Théorème de Chevalley-Warning

Référence : [Ser70] p.12-13.

Théorème 0.1 *Soit $\mathbb{K}$ un corps à q éléments où $q = p^n$ avec p un nombre premier et n un entier. Soient $f_\alpha \in \mathbb{K}[X_1, \ldots, X_n]$ des polynômes à n variables tels que $\sum \deg f_\alpha < n$. Soit V l'ensemble de leurs zéros communs dans $\mathbb{K}^n$. Alors card$(V) \equiv 0[p]$.*

Démonstration On pose :

$$P = \prod_\alpha (1 - f_\alpha^{q-1})$$

Soit $x \in \mathbb{K}^n$.
$\rightsquigarrow$ Examinons le polynôme $P \in \mathbb{K}[X_1, \ldots, X_n]$:
- Si $x \in V$, alors tous les $f_\alpha(x)$ sont nuls (par définition de V) et on a :

$$P(x) = \prod_\alpha 1 = 1$$

- Si $x \neq V$, alors l'un au moins de $f_\alpha(x)$ est non nul (par définition de V) et il vérifie $f_\alpha(x)^{q-1} = 1$ (car f_α est à valeurs dans $\mathbb{K}$ qui est de caractéristique p, donc d'après le théorème de Fermat $x^{q-1} \equiv 1[p]$). D'où :

$$P(x) = 0$$

Ainsi P est la fonction caractéristique de V.
$\rightsquigarrow$ Si pour tout polynôme $f \in \mathbb{K}[X_1, \ldots, X_n]$, on pose :

$$S(f) = \sum_{x \in \mathbb{K}^n} f(x)$$

on a donc :

$$\text{card}(V) \equiv S(P)[p]$$

(car $S(P) = \sum_{x \in \mathbb{K}^n} P(x)$ et $P(x) \neq 0$ si $x \in V$).
$\rightsquigarrow$ Montrons alors que $S(P) = 0$.
L'hypothèse $\sum \deg f_\alpha < n$ entraîne que :

$$\deg(P) = \deg\left(\prod_\alpha (1 - f_\alpha^{q-1})\right) = \sum_\alpha \deg(1 - f_\alpha^{q-1}) \leq \sum_\alpha \deg(f_\alpha^{q-1}) = (q-1)\sum_\alpha \deg(f_\alpha) < (q-1)n$$

Donc P est une combinaison linéaire de monômes $X^u = X_1^{u_1} \times \ldots \times X_n^{u_n}$ avec $\sum u_i < n(q-1)$ (car $P \in \mathbb{K}[X_1, \ldots, X_n]$ et $\deg(P) < n(q-1)$).
$\rightsquigarrow$ Il suffit donc de prouver qu'un tel monôme X^u vérifie $S(X^u) = 0$ et ceci découle du lemme :

Lemme 0.1 *Soit u un entier naturel. Alors :*

$$S(X^u) = \sum_{x \in \mathbb{K}} x^u = \begin{cases} -1 & \text{si } u \geq 1 \text{ et divisible par } q-1 \text{ ;} \\ 0 & \text{sinon.} \end{cases}$$

On suppose par convention que $x^u = 1$ si $u = 0$ et même si $x = 0$.
- Si $u = 0$, alors tous les termes de $S(X^u)$ sont égaux à 1, d'où :

$$S(X^u) = \sum_{x \in \mathbb{K}} 1 = \text{card}\,\mathbb{K} = q \equiv 0[p]$$

– Si $u \geq 1$ et divisible par $q-1$. On a $0^u = 0$ et $x^u = 1$ pour $x \neq 0$ d'après le théorème de Fermat, car $q-1|u$, ie $u = (q-1) \times v$ pour $v \in \mathbb{N}$. D'où :

$$S(X^u) = q - 1 \equiv -1[p]$$

– Si $u \geq 1$ et non divisible par $q-1$. Le fait que $\mathbb{K}^*$ soit cyclique d'ordre $q-1$ montre qu'il existe $y \in \mathbb{K}^*$ tel que $y^u \neq 1$, on a donc :

$$S(X^u) = \sum_{x \in \mathbb{K}} x^u = \sum_{x \in \mathbb{K}^*} x^u = \sum_{x \in \mathbb{K}^*} y^u x^u = y^u S(X^u)$$

car l'application :

$$\begin{aligned} \phi : \mathbb{K}^* &\longrightarrow \mathbb{K}^* \\ x &\longmapsto yx \end{aligned}$$

est une bijection.

D'où $(1 - y^u)S(X^u) = 0$ ce qui implique que $S(X^u) = 0$ car $y^u \neq 0$ (car $y \in \mathbb{K}^*$).

D'où le résultat.

$\rightsquigarrow$ On peut maintenant appliquer le lemme, comme $\sum u_i < n(q-1)$ alors au moins l'un des $u_i < q-1$ donc non divisible par $q-1$, donc $\sum u_i$ ne peut pas être divisible par $q-1$, donc $S(X^u) \equiv 0[p]$.

Références

[Ser70] Jean-Pierre Serre. *Cours d'arithmétique*. Presses universitaires de France, 1970.