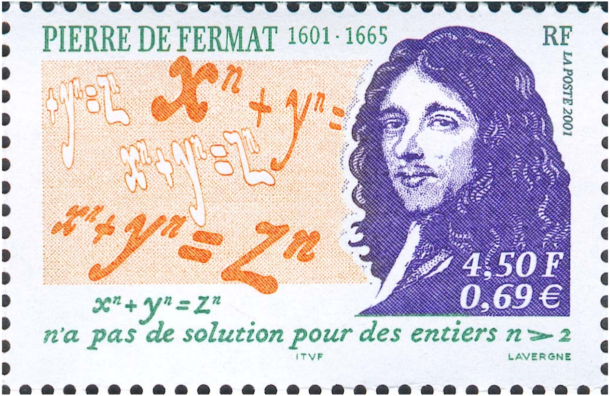

Leçon 46 - Anneaux et corps

17 décembre 2024

⇒ Anneaux

⇒ Idéaux

1. Problèmes

2. Structures d'anneau

    2.1. Définitions et propriétés premières

    2.2.Construction d'anneaux

    2.3. Idéaux

⇒ Anneaux

⇒ Idéaux

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

⇒ Idéaux

1. Problèmes

2. Structures d'anneau

2.1. Définitions et propriétés premières

2.2.Construction d'anneaux

2.3. Idéaux

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

⇒ Idéaux

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-a„eaux de A est un sous-anneau de A.
(On peut étendre à une intersection d'une famille de sous-anneaux).

Exemple...

<u>Exercice</u>
Montrer que l'intersection de deux sous-a„eaux 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

Exercice

On dit que $I \subset A$ est un idéal de l'anneau A, si

- $(I, +)$ est un sous-groupe de $(A, +)$.
- $\forall\, x \in I, y \in A$, $x \star y \in I$ et $y \star x \in I$

Soit $f : A \to A'$ un morphisme d'anneaux. Montrer que $\mathrm{Ker}\, f$ est un idéal de A.

⇒ Anneaux

⇒ Idéaux

⇒ Anneaux
⇒ Idéaux
1. Problèmes
2. Structures d'anneau
2.1. Définitions et propriétés premières
2.2.Construction d'anneaux
2.3. Idéaux

Dans la suite les anneaux sont considérés commutatifs.

Extension de la congruence

on étend à tous les anneaux, la notion de congruence vu dans $\mathbb{Z}$.

Extension de la congruence

on étend à tous les anneaux, la notion de congruence vu dans $\mathbb{Z}$.

Définition - Multiple dans un anneau

Soit a un élément d'un anneau A. On appelle multiple de a, les éléments de l'ensemble $(a) = \{a \times d, d \in A\}$, (parfois noté aA). On dit que a divise b (noté $a|b$) si b est un multiple de a.

Extension de la congruence

on étend à tous les anneaux, la notion de congruence vu dans $\mathbb{Z}$.

Définition - Multiple dans un anneau

Soit a un élément d'un anneau A. On appelle multiple de a, les éléments de l'ensemble $(a) = \{a \times d, d \in A\}$, (parfois noté aA). On dit que a divise b (noté $a|b$) si b est un multiple de a.

Définition - Congruence dans un anneau

Soit m un éléments d'un anneau A. Soient a, b deux éléments de A.
On dit que a est congru à b modulo m, noté $a \equiv b[m]$ ssi $b - a \in (m)$ (ou $m|b - a$).

Extension de la congruence

on étend à tous les anneaux, la notion de congruence vu dans $\mathbb{Z}$.

Définition - Multiple dans un anneau

Soit a un élément d'un anneau A. On appelle multiple de a, les éléments de l'ensemble $(a) = \{a \times d, d \in A\}$, (parfois noté aA). On dit que a divise b (noté $a|b$) si b est un multiple de a.

Définition - Congruence dans un anneau

Soit m un éléments d'un anneau A. Soient a, b deux éléments de A.
On dit que a est congru à b modulo m, noté $a \equiv b[m]$ ssi $b - a \in (m)$ (ou $m|b - a$).

Remarque Notation multiple

Relation d'équivalence

Proposition - Relation d'équivalence

Dans un anneau, la relation de congruence modulo m est une relation d'équivalence

Relation d’équivalence

Proposition - Relation d’équivalence

Dans un anneau, la relation de congruence modulo m est une relation d’équivalence

Exercice

Faire la démonstration

Compatibilité

Théorème - Compatibilité

Si A est un anneau (commutatif) et $m \in A$.
Alors l'addition et la multiplication sont compatibles pour la relation d'équivalence $\equiv [m]$.
Autrement écrit, l'addition et la multiplication sont indépendants du choix du représentant de la classe d'équivalence ; on peut donc définit une addition et une multiplication sur les classes d'équivalence :

$$\overline{x} \overline{+} \overline{x'} = \overline{x + x'} \qquad \overline{x} \overline{\times} \overline{x'} = \overline{x \times x'}$$

Compatibilité

Théorème - Compatibilité

Si A est un anneau (commutatif) et $m \in A$.
Alors l'addition et la multiplication sont compatibles pour la relation d'équivalence $\equiv [m]$.
Autrement écrit, l'addition et la multiplication sont indépendants du choix du représentant de la classe d'équivalence ; on peut donc définit une addition et une multiplication sur les classes d'équivalence :

$$\overline{x} \overline{+} \overline{x'} = \overline{x + x'} \qquad \overline{x} \overline{\times} \overline{x'} = \overline{x \times x'}$$

Démonstration

Idéaux

Analyse Ce qui a marché

Idéaux

Analyse Ce qui a marché

Définition - Idéal de A

Soit A un anneau.

On appelle idéal de A, toute partie I de A tel que :

- $0 \in I$
- $(I, +)$ est un sous-groupe de $(A, +)$ (noté $I < A$)
- $\forall\ a \in I, \forall\ b \in A, ab \in I$

Idéaux

Analyse Ce qui a marché

Définition - Idéal de A

Soit A un anneau.

On appelle idéal de A, toute partie I de A tel que :

- $0 \in I$
- $(I, +)$ est un sous-groupe de $(A, +)$ (noté $I < A$)
- $\forall\, a \in I, \forall\, b \in A, ab \in I$

Exercice

Quels sont les idéaux de $\mathbb{Z}$?

Exercices

Remarque Idéal engendré.

Exercices

Remarque Idéal engendré.

Exercice

Montrer que si I et J sont deux idéaux de $(A,+,\times)$ alors $I\cap J$ et $I+J := \{a+b, a\in I, b\in J\}$ sont des idéaux de A.

Sous-anneaux quotients

Heuristique. Quotientage d'un anneau par un idéal

Parmi les sous-groupes, les sous-groupes distingués permettaient de prolonger la loi interne (par compatibilité) à la structure quotiente qui devenait ainsi un groupe (quotient).

Formellement : si $(H,+) \lhd (G,+)$, alors $\left(\frac{G}{H},\overline{+}\right)$ est un groupe.

Il en est de même pour le quotient d'un anneau par un idéal

Sous-anneaux quotients

Proposition - Anneau quotient

Soit $(A, +, \star)$ un anneau (commutatif) et I un idéal.
Alors $\left(\dfrac{A}{I}, \overline{+}, \overline{\star}\right)$ est un anneau (quotient).

Rappelons que $\dfrac{A}{I}$ désigne l'ensemble des classes d'équivalence de A pour la relation $a \equiv b \iff a - b \in I$.

Sous-anneaux quotients

Proposition - Anneau quotient

Soit $(A,+,\star)$ un anneau (commutatif) et I un idéal.
Alors $\left(\dfrac{A}{I},\overline{+},\overline{\star}\right)$ est un anneau (quotient).

Rappelons que $\dfrac{A}{I}$ désigne l'ensemble des classes d'équivalence de A pour la relation $a \equiv b \Longleftrightarrow a-b \in I$.

Démonstration

Sous-anneaux quotients

Proposition - Anneau quotient

Soit $(A, +, \star)$ un anneau (commutatif) et I un idéal.
Alors $\left(\dfrac{A}{I}, \overline{+}, \overline{\star}\right)$ est un anneau (quotient).

Rappelons que $\dfrac{A}{I}$ désigne l'ensemble des classes d'équivalence de A pour la relation $a \equiv b \Longleftrightarrow a - b \in I$.

Démonstration

<u>Exercice</u>

Montrer que si f est un morphisme d'anneaux A sur B.
Alors $\mathrm{Ker}\ f = \{x \in A \mid f(x) = 0_B\}$ est un idéal de A.
Puis en déduire que $\dfrac{A}{\mathrm{Ker}\ f}$ est un anneau

$\frac{\mathbb{Z}}{a\mathbb{Z}}$

Nous avons enfin une définition propre d'un ensemble dont on a beaucoup parlé.
Comme $a\mathbb{Z}$ est un idéal :

Nous avons enfin une définition propre d'un ensemble dont on a beaucoup parlé.
Comme $a\mathbb{Z}$ est un idéal :

Corollaire - Anneau quotient de $\mathbb{Z}$

Soit $a \in \mathbb{Z}$, l'ensemble $\left(\frac{\mathbb{Z}}{a\mathbb{Z}}, \overline{+}, \overline{\times}\right)$ des classes d'équivalence de $\mathbb{Z}$ est un anneau

Conclusion

Objectifs

⇒ Anneaux

Conclusion

Objectifs

⇒ 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° 327 & 329
- TD jeudi :
  8h-10h : N°313, 318, 317, 328, 335
  10h-12h : N°314, 319, 321, 330, 337