

- × Anneaux et corps
- Probabilités
- Analyse fonctionnelle
- Analyse complexe
- Calcul différentiel
- Géométrie

Anneaux (I)

1) Définition

Un anneau $(A, +, \cdot)$ est un groupe abélien $(A, +)$ avec $\cdot: A \times A \rightarrow A$ tq
 $(a, b) \mapsto a \cdot b$

- i) (associativité) $\forall a, b, c \in A, a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- ii) (distributivité) $\forall a, b, c \in A, (a+b) \cdot c = a \cdot c + b \cdot c$
 $a \cdot (b+c) = a \cdot b + a \cdot c$
- iii) (unité) $\exists 1_A \in A, \forall a \in A, a \cdot 1_A = 1_A \cdot a = a$
 $0_A \neq$

Un anneau $(A, +, \cdot)$ est commutatif si de plus

$$(iv) \forall a, b \in A, a \cdot b = b \cdot a$$

Remarque: $\forall a \in A, a \cdot 0_A = 0_A$. (car: $a \cdot (0_A + 0_A) = a \cdot 0_A + a \cdot 0_A = 0_A$)

Exemples: a) $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$ sont des anneaux

b) $(\mathcal{C}^0(I, \mathbb{R}), +, \cdot)$ où: $(f \cdot g)(x) = f(x)g(x)$
fonctions continues $f: I \rightarrow \mathbb{R}$
intervalle de $\mathbb{R}$

c) $(M_n(\mathbb{Z}), +, \cdot)$ anneau (non commutatif si $n \geq 2$)

2) Construction d'anneaux

a) sous-anneau

si $(B, +, \cdot)$ anneau, si $A \subset B$ tq

$$i) 0_B, 1_B \in A, (A, +) \leq (B, +)$$

et $\forall a, b \in A, a \cdot b \in A$ (stable par produit)
(ii)

alors A est un sous-anneau de B et $(A, +, \cdot)$ est un anneau.

ex: $\mathbb{Z} + \mathbb{Z}i = \{a + ib : a, b \in \mathbb{Z}\}$ sous-anneau de $\mathbb{C}$

$$(car \quad \forall a, b, c, d \in \mathbb{Z}, (a + ib)(c + id) = \underbrace{(ac - bd)}_{\in \mathbb{Z}} + i \underbrace{(ad + bc)}_{\in \mathbb{Z}})$$

b) $\mathbb{Z} + \mathbb{Z}\sqrt{2} = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ sous-anneau de $\mathbb{R}$

c) $\mathbb{Q} + \mathbb{Q}\sqrt{2} + \mathbb{Q}\sqrt{3} + \mathbb{Q}\sqrt{6} = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\}$
est un sous-anneau de $\mathbb{R}$

d) $\mathbb{D} = \left\{ \frac{x}{10^\alpha} : x \in \mathbb{Z}, \alpha \in \mathbb{N} \right\}$ sous-anneau de $\mathbb{Q}$.

« Décimaux »

$$\left(\text{car } \frac{x}{10^\alpha} + \frac{y}{10^\beta} = \frac{10^\beta x + 10^\alpha y}{10^{\alpha+\beta}} \in \mathbb{D} \text{ si } x, y \in \mathbb{Z}, \alpha, \beta \in \mathbb{N} \right)$$

b) Produit

soi $(A, +, \cdot), (B, +, \cdot)$ anneaux alors $(A \times B, +, \cdot)$ est un anneau pour :

$$\forall a, a' \in A, b, b' \in B \quad (a, b) + (a', b') = (a + a', b + b')$$

$$(a, b) \cdot (a', b') = (aa', bb')$$

$$\text{et } 0_{A \times B} = (0_A, 0_B), \quad 1_{A \times B} = (1_A, 1_B)$$

c) Polynômes

* fonctions polynomiales

$$\mathbb{R}[x] = \left\{ f: \mathbb{R} \rightarrow \mathbb{R} \mid \exists n \in \mathbb{N}, a_0, \dots, a_n \in \mathbb{R}, \forall x \in \mathbb{R}, f(x) = a_0 + a_1 x + \dots + a_n x^n \right\}$$

« fonctions polynomiales de $\mathbb{R}$ dans $\mathbb{R}$ »

$(\mathbb{R}[x], +, \cdot)$ anneau (exo)

En effet : si $f(x) = a_0 + a_1 x + \dots + a_n x^n$ si $g(x) = b_0 + b_1 x + \dots + b_m x^m$
(pour $\cdot$) $(n \in \mathbb{N}, a_i, b_j \in \mathbb{R})$

$$\text{alors } \forall x \in \mathbb{R}, f(x)g(x) = a_0 b_0 + a_0 b_1 x + a_0 b_2 x^2 + \dots + a_n b_n x^{2n}$$

$$= a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \dots$$

$$= \sum_{k=0}^{2n} c_k x^k$$

$$\text{ou } \forall 0 \leq k \leq 2n, c_k = \sum_{\substack{0 \leq i \leq n \\ 0 \leq j \leq n \\ i+j=k}} a_i b_j$$

Définition soit $(A, +, \cdot)$ anneau commutatif.

On définit $(A[x], +, \cdot)$

$$A[x] = \left\{ (a_n)_{n \in \mathbb{N}} \in A^{\mathbb{N}} : \underbrace{\forall n \gg 0, a_n = 0}_{\exists N, \forall n \geq N} \right\} = A^{(\mathbb{N})}$$

$$+ : (a_n)_{n \in \mathbb{N}} + (b_n)_{n \in \mathbb{N}} := (a_n + b_n)_{n \in \mathbb{N}}$$

$$\cdot : (a_n)_{n \in \mathbb{N}} \cdot (b_n)_{n \in \mathbb{N}} := (c_n)_{n \in \mathbb{N}} \text{ si } \forall n \in \mathbb{N}, c_n = \sum_{k=0}^n a_k b_{n-k} = \sum_{k=0}^n a_{n-k} b_k$$

Exo: si $\forall n \geq N, a_n = 0$ et $\forall m \geq N', b_m = 0$, alors $\forall n \geq N+N'-1, c_n = 0$

Proposition: $(A[X], +, \cdot)$ est un anneau commutatif.

$$1_{A[X]} = (1, 0, \dots) \quad , \quad 0_{A[X]} = (0, 0, \dots)$$

Notation: $X := (0, 1, 0, \dots)$ (1 en $n=1$ et 0 ailleurs)

(Exo) $X^m = (0, \dots, 0, 1, 0, \dots)$

↑ position m

d'où $(a_n)_{n \in \mathbb{N}} = a_0 + a_1 X + \dots + a_k X^k + \dots$

Degré: $\deg(\sum_{k=0}^m a_k X^k) = \max\{0 \leq k \leq m : a_k \neq 0\}$ si $\sum_{k=0}^m a_k X^k \neq 0$

On dit que $A[X]$ est l'anneau des polynômes à coefficients dans A .

Remarque

$A[[X]] = A^{\mathbb{N}}$, $+, \cdot$ comme pour les polynômes, anneau des séries formelles

$(A[[X]], +, \cdot)$ anneau et $A[X]$ sous-anneau de $A[[X]]$

Remarque: $A = \mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$ $X^2 - X \neq 0$ dans $\mathbb{Z}/2\mathbb{Z}[X]$

mais $\forall x \in \mathbb{Z}/2\mathbb{Z}, x^2 - x = 0$

(polynôme non nul mais fonction polynomiale associée nulle)

3) Quotients

a) $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$

soit $n \in \mathbb{N}$.

Si $k \in \mathbb{Z}$, on note $\bar{k} = k + n\mathbb{Z} = \{k + nd : d \in \mathbb{Z}\} \subset \mathbb{Z}$

(si $n=2$, $\bar{0} = \{\text{pairs}\}$, $\bar{1} = \{\text{impairs}\}$)

on note $\mathbb{Z}/n\mathbb{Z} = \{\bar{k} : k \in \mathbb{Z}\} (= \{\bar{0}, \bar{1}, \dots, \overline{n-1}\} \text{ si } n \geq 1)$

En effet: $\forall k, l \in \mathbb{Z}, \bar{k} = \bar{l} \Leftrightarrow n \mid k-l$

[démon: $\Rightarrow$: si $\bar{k} = \bar{l}$ alors $k \in l + n\mathbb{Z}$ donc $k = l + nd$ pour un $d \in \mathbb{Z}$
donc $k-l = nd$

$\Leftarrow$: $k-l = nd \Rightarrow k + n\mathbb{Z} = l + k-l + n\mathbb{Z} = l + nd + n\mathbb{Z}$

$\subset l + n\mathbb{Z}$

et $= l + n\mathbb{Z}$.

si $k \in \mathbb{Z}$, $k = nq + r$ (division euclidienne) $q \in \mathbb{Z}, 0 \leq r < n$

$\bar{k} = \bar{r}$.

On définit :

$$\text{si } k_1, k_2 \in \mathbb{Z}, \text{ on pose } \overline{k_1 + k_2} := \overline{k_1 + k_2} \quad (\text{dans } \mathbb{Z}/n\mathbb{Z})$$

$$\overline{k_1} \cdot \overline{k_2} := \overline{k_1 \cdot k_2} \quad "$$

Proposition: a) $+$, $\cdot$ bien définies

b) $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ anneau
($n \neq 1$)

démo a) si $\overline{k_1} = \overline{l_1}$ et $\overline{k_2} = \overline{l_2}$ ($k_i, l_i \in \mathbb{Z}$)

$$\text{alors } \overline{k_1 + k_2} = \overline{l_1 + l_2}$$

$$[\text{oui car } k_1 + k_2 - (l_1 + l_2) = \underbrace{k_1 - l_1}_{n \mid k_1 - l_1} + \underbrace{k_2 - l_2}_{n \mid k_2 - l_2}]$$

$$\overline{k_1} \cdot \overline{k_2} = \overline{l_1} \cdot \overline{l_2}$$

$$[\text{oui: } n \mid k_1 k_2 - l_1 l_2 = (k_1 - l_1) k_2 + (k_2 - l_2) l_1]$$

Groupe des inversibles

Si $(A, +, \cdot)$ anneau, on note $A^\times = A^* = \{a \in A : a \text{ inversible pour } \cdot\}$

Déf: $a \in A$ inversible si $\exists b \in A, a \cdot b = 1 = b \cdot a$.

Dans ce cas, b unique et noté $b = a^{-1}$

Exemples

a) $\mathbb{Z}^* = \{\pm 1\}$

b) $\mathbb{R}[X]^* = \mathbb{R}^*$ (degré)

c) $(\mathbb{Z}/12\mathbb{Z})^* = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$

Dans $\mathbb{Z}/12\mathbb{Z}$: $\overline{5} \cdot \overline{5} = \overline{25} = \overline{1}$, $\overline{7} \cdot \overline{7} = \overline{1}$, $\overline{11} \cdot \overline{11} = \overline{1}$

$\overline{3} \cdot \overline{4} = \overline{0} \Rightarrow \overline{3}$ non inversible

d) $\mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i$, $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$

démo: si $z \in \mathbb{Z}[i]$, $|z|^2 \in \mathbb{N}$

si $z \cdot z' = 1$ dans $\mathbb{Z}[i]$, alors $\underbrace{|z|^2}_{\in \mathbb{N}} \underbrace{|z'|^2}_{\in \mathbb{N}} = 1$
 $\Rightarrow |z|^2 = 1 \Rightarrow z = \pm 1 \text{ ou } \pm i$

e) $\mathbb{Z}[\sqrt{2}] = \mathbb{Z} + \mathbb{Z}\sqrt{2}$, $\mathbb{Z}[\sqrt{2}]^* = \{\pm(1 \pm \sqrt{2})^n : n \in \mathbb{N}\}$

Proposition: Si $(A, +, \cdot)$ anneau, alors $(A^*, \cdot)$ groupe.

exo