Compléments sur les anneaux

Je me souviens

1. Donner la définition d'anneau.
2. Donner des exemples d'anneaux
3. Qu'est-ce que le groupe des inversibles ?
4. Qu'est-ce qu'un corps ?
5. Quand dit-on qu'un anneau est intègre ?
6. Qu'est-ce qu'un sous-anneau ?
7. Quelles sont les règles de calcul dans un anneau ?
   - $a \times 0_A =$
   - $a \times (-1_A) =$
   - $a \times \left(\sum_{i=1}^{n} b_i\right) =$
   - $(a+b)^n =$
   - $a^n - b^n =$
   - $(1_A - a)\left(\sum_{k=0}^{n} a_k\right) =.$
8. Qu'est-ce qu'un morphisme d'anneaux ?
9. Et un isomorphisme d'anneaux ?

1 Produit d'anneaux

Définition. Soit A, B deux anneaux. On munit $A \times B$ des lois internes :

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$
$$(x_1, y_1) \times (x_2, y_2) = (x_1 \times x_2, y_1 \times y_2)$$

pour tout $(x_1, y_1), (x_2, y_2) \in A \times B$.
Muni de ces lois, $(A \times B, +, \times)$ est un anneau appelé **anneau produit** de A et B.

Remarque.

- *Cette définition se prolonge au cas d'un nombre fini d'anneaux.*
- *Un anneau produit n'est pas, en général, intègre.*

Exemple. Soit A et B deux anneaux. Quels sont les inversibles de $A \times B$?

2 Idéaux d'un anneau commutatif

2.1 Définition

Remarque. *Si $f : A \to B$ est un morphisme d'anneaux, son image $\operatorname{Im} f$ est un sous-anneau de B, mais son noyau $\operatorname{Ker} f$ n'est pas en général un sous-anneau de A.*

Définition. Soit $(A, +, \times)$ un anneau commutatif. Une partie I de A est un **idéal** de A lorsque :

- I est un sous-groupe de A.
- I est **absorbant**, i.e. :
$$\forall a \in A,\ \forall x \in I,\ a \times x \in I$$

Théorème.

Si $f : A \to B$ est un morphisme d'anneaux commutatifs. Alors son noyau $\operatorname{Ker} f$ est un idéal de A.

Proposition. Si $a \in A$, alors aA est un idéal de A, qu'on appelle **idéal engendré par** a.

Remarque.

- *On peut utiliser la notation (a) pour désigner aA, idéal engendré par a.*
- *Un idéal I pour lequel il existe a tel que $I = aA$ est parfois qualifié de principal. Si tous les idéaux de A sont principaux, on qualifie l'anneau de principal. Ce vocabulaire n'est pas dans le programme officiel.*

Exemple. Que dire d'un idéal qui contient 1_A ?

Exemple. Quels sont les idéaux d'un corps ?

2.2 Idéaux de $\mathbb{Z}$, PGCD d'entiers

Proposition. Les idéaux de $(\mathbb{Z}, +, \times)$ sont les $n\mathbb{Z}$, avec $n \in \mathbb{N}$.

Proposition. Soit $a, b \in \mathbb{Z}$. Alors :

$$(a) + (b) = a\mathbb{Z} + b\mathbb{Z} = \{au + bv,\ u, v \in \mathbb{Z}\}$$

est un idéal de $\mathbb{Z}$.

Définition. Soit $a, b \in \mathbb{Z}$, non tous les deux nuls. Alors il existe un unique entier $d \in \mathbb{N}$, appelé **PGCD de a et b**, tel que :

$$(a) + (b) = (d) \text{ i.e. } a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$$

Notation.

- On note $a \wedge b$ le PGCD de a et b.
- La relation $au + bv = a \wedge b$ s'appelle **relation de Bézout**.

Proposition. Soit $a, b \in \mathbb{Z}$ deux entiers non nuls. Les diviseurs communs à a et b sont les diviseurs de $a \wedge b$.

Remarque. *On retrouve la définition de première année : $a \wedge b$ est le plus grand (au sens de l'ordre naturel, au sens de la divisibilité) entier naturel qui divise à la fois A et B.*

Définition. Soit $a_1, \ldots, a_n \in \mathbb{Z}$, non tous nuls. On appelle **PGCD de** $a_1, \ldots, a_n$ l'unique $d \in \mathbb{N}$ tel que :

$$a_1\mathbb{Z} + \cdots + a_n\mathbb{Z} = d\mathbb{Z}$$

2.3 Idéaux de $\mathbb{K}[X]$

Proposition. Les idéaux de $(\mathbb{K}[X], +, \times)$ sont les $P\,\mathbb{K}[X] = \{PQ,\ Q \in \mathbb{K}[X]\}$, avec $P \in \mathbb{K}[X]$.

2.4 Divisibilité dans un anneau, idéal engendré par un élément

Définition. Soit $(A, +, \times)$ un anneau commutatif, $a, b \in A$. On dit que a **divise** b, et on note $a \mid b$, lorsqu'il existe $c \in A$ tel que $b = ac$, i.e. b est un multiple de a.

Remarque. $a \mid b \iff bA \subset aA$

Définition. Dans $(A, +, \times)$ anneau commutatif, pour $a, b \in A$, on dit que a et b sont **associés** si et seulement si $a \mid b$ et $b \mid a$, c'est-à-dire $aA = bA$.

Proposition.

- La relation *être associés* est une relation d'équivalence sur A.
- Lorsque A est intègre, a et b sont associés si et seulement s'il existe u inversible tel que $a = ub$.

3 Algèbre

3.1 Définition

Définition. Soit $\mathbb{K}$ un corps. On dit que $(A, +, \times, \cdot)$ est une **algèbre sur** $\mathbb{K}$, ou $\mathbb{K}$-algèbre, lorsque :

- $(A, +, \times)$ est un anneau
- $(A, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel
- $\forall \lambda \in K,\ \forall a, b \in A,\ \lambda \cdot (a \times b) = (\lambda.a) \times b = a \times (\lambda \cdot b)$.

L'algèbre est **commutative** si $\times$ l'est, **intègre** si l'anneau $(A, +, \times)$ l'est, **de dimension finie** si l'espace vectoriel $(A, +, \cdot)$ l'est.

3.2 Exemples de référence

Exemple.

- $\mathbb{K}^n$, muni de sa structure produit, est une algèbre sur $\mathbb{K}$.
- $\mathbb{K}[X]$, muni de ses lois usuelles, est une algèbre.
- $(\mathcal{M}_n(\mathbb{K}), +, \times, \cdot)$ est une algèbre.
- Pour E espace vectoriel sur $\mathbb{K}$, $(\mathcal{L}(E), +, \circ, \cdot)$ est une algèbre.
- Pour X ensemble quelconque, $\mathcal{F}(X, \mathbb{K}) = \mathbb{K}^X$, muni de ses opérations usuelles, est une algèbre.

3.3 Sous-algèbre

Définition. Soit $(A, +, \times, \cdot)$ une algèbre. Alors B est une **sous-algèbre** de A si et seulement si :

- B est un sous-anneau de $(A, +, \times)$
- B est un sous-espace vectoriel de $(A, +, \cdot)$

Proposition. B est une sous-algèbre de $(A, +, \times, \cdot)$ lorsque :

- $B \subset A$
- B stable par $+$
- B stable par passage à l'opposé
- $1_A \in B$
- B stable par $\times$
- B stable par combinaisons linéaires

Exemple. L'ensemble $\mathcal{D}_n(\mathbb{K})$ des matrices diagonales est une sous-algèbre de $\mathcal{M}_n(\mathbb{K})$.

Exemple. L'ensemble $\mathcal{T}_n^s(\mathbb{K})$ des matrices triangulaires supérieures est une sous-algèbre de $\mathcal{M}_n(\mathbb{K})$.

3.4 Morphisme d'algèbre

Définition. Soit $(A, +, \times, \cdot), (B, +, \times, \cdot)$ deux algèbres sur $\mathbb{K}$ et $f : A \to B$. On dit que f est un **morphisme d'algèbres** lorsque :

- f est un morphismes d'anneaux
- f est linéaire

Remarque. *Pour vérifier que f est un morphisme d'algèbre, on vérifie que :*

- $f(\lambda a + \mu b) = \lambda f(a) + \mu f(b)$
- $f(a \times b) = f(a) \times f(b)$
- $f(1_A) = 1_B$

Exemple. Soit $t \in \mathbb{K}$ fixé. L'application $P \mapsto P(t)$ est un morphisme d'algèbres entre $\mathbb{K}[X]$ et $\mathbb{K}$ muni de leurs lois usuelles.

Remarque. *On pourrait définir noyau et image d'un morphisme d'algèbres $A \to B$. L'image est une sous-algèbre de B, le noyau est un sous-espace vectoriel et un idéal de A, mais pas en général une sous-algèbre.*

Exercices et résultats classiques à connaître

Nilpotence

120.1

Soit $(A, +, \times)$ un anneau. On dit que $x \in A$ est **nilpotent** lorsqu'il existe $n \in \mathbb{N}^*$ tel que $x^n = 0_A$. On considère $x, y \in A$.

(a) Montrer que, si x est nilpotent et que x et y commutent, alors xy est nilpotent.

(b) Montrer que, si xy ets nilpotent, alors yx est nilpotent.

(c) Montrer que, si x et y sont nilpotents et commutent, alors $x + y$ est nilpotent.

(d) Montrer que, si x est nilpotent, alors $1_A - x$ est inversible et préciser $(1_A - x)^{-1}$.

Exercices

120.2

On définit : $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2},\ a, b \in \mathbb{Z}\}$.

(a) Montrer que $(\mathbb{Z}[\sqrt{2}], +, \times)$ est un anneau.

(b) On définit, pour $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$:

$$N(a + b\sqrt{2}) = a^2 - 2b^2$$

Montrer que N est bien définie, à valeurs dans $\mathbb{R}$.

(c) Montrer que, pour tout $x, y \in \mathbb{Z}[\sqrt{2}]$, $N(xy) = N(x)N(y)$.

(d) En déduire les inversibles de $\mathbb{Z}[\sqrt{2}]$.

120.3

On note : $\mathcal{D} = \left\{ \dfrac{n}{10^k} \text{ où } n \in \mathbb{Z} \text{ et } k \in \mathbb{N} \right\}$ l'ensemble des nombres décimaux. Montrer que $\mathcal{D}$ est un sous-anneau de $(\mathbb{Q}, +, \times)$.

120.4

On note $\mathcal{P}$ l'ensemble des nombres premiers. On se propose d'établir l'existence d'une correspondance bijective entre l'ensemble des sous-anneaux de $(\mathbb{Q}, +, \times)$ et l'ensemble des parties de $\mathcal{P}$.
Pour A un sous-anneau de $\mathbb{Q}$, on note :

$$P(A) = \left\{ p \in \mathcal{P} \text{ t.q. } \frac{1}{p} \in A \right\}$$

(a) Soit A, B deux sous-anneaux de $\mathbb{Q}$. Établir :

$$P(A) = P(B) \implies A = B$$

(b) Soit P un sous-ensemble de $\mathcal{P}$. Déterminer un sous-anneau A de $\mathbb{Q}$ vérifiant : $P(A) = P$.

(c) Conclure.

120.5

Soit $(A, +, \times)$ un anneau commutatif. On note $N(A)$ l'ensemble des éléments nilpotents de A, c'est-à-dire l'ensemble des $x \in A$ tels qu'il existe $n \in \mathbb{N}$, $x^n = 0$. Montrer que $N(A)$ est un idéal de A.

120.6

Soit A et B deux anneaux commutatifs, $f : A \to B$ un morphisme d'anneaux, et I un idéal de A. Est-ce que $f(I)$ est un idéal ?

Petits problèmes d'entrainement

120.7 ✍

(a) Soit $A \subset \mathbb{C}$. Montrer qu'il existe un plus petit sous-corps de $\mathbb{C}$ qui contient $\mathbb{Q}$ et A. On le note $\mathbb{Q}(A)$.

(b) Décrire le sous-corps $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Montrer que c'est un $\mathbb{Q}$-espace vectoriel de dimension 4.

120.8

Soit E l'ensemble des matrices de la forme $\begin{pmatrix} a & 2b \\ -b & a \end{pmatrix}$, où $a, b \in \mathbb{R}$.

(a) Montrer que E est un sous-espace vectoriel de $\mathcal{M}_2(\mathbb{R})$ et donner sa dimension.

(b) Montrer que E est un sous-anneau de $\mathcal{M}_2(\mathbb{R})$, puis montrer que c'est un corps.

(c) Résoudre dans E l'équation $X^2 = I_2$.

120.9

Soit p un nombre premier, $p \geqslant 3$. On note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ et on rappelle que c'est un corps.

(a) Montrer que $f : x \mapsto x^2$ est un morphisme de groupes de $(\mathbb{F}_p^*, \times)$ dans lui-même.

(b) Montrer que $\mathrm{Ker}(f) = \{\overline{-1}, \overline{1}\}$.

(c) Montrer que, pour tout $x \in \mathbb{F}_p^*$, $x^{\frac{p-1}{2}} = \overline{1}$ ou $\overline{-1}$.

(d) Montrer qu'il y a $\dfrac{p-1}{2}$ carrés dans $\mathbb{F}_p^*$.

120.10

Soit $(A, +, \times)$ un anneau commutatif, et I un idéal de cet anneau. On pose :

$$\sqrt{I} = \{a \in A,\ \exists n \in \mathbb{N},\ a^n \in I\}$$

(a) Montrer que $\sqrt{I}$ est un idéal de A.

(b) Justifier que, pour tout I idéal de A, $\sqrt{\sqrt{I}} = \sqrt{I}$.

(c) Pour tout p premier et $\alpha \in \mathbb{N}^*$, montrer que $\sqrt{p^\alpha \mathbb{Z}} = p\mathbb{Z}$.

(d) Plus généralement, si $n \geqslant 2$ se décompose en facteurs premiers sous la forme $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, montrer que :

$$\sqrt{n\mathbb{Z}} = p_1 \dots p_k \mathbb{Z}$$

120.11

Un idéal I d'un anneau commutatif $(A, +, \times)$ est dit **premier** si et seulement si :

$$\forall x, y \in A,\ xy \in I \implies x \in I \text{ ou } y \in I$$

(a) Donner un exemple d'idéal premier dans $\mathbb{Z}$.

(b) Soit $P \in \mathbb{K}[X]$ un polynôme irréductible. Montrer que $P \cdot \mathbb{K}[X]$ est premier.

(c) Soit J et K deux idéaux de A et I un idéal premier. Montrer que :

$$J \cap K = I \implies (J = I \text{ ou } K = I)$$

(d) Soit $(A, +, \times)$ un anneau commutatif dont tout idéal est premier. Établir que A est intègre puis que A est un corps.

120.12

Soit $\mathcal{A}$ l'ensemble $\mathcal{C}^0([0,1], \mathbb{R})$.

(a) Montrer que $\mathcal{A}$ est un anneau pour les opérations usuelles. Est-il commutatif ? Est-il intègre ?

(b) Soit $J \subset [0,1]$ et

$$\mathcal{A}_J = \{f \in \mathcal{A} \text{ t.q. } \forall x \in J,\ f(x) = 0\}$$

Montrer que $\mathcal{A}_J$ est un idéal de $\mathcal{A}$.
Montrer que si $J = \{a\}$ est un singleton, cet idéal est maximal, c'est-à-dire qu'il n'est inclus strictement dans aucun autre idéal strict de $\mathcal{A}$.