

1201
123
125
141
144

12, 50''

Gozard
p. 85, 87

Construction des corps finis

Théorème: Soit p première, $n \in \mathbb{N}^*$ et $q := p^n$. On a : ① Il existe un unique corps fini $\mathbb{F}_q$ à q éléments (à $\mathbb{F}_p$ -isomorphisme), c'est le corps de décomposition de $P = X^q - X \in \mathbb{F}_p[X]$.
② Il existe $\pi \in \mathbb{F}_p[X]$ irréductible de degré n tel que $\mathbb{F}_q \cong \mathbb{F}_p[X] / \langle \pi \rangle$.
③ De plus, $\pi \mid P$ dans $\mathbb{F}_p[X]$ et π scinde sur $\mathbb{F}_q[X]$.

$\mathbb{F}_p \subset \mathbb{F}_p$ ①

Lagrange

$$K = \sqrt[p]{P} = \sqrt[p]{X^q - X}$$

K

$$K \subset K$$

$$\mathbb{F}_p \subset K$$

$$P \mid P' = 1$$

$$|K| = q = |\sqrt[p]{P}|$$

$$\langle \xi \rangle = \mathbb{F}_q^* \quad ②$$

$$\mathbb{F}_p(\xi) = \mathbb{F}_q$$

$$\mathbb{F}_p(\theta) \quad ③$$

$$\theta \neq 0$$

$$P(\theta) = 0, \pi \nmid P$$

Soit K un corps à q éléments. On a $\text{car } K = p$ et le sous corps premier de K est $\mathbb{F}_p$. Par Lagrange, $\forall x \in K^*$ on a $x^{q-1} = 1$ donc $\forall x \in K$ $x^q = x$. Or, $P = X^q - X \in \mathbb{F}_p[X]$ de degré q a au plus q racines distinctes sur K . Puisque tout élément de K est racine de P , on en déduit que K est un corps de décomposition de P sur $\mathbb{F}_p[X]$.

Réciproquement, soit K un corps de décomposition de P sur $\mathbb{F}_p[X]$ et $K := \{x \in K \mid x^q = x\}$. Puisque $F^n: K \rightarrow K$ est un morphisme de corps, $K := \{x \in K \mid F^n(x) = x\}$ est un sous corps de K . Donc K contient $\mathbb{F}_p$, sous corps premier de K . On a $P' = qX^{q-1} - 1 = -1$ dans $\mathbb{F}_p[X]$, et $P \mid P' = 1$ dans $\mathbb{F}_p[X]$. Donc P est séparable et scinde à racines simples sur K . Alors $|K| = q$, et K est un corps de décomposition de P sur $\mathbb{F}_p[X]$. Puisque les corps de décomposition de P sur $\mathbb{F}_p[X]$ sont $\mathbb{F}_p$ -isomorphes, $\mathbb{F}_q$ est unique.

Comme $\mathbb{F}_q^*$ est cyclique, $\exists \xi \in \mathbb{F}_q^*$ générateur. On a $\mathbb{F}_p(\xi) = \mathbb{F}_q$ (car $\mathbb{F}_p(\xi) \subset \mathbb{F}_q(\xi) = \mathbb{F}_q$ et $\mathbb{F}_q = \{0\} \cup \langle \xi \rangle \subset \mathbb{F}_p(\xi)$). Puisque $\mathbb{F}_p$ est le sous corps premier de $\mathbb{F}_q$, et $|\mathbb{F}_q| = |\mathbb{F}_p|^n$, on a $[\mathbb{F}_q : \mathbb{F}_p] = [\mathbb{F}_p(\xi) : \mathbb{F}_p] = n$. Donc le polynôme π minimal de ξ sur $\mathbb{F}_p$ est de degré n , et $\mathbb{F}_q = \mathbb{F}_p(\xi) \cong \mathbb{F}_p[X] / \langle \pi \rangle$.

Puisque $\deg \pi \geq 2$, on a $\pi \nmid X$. Soit $\mathbb{L} = \mathbb{F}_p(\theta)$ un corps de rupture de π sur $\mathbb{F}_p[X]$ où $\theta \neq 0$ dans $\mathbb{F}_p(\theta) \cong \mathbb{F}_p[X] / \langle \pi \rangle \cong \mathbb{F}_q$. Par Lagrange, $\theta^{q-1} = 1$ et $\theta^q = \theta$, donc $P = X^q - X$ annule θ . Alors $\pi \mid P$ dans un corps de décomposition de π , donc dans $\mathbb{F}_q[X]$. Puisque P scinde sur $\mathbb{F}_q[X]$, π l'est également.

Revision

- ① Unicité : Lagrange $\rightarrow K = (\mathbb{F}_p)[X] \rightarrow K = \text{Cap } D(P, \mathbb{F}_p)$
Existence : $K \subset \mathbb{F}_p[X] \rightarrow K = \{x^q : x \in \mathbb{F}_p\} \rightarrow P \mid P^q = 1 \Rightarrow |K| = q$
- ② $\mathbb{F}_q$ cyclique, $\mathbb{F}_q(\xi) = \mathbb{F}_p \rightarrow \pi$ poly min de ξ
- ③ $\forall \theta \in \mathbb{F}_p^* \text{ Capr}, \theta \neq 0$ Lagrange $\rightarrow \pi \mid P, P$ sc sur $\mathbb{F}_q$.

Lemme : Si $K/\mathbb{F}_p$, alors $\mathcal{F}: x \in K \mapsto x^p \in K$ morphisme de corps

On a $\mathcal{F}(1) = 1, \forall x, y \in K \mathcal{F}(xy) = x^p y^p = \mathcal{F}(x) \mathcal{F}(y)$ et par Newton

$$\mathcal{F}(x+y) = (x+y)^p = \sum_{k=0}^p \binom{p}{k} x^k y^{p-k} = (-1)^p x^p + y^p = \mathcal{F}(x) + \mathcal{F}(y)$$

car $\forall k \in [1, p-1] \binom{p}{k} = p \binom{p-1}{k-1}$, par Gauss $p \mid \binom{p}{k}$ d'où $\binom{p}{k} = 0 \text{ sur } \mathbb{F}_p$; et $(-1)^p = 1$ ($p=2, 1=-1$)

Lemme : K corps, $G \subset K^*$ fini, alors G cyclique

Soit $|G| = n = \sum_{d \mid n} \varphi(d)$. Soit $x \in G$, $\text{ord}(x) = d \mid n$. On a $|K(x)| = d$ et $\forall y \in \langle x \rangle y^d = 1$ donc $\langle x \rangle = \sqrt[d]{X^d - 1} \subset K$ (au plus d racines sur K) ou $\langle x \rangle \simeq \mathbb{Z}/d\mathbb{Z}$.

Puisque $H_d = \{y \in G \mid \text{ord}(y) = d\} \subset \langle x \rangle$ et $y \in H_d \Leftrightarrow y \in K^*, \langle y \rangle = \langle x \rangle$, on a

$N_d = |H_d| = |\text{générateurs de } \langle x \rangle| = |\text{générateurs de } \mathbb{Z}/d\mathbb{Z}| = \varphi(d)$. Donc $\forall d \mid n$,

$N_d = 0$ ou $N_d = \varphi(d)$. Puisque $G = \bigcup_{d \mid n} H_d$ (Lagrange), $n = \sum_{d \mid n} N_d = \sum_{d \mid n} \varphi(d)$, on en déduit

$\forall d \mid n, N_d = \varphi(d)$. En particulier $N_n = \varphi(n) > 0$ donc $\exists y \in G, \langle y \rangle = G$.

Application : $\prod_{\lambda \in \mathbb{F}_q^*} \lambda = -1$ et $(p \in \text{Pr}(N) \Leftrightarrow (p-1)! \equiv -1 \pmod{p})$

* On a $\mathbb{F}_q = \{\lambda_0, \lambda_1, \dots, \lambda_{q-1}\}$, $X^q - X = \prod_{i=0}^{q-1} (X - \lambda_i)$ sur $\mathbb{F}_p$. Donc $X^{q-1} - 1 = \prod_{i=1}^{q-1} (X - \lambda_i)$
et en $X = 0, -1 = \prod_{i=1}^{q-1} -\lambda_i = (-1)^{q-1} \prod_{i=1}^{q-1} \lambda_i = \prod_{\lambda \in \mathbb{F}_q^*} \lambda$ car $(-1)^{q-1} = 1$ ($p=2, q-1 \in 2\mathbb{N}, p=2, -1=1$)

* $\Leftrightarrow p \in \text{Pr}(N) \Rightarrow \prod_{k=1}^{p-1} k = -1$ ie $(p-1)! \equiv -1 \pmod{p}$.

$\Leftarrow$ Soit $\bar{x} \in (\mathbb{Z}/p\mathbb{Z})^*, x \in [1, p-1]$. Puisque $(p-1)! \equiv -1 \pmod{p}$, $\bar{x} \mid \left(\prod_{i=1}^{p-1} i \right) = -1$ et $\bar{x} \in \mathbb{Z}/p\mathbb{Z}$

Exemple : $\mathbb{F}_4, \mathbb{F}_8$ et $\mathbb{F}_9$:

$$\mathbb{F}_4 \simeq \mathbb{F}_2[X] / \langle X^2 + X + 1 \rangle; \mathbb{F}_8 \simeq \mathbb{F}_2[X] / \langle X^3 + X + 1 \rangle; \mathbb{F}_9 \simeq \mathbb{F}_3[X] / \langle X^2 + X + 2 \rangle.$$

Lemme : $\pi, P \in K[X], L/K$ et $\pi \mid P$ dans $L[X]$. Alors $\pi \mid P$ dans $K[X]$

Dans $K[X]$ Ann $E, P = \pi Q + R$ avec $Q, R \in K[X]$ $\deg R < \deg \pi$ ou $R = 0$

Vraie dans $L[X]$ et $\exists S \in L[X] P = \pi S = \pi Q + R \downarrow R = \pi(S - Q)$.

Donc $\deg R = \deg \pi + \deg(S - Q) \geq \deg \pi$ si $S - Q \neq 0$, alors $R = 0$ dans tous les cas.

D'où $P = \pi Q$ et $\pi \mid P$ dans $K[X]$.