leçons : 120 : Anneaux $\mathbb{Z}/n\mathbb{Z}$
121. Nombres premiers. Applications.
123. Corps finis. Applications.
142. Algèbre des polynômes à plusieurs indéterminées. Applications.

Théorème de Chevalley-Warning et application

(39)

Références :
Maxime Zavidovique "Un max de Math"
JP Serre "Cours d'arithmétique"

Thm : Soit A un ensemble fini et $(f_\alpha)_{\alpha\in A} \in \mathbb{F}_q[X_1,\dots,X_n]^A$ une famille de polynômes à n variables tels que $\sum_{\alpha\in A} \deg(f_\alpha) < n$ et soit $V = \{x \in \mathbb{F}_q^n \mid \forall \alpha \in A \ f_\alpha(x) = 0\}$

On a alors $\#V \equiv 0 \ [p]$ (où p est premier et q est une puissance de p)

preuve :

① On pose $P = \prod_{\alpha\in A} (1 - f_\alpha^{q-1})$. Soit $x \in \mathbb{F}_q^n$.

Si $x \in V$, alors $\forall \alpha \in A \ f_\alpha(x) = 0$ donc $P(x) = 1$

Si $x \notin V$, alors $\exists \alpha_0 \in A \ f_{\alpha_0}(x) \neq 0$ et on a $f_{\alpha_0}(x)^{q-1} = 1$ car $\mathbb{F}_q^*$ est cyclique d'ordre $q-1$ donc $P(x) = 0$.

D'où $\boxed{P = \mathbb{1}_V}$

② Pour un polynôme $f \in \mathbb{F}_q[X_1,\dots,X_n]$, on pose $S(f) = \sum_{x\in\mathbb{F}_q^n} f(x)$. $S : \mathbb{F}_q[X_1,\dots,X_n] \to \mathbb{F}_q$ est linéaire.

On a alors $S(P) = \sum_{x\in V} 1 = \operatorname{card} V \ [p]$

Il suffit donc de montrer que $S(P) = 0$.

③ $\sum_{\alpha\in A} \deg(f_\alpha) < n$ donc $\deg P \leqslant (q-1) \sum_{\alpha\in A} (\deg f_\alpha) < (q-1)n$

Donc P est une combinaison linéaire de monômes $X^u = X_1^{u_1} \dots X_n^{u_n}$ avec $\sum_{i=1}^n u_i < (q-1)n$

Il suffit, par linéarité, de montrer que $S(X^u) = 0$ pour u tel que $\sum_{i=1}^n u_i < (q-1)n$

④ Lemme : Soit $v \in \mathbb{N}$, alors $S(v) := \sum_{x\in\mathbb{F}_q} x^v = \begin{cases} -1 & \text{si } v \text{ est divisible par } q-1 \text{ et } v \neq 0 \\ 0 & \text{sinon} \end{cases}$

preuve du lemme :

- Si $v = 0$: $S(0) = \sum_{x\in\mathbb{F}_q} x^0 = \sum_{x\in\mathbb{F}_q} 1 = q = 0$
- Si $v \geqslant 1$, v divisible par $q-1$: $S(v) = \sum_{x\in\mathbb{F}_q} x^v = \sum_{x\in\mathbb{F}_q^*} 1 + 0 = q-1 = -1$
- Si $v \geqslant 1$, v non divisible par $q-1$: on prend $y \in \mathbb{F}_q^*$ tel que $y^v \neq 1$

Il existe bien un tel y par cyclicité, il suffit de prendre un générateur.

$$S(v) = \sum_{x \in \mathbb{F}_q} x^v = \sum_{x \in \mathbb{F}_q} (yx)^v = y^v S(v) \quad \text{donc} \quad \underbrace{(1-y^v)}_{\neq 0} S(v) = 0 \quad \text{donc} \quad S(v) = 0$$

⑤ Conclusion :

Soit $X^u = X_1^{u_1} X_2^{u_2} \cdots X_n^{u_n}$ avec $\sum_{i=1}^{n} u_i < (q-1)n$ (*)

On a $S(X^u) = \sum_{\substack{x \in \mathbb{F}_q^n \\ x=(x_1,\dots,x_n)}} \prod_{i=1}^{n} x_i^{u_i} = \prod_{i=1}^{n} S(u_i)$

Or il existe $i \in [\![1,n]\!]$ tel que $u_i < q-1$ par (*) donc $S(X^u) = 0$.

[Application : Soit p un nombre premier. Soient $(u_1, \dots, u_{p-1})$ des entiers, alors on peut en choisir p tels que leur moyenne soit un entier.

preuve : Soit $n = 2p-1$. On pose $\begin{cases} f_1 = X_1^{p-1} + \dots + X_n^{p-1} \in \mathbb{F}_p[X_1, \dots, X_n] \\ f_2 = \overline{u_1} X_1^{p-1} + \dots + \overline{u_n} X_n^{p-1} \in \mathbb{F}_p[X_1, \dots, X_n] \end{cases}$

On pose $V = \{ x \in \mathbb{F}_p^n \mid f_1(x) = f_2(x) = 0 \}$

$\deg f_1 + \deg f_2 = 2p-2 < n$

On peut appliquer le thm de Chevalley-Warning : $\#V \equiv 0 \ [p]$

Or $V \neq \emptyset$ car $(0, \dots, 0) \in V$

Donc V contient un n-uplet non trivial $(x_1, \dots, x_n) \in \mathbb{F}_p^n$.

$f_1(x_1, \dots, x_n) = \#\{ i \in [\![1,n]\!] \mid x_i \neq 0 \} \ [p]$

$f_1(x_1, \dots, x_n) = 0$ donc $\#\{ i \in [\![1,n]\!] \mid x_i \neq 0 \}$ est divisible par p

On en déduit que $\#\{ i \in [\![1,n]\!] \mid x_i \neq 0 \} = p$

$f_2(x_1, \dots, x_n) = \sum_{x_i \neq 0} \overline{u_i} x_i^{p-1} = \sum_{x_i \neq 0} \overline{u_i} = 0_{\mathbb{F}_p}$.

Donc p divise $\sum_{x_i \neq 0} u_i$ ∎