Existence et unicité des corps finis

Mohamed NASSIRI

Références :

Théorie de Galois, Ivan Gozard - p.85,87

Recasage :

• • • • • 123 : Corps finis. Applications.
• • • • • 141 : Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.
• • • • ○ 125 : Extensions de corps. Exemples et applications.

Résumé :

Ce développement est un incontournable sur les corps finis. En réalité, ce sont les corps de décomposition qui vont faire tout le travail.

Prérequis :

Extensions de corps - Corps de rupture et de décomposition - Irréductibilité des polynômes

---

Théorème : Soit p un nombre premier et $n \in \mathbb{N}^*$. On note $q = p^n$.
(1) Il existe un unique corps fini à q éléments. Il est le corps de décomposition sur $\mathbb{F}_p$ de $X^q - X$. On le note $\mathbb{F}_q$
(2) $\mathbb{F}_q = \mathbb{F}_p[\mathrm{X}]/(\pi)$, où π est un polynôme irréductible quelconque de degré n sur $\mathbb{F}_p$.
(3) Si π est un polynôme irréductible de degré n sur $\mathbb{F}_p$, alors $\pi(x) \mid X^q - X$ dans $\mathbb{F}_p[\mathrm{X}]$, donc est scindé sur $\mathbb{F}_q$.

Démonstration.
(1)
• Soit K un corps à q éléments. Comme $\mathrm{car}(K) = p$, $\mathbb{F}_p$ est le sous-corps premier de K.
$(K^*, +)$ est un groupe à $q-1$ éléments, donc par le théorème de Lagrange,

$$\forall x \in K^*,\ x^{q-1} = 1 \ \ (i.e.)\ \ \forall x \in K,\ x^q = x$$

or le polynôme $X^q - X \in \mathbb{F}_p[\mathrm{X}]$, de degré q, admet au plus q racines distinctes dans K. Comme tout élément de K est racine de ce polynôme, on a bien $K = \mathrm{dec}_{\mathbb{F}_p}(X^q - X)$ et on a donc l'unicité (par unicité des corps de décomposition).

• Réciproquement, soit $K = \mathrm{dec}_{\mathbb{F}_p}(X^q - X)$ et $k = \{x \in K \mid x^q = x\}$. k est un sous-corps de K.

Remarquer que $\mathcal{F} : x \mapsto x^q$ n'est autre que l'automorphisme de Frobenius itéré plusieurs fois, et ainsi k est l'ensemble des points fixes de $\mathcal{F}$. On note ce dernier ensemble $Inv(\mathcal{F})$.
Lemme : $Inv(\mathcal{F}) = \{x \in K \mid x^q = x\}$ est un sous-corps de K.
Démonstration
- $0, 1 \in Inv(\mathcal{F})$, c'est clair.
- Soit $(a, b) \in (Inv(\mathcal{F}))^2$, $\mathcal{F}(a + b) = \mathcal{F}(a) + \mathcal{F}(b) = a + b$, donc $a + b \in Inv(\mathcal{F})$
- Soit $(a, b) \in (Inv(\mathcal{F}))^2$, $\mathcal{F}(ab) = \mathcal{F}(a)\mathcal{F}(b) = ab$, donc $ab \in Inv(\mathcal{F})$
- Soit $x \in Inv(\mathcal{F})$, avec $x \neq 0$, $\mathcal{F}(x^{-1}) = (\mathcal{F}(x))^{-1} = x^{-1}$, donc $x^{-1} \in Inv(\mathcal{F})$

On reprend ! Comme k est un sous-corps de K, k contient $\mathbb{F}_p$.
De plus, $(X^q - X)' = qX^{q-1} - 1 \underbrace{=}_{car(k)=p} -1$ qui est premier avec $X^q - X$ donc les racines de $X^q - X$ sont simples. Ainsi $|k| = q$, k est un corps à q éléments, et donc $k = K = \text{dec}_{\mathbb{F}_p}(X^q - X)$.

(2)
• $\mathbb{F}_p/(\pi)$ est une extension algébrique simple (corps de rupture de π sur $\mathbb{F}_p$) donc un corps de cardinal p^n et ainsi $\mathbb{F}_p[\text{X}]/(\pi) = \mathbb{F}_q$.
• $\mathbb{F}_q$ peut toujours être construit ainsi : si ξ est un générateur du groupe (multiplicatif) cyclique $\mathbb{F}_q^*$, alors $\mathbb{F}_q = \mathbb{F}_p[\xi] = \mathbb{F}_p(\xi)$.
Soit $\pi(X) = \text{Irr}(\xi, \mathbb{F}_p, X)$ (c'est une notation pour dire qu'il s'agit du polynôme minimal de ξ sur $\mathbb{F}_p$). Comme $\mathbb{F}_p[\text{X}]/(\pi) \simeq \mathbb{F}_p(\xi)$, il vient $\deg(\pi) = [\mathbb{F}_p(\xi) : \mathbb{F}_p] = n$.
Par le théorème de Lagrange, $\xi^{q-1} = 1$, donc $\pi(x) \mid X^{q-1} - X$ dans $\mathbb{F}_p[\text{X}]$.

(3)
Soit π un polynôme irréductible de degré n sur $\mathbb{F}_p$.
Si $\pi(X) \neq X$ (ce qui est automatique dès que $n \geq 2$), on considère θ une racine de $\pi(X)$ dans $\text{dec}_{\mathbb{F}_p}(\pi(X))$.
$\theta \neq 0$ dans le corps $= \mathbb{F}_p(\theta) \simeq \mathbb{F}_p[\text{X}]/(\pi) \simeq \mathbb{F}_{p^n}$.
Par le théorème de Lagrange, $\theta^{q-1} = 1$, donc $\pi(x) \mid X^{q-1} - 1$ dans $\mathbb{F}_p[\text{X}]$, et donc $\pi(x) \mid X^q - X$ dans $\mathbb{F}_p[\text{X}]$ dans $\mathbb{F}_p[\text{X}]$ (c'est même valable pour $\pi(X) = X$), or ce dernier est scindé sur $\mathbb{F}_q$ donc $\pi(X)$ l'est aussi. □

Remarques :

- On a des exemples de corps finis "simples" :
  - L'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps dès que p est premier.
  - Tout anneau intègre ayant un nombre fini $n \geq 2$ d'éléments est un corps.

- L'assertion (2) se traduit également par le fait qu'il existe des polynômes irréductibles de tout degré dans $\mathbb{F}_p[\text{X}]$.

- L'assertion (3) se traduit par le fait que, dans les corps finis, le corps de rupture est égal au corps de décomposition. Ce qui est quelque chose d'assez remarquable ! En général, c'est totalement faux, et pas besoin de prendre un exemple très sophistiqué pour le voir ... :
  Exemple (classique) : $P(X) = X^3 - 2$ dans $\mathbb{Q}[\text{X}]$.
  Un des corps de rupture est $\mathbb{Q}(\sqrt[3]{2})$ mais il n'est pas corps de décomposition car il ne contient pas les racines complexes $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$ ...2

- On a écrit à un moment de la démonstration :
  " $\mathbb{F}_q$ peut toujours être construit ainsi : si ξ est un générateur du groupe (multiplicatif) cyclique $\mathbb{F}_q^*$, alors $\mathbb{F}_q = \mathbb{F}_p[\xi] = \mathbb{F}_p(\xi)$."
  Il faut savoir que, justement, on ne sait pas, en général, déterminer explicitement un générateur du groupe multiplicatif d'un corps fini ...

- Mises en garde sur le développement :
  Attention à ...