

Licence 1 Maths-Info-Ing/ 2024-2025 / Cours
d'Algèbre / Chapitre 3:
STRUCTURES ALGÉBRIQUES

Enseignant: AKEKE E. D.

October 21, 2024



1 Chapitre 3: STRUCTURES D'ANNEAUX ET CORPS

- Définition et exemples
- L'anneau quotient $\mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N}$
 - Relation de congruence modulo un entier naturel
 - Compatibilité avec l'addition et la multiplication
 - Classes d'équivalence modulo un entier
 - Sous-groupes du groupe quotient $\frac{\mathbb{Z}}{n\mathbb{Z}}$
- Calculs dans un anneau
 - Propriétés
 - Éléments inversibles d'un anneau
 - Éléments inversibles de l'anneau quotient $\frac{\mathbb{Z}}{n\mathbb{Z}}$
- Sous-anneaux
- Idéal d'un anneau commutatif
- Morphisme d'anneaux
- Corps



Définition

Soit $(A, +, \cdot)$ un ensemble muni de deux lois de composition internes. On dit que $(A, +, \cdot)$ est un **anneau** si les conditions suivantes sont satisfaites:

- i) $(A, +)$ est un groupe abélien,
- ii) la seconde loi " \cdot " est associative, c'est à dire

$$\forall a, b, c \in A, \quad a(bc) = (ab)c$$

- iii) la seconde loi est distributive par rapport à la première, c'est à dire:

$$\forall a, b, c \in A, \quad a(b+c) = ab+ac \quad \text{et} \quad (a+b)c = ac+bc.$$





Si de plus la loi \cdot est commutative, on dit que A est un **anneau commutatif**.

Si la loi \cdot possède un élément neutre, on dit que A est un **anneau unitaire**, cet élément neutre se note 1 ou 1_A et s'appelle **élément unité**.



Exemples 1

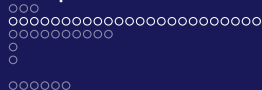
- 1) $(\mathbb{Z}, +, \times)$ est un anneau commutatif unitaire,
- 2) $(\mathbb{D}, +, \times)$ est un anneau commutatif unitaire
- 3) $(\mathbb{Q}, +, \times)$ est un anneau commutatif unitaire,
- 4) $(\mathbb{Q}, +, \times)$ est un anneau commutatif unitaire
- 5) $(\mathbb{R}, +, \times)$ est un anneau commutatif unitaire
- 6) $(\mathbb{C}, +, \times)$ est un anneau commutatif unitaire



Exemples 2

Si $(A, +, \times)$ est un anneau unitaire et E un ensemble non vide alors l'ensemble $\mathcal{A}(E, A)$ des applications de E vers A , est un anneau unitaire pour les lois définies par: pour tout $f, g \in \mathcal{A}(E, A)$,

$$f + g : x \longmapsto f(x) + g(x) \quad \text{et} \quad f.g : x \longmapsto f(x).g(x).$$



Définition

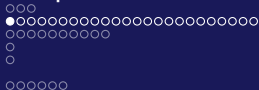
Soit $n \in \mathbb{N}$. Étant donnés $x, y \in \mathbb{Z}$, on dit que x est **congru** à y **modulo** n si et seulement si n divise $y - x$. On écrit alors

$$x \equiv y \pmod{n}$$

Exemples

a) $14 \equiv 2 \pmod{3}$

b) $25 \equiv 0 \pmod{5}$



Proposition

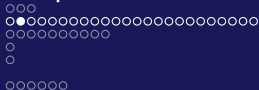
La relation de congruence modulo n est une relation d'équivalence sur \mathbb{Z} , c'est à dire qu'on a les propriétés suivantes:

- (i) *Pour tout entier $x \in \mathbb{Z}$ on a*

$$x \equiv x \pmod{n}$$
- (ii) *Pour entiers $x, y \in \mathbb{Z}$,*

$$x \equiv y \pmod{n} \text{ implique que } y \equiv x \pmod{n}$$
- (iii) *Pour entiers $x, y, z \in \mathbb{Z}$,*

$$\text{si } x \equiv y \pmod{n} \text{ et } y \equiv z \pmod{n} \text{ alors } x \equiv z \pmod{n}.$$



Preuve

Réflexivité:

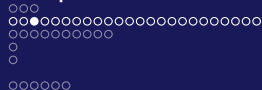
pour tout $x \in \mathbb{Z}$, on a $x - x = 0$ et on sait que n divise 0, d'où n divise $x - x$ et

$$x \equiv x \pmod{n}$$

Symétrie:

Soient $x, y \in \mathbb{Z}$ tels que $x \equiv y \pmod{n}$. Alors il existe $k \in \mathbb{N}$ tel que $y - x = nk$. Ainsi, on a $x - y = n(-k)$ avec $-k \in \mathbb{Z}$, donc $y \equiv x \pmod{n}$. En somme,

$$x \equiv y \pmod{n} \Leftrightarrow y \equiv x \pmod{n}$$



Transitivité:

Soient $x, y, z \in \mathbb{Z}$ tels que

$$x \equiv y \pmod{n} \quad \text{et} \quad y \equiv z \pmod{n}.$$

Alors il existe des entiers $k, q \in \mathbb{Z}$ tels que

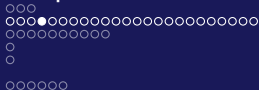
$$y - x = nk \quad \text{et} \quad z - y = nq.$$

On déduit que

$$z - x = n(k + q)$$

avec $k + q \in \mathbb{Z}$, donc $x \equiv z \pmod{n}$. En somme,

$$\text{si } x \equiv y \pmod{n} \quad \text{et} \quad y \equiv z \pmod{n} \quad \text{alors} \quad x \equiv z \pmod{n}$$



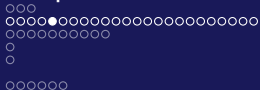
La relation de congruence modulo n étant à la fois **réflexive**, **symétrique** et **transitive** sur \mathbb{Z} , c'est donc une **relation d'équivalence** sur \mathbb{Z} .

Définition

Pour tout $x \in \mathbb{Z}$, on note \bar{x} l'ensemble de tous les éléments $y \in \mathbb{Z}$ qui sont congrus à x modulo n . C'est par définition la **classe d'équivalence** de x modulo n . Ainsi, on a

$$\bar{x} = \{y \in \mathbb{Z} / x \equiv y \pmod{n}\}$$

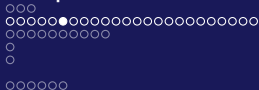
(dans certains ouvrages, cet ensemble est noté $x + n\mathbb{Z}$)



Propriétés

Soient a, b, c, d des entiers relatifs.

- (1) *Si $a \equiv b \pmod n$ et $c \equiv d \pmod n$ alors $a + c \equiv b + d \pmod n$*
- (2) *Si $a \equiv b \pmod n$ et $c \equiv d \pmod n$ alors $a \times c \equiv b \times d \pmod n$*



Preuve Supposons $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$. Il existe $k, q \in \mathbb{Z}$ tels que $b - a = nk$ et $d - c = nq$. (1) Alors

$$(b + d) - (a + c) = n(k + q)$$

avec $k + q \in \mathbb{Z}$, donc

$$a + c \equiv b + d \pmod{n}.$$

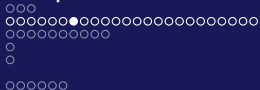
(2) On a $b = a + nk$ et $d = c + nq$. Par conséquent,

$$bd = (a + nk)(c + nq)$$

autrement dit, $bd = ac + anq + nkc + n^2kq$. Ainsi

$$bd - ac = n(aq + kc + nkq)$$

avec $aq + kc + nkq \in \mathbb{Z}$, d'où $a \times c \equiv b \times d \pmod{n}$. □



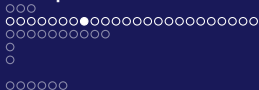
Corollaire

Soient $x, y \in \mathbb{Z}$

$$(i) \quad \forall k \in \mathbb{N}, \quad x \equiv y \pmod{n} \Rightarrow kx \equiv ky \pmod{n}$$

$$(ii) \quad \forall k \in \mathbb{N}^*, \quad x \equiv y \pmod{n} \Rightarrow x^k \equiv y^k \pmod{n}$$

Preuve (exercice facile!)



Définition

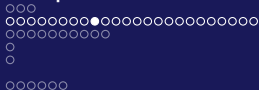
Soit $n \in \mathbb{N}$ et soit $x \in \mathbb{Z}$.

La **classe d'équivalence** de x , **modulo** n , est par définition l'ensemble de tous les entiers $y \in \mathbb{Z}$ tels que

$$x \equiv y \pmod{n}$$

Cet ensemble est souvent noté \bar{x} . Ainsi, on a

$$\bar{x} = \{ y \in \mathbb{Z} / x \equiv y \pmod{n} \}$$



Remarques (Important!)

Soit $n \in \mathbb{N}$

(1) Soient $x, y \in \mathbb{Z}$. On a l'équivalence

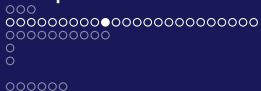
$$x \equiv y \pmod{n} \Leftrightarrow \bar{x} = \bar{y}$$

(2) Soit $x \in \mathbb{Z}$. D'après la division euclidienne de x par n , il existe des entiers relatifs q, r tels que

$$x = nq + r \quad \text{avec la condition} \quad 0 \leq r < n$$

On en déduit que n divise $x - r$, donc

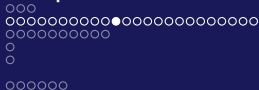
$$x \equiv r \pmod{n}$$



Ce qui équivaut à dire que, modulo n , on a

$$\bar{x} = \bar{r}$$

où r est le reste de la division euclidienne de x par n .



Exemple

Soit $n = 7$.

Pour $x = 2025$, on sait que

$$2025 = 7 \times 289 + 2$$

donc

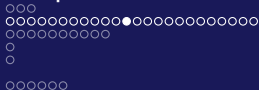
$$2025 \equiv 2 \pmod{7}$$

Ainsi modulo 7, on a

$$\overline{2025} = \overline{2}$$

Pour $x = 789$, on sait que $789 = 7 \times 112 + 5$ donc modulo 7, on a

$$\overline{789} = \overline{5}$$



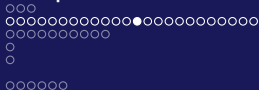
Notons par \mathbb{Z}_n l'ensemble des classes d'équivalence modulo n . Cet ensemble est par définition l'**ensemble quotient modulo n** .

Proposition

Soit $n \in \mathbb{N}$, $n \neq 0$.

L'ensemble quotient \mathbb{Z}_n est fini, précisément cet ensemble contient exactement n éléments.

$$\mathbb{Z}_n = \{ \bar{0}, \dots, \overline{n-1} \}$$



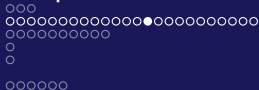
On définit sur l'ensemble \mathbb{Z}_n deux lois de composition internes:

Définition

Pour tout $x, y \in \mathbb{Z}$, on pose

$$\bar{x} + \bar{y} = \overline{x + y} \quad \text{et} \quad \bar{x} \times \bar{y} = \overline{x \times y}.$$

Ces deux lois sont bien définies d'après les propriétés de compatibilité avec l'addition et la multiplication (cf. Propriété 1)



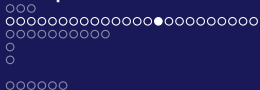
Théorème

Pour tout entier $n \in \mathbb{N}$, $(\mathbb{Z}_n, +, \times)$ est un anneau commutatif unitaire.

*Cet anneau est souvent noté $\frac{\mathbb{Z}}{n\mathbb{Z}}$, appelé l'**anneau quotient modulo n** . Le groupe $(\mathbb{Z}_n, +)$ est aussi noté $\frac{\mathbb{Z}}{n\mathbb{Z}}$ et appelé le **groupe quotient modulo n** .*

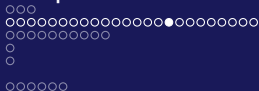
Preuve (voir support de cours)

- 1) L'élément neutre pour la loi quotient $+$ est $\bar{0}$,
- 2) L'élément neutre pour la loi quotient \times est $\bar{1}$,
- 3) Le symétrique noté $-\bar{x}$ de \bar{x} dans le groupe $(\frac{\mathbb{Z}}{n\mathbb{Z}}, +)$ est $\overline{-x}$.



Exercice

- (1) Établir la table de $\frac{\mathbb{Z}}{2\mathbb{Z}}$ la loi $+$, puis la loi \times
- (2) Mêmes questions avec les anneaux $\frac{\mathbb{Z}}{3\mathbb{Z}}$, $\frac{\mathbb{Z}}{6\mathbb{Z}}$.



Corrections

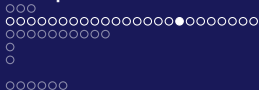
1) La table de $\frac{\mathbb{Z}}{2\mathbb{Z}}$ pour la loi $+$, puis la loi \times .

On a

$$\frac{\mathbb{Z}}{2\mathbb{Z}} = \{\bar{0}, \bar{1}\}$$

$+$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

\times	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

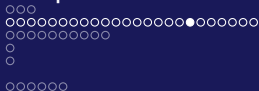


La table de $\frac{\mathbb{Z}}{3\mathbb{Z}}$ pour la loi $+$, puis la loi \times .

On a $\frac{\mathbb{Z}}{3\mathbb{Z}} = \{\bar{0}, \bar{1}, \bar{2}\}$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

\times	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$



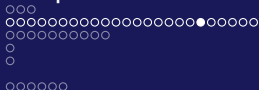
La table de $\frac{\mathbb{Z}}{6\mathbb{Z}}$ pour la loi $+$, puis la loi \times .

On a

$$\frac{\mathbb{Z}}{6\mathbb{Z}} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$$

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

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



Théorème

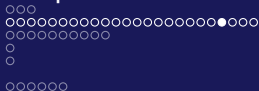
Soient $n \in \mathbb{N}$ et $d \in \mathbb{N}$. Alors d divise n si et seulement si le groupe $(\frac{\mathbb{Z}}{n\mathbb{Z}}, +)$ admet un (**unique**) sous-groupe de cardinal d . Précisément, les sous-groupes du groupe $(\frac{\mathbb{Z}}{n\mathbb{Z}}, +)$ sont de la forme $H_d = \langle \overline{(\frac{n}{d})} \rangle$ où $d \in \mathbb{N}$ divise n et $\overline{(\frac{n}{d})}$ est la classe d'équivalence modulo n de l'entier $\frac{n}{d}$.

NB: nous avons noté par $\langle \overline{(\frac{n}{d})} \rangle$ le sous-groupe engendré par $\overline{(\frac{n}{d})}$ dans le groupe $(\frac{\mathbb{Z}}{n\mathbb{Z}}, +)$.



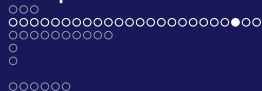
Remarques

Soit $n \in \mathbb{N}$. D'après le théorème précédent, le nombre de sous-groupes du groupe $(\frac{\mathbb{Z}}{n\mathbb{Z}}, +)$ est égal au nombre d'entiers naturels qui divisent n .



Exercice

- (1) Déterminer tous les sous-groupes du groupe $(\frac{\mathbb{Z}}{24\mathbb{Z}}, +)$.
- (2) Déterminer tous les sous-groupes du groupe $(\frac{\mathbb{Z}}{29\mathbb{Z}}, +)$.

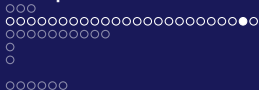


CORRECTION

1) Déterminons tous les sous-groupes du groupe $(\frac{\mathbb{Z}}{24\mathbb{Z}}, +)$.
 D'après le théorème précédent, le nombre de sous-groupes du groupe $(\frac{\mathbb{Z}}{24\mathbb{Z}}, +)$ est égal au nombre d'entiers qui divisent 24.
 L'ensemble des entiers qui divisent 24 est

$$D_{24} = \{ 1, 2, 3, 4, 6, 8, 12, 24 \}$$

Ainsi, il y a 8 sous-groupes dans le groupe quotient $(\frac{\mathbb{Z}}{24\mathbb{Z}}, +)$.



Déterminons ces sous-groupes

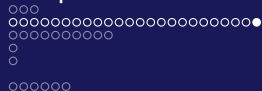
On a

$$H_1 = \langle \overline{\left(\frac{24}{1}\right)} \rangle = \langle \bar{0} \rangle = \{\bar{0}\},$$

$$H_2 = \langle \overline{\left(\frac{24}{2}\right)} \rangle = \langle \bar{12} \rangle = \{\bar{0}, \bar{12}\}$$

$$H_3 = \langle \overline{\left(\frac{24}{3}\right)} \rangle = \langle \bar{8} \rangle = \{\bar{0}, \bar{8}, \bar{16}\},$$

$$H_4 = \langle \overline{\left(\frac{24}{4}\right)} \rangle = \langle \bar{6} \rangle = \{\bar{0}, \bar{6}, \bar{12}, \bar{18}\},$$

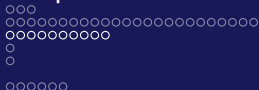


$$H_6 = \langle \overline{\left(\frac{24}{6}\right)} \rangle = \langle \bar{4} \rangle = \{\bar{0}, \bar{4}, \bar{8}, \bar{12}, \bar{16}, \bar{20}\},$$

$$H_8 = \langle \overline{\left(\frac{24}{8}\right)} \rangle = \langle \bar{3} \rangle = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}, \bar{12}, \bar{15}, \bar{18}, \bar{21}\},$$

$$H_{12} = \langle \overline{\left(\frac{24}{12}\right)} \rangle = \langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}, \bar{12}, \bar{14}, \bar{16}, \bar{18}, \bar{20}, \bar{22}\},$$

$$H_{24} = \frac{\mathbb{Z}}{24\mathbb{Z}}$$



Propriétés

Soit $(A, +, \cdot)$ un anneau unitaire. On a les propriétés suivantes

- 1) $\forall x \in A \quad x \cdot 0 = 0 = 0 \cdot x$
- 2) $\forall x, y \in A \quad x(-y) = -(xy) = (-x)y$
- 3) $\forall x, y, z \in A \quad x(y - z) = xy - xz$ et $(x - y)z = xz - yz$
- 4) $\forall x, y, z, t \in A \quad (x + y)(z + t) = xz + xt + yz + yt$
- 5) $\forall x, y \in A \quad (x + y)^2 = x^2 + xy + yx + y^2$

Preuve (voir support de cours)



Insistons sur le fait que l'on peut avoir $xy = 0$ sans que x ou y soit nul, et même $x^n = 0$ sans que x soit nul.

Par exemple, dans l'anneau $\frac{\mathbb{Z}}{6\mathbb{Z}}$, on a

$$\bar{2} \times \bar{3} = \bar{0}$$

mais

$$\bar{2} \neq 0 \quad \text{et} \quad \bar{3} \neq 0$$

Dans l'anneau $\frac{\mathbb{Z}}{4\mathbb{Z}}$, on a $\bar{2} \neq 0$ mais

$$\bar{2} \times \bar{2} = \bar{4} = \bar{0}$$



Formule du binôme de Newton

Soient A un anneau, $n \in \mathbb{N}$ et $a, b \in A$. Alors

$$\text{Si } ab = ba \text{ alors } (a + b)^n = \sum_{k=0}^n C_n^k a^k b^{n-k}$$

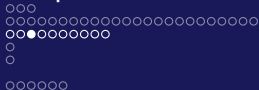
Définition

Soit A un anneau, on dit que $a \in A$ est un **diviseur de zéro** dans A si $a \neq 0$ et s'il existe $b \in A$, $b \neq 0$ tel que

$$ab = 0 \quad \text{ou} \quad ba = 0.$$

Exemples

Dans l'anneau $\mathbb{Z}/6\mathbb{Z}$, l'élément $\bar{3}$ est un diviseur de $\bar{0}$.



Exercice

Déterminer tous les diviseurs de $\bar{0}$ de l'anneau $\mathbb{Z}/24\mathbb{Z}$.



Définition

On dit que l'anneau A est **intègre** si l'anneau A est commutatif, non réduit à zéro et dépourvu de diviseurs de zéro, c'est à dire que

$$\forall a, b \in A, \quad ab = 0 \quad \Rightarrow \quad a = 0 \quad \text{ou} \quad b = 0.$$

Exemples

\mathbb{Z} , \mathbb{Q} , \mathbb{R} sont des anneaux intègres.



Proposition

Soit $m \in \mathbb{N}$.

L'anneau $\mathbb{Z}/m\mathbb{Z}$ est intègre si et seulement si $m = 0$ ou m est un nombre premier.

Preuve (exercice)



Définition

Soit A un anneau unitaire, si $x \in A$ admet un symétrique pour la multiplication, on dit que x est une **unité** de A . On dit aussi que x est un élément **inversible** de A .



Théorème

L'ensemble des éléments inversibles de A se note $U(A)$.

L'ensemble $U(A)$ est stable pour la multiplication, et muni de la multiplication induite $U(A)$ est un groupe dont 1_A est l'élément neutre

Preuve (facile).



Exemples

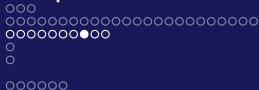
1) $U(\mathbb{Z}) = \{-1, 1\}$

2) $U(\mathbb{R}) = \mathbb{R} \setminus \{0\}$.

Proposition

Soient $m \in \mathbb{N}$ et $x \in \mathbb{Z}$.

L'élément \bar{x} est un élément inversible de l'anneau $\mathbb{Z}/m\mathbb{Z}$ si et seulement si $\text{PGCD}(m, x) = 1$.



Preuve

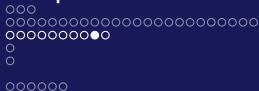
\bar{x} inversible dans l'anneau $\mathbb{Z}/m\mathbb{Z}$ si et seulement si il existe $u \in \mathbb{Z}$ tel que

$$\bar{x} \times \bar{u} = \bar{1}$$

Ceci équivaut à dire que l'entier m divise $xu - 1$, c'est à dire qu'il existe $v \in \mathbb{Z}$ tel que

$$ux + mv = 1,$$

autrement dit $PGCD(m, x) = 1$ d'après le théorème de Bézout.

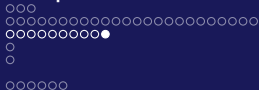


Exercice

- (1) Pour chacun des anneaux suivants, déterminer les éléments inversibles:

$$\frac{\mathbb{Z}}{12\mathbb{Z}}, \frac{\mathbb{Z}}{24\mathbb{Z}}, \frac{\mathbb{Z}}{32\mathbb{Z}}, \frac{\mathbb{Z}}{13\mathbb{Z}}.$$

- (2) Pour chacun des éléments inversibles de l'anneau $\frac{\mathbb{Z}}{24\mathbb{Z}}$ déterminer son inverse.



CORRECTION

Déterminer les éléments inversibles de l'anneau $\frac{\mathbb{Z}}{12\mathbb{Z}}$.

On sait que

$$\frac{\mathbb{Z}}{12\mathbb{Z}} = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \bar{10}, \bar{11} \}$$

Soit $\bar{x} \in \frac{\mathbb{Z}}{12\mathbb{Z}}$. Alors \bar{x} est un élément inversible dans l'anneau $\frac{\mathbb{Z}}{12\mathbb{Z}}$ si et seulement si $\text{PGCD}(x, 12) = 1$.

Ainsi les éléments inversibles de l'anneau $\frac{\mathbb{Z}}{12\mathbb{Z}}$ sont:

$$\bar{1}, \bar{5}, \bar{7}, \bar{11}$$



Définition

Soient A un anneau unitaire et $B \subseteq A$. On dit que B est un sous-anneau de A si:

- i) B est stable pour les deux lois,
- ii) $1_A \in B$,
- iii) B muni des deux lois induites a une structure d'anneau.



Proposition

Soient A un anneau unitaire et $B \subseteq A$. Alors B est un sous-anneau de A si et seulement si:

- i) $\forall a, b \in B, \quad a - b \in B,$
- ii) $1_A \in B,$
- iii) $\forall a, b \in B, \quad ab \in B.$

Exemples

- 1) \mathbb{Z} est un sous-anneau de l'anneau $(\mathbb{Q}, +, \times),$
- 2) \mathbb{Q} est un sous-anneau de l'anneau $(\mathbb{R}, +, \times)$
- 3) $\mathbb{Z}[\sqrt{2}]$ est un sous-anneau de l'anneau $(\mathbb{R}, +, \times)$ où

$$\mathbb{Z}[\sqrt{2}] = \left\{ x \in \mathbb{R} / \exists a, b \in \mathbb{Z}, x = a + b\sqrt{2} \right\}$$





Définition

Soient A un anneau commutatif, I une partie de A .

On dit que I est **un idéal** de A si:

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



Exemples

- (1) Les idéaux de \mathbb{Z} sont exactement les sous-ensembles du type $n\mathbb{Z}$ où $n \in \mathbb{N}$.
- (2) \mathbb{Z} est un sous-anneau de l'anneau $(\mathbb{Q}, +, \times)$, mais n'est pas un idéal de l'anneau $(\mathbb{Q}, +, \times)$.



Définition

Soient A, B deux anneaux unitaires, et $f : A \longrightarrow B$ une application. On dit que f est un **morphisme d'anneaux** (ou un homomorphisme) de A dans B si

- i) $f(1_A) = 1_B$,
- ii) $\forall a, b \in A \quad f(a + b) = f(a) + f(b)$,
- iii) $\forall a, b \in A \quad f(ab) = f(a)f(b)$.

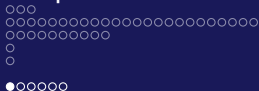


Définition

Soit \mathbb{K} un ensemble non vide muni de deux lois $+$ et \times de composition interne. On dit que $(\mathbb{K}, +, \times)$ est un **corps** si

- i) $(\mathbb{K}, +, \times)$ est un anneau unitaire, et $1_{\mathbb{K}} \neq 0_{\mathbb{K}}$,
- ii) $\forall x \in \mathbb{K} \setminus \{0_{\mathbb{K}}\}, \exists x' \in \mathbb{K}, \quad x x' = 1_{\mathbb{K}} = x' x.$

Si de plus la multiplication est commutative, on dit que \mathbb{K} est un **corps commutatif**.



Exemples

- 1) \mathbb{Q} , \mathbb{R} , \mathbb{C} sont des corps commutatifs pour les lois usuelles.
- 2) $\mathbb{Q}[\sqrt{2}] = \{x \in \mathbb{R} / \exists a, b \in \mathbb{Q}, x = a + b\sqrt{2}\}$ est un corps commutatif (le démontrer!).



Remarques

- 1) Si $(\mathbb{K}, +, \times)$ est un corps alors $\mathbb{K} \setminus \{0\}$ est un groupe pour la loi \times , qui est abélien si et seulement si le corps \mathbb{K} est commutatif.
- 2) Tout corps est un anneau intègre (la réciproque est fautive, par exemple, l'anneau \mathbb{Z} est intègre mais n'est pas un corps). Un corps est donc en particulier un anneau sans diviseurs de zéro.
- 3) Si I est un idéal du corps \mathbb{K} alors $I = \{0\}$ ou $I = \mathbb{K}$.



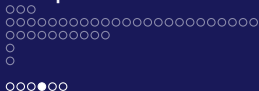
Proposition

Soit $m \in \mathbb{N}$.

L'anneau $\mathbb{Z}/m\mathbb{Z}$ est un corps si et seulement si m est un nombre premier.

Preuve

Supposons que l'anneau $\mathbb{Z}/m\mathbb{Z}$ soit un corps. Alors l'anneau $\mathbb{Z}/m\mathbb{Z}$ est intègre et d'après la proposition 1.3, $m = 0$ ou bien m est un nombre premier. On sait que si $m = 0$, on a $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/0\mathbb{Z}$ qui est isomorphe à \mathbb{Z} et on sait que l'anneau \mathbb{Z} n'est pas intègre. Forcément m est un nombre premier. Réciproquement, si m est un nombre premier alors pour tout entier x tel que $1 \leq x \leq m - 1$, on a $\text{PGCD}(x, m) = 1$ et d'après la proposition 1.4, \bar{x} est un élément inversible de l'anneau $\mathbb{Z}/m\mathbb{Z}$. Donc l'anneau $\mathbb{Z}/m\mathbb{Z}$ est un corps.



Définition

Soient \mathbb{K} un corps et K une partie de \mathbb{K} . On dit que K est un **sous-corps** de \mathbb{K} ou que \mathbb{K} est un **sur-corps** de K si:

- i) K est un sous-anneau de \mathbb{K} ,
- ii) $\forall x \in K \setminus \{0\}, \quad x^{-1} \in K \setminus \{0\}$.



- 1) Par exemple \mathbb{Q} est un sous-corps du corps $\mathbb{Q}[\sqrt{2}]$ qui est lui-même un sous-corps du corps \mathbb{R} .
- 2) Le corps \mathbb{Q} n'a pas de sous-corps propres. En effet, si K est un sous-corps de \mathbb{Q} , montrer que l'on a nécessairement $K = \mathbb{Q}$.
- 3) $\mathbb{Z}/p\mathbb{Z}$ (p premier) n'a pas de sous-corps propres.



Proposition

Soient \mathbb{K} un corps et K une partie de \mathbb{K} . Alors K est un sous-corps de \mathbb{K} si et seulement si les quatre propriétés suivantes sont satisfaites:

- i) $1_{\mathbb{K}} \in K$,
- ii) $\forall x, y \in K, \quad x - y \in K$,
- iii) $\forall x, y \in K, \quad xy \in K$,
- iv) $\forall x \in K \setminus \{0\}, \quad x^{-1} \in K \setminus \{0\}$.



Preuve

Les assertions *i)*, *ii)* et *iii)* expriment que K est un sous-anneau de \mathbb{K} . Et l'assertion *iv)* exprime que tout élément de $K \setminus \{0\}$ est inversible dans l'anneau K .