Développement : Théorème de Kronecker Sources : CVA p. 35

Théorème : $\mathcal{P} = \{$polynôme unitaire P de $\mathbb{Z}[X]$ tel que toute racine z de P est de module $|z| \leq 1\}$.
si $P(z) = 0$ avec $P \in \mathcal{P}$, alors soit z est nul, soit z est une racine de l'unité.

Démonstration :

• 1ère étape : Montrons que $\mathcal{P}_n$ est fini où $\mathcal{P}_n = \{P \in \mathcal{P}, \deg P = n\}$
Soit $n > 0$. On suppose $P \in \mathcal{P}_n$. On va montrer que le coefficient a_k de X^k de P vérifie $|a_k| \leq \binom{n}{k}$.

P a n racines $z_1, \dots, z_n$

$$P(X) = (X - z_1) \cdots (X - z_n) = a_0 + a_1 X + \dots + a_{n-1} X^{n-1} + X^n$$

Par la relation coefficients-racines sur un polynôme unitaire, on a :

$$a_{n-k} = (-1)^k \sum_{1 \leq i_1 < \dots < i_k \leq n} z_{i_1} \times \dots \times z_{i_k}$$

On applique alors l'inégalité triangulaire : $|a_{n-k}| \leq \sum_{1 \leq i_1 < \dots < i_k \leq n} |z_{i_1}| \times \dots \times |z_{i_k}|$

car $|z_i| \leq 1$ $\leq \binom{n}{k}$

Donc $|a_k| \leq \binom{n}{n-k} = \binom{n}{k}$

donc les coefficients sont bornés (par exemple par $n!$) et entiers ($P \in \mathbb{Z}[X]$), il y a donc un nombre fini de coefficients possibles et donc de polynômes de $\mathcal{P}_n$. Donc $\mathcal{P}_n$ est fini.

• Étape 2 : Soit $\mathcal{R}_n$ l'ensemble fini des racines des polynômes de $\mathcal{P}_n$.
Soit $P \in \mathcal{P}_n$ et C_P la matrice compagnon de P. On va montrer que $\chi_{C_P^m}$ est encore dans $\mathcal{P}_n$, $\forall m \in \mathbb{N}^*$.

Montrons que $\chi_{C_P} = P$

$$P = X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 \qquad C_P = \begin{pmatrix} 0 & & & -a_0 \\ 1 & \ddots & 0 & \vdots \\ & \ddots & \ddots & \\ 0 & & 1 & -a_{n-1} \end{pmatrix}$$

$$\chi_{C_P} = \det(XI_n - C_P) = \begin{vmatrix} X & & 0 & a_0 \\ -1 & \ddots & & \vdots \\ & \ddots & X & \\ 0 & & -1 & X + a_{n-1} \end{vmatrix} = \begin{vmatrix} 0 & \cdots & 0 & P \\ -1 & X & 0 & a_1 \\ & \ddots & \ddots & \vdots \\ 0 & & X & \\ & & -1 & X + a_{n-1} \end{vmatrix} \quad L_1 \leftarrow L_1 + XL_2 + \dots + X^{n-1} L_n$$

donc $\chi_{C_P} = (-1)^{n+1} P \, (-1)^{n-1} = P$

donc χ_{C_P} est unitaire de deg n.

$C_P^m \in M_n(\mathbb{Z})$ donc $\chi_{C_P^m}$ est de degré n dans $\mathbb{Z}[X]$ et toujours unitaire.

Remarque: On sait que si Q est un polynôme sur $\mathbb{C}$ et $A \in M_n(\mathbb{C})$ alors A est trigonalisable, donc $\exists P \in Gl_n(\mathbb{C})$ tel que $A = PTP^{-1}$, T triangulaire.

Les valeurs propres de A sont sur la diagonale de T.

$Q(A) = Q(PTP^{-1}) = P\,Q(T)\,P^{-1}$

Le spectre de $Q(A) = \{Q(\lambda) \mid \lambda \in Sp(A)\}$

Donc si $Q = X^m$, on a que les racines de $\chi_{C_P^m}$ sont les z^m (car $\chi_{C_P} = P$) avec z racine de P.

Donc toutes les racines de $\chi_{C_P^m}$ sont de module ≤ 1.

Donc $\chi_{C_P^m} \in \mathcal{P}_n$

On en déduit que si $z \in \mathcal{R}_n$, $z^m \in \mathcal{R}_n$, $\forall m \in \mathbb{N}^*$.

- Étape 3: Conclusion:

Soit $z \in R_n$ $\quad f : \begin{array}{l} \mathbb{N}^* \to \mathcal{R}_n \\ m \mapsto z^m \end{array}$ n'est pas injective car $\mathcal{R}_n$ est fini et $\mathbb{N}^*$ non fini.

Donc, il existe $m, m' \in \mathbb{N}^*$ tel que $z^m = z^{m'} \Rightarrow z = 0$ ou $z^{m-m'} = 1$

Donc z est nul ou z est une racine de l'unité. $\square$

Corollaire: $P \in \mathbb{Z}[X]$ unitaire, irréductible de $\mathbb{Z}$ tel que toutes les racines de P soit de module ≤ 1. Alors $P = X$ ou P est un polynôme cyclotomique.

Démonstration:

On suppose $P \neq X$ alors comme P est irréductible 0 n'est pas racine de P et d'après le théorème de Kronecker, ses racines sont des racines de l'unité. De plus, les racines de P sont simples car P est irréductible donc $P \mid X^N - 1$ pour un certain N. Or $X^N - 1 = \prod_{d \mid N} \Phi_d$, Φ_d irréductible dans $\mathbb{Z}[X]$ (car irréductible sur $\mathbb{Q}$ et unitaire). Donc $P = \Phi_d$ pour un certain d.