141, 144

Ref:

Théorème de Kronecker :

Soit $P \in \mathbb{Z}[X]$, unitaire, $\deg(P)=n$, $P = X^n + a_{n-1}X^{n-1} + \dots + a_0$, tq les racines de P dans $\mathbb{C}$ sont toutes non-nulles de module ≤ 1.

Alors les racines de P sont des racines de l'unité.

démo :

Etape 1 : Montrons qu'à n fixé, on a un nb fini de P ;

On a $P(X) = \prod_{i=1}^{n}(X-\lambda_i)$; $0 < |\lambda_i| \leq 1$

Et $\forall 0 \leq i \leq n-1$ $a_i = (-1)^{n-i} \Sigma_{n-i}(\lambda_1, \dots, \lambda_n)$
$= (-1)^{n-i} \sum_{1 \leq j_1 < \dots < j_{n-i} \leq n} \lambda_{j_1} \cdots \lambda_{j_{n-i}}$

$\Rightarrow |a_i| \leq \sum_{1 \leq j_1 < \dots < j_{n-i} \leq n} 1$

$\leq (n-i)! \times \binom{n}{n-i}$

Les coeffs de P sont dans $\mathbb{Z}$ et bornés ; on a donc un nb fini de P de cette forme.

Etape 2 : Montrons que $|\lambda_i| = 1$, $\forall i$.

Comme $\forall i$, $|\lambda_i| > 0$, on a $a_0 = (-1)^n \lambda_1 \cdots \lambda_n \neq 0$

et $|a_0| \leq 1$. Donc $a_0 = \pm 1$.

Comme $|\lambda_i| \leq 1$, $\forall i$, on a $|\lambda_i| = 1$ $\forall i$, car sinon $\underset{1}{\underset{\shortparallel}{|a_0|}} = |\lambda_1| \dots |\lambda_n| < 1$.

Etape 3 :

Soit $p \in \mathbb{N}^*$. Soit $Q(X) = \prod_i (X - \lambda_i^p) \in \mathbb{C}[X]$. Montrons que $Q \in \mathbb{Z}[X]$.

On a $Q(X) = X^n + b_{n-1}X^{n-1} + \dots + b_0$, avec $b_i = (-1)^{n-i} \Sigma_{n-i}(\lambda_1^p, \dots, \lambda_n^p)$.

Or, dans $\mathbb{Z}[X_1, \dots, X_n]$, les polynômes $\Sigma_{n-i}(X_1^p, \dots, X_n^p)$ sont symétriques.
Le théorème de structure des poly sym nous dit qu'il existe $Q_i \in \mathbb{Z}[X_1, \dots, X_n]$ tq $\Sigma_{n-i}(X_1^p, \dots, X_n^p) = Q_i(\Sigma_1(X_1, \dots, X_n), \dots, \Sigma_n(X_1, \dots, X_n))$.

En évaluant X_i en λ_i par le morphisme d'évaluation, b_{n-i} est ainsi un polynôme à coefficients entiers en les q_j. Donc $b_{n-i} \in \mathbb{Z} \Rightarrow Q \in \mathbb{Z}[X] \Rightarrow Q$ vérifie la prop.

Comme on a un nb fini de poly vérifiant la prop,

leur ens de racine est fini aussi

Donc $\forall\, 1 \leq i \leq n$, $\exists \alpha_i$ tq $\lambda_i^{\alpha_i} = 1$. $\square$

<u>Rem</u> : Si P est aussi irred dans $\mathbb{Z}[X]$, alors P est un polynôme cyclotomique.

<u>démo</u> : Si P est irred dans $\mathbb{Z}[X]$, P est irred dans $\mathbb{Q}[X]$ car P unitaire.

Soit ξ une racine de P. $\cancel{\xi}$ ξ est une racine primitive m-ième de l'unité, pour un $m \geq 1$.

Alors $\begin{array}{l} X-\xi \mid P \\ X-\xi \mid \Phi(m) \end{array}$ dans $\mathbb{C}[X]$ $\Rightarrow$ $P \wedge \Phi(m) \neq /^{0}_{1}$ dans $\mathbb{C}[X]$ $\Rightarrow$ $P \wedge \Phi(m) \neq /^{0}_{1}$ dans $\mathbb{Q}[X]$

$\Rightarrow P = \Phi(m)$ car P, $\Phi(m)$ sont irred unitaires dans $\mathbb{Q}[X]$. $\square$