

ANNEAUX ET ARITHMÉTIQUE

1 Anneaux

1.1 Définition et généralités

Définition 1.1 Anneau

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

- (i) $(A, +)$ 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 $(A, +, \times)$ 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).
- ♦ $(\mathbb{R}^{\mathbb{R}}, +, \times)$ est un anneau commutatif.
- ♦ L'ensemble des polynômes à coefficients dans \mathbb{R} (noté $\mathbb{R}[X]$) est aussi un anneau commutatif.

Notation 1.1

Soit A un anneau. On note A^* l'ensemble des éléments inversibles de A .

Proposition 1.1

Si $(A, +, \times)$ est un anneau, (A^*, \times) est un groupe.

Théorème 1.1 Règle de calcul dans les anneaux

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

- (i) $0_A \times a = a \times 0_A = 0_A$,
- (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 :

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

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



ATTENTION ! Tous les anneaux ne sont pas intègres. Nous verrons par exemple dans le cadre de l'algèbre linéaire des anneaux non intègres.

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 :

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

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

- (i) $B \subset A$;
- (ii) $1_A \in B$;
- (iii) $\forall (a, b) \in B^2, a - b \in B$;
- (iv) $\forall (a, b) \in B^2, a \times b \in B$.

Méthode Sous-anneaux en pratique

Il est souvent plus facile de montrer qu'un triplet $(A, +, \times)$ 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

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

1.3 Morphismes d'anneaux**Définition 1.4 Morphisme d'anneaux**

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

- (i) $f(1_A) = 1_B$,
- (ii) $\forall (a, b) \in A^2, f(a + b) = f(a) \oplus f(b)$,
- (iii) $\forall (a, b) \in A^2, f(a \times b) = f(a) \otimes f(b)$,

REMARQUE. En particulier, f est un morphisme de groupes de $(A, +)$ dans (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 $f : A \rightarrow B$ 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 $f : A \rightarrow B$ un morphisme d'anneaux. Alors $\text{Im } f$ est un sous-anneau de B .



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

2 Corps

2.1 Définition et premières 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 , $K^* = K \setminus \{0_K\}$.

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

Proposition 2.2 Sous-corps

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

- (i) $L \subset K$;
- (ii) $1_K \in L$;
- (iii) $\forall (x, y) \in L^2, x - y \in L$;
- (iv) $\forall (x, y) \in L \times (L \setminus \{0_K\}), x \times y^{-1} \in L$.

Méthode Sous-corps en pratique

Il est souvent plus facile de montrer qu'un triplet $(K, +, \times)$ 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 $(K, +, \times)$ et (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 $f : K \rightarrow L$ un morphisme de corps. Alors

1. $\forall x \in K^*, f(x) \in K^*$ 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 $(A, +, \times)$ 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 $x \in A$ 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 3.3

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

3.2 Arithmétique dans un anneau**Définition 3.3 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 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 $u \in A^*$ (groupe des éléments inversibles de A) tel que $b = au$.

Proposition 3.5 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 $\forall (a, b) \in A^2, ab \in I \implies (a \in I \text{ ou } b \in I)$.
- Un élément a de A est dit **premier** si l'idéal aA est premier et non nul.

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 Idéal annulateur d'un endomorphisme ou d'une matrice carrée

- (i) Soit u un endomorphisme d'un \mathbb{K} -espace vectoriel E . Le noyau du morphisme d'algèbres $P \in \mathbb{K}[X] \mapsto P(u) \in \mathcal{L}(E)$ est un idéal de $\mathbb{K}[X]$ appelé **idéal annulateur** de u .
- (ii) Soit $A \in \mathcal{M}_n(\mathbb{K})$. Le noyau du morphisme d'algèbres $P \in \mathbb{K}[X] \mapsto P(A) \in \mathcal{M}_n(\mathbb{K})$ est un idéal de $\mathbb{K}[X]$ appelé **idéal annulateur** de A .

Proposition 4.7 Polynôme minimal

- (i) Soit u un endomorphisme d'un espace vectoriel de **dimension finie**. L'idéal annulateur de u admet un unique générateur unitaire appelé **polynôme minimal** de u , noté π_u .
- (ii) Soit $A \in \mathcal{M}_n(\mathbb{K})$. L'idéal annulateur de A admet un unique générateur unitaire appelé **polynôme minimal** de A , noté π_A .

Définition 4.6 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 4.7 PPCM de deux polynômes

Soit $(P, Q) \in \mathbb{K}[X]^2$. On appelle PPCM de P et Q tout polynôme $M \in \mathbb{K}[X]$ 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 4.8 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 $P_1 \wedge \dots \wedge P_n$.

Définition 4.9 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 $P_1 \vee \dots \vee P_n$.

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

Proposition 4.8 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 4.9 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 4.10

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 4.11 Théorème des restes chinois

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

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

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 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 $bvm + avn$ 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 4.10 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 $\llbracket 1, n \rrbracket$ premiers avec n .

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

Exemple 4.3

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

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 4.12 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 4.13

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 4.14 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 4.15 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.