

Anneaux et corps

Anneaux quotients.

définition. Soit A un anneau commutatif

On dit que $I \subset A$ est un idéal si

- i) I sous-groupe de $(A, +)$
- ii) $\forall a \in A, \forall i \in I, ai \in I$

Ex. $I = 0, I = A$ sont des idéaux

remarque. $I = A \Leftrightarrow 1 \in I$

Si $I \neq A$ on dit que I idéal propre

Ex. $I = \{P(X, Y) \in \mathbb{C}[X, Y] : P(0, 0) = 0\}$ idéal de $\mathbb{C}[X, Y]$

1) Noyaux

Si $\varphi : A \rightarrow B$ morphisme d'anneaux

(c.-à-d. : $\forall x, y \in A, \varphi(x+y) = \varphi(x) + \varphi(y)$

et $\varphi(xy) = \varphi(x)\varphi(y)$ et $\varphi(1) = 1$)

Alors $\text{Ker } \varphi = \text{noyau de } \varphi = \varphi^{-1}(\{0\})$ est un idéal de A .

« Tous les idéaux sont des noyaux »

2) Définition du quotient.

Soit A anneau, soit $I \leq A$ idéal propre

On note $\forall x \in A, \bar{x} := x + I = \{x + i : i \in I\}$ classe de x modulo I .

remarque. $\forall x, y \in A, \bar{x} = \bar{y} \Leftrightarrow x - y \in I$

($\Rightarrow: x \in \bar{x} = \bar{y} \Rightarrow x = y + i$ pour un $i \in I \Rightarrow x - y = i \in I$)

On définit $A/I = \{x + I : x \in A\}$

$$\forall \bar{x}, \bar{y} \in A/I, \quad \bar{x} + \bar{y} := \overline{x+y}$$
$$\bar{x} \cdot \bar{y} := \overline{xy}$$

Proposition 0) $+$ et $\cdot$ sont des opérations sur A/I

1) $(A/I, +, \cdot)$ anneau [$0_{A/I} = \bar{0}, 1_{A/I} = \bar{1}$]

2) $\pi: A \rightarrow A/I, x \mapsto \bar{x}$ est un morphisme d'anneaux et $\text{Ker } \pi = I$.

démo de 0) si $\bar{x} = \bar{x}'$ et $\bar{y} = \bar{y}'$ avec $x, x', y, y' \in A$
alors $\overline{xy} = \overline{x'y'}$ et $\overline{x+y} = \overline{x'+y'}$

En effet:

$$xy - x'y' = xy - xy' + xy' - x'y' = x(y - y') + y'(x - x')$$

$\underbrace{\quad}_{\in I} \quad \underbrace{\quad}_{\in I} \quad \underbrace{\quad}_{\in I} \quad \underbrace{\quad}_{\in I}$

1^{er} théorème d'isomorphisme. Si $\varphi: A \rightarrow B$ morphisme d'anneaux
alors $A/\text{Ker } \varphi \simeq \varphi(A)$ isomorphisme d'anneaux
 $\bar{x} \longmapsto \varphi(x)$

Exemple. $A = \mathbb{C}[X, Y]$ $I = (X, Y) = \{Xf(X, Y) + Yg(X, Y) : f, g \in \mathbb{C}[X, Y]\}$
 $= \{P(X, Y) \in \mathbb{C}[X, Y] : P(0, 0) = 0\}$

$$A/I \simeq \mathbb{C}$$

car $A \rightarrow \mathbb{C}$ morphisme surjectif de noyau I
 $P(X, Y) \mapsto P(0, 0)$

3) Idéaux premiers et maximaux

Définition Soit $I \subsetneq A$ idéal propre.

on dit que I est premier si $\forall x, y \in A, xy \in I \Rightarrow x \in I \text{ ou } y \in I$

I est maximal si $\forall I \subsetneq J \subsetneq A$ idéal

$$J = I \text{ ou } J = A$$

Théorème. Soit $I \subsetneq A$ idéal propre

1) I premier $\Leftrightarrow A/I$ intègre

2) I maximal $\Leftrightarrow A/I$ corps

Corollaire maximal $\Rightarrow$ premier

Ex. $n\mathbb{Z}$ idéal propre de $\mathbb{Z}$. Et $n\mathbb{Z}$ premier $\Leftrightarrow n=0$ ou n premier
 $n \neq \pm 1$ $n\mathbb{Z}$ maximal $\Leftrightarrow n$ premier

démo du théorème.

1) Soient $x, y \in A$. $xy \in I \Leftrightarrow \overline{xy} = \overline{0}$ (dans A/I)

$$\Leftrightarrow \overline{x} \cdot \overline{y} = \overline{0}$$

$$\Rightarrow \overline{x} \text{ ou } \overline{y} = \overline{0} \text{ si } A/I \text{ intègre}$$

$$\Rightarrow x \text{ ou } y \in I \text{ si } A/I \text{ intègre}$$

donc A/I intègre $\Rightarrow I$ premier

Réciproque : si I premier, $\overline{x} \cdot \overline{y} = \overline{0} \Rightarrow xy \in I \Rightarrow x \text{ ou } y \in I$
 $\Rightarrow \overline{x} \text{ ou } \overline{y} = \overline{0}$

2) Si A/I corps si $I \subsetneq J \subsetneq A$

si $I \neq J$ alors $\exists x \in J \setminus I \Rightarrow \overline{x} \neq \overline{0}$

$$\Rightarrow \exists \overline{y} \in A/I, \overline{x} \cdot \overline{y} = \overline{1}$$

$$\Rightarrow xy = 1 \text{ mod } I = 1 + I$$

$$\Rightarrow xy = 1 + i \text{ (} i \in I \text{)} \Rightarrow 1 = xy - i \in J$$

$$\Rightarrow J=A$$

Réciproquement si I maximal.

$$\text{si } \overline{x} \neq \overline{0} \quad \text{c-à-d } x \in A \setminus I$$

$$I \leq I + Ax = \{i + \lambda x : \lambda \in A\} = \text{idéal de } A$$

$$\Rightarrow I + Ax = A \Rightarrow \exists i \in I, \lambda \in A, i + \lambda x = 1 \Rightarrow \overline{\lambda x} = \overline{1}$$

Exemple: $A = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$

$$I = (3) = 3A = \{3x : x \in A\} \leq A$$

$$A/I = \{\pm \overline{1}, \pm \overline{\sqrt{2}}, \pm \overline{1} \pm \overline{\sqrt{2}}, \overline{0}\}$$

$$\sqrt{2} \cdot (-\sqrt{2}) = -2 = 1 + 3A, (1 + \sqrt{2})(-1 + \sqrt{2}) = 1$$

on en déduit que tous les éléments de $A/I \setminus \{0\}$ sont inversibles.

$$\Rightarrow A/I \text{ corps} \Rightarrow I \text{ maximal.}$$

4) Cas des anneaux principaux

Définition Un anneau intègre A est principal si tous ses idéaux sont de la forme $I = (a)$ pour un $a \in A$

exemple: $\mathbb{Z}$, $K[X]$ si K corps, $\mathbb{Z}[i]$ entiers de Gauss $= \{a + ib : a, b \in \mathbb{Z}\}$

[démon pour $K[X]$: si $I \leq K[X]$ idéal non nul

$$\text{soit } d = \min \{ \deg(P) : P \in I \}$$

$$\text{Soit } P \in I \text{ tq } \deg P = d.$$

$$\text{Alors } (P) = I \text{ car si } Q \in I, Q = PS + R \text{ pour}$$

$$\text{certains } S, R \in K[X] \text{ tq } \deg R < \deg Q \text{ (ou } R=0)$$

$$\Rightarrow R = Q - PS \in I \Rightarrow \text{minimalité de } d = \deg P, R=0 \Leftrightarrow Q=PS$$

Definition. Soit A anneau intègre.

On dit que $a \in A$ est irréductible si a non inversible
et: $\forall b, c \in A, a = bc \Rightarrow b$ ou c inversible

On dit que $a \in A$ est premier si (a) idéal premier

Proposition. Si A principal, si $0 \neq a \in A$ non inversible alors
 a irréductible $\Leftrightarrow a$ premier $\Leftrightarrow (a)$ maximal

Contre-exemple. $A = \mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5} : a, b \in \mathbb{Z}\}$ sous-anneau de $\mathbb{C}$

$$\text{Dans } A: 6 = 2 \cdot 3 = (1+i\sqrt{5})(1-i\sqrt{5})$$

et $2, 3, 1 \pm i\sqrt{5}$ sont irréductibles (et non premiers)

En effet $(1+i\sqrt{5})(1-i\sqrt{5}) \in (2)$ mais $1 \pm i\sqrt{5} \notin (2)$

Vérifions 2 irréductible

Ponons $N: A \rightarrow \mathbb{N}$.

$$z \mapsto |z|^2 = a^2 + 5b^2 \text{ si } z = a + ib\sqrt{5}$$

$$\forall z, z' \in A, N(zz') = N(z)N(z'), \quad N(1) = 1$$

$$\text{Donc } z \in A^* \text{ inversible, } \exists z' \in A, zz' = 1 \Rightarrow \underbrace{N(z)}_{\in \mathbb{N}} \underbrace{N(z')}_{\in \mathbb{N}} = 1$$

$$\Rightarrow N(z) = 1 = |z|^2 \Rightarrow z = \pm 1$$

$$\text{Si } 2 = xy \text{ avec } x, y \in A, \text{ alors } \underbrace{N(2)}_4 = N(x)N(y)$$

$$\Rightarrow N(x)N(y) = 4 \Rightarrow N(x) = 1, N(y) = 4 \text{ ou } N(x) = 4, N(y) = 1$$

~~ou $N(x) = N(y) = 2$~~

$$(\text{car } a^2 + 5b^2 = 2 \text{ n'a pas de solution } a, b \in \mathbb{Z})$$

$\Downarrow$
 x ou y
inversible

démo de la proposition. Soit A principal

Soit $0 \neq a$ non inversible

(a) maximal $\Rightarrow (a)$ premier $\Rightarrow a$ irréductible

[si $a = bc$ alors $bc \in (a) \Rightarrow b \text{ ou } c \in (a)$
si par exemple $b \in (a)$, $b = ax$ pour
un $x \in A \Rightarrow a = bc = axc$
 $\Rightarrow a(1 - xc) = 0 \Rightarrow 1 - xc = 0$
 $\Rightarrow c$ inversible]

a irréductible $\Rightarrow (a)$ maximal

Car si $(a) \subseteq I \subset A$, alors $I = (x)$

pour un $x \in A \Rightarrow a \in (x) \Rightarrow \exists y \in A, xy = a$
 $\Rightarrow x$ ou y inversible
 $\Rightarrow (x) = A$ ou $(x) = (ay^{-1}) = (a)$.

Exercice 1) 2 n'est pas premier dans $\mathbb{Z}[i]$

2) Si p premier impair, alors p premier dans $\mathbb{Z}[i] \Leftrightarrow p \equiv 1 \pmod{4}$

Analyse

Convolution

Définition Soient $f, g: \mathbb{R} \rightarrow \overline{\mathbb{R}} = [-\infty, \infty]$ mesurables

On pose $\forall x \in \mathbb{R}, f * g(x) = \int_{\mathbb{R}} f(x-y)g(y) dy$
(si ça existe)

Exemple. Soient $a, b > 0$ $f(x) = e^{-ax^2}$ $g(x) = e^{-bx^2}$

$$\text{thc, } f * g(x) = \int_{\mathbb{R}} e^{-a(x-y)^2 - by^2} dy = e^{-ax^2} \int_{\mathbb{R}} e^{-(a+b)(y^2 - \frac{2axy}{a+b})} dy$$

$$y^2 - \frac{2axy}{a+b} = \left(y - \frac{a}{a+b}x\right)^2 - \frac{a^2}{(a+b)^2}x^2$$

$$f * g(x) = \int_{\mathbb{R}} e^{-ax^2} e^{\frac{a^2 x^2}{a+b}} e^{-(a+b)\left(y - \frac{a}{a+b}x\right)^2} dy$$

$$= e^{-\frac{ab}{a+b}x^2} \int_{\mathbb{R}} e^{-(a+b)t^2} dt \quad t = y - \frac{ax}{a+b}$$

$$= e^{-\frac{ab}{a+b}x^2} \frac{\sqrt{\pi}}{\sqrt{a+b}}$$

$$s = \sqrt{a+b} t$$

$$\text{car } \int_{\mathbb{R}} e^{-s^2} ds = \sqrt{\pi}$$

$$= g * f(x)$$

Théorème. Soient $p, q, r \geq 1$ tq $\frac{1}{p} + \frac{1}{q} = 1 + \frac{1}{r}$

Si $f \in \mathcal{L}^p$, $g \in \mathcal{L}^q$ alors

- 1) $f * g$ défini p.p. et mesurable
- 2) $f * g \in \mathcal{L}^r$
- 3) si $r = +\infty$ ($\frac{1}{p} + \frac{1}{q} = 1$), $f * g(x)$ existe pour tout x

$$\text{et } \forall x \quad |f * g(x)| \leq \|f\|_{\mathcal{L}^p} \|g\|_{\mathcal{L}^q}$$

démo: Hölder $\Rightarrow$ 3)

Supposons $r < \infty$

$$\frac{1}{r} + \frac{1}{p} - \frac{1}{r} + \frac{1}{q} - \frac{1}{r} = 1$$

$$\frac{1}{q} \leq 1 \Rightarrow \frac{1}{p} + \frac{1}{q} \leq \frac{1}{p} + 1 \Rightarrow \frac{1}{r} \leq \frac{1}{p}$$

Supposons $f, g \geq 0$.

$$f * g(x) = \int_{\mathbb{R}} f(x-y) g(y) dy = \int_{\mathbb{R}} h_x \cdot g$$

$$h_x(y) = f(x-y)$$

$$h_x \cdot g = \underbrace{h_x^{1/n} g^{1/n}}_{f_1} \cdot \underbrace{h_x^{1-\frac{1}{n}} g^{1-\frac{1}{n}}}_{f_2} \cdot \underbrace{g^{1-\frac{1}{n}}}_{f_3}$$

$$p_1 = n, p_2 = \frac{1}{\frac{1}{n} - \frac{1}{n}}, p_3 = \frac{1}{\frac{1}{n} - \frac{1}{n}}$$

Or Inégalité de Hölder généralisée :

$$f_1, \dots, f_k \geq 0 \Rightarrow \int_{\mathbb{R}} f_1 \dots f_k \leq \|f_1\|_{L^{p_1}} \dots \|f_k\|_{L^{p_k}}$$

$$(\forall p_1, \dots, p_k \geq 1, \frac{1}{p_1} + \dots + \frac{1}{p_k} = 1)$$

$$(*) \int_{\mathbb{R}} h_x \cdot g \leq \|h_x^{1/n} g^{1/n}\|_{L^{p_1}} \|h_x^{1-\frac{1}{n}}\|_{L^{p_2}} \|g^{1-\frac{1}{n}}\|_{L^{p_3}}$$

$$\text{Or } \|h_x^{1-\frac{1}{n}}\|_{L^{p_2}} = \left(\int_{\mathbb{R}} h_x^{\frac{1-\frac{1}{n}}{1-\frac{1}{n}}} \right)^{\frac{1}{p_2} - \frac{1}{n}}$$

$$= \left(\int_{\mathbb{R}} f^n \right)^{\frac{1}{n} - \frac{1}{n}} = \|f\|_{L^n}^{n(\frac{1}{n} - \frac{1}{n})} = \|f\|_{L^n}^{1-\frac{1}{n}}$$

$$\text{de même } \|g^{1-\frac{1}{n}}\|_{L^{p_3}} = \|g\|_{L^n}^{1-\frac{1}{n}}$$

$$\text{et } \int_{\mathbb{R}} (f * g(x))^n dx = \underbrace{\left(\int_{\mathbb{R}} \|h_x^{1/n} g^{1/n}\|_{L^n}^n dx \right)}_I \|f\|_{L^n}^{n-1} \|g\|_{L^n}^{n-1}$$

$$I = \int_{\mathbb{R}} dx \left(\int_{\mathbb{R}} dy f(x-y)^n g(y)^n \right) = \int_{\mathbb{R}} dy \left(\int_{\mathbb{R}} f(x-y)^n dx \right) g(y)^n dy$$

$$= \int_{\mathbb{R}} g(y)^n dy \int_{\mathbb{R}} f(x)^n dx = \|g\|_{L^n}^n \|f\|_{L^n}^n$$

Donc $\int_{\mathbb{R}} f * g(x)^r dx \leq \|g\|_{p,q}^r \|f\|_{p,r}^r < \infty$

donc $p, r, f * g(x) < \infty$

et $\|f * g\|_{p,r}^r \leq \|g\|_{p,q}^r \|f\|_{p,r}^r$

$\Rightarrow \|f * g\|_{p,r} \leq \|g\|_{p,q} \|f\|_{p,r}$.

ex. $p = q = r = 1$.

(Cas général: $f = f_+ - f_-$, $g = g_+ - g_-$ où $f_+ = \max\{0, f\}$
 $f_- = \max\{0, -f\}$)

Probabilités

Indépendance

Soit $(\Omega, \mathcal{A}, P)$ espace de probabilités

Définition: $A, B \in \mathcal{A}$ sont indépendants si $P(A \cap B) = P(A)P(B)$

exo: A, B indépendants $\Rightarrow A, B^c$ aussi

$$\begin{aligned} P(A \cap B^c) &= P(A) - P(A \cap B) = P(A) - P(A)P(B) \\ &= P(A)(1 - P(B)) = P(A)P(B^c). \end{aligned}$$

Définition: $A_1, \dots, A_n \in \mathcal{A}$ sont mutuellement indépendants

si $\forall I \subset \{1, \dots, n\}, P(\bigcap_{i \in I} A_i) = \prod_{i \in I} P(A_i)$

Contre-ex. $X, Y, Z : \Omega \rightarrow \{0, 1\}$ v.a. indépendantes

$P(X=0) = P(X=1) = \frac{1}{2}$ même loi pour Y, Z .

$A_1 = \{X=1\}$, $A_2 = \{Y=Z\}$, $A_3 = \{X=Z\}$

alors A_1, A_2 indépendants, A_2, A_3 aussi, A_1, A_3 aussi
 mais non A_1, A_2, A_3 .

En effet: $P(A_1 \cap A_2) = P(X=Y=Z) = P(X=Y=Z=0) + P(X=Y=Z=1)$
 $= \left(\frac{1}{2}\right)^3 + \left(\frac{1}{2}\right)^3 = \frac{1}{4}$
 $P(A_1) = P(X=Y=0) + P(X=Y=1) = \frac{1}{4} + \frac{1}{4} = \frac{1}{2} = P(A_2)$
 $\Rightarrow P(A_1 \cap A_2) = P(A_1) P(A_2)$

$$P(A_1 \cap A_2 \cap A_3) = P(X=Y=Z) = \frac{1}{4} \neq P(A_1) P(A_2) P(A_3) = \left(\frac{1}{2}\right)^3 = \frac{1}{8}$$

Proposition. X, Y v.a. indépendantes $\Rightarrow E(XY) = E(X)E(Y)$

dém. (car X, Y discrètes)

$$E(XY) = \sum_z z P(XY=z) = \sum_z z \sum_x P(XY=z, X=x)$$

$$= \sum_{z \neq 0} z \sum_{x \neq 0} P(Y = \frac{z}{x}, X=x)$$

$$= \sum_{z \neq 0} z \sum_{x \neq 0} P(Y = \frac{z}{x}) P(X=x)$$

$$= \sum_{z \neq 0} \sum_{x \neq 0} \frac{z}{x} \cdot x P(Y = \frac{z}{x}) P(X=x)$$

$$= \sum_{x \neq 0} x \left(\sum_{z \neq 0} \frac{z}{x} P(Y = \frac{z}{x}) \right) P(X=x)$$

$$\underbrace{\sum_{t \neq 0} t P(Y=t)}_{= E(Y)}$$

$$= E(Y)$$

$$= E(Y) \sum_{x \neq 0} x P(X=x) = E(Y) E(X)$$

Déf. Covariance $Cov(X, Y) = E(XY) - E(X)E(Y)$

Cor. X, Y indépendantes $\Rightarrow var(X+Y) = var(X) + var(Y)$

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

Proposition Soient X, Y, X', Y' v.a.

On suppose que $\text{Loi}(X, Y) = \text{Loi}(X', Y')$

Alors $\text{Loi de } X = \text{Loi de } X'$ et $\text{Loi de } Y = \text{Loi de } Y'$

démo. $\forall x$

$$\begin{aligned} P(X=x) &= \sum_y P(X=x, Y=y) \\ &= \sum_y P((X, Y) = (x, y)) \\ &= \sum_y P((X', Y') = (x, y)) \\ &= \sum_y P(X'=x, Y'=y) = P(X'=x). \end{aligned}$$

Contre-exemple de la réciproque.

$Z: \Omega \rightarrow \{0,1\} \times \{0,1\}$ $Z = (X, Y)$

on définit deux lois

$$P_1(Z=(0,0)) = P_1(Z=(0,1)) = P_1(Z=(1,0)) = P_1(Z=(1,1)) = \frac{1}{4}$$

$$P_2(Z=(0,0)) = P_2(Z=(1,1)) = \frac{1}{8} \text{ et } P_2(Z=(0,1)) = P_2(Z=(1,0)) = \frac{3}{8}$$

$$P_1(X=0) = P_1(Z=(0,0)) + P_1(Z=(0,1)) = \frac{1}{2} = P_1(X=1)$$

$$P_2(X=0) = P_2(Z=(0,0)) + P_2(Z=(0,1)) = \frac{1}{8} + \frac{3}{8} = \frac{1}{2} = P_2(X=1)$$

$$\text{de même } P_1(Y=0) = P_2(Y=0), P_2(Y=1) = P_2(Y=1)$$

Mais $\text{Loi}_1 \text{ de } Z \neq \text{Loi}_2 \text{ de } Z$.

Calculs

1°) Soient X, Y v.a.i. tq $X \sim \mathcal{P}(\lambda), Y \sim \mathcal{P}(\mu)$

Déterminer Loi de $X+Y$.

2°) Même question avec $X \sim \mathcal{B}(m, p), Y \sim \mathcal{B}(n, p)$
(cà d $P(X=k) = \binom{m}{k} p^k (1-p)^{m-k}$)

$$\begin{aligned}
1^\circ) \quad P(X+Y=k) &= \sum_{j=0}^k P(X=j, Y=k-j) \\
&= \sum_{j=0}^k P(X=j) P(Y=k-j) \\
&= \sum_{j=0}^k \frac{\lambda^j}{j!} e^{-\lambda} \frac{\mu^{k-j}}{(k-j)!} e^{-\mu} \\
&= e^{-\lambda-\mu} \sum_{j=0}^k \frac{\lambda^j \mu^{k-j}}{j! (k-j)!} = e^{-\lambda-\mu} \sum_{j=0}^k \frac{\binom{k}{j} \lambda^j \mu^{k-j}}{k!} \\
&= \frac{e^{-(\lambda+\mu)}}{k!} (\lambda+\mu)^k
\end{aligned}$$

$$\Rightarrow X+Y \sim \mathcal{P}(\lambda+\mu).$$

$$2^\circ) \quad X \sim \mathcal{B}(m, p) \quad Y \sim \mathcal{B}(n, p)$$

$$\begin{aligned}
P(X+Y=k) &= \sum_{\alpha=0}^k P(X=\alpha, Y=k-\alpha) \\
&= \sum_{\alpha=0}^k P(X=\alpha) P(Y=k-\alpha) \\
&= \sum_{\alpha=0}^k p^\alpha (1-p)^{m-\alpha} \binom{m}{\alpha} \binom{n}{k-\alpha} p^{k-\alpha} (1-p)^{n-(k-\alpha)} \\
&= p^k (1-p)^{m+n-k} \sum_{\alpha=0}^k \binom{m}{\alpha} \binom{n}{k-\alpha} \\
&\quad \underbrace{\qquad\qquad\qquad}_{= \binom{m+n}{k}}
\end{aligned}$$

car $(1+X)^{m+n} = (1+X)^m (1+X)^n$

$\uparrow$
 coeff. de degré k : $\binom{m+n}{k} = \sum_{\alpha=0}^k \binom{m}{\alpha} \binom{n}{k-\alpha}$

Donc $X+Y \sim \mathcal{B}(m+n, p)$.