Existence, unicité et construction des corps finis (2 premiers dans le Perrin)

Étape 0 — Pour $p \in \mathcal{P}$, $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ est un corps fini à p éléments.
— Si $p \in \mathcal{P}$ et $P \in \mathbb{F}_p[X]$ irréductible de degré $d \geq 1$ alors $\frac{\mathbb{F}_p[X]}{(P)}$ est un corps fini, à p^d éléments.

Étape 1 Soit k un corps fini, $\Phi : \begin{vmatrix} \mathbb{Z} \to k \\ 1 \mapsto 1_k \end{vmatrix}$. $\operatorname{Ker}\Phi = n\mathbb{Z}$, $n \in \mathbb{N}$.

$$\mathbb{Z}/\operatorname{Ker}\Phi = \mathbb{Z}/n\mathbb{Z} \hookrightarrow k \text{ donc } \begin{cases} - \ n \neq 0 \text{ car } k \text{ est fini} \\ - \ \mathbb{Z}/n\mathbb{Z} \text{ est intègre donc } n \in \mathcal{P}. \end{cases}$$

Ainsi, k possède une structure de $\mathbb{F}_p$-ev, de dimension finie $d \in \mathbb{N}^*$. Donc $\boxed{\#k = p^d}$

Étape 2 Soit $p \in \mathcal{P}$, $d \in \mathbb{N}^*$.

Analyse Si k est un corps fini de cardinal p^d, alors par le théorème de Lagrange

$$\forall x \in k^*, \ x^{p^d - 1} = 1$$

Donc $\forall x \in k$, $x^{p^d} = x$.

Ainsi, $S_{\mathbb{F}_p}(X^{p^d} - X) \subseteq k \quad (\supseteq \mathbb{F}_p)$

Synthèse Or, $X^{p^d} - X$ est sans facteur carré (dérivé vaut -1), k est commutatif donc

$\#S_{\mathbb{F}_p}(X^{p^d} - X) \geq p^d$. Finalement, $\boxed{k = S_{\mathbb{F}_p}(X^{p^d} - X)}$.

Synthèse $k := \{x \in S_{\mathbb{F}_p}(X^{p^d} - X) \ / \ x^{p^d} - x = 0\}$.

On vérifie que k est un corps (Frob_p^d), par ce qui précède $\boxed{\#k = p^d}$ et $X^{p^d} - X$ est scindé sur k ; donc $\boxed{k = S_{\mathbb{F}_p}(X^{p^d} - X)}$.

Étape 3 $p \in \mathcal{P}$, $d \geq 1$.

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

$$I(p,d) := \{P \in \mathbb{F}_p[X] \ / \ P \text{ irréductible unitaire de degré } d\}.$$

— $X^{p^d} - X$ est sans facteur carré.

— $d' | d$, $P \in I(p,d')$. $\mathbb{F}_{p^{d'}} = \frac{\mathbb{F}_p[X]}{(P)} \ni x := \bar{X}$ $\quad P(x) = 0$; de plus, $x^{p^{d'}} = x$ donc comme $d' | d$,

$$x^{p^d} = x^{p^{kd'}} = x^{p^{d'} p^{d'} \cdots p^{d'}} = x$$

donc $x \in \mathbb{F}_{p^{d'}}$ donc $x^{p^d} - \cancel{x = 0}$.

Or, P est irréductible donc $\boxed{P \mid X^{p^d} - X}$ $\quad (P = \mu_{\mathbb{F}_p, x})$

– Si $P \mid X^{p^d} - X$, $d' = \deg P$.

P unit. est scindé dans $\mathbb{F}_{p^d}$, si x désigne une racine de P,

$$\mathbb{F}_p \subseteq \mathbb{F}_p(x) \simeq \frac{\mathbb{F}_p(X)}{(P)} \subseteq \mathbb{F}_{p^d}$$

donc $\mathbb{F}_{p^{d'}} \subset \mathbb{F}_{p^d}$ donc $\boxed{d' \mid d}$

Remarque Si $P \in I(p,d)$ alors $\boxed{\frac{\mathbb{F}_p(X)}{(P)} = \mathbb{F}_{p^d}}$

Étape 4 $N(p,d) := \# I(p,d)$.

$$p^d = \sum_{d' \mid d} d' N(p,d') \geqslant d N(p,d).$$

c'est-à-dire, $d N(p,d) = p^d - \sum_{\substack{d' \mid d \\ <}} d' N(p,d') \geqslant p^d - \sum_{d'=1}^{d-1} p^{d'}$

$$= p^d - p \frac{p^{d-1} - 1}{p-1}$$

$$= p^d - \frac{\overbrace{p^d - p}^{< p^d}}{\underbrace{p-1}_{\geqslant 2}} > 0.$$

Donc $\boxed{N(p,d) > 0}$

c'est-à-dire, les corps finis sont exactement les $\frac{\mathbb{F}_p(X)}{(P)}$ avec P unit. irr. sur $\mathbb{F}_p$,

et on peut trouver un P unit. irr. de degré d $\forall d \geqslant 1$.

13/11

Remarque avec $\sum$ $L d(e)$ on obtient $N(p,d) \sim \frac{p^d}{d}$.