Références :
Théorie de Galois, Ivan Gozard

Théo. *Soit p premier et $n \in \mathbb{N}^*$. On note $q = p^n$. Il existe un unique corps à q éléments à isomorphisme près. On le note $\mathbb{F}_q$.*

Démonstration. Posons $P = X^q - X \in \mathbb{Z}/p\mathbb{Z}[X]$. Soit $\mathbb{K}$ le corps de décomposition de P sur $\mathbb{Z}/p\mathbb{Z}$. Posons

$$\mathbb{L} = \{x \in \mathbb{K}, P(x) = 0\} = \{x \in \mathbb{K}, x^q = x\} \subset \mathbb{K}.$$

- Montrons que $\mathbb{L}$ est un sous-corps de $\mathbb{K}$.
  - ▶ $1 \in \mathbb{L}$ donc $\mathbb{L}$ non vide.
  - ▶ Si $x, y \in \mathbb{L}$ avec $y \neq 0$, alors
  $$(xy^{-1})^q = x^q(y^{-1})^q = x(y^q)^{-1} = xy^{-1}.$$
  On a donc $xy^{-1} \in \mathbb{L}$.
  - ▶ Si $x \in \mathbb{L}$
    - ▷ Si $p = 2$ et $q = 2^n$, alors
    $$(-x)^{2^n} = x^{2^n} = x = -x \text{ car } \mathrm{Car}(\mathbb{K}) = 2$$
    - ▷ Sinon
    $$(-x)^q = -x^q = -x$$
  - ▶ Si $x, y \in \mathbb{L}$, alors
  $$\begin{aligned}(x+y)^q &= ((x+y)^p)^{p^{n-1}} \\ &= (x^p + y^p)^{p^{n-1}} \\ &= (x+y)^{p^{n-1}} \\ &= \vdots \\ &= x + y\end{aligned}$$
- Montrons que $|\mathbb{L}| = q$ et que $\mathbb{L} = \mathbb{K}$.
  On a que $P' = qX^{q-1} - 1 = -1$ car $p|q$.
  Ainsi, on a $P \wedge P' = 1$ et donc les racines sont simples.
  Or $\deg(P) = q$ donc $|\mathbb{L}| = q$.
  On sait que $\mathrm{Car}(\mathbb{K}) = p$ donc par définition du sous-corps premier $\mathbb{Z}/p\mathbb{Z} \subset \mathbb{L}$. Ainsi, $\mathbb{L}$ est un sous corps de $\mathbb{K}$ contenant les racines de P et $\mathbb{Z}/p\mathbb{Z}$. Ainsi, par définition du corps de décomposition, $\mathbb{L} = \mathbb{K}$.
- Montrons maintenant l'unicité.
  Soit $\mathbb{L}'$ un corps de cardinal q.
  On sait que $\mathrm{Car}(\mathbb{L}') = p$, on a donc $\mathbb{Z}/p\mathbb{Z} \subset \mathbb{L}'$. De plus, $|\mathbb{L}'^*| = q - 1$ donc pour tout $x \in \mathbb{L}'^*$, $x^{q-1} = 1$ ie $x^q = x$. Ainsi, les éléments de $\mathbb{L}'$ sont des racines de $P \in \mathbb{Z}/p\mathbb{Z}[X]$. Par unicité du corps de décomposition, $\mathbb{L}' = \mathbb{K}$.

□

Théo. *Soit p premier et $n \in \mathbb{N}^*$. On note $q = p^n$. Alors $\mathbb{F}_q$ est isomorphe à $\mathbb{F}_p[X]/(\pi)$ où π est un polynôme irréductible quelconque de degré n sur $\mathbb{F}_p$.*

Démonstration. On note $\mathcal{H} = \{P \in \mathbb{F}_p[X],\ P \text{ irréductible de degré } n\}$.

- Montrons qu'il existe $\pi \in \mathcal{H}$ tel que $\mathbb{F}_q = \mathbb{F}_p[X]/(\pi)$.
  On sait que $\mathbb{F}_q^*$ est cyclique.
  Soit ξ un générateur de $\mathbb{F}_q^*$. On a donc que $\mathbb{F}_q = \{0, 1, \xi, ..., \xi^{q-2}\}$.
  On a $\mathbb{F}_q \subset \mathbb{F}_p[\xi] = \{P(\xi), P \in \mathbb{F}_p[X]\}$ et on a $\xi \in \mathbb{F}_q$ donc, pour tout $P \in \mathbb{F}_p[X], P(\xi) \in \mathbb{F}_q$ (car $\mathbb{F}_p \subset \mathbb{F}_q$ et $\mathbb{F}_q$ est un anneau).
  Ainsi, $\mathbb{F}_q = \mathbb{F}_p[\xi] = \mathbb{F}(\xi)$ car ξ est algébrique sur $\mathbb{F}_p$).
  Soit Π le polynôme minimal de ξ. On a donc que $\mathbb{F}_p(\xi)$ est le corps de rupture de Π sur $\mathbb{F}_p$.
  Par unicité des corps de rupture, $\mathbb{F}_q = \mathbb{F}_p(\xi) \simeq \mathbb{F}_p[X]/(\pi)$.
  Or, on a $\deg(\pi) = [\mathbb{F}_q : \mathbb{F}_p] = n$.
- Montrons que, pour tout $P \in \mathcal{H}$, $\mathbb{F}_q \simeq \mathbb{F}_p[X]/(\pi)$.
  Soit π un polynôme irréductible de degré n sur $\mathbb{F}_p[X]$. On sait que $\mathbb{F}_p[X]/(\pi)$ est le corps de rupture de π sur $\mathbb{F}_p$. On a donc
  $$|\mathbb{F}_p[X]/(\pi)| = |\mathbb{F}_p|^{\dim_{\mathbb{F}_p}(\mathbb{F}_p[X]/(\pi))} = p^{\deg(\pi)} = p^n = q.$$

On conclut par le théorème.

□

Corollaire. *Si $\pi \in \mathbb{F}_p[X]$ irréductible de degré $n \in \mathbb{N}^*$, alors π est scindé sur $\mathbb{F}_{p^n}$.*

Démonstration. Si $\pi(X) \neq X$ (Ok si $n \geq 2$).
Soit $\mathbb{D}$ le corps de décomposition de π sur $\mathbb{F}_p$. Soit $\theta \in \mathbb{D}$ une racine de π.
On a que θ est un élément non nul de $\mathbb{F}_p(\theta)$ (car si $\theta = 0$, alors on peut factoriser π par X ce qui est absurde car π est irréductible).
Or $\mathbb{F}_p(\theta)$ est le corps de rupture de π sur $\mathbb{F}_p$.
Par unicité des corps de rupture,

$$\mathbb{F}_p(\theta) \simeq \mathbb{F}_p[X]/(\pi) \simeq \mathbb{F}_{p^n}.$$

Ainsi, pour tout $\theta \in \mathbb{F}_{p^n}^*$, $\theta^{p^n-1} = 1$. Or, quitte à multiplier par une constante non nulle, π est le polynôme minimal de θ sur $\mathbb{F}_p$.
On a donc $\pi(X)|X^{p^n-1} - 1$ sur $\mathbb{F}_p[X]$ donc $\pi(X)|X^{p^n} - X$ sur $\mathbb{F}_p[X]$ (même si $\pi(X) = X$).
Or, on a montré que $\mathbb{F}_{p^n}$ est le corps de décomposition de $X^{p^n} - X$. On a que $X^{p^n} - X$ est scindé sur $\mathbb{F}_{p^n}$ et donc π est scindé sur $\mathbb{F}_{p^n}$. □

Leçons possibles : 125