Théorème de Kronecker

Théorème . Soit $P \in \mathbb{Z}[X]$ unitaire avec $P(0) \neq 0$. Si les racines de P sont dans $\overline{D(0,1)}$, alors ce sont des racines de l'unité.

Preuve :
Soient $z_1, \dots, z_n \in \mathbb{C}$ les racines de P comptées avec multiplicité. En notant $\sigma_1, \dots, \sigma_n$ les fonctions élémentaires symétriques évaluées en $z_1, \dots, z_n$, on a

$$P(X) = \prod_{i=1}^{n}(X - z_i) = X^n + \sum_{i=1}^{n}(-1)^i \sigma_i X^{n-i}.$$

Comme $P \in \mathbb{Z}[X]$, on a $\sigma_1, \dots, \sigma_n \in \mathbb{Z}$. Pour $i \in [\![1, n]\!]$, on a

$$|\sigma_i| = \left| \sum_{1 \leq j_1 < \ldots < j_i \leq n} z_{j_1} \ldots z_{j_i} \right| \leq \sum_{1 \leq j_1 < \ldots < j_i \leq n} 1 = \binom{n}{i}.$$

Donc $\Omega_n := \left\{ P \in \mathbb{Z}[X] \ ; \ \text{deg}(P) = n, \ P \text{ unitaire}, \ \text{Rac}(P) \subset \overline{D(0,1)} \right\}$ est fini.

Pour $k \in \mathbb{N}$, on pose $P_k(X) = \prod_{i=1}^{n}(X - z_i^k) \in \mathbb{C}[X]$. Soient $\Sigma_1, \dots, \Sigma_n$ les fonctions élémentaires symétriques en $z_1^k, \dots, z_n^k$. On a

$$(-1)^i \Sigma_i \in \mathbb{Z}_{\text{sym}}[z_1, \dots, z_n] = \mathbb{Z}[\sigma_1, \dots, \sigma_n],$$

donc $\Sigma_i \in \mathbb{Z}$ pour tout i et ainsi $P_k \in \Omega_n$. Or $E_n := \left\{ z \in \mathbb{C} \ ; \ \exists P \in \Omega_n, P(z) = 0 \right\}$ est fini, car Ω_n est fini et $P \in \Omega_n$ a au plus n racines distinctes. Donc l'application

$$\left| \begin{array}{ccc} \mathbb{N} & \to & E_n \\ k & \mapsto & z_i^k \end{array} \right.$$

n'est pas injective. En particulier, il existe $k, \tilde{k} \in \mathbb{N}$ différents tels que $z_i^k = z_i^{\tilde{k}}$. Comme $z_i \neq 0$, on a $z_i^{|k - \tilde{k}|} = 1$ d'où le résultat.

□

Corollaire . Soit $P \in \mathbb{Z}[X]$ unitaire tels que ses racines soient dans $\overline{D(0,1)}$. Alors P est produit de X et de polynômes cyclotomiques.

Preuve :
Soit $\varphi \in \mathbb{Z}[X]$ un facteur irréductible unitaire de P et supposons $\varphi \neq X$.
φ étant irréductible, on a $\varphi(0) \neq 0$. Par le théorème de Kronecker, ses racines sont des racines de l'unité : il existe $n \in \mathbb{N}$ tel que $\text{Rac}(\varphi) \subset \mathbb{U}_n$.
φ étant irréductible sur $\mathbb{Z}$, il est scindé à racines simples sur $\mathbb{C}$. Donc φ divise $X^n - 1 = \prod_{d|n} \phi_d$, avec ϕ_d les polynômes cyclotomiques. Or ces derniers sont irréductibles, donc $\varphi = \phi_d$ pour d un diviseur de n.

□