Méthodes polynomiales en combinatoire

Antoine Dequay

21 septembre 2022

Notes

— Prof : .

— Leçons : 123, 190, 925.

— Références :

  — Le Barbenchon.

Soit $n \in \mathbb{N}^*$, $\mathbb{K}$ un corps, $P \in \mathbb{K}[X_1, \dots, X_n]$, $S_1, \dots, S_n \subset \mathbb{K}$ tels que $P(S_1 \times \cdots \times S_n) = 0$.

Lemme 1 Si $n = 1$ et $|S_1| > \deg(P)$, alors $P = 0$

Preuve. (peut être admis)

Supposons que $\deg(P) \leq d$ et que P possède $d+1$ racines distinctes.

Si $d \leq 0$, alors $P = 0$. Pour $d \in \mathbb{N}^*$, on procède par récurrence sur $\deg(P)$. Soit donc $P \in \mathbb{K}[X_1]$ de degré d et $\alpha \in \mathbb{K}$ une racine de P. Comme $\mathbb{K}$ est un corps, $\mathbb{K}[X_1]$ est euclidien, donc on peut effectuer la division euclidienne de P par $X_1 - \alpha$: $P = (X_1 - \alpha)Q + R$ avec $\deg(R) = 0$, donc R constant, puis $R = 0$. On a alors $\deg(Q) = \deg(P) - \deg(X_1 - \alpha) = d - 1$. Q a au moins $d + 1 - 1 = d$ racines, donc on peut appliquer l'hypothèse de récurrence, d'où le résultat.

□

Lemme 2 Si $|S_i| > \deg_{X_i}(P)$ pour tout $i \in [\![1, n]\!]$, alors $P = 0$.

Preuve. (peut être admis)

On procède par récurrence sur $n \in \mathbb{N}^*$, le cas $n = 1$ ayant été traité.

Soit $n \geq 2$, et $P \in \mathbb{K}[X_1, \dots, X_n] = \mathbb{K}[X_1, \dots, X_{n-1}][X_n]$. On peut alors appliquer le cas $n = 1$ sur chaque $P(s_1, \dots, s_{n-1}, \cdot)$, $s_1, \dots, s_{n-1} \in S_1, \dots, S_{n-1}$ [1]. Les coefficients de $P = \sum_{i=0}^{\deg_{X_n}(P)} P_i X_n^i$ sont donc nuls sur $S_1 \times \cdots \times S_{n-1}$, et on peut leur appliquer l'hypothèse de récurrence.

□

Lemme 3 Avec, pour $i \in [\![1, n]\!]$, $g_i = \prod_{s \in S_i} (X_i - s)$, il existe $h_1, \dots, h_n \in \mathbb{K}[X_1, \dots, X_n]$ tels que $P = \sum_{i=1}^{n} h_i g_i$ avec $\deg(g_i h_i) \leq \deg(P)$.

Preuve. (peut être admis au début)

On peut effectuer la division euclidienne successive (sur les restes des précédentes) de P par les g_i, on a : $P = \sum_{i=1}^{m} h_i g_i + R_m$ pour $m \in [\![1, n]\!]$.

En particulier, $\deg(R_m) < \deg(g_m) \leq \deg(g_m h_m) = \deg(R_{m-1})$.

Avec $R_0 = P$, la suite $\deg(R_m)$ est donc décroissante, et on a bien, pour tout $m \in [\![1, n]\!]$, $\deg(g_m h_m) \leq \deg(R_{m-1}) \leq \deg(P)$.

1. obligatoire car $\mathbb{K}[X_1, \dots, X_{n-1}]$ n'est pas un corps !

Il reste à voir que $R := R_n = 0$. En raisonnant comme précédemment (sur une division euclidienne selon X_i), $\left(\deg_{X_i}(R_m)\right)_{m\in[\![0,m]\!]}$ est décroissante pour tou $i \in [\![1,n]\!]$. D'où $\deg_{X_i}(R) \leq \deg_{X_i}(R_i) < \deg_{X_i}(g_i) = |S_i|$. De plus, par définition de R, $R(S_1 \times \cdots \times S_n) = 0$. On peut conclure par le lemme précédent.

□

Lemme 4 Soit M un monôme tel que $\deg(M) = \deg(P)$ et $|S_i| > \deg_{X_i}(M)$ pour tout $i \in [\![1,n]\!]$. Alors le coefficient de M dans P est nul.

Preuve. On reprend la décomposition précédente. Dans le membre de gauche, le coefficient de M est celui recherché. Dans celui de droite, à $i \in [\![1,n]\!]$ fixé, on a $\deg(g_ih_i) \leq \deg(M)$ et $\deg_{X_i}(g_i) = |S_i| > \deg_{X_i}(M)$. Ainsi, le coefficient de M dans g_ih_i est nul, donc il en est de même dans le membre de droite, d'où le résultat.

□

Pour 123 :

Théorème 5 (de Chevalley-Warning)

Soit $p \in \mathcal{P}$, $d, n, r \in \mathbb{N}^*$, $q = p^d$ et $P_1, \ldots, P_r \in \mathbb{F}_q[X_1, \ldots, X_n]$ dont la somme des degrés est d'au plus $n-1$.

Alors le nombre de racines communes de $P_1, \ldots, P_r$ sur F_q est divisible par p.

Preuve. Soit S l'ensemble des racines communes à $P_1, \ldots, P_r$. On commence par chercher à construire un polynôme s'annulant sur $\mathbb{F}_q^n$.

Soit $s = (s_1, \ldots, s_n) \in \mathbb{F}_q^n$. On définit :

$$g_s = \prod_{i=1}^{n} \left(1 - (X_i - s_i)^{q-1}\right).$$

Comme $x^{q-1} = 1$ si $x \neq 0$ (Lagrange), le $i$ème terme du produit est nul si $X_i \neq s_i$, et donc $g_s(s) = 1$ et 0 sinon.

Ainsi, en posant $Q = \prod_{i=1}^{r} \left(1 - P_i^{q-1}\right)$, on a $Q(S) = 1$ et $Q = 0$ sinon. On peut donc poser $P = Q - \sum_{s\in S} g_s$, qui est, par définition, nul sur $\mathbb{F}_q^n$.

Examinons le coefficient de $(X_1 \ldots X_n)^{q-1}$ dans P :

— Par le lemme précédent, comme $\deg_{X_i}\left((X_1 \ldots X_n)^{q-1}\right) < q = |\mathbb{F}_q|$ pour $i \in [\![1,n]\!]$, le coefficient recherché est nul (dans $\mathbb{F}_q$).

— Comme $\sum_{i=1}^{r} \deg(P_i) < n$, le coefficient de $(X_1 \ldots X_n)^{q-1}$ dans Q est nul. Il a pour coefficient $(-1)^n$ dans g_s pour $s \in S$, d'où un coefficient dans P de $-\sum_{s\in S}(-1)^n = (-1)^{n+1}|S| = 0$ dans $\mathbb{F}_q$, d'où $|S| \equiv 0 \ (mod\ p)$.

□

Pour 925 :

Théorème 6 Soit G un graphe simple, de degré moyen strictement supérieur à $2p-2$ et de degré maximal au plus $2p-1$, avec p premier.

Alors il existe un sous-graphe de G dont tous les sommets sont de degré p.

Preuve. On se donne X_e pour $e \in E$, on travaille sur $\mathbb{F}_p[X_1, \dots, X_n]$ avec $n = |E|$, dont les valeurs seront prises dans $\{0,1\}^n$. On va chercher à construire un polynôme traduisant la propriété recherchée pour le sous-graphe. Une valuation correspondra alors à un sous-graphe : une arête $e \in E$ apparaîtra dans le sous graphe associé à une valuation si et seulement si $X_e = 1$.

Pour $s \in S$ et $e \in E$, on définit $a_{s,e} := \begin{cases} 1 \text{ si } e \text{ est incidente à } v, \\ 0 \text{ sinon.} \end{cases}$.

A $s \in S$ fixé, on a donc $\sum_{e \in E} a_{s,e} X_e = 0$ si et seulement si le degré de $s \in S$ dans le sous-graphe est multiple de p.

Ainsi, par Fermat, $1 - \left(\sum_{e \in E} a_{s,e} X_e \right)^{p-1} = 1$ si et seulement si s a un degré égal à 0 (n'apparaît pas dans le sous-graphe) ou p dans le sous-graphe (car $2p > 2p-1 =$ le degré maximal de G).

Donc $Q = \prod_{s \in S} \left(1 - \left(\sum_{e \in E} a_{s,e} X_e \right)^{p-1} \right)$ est non nul si et seulement si le sous graphe est vide ou ne contient que des sommets de degré p.

Pour palier au problème du graphe vide, on pose finalement :

$$P = \prod_{s \in S} \left(1 - \left(\sum_{e \in E} a_{s,e} X_e \right)^{p-1} \right) - \prod_{e \in E} (1 - X_e).$$

Il reste à voir que P n'est pas identiquement nul sur $\mathbb{F}_2^n$. Pour cela, on regarde le coefficient de $M = \prod_{e \in E} X_e$ dans P.

Le degré du premier produit est $|S|(p-1)$. Or, $|E| = \dfrac{deg\_moy \times |S|}{2} > |S|(p-1)$, donc M a pour coefficient $(-1)^{n+1} \neq 0$.

Comme $\deg(M) = \deg(P)$, par contraposé du lemme 5, il existe $i \in [\![1, n]\!]$ tel que $|S_i| \leq \deg_{X_i}(M) = 1$. Ainsi, $S_1 \times \cdots \times S_n \neq \mathbb{F}_2^n$, donc P est non identiquement nul, ce qui prouve le résultat !

□