Compléments sur les anneaux

Je me souviens

1. Donner la définition d'anneau.
2. Donner des exemples d'anneaux

① $(A, +, \times)$ 2 lois de ci

tq $(A, +)$ groupe abélien

$\times$ associatif

$\times$ a un neutre noté 1_A

distributivité

② $(\mathbb{R}, +, \times)$ oui, mais bof.

$(M_n(\mathbb{R}), +, \times)$ ← bon exemple d'anneau non intègre non commutatif.

$(\mathcal{L}(E), +, \circ)$

$(\mathbb{Z}, +, \times)$ ← anneau commutatif, intègre

intègre : $xy = 0 \Rightarrow x = 0$ ou $y = 0$

$(\mathbb{K}[X], +, \times)$ anneau commutatif intègre.

3. Qu'est-ce que le groupe des inversibles ?

$(A, +, \times)$

Mque l'ensemble des inversibles $(A^*, \times)$ est un groupe. $\mathcal{U}(A)$

- $\times$ loi de ci de A^*

  Soit $x, y \in A^*$, $x \times y \in A^*$

  car $x \times y$ est inversible et

  $(x \times y)^{-1} = y^{-1} \times x^{-1}$

- $\times$ est associative car elle l'est dans $(A, +, \times)$

- $1_A \in A^*$ car 1_A inversible, d'inverse 1_A.

- Soit $x \in A^*$

  Mque x a un inverse pour $\times$. dans A^* ?

  Par déf de A^*, x a un inverse x^{-1} dans A.

  et $x^{-1} \in A^*$ car x^{-1} est inversible, d'inverse x.

Ccl : $(A^*, \times)$ est un groupe.

Exemple : $(\mathbb{R}^*, \times)$ est un groupe

$(\mathbb{Z}^* = \{-1, 1\}, \times)$ est un groupe

$\mathbb{Z} \setminus \{0\}$ $\quad (\mathcal{M}_n(\mathbb{R}))^* = GL_n(\mathbb{R})$

anneau commutatif tq tout élément $\neq 0_A$ est inversible.

4. Qu'est-ce qu'un corps ?

5. Quand dit-on qu'un anneau est intègre ?

A commutatif et $\forall x, y \quad xy = 0 \Rightarrow x = 0$ ou $y = 0$

6. Qu'est-ce qu'un sous-anneau ?

B sous-anneau de $(A, +, \times)$

signifie : B sous-groupe de $(A, +)$
B stable par $\times$
$1_A \in B$

ou : $B \subset A$
B stable par $+$
(B stable par passage à l'opposé)
B stable par $\times$
$1_A \in B$

7. Quelles sont les règles de calcul dans un anneau ?

- $a \times 0_A = 0_A$
- $a \times (-1_A) = -a$
- $a \times \left(\sum_{i=1}^{n} b_i \right) = \sum_{i=1}^{n} a \times b_i$
- $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$ $\underline{\underline{\text{si}}}$ $a \times b = b \times a$
- $a^n - b^n = (a-b) \sum_{k=0}^{n-1} a^k b^{n-k-1}$ si $ab = ba$
- $(1_A - a)\left(\sum_{k=0}^{n} a^k \right) = 1 - a^{n+1}$

$$(a+b)^2 = (a+b)(a+b)$$
$$= a^2 + ab + ba + b^2$$

8. Qu'est-ce qu'un morphisme d'anneaux ?

9. Et un isomorphisme d'anneaux ?

$f : (A, +, \times) \longrightarrow (B, +, \times)$

tq $\forall x, y \in A$
$$\left| \begin{array}{l} f(x+y) = f(x) + f(y) \\ f(x \times y) = f(x) \times f(y) \\ f(1_A) = 1_B \end{array} \right.$$

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. :

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

Exemple : Dans $(\mathbb{Z}, +, \times)$, notons $I = \{$entiers pairs$\}$

c'est un idéal. Si $x \in I$, $a \in \mathbb{Z}$

xa pair donc $xa \in I$.

Théorème.

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

- On sait déjà que f est un morphisme de groupes,

  donc $\operatorname{Ker} f = f^{-1}(\{0_B\})$ est un sous-groupe de A

- Mq que $\operatorname{Ker} f$ est absorbant.

  Soit $x \in \operatorname{Ker} f$ ie $f(x) = 0_B$

  Soit $a \in A$

  On calcule : $f(ax) = f(a) f(x)$ car f morphisme d'anneaux

  $= f(a)\, 0_B$

  $= 0_B$

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

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.*

exemple. $2\mathbb{Z}$ est l'idéal engendré par 2 dans $\mathbb{Z}$.

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 $a = ub$.