Département de formation doctorale en mathématiques **École doctorale IAEM Lorraine**
UFR STMIA

Spectres euclidiens et inhomogènes des corps de nombres

THÈSE

présentée et soutenue publiquement le 18 novembre 2005

pour l'obtention du

Doctorat de l'université Henri Poincaré – Nancy 1

(spécialité Mathématiques Pures)

par

Jean-Paul Cerri

Composition du jury

Président :	Paul Zimmermann	Directeur de Recherche INRIA, LORIA
Rapporteurs :	Eva Bayer Fluckiger	Professeur, École Polytechnique Fédérale de Lausanne
	Karim Belabas	Professeur, Laboratoire A2X - Université Bordeaux I
Examinateurs :	Christine Bachoc	Professeur, Laboratoire A2X - Université Bordeaux I
	Karim Belabas	Professeur, Laboratoire A2X - Université Bordeaux I
	Guillaume Hanrot	Chargé de Recherche INRIA, LORIA
	Gérald Tenenbaum	Professeur, Institut Élie Cartan - UHP Nancy I

Institut Élie Cartan de Nancy — UMR 7502

Mis en page avec la classe thloria.

Remerciements

Je tiens à remercier en premier lieu Guillaume Hanrot, mon directeur de thèse, pour avoir accepté d'encadrer mon travail, et pour m'avoir laissé libre de choisir l'orientation de mes recherches. Pendant ces trois années, il aura su m'encourager et me faire profiter de sa grande culture mathématique et algorithmique. Sa hauteur de vue a été pour moi un bain de jouvence, et chacune de nos rencontres, même brève, a toujours été un moment particulièrement roboratif.

Je voudrais également adresser mes remerciements à Christine Bachoc, qui a bien voulu, dans un premier temps, partager à distance avec Guillaume Hanrot la tâche d'encadrant. Je lui suis reconnaissant, en particulier, de m'avoir invité à plusieurs reprises et de m'avoir réservé un accueil chaleureux à chacun de mes déplacements à Bordeaux. Je la remercie aussi pour nos conversations, l'acuité de son jugement et l'intérêt qu'elle a manifesté pour mon travail.

De même, je remercie Gérald Tenenbaum qui a accepté, par la suite, d'assumer la fonction de co-encadrant. Je regrette de ne pas avoir pu vraiment participer à l'équipe qu'il dirige, du fait de mes obligations professionnelles, et cette remarque vaut également pour le groupe Spaces dont je n'aurai partagé, à regret, que quelques moments joyeux mais fugaces.

Par ordre chronologique, je remercie Harvey Cohn, pour l'intérêt qu'il a manifesté à l'endroit de mes premiers bricolages et la gentillesse avec laquelle il a toujours répondu à mes courriers, Georges Gras pour m'avoir incité à «reprendre» des études et m'avoir offert la possibilité de passer mon DEA par correspondance, Marie-Christine Haton pour m'avoir encouragé à entreprendre une thèse à Nancy, et Joël Rivat qui a bien voulu se pencher sur mon cas et me mettre en relation avec Guillaume Hanrot.

Je suis également redevable à Eva Bayer Fluckiger de s'être intéressée à moi. Sa disponibilité, son ouverture d'esprit et sa bonne humeur sont autant de qualités qui m'auront marqué. Je la remercie aussi pour son invitation à venir passer quelque temps à Lausanne, et je souhaite que notre future collaboration soit des plus fructueuses.

Parmi les mathématiciens avec lesquels j'ai échangé électroniquement, j'adresse mes remerciements à Hendrik Lenstra Jr., Jesse Deutsch et Franz Lemmermeyer.

Merci à Eva Bayer Fluckiger et à Karim Belabas, d'avoir bien voulu se charger de la lourde tâche de rapporteurs, tâche dont ils se sont acquittés scrupuleusement. La lecture minutieuse qu'ils ont faite de ce mémoire, m'a permis d'en améliorer la rédaction.

Merci à Christine Bachoc et Karim Belabas, qui ont spontanément accepté de faire partie du jury, malgré la distance et leurs emplois du temps chargés.

Merci à Gérald Tenenbaum et à Paul Zimmermann, qui ont bien voulu représenter la recherche nancéienne dans le jury. Je leur suis également reconnaissant des invitations à exposer qu'ils m'ont faites par le passé.

Enfin, je tiens à citer les proches et amis qui m'ont soutenu, Christine bien sûr, Jean-Christophe, Anne, Phiphi, Jacqueline Euriat et ma famille.

Mais comment Ismaël ? Comment se fait-il que vous, simple canotier, ayez la prétention de savoir quoi que ce soit du monde intérieur de la baleine ? L'érudit Stubb, perché sur le cabestan, vous aurait-il fait des cours sur l'anatomie des cétacés ? Vous aurait-il viré une côte au guindeau pour ses démonstrations ? Explique-toi Ismaël. Pouvez-vous disposer sur le pont un cachalot adulte pour l'étudier, comme un cuisinier met un rôti de porc sur un plat ? Sûrement pas. Jusqu'ici, Ismaël, vous vous êtes montré un témoin authentique, mais prenez garde à présent de ne pas vous octroyer le privilège du seul Jonas, celui de discourir de poutres, de solives, de chevrons, de faîtage, de lambourdes, de chevillages, composant la charpente du léviathan, ainsi que des tonneaux de graisse, des laiteries, des beurreries et des fromageries de ses entrailles.

Hermann Melville, *Moby Dick.*[1]

À mes parents et à mon épouse.

[1] traduit de l'américain par Henriette Guex-Rolle.

Table des matières

Liste des figures

Liste des tableaux

Introduction

Les notions que nous allons aborder peuvent être considérées comme des raffinements de la notion de corps de nombres euclidien pour la norme. Pour comprendre ce que nous entendons par là, un rapide survol historique est sans doute nécessaire.

Corps de nombres euclidien

Soit K un corps de nombres c'est-à-dire une extension finie du corps des rationnels $\mathbb{Q}$. Dans ce qui suit nous appellerons stathme pour K, une fonction f définie sur l'anneau $\mathbb{Z}_K$ des entiers de K, à valeurs dans $\mathbb{N}$, et ne s'annulant qu'en 0. Si f vérifie

$$\text{(1)} \qquad \text{Pour tout } (\alpha, \beta) \in \mathbb{Z}_K \times \mathbb{Z}_K \backslash \{0\}, \text{ il existe } \gamma \in \mathbb{Z}_K \text{ tel que } f(\alpha - \beta\gamma) < f(\beta),$$

on dit que f est un stathme euclidien pour K ou encore que K est euclidien pour f.

Le premier exemple connu d'un tel corps est bien entendu $\mathbb{Q}$ (Euclide) et le stathme f naturellement associé est la valeur absolue.

L'intérêt que présentent les corps euclidiens réside dans le fait que leurs anneaux d'entiers sont principaux donc factoriels. C'est pourquoi cette notion a vu apparaître ses premiers développements au dix-neuvième siècle, en France, dans la perspective de la preuve du théorème de Fermat-Wiles, et en Allemagne, dans le cadre des recherches sur la généralisation de la loi de réciprocité quadratique de Gauss. Plus précisément, dans le but de prouver que les anneaux d'entiers de certains corps cyclotomiques $K_n = \mathbb{Q}(\zeta_n)$ (où ζ_n est une racine primitive n-ième de l'unité) étaient factoriels, des mathématiciens ont cherché à transposer l'algorithme de la division euclidienne à ces anneaux, en choisissant comme stathme f associé la norme $N_{K_n/\mathbb{Q}}$.

Notons que l'euclidianité pour la norme d'un corps K s'écrit encore

$$\text{(2)} \qquad \text{pour tout } \xi \in K, \text{ il existe } \Upsilon \in \mathbb{Z}_K \text{ tel que } |N_{K/\mathbb{Q}}(\xi - \Upsilon)| < 1.$$

Ceci est une conséquence immédiate du caractère multiplicatif de $N_{K/\mathbb{Q}}$.

Corps cyclotomiques euclidiens pour la norme

Du côté français, l'idée de systématiser le procédé semble avoir été initiée par Wantzel (1847), qui démontra que K_n était euclidien pour la norme, quand $n = 3$ et 4, mais passa quelque peu hâtivement au cas général. Cauchy qui fut le premier à souligner que l'argumentation de Wantzel était incorrecte, se pencha à son tour sur le problème et parvint à « démontrer » l'euclidianité pour la norme de K_n dans les cas $n = 3$, 4, 5, 7, 9, 12, 15. Il échoua dans une tentative de généralisation, et finit par trouver, à la lueur des travaux de Kummer, un contre-exemple, avec le cas $n = 23$, pour lequel K_n n'est pas factoriel.

De fait, le problème n'était pas inconnu outre-Rhin. Gauss et Dirichlet avaient établi l'euclidianité de K_n pour $n = 4$ bien avant Wantzel. Le cas $n = 3$ semblait également connu et l'école allemande avait continué de chercher dans la même direction, quelques années avant les français, lorsque suite aux travaux de Gauss (1832) et Jacobi (1836), elle avait tenté de répondre à la question suivante : pour quelles valeurs de n, l'assertion suivante

$$\text{(3)} \qquad \text{Pour tout premier } p \equiv 1 \bmod n, \quad \text{il existe } \gamma \in \mathbb{Z}_{K_n} \text{ tel que } N_{K_n/\mathbb{Q}}(\gamma) = p,$$

est-elle vraie ?

Même si Jacobi puis Eisenstein pressentirent que cette propriété était équivalente à la factorialité de $\mathbb{Z}_{K_n}$, le premier à avoir établi l'équivalence et à avoir trouvé un contre-exemple à (3) - probablement suggéré d'ailleurs par Jacobi - fut Kummer (1847). Mais avant cela, il s'était appuyé sur le fait que la factorialité était suffisante pour trouver des valeurs de n vérifiant (3), et pour prouver cette dernière, s'était, tout comme Wantzel, ramené à l'euclidianité de K_n pour la norme. La technique utilisée (inégalité arithmético-géométrique) lui permit d'établir que K_n est euclidien pour la norme si $n = 5$ (lettre à Kronecker, 1844), et une légère amélioration de sa méthode mène à la même conclusion pour $n = 7$ et 11.

On sait aujourd'hui, depuis les travaux de Masley et Montgomery [Ma75], qu'il n'y a que 30 corps K_n distincts principaux (ou factoriels, les deux notions étant équivalentes dans le cas des anneaux d'entiers de corps de nombres). Ils correspondent aux valeurs suivantes de n : 1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84.

En revanche, on ne connaît le caractère euclidien pour la norme que de 15 de ces 30 corps : pour $n = 1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 20, 24$, K_n est euclidien pour la norme, pour $n = 32$, K_n n'est pas euclidien pour la norme.

Pour plus de détails, voir [Len79] (qui met l'accent sur l'aspect historique et dont les précédentes lignes sont largement inspirées), ainsi que [Len75] et [Ak95] (pour l'aspect théorique).

Corps quadratiques euclidiens pour la norme

Les premiers corps quadratiques à avoir attiré l'attention furent les corps complexes $\mathbb{Q}(\sqrt{-1}) = K_4$ et $\mathbb{Q}(\sqrt{-3}) = K_3 = K_6$ pour les raisons évoquées plus haut (Gauss, Dirichlet, Wantzel et Cauchy).

En fait, le cas des corps quadratiques complexes est un cas facile qui peut se traiter par des arguments géométriques simples, et il semblerait qu'un résultat donnant la réponse à la question de la détermination des $\mathbb{Q}(\sqrt{-m})$ euclidiens pour la norme, ait été développé par Dirichlet en 1842. La réponse : il n'y en a que 5, correspondant à $m = 1, 2, 3, 7$ et 11. Pour plus de détails voir section 1.3.2.

Les choses se compliquent singulièrement dès que l'on s'intéresse aux corps quadratiques réels. Il aura fallu plus d'un siècle (de Wantzel, 1848 à Barnes et Swinnerton-Dyer, 1952) pour que, suite aux efforts conjugués de nombreux mathématiciens, on parvienne à dresser la liste complète des corps quadratiques réels euclidiens pour la norme. Ce sont les $\mathbb{Q}(\sqrt{m})$ pour $m = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57$ et 73. On pourrait citer beaucoup de mathématiciens qui se sont investis dans ce problème, en particulier Oppenheim, Rédei, Erdös, Heilbronn, Davenport, Barnes, Swinnerton-Dyer.

Ici, contrairement à ce qui se passe avec les corps cyclotomiques, si le problème de l'euclidianité pour la norme est complètement résolu, le problème de la principalité est encore largement ouvert.

Au cours de ces années de recherche, de nombreux outils furent développés qui vinrent enrichir la panoplie des théoriciens des nombres, en particulier la géométrie des nombres. C'est cette théorie qui a donné naissance à certaines des techniques les plus efficaces du domaine qui nous occupe, et à un concept qui jouera un rôle central dans notre travail, celui de minimum inhomogène.

Les notions de minima euclidien et inhomogène

Si l'on cherche à préciser la notion d'euclidianité pour la norme, on est naturellement amené à définir le minimum euclidien de K, noté $M(K)$, par

$$M(K) = \inf\{\kappa > 0;\ \forall \xi \in K,\ \exists \Upsilon \in \mathbb{Z}_K \text{ tel que } |N_{K/\mathbb{Q}}(\xi - \Upsilon)| < \kappa\}. \tag{4}$$

Il est facile de voir que si $M(K) < 1$, K est euclidien pour la norme et que si $M(K) > 1$, il ne l'est pas. En revanche, lorsque $M(K) = 1$, on ne sait rien a priori du caractère euclidien de K. Toutefois, nous verrons que les résultats établis dans cette thèse permettront de dire que dans ce cas, le corps K n'est pas euclidien pour la norme, dès lors que son groupe des unités est de rang strictement supérieur à 1. La détermination exacte de $M(K)$ dans le cas quadratique réel et la recherche dans le cas général de majorations de $M(K)$ ne dépendant que du discriminant D_K de K ont occupé de nombreux mathématiciens, notamment pendant la première partie du vingtième siècle. Parmi les nombreuses approches développées, les méthodes géométriques, comme nous l'avons déjà dit, se sont montrées particulièrement fructueuses et ont permis de définir un autre invariant fondamental de K, son minimum inhomogène $M(\overline{K})$. Sans entrer dans les détails, $M(\overline{K})$ est défini de la même manière que $M(K)$, à la nuance près que l'on ne travaille plus sur K mais sur $K \otimes_{\mathbb{Q}} \mathbb{R}$. En fait, il s'agit d'un cas particulier de la notion purement géométrique de minimum inhomogène $M(\mathcal{R})$ associé à un réseau $\mathcal{R}$ de $\mathbb{R}^n$ (pour une fonction spécifique). Dans ce cas particulier, le réseau $\mathcal{R}$ correspond à $\mathbb{Z}_K$ (et la fonction spécifique à l'extension de la norme à $K \otimes_{\mathbb{Q}} \mathbb{R}$). Or $M(K) \leq M(\overline{K})$, et il s'avère que dans tous les cas connus $M(\overline{K})$ est atteint par un élément de K ce qui donne $M(K) = M(\overline{K})$.

Une des conjectures les plus fameuses concernant $M(\overline{K})$ est un cas particulier de la conjecture suivante attribuée à Minkowski.

Conjecture. *Pour tout réseau $\mathcal{R}$ de $\mathbb{R}^n$, de volume $v(\mathcal{R})$, le minimum inhomogène $M(\mathcal{R})$*

associé à la fonction produit des coordonnées, vérifie

$$M(\mathcal{R}) \leq \frac{v(\mathcal{R})}{2^n}.$$

Dans le cas des corps de nombres K totalement réels, elle se traduit par

$$M(\overline{K}) \leq \frac{\sqrt{|D_K|}}{2^n},$$

où n et D_K sont respectivement le degré et le discriminant absolu de K. Dans le cas des corps de nombres complexes (i.e. en termes géométriques, pour d'autres fonctions que le produit des coordonnées), il n'y a pas, à notre connaissance, de conjecture du même type, qui mette en relation $M(\overline{K})$ et D_K.

La conjecture de Minkowski a été établie pour $n \leq 6$ et le cas $n = 6$ fait l'objet d'un bel article de McMullen [McM04], qui synthétise les approches précédentes. Dans le cas des corps de nombres, citons également le récent résultat de Bayer Fluckiger [Ba04] qui établit la conjecture pour les sous-corps réels maximaux $\mathbb{Q}(\zeta_{p^k} + \zeta_{p^k}^{-1})$ des corps cyclotomiques $\mathbb{Q}(\zeta_{p^k})$, où ζ_{p^k} est une racine primitive p^k-ième de l'unité, et p un premier impair. Elle établit également que pour tout corps cyclotomique $\mathbb{Q}(\zeta_n)$ on a

$$M(\overline{\mathbb{Q}(\zeta_n)}) \leq \frac{1}{2^n}\sqrt{|D_{\mathbb{Q}(\zeta_n)}|}.$$

Signalons que ce sont des arguments géométriques qui ont également permis à Lenstra [Len77a] de trouver un critère, lié à la taille des familles d'unités exceptionnelles d'un corps de nombres K, permettant d'établir $M(\overline{K}) < 1$, dans des dimensions supérieures à celles qui avaient été explorées jusque là. Cependant, même si sa méthode a permis de trouver de nombreux corps de nombres euclidiens pour la norme, elle ne concerne en rien la détermination explicite de $M(\overline{K})$. Le critère de Lenstra s'énonce ainsi. Soit K un corps de nombres de degré n, de discriminant D_K et de signature (r_1, r_2). S'il existe k unités de E_K (groupe des unités de K), notées ε_i $(1 \leq i \leq k)$, telles que

$$\text{pour tout } i \text{ et tout } j \neq i,\ \varepsilon_i - \varepsilon_j \in E_K,$$

et si

$$k > \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|D_K|},$$

alors K est euclidien pour la norme.

Le recours à $M(\overline{K})$, pour naturel qu'il soit, ne va pas sans poser de nombreuses questions, à commencer par celle de la comparaison à $M(K)$. A-t-on $M(\overline{K}) = M(K)$ pour tout corps de nombres ? Plus ambitieusement, $M(\overline{K})$ est-il toujours atteint par un $\xi \in \mathbb{Z}_K$? Jusque-là, on ne pouvait répondre à la première question que si le groupe des unités de K est de rang r inférieur ou égal à 1, et pour certains cas particuliers en dimension supérieure, par l'affirmative. Quant à la seconde, elle ne faisait que l'objet d'une conjecture dans le cas quadratique réel. D'autres problèmes plus fins, relatifs aux spectres euclidiens et inhomogènes peuvent également été soulevés, auxquels aucune réponse générale n'a été apportée, même si certains cas particuliers sont assez bien connus.

Autres résultats

Signalons, pour terminer avec l'euclidianité pour la norme, quelques résultats généraux remarquables. Tout d'abord, comme dans le cas quadratique complexe, on sait qu'il n'existe qu'un nombre fini de corps cubiques complexes euclidiens pour la norme [Da50a]. Pour ces derniers corps Cassels [Ca52] a établi l'inégalité

$$M(\overline{K}) \geq \frac{\sqrt{|D_K|}}{420}.$$

Ainsi, si K cubique complexe est euclidien pour la norme on doit avoir

$$|D_K| \leq 176400.$$

De même il n'y a qu'un nombre fini de corps quartiques totalement complexes euclidiens pour la norme (voir [Da50b] et [Ca52]), ce qui prouve qu'il n'y a qu'un nombre fini de corps de nombres dont le rang du groupe des unités est inférieur ou égal à 1, euclidiens pour la norme. Pour les corps quartiques totalement complexes, Cassels avait aussi établi une inégalité du type précédent, mais une erreur s'était glissée dans ses calculs. Finalement Van der Linden [VdL83] a corrigé la borne et établi que si K quartique totalement complexe est euclidien pour la norme, alors $|D_K| \leq 230202117$.

De plus il a prouvé qu'il n'y avait que deux corps quartiques totalement complexes cycliques et euclidiens pour la norme, à savoir $\mathbb{Q}(\zeta_5)$ et $\mathbb{Q}(\zeta_{13} + {\zeta_{13}}^3 + {\zeta_{13}}^9)$, où ζ_5 et ζ_{13} sont respectivement une racine primitive cinquième et une racine primitive treizième de l'unité.

Dans le même registre, Heilbronn [He50a] a établi qu'il n'y a qu'un nombre fini de corps cubiques cycliques euclidiens pour la norme, et a conjecturé qu'il existait une infinité de corps cubiques totalement réels euclidiens pour la norme.

Généralisations

Euclidianité pour d'autres stathmes

Il convient d'évoquer maintenant les développements de la théorie de l'euclidianité des corps de nombres pour d'autres stathmes que la norme, et en particulier le lien qui existe entre euclidianité et principalité.

On sait que l'euclidianité entraîne la principalité, mais qu'en est-il de la réciproque ? Si des corps de nombres sont non euclidiens pour la norme, ils peuvent être néanmoins principaux. Dans le cas quadratique complexe $\mathbb{Q}(\sqrt{-m})$, on connaît tous les corps principaux [St67]. Ils correspondent à $m = 1,\ 2,\ 3,\ 7,\ 11,\ 19,\ 43,\ 67$ et 163. Par conséquent on connaît tous les corps principaux non euclidiens pour la norme, à savoir ceux qui sont définis par $m = 19,\ 43,\ 67$ et 163. Dans le cas quadratique réel l'exemple le plus connu est sans conteste $K = \mathbb{Q}(\sqrt{14})$. Plus généralement, si $K = \mathbb{Q}(\sqrt{m})$ (où m est sans facteur carré et $m < 100$) on trouve les corps définis par $m = 14$, 22, 23, 31, 38, 43, 46, 47, 53, 59, 61, 62, 67, 69, 71, 77, 83, 86, 89, 93, 94, et 97, et si la conjecture de Gauss est valable, il y aurait une infinité de corps quadratiques réels principaux, non euclidiens pour la norme. Dans le cas cubique, Clark [Cl96a] a exhibé quelques exemples.

La question qui se pose alors est : étant donné un corps de nombres K, principal mais non euclidien pour la norme, existe-t-il un stathme f pour lequel K est euclidien ?

Une importante caractérisation de l'euclidianité en général a été donnée par Motzkin [Mo49]. Posons $E_0 = \{0\}$, et définissons par récurrence une suite de parties E_i de $\mathbb{Z}_K$ de la façon suivante : les E_j, $0 \leq j \leq i$ étant donnés, E_{i+1} est la réunion de E_i et de l'ensemble des $\Upsilon \in \mathbb{Z}_K \backslash \{0\}$ tels que toute classe résiduelle modulo $\Upsilon \mathbb{Z}_K$ a un représentant dans E_i. Par exemple $E_1 = \{0\} \cup E_K$. On a alors

$$K \text{ est euclidien } \iff \mathbb{Z}_K = \bigcup_{i=0}^{\infty} E_i. \tag{5}$$

Et si l'égalité de droite est vérifiée, un stathme euclidien de K est donné par

$$f(\Upsilon) = \min\{i; \Upsilon \in E_i\}.$$

Motzkin utilisa ce critère pour l'étude des corps quadratiques complexes. Et de fait, on peut établir, par l'argument de Motzkin, que $\mathbb{Q}(\sqrt{-19})$ n'est pas euclidien. En effet, les seules unités sont 1 et -1, et tout idéal non trivial étant de norme supérieure à 4, on a $E_i = E_1 = \{-1, 0, 1\}$ pour tout $i \geq 1$. Cet argument est encore valable pour tous les corps quadratiques complexes principaux et non euclidiens pour la norme, si bien que, dans le cas quadratique complexe, les corps euclidiens sont exactement ceux qui sont euclidiens pour la norme.

Plus tard, Samuel [Sa71] se pencha sur ce critère dans le but de prouver que certains corps de nombres principaux étaient euclidiens. Une cible désignée fut $\mathbb{Q}(\sqrt{14})$ et la nature des calculs effectués menèrent Samuel à établir une connexion entre le critère de Motzkin et une généralisation de la conjecture d'Artin concernant la répartition des nombres premiers p tels qu'un entier donné soit racine primitive modulo p.

Partant du lien découvert par Samuel, Weinberger [We73] parvint à établir que, sous l'hypothèse de Riemann généralisée (GRH), si un corps de nombres a un groupe des unités de rang r supérieur ou égal à 1 (c'est-à-dire $K \neq \mathbb{Q}$ et K non quadratique complexe), et s'il est principal, alors il est euclidien. Ceci prouve donc que (sous GRH) $\mathbb{Q}(\sqrt{14})$ est euclidien.

D'autres travaux suivirent. Lenstra étendit le résultat de Weinberger aux corps globaux [Len77b], précisa celui-ci dans le cas des corps de nombres, et de nombreuses tentatives furent menées pour s'affranchir de l'hypothèse de Riemann. Les plus remarquables sont dues à Gupta, Kumar Murty et Ram Murty [GMM87], Clark et Ram Murty [ClM95], Harper [Ha00], Harper et Ram Murty [HaM03]. En particulier, Harper parvint à prouver que $\mathbb{Q}(\sqrt{14})$ est effectivement euclidien et que tous les corps cyclotomiques principaux, dont la liste a été donnée page 2, sont euclidiens. Harper et Ram Murty ont également établi que si K est une extension galoisienne de $\mathbb{Q}$ de degré n, dont le rang du groupe des unités r vérifie $r > 3$ (condition assurée dès que $n > 8$), K est euclidien si et seulement s'il est principal.

En dehors de ces résultats généraux, il est intéressant de signaler une méthode effective de construction de stathmes adaptés, due à Lenstra [Len74]. Il s'agit des normes dites pondérées et définies de la façon suivante. On considère un corps de nombres K principal, on choisit un idéal premier $\mathfrak{p}$ de $\mathbb{Z}_K$, un réel positif c et on pose $\phi(\mathfrak{p}) = c$ et $\phi(\mathfrak{q}) = \mathrm{N}(\mathfrak{q})$ pour tout idéal premier $\mathfrak{q}$ de $\mathbb{Z}_K$ distinct de $\mathfrak{p}$, où N désigne la fonction norme des idéaux. On étend ensuite multiplicativement ϕ aux idéaux fractionnaires de $\mathbb{Z}_K$, et on pose enfin $f(\alpha) = \phi(\alpha\mathbb{Z}_K)$, pour tout $\alpha \in K$ non nul et $f(0) = 0$. La fonction f est alors une fonction multiplicative de K dans $\mathbb{R}$.

Elle n'a pas tout à fait la forme donnée initialement pour les stathmes, car ses valeurs ne sont pas forcément entières. Toutefois, il n'est pas difficile de voir que si pour tout $k > 0$, l'ensemble des $\alpha \in \mathbb{Z}_K$ vérifiant $f(\alpha) < k$ est fini, ce qui est le cas dès que $c > 1$, et si f vérifie (1), K est euclidien pour un stathme bien choisi.

Reste à choisir $\mathfrak{p}$ et c pour que f vérifie (1). Par exemple, pour $K = \mathbb{Q}(\sqrt{69})$, qui n'est pas euclidien pour la norme bien que principal, si on prend $\mathfrak{p} = (23, \sqrt{69}) = \big((23 + 3\sqrt{69})/2\big)$ et c quelconque strictement supérieur à 25, f vérifie (1) et K est euclidien (voir [CaL00]). Le premier à avoir établi ce résultat fut Clark [Cl94], donnant ainsi le premier exemple de corps de nombres quadratique, euclidien bien que non euclidien pour la norme.

Corps de nombres euclidiens en m étapes (m-stage Euclidean number fields)

Une autre généralisation de la notion d'euclidianité pour la norme s'appuie sur le concept d'euclidianité en plusieurs étapes. Soient K un corps de nombres et m un entier non nul. On dit que K est euclidien en m étapes (implicitement pour la norme) si pour tout α de $\mathbb{Z}_K$ et tout β de $\mathbb{Z}_K\backslash\{0\}$ il existe un entier non nul $k \leq m$ et k couples (q_i, r_i) $(1 \leq i \leq k)$ d'éléments de $\mathbb{Z}_K$ tels que

$$\begin{array}{rcl} \alpha & = & \beta q_1 + r_1 \\ \beta & = & r_1 q_2 + r_2 \\ & \vdots & \\ r_{k-2} & = & r_{k-1} q_k + r_k \end{array} \tag{6}$$

$$\text{et } |N_{K/\mathbb{Q}}(r_k)| < |N_{K/\mathbb{Q}}(\beta)|.$$

Ainsi un corps euclidien en 1 étape est un corps euclidien pour la norme, et l'euclidianité en m étapes implique l'euclidianité en m' étapes dès que $m' \geq m$.

Il est possible de formuler cette définition autrement à l'aide des fractions continues. Si $q_1, q_2, \ldots, q_k$ sont k éléments de $\mathbb{Z}_K$ on note, si l'expression est bien définie,

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

où a_k et b_k sont les éléments de $\mathbb{Z}_K$ définis à l'aide des formules

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

Alors, comme

$$\frac{\alpha}{\beta} = \frac{a_k}{b_k} + (-1)^{k+1} \frac{r_k}{b_k \beta},$$

la condition (6) s'écrit : pour tout $\xi \in K$, il existe un entier non nul vérifiant $k \leq m$, et k éléments $q_1, q_2, \ldots, q_k \in \mathbb{Z}_K$ tels que

$$\left| N_{K/\mathbb{Q}}(\xi - [q_1, q_2, \ldots, q_k]) \right| < \frac{1}{|N_{K/\mathbb{Q}}(b_k)|}. \tag{7}$$

Cooke [Co76] a établi que si K est un corps de nombres dont le rang du groupe des unités r est supérieur ou égal à 1, on a l'équivalence

$$K \text{ principal } \iff \text{il existe un entier non nul } m \text{ tel que } K \text{ est euclidien en } m \text{ étapes.}$$

En revanche, pour $r < 1$, les corps de nombres principaux non euclidiens pour la norme $\mathbb{Q}(\sqrt{-19})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$ et $\mathbb{Q}(\sqrt{-163})$ ne sont euclidiens en m étapes pour aucun m (toujours [Co76]), si bien que les seules extensions quadratiques complexes euclidiennes en m étapes sont celles qui sont euclidiennes pour la norme.

Dans le cas quadratique réel, les choses sont différentes : Cooke a montré que pour $m = 14, 22, 23, 31, 38, 43, 46, 53, 61, 69, 89, 93, 97$, $\mathbb{Q}(\sqrt{m})$ est euclidien en 2 étapes.

Par ailleurs Cooke et Weinberger [CoW75] ont établi que, sous GRH, tout corps de nombres principal K dont le rang du groupe des unités est supérieur ou égal à 1, est euclidien en 4 étapes, Lenstra précisant que si K admet au moins un $\mathbb{Q}$-isomorphisme réel, alors, toujours sous GRH, on peut remplacer 4 par 2 (voir note en fin de [CoW75]).

Ici encore quelques tentatives d'affranchissement de l'hypothèse de Riemann ont été effectuées dans le cas galoisien (voir par exemple [Cl96b]).

Cooke dans [Co76] et [Co77] a également développé d'autres notions intéressantes, en particulier celle de corps de nombres euclidien à l'infini ("ω-stage Euclidean") et celle de profondeur euclidienne. Nous ne les aborderons pas ici.

Objectifs de la thèse

Ce rapide et nécessairement partiel tour d'horizon étant effectué, nous en venons aux questions que nous nous sommes posées et que nous avons tenté d'élucider. Pour de plus amples détails sur la très riche théorie des corps de nombres euclidiens et sur les notions précédemment évoquées, nous renvoyons à l'excellente - bien que comportant quelques imprécisions - étude de Lemmermeyer [Lem95], dont une version actualisée est donnée sur [Lem99].

La première question qui nous a préoccupés était relative à une conjecture de Cohn et Deutsch [CD86], selon laquelle, pour $K = \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$ et $L = \mathbb{Q}\left(\sqrt{2+\sqrt{2+\sqrt{2}}}\right)$, on avait

$$M(K) = M(\overline{K}) = \frac{1}{2} \quad \text{et} \quad M(L) < 1.$$

En réponse à cette question, nous avons développé une approche algorithmique [Ce00] qui nous a permis d'établir

$$M(K) = M(\overline{K}) = \frac{1}{2} \quad \text{et} \quad M(L) = M(\overline{L}) = \frac{1}{2}.$$

Il était naturel de chercher alors à généraliser l'approche précédemment développée aux corps de nombres totalement réels. Pouvait-on, algorithmiquement, calculer $M(K)$? En ayant recours au groupe des unités E_K de K, et en cherchant à généraliser aux corps de nombres de degré quelconque les idées que Barnes et Swinnerton-Dyer avaient utilisées dans le cas quadratique, nous y sommes parvenus [Ce04a]. Dans tous les cas observés on avait

$$M(K) = M(\overline{K}) \in \mathbb{Q}. \tag{8}$$

Cette constatation méritait que l'on se penche sur le lien entre $M(K)$ et $M(\overline{K})$. En utilisant des arguments de théorie ergodique et de dynamique topologique, nous avons alors établi [Ce04b] que pour tout corps de nombres K on a

$$M(K) = M(\overline{K}),$$

et que, si le rang de E_K est strictement supérieur à 1, (8) est vérifiée. En outre, nous avons pu répondre à d'autres questions relatives aux spectres euclidien et inhomogène de K.

Cette thèse sera l'occasion de présenter et accessoirement de compléter ces différents résultats. Nous avons plus ou moins adopté l'ordre chronologique de notre travail, avec l'intention en partant du pragmatique pour aller vers l'aspect plus théorique, de rendre compte de l'élargissement de notre questionnement, et de donner à cet écrit une dynamique qu'il n'aurait pas eue, si nous avions procédé autrement.

Plan de la thèse

Dans le premier chapitre, nous redonnons les définitions et les propriétés élémentaires des objets considérés : les fonctions m_K, $m_{\overline{K}}$, les minima $M(K)$, $M(\overline{K})$, les spectres $\mathrm{sp}(K)$ et $\mathrm{sp}(\overline{K})$. Nous y présentons ensuite les différentes questions que l'on est amené à se poser.

Dans le deuxième chapitre, nous établissons quelques propriétés générales. Nous y montrons en particulier comment calculer $m_K(\xi)$ si $\xi \in K$ et généralisons aux corps de nombres quelconques un résultat de Barnes et Swinnerton-Dyer, selon lequel $\mathrm{sp}(\overline{K})$ est fermé dans le cas quadratique réel.

Le troisième chapitre est consacré à l'aspect algorithmique des choses. Si nous y développons essentiellement notre deuxième approche algorithmique (recours aux unités dans le cas totalement réel), nous évoquons rapidement notre première approche et la façon dont il faudrait transformer l'algorithme pour traiter n'importe quel corps de nombres.

Le quatrième chapitre évoque les questions plus théoriques du lien entre $M(K)$ et $M(\overline{K})$ et entre les spectres euclidien et inhomogène de K.

Enfin dans un cinquième chapitre, nous revenons sur le rapport entre euclidianité et principalité, et en particulier sur l'euclidianité en m étapes.

La conclusion dresse le bilan des questions restant à étudier et des orientations de notre recherche à venir.

Les tables des résultats établis par l'algorithme figurent en fin de document.

Chapitre 1

Définitions, propriétés élémentaires

1.1 Notations

Soit n un entier naturel non nul et soit K un corps de nombres de degré $[K:\mathbb{Q}] = n$ et de signature (r_1, r_2). Nous noterons $\mathbb{Z}_K$ l'anneau des entiers de K et D_K son discriminant absolu.
Désignons par σ_i, où $1 \leq i \leq r_1$, les r_1 $\mathbb{Q}$-isomorphismes de K dans $\mathbb{R}$, et par σ_i, $\sigma_{i+r_2} = \overline{\sigma_i}$, où $r_1 + 1 \leq i \leq r_1 + r_2$, les $2r_2$ $\mathbb{Q}$-isomorphismes conjugués deux à deux de K dans $\mathbb{C}$.
Nous identifierons provisoirement le produit $K \otimes_{\mathbb{Q}} \mathbb{R}$ des complétions archimédiennes de K avec $\mathbb{R}^n$, et nous noterons ϕ le plongement de K dans $\mathbb{R}^n$ défini par

$$\phi(\xi) = \left(\sigma_1(\xi), \ldots, \sigma_{r_1}(\xi), \Re\left(\sigma_{r_1+1}(\xi)\right), \Im\left(\sigma_{r_1+1}(\xi)\right), \ldots, \Re\left(\sigma_{r_1+r_2}(\xi)\right), \Im\left(\sigma_{r_1+r_2}(\xi)\right)\right),$$

où $\xi \in K$. Nous serons amenés plus tard à considérer une autre identification, moins usuelle mais plus pratique pour les calculs. Nous en reparlerons le moment venu.
Rappelons que $\phi(\mathbb{Z}_K)$ est un réseau ($\mathbb{Z}$-module libre de rang n) de $\mathbb{R}^n$.
Soit $N_{K/\mathbb{Q}}$ la norme définie sur K par

$$\forall \xi \in K,\ N_{K/\mathbb{Q}}(\xi) = \prod_{i=1}^{n} \sigma_i(\xi) = \prod_{i=1}^{r_1} \sigma_i(\xi) \prod_{i=r_1+1}^{r_1+r_2} \left|\sigma_i(\xi)\right|^2.$$

Soient E_K le groupe des unités de K et $r = r_1 + r_2 - 1$ le rang de E_K. Nous savons par le théorème de Dirichlet que E_K peut être engendré par les racines de l'unité de K et r unités fondamentales. Nous supposerons par la suite que nous disposons d'un tel système d'unités fondamentales noté $(\varepsilon_i)_{1\leq i\leq r}$.
Notons enfin $\mathcal{L}$ le plongement logarithmique de $K\backslash\{0\}$ dans $\mathbb{R}^{r_1+r_2}$ défini par

$$\text{pour tout } \xi \in K\backslash\{0\},\ \mathcal{L}(\xi) = \left(\ln|\sigma_1(\xi)|, \ldots, \ln|\sigma_{r_1+r_2}(\xi)|\right).$$

Avec les notations précédentes, $\mathcal{L}(E_K)$ est un réseau de l'hyperplan de $\mathbb{R}^{r_1+r_2}$ d'équation

$$\sum_{i=1}^{r_1} x_i + 2\sum_{i=r_1+1}^{r_2} x_i = 0.$$

Il admet $(\mathcal{L}(\varepsilon_i))_{1\leq i\leq r}$ comme $\mathbb{Z}$-base, et le noyau de $\mathcal{L}$ est constitué par les racines de l'unité de K.

Avant d'introduire les notions fondamentales qui seront l'objet de notre étude, il est nécessaire de rappeler quelques définitions et propriétés élémentaires de géométrie des nombres, relatives à la fonction minimum inhomogène attachée à un réseau de $\mathbb{R}^n$.

1.2 Fonction minimum inhomogène associée à un réseau de $\mathbb{R}^n$ pour f_{s_1,s_2}

Soit n un entier naturel non nul se décomposant sous la forme $n = s_1 + 2s_2$ où s_1 et s_2 sont deux entiers naturels pouvant être nuls.
Considérons l'application f_{s_1,s_2} de $\mathbb{R}^n$ dans $\mathbb{R}$ définie par

$$\text{pour tout } x = (x_1, \dots, x_n) \in \mathbb{R}^n,\ f_{s_1,s_2}(x) = \prod_{i=1}^{s_1} x_i \prod_{i=1}^{s_2} \left(x_{s_1+2i-1}^2 + x_{s_1+2i}^2\right),$$

où un produit vide est conventionellement égal à 1.

Soit $\mathcal{R}$ un réseau de $\mathbb{R}^n$.

Définition 1.1. Si x est un élément de $\mathbb{R}^n$, on *appelle minimum inhomogène de x par rapport à $\mathcal{R}$ et f_{s_1,s_2}* et on note $m_{\mathcal{R},(s_1,s_2)}(x)$, le réel positif ou nul défini par

$$m_{\mathcal{R},(s_1,s_2)}(x) = \inf\Big\{|f_{s_1,s_2}(x-X)|;\ X \in \mathcal{R}\Big\}.$$

Ainsi, l'application $m_{\mathcal{R},(s_1,s_2)}$ mesure la proximité aux éléments du réseau $\mathcal{R}$, relativement à la fonction $|f_{s_1,s_2}|$.

Théorème 1.2. *L'application $m_{\mathcal{R},(s_1,s_2)}$ a les propriétés fondamentales suivantes.*

i) *Pour tout x de $\mathbb{R}^n$ et tout X de $\mathcal{R}$, $m_{\mathcal{R},(s_1,s_2)}(x-X) = m_{\mathcal{R},(s_1,s_2)}(x)$.*

ii) *$m_{\mathcal{R},(s_1,s_2)}$ est semi-continue supérieurement sur $\mathbb{R}^n$.*

Preuve. Le premier point est une conséquence immédiate de la définition de $m_{\mathcal{R},(s_1,s_2)}$. Quant au second, il découle sans peine de la continuité de f_{s_1,s_2}. En effet, soient x un élément de $\mathbb{R}^n$ et ϵ un réel positif. Par définition de $m_{\mathcal{R},(s_1,s_2)}$, il existe un élément X de $\mathcal{R}$ tel que

$$|f_{s_1,s_2}(x-X)| \leq m_{\mathcal{R},(s_1,s_2)}(x) + \frac{\epsilon}{2}.$$

La fonction f_{s_1,s_2} étant continue, il existe un voisinage V de x, tel que tout y de V vérifie

$$|f_{s_1,s_2}(y-X)| \leq |f_{s_1,s_2}(x-X)| + \frac{\epsilon}{2}.$$

On en déduit que pour tout y de V,

$$m_{\mathcal{R},(s_1,s_2)}(y) \leq |f_{s_1,s_2}(y-X)| \leq m_{\mathcal{R},(s_1,s_2)}(x) + \epsilon.$$

Ceci caractérise la semi-continuité supérieure de $m_{\mathcal{R},(s_1,s_2)}$ sur $\mathbb{R}^n$. $\square$

On voit alors par le Théorème 1.2 i), que $m_{\mathcal{R},(s_1,s_2)}$ étant définie sur $\mathbb{R}^n$ modulo $\mathcal{R}$, elle induit une application $\tilde{m}_{\mathcal{R},(s_1,s_2)}$ sur le quotient $\mathbb{R}^n/\mathcal{R}$ qui est également semi-continue supérieurement. Or ce quotient est compact et, par une propriété générale des fonctions semi-continues sur les compacts, $\tilde{m}_{\mathcal{R},(s_1,s_2)}$ est bornée et atteint sa borne supérieure. On en déduit le corollaire suivant.

Corollaire 1.3. *L'application* $m_{\mathcal{R},(s_1,s_2)}$ *est bornée sur* $\mathbb{R}^n$ *et atteint sa borne supérieure.*

Ceci nous amène à poser les définitions suivantes.

Définition 1.4. On appelle *minimum inhomogène* du réseau $\mathcal{R}$ pour f_{s_1,s_2} et on note $M_{\mathcal{R},(s_1,s_2)}$ le réel positif ou nul défini par

$$M_{\mathcal{R},(s_1,s_2)} = \sup\left\{ m_{\mathcal{R},(s_1,s_2)}(x);\ x \in \mathbb{R}^n \right\} < +\infty.$$

Définition 1.5. Avec les notations précédentes, si un élément x de $\mathbb{R}^n$ vérifie

$$m_{\mathcal{R},(s_1,s_2)}(x) = M_{\mathcal{R},(s_1,s_2)},$$

on dira qu'il est *critique* (relativement à $\mathcal{R}$ et f_{s_1,s_2} s'il est nécessaire de préciser).

Le Corollaire 1.3 montre que de tels points existent. De plus, par le Théorème 1.2 i), si x est critique, tout $x - X$ où $X \in \mathcal{R}$ est critique.
La conjecture de Minkowski évoquée dans l'introduction s'énonce alors comme suit.

Conjecture (Minkowski). *Pour tout réseau* $\mathcal{R}$ *de* $\mathbb{R}^n$*, de volume* $v(\mathcal{R})$

$$M_{\mathcal{R},(n,0)} \leq \frac{v(\mathcal{R})}{2^n}.$$

Enfin la semi-continuité supérieure de $m_{\mathcal{R},(s_1,s_2)}$ et de $\tilde{m}_{\mathcal{R},(s_1,s_2)}$ a l'importante conséquence suivante.

Corollaire 1.6. *Si* $(u_p)_{p\in\mathbb{N}}$ *est une suite d'éléments de* $\mathbb{R}^n$ *convergeant vers un élément* $u \in \mathbb{R}^n$*, alors on a*

$$\limsup_{p\to+\infty} m_{\mathcal{R},(s_1,s_2)}(u_p) \leq m_{\mathcal{R},(s_1,s_2)}(u).$$

De la même manière si $(\alpha_p)_{n\in\mathbb{N}}$ *est une suite d'éléments du quotient* $\mathbb{R}^n/\mathcal{R}$ *convergeant vers un élément* $\alpha \in \mathbb{R}^n/\mathcal{R}$*, alors on a*

$$\limsup_{p\to+\infty} \tilde{m}_{\mathcal{R},(s_1,s_2)}(\alpha_p) \leq \tilde{m}_{\mathcal{R},(s_1,s_2)}(\alpha).$$

Remarque 1.7. Il est facile de voir que tous ces résultats demeurent exacts pour d'autres fonctions que les f_{s_1,s_2}, par exemple pour les fonctions continues à valeurs dans $\mathbb{R}^+$. Cependant nous n'avons pas besoin ici de travailler avec une classe plus large. Le lecteur intéressé pourra consulter [Ca71].

Ces préliminaires étant établis, nous pouvons désormais revenir au corps de nombres K et définir plus précisément les objets de notre étude.

1.3 Fonctions minimum euclidien et minimum inhomogène associées à un corps de nombres

1.3.1 Premières définitions

On a vu que l'anneau des entiers $\mathbb{Z}_K$ de K a pour image par ϕ un réseau de $\mathbb{R}^n$. Aussi est-il possible de s'intéresser à l'application $m_{\phi(\mathbb{Z}_K),(r_1,r_2)}$ et à son maximum $M_{\phi(\mathbb{Z}_K),(r_1,r_2)}$. Pour justifier l'intérêt que présentent ces objets, nous allons rappeler quelques définitions élémentaires concernant le corps K.

Définition 1.8. Le corps de nombres K est dit *euclidien pour la norme* si et seulement s'il vérifie l'une des deux conditions équivalentes suivantes.

- Pour tout (α, β) de $\mathbb{Z}_K \times \mathbb{Z}_K \backslash \{0\}$, il existe un entier $\gamma \in \mathbb{Z}_K$ tel que l'on ait

$$|N_{K/\mathbb{Q}}(\alpha - \beta\gamma)| < |N_{K/\mathbb{Q}}(\beta)|.$$

- Pour tout ξ de K, il existe un entier $\Upsilon \in \mathbb{Z}_K$ tel que

$$|N_{K/\mathbb{Q}}(\xi - \Upsilon)| < 1.$$

Dans la perspective d'établir qu'un corps de nombres K est euclidien pour la norme, il est donc naturel de s'intéresser à l'application suivante.

Définition 1.9. Si ξ est un élément de K on appelle *minimum euclidien* de ξ (implicitement pour la norme), et on note $m_K(\xi)$, le réel positif ou nul défini par

$$m_K(\xi) = \inf \Big\{ |N_{K/\mathbb{Q}}(\xi - \Upsilon)|;\ \Upsilon \in \mathbb{Z}_K \Big\}.$$

Ainsi, K est euclidien pour la norme si et seulement si pour tout ξ de K, on a

$$m_K(\xi) < 1.$$

Proposition 1.10. *L'application m_K a les propriétés suivantes.*

i) *Pour tout ξ de K, tout entier Γ de $\mathbb{Z}_K$ et toute unité ε de E_K on a*

$$m_K(\varepsilon\xi - \Gamma) = m_K(\xi).$$

ii) *Pour tout ξ de K, il existe un entier Υ de $\mathbb{Z}_K$ tel que*

$$m_K(\xi) = |N_{K/\mathbb{Q}}(\xi - \Upsilon)|.$$

iii) *Pour tout ξ de K, $m_K(\xi) \in \mathbb{Q}$. De plus, $m_K(\xi) = 0$ si et seulement si $\xi \in \mathbb{Z}_K$.*

Preuve. Le point i) est une conséquence de la définition de m_K. En effet, par multiplication par $|N_{K/\mathbb{Q}}(\varepsilon)| = 1$, on a

$$m_K(\xi) = \inf\left\{|N_{K/\mathbb{Q}}(\varepsilon\xi - \varepsilon\Upsilon)|;\ \Upsilon \in \mathbb{Z}_K\right\},$$

et comme $\varepsilon\mathbb{Z}_K = \mathbb{Z}_K = \mathbb{Z}_K + \Gamma$ on a l'égalité cherchée.
Soit maintenant ξ un élément de K. On peut écrire

$$\xi = \frac{1}{d}\beta,$$

où $d \in \mathbb{N}^*$ et $\beta \in \mathbb{Z}_K$. On en tire

$$m_K(\xi) = \frac{1}{d^n}\inf\left\{|N_{K/\mathbb{Q}}(\beta - d\Upsilon)|;\ \Upsilon \in \mathbb{Z}_K\right\}.$$

Comme $N_{K/\mathbb{Q}}(\beta - d\Upsilon) \in \mathbb{Z}$, cette borne inférieure est en fait atteinte par un Υ de $\mathbb{Z}_K$, et l'on a

$$m_K(\xi) = \frac{1}{d^n}|N_{K/\mathbb{Q}}(\beta - d\Upsilon)| \in \mathbb{Q}.$$

De plus, cette dernière quantité est nulle si et seulement si $\beta = d\Upsilon$ ou encore $\xi = \Upsilon$. Ceci établit les points ii) et iii). $\square$

En général, ξ de K étant donné, le calcul de $m_K(\xi)$ n'est pas évident, et nous aborderons ce point plus tard en détail. Toutefois un cas particulièrement simple mérite d'être évoqué ici.

Proposition 1.11. *Soit Γ un élément non nul de $\mathbb{Z}_K$. Supposons en outre que Γ ne soit pas une unité. Alors pour tout $\xi \in K$ tel que $\xi \equiv 1/\Gamma \bmod \mathbb{Z}_K$, on a*

$$m_K(\xi) = \frac{1}{|N_{K/\mathbb{Q}}(\Gamma)|}.$$

Preuve. Tout d'abord par la Proposition 1.10.i), on a $m_K(\xi) = m_K(1/\Gamma)$, et par définition de m_K,

$$m_K(\xi) = \frac{1}{|N_{K/\mathbb{Q}}(\Gamma)|}\inf\left\{|N_{K/\mathbb{Q}}(1 - \Gamma\Upsilon)|\,;\ \Upsilon \in \mathbb{Z}_K\right\}.$$

Or, d'une part $N_{K/\mathbb{Q}}(1-\Gamma\Upsilon) \in \mathbb{Z}$, et d'autre part l'égalité $N_{K/\mathbb{Q}}(1-\Gamma\Upsilon) = 0$ n'est possible que si $\Gamma\Upsilon = 1$, ce qui contredit l'hypothèse $\Gamma \notin E_K$. Par conséquent $N_{K/\mathbb{Q}}(1 - \Gamma\Upsilon) \in \mathbb{Z}^*$ et le choix $\Upsilon = 0$ est évidemment optimal, ce qui donne la conclusion. $\square$

Revenons maintenant au lien entre m_K et la fonction minimum inhomogène associée au réseau $\phi(\mathbb{Z}_K)$ de $\mathbb{R}^n$. De l'identité

$$N_{K/\mathbb{Q}}(\omega) = \prod_{i=1}^{r_1}\sigma_i(\omega)\prod_{i=1}^{r_2}\left(\Re\left(\sigma_{r_1+i}(\omega)\right)^2 + \Im\left(\sigma_{r_1+i}(\omega)\right)^2\right),$$

où $\omega \in K$, on déduit que pour tout ξ de K on a

$$m_K(\xi) = m_{\phi(\mathbb{Z}_K),(r_1,r_2)}(\phi(\xi)).$$

Ceci montre que l'étude de m_K se ramène à celle de la restriction de $m_{\phi(\mathbb{Z}_K),(r_1,r_2)}$ à $\phi(K)$. Ainsi peut-on espérer tirer des renseignements sur m_K de l'étude de $m_{\phi(\mathbb{Z}_K),(r_1,r_2)}$. À titre d'exemple, si $M_{\phi(\mathbb{Z}_K),(r_1,r_2)} < 1$, on sait que K est euclidien pour la norme.

Toutefois, avant de poursuivre, nous allons légèrement modifier le plongement de K dans $\mathbb{R}^n$, et, de façon moins classique, identifier $K \otimes_{\mathbb{Q}} \mathbb{R}$ avec l'espace H défini par

$$H = \mathbb{R}^{r_1} \times \Big\{ z \in \mathbb{C}^{2r_2};\ \forall i \in \{1, \dots, r_2\},\ z_{r_2+i} = \overline{z_i} \Big\}.$$

Le nouveau plongement sera donc plus simplement défini par

$$\Phi(\xi) = (\sigma_i(\xi))_{i=1\dots n}.$$

Pour $x, X, \dots \in H$ on notera $x = (x_1, \dots, x_n)$, $X = (X_1, \dots, X_n)$, etc.

Remarque 1.12. On aurait pu tout aussi bien utiliser $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, équivalent mais plus simple. Toutefois, le plongement que nous choisissons facilitera certaines démarches, notamment la diagonalisation d'endomorphismes remarquables.

Avec ce nouveau point de vue, si $\xi \in K$, la norme de ξ vérifie

$$N_{K/\mathbb{Q}}(\xi) = \prod_{i=1}^{n} \Phi(\xi)_i.$$

On voit facilement que

$$\text{pour tout } \xi \in K,\ m_K(\xi) = \inf \Big\{ \Big| \prod_{i=1}^{n} (\sigma_i(\xi) - X_i) \Big|;\ X \in \Phi(\mathbb{Z}_K) \Big\},$$

et que l'étude de $m_{\phi(\mathbb{Z}_K),(r_1,r_2)}$ sur $\mathbb{R}^n$ se ramène à celle de la fonction suivante.

Définition 1.13. On appelle *fonction minimum inhomogène* de K et on note $m_{\overline{K}}$ la fonction définie sur H par

$$\text{pour tout } x \in H,\ m_{\overline{K}}(x) = \inf \Big\{ \Big| \prod_{i=1}^{n} (x_i - X_i) \Big|;\ X \in \Phi(\mathbb{Z}_K) \Big\}.$$

Ainsi, pour tout $\xi \in K$,

$$m_K(\xi) = m_{\overline{K}}(\Phi(\xi)).$$

Remarque 1.14. On peut vérifier que cette définition équivaut, au sens où les valeurs prises par les deux fonctions sont les mêmes, à celle qui est donnée dans [Lem95] et qui est la suivante.
Si $(\alpha_1, \dots, \alpha_n)$ est une $\mathbb{Z}$-base de $\mathbb{Z}_K$, $m'_{\overline{K}}$ est définie sur $\mathbb{R}^n$ par

$$m'_{\overline{K}}(x_1, \dots, x_n) = \inf \Bigg\{ \Big| \prod_{i=1}^{n} \Big(\sum_{j=1}^{n} (x_j - X_j)\, \sigma_i(\alpha_j) \Big) \Big|;\ X \in \mathbb{Z}^n \Bigg\}.$$

Un avantage du nouveau plongement Φ est que si l'on munit H d'une structure d'algèbre à l'aide du produit

$$(x_1, x_2, \ldots, x_n).(y_1, y_2, \ldots, y_n) = (x_1y_1, x_2y_2, \ldots, x_ny_n),$$

Φ est multiplicatif au sens où pour tout α et tout β de K, on a

$$\Phi(\alpha\beta) = \Phi(\alpha).\Phi(\beta).$$

Avec ces notations, la Proposition 1.10 i) se généralise alors ainsi.

Proposition 1.15. *Pour tout x de H, tout X de $\Phi(\mathbb{Z}_K)$ et toute unité ε de E_K,*

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

Preuve. Comme précédemment, $m_{\overline{K}}$ est définie modulo $\Phi(\mathbb{Z}_K)$ et

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

Or

$$m_{\overline{K}}(\Phi(\varepsilon).x) = \inf\left\{\Big|\prod_{i=1}^{n}(\sigma_i(\varepsilon)x_i - X_i)\Big|;\ X \in \Phi(\mathbb{Z}_K)\right\},$$

et comme

$$\Phi(\varepsilon).\Phi(\mathbb{Z}_K) = \Phi(\varepsilon\mathbb{Z}_K) = \Phi(\mathbb{Z}_K),$$

on a

$$m_{\overline{K}}(\Phi(\varepsilon).x) = \inf\left\{\Big|\prod_{i=1}^{n}(\sigma_i(\varepsilon)x_i - \sigma_i(\varepsilon)X_i)\Big|;\ X \in \Phi(\mathbb{Z}_K)\right\}.$$

Finalement

$$m_{\overline{K}}(\Phi(\varepsilon).x) = \inf\left\{\Big|N_{K/\mathbb{Q}}(\varepsilon)\prod_{i=1}^{n}(x_i - X_i)\Big|;\ X \in \Phi(\mathbb{Z}_K)\right\},$$

ce qui donne l'égalité cherchée. □

Les autres propriétés de $m_{\phi(\mathbb{Z}_K),(r_1,r_2)}$ (correspondant au Théorème 1.2 et aux Corollaires 1.3 et 1.6) se traduisent de la façon suivante.

Théorème 1.16. *La fonction $m_{\overline{K}}$ vérifie*

- *$m_{\overline{K}}$ est semi-continue supérieurement sur H et induit sur $H/\Phi(\mathbb{Z}_K)$ une application également semi-continue supérieurement.*
- *$m_{\overline{K}}$ est bornée sur H et atteint sa borne supérieure.*
- *Si $(x_p)_{p\in\mathbb{N}}$ est une suite d'éléments de H convergeant vers $x \in H$, alors on a*

$$\limsup_{p\to+\infty} m_{\overline{K}}(x_p) \leq m_{\overline{K}}(x).$$

La même propriété est vérifiée par l'application induite par $m_{\overline{K}}$ sur $H/\Phi(\mathbb{Z}_K)$.

Ceci nous conduit à définir les notions de minimum inhomogène et de spectre inhomogène du corps K.

Définition 1.17. On appelle *minimum inhomogène* de K et on note $M(\overline{K})$ le réel défini par

$$M(\overline{K}) = \sup\{m_{\overline{K}}(x);\ x \in H\}.$$

En fait il ne s'agit que de la nouvelle notation de $M_{\phi(\mathbb{Z}_K),(r_1,r_2)}$.

Définition 1.18. L'ensemble des valeurs prises par $m_{\overline{K}}$ sera appelé le *spectre inhomogène* de K. On le notera $\mathrm{sp}(\overline{K})$.

Par le Corollaire 1.3 ou par le Théorème 1.16 on sait qu'il existe des éléments x de H, encore dits *critiques*, qui vérifient

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

Ainsi a-t-on

$$\mathrm{sp}(\overline{K}) \subseteq [0, M(\overline{K})] \quad \text{et} \quad M(\overline{K}) \in \mathrm{sp}(\overline{K}).$$

De même, comme $m_K(\xi) = m_{\overline{K}}(\Phi(\xi))$ pour tout ξ de K, m_K est bornée. Ceci nous conduit à définir les notions de minimum euclidien et de spectre euclidien de K.

Définition 1.19. On appelle *minimum euclidien* de K et on note $M(K)$ le réel défini par

$$M(K) = \sup\{m_K(\xi);\ \xi \in K\}.$$

Par la proposition 1.10 iii) on a

$$0 < M(K) \leq M(\overline{K}).$$

Remarque 1.20. Il est facile de voir que cette définition équivaut à la définition (4) donnée dans l'introduction. En effet, notons provisoirement M_1 le «minimum» tel qu'il est défini par (4) et M_2 celui de la précédente définition. Soit $\kappa > M_1$. Alors pour tout $\xi \in K$, il existe $\Upsilon \in \mathbb{Z}_K$ tel que $|N_{K/\mathbb{Q}}(\xi - \Upsilon)| < \kappa$. D'où $m_K(\xi) < \kappa$ pour tout $\xi \in K$ et $M_2 \leq \kappa$. Ceci étant vrai pour tout $\kappa > M_1$, on en déduit $M_2 \leq M_1$.
Fixons maintenant $\kappa > M_2$. Par la Proposition 1.4.ii), pour tout $\xi \in K$ il existe $\Upsilon \in \mathbb{Z}_K$ tel que $|N_{K/\mathbb{Q}}(\xi - \Upsilon)| = m_K(\xi) \leq M_2 < \kappa$. D'où $M_1 \leq \kappa$ pour tout $\kappa > M_2$, et finalement $M_1 \leq M_2$.
On a donc bien l'égalité $M_1 = M_2$.

Ceci justifie mieux l'appellation minimum euclidien qui pouvait a priori surprendre, s'agissant d'une borne supérieure.

Définition 1.21. L'ensemble des valeurs prises par m_K sera appelé le *spectre euclidien* de K. On le notera $\mathrm{sp}(K)$.

Ainsi a-t-on

$$\mathrm{sp}(K) \subseteq [0, M(K)] \quad \text{et} \quad \mathrm{sp}(K) \subseteq \mathrm{sp}(\overline{K}).$$

Remarque 1.22. Contrairement à ce qui se passe avec les notions inhomogènes, on ne peut pas affirmer ici que $M(K)$ est élément de $\mathrm{sp}(K)$, du moins de façon élémentaire. Ce problème sera développé ultérieurement.

Des définitions respectives de $M(K)$ et de l'euclidianité pour la norme on tire le résultat suivant.

Proposition 1.23. *La connaissance de $M(K)$ donne les informations suivantes.*

- *Si $M(K) < 1$, K est euclidien pour la norme.*
- *Si $M(K) > 1$, K n'est pas euclidien pour la norme.*
- *Si $M(K) = 1$, on ne peut pas a priori conclure sauf s'il existe un élément ξ de K tel que $m_K(\xi) = 1$, auquel cas le corps K n'est pas euclidien pour la norme.*

Notons enfin que la Proposition 1.10 ii) fournit la propriété suivante.

Proposition 1.24. *Pour tout $\xi \in K$ il existe un entier $\Upsilon \in \mathbb{Z}_K$ tel que*

$$|N_{K/\mathbb{Q}}(\xi - \Upsilon)| \leq M(K).$$

Tout ceci amène à de nombreuses questions que nous allons préciser dans la section suivante. Mais avant cela il est peut-être souhaitable d'illustrer les notions précédemment définies par des exemples simples.

1.3.2 Premiers exemples

Le cas $n = 1$ est évident.

Proposition 1.25. *Si $K = \mathbb{Q}$ on a*

$$M(K) = M(\overline{K}) = \frac{1}{2}.$$

Les points critiques correspondent aux points congrus à $1/2$ modulo $\mathbb{Z}$.

Notons que l'on a également

$$\mathrm{sp}(\overline{K}) = \left[0, \frac{1}{2}\right] \text{ et } \mathrm{sp}(K) = \mathrm{sp}(\overline{K}) \cap \mathbb{Q}.$$

Le cas $n = 2$ et $r_1 = 0$ qui correspond aux corps quadratiques complexes est également facile et peut être résolu à l'aide d'arguments géométriques élémentaires (voir [Co80] par exemple). En effet, ici, la norme correspond au carré de la distance euclidienne et le problème s'interprète en termes de proximité géométrique aux entiers du corps.

Proposition 1.26. *Soit m un entier positif et sans facteur carré et soit $K = \mathbb{Q}(\sqrt{-m})$.*

- *Si $m \equiv 1$ ou $2 \bmod 4$, on a*

$$M(K) = M(\overline{K}) = \frac{m+1}{4}.$$

Les points critiques correspondent aux éléments de K congrus à $(1+\sqrt{-m})/2$ modulo $\mathbb{Z}_K = \mathbb{Z} + \mathbb{Z}\sqrt{-m}$.

- *Si $m \equiv 3 \bmod 4$, on a*

$$M(K) = M(\overline{K}) = \frac{(m+1)^2}{16m}.$$

Les points critiques correspondent aux éléments de K congrus à $\pm(1+m)\sqrt{-m}/4m$ modulo $\mathbb{Z}_K = \mathbb{Z} + \mathbb{Z}(1+\sqrt{-m})/2$.

Il est également facile de voir que $\mathrm{sp}(\overline{K}) = [0, M(\overline{K})]$, et que, comme dans le cas $n = 1$, le spectre euclidien est un sous-ensemble strict de $\mathrm{sp}(\overline{K})$, dense dans $\mathrm{sp}(\overline{K})$.

Corollaire 1.27. *Les seuls corps quadratiques complexes euclidiens pour la norme sont les $\mathbb{Q}(\sqrt{-m})$ pour*

$$m = 1,\ 2,\ 3,\ 7 \text{ et } 11.$$

Un cas très simple de corps quadratique réel est le suivant.

Proposition 1.28. *Pour $K = \mathbb{Q}(\sqrt{2})$, on a*

$$M(K) = M(\overline{K}) = \frac{1}{2}.$$

Les points critiques correspondent aux éléments de K congrus à $\sqrt{2}/2$ modulo $\mathbb{Z}_K = \mathbb{Z} + \mathbb{Z}\sqrt{2}$.

Preuve. Dans ce cas on a $H = \mathbb{R}^2$ et $\Phi(u + v\sqrt{2}) = (u + v\sqrt{2}, u - v\sqrt{2})$. Ainsi, si $(x, y) \in H$ on a

$$m_{\overline{K}}(x, y) = \inf\{|(x - (a + b\sqrt{2}))(y - (a - b\sqrt{2}))|;\ (a, b) \in \mathbb{Z}^2\}.$$

Le changement de variables $\{x = \alpha + \beta\sqrt{2},\ y = \alpha - \beta\sqrt{2}\}$ conduit à

$$m_{\overline{K}}(x, y) = \inf\{|(\alpha - a)^2 - 2(\beta - b)^2|;\ (a, b) \in \mathbb{Z}^2\}.$$

En prenant pour a la partie entière de $\alpha + 1/2$ et pour b la partie entière de $\beta + 1/2$, de telle sorte que $|\alpha - a| \leq 1/2$ et $|\beta - b| \leq 1/2$, et en utilisant

$$|(\alpha - a)^2 - 2(\beta - b)^2| \leq \max\left\{(\alpha - a)^2, 2(\beta - b)^2\right\},$$

on obtient

$$m_{\overline{K}}(x, y) \leq \frac{1}{2}.$$

On voit même que l'on a une inégalité stricte si $(\alpha,\beta)\not\equiv(0,\frac{1}{2})$ mod $\mathbb{Z}^2$ ou encore si $(x,y)\not\equiv(\sqrt{2}/2,-\sqrt{2}/2)$ mod $\Phi(\mathbb{Z}_K)$.
Finalement on obtient facilement que lorsque $(\alpha,\beta)\equiv(0,\frac{1}{2})$ mod $\mathbb{Z}^2$,

$$m_{\overline{K}}(x,y)=m_K\left(\frac{\sqrt{2}}{2}\right)=\frac{1}{2},$$

en observant par exemple que pour tout $(a,b)\in\mathbb{Z}^2$,

$$N_{K/\mathbb{Q}}\left(\frac{\sqrt{2}}{2}-a-b\sqrt{2}\right)\equiv\frac{1}{2}\text{ mod }\mathbb{Z}.$$

D'où la conclusion. □

Remarque 1.29. Remarquons que la première partie de la preuve pouvait également s'interpréter géométriquement à l'aide de la Figure 1.1 ci-dessous. Ici $\tau=\sqrt{2}$ et la région hyperbolique R grisée représente les éléments $(x,y)\in H$ vérifiant $|(x-\Phi(0)_1)(y-\Phi(0)_2)|=|xy|\leq 1/2$. Les croix correspondent aux éléments de $\Phi(\mathbb{Z}_K)$ et l'on constate aisément que l'on recouvre bien tout le plan avec des régions similaires à R centrées aux différents points de $\mathbb{Z}_K$. Il suffit pour cela, compte tenu de l'invariance modulo $\Phi(\mathbb{Z}_K)$, d'observer ce qui se passe sur un domaine fondamental (ici nous en avons encadré un). On peut même voir que les seuls points susceptibles de vérifier $m_{\overline{K}}(x,y)=1/2$ sont ceux qui sont congrus à $\Phi(\sqrt{2}/2)$ modulo $\Phi(\mathbb{Z}_K)$.

Notons enfin qu'ici, l'étude des spectres mène à de nouveaux phénomènes que nous détaillerons dans la prochaine section.

Afin d'alléger le propos et les notations nous dirons désormais qu'un point de H qui est dans l'image de K par Φ est *rationnel*, et qu'il est *non rationnel* dans le cas contraire. De plus, si $x\in H$ nous noterons

$$\mathcal{N}(x)=\Big|\prod_{i=1}^{n}x_i\Big|.$$

Ainsi, si $\xi\in K$, $\Phi(\xi)$ est rationnel et

$$|N_{K/\mathbb{Q}}(\xi)|=\mathcal{N}(\Phi(\xi)).$$

1.4 Quelques constats et problèmes

1.4.1 Comparaison de $M(K)$ et $M(\overline{K})$

La première question qui vient à l'esprit concerne la comparaison de $M(K)$ et $M(\overline{K})$. Nous avons vu que

$$M(K)\leq M(\overline{K}),$$

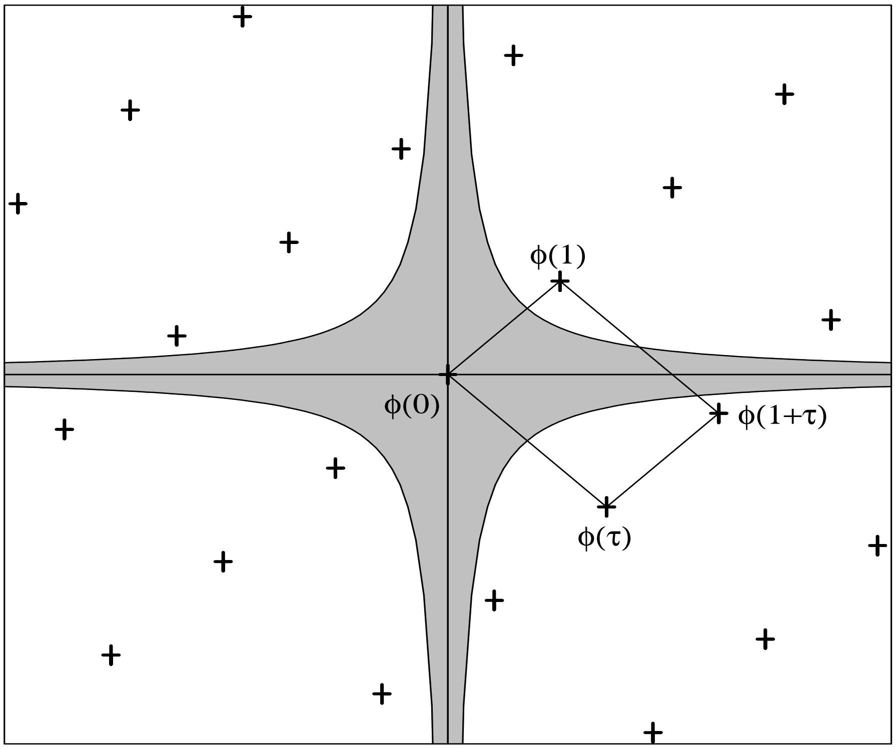

FIG. 1.1: Recouvrement de $\mathbb{R}^2$ par des régions hyperboliques.

et que, dans tous les exemples élémentaires précédents, il y avait en fait égalité entre ces deux nombres. Avant ce travail, le seul résultat connu concernait les corps de nombres K dont le groupe des unités est de rang r inférieur ou égal à 1. Les cas $n = 1$ et $n = 2$, $r_1 = 0$ ont déjà été vus en exemples. Dans le cas quadratique réel ($n = r_1 = 2$), Barnes et Swinnerton-Dyer [BSD52b] ont établi qu'il y avait égalité entre $M(K)$ et $M(\overline{K})$, et Van der Linden [VdL85] a généralisé leur résultat au cas $r = 1$. Ce qui donne le théorème suivant.

Théorème 1.30. *Pour tout corps de nombres K vérifiant $r \leq 1$ on a*

$$M(K) = M(\overline{K}).$$

1.4.2 Rationalité des minima

Un autre résultat intéressant concerne la rationalité de $M(K)$ ou de $M(\overline{K})$. Notons que s'il existe un élément ξ de K vérifiant $m_K(\xi) = M(\overline{K})$, c'est-à-dire un point rationnel critique, on a non seulement l'égalité des deux minima, mais aussi, grâce à la Proposition 1.10 iii),

$$M(K) = M(\overline{K}) \in \mathbb{Q}.$$

Dans tous les cas connus cette propriété est vérifiée, mais aucune démonstration générale n'a pu en être donnée, en dehors bien sûr des cas triviaux $n = 1$ et $n = 2$, $r_1 = 0$. Barnes et Swinnerton-Dyer [BSD52b] l'ont conjecturée dans le cas quadratique réel.

Conjecture 1 (Barnes et Swinnerton-Dyer). *Pour tout corps de nombres quadratique réel K, il existe $\xi \in K$ tel que*
$$m_K(\xi) = M(\overline{K}).$$

1.4.3 Euclidianité de K

On a vu plus haut (Proposition 1.23) que si $M(K) = 1$, on ne peut rien dire a priori de l'euclidianité de K, mais que dans ce cas, s'il existe $\xi \in K$ tel que $m_K(\xi) = 1$, K n'est pas euclidien pour la norme. Ce sera évidemment encore le cas s'il existe ξ de K tel que $m_K(\xi) = M(\overline{K})$, puisqu'alors $M(\overline{K}) \geq 1$, et ceci même si l'on n'a pas $M(\overline{K}) = M(K)$. En particulier dans le cas quadratique réel, si la Conjecture 1 de Barnes et Swinnerton-Dyer est correcte, on aura

$$M(K) = 1 \Rightarrow K \text{ non euclidien pour la norme.}$$

1.4.4 Minimum atteint

Une autre question découle de la Proposition 1.24. On a vu que pour tout ξ de K il existe un $\Upsilon \in \mathbb{Z}_K$ tel que $|N_{K/\mathbb{Q}}(\xi - \Upsilon)| \leq M(K)$. En revenant à la définition de $M(\overline{K})$, il est évident que pour tout $x \in H$ et tout $\epsilon > 0$, il existe un élément X de $\Phi(\mathbb{Z}_K)$ tel que $\mathcal{N}(x - X) \leq M(\overline{K}) + \epsilon$. Mais, bien que cela convienne évidemment pour les points rationnels puisque $M(K) \leq M(\overline{K})$, peut-on prendre $\epsilon = 0$ dans cette dernière inégalité ?

La réponse est non, et l'exemple le plus simple est celui de $K = \mathbb{Q}(\sqrt{13})$ [In49].

Exemple 1.31. Pour $K = \mathbb{Q}(\sqrt{13})$, on a

$$M(K) = M(\overline{K}) = \frac{1}{3}.$$

Modulo $\Phi(\mathbb{Z}_K)$, il y a 4 points rationnels critiques $x_1, \ldots, x_4 \in \Phi(K)$, et 4 suites infinies $(x_{i,p})$ (avec $1 \leq i \leq 4$) de points critiques non rationnels, convergeant vers x_i, tels que

$$\mathcal{N}(x_{i,p} - X) > \frac{1}{3}, \qquad \text{pour tout } x_{i,p} \text{ et tout } X \in \Phi(\mathbb{Z}_K).$$

Ceci nous amène à poser la définition suivante.

Définition 1.32. On dira que $M(\overline{K})$ est *atteint* si pour tout $x \in H$ il existe $X \in \Phi(\mathbb{Z}_K)$ tel que
$$\mathcal{N}(x - X) \leq M(\overline{K}).$$

Ainsi $M(\overline{K})$ est atteint si $n = 1$, si $n = 2$, $r_1 = 0$, si $K = \mathbb{Q}(\sqrt{2})$, et non atteint si $K = \mathbb{Q}(\sqrt{13})$.

1.4.5 Minimum isolé

Les questions suivantes plus fines concernent les points non critiques. Commençons par une définition.

Définition 1.33. On appelle *second minimum inhomogène* et *second minimum euclidien* de K, et on note $M_2(\overline{K})$ et $M_2(K)$ les réels respectivement définis par

$$M_2(\overline{K}) = \sup_{\substack{x\in H\\ m_{\overline{K}}(x)<M(\overline{K})}} \Big(m_{\overline{K}}(x)\Big) \quad \text{et} \quad M_2(K) = \sup_{\substack{\xi\in K\\ m_K(\xi)<M(K)}} \Big(m_K(\xi)\Big).$$

On a donc

$$M_2(K) \leq M_2(\overline{K}) \leq M(\overline{K}).$$

Définition 1.34. $M(\overline{K})$ est dit *isolé* si

$$M_2(\overline{K}) < M(\overline{K}).$$

Par exemple, si $K = \mathbb{Q}$ ou si K est quadratique complexe, $M(\overline{K})$ n'est pas isolé. En revanche, Barnes et Swinnerton-Dyer [BSD52b] ont conjecturé la propriété suivante.

Conjecture 2 (Barnes et Swinnerton-Dyer). *Si K est quadratique réel, $M(\overline{K})$ est isolé.*

Ils ne sont parvenus à établir ce résultat que lorsqu'il y a un nombre fini de points critiques dans $\mathbb{R}^2$ modulo $\Phi(\mathbb{Z}_K)$.
Signalons au passage que cette conjecture est plus forte que la précédente sous l'hypothèse $M(K) = M(\overline{K})$, et en particulier dans le cas quadratique réel. Supposons en effet que $M_2(\overline{K})$ soit strictement inférieur à $M(K) = M(\overline{K})$. Alors on aurait

$$M_2(K) < M(K).$$

Si la Conjecture 1 était fausse, comme $M(K) = M(\overline{K})$, il existerait une suite $(\xi_p)_{p\in\mathbb{N}}$ d'éléments de K, vérifiant

$$\lim_{p\to+\infty} m_K(\xi_p) = M(\overline{K}) \quad \text{et} \quad m_k(\xi_p) < M(\overline{K}) \text{ pour tout p.}$$

Par définition de $M_2(K)$, on obtiendrait $M_2(K) = M(K)$ et une contradiction.

On pourrait également se demander si, comme pour les minima euclidiens et inhomogènes, l'égalité $M_2(K) = M_2(\overline{K})$ est conjecturable. La réponse est non. Godwin [Go55] a donné le contre-exemple suivant.

Exemple 1.35. Si $K = \mathbb{Q}(\sqrt{73})$, on a $\quad M_2(K) < M_2(\overline{K})$.

1.4.6 Allure et comparaison des spectres

Allons plus loin et définissons (avec $p \geq 2$)

$$M_{p+1}(\overline{K}) = \sup_{\substack{x \in H \\ m_{\overline{K}}(x) < M_p(\overline{K})}} \Big(m_{\overline{K}}(x) \Big) \quad \text{et} \quad M_{p+1}(K) = \sup_{\substack{\xi \in K \\ m_K(\xi) < M_p(K)}} \Big(m_K(\xi) \Big).$$

En posant conventionnellement $M_1(\overline{K}) = M(\overline{K})$ (respectivement $M_1(K) = M(K)$), on définit ainsi deux suites décroissantes, et par récurrence on établit sans peine que

$$M_p(K) \leq M_p(\overline{K}), \text{ pour tout } p \geq 1.$$

En outre, dès que l'on a $M_{p+1}(\overline{K}) = M_p(\overline{K})$ (resp. $M_{p+1}(K) = M_p(K)$), la suite $(M_p(\overline{K}))_{p\geq 1}$ (resp. $(M_p(K))_{p\geq 1}$) devient stationnaire. C'est le cas dès $p = 1$ dans les cas élémentaires $n = 1$ et $n = 2$, $r_1 = 0$, où elles sont égales et constantes. On a déjà vu, par l'Exemple 1.35, que dans le cas quadratique réel, les suites ne sont pas nécessairement égales. En revanche, à la lueur de la conjecture d'isolation, on pourrait se poser d'autres questions. Sont-elles strictement décroissantes ? Et si oui, convergent-elles vers 0 ?

Pour ce qui est de la première question, Godwin [Go63] a établi le résultat suivant.

Exemple 1.36. Si $K = \mathbb{Q}(\sqrt{23})$,

$$M(K) = M(\overline{K}) = \frac{77}{46} \text{ est atteint et isolé,}$$

mais les deux suites sont stationnaires dès $p = 2$, avec

$$M_2(\overline{K}) = M_2(K) = \frac{20\sqrt{23} - 31}{46}.$$

Concernant la seconde, Davenport [Da47] et Varnavides [Var48] ont établi le résultat suivant.

Exemple 1.37. Pour $K = \mathbb{Q}(\sqrt{5})$ et $K = \mathbb{Q}(\sqrt{2})$, les deux suites $(M_p(K))_{p\geq 1}$ et $(M_p(\overline{K}))_{p\geq 1}$ sont égales, strictement décroissantes, et convergent respectivement vers

$$\lim_{p\to+\infty} M_p(\overline{K}) = \frac{\sqrt{5}-1}{8} \quad \text{et} \quad \lim_{p\to+\infty} M_p(\overline{K}) = \frac{\sqrt{2}-1}{2}.$$

Une autre question concerne le lien qui existe entre ces deux suites et les spectres $\mathrm{sp}(\overline{K})$ et $\mathrm{sp}(K)$. On a par les définitions,

$$M_p(\overline{K}) \in \overline{\mathrm{sp}(\overline{K})} \quad \text{et} \quad M_p(K) \in \overline{\mathrm{sp}(K)}, \text{ pour tout } p \geq 1,$$

mais que peut-on dire de plus ? Barnes et Swinnerton-Dyer [BSD52b] ont établi la proposition suivante.

Proposition 1.38. *Si K est un corps quadratique réel, $\mathrm{sp}(\overline{K})$ est fermé.*

Ceci implique que dans ce cas

$$M_p(\overline{K}) \in \mathrm{sp}(\overline{K}), \text{ pour tout } p \geq 1.$$

Pour ce qui est du spectre euclidien, l'exemple 1.36 de Godwin montre qu'il n'est pas fermé car dans ce cas, $M_2(K) \notin \mathbb{Q}$ alors que l'on a de toute façon $\mathrm{sp}(K) \subseteq \mathbb{Q}$.

1.4.7 Calcul effectif

S'agissant des corps quadratiques réels, en dehors de cas particuliers pour lesquels $M(\overline{K})$ a été calculé et vérifié égal à $M(K)$, voire parfois même la partie supérieure du spectre déterminée, il y a quelques résultats remarquables concernant des familles infinies de corps. Citons certains de ceux qu'ont établis Varnavides [Var70] (points 1, 2, 3), Inkeri [In50] (points 2, 3), Davenport [Da46] (point 3) et Barnes et Swinnerton-Dyer [BSD52a] (points 4, 5, 6, 7).

Théorème 1.39. *Soit m un entier supérieur ou égal à 2 sans facteur carré et soit $K = \mathbb{Q}(\sqrt{m})$.*

1. *Si m est de la forme $(2k+1)^2+1$ avec $k \geq 0$, on a*

$$M(K) = M(\overline{K}) = \frac{2k+1}{2},$$

avec un point critique rationnel.

2. *Si m est de la forme $4k^2+1$ avec $k \geq 1$, on a*

$$M(K) = M(\overline{K}) = \frac{k}{4},$$

avec deux points critiques rationnels si $k \neq 1$, et trois points critiques rationnels si $k = 1$.

3. *Si m est de la forme $4k^2-1$ avec $k \geq 1$, on a*

$$M(K) = M(\overline{K}) = \frac{2k-1}{2},$$

avec un point critique rationnel.

4. *Si m est de la forme $(2k+1)^2-2$ avec $k \geq 1$, on a*

$$M(K) = M(\overline{K}) = \frac{8k^3+6k^2-6k+1}{2m},$$

avec deux points critiques rationnels.

5. *Si m est de la forme $(2k+1)^2+2$ avec $k \geq 1$, on a*

$$M(K) = M(\overline{K}) = \frac{8k^3+6k^2+6k-1}{2m},$$

avec deux points critiques rationnels.

6. *Si m est de la forme $(2k+1)^2-4$ avec $k \geq 2$, on a*

$$M(K) = M(\overline{K}) = \frac{k^2+k-1}{2k+3},$$

avec deux points critiques rationnels.

7. *Si m est de la forme $(2k+1)^2+4$ avec $k \geq 1$, on a*

$$M(K) = M(\overline{K}) = \frac{k^2}{2k+1},$$

avec quatre points critiques rationnels et quatre suites infinies de points critiques non rationnels convergeant vers les premiers. De plus

$$M_2(K) = M_2(\overline{K}) = \frac{2k^3+k^2+2k-1}{m},$$

correspondant à quatre points rationnels.

Que l'on ait des résultats généraux aussi précis ne doit pas étonner. Pour tous ces corps de nombres, on connaît le groupe des unités, qui, comme nous le verrons plus tard, joue un rôle prépondérant dans la détermination de $M(\overline{K})$.

D'autres résultats du même type sont connus dans le cas cubique complexe et dans le cas quartique totalement complexe, c'est-à-dire dans les deux autres cas où $r = 1$. Pour plus de détails sur ce genre de résultats, voir [Lem95]. Dans tous les cas observés, il existe des points critiques rationnels et l'on a donc toujours $M(K) = M(\overline{K}) \in \mathbb{Q}$.

Ceci étant, en dehors de ces familles, les tables, quand il y en a, sont assez pauvres, et en dimension supérieure, à part quelques cas particuliers, peu de choses sont connues.

Reste l'alternative algorithmique. Cavallar et Lemmermeyer [CaL98] ont traité avec un certain succès le cas cubique. Toutefois, en particulier dans le cas totalement réel, l'algorithme ne permet pas d'obtenir la valeur exacte de $M(K)$ et sert surtout à montrer que $M(\overline{K}) < 1$. Lorsque le calcul aboutit, on a toujours, là encore, $M(K) = M(\overline{K})$. Mais ceci n'est pas étonnant. En effet pour déterminer exactement $M(\overline{K})$, l'idée est de trouver un ξ de K tel que $M(\overline{K}) = m_K(\xi)$.

En dimension plus grande, c'est aussi l'approche algorithmique qui nous a permis [Ce00] de montrer que pour $n = 16$ et 32, le corps $\mathcal{K}_n = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, où ζ_n est une racine primitive n-ième de l'unité, vérifie $M(\mathcal{K}_n) = M(\overline{\mathcal{K}_n}) = 1/2$, conformément à une conjecture de Cohn et Deutsch [CD86]. Nous serons d'ailleurs amenés à préciser ce résultat plus tard.

Citons également le travail de Quême [Qu98]. Le programme qu'il a élaboré ne permet pas toutefois de calculer $M(K)$, mais seulement d'établir $M(K) < 1$ dans les cas favorables.

1.4.8 Questions

Ces considérations nous conduisent aux questions suivantes.

- A-t-on $M(K) = M(\overline{K})$ pour tout corps de nombres K ?
- Que dire de K lorsque $M(K) = 1$ ou $M(\overline{K}) = 1$?
- Que penser des conjectures 1 et 2 de Barnes et Swinnerton-Dyer en dimension supérieure ?

- Peut-on avoir des renseignements particuliers sur les spectres inhomogène et euclidien en dimension supérieure ? Par exemple, y a-t-il des cas où ils sont confondus ? Peut-on dans certains cas dire quelque chose sur leur partie supérieure ?

- À défaut d'avoir des résultats intéressants sur les spectres, que peut-on dire des suites $(M_p(K))_{p\geq 1}$ et $(M_p(\overline{K}))_{p\geq 1}$, et des relations entre ces suites et les spectres dont elles sont respectivement issues ?

- De façon plus concrète, peut-on envisager un algorithme qui permette de calculer $M(\overline{K})$ en dimension supérieure ? Et dans ce cas, des conjectures similaires à celles de Barnes et Swinnerton-Dyer sont-elles vérifiées ?

Autant de questions auxquelles nous allons tenter de répondre dans les pages qui suivent. La réponse à la première de ces questions est oui et nous établirons donc le résultat suivant.

Théorème [Corollaire 4.14]
Pour tout corps de nombres K, on a $M(K) = M(\overline{K})$.

Concernant la deuxième question, si r est le rang du groupe des unités de K, nous montrerons la propriété ci-dessous.

Théorème [Corollaire 4.15]
Si $M(K) = 1$ et si $r > 1$, alors K n'est pas euclidien pour la norme.

Pour ce qui est de la troisième question, nous établirons le résultat suivant.

Théorème [Théorèmes 4.13 et 4.22]
Si $r > 1$, il existe un $\xi \in K$ tel que $M(\overline{K}) = m_K(\xi)$. Si, en outre, K n'est pas un corps CM, $M(\overline{K})$ est isolé.

Une réponse aux questions 3 et 4 sera la suivante.

Théorème [Théorème 4.22 et Corollaire 4.23]
Si $r > 1$ et si K n'est pas un corps CM, alors les spectres inhomogène et euclidien sont confondus et rationnels. Pour tout p on a $M_p(K) = M_p(\overline{K}) \in \mathbb{Q}$ et la suite $(M_p(K))$ est strictement décroissante et converge vers 0. Le spectre inhomogène (ou euclidien) est réduit à la réunion de l'ensemble des $M_p(K)$ et de $\{0\}$.

Enfin, pour ce qui est de l'aspect algorithmique, nous verrons comment calculer $M(K)$, en particulier si K est un corps de nombres totalement réel, et même comment déterminer la partie supérieure du spectre euclidien de K.

Chapitre 2

Prolégomènes

2.1 Un résultat fondamental

Soit K un corps de nombres de degré n, dont le groupe des unités est de rang r. Les cas correspondant à $r = 0$ ($n = 1$ et $n = 2$, $r_1 = 0$) ayant déjà été étudiés et ne faisant l'objet d'aucune difficulté particulière, nous supposerons désormais

$$r \geq 1.$$

Les notations sont les mêmes que celles introduites dans la section 1.1. Rappelons que $(\varepsilon_i)_{1 \leq i \leq r}$ désigne un système d'unités fondamentales de K.

L'objectif est de trouver une formule qui permette de calculer explicitement $m_K(\xi)$ lorsque $\xi \in K$, et de mieux appréhender $m_{\overline{K}}(x)$ lorsque $x \in H$, ce qui sera fait dans les prochaines sections.

Commençons par un lemme général concernant les unités.

Pour tout $i \in \{1, \ldots, r_1 + r_2\}$ posons

$$\Gamma_i = \prod_{j=1}^{r} \max\Big\{|\sigma_i(\varepsilon_j)|, \frac{1}{|\sigma_i(\varepsilon_j)|}\Big\}. \tag{2.1}$$

Lemme 2.1. *Si $c_1, \ldots, c_r$ sont $r = r_1 + r_2 - 1$ réels strictement positifs donnés, il existe une unité $\nu \in E_K$ telle que pour tout $i \in \{1, \ldots, r\}$,*

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

Preuve. Soit $\mathcal{H}$ l'hyperplan de $\mathbb{R}^{r_1+r_2}$ d'équation

$$\sum_{i=1}^{r_1} x_i + 2 \sum_{i=r_1+1}^{r_1+r_2} x_i = 0.$$

On sait que $\mathcal{L}(E_K)$ est un réseau de $\mathcal{H}$ qui admet pour domaine fondamental

$$\mathcal{D} = \Big\{ \sum_{i=1}^{r} \lambda_i \mathcal{L}(\varepsilon_i);\ \lambda_i \in [0, 1) \text{ pour tout } i \Big\}.$$

Pour tout $i \in \{1, \dots, r_1 + r_2\}$, soient I_i l'ensemble des $j \in \{1, \dots, r\}$ tels que $\ln|\sigma_i(\varepsilon_j)| < 0$, et J_i l'ensemble des $j \in \{1, \dots, r\}$ tels que $\ln|\sigma_i(\varepsilon_j)| \geq 0$.
On a $I_i \cup J_i = \{1, \dots, r\}$, et il est facile de voir que pour tout $x \in \mathcal{D}$ et tout $i \in \{1, \dots, r_1 + r_2\}$, on a

$$x_i \in \Big[\sum_{j \in I_i} \ln|\sigma_i(\varepsilon_j)|, \sum_{j \in J_i} \ln|\sigma_i(\varepsilon_j)| \Big]. \tag{2.2}$$

Notons $\mathcal{D}'$ le translaté de $\mathcal{D}$ suivant le vecteur $z \in \mathcal{H}$ défini par

$$z_i = \ln c_i - \sum_{j \in I_i} \ln|\sigma_i(\varepsilon_j)| \text{ pour } i \in \{1, \dots, r\}$$

et

$$z_{r+1} = -\sum_{i=1}^{r} z_i \quad \text{ou} \quad -\frac{1}{2}\left(\sum_{i=1}^{r_1} z_i + 2\sum_{i=r_1+1}^{r} z_i\right),$$

suivant que K est totalement réel ou non.

Comme pour tout $i \in \{1, \dots, r_1 + r_2\}$,

$$\sum_{j \in J_i} \ln|\sigma_i(\varepsilon_j)| - \sum_{j \in I_i} \ln|\sigma_i(\varepsilon_j)| = \sum_{j=1}^{r} \Big| \ln|\sigma_i(\varepsilon_j)| \Big|,$$

on voit par (2.2) que

$$\mathcal{D}' \subseteq \Big\{ x \in \mathcal{H};\ \ln c_i \leq x_i \leq \ln c_i + \sum_{j=1}^{r} \Big| \ln|\sigma_i(\varepsilon_j)| \Big| \ \text{ pour } i = 1, \dots, r \Big\}.$$

Or, par une propriété élémentaire des domaines fondamentaux, on sait que tout translaté de $\mathcal{D}$ suivant un élément de $\mathcal{H}$ contient un élément de $\mathcal{L}(E_K)$. Il existe donc une unité ν de E_K telle que

$$\ln c_i \leq \ln|\sigma_i(\nu)| \leq \ln c_i + \sum_{j=1}^{r} \Big| \ln|\sigma_i(\varepsilon_j)| \Big| \quad \text{pour } i \in \{1, \dots, r\},$$

de telle sorte que

$$c_i \leq |\sigma_i(\nu)| \leq c_i \prod_{j=1}^{r} \exp\Big(\max\big\{ \ln|\sigma_i(\varepsilon_j)|, -\ln|\sigma_i(\varepsilon_j)| \big\} \Big)$$

pour tout $i = 1, \dots, r$. Ceci correspond bien au résultat annoncé. □

On en déduit l'importante proposition suivante.

Proposition 2.2. *Soient $x \in H$ et $k > 0$. Supposons que soit donné un $X \in \Phi(\mathbb{Z}_K)$ tel que $0 < \mathcal{N}(x - X) < k$. Alors il existe une unité $\nu \in E_k$ et un $Y \in \Phi(\mathbb{Z}_K)$ tels que $y = \Phi(\nu) \cdot x - Y$ vérifie*

$$\mathcal{N}(y) < k \quad \text{et} \quad |y_i| \leq \Gamma(k), \text{ pour tout } i \in \{1, \ldots, n\},$$

où

$$\Gamma(k) = \left(k \prod_{j=1}^{r} \Gamma_j\right)^{\frac{1}{n}} \quad ou \quad \left(k \prod_{j=1}^{r_1} \Gamma_j \prod_{j=r_1+1}^{r} \Gamma_j^2\right)^{\frac{1}{n}}, \tag{2.3}$$

suivant que K est totalement réel ou non.

Preuve. Posons $z = x - X$. Comme $\mathcal{N}(z) > 0$, on a $z_i \neq 0$ pour tout $i \in \{1, \ldots, n\}$. Pour $1 \leq i \leq r$ les Γ_i sont strictement positifs, et l'on peut définir c_i par

$$c_i = \frac{\Gamma(k)}{\Gamma_i |z_i|} > 0.$$

Le Lemme 2.1 montre qu'il existe une unité $\nu \in E_K$ telle que

$$\frac{\Gamma(k)}{\Gamma_i} \leq \left| (\Phi(\nu) \cdot z)_i \right| \leq \Gamma(k), \quad \text{pour} \quad i = 1, \ldots, r. \tag{2.4}$$

Or, lorsque K est totalement réel,

$$\mathcal{N}(z) = \left| (\Phi(\nu) \cdot z)_n \right| \prod_{i=1}^{r} \left| (\Phi(\nu) \cdot z)_i \right| < k,$$

et lorsqu'il ne l'est pas,

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

Alors (2.4) et un calcul élémentaire mènent à

$$\left| (\Phi(\nu) \cdot z)_n \right| \leq \left(k \prod_{j=1}^{r} \Gamma_j\right)^{\frac{1}{n}} = \Gamma(k),$$

lorsque K est totalement réel, et à

$$\left| (\Phi(\nu) \cdot z)_{r_1+r_2} \right| \leq \left(k \prod_{j=1}^{r_1} \Gamma_j \prod_{j=r_1+1}^{r} \Gamma_j^2\right)^{\frac{1}{n}} = \Gamma(k),$$

lorsqu'il ne l'est pas.

Dans les deux cas, cette dernière inégalité et (2.4) montrent (par conjugaison dans le cas complexe) que

$$\left| (\Phi(\nu) \cdot z)_i \right| \leq \Gamma(k), \quad \text{pour tout} \quad i \in \{1, \ldots, n\}.$$

On a donc la conclusion avec $y = \Phi(\nu) \cdot z$, c'est-à-dire $Y = \Phi(\nu) \cdot X$. $\square$

Remarque 2.3. La borne $\Gamma(k)$ est certainement améliorable. Quoiqu'il en soit, en théorie, l'intérêt est de borner les y_i, et en pratique, $\Gamma(k)$ ne sera pas trop grande pour les corps que nous serons amenés à étudier.

Lorsque $\mathcal{N}(x - X) = 0$, on peut se demander s'il existe une unité $\nu \in E_K$ et un Y de $\Phi(\mathbb{Z}_K)$ vérifiant $\mathcal{N}(y) = 0$ où $y = \Phi(\nu) \cdot x - Y$, et $|y_i| \leq \Gamma'$, où Γ' est une constante ne dépendant que de K. La réponse est oui, mais en fait, on a beaucoup mieux.

Proposition 2.4. *Soient $x \in H$ et $\epsilon > 0$. Supposons qu'il existe un $X \in \Phi(\mathbb{Z}_K)$ tel que $\mathcal{N}(x-X) = 0$. Alors il existe une unité $\nu \in E_k$ et un $Y \in \Phi(\mathbb{Z}_K)$ tels que $y = \Phi(\nu) \cdot x - Y$ vérifie $\mathcal{N}(y) = 0$ et*

$$|y_i| < \epsilon, \qquad \textit{pour tout} \quad i \in \{1, \dots, n\}.$$

Preuve. Comme $\mathcal{N}(x-X) = 0$, il existe un $m \in \{1, \dots, r_1+r_2\}$ pour lequel $x_m - X_m = 0$. On pourrait raisonner comme plus haut, reprendre la preuve du Lemme 2.1, en travaillant sur la m-ième coordonnée à la place de la $r+1$-ième, puis en prenant dans la preuve de la Proposition 2.2 des c_i arbitrairement petits pour les indices $i \neq m$, etc. Cependant, il y a beaucoup plus simple.
En effet, il suffit de considérer l'intersection de $\mathcal{H}$ avec le quadrant défini par $x_m > 0$ et $x_i < 0$ pout tout $i \neq m$. Cette intersection est non vide. Il est alors facile d'établir, par des arguments géométriques élémentaires, que, $\mathcal{L}(E_K)$ étant un réseau de $\mathcal{H}$, il existe des éléments de $\mathcal{L}(E_K)$ dans cette intersection, donc au moins une unité ε vérifiant

$$|\sigma_i(\varepsilon)| < 1 \qquad \text{pour tout} \quad i \neq m.$$

En considérant alors $y = \Phi(\varepsilon^p) \cdot (x - X)$, où $p \in \mathbb{N}^*$ est assez grand, on aura

$$|y_i| < \epsilon, \qquad \text{pour tout} \quad i \neq m,$$

et

$$|y_m| = 0,$$

d'où le résultat. □

Remarque 2.5. Ceci montre en particulier que l'on peut supprimer l'hypothèse $\mathcal{N}(x - X) > 0$ dans la Proposition 2.2.

Avant de poursuivre, introduisons quelques notations.

Le groupe E_K agit de façon naturelle sur H par

$$(\varepsilon, x) \mapsto \Phi(\varepsilon).x$$

Or, comme $\Phi(\varepsilon) \cdot \Phi(\mathbb{Z}_K) = \Phi(\mathbb{Z}_K)$, si $x \equiv y \bmod \Phi(\mathbb{Z}_K)$, on a alors aussi $\Phi(\varepsilon) \cdot x \equiv \Phi(\varepsilon) \cdot y \bmod \Phi(\mathbb{Z}_K)$. On peut donc quotienter et définir une nouvelle action de E_K sur $H/\Phi(\mathbb{Z}_K)$ par

$$(\varepsilon, \overline{x}) \mapsto \overline{\Phi(\varepsilon) \cdot x},$$

où $\overline{y}$ désigne la classe de $y \in H$ dans $H/\Phi(\mathbb{Z}_K)$. Nous noterons $\mathrm{Orb}(x)$ l'orbite de $\overline{x}$ sous cette action.

Soit maintenant $\mathcal{F}$ un domaine fondamental de $\Phi(\mathbb{Z}_K)$. En pratique, on prendra une $\mathbb{Z}$-base $(e_i)_{1\leq i\leq n}$ de $\mathbb{Z}_K$ et on posera

$$\mathcal{F} = \Big\{ \sum_{i=1}^{n} \lambda_i \Phi(e_i);\ 0 \leq \lambda_i < 1 \Big\}. \tag{2.5}$$

On peut identifier $H/\Phi(\mathbb{Z}_K)$ et $\mathcal{F}$, et le relèvement de $\mathrm{Orb}(x)$ dans $\mathcal{F}$ sera également noté $\mathrm{Orb}(x)$.

Avec ces notations, la Proposition 1.15 montre que

$$\text{pour tout } x \in H \text{ et tout } z \in \mathrm{Orb}(x),\ m_{\overline{K}}(z) = m_{\overline{K}}(x). \tag{2.6}$$

Les Propositions 2.2, 2.4 et la Remarque 2.5 conduisent alors à l'important résultat qui suit.

Théorème 2.6. *Il existe un ensemble fini $\mathcal{A}$ d'éléments de $\Phi(\mathbb{Z}_K)$ tel que*

$$\text{pour tout } x \in H,\ m_{\overline{K}}(x) = \inf_{z\in \mathrm{Orb}(x)} \left(\min_{Z\in\mathcal{A}} \Big(\mathcal{N}(z-Z)\Big)\right).$$

Preuve. Soit k un réel vérifiant

$$k > M(\overline{K}).$$

Soit $\epsilon > 0$ suffisamment petit pour que l'on ait $M(\overline{K}) + \epsilon < k$. Soit $\mathcal{A}$ un ensemble fini d'éléments de $\Phi(\mathbb{Z}_K)$ vérifiant

$$\Phi(\mathbb{Z}_K) \cap \Big(\mathcal{F} + [-\Gamma(k), \Gamma(k)]^n\Big) \subseteq \mathcal{A},$$

où $\Gamma(k)$ est défini par (2.3). Considérons $x \in H$. Comme $m_{\overline{K}}(x) \leq M(\overline{K})$, il existe un X de $\Phi(\mathbb{Z}_K)$ tel que

$$\mathcal{N}(x - X) < m_{\overline{K}}(x) + \epsilon < k.$$

Les Propositions 2.2 et 2.4 montrent qu'il existe alors une unité $\nu \in E_K$ et un $Y \in \Phi(\mathbb{Z}_K)$ tels que si $y = \Phi(\nu)\cdot x - Y$, alors

$$\mathcal{N}(y) < m_{\overline{K}}(x) + \epsilon < k \quad \text{ et } \quad |y_i| \leq \Gamma(m_{\overline{K}}(x) + \epsilon) \text{ pour tout } i.$$

En considérant alors $z \in \mathcal{F}$ congru à y modulo $\Phi(\mathbb{Z}_K)$, on voit que $z \in \mathrm{Orb}(x)$ et $y = z - Z$ où $Z \in \Phi(\mathbb{Z}_K)$ est tel que

$$|z_i - Z_i| \leq \Gamma(m_{\overline{K}}(x) + \epsilon) \text{ pour tout } i.$$

Mais, il est facile de voir que Γ est une fonction croissante. Par conséquent, on a

$$\Gamma(m_{\overline{K}}(x) + \epsilon) \leq \Gamma(k)$$

et ceci implique $Z \in \mathcal{A}$ par choix de $\mathcal{A}$. Par suite, il existe $z \in \mathrm{Orb}(x)$ et $Z \in \mathcal{A}$ tels que

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

Ceci étant vrai pour tout ϵ suffisamment petit, on a

$$\inf_{z\in\mathrm{Orb}(x)}\left(\min_{Z\in\mathcal{A}}\Big(\mathcal{N}(z-Z)\Big)\right)\leq m_{\overline{K}}(x).$$

D'un autre côté, pour tout $z\in\mathrm{Orb}(x)$ et tout $Z\in\Phi(\mathbb{Z}_K)$, on a par (2.6)

$$m_{\overline{K}}(x)=m_{\overline{K}}(z)\leq\mathcal{N}(z-Z),$$

d'où l'inégalité

$$m_{\overline{K}}(x)\leq\inf_{z\in\mathrm{Orb}(x)}\left(\min_{Z\in\mathcal{A}}\Big(\mathcal{N}(z-Z)\Big)\right),$$

et la conclusion. □

Nous verrons plus tard que cela implique que $\mathrm{sp}(\overline{K})$ est fermé, mais avant cela, nous allons montrer comment calculer $m_K(\xi)$ si ξ est un élément quelconque de K.

2.2 Calcul de $m_K(\xi)$ pour $\xi\in K$

Si le résultat précédent a une valeur intrinsèque, il n'est pas effectif pour deux raisons. D'abord on a une borne inférieure définie sur l'orbite qui peut être infinie. D'autre part, l'ensemble $\mathcal{A}$ est défini à partir de $M(\overline{K})$. Or en pratique, on ne connaît pas a priori $M(\overline{K})$. Le premier obstacle est levé lorsque x est un point rationnel, et nous allons développer ici un procédé permettant de calculer $m_K(\xi)$ où $\xi\in K$.

Proposition 2.7. *Soit $x\in H$. Alors,* $\mathrm{Orb}(x)$ *est finie si et seulement si x est un point rationnel, i.e. un élément de $\Phi(K)$.*

Preuve. Supposons d'abord $\mathrm{Orb}(x)$ finie. Alors, comme $r\geq 1$, E_K est infini. Il existe donc deux unités distinctes ε et ε' vérifiant $\Phi(\varepsilon)\cdot x=\Phi(\varepsilon')\cdot x \bmod \Phi(\mathbb{Z}_K)$, ce qui donne

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

Réciproquement, si $x\in\Phi(K)$, x peut s'écrire $\Phi(\Upsilon/d)$ où $\Upsilon\in\mathbb{Z}_K$ et $d\in\mathbb{N}^*$. $\mathrm{Orb}(x)$ est alors l'image par Φ de l'ensemble des classes de $\varepsilon\Upsilon/d$ modulo $\mathbb{Z}_K$, où ε décrit E_K. Mais ce dernier ensemble est fini, car il est en bijection avec l'ensemble des classes de $\varepsilon\Upsilon$ modulo $d\mathbb{Z}_K$, et on sait que $\mathbb{Z}_K/d\mathbb{Z}_K$ est fini, de cardinal d^n. □

On est maintenant en mesure d'établir le principal résultat de cette section.

Théorème 2.8. *Soit $x\in\Phi(K)$ et soit $k>0$ un réel positif donné. Alors* $\mathrm{Orb}(x)$ *est finie et, $z\in\mathrm{Orb}(x)$ étant donné, il n'y a qu'un nombre fini de $Z\in\Phi(\mathbb{Z}_K)$ vérifiant*

$$|z_i-Z_i|\leq\Gamma(k)\ \textit{pour}\ i\in\{1,\ldots,n\},$$

où $\Gamma(k)$ est définie par (2.3). Soit $\mathcal{I}_z$ l'ensemble de ces Z, et posons

$$\mathcal{M}_k=\min_{z\in\mathrm{Orb}(x)}\left(\min_{Z\in\mathcal{I}_z}\Big(\mathcal{N}(z-Z)\Big)\right).$$

Alors

$$\mathcal{M}_k\leq k\ \Rightarrow\ m_{\overline{K}}(x)=\mathcal{M}_k.$$

Preuve. Le caractère fini de $\mathcal{I}_z$ est clair.
Ensuite, pour tout $z \in \mathrm{Orb}(x)$ et tout $Z \in \Phi(\mathbb{Z}_K)$, on a

$$m_{\overline{K}}(x) = m_{\overline{K}}(z) \leq \mathcal{N}(z - Z),$$

et par définition de $\mathcal{M}_k$,

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

Supposons que $m_{\overline{K}}(x) < \mathcal{M}_k$ de telle sorte qu'il existe $X \in \mathcal{R}$ vérifiant

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

Par les Propositions 2.2 et 2.4, il existe une unité ν et un $Y \in \Phi(\mathbb{Z}_K)$ tels que, si $y = \Phi(\nu) \cdot x - Y$, qui est de la forme $z - Z$ avec $(z, Z) \in \mathrm{Orb}(x) \times \Phi(\mathbb{Z}_K)$, on ait

$$\mathcal{N}(y) < \mathcal{M}_k \quad \text{et} \quad |y_i| \leq \Gamma(\mathcal{M}_k) \leq \Gamma(k), \text{ pour tout } i \in \{1, \ldots, n\}.$$

Mais ceci contredit la définition de $\mathcal{M}_k$, et finalement $m_{\overline{K}}(x) = \mathcal{M}_k$. □

On en tire un moyen de calculer explicitement $m_{\overline{K}}(x) = m_K(\xi)$ lorsque $x = \Phi(\xi)$ est un point rationnel.

Corollaire 2.9. *On peut calculer $m_K(\xi) = m_{\overline{K}}(x)$, en un nombre fini d'étapes. On procède comme suit.*
1. *On détermine* $\mathrm{Orb}(x)$.
2. *On calcule $k' = \mathcal{M}_k$ pour un $k > 0$.*
3. *Si $k' \leq k$ on a $m_{\overline{K}}(x) = k'$.*
4. *Sinon on calcule $k'' = \mathcal{M}_{k'}$ et $m_{\overline{K}}(x) = k''$.*

Preuve. Il suffit de prouver que ce qui est avancé au point 4 est exact. Or, comme $\mathcal{M}_k$ est une fonction décroissante de k, si $k' > k$ on a

$$k'' = \mathcal{M}_{k'} \leq \mathcal{M}_k = k'.$$

Ainsi le Théorème 2.8 s'applique et $m_{\overline{K}}(x) = k''$. □

Terminons par une remarque.

Remarque 2.10. Évidemment, il n'est pas nécessaire de procéder de cette manière si x est de la forme $X + \Phi(1/\Upsilon)$ avec $X \in \Phi(\mathbb{Z}_K)$ et $\Upsilon \notin E_K$. La Proposition 1.11 nous donne directement $m_{\overline{K}}(x) = 1/|N_{K/\mathbb{Q}}(\Upsilon)|$. Nous verrons qu'en pratique, il est assez fréquent d'être ramené à cette situation lorsqu'on veut calculer $M(\overline{K})$.

2.3 Propriétés topologiques complémentaires

Dans cette section, nous allons encore une fois généraliser des résultats que Barnes et Swinnerton-Dyer [BSD52b, Théorème L] ont établis dans le cadre des corps quadratiques réels.

Proposition 2.11. *Soit un ensemble fini $\mathcal{A}$ vérifiant la propriété du Théorème 2.6. Alors, pour tout $\lambda \in \mathrm{sp}(\overline{K})$, il existe un $t \in \overline{\mathcal{F}}$ tel que $m_{\overline{K}}(t) = \lambda$ et un $X \in \mathcal{A}$ tel que $\mathcal{N}(t - X) = \lambda$.*

Preuve. Par définition de $\mathrm{sp}(\overline{K})$, il existe $x \in H$ tel que $m_{\overline{K}}(x) = \lambda$. Or

$$m_{\overline{K}}(x) = \inf_{z \in \mathrm{Orb}(x)} \left(\min_{Z \in \mathcal{A}} \Big(\mathcal{N}(z - Z) \Big) \right).$$

Cela signifie que l'on a une suite (z_p) d'éléments de $\mathrm{Orb}(x)$ et une suite (Z_p) d'éléments de $\mathcal{A}$ telle que

$$\lim_{p \to +\infty} \mathcal{N}(z_p - Z_p) = \lambda.$$

La suite (z_p) étant incluse dans $\mathcal{F}$, elle est bornée et on peut en extraire une sous-suite $(z_{\phi(p)})$ convergeant vers un élément t de $\overline{\mathcal{F}}$.

$$\lim_{p \to +\infty} z_{\phi(p)} = t. \tag{2.7}$$

Comme $\mathcal{A}$ est fini, il existe un $X \in \mathcal{A}$ égal à une infinité de termes $Z_{\phi(p)}$, et quitte à extraire une deuxième fois on peut supposer $Z_{\phi(p)} = X$ pour tout p. Ainsi a-t-on

$$\lim_{p \to +\infty} \mathcal{N}(z_{\phi(p)} - X) = \lambda.$$

Par continuité de $\mathcal{N}$ on a alors par (2.7)

$$\mathcal{N}(t - X) = \lambda \quad \text{et donc} \quad m_{\overline{K}}(t) \leq \lambda. \tag{2.8}$$

Or les z_p étant dans $\mathrm{Orb}(x)$ vérifient par (2.6)

$$m_{\overline{K}}(z_p) = m_{\overline{K}}(x), \text{ pour tout } p. \tag{2.9}$$

Par semi-continuité supérieure de $m_{\overline{K}}$ on déduit de (2.7) et (2.9)

$$m_{\overline{K}}(t) \geq \limsup_{p \to +\infty} m_{\overline{K}}(z_{\phi(p)}) = m_{\overline{K}}(x) = \lambda,$$

ce qui compte tenu de (2.8) donne la conclusion. □

Théorème 2.12. *Le spectre inhomogène de K, $\mathrm{sp}(\overline{K})$, est fermé.*

Preuve. Soit $(\lambda_p)_{p \geq 0}$ une suite d'éléments de $\mathrm{sp}(\overline{K})$, convergeant vers un réel λ. Il nous faut montrer que $\lambda \in \mathrm{sp}(\overline{K})$, autrement dit qu'il existe $x \in H$ vérifiant $m_{\overline{K}}(x) = \lambda$.
Par la Proposition 2.11, et avec les mêmes notations que dans celle-ci, pour chaque p, il existe un couple $(t_p, X_p) \in \overline{\mathcal{F}} \times \mathcal{A}$ vérifiant

$$m_{\overline{K}}(t_p) = \lambda_p \quad \text{et} \quad \mathcal{N}(t_p - X_p) = \lambda_p. \tag{2.10}$$

En argumentant de la même manière que précédemment, on peut extraire de (t_p) une sous-suite $(t_{\phi(p)})$ convergeant vers un $t \in \overline{\mathcal{F}}$ et vérifiant

$$\mathcal{N}(t_{\phi(p)} - A) = \lambda_{\phi(p)} \quad \text{pour un } A \text{ donné de } \mathcal{A}. \tag{2.11}$$

Alors on a $m_{\overline{K}}(t) = \lambda$ par un argument similaire à celui de la précédente preuve. En effet, par continuité de $\mathcal{N}$, (2.11) donne $\mathcal{N}(t - A) = \lambda$, d'où

$$m_{\overline{K}}(t) \leq \lambda.$$

Par ailleurs (2.10) indique que

$$m_{\overline{K}}(t_{\phi(p)}) = \lambda_{\phi(p)}, \text{ pour tout } p,$$

et en faisant tendre p vers $+\infty$, la semi-continuité de $m_{\overline{K}}$ donne

$$\lambda = \limsup_{p \to +\infty} m_{\overline{K}}(t_{\phi(p)}) \leq m_{\overline{K}}(t),$$

et la conclusion. $\square$

Chapitre 3

Calcul explicite de $M(K)$ dans le cas totalement réel

Ce chapitre reprend essentiellement l'article "Euclidean minima of totally real number fields. Algorithmic determination", accepté pour publication dans *Mathematics of Computation.*

Nous supposerons que K est un corps de nombres totalement réel de degré $n \geq 2$. Nous aurons par conséquent

$$r = n-1 \quad \text{et} \quad H = \mathbb{R}^n.$$

Notre objectif est de calculer $M(K)$ algorithmiquement. Rappelons que nous disposons d'un système d'unités fondamentales $(\varepsilon_i)_{1\leq i\leq n-1}$. Ici, nous avons donc

$$E_K = \{\pm\varepsilon_1^{m_1}\dots\varepsilon_{n-1}^{m_{n-1}};\ (m_1,\dots,m_{n-1}) \in \mathbb{Z}^{n-1}\}.$$

Dans tout ce qui suit $\mathcal{F}$ désigne encore un domaine fondamental défini à partir d'une $\mathbb{Z}$-base $(e_i)_{1\leq i\leq n}$ de $\mathbb{Z}_K$ par (2.5).

3.1 La stratégie générale

Pour simplifier l'exposé nous supposerons d'abord que nous avons une idée de la valeur exacte de $M(K)$. Nous verrons dans la section 3.3.9 comment trouver un bon candidat pour $M(K)$. Dorénavant nous noterons k la valeur de $M(K)$ pressentie.

En fait, au lieu de prouver $M(K) = k$, nous allons établir, en rapport avec ce qui a été dit plus haut, le résultat suivant.

$$M(\overline{K}) \leq k \text{ et il existe } \xi \in K \text{ tel que } m_K(\xi) = k.$$

En particulier nous aurons

$$M(K) = M(\overline{K}) = k.$$

Nous allons donc travailler avec $m_{\overline{K}}$, ce qui permettra d'utiliser des arguments géométriques. Par ailleurs, nous tenterons de déterminer tous les points critiques rationnels.

Comme $m_{\overline{K}}$ est définie modulo $\Phi(\mathbb{Z}_K)$, il suffit de travailler sur $\mathcal{F}$, c'est-à-dire de montrer que pour tout $x \in \mathcal{F}$, $m_{\overline{K}}(x) \leq k$ et de trouver tous les $\xi \in K$ tels que $\Phi(\xi) \in \mathcal{F}$ et $m_K(\xi) = k$. Toute autre point critique rationnel sera alors congru à l'un de ces $\Phi(\xi)$ modulo $\Phi(\mathbb{Z}_K)$.

Soit k' un réel positif strictement inférieur à k. En pratique on prendra

$$k' = k - \epsilon, \text{ avec } \epsilon > 0 \text{ petit.}$$

Si $X \in \Phi(\mathbb{Z}_K)$ et si $R > 0$, l'ensemble des points x de $H = \mathbb{R}^n$ vérifiant $\mathcal{N}(x - X) \leq R$ est une région hyperbolique centrée en X, et nous dirons que R est son *rayon.*

Considérons une famille finie d'éléments de $\Phi(\mathbb{Z}_K)$, notée $\mathcal{X}$, et les régions hyperboliques centrées aux X de $\mathcal{X}$ et de rayon k'. Tout élément x du sous-ensemble $\mathcal{J}$ de $\mathcal{F}$, recouvert par ces régions hyperboliques, vérifie $m_{\overline{K}}(x) \leq k' < k$, et comme k' est supposé plus petit que $M(\overline{K})$, des «trous» apparaissent dans le recouvrement de $\mathcal{F}$ par ces régions. Ces trous contiennent les points critiques de $\mathcal{F}$.

La Figure 3.1 illustre ce qui se passe avec $K = \mathbb{Q}(\sqrt{2})$. Ici $k' = 0.35$ et nous avons pris pour $\mathcal{F}$ le parallélogramme dont les quatre sommets sont $A = \Phi(0)$, $B = \Phi(1)$, $C = \Phi(\sqrt{2})$ et $D = \Phi(\sqrt{2} - 1)$. Pour $\mathcal{X}$ nous avons pris l'ensemble de ces quatre points. Nous voyons que les quatre régions hyperboliques recouvrent presqu'entièrement $\mathcal{F}$. En fait, un seul trou T apparaît.

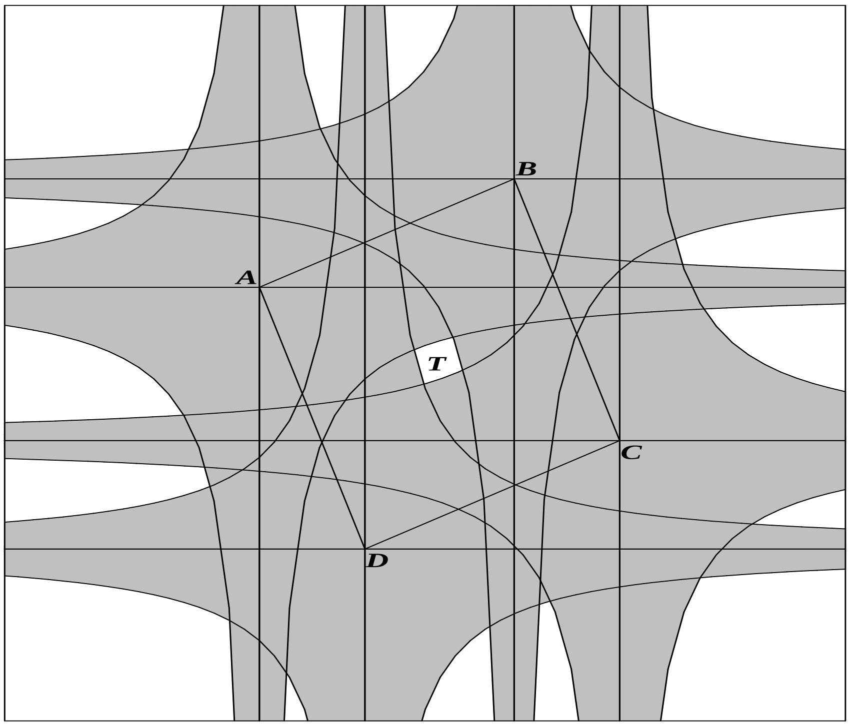

FIG. 3.1: Recouvrement de $\mathcal{F}$ par des régions hyperboliques.

L'idée principale est alors d'analyser l'action du groupe des unités E_K sur les régions non recouvertes de $\mathcal{F}$, de la façon suivante. Soit T un trou apparaissant dans $\mathcal{F}$, et ε

une unité de K vérifiant $\varepsilon \neq \pm 1$, c'est-à-dire ici une unité d'ordre infini. Nous observons les intersections éventuelles de $\Phi(\varepsilon) \cdot T$ avec les trous de $\mathcal{F}$ modulo $\Phi(\mathbb{Z}_K)$. Si $\Phi(\varepsilon) \cdot T$ n'intersecte aucun trou de $\mathcal{F}$ modulo $\Phi(\mathbb{Z}_K)$, on sait par la Proposition 1.15 que pour tout x de T, on a $m_{\overline{K}}(x) \leq k'$, de telle sorte que T peut être éliminé de la liste des régions de $\mathcal{F}$ contenant éventuellement des points critiques. Le cas intéressant est celui d'une intersection non vide. Dans la Figure 3.2, qui correspond à la Figure 3.1, nous voyons ce

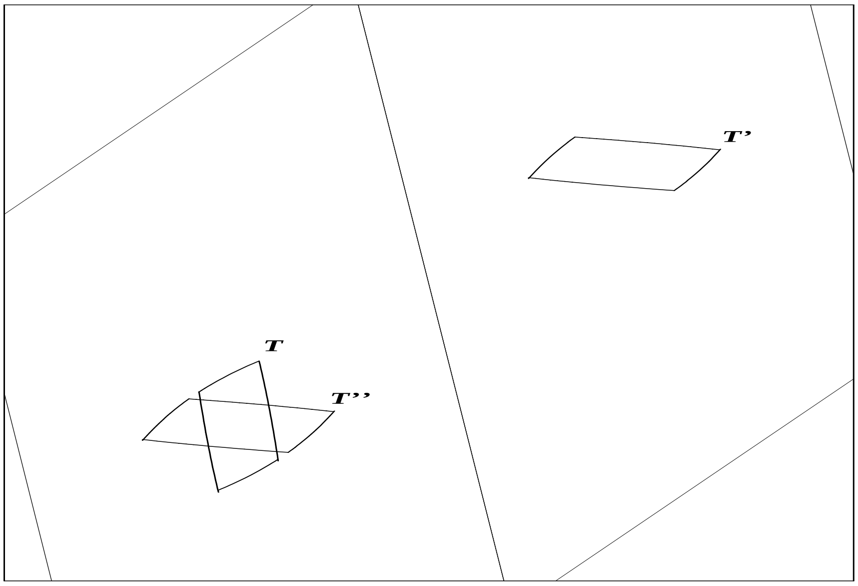

FIG. 3.2: $T'' = \Phi(1+\sqrt{2}) \cdot T - \Phi(1)$ rencontre T.

qui se passe avec $K = \mathbb{Q}(\sqrt{2})$. Ici, $T' = \Phi(1+\sqrt{2}) \cdot T$ et $T'' = \Phi(1+\sqrt{2}) \cdot T - \Phi(1)$. Si $\varepsilon = 1+\sqrt{2}$ et $\Upsilon = 1$, nous pouvons écrire

$$(\Phi(\varepsilon) \cdot T - \Phi(\Upsilon)) \setminus \mathcal{G} \subseteq T,$$

où $\mathcal{G}$ est le sous-ensemble de $H = \mathbb{R}^n$ constitué par les éléments x vérifiant $m_{\overline{K}}(x) \leq k' < k$ (en particulier $\mathcal{J} + \Phi(\mathbb{Z}_K) \subseteq \mathcal{G}$). Cette inclusion correspond au cas de figure le plus simple que l'on puisse rencontrer. Ce que l'on peut dire dans ce cas fera l'objet du prochain théorème.

Remarque 3.1. Ici, nous avons exprimé les choses en termes de trous. Dans la suite, nous considérerons des régions faciles à analyser, plus grandes que les trous. Par exemple, dans l'algorithme, les trous sont remplacés par des régions composées de parallélotopes. Tout ce dont nous avons besoin est de pouvoir partitionner $\mathcal{F}$ en une région recouverte et en régions contenant éventuellement les points critiques. Ensuite nous vérifions que ces régions ont un comportement exploitable sous l'action de E_K.

Cette façon de procéder n'a rien de nouveau. Elle a déjà été exploitée par Barnes et Swinnerton-Dyer [BSD52a] dans le cas quadratique, et Cavallar et Lemmermeyer [CaL98] ont élaboré à partir de l'idée précédente un algorithme de calcul de $M(K)$ dans le cas cubique. Toutefois, nous allons développer ici une procédure plus efficace que les algorithmes existants. Il y a essentiellement trois raisons à cela :

- la façon de découper $\mathcal{F}$ suivant des parallélotopes à faces orthogonales aux axes définis par la base canonique de $H = \mathbb{R}^n$, ce choix permettant de travailler avec une précision optimale,
- le recours à la semi-continuité supérieure de $m_{\overline{K}}$, qui, sous certaines conditions, permettra de ramener l'étude à celle de certains points critiques rationnels,
- le recours à la notion de graphe convenable qui permettra de traiter les cas où $M(\overline{K})$ n'est pas atteint, ce qui n'était pas fait jusqu'alors.

3.2 Arguments théoriques

Comme précédemment nous considérons $k' > 0$ et le sous-ensemble $\mathcal{G}$ de $H = \mathbb{R}^n$ défini par

$$\mathcal{G} = \{x \in H \text{ tels que } m_{\overline{K}}(x) \leq k'\}.$$

Nous prenons aussi une unité $\varepsilon \neq \pm 1$.

3.2.1 Un cas simple

La situation cyclique étudiée dans le prochain théorème est une généralisation de celle observée dans la Figure 3.2. Celui-ci permet de voir que dans la situation particulière où certaines régions contenant des trous s'envoient cycliquement les unes sur les autres, les points x vérifiant $m_{\overline{K}}(x) > k'$ ne peuvent pas être pires que certains points rationnels ξ, pour lesquels, comme on l'a vu, $m_K(\xi)$ est calculable.

Théorème 3.2. *Soient $\mathcal{T}_0, \ldots, \mathcal{T}_{j-1}$ des parties non vides bornées de $H = \mathbb{R}^n$ $(j \geq 1)$. Supposons que pour tout l il existe un $\Upsilon_l \in \mathbb{Z}_K$ tel que*

$$(\Phi(\varepsilon) \cdot \mathcal{T}_l - \Phi(\Upsilon_l)) \setminus \mathcal{G} \subseteq \mathcal{T}_{l+1 \bmod j}. \tag{3.1}$$

Supposons également qu'il existe $x \in \mathcal{T}_0$ vérifiant $m_{\overline{K}}(x) > k'$ et définissons $\Omega \in \mathbb{Z}_K$ par

$$\Omega = \varepsilon^{j-1}\Upsilon_0 + \varepsilon^{j-2}\Upsilon_1 + \ldots + \varepsilon\Upsilon_{j-2} + \Upsilon_{j-1}.$$

Considérons la suite $(y_p)_{p\geq 0}$ définie par $y_0 = x$ et $y_{p+1} = \Phi(\varepsilon^j) \cdot y_p - \Phi(\Omega)$ pour tout $p \geq 0$. Alors, si nous posons

$$\xi = \frac{\Omega}{\varepsilon^j - 1} \quad et \quad t = \Phi(\xi),$$

nous avons

i) *Pour tout $i \in \{1, \ldots, n\}$ tel que $|\sigma_i(\varepsilon)| > 1$ et tout $p \geq 0$, $(y_p)_i = t_i$.*

ii) *La suite $(y_p)_{p\geq 0}$ converge vers t.*

iii) $k' < m_{\overline{K}}(x) \leq m_{\overline{K}}(t)$.

iv) *Si $x \in \Phi(K)$ alors $x = t$.*

Preuve. Montrons d'abord

$$\big(\Phi(\varepsilon^j)\cdot\mathcal{T}_0 - \Phi(\Omega)\big)\setminus\mathcal{G} \subseteq \mathcal{T}_0. \tag{3.2}$$

Posons $z = \Phi(\varepsilon^j)\cdot z_0 - \Phi(\Omega)$ où $z_0 \in \mathcal{T}_0$ et supposons que $z \notin \mathcal{G}$ c'est-à-dire $m_{\overline{K}}(z) > k'$. Définissons $z_1, z_2, \ldots, z_j$ par la formule de récurrence

$$z_{p+1} = \Phi(\varepsilon)\cdot z_p - \Phi(\Upsilon_p),\ \text{pour } 0 \le p < j.$$

Il est facile de voir que

$$z_j = z.$$

Par la Proposition 1.15 on peut donc écrire

$$m_{\overline{K}}(z) = m_{\overline{K}}(z_j) = m_{\overline{K}}(z_{j-1}) = \ldots = m_{\overline{K}}(z_0) > k'.$$

Ainsi, pour tout $p \in \{0, \ldots, j\}$ on a $z_p \notin \mathcal{G}$, et par applications successives de (3.1) on obtient $z_p \in \mathcal{T}_p$ pour tout $p \in \{0, \ldots, j-1\}$, et finalement $z = z_j \in \mathcal{T}_0$, de telle sorte que (3.2) est établie.

Considérons maintenant la suite $(y_p)_{p\ge 0}$. Par la Proposition 1.15 nous voyons par récurrence que pour tout $p \ge 0$

$$m_{\overline{K}}(y_p) = m_{\overline{K}}(x) > k', \tag{3.3}$$

si bien que pour tout $p \ge 0$, $y_p \notin \mathcal{G}$. Ensuite, comme $y_0 = x \in \mathcal{T}_0$, en utilisant (3.2) on établit facilement par récurrence que $y_p \in \mathcal{T}_0$ pour tout $p \ge 0$. Ainsi, comme $\mathcal{T}_0$ était supposée bornée, la suite $(y_p - t)_{p\ge 0}$ est bornée.

Mais la définition de t et la formule de récurrence qui définit $(y_p)_{p\ge 0}$ montrent que $y_p - t = \Phi(\varepsilon^j)^p\cdot(x - t)$ pour tout $p \ge 0$, de telle sorte que

$$|(y_p)_i - t_i| = |\sigma_i(\varepsilon)|^{jp}\,|x_i - t_i| \text{ pour tout } i \in \{1, \ldots, n\} \text{ et pour tout } p \ge 0. \tag{3.4}$$

Supposons $|\sigma_i(\varepsilon)| > 1$. Comme la suite $(|(y_p)_i - t_i|)_{p\ge 0}$ est bornée, nous devons avoir $x_i - t_i = 0$, et par (3.4) nous obtenons

$$(y_p)_i = t_i \text{ pour tout } p \ge 0. \tag{3.5}$$

C'est le point i).

De plus, si $|\sigma_i(\varepsilon)| < 1$, alors (3.4) montre que

$$\lim_{p\to+\infty}(y_p)_i = t_i. \tag{3.6}$$

Mais pout tout $i \in \{1, \ldots, n\}$, on a $|\sigma_i(\varepsilon)| \ne 1$. En effet, s'il existait i vérifiant $|\sigma_i(\varepsilon)| = 1$, K étant totalement réel, on aurait par injectivité de σ_i, $\varepsilon = \pm 1$, ce qui est exclu par hypothèse. Les équations (3.5) et (3.6) donnent alors

$$\lim_{p\to+\infty} y_p = t.$$

C'est le point ii).
Finalement par semi-continuité supérieure de $m_{\overline{K}}$ et par (3.3), nous obtenons

$$k' < m_{\overline{K}}(x) = \limsup_{p\to+\infty} m_{\overline{K}}(y_p) \leq m_{\overline{K}}(t),$$

ce qui donne iii).

Supposons maintenant que $x \in \Phi(K)$.
Nous ne pouvons pas avoir $|\sigma_i(\varepsilon)| \leq 1$ pour tout i. En effet, dans ce cas, comme $\prod |\sigma_i(\varepsilon)| = 1$, on aurait forcément $|\sigma_i(\varepsilon)| = 1$ pour tout i et $\varepsilon = \pm 1$. Il existe donc un $i \in \{1, \dots, n\}$ tel que $|\sigma_i(\varepsilon)| > 1$, et par i) (avec $p = 0$) on a $x_i = t_i$. Or x et t sont tous deux dans $\Phi(K)$, et l'injectivité de σ_i conduit à $x = t$. □

Remarque 3.3. Évidemment la même propriété vaut pour $\mathcal{T}_1$, $\mathcal{T}_2$, ... le seul changement à effectuer concernant la formule donnant Ω, dans laquelle les indices doivent être permutés. Plus précisément, pour $r \in \{0, \dots, j-1\}$, si nous posons $t_r = \Phi(\xi_r)$ où

$$\xi_r = \frac{\Omega_r}{\varepsilon^j - 1},$$

et

$$\Omega_r = \varepsilon^{j-1}\Upsilon_r + \varepsilon^{j-2}\Upsilon_{r+1 \bmod j} + \ldots + \Upsilon_{j-1+r \bmod j},$$

on a la même propriété que dans le Théoreme 3.2 pour $\mathcal{T}_r$ (avec t_r à la place de t). De plus $t_0 = t$ et on a la loi cyclique suivante.

$$t_{r+1 \bmod j} = \Phi(\varepsilon) \cdot t_r - \Phi(\Upsilon_r)$$

pour tout $r \in \{0, \dots, j-1\}$. En particulier, tous les t_r sont dans $\mathrm{Orb}(t)$.

Exemple 3.4. Dans l'exemple $K = \mathbb{Q}(\sqrt{2})$ vu plus haut (Figures 3.1 et 3.2) avec $\varepsilon = 1 + \sqrt{2}$, on a $j = 1$, et $\Upsilon_0 = 1$. Le Théorème 3.2 montre que pour tout x de T qui vérifie $m_{\overline{K}}(x) > 0.35$, on a nécessairement $m_{\overline{K}}(x) \leq m_K(\xi)$ où $\xi = \sqrt{2}/2$. Comme $m_K(\xi)$ est égal à $1/2$ cela mène à l'égalité $M(K) = M(\overline{K}) = 1/2$, déjà rencontrée dans la Proposition 1.28.

Le Théorème 3.2 admet le corollaire suivant, qui peut être utilisé pour montrer que les points critiques sont isolés et pour calculer le second minimum inhomogène $M_2(\overline{K})$.

Corollaire 3.5. *Plaçons-nous sous les hypothèses du Théorème 3.2. Si ε^{-1} agit sur les $\mathcal{T}_l$ de telle sorte que pour tout l il y a un $\Upsilon'_l \in \mathbb{Z}_K$ tel que*

$$\left(\Phi(\varepsilon^{-1}) \cdot \mathcal{T}_l - \Phi(\Upsilon'_l)\right) \backslash \mathcal{G} \subseteq \mathcal{T}_{l-1 \bmod j},$$

et si nous supposons en outre que $\mathcal{T}_0$ est suffisamment «petit» pour avoir

$$(z_1, z_2) \in \mathcal{T}_0^2 \text{ et } z_1 - z_2 \in \Phi(\mathbb{Z}_K) \Rightarrow z_1 = z_2, \tag{3.7}$$

alors on a la conclusion plus forte $x = t$.

Preuve. Définissons y_1' par

$$y_1' = \Phi(\varepsilon^{-j}) \cdot x - \Phi(\Omega'), \tag{3.8}$$

où $\Omega' = \varepsilon^{1-j}\Upsilon_0' + \varepsilon^{2-j}\Upsilon_1' + \ldots + \varepsilon^{-1}\Upsilon_{j-2}' + \Upsilon_{j-1}'$. En recommençant comme dans la démonstration précédente, mais en inversant l'ordre sur les $\mathcal{T}_l$, nous voyons que $y_1' \in \mathcal{T}_0 \backslash \mathcal{G}$. Mais par (3.2), on a encore

$$\Phi(\varepsilon^j) \cdot y_1' - \Phi(\Omega) \in \mathcal{T}_0 \backslash \mathcal{G}.$$

Alors (3.8) donne

$$x - \Phi(\varepsilon^j \Omega' + \Omega) \in \mathcal{T}_0 \backslash \mathcal{G}.$$

Nous voyons alors que x et $x - \Phi(\varepsilon^j\Omega' + \Omega)$ sont tous deux dans $\mathcal{T}_0$, et comme leur différence appartient à $\Phi(\mathbb{Z}_K)$, (3.7) implique qu'ils sont égaux. On a donc

$$\varepsilon^j \Omega' + \Omega = 0. \tag{3.9}$$

Par le Théorème 3.2 (appliqué avec ε^{-1} et $p = 0$) et (3.9), nous trouvons que

$$x_i = \left(\frac{\Omega'}{\varepsilon^{-j} - 1}\right)_i = \left(\frac{\Omega}{\varepsilon^{j} - 1}\right)_i = t_i, \tag{3.10}$$

pour tout i tel que $|\sigma_i(\varepsilon^{-1})| > 1$.

Mais on sait aussi par le Théorème 3.2 que

$$\text{pour tout } i \text{ tel que } |\sigma_i(\varepsilon)| > 1, \; x_i = t_i. \tag{3.11}$$

Puisque pour tout i, $|\sigma_i(\varepsilon)| \neq 1$, (3.10) et (3.11) donnent $x = t$. □

3.2.2 Généralisation

Même si le Théorème 3.2 nous permettra de déterminer $M(K)$ dans un grand nombre de situations, il ne suffira pas pour couvrir tous les cas que nous serons amenés à rencontrer dans la pratique. Nous devons généraliser le précédent résultat et c'est l'objet de cette section.

Soient $\mathcal{T}_i$ $(0 \leq i \leq s-1)$ des parties distinctes et bornées de $H = \mathbb{R}^n$, et $T = \{\mathcal{T}_0, \ldots, \mathcal{T}_{s-1}\}$. Supposons que pour tout $\mathcal{T}_i$ de T il existe un $X_i \in \Phi(\mathbb{Z}_K)$ et s_i entiers $n_{i,1}, \ldots, n_{i,s_i}$ $(s_i > 0)$ tels que

$$(\Phi(\varepsilon) \cdot \mathcal{T}_i - X_i) \setminus \mathcal{G} \subseteq \bigcup_{1 \leq k \leq s_i} \mathcal{T}_{n_{i,k}}, \tag{3.12}$$

où $\mathcal{G}$ est toujours l'ensemble des $x \in H = \mathbb{R}^n$ vérifiant $m_{\overline{K}}(x) \leq k'$.

Pour simplifier les notations nous considérerons les $\mathcal{T}_i$ comme les sommets d'un graphe orienté G et représenterons (3.12) par s_i arêtes orientées ou arcs, dont l'extrémité initiale est $\mathcal{T}_i$ et dont les extrémités finales respectives sont les $\mathcal{T}_{n_{i,k}}$ $(1 \leq k \leq s_i)$. Bien sûr un tel arc peut être une boucle (arc joignant un sommet à lui-même).

Nous écrirons $\mathcal{T}_i \to \mathcal{T}_{n_{i,k}}$ (X_i) ou $\mathcal{T}_i \to \mathcal{T}_{n_{i,k}}$, s'il n'est pas nécessaire de préciser X_i.

Exemple 3.6. Le Théorème 3.2 correspond au graphe orienté

$$G_1 : \mathcal{T}_0 \to \mathcal{T}_1 \ (\Phi(\Upsilon_0)), \dots , \mathcal{T}_{j-1} \to \mathcal{T}_0 \ (\Phi(\Upsilon_{j-1})).$$

Pour décrire un chemin de G nous utiliserons la notation $\mathcal{T}'_1 \to \mathcal{T}'_2 \to \dots \to \mathcal{T}'_k$.

Le graphe orienté G qui représente la situation dans laquelle nous supposons nous trouver et qui est caractérisée par (3.12) a les propriétés suivantes. Si $\mathcal{T}$ et $\mathcal{T}'$ sont des sommets de G, il y a au plus un arc joignant $\mathcal{T}$ à $\mathcal{T}'$, et tout sommet de G a une valence sortante positive. Cette dernière propriété implique que G contient des chemins cycliques (cycles ou circuits). Par conséquent, l'ensemble des cycles simples de G (chemins de la forme $\mathcal{T}'_0 \to \dots \to \mathcal{T}'_k \to \mathcal{T}'_0$, où $k \geq 0$ et tous les $\mathcal{T}'_i$ sont distincts) est *non vide* (prendre un cycle de longueur minimale) et est *fini* (leur longueur ne peut excéder s). Notons cet ensemble $\mathcal{C}$. Chaque élément c de $\mathcal{C}$ de longueur j est de la forme du cycle du Théorème 3.2 (et noté plus haut G_1), $\mathcal{T}'_0 \to \mathcal{T}'_1(X'_0) \dots \to \mathcal{T}'_{j-1}(X'_{j-2}) \to \mathcal{T}'_0(X'_{j-1})$ avec $X'_i = \Phi(\Upsilon_i)$. Il définit, de façon unique, j points rationnels $t_0, \dots , t_{j-1}$ par les formules de la Remarque 3.3.

Définition 3.7. Dans ce contexte, on dira que $t_0, \dots , t_{j-1}$ sont *associés* à c (implicitement t_i correspond à $\mathcal{T}'_i$).

Les t_i sont dans la même orbite et vérifient donc $m_{\overline{K}}(t_0) = \dots = m_{\overline{K}}(t_{j-1})$. Notons ce nombre rationnel $m(c)$ et posons

$$m(G) = \max_{c\in\mathcal{C}} m(c).$$

De plus, notons $\mathcal{E}$ l'ensemble des points rationnels associés aux éléments de $\mathcal{C}$. L'ensemble $\mathcal{E}$ est *fini* et l'on a également

$$m(G) = \max \{m_{\overline{K}}(t);\ t \in \mathcal{E}\}.$$

Finalement posons

$$\mathcal{E}' = \{t \in \mathcal{E} \text{ tels que } m_{\overline{K}}(t) = m(G)\}.$$

Définition 3.8. Un *chemin infini* de G est une suite infinie $(A_i)_{i\geq 0}$ d'arcs de G, vérifiant que, pour tout i, l'extrémité finale de A_i est égale à l'extrémité initiale de A_{i+1}. Si A_i est défini par $\mathcal{T}'_i \to \mathcal{T}'_{i+1}$, nous noterons $(\mathcal{T}'_i)_{i\geq 0}$ le chemin infini défini par les A_i.

Un tel chemin ne peut pas être simple, mais peut présenter une propriété de périodicité.

Définition 3.9. Un chemin infini $(\mathcal{T}'_i)$ est dit *ultimement périodique* s'il existe des entiers $r \geq 0$ et $p \geq 1$ tels que

$$\text{pour tout } i \geq r,\ \mathcal{T}'_{i+p} = \mathcal{T}'_i. \tag{3.13}$$

Soit $(\mathcal{T}'_i)_{i\geq 0}$ un chemin infini ultimement périodique. Soit $\mathcal{P}$ l'ensemble des $p \geq 1$ tels qu'il existe r vérifiant (3.13). $\mathcal{P}$ est non vide et nous pouvons définir le nombre ρ suivant.

$$\rho = \min \mathcal{P} \geq 1. \tag{3.14}$$

Alors nous savons qu'il existe un r_ρ vérifiant

$$\text{pour tout } i \geq r_\rho,\ \mathcal{T}'_{i+\rho} = \mathcal{T}'_i. \tag{3.15}$$

Définition 3.10. L'entier ρ sera appelé la longueur de période de $(\mathcal{T}_i')_{i\geq 0}$ et chaque cycle $\mathcal{T}_i' \to \ldots \to \mathcal{T}_{i+\rho}'$, où $i \geq r_\rho$, sera appelé une période de $(\mathcal{T}_i')_{i\geq 0}$

Définition 3.11. Nous dirons que G est *convenable* si tout chemin infini de G est ultimement périodique.

Exemple 3.12. Le graphe G_1 de l'Exemple 3.6 est convenable. Dans la Figure 3.3 on trouvera des exemples de graphes orientés convenables et non convenables.

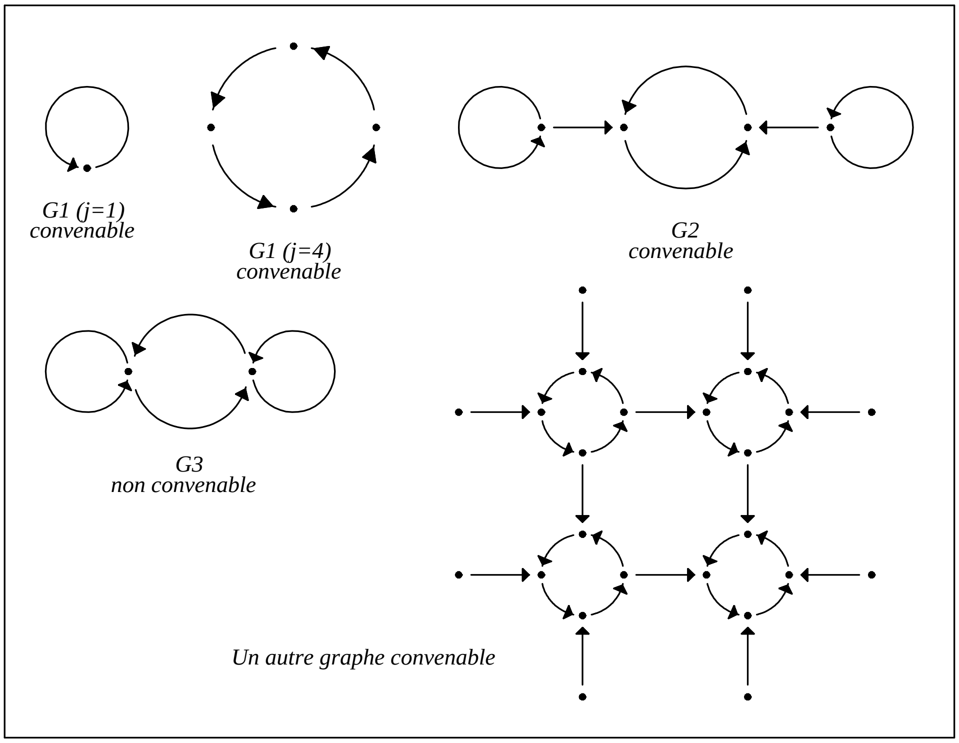

FIG. 3.3: Quelques graphes orientés.

Proposition 3.13. *Supposons que G soit convenable. Alors tout cycle est puissance d'un cycle simple.*

Preuve. Soit c un cycle de G. Notons le $\mathcal{T} \to \ldots \to \mathcal{T}$. Décomposons c sous la forme $c_1c_2\ldots c_d$ ($d \geq 1$) où les c_i sont des cycles de la forme $\mathcal{T} \to \ldots \to \mathcal{T}$ "simples en $\mathcal{T}$". Supposons qu'il existe $i > 1$ avec $c_i \neq c_1$. Alors nous pouvons construire un chemin infini non ultimement périodique, à savoir $c_1c_ic_1c_1c_ic_1c_1c_1c_i\ldots$, ce qui contredit le caractère convenable de G. Ainsi $c = c_1^d$.
Montrons maintenant que c_1 est simple. S'il ne l'était pas, comme il est "simple en $\mathcal{T}$", il serait de la forme $\mathcal{T} \to \ldots \to \mathcal{T}' \to \ldots \to \mathcal{T}' \to \ldots \to \mathcal{T}$ où $\mathcal{T}' \neq \mathcal{T}$ et où $\mathcal{T}$ n'est pas un sommet de $\mathcal{T}' \to \ldots \to \mathcal{T}'$. Si nous décomposons c_1 en le produit des chemins $P_1P_2P_3$ où $P_2 = \mathcal{T}' \to \ldots \to \mathcal{T}'$, nous voyons que $P_1P_3 = P$ et P_2 sont deux cycles ayant un sommet commun $\mathcal{T}'$. Nous pouvons donc définir le chemin infini $PP_2PP_2P_2PP_2P_2P_2P\ldots$ qui n'est pas ultimement périodique puisque $\mathcal{T}$ n'est pas un sommet de P_2. Une fois encore, cela contredit le fait que G soit convenable. $\square$

Remarque 3.14. On peut montrer que la réciproque est exacte. Une autre caractérisation des graphes orientés convenables pourrait être la suivante : deux cycles simples distincts n'ont pas de sommet commun.

Corollaire 3.15. *Supposons que G soit convenable et soit $P = (\mathcal{T}_i')_{i\geq 0}$ un chemin infini de G. Alors, P est ultimement périodique et toute période de P est un cycle simple.*

Preuve. Comme G est convenable P est ultimement périodique. Considérons une période c de longueur ρ. Par la Proposition 3.13, c est la puissance d'un cycle simple c_1, et $c = c_1^d$ avec $d \geq 1$. Mais si $d > 1$, il est clair que c_1 a une longueur $p = \rho/d$ strictement inférieure à ρ. De $c = c_1^d$ et (3.14) nous tirons $p \in \mathcal{P}$, mais ceci contredit (3.14). Ainsi $d = 1$ et c est simple. □

Maintenant, nous allons établir le théorème qui va nous permettre de traiter en pratique toutes les situations, à de très rares exceptions près (problème de dépassement de temps de calcul imposé).

Théorème 3.16. *Supposons que G soit convenable et qu'il existe un $\mathcal{T} \in T$ et un $x \in \mathcal{T}$ tels que $m_{\overline{K}}(x) > k'$. Alors*

i) $k' < m_{\overline{K}}(x) \leq m(G)$.

ii) *Si $x \in \Phi(K)$, il existe un $t \in \mathcal{E}$ tel que $x \equiv t \bmod \Phi(\mathbb{Z}_K)$.*

iii) *Si $x \in \Phi(K)$ est critique, il existe un $t \in \mathcal{E}'$ tel que $x \equiv t \bmod \Phi(\mathbb{Z}_K)$.*

Preuve. Posons $x_0 = x$ et $\mathcal{T}_0' = \mathcal{T}$. Par (3.12) nous savons qu'il existe $X_0' \in \Phi(\mathbb{Z}_K)$ et s_0' éléments de T, notés $\mathcal{T}_{n_{0,k}'}$ $(1 \leq k \leq s_0')$ tels que

$$(\Phi(\varepsilon) \cdot \mathcal{T}_0' - X_0') \setminus \mathcal{G} \subseteq \bigcup_{1\leq k\leq s_0'} \mathcal{T}_{n_{0,k}'}.$$

Soit $x_1 = \Phi(\varepsilon) \cdot x_0 - X_0'$. Comme $m_{\overline{K}}(x_1) = m_{\overline{K}}(x_0) > k'$, on a

$$x_1 \in (\Phi(\varepsilon) \cdot \mathcal{T}_0' - X_0') \setminus \mathcal{G},$$

et nécessairement, il y a un indice $i \in \{1, \ldots, s_0'\}$ pour lequel $x_1 \in \mathcal{T}_{n_{0,i}'}$. Posons $\mathcal{T}_1' = \mathcal{T}_{n_{0,i}'}'$, et continuons avec $x_2 = \Phi(\varepsilon) \cdot x_1 - X_1'$ où X_1' est l'élément de $\Phi(\mathbb{Z}_K)$ associé à $\mathcal{T}_1'$ par (3.12). Nous voyons que nous pouvons construire par récurrence une suite $(x_i)_{i\geq 0}$ et un chemin infini $(\mathcal{T}_i')_{i\geq 0}$ qui vérifie

$$x_0 = x \text{ et pour tout } i \geq 0,\ x_{i+1} = \Phi(\varepsilon) \cdot x_i - X_i',\ \text{où } X_i' \in \Phi(\mathbb{Z}_K),$$

ainsi que

$$\text{pour tout } i \geq 0,\ x_i \in \mathcal{T}_i'. \tag{3.16}$$

De plus, par la Proposition 1.15, on a

$$m_{\overline{K}}(x_i) = m_{\overline{K}}(x) > k' \text{ pour tout } i.$$

G étant convenable, le chemin infini $(\mathcal{T}_i')_{i\geq 0}$ est ultimement périodique. Notons sa longueur de période ρ et considérons une de ses périodes c, décrite par $\mathcal{T}_r' \to \ldots \to \mathcal{T}_{r+\rho}' = \mathcal{T}_r'$, qui est un cycle simple d'après le Corollaire 3.15.
Définissons

$$\mathcal{T}_s'' = \{x_{r+s+i\rho};\ i \in \mathbb{N}\}, \qquad \text{pour } 0 \leq s \leq \rho - 1.$$

Par (3.16) nous savons que pour tout $s \in \{0, \ldots, \rho-1\}$, $\mathcal{T}_s'' \subseteq \mathcal{T}_{r+s}'$. Ceci implique que les $\mathcal{T}_s''$ sont bornées. De plus, par construction, pour tout s il existe $\Upsilon_s \in \mathbb{Z}_K$ (en fait $\Phi^{-1}(X_{r+s}')$) tel que

$$\Phi(\varepsilon)\cdot\mathcal{T}_s'' - \Phi(\Upsilon_s)\backslash\mathcal{G} = \Phi(\varepsilon)\cdot\mathcal{T}_s'' - \Phi(\Upsilon_s) \subseteq \mathcal{T}_{s+1 \bmod \rho}''.$$

En posant $y = x_r \in \mathcal{T}_0''$ qui vérifie $m_{\overline{K}}(y) > k'$, nous voyons que nous sommes exactement sous les hypothèses du Théorème 3.2 (avec y à la place de x, $\mathcal{T}_i''$ à la place de $\mathcal{T}_i$ et ρ à la place de j). Ce théorème définit ρ points rationnels t_i associés au cycle simple c.
Par définition de $m(c)$, et par le Théorème 3.2.iii), nous obtenons

$$k' < m_{\overline{K}}(x) = m_{\overline{K}}(x_r) \leq m(c),$$

et par définition de $m(G)$ nous avons i).

Supposons maintenant que $x \in \Phi(K)$ de telle sorte que, par récurrence, $x_r \in \Phi(K)$. Par le Théorème 3.2.iv) on a $x_r = t_0$, et donc $x_r - t_0 \in \Phi(\mathbb{Z}_K)$. Par la formule de récurrence qui définit les x_i et les formules de la Remarque 3.3, nous pouvons écrire

$$\text{pour tout } k \in \{0, \ldots, r\},\ \Phi(\varepsilon)\cdot(x_{r-k} - t_{-k \bmod \rho}) \in \Phi(\mathbb{Z}_K).$$

Finalement, $x = x_0 \equiv t_{-r \bmod \rho} \bmod \Phi(\mathbb{Z}_K)$ qui est un élément de $\mathcal{E}$ par définition de ce dernier ensemble. Ceci prouve ii).

Supposons maintenant que x soit critique, de telle sorte que nous avons $m_{\overline{K}}(x) = M(\overline{K})$. D'après les définitions, nous voyons que $m_{\overline{K}}(x) \geq m(G)$ et par i) nous obtenons $m_{\overline{K}}(x) = m(G)$ si bien que $m_{\overline{K}}(t_{-r \bmod \rho}) = m(G)$. Comme $t_{-r \bmod \rho} \in \mathcal{E}$, nous trouvons $t_{-r \bmod \rho} \in \mathcal{E}'$. Ceci prouve iii). □

Remarque 3.17. Remarquons que dans (3.12) (comme dans les hypothèses du Théorème 3.2), nous pouvons avoir pour un i donné, $(\Phi(\varepsilon)\cdot\mathcal{T}_i - X_i) \setminus \mathcal{G} = \emptyset$. Ceci n'affecte pas l'argumentation.

Remarque 3.18. Nous pourrions, de la même manière, obtenir une généralisation du Corollaire 3.5. Nous ne le ferons pas ici, parce que la détermination des minima inhomogènes successifs n'est pas notre objectif. Néanmoins, nous donnerons ultérieurement un exemple, pour lequel le Corollaire 3.5 suffit pour calculer le second minimum inhomogène.

3.3 L'algorithme. Aspect théorique

À partir de maintenant, nous fixons une $\mathbb{Z}$-base $(e_i)_{1\leq i\leq n}$ de $\mathbb{Z}_K$. Ainsi, K peut être identifié avec $\mathbb{Q}^n$ via l'application $\Psi : \mathbb{Q}^n \to K$ définie par $\Psi(r) = \sum_{i=1}^n r_i e_i$ pour $r \in \mathbb{Q}^n$.

L'application $\Phi \circ \Psi : \mathbb{Q}^n \to \mathbb{R}^n$ peut être prolongée par continuité par $\overline{\Phi} : \mathbb{R}^n \to \mathbb{R}^n$ via

$$\overline{\Phi}(x) = \left(\sum_{i=1}^{n} x_i \sigma_1(e_i), \dots, \sum_{i=1}^{n} x_i \sigma_n(e_i) \right) \qquad \text{pour tout} \qquad x \in \mathbb{R}^n.$$

$\overline{\Phi}$ est un automorphisme $\mathbb{R}$-linéaire de $\mathbb{R}^n$. Sa matrice inversible (par rapport à la base canonique de $\mathbb{R}^n$) sera notée $M = (m_{i,j})_{1 \le i,j \le n}$. On a $|\det(M)| = \sqrt{D_K}$ et

$$M = (\sigma_i(e_j))_{1 \le i,j \le n}\,.$$

La matrice inverse M^{-1} de M sera notée $M' = \left(m'_{i,j}\right)_{1 \le i,j \le n}$.

Notons $\mathcal{F}$ le parallélotope fondamental de volume $\sqrt{D_K}$ défini par

$$\mathcal{F} = \overline{\Phi}\left([0,1)^{\,n}\right) = \left\{ \sum_{i=1}^{n} x_i \Phi(e_i);\ 0 \le x_i < 1 \right\}.$$

3.3.1 Vue d'ensemble de l'algorithme

Supposons comme précédemment que nous avons une idée de $M(K)$ notée k. Supposons que nous avons à notre disposition un ensemble $\mathcal{X}$ d'éléments de $\Phi(\mathbb{Z}_K)$, et prenons un petit $\epsilon > 0$.

Les calculs sont organisés de la façon suivante.

1. La première étape de l'algorithme consiste à recouvrir $\mathcal{F}$ à l'aide de petits parallélotopes. La forme de ces parallélotopes sera précisée plus tard.

2. Suivant la philosophie exposée dans la section 3.1, la seconde étape consiste à éliminer tous les parallélotopes qui sont absorbés par des éléments de $\mathcal{X}$, au sens suivant.

Définition 3.19. Un parallélotope $\mathcal{B}$ sera dit absorbé par $X \in \mathcal{X}$, s'il est contenu dans une région hyperbolique centrée en X, de rayon $k - \epsilon$.

Chaque parallélotope qui ne peut pas être éliminé sera stocké dans une liste de parallélotopes que nous qualifierons de *parallélotopes problématiques*. Soit $\mathcal{P}_i$, $i = 1 \dots N$, cette liste à la fin de cette étape. Tout x appartenant à la réunion $\mathcal{G}'$ des parallélotopes éliminés vérifiera $m_{\overline{K}}(x) \le k - \epsilon$.

3. Ensuite nous utilisons les unités de E_K pour voir si chaque parallélotope problématique est « équivalent » à un sous-ensemble de $\mathcal{G}'$ et peut donc être éliminé. Rappelons que pour chaque $\mathcal{P}_i$ (bien que ce ne soit pas nécessaire - voir plus loin) on multiplie $\mathcal{P}_i$ par $\Phi(\varepsilon)$, où $\varepsilon \neq \pm 1$ est une unité de E_K, et on translate l'ensemble obtenu vers $\mathcal{F}$ à l'aide d'un élément de $\Phi(\mathbb{Z}_K)$, pour voir si l'on se retrouve dans $\mathcal{G}'$. Si c'est le cas on peut éliminer $\mathcal{P}_i$ et agrandir $\mathcal{G}'$.

En fait, c'est un peu plus compliqué car l'ensemble obtenu à l'issue de la multiplication peut traverser plusieurs domaines fondamentaux et peut être ramené de plusieurs façons vers $\mathcal{F}$. Nous expliquerons cela en détail plus loin. Au fur et à mesure, on mémorise pour chaque $\mathcal{P}$ non éliminable, tous les $\mathcal{P}'$ sur lesquels il peut être envoyé. À la fin de la boucle, il est possible que subsistent quelques $\mathcal{P}$, qui avaient été négativement testés à cause de certains $\mathcal{P}'$ éliminés plus tard. Pour cette raison, il est pertinent de parcourir de nouveau les $\mathcal{P}$ restants et de regarder s'ils ne sont pas uniquement envoyés sur des $\mathcal{P}'$ déjà éliminés, et ceci plusieurs fois, jusqu'à ce que le nombre de parallélotopes restants, encore noté N, se stabilise.

4. L'idée suivante est de découper les parallélotopes restants en 2^n parallélotopes plus petits, et de recommencer tout le processus, et ceci, tant que le nombre de parallélotopes restants diminue. Ainsi, nous obtenons par division $2^n N$ nouveaux parallélotopes notés $\mathcal{P}_i'$, nous allons aux étapes 2 et 3, et si à l'issue des deux tests le nombre de tels parallélotopes problématiques N' est inférieur ou égal à N, nous remplaçons les $\mathcal{P}_i$ par les $\mathcal{P}_i'$ et nous recommençons (découpage des $\mathcal{P}_i, \dots$). Si N' est plus grand que N nous nous arrêtons et nous analysons les $\mathcal{P}_i$ à l'aide du Théorème 3.16. Ce théorème, s'il peut être utilisé, nous permet d'obtenir un ensemble optimal $\mathcal{E}$ de points t_i potentiellement critiques, au sens où s'il existe x vérifiant $m_{\overline{K}}(x) > k - \epsilon$ alors $m_{\overline{K}}(x) \leq m(G) = \max(m_{\overline{K}}(t_i))$. De plus ces points sont rationnels et nous pouvons calculer $m_{\overline{K}}(t_i)$ pour $t_i \in \mathcal{E}$ grâce au Corollaire 2.9. Si la valeur pressentie k est le minimum euclidien on aura

$$\text{pour tout } i,\ m_{\overline{K}}(t_i) \leq k \quad \text{ et il existe un } i \text{ tel que } m_{\overline{K}}(t_i) = k,$$

ce qui établit $M(K) = M(\overline{K}) = k$. De surcroît, dans ces conditions, le Théorème 3.16 prouve que les t_i de $\mathcal{E}'$ sont les seuls points rationnels critiques modulo $\Phi(\mathbb{Z}_K)$.

Remarque 3.20. L'algorithme proposé est sans doute améliorable. On pourrait par exemple imaginer une architecture de type quadtree : commencer par un découpage grossier, avec pour but de mémoriser des parallélotopes absorbés les plus grands possibles, et au fur et à mesure des divisions successives, essayer, lorsqu'on étudie un nouveau parallélotope non absorbé, de l'envoyer, à l'aide d'unités appropriées, sur les parallélotopes de taille supérieure que l'on a mémorisés. Nous n'avons pas cherché à concrétiser cette approche dans la mesure où la version présentée ici était suffisamment efficace. Par ailleurs, que l'algorithme termine, au sens où le graphe retourné serait nécessairement convenable, n'est pas a priori une certitude. Nous reviendrons sur ce point dans le chapitre 4, à l'occasion de la Proposition 4.25.

Remarque 3.21. Il est facile de voir que nous pouvons réduire le domaine d'étude à un demi-parallélotope fondamental. Soit s la symétrie centrale de centre $\frac{1}{2}\Phi(\sum e_i)$. Alors

$$\text{pour tout } x \in \mathbb{R}^n,\ m_{\overline{K}}(s(x)) = m_{\overline{K}}(x).$$

Comme $s(x) = \Phi(\sum e_i) - x$, par la Proposition 1.15 avec $\varepsilon = -1$ et $X = -\Phi(\sum e_i)$, nous obtenons que $m_{\overline{K}}(s(x)) = m_{\overline{K}}(x)$. Par conséquent, si $\mathcal{F}'$ est un sous-ensemble de $\mathcal{F}$ tel que $\mathcal{F} \subseteq \mathcal{F}' \cup s(\mathcal{F}')$, nous pouvons restreindre l'étude à $\mathcal{F}'$. Il est donc naturel de définir un recouvrement de $\mathcal{F}$ par une famille de parallélotopes, invariante sous l'action de s. Les choix de $\mathcal{F}'$ et du recouvrement seront exposés plus tard.

Ceci nous amène à différentes questions, en particulier :

- Comment choisissons-nous $\mathcal{X}$?
- Quel genre de parallélotopes utiliserons-nous pour recouvrir $\mathcal{F}$ (ou $\mathcal{F}'$) ? Ce recouvrement doit être facile à définir, pas trop grossier, et surtout, doit permettre de définir des critères simples et précis pour décider si un parallélotope $\mathcal{P}$ est absorbé par un élément de $\mathcal{X}$ ou non, et pour décider si $\Phi(\varepsilon).\mathcal{P}$ rencontre ou non un $\mathcal{P}'$ modulo $\Phi(\mathbb{Z}_K)$. Pour simplifier nous nommerons ces deux tests le *test d'absorption* et le *test des unités*.
- Quelle sera la forme du test d'absorption ? Peut-elle être optimale ?
- Mêmes questions avec le test des unités.

Nous allons maintenant répondre à ces questions et développer les différentes étapes de l'algorithme que nous avons présentées plus haut.

3.3.2 Le choix des entiers

Nous devons définir un ensemble $\mathcal{X}$ d'éléments de $\Phi(\mathbb{Z}_K)$ susceptibles d'absorber le plus grand nombre possible de parallélotopes. Une approche naïve consiste à considérer les $X \in \Phi(\mathbb{Z}_K)$ vérifiant $X = \overline{\Phi}(t)$ où $t \in \mathbb{Z}^n \cap [-B, B]^n$ et $B > 0$. On pourrait espérer qu'une petite valeur de B soit suffisante, mais ce n'est pas toujours le cas : il faut souvent faire appel à des entiers éloignés si l'on veut être efficace. Il est donc souhaitable de prendre B assez grand, et de ne garder que les $X = \overline{\Phi}(t)$ où $t \in \mathbb{Z}^n \cap [-B, B]^n$, susceptibles d'absorber les parallélotopes recouvrant $\mathcal{F}$. Ceci se fait de la manière suivante.

Pour tout $i \in \{1, \dots, n\}$ nous posons

$$a_i = \sum_{\substack{i=1 \\ m_{i,j} \leq 0}}^{n} m_{i,j} \quad \text{et} \quad b_i = \sum_{\substack{i=1 \\ m_{i,j} > 0}}^{n} m_{i,j}.$$

Comme $\mathcal{F} = \overline{\Phi}([0,1)^n)$, il est facile de voir que

$$\mathcal{F} \subseteq [a_1, b_1] \times \dots \times [a_n, b_n],$$

et que si $X \in \Phi(\mathbb{Z}_K)$ vérifie

$$\mathcal{F} \cap \Big\{ x \in \mathbb{R}^n \ \text{ tel que } \mathcal{N}(x - X) \leq k \Big\} \neq \emptyset,$$

alors, il existe au moins un $i \in \{1, \dots, n\}$ pour lequel nous devons avoir

$$X_i \in [a_i - k^{\frac{1}{n}}, b_i + k^{\frac{1}{n}}].$$

Ainsi nous choisissons $B > 0$ suffisamment grand et nous considérons l'ensemble des $X \in \Phi(\mathbb{Z}_K)$ qui vérifient $X_i \in [a_i - k^{\frac{1}{n}}, b_i + k^{\frac{1}{n}}]$ pour au moins un indice i.

3.3.3 Découpage et recouvrement de $\mathcal{F}$ et de $\mathcal{F}'$

L'idée principale est de recouvrir $\mathcal{F}$ à l'aide de petits parallélotopes de la forme

$$\{x \in \mathbb{R}^n;\ \alpha_i \leq x_i \leq \beta_i\},$$

c'est-à-dire dont les faces sont orthogonales aux axes associés à la base canonique de $\mathbb{R}^n$. Ce recouvrement est de la même nature que celui utilisé dans [Ce00], ou encore que celui auquel a recours Quême [Qu98], et diffère de ceux, apparemment plus naturels, utilisés par Cavallar et Lemmermeyer [CaL98] ou Cohn et Deutsch [CD86], qui consistent à découper $[0,1)^n$ en petits cubes et à travailler alors avec leurs images par $\overline{\Phi}$.

Nous avons, avec les notations introduites plus haut,

$$\mathcal{F} \subseteq [a_1, b_1] \times \ldots. \times [a_n, b_n].$$

Découpons maintenant $[a_1, b_1] \times \ldots. \times [a_n, b_n]$ de la façon suivante. On choisit n entiers positifs pairs $r_1, \ldots, r_n$, et on pose

$$\text{pour tout } i \in \{1, \ldots, n\},\ h_i = \frac{b_i - a_i}{2r_i},$$

$$\text{pour tout } i \in \{1, \ldots, n\} \text{ et pour tout } j \in \{0, \ldots, r_i\},\ y_{j,i} = a_i + 2jh_i,$$

$$\text{pour tout } i \in \{1, \ldots, n\} \text{ et pour tout } j \in \{0, \ldots, r_i - 1\},\ c_{j,i} = a_i + (2j+1)h_i.$$

La Figure 3.4 illustre ces notations avec $n = 2$, $r_1 = 10$ et $r_2 = 8$. Soit

$$L = \{(l_1, \ldots, l_n) \text{ tels que pour tout } i \in \{1, \ldots, n\},\ 0 \leq l_i \leq r_i - 1\}.$$

Si $l = (l_1, \ldots, l_n) \in L$, le parallélotope défini par

$$\mathcal{B}_l = \{x \in \mathbb{R}^n \text{ tels que pour tout } i \in \{1, \ldots, n\},\ y_{l_i,i} \leq x_i \leq y_{l_i+1,i}\},$$

est centré en C_l où

$$(C_l)_i = c_{l_i,i}.$$

Bien sûr, nous avons

$$\mathcal{F} \subseteq \bigcup_{l \in L} \mathcal{B}_l,$$

mais ce recouvrement est prohibitif (beaucoup de $\mathcal{B}_l$ pour ne pas dire la plupart sont inutiles) et nous devons le réduire. Nous procédons de la façon suivante.

Soit $(l_1, \ldots, l_{n-1}) \in \{0, \ldots, r_1 - 1\} \times \ldots \times \{0, \ldots, r_{n-1} - 1\}$. La question est :

$$\text{pour quelles valeurs de } l_n \text{ a-t-on } \mathcal{B}_l \cap \mathcal{F} \neq \emptyset\,?$$

Il est facile de voir que, comme $\overline{\Phi}$ est bijective, ceci équivaut à

$$\overline{\Phi}^{-1}(\mathcal{B}_l) \cap [0,1)^n \neq \emptyset.$$

Pour i et j de $\{1, \ldots, n\}$, posons

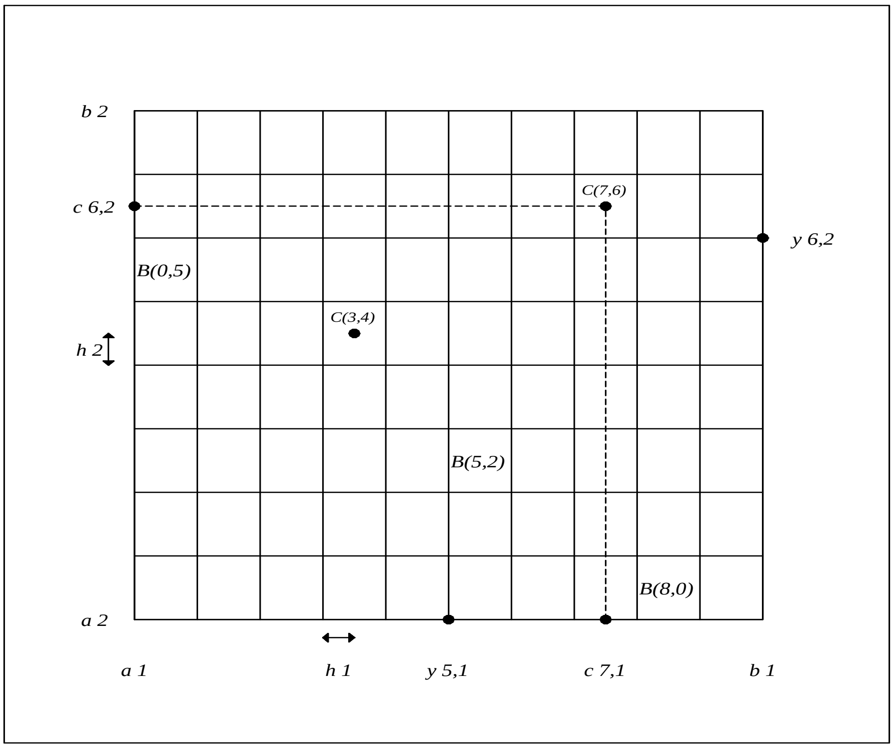

FIG. 3.4: Notations relatives au découpage.

$$\begin{cases} u_{i,j} = y_{l_j+1,j} & \text{si } m'_{i,j} > 0 \quad \text{et} \quad u_{i,j} = y_{l_j,j} \quad \text{sinon,} \\ v_{i,j} = y_{l_j,j} & \text{si } m'_{i,j} > 0 \quad \text{et} \quad v_{i,j} = y_{l_j+1,j} \quad \text{sinon.} \end{cases}$$

Soit $t = (t_i)_{1 \le i \le n} \in \overline{\Phi}^{-1}(\mathcal{B}_l)$. Pour tout $i \in \{1, \ldots, n\}$ la plus grande valeur de t_i est donnée par

$$\mu_i = \sum_{j=1}^{n} m'_{i,j} u_{i,j},$$

et la plus petite valeur de t_i est donnée par

$$\lambda_i = \sum_{j=1}^{n} m'_{i,j} v_{i,j}.$$

Nous pouvons exclure les l_n pour lesquels il existe un i tel que $\mu_i < 0$ ou $\lambda_i > 1$, puisque dans ces cas, pour tout $t \in \overline{\Phi}^{-1}(\mathcal{B}_l)$, $t_i < 0$ ou pour tout $t \in \overline{\Phi}^{-1}(\mathcal{B}_l)$, $t_i > 1$, ce qui implique $\overline{\Phi}^{-1}(\mathcal{B}_l) \cap [0,1)^n = \emptyset$. Ainsi, pour tout $i \in \{1, \ldots, n\}$ nous devons avoir $\mu_i \ge 0$ et $\lambda_i \le 1$. Remplaçant $y_{l_n,n}$ et $y_{l_n+1,n}$ par $a_n + 2l_n h_n$ et $a_n + 2(l_n+1)h_n$ nous trouvons des inégalités qui doivent être vérifiées par l_n, en fonction de $l_1, \ldots, l_{n-1}$. Ces formules sont plutôt lourdes et sont faciles à établir, de telle sorte que nous ne les expliciterons pas ici.

Remarque 3.22. Dans de nombreux cas, l'intervalle ainsi défini pour les valeurs de l_n est vide. En dimension supérieure à 4, il est pertinent de déterminer de la même manière un intervalle contenant l_{n-1} pour $(l_1, \ldots, l_{n-2})$ donné.

Pour obtenir un tel intervalle, nous écrivons, avec les mêmes notations que plus haut

$$\mu_i \leq \begin{cases} \sum_{j=1}^{n-2} m'_{i,j} u_{i,j} + m'_{i,n-1} y_{l_{n-1}+1,n-1} + m'_{i,n}\alpha_i & \text{si } m'_{i,n-1} > 0 \\ \sum_{j=1}^{n-2} m'_{i,j} u_{i,j} + m'_{i,n-1} y_{l_{n-1},n-1} + m'_{i,n}\alpha_i & \text{si } m'_{i,n-1} \leq 0 \end{cases}$$

et

$$\lambda_i \geq \begin{cases} \sum_{j=1}^{n-2} m'_{i,j} v_{i,j} + m'_{i,n-1} y_{l_{n-1},n-1} + m'_{i,n}\beta_i & \text{si } m'_{i,n-1} > 0 \\ \sum_{j=1}^{n-2} m'_{i,j} v_{i,j} + m'_{i,n-1} y_{l_{n-1}+1,n-1} + m'_{i,n}\beta_i & \text{si } m'_{i,n-1} \leq 0, \end{cases}$$

où

$$\begin{cases} \alpha_i = b_n \quad \text{si} \quad m'_{i,n} > 0, \quad \alpha_i = a_n \quad \text{sinon}, \\ \beta_i = a_n \quad \text{si} \quad m'_{i,n} > 0, \quad \beta_i = b_n \quad \text{sinon}. \end{cases}$$

Comme nous devons avoir $\mu_i \geq 0$ et $\lambda_i \leq 1$ pour tout i, ces inégalités nous fournissent l'intervalle désiré pour l_{n-1}.
De même, en plus grande dimension (par exemple si $n \geq 6$) il est intéressant de définir des intervalles contenant l_{n-2} pour $(l_1, \ldots, l_{n-3})$ donné, ou encore des intervalles contenant l_{n-3} pour $(l_1, \ldots, l_{n-4})$ donné, etc. Ce procédé permet d'accélérer les calculs de façon sensible.

Remarque 3.23. On voit sans peine que

$$\left(\frac{1}{2}\Phi\left(\sum_{i=1}^{n} e_i\right)\right)_1 = \frac{b_1 + a_1}{2}.$$

Par conséquent, si nous voulons réduire le domaine d'étude à un demi-parallélotope fondamental, la nature même du recouvrement de $\mathcal{F}$ que nous venons de définir nous amène à choisir

$$\mathcal{F}' = \Big\{x \in \mathcal{F} \text{ tels que } x_1 \in [a_1, \frac{b_1 + a_1}{2}]\Big\},$$

et à travailler avec les $\mathcal{B}_l$ qui vérifient $0 \leq l_1 \leq r_1/2 - 1$.
Ils recouvrent clairement $\mathcal{F}'$. De plus, $l = (l_1, \ldots, l_n)$ étant donné, on a $s(\mathcal{B}_l) = \mathcal{B}_{l'}$ où $l' = (r_1 - 1 - l_1, \ldots, r_n - 1 - l_n)$, et $\mathcal{F}$ est recouvert par les $\mathcal{B}_l$ vérifiant $0 \leq l_1 \leq r_1/2 - 1$ et par leurs images par s.

La Figure 3.5 illustre le recouvrement de $\mathcal{F} = \{a + b\,\Phi(\sqrt{2});\ (a,b) \in [0,1)^2\}$ pour $K = \mathbb{Q}(\sqrt{2})$. Ici les sommets de $\mathcal{F}$ sont $A = \Phi(0)$, $B = \Phi(1)$, $C = \Phi(1+\sqrt{2})$, $D = \Phi(\sqrt{2})$ et $r_1 = r_2 = 10$. Le recouvrement de $\mathcal{F}'$ est donné par les rectangles blancs situés à la gauche de la ligne centrale verticale.

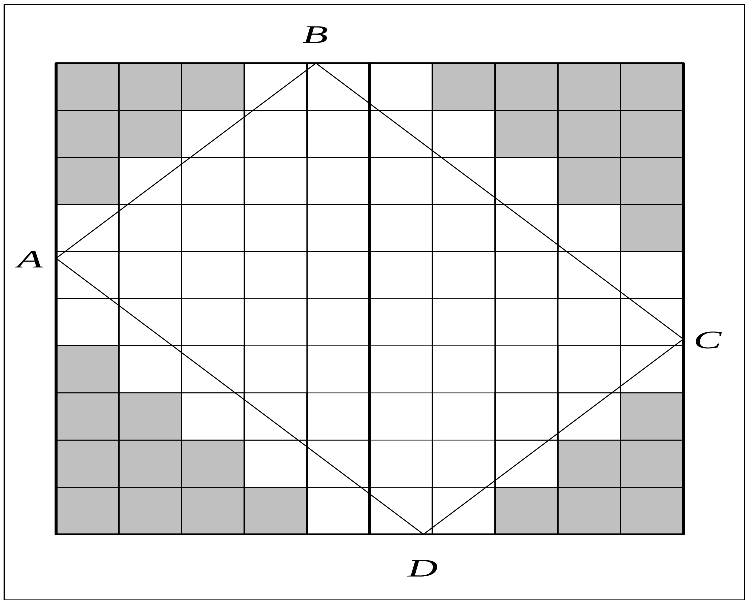

FIG. 3.5: Recouvrement de $\mathcal{F}$ et $\mathcal{F}'$.

3.3.4 Le test d'absorption

Nous passons en revue les $\mathcal{B}_l$ qui recouvrent $\mathcal{F}$ (ou $\mathcal{F}'$ comme vu précédemment dans la Remarque 3.23) et éliminons tous ceux qui sont absorbés par un élément X de $\mathcal{X}$.

Considérons l'un de ces $\mathcal{B}_l$ que nous noterons $\mathcal{P}$. Pour simplifier les notations nous noterons C son centre, de telle sorte que

$$\mathcal{P} = [C_1 - h_1, C_1 + h_1] \times \ldots \times [C_n - h_n, C_n + h_n].$$

Rappelons que nous avons choisi un petit $\epsilon > 0$ et que nous pouvons éliminer $\mathcal{P}$ si

$$\text{(3.17)} \qquad \text{il existe un } X \in \mathcal{X} \text{ tel que pour tout } x \in \mathcal{B}_l,\ \mathcal{N}(x - X) \leq k - \epsilon.$$

Le test est défini de la façon suivante.

Proposition 3.24. *L'assertion suivante est équivalente à (3.17)*

$$\text{(3.18)} \qquad \textit{il existe un } X \in \mathcal{X} \textit{ tel que } \prod_{i=1}^{n} \Big(|C_i - X_i| + h_i \Big) \leq k - \epsilon.$$

Preuve. Soit $x \in \mathcal{B}_l$. L'inégalité triangulaire donne

$$\text{(3.19)} \qquad \text{pour tout } i \in \{1, \ldots, n\},\ |x_i - X_i| \leq |x_i - C_i| + |C_i - X_i|.$$

Mais comme $x_i \in [C_i - h_i, C_i + h_i]$, on a $|x_i - C_i| \leq h_i$, et

$$\text{(3.20)} \qquad \text{pour tout } i \in \{1, \ldots, n\},\ |x_i - X_i| \leq h_i + |C_i - X_i|.$$

En faisant le produit selon i, on obtient

$$\mathcal{N}(x-X) \leq \prod_{i=1}^{n} \Big(|C_i - X_i| + h_i\Big),$$

si bien que (3.18) implique (3.17).
De plus, les inégalités (3.19) et (3.20) sont des égalités pour

$$x_i = \begin{cases} C_i - h_i & \text{si } C_i \text{ est entre } C_i - h_i \text{ et } X_i, \\ C_i + h_i & \text{si } C_i \text{ est entre } C_i + h_i \text{ et } X_i, \end{cases}$$

et il n'est pas difficile de voir que l'on est forcément dans l'un de ces deux cas. Ceci montre que (3.18) est en fait une égalité pour un des sommets de $\mathcal{P}$ et que la majoration utilisée est optimale. Ainsi (3.18) équivaut à (3.17). □

Remarque 3.25. La Proposition 3.24 met en évidence un des avantages de notre découpage. L'inégalité utilisée est la meilleure possible contrairement à ce que l'on obtient avec le découpage élémentaire évoqué plus haut et utilisé par exemple dans [CaL98].

Résumons-nous. Nous passons en revue tous les $\mathcal{B}_l$ recouvrant $\mathcal{F}'$ (voir Remarque 3.23) à l'aide des inégalités vues plus haut et éventuellement de celles évoquées en Remarque 3.22, et nous les soumettons au test de la Proposition 3.24. Si (3.18) est vérifiée par l'un des $\mathcal{B}_l$, celui-ci peut être éliminé et nous savons par la Remarque 3.21, que son image par s, $s(\mathcal{B}_l)$ peut aussi être éliminée du recouvrement de $\mathcal{F}$. Si (3.18) n'est pas vérifiée par $\mathcal{B}_l$, nous stockons $\mathcal{B}_l$ et $s(\mathcal{B}_l)$ dans notre liste de parallélotopes problématiques. La réunion des parallélotopes éliminés constitue la région $\mathcal{G}'$ et nous avons

$$\text{pour tout } x \in \mathcal{G}',\ m_{\overline{K}}(x) \leq k - \epsilon.$$

Remarque 3.26. À chaque étape de l'algorithme, nous ne travaillerons qu'avec la moitié des parallélotopes, mais n'oublierons pas de stocker et de prendre en compte leurs images par s. Pour cela, à chaque étape (test d'absorption, test des unités, découpages successifs des parallélotopes), nous indexerons chaque parallélotope correspondant à $\mathcal{F}'$ à l'aide d'un indice impair $i = 2p - 1$ ($p \geq 1$) et son image par s à l'aide de $i = 2p$.

3.3.5 Le test des unités

Supposons que $\mathcal{P}$ soit un parallélotope problématique trouvé à l'étape précédente. Soit C son centre, de telle sorte que

$$\mathcal{P} = [C_1 - h_1, C_1 + h_1] \times \ldots \times [C_n - h_n, C_n + h_n].$$

On a

$$\Phi(\varepsilon) \cdot \mathcal{P} = [w_1, z_1] \times \ldots \times [w_n, z_n],$$

où

$$\text{pour tout } i,\ w_i = \sigma_i(\varepsilon) C_i - |\sigma_i(\varepsilon)| h_i \quad \text{et} \quad z_i = \sigma_i(\varepsilon) C_i + |\sigma_i(\varepsilon)| h_i.$$

C'est un parallélotope dont les faces sont orthogonales aux axes définis par la base canonique de $\mathbb{R}^n$ (comme les $\mathcal{P}_i$), centré en

$$C'' = (\sigma_i(\varepsilon)C_i)_{1\leq i\leq n}.$$

La détermination des $X \in \Phi(\mathbb{Z}_K)$ tels que $\Phi(\varepsilon)\cdot\mathcal{P} - X$ rencontre $\mathcal{F}$ est le premier problème que nous avons à résoudre.

Considérons d'abord $T = (T_1, \dots, T_n) = \overline{\Phi}^{-1}(C'')$. Soit $X_0 = \overline{\Phi}((\lfloor T_1\rfloor, \dots, \lfloor T_n\rfloor))$. Comme $T - \overline{\Phi}^{-1}(X_0) \in [0,1)^n$, il est clair que $C'' - X_0 \in \mathcal{F}$, et alors

$$(\Phi(\varepsilon)\cdot\mathcal{P} - X_0)\cap\mathcal{F} \neq \emptyset.$$

Comme nous l'avons déjà mentionné, X_0 n'est pas nécessairement le seul vecteur de translation de $\Phi(\mathbb{Z}_K)$ que nous pouvons utiliser pour ramener $\Phi(\varepsilon)\cdot\mathcal{P}$ sur $\mathcal{F}$. D'autres peuvent être utilisés si $\Phi(\varepsilon)\cdot\mathcal{P} - X_0$ a des éléments en dehors de $\mathcal{F}$ mais les différentes possibilités sont faciles à déterminer.

Posons $\mathcal{P}' = \Phi(\varepsilon)\cdot\mathcal{P} - X_0$. C'est un parallélotope centré en $C' = C'' - X_0$ et nous avons $\mathcal{P}' = [C'_1 - h'_1, C'_1 + h'_1]\times\dots\times[C'_n - h'_n, C'_n + h'_n]$, où

$$\text{pour tout } i \in \{1, \dots, n\},\ h'_i = h_i\,|\sigma_i(\varepsilon)|.$$

Pour tout $i \in \{1, \dots, n\}$ la plus petite et la plus grande valeur de $(\overline{\Phi}^{-1}(x))_i$ où $x \in \mathcal{P}'$ sont respectivement

$$\alpha_i = \sum_{j=1}^{n} m'_{i,j}(C'_j - \delta_{i,j}h'_j) \text{ et } \beta_i = \sum_{j=1}^{n} m'_{i,j}(C'_j + \delta_{i,j}h'_j),$$

avec

$$\delta_{i,j} = 1 \text{ si } m'_{i,j} > 0 \quad \text{et} \quad \delta_{i,j} = -1 \text{ sinon.}$$

Ces formules nous donnent aisément les seuls vecteurs de translation possibles de $\Phi(\mathbb{Z}_K)$.

Proposition 3.27. *Avec les notations précédentes, si $X \in \Phi(\mathbb{Z}_K)$ est tel que $\Phi(\varepsilon)\cdot\mathcal{P} - X$ rencontre $\mathcal{F}$, alors X est de la forme $X = X_0 + \overline{\Phi}(\nu_1, \dots, \nu_n)$, où*

$$\textit{pour tout } i \in \{1, \dots, n\},\ \nu_i \in \mathbb{Z} \textit{ et } \lfloor\alpha_i\rfloor \leq \nu_i \leq \lfloor\beta_i\rfloor.$$

Notons que tous les X ainsi définis ne sont pas forcément utiles au sens où l'on n'aura pas nécessairement $(\Phi(\varepsilon)\cdot\mathcal{P} - X)\cap\mathcal{F} \neq \emptyset$, mais que nous sommes sûrs d'avoir ainsi tous les vecteurs de translations de $\Phi(\mathbb{Z}_K)$ susceptibles de ramener une partie de $\Phi(\varepsilon)\cdot\mathcal{P}$ dans $\mathcal{F}$.

Remarque 3.28. Quand pour un i donné, $|\sigma_i(\varepsilon)|h_i$, et par conséquent le nombre de vecteurs de translation possibles, sont trop grands, nous allons directement à l'étape suivante (division du découpage) qui sera décrite dans la section 3.3.6.

Notons X_0, X_1, ..., X_g ($g \geq 0$) ces vecteurs de translation. Comme précédemment soit $\{\mathcal{P}_1, \mathcal{P}_2, \dots, \mathcal{P}_{2q-1}, \mathcal{P}_{2q}\}$ notre liste de parallélotopes problématiques, et notons D_p le centre de $\mathcal{P}_p$.

Proposition 3.29. *Avec les notations précédentes, si pour tout j (avec $0 \leq j \leq g$) nous avons*

$$\left\{ \begin{array}{l} \textit{pour tout } p \in \{1, \dots, 2q\}, \textit{ il existe un } i_p \in \{1, \dots, n\} \textit{ tel que} \\ |(C'' - X_j - D_p)_{i_p}| > \big(1 + |\sigma_{i_p}(\varepsilon)|\big)\, h_{i_p}, \end{array} \right. \tag{3.21}$$

alors $\mathcal{P}$ et $s(\mathcal{P})$ peuvent être éliminés de la liste des parallélotopes problématiques.

Preuve. Soit $x \in \mathcal{P}$. Par construction des X_j nous savons qu'il existe $j \in \{0, \dots, g\}$ tel que $y = \Phi(\varepsilon) \cdot x - X_j \in \mathcal{F}$. Mais $\Phi(\varepsilon) \cdot \mathcal{P} - X_j$ est un parallélotope centré en $C'' - X_j$ isométrique à $\mathcal{P}'$ et nous avons

$$\text{pour tout } i \in \{1, \dots, n\},\ |y_i - C''_i + (X_j)_i| \leq h'_i. \tag{3.22}$$

Soit maintenant $p \in \{1, \dots, 2q\}$. Par (3.21), (3.22) et l'inégalité triangulaire, il existe $i_p \in \{1, \dots, n\}$ tel que $|y_{i_p} - (D_p)_{i_p}| > \big(1 + |\sigma_{i_p}(\varepsilon)|\big)\, h_{i_p} - h'_{i_p}$, ou de façon équivalente $|y_{i_p} - (D_p)_{i_p}| > h_{i_p}$.

Cette dernière inégalité implique

$$y \in \mathcal{F} \quad \text{et pour tout } p \in \{1, \dots, 2q\}\ y \notin \mathcal{P}_p.$$

Ainsi, $m_{\overline{K}}(y) \leq k - \epsilon$, et par la Proposition 1.15 nous obtenons finalement $m_{\overline{K}}(x) \leq k - \epsilon$. Ceci montre que $\mathcal{P}$ peut être éliminé. $\square$

Remarque 3.30. Ici encore, c'est grâce à la nature de notre découpage de $\mathcal{F}$ que nous disposons d'un critère élémentaire pour voir si $\Phi(\varepsilon) \cdot \mathcal{P}$ intersecte ou non un $\mathcal{P}_p$ modulo $\Phi(\mathbb{Z}_K)$. Par ailleurs, il est facile de voir que l'inégalité utilisée dans (3.21) est optimale.

La procédure est désormais simple. Considérons notre ensemble de parallélotopes problématiques $\{\mathcal{P}_1, \mathcal{P}_2, \dots, \mathcal{P}_{2q-1}, \mathcal{P}_{2q}\}$. Par symétrie, nous n'avons besoin de tester que les $\mathcal{P}_{2p-1}$, pour $1 \leq p \leq q$. Si $\mathcal{P}_{2p-1}$ verifie (3.21), nous éliminons $\mathcal{P}_{2p-1}$ et $\mathcal{P}_{2p} = s(\mathcal{P}_{2p-1})$ de la liste. À la fin de la boucle, nous parcourons de nouveau notre nouvelle liste, et recommençons tant que la liste diminue.

Notons que la liste finale vérifie encore

$$\text{pour tout } p,\ s(\mathcal{P}_{2p-1}) = \mathcal{P}_{2p}. \tag{3.23}$$

Remarque 3.31. Nous pouvons avoir recours à plusieurs unités. Dans ce cas, nous faisons le test successivement avec chacune des unités utilisées.

3.3.6 L'étape suivante : division de la partition

Soit $\{\mathcal{P}_1, \mathcal{P}_2, \dots, \mathcal{P}_{2q-1}, \mathcal{P}_{2q}\}$ notre nouvelle liste réduite de parallélotopes problématiques. Ainsi que nous l'avons vu plus haut, l'étape suivante consiste à couper chacun des parallélotopes restants $\mathcal{P}_{2p-1}$ centré en C en 2^n parallélotopes plus petits

$$[C_1 - \eta_1 h_1, C_1 + (1 - \eta_1) h_1] \times \ldots \times [C_n - \eta_n h_n, C_n + (1 - \eta_n) h_n],$$

où $\eta_i \in \{0,1\}$, et à tester chacun d'eux à l'aide de la Proposition 3.24. Si le test est négatif, nous stockons ce petit parallélotope dans une nouvelle liste, en position impaire, et son symétrique par s en position suivante. À la fin nous avons un nouvel ensemble de petits parallélotopes problématiques $\mathcal{P}'_i$ (où $1 \leq i \leq 2q'$) vérifiant la propriété (3.23).

Comme précédemment, nous pouvons recourir aux unités pour éliminer un grand nombre de $\mathcal{P}'_i$ par la Proposition 3.29 et le sous-algorithme décrit plus haut. Si la liste finale est encore notée $\mathcal{P}'_i$ (où $1 \leq i \leq 2q'$), nous comparons q et q'.

Si $q' \leq q$ nous remplaçons l'ancienne liste par la nouvelle et recommençons. Si $q' > q$, nous nous arrêtons et analysons les $\mathcal{P}_i$ $(1 \leq i \leq 2q)$.

3.3.7 Traitement des parallélotopes restants

Stratégie générale

À ce stade il nous reste $2q$ parallélotopes problématiques $\mathcal{P}_1, \ldots, \mathcal{P}_{2q}$ qui vérifient (3.23), et nous savons, par les considérations précédentes, que

$$\mathcal{F} \setminus \bigcup_{1 \leq i \leq 2q} \mathcal{P}_i \subseteq \mathcal{G},$$

où, avec une notation semblable à celle de la section 3.2, $\mathcal{G}$ est la partie de $\mathbb{R}^n$ définie par

$$\mathcal{G} = \{x \in \mathbb{R}^n \text{ tels que } m_{\overline{K}}(x) \leq k - \epsilon\}.$$

Reprenons une unité $\varepsilon \neq \pm 1$, par exemple l'unité (ou une des unités) précédemment utilisée et considérons les parallélotopes problématiques $\mathcal{P}_i$ (où $1 \leq i \leq 2q$). Essayons de les regrouper en régions $\mathcal{T}$ qui vérifient (3.12) et sont les sommets d'un graphe convenable G, comme défini dans la section 3.2.2. Par la façon dont les $\mathcal{P}_i$ ont été sélectionnés, nous avons partiellement (3.12), le seul point auquel nous devons prêter attention étant le traitement des parallélotopes problématiques qui, après multiplication par $\Phi(\varepsilon)$ peuvent être ramenés de différentes manières sur $\mathcal{F}$. Nous reparlerons de ce problème ultérieurement.

Pour définir les $\mathcal{T}_i$ nous pouvons déjà exclure les $\mathcal{P}_i$ qui ne sont intersectés par aucun $\Phi(\varepsilon) \cdot \mathcal{T}_j - X_j$, essayer de regrouper les autres en ensembles cohérents (même vecteur de translation, mêmes intersections ...), à l'aide d'un critère de proximité géométrique, et seulement à la fin, ajouter les $\mathcal{P}_i$ restants (ce qui n'est pas nécessaire de toute façon).
Si nous obtenons un graphe convenable, il reste à calculer les $m_{\overline{K}}(t_i)$ pour $t_i \in \mathcal{E}$ et à appliquer le Théorème 3.16, qui doit donner, si tout va bien, $m(G) = k$.

Les parallélotopes périphériques

Les Figures 3.6 et 3.7 illustrent ce qui se passe avec $K = \mathbb{Q}(\sqrt{2})$, et $A = \Phi(0)$, $B = \Phi(1)$, $C = \Phi(1+\sqrt{2})$, $D = \Phi(\sqrt{2})$ comme sommets de $\mathcal{F}$. Dans la Figure 3.6 nous voyons que nous avons deux régions problématiques (chacune étant composée de quatre parallélotopes). Le problème vient du fait que chacune d'elle peut être envoyée sur elle-même ou sur l'autre via l'action des unités, et que nous ne sommes pas exactement sous les hypothèses (3.12) de la section 3.2.2. Pour surmonter l'obstacle, nous considérons dans la Figure 3.7 un nouveau domaine fondamental, ici $\mathcal{F} - \Phi(2/5)$, avec A', B', C', D' pour sommets. Nous translatons ensuite à l'aide de $\Phi(-1)$ quelques-uns des parallélotopes du recouvrement initial, dont ceux de la région problématique supérieure, de telle sorte que nous obtenons un recouvrement de ce nouveau domaine fondamental. Dans le cas présent, nous vérifions que nous avons une seule région problématique envoyée sur elle-même par l'action d'une unité, et le graphe orienté associé à la situation est G_1 (avec $j = 1$) qui est convenable.

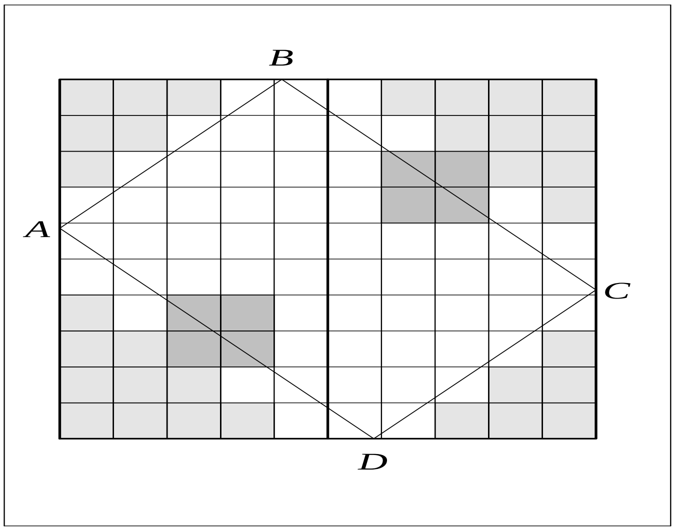

FIG. 3.6: Problèmes périphériques - Avant.

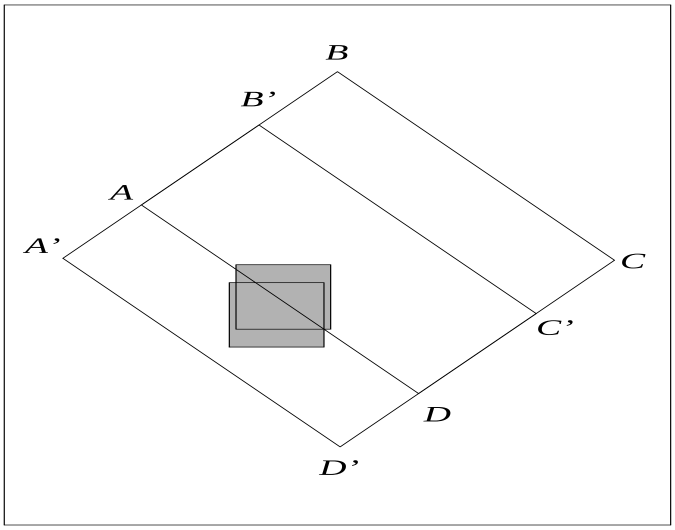

FIG. 3.7: Problèmes périphériques - Après.

En fait, le problème, lorsqu'on a plusieurs possibilités pour le vecteur de translation associé à un parallélotope problématique $\mathcal{P}$, est que, si l'on en fixe un, disons X, $\Phi(\varepsilon) \cdot \mathcal{P} - X$ peut intersecter une région $\mathcal{T}'$ équivalente modulo $\Phi(\mathbb{Z}_K)$ à l'une des $\mathcal{T}$ que nous avons définies, mais qui est en dehors de $\mathcal{F}$ et donc non répertoriée. Dans ce cas, les $\mathcal{P}$ en question sont très petits et proches de la frontière de $\mathcal{F}$, de telle sorte que l'on peut, comme précédemment, considérer un autre domaine fondamental, dont le recouvrement est obtenu par translation de quelques $\mathcal{B}_l$ initiaux. Il suffit alors de vérifier que les résultats de la section 3.2.2 sont compatibles avec ce nouveau recouvrement.

3.3.8 Calcul du minimum inhomogène

Nous avons encore à montrer comment nous calculons $m_{\overline{K}}(t_i)$ pour $t_i \in \mathcal{E}$, ou plus généralement, $m_{\overline{K}}(t)$ pour $t \in \Phi(K)$. Cela se fait à l'aide du Théorème 2.8 et du Corollaire 2.9.

Détermination des orbites

Pour $\xi \in K$, nous définissons

$$\mathrm{Orb}(\xi) = \{\varepsilon\xi \bmod \mathbb{Z}_K;\ \varepsilon \in E_K\}.$$

Il s'agit de l'orbite de ξ sous l'action de E_K sur $K/\mathbb{Z}_K$ définie par $(\varepsilon, \overline{\xi}) \mapsto \overline{\varepsilon\xi}$.
Si $t = \Phi(\xi)$, on a $\mathrm{Orb}(t) = \mathrm{Orb}(\xi)$. Elle équivaut bien sûr à l'orbite de $\overline{\Phi(\xi)}$ dans $\mathbb{R}^n/\Phi(\mathbb{Z}_K)$ telle que nous l'avons définie plus haut.

Afin de calculer cette orbite, nous déterminons d'abord, pour tout $i \in \{1, \ldots, n-1\}$, le plus petit entier positif p_i tel que

$$\varepsilon_i^{p_i}\xi \equiv \xi \bmod \mathbb{Z}_K.$$

Il est alors facile de voir, en se servant de la division euclidienne par les p_i, que pour toute unité $\varepsilon \in E_K$, il existe un $(n-1)$-uplet $(m_1, \ldots, m_{n-1}) \in \{0, \ldots, p_1 - 1\} \times \ldots \times \{0, \ldots, p_{n-1} - 1\}$ tel que

$$\varepsilon\xi \equiv \pm\varepsilon_1^{m_1} \ldots \varepsilon_{n-1}^{m_{n-1}}\xi \bmod \mathbb{Z}_K.$$

Ainsi, nous n'avons qu'à calculer successivement $2p_1 \ldots p_{n-1}$ valeurs, et à stocker chacune d'entre elles, au fur et à mesure.

Notons que si nous avons calculé $m_{\overline{K}}(t)$ où t est associé à un cycle c, il est inutile de calculer $m_{\overline{K}}(t')$ pour $t' \in \mathrm{Orb}(t)$ (car $m_{\overline{K}}(t) = m_{\overline{K}}(t')$), et en particulier il est inutile de calculer $m_{\overline{K}}(t')$ pour t' associé à c.

Sélection des bons entiers

Soit z un élément de $\mathrm{Orb}(t)$. Comment passons-nous en revue les $Z \in \mathcal{R}$ vérifiant

$$|z_i - Z_i| \leq \left(k \prod_{l=1}^{n-1} \Gamma_l\right)^{1/n} \qquad \text{pour tout } i\,?$$

Notons $z = \Phi(\xi)$ où $\xi = \sum \xi_i e_i \in K$, et $Z = \Phi(\Upsilon)$ où $\Upsilon = \sum \Upsilon_i e_i \in \mathbb{Z}_K$. On établit facilement que Υ doit vérifier

$$\text{(3.24)} \qquad \text{pour tout } i \in \{1, \ldots, n-1\},\ |\Upsilon_i - \xi_i| \leq \left(\sum_{i=1}^{n} |m'_{i,j}|\right)\left(k \prod_{l=1}^{n-1} \Gamma_l\right)^{\frac{1}{n}},$$

et $(\Upsilon_1, \ldots, \Upsilon_{n-1})$ étant donné vérifiant (3.24), les n conditions suivantes :

$$\text{(3.25)} \qquad \text{pour tout } i \in \{1, \ldots, n\},\ m_{i,n}\Upsilon_n \in \left[\alpha_i - \left(k \prod_{l=1}^{n-1} \Gamma_l\right)^{\frac{1}{n}}, \alpha_i + \left(k \prod_{l=1}^{n-1} \Gamma_l\right)^{\frac{1}{n}}\right],$$

où

$$\alpha_i = m_{i,n}\xi_n + \sum_{j=1}^{n-1} m_{i,j}(\xi_j - \Upsilon_j).$$

La preuve est élémentaire.

3.3.9 Comment a-t-on une idée de k ?

Dans toutes les sections précédentes, nous avons supposé qu'en fait, nous avions un candidat k pour $M(\overline{K})$, et que nous voulions juste vérifier que k convenait bien.

Comme en général une telle valeur n'est pas a priori connue, nous devons décrire une démarche heuristique qui permet de trouver k. Tout d'abord on essaie l'algorithme avec une valeur raisonnable k', par exemple $k' = 0.999$. Si la première partie (division et élimination) ne renvoie aucun parallélotope problématique, nous essayons alors une valeur plus petite (toujours notée k'), jusqu'à ce qu'on trouve un nombre raisonnable de parallélotopes problématiques : s'il y a trop de tels parallélotopes, nous essayons une plus grande valeur pour k'. Nous appliquons alors le Théorème 3.16, si c'est possible. Dans ce cas, nous avons un graphe orienté G convenable, et nous calculons $m(G)$. Ceci se fait à l'aide du Théorème 2.8 et du Corollaire 2.9 (en commençant avec k'). Si $m(G) < k'$ on a $M(\overline{K}) < k'$ et on recommence avec un k' plus petit. Si $m(G) \geq k'$ alors le Théorème 3.16 donne $M(K) = M(\overline{K}) = m(G)$ et les points critiques rationnels correspondent à $\mathcal{E}'$.

Habituellement, cette procédure converge rapidement.

Si nous voulons juste prouver que K est euclidien pour la norme, on prend $k = 0.999$. Si on a des parallélotopes problématiques qui donnent des points t à évaluer, il n'est pas nécessaire de calculer $m_{\overline{K}}(t)$. Il suffit de trouver pour chaque t, un $X \in \Phi(\mathbb{Z}_K)$ tel que $\mathcal{N}(t - X) < 1$.

3.4 Exemples

3.4.1 L'exemple $K = \mathbb{Q}(\sqrt{13})$

Comme nous l'avons déjà dit, un des avantages du Théorème 3.16 est qu'il nous permet de traiter les corps « pathologiques » comme $\mathbb{Q}(\sqrt{13})$ (voir Exemple 1.31).

Donnons les résultats obtenus pour ce dernier corps. Cela permettra en outre d'illustrer ce que nous avons dit des parallélotopes périphériques.

Soit $K = \mathbb{Q}(\sqrt{13})$ et soient $(e_1, e_2) = (1, -\frac{1+\sqrt{13}}{2})$ et $\varepsilon_1 = \frac{3-\sqrt{13}}{2}$, la $\mathbb{Z}$-base de $\mathbb{Z}_K$ et l'unité fondamentale retournées par PARI [Pa].

En prenant $r_1 = r_2 = 50$, $k = 1/3$, $\epsilon = 0.01$, et en appliquant la procédure d'élimination avec ε_1 et ε_1^{-1} on trouve 16 parallélotopes problématiques (voir Figure 3.8 dans laquelle $A = \Phi(0)$, $B = \Phi(e_1)$, $C = \Phi(e_2)$ et $D = \Phi(e_1 + e_2)$).

D'abord, nous pouvons voir que $\mathcal{P}_1$ se situe au voisinage de $\overline{\Phi}(0, 2/3)$ et est isolé, alors que les $\mathcal{P}_i$ pour $i \in \{8, 10, 12\}$, sont au voisinage de $\overline{\Phi}(1, 2/3)$. Aussi, au lieu de $\mathcal{P}_1$, on peut considérer $\mathcal{P}_1 + \overline{\Phi}(1, 0)$ qui a le même comportement que $\mathcal{P}_8$ sous l'action de ε_1 et ε_1^{-1}, et que nous noterons encore $\mathcal{P}_1$. On a le même phénomène avec $\mathcal{P}_2$ (le symétrique de $\mathcal{P}_1$) que nous translatons sur les $\mathcal{P}_i$ où $i \in \{7, 9, 11\}$. Cela revient à considérer un domaine fondamental légèrement différent (voir Figure 3.8). Avec cette nouvelle approche, tous les $\mathcal{P}_i$ sont à l'intérieur du domaine fondamental et sont ramenés sur celui-ci, après multiplication par ε_1 ou ε_1^{-1}, par un seul vecteur de translation de $\Phi(\mathbb{Z}_K)$.

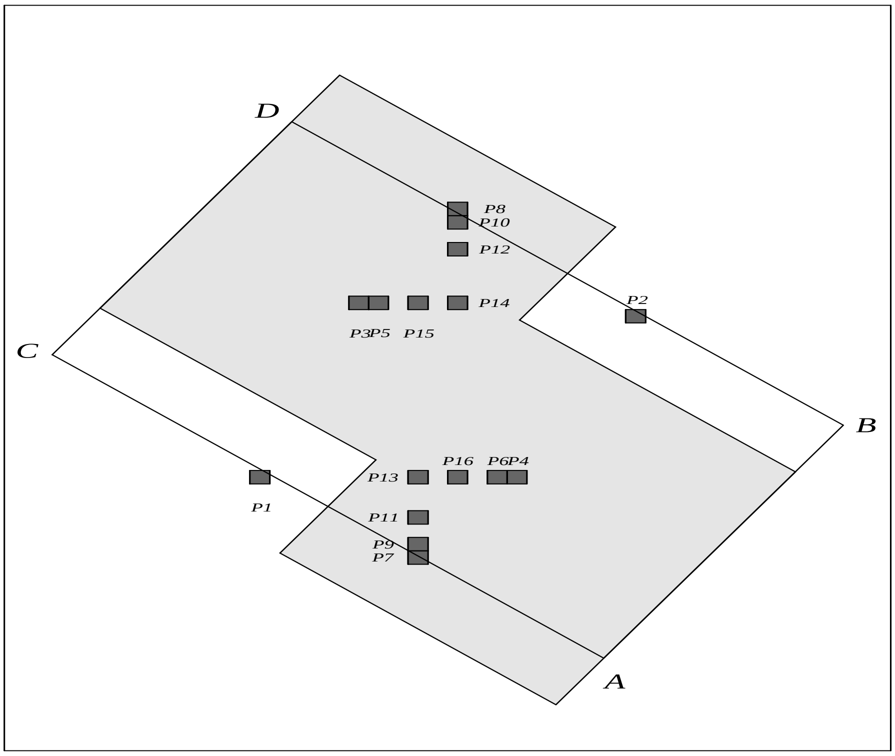

FIG. 3.8: $K = \mathbb{Q}(\sqrt{13})$.

Si nous prenons $\varepsilon = \varepsilon_1$ nous pouvons regrouper les $\mathcal{P}_i$ de la façon suivante.

$\mathcal{T}_1 = \mathcal{P}_3 \cup \mathcal{P}_5$,
$\mathcal{T}_2 = \mathcal{P}_4 \cup \mathcal{P}_6$,
$\mathcal{T}_3 = \mathcal{P}_1 \cup \mathcal{P}_8 \cup \mathcal{P}_{10} \cup \mathcal{P}_{12} \cup \mathcal{P}_{14} \cup \mathcal{P}_{16}$,
$\mathcal{T}_4 = \mathcal{P}_2 \cup \mathcal{P}_7 \cup \mathcal{P}_9 \cup \mathcal{P}_{11} \cup \mathcal{P}_{13} \cup \mathcal{P}_{15}$.

Nous obtenons alors le graphe orienté G suivant :

$$\begin{aligned}
\mathcal{T}_1 &\to \mathcal{T}_2(\Phi(3,1)),\\
\mathcal{T}_2 &\to \mathcal{T}_1(\Phi(1,0)),\\
\mathcal{T}_3 &\to \mathcal{T}_3(\Phi(3,1)),\\
\mathcal{T}_3 &\to \mathcal{T}_1(\Phi(3,1)),\\
\mathcal{T}_4 &\to \mathcal{T}_4(\Phi(1,0)),\\
\mathcal{T}_4 &\to \mathcal{T}_2(\Phi(1,0)).
\end{aligned}$$

Il s'agit d'un graphe convenable, précédemment vu sous l'appellation G_2 dans la Figure 3.3, et nous pouvons appliquer le Théorème 3.16. Nous trouvons quatre points rationnels t_i. Ces points sont $\overline{\Phi}(1/3,1/3)$, $\overline{\Phi}(2/3,2/3)$, $\overline{\Phi}(1,2/3)$ and $\overline{\Phi}(0,1/3)$, qui sont de la forme $\Phi(\xi)$ comme dans la Proposition 1.11, avec $|N_{K/\mathbb{Q}}(\Upsilon)| = 3$. Ainsi nous avons $m_{\overline{K}}(t_i) = 1/3$ pour tout i et

$$M(K) = M(\overline{K}) = \frac{1}{3},$$

avec exactement quatre points critiques rationnels dans $\mathcal{F}$.

3.4.2 Un exemple de calcul de second minimum euclidien

Supposons que nous appliquions l'algorithme avec k, et que nous trouvions, grâce au Théorème 3.16, p points rationnels ($p \geq 2$) $t_0, \ldots, t_{p-1}$, définis comme d'habitude par p parties bornées $\mathcal{T}_i$ ($0 \leq i \leq p-1$), et vérifiant

$$m_{\overline{K}}(t_0) = \ldots = m_{\overline{K}}(t_{r-1}) = k' \quad \text{et} \quad m_{\overline{K}}(t_r) = \ldots = m_{\overline{K}}(t_{p-1}) = k,$$

où

$$1 \leq r \leq p-1 \quad \text{et} \quad k < k'.$$

Alors, nous avons $M(K) = M(\overline{K}) = k'$.

Maintenant considérons $x \in \Phi(K)$ tel que $k < m_{\overline{K}}(x) < k'$. Par le Théorème 3.16, si $x \in \mathcal{T}_i$ où $i \leq r-1$, alors $x = t_i$ et $m_{\overline{K}}(x) = k'$, ce qui est exclu. Par conséquent, $x \in \mathcal{T}_i$ avec $i \geq r$ et $m_{\overline{K}}(x) \leq m_{\overline{K}}(t_i) = k$, ce qui est impossible. Ceci nous permet d'écrire $M_2(K) = k$.

Si de plus, $\mathcal{T}_1, \ldots, \mathcal{T}_r$ vérifient les hypothèses du Corollaire 3.5, nous pouvons faire la même chose avec $x \in \mathbb{R}^n$ (au lieu de $\Phi(K)$), et nous obtenons aussi $M_2(\overline{K}) = k$.

Exemple 3.32. Soit $K = \mathbb{Q}(\sqrt{2+\sqrt{2}})$. Si nous utilisons l'algorithme avec la base d'entiers (e_i) et les ε_i données par PARI, $k = 1/4$, $\epsilon = 0.001$ et $r_1 = r_2 = r_3 = r_4 = 100$, nous trouvons 24 parallélotopes problématiques $\mathcal{P}$ à la fin du processus de division et d'élimination (avec ε_1 et ε_2). Avec 16 de ces derniers, nous pouvons former une région problématique $\mathcal{T}_1$ au voisinage de $x_1 = \overline{\Phi}(1/2,1/2,1/2,1/2)$, qui vérifie les hypothèses du Théorème 3.2 avec $\varepsilon = \varepsilon_1$ et $j = 1$. Elle donne un t_1 qui après calcul, s'avère être x_1. Il est facile de vérifier que x_1 est de la forme $\Phi(\xi)$ avec ξ comme dans la Proposition 1.11 et $|N_{K/\mathbb{Q}}(\Upsilon)| = 2$, de telle sorte que $m_{\overline{K}}(t_1) = 1/2$.

Les autres $\mathcal{P}$ sont isolés, et sont aux voisinages de $\overline{\Phi}(\epsilon_1, 1/2, \epsilon_2, 1/2)$ et $\overline{\Phi}(1/2, \epsilon_3, 1/2, \epsilon_4)$ où $\epsilon_i \in \{0,1\}$. Chacun des 4 premiers est envoyé sur lui-même et sur les 3 autres, et il y a le même phénomène avec les 4 autres. Il est facile de vérifier qu'avec un domaine fondamental légèrement différent, nous aurions seulement 3 régions problématiques $\mathcal{T}$, plus précisément $\mathcal{T}_1$ déjà vue, $\mathcal{T}_2$ au voisinage de $x_2 = \overline{\Phi}(0, 1/2, 0, 1/2)$ qui vérifie les hypothèses du Théorème 3.2 (avec $j = 1$) et $\mathcal{T}_3$ au voisinage de $x_3 = \overline{\Phi}(1/2, 0, 1/2, 0)$ qui fait de même. Les calculs mènent à $t_2 = x_2$ et $t_3 = x_3$. Mais x_2 et x_3 sont de la forme $\Phi(\xi)$ avec ξ comme dans la Proposition 1.11 et $|N_{K/\mathbb{Q}}(\Upsilon)| = 4$. Par conséquent $m_{\overline{K}}(t_2) = m_{\overline{K}}(t_3) = 1/4$. Finalement, en ayant recours à ε_1^{-1} on peut contrôler que les hypothèses du Corollaire 3.5 sont vérifiées par $\mathcal{T}_1$. Nous obtenons ainsi le résultat suivant qui avait été conjecturé par Cohn et Deutsch [CD86] (notons que nous avions déjà établi la première partie de ce résultat dans [Ce00]).

Théorème 3.33. *Si $K = \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$, on a*

$$M(K) = M(\overline{K}) = \frac{1}{2} \quad et \quad M_2(K) = M_2(\overline{K}) = \frac{1}{4}.$$

Comme notre but principal, pour l'instant, est le calcul de $M(K)$, nous n'approfondirons pas dans cette direction, même si incidemment nous avons calculé $M_2(K)$ pour certains corps. Nous y reviendrons toutefois dans le Chapitre 5, lorsque nous serons amenés à déterminer $\mathrm{sp}(K) \cap [1, +\infty[$.

3.5 Une variante

Il n'est pas rare que l'on ait à établir

$$M(\overline{K}) = M(K) = \frac{m}{2^n},$$

où m est un entier positif vérifiant

$$m = |N_{K/\mathbb{Q}}(\Upsilon)| \quad \text{où} \quad \Upsilon \in \mathbb{Z}_K.$$

Dans ce cas, on peut recourir à un critère plus simple qui évite d'avoir recours à E_K. Celui-ci s'énonce de la façon suivante.

Proposition 3.34. *Soit $\mathcal{T}$ une partie bornée de $H = \mathbb{R}^n$. Supposons qu'il existe deux éléments $X = \Phi(\alpha)$ et $Y = \Phi(\beta)$ de $\Phi(\mathbb{Z}_K)$ tels que*

$$\mathcal{N}(X - Y) = |N_{K/\mathbb{Q}}(\alpha - \beta)| \leq m, \tag{3.26}$$

et tels que pour tout $x \in \mathcal{T}$ et pour tout $i \in \{1, \ldots, n\}$,

$$(x_i - X_i)(x_i - Y_i) \leq 0. \tag{3.27}$$

Alors pour tout $x \in \mathcal{T}$, on a

$$m_{\overline{K}}(x) \leq \frac{m}{2^n}.$$

De plus

$$m_{\overline{K}}(x) = \frac{m}{2^n} \quad \Rightarrow \quad \mathcal{N}(X - Y) = m \quad et \quad x = \frac{X + Y}{2}.$$

Preuve. Soit $x \in \mathcal{T}$. Considérons le produit $\mathcal{N}(x-X)\cdot\mathcal{N}(x-Y)$. On a

$$\mathcal{N}(x-X)\cdot\mathcal{N}(x-Y) = \prod_{i=1}^{n}\Big(|x_i - X_i|\cdot|x_i - Y_i|\Big).$$

Mais, par (3.27), pour chaque i, on a

$$|x_i - X_i| + |x_i - Y_i| = |X_i - Y_i|.$$

On en déduit que lorsque

$$|x_i - X_i| = |x_i - Y_i| = \frac{|X_i - Y_i|}{2},$$

c'est-à-dire lorsque $x_i = (X_i + Y_i)/2$, le produit $|x_i - X_i|\cdot|x_i - Y_i|$ est maximal et vaut alors $(X_i - Y_i)^2/4$. Par conséquent on peut écrire, en utilisant (3.26),

$$\mathcal{N}(x-X)\cdot\mathcal{N}(x-Y) \leq \prod_{i=1}^{n}\frac{(X_i - Y_i)^2}{4} = \frac{1}{4^n}\mathcal{N}(X-Y)^2 \leq \frac{m^2}{4^n}, \tag{3.28}$$

et voir qu'il y a égalité entre le premier et le dernier terme de (3.28), si et seulement si

$$x = \frac{X+Y}{2} \quad \text{et} \quad \mathcal{N}(X-Y) = m.$$

On déduit de (3.28) que l'un des deux facteurs $\mathcal{N}(x-X)$ ou $\mathcal{N}(x-Y)$ est inférieur ou égal à $m/2^n$, d'où

$$m_{\overline{K}}(x) \leq \frac{m}{2^n}.$$

Supposons maintenant que $m_{\overline{K}}(x) = m/2^n$. Alors nécessairement $\mathcal{N}(x-X)$ et $\mathcal{N}(x-Y)$ sont supérieurs ou égaux à $m/2^n$, ce qui entraîne qu'il y a égalité dans (3.28) entre le premier et le dernier terme. D'où la conclusion par ce qui précède. $\square$

Ce critère est d'autant plus pratique qu'il présente les caractéristiques suivantes.
Tout d'abord, il est particulièrement adapté à notre découpage. En effet si $\mathcal{P}$ est un parallélotope du recouvrement vérifiant

$$\mathcal{P} = [u_1, v_1] \times \ldots \times [u_n, v_n],$$

la condition (3.27) est particulièrement simple à vérifier pour $\mathcal{T} = \mathcal{P}$. Il suffit d'avoir

$$(u_i - X_i)(u_i - Y_i) \leq 0 \quad \text{et} \quad (v_i - X_i)(v_i - Y_i) \leq 0, \tag{3.29}$$

pour tout $i \in \{1, \ldots, n\}$. En général, dans le cas précis que nous évoquons, les parallélotopes problématiques, c'est-à-dire ceux qui n'ont pas été absorbés par un test similaire au test d'absorption décrit plus haut, vérifient ce genre d'hypothèses de localisation.

Par ailleurs, la seconde partie de la Proposition 3.34 montre qu'il n'y a qu'un candidat éventuel x de $\mathcal{P}$ si (3.29) est vérifiée avec $\mathcal{N}(X-Y) = m$, à savoir $(X+Y)/2$. Autrement dit, que $\mathcal{P}$ contienne ou non ce point importe peu. Il suffit en fait de vérifier si l'on a effectivement

$$m_{\overline{K}}\Big(\frac{X+Y}{2}\Big) = \frac{m}{2^n},$$

pour localiser tous les points rationnels critiques.

Enfin, nous n'avons besoin d'aucune connaissance particulière sur E_K.

C'est ce critère que nous avons utilisé dans [Ce00] pour établir la première partie du Théorème 3.33 et pour établir également que

$$\text{si} \quad K = \mathbb{Q}\Big(\sqrt{2+\sqrt{2+\sqrt{2}}}\Big), \qquad \text{on a} \quad M(\overline{K}) = M(K) = \frac{1}{2}.$$

3.6 Aspects pratiques

3.6.1 Généralités

Le programme a été écrit en C et les calculs ont été essentiellement menés sur un Pentium II 300Mhz. Nous avons utilisé les tables de corps disponibles sur le site du Laboratoire A2X de Bordeaux [A2X]. Nous avons calculé les $\mathbb{Z}$-bases (e_i), M et les ε_i $(1 \le i \le n-1)$ à l'aide du logiciel PARI [Pa] et nous avons choisi des bases LLL-réduites, qui donnent des vecteurs relativement courts et une bonne configuration géométrique.

3.6.2 Découpage, recouvrement et test d'absorption

Dans la première partie de l'algorithme (découpage et recouvrement) quand la borne supérieure trouvée pour l_n (ou l_{n-1}, etc) est proche d'un entier tout en lui étant inférieure, on prend en compte celui-ci pour les valeurs possibles de l_n (ou l_{n-1}, etc). Même chose pour la borne inférieure si elle est proche d'un entier tout en lui étant supérieure. Ainsi sommes-nous sûrs de recouvrir $\mathcal{F}$ et même un peu plus.

Pour le test d'absorption, en général, on prend $\epsilon = 10^{-3}$ (pour $n=2$, parfois, on a besoin d'un ϵ plus petit, mais pour les petits degrés, on peut le faire), et différentes valeurs de B en fonction de n et de K (pour certains corps une petite valeur suffit). Lorsqu'on teste $\mathcal{B}_l$ on utilise d'abord un ensemble particulier d'entiers $\mathcal{I} \subseteq \mathcal{X}$ qui est défini de la façon suivante. $\mathcal{I}$ est initialisé à $\emptyset$. Quand on teste un $\mathcal{B}_l$, on regarde d'abord si $\mathcal{B}_l$ est absorbé par un élément de $\mathcal{I}$, en commençant par le dernier de cette liste. Si ce n'est pas le cas, on cherche dans $\mathcal{X}$ un entier adéquat. Si on en trouve un, on le met dans $\mathcal{I}$ en dernière position et on teste le $\mathcal{B}_l$ suivant. Si on n'en trouve pas, le $\mathcal{B}_l$ étudié est temporairement problématique.

3.6.3 Le test des unités

Pour l'étape suivante (multiplication de $\mathcal{P}$ par $\Phi(\varepsilon)$ et translation) on renforce (3.21) (voir Proposition 3.29) et on prend $(1+|\sigma_{i_p}(\varepsilon)|)h_{i_p}+\epsilon$ à la place de $(1+|\sigma_{i_p}(\varepsilon)|)h_{i_p}$ pour être absolument sûr que l'intersection avec les $\mathcal{P}$ est réduite à $\emptyset$.

Il est ainsi possible que nous sélectionnions un $\mathcal{P}$ qui aurait dû être éliminé. C'est sans conséquence (voir Remarque 3.17). En général on utilise deux unités (la plupart du temps ε_1 et ε_2) pour le test d'élimination.

3.6.4 Détermination des points rationnels critiques

Pour le calcul des t_i donnés par le Théorème 3.16 et des $m_{\overline{K}}(t_i)$, nous devons préciser la façon dont nous nous y prenons. Le problème vient du fait que pour tous les calculs, nous travaillons en virgule flottante, mais que nous voulons des valeurs rationnelles exactes.

Tout d'abord, un cycle $\mathcal{T}_0(X_0) \to \ldots \to \mathcal{T}_0(X_{j-1})$ étant donné, comment pouvons nous calculer ξ, où $\Phi(\xi) = t$ et t correspond à $\mathcal{T}_0$? On sait que

$$\xi = \frac{\Omega}{\varepsilon^j - 1}$$

avec

$$\Omega = \varepsilon^{j-1}\Upsilon_0 + \varepsilon^{j-2}\Upsilon_1 + \ldots. + \varepsilon\Upsilon_{j-2} + \Upsilon_{j-1}.$$

On doit donc avoir

$$\text{pour tout } i,\ \Psi^{-1}(\xi)_i \in \frac{1}{|N_{K/\mathbb{Q}}(\varepsilon^j - 1)|}\mathbb{Z}.$$

La première chose à faire est d'obtenir une valeur exacte pour $|N_{K/\mathbb{Q}}(\varepsilon^j - 1)|$. Pour cela on calcule $|\prod_{i=1}^n(\sigma_i(\varepsilon^j) - 1)|$, on vérifie que le nombre obtenu est suffisamment proche d'un entier N et on identifie $|N_{K/\mathbb{Q}}(\varepsilon^j - 1)|$ à N. Ensuite on calcule t qui est donné par

$$\text{pour tout } i,\ t_i = \frac{\sum_{l=0}^{j-1} \sigma_i(\varepsilon)^l \sigma_i(\Upsilon_{j-1-l})}{\sigma_i(\varepsilon)^j - 1}.$$

Finalement on calcule $u = \Psi^{-1}(\xi) = \overline{\Phi}^{-1}(t)$ à l'aide de M'. On vérifie que tous les u_i obtenus sont proches d'entiers a_i, quand on les multiplie par N, et on identifie u_i à a_i/N, obtenant ainsi la valeur exacte de u. Il n'est pas rare à ce stade que l'on puisse, par simplification, remplacer dans les a_i/N, N par un entier d plus petit. Dans tous les cas, on obtient $u_i \in 1/d\ \mathbb{Z}$ où d est un diviseur de N et on pose $N' = \inf(N, d^n)$ de telle sorte que $N_{K/\mathbb{Q}}(\nu\xi - \Upsilon) \in 1/N'\ \mathbb{Z}$ pour tout $(\nu, \Upsilon) \in E_K \times \mathbb{Z}_K$. Il est alors possible, mais pas indispensable, de re-calculer $t = \overline{\Phi}(u)$.

Remarque 3.35. En relation avec la Proposition 1.11, si le k testé est de la forme $1/p$, on peut chercher des entiers Υ de norme $\pm p$, calculer l'« inverse » de $\Phi(\Upsilon)$ dans $\mathbb{R}^n$ qui, quand il est multiplié par M' doit donner un élément de $1/p\ \mathbb{Z}^n$, identifié par approximation. Il reste à regarder si oui ou non nous trouvons (modulo $\mathbb{Z}$) les coordonnées exactes de ξ déterminées plus tôt, auquel cas il est inutile de calculer $m_K(\xi)$ qui vaut $1/p$.

3.6.5 Détermination des orbites

Dans le cas général, on doit déterminer $\mathrm{Orb}(t)$ ou $\mathrm{Orb}(\xi)$. On vérifie d'abord que ξ n'a pas déjà été rencontré dans une précédente orbite. L'étape suivante consiste à déterminer les p_i $(1 \le i \le n-1)$ comme définis dans la section 3.3.8.

On calcule successivement $\xi_1 = \varepsilon_i\xi - X_1$ avec $X_1 \in \mathbb{Z}_K$ tel que $\Phi(\xi_1) \in \mathcal{F}$, $\xi_2 = \varepsilon_i\xi_1 - X_2$ avec $X_2 \in \mathbb{Z}_K$ tel que $\Phi(\xi_2) \in \mathcal{F}$ (notons que $\xi_2 \equiv \varepsilon_i\xi_1 \bmod \mathbb{Z}_K$), et ainsi de suite, jusqu'à ce qu'on trouve $\xi_{p_i} = \xi$. À chaque étape on identifie $\xi_{j+1} = \Phi^{-1}(\Phi(\varepsilon_i).\Phi(\xi_j)) \bmod \mathbb{Z}_K$ à l'élément le plus proche de $1/d\,\mathbb{Z}_K$, s'il est suffisamment proche, et on re-calcule $\Phi(\xi_{j+1})$.

La dernière étape est la détermination à proprement parler de $\mathrm{Orb}(\xi)$. On fait une boucle dans laquelle on calcule successivement tous les $\xi' = \pm\xi\prod\varepsilon_i^{k_i}$ où pour tout i, $0 \leq k_i \leq p_i - 1$. Pour cela, à chaque étape, on calcule $\varepsilon_i^{k_i} \bmod d\,\mathbb{Z}_K$ et $\Phi(\varepsilon_i^{k_i} \bmod d\,\mathbb{Z}_K)$ à partir de la précédente valeur de cette puissance, par multiplication par $\Phi(\varepsilon_i)$ ou en donnant la valeur $\Phi(1)$, si nécessaire (changement de k_i). On applique ensuite M', on vérifie qu'on est à proximité d'un élément de $\mathbb{Z}_K$ dont les coordonnées sont réduites modulo d, et on prend pour $\Phi(\varepsilon_i^{k_i} \bmod d\,\mathbb{Z}_K)$ son image par Φ.
Ainsi, nous sommes sûrs d'avoir de « bonnes » et petites valeurs pour les puissances successives des unités : nous travaillons modulo $d\,\mathbb{Z}_K$ parce que si nous multiplions $\xi \in 1/d\ \mathbb{Z}_K$ par ε^{k_i} ou par $\varepsilon^{k_i} \bmod d\,\mathbb{Z}_K$ le résultat est le même modulo $\mathbb{Z}_K$. Ensuite, pour le calcul de $\xi' = \pm\xi\prod\varepsilon_i^{k_i} \in 1/d\ \mathbb{Z}_K$, à chaque étape du produit, on identifie le produit partiel à l'élément le plus proche de $1/d\ \mathbb{Z}_K$ s'il est suffisamment proche. Nous connaissons ainsi les valeurs exactes des éléments de $\mathrm{Orb}(\xi)$.

3.6.6 Calcul de $m_{\overline{K}}(t)$

Nous avons encore à déterminer $m_{\overline{K}}(t)$ comme expliqué dans la section 3.3.8. Pour être sûrs d'avoir tous les entiers nécessaires nous prenons $k+\epsilon$ à la place de k dans le Théorème 2.8. Comme pour tout $X \in \mathbb{Z}_K$ et tout $\xi' \in \mathrm{Orb}(x)$, $N_{K/\mathbb{Q}}(\xi' - X) \in 1/N'\ \mathbb{Z}$, nous vérifions que les normes successives que nous calculons sont proches de $1/N'\ \mathbb{Z}$ et nous les identifions aux valeurs de $1/N'\ \mathbb{Z}$ dont elles sont proches.

3.7 Commentaires sur les tables

Les résultats établis figurent en annexes. Nous n'avons donné dans ces tables que les nouveaux résultats. Ainsi y a-t-il des trous, qui correspondent aux résultats déjà publiés par ailleurs.

Parfois, pour $n = 2$, lorsque la valeur trouvée pour $|N_{K/\mathbb{Q}}(\varepsilon^j - 1)|$ était trop grande, nous avons utilisé MAPLE pour la dernière partie des calculs. Pour $n > 2$ cela n'a jamais été le cas.
En général, pour les corps « faciles » le temps de calcul varie de moins de 2 secondes pour $n = 2$, $n = 3$ et même $n = 4$ à moins d'une demi-heure pour $n = 7$, mais, pour quelques rares corps, notamment en degré 3 et 4, il a dépassé 6 heures, la limite que nous nous sommes imposée. Ceci explique quelques lacunes dans les tables. Dans ce cas, nous donnons un intervalle pour $M(K)$.

3.7.1 Corps quadratiques

Pour $n = 2$, nous complétons les tables que l'on peut trouver dans [Lem95] et qui donnent le minimum euclidien de $\mathbb{Q}(\sqrt{m})$ pour $2 \leq m \leq 102$, où m est un entier sans facteur carré.

Apparemment, avant ce travail, il n'y avait pas de minimum connu au-delà de la limite $m = 102$, à l'exception des suites de corps déjà mentionnées (voir [BSD52a] en particulier).

Nous avons calculé $M(K)$ pour $K = \mathbb{Q}(\sqrt{m})$, m sans facteur carré et $103 \leq m \leq 400$, à 28 exceptions près pour m =139, 151, 163, 166, 191, 199, 211, 214, 239, 241, 249, 262, 271, 283, 307, 311, 313, 319, 331, 334, 337, 358, 367, 379, 382, 391, 393 et 394. Ces cas n'ont pas été traités à cause de la taille de l'unité fondamentale ($|\varepsilon| > 10^7$). Bien sûr cela peut être fait en multi-précision.

Dans chaque ligne du tableau, nous donnons m ($K = \mathbb{Q}(\sqrt{m})$), le nombre T de points rationnels critiques de $\mathcal{F}$ et $M(\overline{K}) = M(K)$.

3.7.2 Corps cubiques

Pour $n = 3$, nous complétons les résultats obtenus par Cavallar et Lemmermeyer [CaL98]. Dans la table B.1, nous donnons les premiers minima qui n'avaient pas été calculés dans [CaL98]. Les notations sont les mêmes que celles de la table A.1.
La table B.2 est consacrée aux corps de nombres de discriminant inférieur à 11000 laissés indéterminés dans [CaL98] (en fait, ils sont tous euclidiens pour la norme), et de tous les corps de nombres de discriminant compris entre 11000 et 15000, non étudiés dans [CaL98]. Nous avons récemment découvert que quelques-uns de ces résultats (quand $D_K \leq 12821$) étaient donnés dans la version actualisée de [Lem95] disponible sur le site de Lemmermeyer (voir [Lem99]). Dans tous les cas, nos résultats sont les mêmes.
Dans le même esprit que pour les tables de [CaL98], dans la table B.2, nous ne donnons le minimum euclidien que des corps qui ne sont pas euclidiens pour la norme. Pour les autres, la lettre E indique qu'ils sont euclidiens pour la norme.

3.7.3 Corps quartiques

Pour $n = 4$ nous avons calculé les minima euclidiens des corps de discriminant inférieur à 40000 (table C.1). La nature euclidienne d'un grand nombre d'entre eux avait déjà été établie par Quême [Qu98] mais il avait laissé quelques corps indéterminés. En fait, certains d'entre eux ne sont pas euclidiens pour la norme.

3.7.4 Corps quintiques

Ici, seuls 25 corps de nombres euclidiens pour la norme étaient recensés [Qu98].
Nous avons calculé le minimum euclidien des 156 corps de nombres de discriminant inférieur à 511000 (table D.1). À une exception, ils sont tous euclidiens pour la norme.

3.7.5 Degrés supérieurs

À notre connaissance, très peu de choses étaient connues sur les corps de degré supérieur à 5. Ici nous donnons essentiellement les résultats que nous avons établis pour $n = 6$ (les 156 premiers corps de nombres - table E.1) et $n = 7$ (les 132 premiers corps de nombres

- table F.1). Jusqu'à présent, nous n'avons pas utilisé l'algorithme de façon systématique pour le degré 8. Néanmoins nous avons calculé le minimum euclidien des 18 premiers corps de nombres figurant dans les tables de J. Klüners [Kl]. Les résultats figurent dans la table G.1.

Rappelons que nous avions déjà traité le sous-corps réel maximal du corps cyclotomique $\mathbb{Q}(\zeta_{32})$, $K = \mathbb{Q}\left(\sqrt{2+\sqrt{2+\sqrt{2}}}\right)$, dont le minimum euclidien est $1/2$ [Ce00], par la variante exposée en section 3.5. Nous avons également trouvé par l'algorithme développé ici, que, si $K = \mathbb{Q}\left(\sqrt{2+\sqrt{2+\sqrt{3}}}\right)$, on a $M(K) = M(\overline{K}) = 1/2$.

3.7.6 Remarque conclusive

Par la Proposition 1.11, si on pose

$$\mu(K) = \frac{1}{\inf\left\{|N_{K/\mathbb{Q}}(\Upsilon)|;\ \Upsilon \in \mathbb{Z}_K \backslash \left(E_k \cup \{0\}\right)\right\}},$$

on peut écrire

$$\mu(K) \leq M(K).$$

Il est remarquable d'observer qu'en fait il y a égalité pour les petites valeurs de D_K, le nombre de cas dans lesquels ce phénomène apparaît croissant avec n.
Cette remarque n'est pas en contradiction avec le sentiment que nous avons pu avoir au sujet des corps $\mathbb{Q}(\zeta_{2^n} + \zeta_{2^n}^{-1})$ (où $n \geq 2$ et ζ_{2^n} est une racine primitive 2^n-ième de l'unité) dont le minimum euclidien, qui vaut $1/2$ pour $n \leq 5$, peut être conjecturé égal à $1/2$ pour $n = 6$ et peut-être pour n supérieur à 6 [Ce00].

3.8 Extension au cas complexe

Il va de soi que les idées utilisées jusqu'à présent peuvent être exploitées dans un cadre plus général. Ainsi peut-on s'appuyer sur elles pour développer un algorithme dans le cas des corps de nombres complexes. Nous allons préciser ici comment, sans entrer toutefois dans le détail de la mise en œuvre comme nous avons pu le faire précédemment. Nous verrons qu'il y a peu de choses à changer pour que le programme fonctionne dans le cas général. Ce travail n'a cependant pas encore été fait.

3.8.1 Le recouvrement

Reprenons les notations du cas totalement réel. On fixe une $\mathbb{Z}$-base $(e_i)_{1\leq i\leq n}$ de $\mathbb{Z}_K$ et le domaine fondamental $\mathcal{F} \subseteq H$, défini par

$$\mathcal{F} = \left\{\sum_{i=1}^{n} x_i \Phi(e_i);\ 0 \leq x_i < 1\right\}.$$

Il faut d'abord recouvrir $\mathcal{F}$ par des parallélotopes. Ceux-ci peuvent être définis de la façon suivante.

Si $\alpha = (a_i)_{1\le i\le n}$ et $\beta = (b_i)_{1\le i\le n}$ sont deux n-uplets de $\mathbb{R}^n$ vérifiant pour tout i, $a_i < b_i$, on définit $\mathcal{P}_{\alpha,\beta}$ comme étant l'ensemble des $x \in H$ vérifiant

- $a_i \le x_i \le b_i$ pour $1 \le i \le r_1$,
- $a_{r_1+2i-1} \le \Re(x_{r_1+i}) \le b_{r_1+2i-1}$ pour $1 \le i \le r_2$,
- $a_{r_1+2i} \le \Im(x_{r_1+i}) \le b_{r_1+2i}$ pour $1 \le i \le r_2$.

Notons qu'aucune condition sur les coordonnées x_i avec $i > r_1 + r_2$ n'est nécessaire car si $y \in H$, $y_{r_1+r_2+i} = \overline{y_{r_1+i}}$.

Nous n'entrons pas ici dans les subtilités de la définition d'un tel recouvrement, mais le recours à la matrice $M = (\sigma_i(e_j))_{1\le i,j\le n}$ est encore possible. Comme plus haut, on se servira d'un découpage symétrique par rapport au centre Ω de $\mathcal{F}$, ce qui permet d'avoir recours à la symétrie s par rapport à Ω pour réduire les calculs.

3.8.2 Le test d'absorption

Notons C le centre d'un parallélotope $\mathcal{P}_{\alpha,\beta}$ et posons $h_i = (b_i - a_i)/2$ pour tout $i \in \{1,\dots,n\}$. Pour savoir si $\mathcal{P}_{\alpha,\beta}$ est absorbé par un $X \in \mathcal{X}$, c'est-à-dire vérifie

$$\text{pour tout } x \in \mathcal{P}_{\alpha,\beta},\ \mathcal{N}(x - X) \le k - \epsilon,$$

(3.18) peut être remplacée par la condition suivante.

Proposition 3.36. *Si*

$$\prod_{i=1}^{r_1}\Big(|C_i - X_i| + h_i\Big)\prod_{i}^{r_2}\Big((|\Re(C_{r_1+i}-X_{r_1+i})|+h_{r_1+2i-1})^2+(|\Im(C_{r_1+i}-X_{r_1+i})|+h_{r_1+2i})^2\Big) \le k-\epsilon,$$

alors $\mathcal{P}_{\alpha,\beta}$ est absorbé par X.

Notons que comme dans le cas totalement réel, cette inégalité est optimale.

3.8.3 Le test des unités

Soit $\mathcal{P}_{\alpha,\beta}$, que l'on notera plus simplement $\mathcal{P}$, le parallélotope étudié. Notons C son centre et posons $h_i = (b_i - a_i)/2$ pour $1 \le i \le n$. Soit ε l'unité utilisée et $C'' = (\sigma_i(\varepsilon)C_i)_{1\le i\le n}$. Notons $\mathcal{P}_p$ ($1 \le p \le 2q$) les éléments de la liste des parallélotopes problématiques à un instant donné. Pour pouvoir éliminer $\mathcal{P}$, il nous faut un critère simple permettant d'affirmer que $\Phi(\varepsilon)\cdot\mathcal{P}$ ne rencontre effectivement aucun des $\mathcal{P}_p$ modulo $\Phi(\mathbb{Z}_K)$. Pour cela on a vu qu'il était d'abord nécessaire de déterminer tous les vecteurs de translation permettant de ramener $\Phi(\varepsilon)\cdot\mathcal{P}$ sur $\mathcal{F}$. Cette procédure est, encore ici, rendue possible par le recours à M. En revanche le critère (3.21) doit être modifié. Supposons que nous ayons déterminé tous les vecteurs de translation possibles, et notons-les X_j, avec $1 \le j \le g$. Notons également comme plus haut D_p le centre du parallélotope problématique $\mathcal{P}_p$, qui a les mêmes dimensions (les h_i) que $\mathcal{P}$. On a le critère suivant.

Proposition 3.37. *Si pour tout $j \in \{1, \dots, g\}$ et pour tout $p \in \{1, \dots, 2q\}$, il existe un $i_p \in \{1, \dots, r_1\}$ vérifiant*

$$|(C'' - X_j - D_p)_{i_p}| > (1 + |\sigma_{i_p}(\varepsilon)|) h_{i_p},$$

ou un $i_p \in \{1, \dots, r_2\}$ vérifiant

$$\left|(C'' - X_j - D_p)_{r_1+i_p}\right| > (1 + |\sigma_{r_1+i_p}(\varepsilon)|) \sqrt{h^2_{r_1+2i_p-1} + h^2_{r_1+2i_p}},$$

alors $\mathcal{P}$ et $s(\mathcal{P})$ peuvent être éliminés de la liste des parallélotopes problématiques.

Notons que contrairement à ce qui se passe dans le cas totalement réel, le critère donné ici n'est plus optimal. Toutefois il doit largement suffire en pratique.

3.8.4 L'exploitation des résultats

Pour le reste, il n'y a rien à changer, jusqu'à l'interprétation finale du comportement des régions problématiques. On voit alors que les théorèmes 3.2, 3.16 et leurs corollaires restent valables si au lieu de prendre $\varepsilon \neq \pm 1$ on impose aux unités utilisées la condition

$$\text{pour tout } i \in \{1, \dots, n\},\ |\sigma_i(\varepsilon)| \neq 1.$$

Il est donc tout à fait envisageable de généraliser l'algorithme aux corps de nombres quelconques.

Chapitre 4

Comparaison des spectres et questions de rationalité

Dans ce chapitre nous reprenons pour l'essentiel l'article "Euclidean and inhomogeneous spectra of number fields with unit rank strictly greater than 1", accepté pour publication au *Journal für die reine und angewandte Mathematik*.

Si l'algorithme a permis d'obtenir des résultats, c'est parce que pour tous les corps considérés, on avait $M(K) = M(\overline{K})$ et plus précisément la propriété suivante qui correspond à la Conjecture 1 de Barnes et Swinnerton-Dyer.

$$\text{Il existe } \xi \in K \text{ tel que } M(\overline{K}) = m_K(\xi).$$

Dans cette partie nous allons tenter d'élucider le rapport existant entre minimum inhomogène et minimum euclidien, et même entre spectre inhomogène et spectre euclidien.

4.1 Nouvelles notations

Reprenons les notations employées jusqu'ici et en particulier celles que nous avons utilisées dans la section 3.3. Soit donc comme précédemment Φ le plongement de K dans $H \subseteq \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2}$ défini par

$$\text{pour tout } \xi \in K, \Phi(\xi) = (\sigma_1(\xi), ..., \sigma_{r_1+2r_2}(\xi)).$$

Soit $(e_i)_{1 \leq i \leq n}$ une $\mathbb{Z}$-base de $\mathbb{Z}_K$. K peut être identifié à $\mathbb{Q}^n$ via Ψ où $\Psi(x) = \sum_{i=1}^n x_i e_i$ si $x \in \mathbb{Q}^n$, et de même, $\mathbb{Z}_K$ peut être identifié à $\mathbb{Z}^n$.

On peut prolonger continûment $\Phi \circ \Psi$ de $\mathbb{Q}^n$ à $\mathbb{R}^n$ par une application notée $\overline{\Phi}$ de la façon suivante.

$$\text{Pour tout } x \in \mathbb{R}^n, \ \overline{\Phi}(x) = \left(\sum_{i=1}^n x_i \sigma_1(e_i), ..., \sum_{i=1}^n x_i \sigma_{r_1+2r_2}(e_i) \right).$$

$\overline{\Phi}$ est un $\mathbb{R}$-isomorphisme de $\mathbb{R}^n$ sur H.
En vue de considérations ultérieures, on peut prolonger continûment $\overline{\Phi}$ à $\mathbb{C}^n$ par $\overline{\Phi}'$,

de telle sorte que $\overline{\Phi}'$ soit un $\mathbb{C}$-endomorphisme de $\mathbb{C}^n$ (si $(u,v) \in \mathbb{R}^n \times \mathbb{R}^n$, on pose $\overline{\Phi}'(u+Iv) = \overline{\Phi}(u) + I\overline{\Phi}(v)$).
$\overline{\Phi}'$ est un automorphisme de $\mathbb{C}^n$ et le diagramme suivant , où i_1, i_2 et i_3 sont les injections canoniques, est commutatif.

$$\begin{array}{ccccc} \mathbb{Q}^n & \xrightarrow{i_1} & \mathbb{R}^n & \xrightarrow{i_2} & \mathbb{C}^n \\ \Psi\big\downarrow & & \big\downarrow\overline{\Phi} & & \big\downarrow\overline{\Phi}' \\ K & \xrightarrow[\Phi]{} & H & \xrightarrow[i_3]{} & \mathbb{C}^n \end{array}$$

On peut étendre continûment $N_{K/\mathbb{Q}} \circ \Psi$ de $\mathbb{Q}^n$ à $\mathbb{R}^n$ par $\mathcal{N}'$ définie comme suit.

$$\text{Pour tout } x \in \mathbb{R}^n,\ \mathcal{N}'(x) = \prod_{i=1}^{n} \left(\sum_{j=1}^{n} x_j \sigma_i(e_j) \right).$$

On a alors

$$\mathcal{N} \circ \overline{\Phi} = \mathcal{N}'.$$

Posons également

$$\text{pour tout } x \in \mathbb{R}^n,\ m(x) = \inf\{\mathcal{N}'(x - X);\ X \in \mathbb{Z}^n\}.$$

Il est facile de voir que

$$m = m_{\overline{K}} \circ \overline{\Phi},$$

si bien que l'étude de $m_{\overline{K}}$ se ramène à celle de m.
Comme de plus,

$$\text{si } x \in \mathbb{Q}^n,\ m(x) = m_K(\Psi(x)),$$

on voit que l'étude de m_K se ramène à celle de la restriction de m à $\mathbb{Q}^n$. En particulier

$$\mathrm{sp}(\overline{K}) = m(\mathbb{R}^n) \quad \text{et} \quad \mathrm{sp}(K) = m(\mathbb{Q}^n).$$

Les propriétés de $m_{\overline{K}}$ se traduisent ainsi.

Proposition 4.1. *La fonction m a les propriétés suivantes.*

- *m est définie modulo $\mathbb{Z}^n$.*
- *m est semi-continue supérieurement sur $\mathbb{R}^n$.*
- *Pour tout $x \in \mathbb{R}^n$, et toute unité $\varepsilon \in E_K$,*
$$m\left(\overline{\Phi}^{-1}\left(\Phi(\varepsilon).\overline{\Phi}(x)\right)\right) = m(x).$$

On en déduit que m définit sur $\mathbb{R}^n/\mathbb{Z}^n$ une application $\tilde{m}$ donnée par :

$$\text{pour tout } x \in \mathbb{R}^n,\ \tilde{m}(\overline{x}) = m(x),$$

où $\overline{x}$ est la classe de x modulo $\mathbb{Z}^n$.
Cette application, équivalente à celle induite par $m_{\overline{K}}$ sur $H/\Phi(\mathbb{Z}_K)$, est également semi-continue supérieurement.

4.2 Les résultats de Berend

Notons $\mathbb{T}_n$, le tore de dimension n défini par

$$\mathbb{T}_n = \mathbb{R}^n/\mathbb{Z}^n,$$

et rappelons quelques faits bien connus. $\mathbb{T}_n$ est un groupe additif compact pour la topologie induite par la métrique de $\mathbb{R}^n$. Les endomorphismes (continus) de $\mathbb{T}_n$ peuvent être représentés par les matrices $n \times n$ à coefficients entiers. Les points et les endomorphismes de $\mathbb{T}_n$ peuvent être respectivement relevés en points et transformations linéaires de $\mathbb{R}^n$. Soit f un endomorphisme de $\mathbb{T}_n$. On notera indifféremment f sa matrice, son relèvement à $\mathbb{R}^n$ dont la matrice est la même, et quand on parlera des valeurs propres et des vecteurs propres de f, cela sera au sens ordinaire pour f comme endomorphisme de $\mathbb{C}^n$ (prolongé à $\mathbb{C}^n$ par linéarité de sorte que la matrice de f soit la même). Introduisons maintenant quelques notions fondamentales que nous énoncerons pour $\mathbb{T}_n$ mais qui sont valables dans le cadre plus général des groupes compacts.

Soit $\mathcal{E}$ un ensemble d'endomorphismes de $\mathbb{T}_n$.

Définition 4.2. Un sous-ensemble F de $\mathbb{T}_n$ sera dit *$\mathcal{E}$-invariant* si pour tout $f \in \mathcal{E}$ on a

$$f(F) \subseteq F.$$

Définition 4.3. Un fermé non vide $\mathcal{E}$-invariant F sera dit *$\mathcal{E}$-minimal* s'il ne contient aucun sous-ensemble strict fermé non vide $\mathcal{E}$-invariant.

En utilisant le lemme de Zorn, il est facile de voir que l'on a le résultat suivant (voir par exemple [Fu81] ou [Br76]).

Proposition 4.4. *Tout sous-ensemble fermé non vide $\mathcal{E}$-invariant de $\mathbb{T}_n$ contient un sous-ensemble $\mathcal{E}$-minimal.*

Un cas particulier essentiel est celui où $\mathcal{E}$ est un semi-groupe commutatif d'endomorphismes de $\mathbb{T}_n$.
Dans un article fondamental [Fu67], Furstenberg a établi plusieurs résultats que l'on peut combiner pour obtenir le théorème suivant.

Théorème 4.5. *Soit Σ un semi-groupe d'épimorphismes de $\mathbb{T}_1$. Les conditions suivantes sont équivalentes.*

- *Tout sous-ensemble strict, fermé et Σ-invariant de $\mathbb{T}_1$ est un ensemble fini, composé d'éléments de torsion.*
- *Tout sous-ensemble Σ-minimal est fini et composé d'éléments de torsion.*
- *Σ est non lacunaire,*

où, Σ étant identifié à un semi-groupe multiplicatif d'entiers non nuls, il est dit lacunaire lorsque tous ses éléments positifs sont puissances d'un même entier.

Ce résulat lui permettait alors de généraliser un théorème de Hardy et Littlewood selon lequel, si r est un entier positif donné et si α est irrationnel, l'ensemble $\{n^r\alpha;\ n \in \mathbb{N}\}$ est dense modulo 1.

Quelques années plus tard Berend publia deux articles essentiels [Be83] et [Be84] dans lesquels il généralisa le résultat de Furstenberg à n quelconque. Mais avant de donner les résultats obtenus par Berend nous avons besoin de quelques notations et définitions supplémentaires.

Supposons que Σ soit un semi-groupe commutatif d'endomorphismes de $\mathbb{T}_n$. L'ensemble des vecteurs propres communs aux éléments de Σ appartenant à $\mathbb{C}^n$ 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, relatives à tous les éléments de Σ.

Définition 4.6. Σ est dit *hyperbolique* si pour tout $v \in \mathrm{evec}\Sigma$, $\mathrm{spec}_v\Sigma \not\subseteq \mathbb{C}_1$, où $\mathbb{C}_1$ est le cercle unité de $\mathbb{C}$.

Définition 4.7. 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 vérifiant

$$\text{si } (m,l) \in \mathbb{Z}^2,\ \text{alors } {\alpha_v}^m = {\beta_v}^l \Rightarrow m = l = 0.$$

Énonçons les résultats de Berend.

Théorème 4.8. *Soit Σ un semi-groupe commutatif d'épimorphismes de $\mathbb{T}_n$. Les assertions suivantes sont équivalentes.*

i) *Tout sous-ensemble Σ-minimal de $\mathbb{T}_n$ est composé d'éléments de torsion.*

ii) *Σ est hyperbolique et multi-paramétré.*

Théorème 4.9. *Soit Σ un semi-groupe commutatif d'endomorphismes de $\mathbb{T}_n$. Alors le seul sous-ensemble fermé infini Σ-invariant de $\mathbb{T}_n$ est $\mathbb{T}_n$ lui-même si et seulement si les conditions suivantes sont remplies.*

i) *Il existe $\sigma \in \Sigma$ tel que le polynôme caractéristique de σ^p soit irréductible sur $\mathbb{Z}$ pour tout entier p positif.*

ii) *Pour tout $v \in \mathrm{evec}\Sigma$, il existe $\lambda \in \mathrm{spec}_v\Sigma$ de module strictement supérieur à 1.*

iii) *Σ contient une paire d'endomorphismes rationnellement indépendants.*

Le Théorème 4.8 correspond à une partie de [Be84, Th 2.1], et le Théorème 4.9 correspond à [Be83, Th 2.1]. Pour établir l'implication ii) $\Rightarrow$ i) du Théorème 4.8 Berend s'appuya sur un lemme [Be84, Lemma 4.2] que nous utiliserons également plus tard et qui s'énonce comme suit.

Lemme 4.10. *Soient K un corps de nombres et S un sous-semi-groupe du groupe multiplicatif K^* de K. Supposons que pour tout $s \in S$ il existe un entier positif k tel que $\mathbb{Q}(s^k)$ soit un sous-corps strict de K. Alors il existe un entier positif N et un sous-corps strict F de K tels que $s^N \in F$ pour tout $s \in S$.*

4.3 Le lien

La Proposition 1.15 avec $X = 0$ montre que, si $\varepsilon \in E_K$, m est invariante sous l'action de la fonction $f_\varepsilon : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ définie par

$$f_\varepsilon(x) = \overline{\Phi}^{-1}(\Phi(\varepsilon) \cdot \overline{\Phi}(x)),$$

i.e. pour tout $x \in \mathbb{R}^n$, $m(f_\varepsilon(x)) = m(x)$.

Remarque 4.11. La fonction f_ε, dont la définition peut sembler alambiquée, n'est en fait que le prolongement continu à $\mathbb{R}^n$ de la fonction qui à $y \in \mathbb{Q}^n$ associe les coordonnées dans la base (e_i) de $\varepsilon \Sigma y_j e_j$.

Il est alors facile de voir que l'ensemble $\{f_\varepsilon;\ \varepsilon \in E_K\}$ est un groupe d'automorphismes de $\mathbb{R}^n$, isomorphe au groupe multiplicatif E_K. De plus, pour chaque ε, la Remarque 4.11 montre que la matrice de f_ε relativement à la base canonique a des coefficients entiers, de sorte que si $(x, X) \in \mathbb{R}^n \times \mathbb{Z}^n$, on a

$$f_\varepsilon(x + X) \equiv f_\varepsilon(x) \bmod \mathbb{Z}^n.$$

Par conséquent f_ε induit un endomorphisme de $\mathbb{T}_n$, noté g_ε et défini par

$$g_\varepsilon(\overline{x}) = \overline{f_\varepsilon(x)}.$$

Évidemment, puisque pour tout $x \in \mathbb{R}^n$ on a $m(f_\varepsilon(x)) = m(x)$, on peut écrire

$$\text{pour tout } \alpha \in \mathbb{T}_n,\ \tilde{m}(g_\varepsilon(\alpha)) = \tilde{m}(\alpha). \tag{4.1}$$

Posons maintenant

$$\Sigma = \Big\{g_\varepsilon;\ \varepsilon \in E_K\Big\}.$$

Il est facile de voir que $g_\varepsilon \circ g_{\varepsilon'} = g_{\varepsilon\varepsilon'}$ et qu'en fait, Σ est un groupe commutatif d'automorphismes de $\mathbb{T}_n$, isomorphe à E_K.
Intéressons-nous aux éléments propres du relèvement f_ε de g_ε dans $\mathbb{R}^n$. C'est pour cette raison que nous avons introduit $\overline{\Phi}'$ plus haut. À partir de maintenant on note v_i $(1 \leq i \leq n)$ les vecteurs de la base canonique de $\mathbb{R}^n$ (ou $\mathbb{C}^n$) définis par

$$(v_i)_j = \delta_{i,j},$$

où $\delta_{i,j}$ est le symbole de Kronecker, égal à 1 si $i = j$ et à 0 sinon, et on pose

$$w_i = \overline{\Phi}'^{-1}(v_i) \in \mathbb{C}^n.$$

Comme $\overline{\Phi}'$ est un automorphisme de $\mathbb{C}^n$, les w_i forment une base de $\mathbb{C}^n$. De plus, avec les notations introduites plus haut, on a la propriété suivante.

Proposition 4.12. *Si $u \in \mathrm{evec}\Sigma$, il existe $i \in \{1, \ldots, n\}$ tel que*

$$\mathrm{spec}_u \Sigma = \{\sigma_i(\varepsilon);\ \varepsilon \in E_K\}. \tag{4.2}$$

Preuve. Si on note encore f_ε l'endomorphisme de $\mathbb{C}^n$ dont la restriction à $\mathbb{R}^n$ est f_ε, on a

$$\forall z \in \mathbb{C}^n,\ f_\varepsilon(z) = \overline{\Phi}'^{-1}(\Phi(\varepsilon)\cdot \overline{\Phi}'(z)),$$

de telle sorte que pour tout $i \in \{1,\dots,n\}$,

$$f_\varepsilon(w_i) = \overline{\Phi}'^{-1}(\Phi(\varepsilon)\cdot v_i) = \overline{\Phi}'^{-1}(\sigma_i(\varepsilon)v_i) = \sigma_i(\varepsilon)w_i. \tag{4.3}$$

Ainsi w_i est un vecteur propre de f_ε, correspondant à la valeur propre $\sigma_i(\varepsilon)$, et l'on a

$$w_i \in \mathrm{evec}\Sigma.$$

Soit maintenant u un élément de $\mathrm{evec}\Sigma$. Puisque les w_i forment une base de $\mathbb{C}^n$ on peut écrire $u = \sum u_i w_i$ où pour tout i, $u_i \in \mathbb{C}$. Alors, par définition de $\mathrm{evec}\Sigma$, pour chaque $\varepsilon \in E_K$, u est un vecteur propre de f_ε et il existe $\lambda_\varepsilon \in \mathbb{C}$ qui vérifie $f_\varepsilon(u) = \lambda_\varepsilon u$, ou encore, par (4.3),

$$\sum_{i=1}^n u_i\sigma_i(\varepsilon)w_i = \sum_{i=1}^n \lambda_\varepsilon u_i w_i.$$

Mais $u \neq 0$ et il existe $i_0 \in \{1,\dots,n\}$ tel que $u_{i_0} \neq 0$. Comme les w_i sont indépendants, on doit avoir $u_{i_0}\sigma_{i_0}(\varepsilon) = u_{i_0}\lambda_\varepsilon$, si bien que

$$\lambda_\varepsilon = \sigma_{i_0}(\varepsilon).$$

Ceci mène à

$$\mathrm{spec}_u\Sigma = \{\lambda_\varepsilon;\ \varepsilon \in E_K\} = \{\sigma_{i_0}(\varepsilon);\ \varepsilon \in E_K\}.$$

D'où la conclusion. □

4.4 Minima euclidien et inhomogène

Nous pouvons maintenant donner le premier résultat important.

Théorème 4.13. *Soit K un corps de nombres de degré $n \geq 3$. Si le rang r du groupe des unités de K est strictement supérieur à 1, il existe $\xi \in K$ tel que*

$$M(\overline{K}) = m_{\overline{K}}(\xi) = m_K(\xi).$$

Preuve. Tout d'abord puisqu'il s'agit d'un groupe d'automorphismes, Σ est un semi-groupe d'épimorphismes de $\mathbb{T}_n$. Nous pouvons vérifier facilement qu'il est hyperbolique et multi-paramétré.

Le caractère hyperbolique de Σ est une conséquence de la Proposition 4.12. En effet, si Σ n'était pas hyperbolique, il existerait par (4.2), un indice $i \in \{1,\dots,n\}$ tel que

$$|\sigma_i(\varepsilon)| = 1, \text{ pour tout } \varepsilon \in E_K. \tag{4.4}$$

Si $i > r_1 + r_2$ la propriété est encore vraie pour $i - r_2$ à la place de i, par conjugaison, et on peut supposer $i \leq r_1 + r_2$, si bien que par (4.4), $\mathcal{L}(E_K)$ est inclus dans l'hyperplan d'équation $x_i = 0$ où $i \leq r_1 + r_2$. Mais il est également inclus dans l'hyperplan d'équation $\sum_{1 \leq j \leq r_1} x_j + 2 \sum_{r_1+1 \leq j \leq r_1+r_2} x_j = 0$, qui est distinct du précédent, car $r \geq 1$. Ainsi, on obtient une contradiction au théorème de Dirichlet, par lequel $\mathcal{L}(E_K)$ est un réseau de rang $r = r_1 + r_2 - 1$.

Le caractère multi-paramétré de Σ est aussi une conséquence de la Proposition 4.12. Comme $r \geq 2$ il y a au moins deux unités indépendantes, par exemple ε_1 et ε_2. Alors, $i \in \{1, \ldots, n\}$ étant donné, si $\sigma_i(\varepsilon_1)^l = \sigma_i(\varepsilon_2)^m$ avec l et m entiers, l'injectivité de σ_i donne $\varepsilon_1^l \varepsilon_2^{-m} = 1$ ce qui conduit à $l = m = 0$. Ainsi par la Proposition 4.12, pour tout $u \in \mathrm{evec}\Sigma$, $\mathrm{spec}_u \Sigma$ contient au moins deux valeurs propres rationnellement indépendantes.

On peut donc appliquer le Théorème 4.8.
Considérons à cet effet l'ensemble S défini par

$$S = \{\alpha \in \mathbb{T}_n \text{ tels que } \tilde{m}(\alpha) = M(\overline{K})\}.$$

Rappelons que $\tilde{m}$ est semi-continue supérieurement et atteint donc sa borne supérieure sur le compact $\mathbb{T}_n$. En particulier S est non vide. De plus, par semi-continuité supérieure de $\tilde{m}$, S est un fermé de $\mathbb{T}_n$. En effet, il est facile de voir que si (α_p) est une suite de S, qui converge vers $\alpha \in \mathbb{T}_n$, on a

$$M(\overline{K}) = \limsup_{p \to +\infty} \tilde{m}(\alpha_p) \leq \tilde{m}(\alpha)$$

par semi-continuité, d'où $\alpha \in S$, par les définitions de $M(\overline{K})$ et S.

Maintenant, si $\alpha \in S$, on sait par (4.1) que pour tout $\varepsilon \in E_K$, $\tilde{m}(g_\varepsilon(\alpha)) = \tilde{m}(\alpha)$, et par conséquent que $g_\varepsilon(\alpha) \in S$. Ceci montre que S est Σ-invariant.

Soit S' un sous-ensemble Σ-minimal de S. Par le Théorème 4.8, S' est composé d'éléments de torsion, i.e. d'éléments α de $\mathbb{T}_n$ pour lesquels il existe $k_\alpha \in \mathbb{Z} \backslash \{0\}$ tel que $k_\alpha \alpha = 0$ (dans $\mathbb{T}_n$). Un tel élément se relève nécessairement dans $\mathbb{Q}^n$, et si X/k_α où $X \in \mathbb{Z}^n$ est l'un de ses relèvements, $\xi = 1/k_\alpha \sum X_i e_i$ convient. □

Comme on sait que si $r \leq 1$, $M(K) = M(\overline{K})$ (Théorème 1.30) on a la conséquence fondamentale suivante.

Corollaire 4.14. *Pour tout corps de nombres K on a*

$$M(K) = M(\overline{K}).$$

De plus, si le rang r du groupe des unités de K est strictement plus grand que 1, alors

$$M(K) = M(\overline{K}) \in \mathbb{Q}.$$

Preuve. Comme nous l'avons vu plus haut, c'est une conséquence immédiate de la Proposition 1.10 iii). □

4.5 Décidabilité de l'euclidianité

Des définitions de $M(K)$ et de l'euclidianité pour la norme, la Proposition 1.23, le Théorème 4.13 et le Corollaire 4.14 donnent partiellement la réponse à l'une des questions que nous nous étions initialement posées.

Corollaire 4.15. *Soit K un corps de nombres dont le rang r du groupe des unités est strictement supérieur à 1. Si $M(K) = 1$, alors K n'est pas euclidien pour la norme.*

Posons maintenant

$$\mathcal{A} = \{z \in H \text{ tels que } \mathcal{N}(z) = \prod_{i=1}^{n} |z_i| < 1\}.$$

Il est évident que si $\Phi(\mathbb{Z}_K) + \mathcal{A} = H$ alors K est euclidien pour la norme. Lenstra a conjecturé qu'en fait, il y a équivalence [Len80a]. Grâce au Théorème 4.13, on peut montrer que c'est effectivement vrai dès que $r > 1$.

Théorème 4.16. *Soit K un corps de nombres dont le rang r du groupe des unités est strictement supérieur à 1. On a*

$$K \textit{ est euclidien pour la norme } \iff \Phi(\mathbb{Z}_K) + \mathcal{A} = H.$$

Preuve. Si K est euclidien pour la norme, par les Corollaires 4.14 et 4.15, on a, sous l'hypothèse $r > 1$,

$$M(K) = M(\overline{K}) = M < 1.$$

Soit $z \in H$. On a $m_{\overline{K}}(z) \leq M < 1$ et, par définition de $m_{\overline{K}}(z)$, il existe $Z \in \Phi(\mathbb{Z}_K)$ tel que

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

Ceci implique $z \in \Phi(\mathbb{Z}_K) + \mathcal{A}$, d'où l'égalité $\Phi(\mathbb{Z}_K) + \mathcal{A} = H$. □

Remarque 4.17. En fait, en modifiant légèrement la preuve précédente, on peut voir qu'on a le résultat plus précis suivant. Si

$$\mathcal{A}_k = \{z \in H \text{ tels que } \mathcal{N}(z) \leq k\},$$

alors on peut écrire

$$K \text{ est euclidien pour la norme } \iff \exists\, k \in]\,0, 1\,[\text{ tel que } \Phi(\mathbb{Z}_K) + \mathcal{A}_k = H.$$

Donnons enfin un autre corollaire du Théorème 4.13, déjà mentionné par Lenstra [Len80a].

Corollaire 4.18. *Soit K un corps de nombres dont le rang r du groupe des unités est strictement supérieur à 1. La question de l'euclidianité de K pour la norme est décidable.*

Preuve. Suivons l'argumentation de Lenstra. On prend un domaine fondamental de $\mathbb{Z}_K$, $\mathcal{F} \subseteq H$ et on note comme plus haut

$$\mathcal{A} = \{z \in H \text{ tels que } \mathcal{N}(z) < 1\}.$$

On numérote les éléments non nuls de $\mathbb{Z}_K$ sous la forme $\beta_1, \beta_2, \ldots$ On note $X_1 = \Phi(\beta_1)$, $X_2 = \Phi(\beta_2), \ldots$ On vérifie alors successivement pour $n = 1, 2, 3\ldots$ les conditions suivantes.

I_n : Il existe un $\alpha \in \mathbb{Z}_K$ tel que $\alpha \not\equiv \rho \bmod \beta_n$ pour tout $\rho \in \mathbb{Z}_K$ vérifiant

$$|N_{K/\mathbb{Q}}(\rho)| < |N_{K/\mathbb{Q}}(\beta_n)|.$$

J_n : Le domaine fondamental $\mathcal{F}$ est recouvert par les $n+1$ translatés

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

Si l'une des deux conditions est satisfaite, on s'arrête. Si I_n est vérifiée, alors K n'est pas euclidien pour la norme. Si J_n est vérifiée, alors K est euclidien pour la norme. Supposons que cette procédure de décision ne termine pas. Alors I_n et J_n sont fausses pour tout n. Ceci implique que K est euclidien pour la norme. En effet on aurait alors

$$\text{pour tout } \alpha \in \mathbb{Z}_K \text{ et tout } \beta_n, \text{ il existe } \rho \equiv \alpha \bmod \beta_n \text{ et } |N_{K/\mathbb{Q}}(\rho)| < |N_{K/\mathbb{Q}}(\beta_n)|,$$

ce qui est exactement la définition (1) de l'euclidianité pour la norme. Mais ceci implique aussi que

$$\Phi(\mathbb{Z}_K) + \mathcal{A} \subsetneq H,$$

ce qui contredit le Théorème 4.16. □

Remarque 4.19. Ce résultat très formel ne revêt aucun caractère d'effectivité. En outre, si la vérification de I_n ne pose pas de problème (il n'y a qu'un nombre fini de vérifications à faire), l'élaboration d'un algorithme efficace permettant de vérifier J_n est un problème en soi, même si c'est possible en théorie.

4.6 Spectres euclidien et inhomogène

Nous pouvons chercher à être plus précis en étudiant $\mathrm{sp}(\overline{K})$ et $\mathrm{sp}(K)$.

4.6.1 Le cas non CM

Il est remarquable que, contrairement à ce qui se passe lorsque $n = 2$, les spectres inhomogène et euclidien soient égaux et inclus dans $\mathbb{Q}$, dès lors que $r > 1$ et que K n'est pas un corps CM (extension quadratique totalement complexe d'un corps de nombres totalement réel). Mais avant d'énoncer le résultat principal, commençons par un résultat préliminaire. La preuve du Théorème 4.22 s'appuie sur le lemme suivant.

Lemme 4.20. *Soit K un corps de nombres non CM. Il existe une unité $\varepsilon \in E_K$ telle que pour tout entier positif p on ait $\mathbb{Q}(\varepsilon^p) = K$.*

Preuve. Supposons que le résultat soit faux et que pour tout $\varepsilon \in E_K$, il existe un $p_\varepsilon > 0$ tel que $\mathbb{Q}(\varepsilon^{p_\varepsilon})$ soit un sous-corps strict de K. Alors, E_K étant un sous-semi-groupe du groupe multiplicatif K^* de K, on sait par le Lemme 4.10 qu'il existe un entier positif N et un sous-corps strict F de K tel que

$$\text{pour tout } \varepsilon \in E_K,\ \varepsilon^N \in F.$$

Posons $n' = [F : \mathbb{Q}]$. Comme F est un sous-corps strict de K, n' est un diviseur propre de n et on a

$$2n' \leq n. \tag{4.5}$$

Notons (r_1', r_2') la signature de F. Soit $(\varepsilon_1, ..., \varepsilon_r)$ notre système d'unités fondamentales de K. Comme ε_1,..., ε_r sont indépendantes et comme $N > 0$, $\varepsilon_1^N, \dots, \varepsilon_r^N$ sont r unités indépendantes de F, de telle sorte que $r \leq r'$ où $r' = r_1' + r_2' - 1$ est le rang du groupe des unités de F, i.e. le nombre maximal d'unités indépendantes de F. Ainsi

$$r_1 + r_2 \leq r_1' + r_2',$$

ce qui implique

$$n - r_2 \leq n' - r_2'. \tag{4.6}$$

De (4.5) et (4.6), on tire

$$r_2 \geq r_2 - r_2' \geq n - n' \geq n/2.$$

Mais $n = r_1 + 2r_2$ si bien que la seule possibilité est $(r_1, r_2) = (0, n/2)$, qui conduit à

$$r_2' = 0,\ n' = n/2 \text{ et } r_1' = n/2.$$

Ceci prouve que K est une extension totalement complexe du corps totalement réel F, ce qui est exclu par hypothèse. □

Remarque 4.21. Notons que la réciproque est exacte. En effet, soit K un corps de nombres CM et soit w_K le nombre de racines de l'unité de K. Soit ε une unité quelconque de K. Alors, comme la conjugaison complexe commute avec tous les $\mathbb{Q}$-isomorphismes de K dans $\mathbb{C}$, $\eta = \varepsilon/\overline{\varepsilon}$ est un élément de $\mathbb{Z}_K$ qui a tous ses conjugués de module 1. On en déduit que η est une racine de l'unité de K (voir [Wa82, Lemme 1.6]) donc une racine w_K-ième de 1. Comme $\nu = \varepsilon\overline{\varepsilon}$ est une unité du sous-corps réel maximal K^+ de K, on a $\varepsilon^{2w_K} = \eta^{w_K}\nu^{w_K} = \nu^{w_K} \in K^+$ et $\mathbb{Q}(\varepsilon^{2w_K}) \subsetneq K$.

On peut maintenant énoncer le résultat suivant.

Théorème 4.22. *Soit K un corps de nombres de degré $n \geq 3$. Supposons que le rang r du groupe des unités de K soit strictement supérieur à 1 et que K ne soit pas un corps CM. Ce sera le cas en particulier si K est totalement réel. Alors il existe une suite (s_p) d'éléments de $\mathbb{Q}$, strictement décroissante, vérifiant*

i) $\lim\limits_{p \to +\infty} s_p = 0$.

ii) $m_{\overline{K}}(H) = m(\mathbb{R}^n) = \tilde{m}(\mathbb{T}_n) = \{s_p;\ p \geq 1\} \cup \{0\}$.

iii) *Pour chaque $p \geq 1$ l'ensemble des $\alpha \in \mathbb{T}_n$ tels que $\tilde{m}(\alpha) = s_p$ est fini et se relève en des points de $\mathbb{Q}^n$.*

Ceci implique en particulier que si $x \notin \Phi(K)$, alors $m_{\overline{K}}(x) = 0$.

Preuve. Soit k un réel positif quelconque vérifiant

$$0 < k \leq M(\overline{K}).$$

Notons

$$S_k = \{\alpha \in \mathbb{T}_n \text{ tels que } \tilde{m}(\alpha) \geq k\}.$$

S_k est un sous-ensemble strict fermé de $\mathbb{T}_n$. En effet, S_k est strict parce que sinon on aurait $m(z) \geq k > 0$ pour tout $z \in \mathbb{R}^n$, i.e. $m_{\overline{K}}(x) \geq k > 0$ pour tout $x \in H$, ce qui est évidemment impossible. D'autre part, $\tilde{m}$ étant semi-continue supérieurement, toute limite $\alpha \in \mathbb{T}_n$ d'une suite $(\alpha_p)_{p \geq 0}$ d'éléments de S_k vérifie

$$\tilde{m}(\alpha) \geq \limsup_{p \to +\infty} \tilde{m}(\alpha_p) \geq k,$$

et S_k est fermé.

De plus, comme dans la preuve du Théorème 4.13 avec S, S_k est Σ-invariant par (4.1). On en déduit que, si les hypothèses du Théorème 4.9 sont vérifiées, S_k est fini.

Mais la condition i) est une conséquence du Lemme 4.20. En effet une unité $\varepsilon \in E_K$ étant donnée, comme f_ε^p a les $\sigma_i(\varepsilon)^p = \sigma_i(\varepsilon^p)$ pour valeurs propres associées aux vecteurs propres w_i, le polynôme caractéristique de g_ε^p est $\prod_{i=1}^n (X - \sigma_i(\varepsilon^p))$, qui est le polynôme caractéristique de ε^p, irréductible sur $\mathbb{Z}$ si $[\mathbb{Q}(\varepsilon^p) : \mathbb{Q}] = n$.

D'autre part on peut déduire la condition ii) de l'existence, i étant donné, d'une unité $\varepsilon \in E_K$ vérifiant $|\sigma_i(\varepsilon)| > 1$. Il suffit de prendre ε telle que $\sigma_i(\varepsilon) \notin \mathbb{C}_1$ comme dans la preuve du Théorème 4.13, et si $|\sigma_i(\varepsilon)| < 1$, on considère $1/\varepsilon$.

Enfin, comme $r > 1$, la condition iii) est donnée par l'existence de deux unités indépendantes, par exemple ε_1 et ε_2. Si $g_{\varepsilon_1}^l = g_{\varepsilon_2}^m$, avec l et m entiers, alors en particulier, pour tout $\xi \in K$, $\varepsilon_1^l \xi \equiv \varepsilon_2^m \xi \bmod \mathbb{Z}_K$ qui mène à $(\varepsilon_1^l \varepsilon_2^{-m} - 1)\xi \in \mathbb{Z}_K$. Mais ceci n'est possible que lorsque $\varepsilon_1^l \varepsilon_2^{-m} - 1 = 0$, ce qui implique $l = m = 0$.

Le Théorème 4.9 peut donc être appliqué et S_k est fini.

Soit alors $x \in \mathbb{R}^n$ tel que $\alpha = \overline{x} \in S_k$. Comme pour toute unité de non-torsion ε (ici $r \geq 1$), on a $g_\varepsilon(S_k) \subseteq S_k$, il existe des entiers positifs distincts $l > p > 0$ tels que $g_\varepsilon^l(\alpha) = g_\varepsilon^p(\alpha)$ ce qui donne

$$\Phi(\varepsilon^{l-p}) \cdot \overline{\Phi}(x) \equiv \overline{\Phi}(x) \bmod \ \Phi(\mathbb{Z}_K).$$

Ceci implique que $\overline{\Phi}(x) \in \Phi(K) = \overline{\Phi}(\mathbb{Q}^n)$ et donc que $x \in \mathbb{Q}^n$.

Ainsi, S_k est un sous-ensemble fini de $\mathbb{T}_n$ dont les relèvements sont dans $\mathbb{Q}^n$ et nécessairement $\tilde{m}(S_k) = \tilde{m}(\mathbb{T}_n) \cap [k, M(\overline{K})]$ est un sous-ensemble fini de $\mathbb{Q}$ par la Proposition 1.15.

Posons $s_1 = M(\overline{K}) > 0$, et pour $p \geq 1$, si $s_p > 0$,

$$s_{p+1} = \sup \tilde{m}(\mathbb{T}_n \backslash S_{s_p}),$$

qui est bien défini puisque $S_{s_p} \subsetneq \mathbb{T}_n$.

L'entier p étant donné, si s_p est défini et si $s_p > 0$, comme S_{s_p} est fini et l'ensemble des $\overline{\Psi^{-1}(1/q)}$ $(q \geq 2)$ infini, on voit qu'il existe $q \in \mathbb{N}$, $q \geq 2$, tel que $\overline{\Psi^{-1}(1/q)} \in \mathbb{T}_n \backslash S_{s_p}$, de telle sorte que

$$s_{p+1} \geq \tilde{m}\left(\overline{\Psi^{-1}(1/q)}\right) = m_K(1/q) = 1/q^n > 0.$$

Ainsi, par récurrence, pour tout p, s_p est défini et $s_p > 0$.

Par construction (s_p) est décroissante. Supposons que pour un p donné, on ait $s_{p+1} = s_p$. Alors,

$$\sup \tilde{m}(\mathbb{T}_n \backslash S_{s_p}) = s_p,$$

ce qui signifie qu'il y a des éléments $\alpha \in \mathbb{T}_n$ vérifiant $\tilde{m}(\alpha) < s_p$ aussi près que l'on veut de s_p. Mais ceci est en contradiction par exemple avec le fait que $S_{s_p/2}$ est fini. La suite (s_p) est donc strictement décroissante.

Le même argument ($S_{s_p/2}$ est fini) montre que pour tout p, s_p appartient à $\tilde{m}(\mathbb{T}_n)$.

La suite décroissante (s_p) converge vers un réel $L \geq 0$. Supposons que l'on ait $L > 0$. Comme $S_{L/2}$ est fini, l'ensemble des s_p, qui est un sous-ensemble de $\tilde{m}(\mathbb{T}_n)$ dont tous les éléments sont supérieurs à $L/2$, serait fini. On obtient une contradiction avec le fait que (s_p) est strictement décroissante, et nécessairement $L = 0$. On a bien la propriété i).

L'inclusion $\{s_p;\ p \geq 1\} \cup \{0\} \subseteq \tilde{m}(\mathbb{T}_n)$ est évidente. Supposons qu'il s'agisse d'une inclusion stricte. Alors il existerait un $\alpha \in \mathbb{T}_n$ vérifiant $s_{p+1} < \tilde{m}(\alpha) < s_p$ pour un p donné, ce qui contredit la définition de s_{p+1}. On a donc ii).

La propriété iii) vient du fait que

$$\{\alpha \in \mathbb{T}_n \text{ tels que } \tilde{m}(\alpha) = s_p\} = S_{s_p} \backslash S_{s_{p+1}},$$

de telle sorte que cet ensemble est fini et a ses relèvements dans $\mathbb{Q}^n$, par la propriété générale des S_k précédemment vue. Ceci implique que, pour tout p, s_p est rationnel. □

Ce théorème affirme donc, entre autres choses, que les spectres inhomogène et euclidien de K sont confondus. On peut le traduire en termes de $M_p(K)$ et de $M_p(\overline{K})$.

Corollaire 4.23. *Sous les hypothèses du Théorème 4.22, et si on pose $M_1(K) = M(K)$ et $M_1(\overline{K}) = M(\overline{K})$, alors,*

- *$M(\overline{K}) = M(K)$ est atteint.*
- *Pour tout $p \geq 1$, $M_p(K) = M_p(\overline{K}) \in \mathbb{Q}$.*

- *Pour tout* $p \geq 1$, $M_{p+1}(\overline{K}) < M_p(\overline{K})$.
- $M(\overline{K})$ *est donc isolé.*
- $\lim_{p \to +\infty} M_p(\overline{K}) = 0$.

Preuve. On sait que l'ensemble des $\alpha \in \mathbb{T}_n$ vérifiant $\tilde{m}(\alpha) = M(\overline{K})$ est fini et se relève dans $\mathbb{Q}^n$. La Proposition 1.10 ii) donne alors le premier résultat. Le reste est une conséquence directe du Théorème 4.22, puisque, par les définitions, il est clair que $M_p(K) = M_p(\overline{K}) = s_p$. □

Remarque 4.24. Ces résultats montrent que le recours au Corollaire 3.5 ne se justifie plus, du point de vue algorithmique, lorsqu'on étudie un corps de nombres totalement réel de degré $n \geq 3$.

Nous avons dit dans la Remarque 3.20 qu'à l'issue des calculs effectués dans l'algorithme, l'obtention d'un graphe convenable n'était pas a priori garantie. Les considérations qui précèdent permettent toutefois d'énoncer le résultat suivant.

Proposition 4.25. *Soit K un corps de nombres non CM vérifiant $r > 1$. Alors l'algorithme décrit au chapitre* 3 *termine au sens où pour un découpage assez fin et une famille d'entiers $\mathcal{X}$ assez grande, on obtiendra un graphe convenable.*

Preuve. Le Théorème 4.22 montre que les points t de $\mathcal{F}$ vérifiant $m_{\overline{K}}(t) = M(K)$ sont en nombre fini. Notons-les t_i. Si on fixe une unité d'ordre infini ε, il est facile de voir qu'ils s'envoient les uns sur les autres sous l'action de ε, suivant des cycles disjoints. Supposons que nous définissions des voisinages ouverts $V(t_i)$ de ces points, suffisamment petits pour que pour tout i, $\Phi(\varepsilon) \cdot V(t_i)$ n'intersecte qu'un $V(t_j)$ modulo $\Phi(\mathbb{Z}_K)$, précisément celui qui contient $\Phi(\varepsilon) \cdot t_i$ modulo $\Phi(\mathbb{Z}_K)$. Ceci est toujours possible, car les t_i sont isolés. Alors, par isolation de $M(K)$, il existe $M' < M(K)$ tel que pour tout $t \in \overline{\mathcal{F}} \setminus \cup V(t_i)$, on ait $m_{\overline{K}}(t) < M'$. On peut donc recouvrir $\overline{\mathcal{F}} \setminus \cup V(t_i)$ par les régions ouvertes (hyperboliques dans le cas totalement réel) $\mathcal{R}_X = \{x \in H;\ \mathcal{N}(x - X) < M'\}$, où X décrit $\Phi(\mathbb{Z}_K)$. Comme $\overline{\mathcal{F}} \setminus \cup V(t_i)$ est compact, on peut extraire de ce recouvrement un recouvrement fini, et on a la situation suivante : $\mathcal{F}$ est recouvert par un nombre fini de $\mathcal{R}_X$, à l'exception de voisinages des points critiques qui sont suffisamment petits pour que le graphe obtenu en termes de voisinages (donc en termes de parallélotopes) soit une réunion de cycles disjoints, et en particulier soit un graphe convenable. Cela signifie que pour un découpage assez fin, une famille d'entiers assez grande, et un « rayon » suffisamment proche de $M(K)$, on obtiendra nécessairement un graphe convenable. □

4.6.2 Le cas CM

Il est intéressant de voir que les choses ne se passent pas de la même manière lorsque K est un corps CM, même si $r > 1$. Supposons que K soit une extension quadratique totalement complexe du corps totalement réel K^+, de degré n. Notons σ_i (avec $\sigma_{i+n/2} = \overline{\sigma_i}$), les n $\mathbb{Q}$-isomorphismes de K dans $\mathbb{C}$, et τ_i les $n/2$ $\mathbb{Q}$-isomorphismes de K^+ dans $\mathbb{R}$. On sait que la conjugaison complexe τ induit un automorphisme de K et commute avec tout σ_i, que K/K^+ est galoisienne et que $\mathrm{Gal}(K/K^+) = \{\mathrm{id}, \tau\}$. Soient $z \in K$ et $Z \in \mathbb{Z}_K$. Alors $\mathrm{Tr}_{K/K^+}(z) = z + \overline{z} \in K^+$ et $Z + \overline{Z} \in \mathbb{Z}_{K^+}$. De plus

$$N_{K/\mathbb{Q}}(z - Z) = \prod_{i=1}^{n/2} \sigma_i(z - Z)\overline{\sigma_i(z - Z)}.$$

Mais si $u \in \mathbb{C}$ on peut écrire

$$u\overline{u} \geq \frac{1}{4}(u + \overline{u})^2,$$

de telle sorte que l'on obtient

$$\begin{aligned}
\left|N_{K/\mathbb{Q}}(z - Z)\right| &\geq \frac{1}{4^{n/2}} \prod_{i=1}^{n/2} \Big(\sigma_i(z - Z) + \overline{\sigma_i(z - Z)}\Big)^2 \\
&\geq \frac{1}{2^n} \prod_{i=1}^{n/2} \Big(\sigma_i(z + \overline{z}) - \sigma_i(Z + \overline{Z})\Big)^2 \\
&\geq \frac{1}{2^n} \inf_{Z' \in \mathbb{Z}_{K^+}} \prod_{i=1}^{n/2} \Big(\sigma_i(z + \overline{z}) - \sigma_i(Z')\Big)^2 \\
&\geq \frac{1}{2^n} \left(\inf_{Z' \in \mathbb{Z}_{K^+}} \prod_{i=1}^{n/2} \Big|\tau_i(z + \overline{z}) - \tau_i(Z')\Big| \right)^2 \\
&\geq \frac{1}{2^n} \left(\inf_{Z' \in \mathbb{Z}_{K^+}} \Big|N_{K^+/\mathbb{Q}}\Big((z + \overline{z}) - Z'\Big)\Big| \right)^2 \\
&\geq \frac{1}{2^n} \Big(m_{K^+}(z + \overline{z})\Big)^2.
\end{aligned}$$

Ceci implique

$$m_K(z) \geq \frac{1}{2^n} \Big(m_{K^+}(z + \overline{z})\Big)^2,$$

si bien que, $y \in K^+ \backslash \mathbb{Z}_{K^+}$ étant donné, si on pose $\lambda = m_{K^+}(y) > 0$, alors, pour tout $z \in K$ vérifiant $z + \overline{z} = y$, on a

$$m_K(z) \geq \frac{1}{2^n}\lambda^2 > 0.$$

Mais il y a une infinité de tels $z \in K$ modulo $\mathbb{Z}_K$, et, par semi-continuité supérieure, il y a une infinité non dénombrable de $x \in \mathbb{R}^n$ modulo $\mathbb{Z}^n$ tels que

$$m(x) \geq \frac{1}{2^n}\lambda^2.$$

Ainsi, la situation est complétement différente de celle décrite par le Théorème 4.22, et sous l'hypothèse $r > 1$, on a l'équivalence

$$\forall k > 0,\ S_k = \{\alpha \in \mathbb{T}_n;\ \tilde{m}(\alpha) \geq k\} \text{ est fini } \iff K \text{ n'est pas un corps CM.}$$

Ceci étant, on peut se demander si, malgré tout, on ne peut pas affirmer par exemple que $M(\overline{K})$ est isolé et atteint. À l'heure où nous écrivons ce document, nous n'avons pas complétement élucidé la question, mais pouvons néanmoins donner un résultat qui permet de répondre dans certains cas.

Le corps de nombres K étant CM, on sait qu'il existe un élément D de $\mathbb{Z}_{K^+}$ totalement positif, c'est-à-dire vérifiant $\tau_i(D) > 0$ pour tout i de $\{1, \ldots, n/2\}$, et tel que

$$K = K^+(\sqrt{-D}).$$

On a alors

$$\begin{aligned} H &= \{(z, \overline{z});\ z \in \mathbb{C}^{n/2}\} \\ &= \{(x + \Omega.y, x - \Omega.y);\ (x, y) \in \mathbb{R}^{n/2}\}, \end{aligned}$$

où

$$\Omega = \Big(\sqrt{-\tau_1(D)}, \ldots, \sqrt{-\tau_{n/2}(D)}\Big) \in \mathbb{C}^{n/2}.$$

Si $(\xi, \nu) \in K^+$ et $z = \xi + \nu\sqrt{-D} \in K$ on a, avec les notations précédentes,

$$\Phi(z) = \Big(\Phi'(\xi) + \Omega.\Phi'(\nu), \Phi'(\xi) - \Omega.\Phi'(\nu)\Big),$$

où Φ' désigne le plongement de K^+ dans $\mathbb{R}^{n/2}$. En outre, l'inclusion

$$\mathbb{Z}_{K^+} + \sqrt{-D}\,\mathbb{Z}_{K^+} \subseteq \mathbb{Z}_K$$

se traduit par

$$\Big\{(z, \overline{z});\ z \in \Phi'(\mathbb{Z}_{K^+}) + \Omega \cdot \Phi'(\mathbb{Z}_{K^+})\Big\} \subseteq \Phi(\mathbb{Z}_K).$$

On a alors la proposition suivante.

Proposition 4.26. *Soit K un corps de nombres CM de degré n, dont le groupe des unités est de rang $r > 1$ ce qui équivaut à $n > 4$. Supposons que les deux conditions suivantes soient remplies.*

i) *Il existe $x \in \mathbb{R}^{n/2}$ tel que pour tout $y \in \mathbb{R}^{n/2}$ on ait $m_{\overline{K}}(x + \Omega \cdot y, x - \Omega \cdot y) < M(\overline{K})$.*

ii) *Il existe $y \in \mathbb{R}^{n/2}$ tel que pour tout $x \in \mathbb{R}^{n/2}$ on ait $m_{\overline{K}}(x + \Omega \cdot y, x - \Omega \cdot y) < M(\overline{K})$.*

Alors, il existe un réel positif k strictement inférieur à $M(K)$, tel que l'ensemble des $z \in H$ vérifiant $m_{\overline{K}}(z) \geq k$ soit non vide, fini modulo $\Phi(\mathbb{Z}_K)$, et constitué de points rationnels. En particulier, $M(\overline{K})$ est isolé et atteint.

Preuve. Fixons un réel positif k vérifiant $k < M(\overline{K})$ et posons

$$\mathcal{S}_k = \big\{x \in \mathbb{R}^{n/2} \text{ tels qu'il existe } y \in \mathbb{R}^{n/2} \text{ vérifiant } m_{\overline{K}}(x + \Omega \cdot y, x - \Omega \cdot y) \geq k\big\}.$$

Comme $k < M(\overline{K})$, $\mathcal{S}_k$ est non vide.

De plus $\mathcal{S}_k$ est une partie fermée de $\mathbb{R}^{n/2}$. En effet, considérons une suite $(x_p)_{p\geq 0}$ d'éléments de $\mathcal{S}_k$ convergeant vers un élément $x \in \mathbb{R}^{n/2}$.

Pour tout p il existe un $y_p \in \mathbb{R}^{n/2}$ tel que

$$m_{\overline{K}}(x_p + \Omega.y_p, x_p - \Omega.y_p) \geq k.$$

Comme quel que soit $Y \in \Phi'(\mathbb{Z}_{K^+})$,

$$(\Omega \cdot Y, -\Omega \cdot Y) \in \Phi(\mathbb{Z}_K),$$

et comme $m_{\overline{K}}$ est invariante par translation suivant les vecteurs de $\Phi(\mathbb{Z}_K)$, on a

$$m_{\overline{K}}\big(x_p + \Omega \cdot (y_p + Y), x_p - \Omega \cdot (y_p + Y)\big) = m_{\overline{K}}\big(x_p + \Omega \cdot y_p, x_p - \Omega \cdot y_p\big).$$

On peut donc imposer à la suite (y_p) d'être bornée, en prenant par exemple $y_p \in \mathcal{F}'$, où $\mathcal{F}'$ est un domaine fondamental de $\mathbb{Z}_{K^+}$. Il s'ensuit que l'on peut extraire de (y_p) une sous-suite $(y_{\varphi(p)})$ convergeant vers un élément y de $\overline{\mathcal{F}'}$.

La semi-continuité supérieure de $m_{\overline{K}}$ donne alors

$$m_{\overline{K}}(x + \Omega \cdot y, x - \Omega \cdot y) \geq \limsup_{p\to+\infty} m_{\overline{K}}(x_{\varphi(p)} + \Omega \cdot y_{\varphi(p)}, x_{\varphi(p)} - \Omega \cdot y_{\varphi(p)}) \geq k.$$

Ainsi $x \in \mathcal{S}_k$, et la partie $\mathcal{S}_k$ de $\mathbb{R}^{n/2}$ est fermée.

Par ailleurs $\mathcal{S}_k$ est E_{K^+}-stable au sens où si $\varepsilon \in E_{K^+}$, alors

$$x \in \mathcal{S}_k \Rightarrow \Phi'(\varepsilon) \cdot x \in \mathcal{S}_k.$$

En effet, $\varepsilon \in E_K$ et $m_{\overline{K}}$ est invariante sous l'action de la multiplication par

$$\Phi(\varepsilon) = (\Phi'(\varepsilon), \Phi'(\varepsilon)).$$

On en déduit que pour tout x et tout y de $\mathbb{R}^{n/2}$,

$$m_{\overline{K}}(x + \Omega \cdot y, x - \Omega \cdot y) = m_{\overline{K}}(\Phi'(\varepsilon) \cdot x + \Omega \cdot \Phi'(\varepsilon) \cdot y, \Phi'(\varepsilon) \cdot x - \Omega \cdot \Phi'(\varepsilon) \cdot y).$$

Soient alors $x \in \mathcal{S}_k$ et $y \in \mathbb{R}^{n/2}$ tels que

$$m_{\overline{K}}(x + \Omega \cdot y, x - \Omega \cdot y) \geq k.$$

En posant $y' = \Phi'(\varepsilon) \cdot y$ et $x' = \Phi'(\varepsilon) \cdot x$, on a bien

$$m_{\overline{K}}(x' + \Omega \cdot y', x' - \Omega \cdot y') \geq k,$$

c'est-à-dire

$$x' \in \mathcal{S}_k.$$

Or, comme pour tout $Y \in \Phi'(\mathbb{Z}_{K^+})$, on a $(Y, Y) \in \Phi(\mathbb{Z}_K)$, et comme $m_{\overline{K}}$ est invariante par translation suivant les vecteurs de $\Phi(\mathbb{Z}_K)$, on a en particulier

$$x \in \mathcal{S}_k \Rightarrow x + Y \in \mathcal{S}_k, \text{ pour tout } Y \in \Phi'(\mathbb{Z}_{K^+}).$$

Ceci prouve que l'on peut considérer les classes des éléments de $\mathcal{S}_k$ modulo $\Phi'(\mathbb{Z}_{K^+})$ et raisonner dans $\mathbb{R}^{n/2}/\Phi'(\mathbb{Z}_{K^+})$ qui est isomorphe au tore $\mathbb{T}_{n/2}$. Les classes en question constituent alors un fermé non vide E_{K^+}-stable de $\mathbb{R}^{n/2}/\Phi'(\mathbb{Z}_{K^+})$, et l'on peut comme plus haut se ramener au tore $\mathbb{T}_{n/2}$. Nous n'entrerons pas ici dans le détail, mais on peut de nouveau appliquer le Théorème 4.9. La conséquence en est que l'ensemble des classes considérées est soit fini et constitué de classes de points rationnels (correspondant aux éléments de torsion de $\mathbb{T}_{n/2}$), soit égal à $\mathbb{R}^{n/2}/\Phi'(\mathbb{Z}_{K^+})$, d'où l'on déduit

$$\mathcal{S}_k = \mathbb{R}^{n/2}, \text{ ou } \mathcal{S}_k \subseteq \Phi'(K^+) \text{ et est fini modulo } \Phi'(\mathbb{Z}_{K^+}). \tag{4.7}$$

Supposons alors que pour tout $k < M(\overline{K})$, on ait $\mathcal{S}_k = \mathbb{R}^{n/2}$. Dans ces conditions, pour tout $k < M(\overline{K})$ et pour tout $x \in \mathbb{R}^{n/2}$,

$$\text{il existe } y \in \mathbb{R}^{n/2} \text{ tel que } m_{\overline{K}}(x + \Omega \cdot y, x - \Omega \cdot y) \geq k. \tag{4.8}$$

Soit alors $x \in \mathbb{R}^{n/2}$ quelconque. On sait, par (4.8), qu'il existe pour tout entier positif p, un élément y_p de $\mathbb{R}^{n/2}$ vérifiant

$$M(\overline{K}) \geq m_{\overline{K}}(x + \Omega \cdot y_p, x - \Omega \cdot y_p) \geq M(\overline{K}) - \frac{1}{p}.$$

En raisonnant comme plus haut modulo

$$\Big\{(\Omega \cdot Y, -\Omega \cdot Y);\ Y \in \Phi'(\mathbb{Z}_{K^+})\Big\} \subseteq \Phi(\mathbb{Z}_K),$$

on peut supposer (y_p) bornée, extraire de (y_p) une sous-suite $(y_{\varphi(p)})$ convergeant vers $y \in \mathbb{R}^{n/2}$, et par semi-continuité supérieure de $m_{\overline{K}}$ on obtient

$$m_{\overline{K}}(x + \Omega \cdot y, x - \Omega \cdot y) \geq \limsup_{p \to +\infty} m_{\overline{K}}(x + \Omega \cdot y_{\varphi(p)}, x - \Omega \cdot y_{\varphi(p)}) = M(\overline{K}).$$

Mais ceci contredit la première hypothèse faite dans l'énoncé de la proposition. On en déduit, par (4.7)

$$\text{il existe } k_1 < M(\overline{K}) \text{ tel que } \mathcal{S}_{k_1} \subseteq \Phi'(K^+) \text{ et est fini modulo } \Phi'(\mathbb{Z}_{K^+}). \tag{4.9}$$

Il n'est pas difficile de voir que le même raisonnement peut être mené avec les ensembles

$$\mathcal{T}_k = \big\{y \in \mathbb{R}^{n/2} \text{ tels qu'il existe } x \in \mathbb{R}^{n/2} \text{ vérifiant } m_{\overline{K}}(x + \Omega \cdot y, x - \Omega \cdot y) \geq k\big\},$$

où $k < M(\overline{K})$. On obtient alors

$$\text{il existe } k_2 < M(\overline{K}) \text{ tel que } \mathcal{T}_{k_2} \subseteq \Phi'(K^+) \text{ et est fini modulo } \Phi'(\mathbb{Z}_{K^+}). \tag{4.10}$$

De (4.9) et (4.10), on déduit que si

$$k = \max\{k_1, k_2\} < M(\overline{K}),$$

l'ensemble des couples $(x, y) \in \mathbb{R}^{n/2} \times \mathbb{R}^{n/2}$ vérifiant

$$m_{\overline{K}}(x + \Omega \cdot y, x - \Omega \cdot y) \geq k$$

est non vide, constitué d'éléments de $\Phi'(K^+) \times \Phi'(K^+)$ et est fini modulo $\Phi'(\mathbb{Z}_{K^+}) \times \Phi'(\mathbb{Z}_{K^+})$. On en tire que l'ensemble des $z \in H$ vérifiant $m_{\overline{K}}(z) \geq k$ est non vide, constitué d'éléments de $\Phi(K)$ et fini modulo

$$\mathcal{U} = \Big\{(X + \Omega \cdot Y, X - \Omega \cdot Y);\ (X, Y) \in \Phi'(\mathbb{Z}_{K^+}) \times \Phi'(\mathbb{Z}_{K^+})\Big\}.$$

Mais, $\mathcal{U}$ est un sous-réseau de $\Phi(\mathbb{Z}_K)$, et l'ensemble considéré est encore fini modulo $\Phi(\mathbb{Z}_K)$. □

Corollaire 4.27. *Soit K un corps de nombres CM de degré $n > 4$. Si, avec les notations précédentes, $\mathbb{Z}_{K^+} + \sqrt{-D}\,\mathbb{Z}_{K^+} = \mathbb{Z}_K$, alors $M(\overline{K})$ est isolé et atteint.*

Preuve. Il suffit de trouver x et y de $\mathbb{R}^{n/2}$ vérifiant les hypothèses de la Proposition 4.26. Montrons que $x = y = 0$ convient, c'est-à-dire que pour tout $y \in \mathbb{R}^{n/2}$,

$$m_{\overline{K}}(\Omega \cdot y, -\Omega \cdot y) < M(\overline{K})$$

et que pour tout $x \in \mathbb{R}^{n/2}$,

$$m_{\overline{K}}(x, x) < M(\overline{K}).$$

Soit y quelconque de $\mathbb{R}^{n/2}$. Comme

$$\Big\{(\Omega \cdot Y, -\Omega \cdot Y);\ Y \in \Phi'(\mathbb{Z}_{K^+})\Big\} \subseteq \Phi(\mathbb{Z}_K),$$

on a

$$\begin{aligned}
m_{\overline{K}}(\Omega \cdot y, -\Omega \cdot y) &\leq \inf\Big\{\mathcal{N}\Big(\Omega \cdot (y - Y), -\Omega \cdot (y - Y)\Big);\ Y \in \Phi'(\mathbb{Z}_{K^+})\Big\}. \\
&\leq \inf\left\{\prod_{i=1}^{n/2} \tau_i(D)(y_i - Y_i)^2;\ Y \in \Phi'(\mathbb{Z}_{K^+})\right\}. \\
&\leq N_{K^+/\mathbb{Q}}(D) m_{\overline{K^+}}(y)^2.
\end{aligned}$$

Comme $m_{\overline{K^+}}(y) \leq M(\overline{K^+}) = M(K^+)$, on obtient

$$\text{pour tout } y \in \mathbb{R}^{n/2},\ m_{\overline{K}}(\Omega \cdot y, -\Omega \cdot y) \leq N_{K^+/\mathbb{Q}}(D) M(K^+)^2. \tag{4.11}$$

Un calcul analogue conduit à

$$\text{pour tout } x \in \mathbb{R}^{n/2},\ m_{\overline{K}}(x, x) \leq M(K^+)^2. \tag{4.12}$$

Pour établir que pour tout x et tout y, $m_{\overline{K}}(\Omega \cdot y, -\Omega \cdot y) < M(\overline{K})$ et $m_{\overline{K}}(x, x) < M(\overline{K})$, il nous suffit, par (4.11) et (4.12), de trouver un élément ξ de K vérifiant

$$m_K(\xi) > \max\Big\{M(K^+)^2, N_{K^+/\mathbb{Q}}(D) M(K^+)^2\Big\} = N_{K^+/\mathbb{Q}}(D) M(K^+)^2.$$

Soit alors un élément $\alpha \in K^+$ vérifiant

$$m_{K^+}(\alpha) = M(K^+),$$

dont l'existence est assurée par le Théorème 4.13, et posons

$$\xi = \alpha + \alpha\sqrt{-D} \in K.$$

En utilisant l'inégalité $\prod(a_i^2 + b_i^2) \geq \prod a_i^2 + \prod b_i^2$ et le fait que $\mathbb{Z}_K = \mathbb{Z}_{K^+} + \sqrt{-D}\mathbb{Z}_{K^+}$, on obtient

$$\begin{aligned}
m_K(\xi) &= \inf\left\{\left|N_{K/\mathbb{Q}}\Big((\alpha - \Upsilon) + \sqrt{-D}(\alpha - \Lambda)\Big)\right|;\ (\Upsilon, \Lambda) \in \mathbb{Z}_{K^+}^2\right\} \\
&= \inf\left\{\left|N_{K^+/\mathbb{Q}}\Big((\alpha - \Upsilon)^2 + D(\alpha - \Lambda)^2\Big)\right|;\ (\Upsilon, \Lambda) \in \mathbb{Z}_{K^+}^2\right\} \\
&= \inf\left\{\prod_{i=1}^{n/2}\Big(\tau_i(\alpha - \Upsilon)^2 + \tau_i(D)\tau_i(\alpha - \Lambda)^2\Big);\ (\Upsilon, \Lambda) \in \mathbb{Z}_{K^+}^2\right\} \\
&\geq \inf\left\{\prod_{i=1}^{n/2}\tau_i(\alpha - \Upsilon)^2 + N_{K^+/\mathbb{Q}}(D)\prod_{i=1}^{n/2}\tau_i(\alpha - \Lambda)^2;\ (\Upsilon, \Lambda) \in \mathbb{Z}_{K^+}^2\right\} \\
&\geq \inf\left\{\prod_{i=1}^{n/2}\tau_i(\alpha - \Upsilon)^2;\ \Upsilon \in \mathbb{Z}_{K^+}\right\} + N_{K^+/\mathbb{Q}}(D)\inf\left\{\prod_{i=1}^{n/2}\tau_i(\alpha - \Lambda)^2;\ \Lambda \in \mathbb{Z}_{K^+}\right\} \\
&\geq \Big(1 + N_{K^+/\mathbb{Q}}(D)\Big)\inf\left\{\prod_{i=1}^{n/2}\tau_i(\alpha - \Upsilon)^2;\ \Upsilon \in \mathbb{Z}_{K^+}\right\} \\
&\geq \Big(1 + N_{K^+/\mathbb{Q}}(D)\Big)\, m_{K^+}(\alpha)^2 \\
&\geq \Big(1 + N_{K^+/\mathbb{Q}}(D)\Big)\, M(K^+)^2 \\
&> N_{K^+/\mathbb{Q}}(D)M(K^+)^2.
\end{aligned}$$

D'où la conclusion. □

Chapitre 5

Euclidianité et principalité

Dans ce chapitre nous explorons succinctement le rapport existant entre euclidianité et principalité.

5.1 Le critère de Dedekind-Hasse

La première question à laquelle nous allons répondre est la suivante.

La connaissance de la partie supérieure de $\mathrm{sp}(K)$ permet-elle de savoir si un corps de nombres K est principal ?

Nous savons déjà que si $M(K) < 1$, K est euclidien pour la norme donc principal. En revanche, que pouvons-nous dire si $M(K) \geq 1$? Si l'on observe les tables que l'on a obtenues dans le cas totalement réel pour $n \geq 4$ on trouve 5 corps non euclidiens pour la norme quand $n = 4$ et un seul quand $n = 5$. De plus dans le cas quartique deux de ces corps vérifient $M(K) = 1$. Si l'on compare avec les tables fournies par PARI [Pa], on voit que

- si $n = 4$ et $D_K < 40000$, il y a trois corps principaux non euclidiens pour la norme ($D_K = 18432,\ 34816,\ 35152$) et deux corps non principaux ($D_K = 21025,\ 32625$).
- si $n = 5$ et $D_K < 512000$, il y a un corps principal non euclidien pour la norme ($D_K = 390625$).

Peut-on vérifier ces résultats à l'aide de l'algorithme utilisé ? La réponse est oui et fait l'objet des lignes qui suivent.

Rappelons d'abord le critère de Dedekind-Hasse (voir par exemple [Po50]).

Théorème 5.1. *Un corps de nombres K est principal si et seulement si pour tout $(\alpha, \beta) \in (\mathbb{Z}_K \backslash \{0\})^2$ vérifiant $\beta \nmid \alpha$,*

$$\text{(5.1)} \qquad \textit{il existe } (\gamma, \delta) \in \mathbb{Z}_K^2 \textit{ tel que } 0 < |N_{K/\mathbb{Q}}(\alpha\gamma - \beta\delta)| < |N_{K/\mathbb{Q}}(\beta)|.$$

Ce critère permet de mettre en relation la principalité et la fonction m_K. Posons la définition suivante.

Définition 5.2. Pour tout ξ de $K\backslash\mathbb{Z}_K$ on notera $h_K(\xi)$ le réel défini par

$$h_K(\xi) = \inf\{m_K(\Upsilon\xi);\ \Upsilon \in \mathbb{Z}_K \text{ et } \Upsilon\xi \notin \mathbb{Z}_K\}. \tag{5.2}$$

On a alors les propriétés suivantes.

Proposition 5.3. *La fonction h_K vérifie*

i) *Pour tout $\xi \in K\backslash\mathbb{Z}_K$, $0 < h_K(\xi) \leq m_K(\xi)$.*

ii) *Pour tout $\xi \in K\backslash\mathbb{Z}_K$ et tout $\alpha \in \mathbb{Z}_K$, $h_K(\xi+\alpha) = h_K(\xi)$.*

iii) *Pour tout $\xi \in K\backslash\mathbb{Z}_K$ et toute unité $\varepsilon \in E_K$, $h_K(\varepsilon\xi) = h_K(\xi)$.*

Preuve. Il est facile de voir que si $\xi = \gamma/d$ où $\gamma \in \mathbb{Z}_K$ et $d \in \mathbb{N}^*$, on peut calculer $h_K(\xi)$ en prenant Υ modulo $d\mathbb{Z}_K$. Par la Proposition 1.10, la borne inférieure définissant $h_K(\xi)$ est en fait un minimum pris sur un ensemble fini de rationnels positifs et est donc positive. Par ailleurs en prenant $\Upsilon = 1$ dans (5.2) on obtient finalement i).

Soient maintenant $\xi \in K\backslash\mathbb{Z}_K$ et $\alpha \in \mathbb{Z}_K$. Comme pour tout $\Upsilon \in \mathbb{Z}_K$ tel que $\Upsilon\xi \notin \mathbb{Z}_K$ on a $\Upsilon(\xi+\alpha) \equiv \Upsilon\xi \bmod \mathbb{Z}_K$ et $\Upsilon(\xi+\alpha) \notin \mathbb{Z}_K$, on a par définition de h_K et par $\mathbb{Z}_K$ périodicité de m_K, $h_K(\xi+\alpha) \leq h_K(\xi)$ qui donne ii) par symétrie.

De même, le point iii) est une conséquence immédiate de l'invariance de $\mathbb{Z}_K$ et de m_K sous l'action des unités. $\square$

Ainsi la fonction h_K est définie modulo $\mathbb{Z}_K$.

Le critère de Dedekind-Hasse se traduit alors de la façon suivante.

Proposition 5.4. *Soit K un corps de nombres. Alors K est principal si et seulement si*

$$\text{pour tout } \xi \in K\backslash\mathbb{Z}_K,\ h_K(\xi) < 1. \tag{5.3}$$

Preuve. Par multiplicativité de la norme, (5.1) se reformule ainsi. Pour tout $\xi \in K\backslash\mathbb{Z}_K$

$$\text{il existe } (\gamma,\delta) \in \mathbb{Z}_K^2 \text{ tel que } 0 < |N_{K/\mathbb{Q}}(\gamma\xi - \delta)| < 1, \tag{5.4}$$

ce qui implique $m_K(\gamma\xi) < 1$. Par ailleurs (5.4) ne peut pas être vérifiée si $\gamma\xi \in \mathbb{Z}_K$. On en déduit $h_K(\xi) < 1$.

Réciproquement, comme $|N_{K/\mathbb{Q}}(\gamma\xi - \delta)| = 0$ implique $\gamma\xi \in \mathbb{Z}_K$ ce qui est exclu dans la définition de h_K, on voit que si $h_K(\xi) < 1$, alors (5.4) est vérifiée. $\square$

Remarque 5.5. On pourrait, ici aussi, définir une fonction $h_{\overline{K}}$ sur H plus générale que h_K, de la façon suivante.

$$\text{Pour } x \in H, h_{\overline{K}}(x) = \inf\{m_{\overline{K}}(X \cdot x);\ X \in \Phi(\mathbb{Z}_K) \text{ et } X \cdot x \notin \Phi(\mathbb{Z}_K)\}.$$

On pourrait alors montrer que pour tout point x non rationnel on a $h_{\overline{K}}(x) = 0$.

Intéressons-nous maintenant aux corps non euclidiens pour la norme évoqués plus haut. Comme on est dans le cas totalement réel et comme $n \geq 3$, le Théorème 4.22 indique qu'il n'y a qu'un nombre fini de points $x \in H = \mathbb{R}^n$ modulo $\Phi(\mathbb{Z}_K)$, vérifiant $m_{\overline{K}}(x) \geq 1$ et qu'en outre ils sont rationnels. On en tire qu'il n'y a qu'un nombre fini de $\xi \in K$ modulo $\mathbb{Z}_K$ tels que $m_K(\xi) \geq 1$. Appliquons l'algorithme du Chapitre 3 avec $k = 0.999$. Alors, si l'on obtient à l'issue des calculs un graphe convenable, grâce au Théorème 3.16 on aura connaissance modulo $\mathbb{Z}_K$ de tous les $\xi \in K$ vérifiant $m_K(\xi) \geq 1$. Cet ensemble que l'on notera S contient donc tous les points $\xi \in K \backslash \mathbb{Z}_K$ modulo $\mathbb{Z}_K$ susceptibles de vérifier $h_K(\xi) \geq 1$, s'il y en a. Il suffit alors de calculer $h_K(\xi)$ pour les ξ de S, et de chercher s'il en existe un vérifiant $h_K(\xi) \geq 1$. Donnons deux exemples pour illustrer notre propos.

Exemple 5.6. Soit K le corps de nombres totalement réel de degré $n = 4$ et de discriminant $D_K = 21025$. On a $M(K) = M(\overline{K}) = 1$, avec 6 points rationnels critiques organisés en deux orbites sous l'action de E_K. Dans la base d'entiers (e_1, e_2, e_3, e_4) calculée par PARI, ces points ont pour coordonnées $(0, 0, 1/2, 1/2)$, $(0, 1/2, 1/2, 0)$, $(0, 1/2, 0, 1/2)$, $(0, 1/2, 1/2, 1/2)$, $(1/2, 1/2, 1/2, 0)$ et $(1/2, 0, 0, 1/2)$. Comme $M(K) = 1$, S est réduit à ces six points. Comme chacun d'eux, ξ, appartient à $1/2\mathbb{Z}_K$, pour calculer $h_K(\xi)$, il suffit de déterminer

$$E(\xi) = \Big\{ \Upsilon\xi;\ \Upsilon = \sum_{i=1}^{4} a_i e_i,\ a_i \in \{0,1\} \text{ et } \Upsilon\xi \notin \mathbb{Z}_K \Big\}.$$

Il est alors facile de voir que pour tout ξ de S on a

$$E(\xi) \subseteq S.$$

Ceci prouve que l'on a $h_K(\xi) = 1$ pour tout $\xi \in S$. On en déduit que K n'est pas principal.

Exemple 5.7. Soit K le corps de nombres totalement réel de degré $n = 4$ et de discriminant $D_K = 18432$. On a $M(K) = M(\overline{K}) = 7/4$, avec 1 seul point rationnel critique. Dans la base d'entiers (e_1, e_2, e_3, e_4) déterminée par PARI, ce point ξ a pour coordonnées $(0, 1/2, 1/2, 1/2)$. Appliquons l'algorithme avec $k = 0.999$. Le graphe défini est le même qu'avec $k = 1.75$ et S est réduit à ξ. Comme ξ appartient à $1/2\mathbb{Z}_K$, pour calculer $h_K(\xi)$, il suffit de déterminer

$$E(\xi) = \Big\{ \Upsilon\xi;\ \Upsilon = \sum_{i=1}^{4} a_i e_i,\ a_i \in \{0,1\} \text{ et } \Upsilon\xi \notin \mathbb{Z}_K \Big\}.$$

Or on a $e_2(e_2 + e_3 + e_4) \equiv e_3 + e_4 \bmod 2\mathbb{Z}_K$, ce qui prouve que

$$\xi' = \frac{e_3 + e_4}{2} \in E(\xi).$$

Comme $m_K(\xi') < 1$ on en déduit $h_K(\xi) < 1$, et donc que K est principal.

Le même type de raisonnement convient pour les 4 autres corps évoqués plus haut. Ainsi les corps de discriminants 18432, 34816, 35152 (pour $n = 4$) et 390625 (pour $n = 5$)

constituent les plus petits exemples de corps principaux non euclidiens pour la norme connus en degré 4 et 5. Nous ne savons pas si ces résultats ont déjà fait l'objet d'une publication. À notre connaissance, dans le cas $n = 4$, l'exemple $D_K = 379456$ a été donné par Clark et Ram Murty [ClM95], qui ont en outre établi qu'il était euclidien. Sans doute, y a-t-il d'autres exemples pour $n = 4$ dans la thèse de Clark, mais nous n'avons pas pu la consulter à ce jour.

5.2 Euclidianité en 2 ou 3 étapes

Ceci nous amène à nous poser une seconde question. Les corps principaux non euclidiens pour la norme, découverts à l'aide de l'algorithme, sont-ils euclidiens en 2 étapes (voir Introduction) ?

Compte tenu de ce qui précède, pour chacun des corps en question, il suffit de prendre en considération les $\xi \in K$ qui vérifient $m_K(\xi) \geq 1$. En effet, pour tout autre élément de K, il existe $\Upsilon \in \mathbb{Z}_K$ tel que $|N_{K/\mathbb{Q}}(\xi - \Upsilon)| < 1$, qui est la condition d'euclidianité en une étape. Pour les autres $\xi \in K$, il suffit alors de vérifier qu'il existe $(q_1, q_2) \in \mathbb{Z}_K \times \mathbb{Z}_K \backslash \{0\}$ tel que

$$\left| N_{K/\mathbb{Q}} \left(\xi - q_1 - \frac{1}{q_2} \right) \right| < \frac{1}{|N_{K/\mathbb{Q}}(q_2)|}. \tag{5.5}$$

Comme plus haut, on applique l'algorithme avec $k = 0.999$. Si à l'issue des calculs on obtient un graphe convenable, on connaît grâce au Théorème 3.16 tous les $\xi \in K$ tels que $m_K(\xi) \geq 1$, qui sont en nombre fini modulo $\mathbb{Z}_K$, et on connaît en particulier la partie supérieure du spectre euclidien $\mathrm{sp}(K) \cap [1, +\infty[$. Comme la relation (5.5) est définie modulo $\mathbb{Z}_K$, il suffit de raisonner sur les $\xi \in \mathcal{F}$ renvoyés par l'algorithme. De plus si $\xi' \in \mathrm{Orb}(\xi)$ et si ξ vérifie (5.5), ξ' vérifie également (5.5). En effet si $\xi' = \varepsilon\xi - \Upsilon$, où $(\Upsilon, \varepsilon) \in \mathbb{Z}_K \times E_K$, on a

$$\varepsilon \left(\xi - q_1 - \frac{1}{q_2} \right) = \xi' + \Upsilon - \varepsilon q_1 - \frac{1}{\varepsilon^{-1} q_2},$$

d'où l'on déduit en posant $q_1' = \varepsilon q_1 - \Upsilon$ et $q_2' = \varepsilon^{-1} q_2$,

$$\left| N_{K/\mathbb{Q}} \left(\xi' - q_1' - \frac{1}{q_2'} \right) \right| < \frac{1}{|N_{K/\mathbb{Q}}(q_2')|}.$$

Finalement il suffit de vérifier (5.5) pour un seul ξ par orbite retournée par l'algorithme. À cette fin, nous établissons une liste $\mathcal{Y}$ d'éléments de la forme $q_1 + 1/q_2$, où q_1 appartient à une liste suffisamment importante d'entiers de petites coordonnées dans la base (e_i), et où q_2 fait de même avec la condition $N_{K/\mathbb{Q}}(q_2) \neq 0, \pm 1$. On utilise alors à la place de (5.5) le test : il existe $q_1 + 1/q_2 \in \mathcal{Y}$ tel que

$$\left| N_{K/\mathbb{Q}} \left(\xi - q_1 - \frac{1}{q_2} \right) \right| < \frac{0.999}{|N_{K/\mathbb{Q}}(q_2)|}.$$

Pour les 4 corps en question, le test est positif. On en déduit le résultat suivant.

Proposition 5.8. *En résumé nous avons :*

- *Les corps de nombres quartiques totalement réels de discrimants respectifs* 18432, 34816, 35152 *sont principaux, euclidiens en* 2 *étapes et non euclidiens pour la norme.*
- *Le corps de nombres quintique totalement réel de discriminant* 390625 *est principal, euclidien en* 2 *étapes et non euclidien pour la norme.*

À notre connaissance, ce sont, avec les corps cubiques dont nous parlerons plus bas, les premiers exemples de corps de nombres euclidiens en 2 étapes et non euclidiens pour la norme, en degré supérieur ou égal à 3.

Clark [Cl96b] avait déjà donné un exemple de corps de nombres quartique totalement réel (de discriminant 107653) non euclidien pour la norme et euclidien en au plus 4 étapes, sans toutefois pouvoir préciser si le nombre d'étapes était améliorable. En appliquant la méthode que nous venons de décrire, on trouve 4 éléments ξ de K (modulo $\mathbb{Z}_K$) vérifiant $m_K(\xi) \geq 1$. Ils appartiennent à la même orbite sous l'action de E_K et vérifient tous les quatre $m_K(\xi) = 16/13$. On en déduit

$$M(K) = M(\overline{K}) = \frac{16}{13}.$$

Or un calcul élémentaire montre que pour l'un quelconque de ces quatre éléments ξ, il existe $(q_1, q_2) \in \mathbb{Z}_K \times \mathbb{Z}_K \backslash \{0\}$ vérifiant (5.5). On en déduit que *le corps considéré est euclidien en 2 étapes.*

Il est intéressant de systématiser cette approche pour dresser la liste des premiers corps (totalement réels dans un premier temps) non euclidiens pour la norme et euclidiens en 2 étapes. Nous l'avons fait dans le cas cubique totalement réel, en étudiant tous les corps principaux non euclidiens pour la norme que nous avions identifiés, ainsi que ceux vérifiant la même propriété qui avaient été relevés par Cavallar et Lemmermeyer [CaL98] (malgré certaines erreurs dans les tables de l'article en question où des corps sont annoncés comme principaux alors qu'ils ne le sont pas).

Les résultats figurent en annexe. Dans la table H.1, figurent tous les corps K de discriminant inférieur à 15000 principaux et non euclidiens pour la norme. On y donne la partie supérieure de leur spectre $\mathrm{sp}(K) \cap [1, +\infty[= \mathrm{sp}(\overline{K}) \cap [1, +\infty[$, identifiée par l'algorithme appliqué avec $k = 0.999$, qui retourne à chaque fois un graphe convenable, ce qui permet d'appliquer le Théorème 3.16, et la valeur m pour laquelle K est euclidien en m étapes. Il apparaît que le test naïf décrit plus haut a été positif pour tous les corps étudiés et que l'on a à chaque fois $m = 2$. Nous pouvons donc énoncer le résultat suivant.

Proposition 5.9. *Les* 82 *corps de nombres cubiques, totalement réels, principaux, non euclidiens pour la norme, de discriminant absolu inférieur à* 15000*, sont euclidiens en* 2 *étapes.*

Remarque 5.10. Le cas quadratique, quant à lui, sera probablement beaucoup plus difficile pour la simple raison que l'on n'est même pas sûr d'avoir un nombre fini de ξ (modulo $\mathbb{Z}_K$) vérifiant $m_K(\xi) \geq 1$, et que si c'est néanmoins le cas, il peut y en avoir un nombre prohibitif.

Un prolongement naturel, auquel nous n'avons pas encore réfléchi, consisterait à poser pour $\xi \in K$,

$$m_K^{(2)}(\xi) = \inf\left\{\left|N_{K/\mathbb{Q}}\Big(q_2(\xi - q_1 - 1/q_2)\Big)\right|;\ (q_1, q_2) \in \mathbb{Z}_K \times \mathbb{Z}_K \backslash\{0\}\right\},$$

et à étudier cette fonction comme nous l'avons fait pour m_K. On pourrait de même définir pour $x \in H$,

$$m_{\overline{K}}^{(2)}(x) = \inf\left\{\mathcal{N}\Big(\Phi(q_2)\cdot\Big(x - \Phi(q_1) - \Phi(1/q_2)\Big)\Big);\ (q_1, q_2) \in \mathbb{Z}_K \times \mathbb{Z}_K \backslash\{0\}\right\},$$

qui est encore semi-continue supérieurement sur H, définie modulo $\Phi(\mathbb{Z}_K)$ et invariante sous l'action de E_K. Ainsi, beaucoup des arguments utilisés lors de l'étude de m_K ou $m_{\overline{K}}$ sont encore valables ici.

Il faudrait à l'avenir chercher à définir un algorithme permettant de calculer $m_K^{(2)}(\xi)$ pour $\xi \in K$, et comme avec m_K,

$$M^{(2)}(K) = \sup\left\{m_K^{(2)}(\xi);\ \xi \in K\right\}.$$

La même remarque vaut également pour les fractions continues de longueurs supérieures qui permettraient de définir de façon identique $m_K^{(3)}$, etc.

Conclusion

Comme on le voit, il reste encore de nombreuses pistes à explorer.

En premier lieu, il conviendrait d'étendre l'algorithme au cas général, en suivant les indications données à la fin du Chapitre 3. A priori, cela ne devrait pas poser de problème particulier.

Pour ce qui concerne l'étude des spectres, il reste à élucider le cas $r = 1$ et à apporter quelques précisions dans le cas d'un corps CM vérifiant $r > 1$.

Pour le cas $r = 1$, les conjectures 1 et 2 de Barnes et Swinnerton-Dyer constituent un bel objectif. La théorie ergodique devrait permettre de préciser les choses, et un lien que nous n'avons pas évoqué jusqu'ici peut aussi apporter quelques éléments dans le cas quadratique réel. Il s'agit d'une question d'approximation diophantienne inhomogène (voir par exemple [Pia]) que nous évoquons ici rapidement. Soit K un corps de nombres quadratique réel. Si $\alpha \in \mathbb{Z}_K$ est tel que $(1, \alpha)$ constitue une $\mathbb{Z}$-base de $\mathbb{Z}_K$, et si $\gamma \in \mathbb{R}$, posons

$$\mathcal{M}_\alpha(\gamma) = \liminf_{|n| \to +\infty} |n| \| n\gamma - \alpha \|,$$

où $\|x\|$ désigne la distance de x à $\mathbb{Z}$. Posons également

$$\mathcal{L}(\alpha) = \{\mathcal{M}_\alpha(\gamma);\ \gamma \in \mathbb{R}\} \quad \text{et} \quad \rho(\alpha) = \sup \mathcal{L}(\alpha).$$

On peut alors établir

$$\operatorname{sp}(K) \subseteq \mathcal{L}(\alpha) \subseteq \operatorname{sp}(\overline{K}) \quad \text{et} \quad M(\overline{K}) = \rho(\alpha)\sqrt{D_K}.$$

Or $\mathcal{L}(\alpha)$ semblerait plus facile à analyser que $\operatorname{sp}(K)$ ou $\operatorname{sp}(\overline{K})$. Par exemple, en utilisant la théorie des fractions continues, Pinner est parvenu à déterminer l'allure de la partie supérieure de $\mathcal{L}(\alpha)$ et à établir des résultats qui impliquent la conjecture 1 de Barnes et Swinnerton-Dyer dans des cas particuliers que l'on connaissait déjà. Toutefois, sa méthode semble être généralisable à d'autres cas ([Pi01, Pib]).

Pour les corps CM, parvenir à montrer que $M(\overline{K})$ est isolé ou à défaut trouver un exemple dans lequel cette propriété n'est pas vérifiée, constituerait un autre objectif, moins spectaculaire, mais sans doute plus accessible.

Enfin, restent les questions relatives à l'euclidianité en m étapes, à l'infini, ou pour d'autres stathmes que la norme, que la rédaction de cette thèse nous a permis de découvrir, et qui constituent un enjeu majeur de la théorie. Comme nous l'avons déjà dit, l'élaboration d'un algorithme permettant de calculer $m_K^{(2)}(\xi)$ et $M^{(2)}(K)$, pourrait constituer, dans un premier temps, un prolongement naturel aux considérations du Chapitre 5.

Nous espérons que nos prochaines investigations nous permettront d'élucider ces différents problèmes.

Annexes

Légende des tables

- Dans la table A.1 on a $K = \mathbb{Q}(\sqrt{m})$.
  Dans toutes les autres tables D_K désigne le discriminant absolu de K.

- Dans la table B.2, la lettre E signifie que K est euclidien pour la norme. Dans toutes les autres tables, T est le nombre de points rationnels critiques modulo $\Phi(\mathbb{Z}_K)$.

Annexe A

Corps quadratiques

TAB. A.1: $n = 2$

m	T	$M(K)$	m	T	$M(K)$
103	2	1129671/455054	105	2	8/7
106	4	13967/8010	107	2	637/214
109	4	8709209/7425625	110	1	11/4
111	1	11/4	113	4	3514159/2408708
114	2	343/114	115	4	289554/140875
118	2	835775/306918	119	2	1121/238
122	1	11/2	123	2	393/82
127	2	21904533/9461246	129	2	64/43
130	1	7/2	131	2	4440376/1390041
133	2	299/171	134	2	194659/72963
137	4	4543/3488	138	1	17/4
141	2	275/188	142	1	21/4
143	1	11/2	145	2	3/2
146	1	23/4	149	4	95/61
154	1	15/4	155	1	7/2
157	4	436/217	158	2	539/158
159	2	275/106	161	2	34/23
165	2	41/15	167	2	1909/334
170	1	13/2	173	2	36/13
174	2	115/24	177	2	88/59
178	2	1377/356	179	2	21395567/8380422
181	4	2876/1305	182	1	7/2
183	1	7/2	185	4	113/68
186	2	20947/7502	187	2	729/187
190	2	292671/104044	193	4	k_1
194	1	25/4	195	1	13/2
197	2	7/4	201	2	1844723/1030192
202	4	183203/68276	203	1	11/2
205	2	81/41	206	2	110615/29767
209	2	1467/931	210	1	15/4
213	2	187/71	215	2	361/86
217	4	k_2	218	1	11/2
219	2	805/146	221	2	55/17
222	1	13/2	223	2	2997/446
226	1	15/2	227	2	3079/454
229	4	49/15	230	1	13/2
231	2	923/154	233	4	3715882019/2144801348
235	2	441/94	237	2	227/79

m	T	$M(K)$	m	T	$M(K)$
238	2	24294/5831	246	2	66726/14801
247	2	344693/85293	251	2	12735720/3674891
253	2	3877/1863	254	1	29/4
255	1	15/2	257	2	2
258	1	31/4	259	2	2958475/847226
263	2	1046501/278254	265	4	233/138
266	2	3085/684	267	2	847/178
269	4	517/269	273	2	272/91
274	1	9/2	277	4	5788/2613
278	2	2777/556	281	4	1808417155581/1131100315025
282	2	23231/4704	285	2	71/19
286	2	4068289/1123672	287	2	4433/574
290	1	17/2	291	2	1509/194
293	4	64/17	295	2	1868333/506250
298	4	k_3	299	2	3865/832
301	2	38751/22747	302	2	29948063/8553244
303	2	24489/5046	305	2	529/244
309	2	240/103	310	1	19/4
314	4	3241351/785000	317	4	20231/7925
318	1	29/4	321	2	260/107
322	1	33/4	323	1	17/2
326	1	35/4	327	1	17/2
329	2	784/423	330	1	31/4
335	2	5171/1206	339	2	1000945/195942
341	2	767/279	345	2	40/23
346	1	11/2	347	2	2671668/641603
349	4	k_4	353	4	k_5
354	2	316991/57348	355	2	1419/284
357	2	89/21	359	2	6265/718
362	1	19/2	365	4	81/19
366	2	7290735/1815848	370	1	15/2
371	1	25/4	373	4	k_6
374	2	4225/748	377	2	1459/464
381	2	1501/508	383	2	2057/383
385	2	60263/27380	386	2	569023/111554
389	4	533549/262964	390	1	29/4
395	1	17/2	397	4	31061844/11881813
398	1	37/4	399	1	19/2

où

$$k_1 = \frac{20470649447051}{12448646853700}, \quad k_2 = \frac{344451856454}{230887817937}, \quad k_3 = \frac{1297639985683}{335473872500},$$
$$k_4 = \frac{711233433}{339296404}, \quad k_5 = \frac{52222023079}{20314230788} \quad \text{et} \quad k_6 = \frac{187701339}{104775700}.$$

Annexe B

Corps cubiques

Tab. B.1: $n = 3$

D_K	T	$M(K)$	D_K	T	$M(K)$	D_K	T	$M(K)$
1593	2	1/3	2177	2	1/3	2713	8	1/3
2993	2	1/3	3137	12	209/485	3173	1	1/2
3252	2	5/9	3261	1	1/2	3281	4	9/13
3316	1	1/2	3325	2	7/10	3356	2	1/2
3368	2	1/2	3496	2	13/16	3508	8	113/178
3540	1	1/2	3569	8	7/17	3576	2	1/2
3580	2	1/2	3592	2	5/8	3596	2	1/2
3604	1	1/2	3624	2	1/2	3732	1	1/2
3736	2	1/2	3753	6	11/27	3873	2	3/5
3877	1	1/2	3892	2	7/10	3941	2	7/12
3957	1	1/2	4104	2	1/2	4281	8	79/225
4344	2	1/2	4364	2	1/2	4409	?	[1/3, 10/27[
4481	3	1/2	4493	2	31/36	4596	1	1/2
4597	1	1/2	4628	1	1/2	4641	2	9/11
4649	4	9/13	4692	1	1/2	4749	1	1/2
4765	3	1/2	4825	2	47/80	4841	20	11/27
4844	2	1/2	4852	1	1/2	4853	4	27/53
4857	8	3/7	4860	2	25/36	4892	2	1/2
4933	1	1/2	5073	?	[1/3, 10/27[	5081	4	7/9
5172	2	5/9	5204	3	1/2	5261	2	3/4
5300	3	3/4	5325	1	1/2	5333	1	1/2
5353	?	[1/5, 72/175[	5356	2	1/2	5368	2	1/2
5373	1	1/2	5468	2	1/2	5477	1	1/2
5497	3	1/2	5529	2	7/9	5556	1	1/2
5613	1	1/2	5620	2	7/10	5621	1	1/2
5624	2	1/2	5629	1	1/2	5637	1	1/2
5685	1	1/2	5697	4	7/17	5724	1	7/8
5741	1	1/2	5780	2	23/34	5821	4	7/8
5853	1	1/2	5901	2	9/16	5912	2	5/9
5925	4	137/180	5940	1	1/2	5980	2	13/20
6053	1	1/2	6088	2	25/32	6092	2	1/2
6108	2	1/2	6133	1	1/2	6153	2	5/9
6184	2	23/32	6209	6	83/133	6237	1	1/2
6268	4	17/32	6396	2	1/2	6420	2	1/2
6453	1	1/2	6508	1	5/8	6549	1	1/2
6556	2	25/32	6557	1	1/2	6584	2	1/2

Tab. B.2: $n = 3$

D_K	$M(K)$	D_K	$M(K)$	D_K	$M(K)$	D_K	$M(K)$
10661	E	10929	E	10941	E	10949	E
10997	E	11013	E	11020	E	11028	E
11032	E	11045	E	11057	E	11060	E
11085	E	11092	E	11097	11/9	11109	E
11124	5/4	11137	E	11188	5/4	11197	31/8
11289	E	11293	E	11316	E	11321	E
11324	3/2	11348	9/4	11380	E	11401	167/151
11417	11/3	11421	49/36	11448	E	11476	E
11505	E	11545	E	11576	E	11608	E
11637	5/4	11641	E	11656	11/8	11665	E
11672	E	11688	E	11697	E	11705	213/193
11757	E	11772	E	11777	27/17	11789	E
11821	23/16	11829	E	11848	E	11849	19/9
11853	E	11880	E	11881	E	11884	E
11885	E	11965	23/8	12001	E	12065	1
12081	152/149	12092	E	12140	E	12177	E
12188	E	12197	3/2	12216	E	12248	E
12269	E	12284	E	12309	E	12317	25/22
12325	E	12333	E	12401	E	12409	E
12436	E	12441	E	12552	E	12577	49/19
12632	E	12652	E	12657	E	12660	23/18
12664	E	12685	E	12700	E	12724	E
12744	E	12765	23/20	12788	E	12821	E
12849	E	12852	E	12925	E	13069	E
13089	E	13117	E	13148	E	13153	7/5
13172	E	13189	E	13204	E	13245	E
13257	E	13269	E	13273	E	13332	E
13333	E	13396	E	13433	E	13460	9/8
13473	E	13537	E	13549	41/36	13564	E
13576	11/8	13577	E	13589	E	13608	E
13652	E	13676	3/2	13684	E	13688	E
13689_1	53/39	13689_2	13/3	13693	31/22	13748	E
13765	E	13768	5/2	13785	E	13801	67/17
13861	17/8	13877	E	13897	E	13905	E
13916	16/9	13925	5/4	13928	E	13932	95/48

D_K	$M(K)$	D_K	$M(K)$	D_K	$M(K)$	D_K	$M(K)$
13972	E	14013	2	14036	45/44	14056	19/16
14089	27/7	14129	E	14141	E	14165	E
14189	E	14197	3/2	14229	E	14296	E
14316	E	14360	E	14376	E	14385	E
14388	E	14389	E	14397	9/4	14408	E
14420	E	14424	E	14457	E	14505	8/7
14516	E	14520	40/33	14597	E	14609	E
14653	E	14661	7/2	14668	E	14680	E
14769	E	14824	E	14825	E	14836	E
14876	E	14945	33/5	14956	E	14964	E
14969	E	14977	E	14993	E		

Les corps de nombres de discriminant 13689 sont respectivement engendrés par une racine de $X^3 - 39X - 26$ ($D_K = 13689_1$) et $X^3 - 39X - 91$ ($D_K = 13689_2$).

Annexe C

Corps quartiques

TAB. C.1: $n = 4$

D_K	T	$M(K)$	D_K	T	$M(K)$	D_K	T	$M(K)$
725	20	1/11	1125	4	1/5	1600	3	1/4
1957	2	1/3	2000	3	1/4	2048	1	1/2
2225	6	1/4	2304	1	1/2	2525	8	1/5
2624	3	1/4	2777	1	1/2	3600	3	1/4
3981	2	1/3	4205	16	1/5	4225	6	1/4
4352	1	1/2	4400	3	1/4	4525	8	1/5
4752	2	1/3	4913	6	1/4	5125	4	1/5
5225	6	1/4	5725	8	1/9	5744	3	1/4
6125	16	11/49	6224	1	1/2	6809	1	1/2
7053	2	1/3	7056	2	1/3	7168	1	1/2
7225	6	1/4	7232	2	1/2	7488	1	1/2
7537	1	1/2	7600	3	1/4	7625	6	1/4
8000	6	5/16	8069	4	1/5	8112	2	1/3
8468	1	1/2	8525	8	1/5	8725	16	1/9
8768	3	1/4	8789	4	1/5	8957	4	1/3
9225	6	1/4	9248	2	1/2	9301	2	1/3
9792	6	7/16	9909	2	1/3	10025	6	1/4
10273	1	1/2	10304	2	1/2	10309	52	9/53
10512	3	1/4	10816	3	1/4	10889	1	1/2
11025	6	1/4	11197	2	1/3	11324	1	1/2
11344	1	1/2	11348	2	1/2	11525	8	1/5
11661	6	1/3	12197	12	13/37	12357	4	1/3
12400	3	1/4	12544	1	1/2	12725	40	1/11
13025	6	1/4	13068	1	1/2	13448	1	1/2
13525	8	1/5	13625	6	1/4	13676	1	1/2
13725	12	9/25	13768	1	1/2	13824	1	1/2
13888	3	1/4	13968	2	1/2	14013	4	1/3
14197	18	9/37	14272	2	1/3	14336	1	1/2
14400	6	5/16	14656	1	1/2	14725	28	9/29
15125	20	31/121	15188	2	1/2	15317	2	1/2
15529	1	1/2	15952	1	1/2	16225	6	1/4
16317	12	17/49	16357	2	1/3	16400	3	1/4
16448_1	1	1/2	16448_2	2	1/2	16609	1	1/2
16997	8	1/5	17069	4	1/3	17417	1	1/2
17424	2	1/2	17428	2	1/2	17600	6	11/16
17609	1	1/2	17725	16	1/9	17989	2	1/3
18097	2	1/3	18432	1	7/4	18496	2	9/16

D_K	T	$M(K)$	D_K	T	$M(K)$	D_K	T	$M(K)$
18625	6	$1/4$	18688	1	$1/2$	18736	2	$1/3$
19025	6	$1/4$	19225	6	$1/4$	19429	2	$1/3$
19525	8	$1/5$	19600	3	$1/4$	19664	2	$1/2$
19773	4	$9/13$	19796	2	$1/2$	19821	2	$1/3$
20032	3	$1/4$	20225	6	$1/4$	20308	2	$1/2$
20808	1	$1/2$	21025	6	1	21056	3	$1/4$
21200	1	$1/2$	21208	1	$1/2$	21308	1	$1/2$
21312	1	$1/2$	21469	2	$1/3$	21568	2	$1/2$
21725	28	$11/29$	21737	6	$1/4$	21801	2	$1/3$
21964	1	$1/2$	22000	6	$9/16$	22221	4	$1/3$
22545	1	$1/2$	22592	2	$1/2$	22676	2	$1/2$
22784	1	$1/2$	22896	4	$1/3$	23252	2	$1/2$
23297	1	$1/2$	23301	2	$1/3$	23377	1	$1/2$
23525	8	$1/5$	23552	1	$1/2$	23600	3	$1/4$
23665	1	$1/2$	23724	1	$1/2$	24197	2	$1/2$
24336	4	$1/3$	24400	8	$9/25$	24417	1	$1/2$
24437	8	$1/5$	24525	8	$9/25$	24749	6	$1/7$
24832	1	$1/2$	24917	4	$1/3$	25088	2	$1/2$
25225	6	$1/4$	25488	2	$1/2$	25492	2	$1/2$
25525	8	$1/5$	25717	2	$1/3$	25808	1	$1/2$
25857	4	$1/3$	25893	4	$1/3$	25961	1	$1/2$
26032	2	$1/3$	26125	4	$1/5$	26176	3	$1/4$
26224	2	$1/3$	26225	6	$1/4$	26525	8	$1/5$
26541	4	$1/3$	26569	1	$1/2$	26825	1	$1/2$
26873	2	$7/8$	27004	1	$1/2$	27225	6	$1/4$
27329	1	$1/2$	27472	1	$1/2$	27648	1	$3/4$
27725	28	$16/29$	27792	4	$1/3$	28025	6	$1/4$
28224_1	6	$5/16$	28224_2	6	$7/16$	28400	3	$1/4$
28473	1	$1/2$	28669	4	$1/5$	28677	2	$1/3$
28749	5	$7/16$	29237	4	$1/3$	29248	3	$1/4$
29268	2	$1/2$	29813	30	$13/77$	29952	1	$3/4$
30056_1	3	$1/2$	30056_2	1	$1/2$	30125	4	$1/5$
30273	1	$1/2$	30400	6	$5/16$	30512	3	$1/4$
30544	1	$1/2$	30725	?	$[1/11, 8/59[$	30776	1	$1/2$
30972	1	$1/2$	30976	1	$1/2$	31225	6	$1/4$
31288	1	$1/2$	31532	1	$1/2$	31600	3	$1/4$
31744	1	$1/2$	31808	2	$1/2$	32081	1	$1/2$
32225	6	$1/4$	32368	2	$1/3$	32448	6	$1/3$

D_K	T	$M(K)$	D_K	T	$M(K)$	D_K	T	$M(K)$
32625	6	1	32737	1	1/2	32821	2	1/3
32832	2	1/3	33097	1	1/2	33344	3	1/4
33424	2	1/3	33428	2	1/2	33452	1	1/2
33489	1	1/2	33525	8	11/25	33625	6	1/4
33709	2	1/3	33725	50	19/121	33813	2	1/2
33844	2	1/2	34025	6	1/4	34196	2	1/2
34225	6	9/16	34704	3	1/4	34816	1	7/4
34868	2	1/2	35013	6	1/3	35125	4	1/5
35136	1	1/2	35152	4	16/13	35225	6	1/4
35312	4	1/3	35392	3	1/4	35401	2	1/3
35537_1	1	1/2	35537_2	1	1/2	35537_3	1	1/2
35856	2	1/3	36025	6	1/4	36416	3	1/4
36517	12	13/49	36677	14	11/29	36761	1	1/2
36928	2	1/2	37108	2	1/2	37229	4	1/3
37349	4	9/13	37485_1	16	17/49	37485_2	4	1/3
37489	1	1/2	37525	8	1/5	37773	4	1/3
37885	2	1/3	37952	2	1/2	38000	6	5/16
38225	6	1/4	38720	1	1/2	38725	?	$[1/9, 3/16[$
38864	3	1/4	39377	4	1/3	39528	1	1/2
39600	6	9/16	39605	2	1/2	39744	1	1/2
39800	1	1/2						

Les corps de nombres de discriminant 16448 sont respectivement engendrés par une racine de $X^4 - 2X^3 - 6X^2 + 2$ ($D_K = 16448_1$) et $X^4 - 2X^3 - 7X^2 + 8X + 14$ ($D_K = 16448_2$).

Les corps de nombres de discriminant 28224 sont respectivement engendrés par une racine de $X^4 - 10X^2 + 4$ ($D_K = 28224_1$) et $X^4 - 2X^3 - 13X^2 + 14X + 7$ ($D_K = 28224_2$).

Les corps de nombres de discriminant 35537 sont respectivement engendrés par une racine de $X^4 - 2X^3 - 9X^2 + 5X + 16$ ($D_K = 35537_1$), $X^4 - X^3 - 8X^2 - 3X + 4$ ($D_K = 35537_2$) et $X^4 - 2X^3 - 5X^2 + 5X + 4$ ($D_K = 35537_3$).

Les corps de nombres de discriminant 37485 sont respectivement engendrés par une racine de $X^4 - X^3 - 7X^2 + X + 1$ ($D_K = 37485_1$) et $X^4 - X^3 - 8X^2 + 12X - 3$ ($D_K = 37485_2$).

Annexe D

Corps quintiques

TAB. D.1: $n = 5$

D_K	T	$M(K)$	D_K	T	$M(K)$	D_K	T	$M(K)$
14641	10	1/11	24217	4	1/5	36497	2	1/3
38569	6	1/7	65657	2	1/3	70601	6	1/7
81509	1	1/2	81589	1	1/2	89417	2	1/3
101833	4	1/5	106069	1	1/2	117688	1	1/2
122821	3	1/4	124817	2	1/3	126032	1	1/2
135076	1	1/2	138136	1	1/2	138917	2	1/3
144209	2	1/3	147109	1	1/2	149169	2	1/3
153424	1	1/2	157457	2	1/3	160801	2	1/3
161121	4	1/3	170701	3	1/4	173513	8	1/9
176281	8	1/5	176684	1	1/2	179024	1	1/2
180769	8	1/5	181057	4	1/3	186037	1	1/2
195829	1	1/2	202817	2	1/3	205225	4	1/3
207184	1	1/2	210557	3	1/4	216637	1	1/2
218524	1	1/2	220036	1	1/2	220669	1	1/2
223824	1	1/2	223952	1	1/2	224773	1	1/2
230224	2	1/2	233489	6	1/7	236549	1	1/2
240133	1	1/2	240881	4	1/5	242773	3	1/4
245992	1	1/2	246832	1	1/2	249689	4	1/5
255877	3	1/4	265504	2	1/2	270017	2	1/3
273397	1	1/2	274129	4	1/5	284897	2	1/3
287349	2	1/3	288385	4	1/3	288565	3	1/4
288633	2	1/3	294577	4	1/3	301117	1	1/2
301909	1	1/2	303952	1	1/2	305617	4	1/5
307145	2	1/3	307829	3	1/4	310097	2	1/3
310257	4	1/3	312617	2	1/3	313905	2	1/3
320837	1	1/2	324301	1	1/2	328784	2	1/2
329977	2	1/3	331312	1	1/2	339509	2	1/3
341692	1	1/2	345065	2	1/3	347317	3	1/4
352076	1	1/2	352588	1	1/2	354969	2	1/3
355309	1	1/2	356173	3	1/4	356789	3	1/4
357977	4	1/5	368464	2	1/2	369849	2	1/3
372289	2	1/2	373057	6	1/7	375116	1	1/2
375145	8	1/5	379077	1	1/2	379477	1	1/2
380224	2	1/2	386404	1	1/2	387268	1	1/2
390625	2	7/5	394064	1	1/2	394657	2	1/3
395721	2	1/3	396520	1	1/2	398885	1	1/2

D_K	T	$M(K)$	D_K	T	$M(K)$	D_K	T	$M(K)$
401584	2	1/2	403137	4	1/3	404185	4	1/5
404744	1	1/2	406264	2	1/2	410677	1	1/2
414677	1	1/2	416249	8	1/5	419969	12	1/7
420460	1	1/2	421096	1	1/2	422069	1	1/2
422077	1	1/2	423537	2	1/3	423904	2	1/2
427569	2	1/3	429937	4	1/5	442552	1	1/2
446609	2	1/3	449617	12	1/7	449733	1	1/2
450277	3	1/4	453712	1	1/2	453749	1	1/2
454057	4	1/3	457904	1	1/2	459513	2	1/3
459533	3	1/4	460708	1	1/2	463341	1	1/2
463477	3	1/4	466809	4	1/3	470117	2	1/3
475333	3	1/4	475929	2	1/3	481097	4	1/5
482689	8	1/5	483273	2	1/3	484105	8	1/5
486337	2	1/2	488149	1	1/2	493049	6	1/7
495317	3	1/4	501289	8	1/5	503376	1	1/2
504568	2	1/2	509324	1	1/2	510889	2	1/2

Annexe E

Corps sextiques

TAB. E.1: $n = 6$

D_K	T	$M(K)$	D_K	T	$M(K)$	D_K	T	$M(K)$
300125	168	1/29	371293	12	1/13	434581	24	1/13
453789	6	1/7	485125	8	1/9	592661	6	1/7
703493	48	1/13	722000	3	1/4	810448	3	1/4
820125	8	1/9	905177	14	1/8	966125	4	1/5
980125	8	1/9	1075648	6	1/7	1081856	6	1/7
1134389	6	1/7	1202933	4	1/5	1229312	12	1/7
1241125	4	1/5	1259712	2	1/3	1279733	12	1/7
1292517	8	1/9	1312625	3	1/4	1387029	2	1/3
1397493	2	1/3	1416125	4	1/5	1528713	14	1/8
1541581	4	1/5	1683101	12	1/7	1767625	3	1/4
1868969	1	1/2	1922000	3	1/4	1995125	30	1/11
1997632	7	1/8	2115281	14	1/8	2235125	24	1/9
2249737	14	1/8	2286997	2	1/3	2323397	2	1/3
2415125	30	1/11	2460365	8	1/5	2495261	2	1/3
2501557	2	1/3	2540864	1	1/2	2565429	2	1/3
2591125	4	1/5	2623625	3	1/4	2624293	12	1/7
2661761	1	1/2	2666432	7	1/8	2737625	3	1/4
2738000	3	1/4	2782261	2	1/3	2803712	1	1/2
2806769	6	1/7	2812877	8	1/5	2847089	1	1/2
2847312	2	1/3	2850125	24	1/9	2854789	132	1/13
2908477	8	1/5	2936696	1	1/2	2990117	2	1/3
3022625	3	1/4	3027661	12	1/7	3072812	1	1/2
3081125	4	1/5	3086597	4	1/3	3094889	12	1/7
3151861	2	1/3	3162625	3	1/4	3184733	6	1/7
3195392_1	1	1/2	3195392_2	18	1/7	3296573	12	1/7
3319769	1	1/2	3356224	1	1/2	3359232	7	1/8
3389609	1	1/2	3418281	14	1/8	3438125	8	1/5
3455125	8	1/9	3477989	4	1/5	3486377	3	1/4
3512000	6	1/4	3527069	60	1/13	3549501	4	1/3
3570125	12	1/5	3662336	6	1/7	3697873	1	1/2
3706688	2	1/3	3728437	2	1/3	3728753	14	1/8
3822093	2	1/3	3829849	3	1/4	3916917	2	1/3
3928381	2	1/3	4016873	6	1/7	4022000	6	1/4
4086536	1	1/2	4125937	1	1/2	4126869	8	1/9
4141568	1	1/2	4148928	24	8/49	4170688	2	1/3
4181517	2	1/3	4218557	6	1/7	4222000	6	1/4

D_K	T	$M(K)$	D_K	T	$M(K)$	D_K	T	$M(K)$
4224413	8	1/5	4227136	8	1/5	4254689	1	1/2
4274669	6	1/7	4284928	7	1/8	4305125	50	11/101
4308028	1	1/2	4383253	4	1/5	4418000	6	1/4
4418197	2	1/3	4443861	2	1/3	4448597	12	1/7
4456256	12	1/7	4462625	3	1/4	4507648	1	1/2
4537077	2	1/3	4588625	3	1/4	4601153	1	1/2
4642000	3	1/4	4667249	3	1/4	4733829	2	1/3
4755281	1	1/2	4758548	1	1/2	4778125	4	1/5
4820125	8	1/9	4823921	1	1/2	4824572	1	1/2
4829696	1	1/2	4838537	4	1/5	4840784	3	1/4
4847625	3	1/4	4851125	4	1/5	4905125	12	1/5
4918997	10	1/11	4950125	12	1/5	4966677	4	1/3
5030996	1	1/2	5061125	4	1/5	5061656	1	1/2
5090861	4	1/5	5101781	6	1/7	5160733	6	1/7
5163008	1	1/2	5173625	3	1/4	5192000	3	1/4
5224841	3	1/4	5274997	36	1/13	5279033	1	1/2

Annexe F

Corps heptiques

TAB. F.1: $n = 7$

D_K	T	$M(K)$	D_K	T	$M(K)$	D_K	T	$M(K)$
20134393	6	1/7	25164057	2	1/3	25367689	12	1/13
28118369	6	1/7	30653489	2	1/3	31056073	6	1/7
32354821	3	1/4	32567681	8	1/9	34554953	6	1/7
35269512	6	1/7	39610073	4	1/5	39829313	2	1/3
41153941	3	1/4	41455873	4	1/5	41783473	4	1/5
42855577	6	1/7	43242544	3	1/4	43723857	2	1/3
46643776	1	1/2	49960857	2	1/3	52011969	2	1/3
55073801	6	1/7	55078981	7	1/8	55311169	4	1/5
57936017	2	1/3	58355513	4	1/5	61136809	4	1/5
63128113	6	1/7	65698681	12	1/7	65845693	4	1/5
67159593	6	1/7	68249369	2	1/3	69012929	8	1/9
69678137	4	1/5	69836041	10	1/11	70244521	4	1/5
75602713	4	1/5	75630121	4	1/5	77004029	1	1/2
78373945	4	1/5	78534833	8	1/9	79044293	6	1/7
79397476	1	1/2	79438057	4	1/5	80750473	10	1/11
81323773	1	1/2	81437164	1	1/2	82916101	3	1/4
83266101	3	1/4	83934569	4	1/5	84506041	4	1/5
84824233	16	1/9	86278889	6	1/7	88337321	2	1/3
88383761	8	1/9	88537609	10	1/11	89211436	1	1/2
89781929	4	1/5	89916129	2	1/3	91138133	2	1/3
92507681	12	1/7	93364693	3	1/4	93679973	3	1/4
95402689	4	1/5	96309817	2	1/3	96703369	12	1/7
97212489	2	1/3	97824733	3	1/4	98167689	6	1/7
98295577	20	1/11	99230049	2	1/3	100069857	2	1/3
100269173	1	1/2	100660489	6	1/7	100907057	4	1/5
101109161	4	1/5	101206153	4	1/5	102872809	4	1/5
105058897	4	1/3	105391453	1	1/2	105486613	1	1/2
105537053	7	1/8	105708673	4	1/5	107164437	2	1/3
107680489	12	1/7	107704601	4	1/5	108526193	2	1/3
109652617	4	1/5	110251433	4	1/5	110921461	3	1/4
112831453	3	1/4	112873193	4	1/5	113269137	2	1/3
114059549	3	1/4	114075673	4	1/5	114477761	6	1/7
117757033	2	1/3	117806905	8	1/5	118768997	1	1/2
118870813	1	1/2	118892393	4	1/5	119084961	2	1/3
119292949	3	1/4	119605529	2	1/3	120077752	1	1/2
120230212	1	1/2	120275469	1	1/2	120299213	6	1/7
120919849	2	1/3	124666793	2	1/3	124893376	1	1/2
5439409	24	1/13	125834753	2	1/3	126039593	2	1/3

D_K	T	$M(K)$	D_K	T	$M(K)$	D_K	T	$M(K)$
126123101	3	1/4	126284149	8	1/5	126993449	6	1/7
128513177	2	1/3	129629693	7	1/8	129673145	4	1/5
130548149	6	1/7	130696737	4	1/3	130840257	2	1/3
132205961	6	1/7	134317789	6	1/7	134407793	2	1/3
134589773	3	1/4	135384281	8	1/9	135877157	2	1/3
136997732	1	1/2	137185481	6	1/7	138031669	7	1/8

Annexe G

Corps octiques

TAB. G.1: $n = 8$

D_K	T	$M(K)$	D_K	T	$M(K)$
282300416	15	1/16	309593125	18	1/19
324000000	15	1/16	410338673	30	1/16
432640000	15	1/16	442050625	30	1/16
456768125	10	1/11	483345053	10	1/11
494613125	36	1/19	582918125	20	1/11
656505625	30	1/16	661518125	10	1/11
707295133	12	1/13	733968125	10	1/11
740605625	30	1/16	803680625	10	1/11
852038125	20	1/11	877268125	20	1/11

Annexe H

Corps cubiques totalement réels : partie supérieure du spectre et euclidianité en m étapes

TAB. H.1: Corps cubiques totalement réels euclidiens en 2 étapes

D_K	$\mathrm{sp}(\overline{K}) \cap [1, +\infty[$	m
985	$\{1\}$	2
1345	$\{7/5\}$	2
1825	$\{7/5\}$	2
1929	$\{1\}$	2
1937	$\{1\}$	2
2836	$\{7/4\}$	2
2857	$\{8/5\}$	2
3305	$\{13/9\}$	2
3889	$\{13/7, 1\}$	2
3988	$\{19/8, 11/8, 5/4, 19/16, 133/128\}$	2
4193	$\{7/5\}$	2
4345	$\{7/5\}$	2
4360	$\{41/35\}$	2
4729	$\{149/73, 79/73\}$	2
5089	$\{17/11\}$	2
5281	$\{1\}$	2
5297	$\{21/11\}$	2
5329	$\{9/8\}$	2
5369	$\{21/19\}$	2
5521	$\{23/7, 8/7\}$	2
6185	$\{17/15, 1\}$	2
6241	$\{223/79, 137/79, 125/79, 101/79, 89/79, 1\}$	2
6289	$\{1\}$	2
6401	$\{35/27\}$	2
6452	$\{5/4\}$	2
6868	$\{5/4\}$	2
7273	$\{973/601, 729/601\}$	2
7465	$\{1\}$	2
7481	$\{1\}$	2
7528	$\{17/14\}$	2
7573	$\{41/32, 1\}$	2
7745	$\{7/5\}$	2
7873	$\{29/13, 25/13, 8/5\}$	2
8113	$\{13/7, 1\}$	2
8308	$\{67/50\}$	2
8572	$\{17/16\}$	2
8692	$\{11/10\}$	2

D_K	$\mathrm{sp}(\overline{K}) \cap [1, +\infty[$	m
8905	$\{8/5\}$	2
9073	$\{7/5, 545/469, 43/35, 1\}$	2
9217	$\{17/11, 13/11\}$	2
9325	$\{13/8, 13/10, 41/40, 1\}$	2
9409	$\{337/97, 271/97, 216/97, 149/97, 139/97, 131/97, 125/97, 109/97\}$	2
9745	$\{67/23, 37/23, 8/5, 25/23, 121/115, 1\}$	2
9905	$\{9/5, 27/25\}$	2
10164	$\{27/22\}$	2
10216	$\{7/4, 41/32\}$	2
10261	$\{11/7\}$	2
10333	$\{1\}$	2
10457	$\{27/25\}$	2
10561	$\{11/7\}$	2
11097	$\{11/9\}$	2
11124	$\{5/4\}$	2
11188	$\{5/4\}$	2
11401	$\{167/151, 161/151, 157/151\}$	2
11421	$\{49/36, 1\}$	2
11637	$\{5/4\}$	2
11656	$\{11/8\}$	2
11705	$\{213/193\}$	2
11777	$\{27/17, 1\}$	2
11821	$\{23/16, 37/26, 14/13, 27/26\}$	2
11849	$\{19/9, 29/17, 71/51, 19/17, 167/153\}$	2
11965	$\{23/8, 23/16, 23/20, 1\}$	2
12065	$\{1\}$	2
12081	$\{152/149\}$	2
12317	$\{25/22\}$	2
12577	$\{49/19, 35/19, 8/5, 25/19, 23/19\}$	2
12660	$\{23/18, 29/27\}$	2
12765	$\{23/20\}$	2
13153	$\{7/5\}$	2
13460	$\{9/8, 45/44\}$	2
13549	$\{41/36\}$	2
13576	$\{11/8\}$	2
13693	$\{31/22, 1\}$	2
13801	$\{67/17\}$	2
13861	$\{17/8, 17/16\}$	2
13925	$\{5/4, 13/12\}$	2

D_K	$\mathrm{sp}(\overline{K}) \cap [1, +\infty[$	m
14036	$\{45/44\}$	2
14056	$\{19/16\}$	2
14089	$\{27/7, 8/7, 101/89\}$	2
14397	$\{9/4, 9/8\}$	2
14505	$\{8/7\}$	2
14520	$\{40/33\}$	2

Bibliographie

[A2X] The A2X laboratory, Number field tables available from `ftp://megrez.math.u-bordeaux.fr/pub/numberfields`.

[Ak95] R. Akhtar, *Cyclotomic Euclidean Number Fields*, senior Thesis, Harvard Univ., 1995.

[BSD52a] E.S. Barnes et H.P.F Swinnerton-Deyer, The inhomogeneous minima of binary quadratic forms, I, *Acta Mathematica* **87** (1952), 259–323.

[BSD52b] E.S. Barnes et H.P.F Swinnerton-Deyer, The inhomogeneous minima of binary quadratic forms, II, *Acta Mathematica* **88** (1952), 279–316.

[Ba04] E. Bayer Fluckiger, Upper bounds for Euclidean minima of algebraic number fields (preprint).

[Be83] D. Berend, Multi-invariant sets on tori. *Transactions of the American Mathematical Society* **280**, Number 2 (1983), 509-532.

[Be84] D. Berend, Minimal sets on tori. *Ergodic Theory and Dynamical Systems* **4** (1984), 499-507.

[Br76] J.R. Brown, *Ergodic Theory and Topological Dynamics*, Academic Press, Pure and Applied Mathematics (1976).

[Ca71] J.W.S. Cassels, *Introduction to the Geometry of Numbers*, Springer-Verlag, Classics in Mathematics (1971).

[Ca52] J.W.S. Cassels, The inhomogeneous minimum of binary quadratic, ternary cubic and quaternary quartic forms, *Proc. Cambridge Phil. Soc.* **48** (1952), 72-86 et 519-520 (Corr. F.J. van der Linden 1983)

[CaL98] S. Cavallar et F. Lemmermeyer, Euclidean algorithm in cubic number fields, Győry, Pethő, Sos eds., Proceedings Number Theory Eger 1996, de Gruyter (1998), 123-146.

[CaL00] S. Cavallar et F. Lemmermeyer, Euclidean Windows, *LMS Journal of Computation and Mathematics* **3** (2000), 335-355.

[Ce00] J-P. CERRI, De l'euclidianité de $\mathbb{Q}\left(\sqrt{2+\sqrt{2+\sqrt{2}}}\right)$ et $\mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$ pour la norme, *J. Th. Nombres Bordeaux* **12** (2000), 103–126.

[Ce04a] J-P. CERRI, Euclidean minima of totally real number fields. Algorithmic determination, *Mathematics of Computation*, à paraître.

[Ce04b] J-P. CERRI, Euclidean and inhomogeneous spectra of number fields with unit rank greater than 1, *Journal für die reine und angewandte Mathematik*, à paraître.

[Cl94] D.A. CLARK, A quadratic field which is Euclidean but not norm-Euclidean, *Manuscripta Math.* **83** (1994), 327-330.

[Cl96a] D.A. CLARK, Non-Galois cubic fields which are Euclidean but not Norm-Euclidean, *Mathematics of Computation*, vol. 65, Number **216** (1996), 1675-1679.

[Cl96b] D.A. CLARK, On k-stage Euclidean Algorithms for Galois extensions of $\mathbb{Q}$, *Manuscripta Math.* **90** (1996), 149-153.

[ClM95] D.A. CLARK ET M. RAM MURTY The Euclidean algorithm for Galois extensions of $\mathbb{Q}$, *Journal für die reine und angewandte Mathematik* **459** (1995), 151-162.

[Co80] H. COHN, *Advanced Number Theory*, Dover Publications (1980).

[CD86] H. COHN ET J. DEUTSCH, Use of a computer scan to prove $\mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$ and $\mathbb{Q}\left(\sqrt{3+\sqrt{2}}\right)$ are euclidean, *Mathematics of computation* **46** (1986), 295–299.

[Co76] G.E. COOKE, A weakening of the Euclidean Property for Integral Domains and Applications to Algebraic Number Theory I, *J. reine angew. Math.* **282** (1976), 133-156.

[Co77] G.E. COOKE, A weakening of the Euclidean Property for Integral Domains and Applications to Algebraic Number Theory II, *J. reine angew. Math.* **283** (1977), 71-85.

[CoW75] G.E. COOKE ET P.J. WEINBERGER, On the construction of Division Chains in Algebraic Number Rings, with Applications to SL_2, *Commun. Algebra* **3** (1975), 481-524.

[Da46] H. DAVENPORT, Non-homogeneous binary quadratic forms I, *Proc. Kon. Ned. Akd. Wet.* **49** (1946), 815-821.

[Da47] H. DAVENPORT, Non-homogeneous binary quadratic forms II, III et IV, *Proc. Kon. Ned. Akd. Wet.* **50** (1947), 378-389, 484-491, 741-749 et 909-917.

[Da50a] H. DAVENPORT, Euclid's algorithm in cubic fields with negative discriminant, *Acta Math.* **84** (1950), 159-179.

[Da50b] H. Davenport, Euclid's algorithm in certain quartic fields, *Trans. Amer. Math. Soc.* **68** (1950), 508-532.

[Da55] H. Davenport, H.P.F. Swinnerton-Dyer, Product of n linear inhomogeneous forms, *Proc. London Math. Soc. (3)* **5** (1955), 474-499.

[Fu81] H. Furstenberg, *Recurrence in Ergodic Theory and Combinatorial Number Theory*, Princeton University Press, Princeton, New Jersey (1981).

[Fu67] H. Furstenberg, Disjointness in ergodic theory, minimal sets and a problem in diophantine approximation, *Math. Systems Theory* **1** (1967), 1-49.

[Go55] H.J. Godwin, On the inhomogeneous minima of certain norm-forms, *J. London Math. Soc.* **30** (1955), 114-119.

[Go63] H.J. Godwin, On a conjecture of Barnes and Swinnerton-Dyer, *Proc. Cambridge Phil. Soc.* **59** (1963), 519-522.

[GMM87] R. Gupta, M. Ram Murty et V. Kumar Murty, The Euclidean algorithm for S-integers, *Canadian Math. Society Conference Proceedings*, **7** (1987), 189-201.

[Ha00] M. Harper, *A proof that* $\mathbb{Z}[\sqrt{14}]$ *is Euclidean*, Ph. D. Thesis, McGill University (2000).

[HaM03] M. Harper et M. Ram Murty, Euclidean rings of algebraic integers, *Canadian Journal of Math.*, **56** (2004), no. 1, 71-76.

[He50a] H. Heilbronn, On Euclid's Algorithm in cubic self-conjugate fields, *Proc. Cambridge Phil. Soc.* **46** (1950), 377-382.

[He50b] H. Heilbronn, On Euclid's Algorithm in cyclic fields, *Canad. J. Math.* **3** (1950), 257-286.

[In49] K. Inkeri, Non-homogeneous binary quadratic forms, *Den 11te Skandinaviske Matematiker Kongress Trondheim* (1949), 216-224.

[In50] K. Inkeri, On the Minkowski constant in the theory of binary quadratic forms, *Ann. Acad. Sci. Fenn.* Ser. A1 **66** (1950), 1-35.

[Kl] J. Klüners, Tables available at `http://www.mathematik.uni-kassel.de/~klueners`

[Lem95] F. Lemmermeyer, The Euclidean algorithm in algebraic number fields, *Expositiones Mathematicae* **13** (1995), 385-416.

[Lem99] F. Lemmermeyer, The Euclidean algorithm in algebraic number fields, version actualisée de l'article précédent, disponible à `http://www.rzuser.uni-heidelberg.de/~hb3/survey.ps`

[Len74] H.W. Lenstra Jr. Lectures on Euclidean rings, Bielefeld (1974).

[Len75] H.W. LENSTRA JR., Euclid's algorithm in cyclotomic fields, *J. London Math. Soc.* (2) **10** (1975), 457-465.

[Len77a] H.W. LENSTRA JR., Euclidean Number Fields of large degree, *Invent. Math.* **38** (1977), 237-254.

[Len77b] H.W. LENSTRA JR., On Artin's Conjecture and Euclid's Algorithm in Global Fields, *Invent. Math.* **42** (1977), 201-224.

[Len79] H.W. LENSTRA JR., Euclidean Number Fields 1, *The Mathematical Intelligencer*, (2) **1**, Springer-Verlag (1979), 6-15.

[Len80a] H.W. LENSTRA JR., Euclidean Number Fields 2, *The Mathematical Intelligencer*, (2) **2**, Springer-Verlag (1980), 73-77.

[Len80b] H.W. LENSTRA JR., Euclidean Number Fields 3, *The Mathematical Intelligencer*, (2) **2**, Springer-Verlag (1980), 99-103.

[Ma75] J.M. MASLEY ET H.L. MONTGOMERY, Cyclotomic fields with unique factorization, *J. reine angew. Math.* **272** (1975), 45-48.

[McM04] C.T. MCMULLEN, Minkowski's conjecture, well-rounded lattices and topological dimension (preprint).

[Mo49] T.S. MOTZKIN, The Euclidean algorithm, *Bull. Amer. Math. Soc.* **55** (1949), 1142-1146.

[Pa] C. BATUT, K. BELABAS, D. BERNARDI, H. COHEN, M. OLIVIER, The Pari/GP system, `http://pari.math.u-bordeaux.fr`

[Pi01] C. PINNER, More on inhomogeneous diophantine approximation, *Journal de Théorie des Nombres de Bordeaux* **13** (2001), 539-557.

[Pia] C. PINNER, Notes comparing the inhomogeneous Lagrange and Markoff spectra (preprint).

[Pib] C. PINNER, On the inhomogeneous spectrum of period two quadratics (preprint).

[Po50] H. POLLARD, *The Theory of Algebraic Numbers*, Math. Association of America, New-York (1950).

[Qu98] R. QUÊME, A computer algorithm for finding new Euclidean number fields, *J. Th. Nombres Bordeaux* **10** (1998), 33–48.

[Sa71] P. SAMUEL, About Euclidean Rings, *J. Algebra* **19** (1971), 282-301.

[St67] H.M. STARK, A complete determination of the complex quadratic fields of class-number one, *Mich. Math. J.* **14** (1967), 1-27.

[SD54] H.P.F. SWINNERTON-DYER, The inhomogeneous minima of complex cubic norm forms, *Proc. Cambridge Phil. Soc.* **50** (1954), 209-219.

[Tu84] W.T. TUTTE *Graph Theory*, Encyclopedia of Mathematics and its Applications, vol. 21, Addison-Wesley 1984.

[VdL83] F.J. VAN DER LINDEN, Euclidean rings of integers of fourth degree fields, *Lecture Notes in Math.* **1068**(1983), 139-148.

[VdL85] F.J. VAN DER LINDEN, Euclidean rings with two infinite primes, *CWI Tract 15, Centrum voor Wiskunde en Informatica*, 1985.

[Var48] P.L. VARNAVIDES, Non-homogeneous binary quadratic forms, *Proc. Ned. Acad. Wet.* **51** (1948), 396-404 et 470-481.

[Var70] P.L. VARNAVIDES, The Non-homogeneous Minima of a Class of Binary Quadratic Forms, *Journal of Number Theory* **2** (1970), 333-341.

[Wa82] L.C. WASHINGTON, *Introduction to cyclotomic fields*, Graduate Texts in Math. **83**, Springer-Verlag (1982).

[We73] P. WEINBERGER, On Euclidean rings of algebraic integers, *Proceedings of Symposia in Pure Math.*, **24** (1973), 321-332.

Jean-Paul Cerri
2, route de Saint-Dié
F-88600 Aydoilles
Jean-Paul.CERRI@wanadoo.fr

Résumé

L'objet de cette thèse est double. Tout d'abord elle vise à répondre à certaines questions relatives aux notions de spectres euclidien et inhomogène (pour la norme) d'un corps de nombres, et notamment à celles qui concernent son minimum euclidien (pour la norme). Nous établissons en particulier que pour tout corps de nombres K, le minimum euclidien de K, noté $M(K)$, est égal à son minimum inhomogène $M(\overline{K})$, et que si le rang du groupe des unités de K est strictement supérieur à 1, les spectres euclidiens et inhomogènes de K sont égaux et rationnels lorsque K n'est pas CM. Les résultats que nous établissons sous l'hypothèse $r > 1$, ont pour conséquence particulière la décidabilité de l'euclidianité de K pour la norme.

Nous montrons également comment calculer explicitement $M(K)$. Nous décrivons un algorithme pour le cas où K est totalement réel, qui a permis de construire des tables jusqu'au degré 8 ; nous indiquons comment le transposer à des corps de nombres quelconques. En outre, cet algorithme a permis de trouver de nombreux exemples de corps de nombres principaux, non euclidiens pour la norme et euclidiens en 2 étapes.

Mots-clés: Corps de nombres, minimum et spectre euclidiens, minimum et spectre inhomogènes, algorithmique, euclidianité en m étapes

Abstract

This thesis has a twofold purpose. Firstly, it attempts to address various issues relating to the concepts of Euclidean and inhomogeneous spectra (for the norm form), especially those relating to the Euclidean minimum of a number field (for the norm form). We establish, in particular, that for every number field K, the Euclidean minimum of K, denoted by $M(K)$, and the inhomogeneous minimum of K, $M(\overline{K})$, are equal, and that, if the unit rank of K is strictly greater than 1, the Euclidean and inhomogeneous spectra of K are equal and rational when K is not CM. The results that we have established in the latter case, have as a consequence, the decidability of whether K is norm-Euclidean or not.

We also show how to explicitly compute $M(K)$. We present an algorithm for cases where K is a totally real number field. This algorithm has enabled us to establish tables up to degree 8, and it may be transposed to any number field. Moreover, this algorithm has enabled us to find many examples of number fields with class number 1, which are not norm-Euclidean but m-stage norm-Euclidean for $m = 2$.

Keywords: Number fields, Euclidean minimum and spectrum, inhomogeneous minimum and spectrum, algorithm, m-stage norm-Euclidean