Développement: Groupes finis de matrices à coefficients entiers.

Arthur Maritch-Roy

Dans ce développement, on s'intéresse aux sous-groupes finis de $\mathrm{GL}_n(\mathbb{Z})$, et on montre que leur cardinal peut être borné indépendamment du groupe.

Proposition 1. Soit $M \in \mathrm{GL}_n(\mathbb{Z})$ d'ordre fini d. Alors M est diagonalisable et ses valeurs propres sont des racines d-ièmes de l'unité.

Démonstration. Par définition, le polynôme $X^d - 1$ annule M et ce polynôme est scindé à racines simples. Ainsi M est diagonalisable et ses racines figurent parmi les racines de $X^d - 1$, *i.e.* parmi les racines d-ièmes de l'unité. $\square$

Théorème 2. Soit M une matrice de $\mathrm{GL}_n(\mathbb{Z})$ d'ordre fini. L'ensemble des ordres possibles pour M est fini.

Démonstration. Avec la proposition précédente, on sait que le polynôme caractéristique de M n'a que des racines dans $\mathbb{U}_d$ où d est l'ordre de M. À l'aide des relations coefficients racines, on obtient, si $\chi_M = X^n + \sum_{k=0}^{n-1} a_k X^k = (X - z_1) \cdots (X - z_n)$:

$$a_{n-k} = (-1)^k \sum_{1 \leq i_1 < \ldots < i_k \leq n} z_{i_1} \cdots z_{i_k},$$

et en prenant le module :

$$|a_{n-k}| \leq \binom{n}{k}.$$

Ainsi, puisque χ_M est un polynôme de $\mathbb{Z}[X]$ à coefficients bornés, il n'y a qu'un nombre fini de valeurs possibles pour chaque coefficient, donc un nombre fini de polynômes caractéristiques possibles, indépendamment de l'ordre !

Or l'ordre de la matrice M correspond au ppcm des ordres (dans $(\mathbb{C}^*, \times)$) de ses racines. Comme M ne peut avoir qu'un nombre fini de polynômes caractéristiques possibles, il ne peut y avoir qu'un nombre fini de tels ppcm, donc les ordre possibles pour M sont bien finis. $\square$

Théorème 3. Soit G un sous-groupe fini de $\mathrm{GL}_n(\mathbb{Z})$. Alors son cardinal est borné par 3^{n^2}.

Démonstration. On veut injecter, en réduisant les coefficients, G dans $\mathcal{M}_\backslash(\mathbb{Z}/m\mathbb{Z})$ où m est un entier plus grand que 3. Soient g et h deux éléments de G. On suppose que $g - h$ vaut 0 modulo m. Ainsi on peut écrire $g - h = mB$ avec $B \in \mathcal{M}_n(\mathbb{Z})$. On a alors

$$A := h^{-1}B = (h^{-1}g - I_n)/m \in \mathcal{M}_n(\mathbb{Z}).$$

Puisque $h^{-1}g$ est un élément de G, il est diagonalisable et ses valeurs propres sont des racines de l'unité. Ainsi A est également diagonalisable et ses valeurs propres sont bornées par $\frac{2}{m} < 1$ par inégalité triangulaire. Ainsi la suite des puissances de A tend vers 0 par continuité du produit matriciel. Ainsi les suites des coefficients de A tendent vers 0, mais comme ce sont des suites entières donc elles stationnent. En somme A est nilpotente.

La matrice A est alors diagonalisable et nilpotente, ce qui montre que son polynôme minimal est X est donc que A est nulle. Ainsi, en remontant les calculs, on remarque que l'on a montré que la réduction modulo m est une injection de G dans $\mathcal{M}_n(\mathbb{Z}/m\mathbb{Z})$. En particulier, pour $m = 3$, on obtient le résultat voulu. $\square$

Référence : Sujet X-ENS maths A de 2021.