

Soit $n \in \mathbf{N}^*$. On considère

$$\mathcal{H}: \begin{cases} P \text{ unitaire de degré } n, \text{ à coefficients entiers, et} \\ \forall z \in \mathbf{C}, P(z) = 0 \implies 0 < |z| \leq 1. \end{cases}$$

Soit $P := a_0X^n + \dots + a_{n-1}X + a_n \in \mathbf{C}[X]$.

Théorème 1 (Kronecker). On suppose $P \in \mathcal{H}$. Alors les racines de P sont des racines de l'unité.

Démonstration. Écrivons $P(X) := \prod_{i=1}^n (X - z_i)$ avec $|z_i| \leq 1$ pour tout $i = 1, \dots, n$. Alors

$$\forall k = 1, \dots, n, |a_k| \leq \sum_{1 \leq i_1 < \dots < i_k \leq n} |z_{i_1}| \cdots |z_{i_k}| \leq \binom{n}{k},$$

donc $\mathcal{H}$ est fini. Soit pour tout $k \in \mathbf{N}$, $P_k(X) := \prod_{i=1}^n (X - z_i^k)$. Alors $P_2(X^2) = (-1)^n P(X)P(-X)$ et pour tout $k \geq 1$, $P_{2^{k+1}}(X^2) = (-1)^n P_{2^k}(X)P_{2^k}(-X)$, donc par récurrence immédiate les polynômes $P_{2^k}(X)$, $k \in \mathbf{N}$, vérifient tous $\mathcal{H}$. Ceux-ci sont donc en nombre fini, et l'ensemble R de toutes leurs racines est lui aussi fini. Si $P(z) = 0$ alors $\forall k \in \mathbf{N}$, $z^{2^k} \in R$, donc $\exists k < \ell$, $z^{2^k} = z^{2^\ell}$: z est une racine de l'unité. ■

Références.

190 Méthodes combinatoires, problèmes de dénombrement.