Leçon 51 - Anneaux et corps

06 janvier 2026

⇒ Anneaux

⇒ Sous-anneaux et morphismes

Problèmes

Problème - Structures fondamentales associées à $\mathbb{Z}$

Problèmes

Problème - Structures fondamentales associées à $\mathbb{Z}$

Problème - Théorème de Bézout et le lemme de Gauss dans un anneau

Problèmes

Problème - Structures fondamentales associées à $\mathbb{Z}$

Problème - Théorème de Bézout et le lemme de Gauss dans un anneau

Problème - Quotienter un anneau

⇒ Anneaux

⇒ Sous-anneaux et morphismes

Définition d'un anneau

Définition - Anneaux

Soit A un ensemble muni de deux lois de composition internes notées $+$ et $\star$. On dit que $(A, +, \star)$ est un *anneau* si :

- $(A, +)$ est un groupe commutatif ;
- la loi $\star$ est associative ;
- la loi $\star$ est distributive par rapport à la loi $+$:
  $\forall (x, y, z) \in A^3, x \times (y + z) =$
  $x \times y + x \times z$ (distibutive à gauche)
  $\forall (x, y, z) \in A^3, (x + y) \times z =$
  $x \times z + y \times z$ (distibutive à droite)
- A possède un élément neutre pour $\star$, noté 1.

Si de plus la loi $\star$ est commutative, on dit que $(A, +, \star)$ est un anneau commutatif.

Définition d'un anneau

Définition - Anneaux

Soit A un ensemble muni de deux lois de composition internes notées $+$ et $\star$. On dit que $(A,+,\star)$ est un *anneau* si :

- $(A,+)$ est un groupe commutatif ;
- la loi $\star$ est associative ;
- la loi $\star$ est distributive par rapport à la loi $+$:
  $\forall (x,y,z) \in A^3, x \times (y+z) =$
  $x \times y + x \times z$ (distibutive à gauche)
  $\forall (x,y,z) \in A^3, (x+y) \times z =$
  $x \times z + y \times z$ (distibutive à droite)
- A possède un élément neutre pour $\star$, noté 1.

Si de plus la loi $\star$ est commutative, on dit que $(A,+,\star)$ est un anneau commutatif.

Exemple Anneaux classiques

Définition d'un anneau

Définition - Anneaux

Soit A un ensemble muni de deux lois de composition internes notées $+$ et $\star$. On dit que $(A, +, \star)$ est un *anneau* si :

- $(A, +)$ est un groupe commutatif ;
- la loi $\star$ est associative ;
- la loi $\star$ est distributive par rapport à la loi $+$:
  $\forall (x, y, z) \in A^3, x \times (y + z) =$
  $x \times y + x \times z$ (distibutive à gauche)
  $\forall (x, y, z) \in A^3, (x + y) \times z =$
  $x \times z + y \times z$ (distibutive à droite)
- A possède un élément neutre pour $\star$, noté 1.

Si de plus la loi $\star$ est commutative, on dit que $(A, +, \star)$ est un anneau commutatif.

Exemple Anneaux classiques
Soit $(A, +, \star)$ un anneau. On note 0 l'élément neutre de $+$ et 1 celui de $\star$.

Règles de calcul immédiates

Proposition - Lien + et $\star$

On a les relations suivantes :

- $\forall x \in A, x \star 0 = 0 \star x = 0$ (on dit que 0 est absorbant).
- $\forall (x,y) \in A^2, (-x) \star y = x \star (-y) = -(x \star y)$
- $\forall (x,y) \in A^2, (-x) \star (-y) = x \star y$

Règles de calcul immédiates

Proposition - Lien + et $\star$

On a les relations suivantes :

- $\forall x \in A, x \star 0 = 0 \star x = 0$ (on dit que 0 est absorbant).
- $\forall (x,y) \in A^2, (-x) \star y = x \star (-y) = -(x \star y)$
- $\forall (x,y) \in A^2, (-x) \star (-y) = x \star y$

Démonstration

Intégrité

Définition - Diviseur de 0 et anneau intègre

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

- $a \in A \setminus \{0\}$ est un diviseur de 0 si il existe $b \in A \setminus \{0\}$ tel que $a \star b = 0$ ou $b \star a = 0$.
- A est dit intègre s'il est commutatif et sans diviseurs de 0.

Intégrité

Définition - Diviseur de 0 et anneau intègre

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

- $a \in A\setminus\{0\}$ est un diviseur de 0 si il existe $b \in A\setminus\{0\}$ tel que $a\star b = 0$ ou $b \star a = 0$.
- A est dit intègre s'il est commutatif et sans diviseurs de 0.

Proposition - Simplification (division)

Si A est un anneau intègre, tout élément non nul a de A est régulier pour $\star$, c'est-à-dire que l'on peut simplifier par a :

$$a\star b = a\star c \Rightarrow b = c.$$

Intégrité

Définition - Diviseur de 0 et anneau intègre

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

- $a \in A \setminus \{0\}$ est un diviseur de 0 si il existe $b \in A \setminus \{0\}$ tel que $a \star b = 0$ ou $b \star a = 0$.
- A est dit intègre s'il est commutatif et sans diviseurs de 0.

Proposition - Simplification (division)

Si A est un anneau intègre, tout élément non nul a de A est régulier pour $\star$, c'est-à-dire que l'on peut simplifier par a :

$$a \star b = a \star c \Rightarrow b = c.$$

Démonstration

Exemple d'intégrité

Exemple $\mathbb{Z}$ et $\mathscr{M}_n(\mathbb{K})$

Exemple d'intégrité

Exemple $\mathbb{Z}$ et $\mathscr{M}_n(\mathbb{K})$

Savoir-faire. Exploiter l'intégrité

On exploite l'intégrité dans son sens contraposée : $a \neq 0$ et $b \neq 0 \Longrightarrow ab \neq 0$.
En particulier, si on sait qu'un ensemble est un corps (comme $\frac{\mathbb{Z}}{p\mathbb{Z}}$, alors il est intègre)

Autres règles de calcul

Proposition - Quelques règles de calcul

Les règles de calculs fréquentes :

- $(a_i)_{1\leqslant i\leqslant n}$ et $(b_j)_{1\leqslant j\leqslant p}$ deux familles d'éléments de A. Alors on peut écrire :
  $\left(\sum_{i=1}^n a_i\right)\left(\sum_{j=1}^p b_j\right) = \sum_{(i,j)\in[\![1,n]\!]\times[\![1,p]\!]} a_i b_j$
- formule du binôme : si a et b **commutent pour** $\star$ alors
  $(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$
- factorisation : si a et b **commutent pour** $\star$ alors
  $a^n - b^n = (a-b)\sum_{k=0}^{n-1} a^{n-k-1} b^k$

en notant $xy = x \star y$ et les puissances étant au sens de la loi $\star$.

Autres règles de calcul

Proposition - Quelques règles de calcul

Les règles de calculs fréquentes :

- $(a_i)_{1\leqslant i\leqslant n}$ et $(b_j)_{1\leqslant j\leqslant p}$ deux familles d'éléments de A. Alors on peut écrire :
  $\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{p} b_j\right) = \sum_{(i,j)\in[\![1,n]\!]\times[\![1,p]\!]} a_i b_j$
- formule du binôme : si a et b **commutent pour** $\star$ alors $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$
- factorisation : si a et b **commutent pour** $\star$ alors $a^n - b^n = (a-b)\sum_{k=0}^{n-1} a^{n-k-1} b^k$

en notant $xy = x\star y$ et les puissances étant au sens de la loi $\star$.

Démonstration

Un groupe pour $\star$: le groupe des inversibles

Proposition - Groupe des inversibles

L'ensemble des éléments inversibles de $(A, \star)$ est un groupe pour la loi $\star$. Classiquement, ce groupe est noté $A^\times$.

Un groupe pour $\star$: le groupe des inversibles

Proposition - Groupe des inversibles

L'ensemble des éléments inversibles de $(A, \star)$ est un groupe pour la loi $\star$. Classiquement, ce groupe est noté $A^{\times}$.

Démonstration

Un groupe pour $\star$: le groupe des inversibles

Proposition - Groupe des inversibles

L'ensemble des éléments inversibles de $(A, \star)$ est un groupe pour la loi $\star$. Classiquement, ce groupe est noté $A^\times$.

Démonstration

Exemple $\mathbb{Z}^*$

Un groupe pour $\star$: le groupe des inversibles

Proposition - Groupe des inversibles

L'ensemble des éléments inversibles de $(A, \star)$ est un groupe pour la loi $\star$. Classiquement, ce groupe est noté $A^\times$.

Démonstration

Exemple $\mathbb{Z}^*$

Exemple $(\mathscr{M}_n(\mathbb{K}))^*$

⇒ Anneaux

⇒ Sous-anneaux et morphismes

1. Problèmes

2. Structures d'anneau

2.1. Définitions et propriétés premières

2.2.Construction d'anneaux

Sous-anneaux

Définition - Sous-anneau

Soit $(A, +, \star)$ un anneau. $B \subset A$ est un *sous-anneau* de A si B est stable pour les lois internes $+$ et $\star$ et si ces lois induites munissent B d'une structure d'anneau avec $1 \in B$.

Sous-anneaux

Définition - Sous-anneau

Soit $(A, +, \star)$ un anneau. $B \subset A$ est un *sous-anneau* de A si B est stable pour les lois internes $+$ et $\star$ et si ces lois induites munissent B d'une structure d'anneau avec $1 \in B$.

$(B, +)$ est nécessairement un groupe, stable également pour $\star$: la réciproque est suffisante :

Savoir-faire. Caractérisation des sous-anneaux

Soit B une partie de A. B est un sous-anneau de A si et seulement si il vérifie :

- $1 \in B$
- $\forall (x, y) \in B^2, x - y \in B$
- $\forall (x, y) \in B^2, x \star y \in B$

Sous-anneaux

Définition - Sous-anneau

Soit $(A, +, \star)$ un anneau. $B \subset A$ est un *sous-anneau* de A si B est stable pour les lois internes $+$ et $\star$ et si ces lois induites munissent B d'une structure d'anneau avec $1 \in B$.

$(B, +)$ est nécessairement un groupe, stable également pour $\star$: la réciproque est suffisante :

Savoir-faire. Caractérisation des sous-anneaux

Soit B une partie de A. B est un sous-anneau de A si et seulement si il vérifie :

- $1 \in B$
- $\forall (x, y) \in B^2, x - y \in B$
- $\forall (x, y) \in B^2, x \star y \in B$

Démonstration

Exemple. . .

Exercice

Montrer que l'intersection de deux sous-anneaux de A est un sous-anneau de A.

(On peut étendre à une intersection d'une famille de sous-anneaux).

Exemple. . .

Exercice

Montrer que l'intersection de deux sous-anneaux de A est un sous-anneau de A.
(On peut étendre à une intersection d'une famille de sous-anneaux).

Exemple $2\mathbb{Z}$ est-il un sous-anneau de $(\mathbb{Z}, +, \times)$?

Morphisme (et image) d'anneaux

Définition - Morphisme d'anneaux

Soient $(A, +_A, \star_A)$ et $(A', +_{A'}, \star_{A'})$ deux anneaux. Un morphisme d'anneaux de A dans A' est une application f de A dans A' vérifiant :

- $\forall (x,y) \in A^2, f(x +_A y) = f(x) +_{A'} f(y)$
- $\forall (x,y) \in A^2, f(x \star_A y) = f(x) \star_{A'} f(y)$
- $f(1_A) = 1_{A'}$

Morphisme (et image) d'anneaux

Définition - Morphisme d'anneaux

Soient $(A, +_A, \star_A)$ et $(A', +_{A'}, \star_{A'})$ deux anneaux. Un morphisme d'anneaux de A dans A' est une application f de A dans A' vérifiant :

- $\forall (x, y) \in A^2, f(x +_A y) = f(x) +_{A'} f(y)$
- $\forall (x, y) \in A^2, f(x \star_A y) = f(x) \star_{A'} f(y)$
- $f(1_A) = 1_{A'}$

Exemple Projection canonique

Morphisme (et image) d'anneaux

Définition - Morphisme d'anneaux

Soient $(A, +_A, \star_A)$ et $(A', +_{A'}, \star_{A'})$ deux anneaux. Un morphisme d'anneaux de A dans A' est une application f de A dans A' vérifiant :

- $\forall (x,y) \in A^2, f(x +_A y) = f(x) +_{A'} f(y)$
- $\forall (x,y) \in A^2, f(x \star_A y) = f(x) \star_{A'} f(y)$
- $f(1_A) = 1_{A'}$

Exemple Projection canonique

Exemple Sur $\mathbb{C}$

Morphisme (et image) d'anneaux

Définition - Morphisme d'anneaux

Soient $(A, +_A, \star_A)$ et $(A', +_{A'}, \star_{A'})$ deux anneaux. Un morphisme d'anneaux de A dans A' est une application f de A dans A' vérifiant :

- $\forall (x,y) \in A^2, f(x +_A y) = f(x) +_{A'} f(y)$
- $\forall (x,y) \in A^2, f(x \star_A y) = f(x) \star_{A'} f(y)$
- $f(1_A) = 1_{A'}$

Exemple Projection canonique
Exemple Sur $\mathbb{C}$
Exemple Morphisme de Fröbenius

Transfert

Proposition - Transfert par morphisme d'anneaux

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

- $f(0_A) = 0_{A'}$,
- $\forall\ x \in A, f(-x) = -f(x)$ et $\forall\ x \in A^*, f(x^{-1}) = f(x)^{-1}$

Transfert

Proposition - Transfert par morphisme d'anneaux

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

- $f(0_A) = 0_{A'}$,
- $\forall\ x \in A, f(-x) = -f(x)$ et $\forall\ x \in A^*, f(x^{-1}) = f(x)^{-1}$

Démonstration

Morphisme de groupe multiplicatif

Proposition - Morphisme du groupe $(A^\times, \star)$

Soit $f : A \to A'$ un morphisme d'anneaux. Alors $f^\times : A^\times \to A'^\times$, $x \mapsto f(x)$ est un morphisme de groupes.

Morphisme de groupe multiplicatif

Proposition - Morphisme du groupe $(A^\times, \star)$

Soit $f : A \to A'$ un morphisme d'anneaux. Alors $f^\times : A^\times \to A'^\times$, $x \mapsto f(x)$ est un morphisme de groupes.

Démonstration

Morphisme de groupe multiplicatif

Proposition - Morphisme du groupe $(A^\times, \star)$

Soit $f : A \to A'$ un morphisme d'anneaux. Alors $f^\times : A^\times \to A'^\times$, $x \mapsto f(x)$ est un morphisme de groupes.

Démonstration

Application - Lemme chinois

$\Phi : \dfrac{\mathbb{Z}}{mn\mathbb{Z}} \to \dfrac{\mathbb{Z}}{m\mathbb{Z}} \times \dfrac{\mathbb{Z}}{n\mathbb{Z}}, \overline{a}_{nm} \mapsto (\overline{a}_m, \overline{a}_n)$ est un morphisme d'anneaux bijectif.

Application au morphisme des inversibles.

Morphisme de groupe multiplicatif

Proposition - Morphisme du groupe $(A^\times, \star)$

Soit $f : A \to A'$ un morphisme d'anneaux. Alors $f^\times : A^\times \to A'^\times$, $x \mapsto f(x)$ est un morphisme de groupes.

Démonstration

Application - Lemme chinois

$\Phi : \dfrac{\mathbb{Z}}{mn\mathbb{Z}} \to \dfrac{\mathbb{Z}}{m\mathbb{Z}} \times \dfrac{\mathbb{Z}}{n\mathbb{Z}}, \overline{a}_{nm} \mapsto (\overline{a}_m, \overline{a}_n)$ est un morphisme d'anneaux bijectif.

Application au morphisme des inversibles.

<u>Exercice</u>

A démontrer

Image directe et image réciproque

Proposition - Image directe et image réciproque

Soit $f : A \to A'$, un morphisme d'anneaux.
Si B est un sous-anneau de A, alors $f(B)$ est un sous-anneau de A'.
Si B' est un sous-anneau de A', alors $f^{-1}(B)$ est un sous-anneau de A.

Image directe et image réciproque

Proposition - Image directe et image réciproque

Soit $f : A \to A'$, un morphisme d'anneaux.
Si B est un sous-anneau de A, alors $f(B)$ est un sous-anneau de A'.
Si B' est un sous-anneau de A', alors $f^{-1}(B)$ est un sous-anneau de A.

En particulier $\mathrm{Im}\ f$ est un sous anneau de A' $(B \leftarrow A)$ mais $\mathrm{Ker}\ f$ n'est un sous-anneau de A $(B' \leftarrow \{0\}$
)

Image directe et image réciproque

Proposition - Image directe et image réciproque

Soit $f : A \to A'$, un morphisme d'anneaux.
Si B est un sous-anneau de A, alors $f(B)$ est un sous-anneau de A'.
Si B' est un sous-anneau de A', alors $f^{-1}(B)$ est un sous-anneau de A.

En particulier $\mathrm{Im}\ f$ est un sous anneau de A' $(B \leftarrow A)$ mais $\mathrm{Ker}\ f$ n'est un sous-anneau de A $(B' \leftarrow \{0\}$
) **Démonstration**

Conclusion

Objectifs

⇒ Anneaux

Conclusion

Objectifs

$\Rightarrow$ Anneaux

- Définition : deux lois internes

Conclusion

Objectifs

$\Rightarrow$ Anneaux

- Définition : deux lois internes
- Vocabulaire : intégrité, diviseur de 0, morphisme d'anneaux, sous-anneaux

Conclusion

Objectifs

⇒ Anneaux

- Définition : deux lois internes
- Vocabulaire : intégrité, diviseur de 0, morphisme d'anneaux, sous-anneaux
- Groupes des inversibles

Conclusion

Objectifs

⇒ Anneaux

Pour la prochaine fois

- Lecture du cours : chapitre 18 : Anneaux et corps (fin)
- Exercice n° 340 & 341
- TD jeudi :
  8h-10h : N°338, 342, 344, 348
  10h-12h : N°339, 343, 347, 346