

Compléments sur les anneaux

$$(A, +, \times)$$

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 ?

A est intègre si) A commutatif
 $\left. \begin{array}{l} \end{array} \right\} \forall a, b \in A, ab=0 \Rightarrow a=0 \text{ ou } b=0$
 (pas de diviseur non nul de 0).

B sous-anneau de A

longue

• $B \subset A$

• $0_A \in B \quad \underline{\text{et}} \quad 1_A \in B$

• B stable par

$$\left\{ \begin{array}{l} + \\ \text{par produit et l'opposé} \\ \times \end{array} \right.$$

$f: A \longrightarrow A'$ morphisme d'anneau

lorsque: $\forall x, y \in A$

$$f(x+y) = f(x) + f(y)$$

$$f(x \times y) = f(x) \times f(y)$$

$$f(1_A) = 1_{A'}$$

$f(0_A) = 0_{A'}$ vrai, mais pas dans la déf

si $ab=ba$

$$(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$$

$$\bullet (1_A - a) \left(\sum_{k=0}^n a^k \right) = 1 - a^{n+1}$$

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 $A \times B$?

$f: (A, +, \times) \longrightarrow (B, +, \times)$ morphisme d'anneaux
(de groupes)

$\text{Im } f = f(A)$ sous-groupe de B

$\text{Ker } f = f^{-1}(\{0_B\})$ sous-groupe de A .

en effet: $\text{Ker } f \subset A$

• $f(0_A) = 0_B$ donc $0_A \in \text{Ker } f$

• Soit $a_1, a_2 \in \text{Ker } f$

$$f(a_1 + a_2) = f(a_1) + f(a_2)$$

$$= 0_B + 0_B$$

$$= 0_B$$

donc $a_1 + a_2 \in \text{Ker } f$

• Soit $a \in \text{Ker } f$

$$f(-a) = -f(a)$$

$$= -0_B$$

$$= 0_B$$

donc $-a \in \text{Ker } f$.

$\text{Im } f$ est sous-anneau de B [...] ?

Est-ce que $\text{Ker } f$ sous-anneau de A ?

$$f(1_A) = 1_B \neq 0_B$$

donc $1_A \notin \text{Ker } f$.

donc $\text{Ker } f$ n'est pas un sous-anneau de A .

$$a_1, a_2 \in \text{Ker } f$$

$$f(a_1 a_2) = f(a_1) f(a_2)$$

$$= 0_B \quad 0_B$$

$$= 0_B$$

donc $\text{Ker } f$ stable par $\times$.

Remarque que $1_A \notin \text{Ker } f$!

$$\text{Soit } f(x) = f(1_A x)$$

$$= f(1) f(x)$$

$$= 0_B f(x)$$

$$= 0_B$$

2 Idéaux d'un anneau commutatif

2.1 Définition

Remarque. Si $f : A \rightarrow B$ est un morphisme d'anneaux, son image $\text{Im } f$ est un sous-anneau de B , mais son noyau $\text{Ker } f$ 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. :

$$\forall a \in A, \forall x \in I, a \times x \in I$$

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

Exemple. Quels sont les idéaux d'un corps ?

- Soit I idéal de A tq $1_A \in I$.

$$\text{donc } \forall a \in A, a \times \underset{a}{1_A} \in I \quad (\text{car } I \text{ absorbant})$$

$$\text{donc } A = I.$$

- $(K, +, \times)$ corps base K anneau commutatif où tout élément non nul est inversible.

$(\mathbb{R}, +, \times)$

$(\mathbb{C}, +, \times)$ $-x$

$(\mathbb{Q}, +, \times)$ $\bullet$

I idéal de K .



On peut avoir $I = \{0\}$. On suppose $I \neq \{0\}$

Si $x \in I, x \neq 0$ alors $1_K = x^{-1} \cdot x \in I$ (absorbant)
donc $I = K$

Théorème.

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

- On sait déjà que $\text{Ker } f$ sous-groupe de $(A, +)$

- Soit $a \in A$ et $x \in \text{Ker } f$

alors
$$\begin{aligned} f(ax) &= f(a)f(x) \\ &= f(a) 0_B \\ &= 0_B \end{aligned}$$

donc $ax \in \text{Ker } f$.

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.

Preuve:

• $aA \subset A$

• $0_A = a0_A \in aA$

• aA stable par $+$

• aA stable par produit à l'opposé

• Soit $b \in aA$ et $c \in A$

$\uparrow$
i.e. $\exists b_1 \in A$ s.t. $b = ab_1$

Alors $bc = a(b_1c)$

$\in aA$

} sous-groupe

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

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

$\Leftarrow$ $n\mathbb{Z}$ est un idéal

$\Rightarrow$ Soit I idéal de $\mathbb{Z}$,

alors I est un sous-groupe de $\mathbb{Z}$

donc $\exists n \in \mathbb{N} \mid I = n\mathbb{Z}$.

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 :

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

Preuve.

- $a\mathbb{Z} + b\mathbb{Z} \subset \mathbb{Z}$

- $0 = a0 + b0 \in a\mathbb{Z} + b\mathbb{Z}$

- $a\mathbb{Z} + b\mathbb{Z}$ stable par $+$ et passage à l'opposé. [...]

- Soit $x \in a\mathbb{Z} + b\mathbb{Z}$ et $\exists u, v \in \mathbb{Z} \mid$
 $x = au + bv$

Soit $y \in \mathbb{Z}$

$$xy = a(uy) + b(vy) \\ \in a\mathbb{Z} + b\mathbb{Z}$$

Donc $a\mathbb{Z} + b\mathbb{Z}$ est un idéal de $\mathbb{Z}$

donc $\exists d \in \mathbb{N}$ & $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$

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

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

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 $P \in \mathbb{K}[X]$.

Preuve:

$\Leftarrow$ cf § 2.1 "aA idéal de A"

$\Rightarrow$ Soit I un idéal de $\mathbb{K}[X]$

• On peut avoir $I = \{0\} = 0 \mathbb{K}[X]$

• Sinon notons $D = \{\deg(P), P \in I \text{ et } P \neq 0\}$

alors D partie de $\mathbb{N}$, non vide

donc admet un minimum noté d .

et Il existe $P \in I$ tq $\deg(P) = d$.

Preuve $I = P \cdot \mathbb{K}[X]$

$\supset$ Soit $Q \in P\mathbb{K}[X]$

ie $\exists Q_1$ tq $Q = P Q_1$

$\uparrow$ $\uparrow$
 $\in I$ $\in \mathbb{K}[X]$

donc $Q \in I$ car I idéal

Surf $P\mathbb{K}[X] \subset I$

C) Soit $Q \in I$

On effectue la div. euclidienne de Q par P

donc $\exists Q_1, R$ (uniques) $\frac{Q}{P}$

$$\begin{cases} Q = PQ_1 + R \\ R = 0 \text{ ou } \deg R < \deg P \end{cases}$$

$$\text{donc } R = Q - PQ_1$$

$$\in I \quad \text{car } Q \in I, \quad P \in I \\ \text{donc } PQ_1 \in I$$

Par minimalité de $\deg P$, on a donc $R = 0$

CC : $I = P \cdot K[x].$

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 $a = ub$.

