REPRÉSENTER ET COMPTER LES CORPS DE NOMBRES

JEAN-MARC COUVEIGNES

RÉSUMÉ. Les corps de nombres sont des objets familiers mais on ne leur connaît pas, en général, de modèle canonique et l'on ne sait pas les compter aussi précisément qu'on le souhaiterait. La géométrie des nombres et la théorie de l'interpolation multivariée permettent d'aborder ces deux problèmes.

TABLE DES MATIÈRES

1. CORPS DE NOMBRES

On note $\mathbf{Q}$ le corps des nombres rationnels. Un **corps de nombres** est un corps $\mathbf{K}$ de caractéristique nulle et de dimension finie en tant que $\mathbf{Q}$-espace vectoriel. On note n et on appelle **degré** de $\mathbf{K}$ cette dimension. Le seul corps de nombres de degré 1 est $\mathbf{Q}$ lui-même. Un autre corps de nombres familier est l'ensemble

$$\mathbf{Q}(i) = \{a + bi \,|a, b \in \mathbf{Q}\} \subset \mathbf{C}$$

des nombres complexes à coordonnées rationnelles. Son degré est 2. Une $\mathbf{Q}$-base de $\mathbf{Q}(i)$ est $(1, i)$. Dans cette base la loi de multiplication prend une forme simple

$$(a + bi)(a' + b'i) = aa' - bb' + (ab' + a'b)i.$$

Ce n'est pas le seul corps de nombres de degré 2. Par exemple l'ensemble

$$\mathbf{Q}(\sqrt{5}) = \{a + b\sqrt{5} \,|a, b \in \mathbf{Q}\} \subset \mathbf{R}$$

des nombres réels de la forme $a + b\sqrt{5}$ avec a et b rationnels est lui-aussi un corps de nombres de degré 2. La loi de multiplication dans la $\mathbf{Q}$-base $(1, \sqrt{5})$ est

$$(a + b\sqrt{5})(a' + b'\sqrt{5}) = aa' + 5bb' + (ab' + a'b)\sqrt{5}.$$

Tout élément d'un corps de nombres $\mathbf{K}$ de degré n est racine d'un polynôme à coefficients rationnels de degré $\leqslant n$. On distingue les éléments de $\mathbf{K}$ qui sont racines d'un polynôme *unitaire*

Date: 10 décembre 2020.

à coefficients dans l'anneau $\mathbf{Z}$ *des entiers*. On les nomme **entiers algébriques** de $\mathbf{K}$. Ils forment un sous-anneau de $\mathbf{K}$ noté $\mathbf{O}$. Ce sous-anneau est un $\mathbf{Z}$-module libre de rang n, le degré de $\mathbf{K}$. Par exemple les entiers algébriques dans $\mathbf{Q}(i)$ sont les $a + bi$ avec a et b dans $\mathbf{Z}$. Dans le corps de nombres $\mathbf{Q}(\sqrt{5})$ tous les nombres de la forme $a + b\sqrt{5}$ avec a et b dans $\mathbf{Z}$ sont des entiers algébriques, mais ce ne sont pas les seuls. Le nombre d'or $\alpha = (1 + \sqrt{5})/2$ est entier lui aussi car il est racine du polynôme $x^2 - x - 1$. Le entiers de $\mathbf{Q}(\sqrt{5})$ sont les $a + b\alpha$ avec a et b dans $\mathbf{Z}$.

L'**espace de Minkowski** associé à un corps de nombres $\mathbf{K}$ est le produit tensoriel

$$\mathbf{M} = \mathbf{K} \otimes_{\mathbf{Q}} \mathbf{R}.$$

Il existe deux entier $r \geqslant 0$ et $s \geqslant 0$ tels que $r + 2s = n$ et $\mathbf{M}$ est isomorphe au $\mathbf{R}$-espace vectoriel $\mathbf{R}^r \oplus \mathbf{C}^s$. L'entier r est le nombre d'homomorphismes injectifs ρ du corps $\mathbf{K}$ dans le corps $\mathbf{R}$ des nombres réels. On dit que $\mathbf{K}$ a r plongements réels. L'entier s est le nombre d'homomorphismes injectifs σ du corps $\mathbf{K}$ dans dans le corps $\mathbf{C}$ des nombres complexes, qui ne sont pas des plongements réels, divisé par deux (car on ne distingue pas σ du plongement obtenu en composant σ avec la conjugaison complexe). On dit que $\mathbf{K}$ a $2s$ plongements complexes. On écrit

$$\mathbf{M} \simeq \bigoplus_{\rho} \mathbf{R} \oplus \bigoplus_{\sigma} \mathbf{C}$$

où l'indice ρ parcourt l'ensemble des plongements réels et σ parcourt un ensemble de représentants des paires de plongements complexes conjugués. Cette décomposition permet de munir $\mathbf{M}$ d'un produit scalaire noté $<,>$. Par exemple si $\mathbf{K} = \mathbf{Q}(\sqrt{5})$ on a $r = 2$ et $s = 0$ et

$$< a + b\sqrt{5}, a' + b'\sqrt{5} >= (a + b\sqrt{5})(a' + b'\sqrt{5}) + (a - b\sqrt{5})(a' - b'\sqrt{5}) = 2aa' + 10bb'.$$

et si $\mathbf{K} = \mathbf{Q}(i)$ on a $r = 0$ et $s = 1$ et

$$< a+bi, a'+b'i >= (a+bi)\overline{(a' + b'i)}+\overline{(a + bi)}(a'+b'i) = (a+bi)(a'-b'i)+(a-bi)(a'+b'i) = 2aa'+2bb'.$$

On obtient de la même manière une norme L^2 et une norme L^∞ sur $\mathbf{M}$. Le corps $\mathbf{K}$ et l'anneau des entiers $\mathbf{O}$ s'injectent canoniquement dans l'espace de Minkowski. Le $\mathbf{Z}$-module $\mathbf{O}$ est ainsi réalisé comme sous-groupe additif discret de $\mathbf{M}$. Et le quotient $\mathbf{M}/\mathbf{O}$ est compact. Le volume de ce quotient pour la forme volume associée au produit scalaire $<,>$ est appelé covolume de $\mathbf{O}$. C'est un invariant important du corps de nombres. Concrètement, si $\alpha_1, \ldots, \alpha_n$ est une $\mathbf{Z}$-base de $\mathbf{O}$ et si l'on note $\tau_1, \ldots, \tau_n$ les n plongements (réels ou complexes) de $\mathbf{K}$ alors on définit la matrice

$$A = (\tau_j(\alpha_i))_{1 \leqslant i,j \leqslant n}.$$

Le covolume de $\mathbf{O}$ est le module du déterminant de A. Par exemple pour $\mathbf{K} = \mathbf{Q}(i)$ on obtient

$$A = \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix} \text{ et } \operatorname{covol}(\mathbf{O}) = 2.$$

Et pour $\mathbf{K} = \mathbf{Q}(\sqrt{5})$ on obtient

$$A = \begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{pmatrix} \text{ et } \operatorname{covol}(\mathbf{O}) = \sqrt{5}.$$

Le **discriminant** de $\mathbf{K}$ est le déterminant

$$d_{\mathbf{K}} = \det(AA^t).$$

C'est un nombre entier relatif. Sa valeur absolue est le carré du covolume de $\mathbf{O}$. Par exemple, le discriminant de $\mathbf{Q}(i)$ est -4 et le discriminant de $\mathbf{Q}(\sqrt{5})$ est 5.

Le degré n et le discriminant $d_{\mathbf{K}}$ sont deux invariants importants mais insuffisants : il existe des corps de nombres non-isomorphes de même degré et de même discriminant.

Les trois problèmes naturels suivants sont voisins.

(1) Trouver un système d'invariants d'un corps de nombres, aussi complet et aussi peu redondant que possible,

(2) Trouver une description (un modèle algébrique) d'un corps de nombres aussi concis que possible,

(3) Évaluer le nombre $N_n(H)$ de classes d'isomorphismes de corps de nombres de degré n donné et de discriminant borné en valeur absolue par un entier H donné.

On doit à Cohen, Diaz et Olivier des tables de corps de nombres en petits degrés [6, 7, 8]. Ces tables suggèrent que $N_n(H)$ pourrait être équivalent à $c(n) \times H$ pour $n \geqslant 2$ fixé et $H \to +\infty$, où $c(n)$ est une fonction de n. C'est bien le cas pour $2 \leqslant n \leqslant 5$. Le cas $n = 2$ est élémentaire. Davenport and Heilbronn [10] on étudié le cas $n = 3$ et Bhargava [4, 5] les cas $n = 4, 5$.

Pour des valeurs arbitraires de n, on obtient des estimations plus ou moins grossières de $N_n(H)$ en étudiant la géométrie de l'anneau des entiers $\mathbf{O}$, vu comme un sous-groupe discret de l'espace de Minkoswki $\mathbf{M}$, muni du produit scalaire $<,>$. C'est l'objet de la **géométrie des nombres** dont il est question dans la section suivante.

Schmidt [12] a ainsi montré que $N_n(H)$ est majoré par $H^{\frac{n+2}{4}}$ multiplié par une fonction qui ne dépend que de n. Ellenberg and Venkatesh [11] on montré qu'il existe une constante C telle que $N_n(H)$ est majoré par $H^{\exp(C\sqrt{\log n})}$ multiplié par une fonction qui ne dépend que de n.

2. Le théorème de Minkowski

Soit $\mathbf{E}$ un espace euclidien de dimension n. On note $<,>$ le produit scalaire. On se donne un sous-groupe discret $\mathbf{L}$ de $\mathbf{E}$ tel que le quotient $\mathbf{E}/\mathbf{L}$ soit compact : le rang du $\mathbf{Z}$-module $\mathbf{L}$ est égal à la dimension n de $\mathbf{E}$. On se donne une **fonction de jauge**

$$f : \mathbf{E} \to [0, +\infty[$$

telle que

(1) $f(e) > 0$ si $e \in \mathbf{E}$ est non-nul,

(2) $f(\lambda e) = \lambda f(e)$ si $\lambda > 0$ et $e \in \mathbf{E}$,

(3) $f(e_1 + e_2) \leqslant f(e_1) + f(e_2)$ si $e_1, e_2 \in \mathbf{E}$.

Typiquement on prend pour f la norme L^∞ dans une base de $\mathbf{E}$. On note

$$\mathbf{B} = \{e \in \mathbf{E} \,|\, f(e) \leqslant 1\}$$

la boule unité correspondante. On note $\mathrm{vol}(\mathbf{B})$ le volume pour la forme volume associée au produit scalaire $<,>$ de l'ensemble convexe $\mathbf{B}$. Le second théorème de Minkowski affirme qu'il existe n éléments $l_1, \ldots, l_n$ dans $\mathbf{L}$ qui sont linéairement indépendants et tels que

$$\prod_{1 \leqslant i \leqslant n} f(l_i) \leqslant \frac{2^n \times \mathrm{covol}(\mathbf{L})}{\mathrm{vol}(\mathbf{B})}.$$

Supposons que les f_i sont numérotés de telle sorte que les $f(l_i)$ forment une suite croissante. Alors on déduit de l'inégalité précédente que

$$f(l_i) \leqslant \left(\frac{2^n \times \mathrm{covol}(\mathbf{L})}{\mathrm{vol}(\mathbf{B})} \right)^{\frac{1}{n-i+1}}. \tag{1}$$

Cette inégalité est surtout utile pour les premières valeurs de i. Dans la situation qui nous intéresse $\mathbf{E}$ est l'espace de Minkowski $\mathbf{M}$ d'un corps de nombres et $\mathbf{L}$ est l'anneau $\mathbf{O}$ des entiers. On choisit pour f la norme L^∞ dans la base canonique de $\mathbf{M}$. Schmidt utilise l'inégalité (1) pour montrer que $\mathbf{K}$ est engendré, en tant que $\mathbf{Q}$-algèbre, par un petit nombre d'entiers de petite norme. C'est ainsi qu'il obtient une majoration de $N_n(H)$.

Bhargava, Shankar, Taniguchi, Thorne, Tsimerman, and ZhaoSee ont remarqué [3][Theorem 3.1] que l'existence sur $\mathbf{O}$ d'une structure d'anneau **intègre** compatible avec la métrique induite par la fonction de jauge permet de renforcer l'inégalité (1). On peut montrer par exemple [9][Proposition 1] qu'il existe n entiers $l_1, \ldots, l_n$ dans $\mathbf{O}$ qui sont linéairement indépendants et tels que

$$f(l_i) \leqslant \delta_{\mathbf{K}}^2$$

pour **tout** $1 \leqslant i \leqslant n$ où

$$\delta_{\mathbf{K}} = |d_{\mathbf{K}}|^{\frac{1}{n}}$$

est appelé **discriminant racine** de $\mathbf{K}$. Autrement dit, le $\mathbf{Q}$-espace vectoriel $\mathbf{K}$ admet une base formée d'entiers de petite norme.

Pour construire un modèle du corps de nombres $\mathbf{K}$ il faut un système de générateurs $\kappa_1, \ldots, \kappa_r$ de la $\mathbf{Q}$-algèbre $\mathbf{K}$. Il faut aussi décrire l'idéal des relations algébriques entre ces générateurs. Pour obtenir un modèle aussi concis que possible on choisit un petit nombre de générateurs, tous aussi petits que possible. Typiquement r est de l'ordre de $\log n$. On choisit un degré d, de l'ordre de $\log n$ lui aussi. Et l'on étudie le $\mathbf{Z}$-module des relations entre les monomes $\prod_{1 \leqslant k \leqslant r} \kappa_r^{e_r}$ de degré $\leqslant d$. On mobilise une fois encore le théorème de Minkowski pour montrer qu'il existe quelques relations de degré $\leqslant d$ avec de petits coefficients. On voudrait s'assurer que ces petites relations engendrent l'idéal des relations entre les générateurs $(\kappa_k)_{1 \leqslant k \leqslant r}$. C'est malheureusement très difficile. On se contentera d'un système d'**équations locales**. On cherche donc r équations à coefficents dans $\mathbf{Z}$ dont les différentielles soient linéairement indépendantes aux n points complexes de l'espace affine $\mathbf{A}^r(\mathbf{C})$ définis par les r-coordonnées affines $(\kappa_k)_{1 \leqslant k \leqslant r}$ et les n plongements de $\mathbf{K}$ dans $\mathbf{C}$. Pour montrer l'existence de telles équations, un instrument de géométrie algèbrique locale est requis. C'est le théorème d'Alexander et Hirschowitz [1, 2] selon lequel les problèmes d'interpolation d'Hermite sont génériquement bien posés en degré $d \geqslant 5$. Ce théorème est brièvement introduit dans la section suivante.

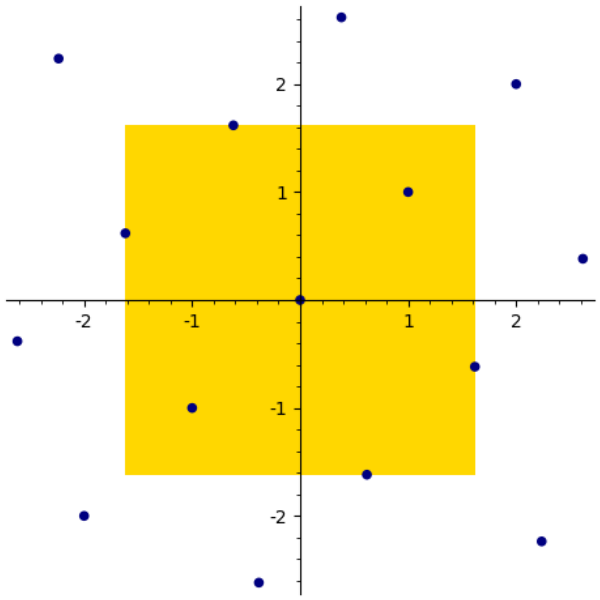

FIGURE 1. L'espace de Minkowski $\mathbf{M} \simeq \mathbf{R} \times \mathbf{R}$ de $\mathbf{Q}(\sqrt{5})$. Les points bleus sont les éléments de l'anneau $\mathbf{O}$ des entiers. Le carré jaune est la plus petite boule L^∞ qui contient deux entiers linéairement indépendants.

3. LE THÉORÈME D'ALEXANDER ET HIRSCHOWITZ POUR L'INTERPOLATION MULTIVARIÉE

Soit $\mathbf{K}$ un corps et $r \geqslant 1$ un entier. Soient P_1, P_2, …, P_n des points dans l'espace affine $\mathbf{A}^r(\mathbf{K}) = \mathbf{K}^r$. Soit $d \geqslant 1$ un entier. Étant donnée une collection $(a_i)_{1 \leqslant i \leqslant n} \in \mathbf{K}^n$ de scalaires, le problème d'**interpolation de Lagrange** s'intéresse à l'existence (et à l'unicité) d'un polynôme f dans $\mathbf{K}[x_1, \ldots, x_r]$ de degré $\leqslant d$ et tel que $f(P_i) = a_i$ pour tout $1 \leqslant i \leqslant n$. Comme la dimension de l'espace des polynômes de degré $\leqslant d$ en r variables est $\binom{d+r}{r}$ on n'espère pas mieux que l'existence si $n \leqslant \binom{d+r}{r}$ et l'unicité si $n \geqslant \binom{d+r}{r}$. On dit donc que le problème d'interpolation est **bien posé** quand l'application d'évaluation $f \mapsto (f(P_1), \ldots, f(P_n))$ de $\mathbf{K}[x_1, \ldots, x_r]_{\leqslant d}$ dans $\mathbf{K}^n$ est injective ou surjective. Il est facile de voir que les problèmes d'interpolation de Lagrange sont **génériquement bien posés**. Autrement dit l'ensemble des problèmes mal posés est un fermé strict de l'ensemble $(\mathbf{A}^r)^n$ des nuages de n points dans $\mathbf{A}^r$. Pour s'en convaincre il suffit d'écrire le déterminant d'un mineur maximal de l'application d'évaluation et de vérifier que les termes de son développement sont des monômes en rn variables de multidegrés deux-à-deux distincts.

Il arrive que l'on souhaite contrôler non seulement les valeurs d'un polynôme de $\mathbf{K}[x_1, \ldots, x_r]$ en n points, mais aussi les valeurs de ses r dérivées partielles en ces n points. On parle alors d'**interpolation d'Hermite**. Un théorème difficile d'**Alexander et Hirschowitz** donne la liste des triplets (r, n, d) pour lesquels le problème générique d'interpolation d'Hermite est bien posé. Cette liste comporte tous les triplets tels que $d \geqslant 5$. C'est ce théorème qui permet de contrôler

les équations locales des petits modèles de corps de nombres. On obtient ainsi [9] le théorème suivant.

Théorème 1 (Petits modèles d'un corps de nombres)**.** *Il existe une constante positive C telle que ce qui suit est vrai. Soit $\mathbf{K}$ un corps de nombre de degré $n \geqslant C$ et de discriminant racine $\delta_{\mathbf{K}}$. Il existe deux entiers $r \leqslant C \log n$ et $d \leqslant C \log n$ tels que $\binom{d+r}{r} \leqslant Cn \log n$ et il existe r polynômes E_1, E_2, …, E_r de degré $\leqslant d$ dans $\mathbf{Z}[x_1, \ldots, x_r]$, ayant tous leurs coefficients bornés par $(n\delta_{\mathbf{K}})^{C \log n}$ en valeur absolue, tels que la $\mathbf{Q}$-variété affine lisse et de dimension nulle définie par les équations*

$$E_1 = E_2 = \cdots = E_r = 0 \text{ et } \det\left(\partial E_i / \partial x_j\right)_{1 \leqslant i,\, j \leqslant r} \neq 0$$

contienne une composante irréductible de corps résiduel $\mathbf{K}$.

On peut résumer ce théorème en disant qu'un corps de nombres de degré n et discriminant racine $\delta_{\mathbf{K}}$ admet une description algébrique de « taille » une constante fois

$$n(\log n)^3(\log \delta_K + \log n).$$

On déduit facilement de ce théorème qu'il existe une constante D telle que si $n \geqslant D$ alors $N_n(H)$ est majoré par $n^{Dn \log^3 n} H^{D \log^3 n}$ pour tout H. L'exposant $\exp(C\sqrt{\log n})$ dans l'estimation de Venkatesh-Ellenberg est ainsi remplacé par un polynôme en $\log n$. On est loin encore de l'exposant 1 suggéré par les données expérimentales.

RÉFÉRENCES

[1] J. Alexander. Singularités imposables en position générale à une hypersurface projective. *Compositio Math.*, 68(3) :305–354, 1988.

[2] J. Alexander and A. Hirschowitz. Polynomial interpolation in several variables. *J. Algebraic Geom.*, 4(2) :201–222, 1995.

[3] M. Bhargava, A. Shankar, T. Taniguchi, F. Thorne, J. Tsimerman, and Y. Zhao. Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves. *ArXiv e-prints*, January 2017.

[4] Manjul Bhargava. The density of discriminants of quartic rings and fields. *Ann. of Math. (2)*, 162(2) :1031–1063, 2005.

[5] Manjul Bhargava. The density of discriminants of quintic rings and fields. *Ann. of Math. (2)*, 172(3) :1559–1591, 2010.

[6] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[7] Henri Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[8] Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier. Counting discriminants of number fields. *J. Théor. Nombres Bordeaux*, 18(3) :573–593, 2006.

[9] Jean-Marc Couveignes. Enumerating number fields. *Annals of Math.*, 192(2) :487–497, 2020.

[10] H. Davenport and H. Heilbronn. On the density of discriminants of cubic fields. II. *Proc. Roy. Soc. London Ser. A*, 322(1551) :405–420, 1971.

[11] Jordan S. Ellenberg and Akshay Venkatesh. The number of extensions of a number field with fixed degree and bounded discriminant. *Ann. of Math. (2)*, 163(2) :723–741, 2006.

[12] Wolfgang M. Schmidt. Number fields of given degree and bounded discriminant. *Astérisque*, (228) :4, 189–195, 1995. Columbia University Number Theory Seminar (New York, 1992).

JEAN-MARC COUVEIGNES, UNIV. BORDEAUX, CNRS, BORDEAUX-INP, IMB, UMR 5251, F-33400 TALENCE, FRANCE.

JEAN-MARC COUVEIGNES, INRIA, F-33400 TALENCE, FRANCE.
Email address: Jean-Marc.Couveignes@u-bordeaux.fr