13 Théorème de Chevalley-Warning

On se place sur un corps fini $\mathbb{F}_q$ de caractéristique p.

Lemme. *Soit* $m \in \mathbb{N}$. $\displaystyle\sum_{x\in\mathbb{F}_q} x^m = \begin{cases} 0 & \text{si } m = 0 \text{ ou } q-1 \nmid m \\ -1 & \text{sinon} \end{cases}$

Preuve.
Si $m = 0$, $\sum_{x\in\mathbb{F}_q} x^m = \sum_{x\in\mathbb{F}_q} 1$ (sachant que $0^0 = 1$) soit $\sum_{x\in\mathbb{F}_q} x^m = q = 0$ dans $\mathbb{F}_q$.

Si $q-1 \nmid m$, soit g un générateur de ${\mathbb{F}_q}^\times$. $x \mapsto gx$ est une bijection de $\mathbb{F}_q$, on peut donc écrire $\sum_{x\in\mathbb{F}_q} x^m = \sum_{x\in\mathbb{F}_q} (gx)^m$ soit $\sum_{x\in\mathbb{F}_q} x^m = g^m \sum_{x\in\mathbb{F}_q} x^m$. Comme g est un générateur de ${\mathbb{F}_q}^\times$ et $q-1 \nmid m$, on a $g^m \neq 1$; on en déduit que $\sum_{x\in\mathbb{F}_q} x^m = 0$.

Enfin, si $m \neq 0$ et m est un multiple de $q-1$, alors $x^m = 1$ $\forall x \in {\mathbb{F}_q}^\times$. Il vient $\sum_{x\in\mathbb{F}_q} x^m = q-1 = -1$ dans $\mathbb{F}_q$.

□

Théorème (Chevalley-Warning). *Soit P_1, ..., P_r des polynômes non nuls de $\mathbb{F}_q[X_1, ..., X_n]$, tels que $\sum_{i=1}^r d^\circ P_i < n$. Alors $\#Z(P_1, ..., P_k) = 0$ [p].*

On a noté $Z(P_1, ..., P_k)$ l'ensemble des racines communes à tous les P_i dans ${\mathbb{F}_q}^n$.

Preuve.
Posons $S = \prod_{i=1}^r \left(1 - P_i^{q-1}\right)$. Montrons que S est la fonction caractéristique de $Z(P_1, ..., P_k)$ sur ${\mathbb{F}_q}^n$. Si $x \in {\mathbb{F}_q}^n$ est racine de tous les P_i, il est clair que $S(x) = 1$. Si $P_i(x) \neq 0$ pour un certain i, alors $P_i(x)^{q-1} = 1$ si bien que $S(x) = 0$. Ainsi, $\#Z(P_1, ..., P_k) = \sum_{x\in{\mathbb{F}_q}^n} S(x)$.

Écrivons $S(X) = \sum_\alpha \lambda_\alpha X^\alpha$ (où les α sont des multi-indices). On a alors $\sum_{x\in{\mathbb{F}_q}^n} S(x) = \sum_\alpha \lambda_\alpha \sum_{x\in{\mathbb{F}_q}^n} x^\alpha$. Fixons $\alpha = (\alpha_1, ..., \alpha_n)$, alors $\sum_{x\in{\mathbb{F}_q}^n} x^\alpha = \prod_{i=1}^n \sum_{x_i\in\mathbb{F}_q} {x_i}^{\alpha_i}$. Comme $\sum_{i=1}^r d^\circ P_i < n$, on a $d^\circ S = (q-1)\sum_{i=1}^r d^\circ P_i < n(q-1)$. Il s'ensuit que dans tout monôme de S, l'un au moins des α_i est $< q-1$. D'après le lemme précédent, on a alors $\sum_{x_i\in\mathbb{F}_q} {x_i}^{\alpha_i} = 0$. Finalement, on a $\sum_{x\in{\mathbb{F}_q}^n} S(x) = 0$ dans $\mathbb{F}_q$, ce qui prouve que $p \mid \sum_{x\in{\mathbb{F}_q}^n} S(x)$. □

Leçons possibles
(**109** Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.)
(**110** Nombres premiers. Applications.)

112 Corps finis. Applications.
117 Algèbre des polynômes à n indéterminées ($n \geqslant 2$). Polynômes symétriques. Applications.

Références
Cours d'arithmétique de Serre.