Gourdon Algèbre (3e) p95
Oraux X-ENS Algèbre 1 (2e) p213

THÉORÈMES DE KRONECKER

102
144

Soient K un corps, et A un sous-anneau de K. Pour $P \in A[X]$, on pose $Z_K(P) = \{\alpha \in K \mid P(\alpha) = 0\}$.
On pose également $B^1 = \{z \in \mathbb{C} \mid |z| \leq 1\}$ et on note $\mathbb{U}$ l'ensemble des racines complexes de l'unité.

Thm 1 : Soit $P \in \mathbb{Z}[X]$ unitaire tel que $Z_{\mathbb{C}}(P) \subseteq B^1$ et $P(0) \neq 0$. Alors $Z_{\mathbb{C}}(P) \subseteq \mathbb{U}$.

Thm 2 : Soit $P \in \mathbb{Z}[X]$ unitaire et irréductible sur $\mathbb{Q}$. Si $Z_{\mathbb{C}}(P) \subseteq B^1$, alors $P = X$ ou P est cyclotomique.

Preuve de Thm 1 : Soit $n \in \mathbb{N}^*$, notons Ω_n l'ensemble des polynômes de degré n satisfaisant les hypothèses.

▸ Soit $P \in \Omega_n$, notons $z_1, \dots, z_n$ les racines de P comptées sans leur multiplicité. D'après les relations coefficients-racines, $P = X^n + \sum_{k=1}^{n} (-1)^k \sigma_k(z_1, \dots, z_n) X^{n-k}$ où $\sigma_k(X_1, \dots, X_n) = \sum_{1 \leq i_1 < \dots < i_k \leq n} X_{i_1} \cdots X_{i_k}$ est le k-ième polynôme symétrique élémentaire (à n variables). Comme $P \in \mathbb{Z}[X]$, pour tout $k \in [\![1, n]\!]$, $\sigma_k(z_1, \dots, z_n) \in \mathbb{Z}$. Or :

$$|\sigma_k(z_1, \dots, z_n)| \leq \sum_{1 \leq i_1 < \dots < i_k \leq n} |z_{i_1}| \cdots |z_{i_k}| \leq \sum_{1 \leq i_1 < \dots < i_k \leq n} 1 = \binom{n}{k}$$

Comme $\sigma_k(z_1, \dots, z_n)$ est entier, il ne peut alors prendre qu'un nombre fini de valeurs ; a fortiori, Ω_n est fini.

▸ Pour $k \in \mathbb{N}^*$, posons $P_k = \prod_{m=1}^{n} (X - z_m^k)$ Pour $r \in [\![1, n]\!]$, posons $\sigma_r^{(k)} := \sigma_r(z_1^k, \dots, z_n^k)$, de sorte que $P_k = X^n + \sum_{r=1}^{n} (-1)^r \sigma_r^{(k)} X^{n-r}$.

Soit $r \in [\![1, n]\!]$. Posons $Q_r(X_1, \dots, X_n) = \sum_{1 \leq i_1 < \dots < i_r \leq n} X_{i_1}^k \cdots X_{i_r}^k$, de sorte que $\sigma_r^{(k)} = Q_r(z_1, \dots, z_n)$. Comme Q_r est symétrique, il existe $T_r \in \mathbb{Z}[X]$ tel que $Q_r(X_1, \dots, X_n) = T_r(\sigma_1(X_1, \dots, X_n), \dots, \sigma_n(X_1, \dots, X_n))$. En particulier, $\sigma_r^{(k)} = T_r(\sigma_1^{(1)}, \dots, \sigma_n^{(1)}) \in \mathbb{Z}$. De là, $P_k \in \mathbb{Z}[X]$. A fortiori, $P_k \in \Omega_n$.

▸ Comme Ω_n est fini, $\bigcup_{P \in \Omega_n} Z_{\mathbb{C}}(P)$ est aussi finie, et ne contient pas 0. De là, pour tout $m \in [\![1, n]\!]$, l'ensemble $\{z_m^k\}_{k \geq 1} = \bigcup_{k \geq 1} Z_{\mathbb{C}}(P_k) \subseteq \bigcup_{P \in \Omega_n} Z_{\mathbb{C}}(P)$ est fini, donc il existe $k_1 > k_2 \geq 1$ tels que $z_m^{k_1} = z_m^{k_2}$, donc $z_m^{k_1 - k_2} = 1$ (car $z_m \neq 0$), et $z_m \in \mathbb{U}$. Ainsi, $Z_{\mathbb{C}}(P) \subseteq \mathbb{U}$. ■

Preuve du Thm 2 : D'après Thm 1, si $P(0) \neq 0$, alors $Z_{\mathbb{C}}(P) \subseteq \mathbb{U}$. Soit $z \in Z_{\mathbb{C}}(P)$, il existe $k \in \mathbb{N}^*$ tel que $z^k = 1$. Quitte à remplacer k par l'un de ses diviseurs, z est une racine primitive k^e de l'unité, donc $\Phi_k \mid P$. Or Φ_k et P sont irréductibles et unitaires, $P = \Phi_k$.
Si $P(0) = 0$, alors $X \mid P$, et par le même argument, $P = X$. ■