Anaël Marit ENS Rennes

THÉORÈME DE KRONECKER

- 102, 144 –

—

On va dans ce développement démontrer un théorème attribué à Kronecker qui montre une certaine rigidité sur le lieu des racines d'un polynôme à coefficients entiers. J'ai ajouté deux applications, une qu'on trouve sur beaucoup d'autres versions et une autre moins connue. Selon votre vitesse, vous pouvez choisir d'en traiter une à l'oral. Je pense que celle sur les matrices apportera un vrai plus au développement, l'autre apparaissant plus comme une curiosité amusante.

Etant donné un polynôme P à coefficients complexes, on notera $\mathcal{Z}(P)$ un $\deg(P)$-uplet composé de toutes ses racines complexes avec multiplicité. Pour $n \in \mathbb{N}^*$ et $1 \leqslant k \leqslant n$, on désigne par $\sigma_{n,k}$ le k-ième polynôme symétrique élémentaire à n indéterminées, soit :

$$\sigma_{n,k} := \sum_{I \in \mathcal{P}_k(\llbracket 1,n \rrbracket)} \prod_{i \in I} T_i \tag{1}$$

avec $\mathcal{P}_k(\llbracket 1, n \rrbracket)$ l'ensemble des parties à k éléments de $\llbracket 1, n \rrbracket$.

Notre objectif est de démontrer :

Théorème 1 (Kronecker ([1], exercice 3.17)). *Soit $P \in \mathbb{Z}[X]$ unitaire dont toutes les racines complexes sont de module au plus 1. Toutes les racines non nulles de P sont des racines de l'unité.*

Le théorème

Commençons par remarquer qu'on peut écrire $P = X^p Q$ avec $Q(0) \neq 0$. Dans ce cas, Q est nécessairement à coefficients entiers, unitaire, et ses racines sont les racines non nulles de P. Quitte à travailler sur Q, on supposera donc dans toute la suite que $P(0) \neq 0$.

On va montrer que toutes les racines de P sont d'ordre fini dans $\mathbb{C}^\times$. Notons n le degré de P. On introduit $\Omega_n := \{Q \in \mathbb{Z}[X] \text{ unitaire} \mid \deg(Q) = n \wedge \mathcal{Z}(Q) \in \bar{B}(0,1)^n\}$. C'est un ensemble fini. En effet, prenons $Q \in \Omega_n$. Alors, en notant $(r_1, \dots, r_n) := \mathcal{Z}(Q)$:

$$Q = X^n + \sum_{k=0}^{n-1} (-1)^{n-k} \sigma_{n,k}(r_1, \dots, r_n) X^k \tag{2}$$

par relations racines-coefficients. Or on a :

$$|\sigma_{n,k}(r_1, \dots, r_n)| \leqslant \sum_{I \in \mathcal{P}_k(\llbracket 1,n \rrbracket)} \prod_{i \in I} |z_i| \leqslant \binom{n}{k} \tag{3}$$

Contactez-moi en cas de coquille à prénom.nom@ens-rennes.fr !

Comme ces coefficients sont entiers, ils ne peuvent prendre qu'un nombre fini de valeurs et Ω_n est fini.

Il découle alors immédiatement que l'ensemble des racines des polynômes de Ω_n est fini. Notons $(z_1, \dots, z_n) = \mathcal{Z}(P)$. Les (z_i) sont non nuls car 0 n'est pas une racine de P par hypothèse. Posons :

$$\forall l \in \mathbb{N}^*,\ Q_l := \prod_{i=1}^{n} (X - T_i^l) \in \mathbb{Z}[X][T_1, \dots, T_n] \tag{4}$$

Pour tout $l \in \mathbb{N}$, Q_l est symétrique en les indéterminées (T_i). Par théorème de structure des polynômes symétriques, il existe $R_l \in \mathbb{Z}[X][S_1, \dots, S_n]$ tel que :

$$Q_l = R_l(\sigma_{n,1}, \dots, \sigma_{n,n}) \tag{5}$$

Ainsi, le polynôme $Q_l(z_1, \dots, z_n) = R_l(\sigma_{n,1}(z_1, \dots, z_n), \dots, \sigma_{n,n}(z_1, \dots, z_n))$ est à coefficients entiers. Comme il est trivialement unitaire et que ses racines sont de module au plus 1, les (z_i^l) sont racines d'un polynôme de Ω_n. Il est résulte que le morphisme de groupes $l \mapsto z_i^l$ ne peut pas être injectif, et donc z_i est d'ordre fini, ce qui achève la démonstration du théorème ! □

Deux applications

Commençons par une première application surprenante de ce théorème, qui complètera agréablement ce développement un peu court :

Application 2. (Sous-groupes finis de $GL_n(\mathbb{Z})$ ([1], remarque 3.20)) Soit $n \in \mathbb{N}^*$. Si G est un sous-groupe fini de $GL_n(\mathbb{Z})$, alors l'ordre de G satisfait l'inégalité :

$$|G| \leqslant \prod_{k=0}^{n-1} (3^n - 3^k) \tag{6}$$

Démonstration. Commençons par donner du sens à ce majorant : il s'agit du cardinal de $GL_n(\mathbb{F}_3)$, où $\mathbb{F}_3$ désigne le corps à 3 éléments. Ceci nous aiguille pour amorcer la preuve : on va construire une injection de G dans $GL_n(\mathbb{F}_3)$. Le candidat est naturel : la projection naturelle $\mathbb{Z} \twoheadrightarrow \mathbb{F}_3$ s'étend en un morphisme d'anneaux $\mathbb{M}_n(\mathbb{Z}) \twoheadrightarrow \mathbb{M}_n(\mathbb{F}_3)$ en l'appliquant coordonnée par coordonnée. Comme un morphisme d'anneaux envoie toujours les inversibles sur les inversibles, celui-ci se retreint en un morphisme de groupes $GL_n(\mathbb{Z}) \twoheadrightarrow GL_n(\mathbb{F}_3)$ dont on notera π la restriction à G. Montrons que π est injectif.

Soit $M \in \mathrm{Ker}(\pi)$. Comme M appartient à G, c'est une matrice d'ordre fini, donc toutes ses valeurs propres complexes sont des racines de l'unité (car le polynôme $X^{|G|} - 1$ annule M). Par ailleurs, $\pi(M) = \bar{I_n}$ la matrice identité de $GL_n(\mathbb{F}_3)$. Ainsi, il existe une matrice A à coefficients entiers telle que :

$$M = I_n + 3A \tag{7}$$

On aura montré notre résultat si on montre que $A = 0$. On isole A dans l'équation :

$$A = \frac{1}{3}(M - I_n) \tag{8}$$

On déduit deux choses de cette écriture :

1. A est diagonalisable dans $\mathbb{C}$. En effet, M est annulée par un polynôme scindé à racines simples, donc est diagonalisable, et la translation par l'identité n'y change rien.
2. Les valeurs propres de A sont exactement les éléments de la forme $\frac{\lambda-1}{3}$ avec λ une valeur propre de M.

Or :

$$\forall \lambda \in \mathrm{Sp}(M),\ \left|\frac{\lambda-1}{3}\right| \leqslant \frac{|\lambda|+1}{3} < 1 \tag{9}$$

car le spectre de M est inclus dans $\mathbb{U}$. On va ainsi chercher à appliquer le théorème de Kronecker au polynôme caractéristique de A, qui est unitaire et à coefficients entiers. Ses racines non nulles sont nécessairement des racines de l'unité, or on a montré que celles-ci sont de module inférieur strict à 1. Donc χ_A n'a pas de racine non nulle et A est nilpotente. Comme elle est également disagonalisable, elle est nulle, et π est injectif. On a bien :

$$|G| \leqslant |GL_n(\mathbb{F}_3)| = \prod_{k=0}^{n-1}(3^n - 3^k) \tag{10}$$

□

Remarque : Pourquoi $\mathbb{F}_3$, et pas un autre corps fini ? En fait, pour n'importe quel nombre premier p, on peut construire pareillement un morphisme $\pi_p : G \to GL_n(\mathbb{F}_p)$ et dérouler la démonstration. Toutefois, pour $p = 2$, on n'aura plus la majoration stricte du module des valeurs propres de A, et donc on ne pourra pas conclure que $A = 0$. Pour les autres nombres premiers, tout fonctionnent pareil ; le choix $p = 3$ est simplement celui qui donne la majoration la plus fine. ♦

Voici une deuxième application, beaucoup plus rapide à traiter, qui demande toutefois de connaître quelques résultats sur la cyclotomie.

Application 3. Soit $P \in \mathbb{Z}[X]$ unitaire et irréductible sur $\mathbb{Q}$. Si toutes les racines complexes de P sont de module au plus 1, alors P est X ou un polynôme cyclotomique.

Démonstration. Si $P(0) = 0$, $X|P$ et par irréductibilité de P, $P = X$. Dans le cas contraire, toutes les racines de P sont des racines de l'unité d'après le théorème de Kronecker. Comme P est irréducible sur $\mathbb{Q}$, c'est le polynôme minimal d'une racine de l'unité, c'est-à-dire que c'est un polynôme cyclotomique. □

Références

[1] Philippe Caldero et Marie Peronnier. *Carnet de voyage en Algébrie*. Calvage et Mounet, 2022. isbn : 9782493230034.