Théorème de Tchebotarev

Alexandre Abouda

8 juillet 2025

Proposition. *Soit p un nombre premier, et ω une racine complexe p-ième de l'unité. Alors tous les mineurs de la matrice de Vandermonde $\left(\omega^{kl}\right)_{0\leq k,l\leq p-1}$ sont non nuls.*

Introduisons $A = \mathbb{Z}[\omega]$, $K = \mathbb{Q}(\omega)$ et $\mathcal{I} = (1-\omega)A$. Notons que $K = \mathbb{Q}[X]/(\phi_p)$ est un $\mathbb{Q}$-espace vectoriel de dimension $\deg \phi_p = p-1$, où ϕ_p désigne le polynôme cyclotomique d'ordre p.

Considérons le morphisme d'anneaux $m : \begin{array}{ccc} K & \longrightarrow & \mathrm{End}(K) \\ x & \longmapsto & m_x : t \mapsto xt \end{array}$ et $N = \det \circ m$.

Lemme 1. *Soit $x \in A$. On a les propriétés suivantes :*
- *$\chi_{m_x} \in \mathbb{Z}[X]$*
- *$x \in A^\times$ si et seulement si $N(x) \in \{-1, 1\}$*

Démonstration du lemme 1. La matrice de m_x dans la base $(1, \omega, ..., \omega^{p-2})$ de K est à coefficients entiers puisque $m_x(\omega^j) = x\omega^j \in A$ pour tout $j \in [\![0, p-2]\!]$. Donc $\chi_{m_x} \in \mathbb{Z}[X]$. Ceci montre le premier point. Notons en particulier que $N(x) \in \mathbb{Z}$ (c'est à un signe près le coefficient constant de χ_{m_x}).

Montrons le second point. Si $x \in A^\times$, il existe $y \in A$ tel que $xy = 1$. Alors $N(x)N(y) = 1$ et comme $N(x)$ et $N(y)$ sont deux entiers par le premier point, il vient $N(x) \in \{-1, 1\}$. Réciproquement supposons $N(x) \in \{-1, 1\}$, on écrit $\chi_{m_x} = XQ(X) + (-1)^{p-1}N(x)$ avec $Q \in \mathbb{Z}[X]$ par le premier point. D'après le théorème de Cayley-Hamilton, $xQ(x) = (-1)^p N(x) \in \{-1, 1\}$, donc x est inversible.

□

Lemme 2. *L'anneau $A/\mathcal{I}$ est isomorphe au corps $\mathbb{Z}/p\mathbb{Z}$.*

Démonstration du lemme 2. Pour tout $P \in \mathbb{Z}[X]$, $P(\omega) \equiv P(1) \pmod{\mathcal{I}}$ donc tout élément de A est congru modulo $\mathcal{I}$ à un entier. La surjection canonique $A \longrightarrow A/\mathcal{I}$ induit alors un morphisme surjectif $\mathbb{Z} \longrightarrow A/\mathcal{I}$. Son noyau est $\mathbb{Z} \cap \mathcal{I}$: c'est un idéal de $\mathbb{Z}$, contenant p puisque $p \equiv \phi_p(1) \equiv \phi_p(\omega) \equiv 0 \pmod{\mathcal{I}}$. C'est donc $\mathbb{Z}$ ou $p\mathbb{Z}$.

Dans le premier cas, l'anneau $A/\mathcal{I}$ serait nul puis $1 - \omega \in A^\times$. Or $N(1-\omega) = \chi_{m_\omega}(1) = \phi_p(1) = p \notin \{-1, 1\}$ donc $1 - \omega$ n'est pas inversible d'après le lemme 1. Ainsi $\mathbb{Z} \cap \mathcal{I} = p\mathbb{Z}$ et le morphisme surjectif $\mathbb{Z} \longrightarrow A/\mathcal{I}$ induit un isomorphisme entre $\mathbb{Z}/p\mathbb{Z}$ et $A/\mathcal{I}$ par le théorème de factorisation.

□

Revenons maintenant à la proposition. Supposons par l'absurde que l'un des mineurs est nul. Il existe $r \in [\![1, p]\!]$ et I, J deux parties de cardinal r de $[\![0, p-1]\!]$ telles que $\left(\omega^{kl}\right)_{(k,l)\in I\times J}$ n'est pas dans $GL_r(\mathbb{C})$.

Ainsi $\left(\omega^{kl}\right)_{(k,l)\in I\times J}$ n'est pas dans $GL_r(K)$: il existe une combinaison linéaire non triviale à coefficients dans A (quitte à multiplier par un entier non nul) entre ses colonnes. Autrement dit, il existe $\lambda = (\lambda_l)_{l\in J} \in A^r \setminus \{0\}$ tel que le polynôme

$$P = \sum_{l\in J} \lambda_l X^l$$

s'annule en ω^k pour tout $k \in I$.

On se ramène au cas où l'un des λ_l n'est pas dans $\mathcal{I}$. En effet si $z \in A \setminus \{0\}$, l'ensemble

$$\{m \in \mathbb{N}\,;\, (1-\omega)^m \mid z\}$$

est fini car si $(1-\omega)^m \mid z$ alors $N((1-\omega)^m) \mid N(z)$ dans $\mathbb{Z}$, c'est-à-dire $p^m \mid N(z)$ donc $m \leq v_p(N(z))$.

La division euclidienne de P par le polynôme unitaire $\prod_{k\in I}\left(X-\omega^k\right)$ s'effectue dans $A[X]$. Il existe $Q \in A[X]$ tel que

$$P = \prod_{k\in I}\left(X-\omega^k\right) Q.$$

En réduisant modulo $\mathcal{I}$,

$$\tilde{P} = \left(X-\tilde{1}\right)^r \tilde{Q}.$$

En particulier pour tout $j \in [\![0, r-1]\!]$, $\tilde{P}^{(j)}(\tilde{1}) = 0$ c'est-à-dire

$$\sum_{l\in J} \tilde{\lambda_l} \prod_{k=0}^{j-1} (\tilde{l} - \tilde{k}) = 0. \tag{1}$$

Mais comme $\left(\prod_{k=0}^{j-1}(X-\tilde{k})\right)_{0\leq j\leq r-1}$ est une famille de r polynômes de degrés échelonnés, tous de degrés au plus $r-1$, c'est une base de $(A/\mathcal{I})[X]_{\leq r-1}$. D'après (1),

$$\sum_{l\in J} \tilde{\lambda_l} R(\tilde{l}) = 0 \tag{2}$$

pour tout polynôme $R \in (A/\mathcal{I})[X]_{\leq r-1}$. Comme J est une partie de $[\![0, p-1]\!]$, les $\tilde{l}$ pour $l \in J$ sont deux à deux distincts d'après le lemme 2. Soit $l \in J$. En prenant $R = \prod_{l'\in J\setminus\{l\}}(X-\tilde{l'})$ dans (2), il vient $\tilde{\lambda_l} = 0$. On en déduit que le polynôme $\tilde{P}$ est nul, une contradiction puisque l'un des λ_l n'est pas dans $\mathcal{I}$.

Voici une application de ce théorème. Notons G le groupe cyclique $\mathbb{Z}/p\mathbb{Z}$ de cardinal p. On note $\mathbb{C}[G]$ l'espace vectoriel complexe des fonctions de G dans $\mathbb{C}$, et $\widehat{G}$ le groupe des caractères de G. Les éléments de $\widehat{G}$ sont les $\chi_k : \tilde{l} \in G \longmapsto \omega^{kl}$ pour $k \in [\![0, p-1]\!]$, où $\tilde{l}$ désigne la classe de l modulo p. Si $f \in \mathbb{C}[G]$, sa transformée de Fourier est l'application $\widehat{f} : \chi \in \widehat{G} \longmapsto \sum_{l\in G} f(l)\overline{\chi(l)}$. On note aussi $S(f)$ le support de f.

Application (Principe d'incertitude de Tao)**.** Soit $f \in \mathbb{C}[G]\setminus\{0\}$. Alors $|S(f)| + |S(\widehat{f})| \geq p+1$.

Démonstration. Si $k \in [\![0, p-1]\!]$,

$$\widehat{f}(\chi_k) = \sum_{l\in G} f(l)\overline{\chi_k(l)} = \sum_{l\in S(f)} f(l)\omega^{-kl}.$$

Mais d'après la proposition, le polynôme $\sum_{l\in S(f)} f(l)X^l$ a au plus $|S(f)|-1$ racines dans $\mathbb{U}_p$, c'est-à-dire $p-|S(\widehat{f})|\leq |S(f)|-1$, ce qui est l'inégalité voulue.

□

Remarque. Ce développement est issu du sujet d'agrégation du concours spécial docteurs 2017. On y trouve d'autres applications de ce théorème.