Existence, unicité et construction des corps finis

Pierron Théo

28 juin 2014

Théorème 1 *Si K est un corps fini alors son cardinal est une puissance d'un nombre premier.*

Démonstration. Soit K un corps fini. On pose

$$\varphi : \begin{cases} \mathbb{Z} & \to & K \\ n & \mapsto & n1_K \end{cases}$$

C'est un morphisme d'anneaux non injectif car K est fini. Son noyau est donc un idéal de $\mathbb{Z}$ non nul qui s'écrit donc $p\mathbb{Z}$ avec $p > 0$.

Alors $\mathbb{Z}/p\mathbb{Z} \simeq \mathrm{Im}(\varphi)$ est un sous-anneau de K qui est donc intègre. Ainsi p est premier et $\mathbb{Z}/p\mathbb{Z}$ est un corps noté $\mathbb{F}_p$.

K est naturellement muni d'une structure de $\mathbb{F}_p$-ev de dimension d (finie car K l'est). On a finalement l'isomorphisme d'ev $K \simeq (\mathbb{F}_p)^d$ donc $|K| = p^d$. ∎

Théorème 2 *Si p est premier et $d > 0$, il existe un corps de cardinal p^d. De plus, il est unique à isomorphisme près.*

Démonstration. Soient p, d comme dans l'énoncé. On pose $P = X^{p^d} - X$ et L le corps de décomposition de P sur $\mathbb{F}_p$. Posons

$$K = \{x \in L, x^{p^d} = x\}$$

Montrons que K est un corps. On a $1 \in K$. De plus, en utilisant le Frobénius, on a

$$(x+y)^{p^d} = (x^p + y^p)^{p^{d-1}} = \ldots = x^{p^d} + y^{p^d} = x + y$$

et

$$(xy)^{p^d} = x^{p^d} y^{p^d} = xy$$

Ainsi K est un sous-corps de L. Comme K est l'ensemble des racines de P et $\deg(P) = p^d$, on a $|K| \leqslant p^d$.

Or P est scindé à racines simples sur L, donc on a au moins p^d éléments dans K. Finalement, $|K| = p^d$ est un corps de décomposition de P sur $\mathbb{F}_p$. Par unicité des corps de décomposition, on a $K = L$. En particulier, on a l'unicité des corps finis. ∎

On note alors $\mathbb{F}_q$ le corps fini à q éléments.

Soit $P \in \mathbb{F}_p[X]$ irréductible sur $\mathbb{F}_p$. Alors $\mathbb{F}_p[X]/P$ est le corps de rupture de P sur $\mathbb{F}_p$. Son cardinal est $p^{\deg P}$, il est donc isomorphe à $\mathbb{F}_{p^{\deg P}}$. Montrons alors que pour tout n, il existe un polynôme irréductible de degré n irréductible sur $\mathbb{F}_p$.

Théorème 3 *Notons $I(n,p)$ l'ensemble des polynômes de $\mathbb{F}_p[X]$ de degré n irréductibles sur $\mathbb{F}_p$. Alors on a la formule*

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

Démonstration.

- Soit $P|X^{p^n}-X$ irréductible. Montrons que $\deg P|n$. Soit K le corps de rupture de P sur $\mathbb{F}_p$.
  Alors K est un corps fini de cardinal $p^{\deg P}$. K est un sous-corps du corps de décomposition de P sur $\mathbb{F}_p$, à savoir $\mathbb{F}_{p^n}$. Ainsi, $\mathbb{F}_{p^n}$ est un ev sur $\mathbb{F}_{p^{\deg P}}$. Il existe donc d tel que $(p^{\deg P})^d = p^n$ donc $(\deg P)d = n$.
- Soit $d|n$ et $P \in I(d,p)$. Montrons que $P|X^{p^n}-X$. Notons $n=dk$.
  Soit α la classe de X dans le corps de rupture $\mathbb{F}_p[X]/P \simeq \mathbb{F}_{p^d}$. On a

$$\alpha^{p^n} = \alpha^{p^{kd}} = (\alpha^{p^d})^{p^{d(k-1)}} = \alpha^{p^{d(k-1)}} = \ldots = \alpha$$

  Donc $X^{p^n}-X$ annule α. P est le polynôme minimal de α donc $P|X^{p^n}-X$.
- $X^{p^n}-X$ est premier avec $-1 = (X^{p^n}-X)'$ donc ses facteurs irréductibles sont simples. On a donc le résultat. ∎

THÉORÈME 4 *Pour tout n, $|I(n,p)| \geqslant 1$.*

Démonstration. En passant au degré dans la formule précédente, on a

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

En particulier, pour tout n, $n|I(n,p)| \leqslant p^n$. On a ensuite

$$n|I(n,p)| = p^n - \sum_{\substack{d|n \\ d\neq n}} d|I(d,n)| \geqslant p^n - \sum_{\substack{d|n \\ d\neq n}} p^d \geqslant p^n - \sum_{d=1}^{n-1} p^d = p^n - \frac{p^n-p}{p-1} > 0$$

D'où $|I(n,p)| \geqslant 1$. ∎