Théorème de KRONECKER

Florian BOUGUET

Références :
– SZPIRGLAS : Mathématiques L3 Algèbre
– FRANCINOU, GIANELLA, NICOLAS : Oraux X-ENS, Algèbre 1

On notera $Z(P)$ l'ensemble des racines complexes d'un polynôme, et $d°P$ son degré.

Soit $n \in \mathbb{N}^*$ et soit Ω_n l'ensemble des polynômes de $\mathbb{R}[X]$ tel que

$$P \in \Omega_n \Leftrightarrow \begin{cases} d°P = n \\ P \in \mathbb{Z}[X] \\ P \text{ unitaire} \\ z \in Z(P) \Rightarrow 0 < |z| \leq 1 \end{cases}$$

La dernière caractérisation de Ω_n se reformule aussi en disant que les racines de P sont de module inférieur à 1 et que X ne divise pas P ou que P a un terme constant non nul.

Theorème 1 (*de* KRONECKER)

Si $P \in \Omega_n$
Alors les racines de P sont racines de l'unité

Preuve :
Soit un tel P, notons

$$\begin{aligned} P &= X^n + a_1 X^{n-1} + \cdots + a_{n-1}X + a_n \\ &= (X - \alpha_1)\dots(X - \alpha_n) \end{aligned}$$

A noter que $a_n \neq 0$ et $0 < \alpha_i \leq 1$. On peut alors utiliser la relation coefficient-racines (se démontre facilement par récurrence sur n) :

$$a_p = (-1)^p \sigma_p(\alpha_1 \dots \alpha_n) \qquad \text{avec } \sigma_p(\alpha_1 \dots \alpha_n) = \sum_{1 \leq i_1 < \cdots < i_p \leq n} \alpha_{i_1} \dots \alpha_{i_p}$$

Les σ_p sont appelés polynômes symétriques élémentaires ; on a par exemple

$$\begin{aligned} \sigma_1(\alpha_1 \dots \alpha_n) &= \alpha_1 + \alpha_2 + \cdots + \alpha_n \\ \sigma_n(\alpha_1 \dots \alpha_n) &= \alpha_1 \alpha_2 \dots \alpha_n \end{aligned}$$

Bon, il est temps de rentrer dans le vif du sujet.

$$|a_p| = \left| \sum_{1 \leq i_1 < \cdots < i_p \leq n} \alpha_{i_1} \dots \alpha_{i_p} \right| \leq \sum_{1 \leq i_1 < \cdots < i_p \leq n} 1 = \binom{n}{p}$$

n étant fixé et a_p étant un entier, a_p ne peut prendre qu'un nombre fini de valeurs. On ne peut donc faire qu'un nombre fini de combinaisons des a_p, majoré (très) grossièrement par

$$2n \left(\max_{1 \leq p \leq n} \binom{n}{p} \right)$$

Quoi qu'il en soit, $\sharp(\Omega_n) < \infty$.

Pour $k \in \mathbb{N}^*$, notons

$$P_k = (X - \alpha_1^k) \dots (X - \alpha_n^k)$$

Remarquons que $P = P_1$. On va montrer que $P_k \in \Omega_n$ pour tout k. Soit donc $k \leq 2$. On peut déjà remarquer que P_k est unitaire de degré n, et $0 < |\alpha_i^k| \leq 1$. Il reste à montrer que ses coefficients sont entiers.

On va introduire,pour $\lambda \in \mathbb{C}$, $Q_k^\lambda = X^k - \lambda$ et, pour finir, le résultant suivant (de taille $k + n$) :

$$R_k(\lambda) = Res(P, Q_k^\lambda) = \begin{vmatrix} 1 & & & & 1 & & \\ a_1 & \ddots & & & 0 & \ddots & \\ \vdots & \ddots & \ddots & & \vdots & \ddots & 1 \\ a_n & & \ddots & 1 & 0 & & 0 \\ & \ddots & & a_1 & \lambda & \ddots & \vdots \\ & & \ddots & \vdots & & \ddots & 0 \\ & & & a_n & & & \lambda \end{vmatrix}$$

On voit bien que R_k est polynomial en λ (si l'on préfère, il est assez aisé de raisonner dans $\mathbb{Z}[\lambda]$) et que ses coefficients sont entiers (les a_p étant entiers). Pour conclure, on va exprimer le résultant en fonction des racines des polynômes (on rappelle que P est unitaire et que ses racines sont les α_i) :

$$R_k(\lambda) = Res(P, Q_k^\lambda) = \prod_{i=1}^{n} Q_k^\lambda(\alpha_i) = \prod_{i=1}^{n} (\alpha_i^k - \lambda) = (-1)^n P_k(\lambda)$$

Les coefficients de R_k sont entiers, donc ceux de P_k les sont aussi. Donc $P_k \in \Omega_n$.

La fin de la démonstration est alors facile. Notons

$$\varphi_i : k \mapsto \alpha_i^k$$

Ω_n étant un ensemble fini, l'ensemble $\cup_{Q \in \Omega_n} Z(Q)$ est lui aussi fini et donc φ_i ne peut être injective. Donc il existe des entiers p et q tels que

$$\alpha_i^p = \alpha_i^q$$

Donc $\alpha_i^{p-q} = 1$ car $\alpha_i \neq 0$.

$\square$