Anneaux et corps
Probabilités
Analyse fonctionnelle
Analyse Complexe
Calcul différentiel
Géométrie

Anneaux & corps

1) Anneaux, sous-anneaux, idéaux

définition. Un anneau $(A, +, \cdot)$ est un groupe abélien $(A, +)$ avec

$$\begin{array}{ccc} A \times A & \longrightarrow & A \\ a, b & \longmapsto & a \cdot b \end{array} \quad \text{tq}$$

1) $\cdot$ est associative c-à-d : $\forall a, b, c \in A, (a \cdot b) \cdot c = a \cdot (b \cdot c)$

2) distributivité : $\forall a,b,c \in A$, $a\cdot(b+c) = a\cdot b + a\cdot c$

$(a+b)\cdot c = a\cdot c + b\cdot c$

Si de plus il existe $0 \neq 1 \in A$ tq : $\forall a \in A$, $a\cdot 1 = 1\cdot a = a$

on dit que A est unitaire

Un anneau $(A,+,\cdot)$ est commutatif si $\forall a,b \in A$, $a\cdot b = b\cdot a$

Remarque. $\forall a \in A$, $0\cdot a = 0$

(car $(0+0)\cdot a = 0\cdot a + 0\cdot a = 0\cdot a$)

exemples

a) $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ ...

b) $(\mathcal{C}^0([a,b],\mathbb{R}),+,\cdot)$ (continues)

c) $(\mathcal{M}_n(\mathbb{Z}),+,\cdot)$ $(n \geq 2 \Rightarrow$ non commutatif)

Construction d'anneaux

- Produit. Si A, B anneaux, alors $A\times B$ aussi pour : $(a,b)+(a',b') = (a+a', b+b')$ et $(a,b)\cdot(a',b') = (aa', bb')$

Sous-anneaux

Soit $(A,+,\cdot)$ anneau.

on dit que $B \subset A$ sous-anneau

si $B \subset A$ sous-groupe

et $\forall b_1, b_2 \in B$, $b_1 b_2 \in B$.

Dans ce cas, $(B,+,\cdot)$ anneau

Exemples : 1) $\mathbb{Z} + \mathbb{Z}i = \{a+ib : a,b \in \mathbb{Z}\}$
(entiers de Gauss)
est un sous-anneau de $(\mathbb{C},+,\cdot)$

(car $(a+ib)(a'+ib') = aa' - bb' + i(ab'+a'b)$)

2) $\mathbb{Z} + \mathbb{Z}\sqrt{2} = \{a+b\sqrt{2} : a,b \in \mathbb{Z}\}$

sous-anneau de $(\mathbb{R},+,\cdot)$

c) $\mathbb{D} = \left\{\frac{k}{10^n} : k \in \mathbb{Z}, n \in \mathbb{N}\right\} \subset \mathbb{Q}$.

sous-anneau de $(\mathbb{Q},+,\cdot)$

(décimaux)

d) $\mathbb{Q} + \mathbb{Q}\sqrt{2} + \mathbb{Q}\sqrt{3} + \mathbb{Q}\sqrt{6} \subset \mathbb{R}$ sous-anneau

Séries formelles.

Soit $(A,+,\cdot)$ commutatif (unitaire)

$(A[[X]],+,\cdot)$ est l'anneau tq :

- $A[[X]] = A^{\mathbb{N}} = \{(a_n)_{n\in\mathbb{N}} : \forall n, a_n \in A\}$

notation $(a_n)_n = \sum_{n\in\mathbb{N}} a_n X^n$

- $\sum_{n\in\mathbb{N}} a_n X^n + \sum_{n\in\mathbb{N}} b_n X^n := \sum_{n\in\mathbb{N}} (a_n+b_n) X^n$

- $\sum_{n\in\mathbb{N}} a_n X^n \cdot \sum_{n\in\mathbb{N}} b_n X^n = \sum_{n\in\mathbb{N}} c_n X^n$

où $\forall n$, $\boxed{c_n = a_0 b_n + a_1 b_{n-1} + \dots + a_n b_0}$

$$= \sum_{k=0}^{n} a_k b_{n-k}$$

C'est bien un anneau

De plus $A \hookrightarrow A[[X]]$, $a \mapsto (a,0,0\dots)$ est injective.

Remarque : dans $\mathbb{Z}[[X]]$, $(1-X)\cdot\left(\sum_{n\in\mathbb{N}} X^n\right) = 1$

- $A[X] = \left\{\sum_{n\in\mathbb{N}} a_n X^n \in A[[X]] : \exists N, \forall n \geq N, a_n = 0\right\}$

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

(en effet si $\forall n \geq p$, $a_n = 0$ et $\forall n \geq q$, $b_n = 0$
alors $\forall n \geq p+q-1$, $c_n = \sum_{k=0}^{n} a_k b_{n-k} = 0$)

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

Soit $n \in \mathbb{N}$.
on note $\forall k \in \mathbb{Z}$, $\overline{k} = k + n\mathbb{Z} \subset \mathbb{Z}$

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{k} : k \in \mathbb{Z}\}$$

Remarque. $\forall k, l \in \mathbb{Z}$, $\overline{k} = \overline{l} \iff n \mid k-l$

on définit: $\forall k_1, k_2 \in \mathbb{Z}$, $\overline{k_1} + \overline{k_2} = \overline{k_1 + k_2}$

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

c'est bien défini!

si $\overline{k_1} = \overline{k_1'}$, $\overline{k_2} = \overline{k_2'}$,

alors $n \mid k_1 - k_1'$ et $n \mid k_2 - k_2'$

$$\Rightarrow \quad n \mid k_1 k_2 - k_1' k_2' = k_1(k_2 - k_2') + (k_1 - k_1')k_2'$$

$(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau.

ex: $n = 2$, $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\} = \{\{\text{pairs}\}, \{\text{impairs}\}\}$

Groupe des inversibles

Soit $(A, +, \cdot)$ anneau commutatif unitaire

on dit que $a \in A$ est inversible

s'il existe $b \in A$ tel que $ab = 1$

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

Notation $A^* = \{a \in A : a \text{ inversible}\}$

Exemples

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

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

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

$[\mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i]$

démo. $N : \mathbb{Z}[i] \longrightarrow \mathbb{N}$

$a + ib \longmapsto a^2 + b^2 = |a+ib|^2$

est multiplicative.

Donc si $z \in \mathbb{Z}[i]^*$, alors $N(zz^{-1}) = 1$

$\Leftrightarrow \underbrace{N(z)}_{\in \mathbb{N}} \underbrace{N(z^{-1})}_{\in \mathbb{N}} = 1$

$\Rightarrow N(z) = 1 = a^2 + b^2$ si $z = a + ib$

$$\Rightarrow \begin{cases} a^2 = 1 \text{ et } b^2 = 0 \iff z = \pm 1 \\ a^2 = 0 \text{ et } b^2 = 0 \iff z = \pm i \end{cases}$$

- $\mathbb{Z}[\sqrt{2}] = \mathbb{Z} + \mathbb{Z}\sqrt{2}$

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

- $(\mathbb{Z}/12\mathbb{Z})^* = \{ \pm \bar{1}, \pm \bar{5} \}$

$(\mathbb{Z}/n\mathbb{Z})^* = \{ \bar{k} : k \text{ premier à } n \}$

Idéaux

définition. Soit $(A, +, \cdot)$ anneau commutatif unitaire.

on dit que $I \subset A$ idéal si

1) $I \leq A$ sous-groupe pour $+$

2) $\forall a \in A, \forall i \in I, \quad a \cdot i \in I$.

Ex: a) les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, $n \in \mathbb{Z}$

Notation. Si $x_1, \dots, x_N \in A$, on note

$$(x_1, \dots, x_N) = Ax_1 + \dots + Ax_N$$

(idéal engendré)

Exc: $(2, X) \subset \mathbb{Z}[X]$

$$\{2\mathbb{Z}[X] + X\mathbb{Z}[X]\} = \{P \in \mathbb{Z}[X] : P(0) \text{ pair}\}$$

Quotients :

Soit $(A, +, \cdot)$ commutatif unitaire

Soit $I \subset A$ idéal.

on note $A/I = \{\overline{x} : x \in A\}$

où $\forall x \in A$, $\overline{x} := x + I = \{x + i : i \in I\}$

Remarque: $\forall x, y \in A$, $\overline{x} = \overline{y} \iff \overline{x} \cap \overline{y} \neq \emptyset$

$\iff x - y \in I$

On définit $+$ et $\cdot$ sur A/I par:

$\forall x, y \in A$, $\overline{x} + \overline{y} = \overline{x+y}$

$\overline{x} \cdot \overline{y} = \overline{xy}$

Proposition. C'est bien défini et $(A/I, +, \cdot)$ est un anneau (si $I \neq A$).

$\overline{x}$ = « x modulo I ».

exemple : $\mathbb{Z}[i]/(3)$ corps de cardinal 9

$\mathbb{Z}[i]/(5) \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

Définition :

Un morphisme d'anneaux est une application $f : A \longrightarrow B$

où A, B anneaux commutatifs unitaires

tq : $\forall a, a' \in A$, $\begin{cases} f(a+a') = f(a) + f(a') \\ f(aa') = f(a)f(a') \\ f(1) = 1 \end{cases}$

Propriétés. 1) $f(0) = 0$

2) $\ker f = f^{-1}(0)$ idéal de A

3) $\operatorname{Im} f = f(A)$ sous-anneau de B

Théorème (1er théorème d'isomorphisme)

si $f : A \to B$ morphisme, alors f induit un isomorphisme (= morphisme bijectif)

$\overline{f} : A/\ker f \xrightarrow{\simeq} \operatorname{Im} f$ $\quad \bar{a} = a + \ker f \longmapsto f(a)$

Ex. $f : \mathbb{Z}[i] \longrightarrow \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

$a+ib \longmapsto (\overline{a+2b}, \overline{a-2b})$

morphisme d'anneaux surjectif de noyau

$(5) = 5\mathbb{Z}[i]$.

d'où $\mathbb{Z}[i]/(5) \xrightarrow{\sim} \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

Probabilités

1) Definitions

a) espace de probabilité

$(\Omega, \mathcal{A}, P)$

Ω : ensemble ; $\mathcal{A}$: tribu ; P : mesure

avec $P(\Omega) = 1$.

Une variable aléatoire (v.a.) est une

fonction $X : \Omega \to (E, \mu)$ mesurable

↑ espace mesuré

où $E = \mathbb{N}$ ou $\mathbb{R}$

↑ discrète ↑ continue

Définition.

Si $X : \Omega \to E$ v.a., la loi de X

est l'application $I \subset E \longmapsto P(X^{-1}(I)) = P(\{\omega \in \Omega : X(\omega) \in I\})$

mesurable

notée parfois : $I \longmapsto P(X \in I)$

Cas où $E = \mathbb{N}$

Loi de X : $n \in \mathbb{N} \longmapsto P(X = n)$

$= P(\{\omega \in \Omega : X(\omega) = n\})$

Cas où $E = \mathbb{R}$, Loi de X : $I \subset \mathbb{R}$ (intervalle) $\mapsto P(X \in I)$

Définition. Espérance et variance

Espérance

Si $X : \Omega \to \mathbb{N}$ v.a, on note $E(X) = \sum_{n \in \mathbb{N}} n P(X = n)$

(si convergence)

Si $X : \Omega \to \mathbb{R}$ v.a

si $\underbrace{\forall I \subset \mathbb{R} \text{ intervalle}}_{\text{il existe } f:\mathbb{R}\to\mathbb{R} \text{ tq}}$, $P(X \in I) = \int_I f$

on note $E(X) = \int_{\mathbb{R}} x f(x)\, dx$

(si convergence)

---

variance. $\text{var}(X) = E\left((X - E(X))^2\right)$

$= E(X^2) - E(X)^2$

Exemples

1) Bernoulli de paramètre $0 \leq p \leq 1$

$X : \Omega \longrightarrow \{0, 1\}$

$P(X=1) = p$, $P(X=0) = 1-p$

$E(X) = p$ $\quad \text{var}(X) = p - p^2 = p(1-p)$

2) Binomiale de paramètres $n \in \mathbb{N}$, et $0 \le p \le 1$

$$P(X=k) = \binom{n}{k} p^k (1-p)^{n-k}$$

$$[X : \Omega \to \{0, \dots, n\}]$$

$$E(X) = \sum_{k=0}^{n} k \binom{n}{k} p^k (1-p)^{n-k}$$

$$= \sum_{k=0}^{n} \frac{n!}{(k-1)!\,(n-k)!} p^k (1-p)^{n-k}$$

$$= \sum_{k=1}^{n} n \binom{n-1}{k-1} p^k (1-p)^{n-k}$$

$$= np \left(p + (1-p)\right)^{n-1} = np$$

$$\mathrm{var}(X) = E(X^2) - E(X)^2$$

$$= \sum_{k=0}^{n} k^2 \binom{n}{k} p^k (1-p)^{n-k} - n^2 p^2$$

$$= \sum_{k=0}^{n} k(k-1) \binom{n}{k} p^k (1-p)^{n-k} - n^2 p^2$$

$$+ \sum_{k=0}^{n} k \binom{n}{k} p^k (1-p)^{n-k}$$

$$= np - n^2p^2 + \sum_{k=2}^{n} n(n-1)\binom{n-2}{k-2} p^k (1-p)^{n-k}$$

$$= np - n^2p^2 + n(n-1)p^2 \left[p + (1-p)\right]^{n-2}$$

$$= np - n^2p^2 + n(n-1)p^2 = np(p - p^2).$$

3) Poisson - $\lambda (>0)$

$$P(X=n) = e^{-\lambda}\frac{\lambda^n}{n!} \quad (n \in \mathbb{N})$$

$$E(X) = \sum_{n=0}^{\infty} n e^{-\lambda}\frac{\lambda^n}{n!} = e^{-\lambda}\sum_{n=1}^{\infty}\frac{\lambda^n}{(n-1)!}$$

$$= \lambda e^{-\lambda}\sum_{n=1}^{\infty}\frac{\lambda^{n-1}}{(n-1)!} = \lambda$$

$\sum_{n=1}^{\infty}\frac{\lambda^{n-1}}{(n-1)!} = e^{\lambda}$

$$var(X) = E\left((X-\lambda)^2\right)$$

$$= E(X^2) - \lambda^2$$

$$= \sum_{n=0}^{\infty} n^2 e^{-\lambda}\frac{\lambda^n}{n!} - \lambda^2 = \sum_{n=0}^{\infty}\frac{n(n-1)e^{-\lambda}\lambda^n}{n!}$$

$$+ \sum_{n=0}^{\infty} n \frac{e^{-\lambda} \lambda^n}{n!} - \lambda^2$$

$$= \lambda^2 + \lambda - \lambda^2 = \lambda$$

4) Géométrique de paramètre $0 \leq p \leq 1$

$$P(X=n) = p(1-p)^n$$

$$E(X) = \sum_{n=0}^{\infty} n p (1-p)^n = p \frac{1-p}{p^2} = \frac{1-p}{p}$$

$$\left(\sum_{n=0}^{\infty} n x^n = x \left(\sum_{n=0}^{\infty} x^n \right)' = x \left(\frac{1}{1-x} \right)' \right.$$

$$\left. = \frac{x}{(1-x)^2} \right)$$

$$E(X^2) = \sum_{n=0}^{\infty} n^2 p (1-p)^n = \sum_{n=0}^{\infty} n(n-1) p (1-p)^n$$

$$+ \sum_{n=0}^{\infty} n p (1-p)^n$$

$$= p \sum_{n \geq 2} n(n-1)(1-p)^n + \frac{1-p}{p}$$

$$= \frac{2p(1-p)^2}{p^3} + \frac{(1-p)}{p}$$

$$= \frac{2(1-p)^2}{p^2} + \frac{(1-p)}{p}$$

$$\Rightarrow \mathrm{Var}(X) = \frac{2(1-p)^2}{p^2} + \frac{(1-p)}{p} - \left(\frac{(1-p)}{p}\right)^2$$

$$= \left(\frac{1-p}{p}\right)^2 + \frac{(1-p)}{p} = \frac{1-p}{p}\left(\frac{1}{p}\right)$$

5) $$P(X \in I) = \int_I \lambda e^{-\lambda x} 1_{\mathbb{R}_{\geq 0}}(x)\, dx$$

(Loi exponentielle)

$\lambda > 0$

$$E(X) = \int_{\mathbb{R}_{\geq 0}} x \lambda e^{-\lambda x} dx = \int_0^\infty \frac{x}{\frac{1}{\lambda}} e^{-\lambda x} dx$$

$$= \frac{1}{\lambda}$$

$$\mathrm{Var}(X) = \int_0^\infty x^2 \lambda e^{-\lambda x} dx - \frac{1}{\lambda^2}$$

$$= + \int_0^\infty 2x e^{-\lambda x} dx \quad - \frac{1}{\lambda^2}$$

$$= \frac{2}{\lambda} \int_0^\infty e^{-\lambda x} dx - \frac{1}{\lambda^2}$$

$$= \frac{1}{\lambda^2} .$$

Analyse fonctionnelle.

1) Espaces L^p.

Soit (X, μ) mesuré. $\overline{\mathbb{R}} = \mathbb{R} \cup \{\pm\infty\}$

définition.

si $1 \leq p < \infty$ réel

$$\mathcal{L}^p(X, \mu) = \left\{ f : X \to \overline{\mathbb{R}} : \text{mesurable et } \int_X |f|^p d\mu < \infty \right\}$$

$$\mathcal{L}^\infty(X,\mu) = \{ f : X \to \overline{\mathbb{R}} : \sup_{ess} |f| < \infty \}$$

où $\sup_{ess} |f| = \inf \{ A \geq 0 : |f| < A \ \mu\text{-p.p.} \}$

$\forall 1 \leq p \leq \infty$, $\forall f, g \in \mathcal{L}^p(X,\mu)$,
on note $f \sim g$ si $f = g$ μ p.p.
et $L^p(X,\mu) = \mathcal{L}^p(X,\mu) / \sim$

Normes

Si $f : X \to \overline{\mathbb{R}}$ mesurable, on pose
$\|f\|_p = \left(\int_X |f|^p \, d\mu \right)^{1/p}$ si $1 \leq p < \infty$
et $\|f\|_\infty = \sup_{ess} |f|$

Proposition. $\forall 1 \leq p \leq \infty$, $\forall f, g \in \mathcal{L}^p(X,\mu)$,

$$f \sim g \Rightarrow \|f\|_p = \|g\|_p$$

Théorème. Inégalité de Minkowski :

Soit $1 \leq p \leq \infty$

$\forall f, g : X \to \overline{\mathbb{R}}$ mesurables,

$$\|f+g\|_p \leq \|f\|_p + \|g\|_p .$$

démo. si $1 < p < \infty$

Lemme si $p, q \geq 1$ et $\frac{1}{p} + \frac{1}{q} = 1$

alors $\forall x, y \geq 0$, $xy \leq \frac{x^p}{p} + \frac{y^q}{q}$

démo : $\ln$ concave

$$\Rightarrow \ln\left(\frac{x^p}{p} + \frac{y^q}{q}\right) \geq \underbrace{\frac{1}{p}\ln(x^p) + \frac{1}{q}\ln(y^q)}_{\ln(xy)}$$

□

d'où : $$\int_X |fg| \, d\mu \leq \|f\|_p \, \|g\|_q$$

En effet : $\forall A > 0$

$$\int_X |fg| \, d\mu \leq A^p \int_X \frac{|f|^p}{p} \, d\mu + \frac{1}{A^q} \int_X \frac{|g|^q}{q} \, d\mu$$

Soit A tq $A^p \|f\|_p^p = \dfrac{\|g\|_q^q}{A^q}$

$\left(A = \sqrt[p+q]{\dfrac{\|g\|_q^q}{\|f\|_p^p}} \right)$

avec ce A : $\displaystyle\int_X |fg|\,d\mu \le \underbrace{A^p \int_X |f|^p\,d\mu}_{\|g\|_q^{\frac{qp}{p+q}} \, \|f\|_p^{p^2/p+q}} \, \|f\|_p^p$

$= \|g\|_q \|f\|_p$.

(Hölder).

ou $\dfrac{1}{p} + \dfrac{1}{q} = 1 \iff p+q = pq$

$$\|f+g\|_p^p = \int_X |f+g|^p\,d\mu$$

$$\le \int_X |f+g|^{p-1}|f|\,d\mu + \int_X |f+g|^{p-1}|g|\,d\mu$$

$$\le \|f\|_p \|(f+g)^{p-1}\|_q + \|g\|_p \|(f+g)^{p-1}\|_q$$

où $\frac{1}{p} + \frac{1}{q} = 1$ c-à-d $q = \frac{1}{1 - \frac{1}{p}} = \frac{p}{p-1}$

$$\|(f+g)^{p-1}\|_q = \left(\int_X |f+g|^{(p-1)q} \, d\mu \right)^{1/q}$$

$$= \|f+g\|_p^{p/q}$$

donc $\|f+g\|_p^p \leq (\|f\|_p + \|g\|_p) \|f+g\|_p^{p/q}$

$$\Leftrightarrow \underbrace{\|f+g\|_p^{p-p/q}}_{= \|f+g\|_p} \leq \|f\|_p + \|g\|_p$$

□

Remarques.

1) Si $\mu(X) < \infty$ alors

$\forall 1 \leq p_1 \leq p_2 \leq \infty$,

$L^\infty(X,\mu) \subset L^{p_2}(X,\mu) \subset L^{p_1}(X,\mu) \subset L^1(X,\mu)$

2) si $X = \mathbb{N}$ et μ = dénombrement

$\forall 1 \leq p_1 \leq p_2 \leq \infty$

$$\ell^1(\mathbb{N}) \subset \ell^{p_1}(\mathbb{N}) \subset \ell^{p_2}(\mathbb{N}) \subset \ell^\infty(\mathbb{N})$$

$$\ell^1(\mathbb{N}) = \mathcal{L}^1(X, \mu)$$

suite jeudi 30/1