Quelques applications du principe des tiroirs en théorie des nombres

Leonardo Zapponi

Résumé. **—** Cette note décrit quelques applications en théorie des nombres d'une méthode introduite par Thue, généralisée ensuite par Scholz, basée sur le principe des tiroirs. On présente d'abord une démonstration altenrative et élémentaire du théorème des deux carrés de Fermat n'utilisant que des rudiments d'arithmetique des entiers. Ensuite, ces mêmes techniques permettent d'obtenir une démonsrtration tout aussi élémentaire et purement algébrique de la finitude du groupe des classes d'un corps de nombres. On étudie enfin plus en détail le cas des corps quadratiques.

Introduction

La démonstration usuelle de la finitude du groupe des classes d'un corps de nombres repose en grande partie sur des résultats de géométrie des nombres et, plus en particulier, sur le théorème du corps convexe de Minkowski. Dans cette note, nous proposons une technique différente, purement algébrique, inspirée par une méthode introduite par Thue, reprise ensuite par Scholz. Bien que la stratégie soit est essentiellement la même que dans la démonstration classique (se résumant en la construction d'éléments de petite norme dans les idéaux d'un anneau d'entiers d'un corps de nombres), les arguments de nature analytique sont remplacés par de simples considérations combinatoires.

Le premier paragraphe est consacré au lemme clé de cette note, qui est une généralisation naturelle du rérsultat de Scholz. Sa démonstration est élémentaire et ne repose que sur le principe des tiroirs.

Dans le second paragraphe, en suivant l'idée originale de Thue, on montre comment le lemme central permette d'obtenir une démonstration élémentaire du théorème des deux carrés de Fermat. Seuls quelques rudiments d'arithmétique (divisibilité, coprimalité, lemme de Gauss, théorème de Wilson...) interviennent dans cette démarche.

Le troisième paragraphe propose une démonstration de la finitude du groupe des classes d'un corps de nombres se passant des résultats de géométrie des nombres. Sa lecture ne requiert qu'une connaissance de base des corps de nombres et de leurs propriétés (anneaux des entiers, idéaux fractionnaires, norme d'un idéal,...) ; on retrouvera toutes ces notions (et bien plus encore) dans [2].

Finalement, dans le dernier paragraphe on étudie plus en détail le cas des corps quadratiques, en obtenant des bornes assez satisfaisantes pour l'ordre du groupe des classes (bien que pas optimales).

Les résultats et méthodes présentés dans cette note ne prédendent en aucun cas d'être originaux (on les retrouvera assez facilement dans la littérature ou sur la toile), l'objectif de ces quelques pages étant simplement de montrer comment des techniques élémentaires et souvent peu connues peuvent amener à des résultats assez subtils.

Je tiens à remercier Alain Kraus et Joseph Oesterlé pour leur disponiblité. Leurs commentaires et questions ont été précieux lors de la rédaction de cette note.

1. Un lemme général

Tous les résultats de cette note s'appuient sur un simple lemme combinatoire. La version la plus simple de ce résultat apparaît dans les travaux de Thue. Une formulation plus générale, habituellement attribuée à Scholz, ne traite que le cas $G = \mathbb{Z}/m\mathbb{Z}$ et $r = 2$. L'énoncé ci-dessous en est une généralisation naturelle.

Lemme 1. — *Soit G un groupe abélien fini (noté additivement) et considérons des nombres réels positifs $t_1, \dots, t_r$ tels que $t_1 \cdots t_r \geq |G|$. Pour toute famille $g_1, \dots, g_r$ d'éléments de G, il existe des entiers $x_1, \dots, x_r$, avec $|x_i| \leq t_i$ et au moins un d'entre eux non nul, tels que $x_1 g_1 + \cdots + x_r g_r = 0$.*

Démonstration. — Pour tout $i \in \{1, \dots, r\}$, posons $S_i = \{0, \dots, m_i\}$, où m_i est la partie entière de t_i. L'ensemble $S = S_1 \times \cdots \times S_r$ étant de cardinal

$$(m_1 + 1) \cdots (m_r + 1) > t_1 \cdots t_r \geq |G|,$$

l'application $g : S \to G$ définie par la relation $g(x_1, \dots, x_r) = x_1 g_1 + \cdots + x_r g_r$ ne peut être injective. Il existe donc deux éléments distincts $(u_1, \dots, u_r)$ et $(v_1, \dots, v_r)$ de S ayant la même image par g. En posant $x_i = u_i - v_i$, on en déduit l'identité $x_1 g_1 + \cdots x_r g_r = 0$. Par construction, les entiers $x_1, \dots, x_r$ vérifient les inégalités $|x_i| \leq t_i$ et ne sont pas tous nuls. □

2. Une première application : le théorème des deux carrés de Fermat

Il existe plusieurs démonstrations du théorème des deux carrés de Fermat. L'une d'entre elles, proposée par Thue, est particulièrement élémentaire et élégante. Outre le lemme 1, elle ne fait intervenir que le lemme de Gauss et le théorème de Wilson. Bien que citée dans la littérature moderne (voir par exemple [1], exercices 1.2 et 1.3 page 27, où l'on retrouvera également la vérsion plus générale de Scholz), elle reste toutefois assez méconnue. Nous profitons donc de ces quelques pages pour la présenter.

Lemme 2. — *Soient a et b deux entiers premiers entre eux. Tout diviseur de $a^2 + b^2$ est somme de deux carrés.*

Démonstration. — Soit n un diviseur de $a^2 + b^2$. Si n est un carré, le lemme est trivialement vérifié. Supposons donc que n n'est pas un carré. En appliquant le lemme 1 avec $G = \mathbb{Z}/n\mathbb{Z}, r = 2, t_1 = t_2 = \sqrt{n}, g_1 = a$ et $g_2 = b$, on en déduit l'existence de deux entiers

x et y, avec $|x|, |y| < \sqrt{n}$ et au moins un d'entre eux non nul, tels que n divise $ax+by$. Dans ce cas, l'entier n divise également

$$(ax - by)(ax + by) + y^2(a^2 + b^2) = a^2(x^2 + y^2).$$

Les entiers a et n étant premiers entre eux (c'est une conséquence de la coprimalité entre a et b), le lemme de Gauss affirme finalement que n divise $x^2 + y^2$. Par construction, on a les inégalités $0 < x^2 + y^2 < 2n$, d'où l'identité $n = x^2 + y^2$. □

***Théorème 3* (Fermat).** — *Un nombre premier est somme de deux carrés si et seulement s'il n'est pas congru à* 3 *modulo* 4.

Démonstration. — Soit p un nombre premier (en particulier, p est congru à 1, 2 ou 3 modulo 4). Tout d'abord, le carré d'un entier étant congru à 0 ou 1 modulo 4, si p est somme de deux carrés alors il est congru à 1 ou 2 modulo 4. Réciproquement, pour $p = 2$, on a l'identité $2 = 1^2 + 1^2$. Pour $p = 2m + 1$ congru à 1 modulo 4, en combinant l'identité

$$(p-1)! = \prod_{n=1}^{m} n(p-n)$$

avec le théorème de Wilson on en déduit que p divise $(m!)^2 + 1$. Il suffit alors d'appliquer le lemme 2. □

3. Une généralisation : la finitude du groupe des classes d'un corps de nombres

Considérons maintenant un corps de nombres K de degré n et soit $\mathcal{O}$ son anneau des entiers. Désignons par $\mathrm{N}(\mathfrak{a})$ la norme d'un idéal non nul $\mathfrak{a}$ de $\mathcal{O}$, qui n'est autre que le cardinal du quotient $\mathcal{O}/\mathfrak{a}$. Si $\mathfrak{a}$ est principal, sa norme coïncide avec la valeur absolue de la norme usuelle de l'un de ses générateurs.

***Lemme 4*.** — *Pour tout idéal non nul $\mathfrak{a}$ de $\mathcal{O}$ il existe un idéal non nul $\mathfrak{b}$ de $\mathcal{O}$ de norme bornée par une constante ne dépendant que de K tel que l'idéal $\mathfrak{ab}$ soit principal.*

Démonstration. — Fixons une $\mathbb{Z}$-base $\omega_1, \ldots, \omega_n$ de $\mathcal{O}$ (ou, plus généralement, une famille d'éléments de $\mathcal{O}$ définissant une $\mathbb{Q}$-base de K). Étant donnés des entiers $x_1, \ldots, x_n$, la norme de l'élément

$$x = x_1\omega_1 + \cdots + x_n\omega_n \in \mathcal{O}$$

est un polynôme homogène en $x_1, \ldots, x_n$ de degré n et s'écrit donc comme combinaison linéaire de monômes de degré n dont les coefficients (qui sont des entiers) ne dépendent que de la base choisie. En utilisant l'inégalité triangulaire, on en déduit l'existence d'une constante M ne dépendant que de la base telle que

$$|\mathrm{N}(x)| \leq M \max\{|x_i|^n\}.$$

En appliquant le lemme 1 avec $G = \mathcal{O}/\mathfrak{a}, r = n, t_i = \mathrm{N}(\mathfrak{a})^{\frac{1}{n}}$ et $g_i = \omega_i$, on en déduit l'existence d'un élément non nul $x = x_1g_1 + \cdots + x_ng_n \in \mathfrak{a}$ tel que $|x_i| \leq \mathrm{N}(\mathfrak{a})^{\frac{1}{n}}$, ce qui amène à l'inégalité

$$|\mathrm{N}(x)| \leq M\,\mathrm{N}(\mathfrak{a}).$$

En posant $x\mathcal{O} = \mathfrak{a}\mathfrak{b}$, l'identité

$$|\,\mathrm{N}(x)| = \mathrm{N}(\mathfrak{a})\,\mathrm{N}(\mathfrak{b}),$$

combinée à l'inégalité ci-dessus, implique que la norme de l'idéal $\mathfrak{b}$ est majorée par M. □

Dans la suite, on note $\mathrm{Cl}(K)$ le groupe des classes de K, i.e. le quotient du groupe des idéaux fractionnaires de K par le sous-groupe de ses idéaux principaux.

Théorème 5. — *Le groupe* $\mathrm{Cl}(K)$ *est fini.*

Démonstration. — Étant donné un idéal fractionnaire non nul $\mathfrak{c}$ de K, il existe un entier non nul n tel que $\mathfrak{a} = n\mathfrak{c}^{-1}$ soit un idéal ordinaire. En appliquant le lemme précédent, on en déduit l'existence d'un idéal $\mathfrak{b}$ de $\mathcal{O}$ de norme bornée par une constante ne dépendant que de K tel que l'idéal $\mathfrak{a}\mathfrak{b}$ soit principal, ce qui se traduit par l'équivalence entre les idéaux fractionnaires $\mathfrak{a}^{-1} = n^{-1}\mathfrak{c}$ (qui est lui-même équivalent à $\mathfrak{c}$) et $\mathfrak{b}$. La finitude de l'ensemble des idéaux de $\mathcal{O}$ de norme bornée permet de conclure. □

4. Un cas particulier : les corps quadratiques

Les bornes obtenues par la méthode décrite dans le paragraphe précédent sont généralement moins fines que celles provenant de la géométrie des nombres. Par exemple, dans le cas d'un corps quadratique K, en explicitant les majorations de la démonstration du lemme 4, on en déduit que tout idéal fractionnaire de K est équivalent à un idéal (ordinaire) de norme bornée par une constante qui est linéaire en la valeur absolue du discriminant de K, là où les résultats de géométrie des nombres permettent d'obtenir des majorants proportionnels à sa racine carrée. Dans ce cas spécifique, nous allons montrer qu'il est néanmoins possible d'appliquer le lemme 1 de manière astucieuse, amenant à des bornes plus satisfaisantes.

Dans la suite de ce paragraphe, on fixe un corps quadratique K d'anneau des entiers $\mathcal{O}$ et on pose $h(K) = |\,\mathrm{Cl}(K)|$. Il existe un unique entier d sans facteur carré tel que $K = \mathbb{Q}(\sqrt{d})$ et on a alors l'inclusion $\mathbb{Z}[\sqrt{d}] \subset \mathcal{O}$.

Lemme 6. — *Tout idéal fractionnaire de* K *est équivalent à un idéal (ordinaire) de norme inférieure ou égale à* $2\sqrt{|d|}$.

Démonstration. — Étant donné un idéal fractionnaire $\mathfrak{c}$ de K, soit n un entier tel que $\mathfrak{a} = n\mathfrak{c}^{-1}$ soit un idéal ordinaire. En posant $G = \mathcal{O}/\mathfrak{a}, r = 2, t_1 = \sqrt{\mathrm{N}(\mathfrak{a})}|d|^{\frac{1}{4}}$, $t_2 = \sqrt{\mathrm{N}(\mathfrak{a})}|d|^{-\frac{1}{4}}, g_1 = 1$ et $g_2 = \sqrt{d}$, le lemme 1 affirme qu'il existe un élément non nul $x = ag_1 + bg_2 \in \mathfrak{a}$ tel que $|a| \leq \sqrt{\mathrm{N}(\mathfrak{a})}|d|^{\frac{1}{4}}$ et $|b| \leq \sqrt{\mathrm{N}(\mathfrak{a})}|d|^{-\frac{1}{4}}$, ce qui amène à la relation

$$|\,\mathrm{N}(x)| = |a^2 - db^2| \leq 2\sqrt{|d|}\,\mathrm{N}(\mathfrak{a}).$$

En posant $x\mathcal{O} = \mathfrak{a}\mathfrak{b}$, l'idéal (ordinaire) $\mathfrak{b}$ est de norme inférieure ou égale à $2\sqrt{|d|}$ et l'idéal fractionnaire $\mathfrak{a}^{-1} = n^{-1}\mathfrak{c}$ (qui est équivalent à $\mathfrak{c}$) est équivalent à $\mathfrak{b}$. □

Théorème 7. — *On a l'inégalité*

$$h(K) \leq \sqrt{|d|}\,(2 + \log(|d|))\,.$$

Démonstration. — Fixons un nombre premier p, un entier naturel e et distinguons différents cas :

— Si p ramifie dans K alors il existe un unique idéal de $\mathcal{O}$ de norme p^e.
— Si p est inerte alors il existe un idéal de $\mathcal{O}$ de norme p^e si et seulement si e est pair, auquel cas il est unique.
— Finalement, lorsque p est décomposé, il existe deux idéaux premiers distincts $\mathfrak{p}$ et $\mathfrak{q}$ de $\mathcal{O}$ divisant p et les idéaux de norme p^e s'expriment de manière unique comme produit $\mathfrak{p}^a\mathfrak{q}^b$, où a et b sont deux entiers naturels tels que $a+b=e$. Il en existe donc $e+1$.

On en déduit que, étant donné un entier naturel $n>0$, il existe au plus $\tau(n)$ idéaux de $\mathcal{O}$ de norme n, où $\tau(n)$ désigne le nombre de diviseurs de n. Pour tout réel $x>0$, on a les relation

$$\sum_{1\leq n\leq x}\tau(n)=\sum_{1\leq n\leq x}\left\lfloor\frac{x}{n}\right\rfloor\leq x\sum_{1\leq n\leq x}\frac{1}{n}\leq x(1+\log(x)).$$

Le lemme 6 amène alors aux inégalités

$$h(K)\leq\sqrt{|d|}\,(2+\log(|d|))\,.$$

□

Références

[1] Lemmermeyer, Franz. Reciprocity laws. From Euler to Eisenstein. Springer Monographs in Mathematics. *Springer-Verlag, Berlin*, 2000.

[2] Samuel, Pierre. Théorie algébrique des nombres. *Hermann, Paris*, 1967.

---

26 mai 2019

LEONARDO ZAPPONI • *E-mail :* leonardo.zapponi@imj-prg.fr