Leçon 52 - Anneaux et corps

07 janvier 2026

⇒ Idéaux et anneaux quotients

⇒ Corps

⇒ Idéaux et anneaux quotients

⇒ Corps

Extension de la congruence

Dans la suite les anneaux sont considérés commutatifs.

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

Extension de la congruence

Dans la suite les anneaux sont considérés commutatifs.
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

Dans la suite les anneaux sont considérés commutatifs.
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 élément 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

Dans la suite les anneaux sont considérés commutatifs.
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 élément 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

<u>Exercice</u>

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 $\left(\dfrac{G}{H}, \overline{+}\right)$ 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 $a \equiv b \Longleftrightarrow a - b \in I$.

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 $\left(\frac{A}{I}, \overline{+}, \overline{\star}\right)$ est un anneau (quotient).

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

Démonstration

Exercice

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 $\frac{A}{\mathrm{Ker}\ f}$ est un anneau

$\dfrac{\mathbb{Z}}{a\mathbb{Z}}$

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

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

Nous avons enfin une définition propre d'un ensemble dont on a beaucoup parlé.

Comme $a\mathbb{Z}$ est un idéal :

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

⇒ Idéaux et anneaux quotients

⇒ Corps

Anneau principal

Proposition - Anneau principal

Soit A un anneau.
On dit qu'un idéal I de A est principal si il existe $a \in I$ tel que $I = (a)$.
On dit qu'un anneau est principal s'il est intègre (commutatif) et tous ses idéaux sont principaux.

Anneau principal

Proposition - Anneau principal

Soit A un anneau.
On dit qu'un idéal I de A est principal si il existe $a \in I$ tel que $I = (a)$.
On dit qu'un anneau est principal s'il est intègre (commutatif) et tous ses idéaux sont principaux.

Exemple $\mathbb{Z}$ est principal

Anneau principal

Proposition - Anneau principal

Soit A un anneau.
On dit qu'un idéal I de A est principal si il existe $a \in I$ tel que $I = (a)$.
On dit qu'un anneau est principal s'il est intègre (commutatif) et tous ses idéaux sont principaux.

Exemple $\mathbb{Z}$ est principal

Savoir-faire. Montrer qu'un anneau est principal

Une méthode qui ne marche pas toujours est de montrer qu'un tel anneau est d'abord euclidien

Anneau euclidien

Définition - Anneau euclidien

Soit A un anneau. On dit que A est euclidien s'il existe une application $\varphi : A \setminus \{0\} \to \mathbb{N}$ (appelé **stathme** euclidien) telle que :

$$\forall\ (a,b) \in A \times A \setminus \{0\}, \exists\ (q,r) \in A^2 \text{ tel que } a = bq + r$$
$$\text{avec } r = 0 \text{ ou } \varphi(r) < \varphi(b)$$

Notons que l'unicité n'est pas demandé.

Anneau euclidien

Définition - Anneau euclidien

Soit A un anneau. On dit que A est euclidien s'il existe une application $\varphi : A \setminus \{0\} \to \mathbb{N}$ (appelé **stathme** euclidien) telle que :

$$\forall\ (a,b) \in A \times A \setminus \{0\}, \exists\ (q,r) \in A^2 \text{ tel que } a = bq + r$$
$$\text{avec } r = 0 \text{ ou } \varphi(r) < \varphi(b)$$

Notons que l'unicité n'est pas demandé.

Proposition - Anneau euclidien ⇒ Anneau principal

Si A est euclidien, alors A est principal

Anneau euclidien

Définition - Anneau euclidien

Soit A un anneau. On dit que A est euclidien s'il existe une application $\varphi : A \setminus \{0\} \to \mathbb{N}$ (appelé **stathme** euclidien) telle que :

$$\forall\ (a,b) \in A \times A \setminus \{0\}, \exists\ (q,r) \in A^2 \text{ tel que } a = bq + r$$
$$\text{avec } r = 0 \text{ ou } \varphi(r) < \varphi(b)$$

Notons que l'unicité n'est pas demandé.

Proposition - Anneau euclidien ⇒ Anneau principal

Si A est euclidien, alors A est principal

Démonstration

Exemple d'anneaux euclidiens

Exemples Nombreux

<u>Exercice</u> On note $\mathbb{Z}[i] = \{a + ib; a, b \in \mathbb{Z}\}$, l'ensemble des entiers de Gauss.

1. Trouver une division euclidienne sur $\mathbb{Z}[i]$
   On prendra, le carré de la fonction module comme stathme
2. En déduire que $\mathbb{Z}[i]$ est principal

⇒ Idéaux et anneaux quotients

⇒ Corps

⇒ Idéaux et anneaux quotients

⇒ Corps

1. Problèmes

2. Structures d’anneau

2.1. Définitions et propriétés premières

2.2.Construction d’anneaux

2.3. Idéaux

2.4. Anneau euclidien. Anneau principal

3. Structures de corps

3.1. Corps

3.2. Idéaux maximaux. Idéaux premiers

3.3. Sous-corps. Morphisme (de corps)

Définition

Définition - Corps

Un corps est un anneau commutatif $(K, +, \times)$ dans lequel tous les éléments autres que 0 sont inversibles pour $\times$ c'est-à-dire que : $(K, +, \times)$ est un corps si :

- $(K, +)$ est un groupe commutatif ;
- $(K^*, \times)$ est un groupe commutatif, où 0 désigne l'élément neutre de K pour $+$ et $K^* = K \setminus \{0\}$.
- la loi $\times$ est distributive par rapport à la loi $+$;

Exemples. Régularité

Exemples Nombreux

Exemples. Régularité

Exemples Nombreux

Tout élément est régulier

Un corps n'a pas de diviseurs de 0. Tout élément autre que 0 est donc régulier (on peut simplifier).

Exemples. Régularité

Exemples Nombreux

Tout élément est régulier

Un corps n'a pas de diviseurs de 0. Tout élément autre que 0 est donc régulier (on peut simplifier).

Démonstration

⇒ Idéaux et anneaux quotients

⇒ Corps

Anneau quotient comme un corps ?

Analyse A quel condition un anneau quotient est-il un corps ?

Anneau quotient comme un corps ?

Analyse A quel condition un anneau quotient est-il un corps ?

Définition - Idéal maximal

Soit I un idéal de A.
On dit que I est maximal s'il $I \neq A$ et A est le seul idéal distinct de I, contenant I

Corps quotient

Proposition - Corps

Soit I un idéal maximal de A. Alors $\left(\frac{A}{I}, \overline{+}, \overline{\times}\right)$ est un corps.

Corps quotient

Proposition - Corps

Soit I un idéal maximal de A. Alors $\left(\frac{A}{I}, \overline{+}, \overline{\times}\right)$ est un corps.

Remarque Réciproque

Corps quotient

Proposition - Corps

Soit I un idéal maximal de A. Alors $\left(\dfrac{A}{I}, \overline{+}, \overline{\times}\right)$ est un corps.

Remarque Réciproque

Exemple $6\mathbb{Z}$ n'est pas maximal

Corps quotient

Proposition - Corps

Soit I un idéal maximal de A. Alors $\left(\frac{A}{I}, \overline{+}, \overline{\times}\right)$ est un corps.

Remarque Réciproque

Exemple $6\mathbb{Z}$ n'est pas maximal

Démonstration

Exemple $\frac{\mathbb{Z}}{p\mathbb{Z}}$ avec p premier.

⇒ Idéaux et anneaux quotients

⇒ Corps

Défintion

Définition - Sous-corps, morphisme

On peut généraliser les définitions précédentes.

- Un sous-corps est un sous-anneau muni d'une structure de corps.
- Un morphisme de corps est un morphisme d'anneaux.
- L'image d'un corps par un morphisme de corps est un corps.

Le dernier point est un exercice à démontrer.

Conclusion

Objectifs

⇒ Idéaux et anneau quotient

⇒ Corps

Conclusion

Objectifs

$\Rightarrow$ Idéaux et anneau quotient

- Idéaux : groupe pour $+$, hemi-stabilité pour $\times$

Conclusion

Objectifs

$\Rightarrow$ Idéaux et anneau quotient

- Idéaux : groupe pour $+$, hemi-stabilité pour $\times$
- Si I est un idéal, $\dfrac{A}{I}$ est un anneau (pour les lois induites)

Conclusion

Objectifs

$\Rightarrow$ Idéaux et anneau quotient

- Idéaux : groupe pour $+$, hemi-stabilité pour $\times$
- Si I est un idéal, $\dfrac{A}{I}$ est un anneau (pour les lois induites)
- Les anneaux (a) (principaux) sont essentiels.
  Donc nécessité d'anneaux principaux (où tous les idéaux sont principaux)

Conclusion

Objectifs

⇒ Idéaux et anneau quotient

- Idéaux : groupe pour $+$, hemi-stabilité pour $\times$
- Si I est un idéal, $\dfrac{A}{I}$ est un anneau (pour les lois induites)
- Les anneaux (a) (principaux) sont essentiels.
  Donc nécessité d'anneaux principaux (où tous les idéaux sont principaux)
- Une condition suffisante : l'anneau est euclidien.

Conclusion

Objectifs

$\Rightarrow$ Idéaux et anneau quotient

$\Rightarrow$ Corps

Conclusion

Objectifs

$\Rightarrow$ Idéaux et anneau quotient

$\Rightarrow$ Corps

- Tous les éléments non nuls sont inversibles

Conclusion

Objectifs

⇒ Idéaux et anneau quotient

⇒ Corps

- Tous les éléments non nuls sont inversibles
- Sous-corps, morphisme de corps

Conclusion

Objectifs

⇒ Idéaux et anneau quotient

⇒ Corps

- Tous les éléments non nuls sont inversibles
- Sous-corps, morphisme de corps
- $\dfrac{A}{I}$ est un corps si I est maximal ou premier.

Conclusion

Objectifs

$\Rightarrow$ Idéaux et anneau quotient

$\Rightarrow$ Corps

Pour la prochaine fois

- Lecture du cours : chapitre 24 : Espaces vectoriels
- Exercice n° 345