théorème de Kronecker

Th 1 : Soit $P(X) \in \mathbb{Z}(X)$ unitaire dont toutes les racines complexes ont une norme non nulle inférieure à 1.
Alors les racines de P sont des racines de l'unité

Dém : Soit $\{z_1, \dots, z_n\}$ les racines de P.

$$P(X) = \prod_{i \in [\![1,n]\!]} (X - z_i) = X^n - \sigma_1 X^{n-1} + \dots + (-1)^n \sigma_n$$

où σ_i la fonction symétrique $i$ème des racines, i.e. $\sigma_i = \sum_{1 \le j_1 < \dots < j_i \le n} z_{j_1} \dots z_{j_i}$

On a donc que $\sigma_i \in \mathbb{Z}$ et aussi

$$|\sigma_i| = \left| \sum_{1 \le j_1 < \dots < j_i \le n} z_{j_1} \dots z_{j_i} \right| \le \sum_{1 \le j_1 < \dots < j_i \le n} |1|$$

Or le nombre de combinaisons de i chiffres distincts compris entre 1 et n est donné par $\binom{n}{i}$

$$|\sigma_i| \le \binom{n}{i} \quad \text{et} \quad \sigma_i \in \mathbb{Z}$$

Chaque coefficient de P ayant un nombre fini de choix possibles, cet ensemble est fini.

$$\mathrm{Card}\left(\{ P \in \mathbb{Z}[X] \mid P \text{ unitaire et ses racines sont de module inférieur ou égal à 1 et non nulle} \} \right) \le \prod_{i=1}^{n} \binom{n}{i}$$

* Considérons pour $k \in \mathbb{N}$ donné

$$P_k(X) = (X - z_1^k) \dots (X - z_n^k)$$

Les racines d'un tel polynôme sont bien de module non nul inférieur ou égal à 1. ~~Donc P_k appartient à l'ensemble Π qui est fini.~~

~~La fonction $\varphi : \mathbb{N} \to \Pi$, $k \mapsto P_k(X)$ est forcément~~

$$P_k(X) = X^n - \sigma'_1 X^{n-1} + \dots + (-1)^n \sigma'_n$$

où $\sigma'_i = \sigma_i(z_1^k, \dots, z_n^k) = \left(\sigma_i(z_1, \dots, z_n)\right)^k \in \mathbb{Z}$

donc $P_k \in F$ qui est fini.

Posons $\Omega_F = \{z \in \mathbb{C} / \exists P \in F, P(z) = 0\}$

Puisque F est fini et chaque P de F a au plus n racines, Ω_F est fini aussi et a au plus n fois le cardinal de F.

Pour chaque z_i racine de P, on peut considérer la fonction $\varphi : \begin{cases} \mathbb{N} \to \Omega_F \\ k \mapsto z_i^k \end{cases}$

Comme Ω_F est fini et $\mathbb{N}$ infini, $\exists k_1, k_2$ tq $z_i^{k_1} = z_i^{k_2}$

et donc $(z_i)^{k_1 - k_2} = 1$ et z_i racine de l'unité.

□ CQFD.

Th 2 : Si $P \in \mathbb{Z}[X]$ unitaire a des racines de module non nul et ≤ 1 et que de plus P est irréductible sur $\mathbb{Q}[X]$ (et aussi sur $\mathbb{Z}[X]$ car primitif), alors P est un polynôme cyclotomique.

En effet, P et Φ_d partagent une racine pour un certain d d'après le th précédent. P et Φ_d sont alors des facteurs irréductibles de $X^n - 1$ dans sa décomposition en facteurs ~~premiers~~ dans $\mathbb{Q}[X]$.

Ils partagent une racine et sont unitaires : ils sont donc égaux.

(On peut utiliser Bézout pour prouver l'impossibilité de partager une racine, même dans $\mathbb{C}$.)