Théorème de Kronecker.

2013 – 2014

Référence : Serge Francinou, Hervé Gianella, Serge Nicolas, *Oraux X-ENS Algèbre 1*, Cassini, 2008, p.213.

Théorème.
On définit

$$\Omega_n := \{P \in \mathbb{Z}[X] \mid P \text{ unitaire}, \deg P = n \text{ et } z \in Z(P) \Rightarrow 0 < |z| \leq 1\}$$

où $Z(P)$ désigne les racines complexes de P.
Si $P \in \Omega_n$, alors les racines de P sont des racines de l'unité.

Démonstration. Montrons dans un premier temps que Ω_n est fini.
On note $z_1, \ldots, z_n$ les racines de P et $\sigma_1, \ldots, \sigma_n$ les fonctions symétriques élémentaires de P évaluées en $(z_1, \ldots, z_n)$.
Alors

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

et $\sigma_i \in \mathbb{Z}$.
Or $|z_i| \leq 1$ donc, pour $1 \leq p \leq n$,

$$|\sigma_p| = \left| \sum_{1 \leq i_1 < \ldots < i_p \leq n} z_{i_1} \cdots z_{i_n} \right| \leq \sum_{1 \leq i_1 < \ldots < i_p \leq n} 1 = \binom{n}{p}.$$

On en déduit que Ω_n est fini.
On considère désormais

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

et montrons que $P_k \in \Omega_n$.
Afin de montrer que $P_k \in \mathbb{Z}[X]$, introduisons le polynôme $Q_k := X^k - Y \in \mathbb{Z}[X, Y]$ et considérons $R_k(Y) := \mathrm{Res}_X(P(X), Q_k(X, Y))$. $P \in \mathbb{Z}[X]$ et $Q_k \in \mathbb{Z}[X, Y]$ donc $R_k \in \mathbb{Z}[Y]$. Par ailleurs,

$$R_k(Y) = \prod_{i=1}^{n} Q_k(z_i) = \prod_{i=1}^{n} (z_i^k - Y) = (-1)^n P_k(Y)$$

donc $P_k \in \mathbb{Z}[X]$. De plus, P_k est unitaire et ses racines sont les z_i^k qui vérifient $0 < |z_i^k| \leq 1$. Par conséquent, $P_k \in \Omega_n$.
Or Ω_n est fini donc l'ensemble des racines des éléments de Ω_n est fini donc, pour $i \in \{1, \ldots, n\}$, l'application

$$\begin{aligned} \mathbb{N}^* &\longrightarrow \mathbb{C} \\ k &\longmapsto z_i^k \end{aligned}$$

n'est pas injective. On en déduit qu'il existe $k \neq l$ tels que $z_i^k = z_i^l$ et $z_i \neq 0$ donc $z_i^{k-l} = 1$ et z_i est une racine de l'unité. □

Corollaire.
Soit $P \in \mathbb{Z}[X]$ unitaire et irréductible tel que $Z(P) \subset D(0,1)$, où $Z(P)$ désigne les racines de P.
Alors $P = X$ ou P est un polynôme cyclotomique.

Démonstration. Supposons $P \neq X$. Alors P est irréductible donc 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 (sinon il serait divisible par $P \wedge P'$ non trivial) et donc $P \mid X^N - 1$ pour un certain N.
Or

$$X^N - 1 = \prod_{d|N} \Phi_d$$

avec Φ_d irréductible sur $\mathbb{Z}$.
$P \neq 1$ donc $P = \Phi_k$ pour un certain k. □

Corollaire.
Tout polynôme de $\mathbb{Z}[X]$ ayant ses racines dans $D(0,1)$ est un produit de puissances de X et de polynômes cyclotomiques.