VM
28/12/14
1

Existence d'un corps fini à p^n éléments

123, 125, 141, 190

Il s'agit de montrer que pour p premier, $n \geq 1$, il existe un polynôme irréductible dans $\mathbb{F}_p[X]$ de degré n.

Lemme 1 : $p^d - 1$ divise $p^m - 1$ ssi d divise m.

Lemme 2 : $X^{p^d} - X$ divise $X^{p^n} - X$ ssi d divise n.

Lemme 3 : Si $P \in \mathbb{F}_p[X]$ est irréductible de degré d, et $d \mid m$, alors P divise $X^{p^m} - X$.

Lemme 4 : Si $P \in \mathbb{F}_p[X]$ est un facteur irréductible de $X^{p^m} - X$ de degré d, alors $d \mid m$ et P est de multiplicité 1 dans $X^{p^m} - X$.

Théorème : Il existe un polynôme irréductible de degré n dans $\mathbb{F}_p[X]$.

dém (lemme 1) $\Leftarrow$ Soit d un diviseur de n. Alors $n = n'd$.

$$a^{n'} - 1 = (a-1)(a^{n'-1} + \dots + a + 1)$$

Avec $a = p^d$, on a $(p^n - 1) = (p^d - 1)(\dots)$ d'où $p^d - 1$ divise $p^n - 1$.

$\Rightarrow$: $n = qd + r$, $0 \leq r < d$.

Alors $p^n - 1 = p^{qd+r} - 1 = p^r(p^{qd} - 1) + p^r - 1$

$p^d - 1$ divise $p^n - 1$ et $p^{qd} - 1$, donc $p^d - 1$ divise $p^r - 1$

donc $r = 0$.

dém (lemme 2) : $X^{p^d} - X$ divise $X^{p^n} - X$ ssi $X^{p^d - 1} - 1$ divise $X^{p^n - 1} - 1$

ssi $p^d - 1$ — $p^n - 1$

ssi d — n.

dém (théorème) : $X^{p^m} - X$ est le produit de l'ensemble des polynômes unitaires irréductibles de degré d dans $\mathbb{F}_p[X]$ pour $d \mid m$.

On écrit l'égalité des degrés, $p^m = \sum_{d \mid m} d\beta(d)$,

où $\beta(d)$ est le nombre de polynômes unitaires irréductibles de degré d dans $\mathbb{F}_p[X]$.

Soit $n \geq 1$. $n f(n) = \sum_{d \mid n} p^{n/d} \mu(d)$ par la formule d'inversion de Möbius.

Soit q_m le produit des facteurs (premiers) irréductibles de n.

Alors p^{n/q_m+1} divise tous les termes de la somme sauf $p^{n/q_m} \mu(q_m) = \pm p^{n/q_m}$. Donc $n f(n) \equiv \pm p^{n/q_m} \left[p^{n/q_m+1}\right]$

Donc $f(n) \neq 0$: $f(n) \geq 1$.

Il suffit de montrer, d'après le lemme 2, que $P \mid X^{p^n} - X$.

dém (lemme 3) : Soit $Q = \text{pgcd}(P, X^{p^n} - X)$.

Soit $K = \mathbb{F}_p[X]/(P)$. Soit $\alpha = \overline{X}$ dans K.

Comme $|K| = p^d$, $\alpha^{p^d} - \alpha = 0$. De plus, $P(\alpha) = 0$.

Par l'identité de Bezout, on a $Q(\alpha) = 0$.

Or Q n'est pas constant égal à 0 car P ne l'est pas, donc Q n'est pas constant. Comme P est irréductible, $P = aQ$, $a \in K^*$, donc P divise $X^{p^q} - X$.

---

dém (lemme 4) : On garde les notations K, α.

On a toujours $\alpha^{p^d} - \alpha = 0$. De plus, comme $P(\alpha) = 0$, et que P divise $X^{p^m} - X$, on a $\alpha^{p^m} - \alpha = 0$.

Soit $\ell = d \wedge m$, $\ell \geq 1$. Par Bézout, il existe u, v tels que $\ell = ud + vm$.

$$p^\ell - 1 = p^{ud+vm} - 1 = p^{vm}\left(p^{ud} - 1\right) + p^{vm} - 1$$
$$= a\left(p^d - 1\right) + b\left(p^m - 1\right) \quad \text{(d'après lemme 1)}$$

où $a, b \in \mathbb{Z}$.

Donc $\alpha^{p^\ell - 1} = \left(\alpha^{p^d - 1}\right)^a \left(\alpha^{p^m - 1}\right)^b = 1$ donc $\alpha^{p^\ell} = \alpha$.

Comme $(x+y)^{p^\ell} = x^{p^\ell} + y^{p^\ell}$ dans $K = \mathbb{F}_p(\alpha)$, on a $x^{p^\ell} = x$ $\forall x \in \mathbb{F}_p(\alpha)$. Or $X^{p^\ell} - X$ a au plus p^ℓ diviseurs, donc $p^\ell \geq p^d$, donc $\ell \geq d$: $\ell = d$ et d divise m.

Si $X^{p^n} - X = Q P^2$, alors en dérivant, $-1 = P(Q'P + 2QP')$ donc P est constant de qui est exclu.

VM
28/12/14
2

Complément : formule d'inversion de Möbius

$n \in \mathbb{N} \setminus \{0\}$ $\quad \mu(n) = \begin{cases} 1 & \text{si } n = 1. \\ (-1)^p & \text{si } n \text{ est le produit de } p \text{ facteurs premiers deux à deux distincts} \\ 0 & \text{sinon} \end{cases}$

Si $g(n) = \sum_{d \mid n} f(d)$, alors $f(n) = \sum_{d \mid n} g\left(\frac{n}{d}\right) \mu(d)$.

---

dém : Soit $\varepsilon(n) = \sum_{d \mid n} \mu(d)$.

Si $n \geq 2$ $\quad n = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, $\alpha_i \geq 1$.

$$\varepsilon(n) = \sum_{\varepsilon_i = 0,1} \mu\left(p_1^{\varepsilon_1} \cdots p_n^{\varepsilon_n}\right) = \sum_{k=0}^{n} \binom{n}{k} (-1)^k = 0.$$

Si $n = 1$, $\varepsilon(1) = \mu(1) = 1$.

Ainsi, $\sum_{d \mid n} \mu(d)\, g\left(\frac{n}{d}\right) = \sum_{d \mid n} \mu(d) \sum_{m \mid \frac{n}{d}} f(m)$

$$= \sum_{d \mid n} \mu(d) \sum_{m \mid \frac{n}{d}} f\left(\frac{n}{md}\right).$$

$$= \sum_{md \mid n} \mu(d)\, f\left(\frac{n}{md}\right)$$

$$= \sum_{k \mid d} f\left(\frac{n}{k}\right) \sum_{d \mid k} \mu(d)$$

$$= \sum_{k \mid d} f\left(\frac{n}{k}\right) \varepsilon(k)$$

$$= f(n).$$

Complément : Unicité du corps à p^n éléments.

Soit K un corps à p^n éléments. Soit P irréd de degré n dans $\mathbb{F}_p[X]$.

$\mathbb{F}_p[X]/(P)$ a aussi p^n éléments.

Soit $\alpha = \bar{X}$ dans $\mathbb{F}_p[X]/(P)$.

$X^{p^n} - X$ est scindé sur K, son facteur P y a une racine β.

Soit $\phi : \mathbb{F}_p[X]/(P) \to K$

défini comme suit : si $x \in \mathbb{F}_p[X]/(P)$, il existe un unique $Q \in \mathbb{F}_p[X]$ de degré $\leq p-1$ tel que $x = Q(\alpha)$. Alors $\phi(x) = Q(\beta)$.

On a ainsi, $\forall Q \in \mathbb{F}_p[X]$ de degré $n-1$,

$$\phi(Q(\alpha)) = Q(\beta).$$

Soit $R \in \mathbb{F}_p[X]$. $R = SP + Q$, $\deg Q \leq n-1$.

$$R(\alpha) = Q(\alpha).$$

$$\phi(R(\alpha)) = \phi(Q(\alpha)) = Q(\beta) = R(\beta)$$

Donc ϕ est un morphisme d'anneau.

De plus, comme $\phi(1) = 1$, il est injectif (morphisme de corps).

$$\phi(x) = \phi(y) \Rightarrow \phi(xy^{-1}) = \phi(x)\,\phi(y)^{-1} = 1 = \phi(1)$$

Donc $\phi(xy^{-1} - 1) = 0$.

On a $\forall a \phi(a) = 0$ vérifié $a = 0$.

K et $\mathbb{F}_p[X]/(P)$ ayant même cardinal, c'est une bijection, donc un Romorphisme.

Schéma de dév :

lemme 1

puis ecrit $X^{p^d} - X$ ...

Puis déf de U_d : ensemble des pol irréd de $\mathbb{F}_p[X]$ unitaire de degré d.

Lemme 2 : $X^{p^m} - X$ est le produit des éléments de l'ensemble des U_d pour $d \mid m$

Théorème : puis déc Thm

puis déc lemme 2