Développement : Théorème de Kronecker.

RM

2022-2023

Référence :

1. Oral à l'agreg

Énoncé :

Théorème (Kronecker) 1 : Soit $\alpha \neq 0$ un entier algébrique (i.e un nombre algébrique dont le polynôme minimal unitaire est dans $\mathbb{Z}[X]$) dont tous les conjugués appartiennent à $D = \{z \in \mathbb{C}, |z| \leq 1\}$ le disque unité. Alors α est une racine de l'unité, i.e il existe $m \in \mathbb{N}^*$ tel que $\alpha^m = 1$.

On rappelle avant quelques notions :
Soit $\mathbb{A}$ un anneau unitaire. On dit que $P \in \mathbb{A}[X_1, ..., X_n]$ est symétrique si $P(X_1, ..., X_n) = P(X_{\sigma(1)}, ..., X_{\sigma(n)})$ pour tout $\sigma \in \mathfrak{S}_n$. Les conjugués d'un nombre algébrique z sont les racines complexes du polynôme μ_z (y compris z).

Définition 2 : Pour $n \in \mathbb{N}$ et $k \in [\![0\,;n]\!]$, on définit le polynôme symétrique élémentaire e_k de $\mathbb{A}[X_1, ..., X_n]$ par

$$e_k = \sum_{I \in \mathcal{P}_k([\![1\,;n]\!])} \prod_{i \in I} X_i$$

où $\mathcal{P}_k([\![1\,;n]\!])$ désigne l'ensemble des parties à k éléments de $\{1, ..., n\}$.

Théorème 3 : Soit $P \in \mathbb{A}[X]$ un polynôme scindé unitaire, dont on note $z_1, ..., z_n$ ses racines. Alors pour tout $k \in [\![0\,;n]\!]$, on a $e_k(z_1, ..., z_n) = (-1)^k a_{n-k}$.

Théorème 4 : Pour tout $P \in \mathbb{A}[X_1, ..., X_n]$ symétrique, il existe un unique polynôme $Q \in \mathbb{A}[X_1, ..., X_n]$ tel que $P(X_1, ..., X_n) = Q(e_1, ..., e_n)$.

Lemme (Gauss) 5 : Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire tel que $P = QR$ avec $Q, R \in \mathbb{Q}[X]$ tous les deux unitaires. Alors $Q \in \mathbb{Z}[X]$ et $R \in \mathbb{Z}[X]$.

Résolution :

Théorème 6 : Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire tel que toutes ses racines complexes appartiennent à $D \setminus \{0\}$. Alors toutes ses racines sont des racines de l'unité.

Démonstration : Notons Ω_n l'ensemble des polynômes unitaires de $\mathbb{Z}[X]$ de degré n dont les racines complexes appartiennent à D. La première étape est de montrer que Ω_n est un ensemble fini à l'aide des relations coefficients-racines (Théorème 3). En effet, soit $Q \in \Omega_n$ dont on note (a_k) les coefficients et (z_i) les racines complexes. En notant $\sigma_k = e_k(z_1, ..., z_n)$ pour tout $k \in [\![0\,;n]\!]$, le Théorème 3 assure que $\sigma_k = (-1)^k a_{n-k}$. Alors pour tout k,

$$|\sigma_k| = \left| \sum_{I \in \mathcal{P}_k([\![1\,;n]\!])} \prod_{i \in I} z_i \right| \leq \sum_{I \in \mathcal{P}_k([\![1\,;n]\!])} \prod_{i \in I} |z_i| \leq card(\mathcal{P}_k([\![1\,;n]\!]) = \binom{n}{k}.$$

On a donc $|a_k| \leq \binom{n}{n-k}$ pour tout $k \in [\![1\,;n]\!]$, d'où Ω_n est bien fini.
On note maintenant (z_i) les racines de P (non nuls) et, pour tout entier k, on définit $P_k = (X - z_1^k)...(X - z_n^k) \in \mathbb{C}[X]$. Ces sont des polynômes unitaires de degré n dont les racines z_i^k sont de module inférieur ou égale à 1 (car $z_i \in D$). Pour $r \in [\![1\,;n]\!]$, le coefficient de X^{n-r} de P_k est $(-1)^r e_r(z_1^k, ..., z_n^k)$ d'après le Théorème 4. Comme le polynôme $e_r(X_1^k, ..., X_n^k) \in \mathbb{Z}[X_1, ..., X_n]$ est symétrique, alors, d'après le Théorème 4, il existe $Q_{r,k} \in \mathbb{Z}[X_1, ..., X_n]$ tel que

$$e_r(X_1^k, ..., X_n^k) = Q_{r,k}(e_1(X_1, ..., X_n), ..., e_n(X_1, ..., X_n)).$$

Or, comme $P \in \mathbb{Z}[X]$, on a $e_m(z_1, ..., z_n) = (-1)^m a_{n-m}$ ou $(a_i)_{i \in [\![1\,;n]\!]}$ les coefficients de P, or $(-1)^m a_{n_m} \in \mathbb{Z}$ et donc, $e_m(z_1, ..., z_n) \in \mathbb{Z}$. Donc $Q_{r,k}(e_1(z_1, ..., z_n), ..., e_n(z_1, ..., z_n)) \in \mathbb{Z}[X]$ et finalement $e_r(z_1^k, ..., z_n^k) \in \mathbb{Z}$. Donc tous les coefficients de P_k sont dans $\mathbb{Z}$, et donc $P_k \in \mathbb{Z}[X]$ et donc $P_k \in \Omega_n$.
Comme l'ensemble Ω_n est fini, l'ensemble des racines de tous les P_k, qui est formellement $\{x \in \mathbb{C} : \exists k \in \mathbb{N} : P_k(x) = 0\}$, est fini. Soit $i \in [\![1\,;n]\!]$, l'ensemble $\{z_i^k : k \in \mathbb{N}\}$ est inclus dans l'ensemble fini de ces racines. Il est donc lui aussi fini et on en déduit qu'il existe deux entiers k et k' tels que $z_i^k = z_i^{k'}$. Comme z_i est non nul, alors en supposant $k > k'$ sans perte de généralité, on a $z_i^{k-k'} = z_i^m = 1$. On conclut que toutes les racines z_i de P sont des racines de l'unité. □

Ceci prouve bien le théorème car si on prend $\alpha \neq 0$ un entier algébrique tels que tous ces conjugués appartient à D, alors son polynôme minimal vérifie le théorème précédent et donc tous les conjugués de α sont des racines de l'unité. Or α et aussi une racine de ce polynôme minimal, donc α est aussi une racine de l'unité ce qui termine la preuve.

Corollaire 7 : Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire et irréductible sur $\mathbb{Q}$ tel que toutes les racines complexes soient de modules au plus 1. Alors $P = X$ ou P est un polynôme cyclotomique.

Démonstration : Si 0 est racine de P alors $X|P$ et donc $P = X$ car P est irréductible et unitaire. Sinon 0 n'est pas racine et on peut appliquer le théorème précédent qui implique que les racines de P sont toutes des racines de l'unité : il existe donc $N \in \mathbb{N}$ tel que P divise $(X^N - 1)^n$, où $n = deg(P)$ (ici il faut prendre N tel que pour tout x racine de P, $x^N = 1$). Or la décomposition en irréductibles dans $\mathbb{Q}[X]$ de $X^N - 1$ est

$$X^N - 1 = \prod_{d|N} \Phi_d(X).$$

Or comme P est unitaire, donc primitif et irréductible dans $\mathbb{Z}[X]$, on en déduit qu'il est irréductible dans $\mathbb{Q}[X]$ et donc qu'il est premier, donc il divise $(X^N - 1)$. Or par unicité de la décomposition en irréductible de $X^N - 1$, on a un $d \in \mathbb{N}$ divisant n tel que $P = \Phi_d$.