Titre : Théorèmes de Chevalley Warning et Erdös Ginzburg Ziv
Recasages : 120,123,142,144,190
Thème : Arithmétique
Références : Zavidovique - Un max de maths

Théorème 1. *(Chevalley Warning) On fixe $q = p^k$ une puissance de nombre premier et $K = \mathbb{F}_q$. Soit $(f_a)_{a\in A}$ une famille de polynômes de $K[X_1, \cdots, X_n]$ tels que*

$$\sum_{a\in A} d^\circ f_a < n$$

On pose $V \subset K^n$ l'ensemble des zéros communs à tous les f_a. On a

$$|V| \equiv 0[p]$$

On pose

$$P = \prod_{a\in A} \left(1 - f_a^{q-1}\right)$$

On remarque que $P(x) = 1$ si $x \in V$, et si $x \notin V$, l'un des $f_a(x)$ est non nul. Comme K^* ests cyclique d'ordre $q-1$, $f_a^{q-1}(x) = 1$ et $P(X) = 0$. Ainsi, $P = \mathbb{1}_V$, finalement, on pose

$$\forall f \in K[X_1, \cdots, X_n], S(f) := \sum_{x\in K^n} f(x) \in K$$

On a donc $|V| \equiv S(P)[p]$. Il suffit de montrer que $S(P) = 0$ dans K. Comme $\sum d^\circ f_a < n$, on a $d^\circ P < n(q-1)$, donc P est combinaison linéaire de monômes de la forme

$$X^u = X_1^{u_1} \cdots X_r^{u_r} \quad \text{avec} \quad \sum_{i=1}^{n} u_i < n(q-1)$$

il suffit de prouver que pour un tel monôme, on a $S(X^u) = 0$. Par le principe des tiroirs, il existe $i \in [\![1, n]\!]$ tel que $u_i < q-1$. On calcule

$$S(X^u) = S(X_i^{u_i}) S(X_1^{u_1} \cdots \widehat{X_i^{u_i}} \cdots X_n^{u_m})$$

Si $y \in K^*$ est un générateur de K^*, on a

$$S(X_i^{u_i}) = \sum_{x\in K^*} x^{u_i} = \sum_{x\in K^*} (yx)^{u_i} = y^{u_i} \sum_{x\in K^*} x^{u_i} = y^{u_i} S(X^{u_i})$$

Comme $u_i < q-1$, $y^{u_i} \neq 1$ et donc $S(X^{u_i}) = 0$ d'où $S(X^u) = 0$ et le résultat.

Théorème 2. *(Erdös Ginzburg Ziv)*
Soient $n \in \mathbb{N}^*$, parmi $2n-1$ entiers $a_1, \cdots, a_{2n-1}$, on peut toujours en choisir n dont la somme est divisible par n.

On traite dans un premier temps le cas où $p := n$ est un nombre premier. On se place dans $K = \mathbb{F}_p$, on pose

$$P_1(X_1, \cdots, X_{2n-1}) := \sum_{i=1}^{2p-1} X_i^{p-1} \quad \text{et} \quad P_2(X_1, \cdots, X_{2p-1}) = \sum_{i=1}^{2p-1} \overline{a_i} X_i^{p-1}$$

Par le théorème de Chevalley Warning, comme 0 est une racine commune de ces polynômes, il existe au moins p racines communes, prenons $(x_1, \cdots, x_{2p-1})$ une telle racine non triviale.

1) Pour $i \in [\![1, 2p-1]\!]$, on a $x_i^{p-1} = 0$ ou 1 dans K suivant si $x_i = 0$ ou non. Donc $P_1(x) = 0$ si et seulement si il existe p ou 0 coordonnées non nulles dans x. Comme $x \neq 0$, il existe exactement p indices $i_1, \cdots, i_p$ avec $x_{i_k} \neq 0$ pour $k \in [\![1, p]\!]$.

2) Le deuxième polynôme nous donne alors

$$0 = P_2(x_1, \cdots, x_{2p-1}) = \sum_{k=1}^{p} \overline{a_{i_k}}$$

Ce qui est bien le résultat voulu

Revenons en au cas général, que l'on traite par récurrence sur n : Le cas $n = 1$ est vide, ensuite, supposons le résultat acquis pour $d < n$. Si n est premier, on conclut par l'étape 1, dans le cas contraire, on écrit $n = pn'$ avec p premier (et donc $p, n' < n$).

1) On écrit $2n - 1 = (2n' - 1)p + p - 1$, par hypothèse de récurrence, on peut construire $2n' - 1$ sous-ensembles de $\{a_1, \cdots, a_{2n-1}\}$ disjoints avec, $\forall i \in [\![1, 2n' - 1]\!]$, E_i est de cardinal p et la somme de ses éléments est divisible par p.

2) Pour $i \in [\![1, 2n' - 1]\!]$, on note s_i la somme des éléments de E_i et $s_i = ps'_i$. On applique notre hypothèse de récurrence sur $s'_1, \cdots, s'_{2n'-1}$: il existe $k_1, \cdots, k_{n'} \in [\![1, 2n' - 1]\!]$ tels que n' divise $\sum_{i=1}^{n'} s'_{k_i}$.

3) On considère enfin $\bigcup_{j=1}^{n'} E_{k_j} \subset \{a_1, \cdots, a_{2n'-1}\}$ de carcinal $pn' = n$ et donc la somme des éléments vaut

$$\sum_{j=1}^{n'} s_{k_j} = p \sum_{j=1}^{n} s'_{k_j}$$

et est divisible par $pn' = n$.