LE THÉORÈME DE CHEVALLEY-WARNING

par

Stef Graillat

Le théorème de Chevalley-Warning donne une relation de congruence sur le nombre de zéros communs d'un ensemble de polynômes à plusieurs indéterminées sur un corps fini. Il trouve donc naturellement sa place dans les leçons :

- 112 : Corps finis. Applications.
- 116 : Algèbres des polynômes à n indéterminées ($n \geqslant 2$). Polynômes symétriques.

La démonstration que nous donnons ici est tirée de [Ser77, p.13]. On pourra aussi regarder dans [Sam97, p.30].

Soit $\mathbf{K}$ un corps fini, p sa caractéristique et q son cardinal (on a donc $q = p^d$, $d \geqslant 1$).

LEMME. — *Soit m un entier $\geqslant 0$. La somme $S_m = \sum_{x\in\mathbf{K}} x^m$ est égale à -1 si $m \geqslant 1$ et m divisible par $q-1$; elle est égale à 0 sinon.*

Démonstration. — On convient que $x^0 = 1$ même si $x = 0$.
Si $m = 0$, alors tous les termes de la somme valent 1 d'où $S_m = q\cdot 1 = 0$ car $\mathbf{K}$ est de caractéristique p. Si m est $\geqslant 1$ et divisible par $q-1$, on a pour $x \neq 0$, $x^m = 1$. En effet, $\mathbf{K}^\star$ est un groupe multiplicatif d'ordre $q-1$ et donc pour $x \in \mathbf{K}^\star$, $x^{q-1} = 1$. Or $q-1$ divise m, donc il existe $r \in \mathbf{Z}$ tel que $m = r(q-1)$ et $x^m = (x^{q-1})^r = 1^r = 1$ pour $x \neq 0$. On a par convention $0^m = 0$ donc $S_m = (q-1)\cdot 1 = -1$. Enfin, si m est $\geqslant 1$ et non divisible par $q-1$, le fait que $\mathbf{K}^\star$ soit cyclique d'ordre $q-1$ montre qu'il existe $y \in \mathbf{K}^\star$ tel que $y^m \neq 1$ (En effet, si pour tout $y \in \mathbf{K}^\star$, on a $y^m = 1$ alors c'est vrai pour y un générateur de $\mathbf{K}^\star$; y étant d'ordre $q-1$ on en déduit que $q-1$ divise m ce qui est exclu.). L'application $\varphi : \mathbf{K}^\star \to \mathbf{K}^\star$, $x \mapsto yx$ est une bijection. Donc

$$S_m = \sum_{x\in\mathbf{K}^\star} x^m = \sum_{x\in\mathbf{K}^\star} (yx)^m = \sum_{x\in\mathbf{K}^\star} y^m x^m = y^m \sum_{x\in\mathbf{K}^\star} x^m = y^m S_m.$$

D'où $(1-y^m)S_m = 0$ et donc $S_m = 0$ car nous avions choisi y tel que $y^m \neq 1$. □

THÉORÈME (Chevalley-Warning). — *Soient $P_1,\dots,P_r$ une famille de polynômes appartenant à $\mathbf{K}[X_1,\dots,X_n]$ tels que $\sum_{i=1}^r \deg P_i < n$ et soit V l'ensemble de leurs zéros communs dans $\mathbf{K}^n$, $V = \{x \in \mathbf{K}^n ; P_1(x) = \cdots = P_r(x) = 0\}$. On a $\operatorname{card} V \equiv 0 \pmod p$.*

Démonstration. — Notons $P = \prod_{i=1}^r (1 - P_i^{q-1})$. Soit $x \in \mathbf{K}^n$. Si $x \in V$ alors $P_i(x) = 0$ pour tout $i = 1,\dots,r$ et donc $P(x) = 1$. Si maintenant $x \notin V$, soit i tel que $P_i(x) \neq 0$. Comme $P_i(x) \in \mathbf{K}^\star$, on a $P_i(x)^{q-1} = 1$ et donc $P(x) = 0$. Ainsi P est « la fonction caractéristique » de V. Notons pour $Q \in \mathbf{K}[X_1,\dots,X_n]$, $S(Q) = \sum_{x\in\mathbf{K}^n} Q(x)$. On a alors $S(P) = \sum_{x\in V} 1 \equiv \operatorname{card} V \pmod p$. Il nous suffit

donc de montrer que S(P) = 0. Pour ce faire, on écrit $P = \sum_{m\in\mathbf{N}^n} c_m X_1^{m_1}\dots X_n^{m_n}$. Par définition, on a

$$\begin{aligned} S(P) &= \sum_{x\in\mathbf{K}^n}\sum_{m\in\mathbf{N}^n} c_m x_1^{m_1}\dots x_n^{m_n} \quad \text{ou} \quad x=(x_1,\dots,x_n)\in\mathbf{K}^n \\ &= \sum_{x\in\mathbf{K}^n} c_m \sum_{m\in\mathbf{N}^n} x_1^{m_1}\dots x_n^{m_n} \\ &= \sum_{m\in\mathbf{N}^n} c_m S_{m_1}\dots S_{m_n}. \end{aligned}$$

L'hypothèse $\sum_{i=1}^r \deg P_i < n$ entraîne que $\deg P < n(q-1)$ car $\deg P = (q-1)\sum_{i=1}^r \deg P_i$. Soit $m\in\mathbf{N}^n$ avec $c_m\neq 0$. Puisque $\deg P < n(q-1)$, on a $\sum_{i=1}^r m_i < n(q-1)$; donc l'un au moins des m_i est $< q-1$. D'après le lemme $S_{m_i}=0$ et par suite $S(P)=0$. □

COROLLAIRE. — *Si* $\sum_{i=1}^r \deg P_i < n$ *et si les* P_i *sont sans terme constant, les* P_i *ont un zéro commun non trivial.*

Démonstration. — Comme les P_i sont sans terme constant, $0\in V$ (ici $0=(0,\dots,0)$). Si $V=\{0\}$ alors $\operatorname{card} V = 1$ et $\operatorname{card} V$ ne serait pas divisible par p. □

Le théorème de Chevalley-Warning a été généralisé par Ax par le cas $r=1$ dans [**Ax64**] et par Katz pour r quelconque dans [**Kat71**]. Leurs démonstrations sont plutôt complexes. On trouva dans [**Wan95**] une démonstration « plus simple » (mais toujours complexe).

THÉORÈME (Ax-Katz). — *Soient* $P_1,\dots,P_r$ *une famille de polynômes appartenant à* $\mathbf{K}[X_1,\dots,X_n]$ *tels que* $\sum_{i=1}^r \deg P_i < n$ *et soit* V *l'ensemble de leurs zéros communs dans* $\mathbf{K}^n$, $V=\{x\in\mathbf{K}^n\,;P_1(x)=\dots=P_r(x)=0\}$. *Si* b *désigne le plus petit entier tel que*

$$b \geqslant \frac{n-\sum_{i=1}^r \deg P_i}{\max\limits_{i=1,\dots,r}\deg P_i},$$

alors $\operatorname{card} V$ *est divisible par* q^b.

On peut montrer que ce résultat est optimal en ce sens que pour chaque n et pour tous degrés $(d_1,\dots,d_r)$ il existe un ensemble de polynômes $P_1,\dots,P_r$ de $\mathbf{K}[X_1,\dots,X_n]$ vérifiant $\deg P_i = d_i$ et telle que la plus grande puissance de q divisant $\operatorname{card} V$ soit exactement q^b.

Références

[Ax64] J. AX – « Zeroes of polynomials over finite fields », *Amer. J. Math.* **86** (1964), p. 255–261.

[Kat71] N. M. KATZ – « On a theorem of Ax », *Amer. J. Math.* **93** (1971), p. 485–499.

[Sam97] P. SAMUEL – *Théorie algébrique des nombres*, Hermann, 1997.

[Ser77] J.-P. SERRE – *Cours d'arithmétique*, Presse Universitaire de France, 1977.

[Wan95] D. Q. WAN – « A Chevalley-Warning approach to p-adic estimates of character sums », *Proc. Amer. Math. Soc.* **123** (1995), no. 1, p. 45–54.

9 décembre 2004

STEF GRAILLAT, Université de Perpignan, 52, avenue Paul Alduy, F-66860 Perpignan Cedex

E-mail : graillat@univ-perp.fr • *Url :* http://gala.univ-perp.fr/~graillat