Construction des corps finis

Par ENS L 1989

Dans la suite, tous les corps sont commutatifs.

Théorème 1:

(i) Pour tout nombre premier $p \in \mathcal{P}$ et tout $n \in \mathbb{N}^*$, il existe un unique corps, à isomorphisme près, de cardinal p^n.

(ii) Si $\mathbb{K}$ est un corps fini alors on dispose de $p \in \mathcal{P}$ et $n \in \mathbb{N}^*$ tel que:

$$|\mathbb{K}| = p^n$$

Lemme 1:

Soit $p \in \mathcal{P}$. Alors l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps que l'on notera $\mathbb{F}_p$.

Preuve :

C'est immédiat par Bézout.

□

Lemme 2:

Soit $p \in \mathcal{P}$ et $\mathbb{K}$ un corps contenant $\mathbb{F}_p$, alors, pour tout $n \in \mathbb{N}$ tout $P \in \mathbb{F}_p[X]$ et tout $x \in \mathbb{K}$, on a:

$$P(x^{p^n}) = P(x)^{p^n}$$

Preuve :

On sait que pour tout $k \in [\![1, p-1]\!]$, $p \mid \binom{p}{k}$. Par suite, pour $x, y \in \mathbb{K}$,

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} = x^p + y^p$$

Montrons par réccurence sur $d := \deg P$ que pour tout $P \in \mathbb{F}_p[X]$ et tout $x \in \mathbb{K}$, $P(x^p) = P(x)^p$.

- **Initialisation**

Pour $d = 1$, le résultat est évident.

- **Hérédité**

Supposons $d \geqslant 2$ tel que pour tout $k < d$, si $\deg(P) = k$ le résultat tienne.

Soit $P \in \mathbb{F}_p[X]$ de degrès d, on dispose donc de $Q \in \mathbb{F}_p[X]$ et $\lambda \in \mathbb{F}_p$ tels que:

$$\deg(Q) < d \quad P = \lambda X^d + Q$$

Soit $x \in \mathbb{K}$,

$$\begin{aligned} P(x)^p &= \left(\lambda x^d + Q(x)\right)^p \\ &= \lambda^p x^p + Q(x)^p \\ &= \lambda^p (x^p)^d + Q(x^p) \\ &= \lambda (x^p) + Q(x^p) \\ &= P(x^p) \end{aligned}$$

Finalement, pour tout $P \in \mathbb{F}_p[X]$, $x \in \mathbb{K}$, $P(x^p) = P(x)^p$. Par réccurence immédiate sur $n \in \mathbb{N}$ on a donc:

$$\forall (P, n, x) \in \mathbb{F}_p[X] \times \mathbb{N} \times \mathbb{K}, \quad P\left(x^{p^n}\right) = P(x)^{p^n}$$

□

Théorème 2:

Soit $p \in \mathcal{P}$ et $n \in \mathbb{N}^*$. Pour $d \in \mathbb{N}$, on note:

$$\mathfrak{I}_p^d := \left\{P \in \mathbb{F}_p[X] \mid \deg(P) = d, P \text{ unitaire et irréductible dans } \mathbb{F}_p[X]\right\}$$

Alors:

$$X^{p^n} - X = \prod_{d \mid n} \prod_{P \in \mathfrak{I}_p^d} P$$

Pour $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$ on notera (P) l'idéal de $\mathbb{K}[X]$ engendré par P.

Lemme 3:

Soient $p \in \mathcal{P}$ et $n \in \mathbb{N}^*$. On note $Q \in \mathbb{F}_p[X]$ un polynôme unitaire irréductible de degrès d. Alors il y a équivalence entre:

$$\begin{aligned} &(i) \quad d \mid n \\ &(ii) \quad Q \mid X^{p^n} - X \end{aligned}$$

Preuve :(Du lemme 3)

On note dans la suite:

$$\mathbb{K} := \mathbb{F}_p[X]/(Q) \quad \text{et} \quad \overline{X} \text{ la classe de } X \text{ dans ce quotient}$$

$\mathbb{K}$ est un corps de cardinal p^d et ainsi, pour tout $x \in \mathbb{K}^*$,

$$x^{|\mathbb{K}^*|} = x^{p^d-1} = 1$$

$(i) \Rightarrow (ii)$

Supposons $d \mid n$, par suite $p^d - 1 \mid p^n - 1$ ainsi, pour tout $x \in \mathbb{K}^*$,

$$x^{p^n-1} = 1$$

En particulier,

$$\overline{X}^{p^n} = \overline{X}$$

Soit

$$\overline{X^{p^n} - X} = 0$$

Puis

$$Q \mid X^{p^n} - X$$

$(ii) \Rightarrow (i)$

Supposons maintenant $Q \mid X^{p^n} - X$

Soit $x \in \mathbb{K}$, on dipose de $P \in \mathbb{F}_p[X]$ tel que $x = \overline{P} = P\left(\overline{X}\right)$, par suite,

$$x^{p^n} = P\left(\overline{X}\right)^{p^n} = P\left(\overline{X}^{p^n}\right) = P\left(\overline{X}\right) = x$$

De plus, comme $|\mathbb{K}^*| = p^d - 1$ si $x \in \mathbb{K}^*$,

$$x^{p^d-1} = 1$$

Si l'on note alors $n = kd + r$ la division euclidienne de n par d, on a:

$$p^n - 1 = \left(p^{kd+r} - 1\right) = p^r\left(p^{kd} - 1\right) + p^r - 1$$

Ainsi, comme $p^d - 1 \mid p^{dk} - 1$, pour tout $x \in \mathbb{K}^*$,

$$\begin{aligned} x^{p^n-1} &= x^{p^r\left(p^{dk}-1\right)} x^{p^r-1} \\ &= \left(x^{p^{dk}-1}\right)^{p^r} x^{p^r-1} \\ &= x^{p^r-1} \end{aligned}$$

Finalement, pour $x \in \mathbb{K}^*$,

$$1 = x^{p^n-1} = x^{p^r-1}$$

Ainsi, le polynôme $P := T^{p^r-1} - 1 \in \mathbb{K}[T]$ s'annule partout sur $\mathbb{K}^*$, mais si $r \neq 0$ son degrès est $p^r - 1 < p^d - 1$ ce qui impossible, par suite $r = 0$ puis:

$$d \mid n$$

□

Lemme 4:

Soient $p \in \mathcal{P}$ et $n \in \mathbb{N}^*$, alors $X^{p^n} - X \in \mathbb{F}_p[X]$ est sans facteur carré.

Preuve :*(Du lemme 4)*

Supposons $P \in \mathbb{F}_p[X]$ tel que $P^2 \mid X^{p^n} - X$. On suppose de plus sans perte de généralité que P est irréductible.

On dispose donc de $Q \in \mathbb{F}_p[X]$ tel que:

$$X^{p^n} - X = P^2 Q$$

Par suite, en dérivant:

$$\left(X^{p^n} - X\right)' = 2PP'Q + P^2Q'$$

D'ou $P \mid \left(X^{p^n} - X\right)$. Mais $\left(X^{p^n}\right)' = p^n X^{p^n-1} = 0$, ainsi

$$P \mid -1$$

Ce qui absurde car P est irréductible donc de degrés supérieur ou égal à 1.

□

Preuve :*(Du théorème 2)*

Soient $p \in \mathcal{P}$ et $n \in \mathbb{N}^*$, le lemme 3 montre que les facteurs irréductible de $X^{p^n} - X$ sont exactement les polynômes irréductible unitaire de degrès un diviseur d de n.

Le lemme 4 montre que tous les facteurs apparaisse à la puissance 1, par suite, comme $X^{p^n} - X$ est unitaire:

$$X^{p^n} - X = \prod_{d|n} \prod_{P \in \mathfrak{I}_p^d} P$$

□

Théorème 3:

Soient $(p,n) \in \mathcal{P} \times \mathbb{N}^*$. Il existe $P \in \mathbb{F}_p[X]$ unitaire, irréductible de degrés n.

Preuve :

On note $(i_d)_d := \left(\left|\mathfrak{I}_p^d\right|\right)_d \in \mathbb{N}^{\mathbb{N}}$.

En regardant les degrès dans le résultat du théorème 2 on trouve:

$$p^n = \sum_{d|n} d i_d$$

Par suite, pour tout $d \in \mathbb{N}^*$,

$$p^d = d i_d + \sum_{k|d, k\neq d} k i_k \geqslant d i_d$$

Puis:

$$\begin{aligned} p^n &\leqslant n i_n + \sum_{d|n, d\neq n} p^d \\ &\leqslant n i_n + \sum_{d=1}^{n-1} p^d \\ &\leqslant n i_n + \frac{p^n - 1}{p-1} \\ &\leqslant n i_n + p^n - 1 \end{aligned}$$

Par suite, $n i_n \geqslant 1$ d'où $i_n > 0$ mais comme $i_n \in \mathbb{Z}$, $i_n \geqslant 1$

Finalement $\left|\mathfrak{I}_p^n\right| \geqslant 1$ soit:

$$\text{On dispose de } P \in \mathbb{F}_p[X] \text{ irréductible unitaire de degrès } n$$

□

Preuve :*(Théorème 1, existence)*

Soient $p \in \mathcal{P}$ et $n \in \mathbb{N}^*$. On note $P \in \mathbb{F}_p[X]$ un polynôme unitaire irréductible de degrès n et alors:

$$\mathbb{K} := \mathbb{F}_p[X]/(P) \text{ est un corps et } \ |\mathbb{K}| = p^n$$

□

Preuve :(Théorème 1, unicité et point (ii))

Soit $\mathbb{K}$ un corps de cardinal fini dont on note 1 le neutre.

Soit:

$$\begin{aligned}\varphi : \mathbb{Z} &\longrightarrow \mathbb{K} \\ k &\longmapsto k \cdot 1 = \left(\underbrace{1 + \ldots + 1}_{k \text{ fois}}\right)\end{aligned}$$

On vérifie aisaiment que φ est un morphisme d'anneau, comme $|\mathbb{K}| < +\infty$ φ n'est pas injective et l'on note alors $p \geqslant 2$ tel que $\mathrm{Ker}(\varphi) = p\mathbb{Z}$.

Supposons que p soit composé.

Notons $a, b \geqslant 2$ tels que $ab = p$, par suite, comme $a, b < p$,

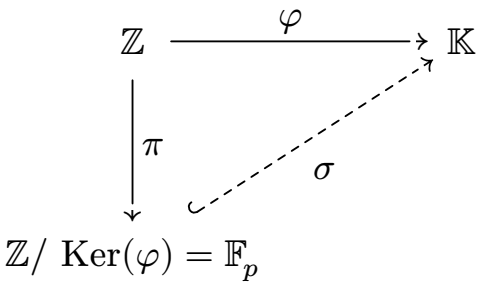
$$\varphi(a) \neq 0 \quad \text{et} \quad \varphi(b) \neq 0$$

Mais, par intégrité de $\mathbb{K}$:

$$0 \neq \varphi(a)\varphi(b) = \varphi(ab) = \varphi(p) = 0$$

Absurde, finalement p est premier.

On dispose donc de $\sigma \in \left(\mathbb{F}_p \longrightarrow \mathbb{K}\right)$ qui est l'unique morphisme rendant le diagramme suivant commutatif:



Finalement, $\sigma\left(\mathbb{F}_p\right) \subseteq \mathbb{K}$ est une extension de corps fini (car $|\mathbb{K}| < +\infty$ toujours) et l'on peut donc munir $\mathbb{K}$ d'une strucure de $\sigma\left(\mathbb{F}_p\right) \simeq \mathbb{F}_p$-ev de dimension finie. En notant $n := \dim_{\mathbb{F}_p}(\mathbb{K})$ On a

$$\mathbb{K} \underset{\text{ev}}{\simeq} \mathbb{F}_p^n$$

Soit

$$|\mathbb{K}| = p^n$$

Soit maintenant $P \in \mathbb{F}_p[X]$ un polynôme unitaire irréductible de degrès n, montrons que:

$$\mathbb{K} \simeq \mathbb{F}_p[X]/(P)$$

On note:

$$\begin{aligned} \cdot^\sigma : \mathbb{F}_p[X] &\longrightarrow \mathbb{K}[X] \\ \sum_{k=0}^{d} a_k X^k &\longmapsto \sum_{k=0}^{d} \sigma(a_k) X^k \end{aligned}$$

On vérifie aisaiment que $\cdot^\sigma$ est un mophisme d'anneau. On note de plus pour $x \in \mathbb{K}$:

$$\begin{aligned} \phi_x : \mathbb{F}_p[X] &\longrightarrow \mathbb{K} \\ Q &\longmapsto Q^\sigma(x) \end{aligned}$$

Tous les ϕ_x sont des morphismes. Par suite, pour tout $x \in \mathbb{K}$, en utilisant le théorème de Lagrange dans $\mathbb{K}^*$,

$$\phi_x(X^{p^n} - X) = x^{p^n} - x = 0$$

Aussi, comme P est irréductible, unitaire de degrès n (qui donc divise n), par le lemme 3,

$$P \mid X^{p^n} - X$$

Notons ainsi $R \in \mathbb{F}_p[X]$ tel que $X^{p^n} - X = PR$

Montrons que P^σ admet une racine dans $\mathbb{K}$.

Supposons par l'absurde que P^σ ne s'annule pas sur $\mathbb{K}$, par suite, pour tout $x \in \mathbb{K}$, $\phi_x(P) \neq 0$, mézalor, comme

$$\forall x \in \mathbb{K}, \quad 0 = \phi_x(X^{p^n} - X) = \phi_x(P)\phi_x(R)$$

On a:

$$\forall x \in \mathbb{K}, \quad \phi_x(R) = R^\sigma(x) = 0$$

Or, comme $\deg(P) \geqslant 1$, $\deg(R^\sigma) = \deg(R) < p^n$, il ne peut donc pas admettre $|\mathbb{K}| = p^n$ racine. Absurde, finalement, on dipose de $z \in \mathbb{K}$ tel que:

$$\phi_z(P) = P^\sigma(z) = 0$$

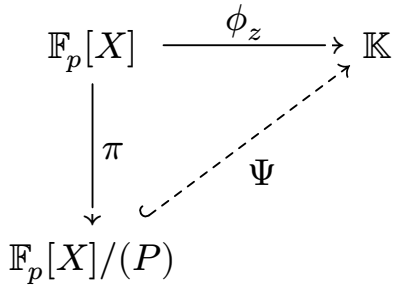
Comme $\mathbb{F}_p[X]$ est infini, ϕ_z n'est pas injective et l'on dipose donc de $\mu \in \mathbb{F}_p[X]$ unitaire tel que:

$$\mathrm{Ker}(\phi_z) = (\mu)$$

Remarquons que les polynômes constant ne sont pas dans $\mathrm{Ker}(\phi_z)$, par suite, $\deg(\mu) \geqslant 1$. Aussi, comme $\phi_z(P) = 0$, $P \in \mathrm{Ker}(\phi_z) = (\mu)$ soit $\mu \mid P$, mais comme P est irréductible et μ non constant:

$$\mu = P$$

En notant Ψ le morphisme rendant le diagramme suivant commuatif,



Ψ nous fournit un morphisme d'anneau injectif de $\mathbb{F}_p[X]/(P)$ dans $\mathbb{K}$. Par égalité des cardinaux, c'est un isomorphisme d'anneau, puis, car $\mathbb{K}$ et $\mathbb{F}_p[X]/(P)$ sont des corps, c'est un isomorphisme de corps.

$$\mathbb{K} \simeq \mathbb{F}_p[X]/(P)$$

□