

ANNEAUX ET CORPS

Définition: Anneau

Soit A un ensemble et $+$ et $\times$ deux lois de composition interne sur A . On dit que $(A, +, \times)$ a une structure d'anneau lorsque :

- $(A, +)$ est un groupe abélien d'élément neutre 0_A ; dit le neutre de A
- $\times$ est associative, distributive par rapport à $+$ et elle admet un élément neutre 1_A ; dit l'unité de A

Si de plus $\times$ est commutative, on dit que $(A, +, \times)$ est un anneau commutatif.

Définition: Anneau intègre

Un anneau $(A, +, \times)$ est dit intègre s'il est commutatif, non nul et

$$\forall a, b \in A, \quad a \times b = 0 \Rightarrow a = 0 \text{ ou } b = 0$$

Propriété: Formules importantes

Soit a, b deux éléments d'un anneau A tels que $ab = ba$. Alors pour tout $n \in \mathbb{N}$

- Formule de binôme de Newton:** $(a + b)^n = \sum_{k=0}^n C_n^k a^k b^{n-k}$
- Formule de factorisation:** $a^{n+1} - b^{n+1} = (a - b) \sum_{k=0}^n a^k b^{n-k}$

Théorème: Groupes des unités

Soit $(A, +, \times)$ un anneau. $\mathbb{U}(A)$ l'ensemble des éléments inversibles muni de $\times$ est un groupe appelé groupe des inversibles.

Définition: Corps

$(\mathbb{K}, +, \times)$ est corps si, et seulement, si :

- $(\mathbb{K}, +, \times)$ est un anneau commutatif;
- $\mathbb{U}(\mathbb{K}) = \mathbb{K}^* = \mathbb{K} \setminus \{0\}$

Tout corps est un anneau intègre

Propriété: L'ensemble $\mathbb{Z}/n\mathbb{Z}$

- $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif.
- $\mathbb{U}(\mathbb{Z}/n\mathbb{Z}) = \{\bar{x}, x \in \llbracket 0, n-1 \rrbracket \text{ et } x \wedge n = 1\}$
- $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps si et seulement si n est premier;

Définition: Sous-anneau

Soit $(A, +, \times)$ un anneau. Un sous-ensemble B de A est dit sous-anneau de A si, et seulement, si

- $1_A \in B$
- Pour $x, y \in B$, $x - y \in B$ et $x \times y \in B$

Auquel cas B muni des lois restreintes est un anneau

Définition: Sous-corps

Soient $(\mathbb{K}, +, \times)$ un corps. On dit qu'une partie $\mathbb{L}$ de $\mathbb{K}$ est un sous-corps de $\mathbb{K}$ si et seulement si :

- $1_{\mathbb{K}} \in \mathbb{L}$
- Pour $x, y \in \mathbb{L}$, $x - y \in \mathbb{L}$ et $x \times y \in \mathbb{L}$
- $\forall x \in \mathbb{L} \setminus \{0\}, x^{-1} \in \mathbb{L}$

Auquel cas $\mathbb{L}$ muni des lois restreintes est un corps

MORPHISME D'ANNEAUX

Définition: Morphisme d'anneaux

Soient A, A' deux anneaux. Une application $f : A \rightarrow A'$ est dite morphisme d'anneaux si:

- $f(1_A) = 1_{A'}$;
- $\forall (x, y) \in A^2: f(x + y) = f(x) + f(y)$ et $f(xy) = f(x)f(y)$.

Si de plus f est bijective, on parle d'isomorphisme d'anneaux

- Même définition que morphisme de corps.
- $\text{Ker} f = f^{-1}(\{0_{A'}\})$ et $\text{Im}(f) = f(A)$.
- f est injective si, et seulement si, $\text{Ker} f = \{0_A\}$

Théorème: Lemme de Chinois

Soit $m, n \in \mathbb{N}^*$ tels que $m \wedge n = 1$, alors $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

Propriété

Les images, directe et réciproque, d'un sous-anneau par un morphisme d'anneaux est un sous-anneau

IDÉAUX D'UN ANNEAU COMMUTATIF

Définition: Idéal

On appelle idéal d'un anneau commutatif A tout **sous-groupe additif** I de A vérifiant la propriété d'absorption : $\forall (a, b) \in A \times I, \quad ab \in I$

Propriété

Soit I un idéal de A . Alors $I = A \iff 1_A \in I \iff \mathbb{U}(A) \cap I \neq \emptyset$.

Les seuls idéaux d'un corps $\mathbb{K}$ sont $\mathbb{K}$ et $\{0\}$.

Propriété: Images d'un idéal

- L'image réciproque (directe) d'un idéal par un morphisme d'anneaux (surjectif) est un idéal
- Le noyau d'un morphisme d'anneaux est un idéal

Définition: Idéal engendré par une partie

Soit S une partie d'un anneau A . On appelle idéal engendré par S l'intersection de tous les idéaux de A contenant S : c'est donc le plus petit idéal (au sens de l'inclusion) de A contenant S .

Propriété: Idéal principal

L'idéal qui engendré par un singleton $\{a\}$ est dit principal: $aA = \{ab \mid b \in A\}$

Propriété: Les idéaux de $\mathbb{Z}$

Soit I un idéal de $\mathbb{Z}$, alors il existe un unique $n \in \mathbb{N}$ tel que $I = n\mathbb{Z}$.

- $a\mathbb{Z} + b\mathbb{Z} = \text{pgcd}(a, b)\mathbb{Z}$.
- $a\mathbb{Z} \cap b\mathbb{Z} = \text{ppcm}(a, b)\mathbb{Z}$.

Propriété: Les idéaux de $\mathbb{K}[X]$

Tout idéal I de $\mathbb{K}[X]$ peut s'écrire de façon unique sous la forme : $P\mathbb{K}[X]$ avec $P \in \mathbb{K}[X]$ normalisé.

INDICATEUR D'EULER

Définition: Indicateur d'Euler

Soit $n \in \mathbb{N}^*$, on note $\varphi(n) = \text{Card}\left(\mathbb{U}\left(\mathbb{Z}/n\mathbb{Z}\right)\right)$.

L'application φ est appelée l'indicateur d'Euler

Propriété: Calcul de φ

- Si $m \wedge n = 1$, alors $\varphi(mn) = \varphi(m)\varphi(n)$
- Soit p un nombre premier et $k \in \mathbb{N}^*$, alors

$$\varphi(p^k) = p^k - p^{k-1}$$

- Si $n = \prod_{i=1}^r p_i^{k_i}$ est la décomposition en facteurs premiers de l'entier n .

$$\text{Alors} \quad \varphi(n) = \prod_{i=1}^r (p_i^{k_i} - p_i^{k_i-1}) = n \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right)$$

Théorème: d'Euler

Soit $n \in \mathbb{N}^*$ et a un entier premier avec n , alors $a^{\varphi(n)} \equiv 1 \pmod{n}$.

ALGÈBRES

Définition: Algèbre

Soit un corps commutatif $\mathbb{K}$ et un ensemble $\mathbb{A}$ muni de deux lois de composition interne $+$, $\times$ et d'une loi de composition externe $."$. On dit que $(\mathbb{A}, +, \times, .)$ est une algèbre sur $\mathbb{K}$ si et seulement si :

- $(\mathbb{A}, +, .)$ est un $\mathbb{K}$ -espace vectoriel;
- $(\mathbb{A}, +, \times)$ est un anneau ;
- $\forall x, y \in \mathbb{A}, \forall \alpha \in \mathbb{K}, \alpha.(x \times y) = (\alpha.x) \times y = x \times (\alpha.y)$

Définition: Sous-algèbre

Soit $(\mathbb{A}, +, \times, .)$ une $\mathbb{K}$ -algèbre et $\mathbb{B} \subset \mathbb{A}$. On dit $\mathbb{B}$ est une sous-algèbre de $\mathbb{A}$ si, et seulement, si

- $1_{\mathbb{A}} \in \mathbb{B}$
- $\forall x, y \in \mathbb{B}, \forall \alpha, \beta \in \mathbb{K} \quad \alpha x + \beta y \in \mathbb{B}$
- $\forall x, y \in \mathbb{B}, \quad x \times y \in \mathbb{B}$

Alors munie des lois restreintes, $\mathbb{B}$ est une $\mathbb{K}$ -algèbre.

Définition: Morphisme d'algèbres

Soient $(\mathbb{A}, +, \times, .)$ et $(\mathbb{A}', +, \times, .)$ deux $\mathbb{K}$ -algèbres. On dit $f : \mathbb{A} \rightarrow \mathbb{A}'$ est un morphisme d'algèbres si et seulement si:

- $f(1_{\mathbb{A}}) = 1_{\mathbb{A}'}$
- $\forall x, y \in \mathbb{A}, \forall \alpha, \beta \in \mathbb{K}, \quad f(\alpha x + \beta y) = \alpha f(x) + \beta f(y)$
- $\forall x, y \in \mathbb{A}, \quad f(x \times y) = f(x) \times f(y)$

Un morphisme d'algèbres est à la fois une application linéaire et un morphisme d'anneaux

CONTACT INFORMATION

Web: www.elamdaoui.com

Email: elamdaoui@gmail.com

Phone: 06 62 30 38 81