102
144

Théorème de Kronecker

- L'oral à l'agreg, Isenmann, p 277
- Carnet de voyage en Algébrie, Caldero, p 30

IP 277 • **Déf 1** : Soit A un anneau. Soit $n \in \mathbb{N}$ et $k \in [\![0 ; n]\!]$. On définit le k-ième polynôme symétrique élémentaire e_k de $A[X_1, \dots, X_n]$ par :

$$e_k = \sum_{I \in \mathcal{P}_k([\![1;n]\!])} \prod_{i \in I} X_i = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} X_{i_1} X_{i_2} \dots X_{i_k}$$

où $\mathcal{P}_k([\![1;n]\!])$ désigne l'ensemble des parties à k éléments de $[\![1;n]\!]$. avec $e_0 = 1$ par convention

• **Exemple** : $e_1 = X_1 + \dots + X_n$

$e_2 = \sum_{i \neq j} X_i X_j$ $\qquad e_n = X_1 \dots X_n$

• **Théorème 2 (relations coefficients - racines)** : Soit $P \in A[X]$ un polynôme scindé unitaire, c-à-d $P(X) = \sum_{i=0}^{n} a_i X^i$ avec $a_n = 1$. On note $z_1, \dots, z_n$ ses racines. Alors $\forall k \in [\![0;n]\!]$, on a :

$$e_k(z_1, \dots, z_n) = (-1)^k a_{n-k}$$

• **Théorème de Kronecker** : Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire dont les racines complexes sont toutes de module inférieur ou égal à 1. On suppose que $P(0) \neq 0$ (0 n'est pas racine). Alors les racines de P sont des racines de l'unité.

Dém : Soit Ω_n l'ensemble des poly unitaires de $\mathbb{Z}[X]$ de degré n dont les racines complexes sont de module ≤ 1.

On veut montrer que Ω_n est un ensemble fini.

Soit $P \in \Omega_n$. On note $(a_k)_{0 \leq k \leq n-1}$ ses coeffs et $(z_i)_{1 \leq i \leq n}$ ses racines complexes.

On pose $\sigma_k = e_k(z_1, \dots, z_n)$ $\forall k \in [\![0;n]\!]$

Alors d'après le théorème 2, $\sigma_k = (-1)^k a_{n-k}$

Si $P = X^n + \sum_{i=0}^{n-1} a_i X^i$ alors $M := C_P = \begin{pmatrix} 0 & 0 & & 0 & -a_0 \\ 1 & 0 & \ddots & \vdots & -a_1 \\ 0 & 1 & \ddots & 0 & \vdots \\ \vdots & & \ddots & 1 & -a_{n-1} \end{pmatrix}$

Alors d'après l'inégalité triangulaire : $\forall k$

$$|\sigma_k| = \left| \sum_{I \in \mathcal{P}_k(\llbracket 1, n \rrbracket)} \prod_{i \in I} z_i \right|$$

$$\leq \sum_{\dots} \prod_{i \in I} |z_i|$$

$$\leq \operatorname{card}\left(\mathcal{P}_k(\llbracket 1, n \rrbracket)\right) \times 1 \qquad \text{car } |z_i| \leq 1$$

$$\leq \binom{n}{k}$$

Ainsi : $|a_k| \leq \binom{n}{m-k} = \binom{n}{k} \; \forall k \in \llbracket 1, n \rrbracket$

CAL 30 Ainsi les coefficients de P sont bornés (par exemple par $m!$) et sont entiers, donc il y a un nombre fini de coeffs possibles, donc de polynômes de Ω_m.

Donc Ω_m est fini.

IP 279 <u>Deuxième étape :</u> Soit $P \in \Omega_m$. On garde les mêmes notations.

Pour tout $k \in \mathbb{N}$, on pose :

$$P_k(X) = \prod_{i=1}^{n} (X - z_i^k) = (X - z_1^k) \dots (X - z_m^k)$$

Alors P_k est de degré m, unitaire, et ses racines sont de module inférieur ou égal à 1.

On montre que $P_k \in \mathbb{Z}[X]$.

Soit M la matrice compagnon de P. Ainsi

PAS $\chi_M = P$. Comme $P \in \mathbb{Z}[X]$, alors $M \in M_n(\mathbb{Z})$

DE Or P est scindé sur $\mathbb{C}$ donc on peut trigonaliser

RÈF M dans $\mathbb{C}$. M est semblable à une matrice triangulaire supérieure avec les z_i sur la diagonale.

Mais alors M^k est semblable à une matrice

triangulaire supérieure avec les z_i^h sur la diagonale, donc P_h est le poly carac de M^k
On $M^h \in M_n(\mathbb{Z})$ car $M \in M_n(\mathbb{Z})$, donc $P_h \in \mathbb{Z}[X]$
Ainsi $P_h \in \Omega_n$.

Comme Ω_n est fini, l'ensemble des racines de tous les P_k, qui est $\{x \in \mathbb{C} ; \exists h \in \mathbb{N}, P_h(x) = 0\}$ est aussi fini (il y a un nombre fini de P_h et P_h a au plus n racines)
Soit $i \in [\![1 ; n]\!]$.
Alors l'ensemble $\{z_i^h ; h \in \mathbb{N}\}$ est inclus dans l'ensemble de ces racines. Il est alors lui aussi fini et donc $\exists h, h' \in \mathbb{N}$ tq $z_i^h = z_i^{h'}$
Comme $z_i \neq 0$ par hypothèse, il existe $m \in \mathbb{N}$ tel que $z_i^m = 1$.
Donc toutes les racines z_i de P sont des racines de l'unité. $\square$

IP 280 <u>Corollaire</u> : Soit $P \in \mathbb{Z}[X]$ unitaire et irréductible sur $\mathbb{Q}$ tel que toutes les racines complexes de P soient de module inférieur ou égal à 1. Alors $P = X$ ou P est un polynôme cyclotomique.

<u>Dém</u> : Si 0 est racine de P, $X \mid P$ et alors $P = X$ car P irréd et unitaire.
Si 0 n'est pas racine, on applique le théorème de Kronecker : toutes les racines de P sont des racines de l'unité.
PAS DE RÉF Si z racine de P, on note d son ordre.
Ainsi z est une racine d-ième de l'unité, donc

Φ_d est le polynôme minimal de z sur $\mathbb{Q}$ (car Φ_d irréd sur $\mathbb{Q}$).
Comme P annule z, alors par minimalité, Φ_d divise P, qui est irréductible dans $\mathbb{Q}[X]$.
Comme Φ_d et P sont unitaires, alors $P = \Phi_d$. $\square$

<u>Remarques</u>:
1) Si P n'est pas unitaire, ce n'est pas vrai : prendre $P(X) = 2X + 1$