x\,a) = x\,(-a) \in x\,A.$$

  Donc $x\,A$ est un sous-groupe de $(A,+)$.
- Pour tout $y = x\,a \in x\,A$ et $b \in A$, on a $y\,b = x\,(a\,b) \in x\,A$. Donc $x\,A$ est un idéal.
- Comme $x = x \times 1_A$, on a bien $x \in x\,A$.
- Enfin, on a vu plus haut que tout idéal de $A$ contenant $x$ contenait aussi $x\,A$.

p.37

**Exercice 9** Montrer qu'un anneau commutatif $A$ non trivial n'ayant que les deux idéaux $A$ et $\{0\}$ est un corps (réciproque de la deuxième question de l'exercice 7 de la page précédente).

**Proposition 5**

Si $I_1$ et $I_2$ sont deux idéaux de $A$, leur **somme** :

$$I_1 + I_2 = \{x_1 + x_2\,;\ (x_1, x_2) \in I_1 \times I_2\}$$

est un idéal de $A$.

C'est le plus petit idéal de $A$ contenant $I_1$ et $I_2$.

Démonstration page 37

### Idéaux de $\mathbb{Z}$

**Exemple** Pour tout $n \in \mathbb{Z}$, l'ensemble $n\,\mathbb{Z} = \{n\,k\,;\ k \in \mathbb{Z}\}$ des multiples de $n$ est un idéal de $\mathbb{Z}$. C'est l'idéal de $\mathbb{Z}$ engendré par $n$ (voir l'exemple de la page précédente).

**Remarque**

Comme $n\,\mathbb{Z} = (-n)\,\mathbb{Z}$ pour tout $n \in \mathbb{Z}$, on peut se limiter à $n \in \mathbb{N}$.
Nous allons voir qu'en fait ce sont les seuls idéaux de $\mathbb{Z}$.

**Lemme 6**

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

**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 $n$.

Démonstration page 37

Un idéal étant en particulier un sous-groupe, on en déduit le résultat important suivant.

**Théorème 7**

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

## 7 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 :

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

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 :

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

**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 notée $\overline{k}$.

p.38 **Exercice 10** Qu'est-ce que $\mathbb{Z}/0\mathbb{Z}$ ? $\mathbb{Z}/1\mathbb{Z}$ ? $\mathbb{Z}/2\mathbb{Z}$ ?

**Proposition 8**

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

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

**Principe de démonstration.** Utiliser la division euclidienne par $n$. Démonstration page 38

**Remarque** $\mathbb{Z}/n\mathbb{Z}$ est appelé **ensemble quotient** de $\mathbb{Z}$ par $n\,\mathbb{Z}$, ce qui explique sa notation.

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

**Proposition 9**

1. Il existe sur $\mathbb{Z}/n\mathbb{Z}$ des lois, notées $+$ et $\times$ (ou implicitement pour le produit) et appelées **lois quotient**, telles que :
$$\forall (x,y) \in (\mathbb{Z}/n\mathbb{Z})^2 \quad \overline{x} + \overline{y} = \overline{x+y} \quad \text{et} \quad \overline{x} \times \overline{y} = \overline{x\,y}.$$
2. $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif d'éléments neutres $\overline{0}$ et $\overline{1}$.
3. La projection canonique $\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ x & \longmapsto & \overline{x} \end{array}$ est un morphisme d'anneaux surjectif de noyau $n\,\mathbb{Z}$.

**Principe de démonstration.** Pour $\alpha$ et $\beta$ dans $\mathbb{Z}/n\mathbb{Z}$, on définit :

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

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

Démonstration page 38

### Remarques

- On peut aussi prendre pour représentants des classes modulo $n \neq 0$, 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 $\mathbb{Z}/5\mathbb{Z} = \{\overline{0}, \pm\overline{1}, \pm\overline{2}\}$.

- Les éléments $0, 1, \ldots, n-1$ sont privilégiés dans leurs classes respectives. Il arrivera donc que l'on note $p$ à la place de $\overline{p}$ lorsque $0 \leqslant p < n$, s'il n'y a pas de confusion possible.

p.39

**Exercice 11** Écrire les tables d'addition et de multiplication de $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$.

Ces anneaux sont-ils intègres ?

**Proposition 10 (Éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$)**

1. La classe de $k \in \mathbb{Z}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si, et seulement si, $k$ est premier avec $n$.
2. Pour $n \in \mathbb{N}^*$, les assertions suivantes sont équivalentes :
   - $(i)$ $\mathbb{Z}/n\mathbb{Z}$ est un corps ;
   - $(ii)$ $\mathbb{Z}/n\mathbb{Z}$ est intègre ;
   - $(iii)$ $n$ est premier.

**Principe de démonstration.** Démonstration page 39

1. L'élément $\overline{k}$ est inversible si, et seulement s'il existe $(u, v) \in \mathbb{Z}^2$ tel que $k\,u + n\,v = 1$ et son inverse est alors $\overline{u}$.
2. On montre $(ii) \Longrightarrow (iii)$ par contraposée : si $n = a\,b$, alors $\overline{a}\,\overline{b} = \overline{0}$.
   $(iii) \Longrightarrow (i)$ : si $n$ est premier, tous les éléments de $[\![1, n-1]\!]$ sont premiers avec $n$.

### Remarque

L'implication $(ii) \Longrightarrow (i)$ est un cas particulier de l'exemple de la page 3.

### Point méthode

Comme on l'a vu dans la démonstration précédente, pour déterminer l'inverse de $\overline{k}$ dans $\mathbb{Z}/n\mathbb{Z}$, il suffit de trouver un couple $(u, v)$ tel que $k\,u + n\,v = 1$ (coefficients de Bézout). L'inverse de $\overline{k}$ est alors $\overline{u}$.

p.40

**Exercice 12** Donner l'inverse de $\overline{13}$ dans $\mathbb{Z}/34\mathbb{Z}$.

## 8 Théorème chinois

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

**Proposition 11**

Soit $n$ et $m$ des entiers 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 $\varphi$ :

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

**Principe de démonstration.** Pour la définition de $\varphi$, 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 $\varphi$ et l'on conclut par cardinalité. Démonstration page 40

Le corollaire suivant n'est que la traduction en termes de congruence de la proposition 11.

**Corollaire 12 (Théorème chinois)**

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

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

et les solutions de ce système sont exactement les entiers congrus à $k$ modulo $n\,m$.

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 $m\,u + n\,v = 1$, on trouve deux entiers $k_1 = m\,u$ et $k_2 = n\,v$ vérifiant respectivement les systèmes de congruences :

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

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

**Remarque** L'obtention d'une telle solution est non triviale, mais sa vérification est immédiate. Il ne faut donc pas oublier de la faire pour repérer une erreur de calcul éventuelle.

**Exemple** Trouvons les entiers $k$ tels que $k^2+k+11 \equiv 0 \quad [143]$, c'est-à-dire tels que $k^2+k+11 \equiv 0 \quad [11]$ et $k^2+k+11 \equiv 0 \quad [13]$.
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.

p.40

**Exercice 13** Finir l'exemple ci-dessus.

# 9 Indicatrice d'Euler

**Définition 8**

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

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

### 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 $\mathbb{Z}/n\mathbb{Z}$.

### Exemples

1. 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 s'ils sont tous premiers avec $n$.
2. Soit $p$ un nombre premier. Pour tout $k \in \mathbb{N}^*$, on a $\varphi(p^k) = p^k - p^{k-1}$ puisque 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 $p^{k-1}$.

p.40

**Exercice 14** Soit $n \in \mathbb{N}^*$. Montrer :

$$\sum_{d|n} \varphi(d) = n.$$

*Indication : on pourra considérer l'ensemble des rationnels de la forme $p/n$, avec $p \in [\![1,n]\!]$.*

**Proposition 13**

Si $n$ et $m$ sont premiers entre eux, alors on a $\varphi(n\,m) = \varphi(n)\,\varphi(m)$.

**Démonstration.** Les anneaux $\mathbb{Z}/(nm)\mathbb{Z}$ et $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ étant isomorphes (théorème chinois), ils ont autant d'éléments inversibles.

Or, les inversibles de l'anneau produit $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ sont évidemment les couples $(u, v)$, où $u$ et $v$ sont inversibles respectivement dans $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}$. On en déduit le résultat. □

**Corollaire 14**

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.** Le résultat est immédiat si $n = 1$ (un produit vide vaut 1). Sinon, $r \geqslant 1$ et puisque les $p_k^{\alpha_k}$ sont premiers entre eux deux à deux, $p_r^{\alpha_r}$ est premier avec $p_1^{\alpha_1} \cdots p_{r-1}^{\alpha_{r-1}}$. À partir de la proposition précédente, on a $\varphi(n) = \varphi(p_1^{\alpha_1} \cdots p_{r-1}^{\alpha_{r-1}})\,\varphi(p_r^{\alpha_r})$.

On en déduit $\varphi(n) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_r^{\alpha_r})$ par récurrence immédiate, sur le nombre de facteurs premiers de $n$. À l'aide du résultat de l'exemple 2 de la page ci-contre, il vient :

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

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

**Calcul de l'indicatrice d'Euler à l'aide d'une méthode de crible** On peut adapter le crible d'Eratosthène (voir livre de première année) pour calculer l'indicatrice d'Euler des $n$ premiers entiers. Cela consiste à multiplier chaque entier $k$ par $1 - \frac{1}{p}$, pour tous les diviseurs premiers $p$ de $k$.

```
    """ Retourne la liste des phi(p)
        pour p in [0,n]"""
    t=list(range(n+1))  # initialement, t[p]=p pour tout p
    for p in range(2,n):
        if t[p] == p: # p est premier
            for k in range(p,n+1,p):
                # on multiplie les multiples
                # de p par 1-1/p
                t[k] -= t[k] // p
    return t
```

# II Anneau des polynômes à une indéterminée

On considère un corps $\mathbb{K}$ (dans la pratique, un sous-corps 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.

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

**Proposition 15**

$\mathbb{K}[X]$ est un anneau intègre.

**Démonstration.** Il est clair que $\mathbb{K}[X]$ est un anneau commutatif non réduit à $\{0\}$.

Soit $A$ et $B$ deux polynômes non nuls. Écrivons :

$$A = \sum_{i=0}^{p} a_i X^i \quad \text{et} \quad B = \sum_{j=0}^{q} b_j X^j \qquad \text{avec} \qquad p = \deg A \quad \text{et} \quad q = \deg B.$$

Par définition du produit, le coefficient du terme de degré $n = p + q$ de $AB$ est $a_p b_q$, donc non nul comme produit d'éléments non nuls du corps $\mathbb{K}$. Ainsi $AB \neq 0$. □

# 1 Propriétés arithmétiques élémentaires

## Divisibilité

**Définition 9**

Soit $(A, B) \in \mathbb{K}[X]^2$. On dit que $B$ **divise** $A$, ou que $A$ est un **multiple** de $B$, s'il existe $Q \in \mathbb{K}[X]$, appelé **quotient** de $A$ par $B$, tel que $A = BQ$. On note $B \mid A$.

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

**Proposition 16**

Les éléments inversibles de $\mathbb{K}[X]$ sont les éléments de $\mathbb{K}^*$.

Démonstration page 41

**Exemples**

1. Les diviseurs de 1 sont les éléments inversibles, c'est-à-dire les polynômes constants non nuls.
2. Tout élément de $\mathbb{K}[X]$ divise 0, mais 0 ne divise que lui-même.

## Polynômes associés

**Proposition 17**

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 41

**Exemples**
1. 0 n'est associé qu'à lui-même.
2. Les éléments inversibles de $\mathbb{K}[X]$ sont les associés de 1.

**Corollaire 18**

Tout élément non nul de $\mathbb{K}[X]$ est associé à un unique polynôme unitaire.

## Polynômes irréductibles

**Définition 10**

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

**Exemple** Tout polynôme de degré 1 est irréductible.

**Proposition 19**

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 41

**Rappel**
- 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.

**Exemple** Montrons que $P = X^3 + X + 1$ est irréductible dans $\mathbb{Q}[X]$.
Supposons $P = QR$, avec $Q$ et $R$ non constants. Alors l'un est de degré 2 et l'autre de degré 1. En particulier, l'un des deux, donc $P$ aussi, admet une racine dans $\mathbb{Q}$. Montrons que c'est impossible.
Soit $p$ et $q$ deux entiers premiers entre eux, avec $q \neq 0$, tels que $P(p/q) = 0$.
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 $P(-1) = -1 \neq 0$.

**Remarque** Plus généralement, un polynôme de $\mathbb{K}[X]$ de degré 2 ou 3 n'ayant aucune racine dans $\mathbb{K}$ est irréductible dans $\mathbb{K}[X]$.

p.41

**Exercice 15** Le polynôme $P = X^4 + X^2 + 1$

1. a-t-il des racines dans $\mathbb{C}$ ? dans $\mathbb{R}$ ? dans $\mathbb{Q}$ ?
2. est-il irréductible dans $\mathbb{C}[X]$ ? dans $\mathbb{R}[X]$ ? dans $\mathbb{Q}[X]$ ?

### Polynômes premiers entre eux

**Définition 11**

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

**Exemple** 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 20**

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 41

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

### Idéaux de $\mathbb{K}[X]$

Si $B$ est un élément de $\mathbb{K}[X]$, l'exemple de la page 7 montre que :

$$B\,\mathbb{K}[X] = \{B\,Q\,;\ Q \in \mathbb{K}[X]\}$$

est un idéal de $\mathbb{K}[X]$.
Comme dans le cas de $\mathbb{Z}$, on a ainsi obtenu tous les idéaux de $\mathbb{K}[X]$.

**Théorème 21**

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

**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 $B$.

Démonstration page 42

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 $\mathbb{K}[X]$.

#### Remarques

- Un **anneau principal** est un anneau intègre $A$ dans lequel tout idéal est principal, c'est-à-dire de la forme $x\,A$, pour un certain $x$ de $A$ (voir l'exemple de la page 7).
- L'anneau $\mathbb{K}[X]$ est ainsi un anneau principal, ainsi que $\mathbb{Z}$ d'après le théorème 7 de la page 8.

- Les résultats arithmétiques qui suivent utilisent cette propriété de principalité de $\mathbb{K}[X]$ et peuvent donc se généraliser à n'importe quel anneau principal (sauf l'algorithme d'Euclide qui utilise la division euclidienne).
- Le même schéma permettrait ainsi de retrouver les résultats classiques de l'arithmétique de $\mathbb{Z}$ en utilisant ses idéaux.

## Lien avec la divisibilité

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

**Proposition 22**

On a :

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

**Démonstration.** On a les équivalences immédiates :

$$B \mid A \iff \exists Q \in \mathbb{K}[X] \quad A = BQ \iff A \in B\,\mathbb{K}[X].$$

Il ne reste plus qu'à vérifier que $A\,\mathbb{K}[X] \subset B\,\mathbb{K}[X] \iff A \in B\,\mathbb{K}[X]$.

- L'implication $\Longrightarrow$ est évidente puisque $A \in A\,\mathbb{K}[X]$.
- Puisque $B\,\mathbb{K}[X]$ est un idéal, si $A \in B\,\mathbb{K}[X]$, alors $\forall Q \in \mathbb{K}[X] \quad AQ \in B\,\mathbb{K}[X]$, ce qui prouve l'implication $\Longleftarrow$. □

**Remarque** On en déduit, grâce à la proposition 17 de la page 14, que deux polynômes sont associés si, et seulement s'ils sont générateurs du même idéal.

**Corollaire 23**

Tout idéal $I$ de $\mathbb{K}[X]$ non réduit à $\{0\}$ est de la forme $A\,\mathbb{K}[X]$ pour un unique polynôme unitaire $A$.

Ce polynôme $A$ est appelé **le générateur** de $I$.

## PGCD

**Exemples** Soit $A$ et $B$ deux polynômes non nuls.

1. L'ensemble des multiples communs à $A$ et $B$ est $A\,\mathbb{K}[X] \cap B\,\mathbb{K}[X]$. Il s'agit donc d'un idéal de $\mathbb{K}[X]$, non nul puisque $AB$ lui appartient. Son générateur $M$ est appelé **le PPCM** de $A$ et $B$. C'est l'unique polynôme unitaire $M \in \mathbb{K}[X]$ tel que :
$$A\,\mathbb{K}[X] \cap B\,\mathbb{K}[X] = M\,\mathbb{K}[X]$$
c'est-à-dire vérifiant :
$$\forall P \in \mathbb{K}[X] \quad (A \mid P \quad \text{et} \quad B \mid P) \iff M \mid P.$$
2. De même que, pour le PPCM, on s'intéresse à $A\,\mathbb{K}[X] \cap B\,\mathbb{K}[X]$ qui est le plus grand idéal de $\mathbb{K}[X]$ contenu dans $A\,\mathbb{K}[X]$ et $B\,\mathbb{K}[X]$, pour le PGCD on va considérer le plus petit idéal de $\mathbb{K}[X]$ contenant $A\,\mathbb{K}[X]$ et $B\,\mathbb{K}[X]$, c'est-à-dire, d'après la proposition 5 de la page 8, leur somme $A\,\mathbb{K}[X] + B\,\mathbb{K}[X]$.

**Définition 12**

Soit $A$ et $B$ deux éléments de $\mathbb{K}[X]$ non tous les deux nuls.

On appelle **PGCD** de $A$ et $B$ le générateur $D$ de l'idéal $A\,\mathbb{K}[X]+B\,\mathbb{K}[X]$.

Il vérifie la relation :

$$\forall P \in \mathbb{K}[X] \quad (P \mid A \quad \text{et} \quad P \mid B) \iff P \mid D.$$

On a la **relation de Bézout** :

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

**Remarques**

- Parmi les diviseurs communs à $A$ et $B$, le PGCD est le polynôme unitaire de degré maximal.
- Si $A = 0$, le PGCD de $A$ et $B$ est le polynôme $B$ normalisé (c'est-à-dire divisé par son coefficient dominant).
- Rappelons que l'on peut obtenir le PGCD par l'algorithme d'Euclide :
  - tant que $B$ est non nul, on remplace $(A,B)$ par $(B,R)$, où $R$ est le reste de la division euclidienne de $A$ par $B$ ;
  - le PGCD recherché est alors $A$ divisé par son coefficient dominant.

**Remarque** La définition précédente se généralise naturellement à $k$ éléments $(A_1,\dots,A_k) \in \mathbb{K}[X]^k$ non tous nuls. L'ensemble :

$$\{A_1U_1 + A_2U_2 + \cdots + A_kU_k\,;\ (U_1,U_2,\dots,U_k) \in \mathbb{K}[X]^k\},$$

noté $A_1\,\mathbb{K}[X] + A_2\,\mathbb{K}[X] + \cdots + A_k\,\mathbb{K}[X]$, est un idéal de $\mathbb{K}[X]$. Son générateur $D$ est le **PGCD** de $(A_1,A_2,\dots,A_k)$ et on a la relation de Bézout :

$$\exists (U_1,U_2,\dots,U_k) \in \mathbb{K}[X]^k \quad D = A_1U_1 + A_2U_2 + \cdots + A_kU_k.$$

## Relation de Bézout

Par définition du PGCD, on a immédiatement les résultats suivants.

**Proposition 24**

Soit $(A,B) \in \mathbb{K}[X]^2$.

1. Si $D$ est le PGCD de $A$ et $B$, alors il existe $U$ et $V$ dans $\mathbb{K}[X]$ tels que $D = AU + BV$.
2. Les polynômes $A$ et $B$ sont premiers entre eux si, et seulement s'il existe $(U,V) \in \mathbb{K}[X]^2$ tel que $AU + BV = 1$.

**Démonstration.** Seule la réciproque du deuxième point reste à démontrer. Si $AU+BV=1$, tout diviseur commun à $A$ et $B$ divise $AU+BV$ donc $1$. On en déduit que les seuls diviseurs communs à $A$ et $B$ sont les polynômes constants non nuls, donc que $A$ et $B$ sont premiers entre eux. □