Théorème de Kronecker

En utilisant les polynômes symétriques, nous montrons ici que toutes les racines d'un polynôme unitaire à coefficients entiers dont les racines sont dans $D(0,1) \setminus \{0\}$, sont en fait des racines de l'unité.

Lemme 1 (Relations de Viète)**.** Soient A un anneau commutatif unitaire intègre et $P = \sum_{i=1}^{n} a_i X^i \in A[X]$ que l'on suppose scindé dans $A[X]$ et tel que $a_n \in A^*$. Si on note $\Sigma_k(X_1, \dots, X_n)$ le k-ième polynôme symétrique élémentaire en n variables et α_1, ..., α_n les racines de P (comptées avec multiplicité), alors $\Sigma_k(\alpha_1, \dots, \alpha_n) = (-1)^k a_{n-k} a_n^{-1}$.

Démonstration. On a $P = a_n \prod_{i=1}^{n}(X - \alpha_i)$. En développant partiellement P, on a de même :

$$P = a_n X^n - a_n(\alpha_1 + \dots + \alpha_n)X^{n-1} + \dots + (-1)^n a_n \alpha_1 \dots \alpha_n$$

Par identification avec la forme développée, les coefficients de X^{n-1} doivent être égaux. En particulier :

$$a_{n-1} = -a_n(\alpha_1 + \dots + \alpha_n) \iff \underbrace{\alpha_1 + \dots + \alpha_n}_{=\Sigma_1(\alpha_1, \dots \alpha_n)} = -a_{n-1} a_n^{-1}$$

Et on procède de même pour trouver les autres coefficients. Par exemple, $a_0 = (-1)^n a_n \alpha_1 \dots \alpha_n \iff \Sigma_n(\alpha_1, \dots \alpha_n) = (-1)^n a_0 a_n^{-1}$. □

Remarque 2. Tout au long de ce développement, nous utiliserons implicitement le fait que tout polynôme à coefficient dans $\mathbb{C}$ (donc à fortiori aussi dans $\mathbb{Z}$) admet n racines complexes comptées avec multiplicité. Il s'agit du théorème de d'Alembert-Gauss.

Théorème 3 (Kronecker)**.** Soit $P \in \mathbb{Z}[X]$ unitaire tel que toutes ses racines complexes appartiennent au disque unité épointé en l'origine (que l'on note D). Alors toutes ses racines sont des racines de l'unité. **[I-P]** p. 279

Démonstration. Notons par Ω_n l'ensemble des polynômes unitaires à coefficients dans $\mathbb{Z}$ tels que toutes leurs racines complexes appartiennent à D. Soit $P \in \Omega_n$ dont on note $a_0, \dots, a_n$ les coefficients et $z_1, \dots, z_n$ les racines complexes. On note $\forall k \in [\![0, n]\!]$, $\sigma_k = \Sigma_k(z_1, \dots, z_n)$. D'après le Lemme 1, on a :

$$\forall k \in [\![0, n]\!], \sigma_k = (-1)^k a_{n-k} \qquad (*)$$

D'où $\forall k \in [\![0,n]\!]$:

$$\begin{aligned}|\sigma_k| &= \left|\sum_{I\in\mathscr{P}_k([\![1,n]\!])}\prod_{i\in I} z_i\right| \\ &\leq \sum_{I\in\mathscr{P}_k([\![1,n]\!])}\prod_{i\in I}|z_i| \\ &\leq |\mathscr{P}_k([\![1,n]\!])| \times 1 \\ &= \binom{n}{k}\end{aligned}$$

Et par $(*)$,

$$\forall k \in [\![0,n]\!],\ |a_k| \leq \binom{n}{n-k} = \binom{n}{k}$$

Ω_n est donc un ensemble fini (car on n'a qu'un nombre limité de choix possibles pour les coefficients a_k).

On pose maintenant

$$\forall k \in \mathbb{N},\ P_k = \prod_{j=0}^{n}(X - z_j^k)$$

qui sont des polynômes unitaires de degré n dont les racines $z_1^k, \dots, z_n^k$ appartiennent toutes à D. Soient $k \in \mathbb{N}$ et $r \in [\![0,n]\!]$. D'après le Lemme 1, le coefficient de X^{n-r} de P_k est $(-1)^r\Sigma_r(z_1^k,\dots,z_n^k)$. Mais, $\Sigma_r(X_1^k,\dots,X_n^k) \in \mathbb{Z}[X]$, donc on peut y appliquer le théorème fondamental des polynômes symétriques :

$$\exists Q_{r,k} \in \mathbb{Z}[X] \text{ tel que } \Sigma_r(X_1^k,\dots,X_n^k) = Q_{r,k}(\Sigma_1(X_1,\dots,X_n),\dots,\Sigma_n(X_1,\dots,X_n))$$

Or, comme $P \in \mathbb{Z}[X]$, on a $\forall j \in [\![0,n]\!]$, $\Sigma_j(z_1,\dots,z_n) \in \mathbb{Z}$ d'après le Lemme 1. En particulier, on a $\Sigma_r(X_1^k,\dots,X_n^k) \in \mathbb{Z}[X]$ car $Q_{r,k} \in \mathbb{Z}[X]$. On en déduit que $\forall k \in \mathbb{N}$, $P_k \in \Omega_n$.

Comme Ω_n est fini, l'ensemble des racines de tous les P_k ; qui est $\{z \in \mathbb{C} \mid \exists k \in \mathbb{N}, P_k(z) = 0\}$ est fini. Soit $j \in [\![1,n]\!]$. L'ensemble $\{z_j^k \mid k \in \mathbb{N}\}$ est inclus dans l'ensemble de ces racines, qui est fini ; il est donc lui-même fini :

$$\exists k \neq k' \text{ tel que } z_j^k = z_j^{k'}$$

Quitte à échanger les deux, on peut supposer $k \geq k'$. Comme $z_j \neq 0$, on a $z_j^{k-k'} = 1$. Donc z_j est une racine de l'unité ; ce que l'on voulait. □

Corollaire 4. Soit $P \in \mathbb{Z}[X]$ unitaire et irréductible sur $\mathbb{Q}$ tel que toutes ses racines complexes soient de module inférieur ou égal à 1. Alors $P = X$ ou P est un polynôme cyclotomique.

Démonstration. Si 0 est racine de P, alors $X \mid P$, donc $P = X$ par irréductibilité et unitarité. Sinon, 0 n'est pas racine de P. On peut donc appliquer le Théorème 3 à P ; et donc les racines de P sont des racines de l'unité. Ainsi, en notant N le maximum des ordres des racines de P, on a :

$$P \mid (X^N - 1)^n \text{ où } n = \deg(P)$$

Or, la décomposition en irréductibles de $X^N - 1$ est

$$X^N - 1 = \prod_{d|N} \Phi_d$$

Puisque $\mathbb{Q}[X]$ est un anneau factoriel, P est premier. Donc d'après le lemme de Gauss, comme $P \mid X^N - 1$:

$$\exists d \mid N \text{ tel que } P = \Phi_d$$

□

Bibliographie

L'oral à l'agrégation de mathématiques **[I-P]**

Lucas Isenmann et Timothée Pecatte. *L'oral à l'agrégation de mathématiques. Une sélection de développements*. 2e éd. Ellipses, 26 mars 2024.
https://www.editions-ellipses.fr/accueil/15218-28346-loral-a-lagregation-de-mathematiques-une-selection-de-developpements-2e-edition-9782340086487.html.