Anneaux et arithmétique

1 Anneaux

1.1 Définition et généralités

Définition 1.1 Anneau

On appelle **anneau** tout triplet $(\mathrm{A}, +, \times)$ où A est un ensemble et $+$ et $\times$ sont des lois internes sur A vérifiant les conditions suivantes :

(i) $(\mathrm{A}, +)$ est un groupe commutatif dont l'élément neutre est généralement noté 0_{A} ou 0,

(ii) $\times$ est associative,

(iii) A possède un élément neutre pour $\times$ généralement noté 1_{A} ou 1,

(iv) $\times$ est distributive sur $+$.

Si $\times$ est commutative, on dit que l'anneau $(\mathrm{A}, +, \times)$ est commutatif.

Exemple 1.1

- $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont trois exemples d'anneaux commutatifs.
- $(\mathbb{R}^n, +, \times)$ est un anneau commutatif (l'addition et la multiplication s'effectuant composante par composante).
- $(\mathbb{K}^{\mathbb{K}}, +, \times)$ est un anneau commutatif.
- L'ensemble des polynômes à coefficients dans $\mathbb{K}$ (noté $\mathbb{K}[\mathrm{X}]$) est aussi un anneau commutatif.
- $(\mathcal{M}_n(\mathbb{K}), +, \times)$ est un anneau mais n'est pas commutatif dès que $n \geq 2$.

Notation 1.1

Soit A un anneau. On note $\mathrm{A}^\times$ l'ensemble des éléments inversibles de A.

Proposition 1.1

Si $(\mathrm{A}, +, \times)$ est un anneau, $(\mathrm{A}^\times, \times)$ est un groupe.

Théorème 1.1 Règle de calcul dans les anneaux

Soient $(\mathrm{A}, +, \times)$ un anneau, $(a, b) \in \mathrm{A}^2$ et $n \in \mathbb{Z}$.

(i) $0_{\mathrm{A}} \times a = a \times 0_{\mathrm{A}} = 0_{\mathrm{A}}$,

(ii) $n(a \times b) = (na) \times b = a \times (nb)$,

Remarque. On peut avoir $1_A = 0_A$ mais il est facile de voir que, dans ce cas, tout élément de A est nul i.e. $A = \{0\}$. On appelle cet anneau l'**anneau nul**.

Définition 1.2 Anneau intègre

On dit qu'un anneau A est intègre s'il est **non nul** et s'il vérifie la propriété suivante :

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

Remarque. On peut généraliser à un produit de plus de deux facteurs.

Exemple 1.2

Les anneaux $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont intègres.
Les anneaux $(\mathbb{R}^{\mathbb{R}}, +, \times)$ et $(\mathbb{R}^n, +, \times)$ pour $n \geq 2$ ne sont pas intègres.

Attention ! Tous les anneaux ne sont pas intègres. Par exemple, $\mathcal{M}_n(\mathbb{K})$ n'est pas un anneau intègre.

Proposition 1.2 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 :

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

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 Sous-anneaux

Définition 1.3 Sous-anneau

Soient $(A, +, \times)$ un anneau et B un ensemble. On dit que B est un sous-anneau de $(A, +, \times)$ si :

(i) $(B, +)$ est un sous-groupe de $(A, +)$;

(ii) $1_A \in B$;

(iii) B est stable par $\times$.

Proposition 1.3

Si B est un sous-anneau de $(A, +, \times)$, alors $(B, +, \times)$ est un anneau. De plus, $1_B = 1_A$.

Proposition 1.4 Caractérisation des sous-anneaux

Soient $(\mathrm{A}, +, \times)$ un anneau et B un ensemble. B est un sous-anneau de $(\mathrm{A}, +, \times)$ si et seulement si :

(i) $\mathrm{B} \subset \mathrm{A}$;

(ii) $1_{\mathrm{A}} \in \mathrm{B}$;

(iii) $\forall (a, b) \in \mathrm{B}^2, a - b \in \mathrm{B}$;

(iv) $\forall (a, b) \in \mathrm{B}^2, a \times b \in \mathrm{B}$.

Méthode Sous-anneaux en pratique

Il est souvent plus facile de montrer qu'un triplet $(\mathrm{A}, +, \times)$ est un anneau en montrant qu'il est un sous-anneau d'un anneau connu.

Exemple 1.3

$(\mathbb{Z}, +, \times)$ est un sous-anneau de $(\mathbb{Q}, +, \times)$ qui est un sous-anneau de $(\mathbb{R}, +, \times)$ qui est un sous-anneau de $(\mathbb{C}, +, \times)$.

Exercice 1.1 Entiers de Gauss

Montrer que $\mathbb{Z}[i] = \{a + ib, (a, b) \in \mathbb{Z}^2\}$ est un sous-anneau de $\mathbb{C}$.

Exercice 1.2

Soit $d \in \mathbb{N}$ qui ne soit pas un carré d'entier. Montrer que $\mathbb{Z}[\sqrt{d}]$ est un sous anneau de $\mathbb{R}$.

Exercice 1.3 Sous-anneaux de $\mathbb{Z}$

Montrer que $\mathbb{Z}$ est le seul sous-anneau de $\mathbb{Z}$.

1.3 Morphismes d'anneaux

Définition 1.4 Morphisme d'anneaux

Soient $(\mathrm{A}, +, \times)$ et $(\mathrm{B}, \oplus, \otimes)$ deux anneaux. On appelle **morphisme d'anneaux** de A dans B toute application $f : \mathrm{A} \to \mathrm{B}$ telle que :

(i) $f(1_{\mathrm{A}}) = 1_{\mathrm{B}}$,

(ii) $\forall (a, b) \in \mathrm{A}^2, f(a + b) = f(a) \oplus f(b)$,

(iii) $\forall (a, b) \in \mathrm{A}^2, f(a \times b) = f(a) \otimes f(b)$,

Remarque. En particulier, f est un morphismes de groupes de $(\mathrm{A}, +)$ dans $(\mathrm{B}, \oplus)$. On peut donc définir le noyau et l'image d'un morphisme d'anneaux.

Remarque. On peut également définir des notions d'**endomorphisme**, d'**isomorphisme** et d'**automorphisme** d'anneaux.

Proposition 1.5 Images directe et réciproque d'un sous-anneau par un morphisme d'anneaux

Soit $f : A \to B$ un morphisme d'anneaux.

(i) Si C est un sous-anneau de A, alors $f(C)$ est un sous-anneau de B.

(ii) Si D est un sous-anneau de B, alors $f^{-1}(D)$ est un sous-anneau de A.

Proposition 1.6

Soit $f : A \to B$ un morphisme d'anneaux. Alors $\operatorname{Im} f$ est un sous-anneau de B.

Attention ! De manière générale, $\operatorname{Ker} f$ n'est pas un sous-anneau de A. En effet, $1_A \notin \operatorname{Ker} f$ à moins que B soit l'anneau nul (i.e. $0_B = 1_B$).

2 Corps

2.1 Définition et pemières propriétés

Définition 2.1 Corps

On appelle corps tout anneau **commutatif** $(K, +, \times)$ dans lequel tout élément non nul est inversible pour $\times$.

Remarque. En particulier, un corps est un anneau.
Pour tout corps K, $K^\times = K \setminus \{0_K\} = K^*$.

Théorème 2.1 Corps et intégrité

Tout corps est **intègre**.

Remarque. On peut donc calculer dans un corps quelconque comme on calculerait dans $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.

Exemple 2.1

$(\mathbb{Q}, +\times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +\times)$ sont des corps.

2.2 Sous-corps

Définition 2.2 Sous-corps

Soit $(K, +, \times)$ un corps et L un ensemble. On dit que L est un sous-corps de $(K, +, \times)$ si

(i) L est un sous-anneau de $(K, +, \times)$;

(ii) L est stable par inversion i.e. $\forall x \in L \setminus \{0_K\}$, $x^{-1} \in L$.

Proposition 2.1

Soient $(\mathrm{K}, +, \times)$ un corps et L un sous-corps de $(\mathrm{K}, +, \times)$. Alors $(\mathrm{L}, +, \times)$ est un corps.

Proposition 2.2 Sous-corps

Soit $(\mathrm{K}, +, \times)$ un corps et L un ensemble. L est un sous-corps de $(\mathrm{K}, +, \times)$ si et seulement si

(i) $\mathrm{L} \subset \mathrm{K}$;

(ii) $1_\mathrm{K} \in \mathrm{L}$;

(iii) $\forall (x, y) \in \mathrm{L}^2, x - y \in \mathrm{L}$;

(iv) $\forall (x, y) \in \mathrm{L} \times (\mathrm{L} \setminus \{0_\mathrm{K}\}), x \times y^{-1} \in \mathrm{L}$.

Méthode **Sous-corps en pratique**

Il est souvent plus facile de montrer qu'un triplet $(\mathrm{K}, +, \times)$ est un corps en montrant qu'il est un sous-corps d'un corps connu.

Exemple 2.2

$(\mathbb{Q}, +, \times)$ est un sous-corps de $(\mathbb{R}, +, \times)$ qui est un sous-corps de $(\mathbb{C}, +, \times)$. $\mathbb{Q}$ est le plus petit sous-corps de $\mathbb{C}$.

Remarque. Un sous-corps est un sous-anneau mais un sous-anneau d'un corps n'est pas forcément un sous-corps. Par exemple, $\mathbb{Q}$ est bien un sous-anneau de $\mathbb{R}$ car $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$. Mais $\mathbb{Z}$ n'est pas un sous-corps de $\mathbb{Q}$ bien qu'il soit un sous-anneau de $\mathbb{Q}$ et que $\mathbb{Q}$ soit un corps.

Exercice 2.1

Montrer que $\mathbb{Q}[i] = \{a + ib, (a, b) \in \mathbb{Q}^2\}$ est un sous-corps de $\mathbb{C}$.

Exercice 2.2

Soit $d \in \mathbb{N}$ qui ne soit pas un carré d'entier. Montrer que $\mathbb{Q}[\sqrt{d}]$ est un sous-corps de $\mathbb{C}$.

2.3 Morphismes de corps

Définition 2.3 Morphisme de corps

Soient $(\mathrm{K}, +, \times)$ et $(\mathrm{L}, \oplus, \otimes)$ deux corps. On appelle **morphisme de corps** de K dans L tout morphisme d'anneaux de K dans L.

Proposition 2.3

Soit $f : \mathrm{K} \to \mathrm{L}$ un morphisme de corps. Alors

1. $\forall x \in \mathrm{K}^*, f(x) \in \mathrm{K}^*$ et $f(x^{-1}) = f(x)^{-1}$.

2. f est injectif.

On peut également définir des notions d'**endomorphisme**, d'**isomorphisme** et d'**automorphisme** de corps.

Exemple 2.3

La conjugaison est un automorphisme de corps de $\mathbb{C}$.

3 Idéaux d'un anneau commutatif

3.1 Idéaux

Définition 3.1 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 3.1

$\{0_A\}$ 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 3.1

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 3.1

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 3.2 Idéal engendré par une partie

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

Proposition 3.2

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

Remarque. En particulier, l'idéal engendré par un unique élément $x \in \mathrm{A}$ est $x\mathrm{A}$.

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

Proposition 3.3

Soit $f : \mathrm{A} \to \mathrm{B}$ un morphisme d'anneaux. Alors $\operatorname{Ker} f$ est un idéal de A.

3.2 Arithmétique dans un anneau

Définition 3.3 Divisibilité

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

Proposition 3.4

La relation de divisibilité est réflexive et transitive.

Exercice 3.2

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 $u \in \mathrm{A}^\times$ (groupe des éléments inversibles de A) tel que $b = au$.

Proposition 3.5 Divisibilité et idéaux

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

Idéaux et éléments premiers entre eux

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

- On dit que deux idéaux I et J de A sont **premiers entre eux** si $\mathrm{I} + \mathrm{J} = \mathrm{A}$.
- On dit que deux éléments a et b de A sont **premiers entre eux** si $a\mathrm{A} + b\mathrm{A} = \mathrm{A}$, 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 $\mathrm{I}_1, \dots, \mathrm{I}_n$ de A sont **premiers entre eux dans leur ensemble** si $\sum_{i=1}^{n} \mathrm{I}_i = \mathrm{A}$.
- On dit que des éléments $a_1, \dots, a_n$ de A sont **premiers entre eux dans leur ensemble** si $\sum_{i=1}^{n} a_i\mathrm{A} = \mathrm{A}$, 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 $(\mathrm{A}, +, \times)$ un anneau commutatif.

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

4 Anneaux usuels

4.1 L'anneau $\mathbb{Z}$

Proposition 4.1

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

Proposition 4.2

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

Proposition 4.3 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 4.1 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 4.2 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 4.3 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 $a_1 \wedge \dots \wedge a_n$.

Définition 4.4 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 $a_1 \vee \dots \vee a_n$.

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

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

Proposition 4.4

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

Proposition 4.5

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

Proposition 4.6 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 4.5 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 4.6 PPCM de deux polynômes

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

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

Définition 4.7 PGCD de plusieurs polynômes

Soit $(\mathrm{P}_1, \dots, \mathrm{P}_n) \in \mathbb{K}[\mathrm{X}]^n$. On appelle PGCD de $\mathrm{P}_1, \dots, \mathrm{P}_n$ tout polynôme $\mathrm{D} \in \mathbb{K}[\mathrm{X}]$ tel que $\sum_{i=1}^{n} \mathrm{P}_i\mathbb{K}[\mathrm{X}] = \mathrm{D}\mathbb{K}[\mathrm{X}]$.
Il existe un unique PGCD unitaire ou nul de $\mathrm{P}_1, \dots, \mathrm{P}_n$ noté $\mathrm{P}_1 \wedge \dots \wedge \mathrm{P}_n$.

Définition 4.8 PPCM de plusieurs polynômes

Soit $(\mathrm{P}_1, \dots, \mathrm{P}_n) \in \mathbb{K}[\mathrm{X}]^n$. On appelle PPCM de $\mathrm{P}_1, \dots, \mathrm{P}_n$ tout polynôme $\mathrm{M} \in \mathbb{K}[\mathrm{X}]$ tel que $\bigcap_{i=1}^{n} \mathrm{P}_i\mathbb{K}[\mathrm{X}] = \mathrm{M}\mathbb{K}[\mathrm{X}]$.
Il existe un unique PPCM unitaire ou nul de $\mathrm{P}_1, \dots, \mathrm{P}_n$ noté $\mathrm{P}_1 \vee \dots \vee \mathrm{P}_n$.

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

Proposition 4.7 Multiplication sur $\mathbb{Z}/n\mathbb{Z}$

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

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

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 4.1

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

Proposition 4.8 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 $\overline{1}$.

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

Proposition 4.9

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

Théorème 4.1

Soit $p \in \mathbb{N}^*$. L'anneau $\mathbb{Z}/p\mathbb{Z}$ est intègre si et seulement si p est premier. Dans ce cas, $\mathbb{Z}/p\mathbb{Z}$ est un corps.

Proposition 4.10 Théorème des restes chinois

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

$$\left\{\begin{array}{ccc} \mathbb{Z}/mn\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ \overline{k}^{mn} & \longmapsto & (\overline{k}^m, \overline{k}^n) \end{array}\right.$$

est bien définie et est un isomorphisme d'anneaux.

Remarque. On peut généraliser ce résultat à plus de deux entiers naturels non nuls à condition que ces entiers soient premiers entre eux deux à deux.

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

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 par ticulière, 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 4.2

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

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

Définition 4.9 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 $[\![0, n-1]\!]$ premiers avec n.
L'application $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ est appelée **indicatrice d'Euler**.

Exemple 4.3

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

Exercice 4.1

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 4.11 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 4.12

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 4.13 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

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

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

Proposition 4.14 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.

5 Structure d'algèbre

Définition 5.1

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 :

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

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

(i) $(\mathrm{E}, +, .)$ est un $\mathbb{K}$-espace vectoriel ;

(ii) $(\mathrm{E}, +, \times)$ est un anneau ;

(iii) $\forall(\lambda, x, y) \in \mathbb{K} \times \mathrm{E}^2,\ \lambda.(x \times y) = (\lambda.x) \times y = x \times (\lambda.y)$.

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

Exemple 5.1

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

Définition 5.2 Sous-algèbre

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

(i) $\mathrm{F} \subset \mathrm{E}$;

(ii) F est un sous-espace vectoriel de E ;

(iii) F est un sous-anneau de E.

Proposition 5.1

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

Proposition 5.2 Caractérisation des sous-algèbres

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

(i) $\mathrm{F} \subset \mathrm{E}$;

(ii) $1_{\mathrm{E}} \in \mathrm{F}$;

(iii) $\forall (\lambda, \mu) \in \mathbb{K}^2,\ \forall (x, y) \in \mathrm{F}^2,\ \lambda.x + \mu.y \in \mathrm{F}$;

(iv) $\forall (x, y) \in \mathrm{F}^2,\ x \times y \in \mathrm{F}$.

Exemple 5.2

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

Définition 5.3 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 $f : E \to F$ telle que :

(i) $f(1_E) = 1_F$,

(ii) $\forall(\lambda,\mu) \in \mathbb{K}^2,\ \forall(x,y) \in E^2,\ f(\lambda.x + \mu.y) = \lambda.f(x) + \mu.f(y)$,

(iii) $\forall(x,y) \in E^2, f(x \times y) = f(x) \times f(y)$,

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.

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

Proposition 5.3 Images directe et réciproque d'une sous-algèbre par un morphisme d'algèbres

Soit $f : E \to F$ 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 5.4

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

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