

Anneaux, corps

Aperçu

1. La structure d'anneau
2. Sous-structures
3. Morphisme d'anneaux
4. L'anneau $\mathbb{Z}/n\mathbb{Z}$
5. La structure d'espace vectoriel
6. La structure d'algèbre

1. La structure d'anneau

1.1 Anneaux

1.2 Éléments inversibles d'un anneau; corps

1.3 Anneau intègre

1.4 Calculs dans un anneau

2. Sous-structures

3. Morphisme d'anneaux

4. L'anneau $\mathbb{Z}/n\mathbb{Z}$

5. La structure d'espace vectoriel

6. La structure d'algèbre

1. La structure d'anneau

1.1 Anneaux

1.2 Éléments inversibles d'un anneau; corps

1.3 Anneau intègre

1.4 Calculs dans un anneau

2. Sous-structures

3. Morphisme d'anneaux

4. L'anneau $\mathbb{Z}/n\mathbb{Z}$

5. La structure d'espace vectoriel

6. La structure d'algèbre

D 1 Soit \top et \star deux lois de composition internes sur un ensemble E . On dit que la loi \star est **distributive** par rapport à la loi \top si l'on a

$$x \star (y \top z) = (x \star y) \top (x \star z) \quad (1)$$

$$(y \top z) \star x = (y \star x) \top (z \star x) \quad (2)$$

pour x, y, z dans E .

On remarquera que les deux égalités sont équivalentes si la loi \star est commutative.

E 2 Dans l'ensemble $\mathcal{P}(E)$ des parties d'un ensemble E , chacune des lois internes \cap et \cup est distributive par rapport à elle-même et à l'autre. Cela résulte des formules du type

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

D 3 On appelle **anneau** un ensemble A muni de deux lois de composition appelées respectivement **addition** et **multiplication**, satisfaisant aux axiomes suivants :

1. Pour l'addition, A est un groupe commutatif.
2. La multiplication est associative et possède un élément neutre.
3. La multiplication est distributive par rapport à l'addition.

On dit que l'anneau A est **commutatif** si sa multiplication est commutative.

Dans la suite On note $(x, y) \mapsto x + y$ l'addition et $(x, y) \mapsto xy$ la multiplication ; on note 0 (ou 0_A) l'élément neutre de l'addition et 1 (ou 1_A) celui de la multiplication. Enfin, on note $-x$ l'opposé de x pour l'addition. Pour économiser les parenthèses, on convient que la multiplication est prioritaire sur l'addition.

Les axiomes d'un anneau s'expriment donc par les identités suivantes :

- (1) $x + (y + z) = (x + y) + z$ (associativité de l'addition)
- (2) $x + y = y + x$ (commutativité de l'addition)
- (3) $0 + x = x + 0 = x$ (zéro)
- (4) $x + (-x) = (-x) + x = 0$ (opposé)
- (5) $x(yz) = (xy)z$ (associativité de la multiplication)
- (6) $x \cdot 1_A = 1_A \cdot x = x$ (élément unité)
- (7) $(x + y) \cdot z = xz + yz$ (distributivité à gauche)
- (8) $x \cdot (y + z) = xy + xz$ (distributivité à droite)

Enfin, l'anneau A est commutatif si l'on a $xy = yx$ pour x, y dans A .

Voici quelques anneaux que nous rencontrerons en MP2I

1. $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sont des anneaux intègres.
2. L'anneau des suites à valeur réelles, $(\mathbb{R}^{\mathbb{N}}, +, \cdot)$, est un anneau commutatif qui n'est pas intègre.
3. L'anneau des applications de \mathbb{R} dans \mathbb{R} , $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \cdot)$, est un anneau commutatif qui n'est pas intègre.
4. L'anneau des matrices carrées $n \times n$, $(\mathcal{M}_n(\mathbb{K}), +, \cdot)$ est un anneau qui n'est pas commutatif et possède des diviseurs de 0.
5. L'anneau des polynômes, $(\mathbb{K}[X], +, \cdot)$, est un anneau intègre (et donc commutatif).
6. ...

E 4

Voici les tables d'addition et multiplication de l'anneau $\mathbb{Z}/6\mathbb{Z} = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5} \}$.

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

et

\cdot	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

1. La structure d'anneau

1.1 Anneaux

1.2 Éléments inversibles d'un anneau; corps

1.3 Anneau intègre

1.4 Calculs dans un anneau

2. Sous-structures

3. Morphisme d'anneaux

4. L'anneau $\mathbb{Z}/n\mathbb{Z}$

5. La structure d'espace vectoriel

6. La structure d'algèbre

D 5 Soit $(A, +, \cdot)$ un anneau.

- ▶ Si $x \in A$ admet un inverse pour la multiplication, on dit que x est un **élément inversible** de A
- ▶ L'ensemble des éléments inversibles de A se note A^\times ou $U(A)^a$.

^aLa notation $U(A)$ provient du fait que l'on dit aussi que x est une **unité** de A pour dire que x est inversible, mais nous n'utiliserons pas cette terminologie dangereuse.

T 6 Soit $(A, +, \cdot)$ un anneau.

1. Si x et y sont deux éléments inversibles d'un anneau A , alors x^{-1} et xy le sont aussi et

$$(x^{-1})^{-1} = x \quad \text{et} \quad (x \cdot y)^{-1} = y^{-1} \cdot x^{-1}.$$

2. (A^\times, \cdot) est un groupe appelé **groupe multiplicatif de l'anneau A** dont 1_A est l'élément neutre.

E 7 $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$.

E 8 Le groupe multiplicatif de $(\mathbb{Z}, +, \cdot)$ est $\{-1, 1\} = \mathbb{U}_2$.

D 9 On dit qu'un anneau \mathbb{K} est un **corps** s'il est commutatif, non réduit à 0 et si tout élément non nul de \mathbb{K} est inversible.

E 10 Les corps usuels sont \mathbb{Q} , \mathbb{R} et \mathbb{C} .

E 11 Il existe un corps à deux éléments $A = \{0, 1\}$ où l'on a $0 + 0 = 1 + 1 = 0$, $0 + 1 = 1 + 0 = 1$, et la multiplication usuelle ;

E 12 Le groupe multiplicatif de $\mathbb{Z}/6\mathbb{Z}$ est $\{1, 5\}$. L'anneau $\mathbb{Z}/6\mathbb{Z}$ n'est donc pas un corps.

1. La structure d'anneau

1.1 Anneaux

1.2 Éléments inversibles d'un anneau; corps

1.3 Anneau intègre

1.4 Calculs dans un anneau

2. Sous-structures

3. Morphisme d'anneaux

4. L'anneau $\mathbb{Z}/n\mathbb{Z}$

5. La structure d'espace vectoriel

6. La structure d'algèbre

D 13 On dit qu'un anneau A est **intègre** s'il est commutatif, non réduit à 0, et si le produit de deux éléments non nuls de A est non nul, ou encore

$$\forall (x, y) \in A^2, xy = 0 \implies (x = 0 \text{ ou } y = 0).$$

P 14 Soit A un anneau intègre, alors on a une règle de simplification pour la multiplication

$$\forall (x, y, a) \in A^3, (ax = ay \text{ et } a \neq 0) \implies x = y$$

$$\forall (x, y, a) \in A^3, (xa = ya \text{ et } a \neq 0) \implies x = y$$

On retiendra surtout que ceci est faux dans un anneau quelconque.

E 15 L'ensemble \mathbb{Z} des entiers relatifs muni de l'addition et la multiplication usuelle, est un anneau intègre.

E 16 Soit E l'anneau des applications de \mathbb{R} dans \mathbb{R} et considérons les deux éléments f et g de cet anneau définis comme suit

$$f(x) = \begin{cases} x & \text{si } x \geq 0, \\ 0 & \text{si } x \leq 0, \end{cases} \quad \text{et} \quad g(x) = \begin{cases} 0 & \text{si } x \geq 0, \\ x & \text{si } x \leq 0, \end{cases}$$

Il est clair que

$$\forall x \in \mathbb{R}, f(x)g(x) = 0,$$

et par suite que $fg = 0$ dans l'anneau considéré; néanmoins on a $f \neq 0$ et $g \neq 0$ (car l'élément 0 de l'anneau E est la fonction qui, en *chaque* $x \in \mathbb{R}$ *sans exception*, prend la valeur 0).

1. La structure d'anneau

1.1 Anneaux

1.2 Éléments inversibles d'un anneau; corps

1.3 Anneau intègre

1.4 Calculs dans un anneau

2. Sous-structures

3. Morphisme d'anneaux

4. L'anneau $\mathbb{Z}/n\mathbb{Z}$

5. La structure d'espace vectoriel

6. La structure d'algèbre

Si x est un élément de A , on a toujours les notations $n.x$ ($n \in \mathbb{Z}$) et x^n ($n \in \mathbb{N}$) :

$$nx = \begin{cases} \overbrace{x + \cdots + x}^n & n > 0 \\ 0 & n = 0, \\ \underbrace{(-x) + \cdots + (-x)}_{-n} & n < 0 \end{cases}, \quad x^n = \begin{cases} \overbrace{x \cdots x}^n & n > 0 \\ 1 & n = 0 \\ \underbrace{x^{-1} \cdots x^{-1}}_{-n} & n < 0 \text{ et } x \text{ inversible} \end{cases}$$

P 17 Soient A un anneau et x, y des éléments de l'anneau A .

1. $x.0 = 0.x = 0$.

2. $x.(-y) = (-x).y = -(xy)$ et $(-x)(-y) = xy$.

(Règle des signes)

3. Pour $n \in \mathbb{N}$, on a

$$(-x)^n = \begin{cases} x^n & \text{si } n \text{ est pair} \\ -x^n & \text{si } n \text{ est impair.} \end{cases}$$

Formule qui reste valable aussi si x est inversible et $n \in \mathbb{Z}$.

P 18 Conséquence de la distributivité

Soit A un anneau, n un entier > 0 . Alors pour $a, x_1, x_2, \dots, x_n \in A$, on a

$$a \left(\sum_{k=1}^n x_k \right) = \sum_{k=1}^n (ax_k) \quad \text{et} \quad \left(\sum_{k=1}^n x_k \right) a = \sum_{k=1}^n (x_k a).$$

T 19 Soient A un anneau, $(x, y) \in A^2$ deux éléments qui commutent ($xy = yx$), alors pour tout entier $n \in \mathbb{N}$,

$$(x + y)^n = \sum_{p=0}^n \binom{n}{p} x^{n-p} y^p;$$

$$x^{n+1} - y^{n+1} = (x - y)(x^n + x^{n-1}y + \cdots + xy^{n-1} + y^n) = (x - y) \sum_{p=0}^n x^{n-p} y^p$$

C 20 Calcul d'une progression géométrique

Soient A un anneau, a un élément de A et n un entier > 0 . Alors

$$1 - a^n = (1 - a)(1 + a + a^2 + \cdots + a^{n-1}).$$

1. La structure d'anneau

2. Sous-structures

2.1 Sous-anneaux

2.2 Idéaux d'un anneau commutatif

3. Morphisme d'anneaux

4. L'anneau $\mathbb{Z}/n\mathbb{Z}$

5. La structure d'espace vectoriel

6. La structure d'algèbre

1. La structure d'anneau

2. Sous-structures

2.1 Sous-anneaux

2.2 Idéaux d'un anneau commutatif

3. Morphisme d'anneaux

4. L'anneau $\mathbb{Z}/n\mathbb{Z}$

5. La structure d'espace vectoriel

6. La structure d'algèbre

D 21 Soit $(A, +, \cdot)$ un anneau et B une partie de A . On dit que B est un **sous-anneau** de A lorsque

- ▶ $1_A \in B$,
- ▶ B est un sous groupe de $(A, +)$,
- ▶ B est stable par produit : $\forall (x, y) \in B^2, xy \in B$.

P 22 *Si B est un sous anneau de A , alors B muni des deux lois induites a une structure d'anneau.*

E 23 ▶ \mathbb{Z} est un sous-anneau de \mathbb{Q} , de \mathbb{R} , de \mathbb{C} .

▶ \mathbb{Q} est un sous-anneau de \mathbb{R} , de \mathbb{C} .

▶ \mathbb{R} est un sous-anneau de \mathbb{C} .

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

E 24 Le seul sous-anneau de \mathbb{Z} est \mathbb{Z} .

Pour un entier $a \geq 2$, l'ensemble $a\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$ et il est stable par produit ; mais $1 \notin a\mathbb{Z}$. $a\mathbb{Z}$ n'est donc pas un sous-anneau de \mathbb{Z} .

1. La structure d'anneau

2. Sous-structures

2.1 Sous-anneaux

2.2 Idéaux d'un anneau commutatif

3. Morphisme d'anneaux

4. L'anneau $\mathbb{Z}/n\mathbb{Z}$

5. La structure d'espace vectoriel

6. La structure d'algèbre

D 25 Soit $(A, +, \cdot)$ un anneau *commutatif* et I une partie de A . On dit que I est un **idéal bilatère** de A lorsque

- ▶ I est un sous groupe de $(A, +)$,
- ▶ $\forall a \in A, \forall x \in I, ax \in I$.

Dans la pratique, on parlera simplement d'**idéal** de A .

R Tout idéal d'un anneau A est un sous-groupe de $(A, +)$, l'inverse peut être faux : \mathbb{Z} est un sous-anneau, mais pas un idéal, de \mathbb{Q} .

T 26 Soit A une partie de \mathbb{Z} . Les assertions suivantes sont équivalentes:

1. A est un sous-groupe de \mathbb{Z} .
2. A est un idéal de \mathbb{Z} .
3. Il existe $n \in \mathbb{N}$ tel que $A = n\mathbb{Z}$.

S'il en est ainsi, l'entier n est unique.

D 27 Soit $(A, +, \cdot)$ un anneau commutatif et $x \in A$. L'ensemble

$$xA = \{ xa \mid a \in A \}$$

est un idéal de A . C'est le plus petit idéal contenant x : on l'appelle **idéal engendré par l'élément x** .

1. La structure d'anneau

2. Sous-structures

3. Morphisme d'anneaux

4. L'anneau $\mathbb{Z}/n\mathbb{Z}$

5. La structure d'espace vectoriel

6. La structure d'algèbre

D 28 Soient A, B deux anneaux. Une application $f : A \rightarrow B$ est appelée **morphisme d'anneaux** si elle vérifie les conditions suivantes:

- ▶ Pour tous $x, y \in A$, $f(x + y) = f(x) + f(y)$.
- ▶ Pour tous $x, y \in A$, $f(xy) = f(x)f(y)$.
- ▶ $f(1_A) = 1_B$.

Si de plus f est bijective, on dit que c'est un **isomorphisme d'anneaux** de A sur B .

P 29 *La composée de deux morphismes de anneaux est un morphisme de anneaux.*

P 30 *Si un morphisme de anneaux est bijectif, l'application réciproque est encore un morphisme de anneaux.*

T 31 Soit $f : A \rightarrow B$ un morphisme d'anneaux.

1. Si A' est un sous-anneau de A , alors l'image directe

$$f(A') = \{ f(x) \mid x \in A' \} = \{ y \in B \mid \exists x \in A', y = f(x) \}$$

est un sous-anneau de B .

En particulier, $\text{Im}(f) = f(A)$ est un sous-anneau de B .

2. Si B' est un sous-anneau de B , alors l'image réciproque

$$f^{-1}(B') = \{ x \in A \mid f(x) \in B' \}$$

est un sous-anneau de A .

3. Supposons A commutatif.

Si J est un idéal de B , alors l'image réciproque

$$f^{-1}(J) = \{ x \in A \mid f(x) \in J \}$$

est un idéal de A .

4. Le noyau $\ker(f)$ de f est un idéal de A .

Un morphisme d'anneaux étant a fortiori un morphisme de groupes, on retrouve immédiatement les résultats suivants.

T 32 *Soit $f : A \rightarrow B$ un morphisme d'anneaux.*

1. *Pour que f soit injectif, il faut, et il suffit que son noyau soit $\{0_A\}$.*
2. *Pour que f soit surjectif, il faut, et il suffit que son image soit B .*
3. *Soit $b \in B$.*
 - ▶ *Si $b \notin \text{Im}(f)$, l'équation $f(x) = b$ d'inconnue $x \in A$ n'a pas de solution.*
 - ▶ *Si $b \in \text{Im}(f)$, alors en notant x_0 un antécédent de b par f , on a*

$$\{ x \in A \mid f(x) = b \} = x_0 + \ker(f) = \{ x_0 + h \mid h \in \ker(f) \}.$$

1. La structure d'anneau

2. Sous-structures

3. Morphisme d'anneaux

4. L'anneau $\mathbb{Z}/n\mathbb{Z}$

4.1 Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

4.2 L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$

5. La structure d'espace vectoriel

6. La structure d'algèbre

1. La structure d'anneau

2. Sous-structures

3. Morphisme d'anneaux

4. L'anneau $\mathbb{Z}/n\mathbb{Z}$

4.1 Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

4.2 L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$

5. La structure d'espace vectoriel

6. La structure d'algèbre

N

Soit $n \in \mathbb{N}$. La relation de congruence modulo n , définie par

$$x \equiv y \pmod{n} \iff \exists k \in \mathbb{Z}, y = x + kn$$

est une relation d'équivalence.

La classe d'équivalence de $x \in \mathbb{Z}$ est souvent notée \dot{x} ou \overline{x}

$$\overline{x} = \{ x + kn \mid k \in \mathbb{Z} \}.$$

On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence modulo n .

P 33 Soit $n \in \mathbb{N}$, $n \geq 1$. Les éléments de $\mathbb{Z}/n\mathbb{Z}$ sont exactement

$$\overline{0}, \overline{1}, \dots, \overline{n-1}$$

et ils sont deux à deux distincts. L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est donc fini de cardinal n .

T 34 Il existe une loi de composition interne, appelée addition, sur l'ensemble $\mathbb{Z}/n\mathbb{Z}$

$$\begin{aligned}\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} &\rightarrow \mathbb{Z}/n\mathbb{Z} \\ (a, b) &\mapsto a + b\end{aligned}$$

telle que pour tout $(x, y) \in \mathbb{Z}^2$,

$$\overline{x} + \overline{y} = \overline{x + y}$$

Muni de cette addition, $\mathbb{Z}/n\mathbb{Z}$ est un groupe abélien.

1. L'élément neutre de $(\mathbb{Z}/n\mathbb{Z}, +)$ est $\overline{0}$, l'opposé de \overline{x} est $\overline{-x}$.
2. L'application $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ est un morphisme surjectif de noyau $n\mathbb{Z}$.
$$x \mapsto \overline{x}$$
3. Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique.
 - ▶ $(\mathbb{Z}/n\mathbb{Z}, +)$ est isomorphe à (\mathbb{U}_n, \cdot) .
 - ▶ Les générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$ sont les éléments \overline{k} tels que $\text{pgcd}(k, n) = 1$.

Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ s'appelle le **groupe-quotient de \mathbb{Z} par $n\mathbb{Z}$** .

R Description des groupes monogènes

Soit $G = \langle a \rangle$ un groupe monogène. Alors,

1. Si a est d'ordre infini, alors G est isomorphe au groupe $(\mathbb{Z}, +)$.
2. Si a est d'ordre fini $p \in \mathbb{N}^*$, alors G est isomorphe au groupe $(\mathbb{Z}/p\mathbb{Z}, +)$.

1. La structure d'anneau

2. Sous-structures

3. Morphisme d'anneaux

4. L'anneau $\mathbb{Z}/n\mathbb{Z}$

4.1 Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

4.2 L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$

5. La structure d'espace vectoriel

6. La structure d'algèbre

T 35 Il existe une loi de composition interne, appelée multiplication, sur l'ensemble $\mathbb{Z}/n\mathbb{Z}$

$$\begin{aligned}\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} &\rightarrow \mathbb{Z}/n\mathbb{Z} \\ (a, b) &\mapsto a \cdot b = ab\end{aligned}$$

telle que pour tout $(x, y) \in \mathbb{Z}^2$,

$$\overline{x} \cdot \overline{y} = \overline{xy}$$

Muni de ces deux lois, $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau commutatif.

1. Les éléments neutres de $\mathbb{Z}/n\mathbb{Z}$ sont $\overline{0}$ et $\overline{1}$.
2. Les éléments inversibles de $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ sont les éléments \overline{k} tels que $\text{pgcd}(k, n) = 1$.
3. L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est intègre si, et seulement si n est premier.
4. L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un corps si, et seulement si n est premier.

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ s'appelle le **anneau-quotient de \mathbb{Z} par $n\mathbb{Z}$** .

D 36 Le nombre des entiers k vérifiant

$$1 \leq k \leq n \quad \text{et} \quad \text{pgcd}(k, n) = 1$$

est noté $\varphi(n)$. L'application $\varphi : \mathbb{N}^* \rightarrow \mathbb{N}^*$ ainsi définie s'appelle **indicateur d'Euler**.

1. La structure d'anneau

2. Sous-structures

3. Morphisme d'anneaux

4. L'anneau $\mathbb{Z}/n\mathbb{Z}$

5. La structure d'espace vectoriel

6. La structure d'algèbre

D 37 Étant donné un corps $(\mathbb{K}, +, \cdot)$, d'éléments neutres $0_{\mathbb{K}}$ et $1_{\mathbb{K}}$, on appelle **espace vectoriel sur \mathbb{K}** un ensemble E muni d'une structure algébrique définie par la donnée

1. d'une loi de composition interne, appelée **addition**

$$\begin{aligned} E \times E &\rightarrow E \\ (x, y) &\mapsto x + y \end{aligned}$$

telle que $(E, +)$ soit un groupe commutatif.

2. D'une loi d'action appelée **multiplication externe**

$$\begin{aligned} \mathbb{K} \times E &\rightarrow E \\ (\lambda, x) &\mapsto \lambda \cdot x \end{aligned}$$

qui satisfait aux axiomes suivants ^a

- ▶ Pour tous $\lambda \in \mathbb{K}, x \in E, y \in E$, $\lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y$.
- ▶ Pour tous $\lambda \in \mathbb{K}, \mu \in \mathbb{K}, x \in E$, $(\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x$.
- ▶ Pour tous $\lambda \in \mathbb{K}, \mu \in \mathbb{K}, x \in E$, $(\lambda \cdot \mu) \cdot x = \lambda \cdot (\mu \cdot x)$.
- ▶ Pour tout $x \in E$, $1_{\mathbb{K}} \cdot x = x$.

^aRègle bien connue : pour économiser les parenthèses, on convient que la multiplication est prioritaire sur l'addition.

Les morphismes d'espaces vectoriels portent le nom d'**applications linéaires**.

D 38 Soient $(E, +, \cdot)$ et (F, \oplus, \odot) deux espaces vectoriels sur le même corps \mathbb{K} . On appelle **application linéaire** de E dans F toute application $f : E \rightarrow F$ telle que pour tous $u, v \in E$, et tout $\alpha \in \mathbb{K}$,

$$f(u + v) = f(u) \oplus f(v) \quad \text{et} \quad f(\alpha \cdot u) = \alpha \odot f(u).$$

1. La structure d'anneau

2. Sous-structures

3. Morphisme d'anneaux

4. L'anneau $\mathbb{Z}/n\mathbb{Z}$

5. La structure d'espace vectoriel

6. La structure d'algèbre

D 39 On appelle \mathbb{K} -algèbre un quadruplet $(A, +, *, \cdot)$ tel que

- ▶ $(A, +, *)$ est un anneau.
- ▶ $(A, +, \cdot)$ est un \mathbb{K} -espace vectoriel.
- ▶ $\forall \lambda \in \mathbb{K}, \forall (x, y) \in A^2, (\lambda \cdot x) * y = x * (\lambda \cdot y) = \lambda \cdot (x * y).$

D 40 Soient $(A, +, *, \cdot)$ et $(B, \oplus, \otimes, \odot)$ deux algèbres sur le même corps \mathbb{K} . On appelle **morphisme d'algèbre** de A dans B toute application $f : A \rightarrow B$ telle que pour tous $u, v \in A$, et tout $\alpha \in \mathbb{K}$,

$$f(u + v) = f(u) \oplus f(v)$$

$$f(\alpha \cdot u) = \alpha \odot f(u)$$

$$f(1_A) = 1_B$$

$$f(u * v) = f(u) \otimes f(v)$$