Construction des corps finis

Théorème
Il existe un corps à $q = p^n$ éléments. C'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$. Il est unique à $\mathbb{F}_p$-isomorphisme près. On le note $\mathbb{F}_q$.

DÉMONSTRATION

- On note L le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p[X]$.
  On note $K = \{x \in L \ / \ x^q - x = 0\}$.

  K est non vide car $1 \in K$.

  Soient $x, y \in K$.
  Si $y \neq 0$ alors $(xy^{-1})^q = x^q(y^q)^{-1} = xy^{-1} \in K$.

  De plus $(-x)^q = \begin{cases} x^q = x = -x & \text{si } p = 2 \\ -x^q = -x & \text{si } p > 2 \end{cases}$ d'où $-x \in K$

  Enfin

  $$\begin{aligned}(x+y)^q &= ((x+y)^p)^{p^{n-1}} = (x^p + y^p)^{p^{n-1}} \text{ par morphisme de Frobenius sur } L \\ &= \dots \\ &= x^{p^n} + y^{p^n} = x + y \in K.\end{aligned}$$

  Comme K a la même structure de corps que L et $K \subset L$, K est un sous-corps de L.

  K a alors le même sous-corps premier que L, c'est-à-dire $\mathbb{F}_p$. Or K contient toutes les racines de $X^q - X$.
  Par minimalité du corps de décomposition, $K = L$.

  On remarque que $(X^q - X)' = qX^{q-1} - 1 = -1$ est premier avec $X^q - X$ qui est donc à racines simples. Donc $L = K$ est de cardinal q.

- Soit L' un autre corps de cardinal q.
  Alors L' est de caractéristique p, c'est-à-dire que le sous-corps premier de L' est $\mathbb{F}_p$.
  Comme L'^* est un groupe multiplicatif à $q-1$ éléments,

  $$\forall x \in L'^*,\ x^{q-1} = 1.$$

  Donc

  $$\forall x \in L,\ x^q = x.$$

  Les éléments de L' (au nombre de q) sont tous des racines de $X^q - X$ dont toutes les racines sont donc dans L'.
  Comme L' contient $\mathbb{F}_p$ et toutes les racines de $X^q - X$, c'est un corps de décomposition de $X^q - X$.
  On conclut par unicité à $\mathbb{F}_p$-isomorphisme près du corps de décomposition. $\square$

Corollaire — *Soit $\pi \in \mathbb{F}_p[X]$ irréductible de degré n. Alors*

$$\mathbb{F}_p[X]/(\pi) \simeq \mathbb{F}_q.$$

De plus, il existe toujours un tel polynôme irréductible π.

DÉMONSTRATION

- $\mathbb{F}_p[X]/(\pi)$ est le corps de rupture de π (polynôme de degré n). D'où $\mathbb{F}_p[X]/(\pi)$ est un corps de degré $p^n = q$. On conclut par unicité.

- Il existe un générateur ξ de $\mathbb{F}_q^*$ car celui-ci est cyclique. On note π le polynôme minimal de ξ dans $\mathbb{F}_p[X]$. Comme $\mathbb{F}_p[X]/(\pi) \simeq \mathbb{F}_p(\xi)$,

  $$\mathbb{F}_p[X]/(\pi) \simeq \mathbb{F}_q.$$

  Ainsi $\text{Card}\,(\mathbb{F}_q) = \text{Card}\,(\mathbb{F}_p)^{\deg \pi}$ soit $\deg \pi = n$. $\square$

Corollaire — *Si $\pi \in \mathbb{F}_p[X]$ de degré n est irréductible, alors $\pi \mid X^q - X$ dans $\mathbb{F}_p[X]$, donc π est scindé dans $\mathbb{F}_q[X]$, donc son corps de rupture est son corps de décomposition.*

DÉMONSTRATION
On note K le corps de décomposition de π sur $\mathbb{F}_p$.
Soit $\xi \in K$ une racine de π. Alors $\mathbb{F}_p(\xi) \simeq \mathbb{F}_p[X]/(\pi) \simeq \mathbb{F}_q$. En particulier, comme tous les éléments de $\mathbb{F}_q$ sont des racines de $X^q - X$, ξ est aussi une racine de $X^q - X$.
Comme π est irréductible, à multiplication par un élément non nul de $\mathbb{F}_p$ près, c'est le polynpome minimal de ξ sur $\mathbb{F}_p[X]$.
Donc $\pi \mid X^q - X$.
On en déduit que π est scindé sur $\mathbb{F}_q[X]$.

On a montré précédemment que toutes les racines de π dans K sont dans $\mathbb{F}_q$ car racines de $X^q - X$. Or $\mathbb{F}_p \subset \mathbb{F}_q$.
Donc $K \subset \mathbb{F}_q$.

Or le corps de rupture $\mathbb{F}_p(\xi) \simeq \mathbb{F}_q$ est inclus dans le corps de décomposition K.
On conclut à l'égalité des corps de rupture et de décomposition. $\square$