Théorème de Kronecker

Théorème 1. Soit $P \in \mathbb{Z}[X]$ unitaire de racines de module inférieur ou égal à 1. Si $P(0) \neq 0$, alors les racines de P sont des racines de l'unité.

Démonstration. Soit $n = \deg P$. Notons $z_1, \dots, z_n$ les racines de P comptées avec multiplicité. En posant σ_i les fonctions symétriques élémentaires, le polynôme P s'exprime :

$$P = X^n - \sigma_1 X^{n-1} + \cdots + (-1)^n \sigma_n.$$

Par hypothèse sur les racines de P, on a la majoration suivante des coefficients dans cette écriture :

$$|\sigma_k| = \left| \sum_{1 \leq i_1 \leq \cdots \leq i_k \leq n} z_{i_1} \dots z_{i_k} \right| = \left| \sum_{I \in \mathcal{P}_k([\![1,n]\!])} \prod_{i \in I} z_i \right| \leq \#\mathcal{P}_k([\![1,n]\!]) \binom{n}{k}.$$

Puisque $P \in \mathbb{Z}[X]$, il y a un nombre fini de choix pour les coefficients σ_i. Autrement dit, l'ensemble suivant est fini :

$$\Omega_n = \{P \in \mathbb{Z}[X],\ P \text{ unitaire},\ \deg P = n,\ \mathcal{Z}(P) \subset \overline{D(0,1)}\}.$$

Considérons maintenant pour $k \in \mathbb{N}^*$ le polynôme suivant unitaire, de degré n et de racines dans $\overline{D(0,1)}$:

$$P_k = \prod_{i=1}^{n} (X - z_i^k) \in \mathbb{C}[X].$$

Si l'on note $\Sigma_1, \dots, \Sigma_n$ les fonctions symétriques élémentaires des z_i^k, alors $(-1)^r \Sigma_r$ est le coefficient de X^{n-r} dans P_k et le polynôme symétrique en les z_i (car en les z_i^k) à coefficients dans $\mathbb{Z}$, donc $P_k \in \mathbb{Z}[X]$. En reprenant ce qui a été vu précédemment, $P_k \in \Omega_n$.

Puisque Ω_n est fini, l'ensemble E des racines d'éléments de Ω_n est aussi nécessairement fini, donc pour tout $i \in \{1, \dots, n\}$, l'application $k \mapsto z_i^k$ ne peut pas être injective : z_i est racine de l'unité. □

Corollaire 2. Si $P \in \mathbb{Z}[X]$ est unitaire *irréductible* de racines de module inférieur ou égal à 1, alors $P = X$ ou P est un polynôme cyclotomique.

Démonstration. Supposons $P \neq X$. Par irréductibilité, $P(0) \neq 0$ (sinon $X|P$). D'après le théorème précédent, les racines de P sont racines de l'unité. Puisque P est à racines simples (sans quoi on aurait $P \wedge P' | P$) il existe $N \in \mathbb{N}^*$ tel que :

$$P | X^N - 1 = \prod_{d|N} \phi_d.$$

Par irréductibilité, P est l'un des termes du produit, un polynôme cyclotomique (irréductible). □

Corollaire 3. Soit $P \in \mathbb{Z}[X]$ unitaire de racines de module inférieur ou égal à 1. Le polynôme P est produit d'une puissance de X et de polynômes cyclotomiques.