Chapitre 2

Anneaux et Corps

I Anneaux

I. A Structure d'anneau

Définition 1.1

On appelle **anneau** un triplet $(A,+,\times)$ où A est un ensemble et $+,\times$ deux lois de composition interne dans A telles que :

- $(A,+)$ est un groupe abélien, son élément neutre est noté 0_A ;
- $\times$ est associative ;
- $\times$ admet un élément neutre noté 1_A, distinct de 0_A, appelé élément unité de A ;
- $\times$ est distributive par rapport à $+$.

Si de plus $\times$ est commutative, l'anneau est dit commutatif.

Exemples 1.2 : $(\mathbb{Z},+,\times)$, $(\mathcal{F}(X,\mathbb{R}),+,\times)$, $(\mathbb{R}[X],+,\times)$, $(\mathcal{M}_n(\mathbb{K}),+,\times)$ et $(\mathcal{L}(E),+,\circ)$ sont des anneaux. Les trois premiers sont commutatifs, les autres non (si $\dim(E)\neq 1$ et $n\geqslant 2$).

Notation : Pour $a,b\in A$, on note $a-b=a+(-b)$. La loi $\times$ est distributive par rapport à la loi $-$ ainsi ainsi définie.

Proposition 1.3

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

- $\forall a\in A, a\times 0_A = 0_A\times a = 0_A$, on dit que 0_A est absorbant.
- pour $a,b\in A$ et $n\in\mathbb{N}$, **si *a* et *b* commutent**, alors :

$$(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k \quad \text{(Formule du binôme)}$$

et

$$\begin{aligned}a^n-b^n&=(a-b)\left(\sum_{k=0}^{n-1}a^{n-1-k}b^k\right)\\&=\left(\sum_{k=0}^{n-1}a^{n-1-k}b^k\right)(a-b)\quad \text{(4}^{\text{e}}\text{ identité remarquable).}\end{aligned}$$

Définition 1.4

Soit $(A,+,\times)$ un anneau. On appelle **sous-anneau** de A une partie B de A stable par les lois $+$ et $\times$ et qui, munie des lois induites, est encore un anneau, avec le même élément unité 1_A.

Proposition 1.5

Soit $(A,+,\times)$ un anneau. Une partie B de A est un sous-anneau de A si et seulement si :

- $1_A\in B$;
- $\forall(x,y)\in B^2, x-y\in B$;
- $\forall(x,y)\in B^2, xy\in B$.

Exemple 1.6 : $\mathbb{Z}$ est un sous-anneau de $\mathbb{R}$.

Définition 1.7

Soit A et B deux anneaux. On appelle **morphisme d'anneau** de A dans B une application f de A dans B telle que :

- $f(1_A)=1_B$;
- $\forall(x,y)\in A^2, f(x+y)=f(x)+f(y)$;
- $\forall(x,y)\in A^2, f(xy)=f(x)f(y)$.

Remarque 1.8 : De même que pour les morphismes de groupes, un endomorphisme d'anneau de A est un morphisme de A dans A, un isomorphisme d'anneau est un morphisme bijectif et un automorphisme d'anneau est un endomorphisme bijectif.

Proposition 1.9

L'image d'un morphisme d'anneau est un sous-anneau.

Remarque 1.10 : Le noyau d'un morphisme d'anneau f n'est jamais un sous-anneau ! (car $f(1_A)=1_B\neq 0_B$).

I. B Produit fini d'anneaux

Définition 1.11

Soit $(A_i)_{i\in[\![1\,;n]\!]}$ une famille finie d'anneaux, alors $(A,+,\times)$ avec :

- $A=\prod_{i=1}^{n}A_i$;
- $\forall x=(x_i)_{i\in[\![1\,;n]\!]}, y=(y_i)_{i\in[\![1\,;n]\!]} : x+y=(x_i+y_i)_{i\in[\![1\,;n]\!]}$;
- $\forall x=(x_i)_{i\in[\![1\,;n]\!]}, y=(y_i)_{i\in[\![1\,;n]\!]} : x+y=(x_i\times y_i)_{i\in[\![1\,;n]\!]}$;

est un anneau, appelé **anneau produit**.

Remarque 1.12 : On fait les opérations coefficient par coefficient.

I. C Diviseurs de zéro, anneau intègre

Attention : Dans un anneau, il peut exister des éléments non nuls dont le produit est nul.

Exemples 1.13 :
- Dans $(\mathcal{F}(\mathbb{R},\mathbb{R}),+,\times)$: $f =$ ______ $\neq 0_{\mathcal{F}}$ et $g =$ ______ $\neq 0_{\mathcal{F}}$, $f \times g = 0_{\mathcal{F}}$.
- Dans $\mathcal{M}_2(\mathbb{R})$, $M =$ ______ $\neq 0_2$, mais $M^2 = 0_2$.

Définition 1.14

Soit $(A,+,\times)$ un anneau et $a \in A$. On dit que a est un **diviseur de zéro** lorsque :

$$a \neq 0_A \text{ et } \exists b \in A \setminus \{0_A\} \mid a \times b = 0_A.$$

Définition 1.15

Un anneau est dit **intègre** lorsqu'il est commutatif et sans diviseur de zéro.

Remarque 1.16 : Dans un anneau intègre, on peut donc simplifier par un élément non nul : si $a \neq 0_A$, alors : $ax = ay \Rightarrow x = y$.

Exemples 1.17 :
- $(\mathbb{Z},+,\times)$ et $(\mathbb{R}[X],+,\times)$ sont des anneaux intègres ;
- si $n \geqslant 2$, $(\mathcal{M}_n(\mathbb{R}),+,\times)$ n'est pas intègre.

I. D Groupe des inversibles d'un anneau

Proposition 1.18

Soit $(A,+,\times)$ un anneau. On note A^* l'ensemble des éléments inversibles (pour la loi $\times$).
Alors $(A^*,\times)$ un un groupe.

Exemples 1.19 : Donner le groupe des inversibles des anneaux : $(\mathbb{Z},+,\times)$, $(\mathbb{R},+,\times)$ et $(\mathcal{M}_n(\mathbb{R}),+,\times)$.

Remarque 1.20 : Les diviseurs de zéro et 0_A sont non-inversibles.

I. E Corps

Définition 1.21

On appelle **corps** un anneau commutatif dont tous les éléments non nuls sont inversibles.

Remarque 1.22 : Un corps est un anneau intègre.

Exemples 1.23 :
- $\mathbb{R}$ et $\mathbb{C}$ sont des corps.
- $\mathbb{R}(X)$ et $\mathbb{C}(X)$ sont des corps (des fractions rationnelles).

Définition 1.24

Soit $(K,+,\times)$ un corps. On appelle **sous-corps** de K une partie L de K stable par $+$ et $\times$ et qui, munie des lois induites, est un corps.

Remarque 1.25 : Pour un sous-corps, on n'a pas besoin de supposer que le neutre de L est le neutre de K, c'est une conséquence du fait que tout élément non nul de K est inversible.

Proposition 1.26

Soit $(K,+,\times)$ un corps et L. Une partie de K est un sous-corps de K si et seulement si :
- $1_K \in L$;
- $\forall x, y \in L, x - y \in L$;
- $\forall x, y \in L, xy \in L$;
- $\forall x \in L \setminus \{0_K\}, x^{-1} \in L$.

Remarque 1.27 : Les trois premières conditions font de L un sous-anneau de K.

Exemples 1.28 :
- $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$;
- $\mathbb{R}$ est un sous-corps de $\mathbb{C}$;
- $\mathbb{Q}[\sqrt{2}] = \left\{a + b\sqrt{2};\ \text{avec } a, b \in \mathbb{Q}\right\}$ est un sous-corps de $\mathbb{R}$.

II Idéaux d'un anneau commutatif

II. A Idéaux d'un anneau commutatif

Définition 2.1

Soit $(A, +, \times)$ un anneau commutatif. On dit que I est un idéal de A si :

- $(I, +)$ est un sous-groupe de $(A, +)$;
- $\forall x \in I, \forall a \in A, a \times x \in I$ (stabilité par la multiplication par un élément de A).

Exemples 2.2 :
- Soit A un anneau commutatif, $\{0\}$ et A sont des idéaux de A. De plus si I est un idéal de A et $1_A \in A$, alors $I = A$.
- $2\mathbb{Z}$ est un idéal de l'anneau $\mathbb{Z}$.
- L'ensemble des suites réelles presque nulles est un idéal de l'anneau des suites réelles.

Proposition 2.3 (Noyau d'un morphisme d'anneaux commutatifs)

Soit A et B des anneaux commutatifs et f un morphisme de A dans B.
Alors le noyau de f est un idéal de A.

Définition/Proposition 2.4

Soit $(A, +, \times)$ un anneau commutatif et $x \in A$. L'ensemble $xA = \{xa;\ \text{avec } a \in A\}$ est un idéal appelé **idéal engendré par x**.

Proposition 2.5

Soit A un anneau commutatif et $(I_i)_{i \in [\![1\,;n]\!]}$ une famille d'idéaux de A.

- L'intersection $\bigcap_{i \in [\![1\,;n]\!]} I_i$ est un idéal de A.
- La somme $\sum_{i=1}^{n} I_i = \left\{ \sum_{i=1}^{n} x_i;\ \text{avec } \forall i \in [\![1\,;n]\!], x_i \in I_i \right\}$ est un idéal de A.

II. B Divisibilité dans un anneau intègre

Définition 2.6

Soit A un anneau intègre et $a, b \in A$. On dit que

- a **divise** b lorsqu'il existe $c \in A$ tel que : $b = ac$;
- a et b sont **associés** lorsque : a divise b et b divise a.

Proposition 2.7

Soit A un anneau intègre et $a, b \in A$, alors :

$$a \text{ et } b \text{ sont associés} \iff \exists x \in A^* \mid b = ax$$

Exemple 2.8 : Dans l'anneau $\mathbb{K}[X]$, quels sont les polynômes de $\mathbb{K}[X]$ associés à un polynôme $P \in \mathbb{K}[X]$?

Proposition 2.9

Soit A un anneau intègre et $x, y \in A$. Alors :

- x divise y si et seulement si $yA \subset xA$;
- x et y sont associés si et seulement si $xA = yA$.

II. C Idéaux de $\mathbb{Z}$ et arithmétique dans $\mathbb{Z}$

Proposition 2.10

Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$ avec $n \in \mathbb{Z}$.

Définition/Proposition 2.11

Soit $a, b \in \mathbb{Z}$, alors il existe un unique $d \in \mathbb{N}$ tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, on l'appelle **PGCD** de a et b et on note $d = a \wedge b$.
Soit $(a_i)_{i \in [\![1\,;n]\!]}$ une famille d'entiers relatifs. Alors il existe un unique $d \in \mathbb{N}$ tel que $\sum_{i=1}^{n} a_i\mathbb{Z} = d\mathbb{Z}$, on l'appelle le **PGCD** de la famille $(a_i)_{i \in [\![1\,;n]\!]}$.

Remarques 2.12 :
- On vérifie que la définition est cohérente avec la définition vue en première année : $a, b \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, donc d diviseur commun de a et b ; et pour $c \in \mathbb{N}, (c \mid a \text{ et } c \mid b) \iff c \mid d$.
- $0 \wedge 0 = 0$.
- De même, si $m = a \vee b$, alors $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.

Théorème 2.13

Soit $a, b, d \in \mathbb{Z}$.

Identité de Bézout : si $a \wedge b = d$, alors il existe deux entiers relatifs x et y tels que : $ax + by = d$.

Théorème de Bézout : a et b sont premiers entre eux si et seulement s'il existe deux entiers relatifs x et y tels que : $ax + by = 1$.

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

Dans cette partie on suppose $n \in \mathbb{N}$ avec $n \geqslant 2$.

III. A Structure d'anneau de $\mathbb{Z}/n\mathbb{Z}$

Proposition 3.1

La loi de composition interne $\times$ sur $\mathbb{Z}/n\mathbb{Z}$:

$$(\dot{a}, \dot{b}) \mapsto (\dot{\overline{a \times b}})$$

est bien définie.

Théorème 3.2

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

Exemples 3.3 : Calculs dans $\mathbb{Z}/6\mathbb{Z}$ et inversibles de $\mathbb{Z}/6\mathbb{Z}$.

III. B Inversibles de $\mathbb{Z}/n\mathbb{Z}$

Théorème 3.4

Soit $\dot{m} \in \mathbb{Z}/n\mathbb{Z}$:

$$\dot{m} \text{ est inversible dans } \mathbb{Z}/n\mathbb{Z} \Leftrightarrow m \wedge n = 1.$$

Remarque 3.5 : Les éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ sont les générateurs du groupe $\mathbb{Z}/n\mathbb{Z}$.

Théorème 3.6

Soit $p \in \mathbb{N}^*$, $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est un nombre premier. Dans ce cas on le note $\mathbb{F}_p$.

Exemple 3.7 : résolution de $x^2 = \dot{1}$ dans $\mathbb{Z}/p\mathbb{Z}$ avec p premier, puis dans $\mathbb{Z}/12\mathbb{Z}$.

III. C Théorème chinois

On note pour $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$: $\dot{a}^{[n]}$ la classe de a modulo n.

Théorème 3.8 (chinois (Qin Jiushao))

Soit m et n des entier naturels tels que $m \wedge n = 1$. L'application :

$$\begin{array}{cccc} \Phi & : & \mathbb{Z}/mn\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ & & \mathrm{cl}_{mn}(a) & \longmapsto & (\mathrm{cl}_m(a), \mathrm{cl}_n(a)) \end{array}$$

où $\mathrm{cl}_k(a)$ désigne la classe de l'entier a dans $\mathbb{Z}/k\mathbb{Z}$, est un isomorphisme d'anneaux.

Corollaire 3.9

Soit m, n deux entiers naturels tels que $m \wedge n = 1$.
$\forall (a, b) \in \mathbb{Z}^2, \exists c \in \mathbb{Z}$ tel que :

$$\begin{cases} x \equiv a\ [m] \\ x \equiv b\ [n] \end{cases} \Leftrightarrow x \equiv c\ [mn]$$

Méthode 3.10

Pour résoudre un tel système, on cherche une solution “évidente” dans de la forme $a + km$ ou de la forme $b + k'n$ (existence assurée par le corollaire), puis :

$$\begin{cases} x \equiv a\ [m] \\ x \equiv b\ [n] \end{cases} \Leftrightarrow \begin{cases} x \equiv c\ [m] \\ x \equiv c\ [n] \end{cases} \Leftrightarrow x \equiv c\ [mn]$$

Si on ne trouve pas de solution évidente (donc $b \neq a$),

$$\begin{cases} x \equiv a\ [m] \\ x \equiv b\ [n] \end{cases} \Leftrightarrow \begin{cases} x = a + km; \quad \text{avec } k \in \mathbb{Z} \\ x = b + k'n; \quad \text{avec } k' \in \mathbb{Z} \\ b - a = km - k'n \end{cases}$$

on part d'une relation de Bézout : $um + vn = 1$ que l'on multiplie par $(b - a)$ pour trouver $k, k' \in \mathbb{Z}$ qui conviennent.

Le théorème chinois se généralise à plus de deux facteurs :

Théorème 3.11

Soit $(n_i)_{i \in [\![1\,;N]\!]}$ avec $N \geqslant 2$, tels que le PGCD de $(n_i)_{i \in [\![1\,;N]\!]}$ est 1. On pose $n = \prod_{i=1}^{N} n_i$. Alors $\mathbb{Z}/n\mathbb{Z}$ et $\prod_{i=1}^{n} (\mathbb{Z}/n_i\mathbb{Z})$ sont isomorphes.

Exemple 3.12 : (Qin Jiushao 1247)
Le général Han Xin a entre 900 et 1000 soldats. Si on les range par 3, il en reste 2 ; si on les range par 5, il en reste 3 et si on les range par 7, il en reste 2. Combien sont-ils ?

III. D Fonction indicatrice d'Euler

Définition 3.13

On appelle **indicatrice d'Euler** de l'entier $n \in \mathbb{N}^*$ le nombre $\varphi(n)$ d'entier de $[\![0\,;n-1]\!]$ premiers avec n.

Remarques 3.14 :
- $\varphi : \mathbb{N}^* \longrightarrow \mathbb{N}^*$ et $\forall n \in \mathbb{N}^*$:

$$\varphi(n) = \mathrm{Card}\,\{k \in [\![0\,;n-1]\!] \mid k \wedge n = 1\}$$

- si $n \geqslant 2$, $\varphi(n)$ est donc le nombre d'éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$;
- $\varphi(n)$ est le nombre d'éléments générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.

Exemples 3.15 : $\varphi(2) =$ __, $\varphi(7) =$ __, $\varphi(12) =$ __.

Remarque 3.16 : Si p est premier, alors $\varphi(p) =$ ______.

Proposition 3.17

Soit $m, n \in \mathbb{N}^*$, si $m \wedge n = 1$, alors $\varphi(m \times n) = \varphi(m) \times \varphi(n)$.

Proposition 3.18

Si p est premier et $\alpha \in \mathbb{N}^*$, alors $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Théorème 3.19

Soit $n \geqslant 2$, si la décomposition en facteurs premiers de n est $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, alors :

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

Théorème 3.20 (Euler)

Soit $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$ tels que $a \wedge n = 1$:

$$a^{\varphi(n)} \equiv 1 \ [n].$$

Théorème 3.21 (Petit théorème de Fermat)

Si p un un nombre premier alors pour tout entier a :

$$a^p \equiv a \ [p].$$

Exemple 3.22 : Cryptage RSA

IV Anneaux $\mathbb{K}[X]$

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

IV. A Rappels

Théorème 4.1

L'anneau $(\mathbb{K}[X], +, \times)$ est intègre et muni d'une division euclidienne : $\forall A, B \in \mathbb{K}[X]$ avec $B \neq 0, \exists!(Q, R) \in \mathbb{K}[X]^2$ tel que :

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

Remarque 4.2 : Les éléments inversibles de l'anneau $(\mathbb{K}[X], +, \times)$ sont ________

____

IV. B Idéaux de $\mathbb{K}[X]$

Théorème 4.3

Tout idéal de $\mathbb{K}[X]$ est de la forme $P_0\mathbb{K}[X]$ avec $P_0 \in \mathbb{K}[X]$.
De plus si l'idéal n'est pas $\{0\}$, alors on peut choisir P_0 unitaire, il est alors unique.

Définition/Proposition 4.4

- Soit P et Q des polynômes de $\mathbb{K}[X]$. Il existe un unique polynôme unitaire $D \in \mathbb{K}[X]$ tel que :

$$D\mathbb{K}[X] = P\mathbb{K}[X] + Q\mathbb{K}[X].$$

  Ce polynôme D est appelé le **PGCD** de P et Q, on le note $P \wedge Q$.
- Soit $(P_i)_{i\in[\![1\,;n]\!]}$ une famille de $n \geqslant 2$ polynômes de $\mathbb{K}[X]$. Il existe un unique polynôme unitaire $D \in \mathbb{K}[X]$ tel que :

$$D\mathbb{K}[X] = \sum_{i=1}^{n} \Big(P_i\mathbb{K}[X]\Big).$$

  Ce polynôme D est appelé le **PGCD** des $(P_i)_{i\in[\![1\,;n]\!]}$.

Remarques 4.5 :
- Si : $\forall i \in [\![1\,;n]\!], B \mid P_i$, alors B divise le PGCD des $(P_i)_{i\in[\![1\,;n]\!]}$.
- Si $B \mid D$ et $D \neq 0$, alors $\deg B \leqslant \deg D$.

Ainsi on retrouve que pour une famille de polynômes non tous nuls, le PGCD est le polynôme unitaire diviseur commun des $(P_i)_{i\in[\![1\,;n]\!]}$ de degré maximal (plus grand pour le degré).

Théorème 4.6 (Bezout)

Soit $(P_i)_{i\in[\![1\,;n]\!]}$ une famille de $n \geqslant 2$ polynômes de $\mathbb{K}[X]$.

- Si D est le PGCD de $(P_i)_{i\in[\![1\,;n]\!]}$, alors il existe $(U_i)_{i\in[\![1\,;n]\!]} \in (\mathbb{K}[X])^n$ tel que : $D = \sum_{i=1}^{n} P_i U_i$.
- Les $(P_i)_{i\in[\![1\,;n]\!]}$ sont premiers entre eux (de PGCD égal à 1) si et seulement si il existe des polynômes $(U_i)_{i\in[\![1\,;n]\!]}$ tels que : $\sum_{i=1}^{n} \Big(P_i U_i\Big) = 1$.

Méthode 4.7

On obtient une relation de Bezout en appliquant l'algorithme d'Euclide.

Exemple 4.8 : Montrer que les polynômes $A = X^3 + 1$ et $B = X^2 + 1$ sont premiers entre eux et donner les couples $(U, V) \in \mathbb{K}[X]$ tels que $AU + BV = 1$.

Théorème 4.9 (Gauss)

Soit $A, B, C \in \mathbb{K}[X]$:

$$\Big(A \mid BC \text{ et } A \wedge B = 1\Big) \Rightarrow A \mid C.$$

Corollaire 4.10

Soit $A, B, C \in \mathbb{K}[X]$:

$$\Big(A \mid C, \quad B \mid C \quad \text{et} \quad A \wedge B = 1\Big) \Rightarrow AB \mid C.$$

IV. C Irréductibles de $\mathbb{K}[X]$

Définition 4.11

Un polynôme de $\mathbb{K}[X]$ est dit **irréductible** lorsqu'il est non constant et qu'il n'a pas d'autre diviseur que les polynômes constants et les polynômes que lui sont associés.

Remarques 4.12 :

- Les polynômes associés à $P \in \mathbb{K}[X]$ sont les λP avec $\lambda \in \mathbb{K}^*$.
- Un polynôme unitaire P est irréductible si et seulement si il est non constants et les seuls polynômes unitaires qui divisent P sont 1 et P.

Exemples 4.13 :

- $X^2 + 1$ est irréductible dans ________ mais pas dans ________ ;
- $X^2 - 2$ est irréductible dans ________ mais pas dans ________ .

Proposition 4.14

Tout polynôme non constant de $\mathbb{K}[X]$ a (au moins) un diviseur irréductible.

Théorème 4.15

Tout polynôme non constant de $\mathbb{K}[X]$ se décompose comme produit de son coefficient dominant et de polynômes irréductibles unitaires. Cette décomposition est unique à l'ordre des facteurs près.

IV. D irréductibles de $\mathbb{C}[X]$ et $\mathbb{R}[X]$

Théorème 4.16 (d'Alembert-Gauss)

Tout polynôme non constant de $\mathbb{C}[X]$ a au moins une racine dans $\mathbb{C}$.

Théorème 4.17

Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.

Théorème 4.18

Les polynômes irréductibles de $\mathbb{R}[X]$ sont :

- les polynômes de degré 1 ;
- les polynômes de degré 2 de discriminant strictement négatif.

Remarque 4.19 : Pour tout $n \geqslant 2$, $X^n - 2$ est irréductibles : ses racines dans $\mathbb{C}$ sont les $\sqrt[n]{2}\omega$ avec $\omega \in \mathbb{U}_n$ et $\sqrt[n]{2} \notin \mathbb{Q}$.
Il existe donc des polynômes irréductibles dans $\mathbb{Q}[X]$ de tout degré $n \geqslant 1$.

V Algèbre

V. A Structure d'algèbre

Définition 5.1

On appelle $\mathbb{K}$**-algèbre** ou algèbre sur le corps K un quadruplé $(\mathcal{A}, +, \times, \cdot)$ tel que :

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

L'algèbre est dite commutative (respectivement intègre) si l'anneau est commutatif (resp. intègre).

Exemples 5.2 :
- Si K est un corps, alors $\mathbb{K}$ est une algèbre ($\dim_{\mathbb{K}}(\mathbb{K}) = 1$) ;
- $\mathbb{C}$ est une $\mathbb{R}$-algèbre de dimension 2.
- $(\mathbb{K}[X], +, \times, \cdot)$, $(\mathcal{L}(E), +\circ, \cdot)$, $(\mathcal{M}_n(\mathbb{K}), +, \times, \cdot)$ et $(\mathcal{F}(X, \mathbb{K}), +, \times, \cdot)$ sont des $\mathbb{K}$-algèbres.

V. B Sous-algèbres

Définition 5.3

Soit $\mathcal{A}$ une algèbre, on dit que $\mathcal{B}$ est une sous-algèbre de $\mathcal{A}$ lorsque $\mathcal{B}$ est un sous-espace vectoriel et un sous-anneau de $\mathcal{A}$.

Proposition 5.4

Soit $\mathcal{A}$ une $\mathbb{K}$-algèbre, $\mathcal{B}$ est une sous-algèbre de $\mathcal{A}$ si et seulement si :

- $\mathcal{B} \subset \mathcal{A}$;
- $1_{\mathcal{A}} \in \mathcal{B}$;
- $\forall \lambda, \mu \in \mathbb{K}, \forall x, y \in \mathcal{B}, \lambda x + \mu y \in \mathcal{B}$;
- $\forall x, y \in \mathcal{B}, x \times y \in \mathcal{B}$.

Exemples 5.5 :
- L'ensemble des matrices diagonales d'ordre n est une sous-algèbre de $\mathcal{M}_n(\mathbb{K})$;
- L'ensemble des fonctions continues sur un intervalle I à valeurs dans $\mathbb{K}$: $\mathcal{C}(I, \mathbb{K})$ est une sous-algèbre de $\mathcal{F}(I, \mathbb{K})$.

V. C Morphismes d'algèbres

Définition 5.6

Soit $\mathcal{A}$ et $\mathcal{B}$ deux $\mathbb{K}$-algèbres, on dit que f est un **morphisme d'algèbres** de $\mathcal{A}$ dans $\mathcal{B}$ lorsque f est un morphisme d'anneau de $\mathcal{A}$ dans $\mathcal{B}$ et une application linéaire de $\mathcal{A}$ dans $\mathcal{B}$ (morphisme d'espace vectoriel).

Exemples 5.7 :
- L'application $f \mapsto f(0)$ est un morphisme d'algèbre de $\mathcal{F}(\mathbb{R}, \mathbb{R})$ dans $\mathbb{R}$;
- L'application $\varphi \mapsto \mathrm{Mat}_{\mathcal{B}_E}(\varphi)$ est un morphisme d'algèbre de $\mathcal{L}(E)$ dans $\mathcal{M}_n(\mathbb{K})$ où E est un $\mathbb{K}$-espace vectoriel de dimension n muni d'une base $\mathcal{B}_E$.