Existence, unicité et construction des corps finis

Riffaut Antonin

2013-2014

Existence et unicité des corps finis Soit k un corps. Le noyau du morphisme d'anneaux $\varphi : n \in \mathbb{Z} \longmapsto n.1_k \in k$ est un idéal de $\mathbb{Z}$, donc de la forme $n\mathbb{Z}$, avec $n \in \mathbb{Z}$. Comme $\mathbb{Z}/n\mathbb{Z} \simeq \operatorname{Im}\varphi$ est intègre, alors $n = 0$ ou n est un nombre premier. Si $n = 0$, φ est injectif, et le sous-corps premier de k est isomorphe à $\mathbb{Q}$. Sinon, le sous-corps premier isomorphe à $\mathbb{Z}/n\mathbb{Z}$. n s'appelle la *caractéristique* de k.

Désormais, k désigne un corps fini de caractéristique p, avec p un nombre premier.

Proposition 1. (i) *Le cardinal de k est une puissance de p.*

(ii) *Réciproquement, pour tout $n \in \mathbb{N}^*$, il existe un corps k de cardinal p^n. De plus, k est unique à isomorphisme près.*

Démonstration. (i) Le sous-corps premier de k étant isomorphe à $\mathbb{Z}/p\mathbb{Z}$, k possède une structure naturelle de $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel. En notant $n = [k : \mathbb{Z}/p\mathbb{Z}]$, alors $|k| = |\mathbb{Z}/p\mathbb{Z}|^n = p^n$.

(ii) Soit $n \in \mathbb{N}^*$. Si k est un corps fini de cardinal p^n, alors k est le corps de décomposition de $X^{p^n} - X$ sur $\mathbb{Z}/p\mathbb{Z}$: en effet, pour tout $x \in k$, x est racine de $X^{p^n} - X$, donc $X^{p^n} - X$ possède ses p^n racines dans k.

Réciproquement, soit K le corps de décomposition de $X^{p^n} - X$ sur $\mathbb{Z}/p\mathbb{Z}$. Soit k l'ensemble des éléments de K qui sont racines de $X^{p^n} - X$. Vérifions que k est un sous-corps de K : d'une part, $1_K \in k$; d'autre part, si $x, y \in k$, alors $x^{p^n} = x$ et $y^{p^n} = y$, donc $(x + y)^{p^n} = x^{p^n} + y^{p^n} = x + y$ et $(xy^{-1})^{p^n} = xy^{-1}$, si bien que $x + y, xy^{-1} \in k$. Par ailleurs, $(X^{p^n} - X)' = -1$ est premier avec $X^{p^n} - X$, donc les racines de $X^{p^n} - X$ sont simples, de sorte que $|k| = p^n$: par conséquent, $k = K$ est un corps à p^n éléments, et il est unique à isomorphisme près, par unicité du corps de décomposition de $X^{p^n} - X$ sur $\mathbb{Z}/p\mathbb{Z}$. ■

On notera $\mathbb{F}_q$ le corps fini à $q = p^n$ éléments.

Construction des corps finis Soit $P \in \mathbb{F}_p[X]$ un polynôme irréductible sur $\mathbb{F}_p$. En notant $n = \deg(P)$, alors $\mathbb{F}_p[X]/(P)$ est le corps de rupture de P sur $\mathbb{F}_p$, de cardinal p^n. Nous allons démontrer que pour tout $n \in \mathbb{N}^*$, il existe un polynôme irréductible sur $\mathbb{F}_p$ de degré n.

Proposition 2. *Pour tout $n \in \mathbb{N}^*$, posons $I(n, p)$ l'ensemble des polynômes de $\mathbb{F}_p[X]$ unitaires, irréductibles, de degré n. Alors pour tout $n \in \mathbb{N}^*$, dans $\mathbb{F}_p[X]$,*

$$X^{p^n} - X = \prod_{d|n} \prod_{P \in I(d,p)} P. \tag{1}$$

Démonstration. • Soit P un facteur irréductible de $X^{p^n} - X$ sur $\mathbb{F}_p$, de degré d. Le corps de rupture de P sur $\mathbb{F}_p$ est un sous-corps de cardinal p^d du corps de décomposition de $X^{p^n} - X$ sur $\mathbb{F}_p$, c'est-à-dire $\mathbb{F}_{p^n}$, donc $d|n$.

- Réciproquement, soient $d|n$, et $P \in I(d,p)$. Soit α une racine de P dans le corps de rupture de P sur $\mathbb{F}_p$; alors $\mathbb{F}_p(\alpha) \simeq \mathbb{F}_{p^d}$. On en déduit que α est racine de $X^{p^n} - X$. Or comme P est irréductible, alors P est le polynôme minimal de α sur $\mathbb{F}_p$, donc $P|X^{p^n} - X$.
  Pour conclure, il suffit de remarquer que les facteurs irréductibles de $X^{p^n} - X$ sur $\mathbb{F}_p$ sont simples (par le même argument que précédemment), d'où la formule annoncée. ■

Corollaire 3. *Pour tout $n \in \mathbb{N}^*$, il existe un polynôme irréductible sur $\mathbb{F}_p$ de degré n.*

Démonstration. Il s'agit de montrer que $\operatorname{card} I(n,p) > 0$. Pour ce faire, en passant au degré dans la formule (1), on obtient

$$p^n = \sum_{d|n} d \operatorname{card} I(d,p).$$

Il s'ensuit que pour tout $d \in \mathbb{N}^*$, $p^d \geq d \operatorname{card} I(d,p)$, puis que

$$\begin{aligned} n \operatorname{card} I(n,p) &= p^n - \sum_{d|n,\, d\neq n} d \operatorname{card} I(d,p) \\ &\geq p^n - \sum_{d|n,\, d\neq n} p^d \\ &\geq p^n - \sum_{d=1}^{n-1} p^d \\ &\geq p^n - p\frac{p^{n-1}-1}{p-1} > 0. \end{aligned}$$

■

Références

[Per] Daniel Perrin, *Cours d'algèbre*, Ellipses.