# 3 Théorème de Kronecker

**Théorème** (Kronecker)**.** *Soit $P \in \mathbb{Z}[X]$ unitaire tel que $P(0) \neq 0$. Si toutes les racines de $P$ sont de module inférieur à 1, ce sont des racines de l'unité.*

Soit $n = \deg P$. Soit $A_n$ l'ensemble des polynômes de degré $n$ vérifiant les mêmes hypothèses que $P$, montrons qu'il est fini. On note $\sigma_j \in \mathbb{Z}[T_1, \cdots, T_n]$ le $j$-ième polynôme symétrique élémentaire, de sorte que pour $Q \in A_n$ de racines $\lambda_1, \cdots, \lambda_n$, on a

$$Q(X) = \prod_{i=1}^{n}(X - \lambda_i) = \sum_{j=0}^{n}(-1)^j \sigma_j(\lambda_1, \cdots, \lambda_n) X^{n-j} = \sum_{j=0}^{n} c_j X^{n-j}.$$

or pour tout $j$, $c_j \in \mathbb{Z}$ car $Q \in \mathbb{Z}[X]$, et

$$|c_j| \leq |\sigma_j(\lambda_1, \cdots, \lambda_n)| \leq \sum_{1 \leq k_1 < \cdots < k_j \leq n} \prod_{\ell=1}^{j} |\lambda_{k_j}| \leq \binom{n}{j}$$

par hypothèse sur les racines de $Q$. On a donc un nombre fini de valeurs possibles pour chaque $c_j$, donc $A_n$ est fini.

Ensuite, notons pour tout $k \in \mathbb{N}^*$, avec $\lambda_1, \cdots, \lambda_n$ les racines de $P$, dont on fait une fois pour toutes un choix d'indexation.

$$P^{(k)} = \prod_{i=1}^{n}(X - \lambda_i^k) = \sum_{j=0}^{n} c_j^{(k)} X^{n-j}.$$

Par construction, les $c_j^{(k)}$ sont tous des polynômes symétriques élémentaires à coefficients entiers en les $\lambda_i$. D'après le théorème de décomposition en polynômes symétriques élémentaires, on a donc

$$c_j^{(k)} = R_{j,k}(\sigma_1(\lambda_1, \cdots, \lambda_n), \cdots, \sigma_n(\lambda_1, \cdots, \lambda_n))$$

pour un certain polynôme $R_{j,k} \in \mathbb{Z}[T_1, \cdots, T_n]$. En conséquence, $c_j^{(k)} \in \mathbb{Z}$ et $P^{(k)} \in A_n$ pour tout $k \in \mathbb{N}^*$.

Comme $A_n$ est fini, par le principe des tiroirs, il existe donc $k \neq k'$ tel que $P^{(k)} = P^{(k')}$, et donc une permutation $\sigma \in \mathcal{S}_n$ telle que

$$(\lambda_1^k, \cdots, \lambda_n^k) = (\lambda_{\sigma(1)}^{k'}, \cdots, \lambda_{\sigma(n)}^{k'}).$$

On démontre maintenant par récurrence sur $\ell \in \mathbb{N}$ que pour tout $i \in [1, n]$,

$$\lambda_{\sigma^\ell(i)}^{k'^\ell} = \lambda_i^{k^\ell}.$$

C'est le cas pour $\ell = 1$ par définition de $\sigma$. Maintenant, si cette formule est vraie pour $\ell \geq 1$, pour tout $i \in [1, n]$,

$$\lambda_{\sigma^{\ell+1}(i)}^{k'^{\ell+1}} = \lambda_{\sigma^\ell(\sigma(i))}^{k'^{\ell+1}} = \left(\lambda_{\sigma(i)}^{k'^\ell}\right) = \lambda_i^{k^{\ell+1}}$$

en appliquant la formule pour $\ell$ à $\lambda_{\sigma(i)}^{k'}$.

En particulier, pour $\ell$ l'ordre de $\sigma$ dans $\mathcal{S}_n$, pour tout $i \in [1, n]$, $\lambda_i^{k^\ell} = \lambda_i^{k'^\ell}$ donc $\lambda_i^{k^\ell - k'^\ell} = 1$. Ainsi, toutes les racines de $P$ sont des racines de l'unité, ce qui conclut la preuve.

**Corollaire 3.1.** *Pour tout $m \geq 3$ entier et tout $n \in \mathbb{N}$, si $G$ est un sous-groupe fini de $\mathrm{GL}_n(\mathbb{Z})$, la projection modulo $m$ de $G$ dans $\mathrm{GL}_n(\mathbb{Z}/m\mathbb{Z})$ est injective. En particulier, tout sous-groupe fini de $\mathrm{GL}_n(\mathbb{Z})$ est isomorphe à un sous-groupe de $\mathrm{GL}_n(\mathbb{Z}/3\mathbb{Z})$.*

*Démonstration.* Soit $A \in G$ tel que $\overline{A} = 1$ dans $\mathrm{GL}_n(\mathbb{Z}/m\mathbb{Z})$, alors $A = I_n + mB$ avec $B \in M_n(\mathbb{Z})$. Comme $G$ est fini, il existe $e$ tel que $A^e = 1$.

De plus, les valeurs propres de $B$ sont annulées par son polynôme caractéristique $\chi_B \in \mathbb{Z}[X]$ qui est unitaire, ce sont donc des entiers algébriques et pour $\beta$ une valeur propre de $B$, $\alpha = 1 + m\beta$ est une valeur propre de $A$ donc $\alpha^e = 1$ et $|\alpha| = 1$. Alors,

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

donc toutes les racines de $\chi_B$ sont nulles par le théorème de Kronecker, or $B$ est diagonalisable sur $\mathbb{C}$ car $A$ l'est, donc $B = 0$ et $A = I_n$. □

Leçons compatibles :

102 Groupe des nombres complexe de module 1, sous-groupe des racines de l'unités. Applications.

105 Groupe des permutations d'un ensemble fini. Applications

142 Algèbre des polynômes à plusieurs indéterminées. Applications

144 Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications.

Référence : [FGN], 5.28.