

Anneaux

I) Rapports

- 1) Définition: Un anneau est un triplet $(A, +, \cdot)$ avec $A \neq \emptyset$, $(A, +)$ gpe abélien, \cdot loi de compo interne sur A { associative possédant un neutre distributive sur $+$
- 2) Morphisme d'anneaux: $A \rightarrow A'$ deux anneaux et $\varphi: A \rightarrow A'$. φ morphisme d'anneaux $\Leftrightarrow \begin{cases} \varphi(x+y) = \varphi(x) + \varphi(y) \\ \varphi(xy) = \varphi(x)\varphi(y) \\ \varphi(1) = 1 \end{cases}$
- 3) Anneau intègre: Un anneau est dit intègre $\Leftrightarrow \mathbb{Z}$ est commutatif et $\forall x \in A', x \neq 0 \Rightarrow x \cdot 0 = 0$.
exemples: \mathbb{Z} et $K[x]$ sont intègres. $M_n(K)$ n'est pas intègre.

II) Ideal (A commutatif)

- 1) Définition: I est un idéal de $A \Leftrightarrow \begin{cases} I \text{ sous-groupe de } (A, +) \\ I \text{ permise de } A, \text{ i.e. } \forall a \in A, \forall x \in I, ax \in I. \end{cases}$
- 2) Exemples:
a) $I = A$ est un idéal de A , et $I = \{0\}$ est un idéal de A .
b) Ideaux de \mathbb{Z} : les idéaux de \mathbb{Z} sont les $(n\mathbb{Z})$.
c) Exemple fondament: le noyau d'un morphisme d'anneaux commutatifs est un idéal.
- 3) Opérations sur les idéaux:
a) Toute intersection, finie ou non, d'idéaux est un idéal.
b) $I_1 + I_2$ deux idéaux de A . Alors $(I_1 + I_2) = \{x_1 + x_2 \mid x_1 \in I_1, x_2 \in I_2\}$ est un idéal de A .
- 4) Ideal engendré par une partie:
a) Définition: Soit A un anneau et X une partie de A . L'idéal engendré par X est $I(X) = \bigcap I_i$.
b) Propriété: $I(X) = \{x \in A \mid \exists \lambda_i \in A, x = \sum \lambda_i x_i\}$ (par commutativité), $\forall x \in A$.
c) Définition: Un idéal engendré par un $x \in A$, de la forme (x) est dit "principal".
Un anneau dont tous les idéaux sont principaux est "principal".

5) Divisibilité dans un anneau

- a) Définition: On dit que $x/y \Leftrightarrow \exists z \in A \mid y = xz$.
- b) Propriété: $x \mid y \Leftrightarrow \exists \lambda \in A, y = \lambda x$.

III) L'anneau \mathbb{Z}

- 1) Rappel: les idéaux de \mathbb{Z} sont les $n\mathbb{Z}$, et ils sont principaux. \mathbb{Z} est un anneau principal.
- 2) Application au PGCD: $(x, y) \in \mathbb{Z}^2$, $\mathbb{Z}x \cap \mathbb{Z}y$ est un idéal de \mathbb{Z} .
Théorème: Si $\mathbb{Z}x + \mathbb{Z}y = \mathbb{Z}d$, alors $d = \text{pgcd}(x, y)$.
- 3) Application au PPCM: $(x, y) \in \mathbb{Z}^2$, $\mathbb{Z}x \cap \mathbb{Z}y$ est un idéal de \mathbb{Z} .
Théorème: Si $\mathbb{Z}x \cap \mathbb{Z}y = \mathbb{Z}p$, $p = \text{ppcm}(x, y)$.
- 4) Remarque: on étend ces définitions à tous les types d'anneaux principaux.

IV) L'anneau $\mathbb{Z}/n\mathbb{Z}$ ($n > 0$)

- 1) Définition:
a) PGC: le produit dans \mathbb{Z} est compatible avec $\mathbb{Z}/n\mathbb{Z}$.
b) Définition: $\bar{x} \cdot \bar{y} = \overline{xy}$
c) PGC: $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau commutatif, et la projection $p: \begin{cases} \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \\ x \mapsto \bar{x} \end{cases}$ est un morphisme d'anneaux.
- 2) Éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$:
a) Propriété: pour $x \in \mathbb{Z}$, \bar{x} inversible dans $\mathbb{Z}/n\mathbb{Z} \Leftrightarrow \text{pgcd}(x, n) = 1 \Leftrightarrow \bar{x}$ est un générateur du groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$.
b) Définition: On note $(\mathbb{Z}/n\mathbb{Z})^*$ l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$. ex: $(\mathbb{Z}/6\mathbb{Z})^* = \{\bar{1}, \bar{5}\} = \{\bar{1}, \bar{-1}\}$
- 3) Une factorisation: Théorème: Soit $f: \mathbb{Z} \rightarrow A$ un morphisme d'anneaux commutatifs. Ker $f = n\mathbb{Z}$ ($n > 0$), et $\exists!$ morphisme $\bar{f}: \mathbb{Z}/n\mathbb{Z} \rightarrow A$ tel que $f = \bar{f} \circ p$. De plus, \bar{f} est injectif. On a donc:
$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{f} & A \\ p \downarrow & \nearrow \bar{f} & \\ \mathbb{Z}/n\mathbb{Z} & & \end{array}$$
- 4) Théorème Chinois:
a) PGC: Soit m, n tq $\text{pgcd}(m, n) = 1$. On considère \bar{x}_m et \bar{x}_n les classes modulo m et n de x . On définit alors:
$$f: \begin{cases} \mathbb{Z} \rightarrow (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \\ x \mapsto (\bar{x}_m, \bar{x}_n) \end{cases}$$
 On constate que f est un morphisme d'anneaux.
b) Théorème: Avec m, n premiers entre eux, \bar{f} est un morphisme d'anneaux surjectif de noyau $(mn\mathbb{Z})$. On en déduit l'isomorphisme:
$$\bar{f}: \mathbb{Z}/mn\mathbb{Z} \xrightarrow{\sim} (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$$

c) Applications: m, n premiers; le théorème assure que $\exists x \in \mathbb{Z} \mid \begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$.
d) Remarque: m, n premiers. le groupe $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ est cyclique isomorphe à $\mathbb{Z}/mn\mathbb{Z}$. Un générateur est $\bar{f}(\bar{x}_m) = (\bar{x}_m, \bar{x}_n)$.
- 5) Idéal de $\mathbb{Q}(n)$:
a) PGC: Comme $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, alors on a aussi $(\mathbb{Z}/m\mathbb{Z})^* \cong (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$, pour m, n premiers.
b) Formule: $n = p_1^{a_1} \dots p_r^{a_r}$ décomposé en facteurs premiers.
$$\varphi(n) = \prod_{i=1}^r (p_i^{a_i} - p_i^{a_i-1}) = n \prod_{i=1}^r (1 - \frac{1}{p_i})$$

② le corps $\mathbb{Z}/p\mathbb{Z}$ avec p premier

1) Théorème: $\mathbb{Z}/p\mathbb{Z}$ est un corps $\Leftrightarrow p$ premier

2) Application: Petit Théorème de Fermat

a) Cas particulier: Si p premier, $p \nmid x \Rightarrow x^{p-1} \equiv 1 [p]$ et $\forall x \in \mathbb{Z}, p \mid (x^p - x)$ ($x^p \equiv x [p]$).

b) Cas général: $x \wedge n = 1 \Rightarrow x^{\varphi(n)} \equiv 1 [n]$

3) Caractéristique d'un corps.

Soit $f: \mathbb{Z} \rightarrow K$ avec K corps commutatif. f est un morphisme d'anneaux commutatifs.

$x \mapsto x \cdot 1_K$

le noyau de f est $\text{Ker} f = n\mathbb{Z}$, $n > 0$.

Si $n = 0$, on dit que K est de caractéristique zéro.

Si $n > 0$, alors n est premier et on dit que K est de caractéristique n .