Un théorème de Kronecker

Patrice Lassère[1]

[1], Université Paul Sabatier, Toulouse

11 août 2023

Exercice 0.1 ★ ***Un théorème de Kronecker***

Par ***polynôme de Sylvester*** *on entend tout polynôme $P \in \mathbb{Z}[X]$ unitaire à racines de module inférieur où égal à 1. Montrer que*

(Kronecker) *Les zéros non nuls d'un polynôme de Sylvester sont des racines de l'unité.*

Solution : *Soit $n \in \mathbb{N}^\star$. Notons Z_n la collection des zéros (comptés avec leurs multiplicités) de l'ensemble $\mathscr{S}_n$ des polynômes de Sylvester de degré inférieur où égal à n.*

*- **Étape 1 :** Pour $n \in \mathbb{N}^\star$: $s_n := \text{card}(\mathscr{S}_n)$ est fini.*

Soit $p(z) = z^n + a_{n-1}z^{n-1} + \dots + a_0 \ = \ \prod_{i=1}^n (z - \zeta_i) \ \in \mathscr{S}_n$, avec les formules de Newton, si $0 \leq k \leq n-1$ on a

$$|a_k| = \Big| \sum_{1 \leq i_1 < \dots < i_k \leq n} (-1)^k \zeta_{i_1} \dots \zeta_{i_k} \Big| \leq \sum_{1 \leq i_1 < \dots < i_k \leq n} |\zeta_{i_1} \dots \zeta_{i_k}| \leq C_n^k \leq n!,$$

les coefficients a_k étant entiers, il n'y a qu'un choix fini de a_k et s_n est fini.

*- **Étape 2 :** $(\ \zeta \in Z_n) \Longrightarrow \big(\ \zeta^k \in Z_n,\ \forall\, k \in \mathbb{N}\big)$.*

Soit $p(z) = z^n + a_{n-1}z^{n-1} + \dots + a_0 \in \mathbb{Z}[X]$, sa matrice compagnon

$$C_p = \begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 1 & -a_{n-1} \end{pmatrix} \in M_n(\mathbb{Z})$$

est triangularisable dans $M_n(\mathbb{C})$, il existe $G \in GL_n(\mathbb{C})$ telle que

$$C_p = G^{-1} \begin{pmatrix} \zeta_1 & & ? \\ & \ddots & \\ 0 & & \zeta_n \end{pmatrix} G.$$

Mais alors

$$C_p^N = G^{-1}\begin{pmatrix}\zeta_1^N & & ? \\ & \ddots & \\ 0 & & \zeta_n^N\end{pmatrix} G \in M_n(\mathbb{Z}),$$

autrement dit C_p^N est une matrice à coefficients dans $\mathbb{Z}$ qui admet $\zeta_1^N, \dots \zeta_n^N$ comme valeurs propres : son polynôme caractéristique répond à la question.

- ***Étape 3 :*** La conclusion.

Supposons qu'il existe un polynôme $p \in K_n$ admettant au moins une racine, (disons ζ_1) qui ne soit ni racine de l'unité, ni de module strictement compris entre 0 et 1, l'ensemble $\{\zeta_1^N\}_{N\in\mathbb{N}^\star}$ est alors de cardinal ***infini****. D'autre part, par la seconde étape $p_{C_p^N}(\zeta_1^N) = 0,\ \forall N \in \mathbb{N}^\star$, si bien que l'ensemble infini $\{\zeta_1^N\}_{N\in\mathbb{N}^\star}$ est inclu dans Z_n de cardinal* ***fini*** *(étape 1) et on a la contradiction désirée.*

Remarques : - *On peut tout aussi bien montrer qu'un polynôme de Sylvester est sans zéros de module strictement compris entre 0 et 1 de la manière suivante : soit $p(z) = z^k \prod_{i=k+1}^n (z-\zeta_i) \in K_n$, toujours avec Newton : $1 \leq |a_k| = |\zeta_{k+1}\dots\zeta_n| \leq 1$, soit $|\zeta_{k+1}| = \dots = |\zeta_n| = 1$.*

- *On pourra aussi consulter les ouvrages de J.M.Arnaudies & J.Bertin* "Groupes, Algèbre et Géométrie" *tome 1, pages 127-128, Ellipse, (1993) ou E.Leichnam* "Exercices corrigés de Mathématiques, Polytechnique, ENS" (Algèbre et Géométrie), *exercice 1-30, Ellipse, (1999) pour d'autres approches.*

- *Un* **entier algébrique** *est une racine d'un polynôme unitaire $P(X) = X^d + a_{d-1}X^{d-1} + \dots + a_1X + a_0 \in \mathbb{Z}[X]$. On a*

« Un entier algébrique est soit entier, soit irrationnel. »

Cette assertion repose essentiellement sur les idées précédentes, en voici donc les étapes principales :

$\rightsquigarrow$ *$\alpha \in \mathbb{C}$ est un entier algébrique si, et seulement si, il est valeur propre d'une matrice à coefficients entiers.*

$\rightsquigarrow$ *Si $A \in M_n(\mathbb{Z})$ admet une valeur propre λ rationnelle, alors A admet un vecteur propre à coordonnées entières associé à la valeur propre λ.*

$\rightsquigarrow$ *Soit α un entier algébrique racine d'un polynôme $P \in \mathbb{Z}[X]$ de degré $n \geq 2$. Si $\alpha \in \mathbb{Q}\setminus\mathbb{Z}$ considérons $k \in \mathbb{Z}$ tel que $k < \alpha < k+1$ et $A := C_P - kI_n \in M_n(\mathbb{Z})$. On vérifie facilement que $\lambda := \alpha - k$ est valeur propre de A, puis en considérant la suite $(A^mX)_m$ où $X \in \mathbb{Z}^n$ vérifie $AX = \lambda X$, conclure.*

Références