

# ANNEAUX ET ARITHMÉTIQUE

## 1 Compléments sur les anneaux

### 1.1 Produit d'anneaux

#### Proposition 1.1 Produit d'anneaux

Soient  $(A_i, +_i, \times_i)_{1 \leq i \leq n}$  une famille finie d'anneaux. Alors on peut munir  $\prod_{i=1}^n A_i$  d'une structure d'anneaux en posant :

$$\forall (a, b) \in \left( \prod_{i=1}^n A_i \right)^2, a + b = (a_i +_i b_i)_{1 \leq i \leq n} \quad \forall (a, b) \in \left( \prod_{i=1}^n A_i \right)^2, a \times b = (a_i \times_i b_i)_{1 \leq i \leq n}$$

On a alors  $0_A = (0_{A_i})_{1 \leq i \leq n}$  et  $1_A = (1_{A_i})_{1 \leq i \leq n}$ .

### 1.2 Idéaux d'un anneau commutatif

#### Définition 1.1 Idéal d'un anneau commutatif

Soit  $(A, +, \times)$  un anneau commutatif. On dit qu'une partie  $I$  de  $A$  est un **idéal** de  $A$  si

- (i)  $I$  est un sous-groupe de  $(A, +)$ ;
- (ii)  $I$  est **absorbant** : pour tout  $(a, x) \in A \times I$ ,  $a \times x \in I$ .

#### Exemple 1.1

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

**REMARQUE.** Si  $1_A \in I$ , alors  $I = A$ .



**ATTENTION !** Un idéal n'est pas forcément un sous-anneau. Par exemple,  $2\mathbb{Z}$  est un idéal de  $\mathbb{Z}$  mais n'est pas un sous-anneau de  $\mathbb{Z}$ .

Un sous-anneau n'est pas forcément un idéal. Par exemple,  $\mathbb{R}$  est un sous-anneau de  $\mathbb{C}$  mais n'est pas un idéal de  $\mathbb{C}$ . En fait, la seule partie d'un anneau qui est à la fois un sous-anneau et un idéal est l'anneau lui-même.

#### Proposition 1.2

Soit  $(A, +, \times)$  un anneau commutatif. Une partie  $I$  de  $A$  est un idéal de  $A$  si et seulement si

- (i)  $0_A \in I$ ;
- (ii)  $\forall (x, y) \in I^2, x + y \in I$ ;
- (iii)  $\forall (a, x) \in A \times I, a \times x \in I$ .

**Exercice 1.1**

Montrer que si  $I$  et  $J$  sont des idéaux d'un anneau commutatif  $A$ , alors  $I \cap J$  et  $I + J$  sont également des idéaux de  $A$ .

**Définition 1.2 Idéal engendré par une partie**

Soit  $(A, +, \times)$  un anneau commutatif. On appelle **idéal engendré** par une partie  $X$  de  $A$  le plus petit idéal contenant  $X$ .

**Proposition 1.3**

Soient  $(A, +, \times)$  un anneau commutatif et  $X$  une partie de  $A$ . L'idéal engendré par  $X$  est l'ensemble des combinaisons linéaires d'éléments de  $\mathcal{P}$ , c'est-à-dire d'éléments de la forme  $\sum_{x \in X} a_x x$  où  $(a_x)_{x \in X}$  est une famille presque nulle d'éléments de  $A$ .

**REMARQUE.** En particulier, l'idéal engendré par un unique élément  $x \in A$  est  $xA$ .

**REMARQUE.** On dit qu'un idéal  $I$  d'un anneau commutatif  $A$  est **principal** s'il existe  $x \in A$  tel que  $I = xA$ .  
On dit qu'un anneau commutatif  $A$  est **principal** si tous ses idéaux sont principaux.

**Proposition 1.4**

Soit  $f : A \rightarrow B$  un morphisme d'anneaux commutatifs. Alors  $\text{Ker } f$  est un idéal de  $A$ .

### 1.3 Divisibilité

**Définition 1.3 Divisibilité**

Soient  $(A, +, \times)$  un anneau commutatif et  $(a, b) \in A^2$ . On dit que  $a$  **divise**  $b$  ou que  $b$  est un **multiple** de  $a$  s'il existe  $c \in A$  tel que  $b = ca$ .

**Proposition 1.5**

La relation de divisibilité est réflexive et transitive.

**Exercice 1.2**

Soient  $a$  et  $b$  deux éléments d'un anneau commutatif **intègre**  $A$ . Montrer que si  $a$  divise  $b$  et  $b$  divise  $A$ , alors il existe  $u \in A^\times$  (groupe des éléments inversibles de  $A$ ) tel que  $b = au$ .

**Proposition 1.6 Divisibilité et idéaux**

Soient  $(A, +, \times)$  un anneau commutatif et  $(a, b) \in A^2$ . Alors  $a$  divise  $b$  si et seulement si  $bA \subset aA$ .

**Idéaux et éléments premiers entre eux**

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

- On dit que deux idéaux  $I$  et  $J$  de  $A$  sont **premiers entre eux** si  $I + J = A$ .
- On dit que deux éléments  $a$  et  $b$  de  $A$  sont **premiers entre eux** si  $aA + bA = A$ , ce qui équivaut à dire que les diviseurs communs de  $a$  et  $b$  sont les inversibles de  $A$  (c'est une version générale du théorème de Bézout).

On peut étendre ces notions à plus de deux idéaux ou plus de deux éléments.

- On dit que des idéaux  $I_1, \dots, I_n$  de  $A$  sont **premiers entre eux dans leur ensemble** si  $\sum_{i=1}^n I_i = A$ .
- On dit que des éléments  $a_1, \dots, a_n$  de  $A$  sont **premiers entre eux dans leur ensemble** si  $\sum_{i=1}^n a_i A = A$ , ce qui équivaut à dire que les diviseurs communs de  $a_1, \dots, a_n$  sont les inversibles de  $A$  (c'est à nouveau une version générale du théorème de Bézout).

**Idéaux et éléments premiers**

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

- On dit qu'un idéal  $I$  de  $A$  est **premier** si  $I \neq A$  et  $\forall (a, b) \in A^2, ab \in I \implies (a \in I \text{ ou } b \in I)$ .
- Un élément  $a$  de  $A$  est dit **premier** si l'idéal  $aA$  est premier et non nul.

## 2 Anneaux usuels

### 2.1 L'anneau $\mathbb{Z}$

**Proposition 2.1**

$(\mathbb{Z}, +, \times)$  est un anneau commutatif intègre.

**Proposition 2.2**

Le groupe des éléments inversibles de l'anneau  $(\mathbb{Z}, +, \times)$  est  $(\{-1, +1\}, \times)$ .

**Proposition 2.3 Idéaux de  $\mathbb{Z}$** 

Les idéaux de l'anneau  $(\mathbb{Z}, +, \times)$  sont les  $a\mathbb{Z}$  avec  $a \in \mathbb{Z}$ .

**REMARQUE.** En d'autres termes,  $\mathbb{Z}$  est un anneau principal.

**REMARQUE.** Les idéaux de l'anneau  $(\mathbb{Z}, +, \times)$  sont également les sous-groupes de  $(\mathbb{Z}, +)$ .

**Définition 2.1 PGCD de deux entiers**

Soit  $(a, b) \in \mathbb{Z}^2$ . On appelle PGCD de  $a$  et  $b$  tout entier  $d \in \mathbb{Z}$  tel que  $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ . Il existe un unique PGCD positif de  $a$  et  $b$  noté  $a \wedge b$ .

**REMARQUE.** Cette définition du PGCD est équivalente à la définition du PGCD vue en première année. Le théorème de Bézout découle alors directement de cette nouvelle définition.

### Définition 2.2 PPCM de deux entiers

Soit  $(a, b) \in \mathbb{Z}^2$ . On appelle PPCM de  $a$  et  $b$  tout entier  $m \in \mathbb{Z}$  tel que  $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$ .  
Il existe un unique PPCM positif de  $a$  et  $b$  noté  $a \vee b$ .

**REMARQUE.** Cette définition du PPCM est équivalente à la définition du PGCD vue en première année.

### Définition 2.3 PGCD de plusieurs entiers

Soit  $(a_1, \dots, a_n) \in \mathbb{Z}^n$ . On appelle PGCD de  $a_1, \dots, a_n$  tout entier  $d \in \mathbb{Z}$  tel que  $\sum_{i=1}^n a_i \mathbb{Z} = d\mathbb{Z}$ .  
Il existe un unique PGCD positif de  $a_1, \dots, a_n$  noté  $a_1 \wedge \dots \wedge a_n$ .

### Théorème 2.1 Bézout

Soit  $(a_1, \dots, a_r) \in \mathbb{Z}^r$ . Alors  $a_1 \wedge \dots \wedge a_r = 1$  si et seulement si il existe  $(u_1, \dots, u_r) \in \mathbb{Z}^r$  tel que  $\sum_{i=1}^r a_i u_i = 1$ .

### Définition 2.4 PPCM de plusieurs entiers

Soit  $(a_1, \dots, a_n) \in \mathbb{Z}^n$ . On appelle PPCM de  $a_1, \dots, a_n$  tout entier  $m \in \mathbb{Z}$  tel que  $\bigcap_{i=1}^n a_i \mathbb{Z} = m\mathbb{Z}$ .  
Il existe un unique PPCM positif de  $a_1, \dots, a_n$  noté  $a_1 \vee \dots \vee a_n$ .

## 2.2 L'anneau $\mathbb{K}[X]$

Dans ce chapitre,  $\mathbb{K}$  désigne un corps.

### Proposition 2.4

$(\mathbb{K}[X], +, \times)$  est un anneau commutatif intègre.

### Proposition 2.5

Le groupe des éléments inversibles de l'anneau  $(\mathbb{K}[X], +, \times)$  est  $\mathbb{K}^*$ .

### Proposition 2.6 Idéaux de $\mathbb{Z}$

Les idéaux de l'anneau  $(\mathbb{K}[X], +, \times)$  sont les  $P\mathbb{K}[X]$  avec  $P \in \mathbb{K}[X]$ .

**REMARQUE.** En d'autres termes,  $\mathbb{K}[X]$  est un anneau principal.

### Définition 2.5 PGCD de deux polynômes

Soit  $(P, Q) \in \mathbb{K}[X]^2$ . On appelle PGCD de  $P$  et  $Q$  tout polynôme  $D \in \mathbb{K}[X]$  tel que  $P\mathbb{K}[X] + Q\mathbb{K}[X] = D\mathbb{K}[X]$ . Il existe un unique PGCD unitaire ou nul de  $P$  et  $Q$  noté  $P \wedge Q$ .

**REMARQUE.** Cette définition du PGCD est équivalente à la définition du PGCD vue en première année. Le théorème de Bézout découle alors directement de cette nouvelle définition.

### Définition 2.6 PPCM de deux polynômes

Soit  $(P, Q) \in \mathbb{K}[X]^2$ . On appelle PPCM de  $P$  et  $Q$  tout polynôme  $M \in \mathbb{Z}$  tel que  $P\mathbb{K}[X] \cap Q\mathbb{K}[X] = M\mathbb{K}[X]$ . Il existe un unique PPCM unitaire ou nul de  $P$  et  $Q$  noté  $P \vee Q$ .

**REMARQUE.** Cette définition du PPCM est équivalente à la définition du PGCD vue en première année.

### Définition 2.7 PGCD de plusieurs polynômes

Soit  $(P_1, \dots, P_n) \in \mathbb{K}[X]^n$ . On appelle PGCD de  $P_1, \dots, P_n$  tout polynôme  $D \in \mathbb{K}[X]$  tel que  $\sum_{i=1}^n P_i \mathbb{K}[X] = D \mathbb{K}[X]$ . Il existe un unique PGCD unitaire ou nul de  $P_1, \dots, P_n$  noté  $P_1 \wedge \dots \wedge P_n$ .

### Théorème 2.2 Bézout

Soit  $(P_1, \dots, P_r) \in \mathbb{K}[X]^r$ . Il existe  $(U_1, \dots, U_r) \in \mathbb{K}[X]^r$  tel que  $\sum_{i=1}^r U_i P_i = P_1 \wedge \dots \wedge P_r$ .

### Définition 2.8 PPCM de plusieurs polynômes

Soit  $(P_1, \dots, P_n) \in \mathbb{K}[X]^n$ . On appelle PPCM de  $P_1, \dots, P_n$  tout polynôme  $M \in \mathbb{K}[X]$  tel que  $\bigcap_{i=1}^n P_i \mathbb{K}[X] = M \mathbb{K}[X]$ . Il existe un unique PPCM unitaire ou nul de  $P_1, \dots, P_n$  noté  $P_1 \vee \dots \vee P_n$ .

## 2.3 L'anneau $\mathbb{Z}/n\mathbb{Z}$

### Proposition 2.7 Multiplication sur $\mathbb{Z}/n\mathbb{Z}$

Soit  $n \in \mathbb{N}^*$ . On définit une multiplication sur  $\mathbb{Z}/n\mathbb{Z}$  en posant

$$\forall (k, l) \in \mathbb{Z}^2, \bar{k} \times \bar{l} = \overline{k \times l}$$

**REMARQUE.**  $\bar{k}$  désigne la classe de congruence de  $k$  dans  $\mathbb{Z}/n\mathbb{Z}$ .

**REMARQUE.** Il faut vérifier que la classe de congruence de  $k \times l$  modulo  $n$  ne dépend que des classes de congruence de  $k$  et  $l$  modulo  $n$ .

### Exemple 2.1

Dans  $\mathbb{Z}/4\mathbb{Z}$ ,  $\bar{7} \times \bar{2} = \bar{14} = \bar{2}$ .

### Proposition 2.8 Structure d'anneau de $\mathbb{Z}/n\mathbb{Z}$

Soit  $n \in \mathbb{N}^*$ .  $(\mathbb{Z}/n\mathbb{Z}, +, \times)$  est un anneau commutatif d'unité  $\bar{1}$ .



**ATTENTION!** L'anneau  $\mathbb{Z}/n\mathbb{Z}$  n'est en général pas intègre. Par exemple, dans  $\mathbb{Z}/10\mathbb{Z}$ ,  $\bar{2} \times \bar{5} = \bar{0}$ .

### Proposition 2.9 Inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$

Soit  $(n, k) \in \mathbb{N}^* \times \mathbb{Z}$ . Alors  $\bar{k}$  est inversible dans  $\mathbb{Z}/n\mathbb{Z}$  si et seulement si  $k \wedge n = 1$ .

### Idéaux de $\mathbb{Z}/n\mathbb{Z}$

Tout idéal de  $(\mathbb{Z}/n\mathbb{Z}, +, \times)$  est un sous-groupe de  $(\mathbb{Z}/n\mathbb{Z}, +)$ . Mais comme pour  $(d, k) \in \mathbb{Z}^2$ ,  $\bar{d} \times \bar{k} = \bar{dk}$ , un sous-groupe de  $(\mathbb{Z}/n\mathbb{Z}, +)$  est également un idéal de  $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ . Les idéaux de  $(\mathbb{Z}/n\mathbb{Z}, +, \times)$  sont donc exactement les sous-groupes de  $(\mathbb{Z}/n\mathbb{Z}, +)$ .

On montre par ailleurs classiquement que les sous-groupes de  $(\mathbb{Z}/n\mathbb{Z})$  sont tous cycliques. On en déduit que l'anneau  $(\mathbb{Z}/n\mathbb{Z}, +, \times)$  est principal.

### Théorème 2.3

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

**REMARQUE.** Notamment, si  $p$  est premier,  $\mathbb{Z}/p\mathbb{Z}$  est intègre. On retrouve alors le lemme d'Euclide. En effet, soit  $(a, b) \in \mathbb{Z}^2$  tel que  $p$  divise  $ab$ . Alors  $\bar{a}\bar{b} = \bar{0}$  dans  $\mathbb{Z}/p\mathbb{Z}$ . Comme  $\mathbb{Z}/p\mathbb{Z}$  est intègre,  $\bar{a} = \bar{0}$  ou  $\bar{b} = \bar{0}$  i.e.  $p$  divise  $a$  ou  $p$  divise  $b$ .

**REMARQUE.** Si  $p$  est premier, on retrouve également le petit théorème de Fermat. En effet,  $((\mathbb{Z}/p\mathbb{Z})^\times, \times)$  est un groupe d'ordre  $p - 1$  car seul  $\bar{0}$  n'est pas inversible dans le corps  $\mathbb{Z}/p\mathbb{Z}$ . On en déduit que pour tout  $n \in \mathbb{Z}$  non multiple de  $p$ ,  $(\bar{n})^{p-1} = \bar{1}$  puisque l'ordre de  $\bar{n}$  divise  $p - 1$ . Ainsi  $n^{p-1} \equiv 1[p]$ . On en déduit que  $n^p \equiv n[p]$ , ce qui est encore valable si  $n$  est multiple de  $p$ , puisque dans ce cas,  $n^p \equiv n \equiv 0[p]$ .

**REMARQUE.** Lorsque  $p$  est un nombre premier,  $\mathbb{Z}/p\mathbb{Z}$  est souvent noté  $\mathbb{F}_p$ .

### Exercice 2.1 Nombre de carrés dans $\mathbb{F}_p$

Soit  $p$  un nombre premier impair. On considère l'application  $f : \begin{cases} \mathbb{Z}/p\mathbb{Z} & \longrightarrow \mathbb{Z}/p\mathbb{Z} \\ x & \longmapsto x^2 \end{cases}$ .

1. Combien chaque élément de  $\text{Im } f$  possède-t-il d'antécédents par  $f$  ?
2. En déduire le cardinal de  $\text{Im } f$ , c'est-à-dire le nombre de carrés dans  $\mathbb{Z}/p\mathbb{Z}$ .

**Exercice 2.2**

Résoudre les équations suivantes :

$$1. \quad x^2 - 3x + 2 = 0 \text{ dans } \mathbb{Z}/101\mathbb{Z};$$

$$2. \quad x^2 + 8x + 4 = 0 \text{ dans } \mathbb{Z}/11\mathbb{Z};$$

$$3. \quad x^2 + 7x + 1 = 0 \text{ dans } \mathbb{Z}/23\mathbb{Z}.$$

**Proposition 2.10 Théorème des restes chinois**

Soit  $(m, n) \in (\mathbb{N}^*)^2$  un couple d'entiers premiers entre eux. Alors l'application

$$\begin{cases} \mathbb{Z}/mn\mathbb{Z} & \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ \bar{k} & \longmapsto (\hat{k}, \tilde{k}) \end{cases}$$

est bien définie et est un isomorphisme d'anneaux.

**REMARQUE.**  $\bar{k}$ ,  $\hat{k}$  et  $\tilde{k}$  désignent respectivement les classes de congruences de  $k$  dans  $\mathbb{Z}/mn\mathbb{Z}$ ,  $\mathbb{Z}/m\mathbb{Z}$  et  $\mathbb{Z}/n\mathbb{Z}$ .

**REMARQUE.** Cet isomorphisme d'anneaux induit également un isomorphisme de groupes de  $(\mathbb{Z}/mn\mathbb{Z})^\times$  sur  $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ .

**Système de congruences**

Soient  $(m, n) \in (\mathbb{N}^*)^2$  un couple d'entiers premiers entre eux et  $(a, b) \in \mathbb{Z}^2$ . Le système  $\begin{cases} x \equiv a[m] \\ x \equiv b[n] \end{cases}$  d'inconnue  $x \in \mathbb{Z}$  admet une infinité de solutions. Plus précisément, si  $x_0$  est une solution particulière, l'ensemble des solutions est  $\{x_0 + kmn, k \in \mathbb{Z}\}$ .

Une relation de Bézout entre  $m$  et  $n$  permet de déterminer une solution particulière du système. Puisque  $m \wedge n = 1$ , il existe  $(u, v) \in \mathbb{Z}^2$  tel que  $um + vn = 1$ . Alors  $bum + avn$  est une solution particulière.

**Exemple 2.2**

Considérons le système de congruences  $(S)$  :  $\begin{cases} x \equiv 12[21] \\ x \equiv 3[16] \end{cases}$ . Puisque  $4 \times 16 - 3 \times 21 = 1$ ,  $12 \times 4 \times 16 - 3 \times 3 \times 21 = 579$  est une solution particulière de  $(S)$ . L'ensemble des solutions de  $(S)$  est donc

$$\{579 + k \times 21 \times 16, k \in \mathbb{Z}\} = \{579 + 336k, k \in \mathbb{Z}\}$$

**Exercice 2.3**

Résoudre l'équation  $x^2 - 3x + 2 = 0$  dans  $\mathbb{Z}/35\mathbb{Z}$ .

**Exercice 2.4 Réciproque du théorème des restes chinois**

Soit  $(m, n) \in (\mathbb{N}^*)^2$  tel que  $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$  soit isomorphe à  $\mathbb{Z}/mn\mathbb{Z}$ . Montrer que  $m \wedge n = 1$ .

**Proposition 2.11 Théorème des restes chinois (extension)**

Soit  $(n_1, \dots, n_r) \in (\mathbb{N}^*)^r$  tels que les  $n_i$  soient premiers entre eux deux à deux. On pose  $n = \prod_{i=1}^r n_i$ . Alors l'application

$$\begin{cases} \mathbb{Z}/n\mathbb{Z} & \longrightarrow \prod_{i=1}^r \mathbb{Z}/n_i\mathbb{Z} \\ \bar{k}^n & \longmapsto (\bar{k}^{n_1}, \dots, \bar{k}^{n_r}) \end{cases}$$

est bien définie et est un isomorphisme d'anneaux.

**Définition 2.9 Indicatrice d'Euler**

Soit  $n \in \mathbb{N}^*$ . On note  $\varphi(n)$  le nombre d'éléments inversibles de  $\mathbb{Z}/n\mathbb{Z}$  i.e. le cardinal de  $(\mathbb{Z}/n\mathbb{Z})^*$ .

C'est également le nombre d'entiers de  $\llbracket 0, n-1 \rrbracket$  premiers avec  $n$ .

L'application  $\varphi : \mathbb{N}^* \rightarrow \mathbb{N}^*$  est appelée **indicatrice d'Euler**.

**REMARQUE.**  $\varphi(n)$  est aussi le nombre d'entiers de  $\llbracket 1, n \rrbracket$  premiers avec  $n$  ou, de manière plus général, le nombre d'entiers premiers avec  $n$  dans un ensemble de  $n$  entiers consécutifs.

**Exemple 2.3**

$\varphi(1) = 1, \varphi(2) = 1, \varphi(3) = 2, \varphi(4) = 2, \varphi(5) = 4, \varphi(6) = 2, \dots$

**Exercice 2.5**

Soit  $n \in \mathbb{N}^*$ . Montrer que  $\sum_{d|n} \varphi(d) = n$  où la somme est prise sur l'ensemble des diviseurs positifs de  $n$ .

**Proposition 2.12 Indicatrice d'Euler d'une puissance de nombre premier**

Soient  $p$  un nombre premier et  $\alpha \in \mathbb{N}^*$ . Alors  $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ .

**Proposition 2.13**

Soit  $(m, n) \in (\mathbb{N}^*)^2$  un couple d'entiers premiers entre eux. Alors  $\varphi(mn) = \varphi(m)\varphi(n)$ .

**REMARQUE.** On dit que l'indicatrice d'Euler est une fonction **arithmétique**.

**REMARQUE.** Le résultat se généralise à un uplet d'entiers naturels non nuls premiers entre eux deux à deux.

**Proposition 2.14 Décomposition en facteurs premiers et indicatrice d'Euler**

Soient  $p_1, \dots, p_r$  des nombres premiers deux à deux distincts et  $(\alpha_1, \dots, \alpha_r) \in (\mathbb{N}^*)^r$ . Alors

$$\varphi\left(\prod_{i=1}^r p_i^{\alpha_i}\right) = \prod_{i=1}^r (p_i^{\alpha_i} - p_i^{\alpha_i-1}) = n \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right)$$

où  $n = \prod_{i=1}^r p_i^{\alpha_i}$ .

**Proposition 2.15 Théorème d'Euler**

Soit  $(n, a) \in \mathbb{N}^* \times \mathbb{Z}$  tel que  $a \wedge n = 1$ . Alors  $a^{\varphi(n)} \equiv 1[n]$ .

**REMARQUE.** Ceci est donc une généralisation du petit théorème de Fermat. En effet, si  $p$  est un nombre premier,  $\varphi(p) = p - 1$  de sorte que pour tout entier  $a$  premier avec  $p$ ,  $a^{p-1} \equiv 1[p]$ .

**Exercice 2.6**

Soient un entier  $n \in \mathbb{N}^*$  et un entier impair  $a \in \mathbb{Z}$ . Montrer que  $a^{2^n-1} \equiv 1[2^n]$ .

### 3 Structure d'algèbre

**Définition 3.1**

Soient  $\mathbb{K}$  un corps et  $E$  un ensemble muni de deux lois internes  $+$  et  $\times$  ainsi que d'une loi externe . i.e. d'une application :

$$\begin{cases} \mathbb{K} \times E & \longrightarrow E \\ (\lambda, x) & \longmapsto \lambda \cdot x \end{cases}$$

On dit que  $(E, +, \times, \cdot)$  est une  **$\mathbb{K}$ -algèbre** si

- (i)  $(E, +, \cdot)$  est un  $\mathbb{K}$ -espace vectoriel ;
- (ii)  $(E, +, \times)$  est un anneau ;
- (iii)  $\forall (\lambda, x, y) \in \mathbb{K} \times E^2$ ,  $\lambda \cdot (x \times y) = (\lambda \cdot x) \times y = x \times (\lambda \cdot y)$ .

**REMARQUE.** Si la loi  $\times$  est commutative, on dit que  $E$  est une algèbre commutative.

**Exemple 3.1**

- Si  $E$  est un  $\mathbb{K}$ -espace vectoriel,  $(\mathcal{L}(E), +, \circ, \cdot)$  est une  $\mathbb{K}$ -algèbre. Elle est non commutative dès que  $\dim E \geq 2$ .
- $(\mathcal{M}_n(\mathbb{K}), +, \times, \cdot)$  est une  $\mathbb{K}$ -algèbre. Elle est non commutative dès que  $n \geq 2$ .
- $\mathbb{K}[X]$  est une  $\mathbb{K}$ -algèbre commutative.
- Si  $X$  est un ensemble,  $(\mathbb{K}^X, +, \times, \cdot)$  est une  $\mathbb{K}$ -algèbre commutative.

**REMARQUE.** Si  $E$  est une  $\mathbb{K}$ -algèbre, alors on peut donner un sens à  $P(x)$  pour  $x \in E$  et  $P \in \mathbb{K}[X]$ .

### Définition 3.2 Sous-algèbre

Soit  $(E, +, \times, .)$  une  $\mathbb{K}$ -algèbre et  $F$  un ensemble. On dit que  $F$  est une **sous-algèbre** de  $E$  si

- (i)  $F \subset E$ ;
- (ii)  $F$  est un sous-espace vectoriel de  $E$ ;
- (iii)  $F$  est un sous-anneau de  $E$ .

### Exemple 3.2 Sous-algèbre engendrée par un vecteur

Soit  $a$  un élément d'une algèbre  $\mathbb{K} \cdot E$ . On pose

$$\mathbb{K}[a] = \text{vect}(a^n, n \in \mathbb{N}) = \{P(a), P \in \mathbb{K}[X]\}$$

Alors  $\mathbb{K}[a]$  est une sous-algèbre **commutative** de  $E$ . On l'appelle sous-algèbre **engendrée par  $a$** . C'est la plus petite sous-algèbre de  $E$  contenant  $a$ .

**REMARQUE.** De manière générale, on peut définir la sous-algèbre engendrée par une partie  $V$  d'une algèbre  $E$ . C'est la plus petite sous-algèbre de  $E$  contenant  $V$ . Elle n'est en général pas commutative à moins que les éléments de  $V$  commutent entre eux.

### Proposition 3.1

Une sous-algèbre d'une  $\mathbb{K}$ -algèbre est une  $\mathbb{K}$ -algèbre.

### Proposition 3.2 Caractérisation des sous-algèbres

Soit  $(E, +, \times, .)$  une  $\mathbb{K}$ -algèbre et  $F$  un ensemble. On dit que  $F$  est une **sous-algèbre** de  $E$  si et seulement si

- (i)  $F \subset E$ ;
- (ii)  $1_E \in F$ ;
- (iii)  $\forall(\lambda, \mu) \in \mathbb{K}^2, \forall(x, y) \in F^2, \lambda \cdot x + \mu \cdot y \in F$ ;
- (iv)  $\forall(x, y) \in F^2, x \times y \in F$ .

**Exemple 3.3**

- Soit  $E$  un espace vectoriel. Alors l'ensemble  $\mathbb{K}\text{Id}_E$  des homothéties de  $E$  est une sous-algèbre commutative de  $\mathcal{L}(E)$ .
- L'ensemble  $\mathbb{K}I_n$  des matrices scalaires de  $\mathcal{M}_n(\mathbb{K})$  est une sous-algèbre commutative de  $\mathcal{M}_n(\mathbb{K})$ .
- L'ensemble des matrices diagonales de  $\mathcal{M}_n(\mathbb{K})$  est une sous-algèbre commutative de  $\mathcal{M}_n(\mathbb{K})$ .
- L'ensemble des matrices triangulaires supérieures/inférieures de  $\mathcal{M}_n(\mathbb{K})$  est une sous-algèbre de  $\mathcal{M}_n(\mathbb{K})$ .
- Si  $I$  est un intervalle de  $\mathbb{R}$ , pour tout  $k \in \mathbb{N} \cup \{+\infty\}$ ,  $(\mathcal{C}^k(I, \mathbb{K}), +, \times, .)$  est une sous-algèbre de  $\mathbb{K}^I$ .
- Soit  $I$  est un intervalle de  $\mathbb{R}$  et  $(k, p) \in (\mathbb{N} \cup \{+\infty\})^2$ . Si  $k \geq p$ , alors  $\mathcal{C}^k(I, \mathbb{K})$  est une sous-algèbre de  $\mathcal{C}^p(I, \mathbb{K})$ .

**Définition 3.3 Morphisme d'algèbres**

Soient  $(E, +, \times, .)$  et  $(F, +, \times, .)$  deux  $\mathbb{K}$ -algèbres. On appelle **morphisme de  $\mathbb{K}$ -algèbres** de  $E$  dans  $F$  toute application  $f : E \rightarrow F$  telle que :

- $f(1_E) = 1_F$ ,
- $\forall (\lambda, \mu) \in \mathbb{K}^2, \forall (x, y) \in E^2, f(\lambda.x + \mu.y) = \lambda.f(x) + \mu.f(y)$ ,
- $\forall (x, y) \in E^2, f(x \times y) = f(x) \times f(y)$ ,

**REMARQUE.** Une application est donc un morphisme d'algèbres si et seulement si elle est à la fois un morphisme d'espaces vectoriels i.e. une application linéaire et un morphisme d'anneaux.

**Exemple 3.4**

Soit  $a \in \mathbb{K}$ . L'application  $\begin{cases} \mathbb{K}[X] & \longrightarrow \mathbb{K} \\ P & \longmapsto P(a) \end{cases}$  est un morphisme de  $\mathbb{K}$ -algèbres.

**Exemple 3.5**

Soit  $(E, +, \times, .)$  une  $\mathbb{K}$ -algèbre. Soit  $x \in E$ . Alors  $\begin{cases} \mathbb{K}[X] & \longrightarrow E \\ P & \longmapsto P(x) \end{cases}$  est un morphisme de  $\mathbb{K}$ -algèbres.

**Exercice 3.1**

Soit  $f : E \rightarrow F$  un morphisme de  $\mathbb{K}$ -algèbres. Montrer que

$$\forall P \in \mathbb{K}[X], \forall x \in E, f(P(x)) = P(f(x))$$

**REMARQUE.** On peut également définir des notions d'**endomorphisme**, d'**isomorphisme** et d'**automorphisme** d'algèbres.

**Exemple 3.6**

Soit  $Q \in \mathbb{K}[X]$ . L'application  $\begin{cases} \mathbb{K}[X] & \longrightarrow \mathbb{K}[X] \\ P & \longmapsto P \circ Q \end{cases}$  est un endomorphisme de  $\mathbb{K}$ -algèbre.

**Exemple 3.7**

Soit  $\mathcal{B}$  une base d'un  $\mathbb{K}$ -espace vectoriel  $E$  de dimension  $n \in \mathbb{N}^*$ . Alors l'application

$$\begin{cases} \mathcal{L}(E) & \longrightarrow \mathcal{M}_n(\mathbb{K}) \\ u & \longmapsto \text{mat}_{\mathcal{B}}(u) \end{cases}$$

est un isomorphisme de  $\mathbb{K}$ -algèbres. On en déduit notamment que,

$$\forall P \in \mathbb{K}[X], \forall u \in \mathcal{L}(E), P(\text{mat}_{\mathcal{B}}(u)) = \text{mat}_{\mathcal{B}}(P(u))$$

**Exemple 3.8**

Soit  $Q \in \text{GL}_n(\mathbb{K})$ . Alors l'application

$$\begin{cases} \mathcal{M}_n(\mathbb{K}) & \longrightarrow \mathcal{M}_n(\mathbb{K}) \\ M & \longmapsto Q^{-1}MQ \end{cases}$$

est un automorphisme de  $\mathbb{K}$ -algèbre. On en déduit notamment que

$$\forall P \in \mathbb{K}[X], \forall M \in \mathbb{K}(X), P(Q^{-1}MQ) = Q^{-1}P(M)Q$$

**Proposition 3.3 Image directe par un morphisme d'algèbres**

Soit  $f : E \rightarrow F$  un morphisme de  $\mathbb{K}$ -algèbres.

- (i) Si  $G$  est une sous-algèbre de  $E$ , alors  $f(G)$  est une sous-algèbre de  $F$ .
- (ii) Si  $H$  est une sous-algèbre de  $F$ , alors  $f^{-1}(H)$  est une sous-algèbre de  $E$ .

**Proposition 3.4**

Soit  $f : E \rightarrow F$  un morphisme de  $\mathbb{K}$ -algèbres. Alors  $\text{Im } f$  est une sous-algèbre de  $F$ .



**ATTENTION !** De manière générale,  $\text{Ker } f$  n'est pas une sous-algèbre de  $E$ . En effet,  $1_E \notin \text{Ker } f$  à moins que  $F$  soit l'algèbre nulle (i.e.  $0_F = 1_F$ ).