N° d'ordre : 4642

THÈSE

présentée à

L'UNIVERSITÉ BORDEAUX 1

ÉCOLE DOCTORALE MATHÉMATIQUES ET INFORMATIQUE

par Pierre LEZOWSKI

pour obtenir le grade de

DOCTEUR

SPÉCIALITÉ : MATHÉMATIQUES PURES

★ ★ ★

Questions d'Euclidianité

★ ★ ★

Soutenue le 7 décembre 2012 à l'Institut de Mathématiques de Bordeaux
devant la commission d'examen composée de

Christine BACHOC	Professeure	Université Bordeaux 1	
Karim BELABAS	Professeur	Université Bordeaux 1	
Jean-Paul CERRI	Maître de conférences	Université Bordeaux 1	Directeur
Renaud COULANGEON	Maître de conférences	Université Bordeaux 1	Co-directeur
Guillaume HANROT	Professeur	ENS Lyon	Président
Gabriele NEBE	Professeure	RWTH Aix-la-Chapelle	Rapporteuse
Denis SIMON	Professeur	Université de Caen	Rapporteur
Damien STEHLÉ	Professeur	ENS Lyon	

Questions d'Euclidianité

(Questions on Euclideanity)

Pierre Lezowski

Institut de Mathématiques de Bordeaux UMR 5251
Université Bordeaux 1
351 cours de la Libération - F 33405 Talence Cedex

Remerciements

Je tiens tout particulièrement à remercier mon directeur de thèse Jean-Paul Cerri. Non seulement le sujet qu'il m'a proposé s'est révélé très intéressant, mais il m'a aussi apporté tout au long de cette thèse une aide considérable et a su faire preuve d'une patience sans limite pour m'encadrer. Ses nombreux encouragements et conseils avisés ont grandement contribué à la rédaction de ce manuscrit.

Je voudrais aussi exprimer ma gratitude aux rapporteurs, Gabriele Nebe et Denis Simon pour leurs remarques précieuses qui ont, je l'espère, permis d'améliorer cette thèse. Je les remercie aussi d'être présents pour la soutenance.

Je tiens aussi à remercier Christine Bachoc, Karim Belabas, Renaud Coulangeon, Guillaume Hanrot et Damien Stehlé qui me font l'honneur et le plaisir d'être membres de mon jury.

Je voudrais remercier les enseignants-chercheurs de l'institut de mathématiques de Bordeaux côtoyés dans les séminaires, groupes de travail ou pour préparer mes enseignements. Merci en particulier à Andreas Enge et à tous les membres du groupe Lfant. Plus généralement, je remercie les créateurs et développeurs de la bibliothèque `pari` qui s'est révélée très utile pour mes algorithmes. Merci aussi aux membres du laboratoire, de l'administration à la bibliothèque, qui contribuent à faire de l'institut un lieu de travail agréable.

Je voudrais par ailleurs remercier tous mes enseignants de mathématiques de Toucy à Bordeaux en passant par Dijon, Bruz et Rennes qui ont su me donner le goût pour les mathématiques. À ce titre, j'adresse des remerciements particuliers à Arnaud Debussche, Laurent Moret-Bailly, Pascal Autissier et Guillaume Ricotta. Je voudrais aussi remercier mes étudiants dont la gentillesse a permis de faire de mes enseignements une parenthèse agréable au sein de mes activités de recherche.

De plus je tiens à remercier toutes les personnes que j'ai pu rencontre au fil de mes études et que j'ai eu la chance de croiser pendant cette thèse : Antoine, Jérémy, Élise à Dijon, les Kerlannais Sébastien, Jérémy, Camille, Alain, Marc et bien sûr, mes colocataires de la rue de Lorgeril, Nicolas et Francky.

Merci aussi aux doctorants que j'ai pu côtoyer au laboratoire ou en partageant la fine cuisine du haut-carré. Tout d'abord, merci à mes collègues du bureau 375, Cédric, Abdillah et Giovanni, mais aussi à Arthur, Aurélien, Nicolas, Pierre, Jean-Matthieu, Pascal, Vincent, Frédéric, Guillaume, Anna, Florence, François, Maël, Louis, Diomba, Nicola, Andrea, Sophie, Alberto, Aurel, Nicolas, Stéphanie, Bruno, Zoé et tous ceux que j'aurais oublié.

Enfin, je voudrais remercier mes parents et ma sœur pour leur soutien constant et indéfectible. Le confort et réconfort qu'ils m'ont apporté depuis toujours est inestimable. Cette thèse leur doit beaucoup.

TABLE DES MATIÈRES

FIGURES ET TABLEAUX

Table des figures

Liste des tableaux

NOTATIONS

$A_{i,X}$	i^{e} ensemble de Motzkin pour l'idéal ou la classe d'idéaux X
$\left(\frac{a}{m}\right)$	symbole de Jacobi (ou de Legendre)
$\left(\frac{a}{p}\right)_4$	symbole de résidu quartique modulo p
disc_K	discriminant du corps de nombres K
$\Gamma(k)$	bornes de calcul d'un minimum euclidien inférieur à k
h_K	nombre de classes de K
$\Lambda(K)$	norme minimale des idéaux de $\mathbf{Z}_K$ différents de $\mathbf{Z}_K$
L_m	notation pour $\mathbf{Q}\left(\sqrt[4]{m}\right)$
$\mathcal{M}_k$	constante de calcul de minimum euclidien inférieur à k
$m_{\overline{K}}$	minimum inhomogène local de K
$M(\overline{K})$	minimum inhomogène de K
$M(K, C)$	minimum euclidien de K par rapport à la classe C
$M(\overline{K}, C)$	minimum inhomogène de K par rapport à la classe C
$m_{K,I}(x)$	minimum euclidien local de l'idéal I en x
$m_{\overline{K},I}(x)$	minimum inhomogène local de l'idéal I en x
$M_p(K)$	p^{e} minimum euclidien de K
$M_p(\overline{K})$	p^{e} minimum inhomogène de K
m_X	minimum euclidien local de X
$M(X)$	minimum euclidien de X
$\mathbf{N}_{L/K}$	norme relative de L sur K
$\mathrm{nrd}_{F/K}$	norme réduite de F sur K
R_i	i^{e} ensemble de Motzkin de l'anneau R
$t_{\mathcal{C}}$	point du domaine fondamental associé au cycle simple $\mathcal{C}$
$\mathrm{trd}_{F/K}$	trace réduite de F sur K
$\overline{x}$	conjugué de x (dans un corps de quaternions)
$[Y : X]$	degré de l'extension Y/X ou indice du sous-groupe X de Y
ζ_K	fonction ζ de Dedekind du corps de nombres K
$\mathbf{Z}_K$	anneaux des entiers algébriques de K
$\mathbf{Z}_K^\times$	unités de K

CHAPITRE I

INTRODUCTION

Nous allons décrire des notions généralisant l'euclidianité pour la norme des corps de nombres. Pour expliquer notre démarche, nous présentons ici un rappel des définitions de base et de quelques résultats déjà connus. Pour un panorama plus complet, on peut consulter les articles de Lenstra ([Len79]) ou Lemmermeyer ([Lem95]).

Corps de nombres euclidiens pour la norme

Soit K un corps de nombres, c'est-à-dire une extension finie de $\mathbf{Q}$. On note $\mathbf{Z}_K$ l'anneau des entiers de K et $\mathbf{N}_{K/\mathbf{Q}}$ la norme.

On dit que le corps K (ou que l'anneau $\mathbf{Z}_K$) est euclidien pour la norme si pour tout couple $(\alpha, \beta) \in \mathbf{Z}_K \times \mathbf{Z}_K \setminus \{0\}$, il existe $\gamma \in \mathbf{Z}_K$ tel que $\left|\mathbf{N}_{K/\mathbf{Q}}(\alpha - \beta\gamma)\right| < \left|\mathbf{N}_{K/\mathbf{Q}}(\beta)\right|$. Avec la multiplicativité de la norme, cette définition équivaut au fait que

$$\text{pour tout } \xi \in K, \text{ il existe } z \in \mathbf{Z}_K \text{ tel que } \left|\mathbf{N}_{K/\mathbf{Q}}(\xi - z)\right| < 1. \tag{I.1}$$

Dans le cas où $K = \mathbf{Q}$, $\mathbf{Z}_K = \mathbf{Z}$, le fait que (I.1) est vérifié est connu au moins depuis Euclide ([Euc32, Proposition 1]). Cette propriété était utilisée au départ pour montrer que $\mathbf{Z}$ est principal, donc factoriel, mais aussi pour calculer des pgcd et des identités de Bézout. Avec (I.1), la même démonstration s'applique et si K est euclidien, alors $\mathbf{Z}_K$ est principal, donc factoriel. En fait, dans le cas des anneaux d'entiers de corps de nombres, les propriétés de principalité et de factorialité sont équivalentes.

Un cas particulièrement simple est celui où K est un corps quadratique imaginaire, c'est-à-dire $K = \mathbf{Q}\left(\sqrt{-m}\right)$ où m est entier positif sans facteur carré. Dans le cas $m = -1$, Gauß a ainsi montré que l'anneau $\mathbf{Z}_{\mathbf{Q}\left(\sqrt{-1}\right)} = \mathbf{Z}[i]$ appelé de nos jours anneaux des entiers de Gauß est euclidien pour la norme. Ainsi $\mathbf{Z}[i]$ est factoriel. Les applications de cette propriété sont nombreuses : on peut citer la recherche de triplets pythagoriciens et le théorème des deux carrés de Fermat. Plus généralement, on connaît la liste complète des quadratiques imaginaires euclidiens pour la norme. Il s'agit des corps $\mathbf{Q}\left(\sqrt{-m}\right)$ pour m appartenant à la liste suivante :

$$1, 2, 3, 7, 11. \tag{I.2}$$

C'est pour montrer la principalité que l'on a cherché à prouver que certains anneaux d'entiers de corps de nombres sont euclidiens pour la norme. Néanmoins, la question des corps quadratiques imaginaires principaux est difficile et même si le résultat avait été conjecturé par Gauß, il a fallu attendre le XX$^{\text{e}}$ siècle et le théorème de Heegner-Baker-Stark pour obtenir leur liste complète : il s'agit des $\mathbf{Q}\left(\sqrt{-m}\right)$ pour les valeurs suivantes de m :

$$1, 2, 3, 7, 11, 19, 43, 67, 163.$$

À partir du XIX^{e} siècle, on s'est particulièrement intéressé au caractère principal des corps cyclotomiques $K = \mathbf{Q}(\zeta_n)$ où n est une racine primitive n^{e} de l'unité. L'argument de l'euclidianité pour la norme est naturel pour progresser dans cette étude. Wantzel a ainsi tenté de combler un trou dans la « preuve » de Lamé du théorème de Fermat-Wiles en utilisant des propriétés d'euclidianité pour la norme. En suivant et en corrigeant ses idées, Cauchy et Kummer ont étudié les corps cyclotomiques et prouvé que certains d'entre eux sont euclidiens pour la norme, mais Kummer a aussi montré que $\mathbf{Q}(\zeta_{23})$ n'est pas principal.

Si les corps cyclotomiques principaux sont totalement connus, la liste exacte de ceux qui sont euclidiens pour la norme n'est pas encore totalement déterminée : on sait que $\mathbf{Q}(\zeta_n)$ est euclidien pour la norme pour

$$n \in \{1, 3, 4, 5, 7, 8, 9, 12, 15, 16, 20, 24\},$$

mais Lenstra a prouvé que $\mathbf{Q}(\zeta_{32})$ est principal mais pas euclidien pour la norme (voir [Akh95] pour les détails de la preuve).

Il s'avère que la recherche de corps de nombres euclidiens pour la norme n'est pas si facile en pratique. En particulier, peu d'exemples de corps de nombres K de degré supérieur ou égal à 5 ayant cette propriété étaient connus avant l'article [Len76] de Lenstra. Son idée, reposant sur l'utilisation de suites particulières d'unités de K, a permis de prouver que de nombreux corps de nombres de degré $n \in \{5, \dots 10\}$ sont euclidiens pour la norme.

Minimum euclidien

La détermination des corps de nombres K quadratiques réels et euclidiens pour la norme est déjà un problème difficile qui n'a été résolu qu'au début des années 1950.

Dans ce cas, il s'agit non seulement de montrer que certains corps sont euclidiens pour la norme, mais aussi de prouver que les autres ne le sont pas. Des arguments de congruence, (on peut par exemple citer ceux de Behrbohm et Rédei, [BR36]) ont permis de traiter de nombreux cas, mais une avancée importante a été effectuée par Davenport qui a prouvé que l'euclidianité de K impliquait que le discriminant de K était borné et a donné une borne explicite raisonnable ([Dav51]). C'est ainsi que la liste complète des corps quadratiques réels euclidiens pour la norme a été trouvée : $K = \mathbf{Q}\left(\sqrt{n}\right)$, $n > 1$ sans facteur carré, est euclidien pour la norme si et seulement si

$$n \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}. \tag{I.3}$$

De nombreux autres auteurs ont contribué à ce résultat. On peut citer parmi eux Erdős, Heilbronn, Chatland, Min, Hua, Inkeri (l'article [Ink47] est le premier à donner la liste complète, au détail près qu'elle contient par erreur $n = 97$), Davenport, Barnes et Swinnerton-Dyer ([BSD52a] signale que $n = 97$ est erronée). Pour une présentation complète et en un seul papier de la démarche, on peut consulter la thèse d'Ennola ([Enn58]) qui améliore la borne de Davenport.

Notons aussi que le cas quadratique est très particulier : comme dans tous les cas où le rang r des unités de K vaut 1, il n'existe qu'un nombre fini de corps K qui sont euclidiens pour la norme. Néanmoins, si $r > 1$, cela n'est pas prouvé et il n'y a aucune raison de le conjecturer.

Pour étudier les corps quadratiques euclidiens, de nouvelles approches ont été développées, et ainsi le minimum euclidien a été défini. L'équation (I.5) donne en effet une interprétation « géométrique » de la détermination de l'euclidianité pour la norme : on cherche à approcher les éléments de K par des éléments du réseau $\mathbf{Z}_K$ par rapport à la norme $\mathbf{N}_{K/\mathbf{Q}}$.

Il est donc naturel d'introduire le minimum euclidien local pour $\xi \in K$,

$$m_K(\xi) := \inf_{z \in \mathbf{Z}_K} \left| \mathbf{N}_{K/\mathbf{Q}}(\xi - z) \right|,$$

ainsi que le minimum euclidien $M(K) := \sup_{\xi \in K} m_K(\xi)$. Cette quantité a été étudiée dans les cas des corps quadratiques réels par Davenport, Barnes, Swinnerton-Dyer dans les années 1950 : plutôt que de s'intéresser directement à K, on plonge K dans $\mathbf{R}^n$ (où n est le degré de K) et on définit le minimum inhomogène local $m_{\overline{K}}(x)$ pour $x \in \mathbf{R}^n$ qui étend le minimum euclidien. Il s'agit donc à présent d'étudier le minimum $M(\overline{K}) = \sup_{x \in \mathbf{R}^n} m_{\overline{K}}(x)$ et de comprendre ses liens avec le minimum euclidien $M(K)$. En effet, étant donné l'observation basique suivante, la valeur de $M(K)$ donne des informations sur l'euclidianité pour la norme :

- si $M(K) < 1$, alors K est euclidien pour la norme,
- si $M(K) > 1$, alors K n'est pas euclidien pour la norme,
- si $M(K) = 1$, alors on ne peut a priori pas conclure.

Barnes et Swinnerton-Dyer ont prouvé que $M(K) = M(\overline{K})$ dans le cas des corps quadratiques réels. Ce raisonnement a été étendu par van der Linden aux corps cubiques complexes et aux corps quartiques totalement imaginaires. Toutefois, cette propriété ne décrit pas totalement le comportement observé de $M(\overline{K})$ et c'est pourquoi Barnes et Swinnerton-Dyer ont fait la conjecture suivante :

$$\text{il existe } \xi \in K \text{ tel que } M(\overline{K}) = m_K(\xi). \tag{I.4}$$

Cela implique en particulier que $M(\overline{K}) = M(K)$, mais a aussi des conséquences plus profondes : par exemple, cela implique que si $M(K) = 1$, alors K n'est pas euclidien pour la norme.

Si la conjecture (I.4) n'est toujours pas prouvée dans le cas quadratique réel, Cerri l'a démontrée quand le rang des unités de K est strictement supérieur à 1. Ainsi, on obtient que $M(K) = M(\overline{K})$ pour tout corps de nombres K. Cela incite à calculer $M(K)$ puisque dans ce cas, la connaissance de $M(K)$ permet de répondre à la question de l'euclidianité pour la norme de K. Par ailleurs, très concrètement, la valeur de $M(K)$ permettra de dire quelle est la meilleure inégalité de la forme de (I.1) qu'on puisse obtenir.

Pour un corps quadratique imaginaire, le calcul du minimum euclidien s'effectue par un raisonnement géométrique élémentaire : si $K = \mathbf{Q}\left(\sqrt{-m}\right)$ où $m > 0$ est un entier sans facteur carré, alors

- $M(K) = M(\overline{K}) = \frac{m+1}{4}$ si $m \equiv 1, 2 \pmod 4$,
- $M(K) = M(\overline{K}) = \frac{(m+1)^2}{16m}$ si $m \equiv 3 \pmod 4$.

Dans ces cas élémentaires, on peut exhiber des éléments $\xi \in K$ tels que $m_K(\xi) = M(K) = M(\overline{K})$.

Pour déterminer des bornes sur $M(K)$ et le calculer, des arguments géométriques élémentaires ne suffisent pas. Ainsi, Barnes et Swinnerton-Dyer ont utilisé les unités $\mathbf{Z}_K^\times$ de K et des raisonnements géométriques fins dans $\mathbf{R}^n$ pour calculer les minima

euclidiens de certains corps quadratiques réels. Cette approche peut se généraliser à un degré quelconque mais les calculs qui en découlent peuvent être très compliqués. Pour cette raison, on a cherché à obtenir des procédures pratiques pour calculer avec un ordinateur le minimum euclidien $M(K)$.

Cavallar et Lemmermeyer ont ainsi décrit un algorithme qui s'applique notamment aux corps cubiques qui permet de calculer $M(K)$ ([CL98]). Cerri a, quant à lui, donné un algorithme utilisant un plongement de K différent et qui s'applique à tous les corps de nombres totalement réels pour calculer $M(K)$ ([Cer07]). Les tests de l'algorithme de Cerri étant optimaux, il donne de meilleurs résultats. Sa démarche repose sur les idées suivantes.

- Étant donné un point ξ de K, on peut calculer le minimum euclidien local $m_K(\xi)$ si on connaît les unités de K.
- Pour calculer $M(K)$, on se ramène à un compact de $\mathbf{R}^n$ que l'on découpe en parallélotopes. Seuls certains de ces parallélotopes sont conservés par l'étude et en faisant agir les unités sur ces parallélotopes, on obtient un graphe. Si ce graphe est convenable, alors le calcul de $M(K)$ se ramène à des calculs de minima euclidiens locaux.

L'application de cet algorithme a permis de trouver de nombreux corps quadratiques réels euclidiens de degré inférieur ou égal à 8.

Néanmoins, il reste encore des problématiques liés au minimum euclidien : d'une part, dans les cas non totalement réels, un tel algorithme n'existe pas, ce qui fait que peu de minima euclidiens sont connus. Par exemple, les minima euclidiens des corps cyclotomiques ne sont pas totalement déterminés, même pour ceux dont on sait qu'ils sont euclidiens pour la norme. Par ailleurs, la question de l'euclidianité des corps de nombres dont le rang des unités est 1 et dont le minimum euclidien vaut 1 n'est pas encore tranchée.

Généralisations

Pour généraliser l'euclidianité, on peut changer (I.1) mais aussi définir l'euclidianité pour des objets plus généraux que les corps de nombres principaux. Ce paragraphe présente différentes approches.

Euclidianité généralisée

Johnson, Queen et Sevilla ont proposé une généralisation de l'euclidianité aux corps de nombres non principaux ([JQS85]). Leur définition s'applique à un corps de nombre K. On dit que K est euclidien au sens généralisé (ou encore G.E.) si pour tout couple $(\alpha, \beta) \in \mathbf{Z}_K \times \mathbf{Z}_K \setminus \{0\}$ tel que l'idéal (α, β) est principal, il existe $\gamma \in \mathbf{Z}_K$ tel que

$$\left|\mathbf{N}_{K/\mathbf{Q}}(\alpha - \beta\gamma)\right| < \left|\mathbf{N}_{K/\mathbf{Q}}(\beta)\right|.$$

Dans le cas où K est un corps quadratique imaginaire, K est euclidien pour la norme si et seulement s'il est G.E. ; cependant, $\mathbf{Q}\left(\sqrt{10}\right)$ et $\mathbf{Q}\left(\sqrt{65}\right)$ sont G.E. mais non euclidiens pour la norme. En fait, si $K = \mathbf{Q}\left(\sqrt{d}\right)$ où d est un entier strictement positif sans facteur carré non congru à 1 modulo 4, alors K est G.E. si et seulement s'il est euclidien pour la norme ou $d = 10$. Les autres cas ne sont pas totalement déterminés,

mais on conjecture que $\mathbf{Q}\left(\sqrt{10}\right)$ et $\mathbf{Q}\left(\sqrt{65}\right)$ sont les seuls corps G.E. non euclidiens pour la norme.

Une connaissance fine du minimum euclidien permet de déterminer si un corps de nombres est G.E. : il suffit de prouver que les seuls points pour lesquels $m_K\left(\frac{\alpha}{\beta}\right) \geqslant 1$ sont tels que (α, β) n'est pas principal. Ainsi, Cerri a trouvé des corps de nombres totalement réels G.E. mais non euclidiens pour la norme de degré strictement supérieur à 2 ([Cer11]).

Euclidianité pour un autre stathme

Notons tout d'abord qu'il n'y a a priori aucune raison de se restreindre au cas particulier de l'euclidianité pour la norme : étant donné un anneau principal quelconque R, on cherche à savoir s'il existe une fonction $f : R \longrightarrow \mathbf{N}$, appelée stathme, telle que

$$\text{pour tout } (\alpha, \beta) \in R \times R \setminus \{0\}, \text{ il existe } \gamma \in R \text{ tel que } f(\alpha - \beta\gamma) < f(\beta). \tag{I.5}$$

Si $R = \mathbf{Z}_K$ et $f = \left|\mathbf{N}_{K/\mathbf{Q}}\right|$, on retrouve la définition (I.1). Hasse a ainsi demandé s'il était possible de définir des stathmes euclidiens autres que la norme si l'anneau des entiers est principal ([Has28]). Motzkin a développé un critère pour étudier l'existence d'un stathme quelconque dans un anneau ([Mot49]). Il s'est particulièrement intéressé au cas quadratique imaginaire et ainsi montré que $\mathbf{Q}\left(\sqrt{-19}\right)$ n'est pas euclidien. Par le même argument, on obtient que les corps quadratiques imaginaires euclidiens sont tous euclidiens pour la norme et donc que (I.2) est aussi la liste complète des corps quadratiques imaginaires euclidiens. Samuel a repris le critère de Motzkin, mais cette fois pour prouver que certains anneaux principaux sont euclidiens ([Sam71]). Il a aussi signalé que l'exemple $\mathbf{Q}\left(\sqrt{14}\right)$ était sans doute un bon candidat pour prouver qu'il existe des corps de nombres euclidiens pour un certain stathme, mais pas pour la norme.

S'appuyant sur les résultats de Samuel, Weinberger a montré sous des hypothèses de Riemann généralisées (GRH) que si le rang des unités de K est supérieur ou égal à 1, alors K est principal si et seulement s'il est euclidien pour un certain stathme ([Wei73]). Plus récemment, les travaux de Gupta, Kumar Murty, Ram Murty, Clark et Harper ont cherché à se passer des hypothèses de Riemann généralisées pour montrer des résultat analogues. Ainsi, Harper a prouvé dans sa thèse ([Har04]) que $\mathbf{Q}\left(\sqrt{14}\right)$ est euclidien et même que tous les corps quadratiques réels de discriminant inférieur à 500 et principaux étaient aussi euclidiens. En utilisant le même raisonnement, il prouve aussi que les cyclotomiques principaux sont également tous euclidiens.

Euclidianité en plusieurs étapes

Cooke a proposé de s'autoriser à effectuer des chaînes de division ([Coo76a] et [Coo76b]). En clair, pour un entier $m \geqslant 1$ fixé, on dit que K est euclidien en m étapes si pour tout $(\alpha, \beta) \in \mathbf{Z}_K \times \mathbf{Z}_K \setminus \{0\}$, il existe $k \leqslant m$, $(\gamma_i)_{1\leqslant i\leqslant k} \in \mathbf{Z}_K^k$ et $(\delta_i)_{1\leqslant i\leqslant k} \in \mathbf{Z}_K^k$ tels que

$$\begin{cases} \alpha - \beta\gamma_1 & = & \delta_1 \\ \beta - \delta_1\gamma_2 & = & \delta_2 \\ \delta_1 - \delta_2\gamma_3 & = & \delta_3 \\ & \vdots & \\ \delta_{k-2} - \delta_{k-1}\gamma_k & = & \delta_k \end{cases} \qquad \text{et } \left|\mathbf{N}_{K/\mathbf{Q}}(\delta_k)\right| < \left|\mathbf{N}_{K/\mathbf{Q}}(\beta)\right|. \tag{I.6}$$

On peut tout de suite remarquer que si K est euclidien en m étapes, alors il est aussi euclidien en l étapes pour tout $l \geqslant m$. De plus s'il existe un entier m tel que K est euclidien en m étapes par rapport à f, alors K est principal. Néanmoins, il existe des corps de nombres qui sont euclidiens en deux étapes mais pas euclidiens par rapport à la norme $\mathbf{N}_{K/\mathbf{Q}}$ (au sens classique, donc en une étape). Par exemple $\mathbf{Q}(\sqrt{14})$ est euclidien en deux étapes.

La notion d'euclidianité en m étapes peut aussi s'exprimer à l'aide des fractions continues. Si $q_1, q_2, \ldots, q_k$ sont k éléments de $\mathbf{Z}_K$, on note, si cette expression est bien définie,

$$[q_1, q_2, \ldots, q_k] = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots \; + \cfrac{1}{q_k}}}} = \frac{a_k}{b_k},$$

où a_k et b_k sont des éléments de $\mathbf{Z}_K$ définis par les formules suivantes :

$$\begin{array}{lll} a_1 &= 1, & b_1 &= 1, \\ a_2 &= q_1 q_2 + 1, & b_2 &= q_2, \\ &\vdots & &\vdots \\ a_k &= q_k a_{k-1} + a_{k-2}, & b_k &= q_k b_{k-1} + b_{k-2}. \end{array}$$

La condition (I.6) s'écrit alors sous la forme suivante : pour tout $\xi \in K$, il existe $1 \leqslant k \leqslant m$ et k éléments $q_1, q_2, \ldots, q_k \in \mathbf{Z}_K$ tels que

$$\left|\mathbf{N}_{K/\mathbf{Q}}(\xi - [q_1, q_2, \ldots, q_k])\right| < \frac{1}{\left|\mathbf{N}_{K/\mathbf{Q}}(b_k)\right|}.$$

En utilisant les résultats de P.M. Cohn et Vaserštein sur GE_2 ([Coh66], [Vas72]), Cooke a ainsi montré que si K admet une infinité d'unités, alors il existe un certain entier $m \geqslant 1$ tel que K est euclidien en m étapes ([Coo76a]). Sous GRH, Cooke et Weinberger ont même montré que si K a une infinité d'unités et est principal, alors K est euclidien en au plus quatre étapes. En supposant en outre que K a un plongement réel, ils ont obtenu que K est alors euclidien en au plus deux étapes ([CW75]).

En pratique, Cooke a vérifié expérimentalement que les corps quadratiques réels principaux de petit discriminant étaient euclidiens en deux étapes. Une étude plus récente a montré que c'était vrai pour tout corps quadratique réel de discriminant inférieur à 8 000 ([GM11]).

Classes euclidiennes

Lenstra a proposé une généralisation de l'euclidianité pour les corps de nombres non principaux ([Len78a]). Il s'agit de considérer les idéaux fractionnaires inversibles à la place des éléments de $\mathbf{Z}_K$. Un cas particulier intéressant est celui où on considère les classes euclidiennes pour la norme : on dit qu'un idéal entier I non nul est euclidien pour la norme si

$$\text{pour tout } \xi \in K, \text{ il existe } z \in I \text{ tel que } \left|\mathbf{N}_{K/\mathbf{Q}}(\xi - z)\right| < |\mathbf{Z}_K/I|. \tag{I.7}$$

Il s'agit bien sûr d'une modification de (I.1) obtenue en remplaçant $\mathbf{Z}_K$ par I. La propriété (I.7) ne dépend en fait que de la classe $[I]$ de I, c'est pourquoi on parle de *classe euclidienne* pour la norme. De plus si $[I]$ est une classe euclidienne, alors le groupe des classes est cyclique, engendré par $[I]$.

Lenstra a présenté les premiers exemples dans son article originel [Len78a] : il a notamment donné tous les corps quadratiques admettant une classe euclidienne pour la norme en s'appuyant sur les travaux d'Ennola. Peu après, van der Linden a prolongé son étude dans sa thèse ([Lin84]) en décrivant le cas où le rang des unités est 1 : comme dans le cas principal, il n'existe qu'un nombre fini de tels corps admettant une classe euclidienne pour la norme.

Il est aussi possible de définir l'euclidianité d'une classe pour un stathme quelconque. En utilisant les résultats de Weinberger, Lenstra a prouvé sous GRH que si K admet au moins deux places infinies et si le groupe des classes est cyclique, alors toute classe engendrant le groupe des classes est euclidienne. Graves a entrepris de généraliser les résultats de Harper dans le cas des classes euclidiennes ([Gra09]), ce qui lui a permis de montrer que $\mathbf{Q}(\sqrt{2}, \sqrt{35})$ admet une classe euclidienne ([Gra11]).

Corps de quaternions

Plutôt que de considérer un corps de nombres K, on peut s'intéresser à un corps de quaternions F, c'est-à-dire une K-algèbre centrale simple de dimension 4 admettant une K-base $(1, i, j, k)$ telle que $ij = -ji = k$, $i^2, j^2 \in K$ et

$$\mathrm{nrd}_{F/K} : \begin{cases} F & \longrightarrow & K \\ x + yi + zj + tk & \longmapsto & x^2 - i^2y^2 - j^2z^2 - k^2t^2 \end{cases}$$

ne représente 0 que trivialement.

L'exemple le plus élémentaire est celui des quaternions sur $K = \mathbf{Q}$ obtenus en prenant $i^2 = j^2 = -1$. On peut lui associer des ordres $\Lambda_1 = \mathbf{Z} + \mathbf{Z}i + \mathbf{Z}j + \mathbf{Z}k$ et $\Lambda_2 = \mathbf{Z} + \mathbf{Z}i + \mathbf{Z}j + \mathbf{Z}\frac{1+i+j+k}{2}$, qui sont des anneaux appelés quaternions de Hamilton et quaternions de Hurwitz. Même si ces anneaux ne sont pas commutatifs, on peut quand même considérer la propriété d'euclidianité : si on fait la division euclidienne comme en (I.5), on parlera d'euclidianité à droite. On peut définir de façon analogue l'euclidianité à gauche. On observe que l'anneau Λ_2 est euclidien à droite et à gauche pour $\mathrm{nrd}_{F/K}$, alors que Λ_1 n'est euclidien ni à droite ni à gauche pour $\mathrm{nrd}_{F/K}$. On peut se servir de l'euclidianité de Λ_2 pour montrer le théorème des quatre carrés de Lagrange.

Pour définir l'euclidianité pour la norme dans le cas général des corps de quaternions sur un corps de nombres, on considère un ordre Λ à la place de $\mathbf{Z}_K$, la norme étant remplacée par $\mathbf{N}_{K/\mathbf{Q}} \circ \mathrm{nrd}_{F/K}$: on dira ainsi que Λ est euclidien à droite pour la norme si pour tout $(\alpha, \beta) \in \Lambda \times \Lambda \setminus \{0\}$, il existe $\gamma \in \Lambda$ tel que

$$\left|\mathbf{N}_{K/\mathbf{Q}} \circ \mathrm{nrd}_{F/K}(\alpha - \beta\gamma)\right| < \left|\mathbf{N}_{K/\mathbf{Q}} \circ \mathrm{nrd}_{F/K}(\beta)\right|.$$

Eichler a ainsi montré que si K est euclidien pour la norme et si F est totalement indéfini sur K, alors tout ordre maximal Λ est euclidien à droite pour $\mathbf{N}_{K/\mathbf{Q}} \circ \mathrm{nrd}_{F/K}$ ([Eic38]).

Dans sa thèse ([Cha06]), Chaubert a étendu la définition et certaines propriétés du minimum euclidien aux corps de quaternions. Il a aussi noté que la construction de Motzkin s'appliquait à ce cas non commutatif.

Plan de la thèse

La thèse se compose de chapitres qui peuvent être lus séparément mais qui partagent certaines idées et techniques.

Dans le chapitre II, nous généralisons l'algorithme de Cerri aux corps de signature quelconque. Nous y décrivons en détail chaque étape de l'algorithme, en insistant sur les techniques pour rendre certaines étapes plus automatiques, notamment la recherche de graphes convenables. Nous donnons aussi de nombreux exemples de résultats obtenus : par exemple, nous donnons de nouvelles valeurs de minima euclidiens de corps cyclotomiques, nous exhibons des corps principaux non euclidiens pour la norme en diverses signatures et nous voyons comment adapter l'algorithme pour étudier l'euclidianité en plusieurs étapes et l'euclidianité généralisée. Enfin, nous étudions rigoureusement les problèmes liés à la précision des calculs et montrons comment les éviter.

Le chapitre III revient très brièvement sur la construction de Motzkin. Le but n'est pas de donner un panorama aussi complet que celui dressé par l'article de Samuel ([Sam71]), mais de rappeler les résultats importants, en particulier dans le cas non commutatif, ce qui nous sera particulièrement utile pour le chapitre V.

Dans le chapitre IV, nous étudions les classes euclidiennes, en particulier pour la norme. Nous commençons par décrire comment modifier la construction de Motzkin dans ce cas. Les idées du chapitre III seront donc réutilisées. Ensuite, nous expliquons comment appliquer l'algorithme du chapitre II pour étudier les classes euclidiennes pour la norme. Cela nous permettra d'obtenir de nouveaux exemples de classes euclidiennes pour la norme. De plus l'algorithme permet de montrer que certains corps de nombres n'admettent pas de classe euclidienne pour la norme. Ainsi, on trouve que $\mathbf{Q}(\sqrt{2}, \sqrt{35})$ n'a pas pas de classe euclidienne pour la norme, alors qu'il admet une classe euclidienne. Dans cette partie, nous généralisons aussi les résultats de Cioffari ([Cio79]) pour montrer que les seuls corps cubiques purs $K = \mathbf{Q}\left(\sqrt[3]{m}\right)$ $(m > 1)$ admettant une classe euclidienne pour la norme sont principaux.

Enfin, nous nous intéressons aux corps de quaternions euclidiens dans le chapitre V. Après avoir défini l'euclidianité d'un ordre Λ d'un corps de quaternions F, nous montrons que si Λ est euclidien, alors Λ est maximal, F est principal et tout ordre maximal de F est euclidien. Nous étudions ensuite les corps de quaternions totalement définis sur $\mathbf{Q}$ ou sur un corps quadratique et grâce à la construction de Motzkin, nous donnons la liste complète de tels corps euclidiens (non nécessairement pour la norme) et voyons qu'ils sont en fait euclidiens pour la norme. Puis nous nous intéressons au cas totalement indéfini sur un corps quadratique imaginaire. En particulier, nous montrons que si F est euclidien pour la norme, alors K est euclidien pour la norme, sauf peut-être dans un cas.

CHAPITRE II

CALCUL DU MINIMUM EUCLIDIEN D'UN CORPS DE NOMBRES

Plan

Ce chapitre reprend l'article [Lez12a], à paraître dans *Mathematics of Computation*.

1 Introduction

Dans ce chapitre, on considère un corps de nombres K. On note $\mathbf{Z}_K$ son anneau des entiers. Les entiers r_1 et $2r_2$ sont les nombres de places respectivement réelles et

imaginaires de K. On note $n = r_1 + 2r_2$ le degré de K et $(\sigma_i)_{1\leqslant i\leqslant n}$ les plongements de K dans $\mathbf{C}$. Quitte à les réordonner, on peut supposer que pour tout $1 \leqslant i \leqslant r_1$,

$$\sigma_i : K \longrightarrow \mathbf{R},$$

et pour tout $r_1 + 1 \leqslant i \leqslant r_1 + r_2$,

$$\overline{\sigma_i} = \sigma_{i+r_2}.$$

On désigne par $\mathbf{N}_{K/\mathbf{Q}}$ la norme usuelle, pour tout $x \in K$, on a

$$\mathbf{N}_{K/\mathbf{Q}}(x) = \prod_{i=1}^{n} \sigma_i(x).$$

On note disc_K le discriminant de K, h_K le nombre de classes de K, $\mathbf{Z}_K^\times$ le groupe des unités de K.

Proposition 1.1 (théorème des unités de Dirichlet)**.** *Le groupe des unités $\mathbf{Z}_K^\times$ est isomorphe au produit du groupe (cyclique d'ordre pair) des racines de l'unité de K et d'un groupe abélien libre de rang $r = r_1 + r_2 - 1$.*

Démonstration. Voir [Sam71]. □

Définition 1.2 (euclidianité par rapport à la norme). On dit que $\mathbf{Z}_K$ est euclidien par rapport à la norme si et seulement si pour tout $(a\,,\,b) \in \mathbf{Z}_K \times \mathbf{Z}_K \setminus \{0\}$, il existe $c \in \mathbf{Z}_K$ tel que

$$\left|\mathbf{N}_{K/\mathbf{Q}}(a - bc)\right| < \left|\mathbf{N}_{K/\mathbf{Q}}(b)\right|.$$

Si la propriété précédente est vérifiée, on dit aussi que *K est euclidien pour la norme*, que $\left|\mathbf{N}_{K/\mathbf{Q}}\right|$ est un algorithme d'Euclide ou encore un stathme. Il n'y a pas de raison de choisir la norme à la place d'un autre algorithme d'Euclide, mais la propriété de multiplicativité de la norme fait que c'est (relativement) plus facile de vérifier que $\left|\mathbf{N}_{K/\mathbf{Q}}\right|$ est un stathme pour $\mathbf{Z}_K$.

En effet, vérifier que $\mathbf{Z}_K$ est euclidien pour la norme revient à prouver que pour tout $\xi \in K$, il existe $z \in \mathbf{Z}_K$ tel que $\left|\mathbf{N}_{K/\mathbf{Q}}(\xi - z)\right| < 1$. Par conséquent, la détermination du caractère euclidien pour la norme de K peut être vu d'un point de vue géométrique. La notion de minimum euclidien sera introduite pour indiquer la « distance » entre K et le réseau $\mathbf{Z}_K$.

2 Minima euclidien et inhomogène de K

2.1 Minimum euclidien de K

Définition 2.1 (minimum euclidien local). Pour tout $\xi \in K$, on appelle *minimum euclidien de K en ξ* le nombre réel positif $m_K(\xi) := \inf_{z\in\mathbf{Z}_K} \left|\mathbf{N}_{K/\mathbf{Q}}(\xi - z)\right|$.

Avec cette définition, on observe immédiatement que le minimum euclidien en ξ est atteint pour tout $\xi \in K$, c'est-à-dire qu'il existe un certain $z \in \mathbf{Z}_K$ tel que $m_K(\xi) = \left|\mathbf{N}_{K/\mathbf{Q}}(\xi - z)\right|$. En particulier, $m_K(\xi) \in \mathbf{Q}$. Toutefois, une telle propriété ne fournit pas de technique pour calculer le minimum euclidien en ξ. Pour y parvenir, nous aurons besoin de connaître les unités $\mathbf{Z}_K^\times$ de K. Nous verrons comment procéder dans la partie 3.1.

Signalons aussi un cas trivial, mais qui s'avère souvent très utile.

Exemple 2.2. Soit $x \in \mathbf{Z}_K$ tel que $x \neq 0$ et $x \notin \mathbf{Z}_K^\times$. Alors $m_K\left(\frac{1}{x}\right) = \frac{1}{\left|\mathbf{N}_{K/\mathbf{Q}}(x)\right|}$.

La définition 2.1 nous permet de reformuler la définition de l'euclidianité pour la norme : K est euclidien pour la norme si et seulement si pour tout $\xi \in K$, $m_K(\xi) < 1$, ce qui mène à la définition naturelle suivante.

Définition 2.3 (minimum euclidien). On pose $M(K) := \sup_{\xi \in K} m_K(\xi)$ et on l'appelle *minimum euclidien de* K.

Nous verrons que $M(K)$ est fini dans la partie 2.3. Le but principal de ce chapitre est de calculer ce réel positif, étant donnée l'observation élémentaire suivante.

1. Si $M(K) < 1$, alors K est euclidien pour la norme.
2. Si $M(K) > 1$, alors K n'est pas euclidien pour la norme.

Nous verrons un résultat plus précis (proposition 2.8) dans le paragraphe 2.3.

2.2 Plongement de K

Rappelons que l'on note $(\sigma_i)_{1 \leqslant i \leqslant n}$ les plongements de K dans $\mathbf{C}$. On pose

$$\Phi : \begin{cases} K & \longrightarrow & \mathbf{R}^n \\ x & \longmapsto & \left(\sigma_1(x), \ldots, \sigma_{r_1}(x), \quad \mathrm{Re}\left(\sigma_{r_1+1}(x)\right), \ldots, \mathrm{Re}\left(\sigma_{r_1+r_2}(x)\right), \right. \\ & & \left. \qquad\qquad \mathrm{Im}\left(\sigma_{r_1+1}(x)\right), \ldots, \mathrm{Im}\left(\sigma_{r_1+r_2}(x)\right)\right) \end{cases}$$

Nous allons déduire des propriétés de K à partir de résultats obtenus sur $\Phi(K)$. Pour ce faire, on étend le produit défini sur K à $\mathbf{R}^n$ via Φ : pour $x = (x_i)_{1 \leqslant i \leqslant n}$ et $y = (y_i)_{1 \leqslant i \leqslant n}$, on pose $x \cdot y := (z_i)_{1 \leqslant i \leqslant n}$ où

$$z_i = \begin{cases} x_i y_i & \text{si } 1 \leqslant i \leqslant r_1, \\ x_i y_i - x_{i+r_2} y_{i+r_2} & \text{si } r_1 < i \leqslant r_1 + r_2, \\ x_{i-r_2} y_i + x_i y_{i-r_2} & \text{si } r_1 + r_2 < i \leqslant n. \end{cases}$$

Avec cette notation, pour tous $\xi, \nu \in K$, $\Phi(\xi\nu) = \Phi(\xi) \cdot \Phi(\nu)$.

Par ailleurs, on introduit $H := K \otimes_{\mathbf{Q}} \mathbf{R}$, que l'on identifie avec $\mathbf{R}^n$ muni du produit défini précédemment et on considère Φ comme une application de K dans H. On étend la norme à H en posant

$$\mathcal{N} : \begin{cases} H & \longrightarrow & \mathbf{R} \\ x = (x_i)_{1 \leqslant i \leqslant n} & \longmapsto & \left|\prod_{i=1}^{r_1} x_i \prod_{i=r_1+1}^{r_1+r_2} (x_i^2 + x_{i+r_2}^2)\right| \end{cases}.$$

Ainsi, pour tout $\xi \in K$, $\left|\mathbf{N}_{K/\mathbf{Q}}(\xi)\right| = \mathcal{N}(\Phi(\xi))$. Avec cette définition, la fonction $\mathcal{N}$ est multiplicative et continue. Cela nous conduit à définir la notion suivante.

2.3 Minimum inhomogène de K

Définition 2.4 (minimum inhomogène). Pour tout $x \in H$, on définit le *minimum inohomogène de K en x* par $m_{\overline{K}}(x) := \inf_{z \in \mathbf{Z}_K} \mathcal{N}(x - \Phi(z))$.

Remarquons que pour tout $\xi \in K$, $m_K(\xi) = m_{\overline{K}}(\Phi(\xi))$. De plus $m_{\overline{K}}$ est le minimum inhomogène par rapport au réseau $\Phi(\mathbf{Z}_K)$ pour l'application $\mathcal{N}$. On peut en déduire les propriétés suivantes de $m_{\overline{K}}$.

Proposition 2.5. *L'application $m_{\overline{K}}$ vérifie les propriétés suivantes.*

1. *Pour tous $\varepsilon \in \mathbf{Z}_K^\times$, $x \in H$, $Z \in \Phi(\mathbf{Z}_K)$ on a $m_{\overline{K}}(\Phi(\varepsilon)\cdot x - Z) = m_{\overline{K}}(x)$.*
2. *$m_{\overline{K}}$ induit une application (aussi notée $m_{\overline{K}}$) sur l'espace quotient $H/\Phi(\mathbf{Z}_K)$.*
3. *$m_{\overline{K}}$ est semi-continue supérieurement sur H et $H/\Phi(\mathbf{Z}_K)$. En particulier, $m_{\overline{K}}$ est bornée et atteint ses bornes.*

Démonstration. 1. Par définition de $m_{\overline{K}}$, en notant $Z = \Phi(z)$ avec $z \in \mathbf{Z}_K$, on a

$$\begin{aligned} m_{\overline{K}}(\Phi(\varepsilon)\cdot x - Z) &= \inf_{t\in\mathbf{Z}_K} \mathcal{N}(\Phi(\varepsilon)\cdot x - \Phi(z) - \Phi(t)), \\ &= \inf_{t\in\mathbf{Z}_K} \mathcal{N}(\Phi(\varepsilon)\cdot(x - \Phi(\varepsilon^{-1}\cdot(z+t)))) \\ &= \inf_{u\in\varepsilon^{-1}(\mathbf{Z}_K+z)} \mathcal{N}(\Phi(\varepsilon)\cdot(x-\Phi(u))). \end{aligned}$$

Or, par multiplicativité de $\mathcal{N}$, $\mathcal{N}(\Phi(\varepsilon)\cdot(x-\Phi(u))) = \mathcal{N}(\Phi(\varepsilon))\cdot\mathcal{N}(x-\Phi(u)) = \mathcal{N}(x-\Phi(u))$, car $\mathcal{N}(\Phi(\varepsilon)) = \left|\mathbf{N}_{K/\mathbf{Q}}(\varepsilon)\right| = 1$. De plus $\varepsilon^{-1}(\mathbf{Z}_K + z) = \mathbf{Z}_K$, on en déduit

$$\inf_{u\in\varepsilon^{-1}(\mathbf{Z}_K+z)} \mathcal{N}(\Phi(\varepsilon)\cdot(x-\Phi(u))) = \inf_{u\in\mathbf{Z}_K} \mathcal{N}(x-\Phi(u)),$$

d'où l'égalité

$$m_{\overline{K}}(\Phi(\varepsilon)\cdot x - Z) = m_{\overline{K}}(x).$$

2. C'est une conséquence facile du premier point.
3. Cela résulte de la continuité de $\mathcal{N}$. En effet, soient $x \in \mathbf{R}^n$ et $\epsilon > 0$. Par définition de $m_{\overline{K}}$, il existe $Z \in \Phi(\mathbf{Z}_K)$ tel que

$$\mathcal{N}(x - Z) < m_{\overline{K}}(x) + \frac{\epsilon}{2}.$$

Par continuité de $\mathcal{N}$, il existe un voisinage V de x dans H tel que pour tout $y \in V$,

$$\mathcal{N}(y - Z) < \mathcal{N}(x - Z) + \frac{\epsilon}{2}.$$

Donc pour tout $y \in V$, on a

$$m_{\overline{K}}(y) \leqslant \mathcal{N}(y - Z) < m_{\overline{K}}(x) + \epsilon.$$

Cela montre que $m_{\overline{K}}$ est semi-continue supérieure dans H, donc elle l'est aussi sur $H/\Phi(\mathbf{Z}_K)$.

Par ailleurs, $H/\Phi(\mathbf{Z}_K)$ est compact. En effet, H est séparé et l'application naturelle $H/\Phi(\mathbf{Z}_K) \longrightarrow H$ est continue et injective, donc $H/\Phi(\mathbf{Z}_K)$ est séparé. Comme l'application $\begin{cases} [0,1]^n & \longrightarrow & H/\Phi(\mathbf{Z}_K) \\ x = (x_i)_{1\leqslant i\leqslant n} & \longmapsto & \Phi\left(\sum_{i=1}^n x_i e_i\right) + \Phi(\mathbf{Z}_K) \end{cases}$ est continue, surjective et $[0,1]^n$ est compact, on obtient que $H/\Phi(\mathbf{Z}_K)$ est effectivement compact.

Dès lors, $m_{\overline{K}}$ est majorée et atteint sa borne supérieure.

□

Comme pour le minimum euclidien, on introduit la quantité suivante.

Définition 2.6 (minimum inhomogène de K). $M(\overline{K}) := \sup_{x\in H} m_{\overline{K}}(x)$.

On voit immédiatement que $M(K) \leqslant M(\overline{K})$. La proposition 2.5 (3) implique que $M(\overline{K})$ est fini et qu'il existe $x \in H$ tel que

$$m_{\overline{K}}(x) = M(\overline{K}) \in \mathbf{R}.$$

Par conséquent, $M(K) \leqslant M(\overline{K})$ est aussi fini. Néanmoins, il serait plus intéressant de savoir s'il existe $\xi \in K$ tel que $m_{\overline{K}}(\Phi(\xi)) = M(\overline{K})$. C'est évidemment vrai dans les cas triviaux où le rang des unités est $r = 0$. En effet, si $K = \mathbf{Q}$, $M(K) = M(\overline{K}) = \frac{1}{2}$; si K est un corps quadratique imaginaire, on plonge K dans $H = \mathbf{C}$ et on effectue des raisonnements géométriques pour calculer $M(\overline{K})$: on trouve $\xi \in K$ tel que $m_K(\xi) = M(\overline{K})$, donc $M(\overline{K}) = M(K)$ (voir [Coh62, chapter VI.8, p. 105]). Par ailleurs, le théorème suivant fournit une réponse positive dans de nombreux cas.

Théorème 2.7. *Rappelons que r désigne le rang des unités.*

1. *Si $r = 1$, alors $M(K) = M(\overline{K})$.*
2. *Si $r > 1$, alors il existe $\xi \in K$ tel que $M(\overline{K}) = m_K(\xi)$. En particulier, $M(K) = M(\overline{K}) \in \mathbf{Q}$.*

L'énoncé (1) a été prouvé par Barnes et Swinnerton-Dyer ([BSD52b]) dans le cas $r_1 = 2, r_2 = 0$. Ce résultat a été étendu par van der Linden ([Lin84]) dans le cas $r = 1$. Cerri a prouvé (2) dans [Cer06].

Si $r = 1$, aucun résultat aussi fort que (2) n'est prouvé. Cependant, aucun contre-exemple n'est connu et le fait que cette propriété soit vraie a été conjecturé dans le cas quadratique réel par Barnes et Swinnerton-Dyer ([BSD52b]).

Ainsi, le calcul de $M(K)$ détermine si K est euclidien ou non pour la norme si $r > 1$. La proposition suivante résume le critère pour décider de l'euclidianité pour la norme de K si on connaît la valeur de $M(K)$.

Proposition 2.8. *Soit K un corps de nombres.*

1. *Si $M(K) < 1$, alors K est euclidien pour la norme.*
2. *Si $M(K) > 1$, alors K n'est pas euclidien pour la norme.*
3. *Si $M(K) = 1$ et si le rang de $\mathbf{Z}_K^\times$ est strictement supérieur à 1, alors K n'est pas euclidien pour la norme.*

Par conséquent, $M(K) = 1$ implique que K n'est pas euclidien pour la norme, sauf peut-être pour des corps de nombres dont le rang des unités vaut 1. Parmi ces corps de nombres, on sait qu'il n'en existe qu'un nombre fini vérifiant $M(K) \leqslant 1$, ce qui permet en théorie de tous les calculer et de vérifier que la proposition 2.8 (3) est aussi vraie pour $r = 1$. Nous allons le faire explicitement dans le cas quadratique réel dans le paragraphe suivant.

2.4 $M(K) = 1$ dans le cas quadratique réel

Dans ce paragraphe, on considère $K = \mathbf{Q}(\sqrt{m})$ où m est un entier sans facteur carré strictement supérieur à 1. On rappelle que $H \simeq \mathbf{R}^2$.

Nous allons prouver le résultat suivant.

Théorème 2.9. *Un corps quadratique réel K vérifie $M(K) = 1$ si et seulement si $K = \mathbf{Q}\left(\sqrt{65}\right)$. En particulier, K est euclidien pour la norme si et seulement si $M(K) < 1$.*

Ainsi, dans le cas particulier des corps quadratiques réels, les conclusions de la proposition 2.8 sont encore vraies.

2.4.1 Borne d'Ennola

Théorème 2.10 ([Enn58, Lemma 11]). *Soit $f(s,t) = as^2 + bst + ct^2$ une forme quadratique, où $a, b, c \in \mathbf{Q}$ vérifient $b^2 - 4ac > 0$. On suppose que f ne représente pas 0 pour $(s,t) \neq (0,0)$. Alors il existe $h, k \in \mathbf{Q}$, tels que*

$$|f(s+h, t+k)| \geqslant \kappa\sqrt{b^2 - 4ac},$$

pour tous entiers s, t, où $\kappa = \dfrac{1}{16 + 6\sqrt{6}}$.

Si $m \equiv 2, 3 \pmod 4$, alors $\mathbf{Z}_K = \mathbf{Z} + \mathbf{Z}\sqrt{m}$. Pour tous $x, y \in \mathbf{R}$, on pose $f(x,y) = x^2 - my^2$. En appliquant le théorème 2.10, on obtient deux rationnels h et k tels que

$$m_K(h + k\sqrt{m}) = m_{\overline{K}}(h + k\sqrt{m}, h - k\sqrt{m}) \geqslant \kappa\sqrt{4m}.$$

Par conséquent, si $m > \frac{1}{4\kappa^2}$, alors $M(K) > 1$. Dès lors, si on s'intéresse aux corps de nombres quadratiques réels K dont le minimum euclidien est inférieur ou égal à 1, il suffit de considérer $m \leqslant 235$, si $m \equiv 2, 3 \pmod 4$.

Si $m \equiv 1 \pmod 4$, alors $\mathbf{Z}_K = \mathbf{Z} + \mathbf{Z}\frac{1+\sqrt{m}}{2}$ et on peut appliquer le théorème 2.10 avec $f(x,y) = \left(x + \frac{y}{2}\right)^2 - m\frac{y^2}{4} = x^2 + xy + \frac{1-m}{4}y^2$. En ce cas, il suffit donc de considérer $m \leqslant \frac{1}{\kappa^2}$, ce qui donne $m \leqslant 941$.

2.4.2 Un lemme classique

À présent, il ne reste plus qu'un nombre fini de cas à traiter. Dans [Enn58], la borne est utilisée pour déterminer les corps de nombres euclidiens pour la norme, mais ici, on veut savoir quand $M(K) = 1$. Pour y parvenir, comme dans [Enn58], on utilise un lemme de congruence classique qui remonte au moins à [BR36].

Lemme 2.11 (Cas $m \equiv 2, 3 \pmod 4$). *Supposons que K est euclidien pour la norme. Si r est un entier vérifiant $0 < r < m$ et est un carré modulo m, alors il existe $X, Y \in \mathbf{Z}$ tels que $X^2 - mY^2 \in \{r, r - m\}$.*

Démonstration. Soit Z un entier tel que $Z^2 \equiv r \pmod m$. On effectue la division euclidienne de $Z\sqrt{m}$ par $-m$: il existe $\alpha, \beta \in \mathbf{Z}$ tels que

$$\left|\mathbf{N}_{K/\mathbf{Q}}\left(Z\sqrt{m} + m(\alpha + \beta\sqrt{m})\right)\right| < m^2.$$

Ensuite, on divise par m pour obtenir

$$\left|m\alpha^2 - (\beta m + Z)^2\right| < m.$$

On écrit $X = \beta m + Z$ et $Y = \alpha$. Alors $X^2 - mY^2 \equiv r \pmod m$. On déduit le résultat de la borne trouvée précédemment. □

On peut obtenir un résultat similaire dans l'autre cas.

Lemme 2.12 (Cas $m \equiv 1 \pmod 4$). *On suppose que K est euclidien pour la norme. Si r est un entier vérifiant $0 < r < m$ et est un carré modulo m, alors il existe $X, Y \in \mathbf{Z}$ tels que $X^2 - mY^2 \in \{4r, 4(r-m)\}$ et $X \equiv Y \pmod 2$.*

Démonstration. On effectue la division euclidienne de $Z\sqrt{m}$ par $-m$: il existe $\alpha, \beta \in \mathbf{Z}$ tels que

$$\left|\mathbf{N}_{K/\mathbf{Q}}\left(Z\sqrt{m} + m\left(\alpha + \beta\frac{1+\sqrt{m}}{2}\right)\right)\right| < m^2.$$

En multipliant par $\frac{4}{m}$, on trouve

$$\left|(2Z+\beta)^2 - m(2\alpha+\beta)^2\right| < 4m$$

On pose $X = 2\mathbf{Z} + \beta$ et $Y = 2\alpha + \beta$, alors $X \equiv Y \equiv \beta \pmod{m}$ et $X^2 - mY^2 \equiv 4r \pmod{4m}$. Comme $-4m < X^2 - 4mY^2 < 4m$, on en déduit que $X^2 - mY^2 \in \{4r, 4(r-m)\}$. □

Par conséquent, pour montrer que K n'est pas euclidien pour la norme, il suffit de trouver un r contredisant les conclusions des lemmes 2.11 ou 2.12. De plus, si on parvient à trouver un tel r, alors $M(K) \geqslant \min\left\{\frac{r+m}{m}, \frac{2m-r}{m}\right\} > 1$.

En effet, si $m \equiv 2, 3 \pmod 4$, alors d'après la preuve du lemme 2.11, on a en fait $m_K\left(\frac{Z\sqrt{m}}{-m}\right) \geqslant \min\{\frac{(r+m)m}{m^2}, \frac{(2m-r)m}{m^2}\}$. Par ailleurs, si $m \equiv 1 \pmod 4$, d'après la preuve du lemme 2.12, on a $m_K\left(\frac{Z\sqrt{m}}{-m}\right) \geqslant \min\{\frac{(4r+4m)m}{4m^2}, \frac{(8m-4r)m}{4m^2}\}$.

Dans [Enn58], ce raisonnement est utilisé [1] dans tous les cas sauf sept d'entre eux, si $m \equiv 2, 3 \pmod 4$ et dans tous les cas sauf vingt-deux si $m \equiv 1 \pmod 4$.

Pour les valeurs restantes de m, soit elles définissent un corps de nombres euclidien pour la norme $K = \mathbf{Q}(\sqrt{m})$, soit des valeurs explicites $x \in K$ sont connues [2] pour lesquelles $m_K(x) > 1$, sauf pour $m = 65$. Dans ce dernier cas $M(K) = m_K\left(\frac{1+\sqrt{65}}{4}\right) = 1$ et K n'est pas euclidien pour la norme.

Par conséquent, dans le cas $r_1 = 2$, $r_2 = 0$, on sait qu'aucun corps euclidien pour la norme K ne vérifie $M(K) = 1$. Cela termine la preuve du théorème 2.9.

Remarque 2.13. Le problème est toujours ouvert pour $(r_1, r_2) \in \{(1,1), (0,2)\}$. Des exemples de corps de nombres de telle signature et avec $M(K) = 1$ seront donnés au paragraphe 5.6.

2.5 Décidabilité de l'euclidianité

Dans ce paragraphe, nous démontrons le résultat suivant, dont l'idée générale est due à Lenstra ([Len80]).

Proposition 2.14. *Soit K un corps de nombres de signature différente de $(1,1)$ et $(0,2)$, alors l'euclidianité de K pour la norme est un problème décidable.*

Démonstration. L'idée de base est que pour ces corps de nombres, K est euclidien pour la norme si et seulement si $M(K) = M(\overline{K}) < 1$. Notons précisément $\mathcal{A} := \{z \in H,\ \mathcal{N}(z) < 1\}$. Dès lors, sous les hypothèses de la proposition, K est euclidien pour la norme si et seulement si $\Phi(\mathbf{Z}_K) + \mathcal{A} = H$.

1. Dans la preuve originale d'Ennola [Enn58], certains corollaires des lemmes 2.11 et 2.12 sont énoncés, mais on peut aussi construire directement des contre-exemples en utilisant l'algorithme de Lagrange-Matthews-Mollin ([Mat00], [Mol01]) pour montrer rapidement que certaines équations de Pell n'admettent pas de solutions de la forme voulue.

2. voir [Enn58, pp. 55–56] où les points critiques et les références sont données.

En effet, si K est euclidien pour la norme, alors pour tout $z \in H$, $m_{\overline{K}}(z) \leqslant M(\overline{K}) < 1$. Donc, par définition de $m_{\overline{K}}(z)$, il existe $Z \in \Phi(\mathbf{Z}_K)$ tel que

$$\mathcal{N}(z - Z) \leqslant \frac{M(\overline{K}) + 1}{2} < 1.$$

Donc $z \in \Phi(\mathbf{Z}_K) + \mathcal{A}$. L'inclusion réciproque étant claire, on en déduit $\Phi(\mathbf{Z}_K) + \mathcal{A} = H$.

Notons alors $\mathcal{F} \subseteq H$ un domaine fondamental de $\mathbf{Z}_K$. Comme $\mathbf{Z}_K \setminus \{0\}$ est dénombrable, on peut noter ses éléments sous la forme $\beta_1, \beta_2, \ldots$. Pour tout i, on pose $X_i = \Phi(\beta_i)$. On vérifie alors successivement pour $n = 1, 2, \ldots$ les conditions suivantes.

I_n : Il existe $\alpha \in \mathbf{Z}_K$ tel que $\alpha \not\equiv \rho \pmod{\beta_n}$ pour tout $\rho \in \mathbf{Z}_K$ tel que

$$\left|\mathbf{N}_{K/\mathbf{Q}}(\rho)\right| < \left|\mathbf{N}_{K/\mathbf{Q}}(\beta_n)\right|.$$

II_n : Le domaine fondamental est recouvert par les $n + 1$ translatés

$$\mathcal{A}, X_1 + \mathcal{A}, \ldots, X_n + \mathcal{A}.$$

On s'arrête si l'une des deux conditions est vérifiée : si c'est I_n, alors K n'est pas euclidien pour la norme, si c'est II_n, alors K est euclidien pour la norme. Il reste donc à voir qu'il existe n tel que I_n ou II_n est vérifiée.

Dans le contraire, pour tout n, I_n et II_n sont fausses. D'une part, cela implique que K est euclidien pour la norme. En effet, pour tout $\alpha \in \mathbf{Z}_K$ et tout $\beta_n \in \mathbf{Z}_K \setminus \{0\}$, il existerait $\rho \equiv \alpha \pmod{\beta_n}$ et $\left|\mathbf{N}_{K/\mathbf{Q}}(\rho)\right| < \left|\mathbf{N}_{K/\mathbf{Q}}(\beta_n)\right|$, c'est-à-dire $m_K\left(\frac{\alpha}{\beta_n}\right) < 1$.

Mais d'autre part $\Phi(\mathbf{Z}_K) + \mathcal{A} \subsetneq H$, ce qui montre que K n'est pas euclidien pour la norme. Cela fournit une contradiction. □

Remarque 2.15. Le fait que l'euclidianité pour la norme soit décidable n'implique pas qu'on a un algorithme pour le faire. En effet, on ne sait pas pour quel n l'une des conditions va être vérifiée. Par ailleurs, la condition II_n n'est pas si facile à tester.

2.6 Bornes pour le minimum euclidien

2.6.1 Bornes inférieures

Pour tout idéal entier I de $\mathbf{Z}_K$, on note $\mathbf{N}I$ le cardinal de $\mathbf{Z}_K/I$. On définit alors l'entier

$$\Lambda(K) = \min\left\{\mathbf{N}I,\ I \text{ idéal entier},\ \{0\} \subsetneq I \subsetneq \mathbf{Z}_K\right\}.$$

On a ainsi $M(K) \geqslant \frac{1}{\Lambda(K)}$. En fait, si on suppose que K est principal, alors il existe un certain entier $x \in \mathbf{Z}_K \setminus (\mathbf{Z}_K^\times \cup \{0\})$ tel que $\Lambda(K) = \mathbf{N}((x)) = \left|\mathbf{N}_{K/\mathbf{Q}}(x)\right|$. Dès lors, $m_K\left(\frac{1}{x}\right) = \frac{1}{\left|\mathbf{N}_{K/\mathbf{Q}}(x)\right|} = \frac{1}{\Lambda(K)}$ (voir l'exemple 2.2). Par ailleurs, si K n'est pas principal, alors K n'est pas euclidien pour la norme et on a $M(K) \geqslant 1$.

Dans le cas $r = 1$, on a aussi des bornes spéciales pour $M(K)$ en fonction du discriminant de K. Elles permettent d'établir les propriétés suivantes.

Théorème 2.16 (Ennola, Cassels, van der Linden)**.** *Soit K un corps de nombres euclidien pour la norme et tel que $r = 1$.*

– *Si $r_1 = 2$, $r_2 = 0$, alors* $\mathrm{disc}_K \leqslant 945$.

– *Si $r_1 = r_2 = 1$, alors* $|\mathrm{disc}_K| \leqslant 170\,520$.

– *Si* $r_1 = 0$, $r_2 = 2$, *alors* $\mathrm{disc}_K \leqslant 230\,202\,117$.

Démonstration. Voir [Enn58], [Cas52] corrigé par [Lin84]. □

2.6.2 Bornes supérieures

Même si des bornes explicites sont connues dans des cas plus ou moins généraux (voir par exemple [Dav52] ou [BF06]), elles ne sont pas utiles pour l'exécution de l'algorithme, parce qu'elles ne sont pas assez bonnes pour de petits discriminants.

3 Outils pour l'algorithme

Le but de cette partie est de décrire des procédures *pratiques* qui vont être utilisées pour l'algorithme général de calcul du minimum euclidien d'un corps de nombres. Pour commencer, on traite le calcul du minimum euclidien local.

3.1 Calcul du minimum euclidien local

La technique est celle décrite par Cerri ([Cer07]) dans le cas totalement réel, écrite ici dans le cas général. Les idées et arguments sont classiques.

On rappelle que $r = r_1 + r_2 - 1$ désigne le rang de $\mathbf{Z}_K^\times$. Comme le cas $r = 0$ est facile, on va supposer que $r \geqslant 1$, c'est-à-dire que $\mathbf{Z}_K^\times$ est infini. Le groupe des unités $\mathbf{Z}_K^\times$ est déterminé par r unités fondamentales, que nous écrirons $\{\varepsilon_1, \ldots, \varepsilon_r\}$ et par les racines de l'unité de K. On identifie $H/\mathbf{Z}_K$ avec un domaine fondamental $\mathcal{F}$.

Les unités agissent sur K par multiplication et on peut étendre cette action à H par

$$\left\{ \begin{array}{ccc} \mathbf{Z}_K^\times \times H & \longrightarrow & H \\ (\varepsilon, x) & \longmapsto & \Phi(\varepsilon) \cdot x \end{array} \right. .$$

La proposition 2.5 (1) montre que $m_{\overline{K}}$ est constante sur les orbites de cette action. Pour $x \in H$, on note $\mathrm{Orb}(x)$ les éléments du domaine fondamental $\mathcal{F}$ qui sont des translatés par des vecteurs de $\Phi(\mathbf{Z}_K)$ d'éléments de l'orbite de x sous l'action des unités.

Remarque 3.1. Soit $x \in H$, l'orbite $\mathrm{Orb}(x)$ est finie si et seulement si $x \in \Phi(K)$.

Démonstration. Si $\mathrm{Orb}(x)$ est finie, on considère la famille $\{\Phi(\varepsilon)\cdot x \pmod{\Phi(\mathbf{Z}_K)}\,,\ \varepsilon \in \mathbf{Z}_K^\times\}$. Comme $r \geqslant 1$, $\mathbf{Z}_K^\times$ est infini et il existe deux unités distinctes ε et ν telles que $\Phi(\varepsilon)\cdot x \equiv \Phi(\nu)\cdot x \pmod{\Phi(\mathbf{Z}_K)}$. Ainsi,

$$x \in \Phi\left(\frac{1}{\varepsilon - \nu}\mathbf{Z}_K\right) \subseteq \Phi(K).$$

Réciproquement, si $x \in \Phi(K)$, alors il existe $a \in \mathbf{Z}_K$ et $b \in \mathbf{Z}_K \setminus \{0\}$ tels que $x = \Phi\left(\frac{a}{b}\right)$. Si on note $\mathcal{S}$ un système de représentants de $\mathbf{Z}_K/b\mathbf{Z}_K$, alors pour tout $\varepsilon \in \mathbf{Z}_K^\times$, il existe $s \in \mathcal{S}$ tel que

$$\Phi(\varepsilon)\cdot\Phi\left(\frac{a}{b}\right) = \Phi\left(\frac{s}{b}\right) \pmod{\Phi(\mathbf{Z}_K)}.$$

Ainsi, $\mathrm{Orb}(x) \subseteq \left\{\Phi\left(\frac{s}{b}\right) \pmod{\Phi(\mathbf{Z}_K)}\,,\ s \in \mathcal{S}\right\}$. Dès lors l'orbite $\mathrm{Orb}(x)$ a au plus $\#\mathcal{S} = \left|\mathbf{N}_{K/\mathbf{Q}}(b)\right|$ éléments. □

Pour tout $1 \leqslant i \leqslant n$, on pose $\Gamma_i := \prod_{j=1}^{r} \max\left\{\left|\sigma_i(\varepsilon_j)\right|, \frac{1}{\left|\sigma_i(\varepsilon_j)\right|}\right\}$, ce qui nous permet de définir

$$\Gamma(k) := \begin{cases} \left(\prod_{i=1}^{n-1} \Gamma_i\right)^{\frac{1}{n}} k^{\frac{1}{n}} & \text{si } K \text{ est totalement réel,} \\ \left(\prod_{i=1}^{r_1} \Gamma_i \prod_{i=r_1+1}^{r_1+r_2-1} \Gamma_i \Gamma_{i+r_2}\right)^{\frac{1}{n}} k^{\frac{1}{n}} & \text{sinon.} \end{cases}$$

Lemme 3.2. *Pour tout $(c_i)_{1\leqslant i\leqslant r} \in (\mathbf{R}_+^*)^r$, il existe une unité $\varepsilon \in \mathbf{Z}_K^\times$ telle que pour tout $1 \leqslant i \leqslant r$,*

$$c_i \leqslant |\sigma_i(\nu)| \leqslant c_i \Gamma_i.$$

Démonstration. La preuve est la même que dans le cas totalement réel (voir [Cer07]). On considère le plongement logarithmique de K :

$$\mathcal{L} : \begin{cases} K \setminus \{0\} & \longrightarrow & \mathbf{R}^{r_1+r_2} \\ x & \longmapsto & (\ln|\sigma_i(x)|)_{1\leqslant i\leqslant r_1+r_2} \end{cases},$$

on remarque que $\mathcal{R} = \mathcal{L}(\mathbf{Z}_K^\times)$ est un réseau de

$$\mathcal{H} = \left\{(x_i)_{1\leqslant i\leqslant r_1+r_2}, \sum_{i=1}^{r_1} x_i + 2\sum_{i=r_1+1}^{r_1+r_2} x_i = 0\right\}.$$

Ainsi, $(\mathcal{L}(\varepsilon_i))_{1\leqslant i\leqslant r}$ est une $\mathbf{Z}$-base de $\mathcal{R}$, donc $(\mathcal{L}(\varepsilon_i))_{1\leqslant i\leqslant r}$ est une base du $\mathbf{R}$-espace vectoriel $\mathcal{H}$.

Définissons alors $x = (x_i)_{1\leqslant i\leqslant r_1+r_2}$ par

$$x_i := \ln(c_i) - \sum_{\substack{1\leqslant l\leqslant r \\ |\sigma_l(\varepsilon_j)|>1}} \ln\left|\sigma_l(\varepsilon_j)\right|,$$

si $1 \leqslant i \leqslant r$ et

$$x_{r_1+r_2} := \begin{cases} -\sum_{i=1}^{r} x_i & \text{si } K \text{ est totalement réel,} \\ -\frac{1}{2}\left(\sum_{i=1}^{r_1} x_i + 2\sum_{i=r_1+1}^{r} x_i\right) & \text{sinon.} \end{cases}$$

Ainsi $x \in \mathcal{H}$. Donc il existe $(\alpha_j)_{1\leqslant j\leqslant r} \in \mathbf{R}^r$ tel que $x = \sum_{j=1}^{r} \alpha_j \mathcal{L}(\varepsilon_j)$. On pose

$$y := \sum_{j=1}^{r} \lfloor \alpha_j \rfloor \mathcal{L}(\varepsilon_j).$$

Si on note $\nu = \prod_{j=1}^{r} \varepsilon_j^{\lfloor\alpha_j\rfloor} \in \mathbf{Z}_K^\times$, alors $y = \mathcal{L}(\nu)$. Soit alors $1 \leqslant i \leqslant r$. On a

$$y_i - \ln(c_i) = y_i - x_i + \sum_{\substack{1\leqslant l\leqslant r \\ |\sigma_l(\varepsilon_j)|>1}} \ln\left|\sigma_l(\varepsilon_j)\right| = \sum_{j=1}^{r} \beta_{i,j} \ln\left|\sigma_i(\varepsilon_j)\right|,$$

où pour $1 \leqslant j \leqslant r$, $\beta_{i,j} = \begin{cases} \lfloor\alpha_j\rfloor - \alpha_j & \text{si } \left|\sigma_i(\varepsilon_j)\right| < 1, \\ \lfloor\alpha_j\rfloor - \alpha_j + 1 & \text{sinon.} \end{cases}$

Ainsi, pour tous $1 \leqslant i, j \leqslant r$, $\beta_{i,j}$ est du signe de $\ln\left|\sigma_i(\varepsilon_j)\right|$ et $|\beta_{i,j}| \leqslant 1$. Par conséquent,

$$0 \leqslant y_i - \ln(c_i) \leqslant \sum_{j=1}^{r} \left|\ln\left|\sigma_i(\varepsilon_j)\right|\right|.$$

On obtient donc $1 \leqslant \frac{|\sigma_i(\nu)|}{c_i} \leqslant \Gamma_i$ et en multipliant par c_i, cela donne l'inégalité désirée. □

Proposition 3.3. *Soit $x \in \Phi(K) \setminus \Phi(\mathbf{Z}_K)$ et $k > 0$. S'il existe $X \in \Phi(\mathbf{Z}_K)$ tel que $0 < \mathcal{N}(x - X) < k$, alors il existe $\nu \in \Phi(\mathbf{Z}_K^\times)$ et $Y \in \Phi(\mathbf{Z}_K)$ tels que*

$$\mathcal{N}(\nu\cdot x - Y) < k \text{ et } \begin{cases} |(\nu\cdot x - Y)_i| \leqslant \Gamma(k) & \text{pour } 1 \leqslant i \leqslant r_1 \\ (\nu\cdot x - Y)_i^2 + (\nu\cdot x - Y)_{i+r_2}^2 \leqslant \Gamma(k)^2 & \text{pour } r_1+1 \leqslant i \leqslant r_1+r_2 \end{cases}.$$

Démonstration. Notons $z = x - X$ et fixons $t_i := \begin{cases} |z_i| & \text{si } i \leqslant r_1 \\ \sqrt{z_i^2 + z_{i+r_2}^2} & \text{si } i > r_1 \end{cases}$ pour tout indice $i \in \{1, \dots, r\}$. Par hypothèse, $\mathcal{N}(z) > 0$, donc $z \neq 0$ et ainsi, pour tout $i \in \{1, \dots, r\}$, on a $t_i \neq 0$, ce qui permet de définir

$$c_i := \frac{\Gamma(k)}{\Gamma_i t_i} > 0.$$

D'après le lemme 3.2, il existe une unité $\varepsilon \in \mathbf{Z}_K^\times$ telle que pour tout $1 \leqslant i \leqslant r$,

$$\begin{cases} \frac{\Gamma(k)}{\Gamma_i} \leqslant |(\nu\cdot z)_i| \leqslant \Gamma(k) & \text{si } i \leqslant r_1, \\ \frac{\Gamma(k)}{\Gamma_i} \leqslant \sqrt{(\nu\cdot z)_i^2 + (\nu\cdot z)_{i+r_2}^2} \leqslant \Gamma(k) & \text{si } i > r_1, \end{cases} \tag{II.1}$$

en notant $\nu := \Phi(\varepsilon)$.

Si K est totalement réel, alors $n = r + 1$ et donc $\mathcal{N}(z) = |(\nu\cdot z)_n| \cdot \prod_{i=1}^r |(\nu\cdot z)_i|$. Or $\mathcal{N}(z) < k$, et donc

$$|(\nu\cdot z)_n| \leqslant \frac{k}{\prod_{i=1}^r |(\nu\cdot z)_i|} \leqslant k \prod_{i=1}^r \frac{\Gamma_i}{\Gamma(k)},$$

d'après (II.1). Mais on a $k \prod_{i=1}^r \frac{\Gamma_i}{\Gamma(k)} = \Gamma(k)$, donc

$$|(\nu\cdot z)_n| \leqslant \Gamma(k).$$

Si K n'est pas totalement réel, alors on a

$$\mathcal{N}(z) = \left((\nu\cdot z)_{r_1+r_2}^2 + (\nu\cdot z)_{r_1+2r_2}^2\right) \cdot \prod_{i=1}^{r_1} |(\nu\cdot z)_i| \cdot \prod_{i=r_1+1}^{r} \left((\nu\cdot z)_i^2 + (\nu\cdot z)_{i+r_2}^2\right) < k.$$

Par conséquent,

$$\begin{aligned} (\nu\cdot z)_{r_1+r_2}^2 + (\nu\cdot z)_{r_1+2r_2}^2 &\leqslant \frac{k}{\prod_{i=1}^{r_1} |(\nu\cdot z)_i| \cdot \prod_{i=r_1+1}^{r} \left((\nu\cdot z)_i^2 + (\nu\cdot z)_{i+r_2}^2\right)} \\ &\leqslant k \prod_{i=1}^{r_1} \frac{\Gamma_i}{\Gamma(k)} \prod_{i=r_1+1}^{r} \frac{\Gamma_i^2}{\Gamma(k)^2} \text{ d'après (II.1)}, \\ &\leqslant \Gamma(k). \end{aligned}$$

Cela montre l'inégalité recherchée dans tous les cas en prenant $Y := \nu \cdot X$. □

Théorème 3.4. *Soit $x \in \Phi(K)$ et $k > 0$. Pour tout $z \in \mathrm{Orb}(x)$, on pose*

$$\mathcal{I}_{z,k} := \{Z \in \Phi(\mathbf{Z}_K), |z_i - Z_i| \leqslant \Gamma(k) \text{ pour tout } 1 \leqslant i \leqslant n\}.$$

On considère le rationnel positif

$$\mathcal{M}_k := \min_{z \in \mathrm{Orb}(x)} \left(\min_{Z \in \mathcal{I}_{z,k}} \mathcal{N}(z - Z) \right).$$

Si $\mathcal{M}_k \leqslant k$, alors $m_{\overline{K}}(x) = \mathcal{M}_k$.

Démonstration. La preuve est identique à celle dans le cas totalement réel ([Cer07]).

La fonction $m_{\overline{K}}$ étant constante sur l'orbite de x, on a pour tout $z \in \mathrm{Orb}(x)$ et $Z \in \mathcal{I}_{z,k}$, $m_{\overline{K}}(x) = m_{\overline{K}}(z) \leqslant \mathcal{N}(z - Z)$. Dès lors,

$$m_{\overline{K}}(x) \leqslant \mathcal{M}_k.$$

On raisonne alors par l'absurde et on suppose que $m_{\overline{K}}(x) < \mathcal{M}_k$. Par définition, cela implique qu'il existe $X \in \Phi(\mathbf{Z}_K)$ tel que

$$\mathcal{N}(x - X) < \mathcal{M}_k \leqslant k.$$

D'après la proposition 3.3, on peut en déduire qu'il existe $v \in \mathbf{Z}_K^\times$ et $Y \in \Phi(\mathbf{Z}_K)$ tels que

$$\mathcal{N}(v \cdot x - Y) < k \qquad \text{et} \qquad |(v \cdot x - Y)_i| \leqslant \Gamma(k) \text{ pour tout } 1 \leqslant i \leqslant n.$$

C'est incompatible avec la définition de $\mathcal{M}_k$. □

Comme la fonction $k \longmapsto \mathcal{M}_k$ est strictement décroissante, le théorème 3.4 implique que l'algorithme suivant nécessite au plus une exécution de la boucle pour obtenir $m_{\overline{K}}(x)$.

Algorithme 3.1 Calcul du minimum euclidien local

ENTRÉE : un corps de nombres K, un point $x \in \Phi(K)$, l'orbite $\mathrm{Orb}(x)$ de x, $k > 0$
SORTIE : $m_K(x)$

1: Calculer $\Gamma(k)$, $\mathcal{M}_k$
2: **tant que** $\mathcal{M}_k > k$ **faire**
3: $k \leftarrow \mathcal{M}_k$, calculer $\Gamma(k)$, $\mathcal{M}_k$
4: **fin tant que**
5: **renvoyer** $\mathcal{M}_k$

Remarques 3.5.

1. L'algorithme ne s'applique qu'aux éléments de $\Phi(K)$, parce que l'orbite des autres éléments de H est infinie (voir remarque 3.1).
2. Si $x = \frac{1}{\xi}$ où $\xi \in \mathbf{Z}_K \setminus \mathbf{Z}_K^\times \cup \{0\}$, alors $m_K(x) = \frac{1}{|\mathbf{N}_{K/\mathbf{Q}}(\xi)|}$, si bien que l'exécution de l'algorithme 3.1 est inutile en ce cas.
3. L'algorithme 3.1 nécessite de connaître l'orbite $\mathrm{Orb}(x)$. Nous verrons comment la calculer au paragraphe 4.3.2.

3.2 Plongement et test d'absorption de K par $\mathbf{Z}_K$

À présent, on s'intéresse au minimum euclidien $M(K)$. L'idée générale va être de prouver que $m_K(\xi) < k$ pour un certain réel k, sauf pour un ensemble fini de points $(\xi_i)_{1\leqslant i\leqslant l}$ de K. Si on trouve alors que $m_K(\xi_i) \geqslant k$ pour un certain i, alors $M(K) = \max_{1\leqslant i\leqslant l} m_K(\xi_i)$.

3.2.1 Présentation et idées générales

On aura besoin de quelques informations sur K. En fait, on suppose que l'on connaît une $\mathbf{Z}$-base $(z_i)_{1\leqslant i\leqslant n}$ de $\mathbf{Z}_K$ et de (bonnes) approximations de $\sigma_j(z_i)$ pour tout $1 \leqslant i, j \leqslant n$. Cela nous permet d'identifier $\mathbf{Q}^n$ et K via l'isomorphisme de $\mathbf{Q}$-espaces vectoriels

$$\Psi : \begin{cases} \mathbf{Q}^n & \longrightarrow & K \\ (q_i)_{1\leqslant i\leqslant n} & \longmapsto & \sum_{i=1}^n q_i z_i \end{cases}.$$

Comme Φ et Ψ sont toutes les deux linéaires, $\Phi \circ \Psi : \mathbf{Q}^n \longrightarrow H$ est linéaire et on peut l'étendre par continuité en une application linéaire $\phi : \mathbf{R}^n \longrightarrow H$ telle que le diagramme suivant commute.

$$\begin{array}{ccc} \mathbf{Q}^n & \xhookrightarrow{\ i\ } & \mathbf{R}^n \\ \downarrow{\scriptstyle \Psi} & & \wr \downarrow{\scriptstyle \phi} \\ K & \xrightarrow{\ \Phi\ } & H \end{array}$$

Or Φ et Ψ sont injectives, donc ϕ est injective, ce qui implique que ϕ est un isomorphisme et sa matrice $\mathcal{M}$ est inversible. On peut donner une expression explicite de $\mathcal{M} = (m_{i,j})_{1\leqslant i,j\leqslant n}$: pour tout $1 \leqslant j \leqslant n$,

$$m_{i,j} = \begin{cases} \sigma_i(z_j) & \text{si } 1 \leqslant i \leqslant r_1, \\ \mathrm{Re}\left(\sigma_i(z_j)\right) & \text{si } r_1 < i \leqslant r_1 + r_2, \\ \mathrm{Im}\left(\sigma_{i-r_2}(z_j)\right) & \text{si } r_1 + r_2 < i \leqslant n. \end{cases} \tag{II.2}$$

De plus Ψ identifie $\mathbf{Z}^n$ et $\mathbf{Z}_K$, donc le réseau $\mathcal{M}\mathbf{Z}^n$ de H est utilisé pour décrire les entiers de K.

Tous les calculs sont effectués dans $H/\mathcal{M}\mathbf{Z}^n$. On identifie le domaine fondamental de $\mathcal{M}\mathbf{Z}^n$ avec $\mathcal{F} = \mathcal{M}[0,1[^n$. On recouvre $\mathcal{F}$ et on le découpe en parallélotopes. Les faces des parallélotopes sont orthogonales aux axes de H. Un découpage différent a été utilisé dans [CL98] pour étudier les corps de nombres cubiques. Celui qu'on utilise ici semble donner de meilleurs résultats car il permet d'utiliser un test optimal (voir remarque 3.8).

En pratique, on applique une réduction LLL (voir [Coh96, paragraphe 2.6]) à $\mathcal{M}$ pour contrôler la taille des coefficients de $\mathcal{M}$ et $\mathcal{M}^{-1}$ (voir paragraphe 6.1.1).

On montre des exemples de découpage et de recouvrement dans les cas quadratiques réel et imaginaire dans la figure II.1. On ne conserve bien sûr que les parallélotopes qui intersectent le domaine fondamental. L'algorithme 3.2 résume les données obtenues ainsi que les étapes de cette procédure.

Remarque 3.6. Pour effectuer des calculs dans H, on utilise des nombres réels flottants et il est nécessaire de connaître une approximation de $\mathcal{M}$.

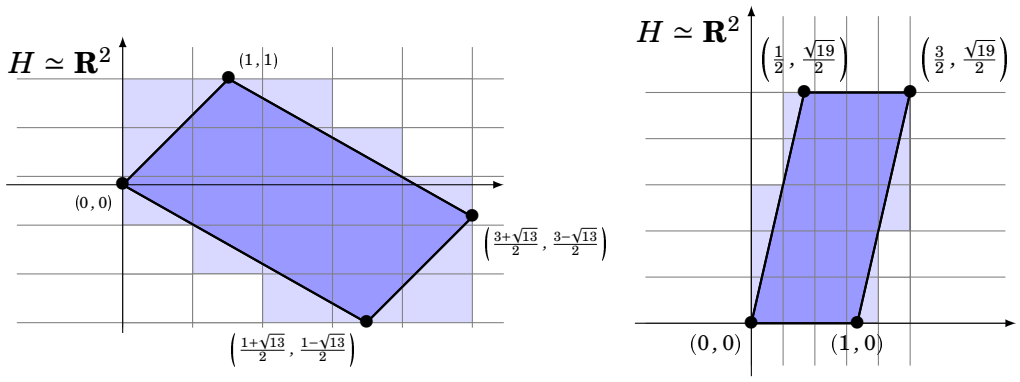


FIGURE II.1 – Exemples de découpage et de recouvrement du domaine fondamental : $K = \mathbf{Q}(\sqrt{13})$ et $K = \mathbf{Q}(\sqrt{-19})$.

Algorithme 3.2 Initialisation des données

ENTRÉE : un corps de nombres K de degré n, un n-uplet $(N_i)_{1 \leqslant i \leqslant n}$ d'entiers, l : le nombre d'unités utilisées ensuite

SORTIE : matrice $\mathcal{M}$, l'image par $\mathbf{\Phi}$ de l unités, une liste de parallélotopes qui recouvrent le domaine fondamental $\mathcal{F}$

1: $\mathcal{T} \leftarrow \varnothing$, calcul de la matrice $\mathcal{M}$ (II.2)
2: réduction LLL de $\mathcal{M}$
3: calcul des plongements de l unités $\mathfrak{E} = \{\upsilon_1, \cdots, \upsilon_l\}$
4: dans chaque direction i, découpage de $[a_i, b_i]$ (voir (II.3) pour la définition précise, $\mathcal{F} \subseteq \prod_{l=1}^{n} [a_l, b_l]$) en N_l segments (de même longueur) $[c_i, d_i]$
5: **pour** tout $\mathcal{P} = \prod_{i=1}^{n} [c_i, d_i]$ **faire**
6: **si** $\mathcal{P} \cap \mathcal{F} \neq \varnothing$ (voir lemme 4.3) **alors**
7: $\mathcal{T} \leftarrow \mathcal{T} \cup \{\mathcal{P}\}$
8: **fin si**
9: **fin pour**
10: **renvoyer** $\mathcal{M}$, $\mathfrak{E}$, $\mathcal{T}$

3.2.2 Condition d'absorption

On choisit $k > 0$ et on rappelle que le but est de savoir quels points x de H vérifient $m_{\overline{K}}(x) < k$. Pour ce faire, on utilise le découpage décrit dans le paragraphe 3.2.1. Pour chaque parallélotope $\mathcal{P}$, on veut savoir s'il existe $z \in \mathbf{\Phi}(\mathbf{Z}_K)$ tel que pour tout $x \in \mathcal{P}$, $\mathcal{N}(x - z) < k$. En ce cas, on dit que $\mathcal{P}$ est absorbé par z.

Chaque entier définit un domaine ouvert dans lequel tous les points x ont un minimum inhomogène strictement plus petit que k. Dans le cas quadratique réel, ces domaines sont hyperboliques, dans le cas quadratique imaginaire, ce sont des disques, voir figure II.2.

Un parallélotope $\mathcal{P}$ est déterminé par son *centre* $c = (c_1, \ldots, c_n)$ et son *pas* $h = (h_1, \ldots, h_n) \in (\mathbf{R}_+)^n$:

$$\mathcal{P} = \{(x_1, \ldots, x_n) \in H, \text{ pour tout } 1 \leqslant i \leqslant n, \ |c_i - x_i| \leqslant h_i\}.$$

Dans l'algorithme 3.2, on prend pour pas $h_i = \frac{b_i - a_i}{2N_i}$.

Proposition 3.7. *Soit $\mathcal{P}$ un parallélotope de centre $c = (c_1, \dots, c_n)$ et de pas $h = (h_1, \dots, h_n)$. Alors $\mathcal{P}$ est absorbé par $z = (z_1, \dots, z_n) \in \mathbf{\Phi}(\mathbf{Z}_K)$ si*

$$\prod_{i=1}^{r_1} (|c_i - z_i| + h_i) \cdot \prod_{i=r_1+1}^{r_1+r_2} \left((|c_i - z_i| + h_i)^2 + (|c_{i+r_2} - z_{i+r_2}| + h_{i+r_2})^2 \right) < k.$$

Démonstration. Soit $x = (x_1, \dots, x_n)$ un point de $\mathcal{P}$. Pour tout $1 \leqslant i \leqslant r_1$, l'inégalité triangulaire implique $|x_i - z_i| \leqslant |c_i - z_i| + h_i$. D'autre part, pour tout $r_1 < i \leqslant r_1 + r_2$, on a

$$(x_i - z_i)^2 + (x_{i+r_2} - z_{i+r_2})^2 \leqslant (|x_i - z_i| + h_i)^2 + (|x_{i+r_2} - z_{i+r_2}| + h_{i+r_2})^2 .$$

Par conséquent, si la condition de la proposition 3.7 est vraie, alors le point x est absorbé par z. □

Remarque 3.8. La condition de la proposition 3.7 est optimale. En effet, il s'agit exactement du test $\mathcal{N}(x - z) < k$ où x est un sommet du parallélotope $\mathcal{P}$.

On choisit une liste fixée d'entiers $\mathcal{L}$ et on applique le test de la proposition 3.7 pour tous les parallélotopes et tous les éléments de $\mathcal{L}$. Tous les parallélotopes qui ne sont pas absorbés sont dits *problématiques*. L'algorithme 3.3 teste si un parallélotope $\mathcal{P}$ peut être absorbé par $\mathcal{L}$.

Algorithme 3.3 Test d'absorption

ENTRÉE : un parallélotope $\mathcal{P}$ de centre c et de pas h, une liste finie $\mathcal{L} \subseteq \mathbf{\Phi}(\mathbf{Z}_K)$, $k \in \mathbf{R}_+^*$.
SORTIE : si $\mathcal{P}$ peut être absorbé pour k par un élément de $\mathcal{L}$.

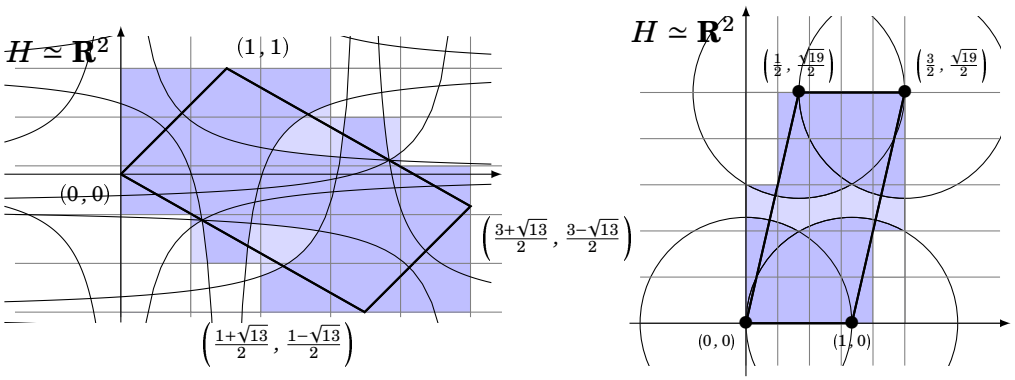
1: **pour** chaque élément $z \in \mathcal{L}$ **faire**
2: $\quad m \leftarrow \prod_{i=1}^{r_1} (|c_i - z_i| + h_i) \cdot \prod_{i=r_1+1}^{r_1+r_2} \left((|c_i - z_i| + h_i)^2 + (|c_{i+r_2} - z_{i+r_2}| + h_{i+r_2})^2 \right)$
3: $\quad$ **si** $m < k$ **alors**
4: $\quad\quad$ **renvoyer vrai**
5: $\quad$ **fin si**
6: **fin pour**
7: **renvoyer faux**

3.2.3 Choix des entiers

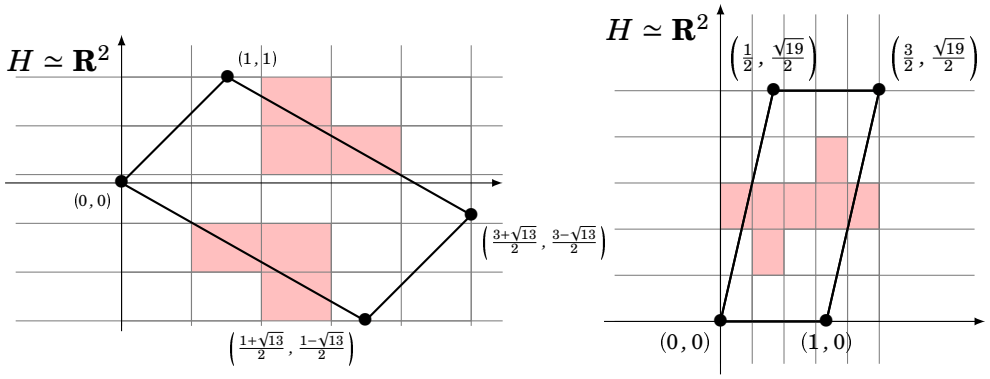
Il faut décider quels entiers vont être utilisés pour absorber les parallélotopes. On choisit un entier naturel $B > 0$ et on calcule $\mathcal{M}x$ pour tout vecteur $x \in \mathbf{Z}^n$ tel que $\|x\|_\infty \leqslant B$. Idéalement, B doit être choisi tel qu'il ne soit pas trop petit car nous voulons absorber autant de parallélotopes que possible, mais aussi pas trop grand, parce que nous testons l'absorption par *tous* ces éléments pour un parallélotope $\mathcal{P}$ qui ne peut pas être absorbé.

Néanmoins, on peut facilement déterminer à l'avance que certains éléments $\mathcal{M}x$ sont inutiles pour l'absorption de parallélotopes. Avec la notation $\mathcal{M} = (m_{i,j})_{1 \leqslant i,j \leqslant n}$, on pose pour tout $i \in \{1, \dots, n\}$,

$$a_i = \sum_{\substack{j=1 \\ m_{i,j} \leqslant 0}}^{n} m_{i,j} \qquad \text{et} \qquad b_i = \sum_{\substack{j=1 \\ m_{i,j} > 0}}^{n} m_{i,j}\,, \tag{II.3}$$



(a) Domaines absorbés par des entiers. Dans les deux cas, on utilise les quatre entiers qui correspondent aux sommets de $\mathcal{F}$, mais on peut aussi utiliser d'autres entiers, particulièrement dans le cas réel.



(b) Parallélotopes problématiques restants, seul les parallélotopes totalement recouverts sont éliminés.

FIGURE II.2 – Absorption de parallélotopes par des entiers, $K = \mathbf{Q}(\sqrt{13})$ et $K = \mathbf{Q}(\sqrt{-19})$ pour $k = \frac{1}{3}$ et $k = 1$ respectivement. Le choix des entiers est crucial, par exemple, dans le premier cas, on pourrait absorber plus de parallélotopes en utilisant plus d'entiers.

de sorte que $\mathcal{F} \subseteq [a_1, b_1] \times \cdots \times [a_n, b_n]$. De plus si pour $X = (X_i)_{1 \leqslant i \leqslant n} \in \Phi(\mathbf{Z}_K)$ et $x \in \mathcal{F}$, on a $\mathcal{N}(x - X) < k$, alors il existe un entier $i \in \{1, \ldots, r_1 + r_2\}$ tel que

$$\begin{cases} \text{ou bien } 1 \leqslant i \leqslant r_1 \text{ et } X_i \in \left]a_i - k^{\frac{1}{n}}, b_i + k^{\frac{1}{n}}\right[, \\ \text{ou bien } r_1 < i \leqslant r_1 + r_2 \text{ et } \begin{cases} X_i \in \left]a_i - k^{\frac{1}{n}}, b_i + k^{\frac{1}{n}}\right[, \\ X_{i+r_2} \in \left]a_{i+r_2} - k^{\frac{1}{n}}, b_{i+r_2} + k^{\frac{1}{n}}\right[\end{cases} . \end{cases} \tag{II.4}$$

Ces estimations peuvent sembler très brutales, mais elles se révèlent très utiles en pratique. On les applique dans l'algorithme 3.4.

3.3 Actions des unités $\mathbf{Z}_K^\times$ sur K

3.3.1 Idées générales

On cherche à absorber des parallélotopes a priori problématiques sans utiliser plus d'entiers. On choisit une unité ε et on écrit $\nu = (\nu_i)_{1 \leqslant i \leqslant n} = \Phi(\varepsilon)$. En pratique,

Algorithme 3.4 Calcul de la liste d'entiers

ENTRÉE : la matrice $\mathcal{M}$, une borne B
SORTIE : une liste d'éléments $\mathbf{\Phi}(\mathbf{Z}_K)$ susceptibles d'absorber des parallélotopes

1: $\mathcal{L} \leftarrow \varnothing$
2: **pour** chaque vecteur $Z \in \mathbf{Z}^n$ tel que $-B \leqslant Z_i \leqslant B$ **faire**
3: calculer $X = \mathcal{M}Z^n$
4: **si** la condition (II.4) est vérifiée **alors**
5: $\mathcal{L} \leftarrow \mathcal{L} \cup \{X\}$
6: **fin si**
7: **fin pour**
8: **renvoyer** $\mathcal{L}$

on travaille directement avec ν, qui est un des plongements d'unités précalculés dans $\mathfrak{E}$ par l'algorithme 3.2. On suppose que l'on a un découpage du domaine fondamental $\mathcal{F}$ en parallélotopes. Certains d'entre eux sont absorbés par des entiers, mais ce n'est pas le cas pour tous. On considère un parallélotope problématique $\mathcal{P}$ et son image sous l'action de ν :

$$\nu \cdot \mathcal{P} = \{\nu \cdot x,\ x \in \mathcal{P}\}.$$

On note c le centre de $\mathcal{P}$ et h son pas.

Lemme 3.9. *Soit $c' = \nu \cdot c = (c'_i)_{1\leqslant i\leqslant n}$, alors $\nu \cdot \mathcal{P}$ est contenu dans le domaine suivant*

$$\mathcal{B} = \left\{(x_i)_{1\leqslant i\leqslant n} \in H, \quad \left\{ \begin{array}{l} \text{pour } 1 \leqslant i \leqslant r_1, |x_i - c'_i| \leqslant h'_i \\ \text{pour } r_1 < i \leqslant r_1 + r_2, (x_i - c'_i)^2 + (x_{i+r_2} - c'_{i+r_2})^2 \leqslant {h'_i}^2 \end{array} \right\},$$

où le n-uplet $h' = (h'_i)_{1\leqslant i\leqslant n}$ est défini par

$$h'_i = \left\{ \begin{array}{ll} h_i\,|\nu_i| & \text{si } 1 \leqslant i \leqslant r_1, \\ \sqrt{(\nu_i^2 + \nu_{i+r_2}^2)(h_i^2 + h_{i+r_2}^2)} & \text{si } r_1 < i \leqslant r_1 + r_2, \\ h'_{i-r_2} & \text{si } r_1 + r_2 < i \leqslant n. \end{array} \right.$$

Démonstration. Il s'agit d'une vérification facile. □

On veut savoir si pour tout $x \in \mathcal{P}$, il existe un certain $z_x \in \mathbf{\Phi}(\mathbf{Z}_K)$ tel que $m_{\overline{K}}(\nu \cdot x - z_x) < k$. Si on peut trouver de tels éléments z_x, alors on peut éliminer $\mathcal{P}$, car pour tout $x \in \mathcal{P}$,

$$m_{\overline{K}}(x) = m_{\overline{K}}(\nu \cdot x - z_x).$$

Cependant, on ne veut pas calculer à nouveau de nombreuses normes pour une immense liste d'éléments $z \in \mathbf{\Phi}(\mathbf{Z}_K)$. À la place, on se ramène au domaine fondamental en translatant $\mathcal{B}$.

On suppose que $\{\mathcal{Q}_j,\ 1 \leqslant k \leqslant l\}$ est un recouvrement de $\mathcal{F}$ tel que pour tout $1 \leqslant j \leqslant l$, $\mathcal{Q}_i$ est un parallélotope de centre $c^{(j)}$ et de pas $h^{(j)}$. On suppose qu'il existe un entier $1 \leqslant m \leqslant l$ tel que tous les parallélotopes $\mathcal{Q}_j$ pour $m < j \leqslant l$ sont absorbés par des entiers.

Définition 3.10. On dit que $z \in \mathbf{\Phi}(\mathbf{Z}_K)$ est un *vecteur de translation* de $\mathcal{B}$ dans $\mathcal{F}$ si on a $(\mathcal{B} - z) \cap \mathcal{F} \neq \varnothing$.

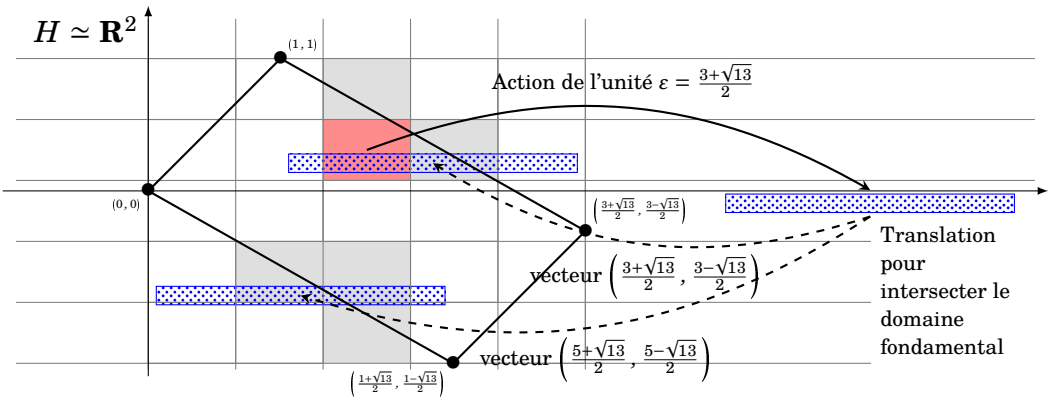


FIGURE II.3 – Action de l'unité $\frac{3+\sqrt{13}}{2}$ sur un parallélotope problématique. Les deux translatés de l'image dans le domaine fondamental intersectent des parallélotopes problématiques. On conserve donc ce problème.

Lemme 3.11. *Soit* $\{z^{(l)},\ 1 \leqslant l \leqslant k\} \subseteq \Phi(\mathbf{Z}_K)$ *la liste de tous les vecteurs de translation possibles de* $\mathcal{B}$ *dans* $\mathcal{F}$. *Si pour tous* $1 \leqslant l \leqslant k$, $1 \leqslant j \leqslant m$, $\left(\mathcal{B} - z^{(l)}\right) \cap \mathcal{Q}_j = \varnothing$, *alors* $\mathcal{P}$ *peut être éliminé de la liste des parallélotopes problématiques.*

La démonstration de ce lemme est très facile, mais insistons sur le fait qu'il faut considérer *tous* les vecteurs de translation. En effet, un translaté de $\mathcal{B}$ qui intersecte le domaine fondamental n'est pas nécessairement inclus dans le domaine fondamental. La figure II.3 montre un exemple de l'action d'une unité dans le cas quadratique réel : deux vecteurs de translation sont possibles dans ce cas. Les deux translatés intersectent le domaine fondamental.

Ainsi, nous sommes amenés à calculer tous les vecteurs de translation de $\mathcal{B}$ dans le domaine fondamental $\mathcal{F}$.

3.3.2 Translations dans le domaine fondamental

Rappelons que l'on note $\mathcal{M} = (m_{i,j})_{1\leqslant i,j\leqslant n}$ et définissons $(a_i)_{1\leqslant i\leqslant n}$ et $(b_i)_{1\leqslant i\leqslant n}$ comme dans le paragraphe 3.2.3. Avec ces notations, $\mathcal{F} \subseteq [a_1, b_1] \times \cdots \times [a_n, b_n]$. Par conséquent, si $(\mathcal{B} - z) \cap \mathcal{F} \neq \varnothing$, alors pour tout $1 \leqslant i \leqslant n$,

$$\left(\left[c'_i - h'_i, c'_i + h'_i\right] - z_i\right) \cap [a_i, b_i] \neq \varnothing,$$

avec les notations du lemme 3.9. Dès lors, on obtient le critère suivant.

Lemme 3.12. *Soit* $z \in H$ *un vecteur de translation de* $\mathcal{B}$ *dans* $\mathcal{F}$. *Alors*
- *il existe* $Z \in \mathbf{Z}^n$ *tel que* $z = \mathcal{M}Z$,
- *pour tout* $1 \leqslant i \leqslant n$, *on a* $c'_i - b_i - h'_i \leqslant z_i \leqslant c'_i - a_i + h'_i$.

Cela fournit une technique pour calculer tous les vecteurs de translation potentiels. À présent, étant donné un tel vecteur z, on a besoin d'un critère pour décider si $\mathcal{B} - z$ intersecte le parallélotope problématique $\mathcal{Q}_j$, de centre $c^{(j)}$ et de pas $h^{(j)}$.

Lemme 3.13. *Si* $(\mathcal{B}-z)\cap\mathcal{Q}_j\neq\varnothing$, *alors pour tout* $1\leqslant i\leqslant n$,

$$c'_i - c_i^{(j)} - h_i^{(j)} - h'_i \leqslant z_i \leqslant c'_i - c_i^{(j)} + h_i^{(j)} + h'_i. \tag{II.5}$$

Démonstration. C'est une conséquence immédiate du fait que pour tout $x\in\mathcal{B}$, pour tout $1\leqslant i\leqslant n$, $|x_i - c'_i|\leqslant h'_i$. □

Notons que le lemme 3.12 peut fournir un ensemble de vecteurs qui contient strictement l'ensemble des vecteurs de translation. Cependant, même si on utilise trop de vecteurs, on ne peut éliminer que des parallélotopes qui sont non problématiques.

Algorithme 3.5 Action d'une unité pour éliminer des parallélotopes

ENTRÉE : une liste de parallélotopes problématiques $\mathcal{T}$, un plongement d'une unité $v\in\mathfrak{E}\subseteq\Phi(\mathbf{Z}_K^\times)$

SORTIE : une liste de parallélotopes problématiques $\mathcal{T}'\subseteq\mathcal{T}$

$\mathcal{T}'\leftarrow\varnothing$, $\mathcal{T}_0\leftarrow\mathcal{T}$
tant que $\#\mathcal{T}'<\#\mathcal{T}_0$ **faire**
  pour chaque $\mathcal{P}\in\mathcal{T}_0$ **faire**
    calculer l'image $\mathcal{B}$ de $\mathcal{P}$ sous l'action de v et une liste $\mathcal{V}$ de tous les vecteurs de translation possibles de $\mathcal{B}$ dans $\mathcal{F}$
    pour chaque $v\in\mathcal{V}$ **faire**
      si un parallélotope $\mathcal{Q}_j\in\mathcal{T}_0$ est tel que pour tout $1\leqslant i\leqslant n$ (II.5) est vraie **alors**
        $\mathcal{T}'\leftarrow\mathcal{T}'\cup\{\mathcal{P}\}$
      fin si
    fin pour
  fin pour
  si $\#\mathcal{T}'<\#\mathcal{T}_0$ **alors**
    $\mathcal{T}_0\leftarrow\mathcal{T}'$, $\mathcal{T}'\leftarrow\varnothing$
  fin si
fin tant que
renvoyer $\mathcal{T}'$

Proposition 3.14. *L'algorithme 3.5 renvoie une liste de parallélotopes* $\mathcal{T}'$ *telle que pour tout* $x\in\mathcal{F}$ *vérifiant* $m_{\overline{K}}(x)\geqslant k$, *il existe* $\mathcal{P}'\in\mathcal{T}'$ *tel que* $x\in\mathcal{P}'$.

Démonstration. C'est une conséquence facile du lemme 3.13. □

On peut répéter cette procédure pour tout élément de l'ensemble $\mathfrak{E}$ qui avait été calculé par l'algorithme 3.2 et appliquer ces tests jusqu'à ce que plus aucun parallélotope problématique ne soit éliminé.

Le test d'absorption et le test des unités nous permettent de prouver avec un ordinateur que $M(\overline{K})<k$ pour une certaine valeur de k. Toutefois, on aimerait pouvoir calculer $M(K)$ exactement. Pour y parvenir, on va utiliser une valeur de k pour laquelle tous les parallélotopes ne sont pas absorbés.

3.4 Parallélotopes problématiques et minimum euclidien

À cette étape, on suppose que pour un certain $k > 0$, il reste m parallélotopes problématiques. On les note $\mathcal{Q}_j$ pour $1 \leqslant j \leqslant m$. On choisit une unité ε qui n'est pas une racine de l'unité telle que pour tout $1 \leqslant i \leqslant n$,

$$|\sigma_i(\varepsilon)| \neq 1.$$

3.4.1 Action des unités (suite)

L'action de l'unité ε ne permet pas d'éliminer de parallélotope problématique car pour tout $1 \leqslant ij \leqslant m$, il existe au moins un vecteur de translation $z \in \Phi(\mathbf{Z}_K)$ tel que $(\varepsilon \cdot \mathcal{Q}_j - z) \cap \mathcal{Q}_l$ est possiblement non vide, pour un certain l.

On construit un graphe orienté $\mathcal{G}$, dont les sommets sont les parallélotopes problématiques $(\mathcal{Q}_j)_{1 \leqslant j \leqslant m}$ et dont les arêtes orientées sont

$$\mathcal{Q}_j \xrightarrow{\ z\ } \mathcal{Q}_l$$

si $(\varepsilon \cdot \mathcal{Q}_j - z) \cap \mathcal{Q}_l$ est possiblement non vide pour un certain $z \in \Phi(\mathbf{Z}_K)$.

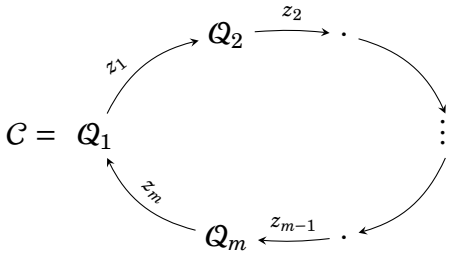
3.4.2 Graphes convenables

Définition 3.15. Un graphe orienté est dit *convenable* si tout chemin infini est ultimement périodique ou, de façon équivalente, si ses cycles simples sont disjoints.

On suppose que l'on peut obtenir un graphe convenable de parallélotopes problématiques. On note $(\mathcal{C}_s)_{1 \leqslant s \leqslant l}$ les cycles simples de $\mathcal{G}$.

À chaque cycle simple $\mathcal{C}$ de $\mathcal{G}$, le théorème suivant va associer un point critique $t_{\mathcal{C}} \in \Phi(K)$ qui a la propriété suivante : pour tout élément x dans les parallélotopes qui correspondent aux sommets de $\mathcal{C}$, $m_{\overline{K}}(x) \leqslant m_{\overline{K}}(t_{\mathcal{C}})$ et $k < m_{\overline{K}}(t_{\mathcal{C}})$. Par conséquent, on va pouvoir calculer le minimum euclidien de K pourvu qu'on parvienne à obtenir un graphe convenable.

Théorème 3.16. *Soit $\mathcal{C}$ un cycle simple de $\mathcal{G}$. On note $\mathcal{Q}_1, \ldots, \mathcal{Q}_m$ les sommets de $\mathcal{C}$ et m éléments $z_1 = \Phi(Z_1), \ldots, z_m = \Phi(Z_m)$ de $\Phi(\mathbf{Z}_K)$ tels que*



(II.6)

Alors, si on définit $\Omega_{\mathcal{C}} = \sum_{j=0}^{m} \varepsilon^j z_{m-j} \in \mathbf{Z}_K$, $\xi_{\mathcal{C}} = \dfrac{\Omega_{\mathcal{C}}}{\varepsilon^m - 1}$ et $t_{\mathcal{C}} = \Phi(\xi_{\mathcal{C}})$, on a pour tout $x \in \mathcal{Q}_1$ tel que $m_{\overline{K}}(x) > k$,

1. *$k < m_{\overline{K}}(x) \leqslant m_{\overline{K}}(t_{\mathcal{C}}) = m_K(\xi_{\mathcal{C}})$,*
2. *si $x \in \Phi(K)$, alors $x = t_{\mathcal{C}}$.*

Démonstration. Il s'agit d'une généralisation assez immédiate de [Cer07, Theorem 4.1], mais nous donnons la preuve pour expliquer la démarche.

Notons $\mathcal{G} := \left\{x \in H,\ m_{\overline{K}}(x) \leqslant k\right\}$ et $\nu := \Phi(\varepsilon)$. On montre tout d'abord que

$$(\nu^m \cdot \mathcal{Q}_1 - \Phi(\Omega_C)) \subseteq \mathcal{Q}_1. \tag{II.7}$$

On pose $q = \nu^m \cdot q_1 - \Phi(\Omega_C)$ pour un certain $q_1 \in \mathcal{Q}_1$. On suppose que $q \notin \mathcal{G}$, c'est-à-dire $m_{\overline{K}}(q) > k$. On peut alors définir $q_2, q_3, \ldots, q_m$ par la formule de récurrence

$$q_{j+1} := \nu \cdot q_j - \Phi(z_j),\ \text{pour } 1 \leqslant j < m.$$

Ainsi, $q_m = q$ et d'après la proposition 2.5 (1), pour tout $j \in \{1, \ldots, m+1\}$,

$$m_{\overline{K}}(q_j) = m_{\overline{K}}(q_1) > k.$$

Dès lors, pour tout $j \in \{1, \ldots, m+1\}$, $q_j \notin \mathcal{G}$ et ainsi, d'après l'hypothèse (II.6), pour tout $j \in \{1, \ldots, m\}$, $q_j \in \mathcal{Q}_j$ et $q = q_{m+1} \in \mathcal{Q}_1$, ce qui prouve (II.7).

On définit alors récursivement la suite $(y_p)_{p\in\mathbf{N}}$ par $y_0 := x$ et pour tout $p \in \mathbf{N}$,

$$y_{p+1} := \nu^m \cdot y_p - \Phi(\Omega_C).$$

On va montrer que

$$\lim_{p\to+\infty} y_p = t_C. \tag{II.8}$$

D'après la proposition 2.5 (1), pour tout $p \in \mathbf{N}$, $m_{\overline{K}}(y_p) = m_{\overline{K}}(x) > k$, donc pour tout $p \in \mathbf{N}$, $y_p \notin \mathcal{G}$. On en déduit par récurrence et en appliquant (II.7) que pour tout $p \in \mathbf{N}$,

$$y_p \in \mathcal{Q}_1.$$

Comme $\mathcal{Q}_1$ est borné, la suite $(y_p - t_C)_{p\in\mathbf{N}}$ est bornée. Or pour tout $p \in \mathbf{N}$, par définition, on a $y_p - t_C = (\nu^m)^p \cdot (x - t_C)$, ce qui implique que pour tous $i \in \{1, \ldots, r_1 + r_2\}$ et $p \in \mathbf{N}$,

$$\begin{cases} \left|(y_p)_i - (t_C)_i\right| = |\sigma_i(\varepsilon)|^{mp} \cdot |x_i - (t_C)_i|\,. \text{ si } i \leqslant r_1, \text{ et sinon,} \\ ((y_p)_i - (t_C)_i)^2 + ((y_p)_{i+r_2} - (t_C)_{i+r_2})^2 = |\sigma_i(\varepsilon)|^{2mp} \cdot (x_i - (t_C)_i)^2 + (x_i - (t_C)_i)^2. \end{cases} \tag{II.9}$$

Rappelons que, par hypothèse, $|\sigma_i(\varepsilon)| \neq 1$ pour tout $i \in \{1, \ldots, r_1 + r_2\}$. Fixons $i \in \{1, \ldots, n\}$. Si $|\sigma_i(\varepsilon)| < 1$, alors, d'après (II.9), si $i \leqslant r_1$, alors

$$\lim_{p\to+\infty} (y_p)_i = (t_C)_i$$

et si $i > r_1$,

$$\lim_{p\to+\infty} (y_p)_i = (t_C)_i\,, \qquad \lim_{p\to+\infty} (y_p)_{i+r_2} = (t_C)_{i+r_2}.$$

Si $|\sigma_i(\varepsilon)| > 1$, alors comme la suite $(y_p - t_C)_{p\in\mathbf{N}}$ est bornée, (II.9) implique que $x_i = (t_C)_i$ et on a donc pour tout $p \in \mathbf{N}$,

$$(y_p)_i = (t_C)_i.$$

Cela montre que (II.8) est vraie.

Par semi-continuité supérieure de $m_{\overline{K}}$, on en déduit que $\limsup_{p\to+\infty} m_{\overline{K}}(y_p) \leqslant m_{\overline{K}}(t_C)$. Ainsi, on obtient le premier point, c'est-à-dire :

$$k < m_{\overline{K}}(x) = \limsup_{p\to+\infty} m_{\overline{K}}(y_p) \leqslant m_{\overline{K}}(t_C).$$

Si on suppose en outre que $x \in \Phi(K)$, il existe un indice $i \in \{1, \dots, r_1\}$ tel que $x_i = (t_C)_i$ ou $i \in \{r_1+1, \dots, r_1+r_2\}$ tel que $x_i = (t_C)_i$ et $x_{i+r_2} = (t_C)_{i+r_2}$. En effet, comme $\prod_{i=1}^{r_1} |\sigma_i(\varepsilon)| \cdot \prod_{i=r_1}^{r_1+r_2} |\sigma_i(\varepsilon)|^2 = 1$, il existe $i \in \{1, \dots, r_1+r_2\}$ tel que

$$|\sigma_i(\varepsilon)| \geqslant 1.$$

Par hypothèse sur ε, cela implique qu'on a même $|\sigma_i(\varepsilon)| > 1$. D'après ce qui précède cela donne

$$\begin{cases} x_i = (t_C)_i & \text{si } i \leqslant r_1, \\ x_i = (t_C)_i \text{ et } x_{i+r_2} = (t_C)_{i+r_2} & \text{si } r_1 < i. \end{cases}$$

Par conséquent, $\sigma_i(x) = \sigma_i(t_C)$. Par injectivité de σ_i, on en déduit que

$$x = t_C.$$

□

Algorithme 3.6 Calcul du minimum associé à un cycle

ENTRÉE : un cycle simple C, une unité ε
SORTIE : une orbite de points $\mathcal{O} \subseteq K$, $m_K(x)$ (pour tout $x \in \mathcal{O}$)
1: calculer ξ_C (voir théorème 3.16), $\mathcal{O} \leftarrow \mathrm{Orb}(\xi_C)$ (voir paragraphe 4.3.2)
2: calculer $m_K(\xi_C)$ avec l'algorithme 3.1
3: **renvoyer** $\mathcal{O}, m_K(\xi_C)$

Théorème 3.17. *On suppose que le graphe $\mathcal{G}$ est convenable. Si $t \in K$ vérifie $m_K(t) > k$, alors il existe un cycle simple C de $\mathcal{G}$ et $\nu \in \mathbf{Z}_K^\times$ tels que $t \equiv \nu \cdot \xi_C \pmod{\mathbf{Z}_K}$.*

Démonstration. Il s'agit d'une extension de [Cer07, Theorem 4.5], écrit dans le cas plus général des corps de nombres de signature quelconque.

On pose $x = \Phi(t) \in \Phi(K)$. Comme $m_{\overline{K}}(x) > k$, il existe une unité μ et un sommet $\mathcal{Q}$ de $\mathcal{G}$ tel que $\Phi(\mu) \cdot x$ appartient à $\mathcal{Q}$ modulo $\Phi(\mathbf{Z}_K)$. On note $x_0 = \Phi(\mu) \cdot x$ et $\mathcal{Q}_0 = \mathcal{Q}$. On peut définir par récurrence deux suites $(x_i)_{i\in\mathbf{N}}$ et $(\mathcal{Q}_i)_{i\in\mathbf{N}}$ en notant que pour tout $i \in \mathbf{N}$, comme $m_{\overline{K}}(\varepsilon \cdot x_i) = m_{\overline{K}}(x_i) = m_{\overline{K}}(x_0) > k$, il existe un sommet $\mathcal{Q}_{i+\infty}$ de $\mathcal{G}$ tel que $\Phi(\varepsilon) \cdot x_i$ appartiennent à $\mathcal{Q}_{i+1}$ modulo $\Phi(\mathbf{Z}_K)$. On prend $x_{i+1} \in \mathcal{Q}_{i+1}$ tel que

$$x_{i+1} \equiv \Phi(\varepsilon) \cdot x_i \pmod{\Phi(\mathbf{Z}_K)}.$$

Cela fournit un chemin infini dans $\mathcal{G}$ passant par les sommets $(\mathcal{Q}_i)_{i\in\mathbf{N}}$.

Or $\mathcal{G}$ est convenable, donc le chemin $(\mathcal{Q}_i)_{i\in\mathbf{N}}$ est ultimement périodique. On considère donc une période de ce chemin qui est un cycle simple :

$$\mathcal{Q}_r \longrightarrow \mathcal{Q}_{r+1} \longrightarrow \dots \longrightarrow \mathcal{Q}_{r+s-1} \longrightarrow \mathcal{Q}_r.$$

On a donc un cycle simple $(\mathcal{Q}_{r+l})_{0\leqslant l<s}$ et un point $x_r \in \mathcal{Q}_r$ tel que $m_{\overline{K}}(x_r) > k$. On peut donc appliquer le théorème 3.16, ce théorème définit explicitement un point $t_C = \Phi(\xi_C) \in \Phi(K)$ tel que $x_r = t_C$. Or, par définition de x_r,

$$x_r \equiv \Phi(\varepsilon^r \cdot \mu) \cdot x \pmod{\Phi(\mathbf{Z}_K)}.$$

Donc, en posant $\nu = (\varepsilon^r \cdot \mu)^{-1} \in \mathbf{Z}_K^\times$, on a

$$x \equiv \Phi(\nu) \cdot t_C \pmod{\Phi(\mathbf{Z}_K)}.$$

Par conséquent, $t \equiv \nu \cdot \xi_C \pmod{\mathbf{Z}_K}$, ce qui achève la preuve. □

Remarques 3.18. – L'hypothèse « ε n'est pas une racine de l'unité » est cruciale, mais il ne s'agit pas d'une limitation dès que le rang des unités r est strictement positif (et le cas $r = 0$ est facile).
– Si l'algorithme parvient à construire un graphe convenable, il va fournir tous les points $\xi \in K$ tels que $M(K) = m_K(\xi)$ (modulo $\mathbf{Z}_K$).
– En fait, si on applique l'algorithme avec la valeur k et si le graphe obtenu est convenable, le théorème 3.17 nous permet de trouver tous les éléments $x \in K$ (modulo $\mathbf{Z}_K$) tels que $m_K(x) > k$.
– Dans les exemples considérés, on trouve toujours un découpage initial pour lequel le graphe obtenu est convenable.
– Le fait que l'on considère des parallélotopes n'a aucune importance. Par conséquent, on peut fusionner des parallélotopes pour obtenir un graphe convenable. Nous verrons comment procéder en pratique au paragraphe 4.3.

4 Description de l'algorithme

4.1 Algorithme général

On décrit ici une procédure générale pour calculer le minimum euclidien d'un corps de nombres K. À chaque étape, on considère trois nombres réels k_0, k_1 et k ayant les propriétés suivantes :

1. $k_0 < k < k_1$,
2. $M(K) < k_1$,
3. probablement, $k_0 < M(K)$.

Initialement, on choisit $k_0 < \frac{1}{\Lambda(K)}$ de sorte que $k_0 < M(K)$ et $k_1 > M(K)$. Ensuite, on applique les tests d'absorption et des unités pour un certain k vérifiant $k_0 < k < k_1$. Si ces tests éliminent tous les problèmes, alors $M(K) < k$ et on peut recommencer avec $k_1 = k$. Sinon, on ne peut pas être sûr que $k < M(K)$. Néanmoins, on cherche à former un graphe convenable. Si cela échoue, on répète les tests avec $k_0 = k$ (ainsi, on sait que *probablement* $k_0 < M(K)$, mais ce n'est pas sûr).

Cette procédure requiert une valeur initiale $\mathcal{K}$ pour k. Comme le test d'absorption (algorithme 3.3) peut avoir une exécution très longue si de nombreux parallélotopes problématiques subsistent, on choisit une « grande » valeur pour $\mathcal{K}$.

Après cette étape, on fixe une valeur de k entre k_0 et k_1. En pratique, on choisit $d \in]0, 1[$ et on prend $k = (1-d)k_0 + dk_1$. De nouveau, on ne veut pas que k décroisse trop rapidement, donc on choisit d plus proche de 1 (par exemple $d = \frac{2}{3}$). Le minimum euclidien peut être égal à $\frac{1}{\Lambda(K)}$. En ce cas, on doit appliquer la procédure pour $k < \frac{1}{\Lambda(K)}$ pour le prouver. C'est pourquoi on choisit une valeur initiale $k_0 < \frac{1}{\Lambda(K)}$.

Ensuite, on détermine une liste $\mathcal{T}$ de parallélotopes problématiques et on itère la boucle suivante :
– remplacer $\mathcal{T}$ par la liste des parallélotopes obtenue en découpant chaque parallélotope $\mathcal{T}$ en deux dans chaque direction,
– essayer de réduire $\mathcal{T}$ par le test d'absorption,
– essayer de réduire $\mathcal{T}$ avec le test des unités.

On décide de stopper l'exécution de cette boucle ainsi : on fixe un entier I et on s'assure qu'on applique au plus I découpages consécutifs sans améliorer le plus petit nombre

Algorithme 4.1 Algorithme général de calcul du minimum euclidien

ENTRÉE : un polynôme irréductible $p \in \mathbf{Z}[X]$ (définissant le corps de nombres K)
SORTIE : $M(K)$ ou échec

1: initialisation des données → matrice $\mathcal{M}$, liste de parallélotopes $\mathcal{T}$, liste de plongements d'unités $\mathfrak{E} = \{\upsilon_1, \ldots, \upsilon_l\}$ (algorithme 3.2)
2: calcul d'une liste d'entiers $\mathcal{L}$ (algorithme 3.4)
3: $k_0 \leftarrow \mathtt{0.9} \cdot \frac{1}{\Lambda(K)}$, $k \leftarrow \mathcal{K}$, $k_1 \leftarrow \infty$, $i \leftarrow 0$,
4: **pour** chaque unité $\nu \in \mathfrak{E}$ **faire**
5: $\quad \mathcal{T} \leftarrow$ action de l'unité ν sur $\mathcal{T}$ (algorithme 3.5)
6: **fin pour**
7: $\mathcal{T}_{\min} \leftarrow \mathcal{T}$
8: **répéter**
9: $\quad \mathcal{T} \leftarrow$ liste obtenue en découpant chaque $\mathcal{P} \in \mathcal{T}$ en deux dans chaque direction $1 \leqslant i \leqslant n$
10: $\quad$ **pour** chaque parallélotope $\mathcal{P} \in \mathcal{T}$ **faire**
11: $\quad\quad$ **si** $\mathcal{P}$ peut être absorbé pour k par $\mathcal{L}$ (algorithme 3.3) **alors**
12: $\quad\quad\quad \mathcal{T} \leftarrow \mathcal{T} \setminus \mathcal{P}$ (algorithme 3.5)
13: $\quad\quad$ **fin si**
14: $\quad$ **fin pour**
15: $\quad$ **pour** chaque unité $\nu \in \mathfrak{E}$ **faire**
16: $\quad\quad \mathcal{T} \leftarrow$ action de l'unité ν sur $\mathcal{T}$ (algorithme 3.5)
17: $\quad$ **fin pour**
18: $\quad$ **si** $\#\mathcal{T}_{\min} < \#\mathcal{T}$ **alors**
19: $\quad\quad i \leftarrow i + 1$
20: $\quad$ **sinon**
21: $\quad\quad \mathcal{T}_{\min} \leftarrow \mathcal{T}$
22: $\quad$ **fin si**
23: **jusqu'à** $\mathcal{T} = \varnothing$ **ou** $i > I$
24: **si** $\mathcal{T} = \varnothing$ **alors**
25: $\quad k_1 \leftarrow k$, $k \leftarrow (1-d) \cdot k_0 + d \cdot k$, $i \leftarrow 0$, $\mathcal{T}_{\min} \leftarrow \mathcal{T}$, **aller à** la ligne 8
26: **fin si**
27: choisir $\nu \in \mathcal{E}$ et calculer le graphe $\mathcal{G}$ associé à l'action de ν sur $\mathcal{T}_{\min}$
28: **si** $\mathcal{G}$ est convenable **alors**
29: $\quad$ **pour** tout cycle simple $\mathcal{C}$ de $\mathcal{G}$ **faire**
30: $\quad\quad$ calculer l'orbite $\mathcal{O}_{\mathcal{C}}$ et le minimum $m_{\mathcal{C}}$ (algorithme 3.6)
31: $\quad$ **fin pour**
32: $\quad m \leftarrow \max_{\mathcal{C}} m_{\mathcal{C}}$
33: $\quad$ **si** $m > k$ **alors**
34: $\quad\quad$ **renvoyer** m et les orbites associées
35: $\quad$ **sinon**
36: $\quad\quad k \leftarrow m - \eta$, **aller à** la ligne 8
37: $\quad$ **fin si**
38: **sinon**
39: $\quad$ **si** $k_1 - k_0 < \epsilon$ **alors**
40: $\quad\quad$ **renvoyer** échec
41: $\quad$ **sinon**
42: $\quad\quad k_0 \leftarrow k$, $k \leftarrow \min\left\{\frac{k+k_1}{2}, k+2\right\}$, $i \leftarrow 0$, **aller à** la ligne 8
43: $\quad$ **fin si**
44: **fin si**

de parallélotopes problématiques trouvés à la fin de la boucle. En pratique, on prend $I = 5$.

Par la suite, on essaie de construire un graphe convenable avec la plus petite liste de parallélotopes problématiques trouvée. Si on y parvient pour la valeur k, on peut utiliser la borne supérieure k_1 de $M(K)$ pour calculer le minimum euclidien local des points associés aux cycles simples. Si la plus grande valeur obtenue est strictement supérieure à k, alors c'est $M(K)$. Dans le cas contraire, on recommence avec $k = m - \eta$ pour η petit, fixé à l'avance. De plus, si on obtient $k_1 < 1$ à une étape, alors on peut conclure que K est euclidien pour la norme.

Théorème 4.1. *L'algorithme 4.1 calcule le minimum euclidien de K et les points critiques quand il ne renvoie pas «* échec *».*

Remarque 4.2. La procédure peut échouer si on ne parvient pas à construire un graphe convenable. En ce cas, il existe un seuil k_2 tel que

- pour $k > k_2$, tous les problèmes sont absorbés,
- pour $k < k_2$, certains problèmes subsistent mais on ne parvient pas à trouver un graphe convenable.

En ce cas, k_0 et k_1 seront proches de k_2. Pour faire en sorte que la procédure s'arrête, on fixe $\epsilon > 0$ tel que, si $k_1 - k_0 < \epsilon$, alors on stoppe la procédure et on dit que l'algorithme échoue. En pratique, ϵ est égal à la précision du test d'absorption (voir table II.9).

Dans les rares cas où l'algorithme 4.1 renvoie *échec*, on découpe plus finement initialement dans chaque direction dans l'algorithme 3.2 et on augmente la taille de la liste $\mathcal{L}$ des entiers dans l'algorithme 3.4. En général, cela permet à une exécution ultérieure de l'algorithme 4.1 d'obtenir un graphe convenable.

En fait, si le rang des unités est strictement supérieur à 1 et si K n'est pas un corps CM, alors il existe un découpage tel que l'algorithme 4.1 obtienne un graphe convenable si on met assez d'entiers dans $\mathcal{L}$. Notons cependant qu'on ne peut pas connaître à l'avance les paramètres d'exécution nécessaires et que cela ne tient pas compte de la précision des calculs. Par ailleurs, pour $r = 1$, même les cas où il y a une infinité de points $x \in H \setminus \Phi(K)$ vérifiant $m_{\overline{K}}(x) \geqslant 1$ peuvent être traités par l'algorithme 4.1, on peut ainsi voir l'exemple $K = \mathbf{Q}(\sqrt{13})$ décrit en détail dans [Cer05, paragraphe 5.10].

4.2 Aspects pratiques

4.2.1 Recouvrement du domaine fondamental et découpages

4.2.1.1 Recouvrement du domaine fondamental Reprenons les notations $\mathcal{M}$, $(a_i)_{1\leqslant i\leqslant n}$ et $(b_i)_{1\leqslant i\leqslant n}$ du paragraphe 3.2.3. Alors $\mathcal{F} \subseteq [a_1, b_1]\times\cdots\times[a_n, b_n]$. Supposons que le parallélotope $\mathcal{P}$ de centre $c = (c_i)_{1\leqslant i\leqslant n}$ et de pas $h = (h_i)_{1\leqslant i\leqslant n}$ vérifie $\mathcal{P} \subseteq [a_1, b_1]\times\cdots\times[a_n, b_n]$. On ne conserve $\mathcal{P}$ que si $\mathcal{P}\cap\mathcal{F} \neq \varnothing$. Comme Φ est une bijection, cela équivaut à $\Phi^{-1}(\mathcal{P}) \cap [0, 1[^n \neq \varnothing$.

Par définition, pour tout $(x_i)_{1\leqslant i\leqslant n} \in \mathcal{P}$, $1 \leqslant i \leqslant n$, $c_i - h_i \leqslant x_i \leqslant c_i + h_i$. On écrit

$\mathcal{M}^{-1} = \left(m'_{i,j}\right)_{1\leqslant i,j\leqslant n}$. Alors pour tout $(x_i)_{1\leqslant i\leqslant n} \in \mathcal{P}$,

$$\sum_{\substack{j=1\\ m'_{i,j}<0}}^{n} m'_{i,j}(c_j + h_j) + \sum_{\substack{j=1\\ m'_{i,j}>0}}^{n} m'_{i,j}(c_j - h_j) \leqslant \sum_{j=1}^{n} m'_{i,j}x_j\,,$$

$$\text{et } \sum_{j=1}^{n} m'_{i,j}x_j \leqslant \sum_{\substack{j=1\\ m'_{i,j}<0}}^{n} m'_{i,j}(c_j - h_j) + \sum_{\substack{j=1\\ m'_{i,j}>0}}^{n} m'_{i,j}(c_j + h_j).$$

Ainsi, on obtient immédiatement la propriété suivante.

Lemme 4.3. *Si au moins l'une des inégalités* $\displaystyle\sum_{\substack{j=1\\ m'_{i,j}<0}}^{n} m'_{i,j}(c_j+h_j)+\sum_{\substack{j=1\\ m'_{i,j}>0}}^{n} m'_{i,j}(c_j-h_j) > 1$

ou $\displaystyle\sum_{\substack{j=1\\ m'_{i,j}<0}}^{n} m'_{i,j}(c_j - h_j) + \sum_{\substack{j=1\\ m'_{i,j}>0}}^{n} m'_{i,j}(c_j + h_j) < 0$ *est vérifiée, alors* $\mathcal{P}\cap\mathcal{F} = \varnothing$.

4.2.1.2 Découpage initial Dans chaque direction $1 \leqslant i \leqslant n$, on choisit un entier strictement positif N_i et on découpe $\mathcal{F}$ en N_i morceaux dans la direction i. Comme observé dans la figure II.2, le découpage doit être assez fin pour espérer absorber des parallélotopes. On élimine les parallélotopes qui n'intersectent pas $\mathcal{F}$ avec le lemme 4.3. De plus, comme on peut le remarquer dans la figure II.3, l'action des unités varie selon les coordonnées. Par conséquent, il peut être intéressant de découper davantage dans les directions correspondant aux « grandes » coordonnées du plongement de l'unité.

4.2.1.3 Découpages suivants On coupe chaque parallélotope en deux dans toutes les directions, ce qui fait que le nombre de parallélotopes problématiques est au plus multiplié par 2^n. Néanmoins, après absorption par les entiers et action des unités, on s'attend à ce que le nombre de parallélotopes problématiques n'augmente pas. De nouveau, on supprime les parallélotopes qui n'intersectent pas $\mathcal{F}$ grâce au lemme 4.3.

4.3 Simplification du graphe

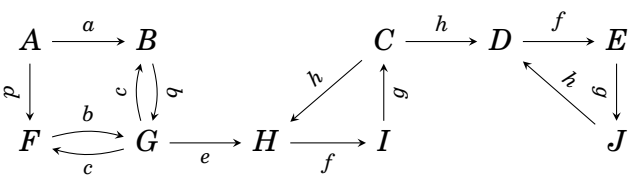
Pour la construction décrite au paragraphe 3.4.2, le fait que l'on traite des parallélotopes n'a pas d'importance : on peut fusionner certains d'entre eux et le théorème 3.17 reste vrai. Pour identifier des graphes convenables, on peut opérer certaines simplifications du graphe $\mathcal{G}$.

Tout d'abord, on élimine tout sommet éventuellement inutile. En effet, si un sommet $\mathcal{V}$ n'est atteint par aucune arête, on peut le supprimer de la liste des sommets.

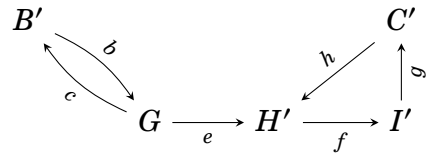
Définition 4.4. Soient $\mathcal{V}$ et $\mathcal{V}'$ deux sommets du graphe $\mathcal{G}$. $\mathcal{V}$ est dit *compatible* avec $\mathcal{V}'$ si pour toute arête $\mathcal{V} \xrightarrow{a} \mathcal{X}$, il existe une arête $\mathcal{V}' \xrightarrow{a} \mathcal{X}$.

Ainsi, si le sommet $\mathcal{V}$ est compatible avec $\mathcal{V}'$, on fusionne $\mathcal{V}$ et $\mathcal{V}'$ en un nouveau sommet $\mathcal{W}$ tel que

$$\begin{cases} \mathcal{U} \xrightarrow{c} \mathcal{W} & \text{si } \mathcal{U} \xrightarrow{c} \mathcal{V} \text{ ou } \mathcal{U} \xrightarrow{c} \mathcal{V}',\\ \mathcal{W} \xrightarrow{d} \mathcal{X} & \text{si } \mathcal{V}' \xrightarrow{d} \mathcal{X}. \end{cases}$$



(A) Graphe initial qui n'est pas convenable, il y a un chemin infini entre B et F (passant par G) qui n'est pas ultimement périodique.



(B) On peut supprimer le sommet A qui n'est pas atteint et fusionner B et F, qui sont compatibles. D'autres simplifications peuvent être effectuées sur la partie droite du graphe pour fusionner les deux 3-cycles. Le nouveau graphe est convenable.

FIGURE II.4 – Exemple de simplification d'un graphe pour le rendre convenable.

Ensuite, on considère les sommets qui sont l'origine d'au moins deux arêtes. Soit $\mathcal{V}$ un tel sommet. On note $\mathcal{V} \xrightarrow{a_i} \mathcal{W}_i$ pour $1 \leqslant i \leqslant l$ les arêtes partant de $\mathcal{V}$. Pour $1 \leqslant i \neq j \leqslant l$, on fusionne $\mathcal{W}_i$ et $\mathcal{W}_j$ si $a_i = a_j$. Ainsi, on obtient un nouveau sommet $\mathcal{W}_{i,j}$ dont les arêtes sont obtenues en regroupant celles de $\mathcal{W}_i$ et $\mathcal{W}_j$.

Ces simplifications sont illustrées dans la figure II.4.

Enfin, pour vérifier que le graphe simplifié est convenable, on calcule ses composantes fortement connexes (en utilisant par exemple l'algorithme de Tarjan, [Tar72]) et on vérifie que ce sont des cycles. En ce cas, on obtient aussi les cycles simples du graphe.

4.3.1 Translations du domaine fondamental

Dans certains cas, le minimum euclidien peut être atteint dans des points qui sont sur le bord du domaine fondamental. Par exemple, pour $K = \mathbf{Q}(\sqrt{13})$, on a $M(K) = m_K\left(\frac{\pm 1+\sqrt{13}}{6}\right) = m_K\left(\frac{\pm 1+\sqrt{13}}{3}\right) = \frac{1}{3}$. Deux des quatre points critiques de K sont sur le bord du domaine fondamental utilisé à la figure II.2. Par conséquent, un point problématique et son translaté peuvent être inclus dans le recouvrement du domaine fondamental. Si cela se produit, on ne pourra pas obtenir de graphe convenable.

Ainsi, on translate le recouvrement du domaine fondamental pour éviter ce problème : dans les directions où les parallélotopes problématiques sont près du bord, on translate de $-\eta$ où $\eta > 0$. Le domaine considéré contiendra toujours un domaine fondamental, mais ne contiendra pas deux points critiques qui sont translatés l'un de l'autre par un vecteur dans $\Phi(\mathbf{Z}_K)$.

4.3.2 Calcul de l'orbite d'un point

Étant donné un point $\xi \in K$, on veut calculer l'ensemble fini $\mathrm{Orb}\,(\Phi(\xi))$. En pratique, les calculs sont effectués avec les éléments de K, donc on mène les calculs avec des éléments de K, dont les coordonnées appartiennent à $\mathbf{Q} \cap [0, 1[$ pour l'écriture

dans la base $(z_i)_{1\leqslant i\leqslant n}$ de $\mathbf{Z}_K$. Écrivons cette réduction sous la forme

$$\begin{cases} K & \longrightarrow & K \\ x = \sum_{i=1}^{n} q_i z_i & \longmapsto & \overline{x} = \sum_{i=1}^{n} (q_i - \lfloor q_i \rfloor) z_i \end{cases}.$$

Ensuite, on cherche à calculer $\mathcal{O} = \left\{\overline{\varepsilon \cdot \xi},\ \varepsilon \in \mathbf{Z}_K^{\times}\right\}$. On note $(\varepsilon_i)_{1\leqslant i\leqslant r}$ les unités fondamentales de K et ν un générateur des racines de l'unité de K. On suppose que ν est d'ordre l. Pour tout $1 \leqslant i \leqslant r$, il existe un entier strictement positif s tel que $\overline{\varepsilon_i^s \cdot \xi} = \overline{\xi}$ (remarque 3.1), on note l_i le plus petit entier ayant cette propriété.

Avec ces notations, on a

$$\mathcal{O} = \left\{\overline{\nu^m \cdot \prod_{i=1}^{r} \varepsilon_i^{m_i} \cdot \xi},\ 0 \leqslant m < l,\ \text{pour tout } 1 \leqslant i \leqslant n,\ 0 \leqslant m_i < l_i\right\}.$$

Cette description explicite de $\mathcal{O}$ est utilisée pour calculer cet ensemble.

4.3.3 Implémentation

L'algorithme général est écrit en C et est disponible en ligne ([Lez12c]). Les calculs exacts font appels à la bibliothèque PARI ([PAR12]). Avec les techniques décrites au paragraphe 3, l'algorithme 4.1 peut calculer le minimum euclidien d'un corps de nombres de degré au plus 8 et de discriminant assez petit à partir de la seule donnée de son polynôme minimal. Pour des degrés plus grands, le manque de précision (voir 6.1) et la durée d'exécution (voir 6.4) rendent l'application de l'algorithme 4.1 plus difficile.

4.4 Exemple

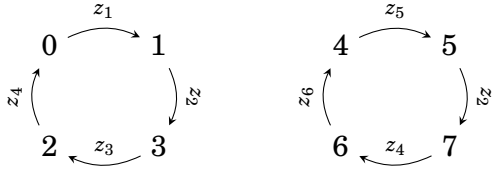
Dans ce paragraphe, nous présentons un exemple d'exécution étape par étape de l'algorithme 4.1.

On considère $p(x) = x^4 - x^3 + 2x^2 - 6x + 3$, α une racine de p et $K = \mathbf{Q}(\alpha)$. Alors $n = 4$, $r_1 = 2$, $r_2 = 1$, $\mathrm{disc}_K = -8\,787$, $\Lambda(K) = 3$, K est principal.

Avec de telles entrées, on obtient une matrice LLL-réduite $\mathcal{M}$ (définie par (II.2)).

On choisit une valeur initiale $\mathcal{K} = 3$. Pour $\mathcal{L}$, on prend tous les entiers utiles $\mathcal{M}Z$, où $Z = (Z_i)_{1\leqslant i\leqslant 4} \in \mathbf{Z}^4$ et $\max_{1\leqslant i\leqslant 4} |Z_i| \leqslant 25$. Il y a 1 520 365 tels éléments ($\simeq 22\%$ de 51^4). La table II.1 présente le nombres de parallélotopes problématiques restants à chaque étape de l'algorithme selon la valeur de k. Pour $k = 0{,}46$, on obtient 322 parallélotopes problématiques dans le meilleur cas.

Après simplification, on trouve le graphe convenable suivant à 8 arêtes. Les éléments écrits sous la forme $(z_i)_{1\leqslant i\leqslant 6}$ sont explicites.



On associe le point $t = \frac{16}{41}\alpha^3 + \frac{21}{41}\alpha^2 + \frac{37}{41}\alpha + \frac{28}{41} \in K$ au premier cycle. L'orbite $\mathrm{Orb}(\Phi(t))$ a huit éléments et contient le point associé à l'autre cycle. Par conséquent, $M(K) = m_K(t) = \frac{21}{41}$ et ce minimum est atteint en huit points de K (modulo $\mathbf{Z}_K$).

valeur de k	3	2,1	1,5	1,1	0,83	0,66	0,54	0,46
après le découpage initial	0	0	0	0	4	256	2 384	7 908
après la première action des unités	–	–	–	–	0	38	522	5 028
après le deuxième découpage	–	–	–	–	–	0	64	4 092
après la deuxième action des unités	–	–	–	–	–	–	22	1 076
après le troisième découpage	–	–	–	–	–	–	34	1 174
après la troisième action des unités	–	–	–	–	–	–	0	426
après les cinquièmes découpage et action des unités	–	–	–	–	–	–	–	322

TABLE II.1 – Parallélotopes problématiques aux différentes étapes de l'exécution de l'algorithme 4.1.

Cet exemple a été obtenu sur un processeur Intel®Xeon®CPU X5570 @ 2.93GHz (avec 4 cœurs). Le minimum euclidien a été calculé en 7 minutes et 13 secondes.

5 Résultats obtenus

L'algorithme 4.1 a été utilisé pour calculer de nombreux minima euclidiens. De nombreuses valeurs étaient déjà connues et listées dans les tables de [Lem95] et [Cer05], ce qui nous a permis de tester la correction de l'algorithme.

5.1 Observations générales

Les corps de nombres de degré au plus 8 et de discriminant « assez petit » sont euclidiens pour la norme et leur minimum vaut $\frac{1}{\Lambda(K)}$. En outre, plus le degré croît, plus on a d'exemples de corps de nombres ayant cette propriété. Plus précisément, si on note

$$b(r_1, r_2) := \inf\left\{|\mathrm{disc}_K|\ ,\ K \text{ corps de signature } (r_1, r_2) \text{ tel que } M(K) > \frac{1}{\Lambda(K)}\right\},$$

la table II.2 donne les valeurs de $b(r_1, r_2)$ pour des corps de nombres de degré inférieur ou égal à 5.

5.2 Corps quartiques purs

5.2.1 Présentation

Plutôt que de considérer un corps de nombres quelconque, on peut se restreindre à une famille de corps et par exemple étudier les corps de nombres « purs », c'est-à-dire de la forme $\mathbf{Q}(\sqrt[l]{m})$ où $l \geqslant 2$ et $m > 1$ sont tels que le polynôme $X^l - m$ est

n	(r_1, r_2)	$b(r_1, r_2)$	nombre de corps de signature (r_1, r_2) tels que $\|\mathrm{disc}_K\| < b(r_1, r_2)$
2	(2, 0)	21	4
3	(3, 0)	169	3
	(1, 1)	135	11
4	(4, 0)	6125	24
	(2, 1)	1600	34
	(0, 2)	400	12
5	(5, 0)	390625	101
	(3, 1)	52519	165
	(1, 2)	9137	61

TABLE II.2 – Borne sur le discriminant pour toujours avoir $M(K) = \frac{1}{\Lambda(K)}$.

irréductible. Avec $l = 2$, on obtient en fait tous les corps quadratiques réels et ceux qui sont euclidiens pour la norme sont bien connus (I.3). Pour $l = 3$, il s'agit des corps cubiques purs dont l'euclidianité pour la norme a été étudiée en détail par Cioffari ([Cio79]). On a ainsi la propriété suivante.

Théorème 5.1 (Cioffari)**.** *Soit m un entier qui n'est pas un cube. Alors $K = \mathbf{Q}(\sqrt[3]{m})$ est euclidien pour la norme si et seulement K est un élément de la liste suivante :*

$$\mathbf{Q}(\sqrt[3]{2}), \mathbf{Q}(\sqrt[3]{3}), \mathbf{Q}(\sqrt[3]{10}).$$

L'objet de ce paragraphe va donc être d'étudier les corps quartiques purs, c'est-à-dire les corps de la forme $\mathbf{Q}(\sqrt[4]{m})$ où m est un entier strictement supérieur à 1 qui n'est pas une puissance quatrième. On va établir le résultat suivant.

Théorème 5.2. *Si L est un corps quartique pur tel que $L \neq \mathbf{Q}(\sqrt[4]{61})$, alors L est euclidien pour la norme si et seulement si $L = \mathbf{Q}(\sqrt[4]{m})$ où*

$$m \in \{2, 3, 5, 12, 20\}.$$

Egami a montré ([Ega79]) qu'il n'y a qu'un nombre fini de corps $\mathbf{Q}(\sqrt[4]{m})$ euclidiens pour la norme pour $m \neq 2p^2$, avec $p \equiv 3 \pmod 8$. Lemmermeyer a indiqué qu'on pouvait se passer de cette hypothèse et a donné une liste finie explicite de candidats dans [Lem89].

5.2.2 Démarche et outils généraux

Nous reprenons le raisonnement décrit par Lemmermeyer, en le complétant pour certains cas. Pour commencer, on limite le nombre de cas possibles grâce à la propriété suivante.

Proposition 5.3 ([Par75, Theorem I p. 107])**.** *Soit L un corps quartique pur. Si le nombre de classes h_L est impair, alors $L = \mathbf{Q}(\sqrt[4]{m})$ où m est l'une des valeurs suivantes (p désigne un nombre premier) :*

- 2,
- $2p^2$, *où* $p \equiv 3 \pmod 8$,
- p, *où* $p \equiv \pm 3 \pmod 8$,
- $4p$, *où* $p \equiv -1, \pm 3 \pmod 8$,
- $2p$, *où* $p \equiv 3 \pmod 8$,
- $8p$, *où* $p \equiv 3 \pmod 8$.

Comme tout corps de nombres euclidien est principal, si on cherche tous les corps quartiques purs L euclidiens pour la norme, on peut supposer que $L = \mathbf{Q}(\sqrt[4]{m})$ où m est l'une des valeurs de la proposition 5.3. Pour alléger l'écriture, on va noter

$$L_m := \mathbf{Q}(\sqrt[4]{m}).$$

5.2.2.1 Propriétés de congruence

Lemme 5.4. *1. Soit L/K une extension galoisienne de corps de nombres. Soit I un idéal de L tel que pour tout $\varphi \in \mathrm{Gal}(L/K)$, $\varphi(I) \subseteq I$. Alors pour tous α, $\beta \in \mathbf{Z}_L$ tels que $\alpha - \beta \in I$,*

$$\mathbf{N}_{L/K}(\alpha) \equiv \mathbf{N}_{L/K}(\beta) \pmod{I \cap \mathbf{Z}_K}.$$

2. Soit I un idéal de $\mathbf{Z}_{L_m}$ invariant par $\varphi_1 : \sqrt[4]{m} \longmapsto -\sqrt[4]{m}$ et $\varphi_2 : \sqrt{m} \longmapsto -\sqrt{m}$, alors pour tous α, $\beta \in \mathbf{Z}_{L_m}$ tels que $\alpha - \beta \in I$,

$$\mathbf{N}_{L_m/\mathbf{Q}}(\alpha) \equiv \mathbf{N}_{L_m/\mathbf{Q}}(\beta) \pmod{I \cap \mathbf{Z}}.$$

Démonstration. 1. C'est une conséquence immédiate de la définition de la norme : pour tout $x \in L$, $\mathbf{N}_{L/K}(x) = \prod_{\varphi \in \mathrm{Gal}(L/K)} \varphi(x)$.

2. Il suffit d'appliquer le premier point deux fois : d'abord avec $L_m/\mathbf{Q}(\sqrt{m})$, puis avec $\mathbf{Q}(\sqrt{m})/\mathbf{Q}$. Le résultat s'en déduit par transitivité de la norme.

□

Lemme 5.5. *Soit f un entier naturel produit de nombres premiers totalement ramifiés dans L_m et deux à deux distincts. S'il existe deux entiers naturels strictement positifs a et b tels que*

1. *$f = a + b$,*
2. *il existe $x \in \mathbf{Z}$ tel que $a \equiv x^4 \pmod f$,*
3. *a et $-b$ ne sont pas des normes d'éléments entiers de L_m,*

alors L_m n'est pas euclidien pour la norme.

Démonstration. Par l'absurde, supposons que L_m est euclidien pour la norme.

Par hypothèse sur f, il existe un idéal entier $\mathfrak{f}$ de $\mathbf{Z}_{L_m}$ tel que $f\mathbf{Z}_{L_m} = \mathfrak{f}^4$.

Or L_m est euclidien, donc principal, donc il existe $t \in \mathbf{Z}_{L_m}$ tel que $\mathfrak{f} = t\mathbf{Z}_{L_m}$. On fait la division euclidienne de x par t : il existe $y \in \mathbf{Z}_{L_m}$ tel que $x - y \in \mathfrak{f}$ et

$$\left|\mathbf{N}_{L_m/\mathbf{Q}}(y)\right| < \left|\mathbf{N}_{L_m/\mathbf{Q}}(t)\right| = \mathbf{N}\mathfrak{f} = f.$$

En appliquant le lemme 5.4 (2) avec $I = \mathfrak{f}$, on obtient que $\mathbf{N}_{L_m/\mathbf{Q}}(x) \equiv \mathbf{N}_{L_m/\mathbf{Q}}(y) \pmod{f}$. Or $x \in \mathbf{Z}$, donc $\mathbf{N}_{L_m/\mathbf{Q}}(x) = x^4 \equiv a \pmod{f}$. Ainsi,

$$-b \equiv a \equiv \mathbf{N}_{L_m/\mathbf{Q}}(y) \pmod{f}.$$

Comme $a, b > 0$, cela implique

$$\mathbf{N}_{L_m/\mathbf{Q}}(y) \in \{a, -b\},$$

ce qui est exclu. □

Remarque. Cet énoncé de congruence est très classique, on peut en voir une formulation un peu plus générale (mais inutile ici) dans [Ega84]. Dans ce papier, Egami attribue les idées de généralisation à Lenstra.

5.2.2.2 Propriétés des entiers D'après le lemme 5.5, pour démontrer que L_m est non euclidien pour la norme, il suffit d'exhiber une décomposition de nombres premiers ramifiés en somme de deux entiers ayant certaines propriétés. Le lemme suivant va permettre de trouver de telles décompositions.

Lemme 5.6. *Soit p un nombre premier.*

1. *Si $p \equiv 5 \pmod 8$ tel que $p \geqslant 101$ et $p \neq 109$, alors il existe $r, s, t, u \in \mathbf{N}$ tels que $p = rs + tu$, $(r, s) = (t, u) = 1$ et $\left(\frac{r}{p}\right) = \left(\frac{s}{p}\right) = \left(\frac{t}{p}\right) = -1$.*
2. *Si $p \equiv 3 \pmod 4$ et $p > 3$, alors il existe deux entiers naturels a et b tels que $2p = a + b$, $a \equiv 5 \pmod 8$ et $\left(\frac{a}{p}\right) = 1$.*
3. *Si $p \equiv 3 \pmod 4$ et $p > 19$, alors il existe deux entiers naturels a et b tels que $p = a + b$, $a = 5 - p \pmod 8$ et $\left(\frac{a}{p}\right) = 1$.*

Démonstration.

1. Pour $p \equiv 5 \pmod{24}$, voir [BR36]. Pour $p \equiv 13 \pmod{24}$, voir [Bra40]. Pour $p = 101$, une décomposition possible est $101 = 2 \cdot 7 + 3 \cdot 29$.
2. On distingue deux cas selon la congruence de p modulo 8.
   – $p \equiv 3 \pmod 8$: pour $p = 11$, on peut prendre $a = 5$, donc on peut supposer que $p \geqslant 19$. Ainsi, il existe $c \in \mathbf{N}$ tel que $2p < 16c < 3p$. Dès lors,

   $$0 < 8c - p < 16c - p < 2p.$$

   De plus $8c - p \equiv 16c - p \equiv 5 \pmod 8$. Comme $16c - p \equiv 2(8c - p) \pmod p$, on a

   $$\left(\frac{16c - p}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{8c - p}{p}\right) = -\left(\frac{8c - p}{p}\right).$$

   Ainsi, $\left(\frac{8c - p}{p}\right) = 1$ ou $\left(\frac{16c - p}{p}\right) = 1$ et on peut choisir $a \in \{8c - p, 16c - p\}$ tel que $\left(\frac{a}{p}\right) = 1$.

– $p \equiv 7 \pmod 8$: alors $p \geqslant 23$ et on peut donc trouver $c \in \mathbf{N}$ tel que $5p < 16c < 6p$. Ainsi

$$0 < 16c - 5p\,,\, 3p - 8c < 2p.$$

On a $16c - 5p \equiv 3p - 8c \equiv 5 \pmod 8$ et, comme $16c - 5p \equiv -2(3p - 8c) \pmod p$,

$$\left(\frac{16c-5p}{p}\right) = \left(\frac{-2}{p}\right)\left(\frac{3p-8c}{p}\right) = -\left(\frac{3p-8c}{p}\right).$$

Par conséquent, on peut choisir $a \in \{16c - 5p\,,\, 3p - 8c\}$ tel que $\left(\frac{a}{p}\right) = 1$.

3. On commence par noter que l'on peut supposer que $p \geqslant 59$ en exhibant les valeurs de a suivantes pour p plus petit.

p	23	31	39	43	47	51
a	6	14	22	10	6	18

On distingue alors deux cas selon la congruence de p modulo 8.

– $p \equiv 3 \pmod 8$: on peut alors trouver un entier $c \in \mathbf{N}$ tel que $2p - 16 < 64c < 3p - 8$. Dès lors, on a

$$0 < 8c + 2\,,\, 8(8c + 2) - 2p < p.$$

De plus $8c + 2 \equiv 8(8c + 2) - 2p \equiv 2 \pmod 8$ et $8(8c + 2) - 2p \equiv 8(8c + 2) \pmod p$, donc

$$\left(\frac{8(8c+2)-2p}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{8c+2}{p}\right) = -\left(\frac{8c+2}{p}\right).$$

Par conséquent, on peut choisir $a \in \{8(8c + 2) - 2p\,,\, 8c + 2\}$ tel que $\left(\frac{a}{p}\right) = 1$.

– $p \equiv 7 \pmod 8$: on peut alors trouver $c \in \mathbf{N}$ tel que $p + 16 < 64c < 2p + 16$. Ainsi,

$$0 < 8c - 2\,,\, 2p - 8(8c - 2) < p.$$

De plus $8c-2 \equiv 2p-8(8c-2) \equiv -2 \pmod 8$. Comme $2p-8(8c-2) \equiv -8(8c-2) \pmod p$, on a

$$\left(\frac{2p-8(8c-2)}{p}\right) = \left(\frac{-2}{p}\right)\left(\frac{8c-2}{p}\right) = \left(\frac{8c-2}{p}\right).$$

Dès lors, on peut choisir $a \in \{2p - 8(8c - 2)\,,\, 8c - 2\}$ tel que $\left(\frac{a}{p}\right) = 1$.

□

D'autre part, il est intéressant de savoir quels entiers ne sont pas des normes. Le lemme suivant donne un critère.

Lemme 5.7. *Soient p un nombre premier tel que $p \equiv 1 \pmod 4$, r et s deux entiers tels que $(r, s) = 1$ et $\left(\frac{r}{p}\right) = \left(\frac{s}{p}\right) = -1$. On note $K = \mathbf{Q}(\sqrt{p})$. Alors rs n'est pas la norme d'un élément de $\mathbf{Z}_K$.*

Démonstration. Comme $(r, s) = 1$, on peut supposer que r est impair. On suppose que $\alpha \in \mathbf{Z}_K$ est tel que $\mathbf{N}_{K/\mathbf{Q}}(\alpha) = rs$, c'est-à-dire qu'il existe deux entiers x et y tels que $x^2 - py^2 = r \cdot (4s)$.

Soit q un facteur premier (impair) de valuation impaire de r (s'il existe). Si q divise y, alors $q \neq p$, donc q divise x. Ainsi, en divisant par q^2 autant de fois que nécessaire, on se ramène au cas où q ne divise pas y. Alors

$$p \equiv \left(xy^{-1}\right)^2 \pmod{q},$$

donc $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = 1$, car $p \equiv 1 \pmod 4$, d'après la loi de réciprocité quadratique. Par conséquent, en faisant le produit sur tous les q, on trouve $\left(\frac{r}{p}\right) = 1$, ce qui est faux. □

Remarque 5.8. Si $p \equiv 3 \pmod 4$, la propriété reste vraie si r est produit de nombres premiers congrus à 3 modulo 4.

5.2.3 Puissances quatrièmes

Pour appliquer le lemme 5.5, il est important de savoir que certains éléments sont des puissances quatrièmes modulo un certain entier f. En pratique, on aura seulement besoin d'une telle propriété pour $f = p$ ou $f = 2p$ où p est un nombre premier impair. Selon la congruence de p modulo 4, on va distinguer les propriétés classiques utiles pour la suite.

Lemme 5.9. *Si $p \equiv 3 \pmod 4$, on note*

$$C := \{t \in \mathbf{Z}/p\mathbf{Z},\ t \not\equiv 0 \pmod p \text{ et } t \text{ carré modulo } p\}.$$

Alors C est un groupe abélien pour la multiplication et l'application $\left\{ \begin{array}{ccc} C & \longrightarrow & C \\ x & \longmapsto & x^2 \end{array} \right.$ *est une bijection. En particulier, pour tout $t \in \mathbf{Z}/p\mathbf{Z}$, t est un carré modulo p si et seulement si c'est une puissance quatrième modulo p.*

Démonstration. Le fait que C est un groupe abélien est clair. Pour voir que l'application d'élévation au carré est une bijection de C, il suffit de prouver que c'est une injection. Or, si $x \in C$ vérifie $x^2 \equiv 1 \pmod p$, alors $(x-1)\cdot(x+1) \equiv 0 \pmod p$, d'où $x \equiv 1 \pmod p$ ou $x \equiv -1 \pmod p$ car $\mathbf{Z}/p\mathbf{Z}$ est un corps. Mais -1 n'est pas un carré modulo p car $p \equiv 3 \mod 4$, donc $x \equiv 1 \pmod p$, ce qui montre que l'élévation au carré est injective et achève la preuve. □

Si $p \equiv 1 \pmod 4$, la situation est un peu plus compliquée. C'est pourquoi on va introduire le symbole de résidu quartique modulo p, noté $\left(\frac{\cdot}{p}\right)_4$. Il est défini pour a premier avec p par

$$\left(\frac{a}{p}\right)_4 \equiv a^{\frac{p-1}{4}} \pmod p.$$

Cette définition est possible parce que, par hypothèse, $p \equiv 1 \pmod 4$, mais aussi car $a^{\frac{p-1}{2}} \equiv 1 \pmod p$ et car $\mathbf{Z}/p\mathbf{Z}$ est un corps. Notons aussi que si $a \in C$, alors $\left(\frac{a}{p}\right)_4 \in \{\pm 1\}$. Avec cette définition, on a la propriétés suivantes.

Lemme 5.10. *Soient $p \equiv 1 \pmod 4$, a et b deux entier premiers avec p.*

1. *Il existe $\alpha \in \mathbf{Z}$ tel que $a \equiv \alpha^4 \pmod p$ si et seulement si $\left(\frac{a}{p}\right)_4 = 1$.*
2. *On a $\left(\frac{a}{p}\right)_4 \left(\frac{b}{p}\right)_4 = \left(\frac{ab}{p}\right)_4$.*

Démonstration. 1. Si a est une puissance quatrième modulo p, on a clairement $\left(\frac{a}{p}\right)_4 = 1$. Réciproquement, si $\left(\frac{a}{p}\right)_4 = 1$, alors $\left(\frac{a}{p}\right) = 1$, donc a est un carré modulo p, disons $a \equiv c^2 \pmod p$, pour un certain entier c. Or $\left(\frac{c}{p}\right) \equiv c^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{4}} \equiv 1 \pmod p$. Donc c est lui-même un carré modulo p, ce qui prouve que a est une puissance quatrième modulo p.

2. C'est une conséquence facile de la définition du résidu quartique modulo p.

□

Pour plus de détails sur la réciprocité quartique, on peut consulter [Lem00].
Pour traiter le cas $f = 2p$, seul le lemme facile énoncé ci-dessous sera utile.

Lemme 5.11. *Soient p un nombre impair et x un entier qui est une puissance quatrième modulo p. Alors x est une puissance quatrième modulo $2p$.*

Démonstration. Soit $\alpha \in \mathbf{Z}$ tel que $x \equiv \alpha^4 \pmod p$. Alors $x \equiv \alpha^4 \pmod{2p}$ ou $x \equiv \alpha^4 + p \pmod{2p}$. Dans le second cas, $x \equiv (\alpha + p)^4 \pmod{2p}$ car $p^4 - p = 2p \cdot \frac{p^3-1}{2}$. Cela montre que x est toujours une puissance quatrième modulo $2p$. □

5.2.4 Ramification totale

Pour appliquer le lemme 5.5, nous aurons besoin de connaître des premiers totalement ramifiés, le lemme suivant va nous fournir de tels premiers.

Lemme 5.12. *Soient p un premier impair et $m \in \{p, 2p, 4p, 8p\}$. Alors p est totalement ramifié dans L_m. De plus, si $m \in \{2p, 8p\}$, alors 2 est totalement ramifié dans L_m.*

Démonstration. Dans tous les cas, notons $\alpha \in L_m$ tel que $\alpha^4 = m$.

- Soit q un nombre premier qui divise m tel que q^2 ne divise pas m. On l'appliquera avec $q = p$ dans tous les cas et $q = 2$ pour $m = 2p$. Soit $\mathfrak{q}$ un facteur premier de $q\mathbf{Z}_{L_m}$. On écrit $q\mathbf{Z}_{L_m} = \mathfrak{q}^e\mathfrak{r}$, où $e \geqslant 1$ et $\mathfrak{r}$ est premier avec $\mathfrak{q}$.
  Comme $\mathfrak{q}$ divise $m\mathbf{Z}_{L_m}$, il divise $\alpha^4\mathbf{Z}_{L_m}$, donc aussi $\alpha\mathbf{Z}_{L_m}$. Par conséquent, $\mathfrak{q}^4$ divise $\alpha^4\mathbf{Z}_{L_m} = m\mathbf{Z}_{L_m}$. Comme $\mathfrak{q}$ est premier avec $\frac{m}{q}$ et $\mathfrak{r}$, cela implique que $\mathfrak{q}^4$ divise $\mathfrak{q}^e$, donc $e \geqslant 4$.
  Mais q est premier, donc $\mathbf{N}\mathfrak{q} \geqslant q$. Par conséquent, $\mathfrak{q}^4$ divise $q\mathbf{Z}_{L_m}$ et $\mathbf{N}\mathfrak{q}^4 \geqslant \mathbf{N}(q\mathbf{Z}_{L_m})$. Ainsi, $q\mathbf{Z}_{L_m} = \mathfrak{q}^4$.
- Il reste à traiter $q = 2$ dans L_{8p}. On note $\mathfrak{q}$ un facteur premier de $2\mathbf{Z}_{L_{8p}}$. Comme précédemment, on écrit $2\mathbf{Z}_{L_{8p}} = \mathfrak{q}^e\mathfrak{r}$ avec $e \geqslant 1$ et $\mathfrak{r}$ premier avec $\mathfrak{q}$. On va alors montrer que $e \geqslant 4$. Comme $\mathbf{N}\mathfrak{q} \geqslant 2$, cela permettra de déduire que $2\mathbf{Z}_{L_{8p}} = \mathfrak{q}^4$.
  Comme $\mathfrak{q}^3$ divise $8\mathbf{Z}_{L_{8p}}$, il divise aussi $\alpha^4\mathbf{Z}_{L_{8p}}$. Par conséquent, $\mathfrak{q}$ divise $\alpha\mathbf{Z}_{L_{8p}}$, donc $\mathfrak{q}^4$ divise $8\mathbf{Z}_{L_{8p}}$, ce qui prouve que $\mathfrak{q}^4$ divise $\mathfrak{q}^{3e}\mathfrak{r}^3$. Ainsi, $e \geqslant 2$. On continue le raisonnement, en notant qu'alors $\mathfrak{q}^8$ divise $\alpha^4\mathbf{Z}_{L_{8p}}$, donc $\mathfrak{q}^8$ divise $\mathfrak{q}^{3e}$, et ainsi $e \geqslant 3$. On en déduit que $\mathfrak{q}^{12}$ divise $\alpha^4\mathbf{Z}_{L_{8p}}$. Dès lors, $\mathfrak{q}^{12}$ divise $\mathfrak{q}^{3e}$, donc $e \geqslant 4$, ce qui permet de conclure comme annoncé. □

5.2.5 Propriétés générales de L_{2p^2}

Dans le cas de L_{2p^2}, $p \equiv 3 \pmod 8$, non traité par Egami, la preuve que nous présentons nécessite une connaissance fine de $\mathbf{Z}_{L_{2p^2}} = \mathbf{Z} + \mathbf{Z}\sqrt[4]{2p^2} + \mathbf{Z}\sqrt{2} + \mathbf{Z}\sqrt[4]{2p^2}\sqrt{2}$, et plus particulièrement des unités $\mathbf{Z}_{L_{2p^2}}^{\times}$. Les unités des corps quartiques purs ont été étudiées en détail. On peut par exemple consulter [Ste73] ou [End83] à ce sujet. Nous allons seulement donner les propriétés utiles dans le cas particulier de L_{2p^2} qui nous intéresse ici. On pose $K = \mathbf{Q}\left(\sqrt{2}\right)$.

Tout élément x de L_{2p^2} peut être écrit sous la forme

$$x_1 + x_2\sqrt[4]{2p^2} + x_3\sqrt{2} + x_4\sqrt[4]{2p^2}\sqrt{2},$$

où $x_1, x_2, x_3, x_4 \in \mathbf{Q}$. Cette écriture fournit un plongement naturel de L_{2p^2} dans $\mathbf{R}$.

Lemme 5.13. *Soit* $U = \left\{u \in \mathbf{Z}_L^{\times},\ \mathbf{N}_{L_{2p^2}/K}(u) = 1\right\}$. *Alors il existe* $\varepsilon_0 \in U$ *tel que tel que* $\varepsilon_0 > 1$ *et pour tout* $u \in U$ *tel que* $u > 1$, $u \geqslant \varepsilon_0$.

Démonstration. Comme le rang des unités de L est 2, on peut considérer un système d'unités fondamentales (ε, ν) de L. On note $\sigma : L_{2p^2} \longrightarrow L_{2p^2}$ le morphisme défini pour $x_1, x_2, x_3, x_4 \in \mathbf{Q}$ par

$$\sigma\left(x_1 + x_2\sqrt[4]{2p^2} + x_3\sqrt{2} + x_4\sqrt[4]{2p^2}\sqrt{2}\right) = x_1 - x_2\sqrt[4]{2p^2} + x_3\sqrt{2} - x_4\sqrt[4]{2p^2}\sqrt{2}.$$

On pose alors

$$f : \left\{\begin{array}{ccc} {L_{2p^2}}^{\times} & \longrightarrow & \mathbf{R}^2 \\ x & \longmapsto & (\ln|x|, \ln|\sigma(x)|) \end{array}\right. .$$

Avec ces notations,

$$f(\mathbf{Z}_{L_{2p^2}}^{\times}) = \left\{(k\ln|\varepsilon| + l\ln|\nu|,\, k\ln|\sigma(\varepsilon)| + l\ln|\sigma(\nu)|,\, (k,l) \in \mathbf{Z}^2\right\},$$

donc $f(\mathbf{Z}_{L_{2p^2}}^{\times})$ est un sous-groupe discret de $\mathbf{R}^2$. En particulier, $f(U)$ est aussi un sous-groupe discret de $\mathbf{R}^2$.

Comme $\mathbf{N}_{L_{2p^2}/K}(\varepsilon), \mathbf{N}_{L_{2p^2}/K}(\nu) \in \mathbf{Z}_K^{\times}$, il existe deux entiers a et b tels que

$$\mathbf{N}_{L_{2p^2}/K}(\varepsilon) = \pm(1+\sqrt{2})^a \qquad \text{et} \qquad \mathbf{N}_{L_{2p^2}/K}(\nu) = \pm(1+\sqrt{2})^b.$$

Si $a = 0$, on pose $\tau := \varepsilon^2$. Si $b = 0$, on pose $\tau := \nu^2$. Dans les autres cas, on pose

$$\tau := \varepsilon^{-2b}\nu^{2a}.$$

Alors $\mathbf{N}_{L_{2p^2}/K}(\tau) = 1$. Notons que $\tau \neq 1$ car (ε, ν) est un système d'unités fondamentales de L_{2p^2}. Quitte à changer τ en $-\tau$, on peut supposer que $\tau > 0$. Quitte à changer τ en $\frac{1}{\tau}$, on peut alors supposer que $\tau > 1$.

Ainsi, $\tau \in U$ et $\tau > 1$. Considérons alors l'ensemble $V = \{u \in U,\ 1 < u \leqslant \tau\}$. Soit $u \in V$. On a alors $u\sigma(u) = \mathbf{N}_{L_{2p^2}/K}(u) = 1$, donc

$$0 < \ln|u| \leqslant \ln|\tau| \text{ et } \ln|\sigma(\tau)| \leqslant \ln|\sigma(u)| < 0.$$

Par conséquent, $f(V) \subseteq f(U) \cap [0, \ln|\tau|] \times [\ln|\sigma(\tau)|, 0]$. Donc $f(V)$ est inclus dans l'intersection d'un sous-groupe discret et d'un compact de $\mathbf{R}^2$. Ainsi, $f(V)$ est fini. En particulier, on peut considérer $\varepsilon_0 \in V$ tel que $\varepsilon_0 > 1$ soit minimal. Dès lors, pour tout $u \in U$ tel que $u > 1$, $u \geqslant \varepsilon_0$. □

Le lemme 5.13 prouve l'existence d'une plus petite unité ε_0 strictement supérieure à 1 telle que $\mathbf{N}_{L_{2p^2}/K}(\varepsilon_0) = 1$. Le résultat suivant, qui s'applique en fait à tout corps quartique pur, permet de construire un système d'unités fondamentales de L_{2p^2} à partir de ε_0.

Lemme 5.14 (Ljunggren)**.** *Soient ε_0 la plus petite unité de L_{2p^2} strictement supérieure à 1 et telle que $\mathbf{N}_{L/K}(\varepsilon_0) = 1$ et $\varepsilon^* = \sqrt{2} - 1$. S'il n'existe pas d'unité ε de L_{2p^2} telle que $\mathbf{N}_{L/K}(\varepsilon) = \pm\varepsilon^*$, alors $(\varepsilon^*, \varepsilon_0)$ est un système d'unités fondamentales de L_{2p^2}.*

Démonstration. Soit $u \in \mathbf{Z}_L^\times$. Alors $\mathbf{N}_{L/K}(u) \in \mathbf{Z}_K^\times$. Comme ε^* est une unité fondamentale de K, il existe $m \in \mathbf{Z}$ tel que

$$\mathbf{N}_{L/K}(u) = \pm{\varepsilon^*}^m$$

Il existe donc $l \in \mathbf{Z}$ tel que $\mathbf{N}_{L/K}(u{\varepsilon^*}^l) \in \{\pm 1, \pm\varepsilon^*\}$ selon la parité de m. Par hypothèse, les cas $\pm\varepsilon^*$ sont impossibles. Le cas -1 est aussi exclu car si on écrit $x = x_1 + x_2\sqrt{2} + x_3\sqrt[4]{2p^2} + x_4\sqrt[4]{2p^2}\sqrt{2}$, pour $x_1, x_2, x_3, x_4 \in \mathbf{Z}$, alors

$$\mathbf{N}_{L/K}(x) = x_1^2 + 2x_2^2 - 4px_3x_4 + \left(2x_1x_2 - px_3^2 - 2px_4^2\right)\sqrt{2}.$$

Par conséquent, $\mathbf{N}_{L/K}(x) = -1$ implique que (x_1, x_2, x_3, x_4) est solution du système suivant.

$$\begin{cases} x_1^2 + 2x_2^2 - 4px_3x_4 = -1 & \text{(II.10a)} \\ 2x_1x_2 - px_3^2 - 2px_4^2 = 0 & \text{(II.10b)} \end{cases}$$

Mais alors, d'après (II.10b),

$$\begin{aligned} 2x_1x_2 &= p(x_3^2 + 2x_4^2) \\ &= p(x_3^2 + (x_4\sqrt{2})^2) \\ &\geqslant 2px_3x_4\sqrt{2} \text{ d'après l'inégalité arithmético-géométrique,} \\ &= \frac{\sqrt{2}}{2}(x_1^2 + 2x_2^2 + 1) \text{ d'après (II.10a)} \\ &\geqslant \frac{\sqrt{2}}{2}(2x_1x_2\sqrt{2} + 1) \text{ d'après l'inégalité arithmético-géométrique,} \\ &= 2x_1x_2 + \frac{\sqrt{2}}{2}, \end{aligned}$$

ce qui est clairement faux. Dès lors, $\mathbf{N}_{L/K}(u{\varepsilon^*}^l) = 1$.

On pose $v = u{\varepsilon^*}^l$. Quitte à considérer $-v$, on peut supposer $v > 0$. Quitte à remplacer v par v^{-1}, on peut alors supposer que $v \geqslant 1$. Comme $\mathbf{N}_{L/K}(v) = 1$, par définition de ε_0, il existe $t \in \mathbf{Z}$ tel que $v = \varepsilon_0^t$. Ainsi, on a montré qu'il existe $a, b \in \mathbf{Z}$ tels que

$$u = \pm{\varepsilon^*}^a{\varepsilon_0}^b,$$

ce qui achève la preuve. □

Notons bien sûr que le résultat de Ljunggren est plus général et donne aussi un système d'unités fondamentales si l'équation $\mathbf{N}_{L/K}(\varepsilon) = \pm\varepsilon^*$ a au moins une solution, mais le lemme 5.14 suffit pour établir la propriété suivante.

Proposition 5.15. *$(\varepsilon^*, \varepsilon_0)$ est un système d'unités fondamentales de L_{2p^2}.*

Démonstration. Pour appliquer le lemme 5.14, on cherche donc à montrer qu'il n'existe pas d'unité ε de L_{2p^2} telle que $\mathbf{N}_{L/K}(\varepsilon) = \pm\varepsilon^*$. On note

$$\varepsilon = x_1 + x_2\sqrt{2} + (y_1 + y_2\sqrt{2})\sqrt[4]{2p^2},$$

où x_1, x_2, y_1 et y_2 sont entiers. Alors

$$\mathbf{N}_{L/K}(\varepsilon) = x_1^2 + 2x_2^2 - 4py_1y_2 + \left(2x_1x_2 - py_1^2 - 2py_2^2\right)\sqrt{2}.$$

On cherche donc à résoudre les systèmes suivants, ou plutôt à prouver qu'ils n'admettent pas de solution entière.

$$\begin{cases} x_1^2 + 2x_2^2 - 4py_1y_2 = -1 & \text{(II.11a)} \\ 2x_1x_2 - py_1^2 - 2py_2^2 = 1 & \text{(II.11b)} \end{cases}$$

$$\begin{cases} x_1^2 + 2x_2^2 - 4py_1y_2 = 1 & \text{(II.12a)} \\ 2x_1x_2 - py_1^2 - 2py_2^2 = -1 & \text{(II.12b)} \end{cases}$$

Pour (II.11), on raisonne par l'absurde, et on suppose que le système admet une solution $(x_1, x_2, y_1, y_2) \in \mathbf{R}^4$. Alors, d'après (II.11b),

$$\begin{aligned} 2x_1x_2 &= 1 + p(y_1^2 + 2y_2^2) \\ &= 1 + p(y_1^2 + (y_2\sqrt{2})^2) \\ &\geqslant 1 + 2py_1y_2\sqrt{2} \text{ d'après l'inégalité arithmético-géométrique,} \\ &= 1 + \frac{\sqrt{2}}{2}(x_1^2 + 2x_2^2 + 1) \text{ d'après (II.11a)} \\ &\geqslant 1 + \frac{\sqrt{2}}{2}(2x_1x_2\sqrt{2} + 1) \text{ d'après l'inégalité arithmético-géométrique,} \\ &= 2x_1x_2 + 1 + \frac{\sqrt{2}}{2}, \end{aligned}$$

ce qui est clairement faux.

Pour (II.12), on raisonne aussi par l'absurde et on suppose que le système admet une solution $(x_1, x_2, y_1, y_2) \in \mathbf{Z}^4$. Alors, d'après (II.12a), x_1 est impair, donc $x_1^2 \equiv 1 \pmod 8$. En évaluant (II.12a) modulo 4, on en déduit que x_2 est pair.

Ainsi, en évaluant (II.12a) modulo 8, on trouve que y_1y_2 est pair. Or (II.12b) implique que y_1 est impair, donc y_2 est pair.

On utilise l'imparité de y_1 et la parité de y_2 pour évaluer (II.12b) modulo 4, on trouve $2x_1x_2 \equiv 2 \pmod 4$, donc $x_1x_2 \equiv 1 \pmod 2$. C'est incompatible avec le fait que x_2 est pair.

□

Corollaire 5.16. *Toute unité de L_{2p^2} est congrue à 1 modulo $\sqrt{2}$.*

Démonstration. D'après la proposition 5.15, toute unité u de L_{2p^2} est de la forme $u = \pm{\varepsilon^*}^m{\varepsilon_0}^n$, avec $m, n \in \mathbf{Z}$. Or $\varepsilon^* = \sqrt{2} - 1 \equiv 1 \pmod{\sqrt{2}}$ et on va prouver que $\varepsilon_0 \equiv 1 \pmod{\sqrt{2}}$, cela nous donnera facilement le résultat.

Par définition de ε_0, $\mathbf{N}_{L/K}(\varepsilon_0) = 1$. Si on note

$$\varepsilon_0 = x_1 + x_2\sqrt{2} + (y_1 + y_2\sqrt{2})\sqrt[4]{2p^2},$$

où x_1, x_2, y_1 et y_4 sont entiers, cela fournit le système d'équations suivant.

$$\begin{cases} x_1^2 + 2x_2^2 - 4py_1y_2 = 1 & \text{(II.13a)} \\ 2x_1x_2 - py_1^2 - 2py_2^2 = 0 & \text{(II.13b)} \end{cases}$$

Ainsi, (II.13a) montre que x_1 est impair et (II.13b) prouve que y_1 est pair. Par conséquent, $\varepsilon_0 \equiv 1 \pmod{\sqrt{2}}$.

□

5.2.6 Raisonnements généraux

Dans ce paragraphe, on élimine tous les cas sauf un nombre fini d'entre eux.

Proposition 5.17. *Soit p un nombre premier tel que $p \equiv 3 \pmod 8$. Alors L_{2p^2} n'est pas euclidien par rapport à la norme.*

Démonstration. Par l'absurde, supposons que L_{2p^2} est euclidien pour la norme. Posons $K = \mathbf{Q}(\sqrt{2})$. Notons $\gamma = \sqrt{2}$, $I = \gamma \mathbf{Z}_{L_{2p^2}}$ et $\alpha = 1 + \sqrt[4]{2p^2}$. On peut effectuer la division euclidienne de α par γ, il existe ainsi $\beta \in \mathbf{Z}_{L_{2p^2}}$ tel que

$$\beta \equiv \alpha \pmod I \qquad \text{et} \qquad \left|\mathbf{N}_{L_{2p^2}/\mathbf{Q}}(\beta)\right| < \left|\mathbf{N}_{L_{2p^2}/\mathbf{Q}}(\gamma)\right| = 4. \tag{II.14}$$

Alors d'après le lemme 5.4 (2), $\mathbf{N}_{L_{2p^2}/\mathbf{Q}}(\beta) \equiv 1 \pmod 2$. Dès lors, (II.14) nous donne $\mathbf{N}_{L_{2p^2}/\mathbf{Q}}(\beta) \in \{\pm 1, \pm 3\}$. Mais il n'existe pas d'élément de norme ± 3 dans K, donc $\mathbf{N}_{L_{2p^2}/\mathbf{Q}}(\beta) \in \{\pm 1\}$ et ainsi $\beta \in \mathbf{Z}_{L_{2p^2}}^{\times}$.

Or, d'après le corollaire 5.16, toute unité de L_{2p^2} est congrue à 1 modulo $\sqrt{2}$, donc

$$\beta \equiv 1 \pmod I.$$

D'après (II.14), cela implique que $\alpha - 1 = \sqrt[4]{2p^2} \in I$, ce qui est faux. Cela fournit une contradiction et achève la preuve. □

Remarque 5.18. En fait, comme ± 7 ne peuvent être obtenues comme normes d'éléments de $\mathbf{Z}_K$, on peut conclure que $M(L_{2p^2}) \geqslant m_{L_{2p^2}}\left(\frac{\alpha}{\gamma}\right) \geqslant \frac{7}{4}$. Cette borne est atteinte pour $p = 3$: grâce à l'algorithme 4.1, on trouve $M(L_{18}) = \frac{7}{4}$.

Proposition 5.19. *Soit p un nombre premier, $p \equiv 5 \pmod 8$ et $p = 101$ ou $p > 109$. Alors ni L_p ni L_{4p} ne sont euclidiens par rapport à la norme.*

Démonstration. On note $K = \mathbf{Q}\left(\sqrt{p}\right)$ et $L = L_p$ ou L_{4p}. Le lemme 5.12 montre que p est totalement ramifié dans L. D'après le lemme 5.6 (1), il existe des entiers naturels r, s, t et u tels que $p = rs + tu$, $(r, s) = (t, u) = 1$ et $\left(\frac{r}{p}\right) = \left(\frac{s}{p}\right) = \left(\frac{t}{p}\right) = -1$. Cela implique que $\left(\frac{-tu}{p}\right) = \left(\frac{rs}{p}\right) = 1$. Ainsi, on a aussi $\left(\frac{-u}{p}\right) = -1$. Par ailleurs, comme $\left(\frac{-1}{p}\right)_4 = -1$, on a $\left(\frac{rs}{p}\right)_4 = 1$ ou $\left(\frac{tu}{p}\right)_4 = 1$ d'après le lemme 5.10. Quitte à échanger rs et tu, on peut supposer que $\left(\frac{rs}{p}\right)_4 = 1$. Notons alors $a = rs$ et $b = tu$.

D'après le lemme 5.10, a est une puissance quatrième modulo p, mais ni a, ni $-b$ ne sont des normes d'éléments de $\mathbf{Z}_L$. Pour voir cela, on note que ce ne sont pas des normes d'éléments de $\mathbf{Z}_K$ d'après le lemme 5.7.

Ainsi, d'après le lemme 5.5, L n'est pas euclidien par rapport à la norme. □

Proposition 5.20. *Soit p un nombre premier, $p \equiv 3 \pmod 8$ et $p \neq 3$. Alors L_{2p} et L_{8p} ne sont pas euclidiens par rapport à la norme.*

Démonstration. On note $K = \mathbf{Q}\left(\sqrt{2p}\right)$ et $L = L_{2p}$ ou L_{8p}. Le lemme 5.12 montre que 2 et p sont totalement ramifiés dans L.

D'après le lemme 5.6 (2), il existe deux entiers naturels a et b tels que $2p = a + b$, $a \equiv 5 \pmod 8$ et $\left(\frac{a}{p}\right) = 1$. Ainsi, a est un carré modulo p et c'est aussi une puissance quatrième modulo p d'après le lemme 5.9. Le lemme 5.11 permet même de conclure que c'est une puissance quatrième modulo $2p$.

Par ailleurs, a n'est pas une norme de $\mathbf{Z}_K$ car $a \equiv 5 \pmod 8$ et $-b$ non plus, car $-b \equiv -1 \pmod 8$.

Donc, d'après le lemme 5.5, L n'est pas euclidien par rapport à la norme. □

Proposition 5.21. *Soit p un nombre premier, $p \equiv 3 \pmod 8$ et $p > 19$. Alors L_p et L_{4p} ne sont pas euclidiens par rapport à la norme.*

Démonstration. On note $K = \mathbf{Q}\left(\sqrt{p}\right)$ et $L = L_p$ ou L_{4p}.

D'après le lemme 5.6 (3), il existe deux entiers naturels a et b tels que $p = a + b$, $a \equiv 2 \pmod 8$ et $\left(\frac{a}{p}\right) = 1$. Ainsi, a est un carré modulo p, et même une puissance quatrième (lemme 5.9).

Par ailleurs, ni a, ni $-b$ ne peuvent être normes d'éléments de $\mathbf{Z}_K$ car $a \equiv 2 \mod 8$ et $-b \equiv -1 \pmod 8$.

Donc, d'après le lemme 5.5, L n'est pas euclidien par rapport à la norme. □

Proposition 5.22. *Soit p un nombre premier, $p \equiv 7 \pmod 8$ et $p > 7$. Alors L_{4p} n'est pas euclidien par rapport à la norme.*

Démonstration. On note $K = \mathbf{Q}\left(\sqrt{p}\right)$ et $L = L_{4p}$.

D'après le lemme 5.6 (3), il existe deux entiers naturels a et b tels que $p = a + b$, $a \equiv -2 \pmod 8$ et $\left(\frac{a}{p}\right) = 1$. D'après le lemme 5.9, a est une puissance quatrième modulo p.

Ni a, ni $-b$ ne sont des normes d'éléments de $\mathbf{Z}_K$ car $a \equiv -2 \pmod 8$ et $-b \equiv -1 \pmod 8$.

On conclut avec le lemme 5.5. □

En combinant la proposition 5.3 et les propositions précédentes pour éliminer tous les cas sauf un nombre fini, on obtient le résultat suivant.

Corollaire 5.23. *Si L est un corps quartique pur euclidien pour la norme, alors $L = \mathbf{Q}(\sqrt[4]{m})$ où m est l'une des valeurs suivantes :*

- 2,
- p *où* $p \in \{3, 5, 11, 13, 19, 29, 37, 53, 61, 109\}$,
- $4p$ *où* $p \in \{3, 5, 7, 11, 13, 19, 29, 37, 53, 61, 109\}$,
- 6,
- 24.

L'objet des paragraphes suivants va être de traiter ces valeurs de m.

5.2.7 Utilisation de l'algorithme

Pour les petites valeurs de m, on peut calculer $M(L_m)$ par l'algorithme 4.1. Dans la table II.3, nous recensons les valeurs obtenues. Les cas euclidiens pour la norme sont en gras. Tous les corps considérés sont principaux sauf L_7.

m	**2**	**3**	**5**	6	7	11	**12**	13	18	**20**	24	28	44
$M(L_m)$	$\frac{1}{2}$	$\frac{11}{12}$	$\frac{5}{16}$	$\frac{23}{16}$	$\frac{27}{14}$	$\frac{125}{44}$	$\frac{1}{2}$	1	$\frac{7}{4}$	$\frac{11}{16}$	$\frac{9}{7}$	$\frac{47}{16}$	$\frac{49}{22}$

TABLE II.3 – Calcul de quelques valeurs de $M(L_m)$.

5.2.8 Utilisation d'un idéal

L'idée est de choisir un idéal I de norme $\mathbf{N}I$, vérifiant les hypothèses du lemme 5.4 (2) et tel que $I \cap \mathbf{Z} = n\mathbf{Z}$. Si on trouve $\alpha \in \mathbf{Z}_{L_m}$ tel qu'il n'existe aucun $\beta \in \mathbf{Z}_{L_m}$ vérifiant

$$\mathbf{N}_{L_m/\mathbf{Q}}(\beta) \equiv \mathbf{N}_{L_m/\mathbf{Q}}(\alpha) \pmod{n} \qquad \text{et} \qquad \left|\mathbf{N}_{L/\mathbf{Q}}(\beta)\right| < \mathbf{N}I, \tag{II.15}$$

alors L_m n'est pas euclidien pour la norme. Pour avoir une chance d'exploiter (II.15), il faut que n soit de l'ordre de $\mathbf{N}I$.

Par exemple, pour $m = 19$, il existe un unique idéal I de norme 38 dans $\mathbf{Z}_{L_{19}}$. En notant $x = \sqrt[4]{19}$, c'est $I = 38\mathbf{Z} + \mathbf{Z}x + \mathbf{Z}x^2 + \mathbf{Z}x^3$. Ainsi $I \cap \mathbf{Z} = 38\mathbf{Z}$, donc $n = 38$. De plus si prend $\alpha = 3$, alors $\mathbf{N}_{L_{19}/\mathbf{Q}}(\alpha) \equiv 5 \pmod{38}$, mais ni 5 ni -33 ne sont normes d'éléments de $\mathbf{Z}_{L_{19}}$, donc L_{19} n'est pas euclidien pour la norme.

La table II.4 montre dans quels autres cas on peut utiliser ce raisonnement.

p	m	$\mathbf{N}I$	n	α
19	19	38	38	3
	76	38	38	5
29	29	29	29	4
53	53	53	53	8
	212	212	106	35
61	244	244	122	28
109	109	109	109	5
	436	436	218	82

TABLE II.4 – Idéaux utilisés pour prouver le caractère non euclidien grâce à (II.15). Pour chaque valeur de m, I est l'unique idéal de norme donnée.

5.2.9 Utilisation d'un corps intermédiaire

L'idée générale est similaire, mais on va obtenir des propriétés plus précises grâce au corps intermédiaire $K = \mathbf{Q}\left(\sqrt{m}\right)$.

Proposition 5.24. *L_{37} et L_{148} ne sont pas euclidiens pour la norme.*

Démonstration. On note $L = L_{37}$ et $K = \mathbf{Q}\left(\sqrt{37}\right)$. On suppose que L est euclidien pour la norme. L'idéal $2\mathbf{Z}_K$ est totalement ramifié dans L/K. On note B un élément au-dessus de $2\mathbf{Z}_K$ tel que $\mathbf{N}_{L/K}(B)\mathbf{Z}_K = 2\mathbf{Z}_K$. Alors on peut faire la division euclidienne de $x = \frac{5+\sqrt{37}}{2}$ par B : il existe $r \equiv x \pmod{B\mathbf{Z}_L}$ tel que $\left|\mathbf{N}_{L/\mathbf{Q}}(r)\right| < 4$.

Comme $2\mathbf{Z}_K$ est totalement ramifié, d'après le lemme 5.4 (1), on a

$$\mathbf{N}_{L/K}(r) \equiv \mathbf{N}_{L/K}(x) \pmod{2\mathbf{Z}_K},$$

ce qui donne $\mathbf{N}_{L/K}(r) \equiv \frac{5-\sqrt{37}}{2} \pmod{2\mathbf{Z}_K}$. Or une unité fondamentale de K est $u = \sqrt{37} - 6$, elle vérifie $u \equiv 1 \pmod{2\mathbf{Z}_K}$. Par conséquent, toute unité de $\mathbf{Z}_K$ est congrue à 1 modulo $2\mathbf{Z}_K$ et $\mathbf{N}_{L/K}(r) \notin \mathbf{Z}_K^\times$. Dès lors,

$$\mathbf{N}_{L/\mathbf{Q}}(r) = \pm 3.$$

Mais on connaît tous les éléments de $\mathbf{Z}_K$ dont la norme vaut ± 3, on peut par exemple les calculer grâce à PARI ([PAR12]). Ainsi, $\mathbf{N}_{L/K}(r) \in \frac{5-\sqrt{37}}{2}\mathbf{Z}_K^\times \cup \frac{5+\sqrt{37}}{2}\mathbf{Z}_K^\times$. Le second cas est impossible car $\mathbf{N}_{L/K}(r) \equiv \frac{5-\sqrt{37}}{2} \pmod{2\mathbf{Z}_K}$ et tout élément de $\mathbf{Z}_K^\times$ est congru à 1 modulo $2\mathbf{Z}_K$. Dès lors, en tant qu'idéaux de $\mathbf{Z}_L$,

$$(\mathbf{N}_{L/K}(r)) = \left(\frac{5-\sqrt{37}}{2}\right).$$

Mais l'idéal $\left(\frac{5-\sqrt{37}}{2}\right)$ est premier dans L, ce qui fournit une contradiction et qui montre que $L = L_{37}$ n'est pas euclidien pour la norme.

Pour $L = L_{148}$, on fait le même raisonnement en prenant $x = \frac{5-\sqrt{37}}{2}$. Avec les mêmes notations, on obtient $\mathbf{N}_{L/K}(r) \equiv \frac{5+\sqrt{37}}{2} \pmod{2\mathbf{Z}_K}$. Par conséquent, en tant qu'idéaux de $\mathbf{Z}_L$,

$$(\mathbf{N}_{L/K}(r)) = \left(\frac{5+\sqrt{37}}{2}\right),$$

ce qui est faux car $\left(\frac{5+\sqrt{37}}{2}\right)$ est premier dans L. Cela fournit une contradiction et montre que $L = L_{148}$ n'est pas euclidien pour la norme. □

5.2.10 Donnée d'un point critique

Étant donné un point $\xi \in L_m$, on peut calculer directement $m_{L_m}(\xi)$ par l'algorithme 3.1.

Ainsi, pour $\xi = \frac{\theta^2+4\theta+2}{8}$, où $\theta = \sqrt[4]{52}$, on trouve $m_{L_{52}} = \frac{17}{16}$, donc L_{52} n'est pas euclidien pour la norme.

De même, pour $\xi = \frac{\theta^3+\theta^2-2\theta-2}{8}$, où $\theta = \sqrt[4]{116}$, on trouve $m_{L_{116}}(\xi) = \frac{29}{16}$, ce qui montre que L_{116} n'est pas euclidien pour la norme.

5.2.11 Bilan

Nous avons étudié L_m pour les valeurs m du corollaire 5.23 à l'exception de $m = 61$. Nous avons obtenu que L_m est euclidien pour la norme pour $m \in \{2, 3, 5, 12, 20\}$ et non euclidien pour la norme pour les autres valeurs. Cela achève la preuve du théorème 5.2.

5.3 Corps cyclotomiques

Avec l'algorithme, on peut calculer quelques valeurs de minimum euclidien de corps cyclotomiques inconnues jusqu'à présent. Soit n un entier strictement positif tel que $n \not\equiv 2 \pmod 4$, on note $K_n := \mathbf{Q}(\zeta_n)$ où ζ_n est une racine primitive n^{e} de l'unité.

n	1	3	4	***5***	***7***	8	***9***	12	***15***	***16***	***20***	***24***
$M(K_n)$	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{2}$	$\mathbf{\frac{1}{5}}$	$\mathbf{\frac{1}{7}}$	$\frac{1}{2}$	$\mathbf{\frac{1}{3}}$	$\frac{1}{4}$	$\mathbf{\frac{1}{16}}$	$\mathbf{\frac{1}{2}}$	$\mathbf{\frac{1}{5}}$	$\mathbf{\frac{1}{4}}$

TABLE II.5 – Minima euclidiens de quelques corps cyclotomiques.

La table II.5 liste toutes les valeurs connues de $M(K_n)$. Elles correspondent aux cas où le polynôme cyclotomique est de degré au plus 8. Dans tous ces cas, le minimum euclidien coïncide avec $\frac{1}{\Lambda(K)}$. Les valeurs en gras étaient inconnues jusqu'à présent.

5.4 Minima successifs

Définition 5.25. On peut définir les minima euclidiens et inhomogènes suivants. Si on pose $M_1(K) = M_1(\overline{K}) = M(K) = M(\overline{K})$, alors on définit par récurrence sur $p > 1$ les p^{e} minima euclidien et inhomogène respectivement par

$$\begin{cases} M_p(K) = \sup\left\{m_K(\xi),\ \xi \in K,\ m_K(\xi) < M_{p-1}(K)\right\}, \\ M_p\left(\overline{K}\right) = \sup\left\{m_{\overline{K}}(x),\ x \in H,\ m_{\overline{K}}(x) < M_{p-1}\left(\overline{K}\right)\right\}. \end{cases}$$

Comme pour le premier minimum, ces deux notions sont étroitement liées dans la plupart des cas (voir [Cer06]).

Théorème 5.26. *Si $r > 1$ et K n'est pas CM, alors, pour tout $p > 0$,*

1. $M_p(K) = M_p\left(\overline{K}\right) \in \mathbf{Q}$,
2. $M_{p+1}(K) < M_p(K)$,
3. *en particulier, $M(\overline{K})$ est isolé, c'est-à-dire que $M_2\left(\overline{K}\right) < M\left(\overline{K}\right)$.*
4. $\lim\limits_{p\to+\infty} M_p(K) = 0$.

Si $r = 1$, on conjecture que (3) est aussi vérifiée. Avec l'algorithme 4.1, on peut chercher à calculer $M_p(K)$ pour certaines valeurs $p > 0$. Pour y parvenir, on choisit k tel que $0 < k < M_p(K)$. Si l'exécution de l'algorithme est fructueuse, on peut trouver un graphe convenable, duquel on déduit tous les points $x \in K$ tels que $m_K(x) \geqslant k$ (grâce au théorème 3.17).

Exemple 5.27. Considérons le corps cubique complexe $K = \mathbf{Q}(x)$ où $x = \sqrt[3]{-7}$. On applique l'algorithme 4.1 pour $k = 2{,}39$. On obtient les trois orbites suivantes de points critiques.

- $\mathcal{O}_1 = \left\{\frac{2}{5}x^2 + \frac{1}{5}x - \frac{2}{5}, \frac{3}{5}x^2 + \frac{4}{5}x - \frac{3}{5}\right\}$ de minimum $\frac{12}{5}$,
- $\mathcal{O}_2 = \left\{\frac{11}{20}x^2 + \frac{13}{20}x - \frac{1}{20}, \frac{9}{20}x^2 + \frac{7}{20}x + \frac{1}{20}\right\}$ de minimum $\frac{49}{20}$,
- $\mathcal{O}_3 = \left\{\frac{1}{2}x^2 + \frac{1}{2}x - \frac{1}{2}\right\}$ de minimum $\frac{5}{2}$.

Dès lors, $M(K) = M\left(\overline{K}\right) = \frac{5}{2}$, $M_2(K) = \frac{49}{20}$, $M_3(K) = \frac{12}{5}$.

Exemple 5.28. Soit $K = \mathbf{Q}(x)$ où x est une racine de $X^3 - X^2 - 4X + 12$. Alors $\mathrm{disc}_K = -676$, $r_1 = r_2 = 1$. Avec l'algorithme 4.1, on obtient les orbites de points $t \in K$ tels que $m_K(t) \geqslant 1$.

- $\mathcal{O}_1 = \left\{\frac{1}{4}x^2 + \frac{1}{2}x - 1, \frac{1}{4}x^2 + x - 1\right\}$ de minimum 1,
- $\mathcal{O}_2 = \left\{\frac{1}{2}x + \frac{1}{2}, \frac{1}{4}x^2 + \frac{3}{4}x - 1\right\}$ de minimum 1,
- $\mathcal{O}_3 = \left\{\frac{1}{4}x^2 + \frac{3}{4}x - \frac{1}{2}\right\}$ de minimum $\frac{7}{4}$,
- $\mathcal{O}_4 = \left\{\frac{1}{4}x^2 + \frac{1}{4}x - \frac{1}{2}\right\}$ de minimum $\frac{7}{4}$,
- $\mathcal{O}_5 = \left\{\frac{1}{2}x\right\}$ de minimum 1.

Par conséquent, $M(K) = M\left(\overline{K}\right) = \frac{7}{4}$, $M_2(K) = 1$. Cet exemple montre qu'on peut avoir des orbites différentes possédant le même minimum euclidien.

5.5 Corps de nombres principaux non euclidiens pour la norme

Pour les petits degrés, on peut calculer de très nombreuses valeurs de minima euclidiens de corps de petits discriminants. Cela nous permet de trouver des corps de nombres principaux qui ne sont pas euclidiens pour la norme. Ici, on établit une liste de tels corps de nombres dans la table II.6. En fait, si la signature est différente de $(6, 0)$, $(4, 1)$ et $(2, 2)$, alors la table fournit un tel corps de nombres de plus petit discriminant (en valeur absolue).

Par conséquent, tous les corps de nombres principaux de telle signature et dont le discriminant est strictement inférieur au discriminant donné (en valeur absolue) sont en fait euclidiens pour la norme.

5.6 Corps de nombres dont le rang des unités et le minimum euclidien sont égaux à 1

Si on suppose que la signature de K est $(r_1, r_2) \notin \{(1, 1), (0, 2)\}$, alors $M(K) = 1$ implique que K n'est pas euclidien pour la norme (voir proposition 2.8 et théorème 2.9). Dans les autres cas, on peut trouver certains corps de nombres dont le minimum euclidien vaut 1. Ils sont tous non euclidiens pour la norme.

Exemple 5.29. Les corps cubiques non totalement réels de discriminant -199, -335, -351, -367, -743, -755 ont un minimum euclidien égal à 1. Il existe aussi des corps de nombres de signature $(0, 2)$ et de minimum euclidien égal à 1, on peut par exemple citer tous les corps de telle signature et de discriminant

$$1436, 1521, 1805, 1872, 2089, 2213, 2448, 2557, 2624, 2677, 2704, 2873, 2925, \ldots$$

n	(r_1, r_2)	un polynôme minimal $K = \mathbf{Q}(x)$	disc_K	$M(K)$	point(s) critique(s)
2	$(2,0)$	$x^2 - 53$	53	$\frac{9}{7}$	$\left\{\frac{2x+3}{7}, \frac{3x+1}{14}\right\}$
	$(0,1)$	$x^2 + 19$	-19	$\frac{25}{19}$	$\left\{\frac{5}{19}x, \frac{14}{19}x\right\}$
3	$(3,0)$	$x^3 - x^2 - 6x + 1$	985	1	$\left\{\frac{2x^2+x+2}{5}, \frac{3x^2+4x+3}{5}\right\}$
	$(1,1)$	$x^3 - x^2 + 4x - 1$	-199	1	$\left\{\frac{3x^2+x+4}{7}, \frac{4x^2+6x+3}{7}\right\}$
4	$(4,0)$	$x^4 - 12x^2 + 18$	18 432	$\frac{7}{4}$	$\left\{\frac{x^3+x^2}{6}\right\}$
	$(2,1)$	$x^4 - x^3 - 5x + 1$	$-4\,564$	1	$\left\{\frac{x^2+x+1}{2}\right\}$
	$(0,2)$	$x^4 - 4x^2 + 5$	1 280	$\frac{5}{4}$	$\left\{\frac{x^3+x}{2}\right\}$
5	$(5,0)$	$x^5 - 10x^3 - 5x^2 + 10x - 1$	390 625	$\frac{7}{5}$	$\left\{\frac{3x^4+3x^3+3x^2+3x+3}{5}, \frac{9x^4+29x^3+19x^2+24x+4}{35}\right\}$
	$(3,1)$	$x^5 - x^4 - 4x^3 + 6x^2 + 3x - 7$	$-156\,848$	$\frac{5}{4}$	$\left\{\frac{x^4+x^3+x^2+x}{2}\right\}$
	$(1,2)$	$x^5 + 2x^3 - x^2 + 2x + 1$	36 025	1	$\left\{\frac{2x^4+2x^3+x^2+4x+3}{5}, \frac{3x^4+3x^3+4x^2+x+2}{5}\right\}$
6	$(6,0)$	$x^6 - 12x^4 - 2x^3 + 36x^2 + 12x - 20$	108 020 304	$\frac{16}{9}$	$\left\{\frac{x^5+2x^3+2x^2+1}{3}, \frac{x^5+2x^3+2x^2+4}{6}\right\}$
	$(4,1)$	$x^6 - 2x^5 - 9x^4 + 18x^3 + 13x^2 - 48x + 17$	$-10\,163\,456$	$\frac{5}{4}$	$\left\{\frac{17x^5+6x^4+12x^3+6x^2+17x+16}{18}\right\}$
	$(2,2)$	$x^6 - 2x^5 - 4x^4 + 6x^3 + 6x^2 + 11x - 27$	1 281 013	1	$\left\{\frac{59x^5+14x^4+53x^3+4x^2+30x+56}{69}, \frac{56x^5+9x^4+62x^3+42x^2+7x+13}{69}\right\}$
	$(0,3)$	$x^6 + x^4 - x^3 + 2x^2 + x + 1$	$-165\,611$	1	$\left\{\frac{3x^5+2x^4+x^3+x^2+3}{5}, \frac{2x^5+3x^4+4x^3+4x^2+3}{5}\right\}$

TABLE II.6 – Corps de nombres principaux et non euclidiens pour la norme de petit discriminant pour une signature donnée. Tous les corps de nombres listés ici admettent une unique orbite critique.

5.7 Euclidianité en deux étapes et euclidianité généralisée

Plusieurs notions ont été introduites pour généraliser l'euclidianité. Dans ce paragraphe, nous présentons deux d'entre elles et nous montrons comment l'algorithme 4.1 peut nous aider à les appréhender.

5.7.1 Euclidianité en deux étapes

Cette généralisation de l'euclidianité a été introduite par Cooke dans [Coo76a] et [Coo76b].

Définition 5.30. On dit que $\mathbf{Z}_K$ est *euclidien en deux étapes pour la norme* si pour tout couple $(\alpha, \beta) \in \mathbf{Z}_K \times \mathbf{Z}_K \setminus \{0\}$, il existe $(\gamma_1, \gamma_2, \delta_1, \delta_2) \in \mathbf{Z}_K^4$ tel que

$$\begin{cases} \alpha - \beta\gamma_1 & = & \delta_1, \\ \beta - \delta_1\gamma_2 & = & \delta_2, \\ \left|\mathbf{N}_{K/\mathbf{Q}}(\delta_2)\right| & < & \left|\mathbf{N}_{K/\mathbf{Q}}(\beta)\right|. \end{cases}$$

On remarque que si K est euclidien pour la norme, alors il est euclidien en deux étapes pour la norme. En effet, si β, $\gamma \in \mathbf{Z}_K$ sont tels que $\alpha - \beta\gamma = \delta$ et $\left|\mathbf{N}_{K/\mathbf{Q}}(\delta)\right| < \left|\mathbf{N}_{K/\mathbf{Q}}(\beta)\right|$, alors on a la division en deux étapes suivante :

$$\left\{\begin{array}{rcl} \alpha - \beta(\gamma+1) & = & \delta - \beta, \\ \beta - (\delta-\beta)\cdot(-1) & = & \delta. \end{array}\right.$$

Par ailleurs, tout corps de nombre euclidien en deux étapes pour la norme est principal.

Lemme 5.31. *Pour montrer qu'un corps de nombres est euclidien en deux étapes pour la norme, il suffit de*

- *calculer tous les points $x \in K$ modulo $\mathbf{Z}_K$ tels que $m_K(x) \geqslant 1$,*
- *choisir un de ces points $x = \frac{\alpha}{\beta}$ où $(\alpha, \beta) \in \mathbf{Z}_K \times \mathbf{Z}_K \setminus \{0\}$ par orbite et trouver une division euclidienne en deux étapes pour (α, β). L'existence d'une telle division euclidienne est indépendante du choix de x dans une orbite donnée et de (α, β).*

Démonstration. Soient $(\alpha, \beta) \in \mathbf{Z}_K \times \mathbf{Z}_K \setminus \{0\}$ et $(\alpha', \beta') \in \mathbf{Z}_K \times \mathbf{Z}_K \setminus \{0\}$ tels que $\frac{\alpha}{\beta} = \frac{\alpha'}{\beta'}$. Supposons que (α, β) admet une division en deux étapes, c'est-à-dire qu'il existe $(\gamma_1, \gamma_2, \delta_1, \delta_2) \in \mathbf{Z}_K^4$ tel que

$$\left\{\begin{array}{rcl} \alpha - \beta\gamma_1 & = & \delta_1, \\ \beta - \delta_1\gamma_2 & = & \delta_2, \\ \left|\mathbf{N}_{K/\mathbf{Q}}(\delta_2)\right| & < & \left|\mathbf{N}_{K/\mathbf{Q}}(\beta)\right|. \end{array}\right.$$

En multipliant les deux premières lignes par $\frac{\beta'}{\beta}$ et la troisième par $\left|\mathbf{N}_{K/\mathbf{Q}}\left(\frac{\beta'}{\beta}\right)\right|$, on obtient

$$\left\{\begin{array}{rcl} \alpha' - \beta'\gamma_1 & = & \frac{\beta'}{\beta}\delta_1, \\ \beta' - \frac{\beta'}{\beta}\delta_1\gamma_2 & = & \frac{\beta'}{\beta}\delta_2, \\ \left|\mathbf{N}_{K/\mathbf{Q}}\left(\frac{\beta'}{\beta}\delta_2\right)\right| & < & \left|\mathbf{N}_{K/\mathbf{Q}}(\beta')\right|. \end{array}\right.$$

Il s'agit d'une division en deux étapes pour (α', β') car $\frac{\beta'}{\beta}\delta_1 = \alpha' - \beta'\gamma_1 \in \mathbf{Z}_K$, ce qui implique que $\frac{\beta'}{\beta}\delta_2 = \beta' - \frac{\beta'}{\beta}\delta_1\gamma_2 \in \mathbf{Z}_K$. Ainsi, l'existence d'une division en deux étapes pour (α, β) ne dépend que de $\frac{\alpha}{\beta}$.

Soient $(\alpha, \beta) \in \mathbf{Z}_K \times \mathbf{Z}_K \setminus \{0\}$, $\varepsilon \in \mathbf{Z}_K^\times$ et $z \in \mathbf{Z}_K$. Il suffit de voir que (α, β) admet une division en deux étapes si et seulement si $(\varepsilon\cdot\alpha - \beta z, \beta)$ admet une division en deux étapes. Une fois que l'on aura montré cette propriété, on saura que l'existence d'une division en deux étapes pour (α, β) dépend seulement de l'orbite de $\frac{\alpha}{\beta}$ modulo $\mathbf{Z}_K$.

Supposons donc que (α, β) admet une division en deux étapes, c'est-à-dire qu'il existe $(\gamma_1, \gamma_2, \delta_1, \delta_2) \in \mathbf{Z}_K^4$ tel que

$$\left\{\begin{array}{rcl} \alpha - \beta\gamma_1 & = & \delta_1, \\ \beta - \delta_1\gamma_2 & = & \delta_2, \\ \left|\mathbf{N}_{K/\mathbf{Q}}(\delta_2)\right| & < & \left|\mathbf{N}_{K/\mathbf{Q}}(\beta)\right|. \end{array}\right.$$

Alors on obtient une division en deux étapes pour $(\varepsilon\cdot\alpha - \beta z, \beta)$ sous la forme :

$$\left\{\begin{array}{rcl} \varepsilon\cdot\alpha - \beta z - \beta(\varepsilon\gamma_1 + z) & = & \varepsilon\delta_1, \\ \beta - \varepsilon\delta_1\varepsilon^{-1}\gamma_2 & = & \delta_2, \\ \left|\mathbf{N}_{K/\mathbf{Q}}(\delta_2)\right| & < & \left|\mathbf{N}_{K/\mathbf{Q}}(\beta)\right|. \end{array}\right.$$

□

Exemples 5.32. – $K = \mathbf{Q}(s)$ où s est une racine $X^3 - X^2 + 3X + 2$. Alors $\mathrm{disc}_K = -307$ et pour $t \in K$, $m_K(t) \geqslant 1$ si et seulement si $t \equiv \frac{1}{2}s^2 + \frac{1}{2} \pmod{\mathbf{Z}_K}$. On pose $x = \frac{s^2+1}{2}$ et on a

$$\begin{cases} s^2 + 1 - 2(-s) & = & (s+1)^2, \\ 2 - (s+1)^2 \cdot (s^2 - 5s + 6) & = & 8s^2 - 11s - 8, \\ \left|\mathbf{N}_{K/\mathbf{Q}}(8s^2 - 11s - 8)\right| = 2 & < & 8 = \left|\mathbf{N}_{K/\mathbf{Q}}(2)\right|. \end{cases}$$

Cela prouve que K est euclidien en deux étapes pour la norme.

– $K = \mathbf{Q}(s)$ où s est une racine de $X^4 - 4X^2 + 5$. Alors $\mathrm{disc}_K = 1280$ et pour $t \in K$, $m_K(t) \geqslant 1$ si et seulement si $t \equiv \frac{1}{2}s^3 - \frac{s}{2} \pmod{\mathbf{Z}_K}$.
On prend $\alpha = s^3 - s$, $\beta = 2$, $\gamma_1 = s^3 + s^2$, $\delta_1 = -s^3 - 2s^2 - s$, $\gamma_2 = s^3 - 2s^2 - 2s + 4$ et $\delta_2 = -2s^3 - 3s^2 + 4s + 7$ pour prouver que K est euclidien en deux étapes pour la norme car $\left|\mathbf{N}_{K/Q}(-2s^3 - 3s^2 + 4s + 7)\right| = 4 < 16 = \left|\mathbf{N}_{K/\mathbf{Q}}(2)\right|$.

– $K = \mathbf{Q}(s)$ où s est une racine de $X^6 - 5X^3 + 4X + 2$. Alors $\mathrm{disc}_K = -12\,781\,568$, $M(K) = \frac{11}{8}$ et pour tout $t \in K$, $m_K(t) \geqslant 1$ si et seulement si $t \equiv \frac{s^5+s^2}{2} \pmod{\mathbf{Z}_K}$. On considère $\alpha = s^5 + s^2$, $\beta = 2$, $\gamma_1 = s^3$, $\delta_1 = s^5 - 2s^3 + s^2$, $\gamma_2 = -x^3 + 4x$, $\delta_2 = s^5 - s^4 - 4s^3 + 2s^2 + 4$. Comme $\left|\mathbf{N}_{K/\mathbf{Q}}(\delta_2)\right| = 16 < 64 = \left|\mathbf{N}_{K/\mathbf{Q}}(\beta)\right|$, on peut conclure que K est euclidien en deux étapes pour la norme.

En fait, on peut conclure plus vite si on a des propriétés particulières sur les points critiques.

Proposition 5.33. *Si K est principal, $M(K) \geqslant 1$ et si K admet une seule orbite de points critiques dont le minimum est supérieur ou égal à $\frac{1}{M(K)}$, alors K est euclidien en deux étapes pour la norme.*

Démonstration. Notons $\mathcal{O}$ l'orbite de points critiques en question et prenons $\frac{\alpha}{\beta} \in \mathcal{O}$, où $\alpha, \beta \in \mathbf{Z}_K \setminus \{0\}$ sont premiers entre eux (cette écriture est possible car K est principal). Il existe $(\gamma, \tau) \in \mathbf{Z}_K \times \mathbf{Z}_K$ tel que $\alpha - \beta\gamma = \tau$ et $\left|\mathbf{N}_{K/\mathbf{Q}}(\tau)\right| = M(K) \cdot \left|\mathbf{N}_{K/\mathbf{Q}}(\beta)\right|$. Dès lors, ou $m_K\left(\frac{\beta}{\tau}\right) < \frac{1}{M(K)} = \frac{\left|\mathbf{N}_{K/\mathbf{Q}}(\beta)\right|}{\left|\mathbf{N}_{K/\mathbf{Q}}(\tau)\right|}$ ou $m_K\left(\frac{\beta}{\tau}\right) \geqslant \frac{1}{M(K)}$.

Dans le premier cas, il existe $\gamma \in \mathbf{Z}_K$ tel que $\left|\mathbf{N}_{K/\mathbf{Q}}(\beta - \tau\gamma)\right| < \left|\mathbf{N}_{K/\mathbf{Q}}(\beta)\right|$, ce qui fournit une division euclidienne en deux étapes pour (α, β).

Dans le second cas, comme il n'existe qu'une orbite de points dont le minimum est supérieur ou égal à $\frac{1}{M(K)}$, $\frac{\beta}{\tau} \in \mathcal{O}$ et $m_K\left(\frac{\beta}{\tau}\right) = M(K)$. Par conséquent, il existe $\varepsilon \in \mathbf{Z}_K^\times$ et $z \in \mathbf{Z}_K$ tels que

$$\frac{\beta}{\tau} = \varepsilon \cdot \frac{\alpha}{\beta} - z.$$

Cela implique que β divise $\tau(\varepsilon\alpha - \beta z)$, ainsi β divise $\tau\alpha$ et donc τ. On peut alors écrire $\frac{\beta}{\tau} = \frac{1}{\kappa}$ où $\kappa \in \mathbf{Z}_K \setminus \{0\}$. Comme $\frac{\beta}{\tau} \notin \mathbf{Z}_K^\times$, on a $M(K) = m_K\left(\kappa^{-1}\right) = \frac{1}{\left|\mathbf{N}_{K/\mathbf{Q}}(\kappa)\right|} < 1$, ce qui est impossible. □

La table II.7 fournit des exemples de corps de nombres euclidiens en deux étapes pour la norme.

5.7.2 Euclidianité généralisée

Johnson, Queen et Sevilla ([JQS85]) ont proposé de généraliser l'euclidianité dans une autre direction. Leur définition est équivalente à la suivante.

n	(r_1, r_2)	polynôme minimal, $K = \mathbf{Q}(x)$	disc_K	$M(K)$	N
3	$(3,0)$	$x^3 - x^2 - 6x + 1$	985	1	1
	$(1,1)$	$x^3 - x^2 + 4x + 1$	-335	1	2
4	$(4,0)$	$x^4 - 2x^3 - 6x^2 + 3x + 5$	42 341	$\frac{7}{5}$	1
	$(2,1)$	$x^4 - x^3 + 6x^2 - x - 1$	$-5\,732$	1	1
	$(0,2)$	$x^4 - x^3 + 3x^2 + 2$	1 436	1	1
5	$(5,0)$	$x^5 - 2x^4 - 6x^3 + 7x^2 + 6x - 5$	1 719 625	1	1
	$(3,1)$	$x^5 - x^3 - 5x^2 + 7$	$-271\,292$	1	1
	$(1,2)$	$x^5 - x^4 + x^3 - 2x - 2$	37 156	1	1
6	$(6,0)$	$x^6 - 3x^5 - 11x^4 + 27x^3 + 43x^2 - 57x - 57$	115 745 625	$\frac{27}{25}$	1
	$(4,1)$	$x^6 - 5x^3 + 4x + 2$	$-12\,781\,568$	$\frac{11}{8}$	1
	$(2,2)$	$x^6 - x^4 - 3x^2 - 2$	1 465 472	1	1
	$(0,3)$	$x^6 - x^5 - 2x^4 - x^3 + 3x^2 + 2x + 2$	$-275\,560$	1	1

TABLE II.7 – Exemples de corps de nombres euclidiens pour la norme en 2 étapes. N désigne le nombre d'orbites de points de minimum euclidien supérieur ou égal à 1.

Définition 5.34. On dit K is *euclidien au sens généralisé* (on dira *G.E.* pour aller plus vite) si pour tout $(\alpha, \beta) \in \mathbf{Z}_K \times \mathbf{Z}_K \setminus \{0\}$ tel que l'idéal (α, β) est principal,

$$m_K\left(\frac{\alpha}{\beta}\right) < 1.$$

Il est immédiat d'observer qu'un corps de nombres principal K est G.E. si et seulement s'il est euclidien pour la norme. Par ailleurs, pour prouver que K est G.E. quand $\mathbf{Z}_K$ n'est pas un anneau principal, il suffit de montrer que pour tout $x = \frac{\alpha}{\beta} \in K$, où $(\alpha, \beta) \in \mathbf{Z}_K \times \mathbf{Z}_K \setminus \{0\}$, vérifiant $m_K(x) \geqslant 1$, l'idéal (α, β) n'est pas principal. En fait, la propriété suivante montre qu'il suffit de considérer certains points.

Lemme 5.35. *Pour montrer qu'un corps de nombres K est G.E., il suffit de*
- *calculer tous les points $x \in K$ modulo $\mathbf{Z}_K$ tels que $m_K(x) \geqslant 1$,*
- *choisir un de ces points $x = \frac{\alpha}{\beta}$ où $(\alpha, \beta) \in \mathbf{Z}_K \times \mathbf{Z}_K \setminus \{0\}$ par orbite modulo $\mathbf{Z}_K$ et montrer que (α, β) n'est pas principal. Cette propriété est indépendante du choix de x dans une orbite donnée et de (α, β).*

Démonstration. Soient $(\alpha, \beta) \in \mathbf{Z}_K \times \mathbf{Z}_K \setminus \{0\}$ et $(\alpha', \beta') \in \mathbf{Z}_K \times \mathbf{Z}_K \setminus \{0\}$ tels que $\frac{\alpha}{\beta} = \frac{\alpha'}{\beta'}$. Supposons que (α, β) est principal, c'est-à-dire qu'il existe $\gamma \in \mathbf{Z}_K$ tel que $\alpha\mathbf{Z}_K + \beta\mathbf{Z}_K = \gamma\mathbf{Z}_K$. En multipliant par $\frac{\beta'}{\beta}$, on a $\alpha'\mathbf{Z}_K + \beta'\mathbf{Z}_K = \frac{\beta'}{\beta}\gamma\mathbf{Z}_K$. Comme $\frac{\beta'}{\beta}\gamma\mathbf{Z}_K = \alpha'\mathbf{Z}_K + \beta'\mathbf{Z}_K \subseteq \mathbf{Z}_K$, on a $\frac{\beta'}{\beta}\gamma \in \mathbf{Z}_K$ et (α', β') est principal.

Soient $(\alpha, \beta) \in \mathbf{Z}_K \times \mathbf{Z}_K \setminus \{0\}$, $\varepsilon \in \mathbf{Z}_K^\times$ et $z \in \mathbf{Z}_K$. Il suffit de voir que (α, β) est principal si et seulement si $(\varepsilon \cdot \alpha - \beta z, \beta)$ est principal. Supposons donc que (α, β) est principal, c'est-à-dire qu'il existe $\gamma \in \mathbf{Z}_K$ tel que $\alpha\mathbf{Z}_K + \beta\mathbf{Z}_K = \gamma\mathbf{Z}_K$. Alors, en

n	(r_1, r_2)	polynôme minimal, $K = \mathbf{Q}(x)$	disc_K	$M(K)$	N	h_K
3	$(3,0)$	$x^3 - 12x - 1$	6 885	$\frac{67}{40}$	6	3
	$(1,1)$	$x^3 + 4x - 1$	-283	$\frac{3}{2}$	1	2
4	$(4,0)$	$x^4 - 9x^2 - 5x + 9$	56 025	$\frac{3}{2}$	1	2
	$(2,1)$	$x^4 - 2x^3 + 5x^2 - 2x - 1$	$-6\,848$	$\frac{4}{3}$	1	2
	$(0,2)$	$x^4 - x^3 + 4x^2 + 3x + 9$	1 521	1	1	2
5	$(5,0)$	$x^5 - 11x^3 - 9x^2 + 14x + 9$	4 010 276	$\frac{3}{2}$	1	2
	$(3,1)$	$x^5 - 2x^4 + 2x^3 - 12x^2 + 21x - 9$	-243219	1	2	2
	$(1,2)$	$x^5 - x^4 - 2x^2 + 4x - 1$	41 381	$\frac{4}{3}$	1	2
6	$(6,0)$	$x^6 - 13x^4 - 2x^3 + 21x^2 + 13x + 1$	49 744 125	$\frac{7}{3}$	1	2
	$(4,1)$	$x^6 - 3x^5 + x^4 + 3x^3 - 7x^2 + 5x + 1$	$-9\,243\,375$	$\frac{5}{3}$	2	2
	$(2,2)$	$x^6 - 3x^5 + 7x^4 - 9x^3 + 5x^2 - x - 1$	1 856 465	1	3	2
	$(0,3)$	$x^6 - 2x^5 + 3x^4 + 4x^2 + 2x + 1$	$-392\,000$	1	3	2

TABLE II.8 – Exemples de corps nombres G.E. non principaux. N désigne le nombre d'orbites dont le minimum est supérieur ou égal à 1.

multipliant par ε, on trouve $\varepsilon \cdot \alpha\mathbf{Z}_K + \beta \cdot \varepsilon\mathbf{Z}_K = \gamma \cdot \varepsilon\mathbf{Z}_K$. Comme $\varepsilon\mathbf{Z}_K = \mathbf{Z}_K$, on obtient $\varepsilon \cdot \alpha\mathbf{Z}_K + \beta\mathbf{Z}_K = \gamma\mathbf{Z}_K$. Dès lors, $(\varepsilon \cdot \alpha - \beta z)\mathbf{Z}_K + \beta\mathbf{Z}_K = \gamma\mathbf{Z}_K$. Ainsi, $(\varepsilon \cdot \alpha - \beta z, \beta)$ est un idéal principal. □

Exemple 5.36. $K = \mathbf{Q}(x)$ où $x^4 - 2x^3 + 3x^2 + 8x - 14 = 0$, $\mathrm{disc}_K = -11\,200$, $r_1 = 2$, $r_2 = 1$, $\mathrm{h}_K = 2$. Pour tout $\xi \in K$, on a $m_K(\xi) \geqslant 1$ si et seulement si $\xi \equiv \frac{\alpha}{\beta} \pmod{\mathbf{Z}_K}$ ou $\xi \equiv \frac{\alpha'}{\beta} \pmod{\mathbf{Z}_K}$ où $\alpha, \alpha', \beta \in \mathbf{Z}_K$ sont définis par

$$\alpha = \frac{1}{8}x^3 - \frac{7}{8}x^2 - \frac{1}{4}x + \frac{5}{4},\ \alpha' = \frac{1}{4}x^3 - \frac{3}{4}x^2 - \frac{1}{2}x + \frac{3}{2} \text{ and } \beta = \frac{1}{8}x^3 + \frac{1}{8}x^2 - \frac{1}{4}x - \frac{3}{4}.$$

Ni (α, β), ni (α', β) ne sont principaux, donc K est G.E..

On peut trouver d'autres exemples de corps de nombres non euclidiens pour la norme mais G.E., certains d'entre eux sont répertoriés dans la table II.8. On va donner un exemple de corps de nombres non principal qui n'est pas G.E..

Exemple 5.37. Soit $K = \mathbf{Q}(x)$ où $x^4 - 3x^2 - 29 = 0$. Alors $\mathrm{disc}_K = -11\,600$, $\mathrm{h}_K = 2$. On trouve deux orbites critiques $\mathcal{O}_1$ de longueur 3 et de minimum $\frac{5}{4}$, et $\mathcal{O}_2$ de longueur 6 et de minimum $\frac{19}{16}$. Par ailleurs, $\frac{x^2+5x+1}{10} \in \mathcal{O}_1$ et $\frac{x^3+x}{10} \in \mathcal{O}_2$. Mais $\left(x^2 + 5x + 1, 10\right) = \left(x^3 + x, 10\right) = \mathbf{Z}_K$, qui est clairement un idéal principal. Dès lors, K n'est pas G.E..

6 Complexité et approximations de calcul

Le but de ce paragraphe est double : d'une part, voir que l'on peut travailler avec des approximations de nombres réels pourvu qu'on prenne assez de précautions, et

d'autre part, comprendre quelles sont les parties de l'algorithme qui rendent son exécution longue.

Pour toute matrice carrée $\mathcal{A} = \left(a_{i,j}\right)_{1\leqslant i,j\leqslant l}$ de taille l, nous écrirons

$$\|\mathcal{A}\|_\infty := \max_{1\leqslant i\leqslant l} \sum_{j=1}^{l} \left|a_{i,j}\right| .$$

6.1 Approximations de calcul

Les procédures décrites dans ce chapitre utilisent des approximations en nombres flottants de nombres réels. Nous allons voir comment nous assurer que les résultats obtenus sont exacts et corrects malgré ces approximations.

6.1.1 Propriétés de la matrice $\mathcal{M}$

Rappelons que $\mathcal{M}$ est obtenue par réduction LLL de la matrice (II.2). Des propriétés classiques des réductions LLL vont nous permettre d'énoncer les propriétés suivantes de $\mathcal{M}$.

Lemme 6.1. $\|\mathcal{M}\|_\infty \leqslant n\left(\frac{2^{\frac{n}{4}}}{\sqrt{n}}\right)^{n-1} \frac{\sqrt{|\mathrm{disc}_K|}}{2^{r_2}}$ *et* $\left\|\mathcal{M}^{-1}\right\|_\infty \leqslant \sqrt{n}\cdot 2^{\frac{n(n-1)}{4}}$.

Démonstration. Commençons par noter qu'avant d'effectuer une réduction LLL, on a $\mathcal{M} = \mathcal{N}\mathcal{M}_2$, où

$$\mathcal{N} = \frac{1}{2}\begin{pmatrix} 2\mathcal{I}_{r_1} & 0 & 0 \\ 0 & \mathcal{I}_{r_2} & \mathcal{I}_{r_2} \\ 0 & \mathcal{I}_{r_2} & -\mathcal{I}_{r_2} \end{pmatrix} \qquad \text{et} \qquad \mathcal{M}_2 = \left(\sigma_i\left(z_j\right)\right)_{1\leqslant i,j\leqslant n},$$

en notant $\mathcal{I}_l$ la matrice identité de taille l. On en déduit que

$$|\det(\mathcal{M})| = \frac{\sqrt{|\mathrm{disc}_K|}}{2^{r_2}},$$

ce déterminant est conservé après réduction LLL.

À présent, on suppose que $\mathcal{M}$ est LLL-réduite. Pour tout l et tout vecteur $v \in \mathbf{R}^l$, on notera $|v| := \sqrt{\sum_{i=1}^{l} v_i^2}$. Pour tout $1 \leqslant j \leqslant n$, $\mathcal{M}_j$ désigne la j^{e} ligne de $\mathcal{M}$. On va déjà prouver que $|\mathcal{M}_j| \geqslant \sqrt{\frac{n}{2}}$ pour tout $1 \leqslant j \leqslant n$.

Pour un tel j, par définition de $\mathcal{M}$, il existe $z_j \in \mathbf{Z}_K \setminus \{0\}$ tel que

$$\left|\mathcal{M}_j\right|^2 = \sum_{i=1}^{r_1+r_2} \left|\sigma_i(z_j)\right|^2 \geqslant \sum_{i=1}^{n} \left|\sigma_i(z_j)\right|^2 .$$

Cette propriété est encore vérifiée après réduction LLL (même si les z_j peuvent être changés). Par conséquent, par l'inégalité arithmético-géométrique,

$$\left|\mathcal{M}_j\right|^2 \geqslant \frac{n}{2}\left(\prod_{i=1}^{n} \left|\sigma_i(z_j)\right|\right)^{\frac{2}{n}} .$$

Mais $\prod_{i=1}^{n} \left|\sigma_i(z_j)\right|^2 = \left|\mathbf{N}_{K/\mathbf{Q}}(z_j)\right| \geqslant 1$, dès lors

$$\left|\mathcal{M}_j\right|^2 \geqslant \frac{n}{2},$$

ce qui prouve que $\left|\mathcal{M}_j\right| \geqslant \sqrt{\frac{n}{2}}$.

Maintenant, comme $\mathcal{M}$ est LLL-réduite, $\prod_{j=1}^{n}\left|\mathcal{M}_j\right| \leqslant 2^{\frac{n(n-1)}{4}}|\det \mathcal{M}|$, par conséquent, pour tout $1 \leqslant j \leqslant n$,

$$\left|\mathcal{M}_j\right| \leqslant \left(\frac{2^{\frac{n+2}{4}}}{\sqrt{n}}\right)^{n-1}|\det \mathcal{M}|\,.$$

Cela permet de majorer chaque coefficient de $\mathcal{M}$. On peut facilement en déduire la borne énoncée sur $\|\mathcal{M}\|_\infty$.

On cherche à présent à borner $\left\|\mathcal{M}^{-1}\right\|_\infty$. Pour tous $1 \leqslant i, j \leqslant n$, notons $\mathcal{M}_{i,j}$ la sous-matrice obtenue en supprimant la i^{e} ligne et la j^{e} colonne de $\mathcal{M}$. On écrit $n_{i,j} := (-1)^{i+j}\det \mathcal{M}_{i,j}$ le cofacteur (i,j) de $\mathcal{M}$. Alors, comme $\mathcal{M}^{-1} = \frac{1}{\det \mathcal{M}}\left(n_{j,i}\right)_{1\leqslant i,j\leqslant n}$, il suffit de majorer $\left|n_{j,i}\right|$ pour obtenir une borne sur $\left\|\mathcal{M}^{-1}\right\|_\infty$.

Notons $(C_k)_{1\leqslant k\leqslant n-1}$ les colonnes de $\mathcal{M}_{j,i}$. Grâce à l'inégalité de Hadamard, on trouve

$$\left|n_{j,i}\right| = \left|\det \mathcal{M}_{j,i}\right| \leqslant \prod_{k=1}^{n-1}|C_k|\,.$$

Mais $|C_k| \leqslant |\mathcal{M}_r|$, où $r = \begin{cases} k & \text{if } k < i \\ k+1 & \text{if } k \geqslant i \end{cases}$. Par conséquent,

$$\left|n_{j,i}\right| \leqslant \frac{\prod_{r=1}^{n}|\mathcal{M}_r|}{|\mathcal{M}_i|}.$$

Alors, comme $\mathcal{M}$ est LLL-réduite, $\prod_{r=1}^{n}|\mathcal{M}_r| \leqslant 2^{\frac{n(n-1)}{4}}|\det \mathcal{M}|$ et on a déjà vu que $|M_i| \geqslant \sqrt{\frac{n}{2}}$, ce qui nous donne

$$\left|\frac{n_{j,i}}{\det \mathcal{M}}\right| \leqslant \sqrt{\frac{2}{n}}\cdot 2^{\frac{n(n-1)}{4}}.$$

La borne sur $\left\|\mathcal{M}^{-1}\right\|_\infty$ recherchée s'en déduit facilement. □

Remarque 6.2. Ces majorations sont génériques et beaucoup plus grandes que les valeurs observées en pratique. Dans les exemples considérés, on a en fait toujours $\left\|\mathcal{M}^{-1}\right\|_\infty < \|\mathcal{M}\|_\infty < 20$. Ainsi, dans l'exemple décrit au paragraphe 4.4, on a

$$\|\mathcal{M}\|_\infty \simeq 5{,}59 \qquad \text{et} \qquad \left\|\mathcal{M}^{-1}\right\|_\infty \simeq 1{,}18.$$

6.1.2 Calcul exact du minimum euclidien local

Comme on travaille avec des points de K, on peut calculer *exactement* le minimum euclidien. Les seules approximations requises sont effectuées pour estimer le nombre réel $\Gamma(k)$. Par conséquent, il suffit d'utiliser un certain $\Gamma'(k)$ vérifiant $\Gamma'(k) \geqslant \Gamma(k)$ même avec les erreurs de calcul.

Cependant, la précision n'est pas le véritable problème ici. En fait, si $\Gamma(k)$ est trop grand (ce qui arrive dès que la valeur absolue d'un plongement de l'unité ε utilisée est trop petit ou trop grand), alors le calcul du minimum euclidien local peut nécessiter trop d'estimations de normes. En pratique, on utilise la bibliothèque PARI ([PAR12]) qui contient une fonction pour calculer la norme d'éléments de corps de nombres.

6.1.3 Recouvrement et découpage du domaine fondamental

Tous les calculs sont effectués en utilisant la matrice $\mathcal{M}$. Mais on ne connaît qu'une approximation notée $\widetilde{\mathcal{M}} = \left(\widetilde{m}_{i,j}\right)_{1\leqslant i,j\leqslant n}$ de $\mathcal{M} = \left(m_{i,j}\right)_{1\leqslant i\leqslant n}$. On suppose que pour tous $1 \leqslant i, j \leqslant n$, on a $\left|\widetilde{m}_{i,j} - m_{i,j}\right| < \epsilon$.

6.1.3.1 Erreurs sur $(a_i)_{1\leqslant i\leqslant n}$ et $(b_i)_{1\leqslant i\leqslant n}$ Pour définir $(a_i)_{1\leqslant i\leqslant n}$ et $(b_i)_{1\leqslant i\leqslant n}$, on a besoin de connaître les signes des coefficients de la matrice $\mathcal{M}$. Toutefois, comme ces coefficients ne sont pas calculés exactement, ce n'est pas nécessairement si facile. Néanmoins, pour effectuer les calculs des bornes, il suffit de déterminer des n-uplets $\widetilde{a} = (\widetilde{a}_i)_{1\leqslant i\leqslant n}$ et $\widetilde{b} = (\widetilde{b}_i)_{1\leqslant i\leqslant n}$ tels que pour tout $1 \leqslant i \leqslant n$, $\widetilde{a}_i \leqslant a_i < b_i \leqslant \widetilde{b}_i$ quelles que soient les erreurs sur a_i et b_i. Donc on définit tout simplement pour $1 \leqslant i \leqslant n$,

$$\widetilde{a}_i = \sum_{\substack{j=1\\ \widetilde{m}_{i,j}<\epsilon}}^{n} \left(\widetilde{m}_{i,j} - \epsilon\right) \qquad \text{and} \qquad \widetilde{b}_i = \sum_{\substack{j=1\\ \widetilde{m}_{i,j}>-\epsilon}}^{n} \left(\widetilde{m}_{i,j} + \epsilon\right).$$

Ainsi, tous les calculs sont effectués dans $\widetilde{\mathcal{F}} = \left[\widetilde{a}_1, \widetilde{b}_1\right] \times \cdots \times \left[\widetilde{a}_n, \widetilde{b}_n\right]$ qui contient le domaine fondamental $\mathcal{F}$.

6.1.3.2 Découpage On choisit un n-uplet d'entiers positifs $(N_i)_{1\leqslant i\leqslant n}$ et on décide de découper le domaine fondamental en N_i morceaux dans la i^{e} direction. Les centres et les pas des parallélotopes sont déterminés par $\widetilde{\mathcal{M}}$, mais, même s'ils diffèrent des centres et des pas théoriques (définis par $\mathcal{M}$), il n'y a pas d'erreur à cette étape : ils constituent un recouvrement de $\mathcal{F}$ par des parallélotopes.

6.2 Calculs flottants pour le test d'absorption

À cette étape, on a un parallélotope problématique $\widetilde{\mathcal{P}}$ de centre $\widetilde{c} = (\widetilde{c}_i)_{1\leqslant i\leqslant n}$ et de pas $\widetilde{h} = \left(\widetilde{h}_i\right)_{1\leqslant i\leqslant n}$. On veut savoir si l'élément $Z = (Z_i)_{1\leqslant i\leqslant n} = \mathcal{M}z$ (où $z \in \mathbf{Z}^n$) absorbe $\widetilde{\mathcal{P}}$ pour la valeur $k > 0$, ce qui se produit (d'après le lemme 3.7) quand $\mathcal{S} < k$ où

$$\mathcal{S} := \prod_{i=1}^{r_1} \left(|\widetilde{c}_i - Z_i| + \widetilde{h}_i\right) \cdot \prod_{i=r_1+1}^{r_1+r_2} \left(\left(|\widetilde{c}_i - Z_i| + \widetilde{h}_i\right)^2 + \left(|\widetilde{c}_{i+r_2} - Z_{i+r_2}| + \widetilde{h}_{i+r_2}\right)^2\right).$$

Cependant, on ne connaît pas Z exactement, mais plutôt $\widetilde{Z} = \left(\widetilde{Z}_i\right)_{1\leqslant i\leqslant n} = \widetilde{\mathcal{M}}z$. À la place de $\mathcal{S}$, on va donc calculer

$$\widetilde{\mathcal{S}} := \prod_{i=1}^{r_1} \left(\left|\widetilde{c}_i - \widetilde{Z}_i\right| + \widetilde{h}_i\right) \cdot \prod_{i=r_1+1}^{r_1+r_2} \left(\left(\left|\widetilde{c}_i - \widetilde{Z}_i\right| + \widetilde{h}_i\right)^2 + \left(\left|\widetilde{c}_{i+r_2} - \widetilde{Z}_{i+r_2}\right| + \widetilde{h}_{i+r_2}\right)^2\right).$$

Le but est donc de trouver un nombre réel $k' > 0$ aussi petit que possible tel que $\mathcal{S}' < k'$ implique $\mathcal{S} < k$. On suppose que la liste des entiers utilisés $\mathcal{L}$ vérifie $\mathcal{L} \subseteq \mathcal{M}[-B, B]^n$. Avec cette notation, on peut borner l'erreur de calcul.

Lemme 6.3.

$$\left|\widetilde{\mathcal{S}} - \mathcal{S}\right| < 2^{r_2} \left((B+1)\|\widetilde{\mathcal{M}}\|_\infty + n\epsilon\right)^n \left[\left(1 + \frac{nB\epsilon}{(B+1)\|\widetilde{\mathcal{M}}\|_\infty + n\epsilon}\right)^n - 1\right].$$

Pour le prouver, on va utiliser le lemme suivant.

Lemme 6.4. *On a les propriétés suivantes*

1. *Soient $a, b, c, d \in \mathbf{C}$, alors $2(ab - cd) = (a - c)(b + d) + (a + c)(b - d)$.*
2. *Soient l un entier strictement positif, $a = (a_1, \dots, a_l) \in \mathbf{C}^l$ et $b = (b_1, \dots, b_l) \in \mathbf{C}^l$. On suppose qu'il existe un nombre réel $\rho > 0$ tel que pour tout $1 \leqslant i \leqslant l$, $|b_i - a_i| < \rho$. Soit de plus A un réel strictement positif tel que pour tout $1 \leqslant i \leqslant l$, $|a_i| \leqslant A$. Alors*
$$\left| \prod_{i=1}^{l} b_i - \prod_{i=1}^{l} a_i \right| < (A + \rho)^l - A^l.$$

Démonstration. La première propriété est claire. Pour la seconde, on calcule

$$\begin{aligned} \left| \prod_{i=1}^{l} b_i - \prod_{i=1}^{l} a_i \right| &= \left| \sum_{i=1}^{l} \left\{ \sum_{1 \leqslant j_1 < \cdots < j_i \leqslant l} \left(\prod_{k=1}^{i} (b_{j_k} - a_{j_k}) \right) \left(\prod_{\substack{j=1 \\ j \notin \{j_1, \dots, j_i\}}}^{l} a_j \right) \right\} \right| \\ &< \sum_{i=1}^{l} \binom{l}{i} \rho^i A^{l-i}, \text{ par l'inégalité triangulaire,} \\ &= (A + \rho)^l - A^l. \end{aligned}$$

□

On peut maintenant s'atteler à la preuve du lemme 6.3.

Démonstration du lemme 6.3. Notons $D = \|\widetilde{\mathcal{M}}\|_\infty$ et $\mathcal{I} = \sqrt{-1}$. On définit le n-uplet $a = (a_i)_{1 \leqslant i \leqslant n}$ par

$$a_i := \begin{cases} \left| \widetilde{c}_i - \widetilde{Z}_i \right| + \widetilde{h}_i & \text{si } 1 \leqslant i \leqslant r_1, \\ \left| \widetilde{c}_i - \widetilde{Z}_i \right| + \widetilde{h}_i + \mathcal{I} \left(\left| \widetilde{c}_{i+r_2} - \widetilde{Z}_{i+r_2} \right| + \widetilde{h}_{i+r_2} \right) & \text{si } r_1 < i \leqslant r_1 + r_2, \\ \left| \widetilde{c}_{i-r_2} - \widetilde{Z}_{i-r_2} \right| + \widetilde{h}_{i-r_2} - \mathcal{I} \left(\left| \widetilde{c}_i - \widetilde{Z}_i \right| + \widetilde{h}_i \right) & \text{si } r_1 + r_2 < i \leqslant n. \end{cases} \tag{II.16}$$

De même, on définit $b = (b_i)_{1 \leqslant i \leqslant n}$ en remplaçant $\widetilde{Z}$ par Z dans (II.16). On écrit $\widetilde{\mathcal{S}}^{(1)} := \prod_{i=1}^{r_1} a_i$, $\widetilde{\mathcal{S}}^{(2)} := \prod_{i=r_1+1}^{n} a_i$, $\mathcal{S}^{(1)} := \prod_{i=1}^{r_1} b_i$ et $\mathcal{S}^{(2)} := \prod_{i=r_1+1}^{n} b_i$, de sorte que $\widetilde{\mathcal{S}} - \mathcal{S} = \widetilde{\mathcal{S}}^{(1)} \widetilde{\mathcal{S}}^{(2)} - \mathcal{S}^{(1)} \mathcal{S}^{(2)}$. Avec le lemme 6.4 (1), on voit que

$$\begin{aligned} 2 \left| \widetilde{\mathcal{S}} - \mathcal{S} \right| \leqslant \left| \widetilde{\mathcal{S}}^{(1)} - \mathcal{S}^{(1)} \right| \left(2 \left| \widetilde{\mathcal{S}}^{(2)} \right| + \left| \widetilde{\mathcal{S}}^{(2)} - \mathcal{S}^{(2)} \right| \right) \\ + \left(2 \left| \widetilde{\mathcal{S}}^{(1)} \right| + \left| \widetilde{\mathcal{S}}^{(1)} - \mathcal{S}^{(1)} \right| \right) \left| \widetilde{\mathcal{S}}^{(2)} - \mathcal{S}^{(2)} \right|. \end{aligned}$$

Remarquons que $\left| \widetilde{\mathcal{S}}^{(1)} \right| \leqslant (D(B+1) + n\epsilon)^{r_1}$ et $\left| \widetilde{\mathcal{S}}^{(2)} \right| \leqslant 2^{r_2} (D(B+1) + n\epsilon)^{2r_2}$. Pour aller plus vite, nous écrirons

$$\mu := \frac{nB\epsilon}{D(B+1) + n\epsilon}.$$

En utilisant le lemme 6.4 (2) deux fois : avec $A = D(B+1) + n\epsilon$, $\rho = nB\epsilon$ pour $\widetilde{\mathcal{S}}^{(1)} - \mathcal{S}^{(1)}$ et avec $A = \sqrt{2}\,(D(B+1) + n\epsilon)$, $\rho = nB\epsilon\sqrt{2}$ pour $\widetilde{\mathcal{S}}^{(2)} - \mathcal{S}^{(2)}$, on obtient

$$\begin{aligned} \left| \widetilde{\mathcal{S}} - \mathcal{S} \right| < & 2^{r_2 - 1} (D(B+1) + n\epsilon)^n \\ & \times \left[\left((1+\mu)^{r_1} - 1 \right) \left((1+\mu)^{2r_2} + 1 \right) + \left((1+\mu)^{r_1} + 1 \right) \left((1+\mu)^{2r_2} - 1 \right) \right]. \end{aligned}$$

On en déduit facilement le résultat. □

$n = [K : \mathbf{Q}]$	valeur approximative de B	précision du test d'absorption
2	1000	10^{-7}
3	200	10^{-5}
4	30	$5 \cdot 10^{-5}$
5	12	$3 \cdot 10^{-4}$
6	6	$3 \cdot 10^{-3}$
7	2	$6 \cdot 10^{-4}$
8	2	$4 \cdot 10^{-2}$

TABLE II.9 – Précision du test d'absorption selon le degré et la taille des entiers utilisés.

Dans les exemples considérés, $\|\widetilde{\mathcal{M}}\|_\infty < 10$. On utilise des nombres flottants avec double précision. Le minimum est environ 1, donc $\epsilon \simeq 10^{-15}$ et on choisit B décroissant avec le degré n. La table II.9 fournit des exemples de la précision requise pour le calcul de normes étendues dans le pire cas.

En pratique, quand on essaie d'absorber des parallélotopes par des entiers pour une valeur $k > 0$, on remplace k par $k' := k - \eta$, où η est la précision à laquelle on calcule les normes étendues (voir lemme 6.3).

6.2.1 Calculs flottants pour l'action des unités

Tous les calculs décrits dans le paragraphe 3.3 sont explicites, mais ils sont effectués en pratique avec des approximations des plongements des unités, de $\mathcal{M}$ et de $\mathcal{M}^{-1}$. On suppose que l'on connaît leurs coordonnées à $\epsilon > 0$ près. On note $v = (v_1, \ldots, v_n)$ l'image par Φ de l'unité utilisée, $c = (c_1, \ldots, c_n) \in H$ le centre du parallélotope $\mathcal{P}$ de pas $h = (h_1, \ldots, h_n)$ considéré.

6.2.1.1 Erreur sur la taille de l'image On a inclus $v \cdot \mathcal{P}$ dans un domaine $\mathcal{B}$ défini avec le pas $h' = (h'_1, \ldots, h'_n) \in \mathbf{R}^n$. L'erreur provient du fait que l'on ne connaît pas v exactement, mais seulement une approximation $\widetilde{v} = (\widetilde{v}_1, \ldots, \widetilde{v}_n)$ telle que pour tout $1 \leqslant i \leqslant n$, $|\widetilde{v}_i - v_i| < \epsilon$. Avec ce n-uplet $\widetilde{v}$, on calcule le n-uplet $\widetilde{h'} = \left(\widetilde{h'}_i\right)_{1 \leqslant i \leqslant n}$ et on a les majorations suivantes.

$$\begin{cases} \left|\widetilde{h'}_i - h'_i\right| < h_i \cdot \epsilon & \text{si } 1 \leqslant i \leqslant r_1 \\ \left|\widetilde{h'}_i - h'_i\right| < \epsilon\sqrt{h_i^2 + h_{i+r_2}^2} & \text{si } r_1 < i \leqslant r_1 + r_2 \end{cases}. \tag{II.17}$$

Remarques 6.5. On a les mêmes majorations pour le pas $\widetilde{h'}_{i+r_2} = \widetilde{h'}_i$ $(r_1 < i \leqslant r_1 + r_2)$. En pratique, on peut augmenter $\widetilde{h'}_i$ pour tenir compte de l'erreur de calcul. Notons également que cette erreur reste petite tant que le pas initial h est assez petit. En tout cas, l'action des unités ne peut éliminer des problèmes que quand le découpage est assez fin, c'est-à-dire que les pas sont assez petits.

6.2.1.2 Erreur sur le centre de l'image Le domaine $\mathcal{B}$ est centré en $c' = v \cdot c$, mais on utilise $\widetilde{v}$ à la place de v. Par conséquent, on calcule $\widetilde{c'} := \widetilde{v} \cdot c$ et, comme dans

(II.17), l'erreur sur les coordonnées du centre est $|c_i| \cdot \epsilon$ si $1 \leqslant i \leqslant r_1$ et $(|c_i| + |c_{i+r_2}|) \cdot \epsilon$ si $r_1 < i \leqslant r_1 + r_2$. Ces erreurs sont majorées par $2\|\widetilde{M}\|_\infty \epsilon$, on peut augmenter le pas $\widetilde{h}'_i$ pour s'assurer que le test avec l'unité est correct.

6.2.1.3 Vecteurs de translation

On va utiliser le lemme élémentaire suivant.

Lemme 6.6. *Soient $x = (x_i)_{1\leqslant i\leqslant n}$, $\alpha = (\alpha_i)_{1\leqslant i\leqslant n}$ et $\beta = (\beta_i)_{1\leqslant i\leqslant n}$ trois n-uplets tels que pour tout $1 \leqslant i \leqslant n$, on a $\alpha_i \leqslant z_i \leqslant \beta_i$. Pour toute matrice $\mathcal{A} = (a_{i,j})_{1\leqslant i,j\leqslant n}$, si on écrit $y = \mathcal{A}x = (y_i)_{1\leqslant i\leqslant n}$, alors pour tout $1 \leqslant i \leqslant n$,*

$$\sum_{\substack{j=1\\ a_{i,j}>-\epsilon}}^{n} (a_{i,j}+\epsilon)\alpha_j + \sum_{\substack{j=1\\ a_{i,j}<\epsilon}}^{n} (a_{i,j}-\epsilon)\beta_j \leqslant y_i \leqslant \sum_{\substack{j=1\\ a_{i,j}>-\epsilon}}^{n} (a_{i,j}+\epsilon)\beta_j + \sum_{\substack{j=1\\ a_{i,j}<\epsilon}}^{n} (a_{i,j}-\epsilon)\beta_j.$$

Ici, on applique ce lemme avec $\alpha = \widetilde{a}'$, $\beta = \widetilde{b}'$ et $\mathcal{A} = \widetilde{\mathcal{M}}^{-1}$. On obtient des bornes correctes sur les y_i pour tout $1 \leqslant i \leqslant n$ même si l'on commet des erreurs de calcul. On prend les entiers dans ces intervalles pour obtenir tous les vecteurs de translation.

6.2.1.4 Intersection avec d'autres problèmes

On suppose que l'on utilise un vecteur de translation $\widetilde{X}$ qui est une approximation de X. L'erreur sur chaque coordonnée de $\widetilde{X}$ est au plus $nB\epsilon$. On prend en compte cette erreur pour décider si $\nu \cdot \mathcal{P} - X$ peut intersecter un parallélotope problématique. En augmentant la taille du domaine contenant $\nu \cdot \mathcal{P} - X$, on peut ne pas éliminer un parallélotope non problématique, mais on ne supprime jamais un parallélotope problématique.

6.3 Complexité de quelques procédures

On s'intéresse seulement au procédures les plus coûteuses.

6.3.1 Calcul du minimum euclidien local

Proposition 6.7. *Soit $x \in K$, l'algorithme 3.1 nécessite au plus*

$$\#\mathrm{Orb}\,(x) \cdot \left(2\Gamma\left(\left|\mathbf{N}_{K/\mathbf{Q}}(x)\right|\right)\left\|\widetilde{\mathcal{M}}^{-1}\right\|_\infty + 1\right)^n$$

calculs de normes d'éléments de K.

Démonstration. Il est immédiat de remarquer que, pour tout $k > 0$, le calcul de $\mathcal{M}_k$ requiert au plus $\#\mathrm{Orb}\,(x) \cdot \left(2\Gamma(k)\left\|\widetilde{\mathcal{M}}^{-1}\right\|_\infty + 1\right)^n$ calculs de normes. □

6.3.2 Test des unités

On considère l'action de $\nu \in \Phi(\mathbf{Z}_K^\times)$ sur un parallélotope problématique quelconque $\mathcal{P}$ de centre c et de pas h.

Proposition 6.8. *Il existe au plus $\left(\left\|\widetilde{\mathcal{M}}^{-1}\right\|_\infty \left(\left\|\widetilde{\mathcal{M}}\right\|_\infty (1 + 2\|\widetilde{\nu}\|_\infty)\right) + 1\right)^n$ vecteurs de translation de $\mathcal{P}$ dans le domaine fondamental $\mathcal{F}$.*

On veut avoir aussi peu de vecteurs de translation que possible. Par conséquent, il est intéressant de choisir $\nu \in \Phi(\mathbf{Z}_K^\times)$ tel que $\|\nu\|_\infty$ est aussi petit que possible. De plus la majoration utilise l'inégalité très peu optimale $|h'_i| \leqslant \|\widetilde{\nu}\|_\infty \left\|\widetilde{\mathcal{M}}\right\|_\infty$, pour tout

(r_1, r_2)	$M(K)$	N	temps
$(0, 2)$	$\frac{1}{7}$	12	10 s
$(3, 1)$	$\frac{1}{13}$	24	16min 23s
$(0, 3)$	$\frac{1}{13}$	36	23min 10s
$(6, 0)$	$\frac{1}{13}$	168	2h 13min 26s
$(7, 0)$	$\frac{1}{7}$	6	1h 38min 52s
$(0, 4)$	$\frac{1}{16}$	15	55h 54min 38s

(a) Plus petit discriminant.

disc_K	$M(K)$	N	temps
4 897	$\frac{1}{5}$	4	3min 58s
8 705	$\frac{1}{5}$	4	21 min 5 s
10 229	$\frac{1}{2}$	1	1min 15s
52 813	$\frac{1}{2}$	1	43min 8s
163 273	$\frac{7}{5}$	2	11min 27s
163 300	1	1	22min 19s

(b) Signature $(1, 2)$.

TABLE II.10 – Quelques chronométrages d'exécution de l'algorithme 4.1. On note N le nombre de points critiques.

$1 \leqslant i \leqslant n$ (avec les notations du paragraphe 3.3). On peut obtenir une meilleure inégalité (et de meilleurs résultats) en découpant davantage dans les directions i où $\widetilde{v}_i$ est « grand ».

Avec cette estimation sur le nombre de vecteurs de translation, on peut borner le nombre d'opérations requises pour le test avec l'unité v.

Proposition 6.9. *L'algorithme 3.5 nécessite au plus*

$$O\left(n \cdot (\#\mathcal{T})^3 \cdot \left(\left\|\widetilde{\mathcal{M}}^{-1}\right\|_\infty \left(\left\|\widetilde{\mathcal{M}}\right\|_\infty (1 + 2\|\widetilde{v}\|_\infty)\right) + 1\right)^n\right)$$

opérations élémentaires avec des flottants.

6.4 Chronométrages

Le temps d'exécution de l'algorithme 4.1 dépend du choix de la valeur initiale $\mathcal{K}$. La dichotomie décrite au paragraphe 4.1 peut être la partie la plus longue de l'exécution. Dans la table II.10, on donne le temps CPU et on ne décrit que le temps requis pour la valeur $k = 0{,}97 \cdot M(K)$, pour laquelle on obtient un graphe convenable dans tous les cas.

Pour expliquer les durées d'exécution observées, remarquons tout d'abord que pour un corps de nombres de degré n, un découpage dans n directions est requis et si $M(K)$ est petit, on devra choisir des N_i assez grands pour tout $1 \leqslant i \leqslant n$ pour avoir des tests d'absorptions efficaces dès le début de l'algorithme.

Ensuite, quand on fixe la signature, les propriétés suivantes de K peuvent rendre certaines parties de l'algorithme 4.1 coûteuses.

- Si $M(K)$ est petit, alors un découpage initial précis sera requis.
- Si les unités de K sont grandes, alors de nombreux vecteurs de translation peuvent être trouvés par l'algorithme 3.5 et le calcul final du minimum euclidien local par l'algorithme 3.1 peut s'avérer long.

– S'il y a beaucoup de points critiques, alors il y aura plus de parallélotopes problématiques et une exécution de l'algorithme 3.1 sera requise pour chaque orbite critique.

CHAPITRE III

CONSTRUCTION DE MOTZKIN

Plan

Le but de ce chapitre est de présenter la construction de Motzkin dans le cadre non nécessairement commutatif pour l'étude des quaternions (voir chapitre V) et pour que les idées soient bien fixées quand nous étudierons les classes euclidiennes au chapitre IV. La référence est l'article de Samuel [Sam71], même s'il est restreint – en apparence – au cas commutatif. Le but n'est pas d'être le plus général possible, mais simplement d'obtenir les résultats dans les cadres qui nous intéressent.

1 Définitions et premières propriétés

Définition 1.1. Soit R un anneau unitaire. On dit que R est *euclidien à droite* s'il existe un ensemble bien ordonné W et une application $\varphi : R \longrightarrow W$ telle que

$$\text{pour tous } a, b \in R,\ b \neq 0,\ \text{il existe } q \in R \text{ tel que } \varphi(a - bq) < \varphi(b). \tag{III.1}$$

En ce cas, on dit que R est euclidien à droite pour φ ou que φ est un *stathme à droite* pour R.

On peut bien sûr définir de façon analogue l'euclidianité à gauche, qui possédera les mêmes propriétés que l'euclidianité à droite. Pour alléger l'écriture, on notera 0 et 1 les premier et deuxième éléments de W pour son bon ordre.

Lemme 1.2 ([Sam71, propositions 1,2 & 3])**.** *Soit R euclidien à droite pour le stathme $\varphi : R \longrightarrow W$. On a alors les propriétés suivantes.*

1. *Si $b \in R \setminus \{0\}$, alors $\varphi(b) > \varphi(0)$.*
2. *Si $b \in R \setminus \{0\}$ vérifie $\varphi(b) = \min_{c \in R\setminus\{0\}} \varphi(c)$, alors $b \in R^\times$.*
3. *R est principal à droite.*

Démonstration. 1. On note $b_0 = b$ et on définit récursivement la suite $(b_n)_{n\geqslant 0}$ de la façon suivante :

$$\text{si } b_n \neq 0,\ \text{on écrit la division } 0 = b_n q_n + b_{n+1},\ \text{avec } \varphi(b_{n+1}) < \varphi(b_n).$$

Ainsi, la suite $(\varphi(b_n))_{n\geqslant 0}$ est une suite strictement décroissante d'éléments de W, donc elle est finie : il existe $n > 0$ tel que $b_n = 0$. Alors $\varphi(0) = \varphi(b_n) < \varphi(b_0) = \varphi(b)$.

2. Soit $a \in R$, on fait la division de a par b : il existe $q \in R$ tel que $\varphi(a - bq) < \varphi(b)$. Par définition de b, cela implique que $\varphi(a-bq) = \varphi(0)$, donc d'après (1), $a-bq = 0$. Ainsi $R = bR$ et donc $b \in R^\times$.

3. Fixons un idéal à droite $\mathfrak{b}$ non nul de R. Soit alors un élément $b \in \mathfrak{b}$ tel que $b \neq 0$ et $\varphi(b) = \min_{c \in \mathfrak{b} \setminus \{0\}}$. Pour tout $a \in \mathfrak{b}$, on peut faire la division de a par b : il existe $q \in R$ tel que $\varphi(a - bq) < \varphi(b)$. Or $a - bq \in \mathfrak{b}$. Donc par définition de b, $a - bq = 0$ et ainsi $\mathfrak{b} = bR$.

□

2 Algorithme minimal et ensembles de Motzkin

Proposition 2.1 ([Sam71, proposition 9])**.** *Si $\varphi_\alpha : R \longrightarrow W$ est une famille non vide de stathmes à droite, alors $\varphi = \inf_\alpha \varphi$ est aussi un stathme à droite. Si $\{\varphi_\alpha\}$ est la famille de tous les stathmes à droite d'image dans W, on appellera φ le* stathme minimal à droite *pour R et W.*

Démonstration. Soient $a, b \in R$, $b \neq 0$. Comme W est bien ordonné, il existe α tel que $\varphi(b) = \varphi_\alpha(b)$. On peut écrire la division de a par b pour φ_α : il existe $q \in R$ tel que $\varphi_\alpha(a - bq) < \varphi_\alpha(b)$. Mais alors, par définition de φ,

$$\varphi(a - bq) \leqslant \varphi_\alpha(a - bq) < \varphi_\alpha(b) = \varphi(b),$$

ce qui montre que φ est un stathme à droite. □

Ce stathme minimal a des propriétés intéressantes que nous allons décrire à présent. Commençons par remarquer que l'image du stathme « ne peut pas avoir de trou », ce qui s'énonce plus précisément comme suit.

Lemme 2.2. *Soit $\varphi : R \longrightarrow W$ le stathme minimal à droite d'un anneau euclidien à droite R. Soient α et $\beta \in W$ tels que β est le plus petit élément de W tel que $\beta > \alpha$. S'il existe $b \in R$ tel que $\varphi(b) = \beta$, alors il existe $a \in R$ tel que $\varphi(a) = \alpha$.*

Démonstration. Par l'absurde, supposons qu'il n'existe pas d'élément $a \in R$ tel que $\varphi(a) = \alpha$. On définit la fonction $\theta : \begin{cases} R & \longrightarrow & W \\ c & \longmapsto & \begin{cases} \alpha & \text{si } b = c \\ \varphi(c) & \text{sinon} \end{cases} \end{cases}$. On va montrer que θ est un stathme à droite. Soient $d, e \in R$ tels que $e \neq 0$. Comme φ est un stathme à droite, il existe $f \in R$ tel que $\varphi(d - ef) < \varphi(e)$. Si $d - ef \neq b$ et $e \neq b$, alors, par définition de θ,

$$\theta(d - ef) = \varphi(d - ef) < \varphi(e) = \theta(e).$$

Il suffit donc de considérer les divisions où b est diviseur (c'est-à-dire $b = e$) ou reste (c'est-à-dire $b = d - ef$). Si b est diviseur, alors $\varphi(d - bf) < \varphi(b) = \beta$. Comme α n'est pas atteint par φ, cela implique que $\varphi(d - bf) < \alpha = \theta(b)$. Ainsi,

$$\theta(d - bf) \leqslant \varphi(d - bf) < \theta(b).$$

Si $b = d - ef$, alors $\varphi(e) > \varphi(d - ef) = \beta$, donc $e \neq b$ et $\theta(e) = \varphi(e)$. Ainsi,

$$\theta(b - ef) \leqslant \varphi(b - ef) < \varphi(e) = \theta(e).$$

Dès lors, θ est un stathme à droite, mais c'est incompatible avec le fait que φ est le stathme minimal à droite pour W. Cela fournit une contradiction et montre qu'il existe $a \in R$ tel que

$$\varphi(a) = \alpha.$$

□

Ensuite, on peut remarquer que la définition du stathme minimal φ impose les valeurs où φ s'annule et vaut 1.

Proposition 2.3. *Soit R un anneau euclidien à droite, de stathme minimal à droite $\varphi : R \longrightarrow W$. Soit $x \in R$. Alors*
- *$\varphi(x) = 0$ si et seulement si $x = 0$,*
- *$\varphi(x) = 1$ si et seulement si $x \in R^\times$.*

Avant de prouver ce résultat, on va énoncer le lemme technique suivant.

Lemme 2.4. *Si $\phi : R \longrightarrow W$ est un stathme à droite, alors $\psi : R \longrightarrow W$ défini par $\psi(0) = \phi(0)$ et, si $b \neq 0$, $\psi(b) = \inf_{d \in Rb \setminus \{0\}} \phi(d)$ est un stathme à droite.*

Démonstration. Soient $a, b \in R$, avec $b \neq 0$. Alors il existe $c \in R$ tel que $\psi(b) = \phi(cb)$. On fait la division euclidienne de ca par cb via ϕ : il existe $q \in R$ tel que

$$\phi(c(a - bq)) = \phi(ca - cbq) < \phi(bc) = \psi(b).$$

Par définition de ψ, on a $\psi(a - bq) \leqslant \phi(c(a - bq))$, on en déduit que ψ est un stathme à droite. □

Démonstration de la proposition 2.3.
- Le premier énoncé est une conséquence facile du lemme 1.2 (1).
- Pour le second, le lemme 1.2 (2) montre que si $\varphi(x) = 1$, alors $x \in R^\times$. Réciproquement, si $x \in R^\times$, alors comme φ est le stathme minimal à droite, le stathme ψ construit par le lemme 2.4 coïncide avec φ. Dès lors $\varphi(x) = \inf_{d \in Rx \setminus \{0\}} \varphi(d)$. Mais $x \in R^\times$, donc $\varphi(x) = \inf_{d \in R \setminus \{0\}} \varphi(d)$. Par ailleurs, $\varphi(1) = \inf_{d \in R \setminus \{0\}} \varphi(d)$. Ainsi φ est constante et égale à $\varphi(1)$ sur $R^\times$. D'après le lemme 1.2 (1), $\varphi(1) > 0$. Par l'absurde, si $\varphi(1) > 1$, alors, d'après le lemme 1.2 (2), pour tout $b \in R \setminus \{0\}$, $\varphi(b) \geqslant \varphi(1) > 1$. Cela montre que 1 n'est pas atteint par φ, c'est impossible d'après le lemme 2.2.

□

En fait, les valeurs du stathme minimal à droite sont reliés aux quotients de la forme R/bR par l'énoncé suivant.

Proposition 2.5 ([Sam71, proposition 10])**.** *Soit $\varphi : R \longrightarrow W$ le stathme minimal à droite d'un anneau euclidien à droite R. Pour $\alpha \in W$, on pose $R_\alpha = \{x \in R,\ \varphi(x) \leqslant \alpha\}$ et $R'_\alpha = \{x \in R,\ \varphi(x) < \alpha\}$. Alors $R_\alpha = \{0\} \cup \{b \in R,\ R'_\alpha \longrightarrow\!\!\!\!\!\rightarrow R/bR\}$.*

Démonstration. Si $b \in R_\alpha \setminus \{0\}$ et si $a + bR$ est une classe modulo bR (avec $a \in R$), alors en écrivant la division de a par b via φ, on trouve $q \in R$ tel que $\varphi(a - bq) < \varphi(b) \leqslant \alpha$, de sorte que $a - bq \in R'_\alpha \cap (a + bR)$. Ainsi, l'application canonique $R'_\alpha \longrightarrow R/bR$ est surjective.

Réciproquement, soit $b \neq 0$ tel que $R'_\alpha \longrightarrow\!\!\!\!\!\rightarrow R/bR$. Supposons que $\varphi(b) > \alpha$. On définit $\theta : R \longrightarrow W$ par $\theta(b) = \alpha$ et $\theta(x) = \varphi(x)$ pour $x \neq b$. Alors θ est un stathme à droite : il suffit en fait de considérer les divisions où b est un diviseur ou un reste.
- Si b est un diviseur dans une division $a = bq + r$, par hypothèse, chaque classe $a + bR$ a un représentant $r \in R'_\alpha$, donc $\theta(r) = \varphi(r) < \alpha = \theta(b)$.
- Si b est un reste dans la division $a = cq + b$, alors $\theta(b) = \alpha < \varphi(b) < \varphi(c) = \theta(c)$.

Ainsi, $\theta : R \longrightarrow W$ est un stathme à droite tel que $\theta(b) < \varphi(b)$. Par construction du stathme minimal à droite φ, c'est impossible. Donc $\varphi(b) \leqslant \alpha$. □

Corollaire 2.6 ([Sam71, proposition 15])**.** *Si R est un anneau euclidien à droite tel que pour tout $b \in R \setminus \{0\}$, le quotient R/bR est fini, alors le stathme minimal $\varphi : R \longrightarrow W$ est à valeurs dans* $\mathbf{N}$.

Démonstration. Notons ω le premier ordinal transfini atteint par φ, s'il existe. Si φ n'est pas à valeurs dans $\mathbf{N}$, il existe $b \in R$ tel que $\varphi(b) = \omega$. Notons que $b \neq 0$ car $\varphi(b) > 0$. D'après la proposition 2.5, toute classe $a + bR$ (avec $a \in R$) admet un représentant r_a tel que $\varphi(r_a) < \varphi(b) = \omega$. Par définition de ω, cela implique que $\varphi(r_a) = n_a \in \mathbf{N}$. Or R/bR est fini, donc $n = 1 + \sup_{s\in S} n_{a_s}$ est fini, si on note $(a_s + bR)_{s\in S}$ un système de représentants fini de R/bR. D'après la proposition 2.5, on obtient $\varphi(b) \leqslant n$, et donc $b \in R_n$. Cela fournit une contradiction, φ est donc à valeurs dans $\mathbf{N}$. □

Comme l'hypothèse selon laquelle le quotient R/bR est fini pour tout $b \in R$ sera toujours vérifiée pour les anneaux qui nous intéressent (c'est par exemple vrai si R est l'anneau des entiers d'un corps de nombres ou si R est un ordre d'un corps de quaternions sur un corps de nombres), nous pourrons toujours raisonner avec des stathmes à valeurs dans $\mathbf{N}$.

En particulier, nous allons nous contenter de la construction des ensembles de Motzkin pour un stathme minimal à valeurs dans $\mathbf{N}$.

Proposition 2.7. *Soit R un anneau unitaire tel que pour tout $b \in R$, le quotient R/bR est fini. On pose $R_0 = \{0\}$ et on définit récursivement la suite croissante $(R_n)_{n\in\mathbf{N}}$ par*

$$R_{n+1} = \{0\} \cup \left\{ b \in R,\ R_n \longrightarrow\!\!\!\!\!\rightarrow R/bR \right\}.$$

R est euclidien à droite si et seulement si $R = \cup_{n\in\mathbf{N}} R_n$.

Démonstration. Si R est euclidien à droite pour un stathme minimal à droite $\varphi : R \longrightarrow W$, alors φ est en fait à valeurs dans $\mathbf{N}$ (corollaire 2.6) et on peut appliquer les résultats de la proposition 2.5 pour montrer que $R = \cup_{n\in\mathbf{N}} R_n$.

Réciproquement, si $R = \cup_{n\in\mathbf{N}} R_n$, on définit $\theta : R \longrightarrow \mathbf{N}$ par $\theta(0) = 0$ et pour $b \neq 0$, $\theta(b) = n$ si et seulement si $b \in R_n \setminus R_{n-1}$. Cela définit un stathme à droite pour R (qui est en fait le stathme minimal). □

Pour appliquer cette construction, il est intéressant de noter que la proposition 2.3 implique que les premiers ensembles de Motzkin sont nécessairement $R_0 = \{0\}$ et $R_1 = \{0\} \cup R^\times$. Ainsi, on a la propriété suivante.

Corollaire 2.8. *Soit R un anneau qui n'est pas un corps (commutatif ou non). Si $R_2 = R_1 = \{0\} \cup R^\times$, alors R n'est pas euclidien.*

Démonstration. Par construction des ensembles R_n, on a pour tout $n \geqslant 2$, $R_n = R_1 = \{0\} \cup R^\times$. Par conséquent, $\cup_{n\in\mathbf{N}} R_n = \{0\} \cup R^\times$. Si R est euclidien, alors d'après la proposition 2.7, $R = \cup_{n\in\mathbf{N}} R_n = \{0\} \cup R^\times$. Ainsi, R est un corps gauche. On en déduit le résultat par contraposée. □

3 Remarques sur l'utilisation

L'objectif initial de Motzkin était de montrer que certains anneaux ne sont pas euclidiens. On peut ainsi appliquer le corollaire 2.8 pour montrer que tous les anneaux d'entiers de corps quadratiques imaginaires non euclidiens pour la norme ne sont en effet euclidiens pour aucun stathme.

Si la construction de Motzkin paraît explicite, elle est en pratique difficile à mettre en œuvre pour trouver le stathme minimal d'un anneau euclidien. En fait, on ne connaît explicitement de stathme minimal que dans des cas simples (voir [Len73]). Néanmoins, la construction de Motzkin s'applique pour montrer que certains anneaux sont euclidiens : par exemple sous GRH pour Weinberger ([Wei73]) ou sans condition pour $\mathbf{Z}(\sqrt{14})$ pour Harper ([Har04]).

CHAPITRE IV

CLASSES EUCLIDIENNES

Plan

1 Définitions et premières propriétés

1.1 Introduction

Tout anneau euclidien étant principal, on peut chercher à étendre cette notion aux anneaux non principaux. Lenstra ([Len78a]) a ainsi défini la notion d'idéal euclidien pour la norme.

Définition 1.1. Soient K un corps de nombres et I un idéal fractionnaire de K. On dit que I est euclidien pour la norme si pour tout $x \in K$, il existe $z \in I$ tel que

$$\left|\mathbf{N}_{K/\mathbf{Q}}(x-z)\right| < \mathbf{N}I. \tag{IV.1}$$

Remarquons que K est euclidien pour la norme si et seulement si l'idéal $\mathbf{Z}_K$ est euclidien pour la norme. Il existe néanmoins des idéaux euclidiens pour la norme non principaux.

L'exemple le plus élémentaire a été donné par Lenstra dans [Len78a].

Exemple 1.2. Soit $K = \mathbf{Q}\left(\sqrt{-5}\right)$, alors $\mathbf{Z}_K = \mathbf{Z}[\sqrt{-5}]$. Ce corps de nombres n'est pas principal, son nombre de classes est $\mathrm{h}_K = 2$. Le corps K admet un idéal euclidien pour la norme, il s'agit de l'idéal $I = (2\,,\, 1+\sqrt{-5})$ de norme 2.

Démonstration. Pour voir cela, il suffit de prouver la condition (IV.1) dans ce cas particulier, c'est-à-dire de montrer que pour tout $x \in K$, il existe $y \in I$ tel que

$$\left|\mathbf{N}_{K/\mathbf{Q}}(x-z)\right| < 2.$$

Comme $\mathbf{N}_{K/\mathbf{Q}}$ est le carré de la norme euclidienne, la figure IV.1 permet de conclure : on peut recouvrir le plan complexe par des disques centrés aux points de I de rayon $\frac{3\sqrt{5}}{5} < \sqrt{2}$. □

On peut faire le même raisonnement pour tous les corps quadratiques imaginaires, nous verrons cette propriété dans la proposition 4.19.

Néanmoins, les exemples de corps de nombres admettant un idéal euclidien pour la norme sont peu nombreux. En fait, en degré supérieur à 3 les seuls exemples non principaux précédemment connus sont pour les corps de nombres suivants :

- le corps cubique complexe de discriminant -283 (van der Linden, [Lin84]),
- le corps cubique complexe de discriminant -331 (Lemmermeyer, [Lem95]),
- le corps de signature $(0\,,\,2)$ et de discriminant 1 521 (Lenstra, [Len78a]).

L'objectif de ce chapitre va donc être de décrire des techniques pour en obtenir d'autres. Ce chapitre contient les résultats exposés dans l'article [Lez12b], paru à l'*International Journal of Number Theory*. Avant de revenir aux idéaux euclidiens pour la norme au paragraphe 2.3, on va se placer dans un cadre plus général.

1.2 Définition générale

Soit R un anneau de Dedekind, les *idéaux fractionnaires* de R sont les éléments de la forme $\left\{\frac{1}{b}I,\ b \in R \setminus \{0\},\ I \text{ idéal de } R\right\}$. On note E l'ensemble des idéaux fractionnaires de R contenant R et $K = \mathrm{Frac}(R)$.

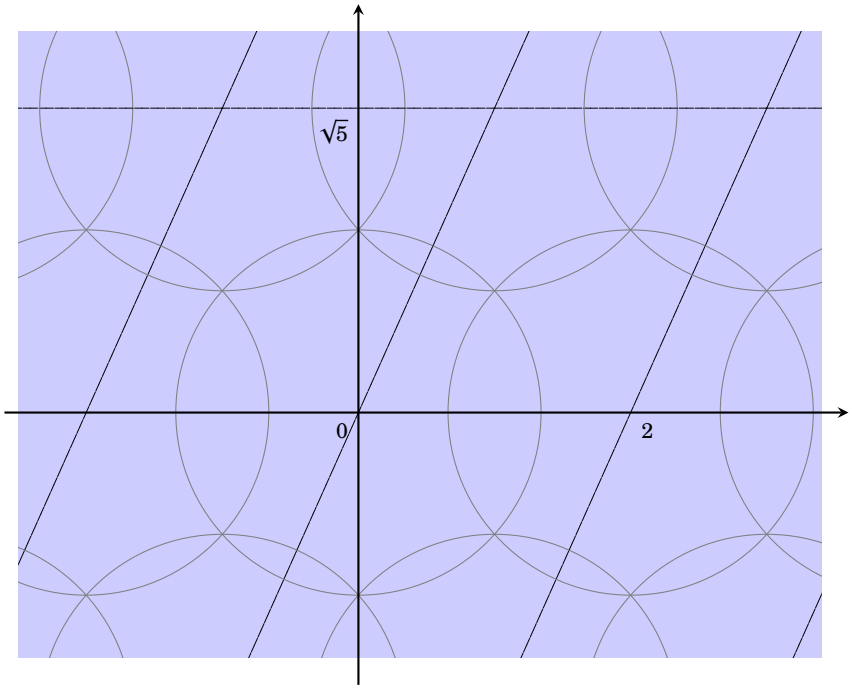


FIGURE IV.1 – On peut recouvrir le plan complexe par des disques de rayon $\frac{3\sqrt{5}}{5}$ centrés aux points de coordonnées dans l'idéal $I = \left(2, 1+\sqrt{-5}\right)$ de norme 2 de $\mathbf{Z}_K$.

Définition 1.3. Soient $\mathfrak{c}$ un idéal fractionnaire non nul, W un ensemble muni d'un bon ordre et φ une fonction de E dans W. On dit que φ est un *algorithme d'Euclide* pour $\mathfrak{c}$ si pour tout $\mathfrak{b} \in E$ et tout $x \in \mathfrak{b}\mathfrak{c} \setminus \mathfrak{c}$, il existe un élément $y \in \mathfrak{c}$ tel que

$$\varphi\left((x+y)^{-1}\mathfrak{b}\mathfrak{c}\right) < \varphi(\mathfrak{b}). \tag{IV.2}$$

Si (IV.2) est vérifiée, on dira aussi que $\mathfrak{c}$ est un idéal euclidien pour φ, ou encore que φ est un *stathme* pour $\mathfrak{c}$. La condition (IV.2) généralise la notion classique d'idéal euclidien pour la norme. En effet, pour un corps de nombres K, si $R = \mathbf{Z}_K$, $\mathfrak{c}$ est un idéal entier non nul de K et $\varphi : \begin{cases} E & \longrightarrow & \mathbf{N} \\ \mathfrak{b} & \longmapsto & \mathbf{N}^{-1}\mathfrak{b} - 1 \end{cases}$, alors la condition (IV.2) équivaut à la condition (IV.1). En particulier, R est euclidien (au sens classique) si et seulement s'il existe un algorithme d'Euclide pour R. On peut aussi en déduire la propriété suivante.

Proposition 1.4. *Si l'idéal non nul $\mathfrak{c}$ entier du corps de nombres K est euclidien pour la norme, alors pour tout idéal entier $I \neq R$, il existe un idéal entier J tel que*

$$\mathbf{N}J < \mathbf{N}I \qquad \text{et} \qquad [I] = [J\mathfrak{c}].$$

Démonstration. Il suffit d'appliquer (IV.2) avec $\mathfrak{b} = I^{-1}$ et $J = (x+y)I\mathfrak{c}^{-1}$. □

Il est aussi important de noter que le fait que $\mathfrak{c}$ est un idéal euclidien ne dépend que de la classe $[\mathfrak{c}]$ de $\mathfrak{c}$ dans le groupe des classes. Plus précisément, on a la propriété suivante.

Proposition 1.5. *Soient $\mathfrak{c}$ un idéal fractionnaire non nul, W un ensemble bien ordonné et $\varphi : E \longrightarrow W$. Si φ est un algorithme d'Euclide pour $\mathfrak{c}$, alors c'est aussi un algorithme d'Euclide pour tout $\mathfrak{d} \in [\mathfrak{c}]$.*

Démonstration. Soit $\mathfrak{d} \in [\mathfrak{c}]$. Alors il existe $k \in K^\times$ tel que $\mathfrak{d} = k\mathfrak{c}$. Soient alors $\mathfrak{b} \in E$ et $x \in \mathfrak{b}\mathfrak{d} \setminus \mathfrak{d}$. Dès lors $k^{-1}x \in \mathfrak{b}\mathfrak{c} \setminus \mathfrak{c}$. Or $\mathfrak{c}$ est euclidien, donc il existe $y \in \mathfrak{c}$ tel que

$$\varphi\left((k^{-1}x + y)^{-1}\mathfrak{b}\mathfrak{c}\right) < \varphi(\mathfrak{b}).$$

Cela peut se récrire

$$\varphi\left((x + ky)^{-1}\mathfrak{b}\mathfrak{d}\right) < \varphi(\mathfrak{b}).$$

Comme $ky \in \mathfrak{d}$, cela montre que φ est un algorithme d'Euclide pour $\mathfrak{d}$. □

En particulier, on peut parler de classe euclidienne.

Définition 1.6. Soit C une classe d'idéaux inversible. On dit que C est une *classe euclidienne* s'il existe $\mathfrak{c} \in C$ tel que $\mathfrak{c}$ est un idéal euclidien. En ce cas, tout idéal $\mathfrak{d} \in C$ est en fait un idéal euclidien.

Notons que si C est une classe euclidienne, alors tous les idéaux de C sont euclidiens pour le même algorithme d'Euclide. On peut donc dire que C est une *classe euclidienne pour la norme* s'il existe $\mathfrak{c} \in C$ tel que $\mathfrak{c}$ est un idéal euclidien pour la norme. En ce cas, tous les idéaux $\mathfrak{d} \in C$ sont des idéaux euclidiens pour la norme.

2 Propriétés des classes euclidiennes

2.1 Algorithme d'Euclide minimal et construction de Motzkin

2.1.1 Définition de l'algorithme d'Euclide minimal

Soit R un anneau de Dedekind qui admet une classe C euclidienne non nulle d'idéaux fractionnaires. On note $K = \mathrm{Frac}(R)$ et E l'ensemble des idéaux fractionnaires de R qui contiennent R. On considère la famille $(\varphi_\alpha)_\alpha$ des algorithmes d'Euclide pour $\mathfrak{c}$ à valeurs dans W.

Comme dans le cas classique, on a la propriété suivante.

Lemme 2.1. *La fonction* $\theta : \left\{ \begin{array}{ccc} E & \longrightarrow & W \\ \mathfrak{b} & \longmapsto & \inf_\alpha \varphi_\alpha(\mathfrak{b}) \end{array} \right.$ *est un algorithme d'Euclide pour $\mathfrak{c}$ et W.*

Démonstration. C'est une conséquence facile du fait que W est muni d'un bon ordre. □

Ainsi, la fonction θ définie par le lemme 2.1 est appelée *algorithme d'Euclide minimal* pour $\mathfrak{c}$. Notons que c'est aussi l'algorithme d'Euclide minimal pour tous les idéaux $\mathfrak{d} \in C$. On dira donc aussi parfois que θ est l'algorithme d'Euclide minimal pour la classe C. Signalons enfin que l'on utilisera parfois la terminologie « stathme » dans ce cadre et que l'on dira donc que θ est un *stathme minimal* pour C.

2.1.2 Propriétés de l'algorithme d'Euclide minimal

Comme dans le cas classique, l'ensemble des valeurs prises par l'algorithme d'Euclide minimal θ pour C « n'a pas de trou ». Plus précisément, il vérifie la propriété suivante.

Lemme 2.2. *Soient $\alpha, \beta \in W$ tels que $\alpha < \beta$ et α est le plus grand élément de W ayant cette propriété. S'il existe $\mathfrak{b} \in E$ tel que $\theta(\mathfrak{b}) = \beta$, alors il existe $\mathfrak{a} \in E$ tel que $\theta(\mathfrak{a}) = \alpha$.*

Démonstration. Par l'absurde, s'il n'existe aucun $\mathfrak{a} \in E$ tel que $\theta(\mathfrak{a}) = \alpha$, on définit la fonction $\vartheta : \left\{ \begin{array}{ccc} E & \longrightarrow & W \\ \mathfrak{d} & \longmapsto & \left\{ \begin{array}{ll} \alpha & \text{si } \mathfrak{d} = \mathfrak{b} \\ \theta(\mathfrak{b}) & \text{sinon} \end{array} \right. \end{array} \right.$. On va montrer que ϑ est un algorithme d'Euclide pour C. Soient donc $\mathfrak{c} \in C$, $\mathfrak{d} \in E$ et $x \in \mathfrak{d}\mathfrak{c} \setminus \mathfrak{c}$. Alors il existe $y \in \mathfrak{c}$ tel que

$$\theta\left((x+y)^{-1}\mathfrak{d}\mathfrak{c}\right) < \theta(\mathfrak{d}).$$

Si $\mathfrak{b} \neq (x+y)^{-1}\mathfrak{d}\mathfrak{c}$ et $\mathfrak{b} \neq \mathfrak{d}$, on obtient comme désiré

$$\vartheta\left((x+y)^{-1}\mathfrak{d}\mathfrak{c}\right) < \vartheta(\mathfrak{d}).$$

Il reste donc à traiter les deux cas suivants :

- si $\mathfrak{b} = \mathfrak{d}$, alors $\theta\left((x+y)^{-1}\mathfrak{d}\mathfrak{c}\right) < \beta$, mais α n'est pas atteint par θ, donc on a en fait $\theta\left((x+y)^{-1}\mathfrak{d}\mathfrak{c}\right) < \alpha$. Par conséquent,

$$\vartheta\left((x+y)^{-1}\mathfrak{d}\mathfrak{c}\right) \leqslant \theta\left((x+y)^{-1}\mathfrak{d}\mathfrak{c}\right) < \alpha = \vartheta(\mathfrak{d}).$$

- si $\mathfrak{b} = (x+y)^{-1}\mathfrak{d}\mathfrak{c}$ et $\mathfrak{d} \neq \mathfrak{b}$, alors $\vartheta(\mathfrak{d}) = \theta(\mathfrak{d}) > \beta$, donc

$$\vartheta\left((x+y)^{-1}\mathfrak{d}\mathfrak{c}\right) = \alpha < \vartheta(\mathfrak{d}).$$

Cela montre que ϑ est un algorithme d'Euclide pour C, ce qui est incompatible avec le fait que θ est l'algorithme d'Euclide minimal pour C. De cette contradiction, on déduit que la valeur α est aussi atteinte par θ.

□

Comme pour la construction de Motzkin classique, on définit pour tout $i \in W$, $A_{i,\mathfrak{c}} := \{\mathfrak{b} \in E,\ \theta(\mathfrak{b}) \leqslant i\}$ et $A'_{i,\mathfrak{c}} := \{\mathfrak{b} \in E,\ \theta(\mathfrak{b}) < i\}$.

Remarque 2.3. Soit $\mathfrak{b} \in E$. Alors $\theta(\mathfrak{b}) = 0$ si et seulement si $\mathfrak{b} = R$. De plus pour $i \geqslant 1$, $\theta(\mathfrak{b}) = i$ si et seulement si $\mathfrak{b} \in A_{i,\mathfrak{c}} \setminus A'_{i,\mathfrak{c}}$.

Démonstration. Si $\theta(\mathfrak{b}) = 0$, alors il ne peut exister aucun $x \in \mathfrak{b}\mathfrak{c} \setminus \mathfrak{c}$ tel que (IV.2) soit vérifiée. Ainsi, $\mathfrak{b}\mathfrak{c} = \mathfrak{c}$, donc $\mathfrak{b} = R$ car $\mathfrak{c}$ est inversible.

L'autre propriété est claire par définition des ensembles $A_{i,\mathfrak{c}}$ et $A'_{i,\mathfrak{c}}$. □

Proposition 2.4. *Pour tout $i \in \mathbf{N}$, les ensembles $A_{i,\mathfrak{c}}$ et $A'_{i,\mathfrak{c}}$ sont liés par la relation*

$$A_{i,\mathfrak{c}} = \{R\} \bigcup \left\{\mathfrak{b} \in E,\ \forall x \in\ \mathfrak{b}\mathfrak{c} \setminus \mathfrak{c},\ \exists y \in \mathfrak{c},\ (x+y)^{-1}\mathfrak{b}\mathfrak{c} \in A'_{i,\mathfrak{c}}\right\}.$$

Démonstration. Si $\mathfrak{b} \in A_{i,\mathfrak{c}} \setminus \{R\}$, alors d'après (IV.2), pour tout $x \in \mathfrak{bc} \setminus \{c\}$, il existe $y \in \mathfrak{c}$ tel que

$$\theta((x+y)^{-1}\mathfrak{bc}) < \theta(\mathfrak{b}) = i.$$

Donc $(x+y)^{-1}\mathfrak{bc} \in A'_{i,\mathfrak{c}}$.

Réciproquement, si $\mathfrak{b} \in \left\{\mathfrak{b} \in E,\ \forall x \in \mathfrak{bc} \setminus \mathfrak{c},\ \exists y \in \mathfrak{c},\ (x+y)^{-1}\mathfrak{bc} \in A'_{i,\mathfrak{c}}\right\}$, on suppose par l'absurde que $\theta(\mathfrak{b}) > i$. On définit alors la fonction

$$\vartheta : \begin{cases} E & \longrightarrow & W \\ \mathfrak{u} & \longmapsto & \begin{cases} \theta(\mathfrak{u}) & \text{si } \mathfrak{u} \neq \mathfrak{b} \\ i & \text{si } \mathfrak{u} = \mathfrak{b} \end{cases} \end{cases}.$$

Alors ϑ est un algorithme d'Euclide pour $\mathfrak{c}$. En effet, si $\mathfrak{b} \neq \mathfrak{u}$, alors pour tout $x \in \mathfrak{uc} \setminus \mathfrak{c}$, il existe $y \in \mathfrak{c}$ tel que

$$\vartheta((x+y)^{-1}\mathfrak{uc}) \leqslant \theta((x+y)^{-1}\mathfrak{uc}) < \theta(\mathfrak{u}) = \vartheta(\mathfrak{u}).$$

Si $\mathfrak{b} = \mathfrak{u}$, alors par hypothèse, pour tout $x \in \mathfrak{bc} \setminus \mathfrak{c}$, il existe $y \in \mathfrak{c}$ tel que $(x+y)^{-1}\mathfrak{bc} \in A'_{i,\mathfrak{c}}$, c'est-à-dire

$$\theta((x+y)^{-1}\mathfrak{bc}) < i = \vartheta(\mathfrak{b}).$$

Ainsi, $\vartheta((x+y)^{-1}\mathfrak{bc}) \leqslant \theta((x+y)^{-1}\mathfrak{bc}) < \vartheta(\mathfrak{b})$. Mais θ est le stathme minimal, donc ϑ ne peut pas être un algorithme d'Euclide. Ainsi, $\theta(\mathfrak{b}) \leqslant i$ et $\mathfrak{b} \in A_{i,\mathfrak{c}}$. □

Avant d'utiliser cette propriété pour la construction de Motzkin, signalons la propriété suivante qui s'appliquera dans tous les cas qui nous intéressent.

Corollaire 2.5. *Si pour tout idéal I entier non nul de R le quotient R/I est fini, alors l'algorithme d'Euclide minimal pour C est à valeurs dans* $\mathbf{N}$.

Démonstration. Soit $\mathfrak{b} \in E$, on choisit $\mathfrak{c} \in C$ entier. Notons que $\mathfrak{bc}/\mathfrak{c}$ est un $R/\mathfrak{b}^{-1}$-module de type fini. Comme $R/\mathfrak{b}^{-1}$ est fini par hypothèse, cela implique que $\mathfrak{bc}/\mathfrak{c}$ est lui aussi fini.

On suppose maintenant que l'algorithme minimal θ n'est pas à valeurs dans $\mathbf{N}$. On note ω le premier ordinal transfini atteint par θ. Il existe alors $\mathfrak{b} \in E$ tel que $\theta(\mathfrak{b}) = \omega$. Soit $\mathcal{S}$ un système de représentants de $\mathfrak{bc}/\mathfrak{c} \setminus \{\mathfrak{c}\}$. Pour tout $x \in \mathcal{S}$, il existe $y_x \in \mathfrak{c}$ tel que

$$\theta((x+y_x)^{-1}\mathfrak{bc}) < \vartheta(\mathfrak{b}) = \omega,$$

donc $\theta((x+y_x)^{-1}\mathfrak{bc}) = n_x \in \mathbf{N}$. On pose $N = \sup_{x\in\mathcal{S}} n_x + 1$, qui est fini car $\mathcal{S}$ est fini. Alors, d'après la proposition 2.4, $\theta(\mathfrak{b}) \leqslant N$, donc $\mathfrak{b} \in A_{N,\mathfrak{c}}$, ce qui est faux. On obtient donc une contradiction, et ainsi θ est à valeurs dans $\mathbf{N}$. □

Si R est l'anneau des entiers d'un corps de nombres, alors pour tout idéal I entier non nul de R, le quotient R/I est fini. On supposera donc dans la suite que cette hypothèse est vérifiée et ainsi que $W = \mathbf{N}$.

2.1.3 Construction de Motzkin

On ne suppose plus que R admet une classe euclidienne, donc on ne peut plus définir les ensembles $A_{i\mathfrak{c}}$ comme au paragraphe précédent via l'algorithme minimal. Toutefois, on peut encore définir récursivement les sous-ensembles de E suivants :

– $A_{0,\mathfrak{c}} = \{R\}$,
– pour $i \in \mathbf{N}$,

$$A_{i+1,\mathfrak{c}} := A_{i,\mathfrak{c}} \bigcup \left\{\mathfrak{b} \in E,\ \forall x \in\ \mathfrak{b}\mathfrak{c} \setminus \mathfrak{c},\ \exists y \in \mathfrak{c},\ (x+y)^{-1}\mathfrak{b}\mathfrak{c} \in A_{i,\mathfrak{c}}\right\}.$$

Lemme 2.6. *Pour $i \in \mathbf{N}$, l'ensemble $A_{i,\mathfrak{c}}$ ne dépend que de la classe C, on le notera donc $A_{i,C}$.*

Démonstration. On raisonne par récurrence sur $i \in \mathbf{N}$.
– Si $i = 0$, la définition ne dépend pas de $\mathfrak{c}$.
– On suppose que la définition de $A_{i,\mathfrak{c}}$ ne dépend que de la classe de $\mathfrak{c}$. On prend $\mathfrak{d} \in C$, alors on peut écrire $\mathfrak{d} = k\mathfrak{c}$ où $k \in K$.
Soit alors $x \in \mathfrak{b}\mathfrak{d} \setminus \mathfrak{d}$, alors $k^{-1}x \in \mathfrak{b}\mathfrak{c} \setminus \mathfrak{c}$, donc il existe $y' \in \mathfrak{c}$ tel que

$$(k^{-1}x + y')^{-1}\mathfrak{b}\mathfrak{c} \in A_{i,C},$$

mais $(k^{-1}x + y')^{-1}\mathfrak{b}\mathfrak{c} = (x + ky')^{-1}\mathfrak{b}k\mathfrak{c} = (x+y)^{-1}\mathfrak{b}\mathfrak{d}$, où $y = ky' \in k\mathfrak{c} = \mathfrak{d}$. Par hypothèse de récurrence, cela montre que la définition de $A_{i+1,\mathfrak{c}}$ ne dépend que de C, ce qui achève la preuve.

□

On peut alors définir $A_C = \bigcup_{i=1}^{\infty} A_{i,C}$, ce qui permet d'énoncer la propriété suivante, qui relie naturellement l'euclidianité et la construction de Motzkin.

Proposition 2.7. *Soient R un anneau de Dedekind et C une classe d'idéaux inversible. Si $A_C = E$, alors l'application $\vartheta : E \longrightarrow \mathbf{N}$ définie par $\vartheta(R) = 0$ et $\vartheta(\mathfrak{b}) = i$ si $\mathfrak{b} \in A_{i,C} \setminus A_{i-1,C}$ est un algorithme d'Euclide pour C. Réciproquement, si R est euclidien par rapport à la classe C et $\mathbf{N}$, alors $A_C = E$.*

Démonstration. Si $A_C = E$, il suffit de vérifier que ϑ vérifie (IV.2). On choisit $\mathfrak{c} \in C$. Soient donc $\mathfrak{b} \in E \setminus \{R\}$ et $x \in \mathfrak{b}\mathfrak{c} \setminus \mathfrak{c}$. Comme $A_C = E$, il existe $i \in \mathbf{N}$ tel que $\vartheta(\mathfrak{b}) = i+1$. Par construction, il existe $y \in \mathfrak{c}$ tel que $(x+y)^{-1}\mathfrak{b}\mathfrak{c} \in A_{i,C}$, donc

$$\vartheta((x+y)^{-1}\mathfrak{b}\mathfrak{c}) \leqslant i < i+1 = \vartheta(\mathfrak{b}).$$

Réciproquement, si C est une classe euclidienne, il suffit de remarquer que les ensembles $A_{i,\mathfrak{c}}$ du paragraphe précédent coïncident avec les ensembles $A_{i,C}$ considérés ici. □

Remarque 2.8. Le stathme défini par la proposition précédente est l'algorithme d'Euclide minimal pour C. On retrouve ainsi le fait que l'algorithme d'Euclide minimal ne dépend que de la classe C.

2.1.4 Calcul de $A_{1,C}$

Comme dans la construction de Motzkin classique, on cherche à déterminer $A_{1,C}$ en toute généralité grâce à l'algorithme d'Euclide minimal θ pour C.

Le lemme élémentaire suivant va se révéler utile.

Lemme 2.9 ([Len78a, 1.12])**.** *Pour $\mathfrak{a},\ \mathfrak{b} \in E$, $\theta(\mathfrak{a}\mathfrak{b}) \geqslant \theta(\mathfrak{a}) + \theta(\mathfrak{b})$.*

Démonstration. Fixons $\mathfrak{a} \in E$, comme $R \subseteq \mathfrak{a}$, on a $\theta(\mathfrak{a}) \leqslant \theta(\mathfrak{ab})$, ce qui permet de définir $\chi_{\mathfrak{a}} : \left\{ \begin{array}{ccc} E & \longrightarrow & \mathbf{N} \\ \mathfrak{b} & \longmapsto & \theta(\mathfrak{ab}) - \theta(\mathfrak{a}) \end{array} \right.$. Comme $R \subseteq \mathfrak{a}$, pour tout $x \in \mathfrak{bc} \setminus \mathfrak{c}$, il existe $y \in \mathfrak{c}$ tel que

$$\chi_{\mathfrak{a}}\left((x+y)^{-1}\mathfrak{bc}\right) + \theta(\mathfrak{a}) = \theta\left((x+y)^{-1}\mathfrak{abc}\right) < \theta(\mathfrak{ab}) = \chi_{\mathfrak{a}}(\mathfrak{b}) + \theta(\mathfrak{a}),$$

cela montre que $\chi_{\mathfrak{a}}$ est un algorithme d'Euclide pour C à valeurs dans $\mathbf{N}$, donc pour tout $\mathfrak{b} \in E$, $\chi_{\mathfrak{a}}(\mathfrak{b}) \geqslant \theta(\mathfrak{b})$. □

Proposition 2.10. *Soit $\mathfrak{b} \in E$. Les propriétés suivantes sont équivalentes.*

1. $\theta(\mathfrak{b}) = 1$,
2. $\mathfrak{p} = \mathfrak{b}^{-1}$ *est un idéal (entier) premier non nul de R tel que $\mathfrak{p} \in C$ et l'application naturelle $R^\times \longrightarrow \left(\frac{R}{\mathfrak{p}}\right)^\times$ est surjective.*

Cette propriété est énoncée dans [Len78a, 1.13], nous allons donner plus de précisions sur la preuve.

Démonstration. – On suppose d'abord que $\mathfrak{p} = \mathfrak{b}^{-1}$ est un idéal (entier) premier non nul de R tel que $\mathfrak{p} \in C$ et l'application naturelle $R^\times \longrightarrow \left(\frac{R}{\mathfrak{p}}\right)^\times$ est surjective. Suivant la remarque 2.3, on cherche à montrer que $\mathfrak{b} \in A_{1,C} \setminus A_{0,C}$.
Pour ce faire, remarquons d'abord que $\mathfrak{b} \neq R$ vu que $\mathfrak{p}$ est premier, donc $\mathfrak{b} \notin A_{0,C}$.
Comme $\mathfrak{p} \in C$ et $\mathfrak{bp} = R$, il s'agit alors de vérifier la propriété suivante :

$$\forall x \in R \setminus \mathfrak{p},\ \exists y \in \mathfrak{p},\ (x+y)^{-1}R = R.$$

Comme R est un anneau de Dedekind, l'idéal $\mathfrak{p}$ premier non nul est en fait maximal et on peut identifier $\left(\frac{R}{\mathfrak{p}}\right)^\times$ et $R \setminus \mathfrak{p}$. Ainsi, par hypothèse, il existe $z \in R^\times$ tel que $z - x \in \mathfrak{p}$. On pose alors $y = z - x \in \mathfrak{p}$. Comme $x + y \in R^\times$, on a $R = R(x+y)$, ce qui était la propriété recherchée.
Cela montre que $\theta(\mathfrak{b}) = 1$.

– Comme $\mathfrak{b} \neq \{0\}$, on pose $\mathfrak{p} = \mathfrak{b}^{-1}$, c'est a priori un idéal fractionnaire non nul de R. Mais $R \subseteq \mathfrak{b}$, donc $\mathfrak{p} \subseteq R$, ce qui montre que $\mathfrak{p}$ est un idéal entier de R.
On écrit $\mathfrak{p} = \mathfrak{p}_1\mathfrak{p}_2$, avec $\mathfrak{p}_1$, $\mathfrak{p}_2$ idéaux fractionnaires de R, qui sont en fait entiers vu que $\mathfrak{p}$ l'est. On note $\mathfrak{b}_1 = \mathfrak{p}_1^{-1}$ et $\mathfrak{b}_2 = \mathfrak{p}_2^{-1}$, comme $\mathfrak{p}_1$ et $\mathfrak{p}_2$ sont entiers, $\mathfrak{b}_1$ et $\mathfrak{b}_1$ sont des éléments de E. Par définition, ils vérifient $\mathfrak{b} = \mathfrak{b}_1\mathfrak{b}_2$. Par conséquent, d'après le lemme 2.9, on a

$$1 = \theta(\mathfrak{b}) \geqslant \theta(\mathfrak{b}_1) + \theta(\mathfrak{b}_2).$$

Quitte à échanger $\mathfrak{b}_1$ et $\mathfrak{b}_2$, on suppose que $\theta(\mathfrak{b}_1) = 1$ et $\theta(\mathfrak{b}_2) = 0$. Ainsi, $\mathfrak{b}_2 = R$, ce qui montre que $\mathfrak{p}_2 = R$ et que $\mathfrak{p}_1 = \mathfrak{p}$. Comme R est un anneau de Dedekind, on en déduit que $\mathfrak{p}$ est premier (et même maximal).
Soit alors $x \in \mathfrak{bc} \setminus \mathfrak{c}$. Comme $\mathfrak{b} \in A_{1,C}$, il existe $y \in \mathfrak{c}$ tel que $(x+y)^{-1}\mathfrak{bc} = R$. Donc $\mathfrak{p} = (x+y)^{-1}\mathfrak{c}$ et ainsi on trouve que $\mathfrak{p} \in C$.
On peut donc raisonner avec $\mathfrak{p}$ comme élément de référence de C. Comme $\mathfrak{bp} = R$ et $\mathfrak{b} \in A_{1,C}$, on a la propriété suivante :

$$\forall x \in R \setminus \mathfrak{p},\ \exists y \in \mathfrak{p},\ (x+y)^{-1}R = R,$$

ce qui équivaut à

$$\forall x \in R \setminus \mathfrak{p},\ \exists z \in R,\ Rz = R,\ \text{et } z - x \in \mathfrak{p}.$$

La condition $Rz = R$ étant équivalente à $z \in R^\times$ pour $z \in R$, et comme $\left(\frac{R}{\mathfrak{p}}\right)^\times$ peut être identifié avec $R \setminus \mathfrak{p}$, la propriété précédente est l'expression de la surjectivité de l'application naturelle

$$R^\times \longrightarrow \left(\frac{R}{\mathfrak{p}}\right)^\times.$$

Cela achève la preuve.

□

Exemple 2.11. On prend $R = \mathbf{Z}$, $C = [\mathbf{Z}]$, alors $A_{1,[\mathbf{Z}]} = \left\{\frac{\mathbf{Z}}{b},\ 1 \leqslant b \leqslant 3\right\}$

En effet, si $\mathfrak{b} \in A_{1,[\mathbf{Z}]} \setminus \mathbf{Z}$, alors on écrit $\mathfrak{p} = \mathfrak{b}^{-1}$ qui est un idéal premier de $\mathbf{Z}$, donc $\mathfrak{p} = p\mathbf{Z}$ pour un certain nombre premier p. Un tel p convient si et seulement si l'application naturelle

$$\mathbf{Z}^\times \longrightarrow \left(\frac{\mathbf{Z}}{p\mathbf{Z}}\right)^\times$$

est surjective, ce qui est le cas pour $p \in \{2, 3\}$ exactement.

2.2 Forme adaptée pour le stathme et idéaux de petit stathme

Dans cette partie, on considère K un corps de nombres, R l'anneau des entiers de K, E est l'ensemble des idéaux fractionnaires de R qui contiennent R.

Lemme 2.12. *Si $\psi : E \longrightarrow \mathbf{N}$ est un algorithme d'Euclide pour R par rapport à la classe C, alors, pour $\mathfrak{b} \in E$, $\psi(\mathfrak{b}) = \min_{\mathfrak{a} \in E} \psi(\mathfrak{a})$ implique que $\mathfrak{b} = R$.*

Démonstration. On suppose que $\mathfrak{b} \neq R$, on note $\mathfrak{c}$ un élément de C. Alors, comme $\mathfrak{c} \neq R$, il existe $x \in \mathfrak{b}\mathfrak{c} \setminus \mathfrak{c}$, donc il existe $z \in x + \mathfrak{c}$ tel que

$$\psi(\mathfrak{b}\mathfrak{c}z^{-1}) < \psi(\mathfrak{b}).$$

Comme $\mathfrak{b}\mathfrak{c}z^{-1} \in E$, cela contredit l'hypothèse selon laquelle $\mathfrak{b}$ est de stathme minimal.

□

Le lemme suivant qui relie stathme et classe d'idéaux est crucial.

Lemme 2.13 ([Len78a, 1.2])**.** *On suppose que l'anneau R admet pour algorithme d'Euclide $\psi : E \longrightarrow \mathbf{N}$ par rapport à la classe C. Alors pour tout $\mathfrak{b} \in E$, il existe un entier $n \in \mathbf{N}$ tel que*

$$[\mathfrak{b}] = C^{-n} \text{ et } n \leqslant \psi(\mathfrak{b}).$$

De plus, si $\psi(\mathfrak{b}) > 0$, alors $n > 0$.

Démonstration. On raisonne par récurrence sur $\psi(\mathfrak{b})$.

– Si $\psi(\mathfrak{b}) = 0$, alors, d'après le lemme 2.12, $\mathfrak{b} = R$.

– Soit $\mathfrak{b} \in E$, tel que $\psi(\mathfrak{b}) \geqslant 1$, on suppose que pour tout $\mathfrak{a} \in E$ vérifiant $\psi(\mathfrak{a}) < \psi(\mathfrak{b})$, il existe un entier $m \leqslant \psi(\mathfrak{a})$ tel que $[\mathfrak{a}] = C^{-m}$. Comme $\psi(\mathfrak{b}) \geqslant 1$, $\mathfrak{b} \neq R$, donc en fixant un élément $\mathfrak{c} \in C$, on a $\mathfrak{bc} \supsetneq \mathfrak{c}$. Ainsi, il existe $z \in x + \mathfrak{c}$ tel que

$$\psi(\mathfrak{bc}z^{-1}) < \psi(\mathfrak{b}),$$

car ψ est un algorithme d'Euclide par rapport à C. On note $\mathfrak{a} = \mathfrak{bc}z^{-1} \in E$.
Par hypothèse de récurrence, il existe un entier $m \leqslant \psi(\mathfrak{a})$ tel que $[\mathfrak{a}] = C^{-m}$. Mais par définition, on a

$$[\mathfrak{b}] = [\mathfrak{a}] \cdot [\mathfrak{c}]^{-1} = C^{-(m+1)}.$$

Comme $m + 1 \leqslant \psi(\mathfrak{b})$, cela permet de conclure.

□

Proposition 2.14. *On suppose que R est euclidien par rapport à la classe C et on considère un élément $\mathfrak{b} \in E \setminus \{R\}$ tel que $\psi(\mathfrak{b}) = \min_{\mathfrak{a} \in E \setminus \{R\}} \psi(\mathfrak{a})$, alors $\mathfrak{b} \in C^{-1}$.*

Remarque 2.15. On dira parfois qu'un tel élément $\mathfrak{b} \in E \setminus \{R\}$ est un élément de *stathme minimal*.

Démonstration. Il s'agit simplement d'appliquer le lemme 2.13 avec un idéal $\mathfrak{b} \in E$ tel que $\psi(\mathfrak{b}) = 1$. Alors $[\mathfrak{b}] = C^{-1}$, ce qui exactement la propriété recherchée. □

Le lemme 2.13 a quelques conséquences importantes dans le cas principal.

Proposition 2.16. *Soit K un corps de nombres dont l'anneau des entiers algébriques R admet une classe d'idéaux euclidienne C.*

– *R est principal si et seulement si C est la classe principale $[R]$.*
– *R est principal si et seulement s'il existe un élément de stathme minimal $\mathfrak{b} \in E \setminus \{R\}$ tel que $\mathfrak{b}^{-1}$ est un idéal principal de R.*

Démonstration. Pour le premier point, il suffit de voir que les éléments de E sont exactement les inverses des idéaux entiers de R. Comme C engendre le groupe des classes d'idéaux, on a le résultat souhaité.

Pour le second point, il suffit de remarquer que $C = \left[\mathfrak{b}^{-1}\right]$ d'après la proposition 2.14 et d'appliquer le premier point. □

Dans le cas général, le lemme 2.13 est essentiel pour prouver des propriétés très importantes des classes euclidiennes.

Théorème 2.17. *Soit R l'anneau des entiers d'un corps de nombres. Alors R admet au plus une classe d'idéaux euclidienne pour un stathme donné. De plus, si R admet une classe euclidienne C, alors le groupe des classes de R est cyclique, engendré par C.*

Démonstration. Le fait que la classe euclidienne est unique, si elle existe, est une conséquence immédiate de la proposition 2.14.

De plus, si R admet une classe euclidienne C, alors pour tout idéal I entier non nul, on a $I^{-1} \in E$, donc d'après le lemme 2.13, il existe $n \in \mathbf{N}$ tel que $[I] = C^n$. Cela montre que le groupe des classes de R est cyclique, engendré par C.

□

2.3 Cas de la norme, propriété des idéaux de petite norme

Dans cette partie, on considère encore le cas où K est un corps de nombres et R son anneau des entiers. On va énoncer un résultat cité dans [Len78a] qui peut s'avérer utile.

Proposition 2.18 ([Len78a, 2.2])**.** *On suppose que R admet une classe euclidienne C par rapport à la norme. Soit $\mathfrak{c}$ un idéal entier de R non nul, différent de R tel que*

$$N(\mathfrak{c}) = \Lambda(K) = \min\{N(\mathfrak{a})\ ,\ \mathfrak{a} \text{ idéal entier de } R \text{ non nul, différent de } R\}\ .$$

Alors $\mathfrak{c}$ est élément de la classe euclidienne C.

Ce résultat est la reformulation de la proposition 2.14 dans le cas particulier où l'algorithme d'Euclide est la norme. On peut de même écrire le lemme 2.13 dans ce cas.

Lemme 2.19. *On suppose que R admet une classe euclidienne C par rapport à la norme. Alors pour tout idéal entier I non nul, il existe un entier naturel $n < \mathbf{N}I$ tel que $[I] = C^n$. De plus n est nul si et seulement si $I = R$.*

En fait, les propriétés de la norme permettent d'améliorer légèrement ce résultat.

Lemme 2.20 ([Lin84, Proposition 2.9])**.** *On suppose que R admet une classe euclidienne C par rapport à la norme. On note $\mathcal{P}$ l'ensemble des puissances de premiers strictement supérieures à 1 qui sont des normes d'idéaux entiers de R. Alors pour tout idéal entier I non nul de R, il existe un entier naturel $n \leqslant \#\{q \in \mathcal{P},\ q \leqslant \mathbf{N}I\}$ tel que*

$$[I] = C^n.$$

Démonstration. On raisonne par récurrence sur $\mathbf{N}I$. Si $\mathbf{N}I = \Lambda(K)$, alors d'après la proposition 2.18, $[I] = C$ et la propriété est vérifiée.

Si $\mathbf{N}I > \Lambda(K)$, on commence par traiter le cas où $\mathbf{N}I$ est puissance d'un premier. On note $\mathfrak{c}$ un idéal non nul de C. D'après la proposition 1.4, il existe un idéal entier J tel que $\mathbf{N}J < \mathbf{N}I$ et $[I] = [J\mathfrak{c}]$. Alors par hypothèse de récurrence, il existe $n \leqslant \#\{q \in \mathcal{P},\ q \leqslant \mathbf{N}J\}$ tel que $[J] = C^n$, donc $[I] = C^{n+1}$ et

$$n + 1 \leqslant \{q \in \mathcal{P},\ q \leqslant \mathbf{N}J\} + 1 \leqslant \{q \in \mathcal{P},\ q \leqslant \mathbf{N}I\},$$

car $\mathbf{N}I \in \mathcal{P}$.

On traite à présent le cas où $\mathbf{N}I$ n'est pas puissance de premier. Alors I n'est pas un idéal premier. Donc il existe deux idéaux entiers non triviaux I_1 et I_2 tels que $I = I_1 I_2$. Par hypothèse de récurrence, il existe deux entiers n_1 et n_2 tels que pour tout $i \in \{1, 2\}$,

$$[I_i] = C^{n_i} \qquad \text{et} \qquad n_i \leqslant \#\{q \in \mathcal{P},\ q \leqslant \mathbf{N}I_i\}.$$

Comme on a alors $[I] = C^{n_1+n_2}$, il reste donc à prouver que $n_1+n_2 \leqslant \#\{q \in \mathcal{P},\ q \leqslant \mathbf{N}I\}$. Pour ce faire, il suffit de remarquer que si on fixe un premier p, alors $\mathbf{N}\mathfrak{a} = p^a \leqslant \mathbf{N}I_1$ et $\mathbf{N}\mathfrak{b} = p^b \leqslant \mathbf{N}I_2$ impliquent $\mathbf{N}(\mathfrak{a}\mathfrak{b}) \leqslant \mathbf{N}I$. □

Ces lemmes donnent une technique pour calculer le groupe des classes d'un corps de nombres euclidien par rapport à une certaine classe d'idéaux.

Proposition 2.21. *Soient K un corps de nombres et R l'anneau des entiers algébriques de K. On suppose que K admet une classe euclidienne pour la norme. Alors le groupe des classes de K est cyclique et engendré par $[\mathfrak{c}]$ où $\mathfrak{c}$ est un idéal propre entier de R de norme minimale.*

Démonstration. Cela résulte du fait que la classe euclidienne (lorsqu'elle existe) engendre le groupe des classes (théorème 2.17). □

Exemple 2.22. On prend $K = \mathbf{Q}\left(\sqrt{-5}\right)$, alors $\mathfrak{c} = (1+\sqrt{-5}, 2)$ est de norme 2 mais n'est pas principal, donc $\mathbf{Z}_K$ n'est pas principal. Néanmoins, R est euclidien par rapport à la classe $[\mathfrak{c}]$ pour la norme (voir exemple 1.2). Ainsi, son groupe des classes est engendré par $[\mathfrak{c}]$ et le nombre de classes est 2.

Remarquons que si K admet une classe euclidienne pour la norme, alors c'est la classe de n'importe quel idéal de norme minimale. Par contraposée, si deux idéaux de norme minimale ne sont pas dans la même classe, alors K n'admet pas de classe euclidienne pour la norme.

Exemples 2.23.
– Soit $K = \mathbf{Q}\left(\sqrt{229}\right)$, on a $\mathrm{h}_K = 3$ et $\mathbf{Z}_K = \mathbf{Z} + \mathbf{Z}\frac{\sqrt{229}-1}{2}$. Alors $\Lambda(K) = 3$ et les deux idéaux suivants sont de norme 3 :

$$I_1 = 3\mathbf{Z} + \mathbf{Z}\frac{\sqrt{229}-1}{2} \qquad \text{et} \qquad I_2 = 3\mathbf{Z} + \mathbf{Z}\frac{\sqrt{229}+1}{2}.$$

Ces idéaux ne sont pas principaux, $I_1 + I_2 = \mathbf{Z}_K$, donc $I_1 I_2 = I_1 \cap I_2 = 3\mathbf{Z}_K$, donc $[I_1] \neq [I_2]$. Par conséquent, K n'admet pas de classe euclidienne pour la norme.

– Posons $K = \mathbf{Q}(x)$, où $x^4 - x^3 - 32x^2 + 23x + 229 = 0$. Alors $\mathrm{h}_K = 3$, $\mathrm{disc}_K = 97025$ et $\Lambda(K) = 4$. Dans ce cas, $\mathbf{Z}_K$ admet deux idéaux I_1 et I_2 de norme 4. On peut prouver que $I_1 I_2 = 2\mathbf{Z}_K$, alors que I_1 et I_2 ne sont pas principaux. Donc $[I_1] \neq [I_2]$, ce qui prouve que K n'admet pas de classe euclidienne pour la norme.

Les paragraphes précédents donnent une technique pour trouver la classe euclidienne par rapport à la norme (si elle existe) étant donné un corps de nombres.

Algorithme 2.1 Détermination de l'existence d'une classe euclidienne pour la norme

ENTRÉE : un corps de nombres K d'anneaux des entiers R
SORTIE : dit si K admet ou non une classe euclidienne pour la norme

1: Calcul d'un idéal entier, propre I de R de norme minimale
2: On détermine si I et R sont principaux.
3: **si** I est principal **alors**
4: **si** R est principal **alors**
5: R peut être euclidien par rapport à la norme. On le teste de façon « classique »
6: **sinon**
7: R n'admet pas de classe euclidienne
8: **fin si**
9: **sinon**
10: R peut être euclidien par rapport à la classe $[I]$. On le teste avec une modification du test classique (« en remplaçant R par I »)
11: **fin si**

2.4 Nombre de classes

On a vu que si K admet une classe euclidienne, alors le groupe des classes est cyclique. Une telle propriété a aussi des conséquences sur le nombre de classes.

Proposition 2.24. *Soit C une classe euclidienne pour la norme, alors le nombre de classes de K vérifie*

1. $\mathrm{h}_K < \min\left\{\left|\mathbf{N}_{K/\mathbf{Q}}(\alpha)\right|,\ \alpha \in \mathbf{Z}_K \setminus \mathbf{Z}_K^\times \cup \{0\}\right\}$,
2. $\mathrm{h}_K \leqslant \min\left\{\#\left\{q \in \mathcal{P},\ q \leqslant \left|\mathbf{N}_{K/\mathbf{Q}}(\alpha)\right|\right\},\ \alpha \in \mathbf{Z}_K \setminus \mathbf{Z}_K^\times \cup \{0\}\right\}$,

où $\mathcal{P}$ désigne l'ensemble des puissances de premiers strictement supérieures à 1 qui sont des normes d'idéaux de $\mathbf{Z}_K$.

Démonstration. Les deux inégalités sont des conséquences des écritures d'une classe d'idéaux comme une puissance de C.

1. L'ordre de C dans le groupe des classes est h_K, or pour tout $\alpha \in \mathbf{Z}_K$, $[\alpha\mathbf{Z}_K] = [\mathbf{Z}_K]$. Mais C est une classe euclidienne, donc d'après le lemme 2.19, il existe un entier $0 < n < \left|\mathbf{N}_{K/\mathbf{Q}}(\alpha)\right|$ tel que
$$[\alpha\mathbf{Z}_K] = C^n.$$
Donc, d'après la proposition 2.21, h_K divise n et en particulier,
$$\mathrm{h}_K < \left|\mathbf{N}_{K/\mathbf{Q}}(\alpha)\right|.$$
2. On fait le même raisonnement en utilisant le lemme 2.20.

□

On peut affiner ce résultat dans des cas particuliers. On a par exemple la propriété suivante.

Proposition 2.25. *Si K est un corps cubique qui admet une classe euclidienne pour la norme, alors $\mathrm{h}_K \leqslant 4$.*

Démonstration. Étudions la ramification de 2 dans $\mathbf{Z}_K$. Si $2\mathbf{Z}_K = \mathfrak{p}\mathfrak{q}\mathfrak{r}$, avec $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}$ idéaux premiers de $\mathbf{Z}_K$, alors, d'après la proposition 2.18, si K admet une classe euclidienne, alors c'est $[\mathfrak{p}]$, $[\mathfrak{q}]$ et $[\mathfrak{r}]$, donc $[\mathfrak{p}] = [\mathfrak{q}] = [\mathfrak{r}]$ et $[\mathfrak{p}]^3 = [\mathbf{Z}_K]$, donc la proposition 2.21 implique que $\mathrm{h}_K \leqslant 3$.

Si $2\mathbf{Z}_K = \mathfrak{p}\mathfrak{q}$, avec $\mathfrak{p}$ et $\mathfrak{q}$ premiers, $\mathbf{N}\mathfrak{p} = 2$, $\mathbf{N}\mathfrak{q} = 4$. Alors, d'après le lemme 2.19, il existe $0 < n < 4$ tel que $[\mathfrak{q}] = [\mathfrak{p}]^n$. Ainsi $[\mathfrak{p}]^{n+1} = [\mathbf{Z}_K]$ et $\mathrm{h}_K \leqslant n+1 \leqslant 4$.

Enfin, si 2 est inerte, alors, d'après la proposition 2.24, $\mathrm{h}_K \leqslant 4$. □

3 Minima euclidien et inhomogène

3.1 Minimum euclidien

Soient K un corps de nombres, $\mathbf{Z}_K$ son anneau des entiers et I un idéal fractionnaire non nul de K.

Définition 3.1 (minimum euclidien par rapport à un idéal). Soit $x \in K$, on pose

$$m_{K,I}(x) := \inf_{z \in I} \frac{\left|\mathbf{N}_{K/\mathbf{Q}}(x-z)\right|}{\mathbf{N}I}.$$

On définit aussi le minimum euclidien de I par $M(K, I) := \sup_{x \in K} m_{K,I}(x)$.

Ainsi, I est euclidien par rapport à la norme si et seulement si pour tout $x \in K$, $m_{K,I}(x) < 1$. On a aussi les propriétés élémentaires suivantes.

Lemme 3.2. *Avec les notations précédentes,*

1. *pour tout $x \in K$, il existe $z \in I$ tel que $m_{K,I}(x) = \frac{\left|\mathbf{N}_{K/\mathbf{Q}}(x-z)\right|}{\mathbf{N}I} \in \mathbf{Q}$,*
2. *pour tout $x \in K$, $m_{K,I}(x) = 0$ si et seulement si $x \in I$,*
3. *si I est entier, pour tout $x \in K$, $m_{K,I}(x) \geqslant \frac{m_K(x)}{\mathbf{N}I}$,*
4. *soit $k \in K^\times$, on note $J = kI$, alors pour tout $x \in K$, $m_{K,J}(x) = m_{K,I}(k^{-1}x)$.*

Démonstration. Les trois premières propriétés sont immédiates. Pour la quatrième, pour $x \in K$, il suffit d'écrire

$$\begin{aligned} m_{K,J}(x) &= \inf_{z \in J} \frac{\left|\mathbf{N}_{K/\mathbf{Q}}(x-z)\right|}{\mathbf{N}J} \\ &= \inf_{z \in I} \frac{\left|\mathbf{N}_{K/\mathbf{Q}}(x-kz)\right|}{\left|\mathbf{N}_{K/\mathbf{Q}}(k)\right| \cdot \mathbf{N}I} \text{ par définition de } J, \\ &= \inf_{z \in I} \frac{\left|\mathbf{N}_{K/\mathbf{Q}}(k^{-1}x-z)\right|}{\mathbf{N}I}, \\ &= m_{K,I}(k^{-1}x). \end{aligned}$$

□

Le lemme 3.2 (4) montre que $M(K, I)$ ne dépend que de la classe $[I]$. Cela permet permet de définir le minimum euclidien d'une classe d'idéaux C inversible par $M(K, C) := M(K, I)$ pour $I \in C$.

Exemple 3.3. Reprenons l'exemple $K = \mathbf{Q}\left(\sqrt{-5}\right)$ avec $I = \left(2, 1+\sqrt{-5}\right)$. La figure IV.1 montre que $M(K, [I]) = \frac{\left(\frac{3\sqrt{5}}{5}\right)^2}{2} = \frac{9}{10}$. En effet, on peut recouvrir le plan complexe avec des disques de rayon $\frac{3\sqrt{5}}{5}$ centrés en I. Par ailleurs,

$$\begin{aligned} m_{K,I}\left(1+\frac{2\sqrt{-5}}{5}\right) &= \frac{1}{\mathbf{N}I} \cdot \min_{\alpha,\beta \in \mathbf{Z}} \left|\mathbf{N}_{K/\mathbf{Q}}\left(1+\frac{2\sqrt{-5}}{5} - 2\alpha - \beta - \beta\sqrt{-5}\right)\right|, \\ &= \frac{1}{2} \cdot \min_{\alpha,\beta \in \mathbf{Z}} \left|(1-2\alpha-\beta)^2 + 5\left(\frac{2}{5}-\beta\right)^2\right|^2, \\ &\leqslant \frac{1}{2} \cdot \frac{9}{5}, \end{aligned}$$

et ce minimum est atteint pour $\alpha = \beta = 0$, donc $m_{K,I}\left(1+\frac{2\sqrt{-5}}{5}\right) = \frac{9}{10}$.

On a évidemment la propriété suivante.

Proposition 3.4. *Soit C une classe d'idéaux inversible. Si $M(K, C) < 1$, alors C est une classe euclidienne pour la norme. Si $M(K, C) > 1$, alors C n'est pas une classe euclidienne pour la norme.*

On va alors introduire le minimum inhomogène pour montrer que $M(K, C)$ est fini, le calculer et traiter le cas $M(K, C) = 1$.

3.2 Minimum inhomogène

Rappelons que l'on avait défini au chapitre II le plongement $\Phi : K \longrightarrow H$ et une fonction $\mathcal{N} : H \longrightarrow \mathbf{R}$, où $H \simeq \mathbf{R}^n$ est muni du produit $\cdot$ tel que pour tous $x, y \in H$,

$$\mathcal{N}(x \cdot y) = \mathcal{N}(x) \cdot \mathcal{N}(y),$$

et pour tout $\xi \in K$,

$$\left|\mathbf{N}_{K/\mathbf{Q}}(\xi)\right| = \mathcal{N}(\Phi(\xi)).$$

Définition 3.5 (minimum inhomogène local par rapport à I). Soient I un idéal fractionnaire non nul et $x \in H$, on pose

$$m_{\overline{K},I}(x) := \inf_{\lambda \in \Phi(I)} \frac{\mathcal{N}(x - \lambda)}{\mathbf{N}I}.$$

La fonction $m_{\overline{K},I}$ a les propriétés suivantes.

Lemme 3.6. *1. Pour tous $x \in H$, $\varepsilon \in \mathbf{Z}_K^\times$, $z \in I$,*

$$m_{\overline{K},I}(\Phi(\varepsilon) \cdot x - \Phi(z)) = m_{\overline{K},I}(x).$$

2. Pour tous $k \in K^\times$, $x \in H$,

$$m_{\overline{K},kI}(x) = m_{\overline{K},I}(\Phi(k^{-1}) \cdot x).$$

3. La fonction $m_{\overline{K},I}$ induit une fonction sur $H/\Phi(I)$, aussi notée $m_{\overline{K},I}$, qui est semi-continue supérieurement.

Cela permet de définir le réel suivant.

Définition 3.7 (minimum inhomogène par rapport à I). On pose

$$M(\overline{K}, I) := \sup_{x \in H} m_{\overline{K},I}(x).$$

Proposition 3.8. *Soit I un idéal fractionnaire non nul de K.*

1. *Il existe $x \in H$ tel que $M(\overline{K}, I) = m_{\overline{K},I}(x) \in \mathbf{R}_+^*$.*
2. *$M(\overline{K}, I)$ ne dépend que de la classe $[I]$, on pourra aussi le noter $M(\overline{K}, [I])$.*

Démonstration. Ce sont des conséquences respectives du lemme 3.6 (3) et (2). □

Ainsi, on obtient que $M(K, [I]) \leqslant M(\overline{K}, [I])$ est fini. Comme dans le cas principal, on cherche à comparer ces deux minima et à savoir si $M(K, [I])$ est atteint.

Théorème 3.9. *Soient K un corps de nombres et I un idéal fractionnaire non nul de K. On note r le rang des unités de K.*

1. *Si $r = 1$, alors $M(K, [I]) = M(\overline{K}, [I])$.*
2. *Si $r \neq 1$, alors il existe $\xi \in K$ tel que $M(K, [I]) = M(\overline{K}, [I]) = m_{K,I}(\xi) \in \mathbf{Q}$.*

Démonstration. Si $r = 0$, c'est évident. Si $r = 1$, c'est la conséquence des travaux de Davenport et Cassels, ensuite généralisés par van der Linden ([Lin84]). Le cas $r > 1$ est l'objet du paragraphe suivant. □

3.3 Comparaison entre $M(K, [I])$ et $M(\overline{K}, [I])$

En suivant le raisonnement de Cerri ([Cer05, chapitre 4]), on utilise les travaux de Berend pour prouver le théorème 3.9 (2) dans le cas $r > 1$. La généralisation est minime, il s'agit simplement de reprendre la démarche de Cerri en remplaçant $\mathbf{Z}_K$ par I.

3.3.1 Notations

Au paragraphe 2.2 du chapitre II, on utilisait un plongement de K dans $H \simeq \mathbf{R}^n$. On va en décrire un autre ici.

Posons $\mathcal{H} := \mathbf{R}^{r_1} \times \left\{ z = (z_i)_{1 \leqslant i \leqslant 2r_2} \in \mathbf{C}^{2r_2}, \text{ pour tout } 1 \leqslant i \leqslant r_2, \overline{z_i} = z_{i+r_2} \right\}$. On munit $\mathcal{H}$ du produit $\cdot$ défini coordonnée par coordonnée. Rappelons que pour tout indice $r_1 < i \leqslant r_1 + r_2$, on a $\sigma_{i+r_2} = \overline{\sigma_i}$. On peut donc définir un plongement

$$\Phi : \begin{cases} K & \longrightarrow & \mathcal{H} \\ \xi & \longmapsto & (\sigma_i(\xi))_{1 \leqslant i \leqslant n} \end{cases}.$$

En notant $(f_i)_{1 \leqslant i \leqslant n}$ une $\mathbf{Z}$-base de l'idéal I, K peut être identifié à $\mathbf{Q}^n$ via

$$\Psi : \begin{cases} \mathbf{Q}^n & \longrightarrow & K \\ x & \longmapsto & \sum_{i=1}^n x_i f_i \end{cases},$$

qui fait aussi correspondre I et $\mathbf{Z}^n$.

On peut prolonger continûment $\Phi \circ \Psi$ de $\mathbf{Q}^n$ à $\mathbf{R}^n$ par une application $\overline{\Phi}$ définie par

$$\text{pour tout } x \in \mathbf{R}^n, \ \overline{\Phi}(x) = \left(\sum_{i=1}^n x_i \sigma_j(f_i) \right)_{1 \leqslant j \leqslant n}.$$

Pour la suite, on prolonge continûment $\overline{\Phi}$ à $\mathbf{C}^n$ en le $\mathbf{C}$-automorphisme Ξ de $\mathbf{C}^n$ défini par

$$\text{pour tous } u, v \in \mathbf{R}^n, \ \Xi(u + \mathcal{I}v) = \overline{\Phi}(u) + \mathcal{I}\overline{\Phi}(v).$$

En notant i_1, i_2 et i_3 les injections canoniques de $\mathbf{Q}^n$ dans $\mathbf{R}^n$, de $\mathbf{R}^n$ dans $\mathbf{C}^n$ et de $\mathcal{H}$ dans $\mathbf{C}^n$, on a ainsi le diagramme commutatif suivant.

$$\begin{array}{ccccc} \mathbf{Q}^n & \xhookrightarrow{i_1} & \mathbf{R}^n & \xhookrightarrow{i_2} & \mathbf{C}^n \\ \wr \downarrow \Psi & & \wr \downarrow \overline{\Phi} & & \wr \downarrow \Xi \\ K & \xrightarrow{\Phi} & \mathcal{H} & \xhookrightarrow{i_3} & \mathbf{C}^n \end{array}$$

On peut alors étendre continûment $\mathbf{N}_{K/\mathbf{Q}} \circ \Psi$ de $\mathbf{Q}^n$ à $\mathbf{R}^n$ en posant

$$\text{pour tout } x \in \mathbf{R}^n, \ \nu(x) = \prod_{i=1}^n \left(\sum_{j=1}^n x_j \sigma_i(f_j) \right).$$

On définit l'extension de $m_{K,I}$ à $\mathbf{R}^n$ par

$$\text{pour tout } x \in \mathbf{R}^n, \ m_I(x) := \inf \left\{ \frac{|\nu(x - X)|}{\mathbf{N}I}, \ X \in \mathbf{Z}^n \right\}.$$

Comme nous avons défini un peu différemment $m_{\overline{K},I}$, il convient de s'assurer que c'est un analogue. Pour ce faire, notons simplement que pour tout $x \in \mathbf{R}^n$,

$$m_I(x) = m_{\overline{K},I}(g \circ \overline{\Phi}^{-1}(x)),$$

où $g : \left\{ \begin{array}{ccc} \mathbf{R}^n & \longrightarrow & \mathbf{R}^n \\ x & \longmapsto & (g_i(x))_{1\leqslant i\leqslant n} \end{array} \right.$ est l'isomorphisme continu de $\mathbf{R}^n$ défini par

$$g_i(x) = \left\{ \begin{array}{ll} \sum_{j=1}^n x_j \sigma_i(f_j) & \text{si } i \leqslant r_1 \\ \mathrm{Re}\left(\sum_{j=1}^n x_j \sigma_i(f_j)\right) & \text{si } r_1 < i \leqslant r_1 + r_2 \\ \mathrm{Im}\left(\sum_{j=1}^n x_j \sigma_i(f_j)\right) & \text{si } r_1 + r_2 < i \leqslant n \end{array} \right.$$

Ainsi, m_I et $m_{\overline{K},I}$ prennent les mêmes valeurs. En particulier,

$$\sup_{x\in\mathbf{R}^n} m_I(x) = M(\overline{K}, [I]).$$

Proposition 3.10. *La fonction m_I vérifie les propriétés suivantes.*

- *m_I est définie modulo $\mathbf{Z}^n$.*
- *m_I est semi-continue supérieurement sur $\mathbf{R}^n$.*
- *Pour tout $x \in \mathbf{R}^n$ et toute unité $\varepsilon \in \mathbf{Z}_K^\times$,*

$$m_I\left(\overline{\Phi}^{-1}\left(\Phi(\varepsilon)\cdot\overline{\Phi}(x)\right)\right) = m_I(x).$$

Ainsi, m_I définit une application $\widetilde{m_I}$ sur $\mathbf{R}^n/\mathbf{Z}^n$ et donnée par

$$\text{pour tout } x \in \mathbf{R}^n,\ \widetilde{m_I}(x + \mathbf{Z}^n) = m_I(x).$$

Cette application est aussi semi-continue supérieurement.

3.3.2 Résultats de Berend

On note $\mathbf{T}_n = \mathbf{R}^n/\mathbf{Z}^n$ le tore de dimension n, c'est un groupe additif compact pour la topologie induite par la métrique de $\mathbf{R}^n$. On appellera « endomorphismes de $\mathbf{T}_n$ » les endomorphismes (continus) de $\mathbf{R}^n$ qui préservent $\mathbf{Z}^n$. Ils peuvent être représentés par des matrices carrées de taille n à coefficients entiers. Ainsi, un tel endomorphisme f peut se relever en un endomorphisme de $\mathbf{R}^n$ (de même matrice). On notera aussi f sa matrice, son relèvement à $\mathbf{R}^n$ et la matrice de ce relèvement.

Soit $\mathcal{E}$ un ensemble d'endomorphismes de $\mathbf{T}_n$.

Définitions 3.11.
- Un sous-ensemble F de $\mathbf{T}_n$ est *$\mathcal{E}$-invariant* si pour tout $f \in \mathcal{E}$, $f(F) \subseteq F$.
- Un fermé non vide $\mathcal{E}$-invariant F est *$\mathcal{E}$-minimal* s'il ne contient aucun sous-ensemble strict fermé non vide $\mathcal{E}$-invariant.

En utilisant le lemme de Zorn, on a la propriété suivante.

Lemme 3.12. *Tout sous-ensemble fermé non vide $\mathcal{E}$-invariant de $\mathbf{T}_n$ contient un sous-ensemble $\mathcal{E}$-minimal.*

Dans le cas particulier où $\mathcal{E}$ est un semi-groupe Σ de $\mathbf{T}_n$, on a d'autres propriétés. L'ensemble des vecteurs propres communs aux éléments de Σ et appartenant à $\mathbf{C}^n$ est noté $\mathrm{evec}\Sigma$. Si $v \in \mathrm{evec}\Sigma$, alors $\mathrm{spec}_v\Sigma$ est l'ensemble des valeurs propres correspondant à v et relatives à tous les éléments de Σ.

Définitions 3.13. – Σ est dit *hyperbolique* si pour tout $v \in \mathrm{evec}\Sigma$, $\mathrm{spec}_v\Sigma \not\subseteq \mathbf{S}^1$, où $\mathbf{S}^1$ est le cercle unité de $\mathbf{C}$.

– Σ est dit *multi-paramétré* si pour tout $v \in \mathrm{evec}\Sigma$, $\mathrm{spec}_v\Sigma$ contient deux éléments α_v et β_v rationnellement indépendants, c'est-à-dire tels que

$$\text{si } (l, m) \in \mathbf{Z}^2 \text{ et } \alpha_v^l = \beta_v^l, \text{ alors } l = m = 0.$$

Théorème 3.14 (Berend, [Ber84, Theorem 2.1])**.** *Soit Σ un semi-groupe commutatif d'épimorphismes de $\mathbf{T}_n$. Les propriétés suivantes sont équivalentes.*

1. *Tout sous-ensemble Σ-minimal de $\mathbf{T}_n$ est composé d'éléments de torsion.*
2. *Σ est hyperbolique et multi-paramétré.*

3.3.3 Application

D'après la proposition 3.10, m_I est invariante sous l'action de la fonction

$$u_\varepsilon : \begin{cases} \mathbf{R}^n & \longrightarrow & \mathbf{R}^n \\ x & \longmapsto & \overline{\Phi}^{-1}\left(\Phi(\varepsilon)\cdot\overline{\Phi}(x)\right) \end{cases},$$

pour tout $\varepsilon \in \mathbf{Z}_K^\times$. En fait, la fonction u_ε est le prolongement continu à $\mathbf{R}^n$ de la fonction qui à $y \in \mathbf{Q}^n$ associe les coordonnées dans la base $(f_i)_{1\leqslant i\leqslant n}$ de $\varepsilon\cdot\sum_{j=1}^n y_j f_j$. Donc pour tout $\varepsilon \in \mathbf{Z}_K^\times$, u_ε est un automorphisme de $\mathbf{R}^n$, dont la matrice dans la base canonique est à coefficients entiers.

Or pour tous $\varepsilon \in \mathbf{Z}_K^\times$, $x \in \mathbf{R}^n$ et $Z \in \mathbf{Z}^n$,

$$u_\varepsilon(x + X) \equiv u_\varepsilon(x) \pmod{\mathbf{Z}^n}.$$

Donc u_ε induit un isomorphisme de $\mathbf{T}_n$, noté g_ε et défini par

$$\text{pour tout } x \in \mathbf{R}^n,\ g_\varepsilon(x + \mathbf{Z}^n) := u_\varepsilon(x) + \mathbf{Z}^n.$$

Ainsi, pour tout $\alpha \in \mathbf{T}_n$, on a

$$\widetilde{m_I}\left(g_\varepsilon(\alpha)\right) = \widetilde{m_I}(\alpha). \tag{IV.3}$$

On pose alors

$$\Sigma := \left\{g_\varepsilon,\ \varepsilon \in \mathbf{Z}_K^\times\right\}.$$

Ainsi, Σ est un groupe commutatif d'automorphismes de $\mathbf{T}_n$.

On note $(v_i)_{1\leqslant i\leqslant n}$ la base canonique de $\mathbf{R}^n$ (ou $\mathbf{C}^n$) dont les vecteurs sont définis par $(v_i)_j = \delta_{i,j}$ (symbole de Kronecker). Pour tout $1 \leqslant i \leqslant n$, on pose alors

$$w_i := \Xi^{-1}(v_i) \in \mathbf{C}^n.$$

Comme Ξ est un automorphisme de $\mathbf{C}^n$, les w_i forment une base de $\mathbf{C}^n$.

Proposition 3.15. *Si $u \in \mathrm{evec}\Sigma$, alors il existe $i \in \{1, \ldots, n\}$ tel que*

$$\mathrm{spec}_u\Sigma = \left\{\sigma_i(\varepsilon),\ \varepsilon \in \mathbf{Z}_K^\times\right\}.$$

Démonstration. On peut étendre u_ε en un endomorphisme de $\mathbf{C}^n$ (encore noté u_ε) de sorte que pour tout $1 \leqslant i \leqslant n$,

$$u_\varepsilon(w_i) = \Xi^{-1}(\sigma_i(\varepsilon)v_i) = \sigma_i(\varepsilon)w_i.$$

Cela montre que $w_i \in \mathrm{evec}\Sigma$ et que la valeur propre associée est $\sigma_i(\varepsilon)$ pour g_ε.

Soit alors $u \in \mathrm{evec}\Sigma$. On décompose $u = \sum_{i=1}^n u_i w_i$ dans la $\mathbf{C}$-base (w_i) de $\mathbf{C}^n$, $((u_i)_{1\leqslant i\leqslant n} \in \mathbf{C}^n)$. Par définition de $\mathrm{evec}\Sigma$, pour tout $\varepsilon \in \mathbf{Z}_K^\times$, il existe une valeur propre $\lambda_\varepsilon \in \mathbf{C}$ telle que $f_\varepsilon(u) = \lambda_\varepsilon u$, ce qui donne

$$\sum_{i=1}^n u_i\sigma_i(\varepsilon)w_i = \sum_{i=1}^n \lambda_\varepsilon u_i w_i.$$

Comme $u \neq 0$ et les vecteurs (w_i) sont libres, il existe $i_0 \in \{1, \dots, n\}$ tel que $\lambda_\varepsilon = \sigma_{i_0}(\varepsilon)$, ce qui nous donne le résultat attendu. □

Proposition 3.16. *Posons $S := \{\alpha \in \mathbf{T}_n,\ \widetilde{m_I}(\alpha) = M(\overline{K}, I)\}$. Si le rang des unités de K est strictement supérieur à 1, alors S contient un élément de torsion.*

Avant de montrer cette proposition, notons qu'elle implique le théorème 3.9 (2).

Démonstration du théorème 3.9 (2). Soit α un élément de torsion de S. Il existe $k_\alpha \in \mathbf{Z}\setminus\{0\}$ tel que $k_\alpha\alpha = 0$ (dans $\mathbf{T}_n$). Donc α se relève en un élément $\frac{X}{k_\alpha}$ de $\mathbf{Q}^n$ (où $X \in \mathbf{Z}^n$). Mais alors, en posant $\xi = \Psi\left(\frac{X}{k_\alpha}\right)$, on obtient un élément de K tel que $m_{K,I}(\xi) = \widetilde{m_I}(\alpha) = M(\overline{K}, I)$. □

Démonstration de la proposition 3.16. Par semi-continuité supérieure de $\widetilde{m_I}$, on sait que l'ensemble S est non vide et fermé, il est Σ-invariant d'après (IV.3). D'après le théorème 3.14, il suffit donc de montrer que Σ est hyperbolique et multi-paramétré. Il suffira en effet de prendre alors tout élément d'un sous-ensemble Σ-minimal de S (qui existe d'après le lemme 3.12).

Le caractère hyperbolique de Σ se déduit de la proposition 3.15. En effet, si Σ n'est pas hyperbolique, alors il existe $1 \leqslant i \leqslant n$ tel que pour tout $\varepsilon \in \mathbf{Z}_K^\times$, $|\sigma_i(\varepsilon)| = 1$. Si $i > r_1 + r_2$, la propriété est encore vraie pour $i - r_2$ par définition des σ_i, donc on peut supposer $1 \leqslant i \leqslant r_1 + r_2$. Dès lors, $\mathcal{L}(\mathbf{Z}_K^\times)$ est inclus dans l'hyperplan d'équation $x_i = 0$. Mais il est aussi inclus dans l'hyperplan $\sum_{j=1}^{r_1} x_j + 2\sum_{j=r_1+1}^{r_1+r_2} x_j = 0$ qui est distinct du précédent car $r = r_1 + r_2 - 1 \geqslant 1$. Cela contredit le fait que $\mathcal{L}(\mathbf{Z}_K^\times)$ est un réseau de rang r.

Pour ce qui est du caractère multi-paramétré, considérons deux unités indépendantes ε_1 et ε_2 (ce qui possible car $r > 1$). Si pour un certain $1 \leqslant i \leqslant n$, il existe deux entiers l, m, tels que $\sigma_i(\varepsilon_1)^l = \sigma_i(\varepsilon_2)^m$, alors, par injectivité de σ_i, $\varepsilon_1^l = \varepsilon_2^m$. Comme ε_1 et ε_2 sont indépendantes, cela implique que $l = m = 0$ et cela achève la preuve. □

Remarque 3.17. Les autres résultats de Cerri concernant le spectre euclidien peuvent tout aussi facilement être généralisés.

3.4 Bornes sur le minimum euclidien

On a la borne évidente suivante.

Lemme 3.18. *Pour tout idéal entier J non nul, $\frac{\max\{M(K),1\}}{\mathbf{N}J} \leqslant M(K,[J])$.*

Même si cette inégalité peut sembler très mauvaise, comme on connaît beaucoup de minima euclidiens de corps de nombres, elle peut servir pour conclure rapidement que K n'admet pas de classe euclidienne pour la norme.

Exemple 3.19. Le corps cubique réel K de discriminant 2 597 n'admet pas de classe euclidienne pour la norme car $M(K) = \frac{5}{2}$ et $\Lambda(K) = 2$.

Par ailleurs, les bornes sur $M(K)$ en fonction du discriminant établies par Ennola ([Enn58]), Cassels ([Cas52], corrigé par van der Linden [Lin84]) sont prouvées en utilisant des formes quadratiques et cubiques. Comme l'avait remarqué van der Linden ([Lin84]), ces raisonnements s'appliquent encore pour les classes euclidiennes pour la norme, si bien qu'on a toujours le résultat suivant.

Théorème 3.20 (Ennola, Cassels, van der Linden)**.** *Soit K un corps de nombres admettant une classe euclidienne pour la norme tel que $r = 1$.*

- *Si $r_1 = 2$, $r_2 = 0$, alors $\mathrm{disc}_K \leqslant 945$.*
- *Si $r_1 = r_2 = 1$, alors $\mathrm{disc}_K \leqslant 170\,520$.*
- *Si $r_1 = 0$, $r_2 = 2$, alors $\mathrm{disc}_K \leqslant 230\,202\,117$.*

3.5 Cas quadratique réel

Théorème 3.21. *Soit $K = \mathbf{Q}\left(\sqrt{m}\right)$, où m est un entier supérieur à 2 sans facteur carré. Alors K admet une classe euclidienne non principale pour la norme si et seulement si*

$$m \in \{10, 15, 85\}.$$

Ce résultat est dû à Lenstra ([Len78a]). Pour des détails sur la preuve on peut se reporter à [Lin84, §5.5]. L'idée est d'utiliser la borne d'Ennola, le fait qu'un tel corps de nombres doit vérifier $\mathrm{h}_K = 2$ et des propriétés des idéaux imposées par l'existence d'une classe euclidienne pour la norme. Cela permet de se ramener à une liste finie de corps de nombres, que l'on traite avec un lemme de congruences.

Comme dans le cas principal, en regardant de plus près la preuve, on observe que la classe $[I]$ ne peut pas être euclidienne pour la norme si $M(K,[I]) = M(\overline{K},[I]) = 1$.

3.6 Décidabilité

Comme au paragraphe 2.5 du chapitre II, on a le résultat suivant.

Proposition 3.22. *Soit K un corps de nombres de signature différente de $(1,1)$ et $(0,2)$, alors l'existence d'une classe euclidienne de K pour la norme est un problème décidable.*

Notons néanmoins que ce résultat ne fournit pas un algorithme effectif pour décider s'il existe une classe euclidienne pour la norme.

4 Corps quadratiques imaginaires

Dans ce paragraphe, nous calculons les minima euclidiens des corps quadratiques imaginaires par rapport à un idéal I de norme minimale.

4.1 Généralités sur les idéaux des corps quadratiques

Soit K un corps de nombres quadratiques. On note disc_K le discriminant de K de sorte que l'anneau des entiers $\mathbf{Z}_K$ de K vérifie $\mathbf{Z}_K = \mathbf{Z} + \frac{\mathrm{disc}_K + \sqrt{\mathrm{disc}_K}}{2}\mathbf{Z}$. On cherche la forme des idéaux de $\mathbf{Z}_K$.

Soient a, b et d des entiers vérifiant $a > 0$, $d > 0$, $-a \leqslant b < a$ et $b^2 \equiv \mathrm{disc}_K \pmod{4a}$. On pose

$$I_{a,b,d} := d\left(a\mathbf{Z} + \frac{-b + \sqrt{\mathrm{disc}_K}}{2}\mathbf{Z}\right).$$

Lemme 4.1. *$I_{a,b,d}$ est un idéal (entier) de $\mathbf{Z}_K$.*

Démonstration. $I_{a,b,d}$ est un sous-groupe de $\mathbf{Z}_K = \mathbf{Z} + \frac{\mathrm{disc}_K + \sqrt{\mathrm{disc}_K}}{2}\mathbf{Z}$ car $b^2 \equiv \mathrm{disc}_K \pmod 2$, donc $b \equiv \mathrm{disc}_K \pmod 2$, d'où $b + \mathrm{disc}_K \equiv 0 \pmod 2$.

Il reste ainsi à vérifier que $I_{a,b,d}$ est stable par multiplication par un élément de $\mathbf{Z}_K$. Soient alors des entiers α, β, λ et μ. On calcule

$$\begin{aligned}
&d\left(a\lambda + \frac{-b + \sqrt{\mathrm{disc}_K}}{2}\mu\right)\left(\alpha + \beta\frac{\mathrm{disc}_K + \sqrt{\mathrm{disc}_K}}{2}\right)\\
=&d\left(a\lambda + \frac{-b + \sqrt{\mathrm{disc}_K}}{2}\mu\right)\left(\alpha + \beta\frac{-b + \sqrt{\mathrm{disc}_K}}{2} + \beta\frac{\mathrm{disc}_K - b}{2}\right)\\
=&d\left[a\lambda\left(\alpha + \beta\frac{\mathrm{disc}_K - b}{2}\right) + \frac{-b + \sqrt{\mathrm{disc}_K}}{2}\left(a\lambda\beta + \mu\alpha + \mu\beta\frac{\mathrm{disc}_K - b}{2}\right)\right.\\
&\qquad\left. + \beta\mu\left(\frac{-b + \sqrt{\mathrm{disc}_K}}{2}\right)^2\right]\\
=&d\left[a\left(\lambda\left(\alpha + \beta\frac{\mathrm{disc}_K - b}{2}\right) + \beta\mu\frac{-b^2 + \mathrm{disc}_K}{4a}\right)\right.\\
&\qquad\left. + \frac{-b + \sqrt{\mathrm{disc}_K}}{2}\left(a\lambda\beta + \mu\alpha + \mu\beta\frac{\mathrm{disc}_K - 3b}{2}\right)\right].
\end{aligned}$$

La congruence $b^2 \equiv \mathrm{disc}_K \pmod{4a}$ formulée en hypothèse assure alors que la quantité calculée est effectivement un élément de I. □

Proposition 4.2. *Les idéaux de $\mathbf{Z}_K$ sont exactement les $I_{a,b,d}$ avec $a, b, d \in \mathbf{Z}$ vérifiant*

$$a > 0, \quad d \geqslant 0, \quad -a \leqslant b < a \quad \textit{et} \quad b^2 \equiv \mathrm{disc}_K \pmod{4a}.$$

Démonstration. Grâce au lemme 4.1, on sait que les $I_{a,b,d}$ sont effectivement des idéaux. Il suffit donc de vérifier que tout idéal I de $\mathbf{Z}_K$ peut s'écrire sous cette forme. Pour le voir, on considère I comme un $\mathbf{Z}$-module de rang 2 dans $\mathbf{Z}_K \subseteq \mathbf{R}^2$. Ainsi, d'après la théorie de la réduction sous forme normale de Hermite, ce $\mathbf{Z}$-module admet une base de la forme $(\alpha e_1, \beta e_1 + \gamma e_2)$ en prenant la base $(e_1, e_2) = \left(1, \frac{\mathrm{disc}_K + \sqrt{\mathrm{disc}_K}}{2}\right)$ et avec α, β et γ entiers vérifiant

$$\alpha > 0, \ \gamma > 0, \ \text{et} \ \frac{-\gamma\mathrm{disc}_K}{2} - \frac{\alpha}{2} \leqslant \beta \leqslant \frac{-\gamma\mathrm{disc}_K}{2} + \frac{\alpha}{2}$$

On pose $d = \mathrm{pgcd}(\alpha, 2\beta + \gamma\mathrm{disc}_K, \gamma)$, $a = \frac{\alpha}{d}$, $c = \frac{\gamma}{d}$ et $b = -\frac{2\beta+\gamma\mathrm{disc}_K}{d}$. Alors $I = I_{a,b,d}$. De plus, $a > 0$, $c > 0$ et $-a \leqslant b \leqslant a$ par construction. Si $b = a$, on peut remplacer b par $-a$ car $I_{a,a,d} = I_{a,-a,d}$. Enfin, pour vérifier que $b^2 \equiv \mathrm{disc}_K \pmod{4a}$, on fait le même calcul que dans la preuve du lemme 4.1. Le fait que I soit un idéal impose cette congruence. □

Lemme 4.3. *Avec les notations précédentes,* $\mathbf{N}\left(I_{a,b,d}\right) = d^2 a$.

Démonstration. Par multiplicativité, $\mathbf{N}\left(I_{a,b,d}\right) = d^2\mathbf{N}\left(I_{a,b,1}\right)$. Pour démontrer que $\mathbf{N}\left(I_{a,b,1}\right) = a$, nous allons vérifier que $\mathbf{Z}_K/I_{a,b,1} \simeq \{0, 1, \ldots, a-1\}$.

Soient deux entiers α_1 et α_2, on note $\alpha = \alpha_1 + \alpha_2\frac{\mathrm{disc}_K+\sqrt{\mathrm{disc}_K}}{2} \in \mathbf{Z}_K$. Alors $\alpha = \alpha_1 + \frac{b+\mathrm{disc}_K}{2}\alpha_2 + \alpha_2\frac{-b+\sqrt{\mathrm{disc}_K}}{2}$. Comme b et disc_K ont même parité, $\alpha_1 + \frac{b+\mathrm{disc}_K}{2}\alpha_2$ est un entier, dont on fait la division euclidienne par a : $\alpha_1 + \frac{b-\mathrm{disc}_K}{2}\alpha_2 = aq + l$, avec $0 \leqslant l < a$. Ainsi, $\alpha \equiv l \pmod{I_{a,b,1}}$.

Par ailleurs, si $l_1, l_2 \in \{0, 1, \ldots, a-1\}$ sont tels que $l_1 \neq l_2$, alors $l_2 - l_1 \notin I_{a,b,1}$. Cela montre que l'on peut bien identifier $\mathbf{Z}_K/I_{a,b,1}$ et $\{0, 1, \ldots, a-1\}$. □

4.2 Raisonnement géométrique

On se restreint à présent au cas où K est un corps quadratique imaginaire. On fixe alors des entiers a, b vérifiant

$$a > 0, \quad -a \leqslant b \leqslant 0 \quad \text{et} \quad b^2 \equiv \mathrm{disc}_K \pmod{4a}. \tag{IV.4}$$

On cherche à calculer $M\left(\overline{K}, I_{a,b,1}\right)$. Pour ce faire, on se place dans le domaine fondamental délimité par 0, $\frac{-b+\sqrt{|\mathrm{disc}_K|}}{2}$, $a + \frac{-b+\sqrt{|\mathrm{disc}_K|}}{2}$ et a et on détermine les cellules de Voronoï, c'est-à-dire les parties les plus proches de chaque sommet.

On suppose en outre que la condition suivante est vérifiée :

$$-b(b+2a) \leqslant |\mathrm{disc}_K|. \tag{IV.5}$$

Lemme 4.4. *Soient a, b deux entiers vérifiant* (IV.4) *et* (IV.5). *Si on note*

$$A := \frac{a}{2} + \left(\frac{2ab + b^2 + |\mathrm{disc}_K|}{4\sqrt{|\mathrm{disc}_K|}}\right)i \text{ et } B := \frac{a-b}{2} + \left(\frac{|\mathrm{disc}_K| - b^2 - 2ab}{4\sqrt{|\mathrm{disc}_K|}}\right)i,$$

alors A et B sont les points les plus éloignés de $I_{a,b,1}$ situés dans le parallélogramme fondamental (voir figure IV.2).

Démonstration. Par symétrie par rapport au centre du parallélogramme, on peut raisonner dans le triangle $\mathcal{T}$ de sommets 0, a, $\frac{-b+i|\mathrm{disc}_K|}{2}$. Alors A est le centre du cercle circonscrit à $\mathcal{T}$. Les hypothèses (IV.4) et (IV.5) assurent que A est à l'intérieur de $\mathcal{T}$ car les angles de $\mathcal{T}$ sont aigus.

En effet, les angles en 0 et a sont aigus car $0 \leqslant \frac{-b}{2} \leqslant a$. D'après le théorème d'Al-Kashi, l'angle en $\frac{-b+i|\mathrm{disc}_K|}{2}$ est aigu si et seulement si

$$a^2 \geqslant \frac{b^2 + |\mathrm{disc}_K|}{4} + \frac{(2a+b)^2 + |\mathrm{disc}_K|}{4},$$

ce qui équivaut à $|\mathrm{disc}_K| \leqslant -b(b+2a)$, c'est-à-dire à la condition (IV.5). □

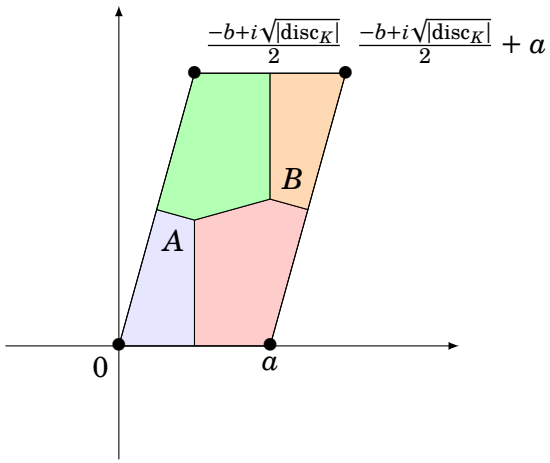


FIGURE IV.2 – diagramme de Voronoï.

Il suffit alors de calculer la distance de $I_{a,b,1}$ aux sommets A et B pour en déduire la proposition suivante.

Proposition 4.5. *Les points de* $\mathbf{R}^2$ *sont situés à une distance inférieure à* $\sqrt{m_{a,b,\mathrm{disc}_K}}$ *de* $I_{a,b,1}$*, où*

$$m_{a,b,\mathrm{disc}_K} = \left(\frac{a}{2}\right)^2 + \frac{\left(b^2 + |\mathrm{disc}_K| + 2ab\right)^2}{16|\mathrm{disc}_K|}.$$

Ce maximum est atteint en A et B.

On va appliquer ce résultat aux corps quadratiques imaginaires $K = \mathbf{Q}\left(\sqrt{-m}\right)$ où m est un entier strictement positif sans facteur carré.

4.3 $m \equiv 1 \pmod 4$

En ce cas, $\mathbf{Z}_K = \mathbf{Z} + \mathbf{Z}\sqrt{-m}$, K a pour discriminant $\mathrm{disc}_K = -4m$.
On considère $I = I_{2,-2,1} = 2\mathbf{Z} + \mathbf{Z}\left(1 + \sqrt{-m}\right)$.

Lemme 4.6. *I est un idéal de* $\mathbf{Z}_K$ *de norme* 2.

Démonstration. Il suffit de vérifier que $-4m = \mathrm{disc}_K \equiv (-2)^2 \pmod 8$, ce qui est le cas car $m \equiv 1 \pmod 4$. Ainsi, $I_{2,-2,1}$ est un idéal de $\mathbf{Z}_K$, sa norme est donnée par le lemme 4.3. □

Proposition 4.7. *Avec les notations précédentes,*

$$M\left(\overline{K}, I\right) = M(K, I) = \frac{(m+1)^2}{8m}.$$

Démonstration. La proposition 4.5 permet de calculer $M\left(\overline{K}, I\right) = \frac{m_{2,-2,-4m}}{\mathbf{N}I}$. Ce minimum étant atteint au point $A \in K$, on a aussi $M(K, I) = M\left(\overline{K}, I\right)$. □

Corollaire 4.8. *Le seuls corps de cette forme admettant une classe euclidienne pour la norme sont* $\mathbf{Q}\left(\sqrt{-1}\right)$ *et* $\mathbf{Q}\left(\sqrt{-5}\right)$ *(ce dernier corps est non principal).*

La figure IV.1 illustre le recouvrement « optimal » que l'on peut faire du plan par des disques centrés en les points de I.

Remarque 4.9. Dans ce cas, on connaît aussi la valeur de $M(K) = M\left(\overline{K}\right) = \frac{m+1}{4}$. On a ainsi l'inégalité stricte

$$\frac{M(K)}{\mathbf{N}I} < M(K, I).$$

Par ailleurs, $M(K, I)$ et $M(K)$ ne coïncident jamais. Cela implique notamment qu'il n'existe pas de tel corps principal.

4.4 $m \equiv 2 \pmod 4$

En ce cas, $\mathbf{Z}_K = \mathbf{Z} + \mathbf{Z}\sqrt{-m}$. On considère $I = 2\mathbf{Z} + \mathbf{Z}\sqrt{-m}$.

Lemme 4.10. *I est un idéal de $\mathbf{Z}_K$ de norme 2.*

Démonstration. Il suffit de remarquer que $I = I_{2,0,1}$ (et que $\mathrm{disc}_K \equiv 0 \pmod 8$). □

Remarque 4.11. Ce cas est en fait encore plus simple, le domaine fondamental et les cellules de Voronoï sont rectangulaires, les points A et B sont confondus.

Proposition 4.12. *Avec les notations précédentes, on a*

$$M(K, I) = M\left(\overline{K}, I\right) = \frac{m+4}{8}.$$

Démonstration. Il suffit d'appliquer la proposition 4.5 et de voir que l'on a en fait $M\left(\overline{K}, I\right) = \frac{m_{2,-2,1}}{\mathbf{N}I}$. Ce minimum étant atteint au point $A \in K$, on a aussi $M(K, I) = M\left(\overline{K}, I\right)$. □

Corollaire 4.13. *Le seul corps de nombres de cette forme admettant une classe euclidienne pour la norme est $\mathbf{Q}\left(\sqrt{-2}\right)$ (qui est en fait principal).*

Remarque 4.14. On connaît la valeur de $M(K) = M\left(\overline{K}\right) = \frac{m+1}{4}$. Les valeurs de $M(K)$ et $M(K, I)$ ne coïncident que pour $m = 2$ (ils valent alors $\frac{3}{4}$). Tous les autres corps de cette forme ne sont pas principaux.

4.5 $m \equiv 3 \pmod 4$

La situation est un peu plus compliquée dans ce cas puisqu'il n'existe pas toujours des idéaux de norme 2.

Proposition 4.15. *Soit $K = \mathbf{Q}\left(\sqrt{-m}\right)$ où $m \equiv 3 \pmod 4$ est un entier positif sans facteur carré.*

1. *Si $m \equiv 7 \pmod 8$, alors $I_{2,-1,1}$ est un idéal de norme 2 de $\mathbf{Z}_K$.*
2. *Si $m \equiv 3, 11 \pmod{24}$, alors $\mathbf{Z}_K$ n'admet pas d'idéal de norme 2 mais au moins un idéal de norme 3 (par exemple $I_{3,-1,1}$).*
3. *Si $m \equiv 19 \pmod{24}$, alors $\mathbf{Z}_K$ n'admet pas d'idéal de norme 2 ou 3, mais au moins un idéal de norme 4 (par exemple $2\mathbf{Z}_K$).*

Démonstration. – Si $m \equiv 7 \pmod 8$, alors $I_{2,-1,1}$ est un idéal de $\mathbf{Z}_K$ car le discriminant disc_K de K vérifie $\mathrm{disc}_K = -m \equiv (-1)^2 \pmod 8$.

– Si $m \equiv 3 \pmod 8$, on montre qu'il n'existe pas d'idéal de norme 2. On raisonne par l'absurde et on suppose qu'il existe un idéal $I_{a,b,d}$ de $\mathbf{Z}_K$ de norme 2. Alors b est un entier tel que $b^2 \equiv m \pmod 8$, c'est-à-dire, $b^2 \equiv 3 \pmod 8$, c'est impossible.
– Si $m \equiv 3 \pmod{24}$, alors $I_{3,-3,1}$ est un idéal de norme 3 de $\mathbf{Z}_K$ car $b^2 = 9 \equiv -3 \pmod{12}$.
– Si $m \equiv 11 \pmod{24}$, alors $I_{3,-1,1}$ est un idéal de norme 3 de $\mathbf{Z}_K$ car $b^2 = 1 \equiv -11 \pmod{12}$.
– Si $m \equiv 19 \pmod{24}$, $\mathbf{Z}_K$ n'admet pas d'idéal de norme 3. En effet, dans le cas contraire, on pourrait écrire cet idéal sous la forme $I_{a,b,d}$ où b est un entier tel que $b^2 \equiv -7 \pmod{12}$, mais il n'existe pas d'entier ayant cette propriété.

□

On connaît désormais un idéal I de norme minimale de K. On peut donc calculer le minimum $M\left(\overline{K}, I\right)$.

Proposition 4.16. *Soit $K = \mathbf{Q}\left(\sqrt{-m}\right)$ où $m \equiv 3 \pmod 4$ est un entier positif sans facteur carré. On désigne par I l'idéal non trivial de $\mathbf{Z}_K$ de norme minimale donné par la proposition 4.15. Alors $M(K, I) = M\left(\overline{K}, I\right)$ et*

1. *si $m \equiv 7 \pmod 8$, alors $M(K, I) = \frac{m^2+10m+9}{32m}$,*
2. *si $m = 3$, alors $M(K, I) = \frac{1}{3}$,*
3. *si $m \equiv 3 \pmod{24}$ et $m \neq 3$, alors $M(K, I) = \frac{(m+9)^2}{48m}$,*
4. *si $m \equiv 11 \pmod{24}$, alors $M(K, I) = \frac{m^2+26m+25}{48m}$,*
5. *si $m \equiv 19 \pmod{24}$, alors $M(K, I) = M(K) = \frac{(m+1)^2}{16m}$.*

Démonstration. Pour $m \neq 3$, c'est encore une conséquence de la proposition 4.5. Cependant, pour $m = 3$, cette proposition ne s'applique pas, mais on connaît la valeur de $M(K, I) = M(K)$ car K est principal. □

Corollaire 4.17. *Les seuls corps de nombres de cette forme admettant une classe euclidienne pour la norme sont $\mathbf{Q}\left(\sqrt{-3}\right)$, $\mathbf{Q}\left(\sqrt{-7}\right)$, $\mathbf{Q}\left(\sqrt{-11}\right)$ et $\mathbf{Q}\left(\sqrt{-15}\right)$ (seul ce dernier corps est non principal).*

Remarque 4.18. Si $\mathbf{Z}_K$ est principal, alors $M(K) = M(K, I)$, donc les seuls corps de cette forme pouvant être principaux correspondent aux cas $m = 7$, $m = 3$, $m = 11$ et $m \equiv 19 \pmod{24}$.

4.5.1 Résumé

Proposition 4.19. *Les corps de nombres quadratiques imaginaires admettant une classe euclidienne pour la norme sont exactement les suivants : $\mathbf{Q}\left(\sqrt{-1}\right)$, $\mathbf{Q}\left(\sqrt{-2}\right)$, $\mathbf{Q}\left(\sqrt{-3}\right)$, $\mathbf{Q}\left(\sqrt{-5}\right)$ (non principal), $\mathbf{Q}\left(\sqrt{-7}\right)$, $\mathbf{Q}\left(\sqrt{-11}\right)$ et $\mathbf{Q}\left(\sqrt{-15}\right)$ (non principal).*

Ce résultat avait déjà été énoncé par Lenstra ([Len78a]). Notons qu'il est encore vrai si on se restreint pas aux classes euclidiennes pour la norme (voir [GR11], qui utilise la construction de Motzkin).

disc_K	h_K	$M(K,[I])$
-283	2	$\frac{3}{4}$
-331	2	$\frac{3}{4}$
-643	2	$\frac{121}{144}$
-648	3	$\frac{3}{4}$
-676	3	$\frac{7}{8}$

TABLE IV.1 – Corps cubiques complexes K non principaux admettant une classe euclidienne pour la norme tels que $\mathrm{disc}_K \geqslant -3\,299$.

5 Algorithme de calcul

5.1 Description

On peut modifier l'algorithme 4.1 du chapitre II, paragraphe 4.1 pour calculer le minimum $M(K,[I])$ d'un corps de nombres. L'idée générale est de remplacer $\mathbf{Z}_K$ par n'importe quel idéal I de norme minimale. En pratique, on connaît une $\mathbf{Z}$-base $(z_i)_{1\leqslant i\leqslant n}$ de l'idéal I et à la place de $\mathcal{M}$ définie par (II.2) p. 21, on utilise la matrice $\mathcal{M}' = \left(m'_{i,j}\right)_{1\leqslant i,j\leqslant n}$ où pour tous $1 \leqslant i, j \leqslant n$,

$$m'_{i,j} = \begin{cases} \sigma_i(z_j) & \text{si } 1 \leqslant i \leqslant r_1, \\ \mathrm{Re}\left(\sigma_i(z_j)\right) & \text{si } r_1 < i \leqslant r_1 + r_2, \\ \mathrm{Im}\left(\sigma_i(z_j)\right) & \text{si } r_1 + r_2 < i \leqslant n. \end{cases}$$

Théorème 5.1. *Étant donné un corps de nombres K, l'algorithme décrit ci-dessus renvoie* échec *ou un idéal I de norme minimale, $M(K,[I])$ et tous les points $x \in K$ modulo I tels que $M(K,[I]) = m_{K,I}(x)$.*

En pratique, quitte à modifier les paramètres, l'exécution de cette procédure est couronnée de succès. De plus elle peut être accélérée si l'on veut simplement savoir si $M(K,[I]) < 1$.

5.2 Exemple d'application aux corps cubiques imaginaires

On considère un idéal I de norme minimale et on calcule $M(K,[I])$ avec l'algorithme décrit précédemment. Les exemples admettant une classe euclidienne non principale pour la norme sont présentés dans la table Table IV.1. Ces exemples sont les seuls tels que $|\mathrm{disc}_K| < 3\,299$.

On sait que si K admet une classe euclidienne pour la norme, alors $\mathrm{h}_K \leqslant 4$ d'après la proposition 2.25. Toutefois, aucun exemple de nombre de classes 4 n'a été trouvé.

5.3 Exemple de Graves

Dans l'article [Gra11], Graves donne l'exemple d'un corps de nombres admettant une classe euclidienne non principale, sans pouvoir dire si cette classe est euclidienne pour la norme. En appliquant l'algorithme, on obtient le résultat suivant.

Théorème 5.2. *$K = \mathbf{Q}\left(\sqrt{2}, \sqrt{35}\right)$ admet une classe euclidienne (non principale), mais aucune classe euclidienne pour la norme.*

Démonstration. Graves a prouvé dans [Gra11] que K a une classe euclidienne.

Par ailleurs, on peut voir K comme $\mathbf{Q}(x)$ où $x^4 - 36x^2 + 289 = 0$. Comme 2 est totalement ramifié dans K, on peut considérer l'idéal I premier au-dessus de 2. Alors

$$M(K, [I]) = m_{K,I}\left(\frac{x^3 + 17x^2 - 19x + 17}{34}\right) = m_{K,I}\left(\frac{x^3 + 17x^2 - 19x + 51}{34}\right) = \frac{7}{4}.$$

Par conséquent, K n'a pas de classe euclidienne pour la norme. □

6 Corps cubiques purs

Soit n un entier strictement supérieur à 1 dont aucun facteur n'est un cube, on appelle corps cubique pur tout corps de nombres K de la forme $K = \mathbf{Q}\left(\sqrt[3]{n}\right)$. Ces corps ont une signature $(1\,,\,1)$ et ont été étudiés par Dedekind ([Ded00]).

Théorème 6.1. *Soit n un entier strictement supérieur à 1 dont aucun facteur n'est un cube, le corps $\mathbf{Q}\left(\sqrt[3]{n}\right)$ admet une classe euclidienne pour la norme si et seulement si $n \in \{2, 3, 10\}$.*

En particulier, un corps cubique pur n'admet jamais une classe euclidienne non principale. Les corps cubiques purs euclidiens pour la norme ont été étudiés par Cioffari (voir [Cio79] et le théorème 5.1 du chapitre II, p. 38).

6.1 Propriétés générales des corps cubiques purs

Comme on suppose que n n'admet aucun facteur qui soit un cube, on peut écrire $n = ab^2$, où a et b sont deux entiers premiers entre eux sans facteur carré. De plus $\mathbf{Q}\left(\sqrt[3]{ab^2}\right) = \mathbf{Q}\left(\sqrt[3]{a^2b}\right)$, donc on peut supposer que $a > b$, quitte à échanger a et b. Dans la suite, on écrit $\alpha = \sqrt[3]{n}$.

6.1.1 Anneaux des entiers et idéaux

L'étude de l'anneau des entiers d'un corps cubique pur est classique et a été effectuée par Dedekind ([Ded00]). Pour une présentation plus moderne, on peut consulter [CT78, II.9.F et II.10.E], ou encore [Coh96, paragraphe 6.4].

Lemme 6.2. *Avec les notations précédentes, on peut décrire l'anneau des entiers de K :*

- *si $a^2 \not\equiv b^2 \pmod 9$, alors $\mathbf{Z}_K = \mathbf{Z} + \mathbf{Z}\alpha + \mathbf{Z}\frac{\alpha^2}{b}$ et $\mathrm{disc}_K = -27a^2b^2$,*
- *si $a^2 \equiv b^2 \pmod 9$, alors $\mathbf{Z}_K = \mathbf{Z}\alpha + \mathbf{Z}\frac{\alpha^2}{b} + \mathbf{Z}\frac{1+a\alpha+\alpha^2}{3}$ et $\mathrm{disc}_K = -3a^2b^2$.*

De plus les premiers se ramifient ainsi dans K :

- *soit p un facteur premier de n, $p \neq 3$, alors p est totalement ramifié dans K,*

– *si* $a^2 \not\equiv b^2 \pmod 9$*, alors* 3 *est totalement ramifié dans* K *; si* $a^2 \equiv b^2 \pmod 9$ *et* $9|n$*, alors* 3 *est totalement ramifié dans* K*,*
– *si* 2 *ne divise pas* n*, alors* 2 *est scindé en deux facteurs distincts.*

Par conséquent, il existe toujours un idéal de norme 2 *dans* K *et* $\Lambda(K) = 2$*.*

6.1.2 Nombre de classes

Le fait que K admette une classe euclidienne impose que le nombre de classe de K vérifie $\mathrm{h}_K \leqslant 4$. La théorie du genre donne des précisions sur le nombre de classes d'un corps cubique pur.

Lemme 6.3 ([BC70], Theorem 4.1)**.** *Soit* t *le nombre de premiers totalement ramifiés dans le corps cubique pur* K*. Si* $t \geqslant 2$*, alors* 3^{t-2} *divise* h_K*.*

Cette propriété a une conséquence importante sur la forme de n.

Corollaire 6.4. *Soit* n *un entier strictement supérieur à* 1 *dont aucun facteur n'est un cube, on suppose que* $K = \mathbf{Q}\left(\sqrt[3]{n}\right)$ *admet une classe euclidienne pour la norme, alors* n *admet au plus trois facteurs premiers.*

Démonstration. D'après le lemme 6.3, l'existence d'une classe euclidienne implique que n a au plus 4 facteurs premiers. De plus n ne peut avoir 4 facteurs premiers que si 3 est l'un d'entre eux. Or si 3 divise $n = ab^2$, alors $a^2 \not\equiv b^2 \pmod 9$ et donc $\mathrm{disc}_K = -27a^2b^2$. Dès lors $-\mathrm{disc}_K \geqslant 27 \cdot (2 \cdot 3 \cdot 5 \cdot 7)^2 = 1\,190\,700 \geqslant 170\,520$, ce qui empêche K d'admettre une classe euclidienne pour la norme d'après le théorème 3.20. □

6.2 Liste de candidats

Le but de ce paragraphe est d'établir une liste de candidats (aussi petite que possible) pouvant admettre une classe euclidienne. Comme Cioffari ([Cio79]) a déjà traité le cas principal, on peut se restreindre au cas non principal.

Proposition 6.5. *Si un corps cubique pur* K *admet une classe euclidienne non principale pour la norme, alors* $K = \mathbf{Q}\left(\sqrt[3]{n}\right)$ *où* n *est l'un des soixante-cinq éléments suivants :*

$$7, 11, 13, 14, 15, 19, 20, 21, 22, 26, 28, 30, 31, 34, 35, 37, 38, 42, 47, 51, 52, 60,$$
$$62, 68, 73, 74, 77, 78, 84, 89, 90, 92, 109, 117, 118, 127, 132, 134, 143, 150, 154,$$
$$156, 161, 163, 170, 172, 175, 181, 190, 206, 233, 244, 260, 275, 325, 350, 388,$$
$$396, 460, 476, 539, 550, 1\,666, 1\,700, 1\,900.$$

Démonstration. D'après la borne de Cassels (théorème 3.20), un tel corps K vérifie $|\mathrm{disc}_K| < 170520$. En utilisant l'expression de disc_K et le corollaire 6.4, on peut établir la liste finie des candidats.

Ainsi, si n est premier, alors $n < \sqrt{\frac{170\,520}{3}}$, donc $n \leqslant 233$. En fait, on a une meilleure borne si $n^2 \not\equiv 1 \pmod 9$. En ce cas, $n < \sqrt{\frac{170\,520}{27}}$, donc $n \leqslant 79$. Avec PARI ([PAR12]), on recense tous les premiers vérifiant ces conditions et tels que $\mathrm{h}_K \leqslant 4$, on obtient les quinze premiers suivants :

$$7, 11, 13, 19, 31, 37, 47, 73, 89, 109, 127, 163, 181, 233.$$

Si n admet exactement deux facteurs premiers $\alpha < \beta$, alors $\alpha < \sqrt[4]{\frac{170520}{3}}$, donc $\alpha \leqslant 13$.

- Si $\alpha = 13$, alors $\beta \leqslant 17$, donc $\beta = 17$. Mais $13 \equiv 4 \pmod 9$ et $17 \equiv -1 \pmod 9$, donc on ne peut pas avoir $a^2 \equiv b^2 \pmod 9$, donc $-\mathrm{disc}_K = 27 \cdot 13^2 \cdot 17^2 > 170520$.
- Si $\alpha = 11$, alors $\beta \leqslant 19$. Comme dans le cas précédent, on peut exclure $\beta \in \{17, 19\}$ par des congruences modulo 9. Donc le seul cas restant est $\beta = 13$, les congruences modulo 9 imposent alors que $n = 11 \cdot 13 = 143$.
- Si $\alpha = 7$, alors $\beta \leqslant 31$ et on trouve les trois valeurs 77, 161 et 539.
- Si $\alpha = 5$, alors $\beta \leqslant 47$ et quatre valeurs de n sont possibles : 35, 175, 275 et 325.
- Si $\alpha = 3$, alors $a^2 \not\equiv b^2 \pmod 9$, donc $\beta < \sqrt{\frac{170520}{27 \cdot 3^2}}$ et $\beta \leqslant 23$. Comme précédemment, on ne garde que les valeurs pour lesquelles $\mathrm{h}_K \leqslant 4$ et on trouve les quatre candidats 15, 21, 51 et 117.
- Si $\alpha = 2$, alors $\beta \leqslant 113$ de sorte que dix-huit candidats sont possibles :

$$20, 14, 28, 22, 26, 52, 34, 68, 38, 92, 62, 74, 172, 118, 244, 134, 388 \text{ et } 206.$$

Examinons enfin le cas où n a trois facteurs premiers distincts, notons les $\alpha < \beta < \gamma$. Alors $\alpha < \sqrt[6]{\frac{170520}{3}}$, donc $\alpha \leqslant 5$.

- Si $\alpha = 5$, alors $5 < \beta < \sqrt[4]{\frac{170520}{3 \cdot 5^2}}$ et aucun premier ne vérifie cette propriété.
- Si $\alpha = 3$, alors $a^2 \not\equiv b^2 \pmod 9$ et donc $\mathrm{disc}_K = -27a^2b^2$. Cela impose $\beta = 5$. Mais alors $5 < \gamma < \sqrt{\frac{170520}{27 \cdot 3^2 \cdot 5^2}}$, ce qui est impossible.
- Si $\alpha = 2$, alors on trouve de même $\beta \leqslant 7$.
  - Si $\beta = 7$, alors $\gamma \leqslant 17$ et on trouve que n vaut 154, 476 ou 1 666.
  - Si $\beta = 5$, alors $\gamma \leqslant 23$, ce qui donne les huit valeurs suivantes possibles pour n : 170, 190, 260, 350, 460, 550, 1 700 et 1 900.
  - Si $\beta = 3$, alors $\gamma \leqslant 13$ (en tenant compte du fait que $a^2 \not\equiv b^2 \pmod 9$), ce qui donne dix possibilités :

$$30, 42, 60, 78, 84, 90, 132, 150, 156 \text{ et } 396.$$

Cela achève la preuve. □

L'objet des paragraphes suivants va être d'étudier ces cas.

6.3 Raisonnements de base

Avant d'utiliser des raisonnements plus techniques, nous signalons ici les valeurs de n qui peuvent être écartées facilement.

6.3.1 Idéaux principaux de norme 2

Si K n'est pas principal mais admet un idéal principal de norme 2 (donc minimale), alors K ne peut pas admettre de classe euclidienne d'après la proposition 2.21. Ainsi, on peut exclure les valeurs suivantes de n :

$$31, 34, 60, 62, 68, 109, 118, 127, 172.$$

n	7	11	13	14	15	19	20
$M(K,[I])$	$\frac{19}{10}$	$\frac{9}{4}$	$\frac{479}{147}$	$\frac{140}{23}$	$\frac{13\,857}{4\,052}$	$\frac{9}{8}$	$\frac{36}{19}$
n	21	22	26	28	30	35	37
$M(K,[I])$	$\frac{24\,749}{4\,976}$	$\frac{335}{66}$	$\frac{24}{19}$	$\frac{883}{332}$	$\frac{5}{4}$	$\frac{6\,859}{1\,215}$	$\frac{181}{75}$
n	38	42	52	73	84	90	117
$M(K,[I])$	$\frac{770\,729}{86\,762}$	$\frac{682\,075}{63\,512}$	$\frac{61}{8}$	$\frac{629\,127}{150\,124}$	$\frac{2\,972\,191}{250\,051}$	$\frac{1\,033\,977}{174\,968}$	$\frac{960\,584}{96\,905}$
n	150	325	350	539			
$M(K,[I])$	$\frac{491\,159}{73\,620}$	$\frac{33\,403}{6\,864}$	$\frac{301\,431}{66\,158}$	$\frac{6\,669\,477}{970\,472}$			

TABLE IV.2 – Calcul de quelques valeurs de minimum euclidien par rapport à une classe de corps cubiques purs.

6.3.2 Application de l'algorithme 2.1

On peut chercher à calculer le minimum $M(K,[I])$ pour un idéal I de plus petite norme 2. En pratique, cela ne fonctionne que lorsque l'unité fondamentale de K n'est « pas trop grosse ». Cela permet ainsi d'éliminer quelques cas.

Proposition 6.6. *Pour les valeurs de n dans la table IV.2, on a $M(K,[I])>1$, donc K n'admet pas de classe euclidienne.*

6.4 Raisonnements par congruence

6.4.1 Outil crucial

Dans la suite du paragraphe, le résultat suivant va être largement utilisé.

Proposition 6.7. *Étant donné un corps de nombres k et $a\in\mathbf{N}$, on peut déterminer en pratique s'il existe $z\in\mathbf{Z}_k$ tel que $\left|\mathbf{N}_{K/\mathbf{Q}}(z)\right|=a$.*

Démonstration. Voir [Coh96], paragraphe 6.4. □

On va à présent utiliser le fait que les facteurs de n (éventuellement à l'exception de 3) sont totalement ramifiés dans K. Même si les raisonnements sont analogues, on va distinguer les cas où les idéaux au-dessus des produits de premiers utilisés sont principaux ou non.

6.4.2 Cas principal

Lemme 6.8. *Soit f un produit de premiers distincts totalement ramifiés dans K, on écrit $\mathfrak{f}$ l'idéal de $\mathbf{Z}_K$ tel que $f\mathbf{Z}_K=\mathfrak{f}^3$. Si $\alpha,\beta\in\mathbf{Z}_K$ vérifient $\alpha\equiv\beta \pmod{\mathfrak{f}}$, alors*

$$\mathbf{N}_{K/\mathbf{Q}}(\alpha)\equiv\mathbf{N}_{K/\mathbf{Q}}(\beta) \pmod{f}.$$

Une propriété tout à fait similaire est énoncée par Egami ([Ega79]), il attribue la parenté de cet argument à Lenstra.

Démonstration. Soit L la fermeture galoisienne de $K/\mathbf{Q}$, on écrit $\mathcal{F} = \mathfrak{f}\mathbf{Z}_L$. Alors $f\mathbf{Z}_L = f\mathbf{Z}_K\mathbf{Z}_L = \mathfrak{f}^3\mathbf{Z}_L = \mathcal{F}^3$.

Par conséquent, si $\varphi : K \longrightarrow L$ est un plongement de K, alors $f\mathbf{Z}_L = \varphi(f\mathbf{Z}_L) = \varphi(\mathcal{F})^3$, donc $\varphi(\mathcal{F}) = \mathcal{F}$. Comme $\alpha \equiv \beta \pmod{\mathcal{F}}$, on a aussi la congruence $\mathbf{N}_{K/\mathbf{Q}}(\alpha) \equiv \mathbf{N}_{K/\mathbf{Q}}(\beta) \pmod{\mathcal{F}}$. Mais $\mathbf{N}_{K/\mathbf{Q}}(\alpha) - \mathbf{N}_{K/\mathbf{Q}}(\beta) \in \mathbf{Z}$ et $\mathcal{F} \cap \mathbf{Z} = f\mathbf{Z}$, donc

$$\mathbf{N}_{K/\mathbf{Q}}(\alpha) \equiv \mathbf{N}_{K/\mathbf{Q}}(\beta) \pmod{f}.$$

□

En pratique, on sait que certains entiers sont des normes.

Lemme 6.9. *Soit p un premier tel que $p \not\equiv 1 \pmod 3$, alors pour tout $x \in \mathbf{Z}/p\mathbf{Z}$, il existe $\alpha \in \mathbf{Z}/p\mathbf{Z}$ tel que $x = \alpha^3$.*

Démonstration. Pour $p = 3$, on peut prendre $\alpha = x$. Pour les autres valeurs de p, on note $p = 3k + 2$ pour un certain entier k. Alors $\alpha = x^{2k+1}$ convient. □

Lemme 6.10. *Soit $f = \prod_{i=1}^{l} p_i$ où $p_i \not\equiv 1 \pmod 3$ sont des premiers distincts totalement ramifiés dans K. On note $f\mathbf{Z}_K = \mathfrak{f}^3$, pour un idéal $\mathfrak{f}$ de $\mathbf{Z}_K$. On suppose que $\mathfrak{f}$ est principal. Si $0 < e < f$ est un entier tel que ni $e - 2f$, ni $e - f$, ni e, ni $e + f$ ne sont des normes d'éléments de $\mathbf{Z}_K$, alors $M(K) > 2$ et par conséquent $M(K, [I]) > 1$ pour tout idéal I de norme minimale 2.*

Démonstration. D'après le lemme 6.9 et le théorème chinois, il existe un entier α tel que $e \equiv \alpha^3 \pmod f$. Par conséquent, $e \equiv \mathbf{N}_{K/\mathbf{Q}}(\alpha) \pmod f$. On écrit $\mathfrak{f} = \gamma\mathbf{Z}_K$ pour $\gamma \in \mathbf{Z}_K \setminus \{0\}$, de sorte qu'il existe $\delta \in \mathbf{Z}_K$ tel que

$$\begin{aligned} m_K\left(\frac{\alpha}{\gamma}\right) &= \left|\mathbf{N}_{K/\mathbf{Q}}\left(\frac{\alpha}{\gamma} - \delta\right)\right| \\ &= \frac{1}{\mathbf{N}\mathfrak{f}}\left|\mathbf{N}_{K/\mathbf{Q}}(\alpha - \delta\gamma)\right|. \end{aligned}$$

Or $\alpha - \delta\gamma \equiv \alpha \pmod{\mathfrak{f}}$, donc d'après le lemme 6.8,

$$\mathbf{N}_{K/\mathbf{Q}}(\alpha - \delta\gamma) \equiv \mathbf{N}_{K/\mathbf{Q}}(\alpha) \equiv e \pmod{f}.$$

Cela implique que $m_K\left(\frac{\alpha}{\gamma}\right) \geqslant \dfrac{\min\{3f - e, e + 2f\}}{f} > 2.$ □

Remarque 6.11. L'hypothèse « $p_i \not\equiv 1 \pmod 3$ » est utilisée pour trouver un élément $\alpha \in \mathbf{Z}_K$ tel que $\mathbf{N}_{K/\mathbf{Q}}(\alpha) \equiv e \pmod f$. Cette hypothèse peut donc être omise si on fournit directement un tel élément α.

Proposition 6.12. *Les corps cubiques purs correspondant aux valeurs* 47, 51, 74, 89, 154, 170, 175, 190, 206, 233, 460, 476, 550, 1 666, 1 700 *n'admettent pas de classe euclidienne pour la norme.*

n	f	e
47	$3 \cdot 47$	29
51	17	2
89	89	5
154	$2 \cdot 11$	4
170	$2 \cdot 5 \cdot 17$	5
175	$3 \cdot 5$	4
233	233	5
460	23	2
476	$2 \cdot 17$	3
550	$2 \cdot 11$	2
1 666	$2 \cdot 17$	3
1 700	17	2

(a) Cas principal

n	f	e
77	$3 \cdot 11$	7
92	23	5
132	11	5
143	11	2
161	23	2
260	$2 \cdot 5$	3
275	11	4
350	5	2
396	11	4
1 900	5	2

(b) Autre cas

TABLE IV.3 – Ces corps n'admettent pas de classe euclidienne pour la norme.

Démonstration. Il suffit d'appliquer le lemme 6.10 avec les valeurs données dans la table IV.3, (a) pour toutes les valeurs sauf 74, 190 et 206. Pour ces valeurs, on note x une racine de $X^3 - n$ dans K.

Pour 74, on peut poser $f = 74 = 2 \cdot 37$. Même si $37 \equiv 1 \pmod 3$, on peut appliquer la remarque 6.11 avec $e = 31$ pour prouver que $M(K, [I]) > 1$ car $179 = \mathbf{N}_{K/\mathbf{Q}}(2x^2 - x - 31) \equiv e \pmod f$.

Pour 190, de même, on prend $f = 190 = 2 \cdot 5 \cdot 19$ et $e = 152$ pour conclure que K n'admet pas de classe euclidienne parce que $532 = \mathbf{N}_{K/\mathbf{Q}}(3\,393x^2 + 19\,506x + 112\,138) \equiv e \pmod f$.

Pour 206, on applique le même raisonnement avec $f = 206 = 2 \cdot 103$ et $e = 31$ car $443 = \mathbf{N}_{K/\mathbf{Q}}(x^2 - 3x - 17) \equiv e \pmod f$. □

On a appliqué un résultat qui ne s'appliquait que quand l'idéal au-dessus d'un produit de premiers totalement ramifié est principal, on peut établir un résultat analogue quand cet idéal n'est pas principal.

6.4.3 Autre cas

Lemme 6.13. *Soit $f = \prod_{i=1}^{l} p_i$ où $p_i \not\equiv 1 \pmod 3$ sont des premiers distincts totalement ramifiés dans K. On écrit $\mathfrak{f}^3 = f\mathbf{Z}_K$, où $\mathfrak{f}$ est un idéal entier de K. On suppose que $[\mathfrak{f}] = [I]$, où I est un idéal de norme minimale 2. Si $0 < e < f$ est un entier tel que ni $e - f$, ni e ne sont des normes d'éléments de $\mathbf{Z}_K$, alors $M(K, [I]) > 1$.*

Démonstration. On applique à nouveau le 6.9 et le théorème chinois pour trouver un entier α tel que $e \equiv \mathbf{N}_{K/\mathbf{Q}}(\alpha) \pmod f$. Il existe alors $\gamma \in \mathfrak{f}$ tel que

$$m_{K,\mathfrak{f}}(\alpha) = \frac{1}{\mathbf{N}\mathfrak{f}} \left| \mathbf{N}_{K/\mathbf{Q}}(\alpha - \gamma) \right|.$$

Or $\alpha - \gamma \equiv \alpha \pmod{\mathfrak{f}}$, donc d'après le lemme 6.8,

$$\mathbf{N}_{K/\mathbf{Q}}(\alpha - \gamma) \equiv \mathbf{N}_{K/\mathbf{Q}}(\alpha) \equiv e \pmod{f}.$$

Dès lors, $m_{K,\mathfrak{f}}(\alpha) \geqslant \frac{\min\{2f-e, e+f\}}{f} > 1$. On en déduit $M(K, [I]) = M(K, [\mathfrak{f}]) > 1$ et K n'admet pas de classe euclidienne pour la norme. □

Proposition 6.14. *Les corps cubiques purs correspondant aux valeurs* 77, 92, 132, 143, 161, 260, 275, 350, 396, 1 900 *n'ont pas de classe euclidenne pour la norme.*

Démonstration. Il suffit d'appliquer le lemme 6.13 avec les valeurs données dans la table IV.3, (b). Pour chaque valeur de n dans la table, $\mathrm{h}_K = 3$. Comme les valeurs de f ne sont pas des normes d'éléments de $\mathbf{Z}_K$, on a $[\mathfrak{f}] = [I]$ ou $[\mathfrak{f}] = [I]^2$. Dans ce dernier cas, $\mathfrak{f}I$ est un idéal principal, donc $2f$ est une norme d'un élément de $\mathbf{Z}_K$. On vérifie rapidement que ce n'est pas le cas, de sorte que $[\mathfrak{f}] = [I]$ et $M(K, [\mathfrak{f}] = M(K, [I])$. □

6.5 Fin de la preuve

Une lecture attentive fait remarquer que quelques valeurs restent à traiter. Pour ce faire, même si les lemmes 6.10 et 6.13 ne s'appliquent pas exactement, l'idée reste similaire : on exhibe un point $t = \frac{a}{b} \in K$ (où a et b sont des éléments non nuls de $\mathbf{Z}_K$) et en calculant

$$\mathbf{N}_{K/\mathbf{Q}}(a - bu)$$

pour tout élément u de l'idéal I de norme 2 (dans les cas restants, cet idéal est unique, on en connaît une $\mathbf{Z}$-base), on remarque qu'il existe $l \in \mathbf{N}$ et $e \in \{0, 1, \ldots, l-1\}$ tels que

$$\mathbf{N}_{K/\mathbf{Q}}(a - bu) \equiv e \pmod{l}.$$

Dès lors, $\mathbf{N}_{K/\mathbf{Q}}(a - bu) \in e + l\mathbf{Z}$. On exclut certaines possibilités parce qu'elles ne sont pas des normes d'éléments de $\mathbf{Z}_K$ et on note N le plus petit entier possible (en valeur absolue). Alors

$$m_{K,I}(t) \geqslant \frac{|N|}{\left|\mathbf{N}_{K/\mathbf{Q}}(b)\right| \cdot \mathbf{N}I} = \frac{|N|}{2\left|\mathbf{N}_{K/\mathbf{Q}}(b)\right|}.$$

Si $|N| \geqslant 2\left|\mathbf{N}_{K/\mathbf{Q}}(b)\right|$, cela prouve que K n'admet pas de classe euclidienne pour la norme.

Par exemple, pour $n = 78$, on écrit $x = \sqrt[3]{n}$, de sorte que $I = 2\mathbf{Z} + \mathbf{Z}x + \mathbf{Z}x^2$ est l'idéal de norme 2 de $\mathbf{Z}_K$. On considère alors $a = x$, $b = 3$ et on calcule pour tous α, β, $\gamma \in \mathbf{Z}_K$

$$\begin{aligned}&\mathbf{N}_{K/\mathbf{Q}}(a + 3(2\alpha + \beta x + \gamma x^2))\\ &= 54 \cdot \left(4\alpha^3 - 234\alpha\beta\gamma - 78\alpha\gamma + 39\beta^3 + 39\beta^2 + 13\beta + 3042\gamma^3 + 1\right) + 24,\end{aligned}$$

ce qui montre que pour tout $u \in I$,

$$\mathbf{N}_{K/\mathbf{Q}}(a - bu) \equiv 24 \pmod{54}.$$

Avec les notations précédentes, on obtient $l = 54$ et $e = 24$. Or ni 24, ni -30 ne sont des normes d'éléments de $\mathbf{Z}_K$, donc $N = 78 \geqslant 54 = 2\left|\mathbf{N}_{K/\mathbf{Q}}(b)\right|$. Ainsi, K n'admet pas de classe euclidienne pour la norme.

Pour les autres valeurs de n, on liste les éléments a, b, l, e et N dans la table IV.4.

n	a	b	l	e	N
78	x	3	54	24	78
134	67	x	134	67	1139
156	x	3	54	50	104
163	32	x	326	168	484
181	60	x	382	248	476
244	x	2	8	4	20
388	97	x	194	97	873

TABLE IV.4 – Cas restants, $x = \sqrt[3]{n}$.

7 Autres exemples

7.1 Corps quartiques totalement imaginaires

Avec l'algorithme, on peut trouver 26 exemples de corps de nombres non principaux admettant une classe euclidienne pour la norme. Ils sont recensés dans la table IV.5. Le premier, de discriminant 1 521, avait déjà donné par Lenstra ([Len78a]). La meilleure borne connue pour de tels corps de nombres est $\mathrm{h}_K \leqslant 6$, mais tous les exemples trouvés vérifient $\mathrm{h}_K = 2$.

7.2 Autres signatures

On peut trouver de nombreux autres exemples de corps de nombres non principaux admettant une classe euclidienne en degré supérieur. En particulier, on a trouvé des exemples vérifiant les propriétés suivantes.

Théorème 7.1. *Il existe des corps de nombres de degré jusqu'à* 6 *admettant une classe euclidienne pour la norme non principale.*

Dans la table IV.6, on donne un exemple pour chaque degré et diverses signatures. Notons que l'on obtient des exemples dont le nombre de classes vaut 3 ou 4.

De plus, pour une signature donnée, le corps de nombres non principal de plus petit discriminant n'admettant pas toujours de classe euclidienne pour la norme. Par exemple, le corps de nombres de discriminant 1 957 et de signature $(3\,,\,0)$ n'admet pas de classe euclidienne pour la norme. En effet, on a $M\,(K,\,[I]) = 1$, où I est l'idéal de norme 2 de $\mathbf{Z}_K$.

disc_K	h_K	$M(K,[I])$	disc_K	h_K	$M(K,[I])$	disc_K	h_K	$M(K,[I])$
1 521	2	$\frac{4}{9}$	3 528	2	$\frac{11}{18}$	4 725	2	$\frac{7}{9}$
1 872	2	$\frac{4}{9}$	3 600[c]	2	$\frac{3}{4}$	4 752	2	$\frac{8}{9}$
2 304	2	$\frac{3}{4}$	3 600[d]	2	$\frac{7}{9}$	5 076	2	$\frac{7}{8}$
2 457[a]	2	$\frac{7}{13}$	3 625	2	$\frac{19}{25}$	5 225	2	$\frac{19}{25}$
2 457[b]	2	$\frac{4}{7}$	3 700	2	$\frac{3}{4}$	5 328	2	$\frac{109}{148}$
2 889	2	$\frac{5}{6}$	4 329[e]	2	$\frac{19}{28}$	5 616	2	$\frac{49}{52}$
2 925	2	$\frac{7}{9}$	4 329[f]	2	$\frac{301}{481}$	6 669[g]	2	< 0.924
3 024	2	$\frac{19}{28}$	4 352	2	$\frac{33}{34}$	6 669[h]	2	< 0.787
3 025	2	$\frac{11}{16}$	4 400	2	$\frac{19}{25}$			

TABLE IV.5 – Exemples de corps de nombres quartiques totalement imaginaires non principaux admettant une classe euclidienne pour la norme. I désigne un idéal de norme minimale. En cas d'ambiguïté, un polynôme minimal est donné ci-dessous. La table est très certainement incomplète.

[a] $x^4 - x^3 + 9x^2 - 4x + 16$
[b] $x^4 - x^3 - 6x^2 - x + 19$
[c] $x^4 + x^2 + 4$
[d] $x^4 - 5x^2 + 25$
[e] $x^4 - x^3 + 11x^2 - 2x + 28$
[f] $x^4 - x^3 - 10x^2 + 7x + 31$
[g] $x^4 - 2x^3 - 12x^2 + 13x + 43$
[h] $x^4 - x^3 - 12x^2 + 2x + 49$

n	(r_1, r_2)	h_K	un polynôme minimal tel que $K = \mathbf{Q}(x)$	disc_K	$M(K, [I])$
3	$(3,0)$	2	$x^3 - x^2 - 14x + 23$	2 777	$\frac{5}{9}$
		3	$x^3 - x^2 - 30x + 64$	8 281	$\frac{27}{28}$
4	$(4,0)$	2	$x^4 - 17x^2 + 36$	21 025	$\frac{5}{16}$
	$(2,1)$	2	$x^4 - 2x^3 + 5x^2 - 2x - 1$	−6 848	$\frac{4}{9}$
		3	$x^4 - x^3 - 3x^2 + 12x - 8$	−27 620	$\frac{7}{8}$
		4	$x^4 - x^3 - 2x^2 + 4x - 24$	−54 764	$\frac{7}{8}$
5	$(5,0)$	2	$x^5 - 11x^3 - 9x^2 + 14x + 9$	4 010 276	$\frac{3}{4}$
	$(3,1)$	2	$x^5 - 2x^4 + 2x^3 - 12x^2 + 21x - 9$	−243 219	$\frac{4}{9}$
	$(1,2)$	2	$x^5 - x^4 - 2x^2 + 4x - 1$	41 381	$\frac{4}{9}$
		3	$x^5 - 2x^4 + 4x^3 - 6x^2 + 3x + 1$	130 925	$\frac{3}{4}$
6	$(2,2)$	2	$x^6 - 2x^5 - x^4 + 7x^3 - 6x^2 + 3x - 1$	1 387 029	< 1
	$(0,3)$	2	$x^6 - 3x^5 + 3x^4 - x^3 + 3x^2 - 3x + 1$	−273 375	< 1

TABLE IV.6 – Quelques nouveaux exemples de corps de nombres K non principaux admettant une classe euclidienne pour la norme. I est un idéal de norme minimale de K.

CHAPITRE V

EUCLIDIANITÉ DES CORPS DE QUATERNIONS

Plan

Ce chapitre contient l'article [CCL12] à paraître à l'*International Journal of Number Theory*.

1 Définitions et premières propriétés

1.1 Introduction

Le but de ce chapitre est d'étudier l'euclidianité des corps de quaternions. Comme pour les corps de nombres, on peut obtenir des résultats pour le seul stathme norme ou en toute généralité.

Dans tout ce chapitre, on considère un *corps de quaternions* F sur un corps de nombres K, c'est un exemple particulier d'algèbre à division centrale de dimension 4 sur un corps de nombres K, de base $(1, i, j, k)$ vérifiant $i^2 = a$, $j^2 = b$ et $k = ij = -ji$ pour a, b éléments non nuls de K. On notera cette algèbre sous la forme $F = \left(\frac{a,b}{K}\right)$. C'est une algèbre à division si et seulement si la forme quadratique (appelée norme réduite) définie pour $x, y, z, t \in K$ par

$$\mathrm{nrd}_{F/K}(x + yi + zj + tk) := x^2 - ay^2 - bz^2 + abt^2$$

ne représente 0 que trivialement.

Pour $x, y, z, t \in K$, on appelle *conjugué* de $x + yi + zj + tk$ l'élément de F

$$\overline{x + yi + zj + tk} := x - yi - zj - tk.$$

Avec cette définition, on a $\mathrm{nrd}_{F/K}(x+yi+zj+tk) = (x+yi+zj+tk)\cdot\overline{x+yi+zj+tk}$. On définit aussi la *trace réduite* de $x + yi + zj + tk$ par

$$\mathrm{trd}_{F/K}(x + yi + zj + tk) := x + yi + zj + tk + \overline{x + yi + zj + tk} = 2x \in K.$$

Les propriétés de base des corps de quaternions sont classiques et peuvent être trouvées dans [Deu35], [Rei75] ou [Vig80]. Toutefois, la terminologie employée par ces ouvrages n'est pas toujours identique. Nous indiquerons le cas échéant les différences.

Comme pour les corps des nombres, même si on va être amené à parler de l'euclidianité de F, l'anneau sur lequel la propriété d'euclidianité va porter ne sera pas F mais un autre défini à partir de F.

1.2 Ordres et idéaux

Nous rappelons les définitions et propriétés de base des ordres et des idéaux.

1.2.1 Définitions de bases

Définition 1.1. Un *idéal* I de F est un $\mathbf{Z}_K$-réseau complet de F, c'est-à-dire qu'il vérifie $KI = F$.

Remarque 1.2. Il existe toujours au moins un idéal, on peut par exemple considérer $I = \mathbf{Z}_K + \mathbf{Z}_K i + \mathbf{Z}_K j + \mathbf{Z}_K k$.

Définition 1.3. Un *ordre* de F est un idéal qui est aussi un sous-anneau de F.

Tout idéal I définit naturellement deux ordres appelés *ordre à droite* et *ordre à gauche* de I et définis par

$$\mathcal{O}_r(I) = \{x \in F,\ Ix \subseteq I\} \qquad \text{et} \qquad \mathcal{O}_r(I) = \{x \in F,\ xI \subseteq I\}.$$

D'après la remarque 1.2, cela montre que tout corps de quaternions F contient au moins un ordre.

Lemme 1.4. *Tout élément x de F entier sur $\mathbf{Z}_K$ appartient à un ordre de F.*

Démonstration. On note $\Gamma = \mathbf{Z}_K[x]$, c'est un sous-anneau de F contenant $\mathbf{Z}_K$. Soit I un idéal (qui existe d'après la remarque 1.2), alors $I\Gamma$ est un idéal car Γ est un $\mathbf{Z}_K$-module de type fini. Comme Γ est un anneau, $\Gamma \subseteq \mathcal{O}_r(I\Gamma)$, donc $x \in \mathcal{O}_r(I\Gamma)$. □

En fait, cela donne une caractérisation des ordres comme suit.

Proposition 1.5. *Soit Γ un sous-anneau de F contenant $\mathbf{Z}_K$, tel que $K \cdot \Gamma = F$ et tel que tout élément de Γ est entier sur $\mathbf{Z}_K$. Alors Γ est un ordre de F.*

Réciproquement, tout ordre de F a ces propriétés.

Démonstration. Notons $F = \oplus_{i=1}^{4} Ku_i$, avec $u_i \in \Gamma$. Comme F est séparable sur K, $\alpha = \det(\mathrm{trd}_{F/K}(u_i u_j))_{1\leqslant i,j\leqslant 4}$ est un élément de $\mathbf{Z}_K$ non nul.

Soit $x \in \Gamma$, alors $x = \sum_{i=1}^{4} r_i u_i$, où $r_i \in K$. Dès lors

$$\mathrm{trd}_{F/K}(xu_j) = \sum_{i=1}^{4} r_i \mathrm{trd}_{F/K}(u_i u_j).$$

Or $\mathrm{trd}_{F/K}(xu_j) \in \mathbf{Z}_K$ car $xu_j \in \Gamma$. Cela donne un système d'équations de déterminant $\alpha \neq 0$, on peut donc appliquer les règles de Cramer pour trouver que pour tout $1 \leqslant i \leqslant 4$,

$$r_i = \frac{\text{élément de } \mathbf{Z}_K}{\alpha}.$$

Par conséquent, $\Gamma \subseteq \alpha^{-1} \cdot \sum_{i=1}^{4} \mathbf{Z}_K u_i$, ce qui montre que Γ est un ordre.

La réciproque est une conséquence facile du lemme 1.4. □

Les ordres sont donc des objets naturels pour généraliser l'anneau des entiers de K comme les entiers de F ne forment en général pas un anneau.

Exemple 1.6. Dans $F = \mathcal{M}_2(\mathbf{Q})$, les matrices $A = \begin{pmatrix} \frac{1}{2} & -3 \\ \frac{1}{4} & \frac{1}{2} \end{pmatrix}$ et $B = \begin{pmatrix} 0 & \frac{1}{5} \\ 5 & 0 \end{pmatrix}$ sont entières, mais ni $A+B$ ni AB ne le sont.

En effet, x^2-x+1 et x^2-1 annulent respectivement A et B, alors que les polynômes minimaux respectifs de $A+B$ et AB sont $x^2 - x + \frac{299}{20}$ et $x^2 + \frac{229}{20}x - 1$.

Exemples 1.7. Dans $\left(\frac{-1,-1}{\mathbf{Q}}\right)$, $\Lambda_1 = \mathbf{Z} \oplus \mathbf{Z}i \oplus \mathbf{Z}j \oplus \mathbf{Z}k$ et $\Lambda_2 = \mathbf{Z} \oplus \mathbf{Z}i \oplus \mathbf{Z}j \oplus \mathbf{Z}\frac{1+i+j+k}{2}$ sont des ordres.

Remarque 1.8. Soit Λ un ordre, alors $\overline{\Lambda} = \Lambda$.

Démonstration. Soit $\lambda \in \Lambda$. Par définition, Λ est un $\mathbf{Z}_K$-module, donc $\mathrm{trd}_{F/K}(\lambda) \in \mathbf{Z}_K \subseteq \Lambda$. Dès lors, $\overline{\lambda} = \mathrm{trd}_{F/K}(\lambda) - \lambda \in \Lambda$. Cela montre que $\overline{\Lambda} \subseteq \Lambda$. Comme $\overline{\Lambda}$ est aussi un ordre, on a l'inclusion réciproque par symétrie. Par conséquent,

$$\overline{\Lambda} = \Lambda.$$

□

Définition 1.9. Un ordre Λ est *maximal* s'il n'est proprement inclus dans aucun autre ordre.

Dans l'exemple 1.7, $\Lambda_1 \subsetneq \Lambda_2$, de sorte que Λ_1 n'est pas maximal. Plus généralement, le lemme de Zorn permet d'affirmer qu'un corps de quaternions admet toujours au moins un ordre maximal (vu qu'il admet au moins un ordre).

Proposition 1.10. *Tout ordre Λ est contenu dans un ordre maximal de F.*

Démonstration. Notons C la collection des ordres de F contenant Λ, alors $\Lambda \in C$, donc $C \neq \varnothing$. Soit alors $\{\Lambda_\alpha\}$ une suite croissante d'éléments de C. Posons $\Lambda' := \sum_\alpha \Lambda_\alpha = \cup_\alpha \Lambda_\alpha$. Alors

- Λ' est un sous-anneau de F,
- $\Lambda' \supseteq \mathbf{Z}_K$,
- $K \cdot \Lambda' = F$,
- soit $x \in \Lambda'$, alors il existe α tel que $x \in \Lambda_\alpha$, donc x est entier sur $\mathbf{Z}_K$.

D'après la proposition 1.5, cela montre que Λ' est un ordre. Comme $\Lambda \subseteq \Lambda'$, on en déduit que $\Lambda' \in C$.

Comme toute suite croissante de C admet une borne supérieure dans C, on peut appliquer le lemme de Zorn pour en déduire que C a un élément maximal, qui est l'ordre maximal recherché. □

1.2.2 Nombres de classes et de types

Soit Λ un ordre. Deux idéaux I et J d'ordre à gauche Λ sont équivalents s'il existe $x \in F \setminus \{0\}$ tel que $I = Jx$. Les classes d'équivalence sont alors appelées les classes à gauche de Λ. On peut définir de même les classes à droite de Λ. Si on suppose que Λ est un ordre maximal, alors les nombres de classes à gauche et à droite sont finis et égaux. De plus ce nombre ne dépend pas de Λ. Ainsi, on l'appelle *nombre de classes* de F et on le note h_F.

Deux ordres Λ et Λ' sont du même *type* (ou encore *conjugués*) s'il existe $x \in F \setminus \{0\}$ tels que $\Lambda' = x^{-1}\Lambda x$. Cela définit une relation d'équivalence sur l'ensemble des ordres maximaux de F. Le nombre de classes pour cette relation est appelé le *nombre de types*, on le note t_F et il vérifie $t_F \leqslant h_F$.

1.2.3 Caractère bilatère, intégrité, primalité des idéaux

Dans tout ce paragraphe, I désigne un idéal de F. Le but est d'énoncer un analogue de la décomposition des idéaux fractionnaires dans les corps de nombres dans le cas des corps de quaternions et de voir le comportement de la norme réduite avec cette décomposition.

Définition 1.11. On appelle norme réduite de I l'idéal fractionnaire de $\mathbf{Z}_K$ engendré par les $\mathrm{nrd}_{F/K}(x)$ où $x \in I$. On le notera $\mathrm{nrd}_{F/K}(I)$.

Étant donné deux idéaux I et J de F quelconques, le produit IJ est défini comme dans le cas commutatif :

$$IJ := \left\{ \sum_{i,\ \text{finie}} \alpha_i\beta_i,\ \alpha_i \in I,\ \beta_i \in J \right\}.$$

Comme les idéaux $\mathrm{nrd}_{F/K}(IJ)$ et $\mathrm{nrd}_{F/K}(I)\mathrm{nrd}_{F/K}(J)$ ne coïncident pas forcément, on va restreindre le cadre d'étude pour voir dans quels cas on peut assurer la validité de cette propriété.

Définition 1.12. I est *bilatère* si $\mathcal{O}_l(I) = \mathcal{O}_r(I)$; il est dit *normal* si $\mathcal{O}_r(I)$ et $\mathcal{O}_r(I)$ sont des ordres maximaux, *entier* s'il est normal et si $I \subseteq \mathcal{O}_l(I)$ (ce qui équivaut à $I \subseteq \mathcal{O}_r(I)$ en ce cas).

Exemple 1.13. Soient Λ un ordre maximal et $x \in \Lambda$. Alors $I = x\Lambda$ est un idéal entier. En effet, son ordre à droite est Λ, tandis que son ordre à gauche est $x\Lambda x^{-1}$. Ce sont des ordres maximaux. De plus comme $x \in \Lambda$, $I \subseteq \Lambda$ (et $I \subseteq x\Lambda x^{-1}$).

Si I est un idéal entier d'ordre à droite Λ, alors

$$|\Lambda/I| = \mathbf{N}_{K/\mathbf{Q}}(\mathrm{nrd}_{F/K}(I))^2.$$

Remarque 1.14. Par conséquent, si I et J sont deux idéaux entiers d'ordre à droite Λ vérifiant $I \subseteq J$ et $\mathrm{nrd}_{F/K}(I) = \mathrm{nrd}_{F/K}(J)$, alors $I = J$.

Définition 1.15. Un idéal *premier* $\mathfrak{P}$ de Λ est un idéal bilatère, propre et entier d'ordre à droite (et à gauche) Λ tel que pour tout couple d'idéaux entiers $(S,\ T)$ d'ordre à droite (et à gauche) Λ vérifiant $ST \subseteq \mathfrak{P}$, on a $S \subseteq \mathfrak{P}$ ou $T \subseteq \mathfrak{P}$.

Remarque 1.16. Soit $\mathfrak{P}$ est un idéal premier, alors $\overline{\mathfrak{P}} = \mathfrak{P}$.

Démonstration. Pour tout idéal premier $\mathfrak{P}$ d'ordre à droite et à gauche Λ, $\overline{\mathfrak{P}}$ est un idéal premier d'ordre à droite et à gauche Λ et vérifiant $\overline{\mathfrak{P}} \cap \mathbf{Z}_K = \mathfrak{P} \cap \mathbf{Z}_K$, donc, d'après la proposition 1.17, $\overline{\mathfrak{P}} = \mathfrak{P}$. □

Proposition 1.17. *Pour tout ordre maximal Λ et tout idéal premier $\mathfrak{p}$ de $\mathbf{Z}_K$, il existe un unique idéal premier $\mathfrak{P}$ d'ordre à droite et à gauche Λ et qui contient $\mathfrak{p}$. On dira que $\mathfrak{P}$ est au-dessus de $\mathfrak{p}$, ce qu'on notera $\mathfrak{P}|\mathfrak{p}\Lambda$. On a ainsi le dictionnaire suivant :*

$$\left\{\begin{array}{ccc} \{\text{idéaux premiers de } \mathbf{Z}_K\} & \longleftrightarrow & \{\text{idéaux premiers de } \Lambda\} \\ \mathfrak{p} & \longmapsto & \mathfrak{P} \mid \mathfrak{p}\Lambda \\ \mathfrak{P} \cap \mathbf{Z}_K & \longleftarrow & \mathfrak{P} \end{array}\right. .$$

Démonstration. Voir [Rei75, Theorem 22.4 p. 191]. □

Proposition 1.18. *Soit Λ un ordre maximal. Tout idéal bilatère $\mathfrak{I}$ d'ordre à droite (et à gauche) Λ se décompose en un produit*

$$\mathfrak{I} = \mathfrak{P}_1 \cdots \mathfrak{P}_l\,,$$

où les $\mathfrak{P}_i$ sont des idéaux premiers d'ordre à droite (et à gauche) Λ.

Démonstration. Voir [Rei75, Theorem 22.10 p. 193]. □

1.2.4 Idéaux maximaux

Étant donné un ordre maximal Λ, les idéaux premiers d'ordre à droite (et à gauche) Λ sont maximaux pour l'inclusion parmi les idéaux bilatères d'ordre à droite et à gauche Λ. Dans ce paragraphe, on ne se restreint plus aux idéaux bilatères.

Définition 1.19. Un idéal *maximal* $\mathfrak{M}$ est un idéal entier propre qui est maximal en tant qu'idéal à droite de son ordre à droite $\mathcal{O}_r(\mathfrak{M})$. En ce cas, il est aussi maximal dans son ordre à gauche $\mathcal{O}_l(\mathfrak{M})$.

Remarque 1.20. Vignéras ([Vig80]) parle d'idéaux *irréductibles*.

Proposition 1.21. *Pour tout idéal maximal $\mathfrak{M}$ d'ordre (maximal) à droite Λ, il existe un unique idéal premier $\mathfrak{P}$ tel que $\mathfrak{P} \subseteq \mathfrak{M}$: c'est l'annulateur de $\mathfrak{M}$ défini par $\mathfrak{P} = \{x \in \Lambda\,,\ \Lambda x \subseteq \mathfrak{M}\}$.*

On a de plus $\mathfrak{M} \cap \mathbf{Z}_K = \mathfrak{P} \cap \mathbf{Z}_K = \mathfrak{p}$ et $nrd_{F/K}(\mathfrak{M}) = \mathfrak{p}$.

Démonstration. voir Reiner ([Rei75, Theorem 22.14 p. 195 et Theorem 24.13 p. 215]). □

Définition 1.22. Soient $I_1, \ldots, I_l$ des idéaux de F. On dit que $I_1 \cdots I_l$ est un produit *cohérent* si pour tout $1 \leqslant i \leqslant l-1$, $\mathcal{O}_r(I_i) = \mathcal{O}_l(I_{i+1})$.

Remarque 1.23. Reiner ([Rei75]) parle de « *proper product* ».

Théorème 1.24. *Tout idéal I entier propre de F admet une décomposition en produit cohérent d'idéaux maximaux de la forme $I = \mathfrak{M}_1 \cdots \mathfrak{M}_l$, avec $\mathcal{O}_l(I) = \mathcal{O}_l(\mathfrak{M}_1)$ et $\mathcal{O}_r(I) = \mathcal{O}_r(\mathfrak{M}_l)$. On a alors*

$$nrd_{F/K}(I) = nrd_{F/K}(\mathfrak{M}_1) \cdots nrd_{F/K}(\mathfrak{M}_l).$$

Démonstration. L'existence d'une décomposition de I en produit cohérent est une propriété classique (cf. [Rei75, Theorem 22.18 p. 196]). La conséquence sur les normes réduites est aussi bien connue, mais faute de référence précise dès que $l > 2$, nous allons la démontrer par récurrence sur l.

Pour $l = 2$, c'est [Rei75, Theorem 24.11].

Soit $l > 2$, on considère le produit cohérent $I = \mathfrak{M}_1 \cdots \mathfrak{M}_l$ de l idéaux maximaux. Alors $\mathcal{O}_r(\mathfrak{M}_1 \cdots \mathfrak{M}_{l-1} \supseteq \mathcal{O}_r(\mathfrak{M}_{l-1})$ qui est un ordre maximal, donc $\mathcal{O}_r(\mathfrak{M}_1 \cdots \mathfrak{M}_{l-1} = \mathcal{O}_r(\mathfrak{M}_{l-1})$. Or I est un produit cohérent, donc $\mathcal{O}_l(\mathfrak{M}_l) = \mathcal{O}_r(\mathfrak{M}_1 \cdots \mathfrak{M}_{l-1})$. Ainsi, I est le produit cohérent des deux idéaux $\mathfrak{M}_1 \cdots \mathfrak{M}_{l-1}$ et $\mathfrak{M}_l$. Comme la propriété est vraie pour $l = 2$, cela implique que $\mathrm{nrd}_{F/K}(I) = \mathrm{nrd}_{F/K}(\mathfrak{M}_1 \cdots \mathfrak{M}_{l-1})\mathrm{nrd}_{F/K}(\mathfrak{M}_l)$ et par hypothèse de récurrence appliquée à $\mathfrak{M}_1 \cdots \mathfrak{M}_{l-1}$, on en déduit que

$$\mathrm{nrd}_{F/K}(I) = \mathrm{nrd}_{F/K}(\mathfrak{M}_1) \cdots \mathrm{nrd}_{F/K}(\mathfrak{M}_l).$$

□

1.3 Ramification

1.3.1 Définitions générales

Soient v une place de K et K_v la complétion de K en v.

Définition 1.25. On dit que v est *ramifiée* dans F si $F_v = F \otimes_K K_v$ est un corps gauche.

Signalons au passage qu'il existe un outil pour calculer la ramification.

Proposition 1.26. *Si $F = \left(\frac{a,b}{K}\right)$, alors v est ramifiée dans F si et seulement si le symbole de Hilbert $(a\,,b)_{K_v}$ vaut -1.*

On peut se rapporter à [Vig80] pour plus de détails.

Le théorème suivant résume les propriétés les plus importantes de la ramification dans les corps de quaternions.

Théorème 1.27. *Une place infinie ramifiée dans F est nécessairement réelle. De plus l'ensemble des places (finies et infinies) ramifiées dans F est fini, non vide et de cardinal pair. Il caractérise F à isomorphisme de K-algèbres près.*

Démonstration. Le fait que toute place infinie ramifiée est réelle est une conséquence du théorème de Frobenius (voir [Per97] par exemple). Pour la parité du nombre de places ramifiées, on peut se rapporter à [Vig80, Propriété II p. 75]. Pour les caractérisations par la ramification, voir [Rei75, paragraphe 32]. □

Définition 1.28. On dit que le corps de quaternions F est *défini* s'il admet une place infinie ramifiée, *totalement défini* si toutes les places infinies sont ramifiées, *indéfini* s'il admet une place infinie non ramifiée, *totalement indéfini* si aucune place infinie n'est ramifiée dans F.

Remarque 1.29. Si F est un corps de quaternions totalement défini sur K, alors K est nécessairement totalement réel et le nombre de places finies ramifiées a même parité que le degré de K.

Définition 1.30. On appelle *discriminant réduit* de F le produit des places finies ramifiées de F.

Ainsi, si F est totalement défini ou indéfini, le discriminant réduit de F caractérise totalement la ramification de F, donc F à isomorphisme de K-algèbres près.

1.3.2 Ramification et idéaux

Proposition 1.31. *Si $\mathfrak{p}$ est une place finie ramifiée dans F, alors l'idéal premier $\mathfrak{P}$ au-dessus de $\mathfrak{p}$ est maximal et $\mathfrak{p}\Lambda = \mathfrak{P}^2$.*

Démonstration. Voir [Rei75, Theorem 22.14 pp. 194–195]. □

Proposition 1.32. *Si $\mathfrak{p}$ est ramifié et Λ est un ordre maximal de F, alors l'idéal premier $\mathfrak{P}$ d'ordre à droite Λ et contenant $\mathfrak{p}$ est maximal. De plus c'est l'unique idéal maximal d'ordre à droite Λ contenant $\mathfrak{p}$.*

Démonstration. Comme $\mathfrak{p}$ est ramifié, $\mathfrak{p}\Lambda = \mathfrak{P}^2$. Par conséquent, $\mathrm{nrd}_{F/K}(\mathfrak{P}) = \mathfrak{p} = \mathrm{nrd}_{F/K}(\mathfrak{M})$ si on note $\mathfrak{M}$ un idéal maximal (d'ordre à droite Λ) contenant $\mathfrak{P}$. D'après la remarque 1.14, $\mathfrak{M} = \mathfrak{P}$ et $\mathfrak{P}$ est en fait maximal.

Par ailleurs, $\mathfrak{P}$ est l'unique idéal maximal d'ordre à droite Λ contenant $\mathfrak{p}$ car $\mathfrak{p}$ détermine un unique idéal premier $\mathfrak{P}$ d'ordre à droite Λ. Tout idéal maximal $\mathfrak{M}$ contenant $\mathfrak{p}$ contient donc $\mathfrak{P}$ et on vient de voir qu'on peut en déduire que $\mathfrak{M} = \mathfrak{P}$. □

1.4 Unités dans le cas totalement défini

On suppose que F est totalement défini de nombre de classes $\mathrm{h}_F = 1$. On considère un ordre maximal Λ de F.

Définition 1.33. On note $\Lambda^\times$ le groupe des unités de Λ et Λ^1 le groupe des unités de norme réduite 1 de Λ.

Lemme 1.34. *Le groupe Λ^1 est fini, l'indice $[\Lambda^\times : \Lambda^1\mathbf{Z}_K^\times]$ vaut 1, 2 ou 4.*

Démonstration. Voir [Vig80, pp. 139–140]. □

On en déduit facilement que l'indice $[\Lambda^\times : \mathbf{Z}_K^\times]$ est fini. On va maintenant donner une formule pour calculer cet indice.

Définition 1.35. On note ζ_K la fonction ζ de Dedekind K, elle est définie pour $\mathrm{Re}\,(s) > 1$ par

$$\zeta_K(s) = \sum_{\{0\}\neq I\subseteq\mathbf{Z}_K} \frac{1}{(\mathbf{N}I)^s}.$$

Théorème 1.36 (Ecke)**.** *La fonction ζ_K admet un prolongement analytique au plan complexe en une fonction méromorphe qui admet un unique pôle simple en $s = 1$.*

En fait, on va seulement s'intéresser aux valeurs de ζ_K en -1 et 2 pour décrire des propriétés de $\Lambda^\times$. Ces valeurs sont liées par la relation suivante.

Lemme 1.37. *Si K est totalement réel, alors*

$$\zeta_K(-1) = |\mathrm{disc}_K|^{\frac{3}{2}} (-2\pi^2)^{-[K:\mathbf{Q}]} \zeta_K(2).$$

Démonstration. Il s'agit simplement d'utiliser l'équation fonctionnelle de la fonction ζ_K (voir par exemple [Nar74, Theorem 7.1, p. 296]). □

Proposition 1.38 (formule de masse d'Eichler)**.** *Soient F un corps de quaternions totalement défini sur un corps de nombres K de discriminant réduit D et de nombre de classes $\mathrm{h}_F = 1$ et Λ un ordre maximal de F, alors*

$$\frac{1}{[\Lambda^\times : \mathbf{Z}_K^\times]} = 2^{1-[K:\mathbf{Q}]} |\zeta_K(-1)| \prod_{\mathfrak{p}|D} (\mathbf{N}\mathfrak{p} - 1).$$

Démonstration. La preuve originelle peut être lue dans un article d'Eichler [Eic37], mais une version plus générale est énoncée dans [Vig80, corollaire 2.3, p. 142]. □

1.5 Le cas du nombre de classes 1

Dans ce paragraphe, on suppose que $\mathrm{h}_F = 1$. On considère un ordre maximal Λ.

1.5.1 Éléments irréductibles et idéaux maximaux

Le fait que le nombre de classes soit égal à 1 permet de raisonner avec les éléments plutôt qu'avec les idéaux. Nous reprenons ici la terminologie et les résultats de Deuring ([Deu35]).

Définition 1.39. Soit $p \in \Lambda$. On dit que p est *irréductible* si $p = qr$, avec $q, r \in \Lambda$ implique que $q \in \Lambda^\times$ ou $r \in \Lambda^\times$.

Proposition 1.40. *Soit $p \in \Lambda$, alors p est irréductible si et seulement si Λp est un idéal maximal, si et seulement si $p\Lambda$ est un idéal maximal.*

Démonstration. Voir [Deu35, p. 92]. □

On peut alors reformuler la décomposition des idéaux entiers en produit d'idéaux maximaux avec ce vocabulaire.

Corollaire 1.41. *Tout élément a de Λ est produit d'éléments irréductibles p_i de Λ. Les p_i ne sont pas uniques, mais les idéaux premiers $\mathfrak{p}_i$ de $\mathbf{Z}_K$ en dessous des idéaux maximaux Λp_i sont uniques à l'ordre près.*

1.5.2 Idéaux normaux

Nous allons à présent décrire une autre propriété agréable du cas principal : pour vérifier qu'un idéal est normal, il suffit de considérer son ordre à droite ou son ordre à gauche.

Proposition 1.42. *Si $\mathrm{h}_F = 1$, alors un idéal I est normal si et seulement si $\mathcal{O}_l(I)$ ou $\mathcal{O}_r(I)$ est maximal,*

Démonstration. Notons $\Lambda = \mathcal{O}_l(I)$. Comme $\mathrm{h}_F = 1$, il existe $h \in F^\times$ tel que $I = \Lambda h$. Ainsi, $\mathcal{O}_r(I) = h^{-1}\Lambda h$ est conjugué à Λ. Donc $\mathcal{O}_r(I)$ est maximal si et seulement si $\Lambda = \mathcal{O}_l(I)$ l'est. □

Corollaire 1.43. *Soient F un corps de quaternions tel que $\mathrm{h}_F = 1$ et Λ un ordre maximal de F. Pour tout idéal entier I d'ordre à droite Λ et tout $b \in \Lambda$, $I + b\Lambda$ est un idéal entier d'ordre à droite Λ.*

Démonstration. L'ordre à droite de $I + b\Lambda$ contient Λ, qui est maximal, donc c'est Λ. Ainsi, d'après la proposition 1.42, $I + b\Lambda$ est normal ; comme $I + b\Lambda \subseteq \Lambda$, on en déduit qu'il est entier. □

Proposition 1.44. *Soient F un corps de quaternions tel que $\mathrm{h}_F = 1$, Λ un ordre maximal, $\mathfrak{M}$ un idéal maximal d'ordre à droite $\mathcal{O}_r(\mathfrak{M}) = \Lambda$ et d'ordre à gauche $\mathcal{O}_l(\mathfrak{M}) = \Lambda'$, $x \in \Lambda'$ et $y \in \Lambda$ tels que $xy \in \mathfrak{M}$. Alors $x \in \mathfrak{M}$ ou $y \in \mathfrak{M}$.*

Démonstration. Si $y \notin \mathfrak{M}$, alors $\mathfrak{M} + y\Lambda$ est un idéal entier d'ordre à droite Λ (d'après le corollaire 1.43) et contenant strictement $\mathfrak{M}$. Comme $\mathfrak{M}$ est maximal, cela implique $\mathfrak{M} + y\Lambda = \Lambda$. Par conséquent, il existe $m \in \mathfrak{M}$ et $\lambda \in \Lambda$ tels que

$$1 = m + y\lambda.$$

Ainsi, $x = xm + xy\lambda$. Or $xm \in \Lambda'\mathfrak{M} = \mathfrak{M}$ et $xy\lambda \in \mathfrak{M}\Lambda = \mathfrak{M}$. Cela montre que $x \in \mathfrak{M}$, comme désiré. □

Corollaire 1.45. *Soient F un corps de quaternions tel que $\mathrm{h}_F = 1$ et Λ un ordre maximal de F. Si $\mathfrak{p}$ est un premier ramifié et $x \in \Lambda$ vérifie $\mathrm{nrd}_{F/K}(x) \in \mathfrak{p}$, alors $x \in \mathfrak{P}$, où $\mathfrak{P}$ est l'unique idéal premier et maximal d'ordre à droite Λ qui contient $\mathfrak{p}$. Si de plus $\mathrm{nrd}_{F/K}(x)\mathbf{Z}_K = \mathfrak{p}$, alors $x\Lambda = \mathfrak{P}$.*

Démonstration. Par hypothèse, $x\overline{x} \in \mathfrak{P}$, qui est un idéal maximal d'après la proposition 1.32. Donc d'après la proposition 1.44, $x \in \mathfrak{P}$ ou $\overline{x} \in \mathfrak{P}$. Dans le second cas, $x \in \overline{\mathfrak{P}}$. Or $\mathfrak{P}$ est bilatère, donc d'après la remarque 1.16, $\overline{\mathfrak{P}} = \mathfrak{P}$. Par conséquent, $x \in \mathfrak{P}$ dans tous les cas.

Enfin, si $\mathrm{nrd}_{F/K}(x)\mathbf{Z}_K = \mathfrak{p}$, alors d'après ce qui précède $x\Lambda \subseteq \mathfrak{P}$. Donc, d'après la remarque 1.14, on a même l'égalité $x\Lambda = \mathfrak{P}$. □

1.5.3 Finitude

Proposition 1.46. *Étant donné un corps de nombres K, il ne peut exister qu'un nombre fini de corps de quaternions F totalement définis sur K de nombre de classes $\mathrm{h}_F = 1$.*

Démonstration. C'est une conséquence de la formule de masse d'Eichler. Soit en effet un tel corps de quaternions F, on note $\mathfrak{q}$ le premier (fini) ramifié de F de norme maximale. D'après la proposition 1.38,

$$\mathbf{N}\mathfrak{q} - 1 \leqslant \prod_{\mathfrak{p}|\mathrm{disc}_F} (\mathbf{N}\mathfrak{p} - 1) = \frac{2^{[K:\mathbf{Q}]-1}}{[\Lambda^\times : \mathbf{Z}_K^\times]|\zeta_K(-1)|} \leqslant \frac{2^{[K:\mathbf{Q}]-1}}{|\zeta_K(-1)|}.$$

Le corps K étant fixé, cela ne laisse qu'un nombre fini de possibilités pour $\mathbf{N}\mathfrak{q}$, donc pour $\mathfrak{q}$ et donc pour la ramification de F, qui caractérise F (d'après le théorème 1.27). □

2 Euclidianité des corps de quaternions

Soit F un corps de quaternions sur un corps K, soit Λ un ordre de F. On s'intéresse à l'euclidianité à droite ou à gauche de l'anneau Λ.

2.1 Pour un stathme quelconque

Définition 2.1. On dit que Λ est *euclidien à droite* (par rapport au *stathme à droite* $\varphi : \Lambda \longrightarrow \mathbf{N}$) si pour tous éléments a, b de Λ, avec $b \neq 0$, il existe $c \in \Lambda$ tel que

$$\varphi(a - bc) < \varphi(b). \tag{V.1}$$

En remplaçant bc par cb dans (V.1), on obtient la définition de l'*euclidianité à gauche* (et d'un *stathme à gauche*). Le fait que l'on considère des stathmes à valeurs dans $\mathbf{N}$ et pas dans un ensemble bien ordonné quelconque n'est pas une restriction d'après le corollaire 2.6 du chapitre III (p. 70). En effet, pour tout $b \in \Lambda \setminus \{0\}$, $\Lambda/b\Lambda$ est fini, de cardinal $\left|\mathbf{N}_{K/\mathbf{Q}}\left(\mathrm{nrd}_{F/K}(b)\right)\right|^2$.

Proposition 2.2. *Soit Λ un ordre, alors Λ est euclidien à droite si et seulement s'il est euclidien à gauche.*

Démonstration. Soit $\varphi : \Lambda \longrightarrow \mathbf{N}$ un stathme à droite. D'après la remarque 1.8, $\overline{\Lambda} = \Lambda$, on peut donc définir $\psi : \begin{cases} \Lambda & \longrightarrow & \mathbf{N} \\ x & \longmapsto & \varphi(\overline{x}) \end{cases}$. Alors pour tous $a, b \in \Lambda$, avec $b \neq 0$, il existe $c \in \Lambda$ tel que $\varphi(\overline{a} - \overline{b}c) < \varphi(\overline{b})$. Or $\varphi(\overline{a} - \overline{b}c) = \varphi(\overline{a - \overline{c}b}) = \psi(a - \overline{c}b)$ et $\varphi(\overline{b}) = \psi(b)$. Cela montre que ψ est un stathme à gauche, donc que Λ est euclidien à gauche. □

On peut donc à présent parler d'*ordre euclidien* sans préciser à droite ou à gauche.

Proposition 2.3. *Si Λ est un ordre euclidien, alors Λ est un ordre maximal.*

Démonstration. S'il est euclidien, alors il est euclidien à droite et on peut considérer un stathme à droite $\varphi : \Lambda \longrightarrow \mathbf{N}$. On considère un ordre Λ' qui contient Λ. Alors Λ et Λ' sont des $\mathbf{Z}$-modules de type fini, donc d'après le théorème de la base adaptée, il existe $d \in \mathbf{Z} \setminus \{0\}$ tel que $d\Lambda' \subseteq \Lambda$. On choisit $b \in \Lambda \setminus \{0\}$ tel que

$$\varphi(b) = \min\left\{\varphi(d),\ d \in \Lambda \setminus \{0\},\ d\Lambda' \subseteq \Lambda\right\}.$$

Soit alors $a \in \Lambda'$, comme $ba \in \Lambda$, $b \in \Lambda \setminus \{0\}$, on peut faire la division euclidienne (à droite) de ba par b : il existe $c \in \Lambda$ tel que

$$\varphi(ba - bc) < \varphi(b).$$

Or $ba - bc \in \Lambda$ et $(ba - bc)\Lambda' = b(a - c)\Lambda' \subseteq b\Lambda' \subseteq \Lambda$. Donc par définition de b, $ba - bc = 0$, d'où $a = c$. Cela montre que $a = c \in \Lambda$. Ainsi, $\Lambda' = \Lambda$. □

Proposition 2.4. *Si Λ est un ordre euclidien, alors le nombre de classes h_F de F est 1.*

Démonstration. La preuve est la même que dans le cas commutatif. Notons $\varphi : \Lambda \longrightarrow \mathbf{N}$ un stathme euclidien à droite. Il suffit alors de prouver que tout idéal I d'ordre à

droite Λ est principal. Quitte à remplacer I par yI pour un certain $y \in F \setminus \{0\}$, on peut supposer que $I \subseteq \Lambda$. Soit alors $b \in I \setminus \{0\}$ tel que

$$\varphi(b) = \min\{\varphi(x),\ x \in I\}.$$

Soit alors $a \in I$, on fait la division euclidienne de a par b via φ : il existe $q \in \Lambda$ tel que

$$\varphi(a - bq) < \varphi(b).$$

Or $b\Lambda \subseteq I$, donc $a - bq \in I$. Par définition de b, cela implique que $a = bq$. Ainsi, $I = b\Lambda$. □

Proposition 2.5. *Si Λ est un ordre maximal euclidien, alors tout ordre maximal est euclidien.*

Démonstration. Comme F a nombre de classes $\mathrm{h}_F = 1$ (d'après la proposition 2.4), son nombre de types est aussi $t_F = 1$. Soit Λ' un ordre maximal. Alors Λ' et Λ sont conjugués, c'est-à-dire qu'il existe $x \in F \setminus \{0\}$ tel que $\Lambda' = x^{-1}\Lambda x$. Cela permet de définir l'application

$$\varphi' : \left\{ \begin{array}{ccc} \Lambda' & \longrightarrow & \mathbf{N} \\ u & \longmapsto & \varphi(uxu^{-1}) \end{array} \right. .$$

Soient alors $a', b' \in \Lambda$, $b' \neq 0$. On peut faire la division euclidienne de $ua'u^{-1}$ par $ub'u^{-1}$ via φ : il existe $q \in \Lambda$ tel que

$$\varphi(ua'u^{-1} - ub'u^{-1}q) < \varphi(ub'u^{-1}). \tag{V.2}$$

Or $ua'u^{-1} - ub'u^{-1}q = u(a' - b'u^{-1}qu)u^{-1}$, de sorte que (V.2) se récrit

$$\varphi'(a' - b'q') < \varphi'(b'),$$

en notant $q' = u^{-1}qu \in \Lambda'$. Cela montre que φ' est un stathme euclidien à droite pour Λ'. □

Cela permet de donner la définition suivante.

Définition 2.6. Soit F un corps de quaternions. On dit que F est *euclidien* s'il admet un ordre euclidien.

Ainsi, F est euclidien si et seulement s'il admet un ordre maximal euclidien, ce qui équivaut au fait que tout ordre maximal est euclidien. Par conséquent, pour prouver la propriété d'euclidianité ou de non euclidianité de F, il suffit de considérer un ordre maximal Λ de F et de prouver que Λ est euclidien ou non.

2.2 Pour la norme

Définition 2.7. On dit que Λ est *euclidien pour la norme à droite* si l'application $N = \left|\mathbf{N}_{K/\mathbf{Q}} \circ \mathrm{nrd}_{F/K}\right|$ est un stathme euclidien à droite.

Rappelons qu'un ordre qui est euclidien pour la norme est nécessairement maximal d'après la proposition 2.3. Par ailleurs, comme pour l'euclidianité en général, il n'y a pas vraiment lieu de parler d'euclidianité à droite ou à gauche pour la norme. En effet, un ordre est euclidien à droite pour la norme si et seulement s'il est euclidien à gauche pour la norme. Pour s'en convaincre, on pourra relire la preuve de la proposition 2.2 en remarquant que $\psi = \varphi = N$ comme la norme est inchangée par conjugaison.

Exemple 2.8. Dans $\left(\frac{-1,-1}{\mathbf{Q}}\right)$, l'ordre maximal $\Lambda = \mathbf{Z} + \mathbf{Z}i + \mathbf{Z}j + \mathbf{Z}\frac{1+i+j+k}{2}$ est euclidien pour la norme.

Comme dans le cas général, on a la propriété suivante.

Proposition 2.9. *Si Λ est un ordre maximal euclidien pour la norme, alors tout ordre maximal est euclidien pour la norme.*

Démonstration. Rappelons que comme Λ est euclidien, son nombre de types est $t_F = 1$. Pour tout $x \in F \setminus \{0\}$, la norme réduite $\mathrm{nrd}_{F/K}$ est invariante par la conjugaison $\begin{cases} F & \longrightarrow & F \\ a & \longmapsto & x^{-1}ax \end{cases}$. Par conséquent, dans la preuve de la proposition 2.5, en notant $\varphi = \left|\mathbf{N}_{K/\mathbf{Q}} \circ \mathrm{nrd}_{F/K}\right|$, on a $\varphi' = \left|\mathbf{N}_{K/\mathbf{Q}} \circ \mathrm{nrd}_{F/K}\right|$, de sorte que tout ordre maximal est euclidien pour la norme. □

En conséquence, on définit l'euclidianité pour la norme d'un corps de quaternions comme suit.

Définition 2.10. Soit F un corps de quaternions. On dit que F est *euclidien pour la norme* s'il admet un ordre euclidien pour la norme. S'il existe, un tel ordre est nécessairement maximal.

Pour vérifier que F est euclidien (ou non) pour la norme, il suffit donc de considérer un ordre maximal quelconque Λ et de voir si Λ est euclidien à droite (ou à gauche, si c'est plus pratique).

2.3 Minimum euclidien

Il s'agit encore d'étudier l'euclidianité des corps de quaternions *pour la norme*. Il est naturel d'étendre la définition du minimum euclidien aux corps des quaternions.

Définition 2.11. Soient Λ un ordre de F et $\xi \in F$, on appelle minimum euclidien de ξ par rapport à Λ le nombre réel

$$m_\Lambda(\xi) := \inf_{\gamma \in \Lambda} \left|\mathbf{N}_{K/\mathbf{Q}} \circ \mathrm{nrd}_{F/K}(\xi - \gamma)\right|.$$

Proposition 2.12. *1. Pour tous $u, v \in \Lambda^\times$, $\xi \in F$ et $\gamma \in \Lambda$, on a $m_\Lambda(u\xi v - \gamma) = m_\Lambda(\xi)$.*

2. Pour tout $\xi \in F$, il existe $\gamma \in \Lambda$ tel que $m_\Lambda(\xi) = \left|\mathbf{N}_{K/\mathbf{Q}} \circ nrd_{F/K}(\xi - \gamma)\right|$. En particulier, $m_\Lambda(\xi) \in \mathbf{Q}$ et $m_\Lambda(\xi) = 0$ si et seulement si $\xi \in \Lambda$.

Démonstration. C'est immédiat. Remarquons que même si on sait qu'il existe un $\gamma \in \Lambda$ tel que $m_\Lambda(\xi) = \left|\mathbf{N}_{K/\mathbf{Q}} \circ \mathrm{nrd}_{F/K}(\xi - \gamma)\right|$, cela ne suffit pas pour calculer $m_\Lambda(\xi)$. □

Proposition 2.13. *L'ordre Λ est euclidien pour la norme si et seulement si pour tout $\xi \in F$, $m_\Lambda(\xi) < 1$.*

Démonstration. C'est une conséquence facile de la multiplicativité de $\mathbf{N}_{K/\mathbf{Q}}$ et de la norme réduite $\mathrm{nrd}_{F/K}$. Notons que cette propriété permet aussi de montrer que les notions d'euclidianité à droite et à gauche pour la norme coïncident. □

Par ailleurs, on peut plonger F dans $\mathbf{R}^{4[K:\mathbf{Q}]}$, définir un minimum inhomogène $\overline{M}(\Lambda)$ et appliquer la technique du paragraphe 3.3 du chapitre IV (page 88) pour prouver le résultat suivant.

Théorème 2.14. *Soit F un corps de quaternions sur un corps K. Si le rang des unités de K est strictement supérieur à 1, alors il existe $\xi \in F$ tel que*

$$\overline{M}(\Lambda) = m_\Lambda(\xi).$$

En particulier $\overline{M}(\Lambda)$ est rationnel et Λ est euclidien pour la norme si et seulement si $\overline{M}(\Lambda) < 1$.

Pour prouver cette propriété, il suffit d'utiliser les unités de $\mathbf{Z}_K$. En se servant des unités de Λ, on peut montrer que le théorème 2.14 reste vrai en supposant que K est un corps quadratique réel et que F est totalement indéfini sur K (voir [BCC09] ou [Cha06, Corollaire 2.3.6]).

Définition 2.15. On appelle minimum euclidien de l'ordre Λ le nombre réel

$$M(\Lambda) := \sup_{\xi \in F} m_\Lambda(\xi).$$

En effet, $M(\Lambda)$ est fini car $M(\Lambda) \leqslant \overline{M}(\Lambda)$. Le théorème 2.14 assure même qu'on a l'égalité $M(\Lambda) = \overline{M}(\Lambda)$ si le rang des unités de K est strictement supérieur à 1.

Proposition 2.16. *Si le nombre de types de F est $t_F = 1$ (ce qui est vrai en particulier si F est euclidien), alors pour tous ordres maximaux Λ et Λ', on a $M(\Lambda) = M(\Lambda')$.*

Démonstration. Soient Λ et Λ' deux ordres maximaux. Comme le nombre de types est égal à 1, Λ et Λ' sont conjugués, c'est-à-dire qu'il existe $x \in F \setminus \{0\}$ tel que $\Lambda' = x^{-1}\Lambda x$. Alors pour tout $\xi \in F$, on a clairement

$$\begin{aligned} m_{\Lambda'}(\xi) &= \inf_{\lambda' \in \Lambda'} \left|\mathbf{N}_{K/\mathbf{Q}} \circ \mathrm{nrd}_{F/K}(\xi - \lambda')\right| \\ &= \inf_{\lambda \in \Lambda} \left|\mathbf{N}_{K/\mathbf{Q}} \circ \mathrm{nrd}_{F/K}(\xi - x^{-1}\lambda x)\right| \\ &= m_\Lambda(x\xi x^{-1}). \end{aligned}$$

Le fait que $\left\{ \begin{array}{ccc} F & \longrightarrow & F \\ \xi & \longmapsto & x\xi x^{-1} \end{array} \right.$ est une bijection permet de conclure. □

Remarques.

– En particulier, si Λ est euclidien pour la norme, alors pour tout ordre maximal $M(\Lambda') = M(\Lambda)$. Ainsi, si $M(\Lambda) > 1$, alors aucun ordre maximal n'est euclidien pour la norme.

– Cela permet aussi de définir le minimum euclidien $M(F)$ d'un corps de quaternions de nombre de types 1 comme le minimum euclidien de n'importe quel ordre maximal.

– La condition sur le nombre de types est nécessaire. En effet, pour $F = \left(\frac{-1,-11}{\mathbf{Q}}\right)$, on peut considérer les deux ordres maximaux suivants :

$$\left\{ \begin{array}{rcl} \Lambda & = & \mathbf{Z} \oplus i\mathbf{Z} \oplus \frac{i+j}{2}\mathbf{Z} \oplus \frac{1+k}{2}\mathbf{Z} \\ \Lambda' & = & \mathbf{Z} \oplus \frac{1+2i+j}{2}\mathbf{Z} \oplus 2i\mathbf{Z} \oplus \frac{2-i-k}{4}\mathbf{Z} \end{array} \right. ,$$

qui vérifient $M(\Lambda) = \frac{18}{11}$ et $M(\Lambda') = \frac{16}{11}$ (voir [Cha06]).

3 Euclidianité des corps de quaternions totalement définis sur un corps de nombres

On suppose à présent que F est un corps de quaternions totalement défini sur un corps de nombres K. D'après la remarque 1.29, cela implique que K est totalement réel.

3.1 Finitude

Proposition 3.1. *Il n'existe qu'un nombre fini de corps de quaternions totalement définis sur un corps de nombres qui sont principaux. En particulier, il n'existe qu'un nombre fini de corps de quaternions totalement définis sur un corps de nombres qui sont euclidiens.*

Démonstration. D'après la proposition 2.4, le nombre de classes de F est $\mathrm{h}_F = 1$. Le lemme 1.37 permet de « récrire »[1] la formule de masse d'Eichler (proposition 1.38) dans le cas $\mathrm{h}_F = 1$ sous la forme

$$\frac{2|\zeta_K(2)| \cdot |\mathrm{disc}_K|^{\frac{3}{2}}}{(2\pi)^{2[K:\mathbf{Q}]}} = \left([\Lambda^\times : \mathbf{Z}_K^\times] \prod_{\mathfrak{p}|\mathrm{disc}_F} (\mathbf{N}\mathfrak{p} - 1) \right)^{-1}. \tag{V.3}$$

Le membre de droite de (V.3) est inférieur à 1 et $\zeta_K(2) > 1$, donc $|\mathrm{disc}_K|^{\frac{3}{2}} < \frac{(2\pi)^{2[K:\mathbf{Q}]}}{2}$, on en déduit que

$$|\mathrm{disc}_K|^{\frac{1}{[K:\mathbf{Q}]}} < (\pi\sqrt{2})^{\frac{4}{3}} < 7{,}31.$$

D'après [Voi08], cette borne implique que le nombre de K possibles est fini. Plus précisément, d'après [Voi08, Table 3], cela montre que $[K : \mathbf{Q}] \leqslant 5$.

Or, d'après la proposition 1.46, à K fixé, il n'y a qu'un nombre fini de corps de quaternions principaux sur K, cela achève la preuve. □

Remarque 3.2. Ce raisonnement est un cas particulier de l'étude des ordres d'Eichler faite par Kirschmer et Voight, voir [KV10]. Dans la paragraphe suivant, nous allons donner leur résultat plus précis sans démonstration qui donne exactement les corps de quaternions totalement définis sur un corps de nombres de nombres de classes $\mathrm{h}_F = 1$.

3.2 Une liste plus précise de candidats

Théorème 3.3 (Kirschmer & Voight, [KV10])**.** *Soit F un corps de quaternions totalement défini sur un corps de nombres K de nombre de classes $\mathrm{h}_F = 1$, alors F est un des éléments de la table V.1.*

Pour être plus compact et comme les informations détaillées ne vont pas être utiles, nous notons parfois seulement $\mathbf{N}_{K/\mathbf{Q}}\mathrm{disc}_F$ et pas disc_F. Même si dans la plupart des cas, pour une de ces normes D donnée, tous les entiers d tels que $\mathbf{N}_{K/\mathbf{Q}}(d) = D$ sont des valeurs possibles de disc_F tels que $\mathrm{h}_F = 1$, il existe des exceptions détaillées dans les tables en ligne associées à l'article [KV10].

1. cette forme avec $\zeta_K(2)$ correspond en fait davantage à l'écriture d'Eichler dans [Eic37]

degré 2	
K	disc_F
$\mathbf{Q}(\sqrt{2})$	$\mathbf{Z}_K$
	$\mathfrak{p}_2\mathfrak{p}_3 = (\sqrt{2})(3)$
	$\mathfrak{p}_2\mathfrak{p}_5 = (\sqrt{2})(5)$
	$\mathfrak{p}_2\mathfrak{p}_7 = (\sqrt{2})(1+2\sqrt{2})$
	$\mathfrak{p}_2\overline{\mathfrak{p}_7} = (\sqrt{2})(1-2\sqrt{2})$
$\mathbf{Q}(\sqrt{5})$	$\mathbf{Z}_K$
	$\mathfrak{p}_2\mathfrak{p}_5 = (2)(\sqrt{5})$
	$\mathfrak{p}_2\mathfrak{p}_{11} = (2)(\frac{7+\sqrt{5}}{2})$
	$\mathfrak{p}_2\overline{\mathfrak{p}_{11}} = (2)(\frac{7-\sqrt{5}}{2})$
$\mathbf{Q}(\sqrt{13})$	$\mathbf{Z}_K$
	$\mathfrak{p}_2\mathfrak{p}_3 = (2)(\frac{1+\sqrt{13}}{2})$
	$\mathfrak{p}_2\overline{\mathfrak{p}_3} = (2)(\frac{1-\sqrt{13}}{2})$
$\mathbf{Q}(\sqrt{17})$	$\mathbf{Z}_K$

degré 3	
disc_K	$\mathbf{N}_{K/\mathbf{Q}}(\mathrm{disc}_F)$
49	7
	8
	13
	29
	43
81	3
	19
	37
148	2
	5
169	5
	13
316	2
321	3

degré 1	
	disc_F
	$2\mathbf{Z}$
	$3\mathbf{Z}$
	$5\mathbf{Z}$
	$7\mathbf{Z}$
	$13\mathbf{Z}$

degré 4	
disc_K	disc_F
725	$\mathbf{Z}_K$
1957	$\mathbf{Z}_K$
2777	$\mathbf{Z}_K$

degré 5	
disc_K	disc_F
24217	$\mathfrak{p}_5$

TABLE V.1 – Tous les corps de quaternions totalement définis sur un corps de nombres de nombre de classes $\mathrm{h}_F = 1$ sont dans ces tables, on note $\mathfrak{p}_i$ pour un idéal premier de norme i, avec des précisions éventuelles s'il y a ambiguïté.

3.3 Techniques et critères généraux

Pour $b \in \Lambda$, on note $\varphi_b : \Lambda \longrightarrow\!\!\!\!\!\rightarrow \Lambda/b\Lambda$ la surjection canonique.

Lemme 3.4. *Soit $b \in \Lambda \setminus \{0\}$. La fonction φ_b a les propriétés suivantes.*

1. *Si $\lambda \in \Lambda$, alors $\left|\varphi_b(\lambda\mathbf{Z}_K^\times)\right| \leqslant \left|\varphi_b(\mathbf{Z}_K^\times)\right|$.*
2. *Pour tout sous-ensemble T de Λ, si $a, c \in \Lambda$ vérifient $a - c \in b\Lambda$, alors $\varphi_b(aT) = \varphi_b(cT)$.*

Démonstration. 1. Notons $r = \left|\varphi_b(\mathbf{Z}_K^\times)\right|$ et $\{u_i,\ 1 \leqslant i \leqslant r\}$ un système de représentants de $\mathbf{Z}_K^\times$ modulo $b\Lambda$: pour tout $x \in \mathbf{Z}_K^\times$, il existe un unique $i \in \{1, \ldots, r\}$ tel que $x - u_i \in b\Lambda$. On va prouver que pour tout $y \in \lambda\mathbf{Z}_K^\times$, il existe un indice $i \in \{1, \ldots, r\}$ tel que $y - \lambda u_i \in b\Lambda$, ce qui va montrer que $\{\lambda u_i,\ 1 \leqslant i \leqslant r\}$ contient un système de représentants de $\lambda\mathbf{Z}_K^\times$ modulo $b\Lambda$ et donc l'inégalité désirée. Soit $y = \lambda u$, avec $u \in \mathbf{Z}_K^\times$. Il existe un indice $i \in \{1, \ldots, r\}$ tel que $u - u_i \in b\Lambda$ et cela implique

$$u\lambda - u_i\lambda = (u - u_i)\lambda \in b\Lambda \tag{V.4}$$

Mais u et u_i sont des éléments de $\mathbf{Z}_K^\times$, donc ils commutent avec tout élément de Λ, de sorte que (V.4) implique $y - \lambda u_i \in b\Lambda$.

2. Un élément de $\varphi(aT)$ est une classe $ax + b\Lambda$, avec $x \in T$. Comme $(a - c)x \in b\Lambda$, on a $ax + b\Lambda = cx + b\Lambda \in \varphi(cT)$. Par conséquent $\varphi_b(aT) \subseteq \varphi_b(cT)$. Par symétrie, on en déduit l'égalité.

□

Soit $b \in \Lambda$ tel que $b \notin \Lambda^\times \cup \{0\}$. L'idéal entier propre $b\Lambda$ admet une décomposition en un produit cohérent

$$b\Lambda = \mathfrak{M}_1 \cdots \mathfrak{M}_l,$$

où les $\mathfrak{M}_i$ sont des idéaux entiers maximaux d'après le théorème 1.24. Alors $\mathfrak{M}_i \cap \mathbf{Z}_K$ est un idéal premier $\mathfrak{p}_i$ de $\mathbf{Z}_K$. On note p_i le premier en dessous de $\mathfrak{p}_i$ et f_i le degré résiduel de $\mathfrak{p}_i$ (de sorte que $\mathbf{N}\mathfrak{p}_i = p_i^{f_i}$).

Proposition 3.5. *Avec ces notations, soient $s \geqslant 1$ et $v_1, \ldots, v_s$ des éléments de Λ tels que pour tout i, $v_i \notin b\Lambda$. Si*

$$\varphi_b\left(\{0\} \cup \bigcup_{i=1}^{s} v_i\Lambda^\times\right) = \Lambda/b\Lambda,$$

alors

$$\prod_{i=1}^{l} p_i^{f_i} + 1 \leqslant s[\Lambda^\times : \mathbf{Z}_K^\times]. \tag{V.5}$$

Démonstration. Posons $m = [\Lambda^\times : \mathbf{Z}_K^\times]$ et soit $\{t_j,\ 1 \leqslant j \leqslant m\}$ un système de représentants de $\Lambda^\times$ modulo $\mathbf{Z}_K^\times$, de sorte que $\Lambda^\times = \cup_{j=1}^m t_j\mathbf{Z}_K^\times$. Pour tout $i \in \{1, \ldots, s\}$, on a

$$\left|\varphi_b(v_i\Lambda^\times)\right| = \left|\bigcup_{j=1}^{m} \varphi_b(v_i t_j \mathbf{Z}_K^\times)\right|.$$

D'après le lemme 3.4 (1), on en déduit

$$\left|\varphi_b(v_i\Lambda^\times)\right| \leqslant m\left|\varphi_b(\mathbf{Z}_K^\times)\right|. \tag{V.6}$$

Posons maintenant $r = \left|\varphi_b(\mathbf{Z}_K^\times)\right|$ et, comme précédemment, soit $\{u_i \in \mathbf{Z}_K^\times,\ 1 \leqslant i \leqslant r\}$ un système de représentants de $\mathbf{Z}_K^\times$ modulo $b\Lambda$. Les ensembles $u_i + \mathfrak{p}_1 \cdots \mathfrak{p}_l$ sont disjoints : sinon, il existerait $i \neq j$ tels que

$$u_i - u_j \in \mathfrak{p}_1 \cdots \mathfrak{p}_l \subseteq \mathfrak{M}_1 \cdots \mathfrak{M}_l = b\Lambda,$$

ce qui est impossible par construction des u_i. De plus pour tout i, $u_i \notin \mathfrak{p}_1 \cdots \mathfrak{p}_l$ car $u_i \in \mathbf{Z}_K^\times$. Ainsi, les $u_i + \mathfrak{p}_1 \cdots \mathfrak{p}_l$ peuvent être considérés comme des éléments distincts de $\mathbf{Z}_K/\mathfrak{p}_1 \cdots \mathfrak{p}_l$. Comme ils sont différents de $\mathfrak{p}_1 \cdots \mathfrak{p}_l$, on obtient

$$r \leqslant [\mathbf{Z}_K : \mathfrak{p}_1 \cdots \mathfrak{p}_l] - 1 = \prod_{j=1}^{l} p_j^{f_j} - 1. \tag{V.7}$$

On déduit des équations (V.6) et (V.7) que pour tout $i \in \{1, \ldots, s\}$,

$$\left|\varphi_b(v_i\Lambda^\times)\right| \leqslant m\left(\prod_{j=1}^{l} p_j^{f_j} - 1\right).$$

Par conséquent,

$$\left|\varphi_b\left(\bigcup_{i=1}^{s} v_i\Lambda^\times\right)\right| \leqslant sm\left(\prod_{j=1}^{l} p_j^{f_j} - 1\right). \tag{V.8}$$

Mais pour tout idéal entier I d'ordre à droite Λ, $|\Lambda/I| = \mathbf{N}_{K/\mathbf{Q}}(\mathrm{nrd}_{F/K}(I))^2$, en particulier

$$|\Lambda/b\Lambda| = \mathbf{N}_{K/\mathbf{Q}}(\mathrm{nrd}_{F/K}(\mathfrak{M}_1 \cdots \mathfrak{M}_l))^2.$$

Or, d'après le théorème 1.24,

$$\mathrm{nrd}_{F/K}(\mathfrak{M}_1 \cdots \mathfrak{M}_l) = \mathrm{nrd}_{F/K}(\mathfrak{M}_1) \cdots \mathrm{nrd}_{F/K}(\mathfrak{M}_l),$$

et donc

$$|\Lambda/b\Lambda| = \mathbf{N}_{K/\mathbf{Q}}(\mathrm{nrd}_{F/K}(\mathfrak{M}_1))^2 \cdots \mathbf{N}_{K/\mathbf{Q}}(\mathrm{nrd}_{F/K}(\mathfrak{M}_l))^2.$$

Comme $\mathrm{nrd}_{F/K}(\mathfrak{M}_i) = \mathfrak{p}_i$ et $\mathbf{N}\mathfrak{p}_i = p_i^{f_i}$, on obtient au final

$$|\Lambda/b\Lambda| = \prod_{i=1}^{l} p_i^{2f_i}. \tag{V.9}$$

Or, par hypothèse, $\varphi_b\left(\{0\} \cup \bigcup_{i=1}^{s} v_i\Lambda^\times\right) = \Lambda/b\Lambda$, ce qui implique

$$\left|\varphi_b\left(\bigcup_{i=1}^{s} v_i\Lambda^\times\right)\right| = |\Lambda/b\Lambda| - 1\,,$$

car pour tout i, $v_i \notin b\Lambda$ et donc $\bigcup_{i=1}^{s} v_i\Lambda^\times \cap b\Lambda = \varnothing$. Ainsi, (V.9) implique

$$\left|\varphi_b\left(\bigcup_{i=1}^{s} v_i\Lambda^\times\right)\right| = \prod_{i=1}^{l} p_i^{2f_i} - 1. \tag{V.10}$$

Enfin, (V.8) et (V.10) donnent

$$\prod_{i=1}^{l} p_i^{2f_i} - 1 \leqslant sm\left(\prod_{j=1}^{l} p_j^{f_j} - 1\right),$$

qui conduit au résultat. □

3.4 Sur le corps des rationnels

Théorème 3.6. *Soit F un corps de quaternions (totalement) défini sur $\mathbf{Q}$. Alors F est euclidien si et seulement si*

$$F \in \left\{\left(\frac{-1,-1}{\mathbf{Q}}\right), \left(\frac{-1,-3}{\mathbf{Q}}\right), \left(\frac{-2,-5}{\mathbf{Q}}\right)\right\}.$$

Dans tous ces cas, il est en fait euclidien pour la norme.

Démonstration. Soit F un corps de quaternions (totalement) défini sur $\mathbf{Q}$. S'il est euclidien, d'après la proposition 2.4, $\mathrm{h}_F = 1$. Ainsi, F appartient à la liste donnée dans l'énoncé ou $F \in \{F_1, F_2\}$ où $F_1 = \left(\frac{-1,-7}{\mathbf{Q}}\right)$ et $F_2 = \left(\frac{-2,-13}{\mathbf{Q}}\right)$. Il s'agit donc dans un premier temps de prouver que F_1 et F_2 ne sont pas euclidiens.

1. Soit Λ un ordre maximal de $F = F_1$ ou F_2. On va montrer que Λ n'est pas euclidien à droite en utilisant la construction de Motzkin : on a $\Lambda_0 = \{0\}$, $\Lambda_1 = \{0\} \cup \Lambda^\times$, on va prouver que $\Lambda_2 = \Lambda_1$. Comme Λ n'est pas un corps gauche, cela prouvera qu'il n'est pas euclidien à droite d'après le corollaire 2.8 du chapitre III (p. 70). Par l'absurde, supposons donc que Λ est euclidien. Soit $b \in \Lambda_2 \setminus \Lambda_1$. On

applique alors la proposition 3.5 avec $s = 1$ et $v_1 = 1$: avec les notations de la proposition,

$$\prod_{i=1}^{l} p_i + 1 \leqslant [\Lambda^\times : \mathbf{Z}_K^\times]. \tag{V.11}$$

Pour F_1 et F_2, la formule de masse d'Eichler (proposition 1.38) permet de calculer $[\Lambda^\times : \mathbf{Z}_K^\times] = 2$ et 1 respectivement. Par conséquent, (V.11) est impossible et $\Lambda_2 = \Lambda_1$.

2. Il reste à prouver que les corps de quaternions donnés par l'énoncé sont euclidiens pour la norme. C'est une propriété très classique. On peut par exemple l'obtenir en exhibant des ordres maximaux et en calculant leur minimum euclidien (on peut se reporter à [Cha06] pour voir le détail des calculs de $M(\Lambda)$.
   – Si $F = \left(\frac{-1,-1}{\mathbf{Q}}\right)$, alors un ordre maximal est $\Lambda = \mathbf{Z} + \mathbf{Z}i + \mathbf{Z}j + \mathbf{Z}\frac{1+i+j+k}{2}$ et on a $M(F) = M(\Lambda) = \frac{1}{2}$.
   – Si $F = \left(\frac{-1,-3}{\mathbf{Q}}\right)$, alors un ordre maximal est $\Lambda = \mathbf{Z} + \mathbf{Z}i + \mathbf{Z}\frac{1+j}{2} + \mathbf{Z}\frac{i+k}{2}$ et on a $M(F) = M(\Lambda) = \frac{2}{3}$.
   – Si $F = \left(\frac{-2,-5}{\mathbf{Q}}\right)$, alors un ordre maximal est $\Lambda = \mathbf{Z} + \mathbf{Z}\frac{-1+i+j}{2} + \mathbf{Z}\frac{2-i+k}{4} + \mathbf{Z}\frac{2+3i+k}{4}$ et on a $M(F) = M(\Lambda) = \frac{4}{5}$.

□

3.5 Le cas quadratique

Théorème 3.7. *Soit F un corps de quaternions totalement défini sur un corps quadratique (réel) K. Alors F est euclidien si et seulement si*

$$F \in \left\{\left(\frac{-1,-1}{\mathbf{Q}(\sqrt{2})}\right), \left(\frac{-1,-1}{\mathbf{Q}(\sqrt{5})}\right), \left(\frac{-1,-1}{\mathbf{Q}(\sqrt{13})}\right), \left(\frac{-1,-3}{\mathbf{Q}(\sqrt{17})}\right)\right\}.$$

De plus tous ces corps de quaternions sont euclidiens pour la norme.

Remarque 3.8. Comme dans le cas totalement défini sur les rationnels, la situation est analogue à celle des corps de nombres quadratiques imaginaires : les seuls cas euclidiens sont en fait euclidiens pour la norme et on a des exemples de corps de quaternions de nombre de classes 1 qui ne sont pas euclidiens (voir proposition 3.15).

La démarche de la preuve est la même que celle du théorème 3.6 : on utilise le fait que le nombre de classes est 1 pour se ramener à une liste finie, puis on prouve que les exemples donnés sont euclidiens pour la norme, enfin, pour les autres, on applique la construction de Motzkin. Néanmoins, dans ces cas, cette étape peut s'avérer plus technique : il sera parfois nécessaire d'aller « une étape plus loin » et de considérer Λ_3.

Proposition 3.9. *Les corps de quaternions F totalement définis sur un corps quadratique (réel) de nombre de classes* 1 *sont donnés par la table V.2.*

Démonstration. Voir [Vig80] ou [KV10]. □

Dans la suite, on va prouver que F_1, F_6, F_{10} et F_{13} sont euclidiens pour la norme, puis on va montrer que les autres ne sont pas euclidiens.

F	K	disc_F	$(a\,,b)$
F_1	$\mathbf{Q}(\sqrt{2})$	$\mathbf{Z}_K$	$(-1\,,-1)$
F_2	$\mathbf{Q}(\sqrt{2})$	$\mathfrak{p}_2\mathfrak{p}_3=(\sqrt{2})(3)$	$(-3\,,\sqrt{2}-2)$
F_3	$\mathbf{Q}(\sqrt{2})$	$\mathfrak{p}_2\mathfrak{p}_5=(\sqrt{2})(5)$	$(\sqrt{2}-2\,,-5)$
F_4	$\mathbf{Q}(\sqrt{2})$	$\mathfrak{p}_2\mathfrak{p}_7=(\sqrt{2})(1+2\sqrt{2})$	$(-\sqrt{2}-4\,,-1)$
F_5	$\mathbf{Q}(\sqrt{2})$	$\mathfrak{p}_2\overline{\mathfrak{p}_7}=(\sqrt{2})(1-2\sqrt{2})$	$(\sqrt{2}-4\,,-1)$
F_6	$\mathbf{Q}(\sqrt{5})$	$\mathbf{Z}_K$	$(-1\,,-1)$
F_7	$\mathbf{Q}(\sqrt{5})$	$\mathfrak{p}_2\mathfrak{p}_5=(2)(\sqrt{5})$	$(\frac{\sqrt{5}-5}{2}\,,-2)$
F_8	$\mathbf{Q}(\sqrt{5})$	$\mathfrak{p}_2\mathfrak{p}_{11}=(2)(\frac{7+\sqrt{5}}{2})$	$(-1\,,2\sqrt{5}-8)$
F_9	$\mathbf{Q}(\sqrt{5})$	$\mathfrak{p}_2\overline{\mathfrak{p}_{11}}=(2)(\frac{7-\sqrt{5}}{2})$	$(-1\,,-2\sqrt{5}-8)$
F_{10}	$\mathbf{Q}(\sqrt{13})$	$\mathbf{Z}_K$	$(-1\,,-1)$
F_{11}	$\mathbf{Q}(\sqrt{13})$	$\mathfrak{p}_2\mathfrak{p}_3=(2)(\frac{1+\sqrt{13}}{2})$	$(-1\,,-2\sqrt{13}-8)$
F_{12}	$\mathbf{Q}(\sqrt{13})$	$\mathfrak{p}_2\overline{\mathfrak{p}_3}=(2)(\frac{1-\sqrt{13}}{2})$	$(-1\,,2\sqrt{13}-8)$
F_{13}	$\mathbf{Q}(\sqrt{17})$	$\mathbf{Z}_K$	$(-1\,,-3)$

TABLE V.2 – Corps de quaternions F totalement définis sur un corps quadratique de nombre de classes $\mathrm{h}_F=1$.

Théorème 3.10 (Bayer, Cerri & Chaubert)**.** *Si F est un corps de quaternions totalement défini dont aucune place finie n'est ramifiée sur un corps quadratique (réel) K dont l'unité fondamentale est de norme -1, alors pour tout ordre maximal Λ,*

$$\frac{\mathrm{disc}_K}{7552+3072\sqrt{6}}\leqslant M(\Lambda)\leqslant\frac{\mathrm{disc}_K}{16}.$$

Démonstration. La preuve utilise les propriétés du réseau E_8, voir [BCC09]. □

Corollaire 3.11. *Les corps de quaternions F_1, F_6 et F_{10} sont euclidiens pour la norme.*

Démonstration. C'est une conséquence immédiate du théorème 3.10. En fait, ce résultat avait déjà été prouvé par Lenstra ([Len78b]). □

Il manque un corps : $F_{13}=\left(\frac{-1,-3}{\mathbf{Q}(\sqrt{17})}\right)$. Pour l'étudier, nous allons utiliser une démarche algorithmique analogue à celle du chapitre II.

On va raisonner dans un cas un peu plus général que requis : soient $d>1$ un entier sans facteur carré, $a\,,b\in\mathbf{Q}$ tels que $a\,,b<0$. On considère un corps de quaternions $F=\left(\frac{a,b}{K}\right)$ totalement défini sur $K=\mathbf{Q}(\sqrt{d})$. Soit Λ un ordre maximal de F. On suppose qu'on a une description de Λ de la forme

$$\Lambda=\bigoplus_{l=1}^{4}(a_{l,1}+a_{l,2}i+a_{l,3}j+a_{l,4}k)\mathbf{Z}_K\,,$$

où $a_{l,m}\in K$ pour tous $1\leqslant l\,,m\leqslant 4$. Alors F peut être écrit

$$F=\bigoplus_{l=1}^{4}(a_{l,1}+a_{l,2}i+a_{l,3}j+a_{l,4}k)K,$$

ce qui donne $F = \Lambda \oplus \Delta$ pour

$$\Delta = \bigoplus_{l=1}^{4} (a_{l,1} + a_{l,2}i + a_{l,3}j + a_{l,4}k)D,$$

où D est un domaine fondamental de K. On peut par exemple prendre $D = \{a + b\theta,\ (a,b) \in [0,1[\cap\mathbf{Q}\}$, où $\theta = \frac{1+\sqrt{d}}{2}$ si $d \equiv 1 \pmod 4$ et $\theta = \sqrt{d}$ sinon. Ainsi, par Λ-périodicité de m_Λ, pour prouver que F est euclidien pour la norme, il suffit d'établir que pour tout $\xi \in \Delta$, il existe un certain $\lambda \in \Lambda$ tel que $\left|\mathbf{N}_{K/\mathbf{Q}} \circ \mathrm{nrd}_{F/K}(\xi - \lambda)\right| < 1$. Les ensembles Λ et Δ peuvent être récrits sous la forme suivante :

$$\Lambda = \left\{ \sum_{l=1}^{4} a_{l,1}z_l + i\sum_{l=1}^{4} a_{l,2}z_l + j\sum_{l=1}^{4} a_{l,3}z_l + k\sum_{l=1}^{4} a_{l,4}z_l;\ x_l,\ y_l \in \mathbf{Z} \right\},$$

$$\Delta = \left\{ \sum_{l=1}^{4} a_{l,1}z_l + i\sum_{l=1}^{4} a_{l,2}z_l + j\sum_{l=1}^{4} a_{l,3}z_l + k\sum_{l=1}^{4} a_{l,4}z_l;\ x_l,\ y_l \in \mathbf{Q} \cap [0,\ 1[\right\},$$

où $z_l = x_l + y_l\theta$. Clairement, Λ et Δ sont isomorphes à $\mathbf{Z}^8$ et $([0,1[\cap\mathbf{Q})^8$ respectivement. On va plonger ces deux ensembles dans $\mathbf{R}^8$. Pour ce faire, notons σ le $\mathbf{Q}$-isomorphisme non trivial de K (défini par $\sigma(\sqrt{d}) = -\sqrt{d}$). On considère la matrice $M \in \mathcal{M}_8(\mathbf{R})$ définie par

$$M = \begin{pmatrix}
a_{1,1} & a_{1,1}\theta & a_{2,1} & a_{2,1}\theta & a_{3,1} & a_{3,1}\theta & a_{4,1} & a_{4,1}\theta \\
\sigma(a_{1,1}) & \sigma(a_{1,1}\theta) & \sigma(a_{2,1}) & \sigma(a_{2,1}\theta) & \sigma(a_{3,1}) & \sigma(a_{3,1}\theta) & \sigma(a_{4,1}) & \sigma(a_{4,1}\theta) \\
a_{1,2} & a_{1,2}\theta & a_{2,2} & a_{2,2}\theta & a_{3,2} & a_{3,2}\theta & a_{4,2} & a_{4,2}\theta \\
\sigma(a_{1,2}) & \sigma(a_{1,2}\theta) & \sigma(a_{2,2}) & \sigma(a_{2,2}\theta) & \sigma(a_{3,2}) & \sigma(a_{3,2}\theta) & \sigma(a_{4,2}) & \sigma(a_{4,2}\theta) \\
a_{1,3} & a_{1,3}\theta & a_{2,3} & a_{2,3}\theta & a_{3,3} & a_{3,3}\theta & a_{4,3} & a_{4,3}\theta \\
\sigma(a_{1,3}) & \sigma(a_{1,3}\theta) & \sigma(a_{2,3}) & \sigma(a_{2,3}\theta) & \sigma(a_{3,3}) & \sigma(a_{3,3}\theta) & \sigma(a_{4,3}) & \sigma(a_{4,3}\theta) \\
a_{1,4} & a_{1,4}\theta & a_{2,4} & a_{2,4}\theta & a_{3,4} & a_{3,4}\theta & a_{4,4} & a_{4,4}\theta \\
\sigma(a_{1,4}) & \sigma(a_{1,4}\theta) & \sigma(a_{2,4}) & \sigma(a_{2,4}\theta) & \sigma(a_{3,4}) & \sigma(a_{3,4}\theta) & \sigma(a_{4,4}) & \sigma(a_{4,4}\theta)
\end{pmatrix},$$

ce qui permet d'identifier Λ à $M \cdot \mathbf{Z}^8$ et Δ à $M \cdot (\mathbf{Q} \cap [0,1[)^8$. Comme pour les corps de nombres, on considère un découpage-recouvrement de $\overline{\Delta} = M \cdot [0,1]^8$ par des parallélotopes dont les faces sont orthogonales aux axes canoniques de $\mathbf{R}^8$: un tel parallélotope est défini par

$$\mathcal{P} = \{(u_l)_{1\leqslant l\leqslant 8} \in \mathbf{R}^8, |u_l - C_l| \leq h_l\},$$

où $C = (c_l)_{1\leqslant l\leqslant 8}$ est le centre du parallélotope et $0 < h_l$ pour tout $1 \leqslant l \leqslant 8$. Pour prouver que F est euclidien pour la norme, il suffit de montrer que pour tout parallélotope $\mathcal{P}$ du découpage-recouvrement, il existe $\lambda \in \Lambda$ tel que

$$\text{pour tout } u \in \mathcal{P},\ \left|\mathbf{N}_{K/\mathbf{Q}}(\mathrm{nrd}_{F/K}(u - \lambda))\right| < 1. \tag{V.12}$$

Dans ce cas, on dit que $\mathcal{P}$ est absorbé par λ. Mais grâce à notre identification, la norme $\left|\mathbf{N}_{K/\mathbf{Q}} \circ \mathrm{nrd}_{F/K}\right|$ peut être écrite sous la forme

$$N(t) = (t_1^2 - at_3^2 - bt_5^2 + abt_7^2)(t_2^2 - at_4^2 - bt_6^2 + abt_8^2).$$

Donc pour s'assurer que la condition (V.12) est vérifiée, il suffit d'établir que

$$A(\mathcal{P},\ \lambda) \cdot B(\mathcal{P},\ \lambda) < 1, \tag{V.13}$$

où

$$A(\mathcal{P},\ \lambda) = (|C_1 - \lambda_1| + h_1)^2 - a(|C_3 - \lambda_3| + h_3)^2 - b(|C_5 - \lambda_5| + h_5)^2 + ab(|C_7 - \lambda_7| + h_7)^2$$

et

$$B(\mathcal{P},\ \lambda) = (|C_2 - \lambda_2| + h_2)^2 - a(|C_4 - \lambda_4| + h_4)^2 - b(|C_6 - \lambda_6| + h_6)^2 + ab(|C_8 - \lambda_8| + h_8)^2.$$

Notons au passage que la condition (V.13) est optimale : comme $a, b < 0$, pour tout $u \in \mathcal{P}$, on a

$$N(u - \lambda) \leq A(\mathcal{P},\ \lambda) \cdot B(\mathcal{P},\ \lambda)$$

et il existe un sommet V de $\mathcal{P}$ tel que

$$N(V - \lambda) = A(\mathcal{P},\ \lambda) \cdot B(\mathcal{P},\ \lambda).$$

Il suffit ainsi de trouver pour chaque $\mathcal{P}$ du découpage-recouvrement un élément λ appartenant à une liste précalculée $\mathcal{S}$ d'éléments de Λ. En pratique, si certains parallélotopes ne sont pas absorbés, on peut découper chacun d'entre eux en 2^8 parallélotopes plus petits et appliquer à nouveau le test d'absorption. L'algorithme 3.1 décrit plus précisément cette procédure.

Algorithme 3.1 Test d'absorption pour F

ENTRÉE : une borne B, un réel k
SORTIE : si **vrai**, alors $M(\Lambda) < k$

1: Calculer la liste $\mathcal{S} = \{M \cdot X,\ X_i \in \mathbf{Z} \cap]-B, B]$ pour tout $i\}$.
2: Définir un découpage-recouvrement de $\overline{\Delta}$ par des parallélotopes. On note T l'ensemble de ces parallélotopes.
3: Pour tout $\mathcal{P} \in T$, chercher $\lambda \in \mathcal{S}$ qui absorbe $\mathcal{P}$ pour k (remplacer 1 par k dans (V.13)). Si un tel λ existe, supprimer $\mathcal{P}$ de T.
4: Si $T = \varnothing$, renvoyer **vrai**.
5: Sinon, couper chaque $\mathcal{P}$ de T en 2^8 parallélotopes et remplacer T par la liste de ces parallélotopes plus petits. Aller à l'étape 3.

Remarque 3.12. Il ne s'agit pas à proprement parler d'un algorithme vu que la terminaison n'est pas garantie (en particulier l'algorithme 3.1 ne peut pas terminer dès que $M(\Lambda) \geqslant k$ et même si $M(\Lambda) < k$, on ne peut assurer sa terminaison), néanmoins, nous allons pouvoir l'exploiter pour montrer que $M(\Lambda) < k$.

Proposition 3.13. *Le corps de quaternions* $F = \left(\frac{-1,-3}{\mathbf{Q}(\sqrt{17})}\right)$ *est euclidien pour la norme.*

Démonstration. On applique l'algorithme 3.1 avec $B = 5$ et $k = 0{,}91$ et en découpant en 60 dans chaque direction. Après deux passages à l'étape 3, tous les parallélotopes sont absorbés. Par conséquent, $M(\Lambda) < 1$ et F est euclidien pour la norme. □

Il s'agit à présent de montrer que les autres candidats de la table V.2 ne sont pas euclidiens.

Lemme 3.14. *Pour F corps de quaternions de la table V.2, l'indice $[\Lambda^\times : \mathbf{Z}_K^\times]$ prend les valeurs suivantes :*

– $[\Lambda^\times : \mathbf{Z}_K^\times] = 1$ *pour* $F = F_3$,

– $[\Lambda^\times : \mathbf{Z}_K^\times] = 2$ *pour* $F = F_8$, F_9, F_{11} *et* F_{12},
– $[\Lambda^\times : \mathbf{Z}_K^\times] = 3$ *pour* $F = F_2$,
– $[\Lambda^\times : \mathbf{Z}_K^\times] = 4$ *pour* $F = F_4$ *et* F_5,
– $[\Lambda^\times : \mathbf{Z}_K^\times] = 5$ *pour* F_7.

Démonstration. C'est une application de la formule de masse d'Eichler (proposition 1.38). □

Proposition 3.15. *Les corps de quaternions F_i de la table V.2 ne sont pas euclidiens pour $i \in \{2, 3, 4, 5, 7, 8, 9, 11, 12\}$.*

Démonstration. Soit Λ un ordre maximal de F_i. On suppose que Λ est euclidien. Cela implique que $\Lambda_1 = \{0\} \cup \Lambda^\times \subsetneq \Lambda_2$ et si $\Lambda_2 \neq \Lambda$, alors $\Lambda_2 \subsetneq \Lambda_3$. On distingue quatre cas.

Cas 1 : $i \in \{3, 8, 9, 11, 12\}$. Comme Λ n'est pas un corps, $\Lambda_1 \subsetneq \Lambda_2$, soit donc $b \notin \{0\} \cup \Lambda^\times$ tel que

$$\varphi_b(\{0\} \cup \Lambda^\times) = \Lambda/b\Lambda.$$

Comme $b \notin \Lambda^\times$ et $1 \notin b\Lambda$, on peut appliquer la proposition 3.5 avec $s = 1$ et $v_1 = 1$, ce qui donne

$$\prod_{i=1}^{l} p_i^{f_i} + 1 \leqslant [\Lambda^\times : \mathbf{Z}_K^\times],$$

avec les notations de la proposition 3.5. Mais $\prod_{i=1}^{l} p_i^{f_i} + 1 \geqslant 3 > [\Lambda^\times : \mathbf{Z}_K^\times]$, ce qui donne une contradiction. Ainsi, Λ n'est pas euclidien.

Cas 2 : $i \in \{4, 5\}$. Comme dans le cas 1, il existe $b \notin \{0\} \cup \Lambda^\times$ tel que

$$\varphi_b(\{0\} \cup \Lambda^\times) = \Lambda/b\Lambda.$$

Dans ce cas, $[\Lambda^\times : \mathbf{Z}_K^\times] = 4$ et la proposition 3.5 implique que $l = 1$, de sorte que $b\Lambda = \mathfrak{M}$ est un idéal entier maximal. Si on note $\mathfrak{p} = \mathfrak{M} \cap \mathbf{Z}_K$ et p le premier en dessous de $\mathfrak{p}$, alors la proposition 3.5 se récrit

$$p^f \leqslant 3,$$

où f est le degré résiduel de $\mathfrak{p}$. Comme 3 est inerte dans $K = \mathbf{Q}(\sqrt{2})$, la seule possibilité est $p = 2$ et $\mathfrak{p} = \sqrt{2}\mathbf{Z}_K$.

Si $F = F_4$, alors un ordre maximal de F est

$$\Lambda = \mathbf{Z}_K \oplus i\mathbf{Z}_K \oplus \frac{1 + \sqrt{2} + \sqrt{2}i + j}{2}\mathbf{Z}_K \oplus \frac{(\sqrt{2} + 1)i + k}{2}\mathbf{Z}_K,$$

où $i^2 = -\sqrt{2} - 4$ et $j^2 = -1$. On peut calculer $\Lambda^\times/\mathbf{Z}_K^\times$ et trouver que ses quatre éléments sont les classes suivantes :

$$\mathbf{Z}_K^\times,\ j\mathbf{Z}_K^\times,\ -\frac{\sqrt{2}}{2}(1 + j)\mathbf{Z}_K^\times \text{ et } \frac{\sqrt{2}}{2}(1 - j)\mathbf{Z}_K^\times.$$

Or

$$j - 1 = \sqrt{2}\left(\sqrt{2}\frac{1 + \sqrt{2} + \sqrt{2}i + j}{2} - i - 1 - \sqrt{2}\right) \in \sqrt{2}\Lambda \subseteq \mathfrak{M} = b\Lambda$$

et

$$\frac{\sqrt{2}}{2}(1+j)+\frac{\sqrt{2}}{2}(1-j)=\sqrt{2}\in\sqrt{2}\Lambda\subseteq\mathfrak{M}=b\Lambda.$$

D'après le lemme 3.4 (2), ces relations impliquent que

$$\varphi_b(\Lambda^\times)\subseteq\varphi_b(\mathbf{Z}_K^\times)\bigcup\varphi_b\left(\frac{\sqrt{2}}{2}(1-j)\mathbf{Z}_K^\times\right),$$

et le lemme 3.4 (1) nous permet alors d'écrire

$$\left|\varphi_b(\Lambda^\times)\right|\leqslant 2\left|\varphi_b(\mathbf{Z}_K^\times)\right|.$$

Mais (V.7) montre que $\left|\varphi_b(\mathbf{Z}_K^\times)\right|\leqslant 2^1-1=1$, ce qui donne $\left|\varphi_b(\mathbf{Z}_K^\times)\right|\leqslant 2$. D'une part, cela implique

$$\left|\varphi_b(\{0\}\cup\Lambda^\times)\right|\leqslant 3,$$

mais d'autre part, (V.9) donne en ce cas

$$|\Lambda/b\Lambda|=p^{2f}=4,$$

ce qui contredit $\varphi_b(\{0\}\cup\Lambda^\times)=\Lambda/b\Lambda$ et montre que Λ n'est pas euclidien.

La preuve est analogue pour $F=F_5$.

Cas 3 : $i=2$. Dans ce cas, $[\Lambda^\times:\mathbf{Z}_K^\times]=3$. Comme précédemment, il existe $b\notin\{0\}\cup\Lambda^\times$ tel que

$$\varphi_b(\{0\}\cup\Lambda^\times)=\Lambda/b\Lambda.$$

En appliquant la proposition 3.5, on trouve $l=1$, $b\Lambda=\mathfrak{M}$ est un idéal entier maximal et $\mathfrak{p}=\mathfrak{M}\cap\mathbf{Z}_K$ est l'idéal premier $\sqrt{2}\mathbf{Z}_K$ au-dessus de 2. De plus d'après la proposition 1.32, $\mathfrak{M}$ est l'unique idéal maximal contenant $\sqrt{2}\mathbf{Z}_K$. Remarquons que si $c\notin\{0\}\cup\Lambda^\times$ vérifie $\varphi_c(\{0\}\cup\Lambda^\times)=\Lambda/c\Lambda$, alors $c\Lambda=\mathfrak{M}=b\Lambda$ et $c\in b\Lambda^\times$. Réciproquement, si $c\in b\Lambda^\times$, alors $c\Lambda=b\Lambda$, $\varphi_c=\varphi_b$ et $\varphi_c(\{0\}\cup\Lambda^\times)=\Lambda/c\Lambda$. Cela implique que

$$\Lambda_2=\{0\}\cup\Lambda^\times\cup b\Lambda^\times.$$

Comme [2] $\Lambda^2\neq\Lambda$, on a $\Lambda_2\subsetneq\Lambda_3$ et il existe un certain $d\in\Lambda$ tel que

$$d\notin\{0\}\cup\Lambda^\times\cup b\Lambda^\times \tag{V.14}$$

et

$$\varphi_d(\{0\}\cup\Lambda^\times\cup b\Lambda^\times)=\Lambda/d\Lambda.$$

Clairement, (V.14) implique que $1\notin d\Lambda$. Supposons que $b\in d\Lambda$. Alors $b\Lambda\subseteq d\Lambda$, et par maximalité de $b\Lambda=\mathfrak{M}$, on a soit $d\Lambda=\Lambda$, soit $d\Lambda=b\Lambda$. Cela implique $d\in\Lambda^\times$ ou $d\in b\Lambda^\times$, ce qui est faux. Par conséquent, $b\notin d\Lambda$, et on peut appliquer la proposition 3.5 avec $s=2$, $v_1=1$, $v_2=b$. Avec les notations de la proposition, on obtient

$$\prod_{i=1}^{l}p_i^{f_i}+1\leqslant 6.$$

Mais 3 et 5 sont inertes dans $K=\mathbf{Q}(\sqrt{2})$ et la seule possibilité est encore $l=1$, $p_1=2$. Par unicité de $\mathfrak{M}$, cela implique $d\Lambda=\mathfrak{M}=b\Lambda$, donc $d\in b\Lambda^\times$, ce qui est absurde.

2. Dans le cas contraire, $\mathbf{N}_{K/\mathbf{Q}}(\mathrm{nrd}_{F/K}(\Lambda))$ serait fini, mais il contient $\mathbf{N}_{K/\mathbf{Q}}^2(\mathbf{Z}_K)$

Cas 4 : $i = 7$. Pour traiter ce cas, on a besoin de spécifier Λ. Nous prenons l'ordre maximal suivant de F_7 :

$$\Lambda = \mathbf{Z}_K \oplus \frac{\frac{\sqrt{5}+1}{2} + i}{2}\mathbf{Z}_K \oplus j\mathbf{Z}_K \oplus \frac{\frac{\sqrt{5}+1}{2}j + k}{2}\mathbf{Z}_K,$$

avec $i^2 = \frac{\sqrt{5}-5}{2}$ et $j^2 = -2$. En ce cas, $[\Lambda^\times : \mathbf{Z}_K^\times] = 5$, mais nous allons aussi avoir besoin d'une description plus précise de $\Lambda^\times/\mathbf{Z}_K^\times$: ses cinq éléments sont les classes $\alpha_i\mathbf{Z}_K^\times$, où les α_i ($1 \leqslant i \leqslant 5$) sont respectivement

$$1, \frac{-\sqrt{5}+1-(\sqrt{5}+1)i}{4}, \frac{\sqrt{5}-1-(\sqrt{5}+1)i}{4}, \frac{-\sqrt{5}-1+2i}{4}, \frac{\sqrt{5}+1+2i}{4},$$

de sorte que

$$\Lambda^\times = \bigcup_{i=1}^{5} \alpha_i\mathbf{Z}_K^\times \qquad \text{et} \qquad j\Lambda^\times = \bigcup_{i=1}^{5} j\alpha_i\mathbf{Z}_K^\times.$$

Comme précédemment, il doit exister $b \notin \{0\} \cup \Lambda^\times$ tel que $\varphi_b(\{0\} \cup \Lambda^\times) = \Lambda/b\Lambda$. En appliquant la proposition 3.5 et en remarquant que 3 est inerte dans $\mathbf{Z}_K$, on obtient (avec les notations de la proposition) $l = 1$, $b\Lambda = \mathfrak{M}$, où $\mathfrak{M}$ est l'unique idéal entier maximal contenant l'idéal premier $2\mathbf{Z}_K$ (voir proposition 1.32). Avec le même raisonnement que dans le cas précédent, cela donne une description explicite de Λ_2 :

$$\Lambda_2 = \{0\} \cup \Lambda^\times \cup j\Lambda^\times.$$

À nouveau, $\Lambda_2 \subsetneq \Lambda$ et il existe un certain $d \in \Lambda$ tel que

$$d \notin \{0\} \cup \Lambda^\times \cup j\Lambda^\times \tag{V.15}$$

et

$$\varphi_d(\{0\} \cup \Lambda^\times \cup j\Lambda^\times) = \Lambda/d\Lambda.$$

Comme dans le cas 3, on voit que $1, j \notin d\Lambda$ et on peut appliquer la proposition 3.5 avec $s_1 = 2$, $v_1 = 1$ et $v_2 = j$. Avec les notations de la proposition, on obtient

$$\prod_{i=1}^{l} p_i^{f_i} + 1 \leqslant 10,$$

et les seules possibilités sont $l = 1$ et $p_1 = 2$ (avec $f_1 = 2$), $l = 1$ et $p_1 = 3$ (avec $f_1 = 2$) ou $l = 1$ et $p_1 = 5$ (avec $f_1 = 1$). Analysons ces trois sous-cas, en notant $p = p_1$.

Sous-cas 1 : $p = 2$. Par unicité de $\mathfrak{M} = j\Lambda$, ce cas mène à une contradiction.

Sous-cas 2 : $p = 3$. On a alors $d\Lambda = \mathfrak{N}$, où $\mathfrak{N}$ est un idéal entier maximal [3] tel que $\mathfrak{N} \cap \mathbf{Z}_K = 3\mathbf{Z}_K$. Comme cela sera utile pour la suite, remarquons qu'on peut déduire des valeurs des α_i ou de l'égalité $j\Lambda = \Lambda j$ la propriété

$$j\Lambda^\times = \Lambda^\times j. \tag{V.16}$$

Comme $\varphi_d(\Lambda_2) = \Lambda/d\Lambda$, il existe $\lambda_2 \in \Lambda_2$ tel que $j + 1 + d\Lambda = \lambda_2 + d\Lambda$. Alors $\lambda_2 = j + 1 - d\lambda$ pour un certain $\lambda \in \Lambda$. Mais $\lambda_2 \in \Lambda_2$, de sorte que $\lambda_2 = 0$ ou $\lambda_2 \in \Lambda^\times$ ou $\lambda_2 \in j\Lambda^\times$. Nous allons prouver que dans chacun de ces trois cas, il existe $\varepsilon \in \Lambda^\times$ tel que

$$j - \varepsilon \in d\Lambda. \tag{V.17}$$

3. Un tel idéal maximal n'est pas nécessairement unique car 3 n'est pas ramifié.

– Dans le premier cas, $\lambda_2 = 0$ implique $j + 1 = d\lambda$ et on peut prendre $\varepsilon = -1$.
– Analysons le deuxième cas où $\lambda_2 \in \Lambda^\times$. On a $\lambda_2(j-1) = -3 - d\lambda(j-1)$ et, comme $3 \in \mathfrak{N} = d\Lambda$ et $j - 1 \in \Lambda$,

$$\lambda_2(j-1) \in d\Lambda. \tag{V.18}$$

Mais $\lambda_2(j-1) = \lambda_2 j - \lambda_2 = j\alpha - \lambda_2$ pour un certain $\alpha \in \Lambda^\times$ d'après (V.16). Cela implique $\lambda_2(j-1)\alpha^{-1} = j - \lambda_2\alpha^{-1}$ et on déduit de (V.18) que

$$j - \lambda_2\alpha^{-1} \in d\Lambda.$$

On peut donc prendre $\varepsilon = \lambda_2\alpha^{-1} \in \Lambda^\times$.
– En ce cas, $\lambda_2 \in j\Lambda^\times$, donc, d'après (V.16), il existe α, $\beta \in \Lambda^\times$ tels que $\lambda_2 = j\alpha = \beta j$. Comme précédemment, $\lambda_2(j-1) = -3 - d\lambda(j-1) \in d\Lambda$. Mais $\lambda_2(j-1) = \beta j(j-1) = -2\beta - \beta j = -3\beta + \beta - j\alpha$, ce qui implique que $j\alpha - \beta \in d\Lambda$. Par conséquent,

$$j - \beta\alpha^{-1} \in d\Lambda,$$

et on peut prendre $\varepsilon = \beta\alpha^{-1}$.

Cela prouve (V.17), on en déduit en utilisant le lemme 3.4 (2) que $\varphi_d(j\Lambda^\times) = \varphi_d(\varepsilon\Lambda^\times) = \varphi_d(\Lambda^\times)$. Au final,

$$\Lambda/d\Lambda = \varphi_d(\Lambda_2) = \varphi_d(\Lambda_1),$$

ce qui implique que $d \in \Lambda_2$. C'est absurde.

Sous-cas 2 : $p = 5$. Comme l'idéal premier $\sqrt{5}\mathbf{Z}_K$ est ramifié dans F, on a $d\Lambda = \mathfrak{N}$ où $\mathfrak{N}$ est l'unique idéal entier maximal (premier, donc bilatère) tel que $\mathfrak{N} \cap \mathbf{Z}_K = \sqrt{5}\mathbf{Z}_K$. Un calcul facile montre que $\mathrm{nrd}_{F/K}(\alpha_3 - \alpha_1) = \sqrt{5}\frac{\sqrt{5}-1}{2} \in \sqrt{5}\mathbf{Z}_K$ et $\mathrm{nrd}_{F/K}(\alpha_4 - \alpha_1) = \mathrm{nrd}_{F/K}(\alpha_5 - \alpha_2) = \sqrt{5}\frac{\sqrt{5}+1}{2} \in \sqrt{5}\mathbf{Z}_K$. D'après le corollaire 1.45, cela implique que $\alpha_3 - \alpha_1$, $\alpha_4 - \alpha_1$, $\alpha_5 - \alpha_2 \in \mathfrak{N} = d\Lambda$, et, comme $\mathfrak{N}$ est bilatère que $j\alpha_3 - j\alpha_1$, $j\alpha_4 - \alpha_1$, $j\alpha_5 - j\alpha_2 \in \mathfrak{N} = d\Lambda$. Ainsi, d'après le lemme 3.4 (2),

$$\varphi_d(\{0\} \cup \Lambda^\times \cup j\Lambda^\times) = \varphi_d(\{0\}) \cup \bigcup_{i=1}^{2} \varphi_d(\alpha_i\mathbf{Z}_K^\times) \cup \bigcup_{i=1}^{2} \varphi_d(j\alpha_i\mathbf{Z}_K^\times).$$

En utilisant le lemme 3.4 (1) et (V.7), on trouve

$$\left|\varphi_d(\{0\} \cup \Lambda^\times \cup j\Lambda^\times)\right| \leqslant 1 + 4 \cdot (5^1 - 1) = 17.$$

Mais on doit aussi avoir $|\varphi_d(\{0\} \cup \Lambda^\times \cup j\Lambda^\times)| = |\Lambda/d\Lambda|$ et ce dernier cardinal est

$$|\Lambda/\mathfrak{N}| = \mathbf{N}_{K/\mathbf{Q}}(\mathrm{nrd}_{F/K}(\mathfrak{N}))^2 = \mathbf{N}_{K/\mathbf{Q}}(\sqrt{5}\mathbf{Z}_K)^2 = 25.$$

Cela fournit une contradiction.

□

Démonstration du théorème 3.7. Si F est euclidien, alors le nombre de classes de F est $\mathrm{h}_F = 1$. Or, d'après la proposition 3.9, seuls treize corps de quaternions totalement définis sur un corps quadratique (réel) vérifient cette propriété. Parmi ces corps, quatre sont euclidiens pour la norme (corollaire 3.11 et proposition 3.13), les autres ne sont pas euclidiens (proposition 3.15). □

disc_K	$\mathbf{N}_{K/\mathbf{Q}}(\mathrm{disc}_F)$
49	7
49	8
81	3
148	2
169	5
316	2

TABLE V.3 – Candidats pour les corps de quaternions F euclidiens totalement définis sur un corps cubique K.

3.6 En degré supérieur

En degré $[K : \mathbf{Q}] \geqslant 3$, la proposition 3.5 s'applique encore pour prouver que certains corps de quaternions ne sont pas euclidiens.

Théorème 3.16. *Soit F un corps de quaternions euclidien pour la norme et totalement définis sur un corps de nombres cubique K, alors F est un élément de la table V.3.*

Démonstration. Rappelons que si F est euclidien, alors $\mathrm{h}_F = 1$ et donc F est un élément de la « liste [4] » suivante, d'après le théorème 3.3.

identifiant	disc_K	$\mathbf{N}_{K/\mathbf{Q}}(\mathrm{disc}_F)$	$[\Lambda^\times : \mathbf{Z}_K^\times]$
C_1	49	7	14
C_2	49	8	12
C_3	49	13	7
C_4	49	29	3
C_5	49	43	2
C_6	81	3	12
C_7	81	19	2
C_8	81	37	1
C_9	148	2	12
C_{10}	148	5	3
C_{11}	169	5	3
C_{12}	169	13	1
C_{13}	316	2	3
C_{14}	321	3	2

Il s'agit donc de montrer que dans certains cas C_i, si F appartient à C_i, alors F n'est pas euclidien. D'après la proposition 3.5, si $[\Lambda^\times : \mathbf{Z}_K^\times] \leqslant 2$, alors $\Lambda_2 = \Lambda_1$ et F n'est pas euclidien. On arrive aux mêmes conclusions si $[\Lambda^\times : \mathbf{Z}_K^\times] = 3$ et si 2 n'est pas une norme d'un élément de $\mathbf{Z}_K$, ce qui permet aussi d'exclure C_4 et C_{10}. Comme ni 3, ni 5 ne sont des normes dans le corps cubique réel de discriminant 49, on peut aussi écarter C_3. □

4. Il ne s'agit pas vraiment d'une liste mais plutôt d'un union de listes finies. Chaque C_i peut contenir plusieurs corps de quaternions

Remarque 3.17. Soit F un corps de quaternions totalement défini sur un corps de nombres quartique K, alors F est un corps de discriminant réduit $\mathrm{disc}_F = \mathbf{Z}_K$ sur K_i, $1 \leqslant i \leqslant 3$, où

$$\mathrm{disc}_{K_1} = 725\,,\ \mathrm{disc}_{K_2} = 1\,957\,,\ \mathrm{disc}_{K_3} = 2\,777.$$

Démonstration. Si F est euclidien, alors $\mathrm{h}_F = 1$, donc F appartient à la liste donnée. L'application de la proposition 3.5 ne permet pas d'écarter de candidat. □

Théorème 3.18. *Il n'existe pas de corps de quaternions F euclidien et totalement défini sur un corps K de degré $[K : \mathbf{Q}] \geqslant 5$.*

Démonstration. D'après la proposition 2.4, si F est euclidien, alors il a un nombre de classes $\mathrm{h}_F = 1$. Or, d'après le théorème 3.3, cela implique que $[K : \mathbf{Q}] \leqslant 5$ et le degré 5 n'est possible que pour $K = \mathbf{Q}(x)$ où $x^5 - 5x^3 - x^2 + 3x + 1 = 0$, de discriminant $\mathrm{disc}_K = 24217$ et $\mathrm{disc}_F = \mathfrak{p}_5$, où $\mathfrak{p}_5$ est l'idéal de norme 5 de $\mathbf{Z}_K$. D'après la formule de masse d'Eichler (proposition 1.38), $[\Lambda^\times : \mathbf{Z}_K^\times] = 3$. En supposant que F admette un ordre maximal Λ qui est euclidien, il existe $b \in \Lambda \setminus \{0\} \cup \Lambda^\times$ tel que

$$\varphi_b(\{0\} \cup \Lambda^\times) = \Lambda/b\Lambda.$$

D'après la proposition 3.5, cela implique que $\prod_{i=1}^{l} p_i^{f_i} + 1 \leqslant 3$ (avec les notations de la proposition). Mais 2 est inerte dans K, donc c'est impossible. Ainsi, F n'est pas euclidien. □

4 Euclidianité des corps de quaternions totalement indéfinis sur un corps de nombres

Dans ce paragraphe, on s'intéresse à l'euclidianité des corps de quaternions totalement indéfinis sur un corps de nombres K. Après avoir présenté quelques outils techniques, nous donnons des propriétés générales de l'euclidianité des corps de quaternions totalement indéfinis, puis nous étudions l'euclidianité pour la norme dans le cas particulier où le corps de base K est un corps quadratique imaginaire.

4.1 Outils techniques

4.1.1 Théorèmes de la progression arithmétique et des normes

Le but de ce paragraphe n'est pas d'énoncer la version la plus générale possible du théorème des normes, dont les premiers énoncés ont été prouvés par Hasse, Schilling, Maaß et Eichler, mais seulement d'en donner une variante utile à l'étude des corps de quaternions euclidiens dans le cas totalement indéfini. Pour cette raison, nous allons seulement énoncer le théorème de la progression arithmétique d'Eichler (qui avait déjà remarqué son application au cadre euclidien).

Théorème 4.1 (théorème de la progression arithmétique d'Eichler, [Eic38, Satz 5])**.** *Soient F un corps de quaternions totalement indéfini sur un corps de nombres K, Λ un ordre maximal de F, $x \in \Lambda$ et $\mathfrak{I}$ un idéal bilatère entier d'ordre à droite (et à gauche) Λ tels que $nrd_{F/K}(x)$ et $nrd_{F/K}(\mathfrak{I})$ sont premiers entre eux.*

Alors pour tout $z \in nrd_{F/K}(x) + \mathfrak{I} \cap \mathbf{Z}_K$, il existe $\lambda \in \mathfrak{I}$ tel que

$$z = nrd_{F/K}(x + \lambda).$$

Notons que réciproquement (et en supposant simplement que $\mathfrak{I}$ est bilatère entier), si $\lambda \in \mathfrak{I}$, alors $\mathrm{nrd}_{F/K}(x+\lambda) \in \mathrm{nrd}_{F/K}(x) + \mathfrak{I} \cap \mathbf{Z}_K$, si bien qu'on peut en déduire le résultat suivant.

Corollaire 4.2 (théorème des normes)**.** *Soient F un corps de quaternions totalement indéfini sur un corps de nombres K et Λ un ordre maximal de F, alors on a l'égalité $nrd_{F/K}(\Lambda) = \mathbf{Z}_K$. En particulier, $nrd_{F/K} : F \longrightarrow K$ est surjective.*

Signalons aussi un corollaire important du théorème des normes.

Proposition 4.3. *Soit F un corps de quaternions totalement indéfini sur un corps de nombres K. Le nombre de classes de F est fini et vérifie $\mathrm{h}_F = \mathrm{h}_K$.*

Démonstration. Voir [Vig80, corollaire 5.7 bis p. 89] □

4.1.2 Écriture des éléments d'un corps de quaternions

Dans un corps de nombres K, on peut écrire tout élément $x \in K \setminus \{0\}$ sous la forme $x = b^{-1}a$ où $a, b \in \mathbf{Z}_K \setminus \{0\}$. Dans un corps de quaternions, la situation n'est pas aussi simple, mais on a tout de même le résultat suivant.

Proposition 4.4. *Soient F un corps de quaternions de nombre de classes $\mathrm{h}_F = 1$ et Λ un ordre maximal de F.*

– *Soient $a, b \in \Lambda$ tels que $a\Lambda + b\Lambda = \Lambda$. Alors il existe $c \in \Lambda$ tel que*

$$nrd_{F/K}(a+bc) \text{ et } nrd_{F/K}(b) \text{ sont premiers entre eux.}$$

– *Pour tout $x \in F \setminus \{0\}$, il existe $a, b, c \in \Lambda$ tels que*

$$x = b^{-1}a - c,$$

et tels que $nrd_{F/K}(a)$ et $nrd_{F/K}(b)$ sont premiers entre eux.

Avant de prouver ce résultat, on va établir le lemme technique suivant.

Lemme 4.5. *Soient K un corps de nombres et F un corps de quaternions sur K tels que $\mathrm{h}_F = \mathrm{h}_K = 1$. Soient $a \in \Lambda \setminus \{0\}$ et $\mathfrak{p}$ un idéal premier (entier) de K tel que $nrd_{F/K}(a) \in \mathfrak{p}$, alors il existe un idéal maximal M d'ordre à droite Λ tel que $M \cap \mathbf{Z}_K = \mathfrak{p}$ et $a \in M$.*

Démonstration. Écrivons $\mathfrak{p} = p\mathbf{Z}_K$ pour $p \in \mathbf{Z}_K$. Alors $a\Lambda + p\Lambda$ est un idéal entier de F d'ordre à droite Λ (d'après le corollaire 1.43). Si $a\Lambda + p\Lambda \subsetneq \Lambda$, il existe alors un idéal maximal M d'ordre à droite Λ tel que $a\Lambda + p\Lambda \subseteq M$ d'après le lemme de Zorn. Alors $p \in M$, donc $\mathrm{nrd}_{F/K}(M)$ divise p^2, donc $M \cap \mathbf{Z}_K = \mathfrak{p}$.

Il reste donc à prouver que $a\Lambda + p\Lambda \subsetneq \Lambda$. Par l'absurde, si $a\Lambda + p\Lambda = \Lambda$, alors il existe $\lambda, \mu \in \Lambda$ tels que $a\lambda + p\mu = 1$. Or $\mathrm{nrd}_{F/K}(a\lambda + p\mu) = \mathrm{nrd}_{F/K}(a)\mathrm{nrd}_{F/K}(\lambda) + p^2\mathrm{nrd}_{F/K}(\mu) + \mathrm{trd}_{F/K}(a\lambda\overline{\mu})p \in \mathfrak{p}$, d'où $1 \in \mathfrak{p}$, ce qui est impossible. □

Démonstration de la proposition 4.4. Commençons par montrer que la seconde propriété se déduit facilement de la première. Comme $K\Lambda = F$, il est toujours possible de trouver $a, b \in \Lambda$, $b \neq 0$, tels que $x = b^{-1}a$. On considère l'idéal $a\Lambda + b\Lambda$ d'ordre à droite Λ. Comme $\mathrm{h}_F = 1$, il est de la forme $d\Lambda$ où $d \in \Lambda \setminus \{0\}$. Quitte à remplacer a par $d^{-1}a$ et b par $d^{-1}b$, on peut donc supposer que $a\Lambda + b\Lambda = \Lambda$. Dès lors, d'après la

première propriété, il existe $c \in \Lambda$ tel que $\mathrm{nrd}_{F/K}(a+bc)$ et $\mathrm{nrd}_{F/K}(b)$ sont premiers entre eux. En remplaçant a par $a+bc$, cela donne $x = b^{-1}a - c$.

À présent, nous démontrons donc la première propriété. Nous supposons ainsi que $a\Lambda + b\Lambda = \Lambda$. Il existe donc $\lambda, \mu \in \Lambda$ tels que

$$a\lambda + b\mu = 1.$$

On va commencer par montrer que pour tout $\mathfrak{p}$ divisant $\mathrm{nrd}_{F/K}(b)$, il existe $\tau_{\mathfrak{p}} \in \Lambda$ tel que $\mathrm{trd}_{F/K}(a+b\tau_{\mathfrak{p}}) \notin \mathfrak{p}$ ou $\mathrm{nrd}_{F/K}(a+b\tau_{\mathfrak{p}}) \notin \mathfrak{p}$.

Si $\mathrm{nrd}_{F/K}(a) \notin \mathfrak{p}$, alors $\tau_{\mathfrak{p}} = 0$ convient. Sinon, d'après le lemme 4.5 (on a $\mathrm{h}_K = \mathrm{h}_F = 1$ d'après la proposition 4.3), il existe M maximal d'ordre à droite Λ tel que $a \in M$. Or $b \notin M$ (sinon, $\Lambda = a\Lambda + b\Lambda \subseteq M$, ce qui est faux). Donc, comme M est maximal, $M + b\Lambda = \Lambda$. Ainsi, il existe $m \in M$ et $\lambda \in \Lambda$ tels que

$$m + b\lambda = 1.$$

Ainsi, $1 - b\lambda \in M$. Or $1 - b\lambda = 1 - \mathrm{trd}_{F/K}(b\lambda) + \overline{\lambda} \cdot \overline{b}$. Si $\mathrm{trd}_{F/K}(b\lambda) \in \mathfrak{p} \subseteq M$, alors $1 + \overline{\lambda} \cdot \overline{b} \in M$. En multipliant à droite par $b \in \Lambda = \mathcal{O}_r(M)$, on obtient que $b \in M$, ce qui est absurde. Donc $\mathrm{trd}_{F/K}(b\lambda) \notin \mathfrak{p}$. Si $\mathrm{trd}_{F/K}(a) \notin \mathfrak{p}$, alors $\tau_{\mathfrak{p}} = 0$ convient. Si $\mathrm{trd}_{F/K}(a) \in \mathfrak{p}$, alors $\tau_{\mathfrak{p}} = \lambda$ convient.

On prouve à présent qu'il existe $\tau \in \Lambda$ tel que pour tout idéal $\mathfrak{p}$ premier divisant $\mathrm{nrd}_{F/K}(b)$, $\mathrm{nrd}_{F/K}(a+b\tau) \notin \mathfrak{p}$ ou $\mathrm{trd}_{F/K}(a+b\tau) \notin \mathfrak{p}$. Pour ce faire, écrivons la décomposition $\mathrm{nrd}_{F/K}(b)\mathbf{Z}_K = \prod_{i=1}^{l} \mathfrak{p}_i^{t_i}$ avec pour tout $i \in \{1, \ldots, l\}$, $t_i > 0$ et $\mathfrak{p}_i = p_i\mathbf{Z}_K$ où $p_i \in \mathbf{Z}_K$. On peut alors écrire pour tout $i \in \{1, \ldots, l\}$ des relations de Bézout de la forme

$$\alpha_i p_i + \beta_i \prod_{\substack{j=1 \\ j \neq i}} p_j = 1,$$

où les $\alpha_i, \beta_i \in \mathbf{Z}_K$. On pose $e_i = \beta_i \prod_{\substack{j=1 \\ j \neq i}} p_j$ et $\tau = \sum_{i=1}^{l} e_i \tau_{\mathfrak{p}_i} \in \Lambda$ de sorte que pour tout $i \in \{1, \ldots, l\}$,

$$\tau - \tau_{\mathfrak{p}_i} \in p_i\Lambda.$$

Soit $i \in \{1, \ldots, l\}$. On écrit $\tau - \tau_{\mathfrak{p}_i} = p_i\lambda_i$ pour $\lambda_i \in \Lambda$. Alors

$$\begin{aligned} \mathrm{nrd}_{F/K}(a+b\tau) &= \mathrm{nrd}_{F/K}(a + b\tau_{\mathfrak{p}_i} + bp_i\lambda_i) \\ &= \mathrm{nrd}_{F/K}(a+b\tau_{\mathfrak{p}_i}) + \mathrm{nrd}_{F/K}(b\lambda_i)p_i^2 + \mathrm{trd}_{F/K}((a+b\tau_{\mathfrak{p}_i})\overline{b\lambda_i})p_i \\ &\equiv \mathrm{nrd}_{F/K}(a+b\tau_{\mathfrak{p}_i}) \pmod{\mathfrak{p}_i}. \end{aligned}$$

Par ailleurs,

$$\begin{aligned} \mathrm{trd}_{F/K}(a+b\tau) &= \mathrm{trd}_{F/K}(a + b\tau_{\mathfrak{p}_i} + bp_i\lambda_i) \\ &= \mathrm{trd}_{F/K}(a+b\tau_{\mathfrak{p}_i}) + p_i\mathrm{trd}_{F/K}(b\lambda_i) \\ &\equiv \mathrm{trd}_{F/K}(a+b\tau_{\mathfrak{p}_i}) \pmod{\mathfrak{p}_i}, \end{aligned}$$

ce qui montre que $a+b\tau$ vérifie les propriétés désirées.

On écrit alors

$$\mathfrak{P} := \prod_{\substack{\mathfrak{p} \mid \mathrm{nrd}_{F/K}(a+b\tau) \\ \mathfrak{p} \mid \mathrm{nrd}_{F/K}(b)}} \mathfrak{p} \text{ et } \mathfrak{Q} := \prod_{\substack{\mathfrak{p} \nmid \mathrm{nrd}_{F/K}(a+b\tau) \\ \mathfrak{p} \mid \mathrm{nrd}_{F/K}(b)}} \mathfrak{p},$$

on considère P, $Q \in \mathbf{Z}_K$ tels que $\mathfrak{P} = P\mathbf{Z}_K$, $\mathfrak{Q} = Q\mathbf{Z}_K$ et une relation de Bézout $eP + dQ = 1$, avec e, $d \in \mathbf{Z}_K$. Comme $(a + b\tau)\Lambda + b\Lambda = \Lambda$, il existe ν, $\mu \in \Lambda$ tels que

$$(a + b\tau)\nu + b\mu = 1.$$

On s'intéresse à présent à $a + b\tau + b\mu dQ$. Sa norme réduite est

$$\mathrm{nrd}_{F/K}(a + b\tau + b\mu dQ) = \mathrm{nrd}_{F/K}(a + b\tau) + \mathrm{nrd}_{F/K}(b\mu)d^2Q^2 + \mathrm{trd}_{F/K}((a + b\tau)\overline{b\mu})dQ.$$

Soit $\mathfrak{p}$ un diviseur premier de $\mathrm{nrd}_{F/K}(b)$. Si $\mathfrak{p}$ divise Q, alors

$$\begin{aligned} \mathrm{nrd}_{F/K}(a + b\tau + b\mu dQ) &\equiv \mathrm{nrd}_{F/K}(a + b\tau) \pmod{\mathfrak{p}} \\ &\not\equiv 0 \pmod{\mathfrak{p}}, \end{aligned}$$

car $\mathfrak{p} \nmid \mathrm{nrd}_{F/K}(a + b\tau)$. Si $\mathfrak{p}$ divise P, alors

$$\begin{aligned} \mathrm{nrd}_{F/K}(a + b\tau + b\mu dQ) &\equiv \mathrm{trd}_{F/K}((a + b\tau)\overline{b\mu}) \pmod{\mathfrak{p}} \\ &\equiv \mathrm{trd}_{F/K}((a + b\tau)\overline{1 - (a + b\tau)\nu}) \pmod{\mathfrak{p}} \\ &\equiv \mathrm{trd}_{F/K}(a + b\tau) - \mathrm{trd}_{F/K}((a + b\tau)\overline{\nu}\overline{a + b\tau}) \pmod{\mathfrak{p}} \\ &\equiv \mathrm{trd}_{F/K}(a + b\tau) \pmod{\mathfrak{p}}, \end{aligned}$$

car un calcul immédiat montre que

$$\mathrm{trd}_{F/K}((a + b\tau)\overline{\nu}\overline{a + b\tau}) = \mathrm{nrd}_{F/K}(a + b\tau)\mathrm{trd}_{F/K}(\nu) \in \mathfrak{p}.$$

Comme $\mathrm{nrd}_{F/K}(a + b\tau) \in \mathfrak{p}$, par construction de τ, $\mathrm{trd}_{F/K}(a + b\tau) \notin \mathfrak{p}$, ce qui montre que $\mathrm{nrd}_{F/K}(a + b\tau + b\mu dQ) \notin \mathfrak{p}$.

En tout cas, on obtient donc que $\mathrm{nrd}_{F/K}(a + b(\tau + \mu dQ))$ et $\mathrm{nrd}_{F/K}(b)$ sont premiers entre eux. Alors

$$x = b^{-1}a = b^{-1}(a + b(\tau + \mu dQ)) - (\tau + \mu dQ),$$

ce qui donne une décomposition de x de la forme recherchée. □

4.2 Propriétés générales

Théorème 4.6. *Soit F un corps de quaternions totalement indéfini sur un corps de nombres K. Si K est euclidien, alors F est euclidien.*

Démonstration. On note $\varphi : \mathbf{Z}_K \longrightarrow \mathbf{N}$ un stathme euclidien pour $\mathbf{Z}_K$, Λ un ordre maximal de F. On va montrer que $\phi = \varphi \circ \mathrm{nrd}_{F/K}$ est un stathme à droite pour Λ. Notons que comme ϕ est invariant par conjugaison, cela prouvera aussi que ϕ est un stathme euclidien à gauche.

Soient donc α, $\beta \in \Lambda$ avec $\beta \neq 0$. Alors $\alpha\Lambda + \beta\Lambda$ est un idéal d'ordre à droite Λ, on peut l'écrire sous la forme $\gamma\Lambda$ où $\gamma \in \Lambda$. D'après la proposition 4.4, il existe $c \in \Lambda$ tel que si on note $a := \gamma^{-1}\alpha + \gamma^{-1}\beta c$ et $b := \gamma^{-1}\beta$, alors

$$\mathrm{nrd}_{F/K}(a) \text{ et } \mathrm{nrd}_{F/K}(b) \text{ sont premiers entre eux.}$$

On fait la division euclidienne de $\mathrm{nrd}_{F/K}(\alpha + \beta c)$ par $\mathrm{nrd}_{F/K}(\beta)$ (dans $\mathbf{Z}_K$) : il existe alors $z \in \mathbf{Z}_K$ tel que

$$\varphi(\mathrm{nrd}_{F/K}(\alpha + \beta c) - \mathrm{nrd}_{F/K}(\beta)z) < \varphi(\mathrm{nrd}_{F/K}(\beta)) = \phi(\beta). \tag{V.19}$$

Or $\mathrm{nrd}_{F/K}(\alpha+\beta c)-\mathrm{nrd}_{F/K}(\beta)z = \mathrm{nrd}_{F/K}(\gamma)\cdot(\mathrm{nrd}_{F/K}(a)-\mathrm{nrd}_{F/K}(b)z)$. Par ailleurs, d'après le théorème 4.1, avec $\mathfrak{I}=\mathrm{nrd}_{F/K}(b)\Lambda$, il existe $\lambda\in\Lambda$ tel que

$$\mathrm{nrd}_{F/K}(a)-\mathrm{nrd}_{F/K}(b)z=\mathrm{nrd}_{F/K}(a-\mathrm{nrd}_{F/K}(b)\lambda).$$

Par conséquent,

$$\begin{aligned}\mathrm{nrd}_{F/K}(\alpha+\beta c)-\mathrm{nrd}_{F/K}(\beta)z &= \mathrm{nrd}_{F/K}(\gamma a-\gamma b\bar{b}\lambda)\\ &= \mathrm{nrd}_{F/K}(\alpha+\beta c-\beta\bar{b}\lambda)\\ &= \mathrm{nrd}_{F/K}(\alpha-\beta(\bar{b}\lambda-c)),\end{aligned}$$

de sorte que (V.19) se reformule en

$$\phi(\alpha-\beta(\bar{b}\lambda-c))<\phi(\beta). \tag{V.20}$$

Comme $\bar{b}\lambda-c\in\Lambda$, cela montre que ϕ est un stathme à droite pour Λ. □

Avant d'en donner une légère généralisation, signalons tout de suite le corollaire immédiat suivant, déjà énoncé par Eichler ([Eic38, Satz 6]).

Corollaire 4.7. *Soit F un corps de quaternions totalement indéfini sur un corps euclidien pour la norme K, alors F est euclidien pour la norme.*

Démonstration. Dans la preuve du théorème 4.6, si on prend $\varphi=\left|\mathbf{N}_{K/\mathbf{Q}}\right|$ comme stathme sur $\mathbf{Z}_K$, alors $\phi=\left|\mathbf{N}_{K/\mathbf{Q}}\circ\mathrm{nrd}_{F/K}\right|$ est un stathme à droite pour Λ. □

En fait, on peut énoncer un résultat faisant apparaître le minimum euclidien.

Théorème 4.8. *Soit F un corps de quaternions sur un corps de nombres K tel que $\mathrm{h}_F=\mathrm{h}_K=1$. Pour tout ordre maximal Λ de F, on a*

$$M(\Lambda)\leqslant M(K).$$

Démonstration. Là encore, il s'agit en fait d'une petite modification de la démonstration du théorème 4.6. En ce cas, $\varphi=\left|\mathbf{N}_{K/\mathbf{Q}}\right|$ et la « division » donnée en (V.19) s'écrit

$$\left|\mathbf{N}_{K/\mathbf{Q}}(\mathrm{nrd}_{F/K}(\alpha-\beta c)-\mathrm{nrd}_{F/K}(\beta)z)\right|\leqslant M(K)\cdot\left|\mathbf{N}_{K/\mathbf{Q}}(\mathrm{nrd}_{F/K}(\beta))\right|.$$

Avec le même raisonnement, (V.20) s'écrit alors

$$\left|\mathbf{N}_{K/\mathbf{Q}}\circ\mathrm{nrd}_{F/K}(\alpha-\beta(\bar{b}\lambda-c))\right|\leqslant M(K)\cdot\left|\mathbf{N}_{K/\mathbf{Q}}\circ\mathrm{nrd}_{F/K}(\beta)\right|,$$

ce qui montre que $m_\Lambda\left(\frac{\alpha}{\beta}\right)\leqslant M(K)$, donc

$$M(\Lambda)\leqslant M(K).$$

□

4.3 Méthode pour prouver la caractère non euclidien pour la norme

Dans le paragraphe précédent, on a majoré le minimum euclidien d'un ordre maximal d'un corps de quaternions F sur un corps de nombres K en fonction du minimum euclidien de K. Ici, on cherche à minorer le minimum euclidien d'un ordre maximal de F en certains points par un minimum euclidien local de K. Ainsi, on pourra prouver dans certains cas que F n'est pas euclidien pour la norme.

Proposition 4.9. *Soient K un corps de nombres, F un corps de quaternions totalement indéfini sur K de nombre de classes $\mathrm{h}_F = 1$ et $t \in \mathbf{Z}_K$ un produit de premiers ramifiés distincts dans F. Alors pour tout ordre maximal Λ de F et pour tout $a \in \mathbf{Z}_K$ premier avec t, il existe $\xi \in \Lambda$ tel que*

$$m_\Lambda(\xi) \geqslant m_K\left(\frac{a}{t}\right).$$

Démonstration. Soit Λ un ordre maximal de F et $a \in \mathbf{Z}_K$ premier avec t. On écrit $t = \prod_{i=1}^{l} t_i$ où les $(t_i)_{1\leqslant i\leqslant l} \in \mathbf{Z}_K^l$ sont des premiers ramifiés distincts de F. Alors pour tout $1 \leqslant i \leqslant l$, il existe un idéal premier $\mathfrak{P}_i$ d'ordre à droite Λ tel que $t_i\Lambda = \mathfrak{P}_i^2$. Comme $\mathrm{h}_F = 1$, pour tout $1 \leqslant i \leqslant l$, il existe $\tau_i \in \Lambda$ tel que $\mathfrak{P}_i = \tau_i\Lambda$. Notons $\tau = \prod_{i=1}^{l} \tau_i$, de sorte que, par construction $\mathrm{nrd}_{F/K}(\tau)\mathbf{Z}_K = t\mathbf{Z}_K$.

Par ailleurs, d'après le théorème des normes (corollaire 4.2), il existe $\alpha \in \Lambda$ tels que

$$\mathrm{nrd}_{F/K}(\alpha) = a.$$

Posons $\xi = \tau^{-1}\alpha$ et soit alors $\lambda \in \Lambda$ tel que

$$\begin{aligned} m_\Lambda(\xi) &= \left|\mathbf{N}_{K/\mathbf{Q}}(\mathrm{nrd}_{F/K}(\xi - \lambda))\right|, \\ &= \frac{\left|\mathbf{N}_{K/\mathbf{Q}}(\mathrm{nrd}_{F/K}(\alpha - \tau\lambda))\right|}{\left|\mathbf{N}_{K/\mathbf{Q}}(\mathrm{nrd}_{F/K}(\tau))\right|}. \end{aligned}$$

L'idéal $I = \tau\Lambda = \prod_{i=1}^{l} \mathfrak{P}_i$ est bilatère et $\mathrm{nrd}_{F/K}(\alpha) = a$ est premier avec $\mathrm{nrd}_{F/K} I = \tau\mathbf{Z}_K$, donc d'après le théorème 4.1, $\mathrm{nrd}_{F/K}(\alpha - \tau\lambda) \in \mathrm{nrd}_{F/K}(\alpha) + I \cap \mathbf{Z}_K$.

Or pour tout $1 \leqslant i \leqslant l$, $I \cap \mathbf{Z}_K \subseteq \mathfrak{P}_i \cap \mathbf{Z}_K = t_i\mathbf{Z}_K$, donc $I \cap \mathbf{Z}_K \subseteq t\mathbf{Z}_K$ car les $(t_i)_{1\leqslant i\leqslant l}$ sont deux à deux distincts. On peut donc écrire $\mathrm{nrd}_{F/K}(\alpha - \tau\lambda) = \mathrm{nrd}_{F/K}(\alpha) + tz = a + tz$ pour un certain $z \in \mathbf{Z}_K$. Ainsi

$$m_\Lambda(\xi) = \frac{\left|\mathbf{N}_{K/\mathbf{Q}}(a + tz)\right|}{\left|\mathbf{N}_{K/\mathbf{Q}}(t)\right|} \geqslant m_K\left(\frac{a}{t}\right).$$

□

4.4 Cas des corps quadratiques imaginaires

En utilisant les méthodes des paragraphes précédents, nous allons étudier les corps de quaternions euclidiens pour la norme et totalement indéfinis sur un corps quadratique imaginaire.

Théorème 4.10. *Soit F un corps de quaternions totalement indéfini sur un corps quadratique imaginaire K. Supposons que $F \neq \left(\frac{-2,-5}{\mathbf{Q}(\sqrt{-19})}\right)$. Alors F est euclidien pour la norme si et seulement si K est euclidien pour la norme.*

Le reste de ce paragraphe va être consacré à la preuve de ce résultat. Rappelons que si K est euclidien pour la norme, alors F est euclidien pour la norme d'après le corollaire 4.7. Il va donc s'agir de prouver l'implication réciproque : supposons ainsi que F est euclidien pour la norme. Nous commençons par restreindre les cas possibles pour K.

Proposition 4.11. *Soient $K = \mathbf{Q}(\sqrt{-d})$, où d est entier strictement positif sans facteur carré, et F un corps de quaternions sur K. Si F est euclidien pour la norme, alors $d \in \{1, 2, 3, 7, 11, 19\}$.*

Pour prouver cette proposition, on va utiliser le lemme suivant.

Lemme 4.12. *Soient F un corps de quaternions totalement indéfini $K = \mathbf{Q}(\sqrt{-d})$ de nombre de classes $\mathrm{h}_F = 1$ et Λ un ordre maximal de F. Si $m \in \mathbf{R}_+$ est tel que $m < \frac{d}{16}$ et t est un produit de premiers ramifiés dans F tel que*

- *ou t est réel et $|t| \geqslant \frac{\sqrt{d}}{\sqrt{d}-4\sqrt{m}}$,*
- *ou t n'est pas réel et $|t| \geqslant \frac{2}{\sqrt{d}-4\sqrt{m}}$,*

alors il existe $\xi \in F$ tel que $m_\Lambda(\xi) \geqslant m$.

Démonstration. Pour tout $x \in K$ tel que $\sqrt{m} \leqslant \mathrm{Im}\,(x) \leqslant \frac{\sqrt{d}}{2} - \sqrt{m}$, on a $m_K(x) \geqslant m$ (si un tel x existe). Par conséquent, on va essayer de construire un tel x de la forme $x = \frac{\alpha}{t}$, où $\alpha \in \mathbf{Z}_K$.

Pour ce faire, écrivons $t = t_1 + t_2\frac{1+I\sqrt{d}}{2}$ où $t_1, t_2 \in \mathbf{Z}$ (rappelons qu'on note $I \in \mathbf{C}$ tel que $I^2 = -1$).

- Si $t_2 = 0$ (c'est-à-dire si t est réel), considérons $\alpha = \pm\alpha'\frac{1+I\sqrt{d}}{2}$, où $\alpha' \in \mathbf{Z}$ et $\pm$ est le signe de t. On veut obtenir

$$\sqrt{m} \leqslant \mathrm{Im}\left(\frac{\alpha}{t}\right) = \frac{\alpha'\sqrt{d}}{2|t|} \leqslant \frac{\sqrt{d} - 2\sqrt{m}}{2}.$$

  On peut trouver un tel entier α' si la différence des membres de droite et de gauche est supérieure à 1, ce qui équivaut à $|t| \geqslant \frac{\sqrt{d}}{\sqrt{d}-4\sqrt{m}}$.

- Si $t_2 \neq 0$, considérons $\alpha = \pm\alpha'$, où $\alpha' \in \mathbf{Z}$ et $\pm$ est le signe de t_2. Alors $\mathrm{Im}\left(\frac{\alpha}{t}\right) = \frac{\alpha'|t_2|\sqrt{d}}{2|t|^2}$ et on veut trouver un entier α' tel que

$$\sqrt{\frac{m}{d}} \cdot \frac{|t|^2}{\frac{|t_2|}{2}} \leqslant \alpha' \leqslant \frac{|t|^2}{\frac{|t_2|}{2}} \cdot \frac{1 - 2\sqrt{\frac{m}{d}}}{2},$$

  ce qui est possible si

$$\frac{|t|^2}{\frac{|t_2|}{2}} \geqslant \frac{2}{1 - 4\sqrt{\frac{m}{d}}}.$$

  Comme $\frac{|t|^2}{\frac{|t_2|}{2}} \geqslant |t|\sqrt{d}$, on obtient la propriété voulue si

$$|t| \geqslant \frac{2}{\sqrt{d} - 4\sqrt{m}}.$$

Sous les conditions du lemme, il existe donc $\alpha \in \mathbf{Z}_K$ tel que $m_K\left(\frac{\alpha}{t}\right) \geqslant m$. Quitte à simplifier la fraction $\frac{\alpha}{t}$, on peut supposer que les entiers α et t sont premiers entre eux. Ainsi, en appliquant la proposition 4.9, on trouve $\xi \in \Lambda$ tel que $m_\Lambda(\xi) \geqslant m_K\left(\frac{\alpha}{t}\right) \geqslant m$. □

Démonstration de la proposition 4.11. Si F est euclidien, alors $\mathrm{h}_F = 1$ d'après la proposition 2.4. Dès lors, $\mathrm{h}_K = \mathrm{h}_F = 1$ (d'après la proposition 4.3). Les corps quadratiques imaginaires $\mathbf{Q}\left(\sqrt{-d}\right)$ qui sont principaux sont bien connus (c'est le théorème de Heegner-Baker-Stark, voir par exemple [Cox97, Theorem 7.30 et Theorem 12.34]), ils correspondent aux valeurs de d suivantes :

$$d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}.$$

Il s'agit donc de prouver que les valeurs 43, 67 et 163 sont impossibles. Pour ce faire, on va bien sûr appliquer le lemme 4.12. On note Λ un ordre maximal de F.

Cas $d = 43$. On rappelle que F est totalement indéfini, donc que F admet au moins deux premiers ramifiés. On distingue deux sous-cas.

- S'il existe un premier $\mathfrak{p}$ ramifié dans F de la forme $\mathfrak{p} = t\mathbf{Z}_K$, où $t \notin \mathbf{R}$. Alors $|t| = \sqrt{\mathbf{N}\mathfrak{p}} > 1$. Or $\frac{2}{\sqrt{d}-4} < 1$, donc d'après le lemme 4.12 avec $m = 1$, il existe $\xi \in F$ tel que $m_\Lambda(\xi) \geqslant 1$, ainsi F n'est pas euclidien pour la norme.
- Sinon, pour tous premiers $\mathfrak{p}_1, \mathfrak{p}_2$ ramifiés dans F, il existe $t \in \mathbf{R}$ tel que $\mathfrak{p}_1\mathfrak{p}_2 = t\mathbf{Z}_K$. Alors $|t| \geqslant 2 \cdot 3 = 6$. Or $\frac{\sqrt{d}}{\sqrt{d}-4} < 6$. Donc il existe $\xi \in \Lambda$ tel que $m_\Lambda(\xi) \geqslant 1$, en particulier, F n'est pas euclidien pour la norme.

Cas $d = 67, 163$. Ils sont tout à fait analogues, il suffit de calculer les bornes du lemme 4.12. Pour fixer les idées, on donne des approximations ci-dessous.

d	$\frac{\sqrt{d}}{\sqrt{d}-4}$	$\frac{2}{\sqrt{d}-4}$
67	$< 1{,}96$	$< 0{,}48$
163	$< 1{,}46$	$< 0{,}23$

□

Lemme 4.13. *Soit F un corps de quaternions totalement indéfini sur $K = \mathbf{Q}(\sqrt{-19})$. Si $F \neq \left(\frac{-2,-5}{K}\right)$, alors F n'est pas euclidien pour la norme.*

Démonstration. Tout d'abord, on peut appliquer le lemme 4.12 si t est un produit de premiers ramifiés et si

- t est réel et $|t| \geqslant \frac{\sqrt{19}}{\sqrt{19}-4}$, donc en particulier si $|t| \geqslant 12{,}2$,
- ou t n'est pas réel et $|t| \geqslant \frac{2}{\sqrt{19}-4}$, donc en particulier si $|t|^2 \geqslant 31{,}1$,

alors F n'est pas euclidien pour la norme. On suppose à présent que F est euclidien pour la norme. Par conséquent, soit $\mathfrak{p}$ un premier de $\mathbf{Z}_K$, on considère le premier p tel que $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$.

- Si p est inerte, alors $\mathfrak{p} = t\mathbf{Z}_K$ pour $t \in \mathbf{Z}$. Donc $|t| \leqslant 11$.
- Si p est décomposé ou totalement ramifié, alors $\mathfrak{p} = t\mathbf{Z}_K$ pour $t \in \mathbf{C} \setminus \mathbf{R}$, donc $\mathbf{N}\mathfrak{p} = |t|^2 \leqslant 31$.

Dès lors, si $\mathfrak{p}$ est ramifié dans F, alors

$$\mathfrak{p} \in \{2\mathbf{Z}_K, 3\mathbf{Z}_K\} \cup \{\mathfrak{p}_i, \overline{\mathfrak{p}_i},\ i \in \{5, 7, 11, 17, 23\}\} \cup \{\mathfrak{p}_{19}\},$$

où $\mathfrak{p}_i$ désigne un idéal premier au-dessus de l'entier i (et $\overline{\mathfrak{p}_i}$ son conjugué). Comme K est principal, pour tout $i \in \{7, 11, 17, 19, 23\}$, il existe $t_i \in \mathbf{Z}_K$ tel que

$$\mathfrak{p}_i = t_i \mathbf{Z}_K.$$

Alors, d'après la proposition 4.9, 2 ne peut être ramifié dans F car $m_K\left(\frac{\frac{\sqrt{-19}+1}{2}}{2}\right) = \frac{5}{4}$. De même, ni $\mathfrak{p}_i$, ni $\overline{\mathfrak{p}_i}$ ne peuvent être ramifiés dans F si $i \in \{7, 11, 17, 19, 23\}$ car pour tout i, il existe $a_i \in \mathbf{Z}_K$ tel que $m_K\left(\frac{a_i}{t_i}\right) = m_K\left(\frac{a_i}{\overline{t_i}}\right) \geqslant 1$, donné par la table suivante.

i	a_i	$m_K\left(\frac{a_i}{t_i}\right) = m_K\left(\frac{a_i}{\overline{t_i}}\right)$
7	3	1
11	5	1
17	7	1
19	5	$\frac{25}{19}$
23	5	$\frac{25}{23}$

Par conséquent, les seuls premiers ramifiés peuvent être $3\mathbf{Z}_K$, $\mathfrak{p}_5$ et $\overline{\mathfrak{p}_5}$. Comme le nombre de places ramifiées est pair et comme aucune place à l'infini n'est ramifiée, exactement deux de ces trois premiers sont ramifiés.

Si 3 est ramifié, alors $\mathfrak{p}_5$ ou $\overline{\mathfrak{p}_5}$ est ramifié, donc $t = 3t_5$ ou $t = 3\overline{t_5}$ est un produit non réel de premiers ramifiés. Mais $|3t_5|^2 = |3\overline{t_5}|^2 = 45 > 31$, donc en ce cas, d'après le lemme 4.12, F n'est pas euclidien pour la norme.

Par conséquent, la seule ramification possible pour F est $\{\mathfrak{p}_5, \overline{\mathfrak{p}_5}\}$, ce qui arrive exactement pour $F = \left(\frac{-2,-5}{K}\right)$ (à isomorphisme près). □

En combinant la proposition 4.11 et le lemme 4.13, on obtient alors une démonstration du théorème 4.10.

Remarque 4.14. Pour $F = \left(\frac{-2,-5}{\mathbf{Q}(\sqrt{-19})}\right)$ (ramifiée en $\mathfrak{p}_5$ et $\overline{\mathfrak{p}_5}$), les techniques décrites précédemment montrent qu'il existe $\xi \in F$ tel que

$$m_\Lambda(\xi) \geqslant m_K\left(\frac{\sqrt{-19}+2}{5}\right) = \frac{23}{25}.$$

Mais cela ne suffit pas pour savoir si F est euclidien pour la norme ou non.

CHAPITRE VI

CONCLUSION ET PERSPECTIVES

Corps de nombres

Nous avons vu que l'algorithme décrit par Cerri dans le cas totalement réel se généralisait au cas quelconque, ce qui a permis d'obtenir de nombreux exemples. Néanmoins, la question de l'euclidianité pour la norme des corps cubiques complexes reste ouverte. Pour pouvoir y répondre, il faudrait certainement établir une meilleure borne sur le discriminant (de l'ordre de grandeur de celle d'Ennola [Enn58]), mais aussi pouvoir déterminer plus efficacement des points critiques de ces corps de nombres. Un tel travail s'appliquerait aussi aux classes euclidiennes non principales de corps cubiques complexes.

Par ailleurs, Shapira et Wang ont récemment étendu le résultat de Cerri sur le spectre euclidien au cas CM pour un degré strictement supérieur à 7 ([SW12]). Dans le même article, ils ont aussi établi une borne sur le dénominateur des points critiques d'un corps de nombres. Il serait donc intéressant de voir si cette borne a des applications algorithmiques pour leur détermination ou le calcul du minimum euclidien.

Corps de quaternions

Pour ce qui est de l'euclidianité des corps de quaternions, de nombreuses problématiques persistent. Tout d'abord, on ne sait toujours pas répondre à la question d'Eichler : existe-t-il des corps de quaternions euclidiens pour la norme et totalement indéfinis sur un corps de nombres non euclidien pour la norme ? Dans le cas quadratique imaginaire, notre étude a montré que cela ne pouvait se produire que dans un cas, mais nous ne sommes pas encore capables de le traiter.

Dans le cas totalement défini, il n'existe qu'un nombre fini de cas euclidiens. Les exemples euclidiens connus le sont tous pour la norme, il serait donc intéressant d'en trouver un euclidien pour un autre stathme, mais pas pour la norme, au moins dans le cas défini.

Dans cette optique et plus généralement, pour traiter plus d'exemples, on peut chercher à étendre la démarche algorithmique appliquée aux corps de nombres dans le cas des corps de quaternions. En premier lieu, il s'agit de pouvoir calculer le minimum euclidien local. La généralisation de l'algorithme appliqué aux corps de nombres qui utilise la multiplicativité de la norme ne paraît pas aisée. Néanmoins, les autres parties de l'algorithme de calcul du minimum euclidien devraient pouvoir s'étendre sans trop de changements.

INDEX

N

O

P

Q

R

S

T

BIBLIOGRAPHIE

[Akh95] Reza Akhtar. Cyclotomic Euclidean Number Fields, 1995. Harvard University, senior thesis.

[BC70] Pierre Barrucand & Harvey Cohn. A rational genus, class number divisibility, and unit theory for pure cubic fields. *Journal of Number Theory*, tome 2 (1) : pages 7–21, 1970.

[BCC09] Eva Bayer, Jean-Paul Cerri & Jérôme Chaubert. Euclidean minima and central division algebra. *International Journal of Number Theory*, tome 5 : pages 1155–1168, 2009.

[Ber84] Daniel Berend. Minimal sets on tori. *Ergodic Theory and Dynamical Systems*, tome 4 (4) : pages 499–507, 1984.

[BF06] Eva Bayer-Fluckiger. Upper bounds for Euclidean minima of algebraic number fields. *Journal of Number Theory*, tome 121 : pages 305–323, 2006.

[BR36] Hermann Behrbohm & László Rédei. Der Euklidische Algorithmus in quadratischen Zahlkörpern. *Journal für die reine und angewandte Mathematik*, tome 174 : pages 192–205, 1936.

[Bra40] Alfred Brauer. On the non-existence of the Euclidean algorithm in certain quadratic number fields. *American Journal of Mathematics*, tome 62 : pages 697–716, 1940.

[BSD52a] Eric S. Barnes & H. Peter F. Swinnerton-Dyer. The inhomogeneous minima of binary quadratic forms (I). *Acta Mathematica*, tome 87 : pages 259–323, 1952.

[BSD52b] Eric S. Barnes & H. Peter F. Swinnerton-Dyer. The inhomogeneous minima of binary quadratic forms (II). *Acta Mathematica*, tome 88 : pages 279–316, 1952.

[Cas52] John William Scott Cassels. The inhomogeneous minimum of binary quadratic, ternary cubic and quaternary quartic form. *Proceedings of the Cambridge Philosophical Society*, tome 48 : pages 72–86, 1952.

[CCL12] Jean-Paul Cerri, Jérôme Chaubert & Pierre Lezowski. Euclidean totally definite quaternion fields over the rational field and over quadratic number fields, 2012. À paraître dans *International Journal of Number Theory*.

[Cer05] Jean-Paul Cerri. *Spectres euclidiens et inhomogènes des corps de nombres*. Thèse de doctorat, Université Nancy 1, 2005.

[Cer06] Jean-Paul Cerri. Euclidean and inhomogeneous spectra of number fields with unit rank strictly greater than 1. *Journal für die reine und angewandte Mathematik*, tome 592 : pages 49–62, 2006.

[Cer07] Jean-Paul Cerri. Euclidean minima of totally real number fields. Algorithmic determination. *Mathematics of Computation*, tome 76 : pages 1547–1575, 2007.

[Cer11] Jean-Paul Cerri. Some generalized Euclidean and 2-stage Euclidean number fields that are not norm-Euclidean. *Mathematics of Computation*, tome 80 (276) : pages 2289–2298, 2011.

[Cha06] Jérôme Chaubert. *Minimum euclidien des ordres maximaux dans les algèbres centrales à division*. Thèse de doctorat, École Polytechnique Fédérale de Lausanne, 2006.

[Cio79] Vincent G. Cioffari. The Euclidean condition in pure cubic and complex quartic fields. *Mathematics of Computation*, tome 33 : pages 389–398, 1979.

[CL98] Stefania Cavallar & Franz Lemmermeyer. The Euclidean algorithm in cubic number fields. Dans Kálmán Győry, Attila Pethő & Vera T. Sos, rédacteurs, *Proceedings Number Theory Eger 1996*, pages 123–146. 1998.

[Coh62] Harvey Cohn. *Advanced Number Theory*. Dover, 1962.

[Coh66] Paul Moritz Cohn. On the structure of the GL_2 of a ring. *Institut des Hautes Études Scientifiques. Publications Mathématiques*, tome 30 : pages 5–53, 1966.

[Coh96] Henri Cohen. *A Course in Computational Algebraic Number Theory*, tome 138 de *Graduate Texts in Mathematics*. Springer, 1996.

[Coo76a] George E. Cooke. A weakening of the Euclidean property for integral domains and applications to algebraic number theory. I. *Journal für die reine und angewandte Mathematik*, tome 282 : pages 133–156, 1976.

[Coo76b] George E. Cooke. A weakening of the Euclidean property for integral domains and applications to algebraic number theory. II. *Journal für die reine und angewandte Mathematik*, tome 283-284 : pages 71–85, 1976.

[Cox97] David A. Cox. *Primes of the form $x^2 + ny^2$*, tome 34 de *Pure and applied mathematics*. John Wiley & Sons, 1997.

[CT78] Harvey Cohn & Olga Taussky. *A classical invitation to algebraic numbers and class fields*. Universitext. Springer, 1978.

[CW75] George E. Cooke & Peter J. Weinberger. On the construction of division chains in algebraic number rings, with applications to SL_2. *Communications in Algebra*, tome 3 : pages 481–524, 1975.

[Dav51] Harold Davenport. Indefinite binary quadratic forms and Euclid's algorithm in real quadratic fields. *Proc. London Math. Soc.*, tome 53 : pages 65–82, 1951.

[Dav52] Harold Davenport. Linear forms associated with an algebraic number field. *Quarterly Journal of Mathematics*, tome 2 : pages 32–41, 1952.

[Ded00] Richard Dedekind. Über die Anzahl der Idealklassen in reinen kubischen Zahlkörpern. *Journal für die reine und angewandte Mathematik*, tome 121 : pages 40–123, 1900.

[Deu35] Max Deuring. *Algebren*, tome 4 de *Ergebnisse der Mathematik und ihrer Grenzgebiete*. Springer, 1935.

[Ega79] Shigeki Egami. Euclid's Algorithm in Pure Quartic Fields. *Tokyo Journal of Mathematics*, tome 2 (2) : pages 379–385, 1979.

[Ega84] Shigeki Egami. On Finiteness of the Numbers of Euclidean Fields in Some Classes of Number Fields. *Tokyo Journal of Mathematics*, tome 7 (1) : pages 183–198, 1984.

[Eic37] Martin Eichler. Über die Klassennzahl total definiter Quaternionenalgebren. *Mathematische Zeitschrift*, tome 43 : pages 102–109, 1937.

[Eic38] Martin Eichler. Allgemeine Kongruenzklasseneinteilungen der Ideale einfacher Algebren über algebraischen Zahlkörpern und ihre L-Reihen. *Journal für die reine und angewandte Mathematik*, tome 179 : pages 227–251, 1938.

[End83] Akira Endô. On units of pure quartic number fields. *Pacific Journal of Mathematics*, tome 109 (2) : pages 327–333, 1983.

[Enn58] Veikko Ennola. *On the First Inhomogeneous Minimum of Indefinite Binary Quadratic Forms and Euclid's Algorithm in Real Quadratic Fields*. Thèse de doctorat, University of Turku, 1958.

[Euc32] Euclide. *Éléments, livre VII*. Denis Henrion (traduction), 1632. `http://gallica.bnf.fr/ark:/12148/bpt6k68013g/f260.image`.

[GM11] Xavier Guitart & Marc Masdeu. Continued fractions in 2-stage euclidean quadratic fields, 2011. To appear in *Mathematics of Computation*, `http://arxiv.org/abs/1106.0856`.

[GR11] Hester Graves & Nick Ramsey. Euclidean ideals in quadratic imaginary fields. *Journal of the Ramanujan Mathematical Society*, tome 26 (1) : pages 85–97, 2011.

[Gra09] Hester K. Graves. *On Euclidean Ideal Classes*. Thèse de doctorat, University of Michigan, 2009.

[Gra11] Hester Graves. $\mathbf{Q}\left(\sqrt{2}, \sqrt{35}\right)$ has a non-principal Euclidean ideal. *International Journal of Number Theory*, tome 7 : pages 2269–2271, 2011.

[Har04] Malcolm Harper. $\mathbf{Z}(\sqrt{14})$ is Euclidean. *Journal Canadien de Mathématiques*, tome 56 (1) : pages 55–70, 2004.

[Has28] Helmut Hasse. Über eindeutige Zerlegung in Primelemente oder in Primhauptideale in Integritätsbereichen. *Journal für die reine und angewandte Mathematik*, tome 159 (3-12) : pages 60–61, 1928.

[Ink47] Kustaa Inkeri. Über den Euklidischen Algorithmus in quadratischen Zahlkörpern. *Annales Academiæ Scientiarum Fennicæ. Series A I. Mathematica–Physica*, tome 41 : pages 1–35, 1947.

[JQS85] David H. Johnson, Clifford S. Queen & Alicia N. Sevilla. Euclidean real quadratic number fields. *Archiv der Mathematik*, tome 44 : pages 340–347, 1985.

[KV10] Markus Kirschmer & John Voight. Algorithmic enumeration of ideal classes for quaternion orders. *SIAM Journal on Computing (SICOMP)*, tome 39 (5) : pages 1714–1747, 2010.

[Lem89] Franz Lemmermeyer. *Euklidische Ringe*. Diplomarbeit, Fakultät für Mathematik, Universität Heidelberg, Août 1989.

[Lem95] Franz Lemmermeyer. The Euclidean algorithm in algebraic number fields. *Expositiones Mathematicae*, tome 13 : pages 385–416, 1995. Version mise à jour disponible à l'adresse `http://www.rzuser.uni-heidelberg.de/~hb3/publ/survey.pdf`.

[Lem00] Franz Lemmermeyer. *Reciprocity laws*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2000. From Euler to Eisenstein.

[Len73] Hendrik W. Lenstra, Jr. De kleinste algoritme van enkele euclidische ringen, 1973. Universiteit van Amsterdam, `http://www.math.leidenuniv.nl/~hwl/PUBLICATIONS/doctoraal/art.pdf`.

[Len76] Hendrik W. Lenstra, Jr. Euclidean number fields of large degree. *Inventiones Mathematicae*, tome 38 (3) : pages 237–254, 1976.

[Len78a] Hendrik W. Lenstra, Jr. Euclidean ideal classes. *I.H.É.S.*, 1978. 32 pages, `http://www.math.leidenuniv.nl/~hwl/PUBLICATIONS/1978b/art.pdf`.

[Len78b] Hendrik W. Lenstra, Jr. Quelques exemples d'anneaux euclidiens. *Comptes Rendus de l'Académie des Sciences de Paris*, tome 286 : pages 683–685, 1978.

[Len79] Hendrik W. Lenstra, Jr. Euclidean number fields 1. *The Mathematical Intelligencer*, tome 2 : pages 6–15, 1979.

[Len80] Hendrik W. Lenstra, Jr. Euclidean number fields 2. *The Mathematical Intelligencer*, tome 2 : pages 73–77, 1980.

[Lez12a] Pierre Lezowski. Computation of the Euclidean minimum of algebraic number fields, 2012. À paraître dans *Mathematics of Computation*.

[Lez12b] Pierre Lezowski. Examples of norm-Euclidean ideal classes. *International Journal of Number Theory*, tome 8 (5), 2012.

[Lez12c] Pierre Lezowski. Programme *euclid*, version `1.0`, 2012. Disponible à l'adresse `http://www.math.u-bordeaux1.fr/~lezowski/euclid/`.

[Lin84] Franciscus Jozef van der Linden. *Euclidean rings with two infinite primes*. Thèse de doctorat, Centrum voor Wiskunde en Informatica, Amsterdam, 1984.

[Mat00] Keith Matthews. The Diophantine equation $x^2 - Dy^2 = N$, $D > 1$, in integers. *Expositiones Mathematicae*, tome 18 : pages 323–331, 2000.

[Mol01] Richard Mollin. Simple continued fraction solutions for Diophantine equations. *Expositiones Mathematicae*, tome 19 : pages 55–73, 2001.

[Mot49] Theodore Motzkin. The Euclidean algorithm. *Bulletin of the American Mathematical Society*, tome 55 : pages 1142–1146, 1949.

[Nar74] Władysław Narkiewicz. *Elementary and analytic theory of algebraic numbers*, tome 57 de *Monografie Matematyczne*. Państwowe Wydawnictwo Naukowe, 1974.

[Par75] Charles J. Parry. Pure quartic number fields whose class numbers are even. *Journal für die reine und angewandte Mathematik*, tome 272 : pages 102–112, 1975.

[PAR12] The PARI Group, Bordeaux. *PARI/GP, version* `2.6.0`, 2012. Disponible à l'adresse `http://pari.math.u-bordeaux.fr/`.

[Per97] Daniel Perrin. *Cours d'algèbre*. Ellipses, 1997.

[Rei75] Irving Reiner. *Maximal Orders*, tome 5 de *L.M.S. Monographs*. Academic Press, 1975.

[Sam71] Pierre Samuel. About Euclidean Rings. *Journal of Algebra*, tome 19 : pages 282–301, 1971.

[Ste73] Hans-Joachim Stender. Grundeinheiten für einige unendliche Klassen reiner biquadratischer Zahlkörper mit einer Anwendung auf die diophantische Gleichung $x^4 - ay^4 = \pm c$ ($c = 1,\ 2,\ 4$ oder 8). *Journal für die Reine und Angewandte Mathematik*, tome 264 : pages 207–220, 1973.

[SW12] Uri Shapira & Zhiren Wang. Remarks on Euclidean Minima, 2012. `http://arxiv.org/abs/1207.5101`.

[Tar72] Robert E. Tarjan. Depth-first search and linear graph algorithms. *SIAM Journal on Computing*, tome 1 : pages 146–160, 1972.

[Vas72] Leonid N. Vaserštein. The group SL_2 over Dedekind rings of arithmetic type. *Matematicheskiĭ Sbornik. Novaya Seriya*, tome 89(131) : pages 313–322, 351, 1972.

[Vig80] Marie-France Vignéras. *Arithmétique des algèbres de quaternions*, tome 800 de *Lecture Notes in Mathematics*. Springer, 1980.

[Voi08] John Voight. Enumeration of totally real number fields of bounded root discriminant. Dans *Proceedings of the 8th international conference on Algorithmic number theory (ANTS VIII)*, pages 268–281. Springer Verlag, 2008.

[Wei73] Peter J. Weinberger. On Euclidean rings of algebraic integers. Dans *Proceedings of the Symposium on Pure Mathematics*, tome 24, pages 321–332. 1973.

Résumé

Nous étudions l'euclidianité des corps de nombres pour la norme et quelques unes de ses généralisations. Nous donnons en particulier un algorithme qui calcule le minimum euclidien d'un corps de nombres de signature quelconque. Cela nous permet de prouver que de nombreux corps sont euclidiens ou non pour la norme. Ensuite, nous appliquons cet algorithme à l'étude des classes euclidiennes pour la norme, ce qui permet d'obtenir de nouveaux exemples de corps de nombres avec une classe euclidienne non principale. Par ailleurs, nous déterminons tous les corps cubiques purs avec une classe euclidienne pour la norme. Enfin, nous nous intéressons aux corps de quaternions euclidiens. Après avoir énoncé les propriétés de base, nous étudions quelques cas particuliers. Nous donnons notamment la liste complète des corps de quaternions euclidiens et totalement définis sur un corps de nombres de degré au plus deux.

Mots-clés : corps de nombres, minimum euclidien, minimum inhomogène, classes euclidiennes, corps de quaternions, théorie algorithmique des nombres.

⋆ ⋆ ⋆

Abstract

We study norm-Euclideanity of number fields and some of its generalizations. In particular, we provide an algorithm to compute the Euclidean minimum of a number field of any signature. This allows us to study the norm-Euclideanity of many number fields. Then, we extend this algorithm to deal with norm-Euclidean classes and we obtain new examples of number fields with a non-principal norm-Euclidean class. Besides, we describe the complete list of pure cubic number fields admitting a norm-Euclidean class. Finally, we study the Euclidean property in quaternion fields. First, we establish its basic properties, then we study some examples. We provide the complete list of Euclidean quaternion fields, which are totally definite over a number field with degree at most two.

Keywords : number fields, Euclidean minimum, inhomogeneous minimum, Euclidean classes, quaternion field, algorithmic number theory.