Théorème de Kronecker

Théorème. *Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire dont toutes les racines complexes sont dans le disque unité fermé. Alors les racines de P sont 0 ou des racines de l'unité, et P est un produit de X et de polynômes cyclotomiques.*

Lemme. *A un anneau (On l'utilisera pour $\mathbb{Z}$), $n \geq 1$, On note $\sigma_k = \sum_{1 \leq i_1 < i_2 < .. < i_k \leq n} X_{i_1}..X_{i_k}$ le k-ième polynôme symétrique élémentaire (avec la convention $\sigma_0 = 1$). Alors*

$$A[X_1, .., X_n]^{S_n} = A[\sigma_0, \sigma_1, .., \sigma_n]$$

Démonstration. On munie $\mathbb{N}^n$ de l'ordre lexicographique, et pour $P = \sum_{\alpha \in \mathbb{N}^n} P_\alpha X^\alpha$, on note $o(P) = \sup(\alpha | P_\alpha \neq 0)$. Soit $P \in A[X_1, .., X_n]^{S_n}$ non constant, $\alpha = o(P)$. Comme P est symétrique, on a $\alpha_1 \geq .. \geq \alpha_n$.
On note $\beta_n = \alpha_n$ et $\beta_k = \alpha_k - \beta_{k+1}$, tel que pour tout k, $\beta_k + .. + \beta_n = \alpha_k$. On a alors :

$$o(P - P_\alpha \sigma_1^{\beta_1} \sigma_2^{\beta_2} .. \sigma_n^{\beta_n}) < o(P)$$

Comme l'ordre lexicographique est bien fondé, cette procédure se poursuit jusqu'à ce que P soit constant. □

Démonstration. Soit n le degré de P. Quitte à diviser P par un X^k, on suppose $P(0) \neq 0$.
On note ξ_1,..,xi_n les racines (avec multiplicité) de P.
Soit E l'ensemble des polynômes de degré n unitaires à coefficients entiers dont toutes les racines complexes sont dans le disque unité fermé. Montrons que E est fini.
En effet, pour tout Q dans E, de racines $\omega_1, .., \omega_n$. Soit $0 \leq k \leq n$, on a

$$|Q_k| = |(-1)^k \sigma_{n-k}(\omega_1, .., \omega_n)| \leq C_k^n$$

Donc $|E| \leq \Pi_{k=0}^n C_k^n < \infty$; E est fini.

Soit $P^m = \Pi_{k=0}^n (X - \xi_k^m)$. Vérifions que P^m est dans E. Il suffit de vérifier que P^m est à coefficient entier.
Première méthode :

$$P_k^m = (-1)^k \sigma_{n-k}(\xi_1^m, .., \xi_n^m)$$

C'est un polynôme en les $(\xi_k)_k$ à coefficients entiers, symétrique en les $(\xi_k)_k$, donc c'est un polynôme entier en les $\sigma_k(\xi_1, .., \xi_n)$, qui sont entier car P est à coefficients entiers. Donc P^m est dans E.
Seconde méthode :
Soit $C \in M_n(\mathbb{Z})$ la matrice compagnon associée à P. On peut trigonaliser cette matrice, et on observe alors que pour tout m, on a $P^m = \chi_{C^m} \in \mathbb{Z}[X]$.

Comme E est fini, il existe $r < s$ tels que $P^r = P^s$. Il existe donc une permutation $\phi \in S_n$ telle que pour tout k, $\xi_k^r = \xi_{\phi(k)}^s$. Soit N l'ordre de ϕ, on a $\xi_k^{s^N} = \xi_{\phi^N(k)}^{s^N} = \xi_k^{r^N}$, donc pour tout k, $\xi_k^{s^N - r^N} = 1$: les ξ_k sont des racines de l'unité. □

Corollaire. *Soit G un sous-groupe de $GL_n(\mathbb{Z})$ dont les éléments sont d'exposant fini, et $m \geq 3$. On note $\pi_m : GL_n(\mathbb{Z}) \to GL_n(\mathbb{Z}/m\mathbb{Z})$ la projection. Alors $\pi_{|G}$ est injectif. De plus, si les éléments non triviaux de G sont d'ordre impairs, alors cela marche aussi pour $m = 2$.*

Démonstration. Soit $M \in G \setminus \{I_n\}$ tel que $\pi_m(M) = I_n$. Il existe $N \in M_n(\mathbb{Z})$ telle que $M = I_n + mN$. On note P_M, P_N les polynômes caractéristiques de M, N, comme M est d'exposant fini, ses racines sont des racines de l'unité. On vérifie aisément que

$$P_N(X) = m^{-n} P_M(1 + mX)$$

Donc les racines de P_N sont de la forme $\frac{\xi - 1}{m}$ où ξ est une racine de l'unité différente de -1 si M est d'ordre impair. Alors $|\frac{\xi-1}{m}| < 1$, donc selon le théorème, $\frac{\xi-1}{m} = 0$ et $N = 0$. □

Polygones constructibles

Théorème. *Le polygone régulier à n coté est constructible si et seulement si n est produit de puissances de 2 et de nombres premiers de la forme $2^n + 1$ distincts.*

Notation : $w_n = \exp(2\pi i/n)$. Le polygone régulier à n coté est constructible si et seulement si il existe une tour d'extensions de degré consécutif 2, notées $\mathbb{Q} = K_0 \subset K_1 \subset .. \subset K_r$ telle que $w_n \in K_r$.

Lemme. *Soient n, m premiers entre eux, w_{nm} est constructible si et seulement si w_n et w_m le sont.*

Démonstration. On a $w_{nm}^n = w_m$, $w_{nm}^m = w_n$. Réciproquement, il existe $u, v \in \mathbb{Z}$ tels que $un + vm = 1$. Alors $w_{nm} = w_n^u w_m^v$. □

Lemme. *w_{2^n} est constructible et si p est un nombre premier impair tel que w_{p^n} est constructible, alors $n = 1$ et $p - 1$ est une puissance de 2.*

Démonstration. w_{2^n} est constructible par construction de médiatrices successives du diamètre du cercle.
Si w_{p^n} est constructible, alors $[\mathbb{Q}(w_{p^n}) : \mathbb{Q}]$ est une puissance de 2.
Or, $[\mathbb{Q}(w_{p^n}) : \mathbb{Q}] = \deg(\phi_{p^n}) = \varphi(p^n) = p^{n-1}(p-1)$. Donc $p^{n-1} = 1$ et $(p-1)$ est une puissance de 2. □

Il suffit donc de montrer que les nombres premiers impairs p tels que $p - 1$ est une puissance de 2 sont bien constructibles.

Démonstration. Soit p un tel nombre premier, G le groupe des $\mathbb{Q}$-automorphismes de $\mathbb{Q}(w_p)$, montrons que $G \cong (\mathbb{Z}/p\mathbb{Z})^*$.
Les racines de ϕ_p sont exactement les w_p^k, $k \in (\mathbb{Z}/p\mathbb{Z})^*$. Un élément de G est entièrement déterminé par sa valeur en w_p, ce qui donne un morphisme injectif :

$$\begin{cases} G \to (\mathbb{Z}/p\mathbb{Z})^* \\ \sigma \mapsto \sigma(w_p) \end{cases}$$

Il suffit de montrer la surjectivité. Soit $k \in (\mathbb{Z}/p\mathbb{Z})^*$. Les morphismes d'anneau suivants : $Ev_1 : \begin{cases} \mathbb{Q}[X] \to \mathbb{Q}(w_n) \\ Q(X) \mapsto Q(w_p) \end{cases}$ et $Ev_k : \begin{cases} \mathbb{Q}[X] \to \mathbb{Q}(w_n) \\ Q(X) \mapsto Q(w_p^k) \end{cases}$ passent au quotient en des isomorphismes entre $\mathbb{Q}(w_n)$ et $\frac{\mathbb{Q}[X]}{(\phi_p)}$; composer les deux donne un automorphisme qui envoie w_p sur w_p^k, ce qui achève cette partie de la preuve.
G est donc cyclique : soit $\sigma \in G$ un générateur de G. σ est d'ordre $p - 1 = 2^n$. On définie $K_k = \mathrm{Fix}(\sigma^{2^k})$, on considère la tour d'extension $K_0 \subset .. \subset K_n$.
- $K_n = \mathbb{Q}(w_p)$ car $\sigma^{2^n} = Id$.

- $K_0 = \mathbb{Q}$. En effet, $(w_p^k)_{k=1..p-1}$ est une $\mathbb{Q}$-base de $\mathbb{Q}(w_p)$ (par argument de dimension) et si $\sum_{k=1}^{p-1} \lambda_k w_p^k$ est fixé par σ, comme σ agit comme le générateur de $(\mathbb{Z}/p\mathbb{Z})^*$, il agit comme une permutation cyclique de $(\mathbb{Z}/p\mathbb{Z})^*$, donc tous les λ_k sont égaux et $\sum_{k=1}^{p-1} \lambda_k w_p^k = -\lambda_1 \in \mathbb{Q}$.
- $[K_{k+1} : K_k] \leq 2$: En effet, si on note $\tau_k = \sigma^{2^k}_{|K_{k+1}}$, alors c'est un K_k-endomorphisme linéaire de K_{k+1} (il suffit de vérifier que K_{k+1} est stable par σ^{2^k}). $\tau_k^2 = Id_{K_{k+1}}$ donc τ_k est diagonalisable de valeur propre ± 1. La valeur propre 1 est simple car son espace propre associé est K_k. La valeur propres -1 est simple car si v, w sont deux vecteurs propres de -1, alors v/w est un vecteur propre de 1, donc est dans K_k et v, w sont K_k-liés. Ainsi, $[K_{+1} : K_k] \leq 2$.

□

Référence : Tauvel