Théorème de Kronecker et application

S. Francinou, H. Gianella, S. Nicolas, *Exercices de mathématiques, Oraux X-ENS, Algèbre 1*, 3e édition, Cassini. Exercice 5.33 page 213 pour le premier théorème.

S. Francinou, H. Gianella, S. Nicolas, *Exercices de mathématiques, Oraux X-ENS, Algèbre 2*, 3e édition, Cassini. Exercice 3.20 page 205 pour le second théorème.

Recasage : 142, 144.

Théorème 1

Soit $P \in \mathbb{Z}[X]$ unitaire dont les racines complexes sont de module inférieur ou égal à 1. On suppose que $P(0) \neq 0$. Alors les racines de P sont des racines de l'unité.

▷ Notons Ω_n l'ensemble des polynômes unitaires de $\mathbb{Z}[X]$, de degré n, dont les racines sont de module inférieur ou égal à 1.

– *Étape 1 : Montrons que Ω_n est fini.* Soit $P \in \Omega_n$. Notons $z_1, \dots, z_n$ ses racines et $\sigma_1, \dots, \sigma_n$ les fonctions symétriques élémentaires associées. Pour tout $k \in [\![1, n]\!]$, on a $\sigma_k \in \mathbb{Z}$ et, comme $|z_1|, \dots, |z_n| \leq 1$,

$$|\sigma_k| = \left| \sum_{\substack{I \in \mathfrak{P}([\![1,n]\!]) \\ \#I = k}} \prod_{i \in I} z_i \right| \leq \#\{I \in \mathfrak{P}([\![1, n]\!]),\ \#I = k\} = \binom{n}{k}.$$

L'ensemble des $(\sigma_k)_{1 \leq k \leq n}$ est donc fini. Comme tout $P \in \Omega_n$ s'écrit $P = X^n - \sigma_1 X^{n-1} + \dots + (-1)^n \sigma_n$, on en déduit que Ω_n est fini (et $|\Omega_n| \leq 2^n - 1$).

– *Étape 2 : Principe des tiroirs.* Soit $P \in \Omega_n$ que l'on écrit

$$P = \prod_{i=1}^{n} (X - z_i).$$

Montrons que pour tout $k \in \mathbb{N}^*$, $P_k = \prod_{i=1}^{n} (X - z_i^k) \in \Omega_n$.

⋆ P_k est bien unitaire de degré n et ses racines z_i^k sont de module inférieur ou égal à 1.

⋆ Il reste donc à vérifier que $P_k \in \mathbb{Z}[X]$. Or pour $i \in [\![1, n]\!]$, le coefficient de X^{n-i} dans l'écriture de P_k dans la base canonique est $(-1)^i \sigma_i(z_1^k, \dots, z_n^k)$ où $\sigma_i(z_1^k, \dots, z_n^k)$ sont les fonctions symétriques élémentaires associées à $z_1^k, \dots, z_n^k$. Ces fonctions sont des polynômes symétriques en $z_1, \dots, z_n$ à coefficients dans $\mathbb{Z}$. D'après le théorème de structure, $\sigma_i(z_1^k, \dots, z_n^k) \in \mathbb{Z}[\sigma_1, \dots, \sigma_n]$ pour tout $1 \leq i \leq n$. Ainsi, $P_k \in \mathbb{Z}[X]$.

Ainsi, comme Ω_n est fini, il existe $k > \ell$ tel que $P_k = P_\ell$ donc $\forall 1 \leq i \leq n$, $z_i^k = z_i^\ell$, d'où, comme 0 n'est pas une racine de P, $z_i^{k-\ell} = 1$, $\forall 1 \leq i \leq n$. □

Corollaire 2

Soient $m \geq 3$ et $n \in \mathbb{N}$. Si G est un groupe fini de $\mathrm{GL}_n(\mathbb{Z})$ alors G est isomorphe à un sous-groupe de $\mathrm{GL}_n(\mathbb{Z}/m\mathbb{Z})$.

▷ Il suffit de montrer que la projection canonique $G \to \mathrm{GL}_n(\mathbb{Z}/m\mathbb{Z})$ est injective.

Soit $A \in G$ tel que $\overline{A} = \overline{I_n} \in \mathrm{GL}_n(\mathbb{Z}/m\mathbb{Z})$. Il existe $B \in \mathcal{M}_n(\mathbb{Z})$ telle que $A = I_n + B$. Soit β une valeur propre de B. Alors $\alpha = 1 + m\beta$ est valeur propre de A. Or, d'après le théorème de Lagrange, $A^{|G|} = I_n$ donc $\alpha^{|G|} = 1$ et en particulier $|\alpha| = 1$. Alors,

$$|\beta| = \frac{|\alpha - 1|}{m} \leq \frac{2}{m} < 1.$$

Ainsi, $(-1)^n \chi_B \in \mathbb{Z}[X]$ est unitaire et ses racines sont de module < 1. On déduit du théorème de Kronecker que $\chi_B = (-X)^n$.

Or, comme $X^{|G|} - 1$ est scindé à racines simples et annule A, A est diagonalisable, donc B est diagonalisable. Ainsi, $B = 0$ et $A = I_n$. □

Corollaire 3

Si G est un sous-groupe fini de $\mathrm{GL}_n(\mathbb{Z})$, alors

$$|G| \leq (3^n - 3^{n-1})(3^n - 3^{n-2}) \cdots (3^n - 3)(3^n - 1).$$