(G)

Existence et "dénombrement" des poly. inéd. sur $\mathbb{F}_q$

Leçons : 123, 125, 141, 144

Réf. : Demazure, Cours d'algèbre p 220

Lemme :

Soient $q, r, n \in \mathbb{N}$ $r, n \geq 1$ et $q \geq 2$.

Alors $\boxed{q^r - 1 \mid q^n - 1 \iff r \mid n}$

Proposition :

Soit $n \in \mathbb{N}$, $n > 0$, et $q = p^\alpha$ où p premier et $\alpha \in \mathbb{N}$, $\alpha > 0$.
Dans $\mathbb{F}_q[X]$, $X^{q^n} - X$ est exactement le produit des polynômes unitaires inéductibles dont le degré divise n.

Corollaire :

Soit m_n le nombre de polynômes unitaires inéductibles de degré n.

On a $\boxed{\dfrac{q^n - q^{\lfloor \frac{n}{2} \rfloor + 1}}{n} \leq m_n \leq \dfrac{q^n}{n}}$

En particulier, il existe des polynômes inéductibles dans $\mathbb{F}_q$ de tout degré (> 0), et $\boxed{m_n \underset{+\infty}{\sim} \dfrac{q^n}{n}}$

Lemme

$\Rightarrow$ Si $q^r - 1 \mid q^n - 1$, alors $n \geq r$.

On a alors $n = ar + b$ où $0 \leq b < r$ et $a \geq 1$

Il q $b = 0$

$$q^n - 1 = q^{ar} q^b - 1 = (q^r)^a q^b - q^b + q^b - 1$$

donc $$q^n - 1 = q^b \left((q^r)^a - 1 \right) + q^b - 1$$

et $x^a - 1 = (x-1)(x^{a-1} + \dots + 1)$ donc

$$q^n - 1 = q^{\overbrace{b}^{n-ar}}\left(q^n - 1\right)\left(q^{r(a-1)} + \dots + 1\right) + q^b - 1$$

$n = ar + b$

$$(*)\quad q^n - 1 = \left(q^r - 1\right)\underbrace{\left(q^{n-r} + q^{n-2r} + \dots + q^{n-ar}\right)}_{\in \mathbb{N}} + \underbrace{q^b - 1}_{< q^r - 1}$$

Donc $(*)$ est la division euclidienne de $q^n - 1$ par $q^r - 1$, et comme $q^r - 1 \mid q^n - 1$ par hypothèse,

$$q^b = 1 \quad \downarrow q \geq 2$$

donc $\boxed{b = 0}$ et $\boxed{r \mid n}$

($\Leftarrow$) Si $r \mid n$, alors il existe $a \in \mathbb{N}^*$ tel que $n = ar$.

Donc $$q^n - 1 = \left(q^r\right)^a - 1 = \left(q^r - 1\right)\underbrace{\left(q^{r(a-1)} + \dots + 1\right)}_{\in \mathbb{N}}$$

donc $\boxed{q^r - 1 \mid q^n - 1}$

Proposition

1) Soit $P \in \mathbb{F}_q[X]$, P unitaire irréductible et $\deg(P) = r \mid n$.
Π_q $P \mid X^{q^n} - X$. On pose $S = X^{q^n} - X$

On suppose que $P \neq X$ (sinon c'est évident)

Soit $\Pi : \mathbb{F}_q[X] \longrightarrow \mathbb{F}_q[X]/(P) = K$

$$Q \longmapsto Q(\alpha) \quad \text{où} \quad \alpha = \Pi(X).$$

- P est irréductible dans $\mathbb{F}_q[X]$ donc K est un corps fini de cardinal q^r $(r = \deg(P))$.

- $\pi(x) = \alpha \in K^*$ car $P \nmid X$ et $|K^*| = q^n - 1$

  donc $\alpha^{q^n - 1} = 1$

- $r \mid n$ donc par le lemme $q^r - 1 \mid q^n - 1$ donc $\alpha^{q^n - 1} = 1$

  donc $\alpha^{q^n} = \alpha$

Par conséquent, $S(\alpha) = 0$ d'où $S \in \ker \pi = (P)$

donc $\boxed{P \mid X^{q^n} - X}$

2) Soit $P \in \mathbb{F}_q[X]$ un facteur unitaire irréductible de S, $\deg(P) = r$.
Montrer que $r \mid n$, ce qui équivaut à montrer que $q^r - 1 \mid q^n - 1$

Avec les notations du 1) on a $K = \mathbb{F}_q[\alpha]$

Par hypothèse, $P \mid X^{q^n} - X$ donc $\alpha^{q^n} = \alpha$

On pose $A = \{a \in K,\ a^{q^n} = a\}$.

Alors : . A est un sous-anneau de K

. $\alpha \in A$ et par le morphisme de Frobenius,

$\forall Q \in \mathbb{F}_q[X]$, $(Q(\alpha))^{q^n} = Q(\alpha^{q^n}) = Q(\alpha)$

donc $\mathbb{F}_q[\alpha] = K \subset A$.

donc $\underline{A = K}$ et pour tout $a \in K$, $a^{q^n} = a$

On, K est un corps fini, donc K^* est cyclique et $|K^*| = q^r - 1$

Soit a un générateur de K^*. Alors

$\begin{cases} \mathrm{ord}(a) = q^r - 1 \\ a^{q^n} = a \text{ donc } a^{q^n - 1} = 1 \end{cases}$ donc $q^r - 1 \mid q^n - 1$

donc $\boxed{r \mid n}$

3) $\mathbb{F}_q$ $X^{q^n} - X$ n'a pas de facteur multiple

$\mathbb{F}_q$ est de caractéristique p qui divise q,

donc $(X^{q^n} - X)' = \underbrace{q^n}_{=0} X^{q^n-1} - 1 = -1$

donc $S \wedge S' = 1$ et $X^{q^n} - X$ n'a pas de facteur multiple

Corollaire

$$X^{q^n} - X = \prod_{r \mid n} \underbrace{(P \in \mathbb{F}_q[X],\ P \text{ irréd. unitaire et } \deg(P) = r)}_{m_r}$$

donc $q^n = \sum_{r \mid n} r\, m_r$ (degrés)

- "n divise n" donc $n\, m_n \leq q^n$ donc $m_n \leq \frac{q^n}{n}$

- $$q^n - n\, m_n = \sum_{\substack{r \mid n \\ r < n}} r\, m_r$$
$$\leq \sum_{r \leq \lfloor \frac{n}{2} \rfloor} r\, m_r$$
$$\leq \sum_{r \leq \lfloor \frac{n}{2} \rfloor} q^r$$
$$\leq \frac{q^{\lfloor \frac{n}{2} \rfloor + 1} - 1}{q - 1}$$

somme géométrique

$$q^n - n\, m_n \leq q^{\lfloor \frac{n}{2} \rfloor + 1}$$

donc $$\frac{q^n - q^{\lfloor \frac{n}{2} \rfloor + 1}}{n} \leq m_n$$

On a bien $$\frac{q^n - q^{\lfloor \frac{n}{2} \rfloor + 1}}{n} \leq m_n \leq \frac{q^n}{n}$$ et l'équivalent $m_n \sim \frac{q^n}{n}$