# Théorème de Chevalley–Warning

Arnaud Girand

17 juin 2012

Référence :
- [Ser95], p. 12–13

Soit $p$ un nombre premier et $r \geq 1$ ; on pose $q := p^r$.

**Lemme 1**
*Soit $u \in \mathbb{N}$.*
*On pose :*

$$S(X^u) := \sum_{x \in \mathbb{F}_q} x^u$$

*Alors :*

$$S(X^u) = \begin{cases} -1 & \text{si } u \geq 1 \text{ et } q-1|u \\ 0 & \text{sinon} \end{cases}$$

Démonstration :
- Si $u = 0$, on a $S(X^u) = q \times 1 = 0$, d'où le résultat.
- Si $u \geq 1$ et $q-1|u$, i.e $\exists k \in \mathbb{N}$, $u = (q-1)k$, alors $0^u = 0$ et, par théorème de Lagrange, $\forall x \in \mathbb{F}_q^*$, $x^u = (x^{q-1})^k = 1^k = 1$. De fait, $S(X^u) = q - 1 = 1$.
- Si $u \geq 1$ et $q-1 \nmid u$, alors comme $\mathbb{F}_q^*$ est cyclique d'ordre $q-1$ il existe $y \in \mathbb{F}_q^*$ tel que $y^u \neq 1$ (cf. infra). De fait :

$$\begin{aligned} S(X^u) &= \sum_{x \in \mathbb{F}_q} x^u \\ &= \sum_{x \in \mathbb{F}_q^*} x^u \\ &= \sum_{x \in \mathbb{F}_q^*} (xy)^u \\ &= y^u S(X^u) \end{aligned}$$

De fait $(1 - y^u)S(X^u) = 0$ donc (comme $y^u \neq 1$) $S(X^u) = 0$.

**Proposition 1 (Chevalley–Warning)**
*Soit $A$ un ensemble fini.*
*Soit $(f_\alpha)_{\alpha \in A} \in \mathbb{F}_q[X_1, \ldots, X_n]^A$ telle que :*

$$\sum_{\alpha \in A} \deg(f_\alpha) < n$$

*On considère la courbe algébrique $V := \{\underline{x} \in \mathbb{F}_q^n \,|\, \forall \alpha \in A,\ f_\alpha(\underline{x}) = 0\}$ définie par les $f_\alpha$.*
*Alors :*

$$\operatorname{card}(V) \equiv 0 [p]$$

Démonstration : Commençons par fixer $\underline{x} \in \mathbb{F}_q^n$ et posons :

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

- Si $\underline{x} \in V$, alors il est clair que $P(\underline{x}) = 1$.
- Dans le cas contraire, il existe $\alpha_0 \in A$ tel que $f_{\alpha_0}(\underline{x}) \neq 0$ et donc $f_{\alpha_0}^{q-1}(\underline{x}) = 1$, d'où $P(\underline{x}) = 0$.

De fait $P$ est la fonction caractéristique $\chi_V$ de $V$.

Soit $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ ; on pose :

$$S(f) := \sum_{\underline{x} \in \mathbb{F}_q^n} f(\underline{x})$$

Comme $P = \chi_V$ on a nécessairement $\mathrm{card}(V) \equiv S(P)[p]$. Il nous reste donc à montrer que $S(P) = 0$ dans $\mathbb{F}_q$.

Comme $\sum \deg(f_\alpha) < n$ on a $\deg(P) < n(q-1)$ donc $P$ est combinaison linéaire de monômes $\underline{X^u} := \prod_{i=1}^n X_i^{u_i}$, avec $|\underline{u}| < n(q-1)$. Or :

$$\begin{aligned} S(\underline{X^u}) &= \sum_{\underline{x} \in \mathbb{F}_q^n} \prod_{i=1}^n x_i^{u_i} \\ &= \prod_{i=1}^n \sum_{x \in \mathbb{F}_q} x^{u_i} \\ &= \prod_{i=1}^n S(X^{u_i}) \\ &= 0 \text{ car au moins l'un des } u_i \text{ vérifie } u_i < q-1 \text{ donc } q-1 \nmid u_i \text{ (lemme 1)} \end{aligned}$$

**Détails supplémentaires :**

- *Il existe $y \in \mathbb{F}_q^*$ tel que $y^u \neq 1$ ($u \geq 1$ et $q-1 \nmid u$)* . Dans le cas contraire on aurait, si $y_0$ engendre $\mathbb{F}_q^*$, $y_0^u = 1$ et alors par division euclidienne $u = a(q-1) + r$, avec $0 < r < q-1$. Or ceci impliquerait $y_0^r = 1$ ce qui est absurde car $y_0$ est d'ordre $q-1$.

# Références

[Ser95] Jean-Pierre Serre. *Cours d'arithmétique*. Presses Universitaires de France, 1995.