

Anneaux et corps

Définitions K corps, $P(x) \in K[X]$

Corps de rupture Un corps de rupture pour P sur K est un corps de la forme $L = K(\alpha)$ où $\alpha \in L$ racine de P .

Remarque. $L = K[X]/(P_\alpha)$ où $P_\alpha \in K[X]$ irréductible divise P .
 $\alpha \mapsto X$

Corps de décomposition Un corps de décomposition de P sur K est un corps de la forme $L = K(\alpha_1, \dots, \alpha_m)$ où $P = c(X-\alpha_1) \dots (X-\alpha_m)$ ($c \in K^*$)

ex: $\mathbb{Q}(\sqrt[3]{2})$ est un corps de rupture pour X^3-2 sur $\mathbb{Q}$
 $\mathbb{Q}(\sqrt[3]{2}, j) \xrightarrow{\quad} \text{décomposition de } X^3-2 \text{ sur } \mathbb{Q}$
 $\cong \mathbb{Q}(\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2})$

$K(\alpha) =$ le corps engendré par α sur $K =$ le plus petit sous-corps de L qui contient K, α .

Proposition. Si $P(X) \in K[X]$ il existe un corps de décomposition de P sur K .
2) deux corps de décomposition de P sur K sont K -isomorphes
démon: 1) récurrence sur $\deg P$
2) admiss

Définition un corps K est algébriquement clos si $\forall P \in K[X]$ non constant, P a une racine dans K .
ex: $\mathbb{C}$, $\overline{\mathbb{Q}} = \{x \in \mathbb{C} : x \text{ algébrique sur } \mathbb{Q}\}$

Proposition (relations racines-coefficients) Soit $P(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_0 \in K[X]$

alors: $\forall 0 \leq k \leq n$, $\frac{a_k}{a_n} = (-1)^{n-k} \sum_{1 \leq i_1 < \dots < i_{n-k} \leq n} \pi_{i_1} \dots \pi_{i_{n-k}}$ $= a_n (X-\pi_1) \dots (X-\pi_n)$

ex: $\frac{a_0}{a_n} = (-1)^n \pi_1 \dots \pi_n$, $\frac{a_{n-1}}{a_n} = -\pi_1 - \dots - \pi_n$.

Exercice: si $P(X) = X^3 + pX + q = (X-\pi_1)(X-\pi_2)(X-\pi_3)$ alors $\Delta = (\pi_1-\pi_2)^2(\pi_2-\pi_3)^2(\pi_1-\pi_3)^2 = -4p^3 - 27q^2$
 $0 = \pi_1 + \pi_2 + \pi_3$ $\uparrow = \pi_1\pi_2 + \pi_2\pi_3 + \pi_1\pi_3$ $q = -\pi_1\pi_2\pi_3$

Corps finis

1) Sous-groupes finis de K^*

Théorème. Soit K corps, Soit $G \leq K^*$ sous-groupe fini
ALORS. G cyclique.

démon a) $K = \mathbb{C}$ Soit $n = |G|$. $\forall g \in G$, $g^n = 1 \Rightarrow g \in \mu_n = \{e^{\frac{2ik\pi}{n}} : 0 \leq k \leq n-1\}$
 $\Rightarrow G \leq \mu_n \Rightarrow G = \mu_n = \langle e^{2i\pi/n} \rangle$
 $|G| = |\mu_n| = n$

b) Cas général $|G| = n$, $G \leq K^*$

$\forall d | n$, $N_d =$ nombre d'éléments de G d'ordre d .

$\sum_{d|n} N_d = n$ ($G = \bigcup_{d|n} \{\text{éléments d'ordre } d\}$)

Or $N_d = 0$ ou $\varphi(d)$. En effet si $N_d > 0$, soit $g \in G$ d'ordre d .
Alors $\forall x \in \langle g \rangle$, $x^d = 1$. Or l'équation $x^d = 1$
a au plus d solutions. Donc $\langle g \rangle = \{x \in G : x^d = 1\}$

Donc $x \in G$ d'ordre $d \Rightarrow x = g^k$ avec $k \wedge d = 1$

$$\Rightarrow Nd = \varphi(d).$$

En particulier, $\forall d \mid n, Nd \leq \varphi(d)$ Mais $\sum_{d \mid n} Nd = n = \sum_{d \mid n} \varphi(d)$
donc $\forall d \mid n, Nd = \varphi(d) \Rightarrow Nm = \varphi(m) > 0$ compter dans $(\mathbb{Z}/n\mathbb{Z}, +)$

ex: $(\mathbb{Z}/17\mathbb{Z})^* = \langle 3 \rangle$

$$3^2 = 9$$

$$3^4 = 81 = -4 \pmod{17}$$

$$3^8 = -1 \pmod{17}$$

$$3^{16} = 1 \pmod{17}$$

b) Caractéristique

Si K corps, le morphisme $\mathbb{Z} \rightarrow K$ est d'anneaux
 $m \mapsto \underbrace{1+1+\dots+1}_{m \text{ fois}}$
de noyau $c\mathbb{Z}$ où $c \geq 0$.

$c = 0$ ou p premier. ($\mathbb{Z}/c\mathbb{Z} \hookrightarrow K$)
injectif $\Rightarrow \mathbb{Z}/c\mathbb{Z}$ intègre

Caractéristique de $K = c$.

ex: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont de caractéristique 0, $\mathbb{Z}/p\mathbb{Z}$ de caractéristique p premier

$\mathbb{Z}[\sqrt{2}]/(3)$ de caractéristique 3

$\mathbb{Z}/p\mathbb{Z}(X)$ de caractéristique p premier

c) Théorème.

1°) Si K corps fini, alors K de cardinal p^n pour un p premier et $n \geq 1$

2°) $\forall p$ premier, $\forall n \geq 1$, il existe un corps de cardinal p^n , unique à isomorphisme près.

dém: 1°) car $(K) = p$ premier. Donc $\mathbb{Z}/p\mathbb{Z} \rightarrow K$ injectif

donc $\mathbb{Z}/p\mathbb{Z} \subset K$ sous-corps

donc K est un $\mathbb{Z}/p\mathbb{Z}$ -espace vectoriel $\Rightarrow (K, +) \cong (\mathbb{Z}/p\mathbb{Z})^n, +)$

$$\Rightarrow |K| = p^n \quad (n = \dim_{\mathbb{Z}/p\mathbb{Z}} K)$$

2°) voir ci-dessous.

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$$

Exc.

$$\mathbb{F}_2[X]/(X^3+X+1) \cong \mathbb{F}_2[X]/(X^3+X^2+1)$$

corps de cardinal 8

Rappel: $\dim_K K[X]/(p) = \deg p$

$$\varphi: \mathbb{F}_2[X] \rightarrow \mathbb{F}_2[X]/(X^3+X^2+1)$$

$$x(X) \mapsto \overline{(X+1)}$$

φ morphisme surjectif de noyau ? $\boxed{(X^3+X+1)}$

$$\varphi(X)^3 + \varphi(X) + \varphi(1) = (X+1)^3 + (X+1) + 1 \pmod{X^3+X^2+1}$$

$$= X^3 + 3X^2 + 3X + 1 + X + 1 + 1 = X^3 + X^2 + 1 = 0 \pmod{X^3+X^2+1}$$

$$\text{1° thm d'iso} \Rightarrow \mathbb{F}_2[X]/(X^3+X+1) \cong \mathbb{F}_2[X]/(X^3+X^2+1)$$

$$\Rightarrow \mathbb{Z}[\sqrt[2]{2}]/(2) \cong \mathbb{Z}[\sqrt[2]{2}]/(2)$$

demo de l'unicité.
Existence admise.

Soit K_0 corps de cardinal p^m p premier, $m \geq 1$
Soit K corps de cardinal p^m

$$K_0^* \text{ cyclique} = \langle \alpha \rangle \Rightarrow K_0 = \mathbb{F}_p[\alpha]$$

Soit $P \in \mathbb{F}_p[X]$ polynôme minimal de α .

P irréductible (ou $\mathbb{F}_p[X]/(P) \cong K_0$)

$$\forall x \in K, x^{p^m} = x \quad (x \neq 0 \Rightarrow x \in K^* \Rightarrow x^{p^m-1} = 1)$$

$$\Rightarrow X^{p^m} - X = \prod_{x \in K} (X - x)$$

$$\text{On a vrai aussi pour } K_0 = \mathbb{F}_p[X]/(P) \Rightarrow X^{p^m} = X \text{ mod } P \Rightarrow P \mid X^{p^m} - X$$

$$\Rightarrow P \text{ scinde sur } K \Rightarrow \exists x \in K, P(x) = 0$$

$$\mathbb{F}_p[X] \longrightarrow K \quad \text{induit un morphisme } \mathbb{F}_p[X]/(P) \xrightarrow{\sim} K$$

$$x \mapsto x$$

$$x + (P) \mapsto x$$

Injectif (morphisme de corps) $\Rightarrow$ isomorphisme (même cardinal)

Existence

Théorème. Soit $\mathbb{F}_q$ corps de cardinal q

$$\text{Alors } X^{q^n} - X = \prod_{d \mid n} \prod_{P \in \text{Id}(q)} P$$

$$\text{où } \text{Id}(q) = \{ \text{irréductibles unitaires } \in \mathbb{F}_q[X] \}$$

Corollaire

$$q^n = \sum_{d \mid n} d |\text{Id}(q)|$$

$$\Rightarrow n |\text{Id}(q)| = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d$$

$$\text{où } \mu(k) = \begin{cases} (-1)^r & \text{si } k = p_1 \dots p_r \text{ } p_i \text{ nombre premier} \\ 0 & \text{sinon} \end{cases} \quad (\text{Möbius})$$

$$\text{Conséquence: } |\text{Id}(q)| = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d \geq \frac{1}{n} \left(q^n - \sum_{\substack{d \mid n \\ d < n}} q^d \right) \geq \frac{1}{n} \left(q^n - \sum_{d < n} q^d \right) > 0$$

$$\Rightarrow |\text{Id}(q)| \neq 0$$

Soit $P \in \text{Id}(q)$ alors $\mathbb{F}_p[X]/(P)$ corps de cardinal p^n .

$$\text{Ex: } |\text{Id}_4(2)| = |\{ \text{irréductibles de degré 4, unitaires sur } \mathbb{F}_2 \}| = \frac{1}{4} (2^4 - 2^2) = \frac{16-4}{4} = 3$$

$$X^4 + X + 1, X^4 + X^3 + 1, X^4 + X^2 + X + 1$$

$$\text{demo de } X^{q^n} - X = \prod_{d \mid n} \prod_{P \in \text{Id}(q)} P$$

$$1) \text{ si } P \in \text{Id}(q) \text{ alors } P \mid X^{q^d} - X \quad (\text{raisonner dans } \mathbb{F}_q[X])$$

$$\text{ou } d \mid n, q^d - 1 \mid q^n - 1 \Rightarrow X^{q^d-1} - 1 \mid X^{q^n-1} - 1 \Rightarrow X^{q^d} - X \mid X^{q^n} - X$$

$$2) (X^{q^n} - X)' = -1 \text{ dans } \mathbb{F}_q[X] \text{ donc les facteurs irréductibles n'apparaissent qu'une fois}$$

$$3) \text{ Soit } P \text{ irréductible } \in \mathbb{F}_q[X] \text{ t.q. } P \mid X^{q^n} - X$$

Soit $d = \deg P$.

$$P \mid (X^{q^d} - X \wedge X^{q^n} - X)$$

$$\text{ou } X^{q^d} - X \wedge X^{q^n} - X = X((X^{q^d-1} - 1) \wedge (X^{q^n-1} - 1))$$

$$\begin{aligned}
 \text{On } q^d - 1 \wedge q^m - 1 &= q^{d \wedge m} - 1 \\
 \Rightarrow X^{q^d - 1} - 1 \wedge X^{q^m - 1} - 1 &= X^{q^d - 1 \wedge q^m - 1} - 1 \\
 &= X^{q^{d \wedge m} - 1} - 1
 \end{aligned}$$

$$\begin{aligned}
 (m = kb + r \text{ avec } 0 \leq r < b) \\
 \Rightarrow q^m - 1 &= \underbrace{q^m - q^r}_{= q^r(q^{kb} - 1)} + q^r - 1 \\
 &= q^r(q^b - 1)(\dots)
 \end{aligned}$$

$$\begin{aligned}
 \text{Donc } P \mid X^{q^{d \wedge m}} - X \\
 \Rightarrow \text{dans le corps } \underbrace{\mathbb{F}_q[X]/(P)}_{\text{cardinal } q^d} : \forall x, x^{q^{d \wedge m}} = x \Rightarrow q^d \leq q^{d \wedge m} \Rightarrow d = d \wedge m \Rightarrow d \mid m \quad \square
 \end{aligned}$$