PRÉPARATION À L'AGRÉGATION EXTERNE : THÉORÈME DE KRONECKER

TONY LIMAGNE

Résumé. Il existe plusieurs manières de définir la complexité d'un polynôme à coefficients entiers (disons sa "hauteur"). La hauteur la plus naïve consiste à prendre comme mesure de complexité le maximum des modules des coefficients. Une autre manière consiste à construire une mesure à partir des racines : c'est la mesure de Malher. À l'aide des relations coefficients-racines et du principe des tiroirs de Dirichlet on peut caractériser les polynmes de $\mathbb{Z}[X]$ dont la mesure de Malher vaut 1. De façon assez surprenante, cette description est explicite : ce sont les polynômes qui admettent pour racines 0 ou des racines de l'unité. Et lorsqu'on restreint à l'ensemble des polynômes irréductibles de $\mathbb{Z}[X]$ on obtient même une caractérisation via les polynômes cyclotomiques. On aurait tord de reléguer ce résultat au rang d'une simple curiosité mathématique. Il s'agit en fait d'un cas particulier important d'un célèbre théorème de géométrie diophantienne : le théorème de Northcott.

Le développement ci-dessous est adapté pour les leçons 105, 127, 141, 144 et 190.

1. Préliminaires

Soit $f \in \mathbb{C}[X]$ de degré $n \geqslant 1$, écrit $f(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_0$. La *mesure de Malher* de f est par définition le nombre positif

$$M(f) = |a_n| \prod_{k=1}^{n} \max\{1, |\alpha_k|\},$$

où $\alpha_1, \ldots, \alpha_n$ sont les racines de f (comptées sans multiplicité). En particulier on a $M(f) \geqslant 1$. En pratique, la mesure de Malher s'utilise en lien avec les nombres algébriques. En effet, on sait qu'un nombre algébrique α est racine d'un unique polynôme irréductible et unitaire sur $\mathbb{Q}$. En multipliant ce polynôme par le ppcm de ses coefficients on obtient un polynôme à coefficients dans $\mathbb{Z}$ peut-être pas unitaire mais toujours irréductible (sur $\mathbb{Z}$) : c'est le *polynôme minimal de α sur $\mathbb{Z}$*. L'intérêt de ce passage de "$\mathbb{Q}[X]$ à $\mathbb{Z}[X]$" est de pouvoir effectuer des raisonnements de dénombrement (sur les coefficients des polynômes). Une question naturelle est-alors : peut-on caractériser les polynômes de $\mathbb{Z}[X]$ unitaire de mesure de Malher minimale (c'est-à-dire égale à 1) ?

2. Développement

Théorème 1 (Kronecker)**.** Soit $f \in \mathbb{Z}[X]$ unitaire, de degré $n \geqslant 1$ qui n'admet pas 0 pour racine.

Date: Année 2024.

(1) Si les racines complexes $\alpha_1, \dots, \alpha_n$ de f sont de module inférieur ou égal à 1 alors $\alpha_1, \dots, \alpha_n$ sont des racines de l'unité. Dans ce cas, on dit que f est un *polynôme de Kronecker*.

(2) Si de plus f est irréductible sur $\mathbb{Z}$ alors f est un polynôme cyclotomique.

Démonstration. (1) Fixons $k \in [\![1, n]\!]$. D'après les relations coefficients racines, le k^e coefficient de f est

$$\tau_k = \pm\Sigma_{n-k}(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}, \tag{R}$$

où Σ_k désigne la k^e fonction symétrique élémentaire. Et puisque $\alpha_1, \dots, \alpha_n$ sont de module inférieur ou égal à 1 on a donc

$$|\tau_k| \leqslant \binom{n}{k} \leqslant \max_{1 \leqslant k \leqslant n} \binom{n}{k}.$$

On en déduit que l'ensemble Ω des polynômes de Kronecker est fini, de même que l'ensemble A des racines des polynômes de Ω. Pour $N \in \mathbb{N}^*$ notons

$$f_N = (X - \alpha_1^N) \cdots (X - \alpha_n^N).$$

Toujours par les relations coefficients-racines, le k^e coefficient de f_N est

$$\pm\Sigma_{n-k}(\alpha_1^N, \dots, \alpha_n^N) = T_k(\alpha_1, \dots, \alpha_N),$$

où $T_k = \pm\Sigma_{n-k}(X_1^N, \dots, X_n^N)$. Le polynôme T_k est symétrique à coefficients entiers (puisque Σ_{n-k} l'est aussi). Le théorème de structure des polynômes symétriques donne donc $T_k \in \mathbb{Z}[\Sigma_1, \dots, \Sigma_n]$ et d'après l'égalité (R) on a

$$T_k(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}\,.$$

Ainsi on a f_N est un polynôme de Kronecker. Comme A est fini, l'application

$$\mathbb{N}^* \to \Omega \to A, n \mapsto f_n \mapsto \alpha_k^n,$$

est non injective [1] et il existe donc deux entiers n, m vérifiant $1 \leqslant n < m$ et $\alpha_k^m = \alpha_k^n$ c'est-à-dire $\alpha_k^{m-n} = 1$, ce qui conclut.

(2) Supposons de plus f irréductible sur $\mathbb{Z}$. Écrivons les racines $\alpha_1, \dots, \alpha_n$ de f sous la forme

$$\alpha_k = \exp\left(\frac{2i\pi l_k}{m_k}\right),$$

avec $m_k \geqslant 2$ et $l_k \in [1, m_k - 1]$ deux entiers. Les éléments $\alpha_1, \dots, \alpha_r$ sont dans le groupe M^e des racines de l'unité, où $M = \mathrm{ppcm}(m_1, \dots, m_n)$. Le polynôme f divise alors

$$X^M - 1 = \prod_{d|M} \Phi_d(X).$$

Or les polynômes cyclotomiques Φ_d sont à coefficients entiers et irréductibles sur $\mathbb{Z}$ de sorte que $f = \Phi_d$ pour un certain diviseur d de n (par le lemme d'Euclide et irréductibilité de f sur $\mathbb{Z}$). □

Remarque 2. (1) Le théorème 1 est un énoncé de minimisation. Il se peut se reformuler : un polynôme f unitaire et non constant de $\mathbb{Z}[X]$ est de mesure de Malher $M(f) = 1$ si et seulement si les racines complexes de f sont soient

1. C'est le principe des tiroirs de Dirichlet.

nulles ou soient des racines de l'unité (la disjonction n'est pas exclusive). Dans le cas où f est irréductible sur $\mathbb{Z}$ on obtient même

$$M(f) = 1 \quad \Leftrightarrow \quad f \text{ est un polynôme cyclotomique.}$$

(2) On peut justifier d'une autre manière que les polynômes f_N sont à coefficients entiers sans faire appel au théorème de structure des polynômes symétriques. En effet, notons $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ le corps de décomposition de f sur $\mathbb{Q}$. On sait que l'extension $K/\mathbb{Q}$ est galoisienne finie. Le corps des invariants sous l'action du groupe de Galois $G = \mathrm{Gal}(K/\mathbb{Q})$ est donc $\mathbb{Q}$. Chaque polynôme f_N est laissé fixe par les éléments de G, de sorte que f_N est à coefficients rationnels. Ensuite, on sait que les coefficients de f_N sont des polynômes en $\alpha_1, \ldots, \alpha_n$ qui sont des entiers algébriques. Ainsi les coefficients de f_N sont des entiers algébriques rationnels, donc des entiers relatifs (voir [HL, Chap. 8, §8.5, Exercice 8.3.5]).
Une autre manière de faire est de passer par les matrices compagnons. On note C_f la matrice compagnon de f. On sait déjà que C_f est à coefficients entiers. Lorsque $Q \in \mathbb{C}[X]$ et $A \in \mathrm{M}_n(\mathbb{C})$ on sait que le spectre de $Q(A)$ est l'ensemble

$$\{Q(\lambda) : \lambda \in \mathrm{Sp}(A)\}.$$

En particulier le spectre de C_f^N est $\{\alpha_k^N : k\}$ de sorte que $f_N = \pm\chi_{C_f^N}$ où $\chi_{C_f^N}$ est le polynôme caractéristique de C_f^N. Or C_f^N appartient à $\mathrm{M}_n(\mathbb{Z})$ et donc f_N est à coefficients entiers (voir [CP, Chap. I, §3, Exercice 3.17]).

Référence : [FGN, Chap. 4, Exercice 4.47] et [G, Chap. 2, §5, Problème 8].

Exercice 3 (Lemme de Serre)**.** Soient deux entiers $m \geqslant 3$ et $n \geqslant 1$. Soit G un sous-groupe fini de $\mathrm{GL}_n(\mathbb{Z})$. Montrer que le morphisme de réduction modulo m

$$G \to \mathrm{GL}_n(\mathbb{Z}/m\,\mathbb{Z}),$$

est injectif. En particulier, tout sous-groupe fini de $\mathrm{GL}_n(\mathbb{Z})$ est isomorphe à un sous-groupe de $\mathrm{GL}_n(\mathbb{F}_3)$.

Référence : [CP, Chap. I, §3, Remarque (3.20)].

Remarque 4. En 1933 D.H. Lehmer formula la conjecture suivante : pour tout $\epsilon > 0$, existe-il un polynôme f de $\mathbb{Z}[X]$ unitaire et non constant tel que

$$1 < M(f) < 1 + \epsilon \ ?$$

Encore aujourd'hui cette conjecture reste irrésolue (malgré d'actives recherches).

3. Polynômes de Kronecker

Il est clair qu'il y a que deux polynômes de Kronecker de degré 1 : $X - 1$ et $X + 1$. La méthode de dénombrement utilisée dans la preuve peut être employée pour déterminer les polynômes de Kronecker de degré 2. En effet, un tel polynôme s'écrit $X^2 + aX + b$ avec $a, b \in \mathbb{Z}, b \neq 0$, $|c| \leqslant 1$ et

$$|b| \leqslant \binom{2}{1} = 2,$$

ce qui laisse six possibilités : X^2+1, X^2+X+1, X^2-X+1, X^2-1, X^2-2X+1 et X^2+2X+1. La vraie difficulté commence à partir du cas $n = 3$. En fait il serait très difficile de trouver une formule du nombre $\mathrm{Kr}(n)$ de polynômes de Kronecker

de degré n. Une façon de palier à cette difficulté consiste à traiter ce problème de dénombrement du point de vue des séries génératrices. L'article [BM] trouve ainsi une formule faisant intervenir l'indicatrice ϕ d'Euler :

$$\sum_{n=0}^{+\infty} \mathrm{Kr}(n) z^n = \prod_{n=1}^{+\infty} \frac{1}{1-z^{\phi(n)}},$$

ce qui permet de calculer de proche en proche les termes $\mathrm{Kr}(n)$. En pratique on utilise le fait suivant : si un polynôme irréductible sur $\mathbb{Q}$ divise un polynôme de Kronecker alors il s'agit d'un polynôme cyclotomique. Et puisque l'anneau $\mathbb{Z}[X]$ est factoriel, on en déduit qu'un polynôme de Kronecker se factorise sur $\mathbb{Z}$ de manière unique en un produit de polynômes cyclotomiques (avec eventuellement des répétitions). Il se trouve qu'avec cette remarque et des techniques assez élémentaires le cas $n = 3$ est encore à porter de main.

Exercice 5. Déterminer tous les polynômes de Kronecker de degré 3.

Démonstration. Soit f un polynôme de Kronecker de degré 3. On distingue trois cas :

(1) *f est produit de trois polynômes cyclotomiques de degré* 1. Les seuls polynômes cyclotomiques de degré 1 sont $\Phi_1 = X - 1$ et $\Phi_2 = X + 1$. On a donc quatre possibilités pour f : Φ_1^3, Φ_2^3, $\Phi_1\Phi_2^2$ et $\Phi_1^2\Phi_2$.

(2) *f est produit d'un polynôme cyclotomique de degré* 1 *et d'un polynôme cyclotomique de degré* 2. Pour ce qui est du facteur de degré 1, il est à prendre parmi Φ_1 et Φ_2. Ensuite il faut caractériser les polynômes cyclotomiques de degré 2. Pour cela on cherche à résoudre l'équation diophantienne $\phi(k) = 2$. Soient k une solution et $p_1, \dots, p_r$ les facteurs premiers de k. À partir de la formule bien connue $\phi(k) = k\prod_{l=1}^{r}\left(1 - \frac{1}{p_l}\right)$ l'équation initiale $\phi(k) = 2$ devient

$$k\prod_{l=1}^{r}(p_l - 1) = 2\prod_{l=1}^{r} p_l. \tag{F}$$

Les seuls entiers d divisible par 2 tels que $d + 1$ est premier sont 1 et 2 de sorte que $p_l = 2$ ou 3 pour tout $i = 1, \dots, r$. On écrit alors $k = 2^\alpha 3^\beta$ avec $\alpha, \beta \in \mathbb{N}$. Si $\alpha \geqslant 1$ et $\beta \geqslant 1$ alors la relation (F) devient $2^\alpha 3^{\beta-1} = 2$ et donc $k = 2 \times 3 = 6$. Si $\alpha = 0$ et $\beta \geqslant 1$ alors la relation (F) devient $3^\beta = 3$ et donc $k = 3$. Si $\alpha \geqslant 1$ et $\beta = 1$ alors la relation (F) devient $2^\beta = 4$ et donc $k = 4$. Il y a donc en tout trois polynômes cyclotomiques de degré 2 : $\Phi_3 = X^2+X+1$, $\Phi_4 = X^2 - 1$ et $\Phi_6 = X^2 - X + 1$.

Ainsi il y a $2 \times 3 = 6$ possibilités d'écrire f comme produit d'un polynôme cyclotomique de degré 1 et d'un polynôme cyclotomique de degré 2, à savoir $\Phi_1\Phi_3$, $\Phi_2\Phi_3$, $\Phi_1\Phi_4$, $\Phi_2\Phi_4$, $\Phi_1\Phi_6$ et $\Phi_2\Phi_6$.

(3) *f est un polynôme cyclotomique de degré* 3. Ce dernier cas n'est pas possible. En effet, s'il existait un polynôme cyclotomique de degré 3 alors il admettrait une racine réelle (puisqu'il est à coefficients réels). Cette racine serait une racine primitive de l'unité. Or la seule racine primitive n^e de l'unité qui soit réelle est -1, dans le cas où $n = 2$, ce qui n'est pas le cas ici. Absurde.

Nous avons donc en tout dix polynômes de Kronecker de degré 3. □

4. Quelques questions bêtes auxquelles il faut absolument savoir répondre rapidement

(1) Donner un contre-exemple au théorème de Kronecker dans le cas où f n'est pas supposé unitaire. [2]

(2) Donner un contre-exemple au théorème de Kronecker dans le cas où f n'est pas supposé à coefficients entiers. [3].

(3)

Références

[FGN] S. Francinou, H Gianella et S. Nicolas, *Oraux X-ENS*, Vol. 1, Cassini, 2019.

[G] X. Gourdon, *Algèbre et probabilités*, 3^e édition, Ellipses, 2021.

[CP] Ph. Caldero et M. Peronnier, *Carnet de voyage en Algébrie*, Calvage & Mounet, 2022.

[BM] B.W. Boyd et H.L Montgomery, *Cyclotomic partitions*, dans Number theory (Banff, AB, 1988) (1990).

[D] P.A. Damianou, *Monic polynomial in $\mathbb{Z}[X]$ with roots in the unit disc*, The American Mathematical Monthly **108** (2001), no. 3.

[HL] D. Hernandez et Y. Laszlo, *Introduction à la théorie de Galois*, Éditions de l'école polytechnique, 2012 [4].

2. Réponse : $2X + 1$.
3. Réponse : $X^2 - \frac{6}{5}X + 1$
4. Attention ! Ce livre ne fait pas partie de la bibliothèque officielle du jury.