

# LA FAMEUX THÉORÈME DE CHEVALLEY-WARNING EN TANT QU'ÉTAPE PRÉLIMINAIRE À LA PREUVE DU THÉORÈME D'ERDÖS-GINZBURG-ZIV.

$\mathbf{K}$  désigne un corps fini de cardinal  $q = p^\alpha$ .

**Théorème** (Chevalley-Warning). *Soit  $(f_a)_{a \in A}$  une famille de polynômes de  $\mathbf{K}[X_1, \dots, X_m]$ , indexée par un ensemble  $A$ . On suppose que les degrés de ces polynômes vérifient :*

$$\sum_{a \in A} \deg(f_a) < m.$$

*On pose  $V \subset K^m$  l'ensemble des points où tous les  $f_a$  s'annulent simultanément. Le cardinal de  $V$  vérifie :*

$$\text{card}(V) \equiv 0 \pmod{p}.$$

PREUVE. On considère le polynôme :

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

et on va faire ça progressivement :

- (1) Il est clair que  $P(x) = 1_{\mathbf{K}}$  si  $x \in V$  et s'il existe  $a \in A$  tel que  $f_a(x) \neq 0$  alors, puisque que  $\mathbf{K}^\times$  est cyclique d'ordre  $q-1$ , on a  $f_a^{q-1}(x) = 1_{\mathbf{K}}$  et donc  $P(x) = 0_{\mathbf{K}}$ . Finalement, en définissant  $S(f) := \sum_{x \in K^m} f(x) \in \mathbf{K}$  pour tout polynôme  $f \in \mathbf{K}[X_1, \dots, X_m]$ , on a :

$$S(P) = \sum_{x \in \mathbf{K}^m} P(x) = \text{card}(V)1_{\mathbf{K}}.$$

- (2) On va montrer que  $S(P) = 0_{\mathbf{K}}$ . D'abord, la condition  $\sum_{a \in A} \deg(f_a) < m$  entraîne  $\deg(P) < m(q-1)$ . Il suffit donc de montrer  $S(X^u) = 0_{\mathbf{K}}$  pour tout multi-indice  $u = (u_1, \dots, u_m)$  tel que  $\sum_{i=1}^m u_i < m(q-1)$ . Par le principe des tiroirs, il existe un indice  $i$  tel que  $u_i < q-1$ . On calcule :

$$S(X^u) = S(X_i^{u_i})S(X_1^{u_1} \dots \hat{X}_i^{u_i} \dots X_m^{u_m}).$$

- (3) Ah oui, mais si  $y \in \mathbf{K}^\times$  est un générateur de  $\mathbf{K}^\times$  et avec la convention  $0^0 = 0$  :

$$S(X_i^{u_i}) = \sum_{x \in \mathbf{K}} x^{u_i} = \sum_{x \in \mathbf{K}^\times} (yx)^{u_i} = y^{u_i} S(X_i^{u_i}).$$

Comme  $u_i < q-1$ , on est sûr que  $y^{u_i} \neq 1_{\mathbf{K}}$  et donc  $S(X_i^{u_i}) = 0 = S(X^u)$ .

- (4) En conclusion, on a montré :

$$\text{card}(V)1_{\mathbf{K}} = 0_{\mathbf{K}}$$

et comme  $\mathbf{K}$  est de caractéristique  $p$ , on a bien :

$$\text{card}(V) \equiv 0 \pmod{p}.$$

□

**Théorème** (Erdős-Ginzburg-Ziv). *Soit  $n \in \mathbf{N}$ . Parmi  $2n - 1$  entiers  $a_1, \dots, a_{2n-1}$ , on peut toujours en trouver  $n$  dont la somme est divisible par  $n$ . En plus, c'est optimal.*

PREUVE. Il faut commencer par :

*Étape 1. Le cas où l'entier  $n$  est premier auquel cas il sera noté  $p$ .*

On se place dans le corps  $K = \mathbf{F}_p$  et notera  $\bar{a}$  la classe modulo  $p$  de  $a \in \mathbf{N}$ . On va appliquer le théorème de Chevalley-Waring avec les polynômes :

$$P_1(X_1, \dots, X_{2p-1}) = \sum_{i=1}^{2p-1} X_i^{p-1} \quad \text{et} \quad P_2(X_1, \dots, X_{2p-1}) = \sum_{i=1}^{2p-1} \bar{a}_i X_i^{p-1}.$$

Puisque  $0 \in \mathbf{K}^{2p-1}$  est une racine commune à ces polynômes, on est assuré de l'existence d'une racine non triviale notée  $(x_1, \dots, x_{2p-1})$ . Il y a deux choses à voir :

- (1) D'abord comme  $x_i^{p-1} = 1_{\mathbf{K}}$  si  $x_i \neq 0_{\mathbf{K}}$  et  $x_i^{p-1} = 0_{\mathbf{K}}$  sinon, on en déduit (toujours car  $\mathbf{K}$  est de caractéristique  $p$ ) que la relation  $P_1(x_1, \dots, x_{2p-1}) = 0_{\mathbf{K}}$  implique qu'il existe très exactement  $p$  éléments  $x_{n_1}, \dots, x_{n_p}$  non nuls.
- (2) C'est fini en considérant la deuxième relation  $P_2(x_1, \dots, x_{2p-1}) = 0_{\mathbf{K}}$  puisque :

$$0_{\mathbf{K}} = P_2(x_1, \dots, x_{2p-1}) = \sum_{i=1}^p \bar{a}_{n_i} x_{n_i}^{p-1} = \sum_{i=1}^p \bar{a}_{n_i}.$$

*Étape 2. Le cas général où l'entier  $p$  redevient  $n \in \mathbf{N}$ .*

On va procéder par récurrence (forte) sur  $n \in \mathbf{N}$ . L'initialisation pour  $n = 1$  n'est pas difficile. Supposons donc le résultat montré jusqu'au rang  $n - 1$ ,  $n \geq 1$ . Si  $n$  est premier, c'est l'étape 1, sinon on écrit  $n = pn'$  avec  $p$  premier et  $n' < n$ .

- (1) On écrit  $2n - 1 = (2n' - 1)p + p - 1$  et par hypothèse de récurrence on peut construire  $(2n' - 1)$  sous-ensembles disjoints de  $E := \{a_1, \dots, a_{2n-1}\}$  de la façon suivante : pour  $i \in \{1, \dots, 2n' - 1\}$ ,  $E_i \subset E \setminus (E_1 \cup \dots \cup E_{i-1})$  est de cardinal  $p$  et la somme de ses éléments est divisible par  $p$ . À la fin,  $E \setminus (E_1 \cup \dots \cup E_{2n'-1})$  est de cardinal  $p - 1$  et on ne peut plus continuer.
- (2) Pour  $i \in \{1, \dots, 2n' - 1\}$ , on note  $s_i$  la somme des éléments de  $E_i$  et  $s_i = ps'_i$ . On applique encore l'hypothèse de récurrence avec les  $s'_i$  : il existe  $k_1, \dots, k_{n'}$  tel que  $n'$  divise  $s'_1 + \dots + s'_{k_{n'}}$ .
- (3) Pour conclure, il suffit de considérer le sous-ensemble

$$\bigcup_{j=1}^{n'} E_{k_j} \subset \{a_1, \dots, a_{2n-1}\}$$

qui est de cardinal  $pn' = n$  et dont la somme de ses éléments vaut

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

qui est divisible par  $pn' = n$ .

*Étape 3. Le résultat est optimal.*

On considère  $(2n - 2)$  entiers parmi lesquels  $(n - 1)$  valent 0 et  $(n - 1)$  valent 1. On ne peut pas trouver  $n$  éléments dont la somme soit divisible par  $n$ , puisqu'elle est toujours inférieure à  $n$  et strictement positive.  $\square$

**Références.** M. Zavidovique, *Un Max de Maths*

**120** Anneaux  $\mathbf{Z}/n\mathbf{Z}$ . Applications.

**121** Nombres premiers. Applications.

**123** Corps finis. Applications.

**142** Algèbre des polynômes à plusieurs indéterminées. Applications.

**144** Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications