142

Algèbre des polynômes à plusieurs indéterminées. Applications.

Cadre : A anneau commutatif unitaire, K un corps commutatif, $n \geq 2$

I- Polynômes à n-indéterminées

[RDO 185] 1°/ Algèbre $A[X_1 \dots X_n]$

Déf 1 : On appelle polynôme à n-indéterminées sur A toute famille presque nulle d'élément de A indexée par $\mathbb{N}^n$: $P = (a_i)_{i \in \mathbb{N}^n}$. On note $A[X_1 \dots X_n]$ les polynômes à n-indéterminées à coefficient dans A.

Déf 2 : Soient $P = (a_i)_{i \in \mathbb{N}^n}$ et $Q = (b_i)_{i \in \mathbb{N}^n}$ deux polynômes de $A[X_1 \dots X_n]$ et $\lambda \in A$. On définit :

* $P + Q = (a_i + b_i)_{i \in \mathbb{N}^n}$
* $P \cdot Q = (\sum_{k+l=i} a_k b_l)_{i \in \mathbb{N}^n}$
* $\lambda \perp P = (\lambda a_i)_{i \in \mathbb{N}}$

Thm 3 : $(A[X_1 \dots X_n], +, \cdot, \perp)$ est une A-algèbre commutative

Thm 4 : Tout polynôme P de $A[X_1 \dots X_n]$ peut s'exprimer de façon unique comme CL de la famille : $(X_1^{i_1} \dots X_n^{i_n})_{(i_1, \dots, i_n) \in \mathbb{N}^n}$

Exemple 5 : $P = (a_i)_{i \in \mathbb{N}^n}$ s'écrit $P = \sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} a_{i_1 \dots} a_{i_n} X_1^{i_1} \dots X_n^{i_n}$

[RDO 183] Thm 6 : $A[X_1 \dots X_n] \simeq A[X_1 \dots X_{n-1}][X_n]$

Appl 7 : Si A ann. intègre, $A[X_1 \dots X_n]$ est un ann. intègre

Exemple 8 : * le déterminant est un polynôme en ts ces coefficients.
* la trace est un polynôme en $(m_{ii})_{1 \leq i \leq n}$
* le polynôme caractéristique χ_A

2°/ Degré et polynôme homogène

Déf 9 : Soit $1 \leq q \leq n$ et $P \in A[X_1 \dots X_n]$. On appelle degré partiel du polynôme P en l'indéterminée X_q, le degré de ce polynôme considéré comme un élt de $A[X_1, \dots X_n][X_q]$. On le note $\deg_{X_q}(P)$.

Ex 10 : $P = 5 - 5X^2 - 3X^5 + Y + X^2Y^7 - Y^8$

$\deg_X(P) = 5$ et $\deg_Y(P) = 8$

Déf 11 : Soit $P = (a_i)_{i \in \mathbb{N}^n}$ un polynôme de $A[X_1 \dots X_n]$

* Si $P \neq 0$, l'ens. $\{ \sum_{k=1}^{n} i_k,\ i = (i_1, \dots i_n) / a_i \neq 0 \}$ admet un plus grand élt qui est le degré total de P, noté $\deg(P)$.
* Si $P = 0$, $\deg(P) = -\infty$

Exemple 12 : $\deg(P) = 9$

Prop 13 : Soient $P, Q \in A[X_1 \dots X_n]$

* $\deg(P+Q) \leq \sup(\deg P, \deg Q)$
* $\deg(P \cdot Q) \leq \deg(P) + \deg(Q)$

Déf 14 : Un polynôme homogène de degré d en n variables est un polynôme vérifiant : $\forall T, X_1, \dots, X_n \in A[X_1 \dots X_n, T]$

$P(TX_1, \dots, TX_n) = T^d P(X_1, \dots, X_n)$

Rmq 15 : Pour un polynôme d-homogène non nul, d n'est autre que le degré total.

Ex 16 : $P(X,Y,Z) = X^3 + X^2Y + Y^2Z + Z^3 + XYZ$ est 3-homogène.

Prop 17 : Si deux polynômes de $A[X_1, \dots, X_n]$ sont respectivement p-homogènes et q-homogène alors leur produit est (p+q)-homogène

Classification des polynômes homogènes de degré ≤ 2 :
- degré 0 : les constantes $\lambda \in A$
- degré 1 : les formes linéaires
- degré 2 : les formes quadratiques

Thm 18 : Le sous-ens. V_d de $A[X_1, \dots, X_n]$ constitués par les polynômes d-homogène est un sous-module.
$A[X_1 \dots X_n]$ est en somme directe avec la famille de sous module $(V_p)_{p \in \mathbb{N}}$

Appl 19 : Soit A un ann. intègre. Soient $P, Q \in A[X_1 \dots X_n]$
$\deg(P \cdot Q) = \deg(P) + \deg(Q)$ mal placé

Appl 20 : Thm de Molien
Soit G un sg fini de $GL_n(\mathbb{C})$. Alors $G \curvearrowright \mathbb{C}[X_1 \dots X_n]$ via $\forall A \in G, \forall P \in \mathbb{C}[X_1, \dots, X_n]$ $A \cdot P = P(A^{-1}(X_1 \dots X_n))$
On considère la restriction de cette action à l'espace V_d.
On a : $\frac{1}{|G|} \times \sum_{A \in G} \frac{1}{\det(I - tA)} = \sum_{d \geq 0} \dim(V_d^G)\, t^d$

DVPT 1

3°/ Propriétés arithmétiques (A ann. intègre)

$\mathbb{K}[X_1..X_n]$ est intègre. Les résultats de la divisibilité sur les Ann. intègre s'appliquent donc à $\mathbb{K}[X_1...X_n]$. La principale différence entre $\mathbb{K}[X]$ et $\mathbb{K}[X_1..X_n]$ est l'absence de div. euclidienne ds $\mathbb{K}[X_1..X_n]$

<u>Prop 21</u>: Pour $n\geq 2$, l'ann. $\mathbb{K}[X_1..X_n]$ n'est pas principal.

<u>Thm 22</u>: (thm de transfert)
Si A est un ann. factoriel, $A[X_1,..,X_n]$ est un ann. factoriel.
$\hookrightarrow$ * existence du PGCD et PPCM
* thm de Gauss
* lemme d'euclide

<u>Prop 23</u>: Dans $A[X_1..X_n]$ intègre, on a $B \in A[X_1,..,X_{n-1}]$
$X_n - B \mid P \iff A(X_1,..,X_{n-1},B) = 0$

<u>Ex 24</u>: Dans $\mathbb{Q}[X,Y,Z]$, $Z^3+X^3+Y^3+mXYZ$ est divisible par $X+Y+Z$ ssi $m=-3$

<u>Cor 25</u>: Soit $A\in A[X_1..X_n]$.
$\prod_{1\leq i<j\leq n}(X_j-X_i) \mid A \iff \forall 1\leq i<j\leq n \quad X_j-X_i \mid A$

<u>App 26</u>: Calcul du déterminant de Vandermonde

II - Fonction polynôme

1°/ Définitions

<u>Prop 27</u>: (Propriété universelle)
A ann. commutatif, alors pour tout A-algèbre B commutative et pour tout n-uplet $(b_1,..,b_n)\in B^n$, il existe un unique morph. de A-algèbre $f: A[X_1,..,X_n] \longrightarrow B$
$X_i \longmapsto b_i \quad \forall i\in\{1...n\}$

<u>Déf 28</u>: Soit $P=\sum_{i\in\mathbb{N}^n} a_i X_1^{i_1}...X_n^{i_n} \in A[X_1..X_n]$ alors l'appl. $\tilde{P}: A^n \longrightarrow A$, $(x_1,..,x_n) \longmapsto \sum a_i x_1^{i_1}...x_n^{i_n}$ est appelée <u>fonction polynôme</u> associée au polynôme P.

<u>Prop 29</u>: Supposons A intègre infini, soient $(A_i)_{i\in[\![1,n]\!]}$ des parties infini de A. Si $\tilde{P}$ s'annule en tout point de $\prod_{i=1} A_i$, alors $P=0$

⚠ ce résultat est faux pour des corps finis

<u>Prop 30</u>: Soit A ann. intègre.
$A[X_1..X_n] \longrightarrow F(A^n,A)$ est injective ssi $card(A)=+\infty$
$P \longmapsto \tilde{P}$

<u>App 31</u>: Soit K' un corps infini et L une extension de K'.
Soient $(A,B)\in \mathcal{M}_n(K')$ deux matrices semblables sur L
Alors A et B semblables sur K'

2°/ Corps fini

Soient q une puissance d'un nbr premier et $\mathbb{F}_q$ un corps à q élts.

<u>Thm 32</u>: (Chevalley - Warning) souvent pris en dvlpt
Soient $P_1,..,P_r \in \mathbb{F}_q[X_1,..,X_n]$ vérifiant $\sum_{i=1}^{r} deg(P_i) < n$
Alors en notant $V=\{x\in\mathbb{F}_q^n \,/\, P_1(x)=...=P_r(x)=0\}$, on a
$|V| \equiv 0[p]$

<u>Appl. 33</u>: (Thm Erdös- Ginzburg-Ziv) **DVPT 2**
Soit $n\in\mathbb{N}^*$ et $a_1,..,a_{2n-1}$ des entiers
Alors il existe des indices $i_1,..,i_n \in\{1,..,2n-1\}$ tels que
$a_{i_1}+..+a_{i_n} \equiv 0[n]$

<u>Cor 34</u>: Avec les mêmes notations et si les P_i sont sans termes constants, alors ils ont un zéro commun non trivial

3°/ Corps $\mathbb{R}$ ou $\mathbb{C}$

<u>Prop 35</u>: Si $F_1, F_2 \in \mathbb{K}[X_1,..X_n]$ ($\mathbb{K}=\mathbb{R}$ ou $\mathbb{C}$) tels que les fonctions polynômes coïncident sur un ouvert non vide de $\mathbb{K}^n$
Alors $F_1=F_2$

<u>Appl. 36</u>: $\forall A\in\mathcal{M}_n(\mathbb{C})$ $\chi_A(A)=0$ (Cayley- Hamilton)

<u>Appl. 37</u>: $\forall A,B\in\mathcal{M}_n(\mathbb{C})$ $\chi_{AB}=\chi_{BA}$

III- Polynômes symétriques

1°/ Définitions

[RDO 100] Déf 38 : Un polynôme $P \in A[X_1 \dots X_n]$ est symétrique ssi $\forall \sigma \in S_n \quad P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n)$

Rmq 39 : les polynômes symétriques sont stables par $+$ et $\times$ et forment un sous ann. de l'anneau des polynômes.

Déf/Prop 40 : Dans $A[X_1, \dots, X_n]$, les n polynômes Σ_p $1 \leq p \leq n$ définis par $\Sigma_p = \sum_{1 \leq i_1 < i_2 < \dots < i_p \leq n} X_{i_1} \dots X_{i_p}$ sont symétriques et portent le nom de polynômes symétriques élémentaires.

Rmq 41 : Σ_p est p-homogène et le degré partiel par rapport à chaque indéterminée est 1.

Ex 42 : $\Sigma_1 = X_1 + X_2 + \dots + X_n \quad \Sigma_n = X_1 \times X_2 \times \dots \times X_n$

Appl. 43 : Relation coefficient / racine
Soit $P = a_0 X^n + a_1 X^{n-1} + \dots + a_n \in \mathbb{K}[X]$, $a_0 \neq 0$
$P = a_0 (X - x_1) \cdots (X - x_n)$, Alors $\forall 1 \leq p \leq n \quad \Sigma_p(x_1, \dots, x_n) = (-1)^p \frac{a_p}{a_0}$

Déf 44 : Soit $P = \sum_{i \in \mathbb{N}^n} a_i X_1^{i_1} \dots X_n^{i_n} \in A[X_1, \dots, X_n]$
On définit le poids $\pi(P)$ de P par :
- $\pi(P) = -\infty$ si $P = 0$
- $\pi(P) = \max_{\substack{i \in \mathbb{N}^n \\ a_i \neq 0}} \{ \sum_{k=1}^{n} k i_k \}$

Ex 45 : $P = XY + X^2Y + XY^2 + YZ \qquad \pi(P) = 5$

Prop/déf 46 : Soit $P \in A[X_1 \dots X_n]$ un polynôme symétrique. Alors P a même degré partiel par rapport à chaque indéterminée. Ce degré partiel s'appelle l'ordre de P, noté $w(P)$

Ex 47 : $w(\Sigma_p) = 1 \quad \forall 1 \leq p \leq n$

2°/ Théorème de structure

Lemme 48 : Soit $P \in A[X_1 \dots X_n]$ tel qu'en substituant 0 à l'une des quelconques indéterminées, on obtient le polynôme nul. Alors P est divisible par $\Sigma_n = X_1 \times \dots \times X_n$

Thm 49 : Soit $P \in A[X_1 \dots X_n]$ un polynôme symétrique de degré p et d'ordre w. Il existe un unique polynôme Q de $A[Y_1, \dots, Y_n]$ tq $P(X_1 \dots X_n) = Q(\Sigma_1 \dots \Sigma_n)$
Ce polynôme Q est de poids p et de degré w.

Ex 50 : Dans $A[X_1, X_2, X_3]$, $P = X_1^2 X_2 + X_1^2 X_3 + X_2^2 X_1 + X_2^2 X_3$ s'écrit $P = \Sigma_1 \Sigma_2 - 3\Sigma_3$

3°/ Applications

App 51 : Soit $P \in \mathbb{Z}[X]$ unitaire, $u_1 \dots u_n$ ses racines. Alors pour tout $F \in \mathbb{Z}[X_1 \dots X_n]$ symétrique, $F(u_1, \dots, u_n) \in \mathbb{Z}$

Appl 52 : Thm de D'Alembert-Gauss
Le corps $\mathbb{C}$ est algébriquement clos

Appl. 53 : Soit $A \in \mathcal{M}_n(\mathbb{C})$ tq $\forall k \in \mathbb{N}^* \quad Tr(A^k) = 0$
Alors A n'est nilpotente.

Références :

- [RDO] E. Ramis / C. Deschamps / J. Odoux Algèbre
- [GOU] Gourdon, Algèbre
- [GOB] Goblot, Algèbre commutative
- [Oraux X-ENS] Algèbre 2
- [ZAV] Zavidovique, un max de Maths

Développement: Théorème de Molien

Justine VELLY & Joséphine BOULANGER

8 octobre 2015

Référence : Gabriel Peyré, L'algèbre discrète de la transformée de Fourier

Notation : Soit G un sous-groupe fini de $GL_n(\mathbb{C})$. Il agit linéairement sur $\mathbb{C}[X_1, ..., X_n]$ via :

$$\begin{aligned}\forall A \in G, \ \forall P \in \mathbb{C}[X_1, ..., X_n], \ A.P(X_1, ..., X_n) &= P({}^t(A^{-1t}(X_1, ..., X_n))) \\ &= P({}^t(\textstyle\sum_{j=1}^n \alpha_{1,j}X_j, ..., \sum_{j=1}^n \alpha_{n,j}X_j))\end{aligned}$$

qui est une notation pratique pour dire que l'on substitue $\sum_{j=1}^{n} \alpha_{i,j}X_j$ à X_i, si l'on note $A^{-1} = (\alpha_{i,j})_{1 \leq i,j \leq n}$.
Soit V_d le sous-espace (de dimension finie) de $\mathbb{C}[X_1, ..., X_n]$ des polynômes homogènes de degré d.
On remarque que V_d est stable par l'action de G sur $\mathbb{C}[X_1, ..., X_n]$, i.e

$$\forall A \in G, \ \forall P \in V_d, \ A.P \in V_d$$

(une substitution linéaire des variables dans un polynômes homogènes reste un polynôme homogène de degré d).
La restriction de l'action de G sur $\mathbb{C}[X_1, ..., X_n]$ à V_d induit un morphisme de groupe

$$\begin{array}{rccc}\rho_d & : & G & \rightarrow & GL(V_d) \\ & & g & \mapsto & \rho(g) : (P \mapsto g.P)\end{array}$$

On note $V_d^G = \{P \in V_d, \forall g \in G, g.P = P\} = \{P \in V_d, \forall g \in G, \rho_d(g)(P) = P\}$ l'ensemble des polynômes $P \in V_d$ invariants sous l'action de G.

Théorème 1 (***Théorème de Molien***)

$$\frac{1}{|G|}\sum_{A \in G}\frac{1}{det(I - tA)} = \sum_{d \geq 0} dim(V_d^G)t^d$$

Démonstration : Posons $\begin{array}{rccc}\chi_d & : & G & \rightarrow & \mathbb{C} \\ & & A & \mapsto & Tr(\rho_d(A))\end{array}$

On a d'abord besoin du lemme suivant :

Lemme 1

$$dim(V_d^G) = \frac{1}{|G|}\sum_{g \in G}\chi(g)$$

Démonstration : Soit $R_G = \frac{1}{|G|}\sum_{g\in G}\rho_d(g)$.

On va montrer que R_G est un projecteur sur V_d^G, c'est-à-dire que $Im(R_G) = V_d^G$ et $R_G^2 = R_G$.

Montrons tout d'abord que $Im(R_G) = V_d^G$.

Soit $y = R_G(x) \in Im(R_g)$. Alors, pour tout $s \in G$, on a :

$$\begin{aligned}
\rho(s)(y) &= \rho_d(s)(\frac{1}{|G|}\sum_{g\in G}\rho_d(g)(x)) \\
&= \frac{1}{|G|}\sum_{g\in G}\rho_d(s)(\rho_d(g)(x)) \quad \text{par linéarité de } \rho_d(s) \\
&= \frac{1}{|G|}\sum_{g\in G}\rho_d(sg)(x) \quad \text{car } \rho_d \text{ est un morphisme} \\
&= \frac{1}{|G|}\sum_{h\in G}\rho_d(h)(x) \quad \text{car } g \in G \mapsto sg \text{ est une bijection de } G \text{ sur lui-même} \\
&= R_G(x) = y
\end{aligned}$$

Donc, $y \in V_d^G$.

Réciproquement, si $x \in V_d(G)$, alors pour tout $g \in G$, $\rho_d(g)(x) = x$ et donc,

$$R_G(x) = \frac{1}{|G|}\sum_{g\in G}\rho_d(g)(x) = \frac{1}{|G|}\sum_{g\in G} x = \frac{1}{|G|} \times |G| \times x = x$$

et donc $x \in Im(R_G)$.

Ainsi, R_G est d'image V_d^G.

De plus, le calcul précédent donne $R_G^2 = R_G$.

Donc, R_G est un projecteur sur V_d^G.

Alors, en écrivant la matrice de R_G dans une base adaptée à son image et à son noyau, on obtient que $Tr(R_G) = dim(V_d^G)$.

Or, par linéarité de la trace,

$$Tr(R_G) = Tr(\frac{1}{|G|}\sum_{g\in G}\rho_d(g)) = \frac{1}{|G|}\sum_{g\in G}\underbrace{Tr(\rho_d(g))}_{\chi_d(g)}$$

D'où

$$dim(V_d^G) = \frac{1}{|G|}\sum_{g\in G}\chi_d(g)$$

■

Lemme 2

Pour tout $A \in G$, on a l'égalité des séries suivantes,

$$\frac{1}{det(I - tA)} = \sum_{d\geq 0}\chi_d(A^{-1})t^d$$

Démonstration : Comme G est fini, on a d'après le théorème de Lagrange, $X^{|G|} - 1$ qui est un polynôme annulateur pour tous les éléments de G. Comme il est scindé à racines simples, les éléments de G sont tous diagonalisables.

Soit alors $A \in G$, et $\lambda_1, ..., \lambda_n$ les valeurs propres de A. On a :

$$\frac{1}{det(I - tA)} = \prod_{i=1}^{n}\frac{1}{1 - t\lambda_i} = \prod_{i=1}^{n}\sum_{k\geq 0}\lambda_i^k t^k = \sum_{k\geq 0}\left(\sum_{k_1+...+k_n=k}\lambda_1^{k_1}...\lambda_n^{k_n}\right)t^k$$

où la dernières série est obtenue par produit de Cauchy des n séries.
Soit un élément de la base canonique de V_d, $X_1^{k_1}...X_n^{k_n}$ avec $k_1 + ... + k_n = d$.
La trace est invariante par changement de base, on peut donc supposer que A est diagonale (avec les valeurs propres dans l'ordre de leur numérotation).
On a alors

$$\rho_d(A^{-1})(X_1^{k_1}...X_n^{k_n}) = (\lambda_1 X_1)^{k_1}...(\lambda_n X_n)^{k_n} = \lambda_1^{k_1}...\lambda_n^{k_n}(X_1^{k_1}...X_n^{k_n})$$

Donc $\lambda_1^{k_1}...\lambda_n^{k_n}$ est une valeur propre de $\rho_d(A^{-1})$
Et donc,

$$\chi_d(A^{-1}) = Tr(\rho_d(A^{-1})) = \sum_{k_1+...k_n=d} \lambda_1^{k_1}...\lambda_n^{k_n}$$

D'où $$\frac{1}{det(I-tA)} = \sum_{k\geq 0}\left(\sum_{k_1+...+k_n=k} \lambda_1^{k_1}...\lambda_n^{k_n}\right) t^k = \sum_{k\geq 0} \chi_d(A^{-1})t^k$$

ce qui fallait démontrer. ■

Pour conclure, il suffit d'écrire

$$\begin{aligned}\frac{1}{|G|}\sum_{A\in G}\frac{1}{det(I-tA)} &= \frac{1}{|G|}\sum_{A\in G}\sum_{d\geq 0}\chi_d(A^{-1})t^d \quad \text{lemme 2}\\ &= \sum_{d\geq 0}\left(\frac{1}{|G|}\sum_{A\in G}\chi_d(A^{-1})\right)t^d \quad \text{car l'une des somme est finie}\\ &= \sum_{d\geq 0} dim(V_d^G)t^d \text{ lemme 1 + inversion est une bijection de } G \text{ sur lui-même}\end{aligned}$$ ■

Développement: Théorème d'Erdös-Ginzburg-Ziv

Justine VELLY & Joséphine BOULANGER

8 octobre 2015

Référence : Maxime Zavidovique, Un max de Maths

Ce développement consiste en la preuve du théorème d'Erdös-Ginzbur-Ziv. On commence par rappeler le théorème de Chevalley-Warning, qui est un outil essentiel de la démonstration.

Théorème 1 (***Chevalley-Warning***)

Soit q une puissance d'un nombre premier p ($q = p^d$). Soient $f_1, ..., f_r \in \mathbb{F}_q[X_1, ..., X_n]$, vérifiant la condition

$$\sum_{i=1}^{r} deg(f_i) < n$$

Alors, en notant $V = \{x \in \mathbb{F}_q^n / f_1(x) = ... = f_r(x) = 0\}$, l'ensemble des zéros communs aux polynômes $f_1, ..., f_r$, on a :

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

Venons en maintenant au théorème d'Erdös-Ginzburg-Ziv.

Théorème 2 (***Erdös-Ginzburg-Ziv***)

Soit $n \in \mathbb{N}^*$, et $a_1, ..., a_{2n-1}$ des entiers. Alors, il existe des indices $i_1, ..., i_n \in \{1, ..., 2n-1\}$ tels que

$$a_{i_1} + a_{i_2} + ... + a_{i_n} \equiv 0[n]$$

Démonstration : Notons EGZ l'ensemble des entiers $n \in \mathbb{N}^*$ vérifiant le théorème d'Erdös-Ginzburg-Ziv.

Plus précisément,

$$EGZ = \{n \in \mathbb{N}^*, \forall a_1, ..., a_{2n-1} \in \mathbb{N}, \text{ il exite des indices } i_1, ..., i_n \in \{1, ..., 2n-1\} / a_{i_1} + ... + a_{i_n} \equiv 0[n]\}$$

Le but est de montrer que $EGZ = \mathbb{N}^*$.

Pour cela, on va procéder en deux étapes. On va d'abord montrer que EGZ contient tous les nombres premiers, puis que EGZ est stable par multiplication, comme chaque entier peut se décomposer en produit de nombre entier, on a $EGZ = \mathbb{N}^*$.

premier

1. **EGZ contient tous les nombres premiers :**
   Soit p premier et $a_1, ..., a_{2p-1}$ des entiers. On travaille dans $\mathbb{F}_p$ et on considère les deux polynômes

$$f_1 = \sum_{i=1}^{2p-1} \overline{a_i} X_i^{p-1} \text{ et } f_2 = \sum_{i=1}^{2p-1} X_i^{p-1}$$

Alors, comme $deg(f_1)+deg(f_2) \leq 2p-2 < 2p-1$ (le nombre de variables), on peut appliquer le théorème de Chevalley-Warning. En conservant les notations du théorème, on a donc,

$$p \mid |V|$$

Or, $(0, ..., 0) \in V$ donc $|V| \geq 2$.
Donc, il existe $(x_1, ...x_{2p-1}) \in V$ non nul, tel que

$$f_1(x_1, ..., x_{2p-1}) = f_2(x_1, ..., x_{2p-1}) = 0$$

Or, $x^{p-1} = 1$ dans $\mathbb{F}_p$, si et seulement si, x est non nul dans $\mathbb{F}_p$.
Notons alors

$$W = \{i \in \{1, ..., 2p-1\}/x_i \neq 0\}$$

On a alors

$$f_2(x_1, ..., x_{2p-1}) = \sum_{i \in W} x_i^{p-1} = \overline{|W|} = 0$$

Or, $1 \leq |W| \leq 2p-1$. Donc, $|W| = p$.
Donc, en notant $W = \{i_1, ..., i_p\}$, on a

$$f_1(x_1, ..., x_{2p-1}) = \sum_{k=1}^{2p-1} \overline{a_{i_k}} x_{i_k}^{p-1} = \sum_{k=1}^{p} \overline{a_{i_k}} = 0$$

c'est à dire

$$a_{i_1} + ... + a_{i_p} \equiv 0[p]$$

2. **EGZ est stable par multiplication**
Soient $m, n \in EGZ$. On veut montrer que $nm \in EGZ$.
Soient donc $a_1, ..., a_{2nm-1}$ des entiers.
Prenons en $2n-1$. Comme $n \in EGZ$, il existe un ensemble I_1 d'indices, de cardinal n, tel que $I_1 \subset \{1, ..., 2nm-1\}$ et

$$\sum_{i \in I_1} a_i \equiv 0[n]$$

Considérons ensuite les entiers (a_i) avec $i \in \{1, ..., 2nm-1\} \setminus I_1$. Prenons en $2n-1$. Il existe alors I_2 tel que $I_2 \subset \{1, ..., 2nm-1\} \setminus I_1$, $|I_2| = n$ et

$$\sum_{i \in I_2} a_i \equiv 0[n]$$

Terminons le procédé après avoir construit l'ensemble d'indices I_{2m-1}, ce qui est possible car au bout de $2m-2$ étapes, il reste

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

Pour $j \in \{1, ..., 2m-1\}$, soit c_j défini par

$$\sum_{i \in I_j} a_i = nc_j$$

Alors, comme $m \in EGZ$, on peut finalement extraire un sous-ensemble d'indices J tel que

$$\sum_{j \in J} c_j \equiv 0[m]$$

Alors,

$$\sum_{j \in J} \sum_{i \in I_j} a_i = n \underbrace{\sum_{j \in J} c_j}_{\text{divisible par } m} \equiv 0[nm]$$

Donc, ces nm derniers entiers répondent au problème posé. ■

$2n-1$ entiers est optimal

$\rightarrow (\underbrace{1, ..., 1}_{n-1}, \underbrace{0, ..., 0}_{n-1})$

aucune somme de n entiers n'est divisible par n.