(Anneaux & corps)

Critères d'irréductibilité des polynômes

1) Cas général K = corps

Proposition. a) Si $P \in K[X]$ de degré 1 alors P irréductible

[car si $P = AB$ alors $\deg P = \deg A + \deg B$ (= 1)

$\Rightarrow \deg A$ ou $\deg B = 0$

$\Rightarrow A$ ou $B \in (K[X])^* = K^*$]

b) Si $\deg P = 2$ ou 3 alors

P irréductible $\Leftrightarrow P$ n'a pas de racine dans K

[si $P(\alpha) = 0$ alors $X - \alpha \mid P$ dans $K[X]$

donc P a une racine $\Rightarrow P$ réductible

Réciproquement si $P = AB$ avec $\deg A, \deg B > 0$

(c-à-d A, B non inversibles)

alors $\underbrace{\deg P}_{=2 \text{ ou } 3} = \underbrace{\deg A}_{\geq 1} + \underbrace{\deg B}_{\geq 1} \Rightarrow \deg A$ ou $\deg B = 1$

Si par exemple $A = \lambda X + \mu$ avec $\lambda \neq 0$

alors $P(\alpha) = 0$ avec $\alpha = -\frac{\mu}{\lambda} \in K$

$\| $

$A(\alpha)B(\alpha)$

exemple. $P(X) = X^3 - 3X + 1$ irréductible sur $\mathbb{Q}$.

en effet il suffit de montrer que P sans racine dans $\mathbb{Q}$

Par l'absurde si $P(r) = 0$ avec $r = \frac{a}{b}$ où $a \in \mathbb{Z}$, $b \in \mathbb{Z}_{>0}$

alors $a \wedge b = 1$

$a^3 - 3a^2b + b^3 = 0$

$\Rightarrow a^3 = 3a^2b - b^3 \Rightarrow b \mid a^3$

$\Rightarrow b \mid a \Rightarrow r = \frac{a}{b} \in \mathbb{Z}$.

(lemme de Gauss)

$\Rightarrow r^3 - 3r + 1 = 0 \Rightarrow r \mid 1$ dans $\mathbb{Z}$

$\Rightarrow r = \pm 1$ absurde

car $P(1) = -1$, $P(-1) = 3 \neq 0$.

En revanche sur $\mathbb{R}$: $X^3 - 3X + 1 = \left(X - 2\cos\frac{2\pi}{9}\right)\left(X - 2\cos\frac{4\pi}{9}\right)\left(X - 2\cos\frac{8\pi}{9}\right)$

2) Sur $\mathbb{R}$ ou $\mathbb{C}$.

a) Les irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1 (théorème de d'Alembert-Gauss)

b) Les irréductibles de $\mathbb{R}[X]$ sont

- les polynômes de degré 1
- les polynômes de degré 2 de discriminant <0

[En effet si $P \in \mathbb{R}[X]$ a une racine $z \in \mathbb{C} \setminus \mathbb{R}$,
alors $P(z) = P(\bar{z}) = 0$
$\Rightarrow \underbrace{(X-z)(X-\bar{z})}_{X^2 - 2\mathrm{Re}(z)X + |z|^2 \in \mathbb{R}[X]} \mid P$.]

Ex. Factoriser X^4+1 sur $\mathbb{C}$, sur $\mathbb{R}$, sur $\mathbb{Q}$.

sur $\mathbb{C}$ $\quad x^4+1=0 \Leftrightarrow x = e^{\pm i\frac{\pi}{4}}, e^{\pm\frac{3i\pi}{4}}$

$$X^4+1 = \underbrace{(X-e^{i\pi/4})(X-e^{-i\pi/4})}(\underbrace{X-e^{3i\pi/4}})(X-e^{-3i\pi/4})$$

sur $\mathbb{R}$ $\quad X^4+1 = (X^2-\sqrt{2}X+1)\cdot(X^2+\sqrt{2}X+1)$

irréductibles

$e^{\pm i\pi/4} = \frac{1\pm i}{\sqrt{2}} \qquad e^{\pm 3i\pi/4} = \frac{-1\pm i}{\sqrt{2}}$

sur $\mathbb{Q}$: X^4+1 irréductible.

car $X^2 \pm \sqrt{2}X + 1 \notin \mathbb{Q}[X]$.

3) sur $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ $\quad p$ premier

a) Trouver les irréductibles de $\mathbb{F}_2[X]$ de degré 2, 3 ou 4

degré 2 : ~~X^2~~, X^2+X+1, ~~X^2+X~~, ~~X^2+1~~

X^2+X+1 irréductible car pas de racine parmi $\{\bar{0},\bar{1}\}$

($(X+1)^2$)

degré 3 : X^3+X^2+1, X^3+X+1.

(X^3+X^2+X+1 s'annule en $\bar{1}$)

degré 4 : $\boxed{X^4+X^3+1}$, ~~X^4+X^2+1~~, $\boxed{X^4+X+1}$, $\boxed{X^4+X^3+X^2+X+1}$

$\boxed{\ }$: les irréductibles

(polynômes de degré 4 qui ne s'annulent pas sur $\mathbb{F}_2=\{\bar{0},\bar{1}\}$)

(On a $(X^2+X+1)^2 = X^4+X^2+1$ dans $\mathbb{F}_2[X]$)

b) Trouver les irréductibles (unitaires) sur $\mathbb{F}_3$ de degré 2

X^2+aX+b

$\Delta = a^2-4b$

P	X^2+X+1	X^2+X-1	X^2+1	X^2-1	X^2-X+1	X^2-X-1
Δ	0	-1	-1	1	0	-1

-1 n'est pas un α^2, $\alpha \in \mathbb{F}_3 = \{\pm\overline{1}, \overline{0}\}$

remarque $X^2+X+1 = (X-1)^2$ dans $\mathbb{F}_3[X]$

4) Sur $\mathbb{Q}$.

a) contenu

définition. Si $P = a_0 + a_1 X + \cdots + a_n X^n$, $n \in \mathbb{N}$

$a_i \in \mathbb{Z}$, $c(P) = \text{pgcd}(a_0, \ldots, a_n)$

lemme de Gauss $c(PQ) = c(P)c(Q)$ $\left(\forall P, Q \in \mathbb{Z}[X]\right)$

démo. $\forall \lambda \in \mathbb{Z}$, $c(\lambda P) = \lambda c(P)$

on se ramène à $c(P) = c(Q) = 1$

(remplacer P par $\frac{P}{c(P)}$ et Q par $\frac{Q}{c(Q)}$)

Alors si $c(P)=c(Q)=1$, $c(PQ)=1$.

En effet si $c(PQ)\neq 1$ alors $\exists p$ premier /

p | tous les coefficient de PQ.

On $\mathbb{Z}[X] \longrightarrow \mathbb{F}_p[X]$ morphisme d'anneaux

$A(X) \longmapsto \overline{A}(X)$

$c_0+\dots+c_dX^d \longmapsto \overline{c_0}+\overline{c_1}X+\dots+\overline{c_d}X^d$

donc $\overline{PQ} = 0$ dans $\mathbb{F}_p[X]$

$\overline{PQ}$ " $\overline{P}\,\overline{Q}$

On $\mathbb{F}_p[X]$ intègre donc $\overline{P}$ ou $\overline{Q} = 0$ dans $\mathbb{F}_p[X]$

$\Rightarrow p \mid \underbrace{c(P)}_{=1}$ ou $\underbrace{c(Q)}_{=1}$ absurde □

Corollaire. Si $P\in\mathbb{Z}[X]$ alors

P irréductible dans $\mathbb{Z}[X] \iff \begin{cases} P = p \in \mathbb{Z} \text{ nombre premier} \\ \text{ou} \\ \deg P>0 \text{ et } c(P)=1 \\ \text{et } P \text{ irréductible sur } \mathbb{Q}. \end{cases}$

Critère de la réduction mod p premier

Proposition. Soit $P\in\mathbb{Z}[X]$. Si p nombre premier $\nmid a_d$

$P=a_0+\dots+a_dX^d$

Si $\overline{P} = \overline{a_0} + \dots + \overline{a_d} X^d$ est irréductible dans $\mathbb{F}_p[X]$

alors P irréductible sur $\mathbb{Q}$.

ex.

Exercice 20. Montrer que f est irréductible dans $\mathbb{Q}[x]$ dans chacun des cas suivants :

(1) $f = x^4 - 8x^3 + 12x^2 - 6x + 2$;

(2) $f = x^5 - 12x^3 + 36x - 12$;

(3) $f = x^4 - x^3 + 2x + 1$;

$P = X^4 - X^3 + 2X + 1$ irréductible sur $\mathbb{Q}$.

solution : mod 2 $\quad \overline{P} = X^4 + X^3 + 1$ irréductible sur $\mathbb{F}_2$

$\Rightarrow$ P irréductible (dans $\mathbb{Z}[X]$ $\Rightarrow$) sur $\mathbb{Q}$.

contre-exemple. $X^4 + 1$ est irréductible sur $\mathbb{Q}$

mais réductible sur $\mathbb{F}_p$ ($\forall p$ premier) [exo]

[dans $\mathbb{F}_2[X]$, $X^4 + 1 = (X+1)^4$

dans $\mathbb{F}_3[X]$, $X^4 + 1 = X^4 - 2X^2 + 1 + 2X^2$

$= (X^2 - X + 1)^2 - X^2$

$= (X^2 - 2X + 1)(X^2 + 1)$]

(Analyse fonctionnelle)

Espaces de Hilbert

Définition. H un $\mathbb{R}$-espace vectoriel (resp. un $\mathbb{C}$-espace vectoriel) avec

$\langle \cdot, \cdot \rangle : H \times H \longrightarrow \mathbb{R}$ produit scalaire

(resp. $\langle \cdot, \cdot \rangle : H \times H \to \mathbb{C}$ un produit scalaire hermitien)

[bilinéaire symétrique et $\forall 0 \neq x \in H$, $\langle x, x \rangle > 0$]

est un espace de Hilbert si $(H, \|\cdot\|)$ est complet

(où $\forall x \in H$, $\|x\| = \sqrt{\langle x, x \rangle}$)

ex: les espaces euclidiens (de dimension finie)

- $\ell^2(\mathbb{N}) = \left\{ (a_n)_n \in \mathbb{R}^{\mathbb{N}} : \sum_{n=0}^{\infty} a_n^2 < \infty \right\}$

Pour $\langle (a_n), (b_n) \rangle := \sum_{n=0}^{\infty} a_n b_n$.

- $L^2([0, 2\pi[) = \left\{ f : [0, 2\pi[\to \mathbb{C} : \int_0^{2\pi} |f|^2 < \infty \right\}_{/\sim}$

avec $\langle f, g \rangle = \frac{1}{2\pi} \int_0^{2\pi} f\,\overline{g}$.

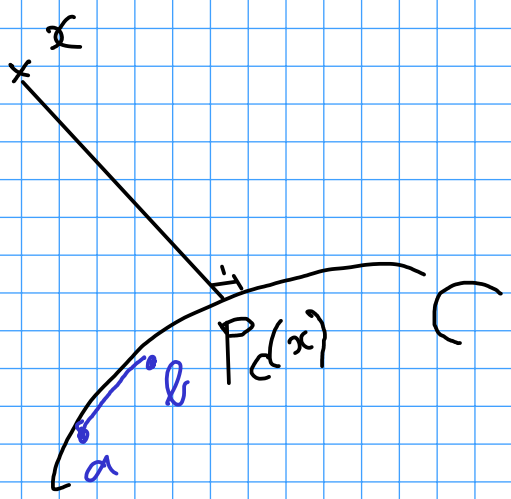
1) Projection sur un convexe fermé

Soit H un espace de Hilbert (réel)

Théorème. $\forall C \subset H$ convexe fermé,

$\forall x \in H$, $\exists!\ p_C(x) \in C$, $\|x - p_C(x)\| = d(x, C)$

$= \inf \{ \|x - z\| : z \in C \}$



Rappel: C convexe c-à-d: $\forall a, b \in C$, $\forall 0 \le t \le 1$

$ta + (1-t)b \in C$

démo. - existence

$\exists (y_n)_n \in C^{\mathbb{N}}$, $\lim_{n \to \infty} \|x - y_n\| = d(x, C)$

$\forall p,q,\quad \|y_p - y_q\|^2 = \|x-y_q-(x-y_p)\|^2$

$= \|x-y_q\|^2 + \|x-y_p\|^2 - 2\langle x-y_q, x-y_p\rangle$

$= \underbrace{2\|x-y_q\|^2}_{\xrightarrow[q\infty]{} 2d(x,C)^2} + \underbrace{2\|x-y_p\|^2}_{\xrightarrow[p\infty]{} 2d(x,C)^2} - \underbrace{4\left\|x-\frac{y_p+y_q}{2}\right\|^2}_{\geq 4d(x,C)^2}$

$\leq 2\|x-y_q\|^2 + 2\|x-y_p\|^2 - 4d(x,C)^2$

Soit $\varepsilon > 0$, $\exists N$, $\forall n \geq N$ $\|x-y_n\|^2 \leq d(x,C)^2 + \varepsilon$

$\Rightarrow \forall p,q \geq N$, $\|y_p - y_q\|^2 \leq 2\varepsilon$

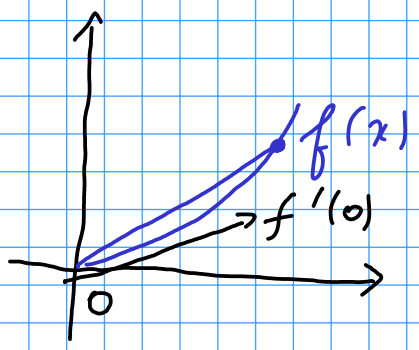
Donc (y_n) de Cauchy donc $\lim_{n\infty} y_n = y \in H$

existe. C fermé $\Rightarrow y \in C$.

<u>unicité</u>

Lemme si $f : [0,1] \to \mathbb{R}$ convexe dérivable, alors f a un minimum en 0

$\Leftrightarrow f'(0) \geq 0$



démo: $\forall x > 0$, $\dfrac{f(x)-f(0)}{x} \geq f'(0)$

et $f'(0) = \lim\limits_{\substack{x \to 0 \\ x>0}} \dfrac{f(x)-f(0)}{x}$.

Application

Supposons que $\|x-y_1\| = \|x-y_2\| = d(x,C)$ où $y_1, y_2 \in C$

$f(t) = \| x - \underbrace{(1-t)y_1 + tz}_{\in C} \|^2$ où $z \in C$

$(\forall 0 \leq t \leq 1)$

$$f(t) = \|x-y_1\|^2 + t^2\|z-y_1\|^2 - 2t\langle x-y_1, z-y_1\rangle$$

$f''(t) = 2\|z-y_1\|^2 \geq 0 \Rightarrow f$ convexe

$\forall t$, $f(t) \geq f(0)$ par définition de y_1

$\Rightarrow$ (lemme) $f'(0) = -2\langle x-y_1, z-y_1\rangle \leq 0$

donc $\forall z \in C$, $\langle x - y_1, z - y_1 \rangle \leq 0$

$\Rightarrow \langle x - y_1, y_2 - y_1 \rangle \leq 0$

de même $\langle x - y_2, y_1 - y_2 \rangle \leq 0$

$\Leftrightarrow \langle y_2 - x, y_2 - y_1 \rangle \leq 0$

$\|y_2 - y_1\|^2 = \langle y_2 - y_1, y_2 - y_1 \rangle \leq 0 \Rightarrow y_1 = y_2$.

En particulier : $\forall z \in C$, $\langle x - p_C(x), z - p_C(x) \rangle \leq 0$

Corollaire : Si $C = F \leq H$ sous-espace vectoriel fermé

alors $\forall z \in F$, $\langle x - p_F(x), \underbrace{z - p_F(x)}_{z'} \rangle \leq 0$

$\Rightarrow \forall z' \in F$, $\langle x - p_F(x), z' \rangle = 0$

$\Rightarrow x - p_F(x) \in F^\perp \quad (\forall x \in H)$

$\Rightarrow H = F \oplus F^\perp$

Corollaire. Si $F \leq H$ fermé alors $F^{\perp\perp} = F$

Remarque. Si $(e_1, \dots, e_n)$ base orthonormée de F

alors $d(x,F)^2 = \|x - p_F(x)\|^2$

$$= \|x - \langle x, e_1\rangle e_1 - \dots - \langle x, e_n\rangle e_n\|^2$$

autrement dit : $p_F(x) = \langle x, e_1\rangle e_1 + \dots + \langle x, e_n\rangle e_n$

$[\forall i \neq j, \langle e_i, e_j\rangle = 0, \forall i \ \|e_i\|^2 = 1]$

Exercice # 13. Déterminer la quantité suivante

$$m = \inf_{(a,b)\in\mathbb{R}^2} \int_0^{2\pi} |\sin x - a - bx|^2 \, dx.$$

La borne inférieure est-elle atteinte?

(feuille 2)

Solution. $H = L^2([0, 2\pi[)$

- $\langle f, g\rangle = \frac{1}{2\pi}\int_0^{2\pi} fg$

$m = 2\pi \, d(\sin x, F)^2$ où $F = \text{Vect}\{1, x\}$

$\Rightarrow m = 2\pi \|\sin x - p_F(\sin x)\|^2$

Trouver une bas orthonormée de F v_1, v_2

Puis Calculer $\langle \sin x, v_1 \rangle$, $\langle \sin x, v_2 \rangle$

$v_1 = 1$

$v_2' = x + t v_1 = x + t$ où t tq

$$\langle v_2', v_1 \rangle = 0 \Leftrightarrow \frac{1}{2\pi} \int_0^{2\pi} (x+t)\,dx = 0$$

$$\Rightarrow \quad \pi + t = 0 \Leftrightarrow t = -\pi.$$

d'où $v_2' = x - \pi$

Soit $v_2 = \dfrac{v_2'}{\|v_2'\|} = \dfrac{x-\pi}{\sqrt{\frac{1}{2\pi}\int_0^{2\pi} (x-\pi)^2\,dx}} = \dfrac{\sqrt{3}(x-\pi)}{\pi}$

Donc $\left(1, \sqrt{3}\,\dfrac{x-\pi}{\pi}\right)$ base orthonormée de F

$$\langle \sin x, v_1 \rangle = \frac{1}{2\pi} \int_0^{2\pi} \sin x\,dx = 0$$

$$\langle \sin x, v_2 \rangle = \frac{1}{2\pi} \int_0^{2\pi} \sin x \sqrt{3}\,\frac{(x-\pi)}{\pi}\,dx = \dots$$

(Probalités)

Notions de convergences

Définitions Soit X v.a. $X_n, X : \Omega \to \mathbb{R}$

Soit $(X_n)_n$ suite de v.a.

- on dit que (X_n) converge presque sûrement vers X si $P(\lim X_n = X) = 1$

$$= P\left(\left\{ \omega \in \Omega : \lim_n X_n(\omega) = X(\omega) \right\}\right) = 1$$

Notation $X_n \xrightarrow{p.s.} X$

- on dit que (X_n) converge vers X en probabilités si $\forall \varepsilon > 0$, $P(|X_n - X| \geq \varepsilon) \xrightarrow[n\infty]{} 0$

notation. $X_n \xrightarrow{P} X$

- on dit que (X_n) converge vers X en loi si $\forall f : \mathbb{R} \to \mathbb{R}$ continue bornée,

$$E(f(X_n)) \xrightarrow[n\infty]{} E(f(X))$$

notation $X_n \xrightarrow{\mathcal{L}} X$

Proposition $p.s. \Rightarrow P. \Rightarrow \mathcal{L}.$

contre-exemple : $\mathcal{L} \not\Rightarrow P.$

(X_n) v.a. i.i.d « variables aléatoires indépendantes identiquement distribuées »

$\forall n$: $P(X_n=0) = P(X=0) = P(X_n=1) = P(X=1) = \frac{1}{2}$

$X_n \overset{\mathcal{L}}{=} X$ $\qquad \forall n,\ E(f(X_n)) = E(f(X)) = \frac{f(0)+f(1)}{2}$

$\| \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \|$

$P(X_n=0) f(0) + P(X_n=1) f(1)$

Mais $P(|X_n - X| = 1) = P(X_n - X = 1) + P(X_n - X = -1)$

$= P(X_n=1, X=0) + P(X_n=0, X=1)$

$= \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$

$P(|X_n - X| = 0) = P(X_n = X = 0) + P(X_n = X = 1)$

$= \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$

Donc $P(|X_n - X| \geq 1) = \frac{1}{2} \not\xrightarrow[n\infty]{} 0$

Démo. p.s. $\Rightarrow$ P.

$\lim_{n\infty} X_n(\omega) = X(\omega)$

$\Leftrightarrow \forall k \geq 1, \exists N, \forall n \geq N \quad |X_n(\omega) - X(\omega)| < \frac{1}{k}$

donc $\{\omega : \lim_n X_n(\omega) = X(\omega)\}$

$= \bigcap_{k \geq 1} \bigcup_{N \geq 1} \bigcap_{n \geq N} \left\{ |X_n - X| < \frac{1}{k} \right\}$

$P\left(\bigcap_{k \geq 1} \bigcup_{N \geq 1} \bigcap_{n \geq N} \left\{ |X_n - X| < \frac{1}{k} \right\} \right) = 1$

décroissante

$$\forall k, \quad P\left(\bigcup_N \bigcap_{n\geq N} \left\{|X_n - X| < \frac{1}{k}\right\}\right) = 1$$

Soit k fixé

$$\Rightarrow P\left(\bigcap_N \bigcup_{n\geq N} \left\{|X_n - X| \geq \frac{1}{k}\right\}\right) = 0$$

$$\Rightarrow \lim_{N\infty} P\left(\bigcup_{n\geq N} \left\{|X_n - X| \geq \frac{1}{k}\right\}\right) = 0$$

$$\geq P\left(\left\{|X_N - X| \geq \frac{1}{k}\right\}\right)$$

$$\Rightarrow \lim_{N\infty} P\left(\left\{|X_N - X| \geq \frac{1}{k}\right\}\right) = 0.$$

$P. \Rightarrow \mathcal{L}.$

Soit $f : \mathbb{R} \to \mathbb{R}$ continue bornée

$$\lim_{R\infty} P(|X| > R) = P(X = \pm\infty) = 0$$

Soit $\varepsilon > 0$. $\exists\ R > 0$, $P(|X| > R) < \varepsilon$

f uniformément continue sur $[-2R, 2R]$.

$$\Rightarrow \exists_{0<\eta<R},\ |x-y| \leq \eta \Rightarrow |f(x) - f(y)| \leq \varepsilon$$

$$-2R \leq x, y \leq 2R$$

$$|E(f(X_n)) - E(f(X))| \leq E(|f(X_n) - f(X)|)$$

$$\leq P(|X_n - X| \leq \eta, |X| \leq R)\,\varepsilon$$

$$+ P(|X_n - X| > \eta, |X| \leq R)\, 2\|f\|_\infty$$

$$+ P(|X| > R)\, 2\|f\|_\infty$$

$$\leq \varepsilon + 2\|f\|_\infty \underbrace{P(|X_n - X| > \eta)}_{\xrightarrow[n\infty]{} 0} + 2\|f\|_\infty \varepsilon$$

$$\leq (4\|f\|_\infty + 1)\varepsilon \quad \text{si } n \gg 0.$$

□

Prochain cours le 7 mars