Références :
Algèbre 1, Serge Francinou

Théo (Relation coefficients/racines)**.** *Soit $P = X^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$ un polynôme unitaire de $\mathbb{K}[X]$ de degré n. Supposons P scindé dans $\mathbb{K}[X]$. Notons $x_1, ..., x_n$ ses racines (pas forcément distinctes). On définit, pour tout $p \in [\![1, n]\!]$,*

$$\sigma_p = \sum_{1 \leq i_1 < ... < i_p \leq n} \prod_{i=1}^{p} x_{i_p}.$$

Alors on a

$$\sigma_k = (-1)^k a_{n-k}.$$

Théo. *Soit $P \in A[X_1, ..., X_n]$ symétrique. Alors il existe un unique polynôme $Q \in A[Y_1, ..., Y_n]$ tel que $P(X_1, ..., X_n) = Q(\Sigma_1, ..., \Sigma_n)$.*

Théo. *Soit P un polynôme unitaire de $\mathbb{Z}[X]$ dont les racines complexes sont toutes de module inférieure ou égal à 1. On suppose $P(0) \neq 0$. Alors toutes les racines de P sont des racines de l'unité.*

Démonstration. Notons $z_1, ..., z_n$ les racines de P (n étant le degré de P) et soit $\sigma_1, ..., \sigma_n$ les fonctions symétriques élémentaires des z_i. On a donc

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

et les σ_i sont donc dans $\mathbb{Z}$. Comme $|z_i| \leq 1$ pour tout $i \in [\![1, n]\!]$, on obtient, pour tout $p \in [\![1, n]\!]$, la majoration

$$|\sigma_p| = \left| \sum_{I \in \mathcal{P}_p([\![1,n]\!])} \prod_{i \in I} x_{i_p} \right| \leq \sum_{I \in \mathcal{P}_p([\![1,n]\!])} 1 = Card(\mathcal{P}_p([\![1, n]\!]) = \binom{n}{p}$$

Cela montre que l'ensemble Ω_n des polynômes unitaires de $\mathbb{Z}[X]$ de degré n, dont les racines complexes sont de module inférieur ou égal à 1 est fini.
On va maintenant considérer, pour tout $k \in \mathbb{N}^*$, les polynômes $P_k(X) = (X - z_1^k)...(X - z_n^k)$. Ce sont des polynômes unitaires de degré n dont les racines z_i^k sont de module inférieur ou égal à 1. Pour $r \in [\![1, n]\!]$, le coefficient de X^{n-r} dans P_k est $(-1)^r \sigma_r(z_1^k, ..., z_n^k)$. Il s'agit donc d'un polynôme symétrique en $z_1, ..., z_n$ à coefficients dans $\mathbb{Z}$. Il est donc égal, par le théorème de structure des polynômes symétriques, à un polynôme à coefficients entiers en les fonctions symétriques élémentaires des z_i. Il en résulte que pour tout entier k, $P_k \in \mathbb{Z}[X]$ et donc que $P_k \in \Omega_n$. Comme Ω_n est fini, et que chaque élément de Ω_n admet au plus n racines complexes distinctes, l'ensemble des racines des éléments de Ω_n est aussi fini. En particulier, pour tout $i \in [\![1, n]\!]$, l'application $k \mapsto z_i^k$ ne peut pas être injective (car dans ce cas-là, on aurait une infinité de polynôme P_k dans Ω_n). Il existe donc deux entiers $k \neq l$ tels que $z_i^k = z_i^l$. Comme z_i est supposé non nul, il s'agit d'une racine de l'unité. □

Cor. Soit $P \in \mathbb{Z}[X]$ unitaire et irréductible tel que toutes les racines de P soient dans $D(0, 1)$. 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 et donc $P | X^N - 1$ pour un certain N. Or

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

avec ϕ_d irréductible sur $\mathbb{Z}[X]$ (irréductible sur $\mathbb{Q}[X]$ et primitif car unitaire). De plus $P \neq 1$ (car P irréductible) donc $P = \phi_d$ pour un certain d. □

Leçons possibles : 102 - 144