Théorème de Chevalley-Warning

Leçons: 120, 123, 126, 144

Références: Serre p 12-13, Zavidovique p 32

Théorème Chevalley-Warning Soient k un corps fini à $q = p^n$ éléments et $m \in \mathbb{N}^*$. Soit A un ensemble fini et $(f_\alpha)_{\alpha \in A}$ une famille de polynômes de $k[X_1, \dots, X_m]$ telle que

$$\sum_{\alpha \in A} \deg f_\alpha < m.$$

Soit V l'ensemble des racines communes aux polynômes f_α, alors $\#V = 0 \ [p]$

Lemme: $u \in \mathbb{N}$, alors $\sum_{x \in k} x^u = \begin{cases} -1 \text{ si } u \geq 1 \text{ et } q-1 \text{ divise } u \\ 0 \text{ sinon.} \end{cases} =: S(X^u)$

Dém: Si $u = 0$, $\sum_{x \in k} x^u = q = 0$. Si $u \geq 1$ est divisible par $q-1$,

Serre p 12

$$\sum_{x \in k} x^u = 0^u + \sum_{x \in k^\times} \underbrace{x^u}_{=1 \text{ par Lagrange}} = q - 1 = -1.$$

Si enfin $u \geq 1$ est non divisible par $q-1$, comme $k^\times$ est cyclique d'ordre $q-1$, il existe $y \in k^\times$ tq $y^u \neq 1$. On a donc

$$\sum_{x \in k^\times} x^u = \sum_{x \in k^\times} (yx)^u = y^u \sum_{x \in k^\times} x^u \text{ donc par intégrité, } \sum_{x \in k^\times} x^u = 0. \quad \square$$

Démo: On considère le polynôme $P(X_1, \dots, X_m) = \prod_{\alpha \in A} (1 - f_\alpha^{q-1}(X_1, \dots, X_m))$.

On commence par remarquer que P est la fonction indicatrice de V:

Serre p 13

- si $x \in V \subset k^m$, on a $f_\alpha(x) = 0 \ \forall \alpha \in A$ d'où $P(x) = 1$.
- si $x \in k^m - V$, il existe $\alpha \in A$ tq $f_\alpha(x) \neq 0$ et dans ce cas, le théorème de Lagrange donne $f_\alpha^{q-1}(x) = 1$ et donc $P(x) = 0$.

Si pour tout polynôme f, on pose $S(f) = \sum_{x \in k^m} f(x)$, on a donc $S(P) = \sum_{x \in k^m} P(x)$ donc en réduisant mod p, $S(P) = \#V \bmod p$.

car $P = \mathbb{1}_V$

Par hypothèse sur les degrés des f_α, on a $\deg P = \sum_{\alpha \in A} (q-1) \deg f_\alpha$

$< m(q-1)$

donc P est combinaison linéaire de monômes $X^u = X_1^{u_1} \cdots X_m^{u_m}$ où $\sum_{i=1}^{m} u_i < m(q-1)$

$$P = \sum_{|u| < m(q-1)} \alpha_u X^u \quad \text{avec } \alpha_u \in k. \text{ Ainsi}$$

$$S(P) = \sum_{x \in k^m} \sum_{|u| < m(q-1)} \alpha_u x^u = \sum_{|u| < m(q-1)} \alpha_u \underbrace{\sum_{x \in k^m} x^u}_{= S(X^u)}$$

voir éventuellement Zavidovique p35

On $S(X^u) = \sum_{(x_1, \dots, x_m) \in k^m} x_1^{u_1} \cdots x_m^{u_m} = \left(\sum_{x_1 \in k} x_1^{u_1}\right) \cdots \left(\sum_{x_m \in k} x_m^{u_m}\right)$

$$= \prod_{j=1}^{m} S(X^{u_j})$$

On $\sum_{i=1}^{m} u_i < m(q-1)$ donc par principe des tiroirs $\exists u_i < q-1$

et d'après le lemme, pour un tel u_i, $S(X^{u_i}) = 0$ donc $S(X^u) = 0$.

d'où $S(P) = 0$

et enfin $\#V \equiv S(P) \equiv 0 \mod p$. □

Théorème Erdös-Ginzburg-Ziv Soit $n \in \mathbb{N}^*$, alors parmi $2n-1$ entiers $a_1, \dots, a_{2n-1}$, on peut toujours en trouver n dont la somme est divisible par n.

Dém: On commence par le montrer pour un nombre premier p. Soient pour cela $a_1, \dots, a_{2p-1}$ des entiers et considérons les deux polynômes de $\mathbb{F}_p[X_1, \dots, X_{2p-1}]$ suivants (Zavidovique.) :

$$\begin{cases} P_1(X_1, \dots, X_{2p-1}) = \sum_{k=1}^{2p-1} X_k^{p-1} \\ P_2(X_1, \dots, X_{2p-1}) = \sum_{k=1}^{2p-1} \overline{a_k} X_k^{p-1} \end{cases}$$

vérifiant ainsi $\deg P_1 + \deg P_2 = 2p-2 < 2p-1$. Comme ils ont $(0, \dots, 0)$ pour racine commune évidente, le théorème de Chevalley-Warning assure en outre qu'ils possèdent une racine commune $(x_1, \dots, x_{2p-1})$

non triviale.

Par ailleurs, d'après le théorème de Lagrange, pour $x \in \mathbb{F}_p$, on a $x^{p-1} = 1$ si et seulement si x est non nul donc si on note W l'ensemble des indices i pour lesquels x_i est non nul, on obtient :

$$0 = P_1(x_1, \dots, x_{2p-1}) = \sum_{i \in W} \overline{x_i^{p-1}} = \#W \bmod p$$

$(x_1, \dots, x_{2p-1}) \neq (0, \dots, 0)$ donc $W \neq \phi$

Ainsi $\#W$ est un entier divisible par p vérifiant $1 \leq \#W \leq 2p-1$, ce qui impose $\#W = p$. On note donc $W = \{i_1, \dots, i_p\}$. On a alors

$$0 = P_2(x_1, \dots, x_{2p-1}) = \sum_{i \in W} \overline{a_i x_i^{p-1}} = \sum_{j=1}^{p} \overline{a_{i_j}}$$

autrement dit p divise la somme $a_{i_1} + \dots + a_{i_p}$: c'est ce qu'on voulait.

D'après le théorème fondamental de l'arithmétique, il suffit de montrer que si m et n sont deux entiers pour lesquels on a le résultat, celui-ci reste vrai pour mn. On considère $a_1, \dots, a_{2mn-1}$ entiers.

Comme le résultat est vrai pour n, il existe $I_1 \subset \{1, \dots, 2mn-1\}$ de cardinal n tel que

$$\sum_{i \in I_1} \overline{a_i} \equiv 0 \bmod n$$

De même, il existe $I_2 \subset \{1, \dots, 2mn-1\} - I_1$ de cardinal n tel que

$$\sum_{i \in I_2} a_i \equiv 0 \bmod n.$$

On termine ce procédé après avoir construits l'ensemble d'indices I_{2m-1} car au bout de $2m-2$ étapes, il reste

$$2mn - 1 - (2m-2)n = 2n - 1 \text{ entiers.}$$

Pour $j \in \{1, \dots, 2m-1\}$, on considère l'entier c_j pour lequel on a

$$\sum_{i \in I_j} a_i = c_j n.$$

Comme le résultat est aussi vrai pour n, il existe $J \subset \{1, \dots, 2n-1\}$ de cardinal n tel que $\sum_{j \in J} c_j \equiv 0 \mod n$.

On a alors $\sum_{j \in J} \underbrace{\sum_{i \in I_j} a_i}_{\text{somme de } n \text{ entiers}} = n \left(\sum_{j \in J} c_j \right) \equiv 0 \mod n^n$

car $\#J = n$ et $\#I_j = n \ \forall j \in J$. □

NB: La quantité $2n-1$ est optimale : parmi $2n-2$ entiers, il peut ne pas en exister n dont la somme soit divisible par n.

Exemple : $\underbrace{0, \dots, 0}_{n-1}, \underbrace{1, \dots, 1}_{n-1}$