Méthodes algorithmiques pour les réseaux algébriques

Thomas Camus

Communauté
UNIVERSITÉ Grenoble Alpes

THÈSE

Pour obtenir le grade de

DOCTEUR DE LA COMMUNAUTÉ UNIVERSITÉ GRENOBLE ALPES

Spécialité : **Mathématiques**

Arrêté ministériel : 25 mai 2016

Présentée par

Thomas Camus

Thèse dirigée par **Philippe ELBAZ-VINCENT**

préparée au sein du Laboratoire **Institut Fourier**
dans l'École Doctorale **Mathématiques, Sciences et Technologies de l'Information, Informatique**

Méthodes algorithmiques pour les réseaux algébriques

Thèse soutenue publiquement le **10 juillet 2017**,
devant le jury composé de :

M. Roland BACHER
Maître de conférences à l'Université Grenoble Alpes, Grenoble, Examinateur
M. Karim BELABAS
Professeur à l'Université de Bordeaux, Talence, Rapporteur
M. Renaud COULANGEON
Maître de conférences à l'Université de Bordeaux, Talence, Examinateur
M. Philippe ELBAZ-VINCENT
Professeur à l'Université Grenoble Alpes, Grenoble, Directeur de thèse
M. Graham ELLIS
Professeur à National University of Ireland, Galway, Ireland, Examinateur
M. Paul E. GUNNELLS
Professeur à University of Massachussetts, Amherst, USA, Rapporteur
Mme. Gabriele NEBE
Professeur à RWTH Aachen University, Aachen, Allemagne, Examinatrice
M. Damien STEHLÉ
Professeur à l'École Normale Supérieure de Lyon, Lyon, Président

REMERCIEMENTS

Ben si, si c'est l'même volume sonore, on dit « équidistant ». S'ils sont équidistants en même temps que nous, on peut repérer le dragon par rapport à une certaine distance. Si le dragon s'éloigne, on s'ra équidistants, mais ça s'ra vachement moins précis...et pas réciproque.

Mes premiers remerciements sont naturellement adressés aux membres du jury, qui ont accepté d'examiner mes travaux. En particulier, je remercie Karim Belabas et Paul Gunnells d'avoir accepté de rapporter ma thèse. Leurs commentaires justes et précis m'ont permis d'étoffer ma vision de ce domaine de recherche. Durant ma thèse, j'ai bénéficié du soutien financier partiel du LabEx PERSYVAL-Lab (ANR-11-LABX-2005).

Je suis très reconnaissant à Philippe d'avoir supervisé mes recherches pendant mon stage de master et tout au long de ma thèse. Il a indéniablement su attiser ma curiosité avec ses nombreuses questions et suggestions. Ses conseils et remarques, mathématiques ou autres, ont toujours été d'une aide précieuse. Ses irruptions dans le bureau 34C pour évoquer des sujets aussi variés que la cohomologie des groupes, le choix d'une pâte thermique ou la dégustation d'un vin de noix maison auront certainement marqué les occupants dudit bureau.

D'ailleurs, les occupants du bureau 34C ne sont pas étrangers au bon déroulement de cette thèse : Marie-Angela (et ses « regarde dans la doc ! » devenus historiques), Kevin (maître incontesté des imitations animales divers et variées), mais aussi Clément et Titouan. Sans l'ambiance mêlant entraide, bonne humeur, caféine, insultes et contre-productivité qui règne dans ce bureau, c'est avec bien plus de difficultés que j'aurais surmonté les embûches inhérentes à la thèse. Il me faut aussi remercier Will, avec qui les séances de visionnage de nanars, de chasse aux zombies ou de grimpe ont toujours contenu la juste dose d'absurdité en rapport avec la coupe de cheveux.

Enfin, ces remerciements ne seraient pas complets sans souligner le soutien infaillible et les encouragements réguliers de ma famille, que ce soit pendant ma thèse ou tout au long de mes études. Je suis particulièrement reconnaissant à Johanne d'avoir supporté mes digressions mathématico-informatiques quotidiennes et mon humeur fluctuante pendant ces trois années.

TABLE DES MATIÈRES

INTRODUCTION

La géométrie des nombres, dont la fondation est attribuée à Minkowski avec la publication de l'ouvrage *Geometrie der Zahlen* en 1896 [Min96], est une branche de la théorie des nombres qui utilise des résultats de nature géométrique pour traiter des questions arithmétiques. Les objets d'étude principaux de cette théorie sont les *réseaux*, c'est-à-dire des maillages réguliers de points dans un espace euclidien. Bien que cette structure soit en apparence simple, elle contient en fait une richesse et une complexité étonnante.

De tout temps, ce sont les applications pratiques et théoriques qui ont fait naître la nécessité de mieux appréhender la notion de réseau. Parmi les résultats les plus anciens, citons le théorème des unités de Dirichlet, établi en 1889 [Dir89, p.639–644], qui s'appuie sur la structure de réseau associée à l'anneau des entiers d'un corps de nombres. Encore aujourd'hui, les réseaux sont au cœur de l'attention : ils sont par exemple des candidats idéaux pour fournir des schémas cryptographiques suffisamment tenaces pour résister à l'arrivée prochaine des ordinateurs quantiques [NIST16]. Ces dernières années, les calculs explicites en cohomologie des groupes ont connu un intérêt croissant et motivé l'étude des réseaux, notamment à travers les travaux de Soulé [Sou78], Lee et Szczarba [LS76 ; LS78], Ash, Gunnels et McConnell [AGM02 ; AGM08 ; AGM10 ; AGM11 ; AGM12 ; AGM15], Elbaz-Vincent, Gangl et Soulé [EVGS02 ; EVGS13] et Dutour Sikirić, Ellis et Schürmann [DSES11]. Ces travaux utilisent de manière cruciale la structure cellulaire de l'ensemble des réseaux, structure qui découle principalement de la théorie de la réduction de Voronoï [Vor08]. Les groupes de cohomologie sont des objets extrêmement complexes, dont la compréhension permettrait de résoudre une multitude de conjectures fondamentales, que ce soit en mathématiques [BFEH13 ; EV15] ou en physique théorique [DW90].

De la *Geometrie der Zahlen* aux réseaux algébriques

De manière plus formelle, un réseau est un $\mathbb{Z}$-module de rang maximal inclus dans un espace euclidien. En observant cette définition, il est naturel de se poser la question suivante : peut-on généraliser la théorie des réseaux en remplaçant $\mathbb{Z}$ par un autre anneau ? Plus précisément, peut-on remplacer $\mathbb{Z}$ par l'anneau des entiers d'un corps de nombres ? Cette question est loin d'être neuve : en 1907, Minkowski abordait déjà dans [Min07] des problèmes d'approximation diophantienne sur des anneaux d'entiers quadratiques imaginaires. Cependant, jusqu'aux travaux de Rogers et Swinnerton-Dyer [RSD58], la plupart des auteurs se restreignent au cas d'un anneau principal, évacuant de ce fait une large part des difficultés théoriques liées au passage de $\mathbb{Z}$ à un autre anneau. C'est essentiellement dans cet article que les bases de la théorie des *réseaux algébriques* [1] sont jetées, c'est-à-dire des réseaux sur l'anneau des entiers d'un corps de nombres. Parallèlement à ces travaux, Humbert [Hum39 ; Hum49] a développé entre 1939 et 1949 la théorie des *systèmes de formes définies positives* [2], qui généralisent les formes quadratiques définies positives. Il est bien connu que les réseaux euclidiens et les formes quadratiques définies positives sont les deux facettes d'une même pièce ; les systèmes de formes intronisés par Humbert jouent le même rôle pour les réseaux algébriques que les formes quadratiques définies positives pour les réseaux euclidiens.

Depuis, la théorie des réseaux algébriques et des formes de Humbert n'a eu de cesse de s'étendre et de se diversifier ; une multitude de résultats classiques ont été prolongés, modifiés ou reformulés. Les travaux de Watanabe et Masanori sur l'extension de la géométrie des nombres dans un cadre *adélique* [MW01 ; Wat00] ont mené la théorie vers un niveau de généralité encore supérieur. L'étude des formes de Humbert est aujourd'hui scindée en deux branches distinctes, l'une *multiplicative* et l'autre *additive*. La notion fondamentale de constante de Hermite a été généralisée dans ces deux contextes, principalement par Leibak [Lei05] dans le cadre additif et par Baeza, Icaza et Coulangeon [BI97 ; Bae+01] dans le cadre multiplicatif. Récemment, les efforts se sont concentrés vers l'adaptation de la théorie de la réduction de Voronoï [Vor08]. Du point de vue multiplicatif, les progrès réalisés sur ce sujet sont essentiellement dus à Coulangeon et Braun [Cou01 ; BC15]. Okuda, Yano, Watanabe et Hayashi [OY10 ; WYH13] sont les principaux instigateurs des dernières avancées sur la théorie de Voronoï algébrique et additive.

Questions algorithmiques classiques...

Les réseaux et les formes quadratiques ne sont pas des objets étudiés seulement pour leur richesse théorique ; ils offrent une complexité qui en font des structures passionnantes à analyser du point de vue des *méthodes algorithmiques*. Lagrange considérait déjà des questions effectives sur les réseaux en 1773 [DL73], tout comme Korkine et Zolotareff en 1877 [KZ77] et Voronoï en 1908 [Vor08]. Cependant, ce n'est réellement qu'en 1982 avec la publication de l'article fondateur de Lenstra, Lenstra et Lovász [LLL82] que l'étude informatique de ces

1. Même si cette terminologie n'apparaîtra qu'une vingtaine d'années plus tard dans [Cha83].
2. Qui sont simplement appelés les *formes de Humbert* de nos jours.

objets a pris son essor. Dans cet article, les auteurs décrivent un algorithme (communément appelé algorithme LLL) qui permet aujourd'hui [3] de calculer un conditionnement propice à l'attaque d'un problème algorithmique fondamental sur les réseaux : le *problème du plus court vecteur* (abrégé SVP [4]). Grâce à son caractère discret, un réseau possède toujours un plus court vecteur non nul ; le SVP consiste justement à déterminer un tel vecteur et/ou à en déterminer la longueur. Ce problème est au cœur de l'algorithmique des réseaux : maintes questions effectives concernant ces objets se réduisent au SVP ou à l'une de ses variantes. Si van Emde Boas [EB81] soupçonnait déjà ce problème d'être **NP**-dur en 1981, il a fallu attendre 1998 et les travaux novateurs de Ajtai [Ajt98] pour que cette conjecture soit quasiment [5] résolue. Néanmoins, la compréhension exhaustive de cette question est encore à l'heure actuelle un problème ouvert. L'algorithme LLL est la clé de voûte de nombre des meilleurs algorithmes connus pour traiter le SVP. Il est notamment utilisé par l'algorithme de Kannan [Kan83], qui est déterministe et de complexité super-exponentielle, et la méthode de Ajtai, Kumar et Sivakumar [AKS01], probabiliste mais de complexité « seulement » exponentielle.

Plus généralement, l'algorithme LLL permet d'obtenir des bases particulières de réseaux, les bases *réduites*. Une base est dite réduite si elle possède des propriétés géométriques proches de celles d'une base orthonormée d'un espace euclidien. Il n'existe pas un concept universel de réduction ; une multitude de notions coexistent, hiérarchisées en fonction de l'exigence des propriétés qui les définissent et de la complexité des algorithmes permettant de les satisfaire [Ngu07, §3.3, p.47–51]. C'est à Lagrange [DL73] que l'on doit la notion de réduction la plus ancienne et la plus naturelle, mais cette dernière n'est malheureusement définie qu'en dimension 2. Mathématiquement parlant, les réductions les plus inspectées sont celles de Minkowski [Min96] et de Hermite, Korkine et Zolotareff [KZ77], qui sont des réductions fortes mais difficiles à obtenir. La théorie de la réduction de Voronoï [Vor08] est elle aussi d'un intérêt théorique incontestable, mais elle n'est à l'heure actuelle effective que jusqu'en dimension 8 [Bar57 ; JC93 ; DSSV07]. Au contraire, la populaire réduction au sens de Lenstra, Lenstra et Lovász est calculable en temps polynomial mais propose des bases d'une qualité moindre. Les avancées sur la réduction de réseaux sont motivées par de nombreuses applications [NV10], allant de la cryptanalyse à la théorie des nombres, en passant par la factorisation polynomiale et l'optimisation linéaire en nombres entiers.

Au-delà de ces problématiques très spécifiques, une autre question dépassant largement le cadre des réseaux mérite une attention particulière : le problème de l'isométrie. Il s'agit de décider si deux réseaux partagent les mêmes caractéristiques algébriques et géométriques. Le problème de l'isométrie de réseaux est la spécification dans le langage des réseaux de la question très générale qui consiste à décider si deux structures algébriques, géométriques et/ou combinatoires sont isomorphes. La version la plus connue et la plus étudiée de cette question est celle de l'isomorphisme de graphes, à tel point qu'elle est devenue centrale en théorie

3. Cette application n'est pas mentionnée dans l'article de Lenstra, Lenstra et Lovász, dont le but initial était de proposer un algorithme efficace de factorisation de polynômes entiers.

4. Pour *Shortest Vector Problem*.

5. Plus précisément, Ajtai a montré que le SVP est **NP**-dur en norme l_2 sous des réductions probabilistes.

de la complexité. C'est en effet l'un des rares problèmes algorithmiques « vraisemblablement facile » dont on ne connaisse pas d'algorithme de résolution efficace [6]. Depuis sa résolution sous-exponentielle par Babai et Luks [BL83] et Zemlyachenko, Korneenko et Tyshkevich [ZKT85] jusqu'à la proposition d'algorithme quasi-polynomial [Bab15] de Babai, ce problème est la cible d'une kyrielle de recherches réparties sur plus de quarante ans.

Si notre compréhension du problème de l'isomorphisme de graphes s'accroît au fil des années, ce n'est pas le cas pour l'isométrie de réseaux. Du point de vue de la complexité, la panoplie de résultats dont on dispose est modeste. Citons tout de même les travaux de Haviv et Regev [HR14], dans lesquels un algorithme théorique optimal permettant d'énumérer toutes les isométries entre deux réseaux est proposé. Haviv et Regev ont aussi mis en évidence dans ce même article que l'isométrie de réseaux est, comme l'isomorphisme de graphes, un problème « vraisemblablement facile ». D'autre part, Dutour Sikirić, Schürmann et Vallentin [DSSV09] ont prouvé que le problème de l'isométrie de réseaux est au moins aussi difficile que le problème de l'isomorphisme de graphes. Concernant les algorithmes pratiques, la méthode de Plesken et Souvignier [PS97] est encore aujourd'hui la plus efficace et la plus aisément accessible.

...et généralisation aux réseaux algébriques

Une proportion considérable des résultats théoriques sur les réseaux et les formes quadratiques possèdent un équivalent algorithmique, parfois partiel ou approché. De plus, il est courant de disposer d'implantations de ces algorithmes qui soient à la fois performantes et largement disponibles. L'exemple de l'algorithme LLL illustre parfaitement cette situation : outre le fait que ce soit une version effective de l'inégalité de Hermite, une multitude de logiciels et de librairies en proposent des implantations compétitives (comme `PARI/gp` [PARI/gp] et `MAGMA` [MAGMA]). Le constat est tout autre pour les réseaux algébriques et les formes de Humbert : maints algorithmes destinés aux réseaux euclidiens ne sont pas généralisés et/ou implantés pour les réseaux algébriques. Par exemple, le système `MAGMA` propose quelques structures et fonctions dédiées aux réseaux algébriques, mais celles-ci sont soit élémentaires, soit limitées à des situations très particulières.

Les travaux de Fieker et Pohst [FP96] font partie des premiers résultats remarquables concernant l'algorithmique des réseaux algébriques. Cet article propose une tentative d'extension de deux des algorithmes les plus importants sur les réseaux : l'algorithme LLL et l'algorithme de Fincke et Pohst [FP85], qui permet d'énumérer tous les vecteurs courts d'un réseau. Soulignons tout de même que certaines méthodes antérieures aux travaux de Fieker et Pohst et dédiées aux modules de type fini sur un anneau de Dedekind (notamment dues à Bosma et Pohst [BP91] et Cohen [Coh96]) sont utilisables sur les réseaux algébriques. Plus récemment, Fieker et Stehlé [FS10] ont mis en avant une version fonctionnelle, maîtrisée et polyvalente de l'algorithme LLL adaptée aux réseaux algébriques. Cependant, les environnements mathématiques les plus populaires, comme `PARI/gp` et `MAGMA`, ne proposent d'implantations (même naïves) ni pour

6. De manière plus formelle, on ne connaît pour ce problème ni de preuve de **NP**-complétude, ni d'algorithme de résolution polynomial.

l'algorithme de Fieker et Pohst, ni pour celui de Fieker et Stehlé. L'algorithme LLL est donc l'un des algorithmes propagés de manière abstraite aux réseaux algébriques, mais dont les implantations sont encore manquantes à l'heure actuelle. Les aspects effectifs de la théorie de la réduction de Voronoï [Vor08] ont quant à eux été généralisés par Watanaba, Yano et Hayashi [WYH13] et Braun, Coulangeon, Nebe et Schönnenbeck [Bra+15].

Au delà de ces exemples de méthodes classiques *théoriquement* généralisées pour les réseaux algébriques, tout un pan de l'algorithmique des réseaux n'a peu ou pas été étudié sous cet angle. Il n'existe pas d'algorithme efficace permettant de traiter le problème de l'isométrie de réseaux algébriques ; en particulier, la méthode de Plesken et Souvigier [PS97] n'est à l'heure actuelle pas adaptée pour prendre en charge ces objets. Remarquons néanmoins que des problèmes d'isométries sur des familles de réseaux plus larges que les réseaux « classiques » ont été considérés du point de vue algorithmique par Braun, Coulangeon, Nebe et Schönnenbeck [Bra+15]. D'autre part, les algorithmes de Kannan [Kan83] et Ajtai, Kumar et Sivakumar [AKS01] permettant de résoudre le SVP ne sont pas optimisés pour les réseaux algébriques.

Plan et contributions

Cette thèse se compose de cinq chapitres. Les chapitres I et IV peuvent être lus séparément ; le chapitre III fait régulièrement appels aux notions et résultats présentés dans le chapitre II. Le chapitre V détaille les implantations des différents algorithmes explicités, et ne peut donc pas être abordé sans une lecture préalable des chapitres précédents.

Nous présentons dans le chapitre I une adaptation de l'algorithme LLL pour les réseaux algébriques sur un anneau quadratique imaginaire et euclidien. Cet algorithme est essentiellement dû à Napias [Nap96], mais nous y avons ajouté plusieurs optimisations. Nous proposons aussi une analyse heuristique inédite des « résultats moyens » qu'il renvoie, en nous basant notamment sur les travaux de Schneider, Buchmann et Lindmer [SBL10]. Détailler cet algorithme nous donne l'occasion d'aborder dans un cadre algébrique simple une première généralisation de la notion de réseau euclidien. Nous montrons en particulier que la plupart des résultats classiques se prolongent facilement dans cette situation. Ce chapitre est essentiellement introductif et élémentaire, et peut être vu comme un échauffement avant l'exposition de notions plus avancées.

Le chapitre II est consacré à l'introduction des notions de réseaux algébriques et de formes de Humbert. Nous prenons le soin de nous placer dans une situation aussi générale que possible. Si plusieurs des résultats mis en avant de ce chapitre sont connus, nous nous attachons à les présenter dans un cadre et un langage unifiés. Ceci nous donne l'occasion d'étendre et préciser plusieurs travaux, notamment les résultats de Leibak [Lei05] sur la constante de Hermite généralisée dans un contexte additif. Nous établissons de plus de manière détaillée et inédite la correspondance qui relie les formes de Humbert et les réseaux algébriques.

Nous nous intéressons à l'algorithme de Plesken et Souvignier [PS97] dans le chapitre III. Plus précisément, nous détaillons des modifications à apporter à cette méthode lui autorisant la prise en charge des réseaux algébriques et des formes de Humbert, et ceci sans passer par

l'identification usuelle d'un réseau algébrique à un réseau euclidien, utilisée par exemple dans [Bra+15, §7.2]. En exhibant un algorithme performant permettant de résoudre le problème de l'isométrie entre réseaux algébriques, nous comblons ainsi une des lacunes majeures de l'algorithmique de ces objets. Au prix d'ajustements mineurs, la méthode présentée permet de plus de déterminer le groupe des automorphismes d'un réseau algébrique ; c'est d'ailleurs sous cet angle que nous développons ce chapitre. En guise d'illustration, nous montrons comment traiter le problème de la G-équivalence entre formes quadratiques et entre formes de Humbert. Cette illustration englobe notamment le cas de l'équivalence de formes quadratiques modulo certains groupes de congruence.

Dans le chapitre IV, nous étudions plus en détails la complexité du problème de l'isométrie entre réseaux euclidiens, encore mal compris à l'heure actuelle. Nous établissons en particulier une réduction inédite entre une forme faible de cette question et le problème de l'isomorphisme de graphes. Utilisée conjointement avec les avancées récentes de Babai [Bab15], cette réduction nous permet de mettre en lumière le fait que la complexité des algorithmes actuellement utilisés (comme l'algorithme de Plesken et Souvignier [PS97] ou celui, théorique, de Haviv et Regev [HR14]) réside essentiellement dans une phase de précalcul.

Finalement, le chapitre V rassemble des remarques et astuces concernant les implantations des algorithmes présentés et les résultats expérimentaux obtenus. Nous avions en effet à cœur de ne pas nous contenter de proposer des méthode théoriques, mais aussi de détailler des implantations efficaces de ces dernières. Les codes que nous avons développés utilisent largement les fonctionnalités offertes par la bibliothèque `PARI/gp` [PARI/gp]. Nous montrons notamment dans ce chapitre que les réductions obtenues dans le chapitre précédent se transposent en des algorithmes parfois plus efficaces que les méthodes actuellement utilisées.

ALGORITHME LLL SUR UN CORPS QUADRATIQUE IMAGINAIRE ET EUCLIDIEN

Sommaire

I.1 Introduction

Nous abordons dans ce chapitre une première généralisation de la notion de réseau sur d'autres structures algébriques que l'anneau $\mathbb{Z}$. Une proportion considérable des résultats théoriques sur les réseaux utilisent à la fois la principalité de $\mathbb{Z}$ et son caractère discret (vu comme sous-ensemble de $\mathbb{R}$). Dès lors, sous quelles hypothèses est-il possible d'obtenir des résultats similaires sur d'autres anneaux ? En suivant cette réflexion, il est naturel de voir apparaître les anneaux d'entiers quadratiques imaginaires et euclidiens, qui, comme $\mathbb{Z}$, sont à la fois discrets et principaux.

Cette étude nous conduira rapidement vers l'une des questions fondamentales concernant l'algorithmique des réseaux : étant donné un réseau, est-il possible d'évaluer la longueur d'un des plus courts vecteur du réseau ? Et est-il possible de calculer l'un de ces plus courts vecteurs ? Si Ajtai [Ajt96 ; Ajt98] a prouvé dans une série d'importants développements que ces problèmes algorithmiques sont **NP**-complets (en norme l_2 et sous des réductions probabilistes), il est possible depuis les travaux de Lenstra, Lenstra et Lovász [LLL82] de les résoudre approximativement mais en un temps raisonnable. Nous étudions ici les réponses apportées à ces questions sur d'autres structures algébriques que $\mathbb{Z}$, notamment par Napias [Nap96], tout en suggérant quelques améliorations et applications. Dans la continuité des travaux de Schneider, Buchmann et Linder [SBL10], nous proposons enfin une analyse heuristique des résultats renvoyés par l'algorithme présenté. Puisque ce chapitre se veut élémentaire et introductif, nous prenons le soin d'amplement détailler les démonstrations.

I.2 Corps de nombres admissibles et réseaux algébriques

Dans tout ce chapitre et pour tout $n \geqslant 1$, le $\mathbb{C}$-espace vectoriel $\mathbb{C}^n$ est équipé de son produit scalaire hermitien usuel, défini pour tous $x := (x_1, \ldots, x_n), y := (y_1, \ldots, y_n) \in \mathbb{C}^n$ par

$$\langle x \,|\, y \rangle := \overline{x_1} y_1 + \cdots + \overline{x_n} y_n,$$

où $\overline{x_i}$ désigne le conjugué complexe de x_i. La norme hermitienne associée à ce produit scalaire est notée $\|\cdot\|$. Enfin, on désigne par $|\cdot|$ le module complexe usuel.

I.2.1 Corps de nombres admissibles

Soient K un corps de nombres et $\mathcal{O}_K$ son anneau d'entiers. Dans l'optique d'introduire la notion de réseau « sur $\mathcal{O}_K$ » dans un contexte aussi élémentaire que possible, il est souhaitable que $\mathcal{O}_K$ possède des propriétés similaires à celles de $\mathbb{Z}$. Il est en particulier naturel d'exiger que $\mathcal{O}_K$ soit un ensemble discret. Rappelons que si le couple (r,s) désigne la signature de K, on identifie $\mathcal{O}_K$ à une partie discrète de $\mathbb{R}^r \times \mathbb{C}^s$ (voir [Sam67, prop.2, p.69] et plus généralement le Chapitre II). Ainsi :

- Si $(r,s) = (1,0)$, on a $K = \mathbb{Q}$ et $\mathcal{O}_K = \mathbb{Z}$, qui est une partie discrète de $\mathbb{R}$. C'est le cadre d'étude de la théorie classique des réseaux.

- Si $(r,s) = (0,1)$, K est un corps quadratique imaginaire et $\mathcal{O}_K$ est une partie discrète de $\mathbb{C}$. Cette situation est la « généralisation complexe » de la situation précédente.
- Les autres cas sont plus délicats à traiter : $\mathcal{O}_K$ est une partie discrète d'un objet qui n'est de dimension 1 ni sur $\mathbb{R}$, ni sur $\mathbb{C}$, ce qui complexifie considérablement l'introduction des notions théoriques qui vont suivre.

Nous supposerons donc que la signature de K est $(0,1)$. Autrement dit, K est un corps de nombres quadratique imaginaire, nécessairement de la forme $K = \mathbb{Q}(i\sqrt{D})$ avec $D \in \mathbb{N}_{>0}$ sans facteurs carrés. Dans tout ce chapitre, nous voyons K comme un sous-corps du corps $\mathbb{C}$ des nombres complexes. On note $\mathcal{O}_K$ l'anneau des entiers algébriques de K et $\mathcal{O}_K^\times$ le sous-groupe des unités de $\mathcal{O}_K$. Nous utiliserons régulièrement la propriété *d'unimodularité* de ces corps :

Définition I.2.1 *Un corps de nombres quadratique (imaginaire ou réel) K est dit unimodulaire*[1] *si*

$$\mathcal{O}_K^\times \subset \{z \in \mathbb{C} \,:\, |z| = 1\}. \tag{P1}$$

Proposition I.2.2 *Un corps de nombres quadratique est unimodulaire si et seulement s'il est imaginaire.*

Démonstration. Un corps quadratique réel ne peut pas être unimodulaire. En effet, d'après le théorème des unités de Dirichlet [Sam67, thm.1, p.72], si K est réel, le groupe $\mathcal{O}_K^\times$ n'est pas fini, et ne peut donc pas être contenu dans $\{x \in \mathbb{R} \,:\, |x| = 1\} = \{\pm 1\}$.

Si $K = \mathbb{Q}(i\sqrt{D})$ avec $D \in \mathbb{N}_{>0}$ sans facteurs carrés, d'après [Sam67, p.76] on a

$$\mathcal{O}_K^\times = \begin{cases} \{\pm 1, \pm i\} & \text{si } D = 1, \\ \{e^{\frac{ik\pi}{3}} \,:\, 0 \leqslant k \leqslant 5\} & \text{si } D = 3, \\ \{-1, +1\} & \text{sinon,} \end{cases}$$

ce qui montre en particulier que K est unimodulaire. □

Nous avons ainsi distingués les corps K pour lesquels $\mathcal{O}_K$ peut raisonnablement être considéré comme un ensemble discret. Comme nous l'avons déjà remarqué, de nombreux résultats sur les réseaux utilisent de manière directe ou indirecte[2] le fait que $\mathbb{Z}$ soit un anneau euclidien. Cette propriété est souvent exploitée sous la forme suivante :

$$\textit{Pour tout } x \in \mathbb{R}, \textit{ il existe } y \in \mathbb{Z} \textit{ tel que } |x - y| < 1.$$

Nous demandons au corps de nombres K de vérifier une propriété analogue :

Définition I.2.3 *Un corps de nombres K quadratique imaginaire est dit géométriquement euclidien si*

$$m_K := \sup_{x \in \mathbb{C}} \inf_{y \in \mathcal{O}_K} |x - y|^2 < 1 \tag{P2}$$

1. C'est un abus de langage ; on devrait plutôt dire que $\mathcal{O}_K$ *est unimodulaire*.
2. Notamment car un anneau euclidien est en particulier principal.

Il s'avère que cette propriété est très restrictive :

Proposition I.2.4 *Soit $D \in \mathbb{N}_{>0}$ sans facteurs carrés. Le corps de nombres $K = \mathbb{Q}(i\sqrt{D})$ est géométriquement euclidien si et seulement si $D \in \{1, 2, 3, 7, 11\}$.*

Démonstration. D'après [Sam67, p.43], l'anneau des entiers de K est $\mathbb{Z} + \omega_D\mathbb{Z}$, où

$$\omega_D := \begin{cases} i\sqrt{D} & \text{si } D \equiv 1, 2 \mod 4, \\ \frac{1+i\sqrt{D}}{2} & \text{sinon.} \end{cases}$$

Soit $x \in \mathbb{C}$. Par un jeu de translations et de symétries, on peut supposer sans perte de généralité que x est dans le demi-parallélogramme fondamental T de $\mathcal{O}_K$ (grisé sur la Figure I.1). Ce triangle T est l'enveloppe convexe de $\{0, 1, \omega_D\}$.

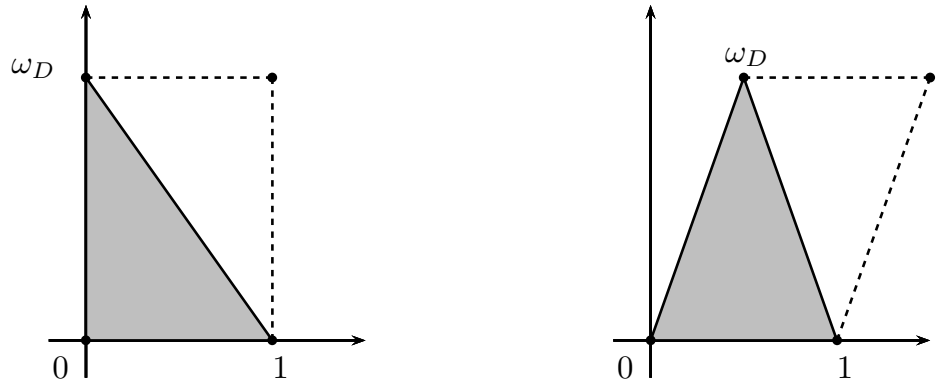


Fig. I.1 – Parallélogramme fondamental de $\mathcal{O}_K$ pour $d \equiv 1, 2 \mod 4$ (à gauche) et $d \equiv 3 \mod 4$ (à droite).

Soient Ω le centre du cercle inscrit $\mathscr{C}$ du triangle T (voir la Figure I.2) et r son rayon. On note α, β, γ les milieux respectifs des segments $[\omega_D; 1]$, $[0; \omega_D]$ et $[0; 1]$. Remarquons que dans le cas où $D \equiv 1, 2 \mod 4$, les points α et Ω sont confondus. On obtient ainsi une partition de T (présentée sur la Figure I.3).

Supposons que x appartienne à l'enveloppe convexe de $\{0, \gamma, \Omega, \beta\}$. Puisque $0, 1$ et ω_D sont dans $\mathscr{C}$, on a

$$\begin{cases} 1 \leqslant 2r, \\ |\omega_D| \leqslant 2r, \end{cases}$$

ce qui entraîne

$$\begin{cases} |\gamma| \leqslant r, \\ |\beta| \leqslant r. \end{cases}$$

Par conséquent, β et γ appartiennent au disque de rayon r centré en 0. Ainsi, l'enveloppe convexe de $\{0, \gamma, \Omega, \beta\}$ est inclue dans ce disque. Puisque x est dans cette enveloppe, $|x| \leqslant r$.

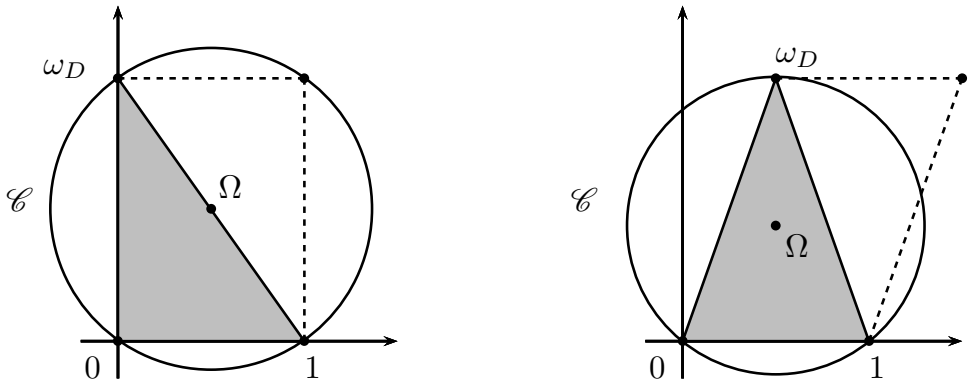


Fig. I.2 – Centre du cercle inscrit du demi-parallélogramme fondamental de $\mathcal{O}_K$ pour $d \equiv 1,2 \mod 4$ (à gauche) et $d \equiv 3 \mod 4$ (à droite).

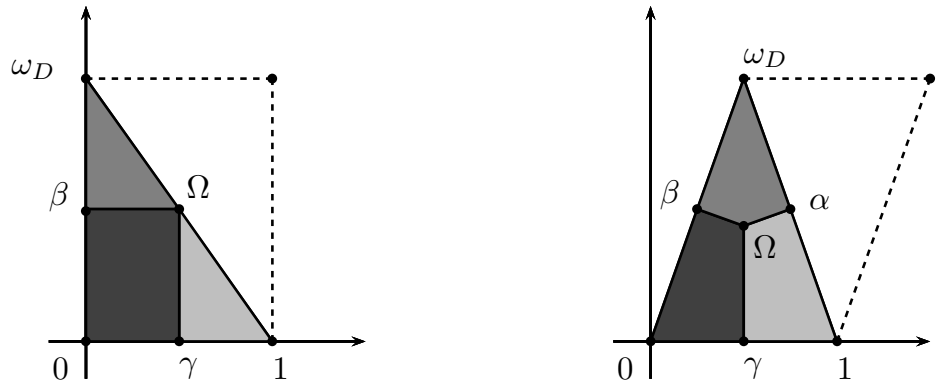


Fig. I.3 – Partition du demi-parallélogramme fondamental de $\mathcal{O}_K$ pour $d \equiv 1,2 \mod 4$ (à gauche) et $d \equiv 3 \mod 4$ (à droite).

En appliquant cet argument aux autres éléments du découpage effectué, on obtient finalement que pour tout $x \in \mathbb{C}$:

$$\inf_{y \in \mathcal{O}_K} |x-y|^2 \leqslant r^2.$$

Pour $x = \Omega$ dans la situation précédemment décrite, cette borne inférieure est atteinte. Par conséquent :

$$\sup_{x \in \mathbb{C}} \inf_{y \in \mathcal{O}_K} |x-y|^2 = r^2.$$

Reste donc à déterminer la valeur de r^2. Dans le cas où $D \equiv 1,2 \mod 4$, on obtient par une simple application du théorème de Pythagore que $r^2 = \frac{D+1}{4}$. On a donc $r^2 < 1$ si et seulement si $D \in \{1,2\}$.

Supposons maintenant que $D \equiv 3 \mod 4$. Il nous faut déterminer $|\Omega|^2$. On peut écrire $\Omega = \frac{1}{2} + iw$ avec $w \in \mathbb{R}$. On a donc

$$|\Omega|^2 = |\Omega - \omega_D|^2 = |\Omega - 1|^2,$$

ce qui entraîne que $w = \frac{D-1}{4\sqrt{D}}$. Par conséquent, on a $r^2 = |\Omega|^2 = \frac{(D+1)^2}{16D}$. Ainsi, $r^2 < 1$ si et seulement si $D \in \{3, 7, 11\}$, ce qui termine la preuve. □

L'emploi du terme *géométriquement euclidien* est justifié par la proposition suivante. Exceptionnellement, on ne suppose pas que K est un corps de nombres quadratique. On note N_K la norme de $K/\mathbb{Q}$.

Proposition I.2.5 *Soit K un corps de nombres. Le minimum euclidien de K, défini comme :*

$$m_K := \sup_{x \in K} \inf_{y \in \mathcal{O}_K} |\mathrm{N}_K(x-y)|$$

vérifie les propriétés suivantes :

- *Si $m_K < 1$, $\mathcal{O}_K$ est euclidien pour $|\mathrm{N}_K(\cdot)|$. On dit alors que*[3] *K est fortement norme-euclidien.*
- *Si $m_K > 1$, $\mathcal{O}_K$ n'est pas norme-euclidien.*

Démonstration.

- Supposons que $m_K \leqslant 1$. Puisque $\mathcal{O}_K$ est une partie discrète et fermée de K pour la topologie induite par $|\mathrm{N}_K(\cdot)|$, pour tout $x \in K$, il existe $y_x \in \mathcal{O}_K$ tel que

  $$\inf_{y \in \mathcal{O}_K} |\mathrm{N}_K(x-y)| = |\mathrm{N}_K(x-y_x)|.$$

  Soient $\alpha, \beta \in \mathcal{O}_K$, avec β non nul. Posons $x = \alpha\beta^{-1}$. D'après ce qui précède et par hypothèse, il existe $y_x \in \mathcal{O}_K$ tel que

  $$|\mathrm{N}_K(x-y_x)| < 1.$$

  En remarquant que

  $$|\mathrm{N}_K(\alpha - \beta y_x)| = |\mathrm{N}_K(\beta)| \cdot |\mathrm{N}_K(x-y_x)|.$$

  on obtient la norme-euclidianité recherchée.
- On commence par remarquer que

  $$1 < m_K \leqslant \inf\{k > 0 \,:\, \forall\, x \in K, \exists\, y \in \mathcal{O}_K \,:\, |\mathrm{N}_K(x-y)| < k\}.$$

  Puisque K est le corps des fractions de $\mathcal{O}_K$, cette inégalité entraîne l'existence de $\varepsilon > 0$ et de $\alpha, \beta \in \mathcal{O}_K$ avec $\beta \neq 0$ tels que pour tout $y \in \mathcal{O}_K$:

  $$|\mathrm{N}_K(\alpha - \beta y)| \geqslant (1+\varepsilon)|\mathrm{N}_K(\beta)| > |\mathrm{N}_K(\beta)|.$$

  Ainsi, $|\mathrm{N}_K(\cdot)|$ ne peut pas être un stathme euclidien. □

3. Comme pour l'unimodularité, c'est un abus de langage ; on devrait plutôt dire que *$\mathcal{O}_K$ est fortement norme-euclidien*.

Le cas $m_K = 1$ est critique : il existe des corps de nombres qui ne sont pas fortement norme-euclidiens, mais dont l'anneau d'entiers est norme-euclidien. Pour une étude détaillée de ces questions d'euclidianité, nous renvoyons le lecteur vers [Lez12]. Si K est quadratique imaginaire, on a $\mathrm{N}_K(x) = |x|^2$ pour tout $x \in K$, et puisque K dense dans $\mathbb{C}$, les notions d'euclidianité géométrique et de norme-euclidianité sont confondues.

Les corps $K = \mathbb{Q}(i\sqrt{D})$ avec $D \in \{1, 2, 3, 7, 11\}$ seront dits *admissibles*. Leur structure est résumée dans la Figure I.4.

D	1	2	3	7	11
$\mathcal{O}_K$	$\mathbb{Z}+i\mathbb{Z}$	$\mathbb{Z}+i\sqrt{2}\mathbb{Z}$	$\mathbb{Z}+\frac{1+i\sqrt{3}}{2}\mathbb{Z}$	$\mathbb{Z}+\frac{1+i\sqrt{7}}{2}\mathbb{Z}$	$\mathbb{Z}+\frac{1+i\sqrt{11}}{2}\mathbb{Z}$
$\mathcal{O}_K^\times$	$\{\pm 1, \pm i\}$	$\{\pm 1\}$	$\left\{e^{\frac{ik\pi}{3}} \ : \ 0 \leqslant k \leqslant 5\right\}$	$\{\pm 1\}$	$\{\pm 1\}$
m_K	$1/2$	$3/4$	$1/3$	$4/7$	$9/11$

Fig. I.4 – Structure des corps de nombres admissibles.

I.2.2 Réseaux algébriques

Sauf mention du contraire, K désigne dans tout ce paragraphe un corps de nombres quadratique imaginaire, non nécessairement admissible.

I.2.2.1 Généralités

Les réseaux algébriques, que nous appellerons aussi $\mathcal{O}_K$-réseaux, étendent au cadre imaginaire la notion de réseau euclidien.

Définition I.2.6 *Un réseau algébrique de rang n sur K est un sous-groupe Λ de $\mathbb{C}^n$ pour lequel il existe $\mathcal{B} := (b_1, \ldots, b_n)$ une $\mathbb{C}$-base de $\mathbb{C}^n$ telle que*

$$\Lambda = \mathcal{O}_K b_1 \oplus \cdots \oplus \mathcal{O}_K b_n.$$

La famille $\mathcal{B}$ est appelée une base de Λ.

Cette définition est similaire à celle donnée dans le contextes euclidien classique. Nous nous restreignons aux réseaux algébriques qui sont des $\mathcal{O}_K$-modules *libres* car nous supposerons rapidement que K est un corps admissible, ce qui entraîne en particulier que $\mathcal{O}_K$ est un anneau principal (car euclidien). Néanmoins, en toute généralité, il nous faudrait plutôt considérer des objets de la forme

$$\mathfrak{a}_1 b_1 \oplus \cdots \oplus \mathfrak{a}_n b_n,$$

où les $\mathfrak{a}_i$ sont des idéaux fractionnaires de K. C'est d'ailleurs ce que nous ferons dans les prochains chapitres.

Un $\mathcal{O}_K$-réseau est en particulier un $\mathcal{O}_K$-module libre de rang fini n. La définition précédente n'est pas celle que l'on retrouve parfois dans le contexte classique (où un réseau de $\mathbb{R}^n$ est défini comme un sous-groupe discret maximal). Dans la mesure où, toujours dans le cas classique, cette définition est équivalente à l'existence d'une base, et que c'est sous cette forme qu'on implante un réseau, nous nous contenterons (dans ce chapitre) de la formulation précédente. Soulignons néanmoins la propriété suivante, qui est fondamentale.

Proposition I.2.7 *Un $\mathcal{O}_K$-réseau de $\mathbb{C}^n$ est une parte discrète et fermée de $\mathbb{C}^n$ (pour la topologie induite par le produit scalaire hermitien usuel de $\mathbb{C}^n$).*

Les sous-groupes vérifiant la Définition I.2.6 sont parfois appelés réseaux algébriques *de rang maximal*. Cette terminologie étant ambiguë dans le cas général, nous préférons introduire la notion de réseau *relatif* :

Définition I.2.8 *On appelle $\mathcal{O}_K$-réseau relatif de $\mathbb{C}^n$ tout $\mathcal{O}_K$-réseau Λ d'un sous-$\mathbb{C}$-espace vectoriel E de $\mathbb{C}^n$. Si $\dim_{\mathbb{C}}(E) = m$, on dit que Λ est de rang m.*

Comme précédemment, un $\mathcal{O}_K$-réseau relatif de $\mathbb{C}^n$ de rang m est un $\mathcal{O}_K$-module libre de rang m. De plus, un $\mathcal{O}_K$-réseau est un $\mathcal{O}_K$-réseau relatif de rang maximal n. Réciproquement, un $\mathcal{O}_K$-réseau relatif de $\mathbb{C}^n$ peut être vu comme un $\mathcal{O}_K$-réseau de rang maximal de manière immédiate. C'est pourquoi dans la suite, nous nous restreindrons sauf mention du contraire aux réseaux algébriques de rang maximal.

Un réseau algébrique possède une infinité de bases ; le passage d'une base à une autre fonctionne comme dans le cas classique. Nous appelons *base standard de* $\mathbb{C}^n$ la $\mathbb{C}$-base

$$\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \cdots, \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

Proposition I.2.9 *Soit Λ un $\mathcal{O}_K$-réseau de $\mathbb{C}^n$ de base $\mathcal{B}$. Une $\mathbb{C}$-base $\mathcal{B}'$ de $\mathbb{C}^n$ est une base de Λ si et seulement s'il est possible de passer de $\mathcal{B}$ à $\mathcal{B}'$ par un élément de $\mathrm{GL}_n(\mathcal{O}_K)$, c'est-à-dire s'il existe une matrice $U \in \mathrm{GL}_n(\mathcal{O}_K)$ telle que $B' = BU$, où B et B' sont les matrices de $\mathcal{B}$ et $\mathcal{B}'$ dans la base standard de $\mathbb{C}^n$.*

À titre de comparaison, les changements de bases d'un réseau euclidien de $\mathbb{R}^n$ se font par les éléments de $\mathrm{GL}_n(\mathbb{Z})$; il est donc naturel de voir apparaître le groupe $\mathrm{GL}_n(\mathcal{O}_K)$ lors du passage de $\mathbb{Z}$ à $\mathcal{O}_K$.

I.2.2.2 Minimum, vecteurs minimaux et déterminant

La structure hermitienne de $\mathbb{C}^n$ permet de définir plusieurs constantes fondamentales d'un réseau algébrique. On fixe Λ un $\mathcal{O}_K$-réseau de $\mathbb{C}^n$.

Minimum et vecteurs minimaux. La définition du minimum[4] de Λ est identique à celle employée dans le contexte euclidien.

Définition I.2.10 *Le minimum d'un réseau algébrique Λ est*

$$m(\Lambda) := \inf_{x \in \Lambda \setminus \{0\}} \|x\|^2.$$

Un élément $x \in \Lambda$ tel que $\|x\|^2 = m(\Lambda)$ est appelé un vecteur minimal de Λ. L'ensemble des vecteurs minimaux de Λ est noté $S(\Lambda)$.

Puisque Λ est une partie discrète et fermée de $\mathbb{C}^n$, $m(\Lambda)$ est toujours atteint et $S(\Lambda)$ est une partie finie non vide de $\mathbb{C}^n$. De plus, $|S(\Lambda)|$ est toujours divisible par $|\mathcal{O}_K^\times|$: si $x \in S(\Lambda)$ et $\lambda \in \mathcal{O}_K^\times$, alors $\lambda x \in S(\Lambda)$ par hypothèse d'unimodularité (P1). En particulier, $|S(\Lambda)|$ est toujours pair.

Dans la suite, nous nous intéresserons plus spécifiquement à la grandeur $m(\Lambda)$. Nous mettrons en valeur un algorithme qui, comme l'algorithme LLL [LLL82] pour les réseaux euclidiens, permet d'approximer $m(\Lambda)$ en obtenant un vecteur quasi-minimal de Λ. Nous expliquerons aussi via la notion de déterminant pourquoi cet algorithme permet d'obtenir une base de Λ dont l'orthogonalité est contrôlée.

Déterminant. Soit $\mathcal{B} := (b_1, \dots, b_n)$ une famille de vecteurs de $\mathbb{C}^n$. Le déterminant de $\mathcal{B}$, noté $\Delta(\mathcal{B})$, est la grandeur

$$\Delta(\mathcal{B}) := |\det_{\mathcal{B}_0}(\mathcal{B})|^2,$$

où $\mathcal{B}_0$ est une $\mathbb{C}$-base orthonormée de $\mathbb{C}^n$. Le discriminant ne dépend pas de la base orthonormée choisie, puisque le passage d'une base orthonormée à une autre se fait par une matrice unitaire. En particulier, nous prendrons toujours pour $\mathcal{B}_0$ la base standard de $\mathbb{C}^n$.

Définition I.2.11 *On appelle déterminant de Λ, noté $\Delta(\Lambda)$, le déterminant d'une base de Λ.*

C'est ici que la propriété d'unimodularité (P1) intervient : en vertu de la Proposition I.2.9 et de l'unimodularité de K, le déterminant de Λ ne dépend pas non plus de la base du réseau choisie pour le calculer puisque

$$\mathrm{GL}_n(\mathcal{O}_K) = \left\{A \in \mathrm{M}_n(\mathcal{O}_K) \,:\, \det(A) \in \mathcal{O}_K^\times\right\} \subset \{A \in \mathrm{M}_n(\mathbb{C}) \,:\, |\det(A)| = 1\}.$$

Donnons une interprétation du déterminant d'un réseau algébrique en terme de produit scalaire. Si $\mathcal{B} := (b_1, \dots, b_m)$ est une famille de $\mathbb{C}^n$, on appelle matrice de Gram de $\mathcal{B}$ la matrice hermitienne de taille m définie pour tous $1 \leqslant i, j \leqslant m$ par

$$\mathrm{Gram}(\mathcal{B})_{i,j} := \langle b_i \,|\, b_j \rangle.$$

On appelle de déterminant de Gram de $\mathcal{B}$ le déterminant de sa matrice de Gram.

4. Les définitions diffèrent suivant les auteurs ; on définit parfois le minimum comme $\inf_{x \in \Lambda \setminus \{0\}} \|x\|$. Le même problème se pose pour les définitions du discriminant et déterminant.

Proposition I.2.12 *Le déterminant d'un réseau algébrique Λ de base $\mathcal{B}$ est égal au déterminant de Gram de $\mathcal{B}$.*

Démonstration. Soit B la matrice de $\mathcal{B}$ dans la base standard de $\mathbb{C}^n$. Puisque cette base est orthonormée, on peut écrire

$$\mathrm{Gram}(\mathcal{B}) = B\overline{B}^{\intercal},$$

ce qui entraîne

$$\det(\mathrm{Gram}(\mathcal{B})) = |\det(B)|^2.$$

Comme $\Delta(\Lambda) = |\det(\mathcal{B})|^2 = |\det(B)|^2$, le résultat est démontré. □

I.2.3 Inégalités géométriques classiques

Nous prouvons ici deux inégalités classiques qui permettent de majorer ou minorer les constantes définies dans le paragraphe précédent. On fixe Λ un $\mathcal{O}_K$-réseau de $\mathbb{C}^n$.

I.2.3.1 Inégalité de Hadamard

Commençons par étendre l'inégalité de Hadamard [Mar03, §2.1, p.37–39] aux réseaux algébriques.

Théorème I.2.13 (Inégalité de Hadamard) *Toute base $\mathcal{B} := (b_1, \dots, b_n)$ de Λ vérifie*

$$\Delta(\Lambda) \leqslant \prod_{i=1}^{n} \|b_i\|^2. \tag{I.1}$$

Il est possible (comme dans [Nap96]) de démontrer ce résultat en utilisant le procédé d'orthogonalisation de Gram/Schmidt, mais nous préférons ici généraliser la preuve de [Mar03, §2.1, p.37–39], plus élémentaire.

Lemme I.2.14 *Soient $\mathcal{B}' := (b_2, \dots, b_n)$ et $F := \mathrm{Vect}_{\mathbb{C}}(\mathcal{B}')$. Alors $\Lambda' := \Lambda \cap F$ est un $\mathcal{O}_K$-réseau de F. De plus, si on note π la projection orthogonale sur $F^{\perp}$, on a*

$$\Delta(\Lambda) = \|\pi(b_1)\|^2 \Delta(\Lambda').$$

Démonstration. Λ' est un $\mathcal{O}_K$-réseau F puisque $\mathcal{B}'$ est une $\mathbb{C}$-base de F qui génère Λ' sur $\mathcal{O}_K$, donc une base de Λ' vu comme réseau algébrique. Soient $\mathcal{B}'_0$ et $\mathcal{B}''_0$ des $\mathbb{C}$-bases orthonormées de F et $F^{\perp}$ respectivement. Soit $\mathcal{B}_0 := \mathcal{B}'_0 \cup \mathcal{B}'_0$ la $\mathbb{C}$-base orthonormée de $\mathbb{C}^n$ formée de la concaténation de $\mathcal{B}'_0$ et $\mathcal{B}''_0$. Dans cette base, la matrice de $\mathcal{B}$ est de la forme

$$\mathrm{Mat}_{\mathcal{B}_0}(\mathcal{B}) = \begin{pmatrix} \|\pi(b_1)\| & * & \cdots & * \\ 0 & & & \\ \vdots & & \mathrm{Mat}_{\mathcal{B}'_0}(\mathcal{B}') & \\ 0 & & & \end{pmatrix},$$

ce qui entraîne l'égalité

$$\Delta(\Lambda) = |\det_{\mathcal{B}_0}(\mathcal{B})|^2 = \|\pi(b_1)\|^2 |\det_{\mathcal{B}'_0}(\mathcal{B}')|^2 = \|\pi(b_1)\|^2 \Delta(\Lambda').$$

□

Démonstration de l'inégalité de Hadamard. On procède par récurrence sur n. Le cas $n = 1$ est trivial (il y a même égalité). Soit $n \geqslant 2$; supposons le résultat acquis au rang $n-1$.

Soit Λ un $\mathcal{O}_K$-réseau de $\mathbb{C}^n$. Fixons $\mathcal{B} := (b_1, \dots b_n)$ une base de Λ. Soient $\mathcal{B}' := (b_2, \dots, b_n)$ et $F := \mathrm{Vect}_{\mathbb{C}}(\mathcal{B}')$. D'après le lemme précédent, $\Lambda' = \Lambda \cap F$ un $\mathcal{O}_K$-réseau de F tel que :

$$\Delta(\Lambda) = \|\pi(b_1)\|^2 \Delta(\Lambda') \leqslant \|b_1\|^2 \Delta(\Lambda').$$

Or F est de dimension $n-1$, et Λ' a pour base $\mathcal{B}'$. Ainsi, par hypothèse de récurrence :

$$\Delta(\Lambda') \leqslant \prod_{i=2}^{n} \|b_i\|^2.$$

L'inégalité de Hadamard est démontrée. □

I.2.3.2 Inégalité et constante de Hermite

Afin de généraliser l'inégalité de Hermite, nous supposons dans ce paragraphe que K est un corps admissible ; il satisfait en particulier la propriété (P2) d'euclidianité géométrique. Rappelons que cela signifie que

$$m_K := \sup_{x \in \mathbb{C}} \inf_{y \in \mathcal{O}_K} |x - y|^2 < 1.$$

Théorème I.2.15 (Inégalité de Hermite) *Tout $\mathcal{O}_K$-réseau Λ de $\mathbb{C}^n$ possède une base $(b_1, \dots, b_n)$ telle que*

$$\prod_{i=1}^{n} \|b_i\|^2 \leqslant \left(\frac{1}{1-m_K}\right)^{\frac{n(n-1)}{2}} \Delta(\Lambda).$$

Cette inégalité se démontre de manière élémentaire en procédant par récurrence sur la dimension, et ceci à l'aide de projections orthogonales. Fixons Λ un $\mathcal{O}_K$-réseau de $\mathbb{C}^n$. Soient $b_1 \in S(\Lambda)$ un vecteur minimal et $H := \mathbb{C}b_1^{\perp}$ l'hyperplan orthogonal à $\mathbb{C}b_1$. On note π la projection orthogonale sur H. Soit $\Lambda' := \pi(\Lambda)$

Lemme I.2.16 *Le groupe Λ' est un $\mathcal{O}_K$-réseau de H.*

Démonstration. $\Lambda \cap \mathbb{C}b_1$ est un sous-$\mathcal{O}_K$-module libre de rang 1 de Λ. En effet, d'après le théorème de structure des sous-groupes discrets de $\mathbb{R}^n$, $\Lambda \cap \mathbb{C}b_1$ est de rang au plus $\dim_{\mathbb{R}}(\mathbb{C}b_1) = 2$ sur $\mathbb{Z}$, ce qui entraîne directement que Λ est de rang 1 sur $\mathcal{O}_K$ (puisque $\mathcal{O}_K$ est de rang 2 sur $\mathbb{Z}$).

En utilisant le théorème de la base adaptée, on obtient l'existence de $(b, b_2, \dots, b_n)$ une base de Λ et de $\lambda \in \mathcal{O}_K$ tel que $\Lambda \cap \mathbb{C}b_1 = \mathcal{O}_K \lambda b$. En particulier, $b \in \mathbb{C}b_1$, et donc $\pi(b) = 0$. Ainsi, $(\pi(b_2), \dots, \pi(b_n))$ est une famille de H générant Λ en tant que $\mathcal{O}_K$-module. De plus, elle est génératrice de H sur $\mathbb{C}$ (puisque $(b, b_2, \dots, b_n)$ est une base de Λ, donc une base de $\mathbb{C}^n$), et contient $n-1 = \dim_{\mathbb{C}}(H)$ vecteurs : c'est une base de H. □

Fixons $b \in \mathbb{C}^n$ tel que $\Lambda \cap \mathbb{C}b_1 = \mathcal{O}_K b$.

Lemme I.2.17 *Soit $(b'_2,\dots,b'_n)$ une base de Λ'. Pour tout $2 \leqslant i \leqslant n$, soit $b_i \in \Lambda$ tel que $\pi(b_i) = b'_i$. Alors $\mathcal{B} := (b, b_2, \dots, b_n)$ est une base de Λ.*

Démonstration. Il est clair que $\mathcal{B}$ est une $\mathbb{C}$-base de $\mathbb{C}^n$. Reste à vérifier qu'elle est génératrice de Λ sur $\mathcal{O}_K$. Soit $x \in \Lambda$. On peut écrire $\pi(x) = \sum_{i=2}^n \lambda_i b'_i$ avec $\lambda_2,\dots,\lambda_n \in \mathcal{O}_K$. Alors $y = \sum_{i=2}^n \lambda_i b_i$ est un élément de Λ tel que $\pi(y) = \pi(x)$. En particulier, $x-y \in \Lambda \cap \mathbb{C}b_1 = \mathcal{O}_K b$. D'où le résultat. □

Lemme I.2.18 *Soit $x' \in \Lambda'$. Il existe $x \in \Lambda$ tel que $\pi(x) = x'$ et*

$$\|x\|^2 \leqslant \frac{1}{1-m_K}\|x'\|^2.$$

Démonstration. On suppose que $x' \neq 0$, sinon le résultat est trivial. Il existe $x_0 \in \Lambda$ tel que $\pi(x_0) = x'$. En particulier, on peut écrire $x_0 = x' + \alpha b_1$ avec $\alpha \in K$. Alors pour tout $\lambda \in \mathcal{O}_K$, $x_\lambda = x_0 - \lambda b_1 = x' - (\alpha-\lambda)b_1$ est un élément de Λ tel que $\pi(x_\lambda) = x'$.

Par définition de m_K, on peut trouver $\lambda_0 \in \mathcal{O}_K$ tel que $|\alpha-\lambda_0|^2 \leqslant m_K$. Alors $x_{\lambda_0} \in \Lambda$ vérifie $\pi(x_{\lambda_0}) = x'$ et, par minimalité de b_1 :

$$\|x_{\lambda_0}\|^2 = \|x' + (\alpha-\lambda_0)b_1\|^2 = \|x'\|^2 + |\alpha-\lambda_0|^2\|b_1\|^2 \leqslant \|x'\|^2 + m_K\|x_{\lambda_0}\|^2,$$

ce qui entraîne finalement

$$\|x_{\lambda_0}\|^2 \leqslant \frac{1}{1-m_K}\|x'\|^2.$$ □

Lemme I.2.19 *Le déterminant de Λ vérifie*

$$\Delta(\Lambda) = \|b\|^2\Delta(\Lambda').$$

Démonstration. Soient $\mathcal{B}'_0$ une $\mathbb{C}$-base orthonormée de H et $\mathcal{B}_0 := \left\{\frac{b}{\|b\|}\right\} \cup \mathcal{B}'_0$ la $\mathbb{C}$-base orthonormée de $\mathbb{C}^n$ formée de la concaténation de la $\mathbb{C}$-base orthonormée $\left\{\frac{b}{\|b\|}\right\}$ de $\mathbb{C}b$ et de $\mathcal{B}'_0$. D'après le Lemme I.2.16 et le Lemme I.2.17, il existe $\mathcal{B} := (b, b_2, \dots, b_n)$ une base Λ telle que $\mathcal{B}' := (\pi(b_2),\dots,\pi(b_n))$ soit une base de Λ'. Alors la matrice de $\mathcal{B}$ dans la base $\mathcal{B}_0$ est de la forme

$$\mathrm{Mat}_{\mathcal{B}_0}(\mathcal{B}) = \begin{pmatrix} \|b\| & 0 & \cdots & 0 \\ * & & & \\ \vdots & & \mathrm{Mat}_{\mathcal{B}'_0}(\mathcal{B}') & \\ * & & & \end{pmatrix},$$

ce qui prouve le résultat annoncé. □

Les quatre lemmes précédents permettent de prouver l'inégalité de Hermite :

Démonstration de l'inégalité de Hermite. Comme annoncé, on procède par récurrence sur la dimension n du réseau algébrique considéré. Pour $n = 1$, c'est évident. Soit $n \geqslant 2$; supposons le résultat acquis au rang $n-1$.

Soient Λ un $\mathcal{O}_K$-réseau de $\mathbb{C}^n$ et $b_1 \in S(\Lambda)$. On utilise les mêmes notations que dans les lemmes précédents. D'après le Lemme I.2.16, Λ' est un réseau de rang $n-1$; par hypothèse de récurrence, il existe donc une base $(b'_2, \dots, b'_n)$ de Λ' telle que

$$\prod_{i=2}^{n} \|b'_i\|^2 \leqslant \left(\frac{1}{1-m_K}\right)^{\frac{(n-1)(n-2)}{2}} \Delta(\Lambda').$$

Soit $b \in \mathbb{C}^n$ tel que $\Lambda \cap \mathbb{C}b_1 = \mathcal{O}_K b$. D'après le Lemme I.2.17 et le Lemme I.2.18, il existe une base $(b, b_2, \dots, b_n)$ de Λ telle que pour $2 \leqslant i \leqslant n$

$$\|b_i\|^2 \leqslant \frac{1}{1-m_K}\|b'_i\|^2.$$

Finalement, on obtient que

$$\|b\|^2 \prod_{i=2}^{n} \|b_i\|^2 \leqslant \left(\frac{1}{1-m_K}\right)^{n-1} \|b\|^2 \prod_{i=2}^{n} \|b'_i\|^2 \leqslant \left(\frac{1}{1-m_K}\right)^{\frac{n(n-1)}{2}} \|b\|^2 \Delta(\Lambda').$$

En utilisant le Lemme I.2.19 et l'hypothèse de récurrence sur Λ', l'inégalité de Hermite est démontrée. □

Il en découle immédiatement un premier corollaire :

Corollaire I.2.20 *Tout $\mathcal{O}_K$-réseau Λ de $\mathbb{C}^n$ vérifie*

$$m(\Lambda) \leqslant \left(\frac{1}{1-m_K}\right)^{\frac{n-1}{2}} \Delta(\Lambda)^{\frac{1}{n}}.$$

Ce corollaire permet de définir proprement la constante de Hermite associée à un corps de nombres admissible, qui prolonge la notion fondamentale de constante de Hermite classique.

Définition I.2.21 *La constante de Hermite pour la dimension n et le corps K est*

$$\gamma_{K,n} := \sup_{\Lambda} \frac{m(\Lambda)}{\Delta(\Lambda)^{\frac{1}{n}}},$$

la borne supérieure étant prise sur l'ensemble des $\mathcal{O}_K$-réseaux de $\mathbb{C}^n$.

Remarquons que $\gamma_{K,n} \leqslant \left(\frac{1}{1-m_K}\right)^{\frac{n-1}{2}}$ d'après le Corollaire I.2.20. Via la constante de Hermite, il est facile de réexprimer le Corollaire I.2.20 :

Proposition I.2.22 *Tout $\mathcal{O}_K$-réseau Λ de $\mathbb{C}^n$ vérifie*

$$\Delta(\Lambda) \geqslant m(\Lambda)^n \gamma_{K,n}^{-n}.$$

I.3 Bases réduites au sens de Lenstra, Lenstra et Lovász

Dans toute cette section, on fixe $K := \mathbb{Q}(i\sqrt{D})$ avec $D \in \mathbb{N}_{>0}$. En particulier et sauf mention du contraire, on ne suppose pas que K est géométriquement euclidien (propriété (P2)).

I.3.1 Procédé d'orthogonalisation de Gram/Schmidt

Nous rappelons ici le *procédé d'orthogonalisation de Gram/Schmidt* (abrégé GSOP dans la suite [5]) sur $\mathbb{C}^n$, qui permet d'obtenir à partir d'une famille de vecteurs de $\mathbb{C}^n$ une famille *orthogonale* générant sur $\mathbb{C}$ le même espace que la famille originale. La construction classique du GSOP est par exemple présentée dans [VZGG03, p.463].

Soit $\mathcal{B} := (b_1, \dots, b_n)$ une $\mathbb{C}$-base de $\mathbb{C}^n$. Pour tout $1 \leqslant i \leqslant n$, on pose

$$b_i^* := \sum_{j=1}^{i-1} \mu_{i,j} b_j^*, \tag{I.2}$$

où les $\mu_{i,j}$ sont des éléments de $\mathbb{C}$ définis pour tous $1 \leqslant i, j \leqslant n$ par :

$$\mu_{i,j} := \begin{cases} \dfrac{\langle b_i \mid b_j^* \rangle}{\|b_j^*\|^2} & \text{si } j < i, \\ 1 & \text{si } i = j, \\ 0 & \text{sinon.} \end{cases}$$

Cette définition est cohérente, dans le sens où $b_i^* \neq 0$ pour tout $1 \leqslant i \leqslant n$. En effet, puisque $\mathcal{B}$ est une $\mathbb{C}$-base, elle est $\mathbb{C}$-libre. La combinaison linéaire (I.2) n'est donc jamais nulle (ce qui se démontre facilement par récurrence). La proposition suivante résume les propriétés classiques du GSOP.

Proposition I.3.1 *Soit $\mathcal{B} := (b_1, \dots, b_n)$ une $\mathbb{C}$-base de $\mathbb{C}^n$. Notons $\mathcal{B}^* := (b_1^*, \dots, b_n^*)$ et $\mathcal{M} := (\mu_{i,j})_{1 \leqslant i,j \leqslant n}$ les familles obtenues par le GSOP sur cette base [6]. Alors :*

- *Pour tout $1 \leqslant i \leqslant n$, on a*
$$b_i = \sum_{j=1}^{n} \mu_{i,j} b_j^*. \tag{I.3}$$
Ainsi, si B et B^* sont les matrices de $\mathcal{B}$ et $\mathcal{B}^*$, on a $B = MB^*$, où M est la matrice définie pour tout $1 \leqslant i, j \leqslant n$ par $M_{i,j} := \mu_{i,j}$. En particulier, $\det(B) = \det(B^*)$.
- *La famille $(b_1^*, \dots, b_n^*)$ est orthogonale.*
- *Pour tout $1 \leqslant i \leqslant n$, on a $\mathrm{Vect}_{\mathbb{C}}(b_1, \dots, b_i) = \mathrm{Vect}_{\mathbb{C}}(b_1^*, \dots, b_i^*)$. En particulier, $\mathcal{B}^*$ est une $\mathbb{C}$-base de $\mathbb{C}^n$.*

5. Pour *Gram/Schmidt Orthogonalization Process*.
6. Dans la suite, nous réservons les notations $\mathcal{B}^*$ et $\mathcal{M}$ à de tels objets.

- *Pour tout* $1 \leqslant i \leqslant n$, b_i^* *est la projection de* b_i *sur le supplémentaire orthogonal de* $\mathrm{Vect}_{\mathbb{C}}(b_1, \ldots, b_{i-1})$. *En particulier,* $\|b_i^*\| \leqslant \|b_i\|$.

Démonstration.

- C'est l'écriture matricielle de (I.2). L'égalité des déterminants est obtenue en remarquant que M est une matrice triangulaire inférieure dont la diagonale est constituée de 1.
- On procède par récurrence, en montrant que pour tout $2 \leqslant i \leqslant n$, b_i^* est orthogonal à $(b_1^*, \ldots, b_{i-1}^*)$.
- Encore une fois, on procède par récurrence sur $1 \leqslant i \leqslant n$.
- Découle de la décomposition (I.2) et des points précédents. D'autre part, si $b_i = b_i^* + x$, où $x \in \mathrm{Vect}_{\mathbb{C}}(b_1, \ldots, b_{i-1}) = \mathrm{Vect}_{\mathbb{C}}(b_1^*, \ldots, b_{i-1}^*)$, alors par orthogonalité

$$\|b_i\|^2 = \|b_i^*\|^2 + \|x\|^2 \geqslant \|b_i^*\|^2. \qquad \square$$

En utilisant le fait que K est unimodulaire (hypothèse (P1)), il est possible de compléter ces propriétés.

Corollaire I.3.2 *Le déterminant de Gram de* $\mathcal{B}$ *est égal au déterminant de Gram de* $\mathcal{B}^*$, *qui est donné par*

$$\det(\mathrm{Gram}(\mathcal{B})) = \det(\mathrm{Gram}(\mathcal{B}^*)) = \prod_{i=1}^{n} \|b_i^*\|^2.$$

Démonstration. La relation $E = ME^*$ entraîne que

$$\mathrm{Gram}(\mathcal{B}) = M \cdot \mathrm{Gram}(\mathcal{B}^*) \cdot \overline{M}^{\mathsf{T}}.$$

Puisque $\det(M) = 1$, la première égalité est démontrée. La seconde s'obtient en remarquant que puisque $\mathcal{B}^*$ est orthogonale, on a $\mathrm{Gram}(\mathcal{B}^*) = \mathrm{Diag}(\|b_1^*\|^2, \ldots, \|b_n^*\|^2)$. $\square$

L'algorithme pour calculer $\mathcal{B}^*$ et $\mathcal{M}$ est trivial. Cependant, dans la suite, nous ne nous intéresserons qu'aux grandeurs $\|b_i^*\|^2$, et non aux vecteurs b_i^*. C'est pourquoi il est intéressant, ne serait-ce que pour des contraintes d'espace mémoire, de considérer une modification du GSOP ne travaillant qu'avec ces normes, que nous appellerons *GSOP en norme*. C'est une des améliorations proposées dans [GM05, §III] (mais seulement sur $K = \mathbb{Q}(i)$) par rapport à l'algorithme LLL original [LLL82] et certaines de ses extensions (comme [Nap96]). Cette construction est essentiellement la conséquence des deux propriétés suivantes.

Proposition I.3.3 *Soit* $\mathcal{B} := (b_1, \ldots, b_n)$ *une* $\mathbb{C}$*-base de* $\mathbb{C}^n$.

- *Pour tous* $1 \leqslant j < i \leqslant n$, *on a*

$$\mu_{i,j} = \frac{1}{\|b_j^*\|} \left(\langle b_i \mid b_j \rangle - \sum_{k=1}^{j-1} \overline{\mu_{j,k}} \mu_{i,k} \|b_k^*\|^2 \right).$$

- *Pour tout* $1 \leqslant i \leqslant n$, *on a*

$$\|b_i^*\|^2 = \|b_i\|^2 - \sum_{j=1}^{i-1} |\mu_{i,j}|^2 \|b_j^*\|^2.$$

Démonstration. Soient $1 \leqslant j < i \leqslant n$.

- Par définition, $\mu_{i,j} = \frac{\langle b_i \mid b_j^* \rangle}{\|b_j^*\|^2}$. Or

$$\langle b_i \mid b_j^* \rangle = \langle b_i \mid b_j - \sum_{k=1}^{j-1} \mu_{j,k} b_k^* \rangle = \langle b_i \mid b_j \rangle - \sum_{k=1}^{j-1} \overline{\mu_{j,k}} \mu_{i,k} \|b_k^*\|^2.$$

  D'où le premier point.
- Par définition,

$$\|b_i^*\|^2 = \langle b_i^* \mid b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^* \rangle.,$$

  ce qui entraîne par orthogonalité que

$$\|b_i^*\|^2 = \langle b_i^* \mid b_i \rangle = \langle b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^* \mid b_i \rangle = \langle b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^* \mid \sum_{j=1}^{i} \mu_{i,j} b_j^* \rangle.$$

  Finalement, on en déduit, toujours par orthogonalité, que

$$\|b_i^*\|^2 = \|b_i\|^2 - \sum_{j=1}^{i-1} |\mu_{i,j}|^2 \|b_j^*\|^2.$$ □

Le calcul du GSOP en norme est implanté par l'Algorithme I.1. Si $\mathcal{B} := (b_1, \ldots, b_n)$ est une famille de vecteurs de $\mathbb{C}^n$, nous appellerons $\|\mathcal{B}\|^2$ la famille $(\|b_1\|^2, \ldots, \|b_m\|^2)$.

Proposition I.3.4 *Soit $\mathcal{B} := (b_1, \ldots, b_n)$ une $\mathbb{C}$-base de $\mathbb{C}^n$. Appliqué à $\mathcal{B}$, l'Algorithme I.1 renvoie les familles $\|\mathcal{B}^*\|^2$ et $\mathcal{M}$ du GSOP en norme de $\mathcal{B}$. Plus précisément, si $1 \leqslant j \leqslant n$, à la fin de la j-ième itération de la boucle (3), les $\mu_{k,l}$ sont correctement calculés pour tous $1 \leqslant l \leqslant j < k \leqslant n$, et pour tout $1 \leqslant k \leqslant n$, on a*

$$N_k = \|b_k\|^2 - \sum_{i=1}^{\min(k-1,j)} |\mu_{k,i}|^2 \|b_i^*\|^2.$$

Démonstration. On procède par récurrence sur $1 \leqslant j \leqslant n$.

À la fin de la boucle (3) rang $j = 1$, on a $N_1 = \|b_1\|^2 = \|b_1^*\|^2$. De plus, pour tout $1 < i \leqslant n$, les $\mu_{i,1}$ sont correctement calculés. Enfin, pour $1 < k \leqslant n$, on a $N_k = \|b_k\|^2 - |\mu_{k,1}|^2 \|b_1\|^2$. Le résultat annoncé est vérifié au rang 1.

Soit $2 \leqslant j \leqslant n$; supposons le résultat acquis au rang $j-1$. Les N_k n'étant pas modifiés pour $1 \leqslant k \leqslant j$, on a toujours à la fin de la boucle que $N_k = \|b_k^*\|^2$ pour tout $1 \leqslant k \leqslant j$ par hypothèse de récurrence. De même, les $\mu_{k,l}$ ne sont pas modifiés pour $1 \leqslant l < j \leqslant k \leqslant n$, et restent donc correctement calculés à la fin de la boucle par hypothèse de récurrence. Ces deux points entraînent, en utilisant la Proposition I.3.3, que les $\mu_{k,l}$ sont bien calculés à la fin de la boucle pour $1 \leqslant l \leqslant j < k \leqslant n$.

Soit $j+1 \leqslant k \leqslant n$. Notons $\widetilde{N}_k$ la valeur de N_k à la fin de la boucle. On a

$$\widetilde{N}_k = N_k - |\mu_{k,j}|^2 N_j,$$

et donc par hypothèse de récurrence

$$\begin{aligned}\widetilde{N}_k &= \|b_k\|^2 - |\mu_{k,j}|^2\|b_j^*\|^2 - \sum_{i=1}^{\min(k-1,j-1)} |\mu_{k,i}|^2\|b_i^*\|^2 \\ &= \|b_k\|^2 - \sum_{i=1}^{\min(k-1,j)} |\mu_{k,i}|^2\|b_i^*\|^2.\end{aligned}$$

Enfin, le fait que $N_j = \|b_j^*\|^2$ provient de la Proposition I.3.3. □

```
Données :
    • Une ℂ-base ℬ de ℂ^n.
Résultat :
    • Les sorties (‖ℬ*‖², ℳ) du GSOP en norme de ℬ.
pour j = 1 à n faire
    N_i ← ‖b_i‖²
pour j = 1 à n faire
    pour i = j + 1 à n faire
        μ_{i,j} ← (1/N_j) (⟨b_i | b_j⟩ − Σ_{k=1}^{j−1} conj(μ_{j,k}) μ_{i,k} N_k)
        N_i ← N_i − |μ_{i,j}|² N_j
retourner ((N_1, ..., N_n), (μ_{i,j})_{1⩽i,j⩽n})
```

Algorithme I.1 - Calcul du GSOP en norme.

I.3.2 Réduction au sens de Lenstra, Lenstra et Lovász

En tant qu'analogues discrets des espaces hermitiens, on pourrait attendre des réseaux algébriques qu'ils possèdent des bases orthogonales ou orthonormées. Ce n'est généralement pas le cas, et c'est ce qui motive l'introduction de la notion de *base réduite*. Notons qu'il n'existe pas une mais plusieurs notions de réduction, qui possèdent chacune leurs particularités propres. Nous ne nous intéresserons ici qu'à la notion réduction la plus populaire : la réduction au sens de Lenstra, Lenstra et Lovász [LLL82].

I.3.2.1 Définition

Nous présentons dans cette section la notion de base réduite au sens de Lenstra, Lenstra et Lovász (abrégé LLL). Cette notion fût introduite dans [LLL82], dans le but initial de développer un algorithme efficace de factorisation d'un polynôme dans $\mathbb{Q}[X]$. Dans la prochaine

section, nous détaillerons un algorithme, communément appelé algorithme de réduction LLL ou algorithme LLL, permettant d'obtenir de telles bases.

Définition I.3.5 *Une $\mathbb{C}$-base $\mathcal{B} := (b_1, \dots, b_n)$ de $\mathbb{C}^n$ est dite (η, δ)-LLL réduite si les conditions suivantes sont vérifiées :*

$$|\mu_{i,j}|^2 \leqslant \eta \tag{LLL1}$$

pour tous $1 \leqslant j < i \leqslant n$, et

$$\|b_i^*\|^2 \geqslant (\delta - |\mu_{i,i-1}|^2)\|b_{i-1}^*\|^2 \tag{LLL2}$$

pour tout $1 < i \leqslant m$.

Les paramètres η et δ sont tels que $\eta < \delta < 1$. On appelle parfois constante de Lovász le paramètre δ. La condition (LLL1) est une condition de réduction en taille, alors que (LLL2) est une condition d'orthogonalité, appelée condition de Lovász. L'emploi de cet terminologie sera justifié dans le prochain paragraphe. L'étude et le calcul des bases LLL-réduites sont motivés par une multitudes d'applications pratiques. Le lecteur intéressé par un panorama sur ce sujet passionnant pourra consulter [NV10]. Mentionnons tout de même quelques exemples :

- La factorisation de polynômes à coefficients rationnels [LLL82, p.526-529] ou dans d'autres structures [Rob04, p.1434-1438].
- L'efficacité de la technologie MIMO (*Multiple-Input Multiple-Output*), fondamentale dans le domaine des télécommunications, est considérablement accrue en travaillant avec des bases réduites [GM05, p.2].
- Plusieurs schémas de chiffrement, comme NTRU [HPS98, p.272-275] ou certains schémas SHE [Sil13, p.5-7], s'appuient sur la difficulté de trouver des vecteurs courts d'un réseau. Même si certains algorithmes de réduction actuels s'exécutent en temps polynomial, ils ne permettent de calculer que des vecteurs « relativement » courts ; la recherche de vecteurs courts en grande dimension reste très coûteuse. À titre d'exemple, l'attaque du schéma NTRU le plus résistant présenté dans [HPS98, p.275-276] nécessite de réduire un réseau de dimension environ 1000.

I.3.2.2 SVP$_\gamma$ et défaut d'orthogonalité

Nous mettons en valeur dans ce paragraphe l'utilité de la LLL réduction pour le *Shortest Vector Problem with parameter* γ (SVP$_\gamma$), qui intervient par exemple dans l'attaque du schéma NTRU [HPS98, p.272-275]et dans les problèmes de factorisations polynomiaux [LLL82 ; Rob04]

Étant donné un $\mathcal{O}_K$-réseau $\Lambda \subset \mathbb{C}^n$ et un paramètre $\gamma \geqslant 1$, le SVP$_\gamma$ sur Λ consiste à approximer l'un des plus courts vecteurs de Λ à un facteur γ près, c'est-à-dire à trouver un vecteur $x \in \Lambda$ tel que

$$0 < \|x\|^2 \leqslant \gamma \cdot m(\Lambda).$$

Pour $\gamma = 1$, le SVP$_\gamma$ correspond au problème du plus court vecteur usuel. Obtenir une base (η, δ)-LLL réduite d'un réseau Λ permet justement d'approximer $m(\Lambda)$ d'un facteur ne dépendant que du corps K et le dimension n du réseau.

Soit $\Lambda = \mathcal{O}_k b_1 \oplus \cdots \mathcal{O}_K b_n$ un $\mathcal{O}_K$-réseau de $\mathbb{C}^n$. On note $\mathcal{B}^*$ et $\mathcal{M}$ les familles issues du GSOP de $\mathcal{B} := (b_1, \ldots, b_n)$. Pour tout corps de nombres K, on note μ_K le groupe des racines de l'unité de K et Σ_K l'ensemble des plongements de K dans $\mathbb{C}$.

Lemme I.3.6 *Soit K un corps de nombres de degré d. Pour tout $x \in \mathcal{O}_K \setminus \{0\}$, on a*

$$\sum_{\sigma \in \Sigma_K} |\sigma(x)|^2 \geqslant d,$$

avec égalité si et seulement si $x \in \mu_K$. En particulier, si K est un corps quadratique imaginaire, $m(\mathcal{O}_K) = 1$ et $S(\mathcal{O}_K) = \mu_K$.

Démonstration. Soit $x \in \mathcal{O}_K \setminus \{0\}$. En utilisant l'inégalité arithmético-géométrique, on montre que

$$\sum_{\sigma \in \Sigma_K} |\sigma(x)|^2 \geqslant d \left(\prod_{\sigma \in \Sigma_K} |\sigma(x)|^2 \right)^{1/d} = d \, |\mathrm{N}_K(x)|^{2/d}, \tag{I.4}$$

où N_K désigne la norme de $K/\mathbb{Q}$. Le fait que $x \in \mathcal{O}_K \setminus \{0\}$ entraînant $|\mathrm{N}_K(x)| \geqslant 1$, l'inégalité annoncée est démontrée. De plus, si $x \in \mu_K$, $\sigma(x)$ est une racine de l'unité dans $\mathbb{C}$ pour tout $\sigma \in \Sigma_K$, ce qui entraîne en particulier que $|\sigma(x)| = 1$. Ainsi, le terme de gauche de l'inégalité (I.4) est bien égal à d puisque $|\Sigma_K| = d$.

Supposons maintenant que ce terme est égal à d. En utilisant le cas d'égalité de l'inégalité arithmético-géométrique dans (I.4), on montre que ceci équivaut à $|\sigma(x)| = 1$ pour tout $\sigma \in \Sigma_K$. Cette propriété est aussi vérifiée par x^k pour tout $k \in \mathbb{N}$. Le polynôme minimal de x^k est donc un polynôme de degré n à coefficients entiers et ayant toutes racines complexes de module 1. Les relations coefficients-racines montrent que l'ensemble de ces polynômes est fini, ce qui entraîne l'existence de $k \in \mathbb{N}_{>1}$ tel que $x^k = x$. Ainsi, x est bien une racine de l'unité dans K.

Enfin, si K est un corps quadratique imaginaire, on a $d = 2$ et

$$\sum_{\sigma \in \Sigma_K} |\sigma(x)|^2 = 2|x|^2$$

pour tout $x \in K$, ce qui prouve l'assertion $m(\mathcal{O}_K) = 1$ et $S(\mathcal{O}_K) = \mu_K$. □

Lemme I.3.7 *Soit $x \in \Lambda$ non nul. Alors :*

$$\|x\|^2 \geqslant \min_{1 \leqslant i \leqslant n} \|b_i^*\|^2.$$

Démonstration. On peut écrire

$$x = \sum_{i=1}^{n} x_i b_i$$

avec $x_i \in \mathcal{O}_K$ pour tout $1 \leqslant i \leqslant n$. Soit $1 \leqslant m \leqslant n$ l'indice maximal tel que $x_m \neq 0$. Pour tout $1 \leqslant i \leqslant n$, d'après (I.3), on a

$$b_i = \sum_{j=1}^{i} \mu_{i,j} b_j^*$$

et donc, puisque $\mu_{m,m} = 1$,

$$x = x_m b_m^* + \sum_{i=1}^{m-1} \nu_i b_i^*,$$

où $\nu_i = \sum_{j=i}^{m} x_j \mu_{j,i} \in \mathbb{C}$ pour tout $1 \leqslant i \leqslant m-1$. Dès lors, par orthogonalité de la famille $\mathcal{B}^*$,

$$\begin{aligned} \|x\|^2 &= |x_m|^2 \|b_m^*\|^2 + \sum_{i=1}^{m-1} |\nu_i|^2 \|b_i^*\|^2 \\ &\geqslant |x_m|^2 \|b_m^*\|^2 \\ &\geqslant m(\mathcal{O}_K) \min_{1 \leqslant i \leqslant n} \|b_i^*\|^2. \end{aligned}$$

Le lemme précédent permet de conclure. □

Ce résultat permet de résoudre le SVP_γ à l'aide des bases réduites pour un facteur γ donné.

Théorème I.3.8 *Supposons maintenant que la base $\mathcal{B}$ est (η, δ)-LLL réduite. Alors*

$$\|b_1\|^2 \leqslant \left(\frac{1}{\delta - \eta}\right)^{n-1} m(\Lambda). \tag{I.5}$$

En particulier, b_1 réponds au SVP_γ sur Λ pour $\gamma = \left(\frac{1}{\delta-\eta}\right)^{n-1}$.

Démonstration. Puisque $\mathcal{B}$ est (η, δ)-LLL réduite, on a pour tout $2 \leqslant i \leqslant n$

$$\|b_i^*\|^2 \geqslant (\delta - |\mu_{i,i-1}|^2)\|b_{i-1}^*\|^2 \geqslant (\delta - \eta)\|b_{i-1}^*\|^2$$

et donc, par une récurrence immédiate,

$$\|b_i^*\|^2 \geqslant (\delta - \eta)^{i-1} \|b_1^*\|^2.$$

Soit $1 \leqslant i \leqslant n$ tel que

$$\|b_i^*\|^2 = \min_{1 \leqslant k \leqslant n} \|b_k^*\|^2.$$

D'après le lemme précédent, pour tout $x \in \Lambda$ non nul, on a

$$\begin{aligned} \|x\|^2 &\geqslant \|b_i^*\|^2 \\ &\geqslant (\delta - \eta)^{i-1} \|b_1^*\|^2 \\ &\geqslant (\delta - \eta)^{n-1} \|b_1^*\|^2. \end{aligned}$$

Donc en prenant la borne inférieure et puisque $b_1^* = b_1$, on obtient

$$\|b_1\|^2 \leqslant \left(\frac{1}{\delta - \eta}\right)^{m-1} m(\Lambda).$$

Le vecteur b_1 réponds donc au SVP_γ comme annoncé. □

Soulignons que le facteur $\left(\frac{1}{\delta-\eta}\right)^{n-1}$ ne dépend pas du réseau Λ ; la LLL-réduction permet de répondre au SVP_γ avec un facteur γ valable pour tous les réseaux algébriques sur un corps donné et d'un rang fixé. Les bases réduites possèdent une autre propriété fondamentale : elles sont satisfaisantes du point de vue de l'orthogonalité. On appelle défaut d'orthogonalité de la base $\mathcal{B}$ la grandeur

$$\delta(\mathcal{B}) := \frac{\prod_{i=1}^{n} \|b_i\|^2}{\Delta(\Lambda)}.$$

D'après l'inégalité de Hadamard (Théorème I.2.13), $\delta(\mathcal{B}) \in [1; +\infty[$. D'autre part, d'après le Corollaire I.3.2, $\delta(\mathcal{B}) = 1$ si et seulement si $\mathcal{B}$ est orthogonale. Cette constante $\delta(\mathcal{B})$ quantifie l'écart à l'orthogonalité d'une base : plus $\delta(\mathcal{B})$ est grand, « moins » la base $\mathcal{B}$ est orthogonale.

Il s'avère que si $\mathcal{B}$ est une base (η, δ)-LLL réduite, $\delta(\mathcal{B})$ est majoré indépendamment de $\mathcal{B}$ et du réseau algébrique Λ. Ainsi, pour une dimension donnée et quel que soit le réseau considéré, on peut se ramener à une base dont on maîtrise le défaut d'orthogonalité.

Proposition I.3.9 *Supposons que $\mathcal{B}$ est (η, δ)-LLL réduite. Alors $\delta(\mathcal{B})$ est majoré indépendamment de $\mathcal{B}$:*

$$\delta(\mathcal{B}) \leqslant \prod_{i=1}^{n} \left(1 + \frac{\eta}{\delta-\eta-1}\left(1 - \frac{1}{(\delta-\eta)^{i-1}}\right)\right).$$

Démonstration. Soit $1 \leqslant i \leqslant n$. Puisque $\mathcal{B}$ est (η, δ)-LLL réduite, on montre facilement par récurrence que pour tout $1 \leqslant j \leqslant i$

$$\|b_i^*\|^2 \geqslant (\delta-\eta)^{i-j} \|b_j^*\|^2.$$

D'après (I.3), on peut écrire

$$b_i = \sum_{j=1}^{i} \mu_{i,j} b_j^*.$$

En utilisant l'inégalité précédente, l'orthogonalité de $\mathcal{B}^*$ et la condition (LLL1) de (η, δ)-LLL réduction, on en déduit que

$$\begin{aligned} \|b_i\|^2 &= \|b_i^*\|^2 + \sum_{j=1}^{i-1} |\mu_{i,j}|^2 \|b_j^*\|^2 \\ &\leqslant \left(1 + \eta \sum_{j=1}^{i-1} \frac{1}{(\delta-\eta)^{i-j}}\right) \|b_i^*\|^2. \end{aligned}$$

Or la formule de sommation géométrique donne

$$\sum_{j=1}^{i-1} \frac{1}{(\delta-\eta)^{i-j}} = \frac{1}{\delta-\eta-1}\left(1 - \frac{1}{(\delta-\eta)^{i-1}}\right),$$

donc

$$\|b_i\|^2 \leqslant \left(1 + \frac{\eta}{\delta-\eta-1}\left(1 - \frac{1}{(\delta-\eta)^{i-1}}\right)\right) \|b_i^*\|^2.$$

D'après le Corollaire I.3.2, $\Delta(\Lambda) = \prod_{i=1}^{n} \|b_i^*\|^2$. Ainsi, en prenant le produit pour $1 \leqslant i \leqslant n$ dans l'inégalité précédente, on obtient que

$$\prod_{i=1}^{n} \|b_i\|^2 \leqslant \Delta(\Lambda) \prod_{i=1}^{n} \left(1 + \frac{\eta}{\delta - \eta - 1}\left(1 - \frac{1}{(\delta-\eta)^{i-1}}\right)\right).$$

D'où le résultat annoncé. □

I.4 Algorithme de réduction LLL

Dans toute cette section, on fixe un corps de nombres admissible $K := \mathbb{Q}(i\sqrt{D})$ avec $D \in \{1, 2, 3, 7, 11\}$. Ce corps est donc unimodulaire et géométriquement euclidien, au sens des propriétés (P1) et (P2).

I.4.1 Présentation

Nous avons expliqué dans la section précédente l'utilité des bases LLL réduites, notamment pour le SVP_γ. Néanmoins, l'existence de telles bases n'est pas évidente. L'algorithme que nous détaillons permet justement de calculer des bases (δ, m_K)-LLL réduites lorsque K vérifie des hypothèses convenables. L'algorithme de réduction (Algorithme I.2) que nous proposons est essentiellement le même que celui de Napias [Nap96], lui même très semblable à l'algorithme LLL original [LLL82]. Nous y avons ajouté les optimisations de [GM05, §III], c'est-à-dire le passage du GSOP au GSOP en norme. D'autre part, nous prenons de plus le soin d'analyser plus en détails sa terminaison et les résultats qu'il renvoie.

Résumons de manière informelle le principe de l'algorithme. D'une part, la condition (LLL1) de LLL réduction est facile à obtenir en exploitant directement la propriété (P2), et ce sans modifier les vecteurs du GSOP. D'autre part, la condition (LLL2) est obtenue par permutations successives, de sorte que les vecteurs les plus courts remontent progressivement en tête de la base.

Dans les deux prochaines sections, nous prouvons que l'Algorithme I.2 se termine et calcule effectivement une base réduite du réseau considéré. Nous reprenons pour cela essentiellement la stratégie de preuve mise en avant dans [VZGG03, p.468-472], ainsi que l'idée de [Nap96] d'utiliser l'inégalité de Hermite.

I.4.2 Preuve de l'algorithme

Dans ce paragraphe et le suivant, on se donne Λ un $\mathcal{O}_K$-réseau de $\mathbb{C}^n$ de base $\mathcal{B} := (b_1, \ldots, b_n)$. De plus, on fixe un réel δ tel que $m_K < \delta < 1$. On notera toujours $\mathcal{B}^*$, $\|\mathcal{B}^*\|^2$ et $\mathcal{M}$ les familles issues du GSOP et du GSOP en norme de $\mathcal{B}$.

Admettons provisoirement que l'Algorithme I.2 se termine et montrons qu'il renvoie effectivement une base (m_K, δ)-LLL réduite du réseau considéré. Le fait que cet algorithme renvoie

```
Données :
    • Une base $\mathcal{B} := (b_1, \dots, b_n)$ d'un $\mathcal{O}_K$-réseau $\Lambda$ de $\mathbb{C}^n$.
    • Un paramètre de qualité $\delta$ tel que $m_K < \delta < 1$.
Résultat :
    • Une base $\mathcal{B}' := (b'_1, \dots, b'_n)$ $(m_K, \delta)$-LLL-réduite de $\Lambda$.
1  $\mathcal{B}' \leftarrow \mathcal{B}$
2  $(\mathcal{N} := (N_1, \dots, N_n), \mathcal{M} := (\mu_{i,j})_{1 \leqslant i,j \leqslant n}) \leftarrow$ normGSOP($\mathcal{B}$) (Algorithme I.1)
3  $i \leftarrow 2$
4  tant que $i \leqslant n$ faire
5      pour $j = i-1$ à $n$ faire
6          si $|\mu_{i,j}|^2 > m_K$ alors
7              SIZE_RED($\mathcal{B}', \mathcal{M}, i, j$) (Algorithme I.3)
8      si $i > 1$ et $N_i < (\delta - |\mu_{i,i-1}|^2) N_{i-1}$ alors
9          $(\mathcal{B}', \mathcal{N}, \mathcal{M}) \leftarrow$ SWAP($\mathcal{B}', \mathcal{N}, \mathcal{N}, i$) (Algorithme I.4)
10         $i \leftarrow i-1$
11     sinon
12         $i \leftarrow i+1$
13 retourner $\mathcal{B}'$
```

Algorithme I.2 - Algorithme de réduction LLL.

une base du réseau est trivial : les seules opérations effectuées sont de la forme $b_i \leftarrow b_i - \lambda b_j$ avec $\lambda \in \mathcal{O}_K$ et de la forme $b_i \leftrightarrow b_j$; il est facile de prouver que de telles opérations laissent les réseaux algébriques invariants.

I.4.2.1 Procédure SIZE_RED

On commence par étudier l'Algorithme I.3, qui implante la procédure de réduction en taille SIZE_RED. Cette procédure vise essentiellement à s'assurer que la première condition (LLL1) de LLL-réduction est vérifiée.

Lemme I.4.1 *Soient $1 \leqslant j < i \leqslant n$. Considérons la famille $\widetilde{\mathcal{B}} := (\widetilde{b}_1, \dots, \widetilde{b}_n)$ définie pour tout $1 \leqslant k \leqslant n$ par*

$$\widetilde{b}_k := \begin{cases} b_i - \lceil \mu_{i,j} \rfloor b_j & \text{si } k = i, \\ b_k & \text{sinon,} \end{cases}$$

où $\lceil \mu_{i,j} \rfloor$ désigne un élément de $\mathcal{O}_K$ tel que $|\lceil \mu_{i,j} \rfloor - \mu_{i,j}|^2 \leqslant m_K$. Notons $\widetilde{\mathcal{B}}^*$ et $\widetilde{\mathcal{M}}$ les familles issues du GSOP de $\widetilde{\mathcal{B}}$. Alors $\widetilde{\mathcal{B}}^* = \mathcal{B}^*$ et pour tous $1 \leqslant l < k \leqslant n$

$$\widetilde{\mu}_{k,l} = \begin{cases} \mu_{i,l} - \lceil \mu_{i,j} \rfloor \mu_{j,l} & \text{si } k = i, \\ \mu_{k,l} & \text{sinon.} \end{cases}$$

En particulier, après l'appel à l'Algorithme I.3 dans l'Algorithme I.2, le GSOP en norme de $\mathcal{B}$ est correctement mis à jour.

Données :
- Une base $\mathcal{B} := (b_1, \dots, b_n)$ d'un $\mathcal{O}_K$-réseau Λ de $\mathbb{C}^n$.
- La famille $\mathcal{M} := (\mu_{i,j})_{1 \leqslant i,j \leqslant n}$ du GSOP de $\mathcal{B}$.
- Les indices $1 \leqslant j < i \leqslant n$ à réduire.

Résultat :
- La base $\mathcal{B}$ après l'opération de réduction en taille
- Les mises à jour de $\mathcal{M}$ correspondantes.

$b_i \leftarrow b_i - \lceil \mu_{i,j} \rfloor b_j$; // $\lceil \mu_{i,j} \rfloor \in \mathcal{O}_K$ tel que $|\lceil \mu_{i,j} \rfloor - \mu_{i,j}|^2 \leqslant \eta_k$
pour $k = 1$ à j faire
  $\mu_{i,k} \leftarrow \mu_{i,k} - \lceil \mu_{i,j} \rfloor \mu_{j,k}$

Algorithme I.3 - Procédure SIZE_RED.

Démonstration. On a $\widetilde{b}_k^* = b_k^*$ pour tout $1 \leqslant k < i$ et $\widetilde{\mu}_{k,l} = \mu_{k,l}$ pour tous $1 \leqslant l < k < i$ puisque la famille $(b_1, \dots, b_{i-1})$ n'est pas modifiée. Ainsi, si $1 \leqslant l < i$, on a

$$\begin{aligned}\widetilde{\mu}_{i,l} &= \frac{\langle \widetilde{b}_i \mid b_l^* \rangle}{\|b_l^*\|^2} \\ &= \frac{1}{\|b_l^*\|^2} \left(\langle b_i \mid b_l^* \rangle - \lceil \mu_{i,j} \rfloor \langle b_j \mid b_l^* \rangle \right) \\ &= \mu_{i,l} - \lceil \mu_{i,j} \rfloor \mu_{j,l}.\end{aligned}$$

Il suffit ensuite de montrer par récurrence sur $i \leqslant l \leqslant n$ que $\widetilde{b}_l^* = b_l^*$, puisque cette égalité entraîne par définition que $\widetilde{\mu}_{k,l} = \mu_{k,l}$ pour $l < k \leqslant n$.

D'une part, d'après l'égalité (I.3) de la Proposition I.3.1, on a $b_j = \sum_{k=1}^{j} \mu_{j,k} b_k^* = \sum_{k=1}^{i-1} \mu_{j,k} b_k^*$, et donc

$$\begin{aligned}\widetilde{b}_i^* &= \widetilde{b}_i - \sum_{k=1}^{i-1} \widetilde{\mu}_{i,k} \widetilde{b}_k^* \\ &= b_i - \sum_{k=1}^{i-1} \mu_{i,k} b_k^* - \lceil \mu_{i,j} \rfloor \left(b_j - \sum_{k=1}^{i-1} \mu_{j,k} b_k^* \right) \\ &= b_i^*.\end{aligned}$$

D'autre part, par hypothèse de récurrence, si $i < l \leqslant n$,S

$$\begin{aligned}\widetilde{b}_l^* &= \widetilde{b}_l - \sum_{k=1}^{l-1} \widetilde{\mu}_{l,k} \widetilde{b}_k^* \\ &= b_l - \sum_{k=1}^{l-1} \mu_{l,k} b_k^* \\ &= b_l^*.\end{aligned}$$

Le fait que l'Algorithme I.3 mette correctement à jour le GSOP en norme est une conséquence évidente de ce qui précède. □

Lemme I.4.2 *Soient* $1 \leqslant j < i \leqslant n$.

- *Après la* (i,j)*-ième exécution de la boucle* (5) *de l'Algorithme I.2, on a pour tout* $j \leqslant k < i$

$$|\mu_{i,k}|^2 \leqslant m_K.$$

- *En arrivant au test* (8) *de l'Algorithme I.2 au rang* i*, on a pour tout* $1 \leqslant k < i$

$$|\mu_{i,k}|^2 \leqslant m_K.$$

Démonstration. Commençons par prouver le premier point. À i fixé, on procède par récurrence sur j allant de $i-1$ à 1. Comme précédemment, on note $\widetilde{\mathcal{M}}$ la famille $\mathcal{M}$ après application de l'Algorithme I.3. Plaçons nous au rang $j = i-1$. D'après le lemme précédent, on a

$$|\widetilde{\mu}_{i,i-1}|^2 = |\mu_{i,i-1} - \lceil \mu_{i,i-1} \rfloor \mu_{i-1,i-1}|^2 = |\mu_{i,i-1} - \lceil \mu_{i,i-1} \rfloor|^2 \leqslant m_K.$$

Soit $1 \leqslant j < i-1$. Supposons le résultat vrai au rang $j+1$. D'après le lemme précédent, l'égalité

$$\widetilde{\mu}_{i,l} = \mu_{i,l} - \lceil \mu_{i,j} \rfloor \mu_{j,l} = \begin{cases} \mu_{i,j} - \lceil \mu_{i,j} \rfloor & \text{si } l = j, \\ \mu_{i,l} & \text{sinon.} \end{cases}$$

est vérifiée pour tout $j \leqslant l < i$. D'où le résultat en appliquant l'hypothèse de récurrence. Le second point découle directement du premier point et du lemme précédent. □

La procédure `SIZE_RED` est donc effectivement la composante de l'Algorithme I.2 permettant d'obtenir une base du réseau considéré [7] vérifiant la condition (LLL1).

I.4.2.2 Procédure `SWAP`

Obtenir une base satisfaisant la condition de LLL-réduction (LLL2) est plus délicat ; on procède par permutation de vecteurs consécutifs de la base suivant si la condition est vérifiée. De telles permutations impliquent de mettre à jour le GSOP en norme. De manière naïve, il serait possible d'échanger les vecteurs considérés puis de recalculer complètement le GSOP en norme ; mais ceci entraîne beaucoup de calculs superflus. C'est pourquoi la fonction `SWAP` (Algorithme I.4) implante une manière optimisée de procéder, justifiée par le lemme suivant.

Lemme I.4.3 *Soit* $1 < i \leqslant n$. *Considérons la famille* $\widetilde{\mathcal{B}} := (\widetilde{b}_1, \ldots, \widetilde{b}_n)$ *définie pour tout* $1 \leqslant k \leqslant n$ *par*

$$\widetilde{b}_k := \begin{cases} b_i & \text{si } k = i-1, \\ b_{i-1} & \text{si } k = i, \\ b_k & \text{dans les autres cas.} \end{cases}$$

Notons $\widetilde{\mathcal{B}}^* := (\widetilde{b}_1^*, \ldots, \widetilde{b}_n^*)$ *et* $\widetilde{\mathcal{M}} := (\widetilde{\mu}_{i,j})_{1 \leqslant i,j \leqslant n}$ *les familles issues du GSOP de* $\widetilde{\mathcal{B}}$. *Alors :*

7. Puisque les seules opérations effectuées sont de la forme $b_j \leftarrow b_j - \lambda b_i$ avec $\lambda \in \mathcal{O}_K$.

- $\widetilde{b}_k^* = b_k$ *pour tout* $k \notin \{i-1, i\}$.
- $\widetilde{\mu}_{k,l} = \mu_{k,l}$ *pour tous* $l < k$ *et* $k, l \notin \{i-1, i\}$.
- $\widetilde{\mu}_{i,k} = \mu_{i-1,k}$ *pour tout* $k < i-1$.
- $\widetilde{\mu}_{i-1,k} = \mu_{i,k}$ *pour tout* $k < i-1$.
- $\widetilde{b}_{i-1}^* = b_i^* + \mu_{i,i-1} b_{i-1}^*$. *En particulier,* $\|\widetilde{b}_{i-1}^*\|^2 = \|b_i^*\|^2 + |\mu_{i,i-1}|^2 \|b_{i-1}^*\|^2$.
- $\widetilde{\mu}_{i,i-1} = \overline{\mu_{i,i-1}} \dfrac{\|b_{i-1}^*\|^2}{\|\widetilde{b}_{i-1}^*\|^2}$.
- $\|\widetilde{b}_i^*\|^2 = \dfrac{\|b_{i-1}^*\|^2 \|b_i^*\|^2}{\|\widetilde{b}_{i-1}^*\|^2}$.
- $\widetilde{\mu}_{k,i-1} = \mu_{k,i} \dfrac{\|b_i^*\|^2}{\|\widetilde{b}_{i-1}^*\|^2} + \mu_{k,i-1} \widetilde{\mu}_{i,i-1}$ *pour tout* $k > i$.
- $\widetilde{\mu}_{k,i} = \mu_{k,i-1} - \mu_{k,i} \mu_{i,i-1}$ *pour tout* $k > i$.

En particulier, l'Algorithme I.4 met correctement à jour le GSOP en norme de la base $\mathcal{B}$ *après un échange* $b_i \hookleftarrow b_{i-1}$ *dans l'Algorithme I.2.*

Démonstration. La preuve est purement calculatoire. □

```
Données :
    • Une base B := (b_1, ..., b_n) d'un O_K-réseau Λ de C^n.
    • Les familles N := (N_1, ..., N_n) et M := (μ_{i,j})_{1≤i,j≤n} du GSOP en norme de B.
    • L'indice 1 < i ≤ m pour l'échange b_i ↔ b_{i-1}.
Résultat :
    • La base B après l'échange.
    • Les mises à jour de N et M correspondantes.
(B̃, Ñ, M̃) ← (B, N, M)
b̃_{i-1} ← b_i
b̃_i ← b_{i-1}
Ñ_{i-1} ← N_i + |μ_{i,i-1}|^2 N_{i-1}
Ñ_i ← N_i N_{i-1} / Ñ_{i-1}
μ̃_{i,i-1} ← conj(μ_{i,i-1}) N_{i-1} / Ñ_{i-1}
pour k = 1 à i-2 faire
    μ̃_{i,k} ← μ_{i-1,k}
    μ̃_{i-1,k} ← μ_{i,k}
pour k = i+1 à n faire
    μ̃_{k,i-1} ← μ_{k,i} N_i / Ñ_{i-1} + μ_{k,i-1} μ̃_{i,i-1}
    μ̃_{k,i} ← μ_{k,i-1} - μ_{k,i} μ_{i,i-1}
retourner (B̃, Ñ, M̃)
```

Algorithme I.4 - Fonction SWAP.

I.4.2.3 Bilan

Finalement, les lemmes précédents permettent de conclure sur le résultat renvoyé par l'Algorithme I.2.

Proposition I.4.4 *À chaque entrée dans la boucle principale* (4) *de l'Algorithme I.2 au rang* $1 \leqslant i \leqslant n$*, on a*

- $|\mu_{k,l}|^2 \leqslant m_K$ *pour tous* $1 \leqslant l < k < i$.
- $\|b_k^*\|^2 \geqslant (\delta - |\mu_{k,k-1}|^2)\|b_{k-1}^*\|^2$ *pour tout* $1 < k < i$.

En particulier, si l'Algorithme I.2 se termine, il renvoie une base [8] (m_K, δ)*-LLL réduite du* $\mathcal{O}_K$*-réseau* Λ.

Démonstration. On procède par récurrence sur $1 \leqslant i \leqslant n$. Initialement, il n'y a rien à démontrer puisque $i = 2$. Plaçons nous à un rang $1 \leqslant i \leqslant n$ quelconque, et supposons les deux invariants vrais en entrant en (4). Montrons qu'ils restent vrais en (12).

- D'après le Lemme I.4.2 et l'hypothèse de récurrence, en arrivant au test (8), on a $|\mu_{k,l}|^2 \leqslant m_K$ pour tous $1 \leqslant l < k < i$, mais aussi pour $1 \leqslant l < k = i$. Dès lors, d'après Lemme I.4.3, le premier invariant est vérifié en (12), qu'il y ait échange $b_{i-1} \hookleftarrow b_i$ ou non.
- La famille $\mathcal{B}^*$ n'est pas modifiée par la boucle (5) d'après le Lemme I.4.2. D'autre part, d'après le Lemme I.4.3, un échange $b_{i-1} \hookleftarrow b_i$ n'affecte pas les b_k^* et les $\mu_{k,l}$ pour $1 \leqslant l < k < i-1$. Ainsi, s'il y a échange, le deuxième invariant est vrai en (12). Mais c'est aussi le cas si l'échange n'est pas effectué, par définition du test (8).

Le cas particulier est vrai puisque l'algorithme se termine lorsque $i = n+1$. □

Nous avons donc montré que l'Algorithme I.2 effectue correctement le calcul attendu ; reste à montrer qu'il se termine.

I.4.3 Terminaison et complexité

La terminaison de l'Algorithme I.2 n'est pas immédiate. Afin de la prouver, on étudie les variations des déterminants de Gram successifs de la base initiale. On suppose que $n \geqslant 2$ (si $n = 1$, il n'y a rien à vérifier). Dans la suite , on note B, B^* et M les matrices de $\mathcal{B}$, $\mathcal{B}^*$ et $\mathcal{M}$ (dans la base standard de $\mathbb{C}^n$) respectivement, de sorte que $B = MB^*$ (égalité démontrée dans la Proposition I.3.1). Pour tout $1 \leqslant r \leqslant n$, soit B_r (resp. B_r^*) la matrice de $\mathcal{B}_r := (b_1, \ldots, b_r)$ (resp. de $\mathcal{B}_r^* := (b_1^*, \ldots, b_r^*)$). On note $\Delta_r(\mathcal{B})$ le déterminant de Gram de $\mathcal{B}_r$. On pose aussi $\Delta_0(\mathcal{B}) := 1$.

Lemme I.4.5 *Pour tout* $1 \leqslant r \leqslant n$*, on a*

$$\Delta_r(\mathcal{B}) = \prod_{i=1}^{r} \|b_i^*\|^2.$$

8. Encore une fois, les seules opérations effectuées sont de la forme $b_j \leftarrow b_j - \lambda b_i$ avec $\lambda \in \mathcal{O}_K$ et $b_{i-1} \hookleftarrow b_i$.

Démonstration. Il suffit de remarquer que $\mathcal{B}_r^*$ est la famille associée au GSOP de $\mathcal{B}_r$ et d'appliquer le Corollaire I.3.2. □

Considérons maintenant la grandeur

$$\Delta_\infty(\mathcal{B}) := \prod_{r=1}^{n-1} \Delta_r(\mathcal{B}) = \prod_{r=1}^{n-1} \prod_{i=1}^{r} \|b_i^*\|^2.$$

Nous allons montrer que $\Delta_\infty(\mathcal{B})$ ne peut que décroître au cours de l'exécution de l'Algorithme I.2. Ceci permettra de prouver la convergence annoncée. Commençons par minorer $\Delta_\infty(\mathcal{B})$ indépendamment de la base $\mathcal{B}$.

Lemme I.4.6 *La grandeur $\Delta_\infty(\mathcal{B})$ est minorée indépendamment de la base $\mathcal{B}$ de Λ choisie :*

$$\Delta_\infty(\mathcal{B}) \geqslant m(\Lambda)^{\frac{n(n-1)}{2}} \prod_{r=1}^{n-1} \gamma_{K,r}^{-r}.$$

Démonstration. Pour tout $1 \leqslant r \leqslant n$, notons Λ_r le $\mathcal{O}_K$-réseau de $\mathbb{C}^r$ de base $\mathcal{B}_r$. D'après la Proposition I.2.12, $\Delta_r(\mathcal{B}) = \Delta(\Lambda_r)$. Comme conséquence de l'inégalité de Hermite, nous avons vu dans la Proposition I.2.22 que

$$\Delta_r(\mathcal{B}) \geqslant m(\Lambda_r)^r \gamma_{K,r}^{-r} \geqslant m(\Lambda)^r \gamma_{K,r}^{-r}.$$

Ainsi :

$$\Delta_\infty(\mathcal{B}) = \prod_{r=1}^{n-1} \Delta_r(\mathcal{B}) \geqslant \prod_{r=1}^{n-1} m(\Lambda)^r \gamma_{K,r}^{-r} = m(\Lambda)^{\frac{n(n-1)}{2}} \prod_{r=1}^{n} \gamma_{K,r}^{-r}.$$ □

D'après le Lemme I.4.2, $\mathcal{B}^*$ n'est pas modifiée par l'application de la procédure `SIZE_RED` (Algorithme I.3). Ainsi, $\Delta_\infty(\mathcal{B})$ n'est pas modifié par la boucle (5) de l'Algorithme I.2. Reste donc à étudier l'effet de `SWAP` (Algorithme I.4) sur cette grandeur.

Lemme I.4.7 *Soit $1 < i \leqslant n$. Supposons que le test (8) de l'Algorithme I.2 est validé au rang i, et donc que b_{i-1} et b_i sont échangés. Notons $\widetilde{\mathcal{B}}$ la famille $\mathcal{B}$ après cet échange (c'est-à-dire après l'application de* `SWAP`*) et $\widetilde{\mathcal{B}}^*$ son GSOP. Alors :*

- $\|\widetilde{b}_{i-1}^*\|^2 < \delta \|b_i^*\|^2$.
- $\Delta_r(\widetilde{\mathcal{B}}) = \Delta_r(\mathcal{B})$ *pour tout* $0 \leqslant r \leqslant n$, $r \neq i-1$.
- $\Delta_{i-1}(\widetilde{\mathcal{B}}) \leqslant \delta \Delta_{i-1}(\mathcal{B})$.

Démonstration.

- D'après le Lemme I.4.3, on a $\|\widetilde{b}_{i-1}^*\|^2 = \|b_i^*\|^2 + |\mu_{i,i-1}|^2 \|b_{i-1}^*\|^2$. Puisqu'on suppose le test (8) validé, on a $\|b_i^*\|^2 < (\delta - |\mu_{i,i-1}|^2)\|b_{i-1}^*\|^2$. Donc $\|\widetilde{b}_{i-1}^*\|^2 < \delta \|b_i^*\|^2$.
- Soit $r \neq i-1$. Si $r < i-1$, le résultat est trivial, puisque $\widetilde{\mathcal{B}}_r = \mathcal{B}_r$. Supposons donc que $r \geqslant i$. L'échange de b_i et b_{i-1} correspond à l'application d'une matrice de permutation P à $\mathcal{B}$. Ainsi :
$$\mathrm{Gram}(\widetilde{\mathcal{B}}_r) = P \cdot \mathrm{Gram}(\mathcal{B}_r) \cdot P^{\intercal}.$$
Comme les matrices de permutation sont orthogonales, on obtient que $\Delta_r(\widetilde{\mathcal{B}}) = \delta \Delta_r(\mathcal{B})$.

- On sait d'après le Lemme I.4.5 que

$$\begin{cases} \Delta_{i-1}(\mathcal{B}) = \prod_{k=1}^{i-1} \|b_k^*\|^2 = \Delta_{i-2}(\mathcal{B})\|b_{i-1}^*\|^2, \\ \Delta_{i-1}(\widetilde{\mathcal{B}}) = \prod_{k=1}^{i-1} \|\widetilde{b}_k^*\|^2 = \Delta_{i-2}(\widetilde{\mathcal{B}})\|\widetilde{e}_{i-1}^*\|^2. \end{cases}$$

D'une part, d'après le premier point, $\|\widetilde{b}_{i-1}^*\|^2 < \delta\|b_i^*\|^2$, et d'autre part, d'après le second point, $\Delta_{i-2}(\widetilde{\mathcal{B}}) = \Delta_{i-2}(\mathcal{B})$. D'où le résultat. □

Proposition I.4.8 *Notons $\mathcal{B} := (b_1, \dots, b_n)$ la base initiale de Λ donnée en entrée de l'Algorithme I.2 et $\|\mathcal{B}\|_\infty := \max_{1\leqslant i\leqslant n} \|b_i\|$. On a :*

- $\Delta_\infty(\mathcal{B}) \leqslant \|\mathcal{B}\|_\infty^{n(n-1)}$.
- *Si $\widetilde{\mathcal{B}}$ désigne la base de Λ obtenue à partir de $\mathcal{B}$ après une itération de la boucle principale (4) de l'Algorithme I.2, on a $\Delta_\infty(\widetilde{\mathcal{B}}) \leqslant \delta\Delta_\infty(\mathcal{B})$. En particulier,*

$$O\left(n^2 \log_\delta\left(\frac{m(\Lambda)\prod_{r=1}^{n-1}\gamma_{K,r}^{-r/n^2}}{\|\mathcal{B}\|_\infty}\right)\right)$$

appels à la procédure SWAP *sont effectués par l'Algorithme I.2*

Démonstration.

- Par définition, on a

$$\Delta_\infty(\mathcal{B}) = \prod_{r=1}^{n-1}\prod_{i=1}^{r} \|b_i^*\|^2 = \prod_{r=1}^{n-1} \|b_r^*\|^{2(n-r)}.$$

Or d'après la Proposition I.3.1, on a $\|b_r^*\|^2 \leqslant \|b_r\|^2$ pour tout $1 \leqslant r \leqslant n$. Ainsi :

$$\begin{aligned} \Delta_\infty(\mathcal{B}) &= \prod_{r=1}^{n-1} \|b_r^*\|^{2(n-r)} \\ &\leqslant \prod_{r=1}^{n-1} \|b_r\|^{2(n-r)} \\ &\leqslant \prod_{r=1}^{n-1} \|\mathcal{B}\|_\infty^{2(n-r)} \\ &= \|\mathcal{B}\|_\infty^{n(n-1)}. \end{aligned}$$

- Soit un appel à SWAP est effectué, et dans ce cas $\Delta_\infty(\widetilde{\mathcal{B}}) \leqslant \delta\Delta_\infty(\mathcal{B})$ d'après le lemme précédent, soit SWAP n'est pas appelée et $\Delta_\infty(\widetilde{\mathcal{B}}) = \Delta_\infty(\mathcal{B})$.

Calculons le nombre maximal d'appels à SWAP qu'il est possible d'effectuer. D'après le Lemme I.4.6, l'inégalité

$$\Delta_\infty(\widetilde{\mathcal{B}}) \geqslant m(\Lambda)^{\frac{m(m-1)}{2}} \prod_{r=1}^{n-1} \gamma_{K,r}^{-r}$$

est vérifiée pour toute base $\widetilde{\mathcal{B}}$ de Λ calculée en tout point de l'Algorithme I.2. Il est donc possible d'effectuer au plus

$$\max\left\{ m \in \mathbb{N} : \delta^m \Delta_\infty(\mathcal{B}) \geqslant m(\Lambda)^{\frac{m(m-1)}{2}} \prod_{r=1}^{n-1} \gamma_{K,r}^{-r} \right\}$$

appels à SWAP, c'est-à-dire au plus

$$\left\lfloor \log_\delta\left(m(\Lambda)^{\frac{m(m-1)}{2}} \prod_{r=1}^{n-1} \gamma_{K,r}^{-r} \right) - \log_\delta\left(\Delta_\infty(\mathcal{B})\right) \right\rfloor.$$

Finalement, d'après le premier point, le nombre d'utilisation de SWAP est borné par

$$\log_\delta\left(m(\Lambda)^{\frac{m(m-1)}{2}} \prod_{r=1}^{n-1} \gamma_{K,r}^{-r} \right) - \log_\delta\left(\|\mathcal{B}\|_\infty^{n(n-1)}\right) \in O\left(n^2 \log_\delta\left(\frac{m(\Lambda)\prod_{r=1}^{n-1} \gamma_{K,r}^{-r/n^2}}{\|\mathcal{B}\|_\infty} \right) \right).$$

□

La terminaison est alors un corollaire immédiat.

Corollaire I.4.9 *L'Algorithme I.2 se termine.*

Démonstration. Nous avons montré que le nombre d'appels à SWAP est fini, ce qui prouve directement la terminaison annoncée. □

Finalement, les résultats de ce paragraphe et du précédent permettent de conclure à la correction de l'algorithme. Nous y ajoutons une analyse de sa complexité algébrique. Cette complexité est exprimée en terme du nombre d'opérations élémentaires effectuées, c'est-à-dire les opérations exécutées dans $\mathbb{C}$ [9]. Notons néanmoins qu'il n'est pas judicieux de les considérer comme opérations algorithmiques effectuées à temps constant, et ceci même dans le cas rationnel usuel. Une étude plus détaillée de cette question se trouve dans [VZGG03, p.473-475].

Théorème I.4.10 *Soient $K := \mathbb{Q}(i\sqrt{D})$ avec $D \in \{1,2,3,7,11\}$ et $n \in \mathrm{N}_{\geqslant 1}$. Étant donnée une base $\mathcal{B}$ d'un $\mathcal{O}_K$-réseau Λ de $\mathbb{C}^n$ et un paramètre δ tel que $m_K < \delta < 1$, l'Algorithme I.2 renvoie une base (m_K, δ)-LLL réduite de Λ en effectuant*

$$O\left(n^4 \log_\delta\left(\frac{m(\Lambda)\prod_{r=1}^{n-1} \gamma_{K,r}^{-r/n^2}}{\|\mathcal{B}\|_\infty} \right) \right)$$

opérations élémentaires.

9. Si $\Lambda \subset K^n$ (resp. $\Lambda \subset \mathcal{O}_K^n$), toutes les opérations considérées sont effectuées dans K (resp. dans $\mathcal{O}_K$).

Démonstration. La terminaison et la correction du résultat ont été démontrées par la Proposition I.4.4 et le corollaire précédent. Reste l'analyse de complexité.

La fonction `normGSOP` (Algorithme I.1) effectue $O(n^3)$ opérations élémentaires. En effet, au rang $1 \leqslant i < j \leqslant n$, le calcul de $\mu_{i,j}$ et de N_j prends un nombre $s_{i,j} \in O(n)$ d'opérations élémentaires, et l'algorithme nécessite donc

$$\left(\sum_{j=1}^{n}\sum_{i=j+1}^{n} s_{i,j}\right) \in O\left(nr^3\right)$$

opérations élémentaires. Il est facile de voir que la fonction `SWAP`(Algorithme I.4) effectue $O(n)$ opérations élémentaires. D'autre part, chaque appel à la procédure `SIZE_RED` (Algorithme I.3) entraîne $O(n)$ opérations élémentaires, et donc le coût de la boucle (5)de l'Algorithme I.2 est $O(n^2)$ opérations élémentaires. Ainsi, chaque itération de la boucle principale (4) de l'Algorithme I.2 nécessite $O(n^2)$ opérations élémentaires.

Calculons le nombre d'iterations de la boucle (4) effectuée par l'Algorithme I.2. Si s et p désignent respectivement le nombre d'appels à `SWAP` effectué par l'algorithme et le nombre de fois que la condition (8) a été invalidée à un instant donné, alors l'entier $\kappa = i + s - p$ est constant tout au long de l'exécution (puisque $i \leftarrow i+1$ entraîne $p \leftarrow p+1$ et $i \leftarrow i-1$ entraîne $s \leftarrow s+1$). Or initialement, $\kappa = 2$. Puisque l'algorithme se termine lorsque $i = n+1$, on obtient une fois l'exécution terminée $n+1+s-p = 2$. Mais le nombre d'itérations de (4) est donné par $s+p$ à la fin de l'exécution.

Ainsi, le nombre d'itérations de (4) est, d'après la Proposition I.4.8 :

$$s + p = 2s + n - 1 \in O\left(n^2 \log_\delta\left(\frac{m(\Lambda)\prod_{r=1}^{n-1}\gamma_{K,r}^{-r/n^2}}{\|\mathcal{B}\|_\infty}\right)\right).$$

En conclusion : l'algorithme effectue un premier calcul de $O(n^3)$ opérations élémentaires, puis

$$O\left(n^2 \log_\delta\left(\frac{m(\Lambda)\prod_{r=1}^{n-1}\gamma_{K,r}^{-r/n^2}}{\|\mathcal{B}\|_\infty}\right)\right)$$

itérations, chacune entraînant $O(n^2)$ opérations élémentaires. Ainsi,

$$O\left(n^4 \log_\delta\left(\frac{m(\Lambda)\prod_{r=1}^{n-1}\gamma_{K,r}^{-r/n^2}}{\|\mathcal{B}\|_\infty}\right)\right)$$

opérations élémentaires sont effectuées. □

Remarque I.4.11 La terminaison de l'algorithme découle essentiellement du Lemme I.4.6, qui est lui même une conséquence de la propriété d'unimodularité (P1). Toute hypothèse sur les corps de nombres ou les réseaux considérés permettant d'établir une minoration de $\Delta_\infty(\mathcal{B})$ indépendamment de la base du réseau choisie permet de prouver la convergence de l'algorithme.

I.5 Analyse heuristique du cas moyen

Dans cette section, on fixe $K := \mathbb{Q}(i\sqrt{D})$ avec $D \in \{1, 2, 3, 7, 11\}$.

I.5.1 Idée générale

Lorsque $\mathcal{B} := (b_1, \ldots, b_n)$ est une base (δ, m_K)-LLL réduite d'un $\mathcal{O}_K$ réseau Λ de $\mathbb{C}^n$, nous avons montré dans le Théorème I.3.8 que

$$\|b_1\|^2 \leqslant \left(\frac{1}{\delta - m_K}\right)^{n-1} m(\Lambda).$$

Pour établir cette inégalité, nous avons supposé que les coefficients $\mu_{i,i-1}$ associés au GSOP de $\mathcal{B}$ atteignent la borne de réduction (LLL1), c'est-à-dire que $|\mu_{i,i-1}|^2 = m_K$ pour tout $2 \leqslant i \leqslant n$. En pratique, cette borne est rarement atteinte : le vecteur obtenu est généralement plus court que ce que prévoit l'estimation théorique. C'est pourquoi, en adaptant les travaux de [SBL10], nous remplaçons cette hypothèse par une distribution probabiliste des coefficients $|\mu_{i,i-1}|^2$, obtenue empiriquement. Nous faisons cette étude pour le SVP_γ ; il est néanmoins possible d'obtenir des résultats similaires concernant le défaut d'orthogonalité en s'inspirant de la méthode présentée.

Proposition I.5.1 *Soit $\mathcal{B} := (b_1, \ldots, b_n)$ une base de $\mathbb{C}^n$ choisie arbitrairement [10], à laquelle on a appliqué l'Algorithme I.2 avec un coefficient δ tel que $m_K < \delta < 1$. Soit Λ le $\mathcal{O}_K$-réseau de $\mathbb{C}^n$ de base $\mathcal{B}$. Supposons que les coefficients $|\mu_{i,i-1}|^2$ associés au GSOP de $\mathcal{B}$ sont des variables aléatoires de même loi, donnée par une densité de probabilité p. Alors :*

$$\mathbb{E}(\log(\|b_1\|^2)) \leqslant \mathbb{E}(\log(m(\Lambda))) - (n-1)\int_0^{m_K} \log(\delta - x)p(x)dx. \tag{I.6}$$

Démonstration. Puisque $\mathcal{B}$ est supposée (m_K, δ)-LLL réduite, une récurrence immédiate montre que pour tout $2 \leqslant k \leqslant n$

$$\|b_1\|^2 \prod_{i=2}^{k} (\delta - |\mu_{i,i-1}|^2) \leqslant \|b_k^*\|^2,$$

ce qui entraîne d'après le Lemme I.3.7 que

$$\|b_1\|^2 \prod_{i=2}^{n} (\delta - |\mu_{i,i-1}|^2) \leqslant m(\Lambda).$$

En passant au logarithme puis en prenant les espérances, on obtient finalement

$$\mathbb{E}(\log(\|b_1\|^2)) \leqslant \mathbb{E}(\log(m(\Lambda))) - \sum_{i=2}^{n} \mathbb{E}(\log(\delta - |\mu_{i,i-1}|^2)).$$

10. Nous nous contentons ici d'utiliser la terminologie « base choisie arbitrairement », quelque peu impropre. Nous donnons dans la Remarque I.5.2 plus de détails sur la notion de *base aléatoire*.

Or les $|\mu_{i,i-1}|^2$ sont des variables aléatoires de même loi donnée par la densité de probabilité p, et donc pour tout $2 \leqslant i \leqslant n$, on a

$$\mathbb{E}(\log(\delta - |\mu_{i,i-1}|^2)) = \int_0^{m_K} \log(\delta - x)p(x)dx.$$

D'où le résultat. □

Une fois connue la distribution des coefficients $|\mu_{i,i-1}|^2$, cette proposition fournit un résultat « en moyenne » sur la longueur du premier vecteur obtenu par LLL-réduction, contrairement au Théorème I.3.8 qui fournit un résultat « dans le pire cas ». Cependant, afin d'établir ce résultat moyen, il nous faut déterminer la densité p régissant la distribution des $|\mu_{i,i-1}|^2$. Cet un exercice délicat, qui est actuellement hors de notre portée. C'est pourquoi, comme dans [SBL10], cette densité est approximée de manière empirique.

I.5.2 Résultats expérimentaux

On garde les notations du paragraphe précédent. Nous détaillons dans ce paragraphe comment la distribution des $|\mu_{i,i-1}|^2$ a été expérimentalement déterminée et les conclusions que nous en avons tirée.

I.5.2.1 Méthode

Dans un premier temps, nous avons tiré 500 bases de $\mathbb{C}^n$, pour n variant entre 50 et 150. Nous avons pour cela généré des familles aléatoires de n vecteurs de $\mathbb{C}^n$, ce qui fournit presque sûrement une base de $\mathbb{C}^n$. L'application du GSOP à la famille générée permet de s'en assurer : l'obtention d'un vecteur nul lors du GSOP signifie exactement que la famille est liée. Après plusieurs séries de tests en des dimensions variables, nous avons remarqué que la distribution des coefficients $|\mu_{i,i-1}|^2$ ne varie pas suivant la dimension utilisée. Nous avons donc choisi de travailler en petite dimension, de manière à effectuer un grand nombre de calculs en un temps raisonnable. Nous avons implanté une version adaptée [11] de l'Algorithme I.2, utilisée pour obtenir la distribution empirique discrète des coefficients $|\mu_{i,i-1}|^2$.

Remarque I.5.2 Lors d'une étude heuristique et/ou probabiliste, la notion de *réseau aléatoire* peut avoir plusieurs définitions :

- On peut se contenter de choisir aléatoirement une base de l'espace euclidien ou hermitien considéré, ce qui revient à tirer un élément de $\mathrm{GL}_n(\mathbb{R})$ ou $\mathrm{GL}_n(\mathbb{C})$. En procédant de la sorte, on néglige le fait que deux bases peuvent engendrer le même réseau. Choisir aléatoirement une base n'est donc pas équivalent au fait de choisir aléatoirement un élément de l'ensemble des réseaux d'une dimension donnée. Plusieurs familles d'éléments de $\mathrm{GL}_n(\mathbb{R})$ sont populaires dans le cadre de tirages aléatoires, comme les bases de Ajtai [Ajt03], les bases de type *knapsack* [GM03], les bases de déterminant borné ou les bases de norme (l_p ou infinie) bornée.

11. De sorte à limiter le nombre de calculs, puisqu'on ne s'intéresse qu'aux coefficients $\mu_{i,i-1}$.

- Il est possible de choisir de manière aléatoire et uniforme un élément de l'ensemble des réseaux équipé d'une mesure fixée. Plusieurs choix sont naturels pour cette mesure, provenant généralement d'extensions de la mesure de Lebesgue [Ngu07, §3.4, p.52–54].

Nous avons choisit d'exprimer la Proposition I.5.1 avec des bases aléatoires ; il est tout à fait possible de réécrire ce résultat en termes de réseaux aléatoires. C'est d'ailleurs ce format qui est utilisé dans [SBL10]. De même, les résultat expérimentaux présentés dans ce paragraphe ont été obtenus en générant des bases aléatoires de norme infinie bornée. La méthodologie présentée reste valable pour d'autres types de tirages, mais les conclusions peuvent différer ; la distribution des $\mu_{i,i-1}$ peut fortement varier suivant la distribution des bases ou réseaux choisie.

La méthode de Levenberg-Marquardt, implantée par la commande `fit` du logiciel [Gnuplot], a ensuite permis d'interpoler cette distribution discrète avec une fonction de la forme :

$$p(x) = \begin{cases} \frac{a}{x+b} e^{-x/c} & \text{si } x \in [0, m_K], \\ 0 & \text{sinon.} \end{cases}$$

Une fois normalisée, c'est-à-dire divisée par la valeur de son intégrale (calculée avec [Scilab]), cette fonction peut être considérée comme la densité de probabilité de la distribution recherchée. Dès lors, le calcul de $\int_0^{m_K} \log(\delta - x) p(x) dx$ a pu être effectué avec [Scilab].

I.5.2.2 Résultats et conclusions

La Figure I.6 présente la distribution et l'interpolation obtenue dans le cas $D = 1$. Les valeurs obtenues pour les autres valeurs de D (qui sont très similaires) sont présentées sur la Figure I.7. Les résultats des différents calculs effectués sont détaillés pour toutes les valeurs admissibles de D dans la Figure I.5.

La borne extrémale (I.5) du Théorème I.3.8 peut se réécrire sous la forme

$$\log(\|b_1\|^2) \leqslant \log(m(\Lambda)) + (n-1) \log\left(\frac{1}{\delta - m_K}\right).$$

On peut donc voir la grandeur $\log\left(\frac{1}{\delta - m_K}\right)$ comme un facteur correctif entre $\log(m(\Lambda))$ et $\log(\|b_1\|^2)$ dans le pire cas. Dans le cas moyen, l'inégalité (I.6) de la Proposition I.5.1 prédit que ce facteur correctif est égal à $-\int_0^{m_K} \log(\delta - x) p(x) dx$. Le rapport entre ces deux grandeurs présenté dans la dernière ligne de la Figure I.5 permet donc de comparer les prédictions du cas moyens face à celles du pire cas. Ce rapport oscille entre $0,06$ et $0,17$: le facteur correctif du cas moyen est entre $5,8$ fois et $16,6$ fois plus petit que le facteur correctif du pire cas. De manière impropre, la version moyenne de l'inégalité (I.5) est

$$\|b_1\|^2 \leqslant \left(\frac{1}{\delta - \eta_k}\right)^{\alpha_K (n-1)} m(\Lambda),$$

où $0,06 \leqslant \alpha_K \leqslant 0,17$ est le coefficient de la dernière ligne de la Figure I.5. En conclusion : le premier vecteur d'une base (δ, m_K)-LLL réduite d'un $\mathcal{O}_K$-réseau $\Lambda \subset \mathbb{C}^n$ est en moyenne $\left(\frac{1}{\delta-\eta_k}\right)^{\alpha_K}$ fois plus court que ce que prévoit la théorie.

D	1	2	3	7	11
m_K	0,5	0,75	0,333333	0,571429	0,81818
a	0,0012326	0,0016804	0,00078509	0,0013315	0,001728
b	0,0050013	0,0053303	0,0041403	0,0049369	0,005117
c	0,24963	0,27361	0,37761	0,25022	0,27178
$\int_0^{m_K} p(x)dx$	0,004157	0,005762	0,002924	0,004530	0,005991
$\int_0^{m_K} \log(\delta - x)\tilde{p}(x)dx$	- 0,076510	- 0,0918323	- 0,070841	- 0,079664	- 0,092795
$\frac{\int_0^{m_K} \log(\delta-x)\tilde{p}(x)dx}{\log(\delta-\eta_k)}$	0,107254	0,064348	0,168436	0,091472	0,052685

Fig. I.5 – Résultats expérimentaux sur les distributions des $|\mu_{i,i-1}|^2$. On désigne par $\tilde{p}$ la normalisation de p.

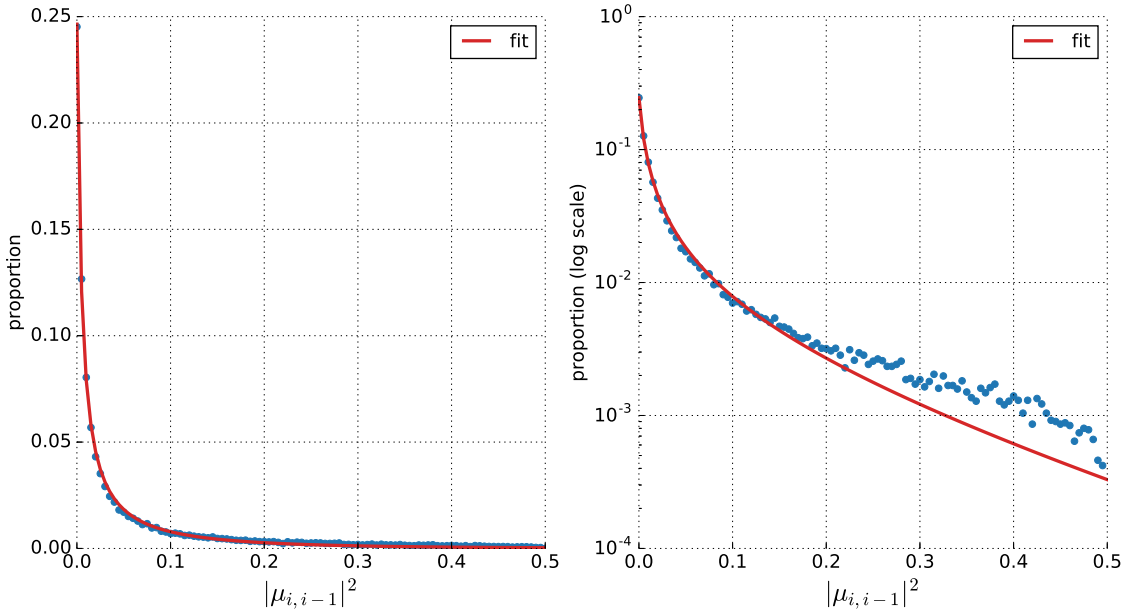


Fig. I.6 – Distribution et interpolations obtenues pour $K = \mathbb{Q}(i)$ et $\delta = 0,99$. Échelle linéaire à gauche, logarithmique à droite.

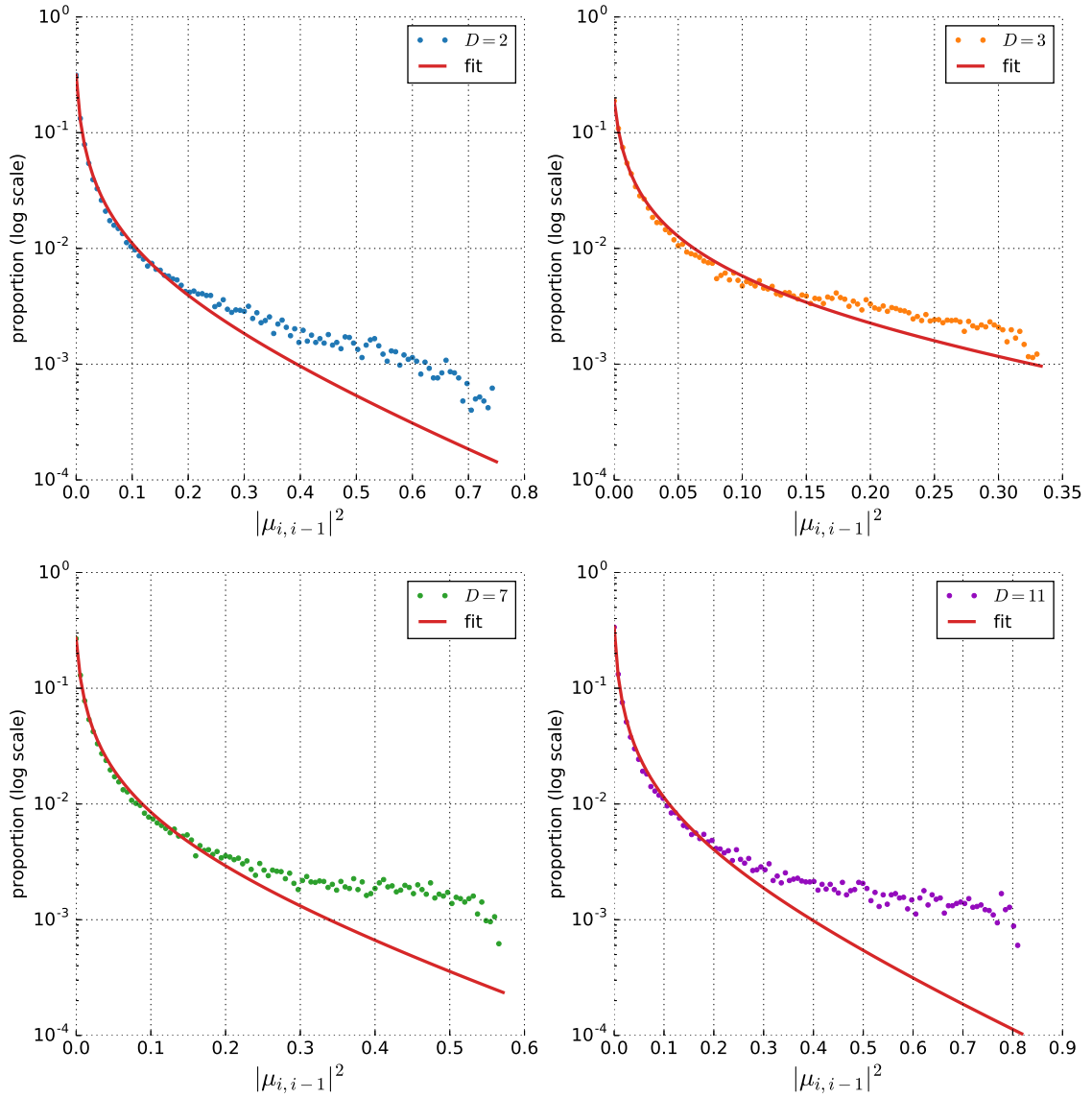


Fig. I.7 – Distribution et interpolations obtenues pour $K = \mathbb{Q}(i\sqrt{D})$ avec $D \in \{2, 3, 7, 11\}$ et $\delta = 0,99$ (échelles logarithmiques).

II

RÉSEAUX ET FORMES : LE CADRE ALGÉBRIQUE GÉNÉRALISÉ

Sommaire

II.1 Introduction

Ce chapitre introduit les notions de réseaux algébriques (généralisation des réseaux euclidiens) et de formes de Humbert (généralisation des formes quadratiques définies positives). Nous nous plaçons dans un cadre de travail aussi étendu que possible, qui englobe notamment le cas euclidien et le cas quadratique imaginaire présenté dans le chapitre précédent. Nous explicitons et généralisons de ce fait plusieurs résultats connus concernant ces objets. Nous mettons en particulier en valeur la correspondance profonde qui relie les réseaux algébriques et les formes de Humbert. Nous proposons aussi une extension des résultats de Leibak [Lei05] sur la constante de Hermite généralisée dans un contexte additif. Ce chapitre est donc essentiellement un travail de collection, de réécriture et de généralisation de divers définitions et résultats issus de la littérature. Dans cet objectif, nous prenons le soin de détailler les démonstrations, de manière à les rendre aussi élémentaires que possible.

Pour plus de détails sur le contexte général des corps de nombres, et plus précisément sur la théorie de Minkowski, nous renvoyons le lecteur vers [Neu13 ; Sam67]. Pour tout ce qui a trait à la théorie classique des réseaux et formes quadratiques, l'excellent livre de Martinet [Mar03] reste une référence incontournable. Concernant les réseaux algébriques, nous utilisons principalement les définitions de [O'M73 ; FS10 ; OY10]. Enfin, les références employées pour les formes de Humbert sont essentiellement les articles originaux de Humbert [Hum39 ; Hum49], ainsi que [Lei05].

II.2 Corps de nombres et structure euclidienne

II.2.1 Espace euclidien associé à un corps de nombres

Soient K un corps de nombres de degré d et $\mathcal{O}_K$ son anneau d'entiers. Soient (r,s) la signature de K et $\delta := r+s$. L'ensemble Σ_K des plongements de corps de K dans $\mathbb{C}$ est ordonné de la manière suivante :

- On désigne par $\sigma_1,\dots,\sigma_r$ les plongements réels de K.
- On désigne par $\sigma_{r+1},\dots,\sigma_d$ les plongements complexes de K, de telle sorte que $\sigma_{\delta+i} = \overline{\sigma}_{r+i}$ pour tout $1 \leqslant i \leqslant s$.

L'ensemble $K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R}$ est un $\mathbb{Q}$-espace vectoriel de dimension infinie, un K-espace vectoriel (à gauche) de dimension infinie mais aussi une $\mathbb{R}$-algèbre (à droite) de dimension d. Un plongement $\sigma \in \Sigma_K$ se prolonge naturellement [1] en un morphisme de $\mathbb{R}$-algèbres $\sigma : K_{\mathbb{R}} \longrightarrow \mathbb{C}$ en posant $\sigma(x \otimes y) := y\sigma(x)$ pour tous $x \in K$ et $y \in \mathbb{R}$. En tant que $\mathbb{R}$-espaces vectoriels, $K_{\mathbb{R}}$ et $\mathbb{R}^r \oplus \mathbb{C}^s$ sont isomorphes, et un isomorphisme est donné par

$$\begin{array}{rccc} \Phi_1 : & K_{\mathbb{R}} & \longrightarrow & \mathbb{R}^r \oplus \mathbb{C}^s \subset \mathbb{C}^\delta \\ & x & \longmapsto & (\sigma_1(x),\dots,\sigma_\delta(x)) \end{array} .$$

1. Dans le sens où il existe un unique prolongement $\tilde{\sigma}$ de σ en un morphisme de $\mathbb{R}$-algèbres tel que $\tilde{\sigma}(x \otimes 1) = \sigma(x)$ pour tout $x \in K$.

Cet isomorphisme n'est pas canonique : il dépend de l'agencement choisit sur Σ_K. On munit $K_{\mathbb{R}}$ du produit scalaire euclidien défini pour tous $x, y \in K_{\mathbb{R}}$ par

$$T_2(x,y) := \sum_{\sigma\in\Sigma_K} \overline{\sigma}(x)\sigma(y),$$

On appelle norme T_2 la norme euclidienne associée. On introduit un produit scalaire sur $\mathbb{R}^r \oplus \mathbb{C}^s$ faisant de Φ_1 une isométrie en posant pour tous $x, y \in \mathbb{R}^r \oplus \mathbb{C}^s$

$$\langle x \,|\, y\rangle := \sum_{i=1}^{r} x_i y_i + \sum_{i=r+1}^{\delta} 2\Re(\overline{x_i} y_i) = \sum_{i=1}^{\delta} \varepsilon_i \Re(\overline{x_i} y_i),$$

où $\varepsilon_i = 1$ si $1 \leqslant i \leqslant r$ et $\varepsilon_i = 2$ si $r+1 \leqslant i \leqslant \delta$.

Posons $K_{\mathbb{R}}^n := (K \otimes_{\mathbb{Q}} \mathbb{R})^n$. C'est un $\mathbb{R}$-espace vectoriel de dimension nd, un K-espace vectoriel de dimension infinie mais aussi un $K_{\mathbb{R}}$-module libre de rang n. Si $x \in K_{\mathbb{R}}^n$ et $\sigma \in \Sigma$, on note $\sigma(x)$ le vecteur obtenu en appliquant σ à chacune des composantes de x. On déduit de Φ_1 un isomorphisme (lui aussi non canonique) de $\mathbb{R}$-espaces vectoriels :

$$\begin{array}{rccc} \Phi_n : & K_{\mathbb{R}}^n & \longrightarrow & \left\{x \in (\mathbb{C}^n)^\delta \,:\, x_1, \dots, x_r \in \mathbb{R}^n\right\} . \\ & x & \longmapsto & (\sigma_1(x), \dots, \sigma_\delta(x)) \end{array}$$

Dans la suite, on pose [2]

$$\mathbb{R}^{nr} \oplus \mathbb{C}^{ns} := \left\{x \in (\mathbb{C}^n)^\delta \,:\, x_1, \dots, x_r \in \mathbb{R}^n\right\}.$$

Afin d'alléger les notations et lorsque le contexte sera clair, nous utiliserons la notation Φ à la place de Φ_n. On équipe $K_{\mathbb{R}}^n$ du produit scalaire induit par celui de $K_{\mathbb{R}}$: pour tous $x, y \in K_{\mathbb{R}}^n$, on pose

$$T_2^n(x,y) := \sum_{i=1}^{n} T_2(x_i, y_i).$$

On procède de manière analogue sur $\mathbb{R}^{nr} \oplus \mathbb{C}^{ns}$ en définissant

$$\langle x \,|\, y\rangle := \sum_{i=1}^{n}\sum_{j=1}^{\delta} \varepsilon_j \Re(\overline{x_{j,i}} y_{j,i})$$

pour tous $x, y \in \mathbb{R}^{nr} \oplus \mathbb{C}^{ns}$, où $x = (x_1, \dots, x_\delta)$ et $x_i = (x_{i,1}, \dots, x_{i,n})$ pour tout $1 \leqslant i \leqslant \delta$ (et de même pour y). Ces définitions font de Φ_n une isométrie. Lorsque le contexte sera clair, nous utiliserons la notation usuelle $\langle \cdot \,|\, \cdot \rangle$ à la place de $T_2^n(\cdot,\cdot)$ et nous noterons $\|\cdot\|$ la norme associée à ce produit scalaire

L'isométrie Φ et l'isomorphisme entre $\mathbb{R}^2$ et $\mathbb{C}$ donné par le choix de la $\mathbb{R}$-base $(1, i)$ de $\mathbb{C}$ induisent une isométrie Ψ entre $K_{\mathbb{R}}^n$ muni de la norme T_2 et $\mathbb{R}^{nd}$ muni du produit scalaire défini pour tous $x = (x_1, \dots, x_d) \in (\mathbb{R}^n)^d$ et $y = (y_1, \dots, y_d) \in (\mathbb{R}^n)^d$ par

$$\langle x \,|\, y\rangle := \sum_{i=1}^{n}\sum_{j=1}^{d} \widetilde{\varepsilon}_j \Re(\overline{x_{j,i}} y_{j,i}),$$

2. C'est un abus de notation justifié par une identification évidente.

où $\widetilde{\varepsilon}_j = 1$ si $1 \leqslant j \leqslant r$ et $\widetilde{\varepsilon}_j = 2$ si $r+1 \leqslant j \leqslant d$. Dans la suite, il nous sera parfois pratique de considérer cette isométrie plutôt que Φ. Il est possible de tordre la norme T_2 sur $K_{\mathbb{R}}$ afin de faire de Ψ une isométrie entre $K_{\mathbb{R}}$ et $\mathbb{R}^d$ muni de sa structure euclidienne usuelle. Si cette approche a le mérite de rendre certains résultats plus explicites, elle complexifie aussi grandement les démonstrations de certaines propriétés. Nous renvoyons le lecteur vers [Neu13, §I.5, p.28–34] pour plus de détails sur ces choix.

Exemple II.2.1 Prenons $K = \mathbb{Q}$. Dans ce cas, il est bien connu (voir [Rot08, prop.2.58, p.81]) que le $\mathbb{R}$-espace vectoriel $\mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{R}$ est naturellement isomorphe à $\mathbb{R}$ (l'isomorphisme naturel en question est d'ailleurs l'application Φ_1). La structure de $\mathbb{Q}_{\mathbb{R}}$-module libre de rang n de $\mathbb{Q}_{\mathbb{R}}^n$ est donc de ce fait naturellement une structure de $\mathbb{R}$-espace vectoriel de dimension n (voir [Rot08, thm.2.65, p.86–87]). De plus, on peut vérifier que la norme T_2 sur $\mathbb{Q}_{\mathbb{R}}^n$ est exactement la norme euclidienne usuelle de $\mathbb{R}^n$. Le cadre d'étude algébrique présenté dans ce paragraphe englobe la théorie classique des réseaux euclidiens et des formes quadratiques telle qu'elle est par exemple détaillée dans [Mar03, §1, p.1–35]

Exemple II.2.2 Soit $D \in \mathbb{N}_{>0}$ sans facteurs carrés. L'anneau $\mathbb{Q}(i\sqrt{D}) \otimes_{\mathbb{Q}} \mathbb{R}$ étant isomorphe à $\mathbb{C}$, la structure de $\mathbb{Q}(i\sqrt{D})_{\mathbb{R}}$-module libre de rang n de $\mathbb{Q}(i\sqrt{D})_{\mathbb{R}}^n$ s'identifie à une structure $\mathbb{C}$-espace vectoriel de dimension n.

Remarquons que la norme induite sur $\mathbb{C}^n$ par la norme T_2 sur $\mathbb{Q}(i\sqrt{D})_{\mathbb{R}}^n$ n'est pas la norme hermitienne usuelle de $\mathbb{C}^n$: du point de vue purement géométrique, le cadre de travail que nous présentons dans ce chapitre est diffèrent de celui présenté dans le chapitre précédent. Néanmoins, les notions que nous allons introduire dans la suite de ce chapitre ne sont pas modifiées par ce changement de structure. Seule la notion de LLL-réduction présentée dans la Section I.3.2 est délicate à généraliser et utiliser pour la norme T_2 (nous renvoyons le lecteur vers [FS10] pour de plus amples informations sur ce vaste sujet).

Dans le reste de ce chapitre, afin d'alléger les notations, on fixe un entier $n \geqslant 1$ et on note $E := K_{\mathbb{R}}^n$.

II.2.2 Endomorphismes de $(K \otimes_{\mathbb{Q}} \mathbb{R})^n$

On note $\mathrm{End}_{K_{\mathbb{R}}}(E)$ la $\mathbb{R}$-algèbre des endomorphismes $K_{\mathbb{R}}$-linéaires (ou $K_{\mathbb{R}}$-endomorphismes) de E. Via le choix d'une $K_{\mathbb{R}}$-base de E, cette algèbre est identifiée à la $\mathbb{R}$-algèbre $\mathrm{M}_n(K_{\mathbb{R}})$ des matrices carrées de taille n à coefficients dans $K_{\mathbb{R}}$. Si $\sigma \in \Sigma_K$ et $A \in \mathrm{M}_n(K_{\mathbb{R}})$, on note $\sigma(A)$ la matrice obtenue en appliquant σ à chacun des coefficients de A. Puisque l'application Φ_1 définie dans le paragraphe précédent est un isomorphisme, l'identification fondamentale suivante résulte d'une vérification directe :

Proposition II.2.3 *L'application* [3]

$$\begin{array}{rccc} \Phi : & \mathrm{M}_n(K_{\mathbb{R}}) & \longrightarrow & \mathrm{M}_n(\mathbb{R})^r \oplus \mathrm{M}_n(\mathbb{C})^s := \left\{A \in \mathrm{M}_n(\mathbb{C})^\delta \ : \ A_1, \ldots, A_r \in \mathrm{M}_n(\mathbb{R})\right\} \\ & A & \longmapsto & (\sigma_1(A), \ldots, \sigma_\delta(A)) \end{array}$$

3. Encore appelée Φ afin d'alléger les notations.

est un isomorphisme de $\mathbb{R}$-algèbres. En particulier, $\mathrm{M}_n(K_\mathbb{R})$ est de dimension dn^2 sur $\mathbb{R}$.

Pour tous $A \in \mathrm{M}_n(\mathbb{R})^r \oplus \mathrm{M}_n(\mathbb{C})^s$ et $x \in \mathbb{R}^{nr} \oplus \mathbb{C}^{ns}$, on pose $Ax := (A_1x_1, \dots, A_\delta x_\delta)$. Cette action est compatible avec celle de $\mathrm{M}_n(K_\mathbb{R})$ sur E, dans le sens où $\Phi(Ax) = \Phi(A)\Phi(x)$. En particulier, on déduit de cette remarque l'isomorphisme de groupes suivant :

Proposition II.2.4 *La restriction de Φ à*

$$\mathrm{GL}_n(K_\mathbb{R}) := \{A \in \mathrm{M}_n(K_\mathbb{R}) \text{ inversible}\}$$

induit un isomorphisme de groupes

$$\Phi : \mathrm{GL}_n(K_\mathbb{R}) \longrightarrow \mathrm{GL}_n(\mathbb{R})^r \times \mathrm{GL}_n(\mathbb{C})^s := \left\{A \in \mathrm{GL}_n(\mathbb{C})^\delta \ : \ A_1, \dots, A_r \in \mathrm{GL}_n(\mathbb{R})\right\}.$$

Plusieurs travaux plus anciens (comme [FP96]) définissent un cadre d'étude limité à K^n, et non à $K_\mathbb{R}^n$. Afin de replacer ces résultats dans notre contexte, il est nécessaire de se restreindre à l'étude des $K_\mathbb{R}$-endomorphismes de E qui préservent l'image de K^n dans E par le plongement

$$\begin{array}{rccc} \iota : & K^n & \longrightarrow & E \\ & x & \longmapsto & (x_1 \otimes 1, \dots, x_n \otimes 1) \end{array}.$$

Il s'avère que cela revient effectivement à étudier les K-endomorphismes de K^n.

Proposition II.2.5 *Soit $u \in \mathrm{End}_{K_\mathbb{R}}(E)$. L'inclusion $u(K^n) \subset K^n$ est vérifiée si et seulement s'il existe $v \in \mathrm{End}_K(K^n)$ tel que le diagramme*

$$\begin{array}{ccc} K^n & \xrightarrow{\iota} & E \\ {\scriptstyle v}\downarrow & & \downarrow{\scriptstyle u} \\ K^n & \xrightarrow[\iota]{} & E \end{array}$$

soit commutatif. En particulier, les anneaux $\mathrm{End}_K(K^n)$ et $\mathrm{End}_{K_\mathbb{R}}(E)$ sont isomorphes.

Démonstration. Considérons le morphisme d'anneaux injectif $\chi : \mathrm{End}_K(K^n) \longrightarrow \mathrm{End}_{K_\mathbb{R}}(E)$ défini pour tout $u \in \mathrm{GL}_n(K)$ par

$$\begin{array}{rccc} \chi(u) : & E & \longrightarrow & E \\ & x \otimes y & \longmapsto & u(x) \otimes y \end{array}.$$

Nous utilisons tacitement l'isomorphisme de $K_\mathbb{R}$-modules naturel entre $K \otimes_\mathbb{Q} \mathbb{R}^n$ et $(K \otimes_\mathbb{Q} \mathbb{R})^n$, explicité dans [Rot08, thm.2.65, p.86–87]. Si $u \in \mathrm{End}_{K_\mathbb{R}}(E)$, pour tout $x \in K^n$, il existe un unique $y_x \in K^n$ tel que $u(\iota(x)) = \iota(y_x)$. Par $K_\mathbb{R}$-linéarité, on montre que $\chi(x \mapsto y_x) = u$, ce qui prouve que χ est surjectif. □

Ce résultat reste valable lorsqu'on ne considère que des applications inversibles.

Corollaire II.2.6 *Les groupes $\mathrm{GL}_K(K^n)$ et $\{u \in \mathrm{GL}_{K_\mathbb{R}}(E) \ : \ u(K^n) \subset K^n\}$ sont isomorphes.*

II.2.3 Automorphismes orthogonaux

Un automorphisme $u \in \mathrm{GL}_{K_\mathbb{R}}(E)$ est dit *orthogonal* s'il préserve la norme T_2 sur E, c'est-à-dire si

$$\langle u(x) \,|\, u(y)\rangle = \langle x \,|\, y\rangle \text{ pour tous } x, y \in E. \tag{II.1}$$

Les automorphismes orthogonaux sont donc les applications qui préservent la structure *algébrique* de E (comme éléments de $\mathrm{GL}_{K_\mathbb{R}}(E)$) et sa structure euclidienne : la condition (II.1) est exactement la condition vérifiée par un automorphisme orthogonal de E vu comme espace euclidien. Il est trivial de montrer que le sous-ensemble $\mathrm{O}_{K_\mathbb{R}}(E)$ des éléments orthogonaux de $\mathrm{GL}_{K_\mathbb{R}}(E)$ est un sous-groupe de $\mathrm{GL}_{K_\mathbb{R}}(E)$. Nous appellerons *base standard* de E la $K_\mathbb{R}$-base

$$\mathcal{E} := \left(\begin{pmatrix} 1\otimes 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \cdots, \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1\otimes 1 \end{pmatrix} \right).$$

Le choix de cette $K_\mathbb{R}$-base permet d'identifier $\mathrm{O}_{K_\mathbb{R}}(E)$ à

$$\mathrm{O}_n(K_\mathbb{R}) := \{A \in \mathrm{GL}_n(K_\mathbb{R}) \,:\, \langle Ax \,|\, Ay\rangle = \langle x \,|\, y\rangle \text{ pour tous } x, y \in E\}.$$

L'analogue de la Proposition II.2.4 pour les automorphismes orthogonaux est donné par l'identification suivante :

Proposition II.2.7 *La restriction de Φ à $\mathrm{O}_n(K_\mathbb{R})$ induit un isomorphisme de groupes*

$$\Phi : \mathrm{O}_n(K_\mathbb{R}) \longrightarrow \mathrm{O}_n(\mathbb{R})^r \oplus \mathrm{U}_n(\mathbb{C})^s := \left\{A \in \mathrm{U}_n(\mathbb{C})^\delta \,:\, A_1, \ldots, A_r \in \mathrm{O}_n(\mathbb{R})\right\}.$$

Démonstration. Rappelons que Ψ désigne l'isométrie entre E et $\mathbb{R}^{nd}$ équipé du produit scalaire

$$\langle x \,|\, y\rangle := \sum_{i=1}^{n}\sum_{j=1}^{d} \widetilde{\varepsilon}_j \mathfrak{R}(\overline{x_{j,i}} y_{j,i}),$$

induite par Φ et par le choix de la $\mathbb{R}$-base $(1, i)$ de $\mathbb{C}$. On note aussi Ψ le morphisme de $\mathbb{R}$-algèbres induit :

$$\begin{array}{rccc} \Psi : & \mathrm{M}_n(K_\mathbb{R}) & \longrightarrow & \mathrm{M}_{nd}(\mathbb{R}) \\ & A & \longmapsto & \mathrm{Diag}\left(\sigma_1(A), \ldots, \sigma_r(A), \rho\sigma_{r+1}(A), \ldots, \rho\sigma_\delta(A)\right) \end{array},$$

où ρ est le morphisme de $\mathbb{R}$-algèbres :

$$\begin{array}{rccc} \rho : & \mathrm{M}_n(\mathbb{C}) & \longrightarrow & \mathrm{M}_{2n}(\mathbb{R}) \\ & A & \longmapsto & \begin{pmatrix} \mathfrak{R}(A) & -\mathfrak{I}(A) \\ \mathfrak{I}(A) & \mathfrak{R}(A) \end{pmatrix} \end{array}.$$

Pour tous $x \in \mathbb{R}^{nr} \oplus \mathbb{C}^{ns}$ et $A \in \mathrm{M}_n(\mathbb{R})^r \oplus \mathrm{M}_n(\mathbb{C})^s$, on a $\Psi(Ax) = \Psi(A)\Psi(x)$. En particulier, l'égalité

$$\langle \Psi(A)x \,|\, \Psi(A)y \rangle = \langle x \,|\, y \rangle$$

est vérifiée pour tout $A \in \mathrm{O}_n(K_{\mathbb{R}})$ et tous $x, y \in \mathbb{R}^{nd}$. Cette relation montre que $\Psi(A)$ est la matrice dans la base standard[4] de $\mathbb{R}^{nd}$ d'un endomorphisme orthogonal f de $\mathbb{R}^{nd}$. Soit $P \in \mathrm{GL}_{nd}(\mathbb{R})$ la matrice diagonale telle que :

- les nr premiers coefficients diagonaux de P sont égaux à 1.
- les $2ns$ coefficients diagonaux de P restants sont égaux à $1/\sqrt{2}$.

Par construction, on a $P^{-1}\Psi(A)P = \Psi(A)$. D'autre part, les colonnes de cette matrice P forment une base orthonormée de $\mathbb{R}^{nd}$. Ainsi, la matrice $P^{-1}\Psi(A)P$ de f dans cette base est une matrice orthogonale. Nous avons donc montré que $\Psi(A)$ est une matrice orthogonale, ce qui revient à dire que les matrices $\sigma_1(A), \ldots, \sigma_r(A)$ et $\rho\sigma_{r+1}(A), \ldots, \rho\sigma_\delta(A)$ le sont aussi. Or pour tout $r < i \leqslant \delta$, l'orthogonalité de $\rho\sigma_i(A)$ équivaut au fait que $\sigma_i(A)$ soit hermitienne. D'où l'identification annoncée. □

L'isomorphisme Φ_1 permet de définir une involution $\mathbb{R}$-linéaire sur $K_{\mathbb{R}}$, donnée pour tout $z \in K_{\mathbb{R}}$ par $\overline{z} := \Phi_1^{-1}(\overline{\Phi_1(z)})$. Si $A \in \mathrm{M}_n(K_{\mathbb{R}})$, on note $A^* := \overline{A}^{\mathsf{T}}$ la matrice adjointe de A pour cette involution. L'introduction de cette involution permet de retrouver un critère d'orthogonalité usuel.

Corollaire II.2.8 *Une matrice $A \in \mathrm{M}_n(K_{\mathbb{R}})$ est orthogonale si et seulement si $A^*A = AA^* = \mathrm{I}_n$.*

Démonstration. Nous avons montré que $A \in \mathrm{M}_n(K_{\mathbb{R}})$ est orthogonale si et seulement si $\Psi(A) \in \mathrm{O}_{nd}(\mathbb{R})$. Pour tout plongement $\sigma \in \Sigma_K$, on a $\sigma(A^*) = \sigma(A)^*$, où $\sigma(A)^*$ désigne la matrice adjointe (transposée si σ est un plongement réel) de $\sigma(A)$ pour la conjugaison complexe. Ainsi, $\Psi(A^*) = \Psi(A)^{\mathsf{T}}$. Puisque Ψ est un morphisme de groupes, le résultat est démontré. □

En particulier, on déduit de la relation $\Psi(A^*) = \Psi(A)^{\mathsf{T}}$ que A^* est la matrice adjointe (au sens euclidien) de A pour la forme T_2 :

Corollaire II.2.9 *Soit $A \in \mathrm{M}_n(K_{\mathbb{R}})$. Pour tous $x, y \in E$, on a $\langle Ax \,|\, y \rangle = \langle x \,|\, A^*y \rangle$.*

Dans la continuité de la Proposition II.2.5, on montre ensuite que :

Corollaire II.2.10 *Le sous-groupe*

$$\{u \in \mathrm{O}_{K_{\mathbb{R}}}(E) \,:\, u(x) \in K^n \text{ pour tout } x \in K^n\}$$

des $K_{\mathbb{R}}$-automorphismes orthogonaux préservant K^n est isomorphe au groupe

$$\mathrm{O}_K(K^n) := \{u \in \mathrm{GL}_K(K^n) \,:\, \langle u(x) \,|\, u(y) \rangle = \langle x \,|\, y \rangle \text{ pour tous } x, y \in K^n\}$$

des K-automorphismes orthogonaux de K^n.

4. qui n'est pas une base orthonormée de $\mathbb{R}^{nd}$, mais seulement orthogonale ! En effet, nous avons fait le choix de ne pas tordre la norme T_2 sur $K_{\mathbb{R}}$, ce qui nous force à considérer une version tordue du produit scalaire classique de $\mathbb{R}^{nd}$.

II.2.4 Endomorphismes symétriques

Un $K_{\mathbb{R}}$-endomorphisme $u \in \mathrm{End}_{K_{\mathbb{R}}}(E)$ est dit *symétrique* si

$$\langle u(x) \,|\, y\rangle = \langle x \,|\, u(y)\rangle \text{ pour tous } x, y \in E.$$

En particulier, un $K_{\mathbb{R}}$-endomorphisme de E est symétrique s'il l'est en tant qu'endomorphisme de l'espace euclidien E. L'ensemble $\mathrm{H}_{K_{\mathbb{R}}}(E)$ de ces endomorphismes est une sous-$\mathbb{R}$-algèbre de $\mathrm{End}_{K_{\mathbb{R}}}(E)$. Le choix de la base standard de E permet d'identifier $\mathrm{H}_{K_{\mathbb{R}}}(E)$ à

$$\mathrm{H}_n(K_{\mathbb{R}}) := \{A \in \mathrm{M}_n(K_{\mathbb{R}}) \,:\, \langle Ax \,|\, y\rangle = \langle x \,|\, Ay\rangle \text{ pour tous } x, y \in E\}.$$

En employant la même stratégie que pour la Proposition II.2.7 on montre l'identification suivante :

Proposition II.2.11 *La restriction de Φ à $\mathrm{H}_n(K_{\mathbb{R}})$ induit un isomorphisme de $\mathbb{R}$-algèbres*

$$\Phi : \mathrm{H}_n(K_{\mathbb{R}}) \longrightarrow \mathrm{S}_n(\mathbb{R})^r \oplus \mathrm{H}_n(\mathbb{C})^s := \left\{A \in \mathrm{H}_n(\mathbb{C})^\delta \,:\, A_1, \ldots, A_r \in \mathrm{S}_n(\mathbb{R})\right\}.$$

En particulier, $\mathrm{H}_n(K_{\mathbb{R}})$ est de dimension $\frac{dn(n+1)}{2}$ sur $\mathbb{R}$.

Comme dans le paragraphe précédent, on déduit un critère classique basé sur l'involution précédemment introduite.

Corollaire II.2.12 *Un élément $A \in \mathrm{M}_n(K_{\mathbb{R}})$ est symétrique si et seulement si $A^* = A$.*

Exemple II.2.13 Dans la situation $K = \mathbb{Q}$ et $E = \mathbb{R}^n$ de l'exemple Exemple II.2.1, on remarque que les notions de $K_{\mathbb{R}}$-automorphisme orthogonal et de $K_{\mathbb{R}}$-endomorphisme symétrique sont exactement celles d'automorphisme orthogonal et d'endomorphisme symétrique d'un espace euclidien. L'involution $\mathbb{R}$-linéaire sur E définie plus haut se réduit à l'opérateur de transposition, et les Corollaire II.2.10 et Corollaire II.2.12 établissent le lien classique entre transposition de matrices et adjonction d'applications linéaires entre espaces euclidiens.

Exemple II.2.14 De manière similaire, lorsque $K = \mathbb{Q}(i\sqrt{D})$ (situation de l'Exemple II.2.2), le groupe $\mathrm{O}_n(K_{\mathbb{R}})$ est isomorphe au groupe $\mathrm{U}_n(\mathbb{C})$ des matrices unitaires complexes. Or il est bien connu que ces matrices représentent exactement les $\mathbb{C}$-endomorphismes unitaires de $\mathbb{C}^n$. Ainsi, les notions de $K_{\mathbb{R}}$-endomorphisme orthogonal et de $\mathbb{C}$-endomorphisme unitaire sont confondues. La même remarque est valable pour les $K_{\mathbb{R}}$-endomorphismes symétriques et les $\mathbb{C}$-endomorphismes hermitiens.

II.3 Réseaux algébriques

II.3.1 Premières définitions et résultats de structure

Nous introduisons dans ce paragraphe les premières définitions et propriétés concernant les réseaux algébriques. Nous en profitons pour rappeler des résultats analogues sur les réseaux euclidiens.

Définition II.3.1 *Un sous-groupe Λ de E est appelé un réseau algébrique*[5] *de rang n sur K si :*

- *Λ est un $\mathbb{Z}$-réseau de E, c'est-à-dire un sous-groupe discret de E de rang nd.*
- *Λ est un sous-$\mathcal{O}_K$-module de E.*

Nous nous plaçons dans le cadre de travail de [FS10 ; OY10 ; WYH13]. Certains travaux plus anciens ne considèrent que des familles restreintes de réseaux algébriques :

- Comme de nombreux autres auteurs, Fieker et Pohst se limitent dans [FP96] au cas des réseaux algébriques inclus dans K^n.
- Comme nous l'avons fait dans le chapitre précédent, Braun et Coulangeon [BC15] et Napias [Nap96] se restreignent en plus au cas où K est un corps de nombres quadratique imaginaire et euclidien. En particulier, les réseaux algébriques de rang n sur de tels corps sont toujours des sous-$\mathcal{O}_K$-modules libres de rang n de $\mathbb{C}^n$.

Néanmoins, comme nous le verrons plus loin, l'exemple des réseaux algébriques de K^n reste fondamental pour plusieurs raisons.

Exemple II.3.2 Reprenons l'exemple $K = \mathbb{Q}$. Puisque $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$ et $K_{\mathbb{Q}}^n = \mathbb{R}^n$, les réseaux euclidiens de $\mathbb{R}^n$ (c'est-à-dire les sous-groupes discrets de rang n) sont exactement les réseaux algébriques de rang n sur $\mathbb{Q}$. Les réseaux euclidiens sont donc des réseaux algébriques. Remarquons que réciproquement, les réseaux algébriques sont des réseaux euclidiens dotés d'une structure (algébrique) supplémentaire.

Il faut noter que nous ne considérons dans la définition précédente que les réseaux algébriques *de rang maximal* de E. Sauf mention du contraire, par *réseau algébrique*, nous désignerons toujours les *réseaux algébriques de rang maximal*, au sens de cette définition. Nous reviendrons plus loin sur les réseaux algébriques qui ne sont pas de rang maximal, appelés *réseaux algébriques relatifs*.

Commençons par rappeler une conséquence du théorème de structure des modules de type fini sur un anneau de Dedekind (voir par exemple [Coh00, §1.2.1, p.6–13]), qui généralise le théorème de structure des $\mathbb{Z}$-modules de type fini (voir [Coh93, thm.2.4.1, p.66]).

Proposition II.3.3 *Soit Λ un réseau algébrique de K^n. Il existe des idéaux fractionnaires $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ de K et $(b_1, \dots, b_n)$ une K-base de K^n tels que*

$$\Lambda = \mathfrak{a}_1 b_1 \oplus \cdots \oplus \mathfrak{a}_n b_n.$$

Il s'avère que les réseaux algébriques de E ont une structure similaire à ceux de K^n. Avant de démontrer ce fait, on introduit la notion d'isomorphisme entre réseaux algébriques.

Définition II.3.4 *Deux réseaux algébriques Λ et Λ' de E sont dits isomorphes s'il existe un $K_{\mathbb{R}}$-automorphisme $u \in \mathrm{GL}_{K_{\mathbb{R}}}(E)$ tel que $u(\Lambda) = \Lambda'$. Dans ce cas, on note $\Lambda \cong \Lambda'$.*

5. La terminologie $\mathcal{O}_K$-réseau est parfois employée. On trouvera aussi dans la littérature la terminologie *réseau sur un corps de nombres*, notamment dans [FP96].

Notons que, comme dans le cas euclidien, la notion d'isomorphisme préserve seulement la structure algébrique, mais pas nécessairement la structure euclidienne. Nous reviendrons dans le paragraphe suivant sur cette notion, en montrant notamment que la situation est nettement plus riche que dans le cas euclidien.

Théorème II.3.5 *Soit Λ un réseau algébrique de E. Il existe Λ_0 un réseau algébrique de K^n tel que $\Lambda \cong \Lambda_0$. En particulier, il existe des idéaux fractionnaires $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ de K et $(b_1, \dots, b_n)$ une $K_{\mathbb{R}}$-base de E tels que*

$$\Lambda = \mathfrak{a}_1 b_1 \oplus \cdots \oplus \mathfrak{a}_n b_n. \tag{II.2}$$

Démonstration. L'existence du réseau algébrique Λ_0 est démontrée dans [OY10, §2], à l'aide de [LLN09, lem.3.2]. D'autre part, si $(b_1, \dots, b_n)$ est une K-base de K^n, alors $(\iota(b_1), \dots, \iota(b_n))$ est une $K_{\mathbb{R}}$-base de E. Utilisé conjointement avec la Proposition II.3.3, ce fait montre l'existence d'une relation de la forme (II.2) pour les réseaux algébriques de E. □

Définition II.3.6 *Soit Λ un réseau algébrique de E. Une famille $(\mathfrak{a}_i, b_i)_{1 \leqslant i \leqslant n}$ où $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ sont des idéaux fractionnaires de K et $(b_1, \dots, b_n)$ une $K_{\mathbb{R}}$-base de E et telle que*

$$\Lambda = \mathfrak{a}_1 b_1 \oplus \cdots \oplus \mathfrak{a}_n b_n \tag{II.3}$$

est appelée une pseudo-base de Λ. Par abus de langage, une $K_{\mathbb{R}}$-base $(b_1, \dots, b_n)$ de E est appelée une base de Λ s'il existe $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ des idéaux fractionnaires de K tels que $(\mathfrak{a}_i, b_i)_{1 \leqslant i \leqslant n}$ soit une pseudo-base de Λ.

Bien évidemment, lorsque l'anneau $\mathcal{O}_K$ est principal, tous les réseaux algébriques sont des $\mathcal{O}_K$-modules *libres*. Il est donc possible de remplacer les idéaux $\mathfrak{a}_i$ par $\mathcal{O}_K$ dans la relation (II.3). Dans cette situation, on parle simplement de *base* d'un réseau algébrique. C'est notamment le cas des réseaux euclidiens qui sont des $\mathbb{Z}$-modules libres particuliers : un sous-ensemble $\Lambda \subset \mathbb{R}^n$ est un réseau euclidien si et seulement s'il existe $(b_1, \dots, b_n)$ une $\mathbb{R}$-base de $\mathbb{R}^n$ telle que

$$\Lambda = \mathbb{Z} b_1 \oplus \cdots \oplus \mathbb{Z} b_n.$$

Exemple II.3.7 Dans le chapitre précédent, nous avons défini un réseau algébrique sur $\mathbb{Q}(i\sqrt{D})$ comme un objet vérifiant une relation de la forme (II.3) avec $\mathfrak{a}_i = \mathcal{O}_K$ pour tout $1 \leqslant i \leqslant n$. En particulier, nous nous sommes restreints aux réseaux algébriques *libres*. Puisque nous avons rapidement supposé que $\mathcal{O}_K$ est un anneau euclidien (donc en particulier principal), il était naturel d'imposer cette restriction dans l'objectif d'une généralisation naïve de la notion de réseau.

La manipulation algorithmique des réseaux algébriques est grandement facilitée par l'existence des pseudo-bases. Le prérequis à une étude algorithmique plus poussée est d'être en mesure de calculer et manipuler de telles familles. Fort heureusement, plusieurs algorithmes élémentaires sur les réseaux euclidiens ont été étendus au cas des pseudo-bases de réseaux algébriques. Le lecteur intéressé par un panorama sur le sujet pourra consulter [BP91] et [Coh00, p.25–47]. Retenons notamment :

- Le calcul de la forme normale de Hermite sur un anneau de Dedekind, présenté dans [Coh96, §2-3, p.1686–1696] et récemment amélioré dans [BFH17], qui permet d'obtenir une pseudo-base essentiellement unique d'un réseau algébrique à partir d'une famille génératrice (chose très utile lors de la détermination d'une pseudo-base de la somme de deux réseaux algébriques, où la famille génératrice en question est obtenue par concaténation d'une pseudo-base de chaque réseau algébrique considéré). Plusieurs opérations sur les réseaux algébriques sont rendues très aisées par l'existence de la forme normale de Hermite : les tests d'égalité et d'inclusion, certains calculs de noyaux et d'images, la détermination de la somme, du produit, de l'intersection...
- La détermination de la forme normale de Smith (voir [Coh96, §4, p.1696–1699]), propice à l'étude de la structure des quotients de réseaux algébriques.

Notons que les systèmes de calcul [PARI/gp] et [MAGMA] offrent une implantation (partiellement optimisée) de l'algorithme permettant d'obtenir la forme normale de Hermite sur un anneau de Dedekind. S'il n'est pas trivial d'obtenir une pseudo-base d'un réseau algébrique à partir d'une $\mathbb{Z}$-base, l'opération inverse est au contraire très aisée :

Proposition II.3.8 *Soient Λ un réseau algébrique de E et $(\mathfrak{a}_i, b_i)_{1\leqslant i\leqslant n}$ une pseudo-base de Λ. Si pour tout $1 \leqslant i \leqslant n$, $(\omega_1^{(i)}, \dots, \omega_d^{(i)})$ est une $\mathbb{Z}$-base de $\mathfrak{a}_i$, la famille $(\omega_j^{(i)} b_i)_{1\leqslant j\leqslant d}^{1\leqslant i\leqslant m}$ est une base de Λ vu comme réseau euclidien.*

Démonstration. Par définition, on a

$$\begin{cases} \Lambda = \mathfrak{a}_1 b_1 \oplus \cdots \oplus \mathfrak{a}_n b_n \\ \mathfrak{a}_i = \mathbb{Z}\omega_1^{(i)} \oplus \cdots \oplus \mathbb{Z}\omega_d^{(i)} \text{ pour tout } 1 \leqslant i \leqslant n. \end{cases}$$

On déduit que

$$\Lambda = \left(\bigoplus_{j=1}^{d} \mathbb{Z}\omega_j^{(1)}\right) b_1 \oplus \cdots \oplus \left(\bigoplus_{j=1}^{d} \mathbb{Z}\omega_j^{(n)}\right) b_n = \bigoplus_{\substack{1\leqslant i\leqslant n \\ 1\leqslant j\leqslant d}} \mathbb{Z}\omega_j^{(i)} b_i.$$

Ainsi, la famille $(\omega_j^{(i)} b_i)_{1\leqslant j\leqslant d}^{1\leqslant i\leqslant m}$ est bien une $\mathbb{Z}$-base de Λ, qui est aussi une $\mathbb{R}$-base de E. C'est donc bien une base de Λ vu comme réseau euclidien. □

Nous avons déjà utilisé cette propriété dans le chapitre précédent, en remarquant qu'un réseau algébrique de rang n sur $\mathbb{Q}(i\sqrt{D})$ est un réseau euclidien de rang $2n$.

II.3.2 Classes d'isomorphie de réseaux algébriques

Dans le cas des réseaux euclidiens, la notion d'isomorphisme est peu intéressante : deux réseaux euclidiens (de même rang) sont nécessairement isomorphes. La situation est plus riche pour les réseaux algébriques. Commençons par rappeler une formule de changement de pseudo-bases, que nous prenons ici le soin de redémontrer.

Proposition II.3.9 *Soit $\Lambda = \mathfrak{a}_1 b_1 \oplus \cdots \oplus \mathfrak{a}_n b_n$ un réseau algébrique de E. Soient $(\mathfrak{b}_1, \ldots, b_n)$ une famille d'idéaux fractionnaires de K et $(c_1, \ldots, c_n)$ une $K_{\mathbb{R}}$-base de E. Soient $P \in \mathrm{GL}_n(K_{\mathbb{R}})$ telle que $b_j = \sum_{i=1}^n P_{i,j} c_i$ pour tout $1 \leqslant j \leqslant n$ et Q son inverse. Les propositions suivantes sont équivalentes :*

(i) La famille $(\mathfrak{b}_i, c_i)_{1 \leqslant i \leqslant n}$ est une pseudo-base de Λ.

(ii) $P_{i,j} \in \mathfrak{b}_i \mathfrak{a}_j^{-1}$ et $Q_{i,j} \in \mathfrak{a}_i \mathfrak{b}_j^{-1}$ pour tous $1 \leqslant i, j \leqslant n$.

(iii) $P_{i,j} \in \mathfrak{b}_i \mathfrak{a}_j^{-1}$ pour tous $1 \leqslant i, j \leqslant n$ et $\det(P)(\mathfrak{a}_1 \cdots \mathfrak{a}_n) = (\mathfrak{b}_1 \cdots \mathfrak{b}_n)$.

Démonstration. Commençons par montrer l'équivalence entre les deux premiers points. Par définition, la famille $(\mathfrak{b}_i, c_i)_{1 \leqslant i \leqslant n}$ est une pseudo-base de Λ si et seulement si $\Lambda = \mathfrak{b}_1 c_1 \oplus \cdots \oplus \mathfrak{b}_n c_n$. L'inclusion $\Lambda \subset \oplus_{i=1}^n \mathfrak{b}_i c_i$ est vérifiée si et seulement si

$$\mathfrak{a}_j b_j = \sum_{i=1}^n \mathfrak{a}_j P_{i,j} c_i \subset \bigoplus_{i=1}^n \mathfrak{b}_i c_i$$

pour tout $1 \leqslant j \leqslant n$, ce qui revient à exiger que $P_{i,j} \in \mathfrak{b}_i \mathfrak{a}_j^{-1}$ pour tous $1 \leqslant i, j \leqslant n$. En raisonnant de même avec l'autre inclusion, on montre ainsi l'équivalence entre les deux premiers points.

Supposons maintenant que $P_{i,j} \in \mathfrak{b}_i \mathfrak{a}_j^{-1}$ et $Q_{i,j} \in \mathfrak{a}_i \mathfrak{b}_j^{-1}$ pour tous $1 \leqslant i, j \leqslant n$. On a

$$\det(P) = \sum_{\tau \in \mathfrak{S}_n} \varepsilon(\tau) \prod_{i=1}^n P_{i,\tau(i)} \in \sum_{\tau \in \mathfrak{S}_n} \prod_{i=1}^n \mathfrak{b}_i \mathfrak{a}_{\tau(i)}^{-1} = (\mathfrak{b}_1 \cdots \mathfrak{b}_n)(\mathfrak{a}_1 \cdots \mathfrak{a}_n)^{-1},$$

d'où

$$\det(P)(\mathfrak{a}_1 \cdots \mathfrak{a}_n) \subset (\mathfrak{b}_1 \cdots \mathfrak{b}_n).$$

De même, on montre que

$$\det(Q)(\mathfrak{b}_1 \cdots \mathfrak{b}_n) \subset (\mathfrak{a}_1 \cdots \mathfrak{a}_n),$$

ce qui entraîne finalement l'égalité

$$\det(P)(\mathfrak{a}_1 \cdots \mathfrak{a}_n) = (\mathfrak{b}_1 \cdots \mathfrak{b}_n). \tag{II.4}$$

Enfin, on déduit de la formule classique

$$Q = \det(P)^{-1} \operatorname{Comat}(P)^{\intercal}$$

l'implication entre les points (iii) et (ii). □

Notons en particulier que les changements de pseudo-bases se font par des matrices à coefficients dans K, et non à coefficients dans $K_{\mathbb{R}}$. Dans la suite, on note $\mathrm{Cl}(K)$ le groupe des classes d'idéaux de K.

Définition II.3.10 *Soit $\Lambda = \mathfrak{a}_1 b_1 \oplus \cdots \oplus \mathfrak{a}_n b_n$. On appelle classe de Steinitz de Λ la classe de l'idéal produit $(\mathfrak{a}_1 \cdots \mathfrak{a}_n)$ dans $\mathrm{Cl}(K)$.*

D'après l'égalité (II.4) de la proposition précédente, la classe de Steinitz d'un réseau est bien définie : elle ne dépend pas de la pseudo-base utilisée pour la calculer. Il s'avère même qu'elle est invariante par $K_{\mathbb{R}}$-isomorphisme. Commençons par rappeler un résultat de structure classique, démontré par exemple dans [Coh00, thm.1.2.19, p.9].

Proposition II.3.11 *Soit Λ un réseau algébrique de E. Il existe $(b_1, \dots, b_n)$ une $K_{\mathbb{R}}$-base de E et $\mathfrak{a}$ un idéal fractionnaire de K tels que*

$$\Lambda = \mathfrak{a}b_1 \oplus \mathcal{O}_k b_2 \oplus \cdots \oplus \mathcal{O}_K b_n. \tag{II.5}$$

Comme remarquée dans [FP96, §2], cette représentation est agréable du point vue théorique mais rarement avantageuse du point de vue algorithmique. Notons que, par unicité de la classe de Steinitz dans $\mathrm{Cl}(K)$, l'idéal fractionnaire $\mathfrak{a}$ apparaissant dans la relation (II.5) est unique à multiplication par un élément de $K^\times$ près. On déduit notamment de ce résultat le théorème de Steinitz.

Théorème II.3.12 (Théorème de Steinitz) *La classe de Steinitz d'un réseau algébrique de E le caractérise complètement modulo $\mathrm{GL}_{K_{\mathbb{R}}}(E)$.*

Démonstration. Soient Λ et Λ' deux réseaux algébriques de E. Supposons dans un premier temps que Λ et Λ' sont $K_{\mathbb{R}}$-isomorphes. Il existe $u \in \mathrm{GL}_{K_{\mathbb{R}}}(E)$ tel que $u(\Lambda) = \Lambda'$. Soient $(\mathfrak{a}_i, b_i)_{1\leqslant i\leqslant n}$ et $(\mathfrak{a}'_i, b'_i)_{1\leqslant i\leqslant n}$ des pseudo-bases de Λ et Λ' respectivement. On a

$$u(\Lambda) = \mathfrak{a}_1 u(b_1) \oplus \cdots \oplus \mathfrak{a}_n u(b_n) = \Lambda',$$

ce qui signifie que la famille $(\mathfrak{a}_i, u(b_i))_{1\leqslant i\leqslant n}$ est une pseudo-base de Λ'. Si P désigne la matrice de u dans les bases $(b_1, \dots, b_n)$ et $(b'_1, \dots, b'_n)$, ceci entraîne d'après la Proposition II.3.9 que

$$\det(P)(\mathfrak{a}_1 \cdots \mathfrak{a}_n) = (\mathfrak{a}'_1 \cdots \mathfrak{a}'_n).$$

Ainsi, Λ et Λ' ont bien la même classe de Steinitz.

Réciproquement, montrons que si Λ et Λ' ont la même classe de Steinitz que, alors $\Lambda \cong \Lambda'$. Considérons des pseudo-bases de Λ et Λ' de la forme (II.5) :

$$\Lambda = \mathfrak{a}b_1 \oplus \mathcal{O}_K b_2 \oplus \cdots \oplus \mathcal{O}_K b_n$$

et

$$\Lambda' = \mathfrak{a}'b'_1 \oplus \mathcal{O}_K b'_2 \oplus \cdots \oplus \mathcal{O}_K b'_n,$$

où $(b_1, \dots, b_n)$ et $(b'_1, \dots, b'_n)$ sont des $K_{\mathbb{R}}$-bases de E et $\mathfrak{a}$ et $\mathfrak{a}'$ sont des idéaux fractionnaires de K. Puisque Λ et Λ' ont la même classe de Steinitz, $\mathfrak{a}$ et $\mathfrak{a}'$ sont égaux dans $\mathrm{Cl}(K)$: il existe $\zeta \in K^\times$ tel que $\zeta\mathfrak{a} = \mathfrak{a}'$. On peut alors démontrer que $u \in \mathrm{GL}_{K_{\mathbb{R}}}(E)$ défini par

$$u(b_i) = \begin{cases} \zeta b'_1 & \text{si } i = 1, \\ b'_i & \text{sinon.} \end{cases}$$

est un isomorphisme entre Λ et Λ'. □

Remarque II.3.13 Nous avons notamment montré que si u est un $K_{\mathbb{R}}$-isomorphisme entre deux réseaux algébriques Λ et Λ' de E, la matrice de u relativement à une base de Λ et une base de Λ' est un élément de $\mathrm{GL}_n(K)$.

On déduit de la Proposition II.3.9 et de l'argument utilisé dans la première partie de la preuve du Théorème II.3.12 une caractérisation des éléments de $\mathrm{GL}_{K_{\mathbb{R}}}(E)$ qui préservent un réseau algébrique donné :

Corollaire II.3.14 *Soient $\Lambda = \mathfrak{a}_1 b_1 \oplus \cdots \oplus \mathfrak{a}_n b_n$ un réseau algébrique de E et $u \in \mathrm{GL}_{K_{\mathbb{R}}}(E)$. Notons P et Q les matrices de u et u^{-1} dans la base $(b_1, \dots, b_n)$. Les propositions suivantes sont équivalentes :*

(i) $u(\Lambda) = \Lambda$.

(ii) $P_{i,j} \in$ *et* $Q_{i,j}$ *sont des éléments de* $\mathfrak{a}_i \mathfrak{a}_j^{-1}$ *pour tous* $1 \leqslant i, j \leqslant n$.

(iii) $P_{i,j} \in \mathfrak{a}_i \mathfrak{a}_j^{-1}$ *pour tous* $1 \leqslant i, j \leqslant n$ *et* $\det(P) \in \mathcal{O}_K^\times$.

En particulier, cette caractérisation permet de décrire explicitement le stabilisateur d'un réseau algébrique dans $\mathrm{GL}_n(K_{\mathbb{R}})$.

Définition II.3.15 *Soit $\mathfrak{A} := (\mathfrak{a}_1, \dots, \mathfrak{a}_n)$ une famille d'idéaux fractionnaires de K. On note $\mathrm{GL}_n(\mathfrak{A})$ le sous-groupe des éléments $P \in \mathrm{GL}_n(K_{\mathbb{R}})$ tels que $\det(P) \in \mathcal{O}_K^\times$ et $P_{i,j} \in \mathfrak{a}_i \mathfrak{a}_j^{-1}$ pour tous $1 \leqslant i, j \leqslant n$.*

En vertu de la proposition précédente, le stabilisateur de $\Lambda = \mathfrak{a}_i b_i \oplus \cdots \oplus \mathfrak{a}_n b_n$ dans $\mathrm{GL}_{K_{\mathbb{R}}}(E)$ s'identifie à $\mathrm{GL}((\mathfrak{a}_1, \dots, \mathfrak{a}_n))$ via le choix de la $K_{\mathbb{R}}$-base $(b_1, \dots, b_n)$. Choisissons $\mathfrak{a}_1, \dots, \mathfrak{a}_{h_K}$ un système de représentants des classes d'idéaux de K et $(b_1, \dots, b_n)$ une $K_{\mathbb{R}}$-base de E. Pour tout $1 \leqslant k \leqslant h_K$, considérons le réseau algébrique Λ_k de E défini par :

$$\Lambda_k = \mathfrak{a}_k b_1 \oplus \mathcal{O}_K b_2 \oplus \cdots \oplus \mathcal{O}_K b_n.$$

Le choix de la $K_{\mathbb{R}}$-base $(b_1, \dots, b_n)$ permet d'identifier le stabilisateur de Λ_k dans $\mathrm{GL}_{K_{\mathbb{R}}}(E)$ au groupe $\mathrm{GL}_n((\mathfrak{a}_k, \mathcal{O}_K, \dots, \mathcal{O}_K))$, que nous noterons dans la suite $\mathrm{GL}_n(\mathfrak{a}_k)$. D'après la Proposition II.3.9, un élément $P \in \mathrm{GL}_n(K_{\mathbb{R}})$ appartient à $\mathrm{GL}_n(\mathfrak{a}_k)$ si et seulement si $\det(P) \in \mathcal{O}_K^\times$ et, pour tous $1 \leqslant i, j \leqslant n$, on a

$$P_{i,j} \in \begin{cases} \mathfrak{a}_k & \text{si } i = 1 \text{ et } j \geqslant 2, \\ \mathfrak{a}_k^{-1} & \text{si } j = 1 \text{ et } i \geqslant 2, \\ \mathcal{O}_K & \text{sinon.} \end{cases}$$

Remarquons que pour $\mathfrak{a}_k = \mathcal{O}_K$, cette définition est la définition usuelle de $\mathrm{GL}_n(\mathcal{O}_K)$; on retrouve d'ailleurs la formule de changements de bases utilisée dans la Proposition I.2.9 du chapitre précédent. On obtient une description explicite de l'ensemble $\mathscr{L}_n(K_{\mathbb{R}})$ des réseaux algébriques de rang n sur K :

$$\mathscr{L}_n(K_{\mathbb{R}}) = \bigsqcup_{k=1}^{h} \mathrm{GL}_{K_{\mathbb{R}}}(E) \cdot \Lambda_k \cong \bigsqcup_{k=1}^{h} \mathrm{GL}_n(K_{\mathbb{R}}) / \mathrm{GL}_n(\mathfrak{a}_k). \tag{II.6}$$

Notons que si $\mathcal{O}_K$ est un anneau principal, c'est une identification similaire à celle du cas euclidien :

$$\mathscr{L}_n(K_{\mathbb{R}}) \cong \mathrm{GL}_n(K_{\mathbb{R}})/\mathrm{GL}_n(\mathcal{O}_K).$$

En particulier, dans cette situation, le stabilisateur d'un réseau algébrique est toujours isomorphe à $\mathrm{GL}_n(\mathcal{O}_K)$. Si $\mathcal{O}_K$ n'est pas principal, le stabilisateur d'un réseau ne caractérise en général pas sa classe d'isomorphie : par exemple, $\mathrm{GL}_n(\mathcal{O}_K)$ et $\mathrm{GL}((\mathfrak{a},\dots,\mathfrak{a}))$ sont égaux pour tout idéal $\mathfrak{a}$ de K, mais si $\mathfrak{a}^n$ n'est pas principal, les réseaux $\mathfrak{a}b_1 \oplus \cdots \oplus \mathfrak{a}b_n$ et $\mathcal{O}_K b_1 \oplus \cdots \mathcal{O}_K b_n$ ne peuvent pas être $K_{\mathbb{R}}$-isomorphes en vertu du Théorème II.3.12.

Enfin, il faut souligner que l'identification (II.6) ne dépend qu'à un isomorphisme (non canonique) près du choix du système de représentants de $\mathrm{Cl}(K)$:

Proposition II.3.16 *Soient $\mathfrak{a},\mathfrak{b}$ des idéaux fractionnaires de K. Si $\mathfrak{a}$ et $\mathfrak{b}$ sont égaux dans $\mathrm{Cl}(K)$, les groupes $\mathrm{GL}_n(\mathfrak{a})$ et $\mathrm{GL}_n(\mathfrak{b})$ sont isomorphes.*

Démonstration. Si $\mathfrak{a}$ et $\mathfrak{b}$ sont égaux dans $\mathrm{Cl}(K)$, il existe $\zeta \in K^\times$ tel que $\zeta\mathfrak{a} = \mathfrak{b}$. En considérant la matrice $U := \mathrm{Diag}(\zeta, 1, \dots, 1) \in \mathrm{GL}_n(K)$, on montre que

$$\begin{array}{ccc} \mathrm{GL}_n(\mathfrak{a}) & \longrightarrow & \mathrm{GL}_n(\mathfrak{b}) \\ P & \longmapsto & UPU^{-1} \end{array}$$

est un isomorphisme de groupes. □

Exemple II.3.17 Lorsque $K = \mathbb{Q}$, un réseau de rang n est toujours isomorphe à $\mathbb{Z}^n$. En particulier son stabilisateur dans $\mathrm{GL}_n(\mathbb{R})$ s'identifie à $\mathrm{GL}_n(\mathbb{Z})$ et l'ensemble $\mathscr{L}_n(\mathbb{R})$ des réseaux euclidiens de rang n s'identifie à $\mathrm{GL}_n(\mathbb{R})/\mathrm{GL}_n(\mathbb{Z})$.

Exemple II.3.18 Nous nous sommes restreints dans le chapitre précédent à la « partie libre » de l'ensemble des réseaux de rang n sur $K := \mathbb{Q}(i\sqrt{D})$, c'est-à-dire à

$$\mathrm{GL}_{K_{\mathbb{R}}}(E) \cdot \mathcal{O}_K^n \cong \mathrm{GL}_n(\mathbb{C})/\mathrm{GL}_n(\mathcal{O}_K).$$

II.3.3 Minimum et vecteurs minimaux

Le minimum d'un réseau algébrique est défini comme le minimum du réseau euclidien associé :

Définition II.3.19 *Le minimum d'un réseau algébrique Λ est*

$$m(\Lambda) := \inf_{x \in \Lambda \setminus \{0\}} \|x\|^2.$$

Un élément $x \in \Lambda$ tel que $\|x\|^2 = m(\Lambda)$ est appelé un vecteur minimal de Λ. L'ensemble des vecteurs minimaux de Λ est noté $S(\Lambda)$.

En vertu du caractère discret et fermé de Λ dans E, l'ensemble $S(\Lambda)$ est fini et non vide. Plus généralement, si $c \in \mathbb{R}_{>0}$, l'ensemble

$$\{x \in \Lambda \,:\, 0 < \|x\|^2 \leqslant c\}$$

est lui aussi fini, et non vide si $c \geqslant m(\Lambda)$. D'autre part, deux réseaux algébriques $K_{\mathbb{R}}$-isométriques étant en particulier isométriques comme réseaux euclidiens, ils ont le même minimum et leurs vecteurs minimaux sont en bijection.

II.3.4 Discriminant et inégalité de Hadamard généralisée

On note $\mathrm{N}_{K_{\mathbb{R}}}$ la norme de la $\mathbb{R}$-algèbre $K_{\mathbb{R}}$: si $x \in K_{\mathbb{R}}$, on a

$$\mathrm{N}_{K_{\mathbb{R}}}(x) = \prod_{\sigma \in \Sigma_K} \sigma(x),$$

Ainsi, $\mathrm{N}_{K_{\mathbb{R}}}$ coïncide sur K avec la norme de $K/\mathbb{Q}$, notée N_K. De plus, si $\mathfrak{a}$ est un idéal fractionnaire de K, on note $\mathcal{N}(\mathfrak{a})$ sa norme. Rappelons que si $x \in K$, on a $\mathcal{N}((x)) = \mathrm{N}_K(x) = \mathrm{N}_{K_{\mathbb{R}}}(x)$.

Lemme II.3.20 *Soit $\Lambda = \mathfrak{a}_1 b_1 \oplus \cdots \oplus \mathfrak{a}_n b_n$ un réseau algébrique de E. Soient B la matrice formée des vecteurs $b_1, \ldots, b_n$ et $\mathfrak{a} := (\mathfrak{a}_1 \cdots \mathfrak{a}_n)$. La grandeur $N_{K_{\mathbb{R}}}(\det(B))\mathcal{N}(\mathfrak{a})$ ne dépend pas de la pseudo-base de Λ choisie.*

Démonstration. Soient $(\mathfrak{b}_i, c_i)_{1 \leqslant i \leqslant n}$ une autre pseudo-base de Λ, C la matrice formée des vecteurs $c_1, \ldots, c_n$ et $\mathfrak{b} := (\mathfrak{b}_1 \cdots \mathfrak{b}_n)$. D'après la Proposition II.3.9, la matrice $P \in \mathrm{GL}_n(K)$ telle que $B = PC$ vérifie $\det(P)\mathfrak{a} = \mathfrak{b}$. Ainsi

$$\mathrm{N}_{K_{\mathbb{R}}}(\det(C))\mathcal{N}(\mathfrak{b}) = \mathrm{N}_{K_{\mathbb{R}}}(\det(P^{-1}B))\mathcal{N}(\det(P)\mathfrak{a}) = \mathrm{N}_{K_{\mathbb{R}}}(\det(B))\mathcal{N}(\mathfrak{a}).$$

D'où le résultat annoncé. □

Définition II.3.21 *Soit $\Lambda = \mathfrak{a}_1 b_1 \oplus \cdots \oplus \mathfrak{a}_n b_n$ un réseau algébrique de E. Soient B la matrice formée des vecteurs $b_1, \ldots, b_n$ et $\mathfrak{a} := (\mathfrak{a}_1 \cdots \mathfrak{a}_n)$. Le discriminant de Λ est*

$$\Delta(\Lambda) := \left|N_{K_{\mathbb{R}}}(\det(B))\right| \mathcal{N}(\mathfrak{a}).$$

Notons que pour $K = \mathbb{Q}$ et $\mathfrak{a}_i = \mathbb{Z}$ pour tout $1 \leqslant i \leqslant n$, on retrouve la notion usuelle de discriminant d'un réseau euclidien définie dans [Mar03, def.1.2.4, p.5]. De plus, pour $K = \mathbb{Q}(i\sqrt{D})$ et $\mathfrak{a}_i = \mathcal{O}_K$ pour tout $1 \leqslant i \leqslant n$, cette définition généralise celle donnée dans la Section I.2.2.2 (puisque $\mathcal{N}(\mathcal{O}_K) = 1$ et $\mathrm{N}_{K_{\mathbb{R}}}(x) = |x|^2$ pour tout $x \in K_{\mathbb{R}}$). L'inégalité de Hadamard classique ([Mar03, §2.1, p.37–39]), que nous avons déjà étendue dans la Section I.2.3.1, se généralise d'ailleurs aisément au cas des réseaux algébriques généraux :

Proposition II.3.22 (Inégalité de Hadamard) *Soit $(b_1, \ldots, b_n)$ une base de Λ. On a l'inégalité*

$$\Delta(\Lambda)^{1/d} \leqslant \mathcal{N}(\mathfrak{a})^{1/d} \prod_{i=1}^{n} \|b_i\|.$$

Démonstration. On considère $(b'_1, \dots, b'_n)$ la $K_{\mathbb{R}}$-base orthogonale de E définie par

$$\begin{cases} b'_1 = b_1, \\ b'_{i+1} = b_{i+1} - \sum_{j=1}^{i} \mu_{i+1,j} b'_j \quad \forall\, 1 \leqslant i < n. \end{cases}$$

où les $\mu_{i,j}$ sont des éléments de $\mathbb{R}$ définis pour tous $1 \leqslant i, j \leqslant n$ par :

$$\mu_{i,j} = \begin{cases} \dfrac{\langle b_i \mid b'_j \rangle}{\|b'_j\|^2} & \text{si } j < i, \\ 1 & \text{si } i = j, \\ 0 & \text{sinon.} \end{cases}$$

On vérifie que[6] $\det(b_1, \dots, b_n) = \det(b'_1, \dots, b'_n)$ et $\|b_i\| \geqslant \|b'_i\|$ pour tout $1 \leqslant i \leqslant n$. Puisque $(b'_1, \dots, b'_n)$ est une base orthogonale, on a

$$|\det(b'_1, \dots, b'_n)|^2 = \prod_{i=1}^{n} \|b'_i\|^2.$$

Finalement, en utilisant que $\mathrm{N}_{K_{\mathbb{R}}}(x) = x^d$ pour $x \in \mathbb{R}$, on obtient

$$|\mathrm{N}_{K_{\mathbb{R}}}(\det(b_1, \dots, b_n))| = \mathrm{N}_{K_{\mathbb{R}}}\left(\prod_{i=1}^{n} \|b'_i\|\right) = \prod_{i=1}^{n} \|b'_i\|^d \leqslant \prod_{i=1}^{n} \|b_i\|^d.$$

En multipliant de part et d'autre par $\mathcal{N}(\mathfrak{a})$, l'inégalité annoncée est démontrée. □

II.3.5 Isométrie et groupe d'automorphisme

Les réseaux algébriques étant en particulier des réseaux euclidiens, on peut parler d'isométrie et d'automorphisme de réseaux algébriques au sens euclidien :

Définition II.3.23 *Deux réseaux algébriques Λ et Λ' de E sont dits $\mathbb{R}$-isométriques s'il existe $u \in \mathrm{O}_{\mathbb{R}}(E)$ tel que $u(\Lambda) = \Lambda'$. Une $\mathbb{R}$-isométrie de Λ sur lui même est appelée un $\mathbb{R}$-automorphisme de Λ. On note $\mathrm{Aut}_{\mathbb{R}}(\Lambda)$ le groupe des $\mathbb{R}$-automorphismes de Λ.*

La notion de $K_{\mathbb{R}}$-isomorphisme introduite dans le paragraphe précédent tient compte de la structure algébrique mais pas de la structure euclidienne. Au contraire, une $\mathbb{R}$-isométrie préserve toute la structure euclidienne, mais seulement une partie de la structure algébrique (la structure de $\mathbb{Z}$-module est préservée mais pas celle de $\mathcal{O}_K$-module). Ainsi, comme suggéré dans [OY10], l'extension naturelle de la notion d'isométrie entre réseaux algébriques est plutôt celle de $K_{\mathbb{R}}$-isométrie.

6. Le lecteur attentif remarquera que nous introduisons ici une généralisation de procédé d'orthogonalisation de Gram/Schmidt et de ses propriétés (voir la Section I.3.1).

Définition II.3.24 *Deux réseaux algébriques Λ et Λ' de E sont dits $K_{\mathbb{R}}$-isométriques s'il existe $u \in \mathrm{O}_{K_{\mathbb{R}}}(E)$ tel que $u(\Lambda) = \Lambda'$. Une $K_{\mathbb{R}}$-isométrie de Λ sur lui même est appelée un $K_{\mathbb{R}}$-automorphisme de Λ. On note $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$ le groupe des $K_{\mathbb{R}}$-automorphismes de Λ.*

Alternativement, une $K_{\mathbb{R}}$-isométrie est une application qui est à la fois un $K_{\mathbb{R}}$-isomorphisme et une $\mathbb{R}$-isométrie. Le groupe des $K_{\mathbb{R}}$-automorphismes de Λ est donc simplement le sous-groupe des éléments $K_{\mathbb{R}}$-linéaires de $\mathrm{Aut}_{\mathbb{R}}(\Lambda)$. De même, deux réseaux algébriques sont $K_{\mathbb{R}}$-isométriques s'il existe une $\mathbb{R}$-isométrie $K_{\mathbb{R}}$-linéaire entre ces derniers. On déduit de ces remarques la finitude de $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$:

Proposition II.3.25 *Soit Λ un réseau algébrique de $K_{\mathbb{R}}^n$. Les groupes $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$ et $\mathrm{Aut}_{\mathbb{R}}(\Lambda)$ sont finis.*

Démonstration. Puisque Λ est un $\mathbb{Z}$-réseau euclidien, on sait d'après [Mar03, thm.1.4.2, p.12] que $\mathrm{Aut}_{\mathbb{R}}(\Lambda)$ est un groupe fini. Comme $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$ est un sous-groupe de $\mathrm{Aut}_{\mathbb{R}}(\Lambda)$, le résultat est démontré. □

Soulignons que la preuve de la finitude du groupe des automorphismes d'un réseau euclidien n'est pas constructive, dans le sens où elle ne fournit pas de borne sur la taille de ce dernier. La démonstration s'appuie en effet sur le caractère discret de $\mathrm{GL}_n(\mathbb{Z})$ et sur la compacité de $\mathrm{O}_n(\mathbb{R})$.

Exemple II.3.26 Pour $K = \mathbb{Q}$, les notions de $\mathbb{R}$-isométrie et $K_{\mathbb{R}}$-isométrie sont confondues. En particulier, on parlera simplement d'isométrie et d'automorphisme dans ce cas, et le groupe d'automorphisme d'un réseau euclidien Λ sera noté $\mathrm{Aut}(\Lambda)$.

Nous introduisons dans la suite de ce paragraphe la notion de *décomposition isotypique* d'un réseau algébrique, qui nous sera notamment utile pour déterminer le groupes des $K_{\mathbb{R}}$-automorphismes du réseau algébrique $\mathcal{O}_K^n$. Avant cela, il nous faut revenir sur la notion de réseau algébrique relatif.

Définition II.3.27 *Un réseau algébrique relatif de E est une paire (Λ, E') telle que*

- *E' est un sous-$K_{\mathbb{R}}$-module de E.*
- *Λ est un sous-$\mathcal{O}_K$-module et un réseau euclidien (pas nécessairement de rang maximal) de E'.*

Nous désignerons souvent un réseau algébrique relatif (Λ, E') seulement par Λ. Un réseau algébrique relatif de E est en particulier un $\mathbb{Z}$-réseau de rang inférieur ou égal à nd et un $\mathcal{O}_K$-module de rang inférieur ou égal à n. Il est bon de rappeler que les sous-$K_{\mathbb{R}}$-modules de E ne sont pas nécessairement libres, ce qui complexifie grandement l'étude des réseaux algébriques relatifs.

Définition II.3.28 *Soient $\Lambda \subset E$ un réseau algébrique et $(\Lambda_i, E_i)_{1 \leqslant i \leqslant r}$ des réseaux algébriques relatifs E. On dit que Λ est la somme orthogonale des (Λ_i, E_i) si*

(i) $\Lambda = \Lambda_1 + \cdots + \Lambda_r$.

(ii) Les sous-$K_{\mathbb{R}}$-modules E_i sont deux-à-deux orthogonaux comme sous-$\mathbb{R}$-espaces vectoriels de E.

Dans ce cas, on note

$$\Lambda = (\Lambda_1, E_1) \perp \cdots \perp (\Lambda_r, E_r).$$

On dit que Λ est irréductible s'il ne possède pas de décomposition orthogonale de la forme

$$\Lambda = (\Lambda_1, E_1) \perp (\Lambda_2, E_2)$$

avec (Λ_1, E_1) et (Λ_2, E_2) des réseaux algébriques relatifs non nuls.

Dans la suite, une relation de la forme $\Lambda = (\Lambda_1, E_1) \perp \cdots \perp (\Lambda_r, E_r)$ sera souvent appelée une *décomposition orthogonale* de Λ, et les réseaux algébriques relatifs (Λ_i, E_i) seront appelés les *facteurs* de la décomposition. Si $\Lambda = (\Lambda_1, E_1) \perp \cdots \perp (\Lambda_r, E_r)$ comme réseau algébrique, alors $\Lambda = \Lambda_1 \oplus \cdots \oplus \Lambda_r$ et $E = E_1 \oplus \cdots \oplus E_r$. De plus, cette décomposition est aussi celle de Λ vu comme un réseau euclidien (au sens de [Mar03, §1.4, p.15]). En particulier, on en déduit que

$$m(\Lambda) = \min_{1 \leqslant i \leqslant r} m(\Lambda_i)$$

et

$$S(\Lambda) = \bigcup_{\substack{1 \leqslant i \leqslant r \\ m(\Lambda_i) = m(\Lambda)}} S(\Lambda_i).$$

Commençons par démontrer une généralisation du théorème de décomposition de Eichler et Kneser [7] [Mar03, thm.1.4.5, p.15] :

Théorème II.3.29 *Un réseau algébrique $\Lambda \subset E$ possède une décomposition orthogonale*

$$\Lambda = (\Lambda_1, E_1) \perp \cdots \perp (\Lambda_r, E_r)$$

en réseaux algébriques relatifs irréductibles. De plus, cette décomposition est unique à permutation des facteurs près.

Démonstration. Commençons par prouver l'existence d'une telle décomposition. Si Λ est irréductible, il n'y a rien à démontrer. Sinon, il existe (Λ_1, E_1) et (Λ_2, E_2) des réseaux algébriques relatifs non nuls de E tels que $\Lambda = (\Lambda_1, E_1) \perp (\Lambda_2, E_2)$. Puisque

$$\mathrm{rg}_{\mathbb{Z}}(\Lambda) > \max\left(\mathrm{rg}_{\mathbb{Z}}(\Lambda_1), \mathrm{rg}_{\mathbb{Z}}(\Lambda_2)\right),$$

un raisonnement inductif sur le $\mathbb{Z}$-rang prouve l'existence.

Reste à prouver l'unicité d'une telle décomposition. Pour cela, nous construisons une décomposition orthogonale particulière de Λ et prouvons c'est la seule décomposition orthogonale

7. Ce résultat (dans le cas euclidien) est essentiellement dû à Eichler, mais sa démonstration a été simplifiée par Kneser. Notons d'ailleurs que la preuve de Kneser est constructive, dans le sens où elle fournit un algorithme permettant de calculer la décomposition orthogonale irréductible d'un réseau euclidien. Le lecteur intéressé par ces aspects algorithmiques pourra consulter [HV98, §4.3].

irréductible de Λ. Un élément $x \in \Lambda$ est dit *réduit* s'il ne peut pas être écrit comme une somme de deux vecteurs non nuls de Λ strictement plus courts que x. On note $\mathfrak{R}$ l'ensemble des vecteurs réduits de Λ. Fixons $(\omega_1, \dots, \omega_d)$ une $\mathbb{Q}$-base de K. Deux vecteurs réduits $x, y, \in \mathfrak{R}$ sont dits *équivalents*, noté $x \sim y$, s'il existe une séquence $x_0 = x, x_1, \dots, x_N = y \in \mathfrak{R}$ telle que pour tout $0 \leqslant i < N$, il existe $1 \leqslant k, l \leqslant d$ tels que $\langle \omega_k x_i \,|\, \omega_l x_{i+1} \rangle \neq 0$. Cette relation est une relation d'équivalence sur $\mathfrak{R}$. Soit $\mathcal{R}$ un système de représentants de $\mathfrak{R}/\sim$ et, pour tout $x \in \mathcal{R}$, soit $\mathfrak{R}_x$ la classe d'équivalence de x. Pour tout $x \in \mathcal{R}$, considérons le réseau relatif (Λ_x, E_x) de E formé de

$$E_x := \mathrm{Vect}_{K_{\mathbb{R}}}(\mathfrak{R}_x) \subset E$$

et

$$\Lambda_x := \mathrm{Vect}_{\mathcal{O}_K}(\mathfrak{R}_x) \subset \Lambda$$

Montrons que $\Lambda = \perp_{x \in \mathcal{R}} (\Lambda_x, E_x)$.

Il faut dans un premier temps prouver que les sous-$\mathbb{R}$-espaces vectoriels E_x sont deux-à-deux orthogonaux. Soient $x, y \in \mathcal{R}$ distincts, $x' \in E_x$ et $y' \in E_y$. Puisque $(\omega_1, \dots, \omega_d)$ est une $\mathbb{Q}$-base de K, on a

$$E_x = \mathrm{Vect}_{\mathbb{R}}(\{\omega_i z \,:\, 1 \leqslant i \leqslant d,\, z \in \mathfrak{R}_x\}).$$

En particulier, on peut écrire

$$x' = \sum_{\substack{1 \leqslant i \leqslant d \\ z \in \mathfrak{R}_x}} \alpha_{i,z} \omega_i z,$$

où les $\alpha_{i,z}$ sont des coefficients réels nuls sauf pour un nombre fini de couples $(i, z) \in \{1, \dots, n\} \times \mathfrak{R}_x$. De même, on peut écrire

$$y' = \sum_{\substack{1 \leqslant j \leqslant d \\ t \in \mathfrak{R}_y}} \beta_{j,t} \omega_j t,$$

où les $\beta_{j,t}$ sont des coefficients réels nuls sauf pour un nombre fini de couples $(j, t) \in \{1, \dots, n\} \times \mathfrak{R}_y$. Dès lors, par $\mathbb{R}$-bilinéarité, on a

$$\langle x' \,|\, y' \rangle = \sum_{\substack{1 \leqslant i,j \leqslant d \\ z \in \mathfrak{R}_x \\ t \in \mathfrak{R}_y}} \alpha_{i,z} \beta_{j,t} \langle \omega_i z \,|\, \omega_j t \rangle.$$

Pour tout $z \in \mathfrak{R}_x$, tout $t \in \mathfrak{R}_y$ et tous $\leqslant i, j \leqslant d$, on a $\langle \omega_i z \,|\, \omega_j t \rangle = 0$; en effet, dans le cas contraire, cela entraînerait que $x \sim y$, ce qui est impossible puisque x et y sont choisis distincts dans $\mathcal{R}$. Les espaces E_x sont donc bien deux-à-deux orthogonaux.

Reste à montrer que $\Lambda = \sum_{x \in \mathcal{R}} \Lambda_x$. Remarquons que $\mathcal{R}$ est fini. En effet, pour tous $x_1, \dots, x_k \in \mathcal{R}$ distincts, on a

$$k \leqslant \mathrm{rg}_{\mathbb{Z}} \left(\sum_{i=1}^{k} \Lambda_{x_i} \right) = \sum_{i=1}^{k} \mathrm{rg}_{\mathbb{Z}} \left(\Lambda_{x_i} \right) \leqslant \mathrm{rg}_{\mathbb{Z}}(\Lambda) = nd.$$

De plus, tout élément de Λ est une somme (finie) d'éléments de $\mathfrak{R}$ (donc un élément de $\sum_{x\in\mathcal{R}}\Lambda_x$). En effet, si $x\in\Lambda$ est réduit, il n'y a rien à démontrer. Sinon, x est une somme de deux vecteurs strictement plus courts, et une récurrence sur la longueur des vecteurs considérés (qui est un ensemble discret) permet de conclure.

Finalement, montrons que toute décomposition orthogonale en facteurs irréductibles de Λ est égale à la décomposition $\perp_{x\in\mathcal{R}}(\Lambda_x, E_x)$. Supposons donc donné $\Lambda = (\Lambda_1, E_1)\perp\cdots\perp(\Lambda_r, E_r)$ une décomposition orthogonale en réseaux algébriques irréductibles. Pour tout $x\in\mathcal{R}$ il existe $1\leqslant i_x\leqslant r$ tel que $\Lambda_x\subset\Lambda_{i_x}$. Puisque

$$\Lambda = \bigoplus_{x\in\mathcal{R}}\Lambda_x = \bigoplus_{i=1}^{r}\Lambda_i,$$

chaque Λ_i est égal à la somme orthogonale des réseaux Λ_x qu'il contient. Par irréductibilité, on a donc l'égalité $\Lambda_x = \Lambda_{i_x}$. Ceci entraîne que $E_x\subset E_{i_x}$. Comme $E_i\cap E_j = \{0\}$ pour $i\neq j$, on a aussi $E_y\cap E_{i_x} = \{0\}$ pour tous $x, y\in\mathcal{R}$ distincts. En utilisant l'égalité

$$E = \bigoplus_{i=1}^{r}E_i = \bigoplus_{x\in\mathcal{R}}E_x,$$

on en déduit que $E_x = E_{i_x}$, ce qui conclut la preuve. □

À l'aide de ce résultat, il est possible de relier $\mathrm{Aut}_{K_\mathbb{R}}(\Lambda)$ aux groupes $\mathrm{Aut}_{K_\mathbb{R}}(\Lambda_i)$. Soit (Λ, E') un réseau algébrique relatif de E. Le $K_\mathbb{R}$-module E' est dotée d'une structure d'espace euclidien induite par celle de E. On note $\mathrm{Aut}_{K_\mathbb{R}}(\Lambda, E')$ le groupe (fini) des $K_\mathbb{R}$-automorphismes orthogonaux de E' qui préservent Λ. De même, deux réseaux algébriques relatifs (Λ_1, E_1') et (Λ_2, E_2') de E sont $K_\mathbb{R}$-isométriques s'il existe un isomorphisme de $K_\mathbb{R}$-modules $f : E_1'\longrightarrow E_2'$ qui est une $\mathbb{R}$-isométrie et telle que $f(\Lambda_1) = f(\Lambda_2)$.

Un réseau algébrique est dit *$K_\mathbb{R}$-isotypique* si les facteurs de sa décomposition orthogonale irréductibles sont deux-à-deux $K_\mathbb{R}$-isométriques. En rassemblant les facteurs $K_\mathbb{R}$-isométriques de la décomposition orthogonale irréductible d'un réseau algébrique $\Lambda\subset E$, on obtient sa *décomposition $K_\mathbb{R}$-isotypique*. La décomposition $K_\mathbb{R}$-isotypique de Λ est donc de la forme

$$\Lambda = \left(\bigoplus_{i=1}^{r_1}\Lambda_{1,i}, \bigoplus_{i=1}^{r_1}E_{1,i}\right)\perp\cdots\perp\left(\bigoplus_{i=1}^{r_s}\Lambda_{s,i}, \bigoplus_{i=1}^{r_s}E_{s,i}\right),$$

où les réseaux algébriques relatifs irréductibles $(\Lambda_{i,j}, E_{i,j})$ et $(\Lambda_{i,k}, E_{i,k})$ sont deux à deux $K_\mathbb{R}$-isométriques pour tout $1\leqslant i\leqslant s$ et tous $1\leqslant j,k\leqslant r_i$. Il est maintenant possible de lier le groupe des $K_\mathbb{R}$-automorphismes d'un réseau algébrique à ceux de ses facteurs orthogonaux irréductibles.

Théorème II.3.30 *Soient Λ un réseau algébrique de E et $\Lambda = (\Lambda_1, E_1)\perp\cdots\perp(\Lambda_s, E_s)$ sa décomposition $K_\mathbb{R}$-isotypique. On a*

$$\mathrm{Aut}_{K_\mathbb{R}}(\Lambda)\cong\mathrm{Aut}_{K_\mathbb{R}}(\Lambda_1, E_1)\oplus\cdots\oplus\mathrm{Aut}_{K_\mathbb{R}}(\Lambda_s, E_s). \tag{II.7}$$

De plus, si Λ est $K_{\mathbb{R}}$-isotypique tel que ses r facteurs orthogonaux irréductibles sont $K_{\mathbb{R}}$-isométriques à un réseau algébrique relatif (Λ_0, E_0), il y a un isomorphisme de groupes

$$\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda) \cong \mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda_0, E_0) \wr \mathfrak{S}_r. \tag{II.8}$$

Démonstration. Commençons par démontrer l'isomorphisme (II.7). Par unicité de la décomposition $K_{\mathbb{R}}$-isotypique (qui découle de l'unicité de la décomposition orthogonale en facteurs irréductibles), on a $f(\Lambda_i) = \Lambda_i$ pour tout $1 \leqslant i \leqslant s$ et tout $f \in \mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$. Le morphisme de groupes

$$\begin{array}{ccc} \mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda) & \longrightarrow & \mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda_1, E_1) \oplus \cdots \oplus \mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda_s, E_s) \\ f & \longmapsto & (f_{|E_1}, \ldots, f_{|E_s}) \end{array}$$

est donc bien défini, et bijectif puisque $E = E_1 \perp \cdots \perp E_s$ et $\Lambda = \Lambda_1 \oplus \cdots \oplus \perp \Lambda_s$.

Établissons maintenant l'isomorphisme (II.8). Rappelons que le produit en couronne $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda_0, E_0) \wr \mathfrak{S}_r$ s'identifie au produit cartésien $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda_0, E_0)^r \times \mathfrak{S}_r$ muni de la loi de groupe

$$(f_1, \ldots, f_r, \sigma) \cdot (g_1, \ldots, g_r, \tau) := (f_1 g_{\sigma(1)}, \ldots, f_r g_{\sigma(r)}, \sigma\tau),$$

où $f_1, \ldots, f_r, g_1, \ldots, g_r \in \mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda_0, E_0)$ et $\sigma, \tau \in \mathfrak{S}_r$. On suppose que

$$\Lambda = (\Lambda_1, E_1) \perp \cdots \perp (\Lambda_r, E_r),$$

où pour tout $1 \leqslant i \leqslant r$, (Λ_i, E_i) est un réseau algébrique relatif irréductible de E qui est $K_{\mathbb{R}}$-isométrique à (Λ_0, E_0). On note $\phi_i : E_i \longrightarrow E_0$ la $K_{\mathbb{R}}$-isométrie en question. Pour tout $f \in \mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$, il existe une permutation $\sigma_f \in \mathfrak{S}_r$ telle que $f_{|E_i}$ est une $K_{\mathbb{R}}$-isométrie entre Λ_i et $\Lambda_{\sigma_f(i)}$ pour tout $1 \leqslant i \leqslant r$. Ainsi, le morphisme de groupes

$$\begin{array}{ccc} \mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda) & \longrightarrow & \mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda_0, E_0) \wr \mathfrak{S}_r \\ f & \longmapsto & \left(\phi_{\sigma_f(1)} f_{|E_1} \phi_1^{-1}, \ldots, \phi_{\sigma_f(r)} f_{|E_r} \phi_r^{-1}, \sigma_f\right) \end{array}$$

est bien défini. On vérifie que le morphisme réciproque de cette application est le morphisme qui à $(f_1, \ldots, f_r, \sigma) \in \mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda_0, E_0) \wr \mathfrak{S}_r$ associe l'unique application $f \in \mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$ telle que la restriction $f_{|E_i} : E_i \longrightarrow E_{\sigma}(i)$ soit égale à $\phi_{\sigma(i)}^{-1} f_i \phi_i$ pour tout $1 \leqslant i \leqslant r$. □

Le groupe $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda, E')$ où (Λ, E') est un réseau algébrique relatif est généralement difficile à expliciter, notamment si E n'est pas un $K_{\mathbb{R}}$-module libre. Néanmoins, ce résultat permet d'expliciter le groupe d'automorphisme de $\mathcal{O}_K^n$, situation dans laquelle cette difficulté liée à la liberté n'apparaît pas. Soit μ_K le groupe des racines de l'unité de K.

Lemme II.3.31 *Pour tout $x \in \mathcal{O}_K \setminus \{0\}$, on a $\|x\|^2 \geqslant d$, avec égalité si et seulement si $x \in \mu_K$.*

Démonstration. C'est une reformulation du Lemme I.3.6. □

Dans la suite, on note $(\varepsilon_1, \ldots, \varepsilon_n)$ la $K_{\mathbb{R}}$-base standard de E, définie au début de la Section II.2.3.

Proposition II.3.32 *Soit $\mathcal{O}_K^n$ le réseau algébrique de E donné par $\mathcal{O}_K^n = \mathcal{O}_K\varepsilon_1 \oplus \cdots \oplus \mathcal{O}_K\varepsilon_n$, où $(\varepsilon_1, \ldots, \varepsilon_n)$ désigne la $K_\mathbb{R}$-base standard de E. On a*

$$\mathrm{Aut}_{K_\mathbb{R}}(\mathcal{O}_K^n) \cong \mu_K \wr \mathfrak{S}_n.$$

Démonstration. Les facteurs orthogonaux irréductibles de $\mathcal{O}_K^n$ sont exactement les réseaux algébriques relatifs $(\mathcal{O}_K\varepsilon_i, K_\mathbb{R}\varepsilon_i)$ pour $1 \leqslant i \leqslant n$. Ces réseaux algébriques sont tous $K_\mathbb{R}$-isométriques au réseau algébrique (de rang maximal) $\mathcal{O}_K$ de $K_\mathbb{R}$. Ainsi, $\mathcal{O}_K^n$ est un réseau $K_\mathbb{R}$-isotypique et en vertu du théorème précédent, on a

$$\mathrm{Aut}_{K_\mathbb{R}}(\mathcal{O}_K^n) \cong \mathrm{Aut}_{K_\mathbb{R}}(\mathcal{O}_K) \wr \mathfrak{S}_n.$$

Reste à montrer que $\mathrm{Aut}_{K_\mathbb{R}}(\mathcal{O}_K) \cong \mu_K$. Comme remarqué dans [Bel04, §4.3, p.28–29], il est possible de choisir $(\omega_1, \ldots, \omega_d)$ une $\mathbb{Q}$-base de K telle que $\omega_1 = 1$. Puisque cette base est une $\mathbb{R}$-base de $K_\mathbb{R}$, on montre que

$$\mathrm{Aut}_{K_\mathbb{R}}(\mathcal{O}_K) \cong \left\{x \in \mathcal{O}_K^\times \,:\, \langle \omega_i x \,|\, \omega_j x\rangle = \langle \omega_i \,|\, \omega_j\rangle \ \forall\, 1 \leqslant i, j \leqslant d\right\}.$$

En particulier, un élément $x \in \mathrm{Aut}_{K_\mathbb{R}}(\mathcal{O}_K)$ vérifie en particulier $\|x\|^2 = \|\omega_1\|^2 = \|1\|^2 = d$, ce qui entraîne que $x \in \mu_K$ d'après le lemme précédent. Réciproquement, considérons $x \in \mu_K$. Puisque $\sigma(x)$ est une racine de l'unité dans $\mathbb{C}$, on a pour tout $1 \leqslant i, j \leqslant d$

$$\langle \omega_i x \,|\, \omega_j x\rangle = \sum_{\sigma\in\Sigma_K} |\sigma(x)|^2 \overline{\sigma}(\omega_i)\sigma(\omega_j) = \sum_{\sigma\in\Sigma_K} \overline{\sigma}(\omega_i)\sigma(\omega_j) = \langle \omega_i \,|\, \omega_j\rangle,$$

ce qui montre que $x \in \mathrm{Aut}_{K_\mathbb{R}}(\Lambda)$. □

Puisque le groupe des racines de l'unité de $\mathbb{Q}$ est $\mu_\mathbb{Q} = \{\pm 1\}$, ce résultat généralise l'identification classique $\mathrm{Aut}(\mathbb{Z}^n) \cong \{\pm 1\} \wr \mathfrak{S}_n$, démontrée dans [Mar03, thm.4.1.1, p.110]. Rappelons que pour tout corps K, le groupe μ_K est cyclique (voir [Sam67, §1.6, p.28–29]). Ainsi, $\mathrm{Aut}_{K_\mathbb{R}}(\mathcal{O}_K)$ s'identifie à un groupe symétrique généralisé, et est donc formé de matrices monomiales.

II.4 Formes de Humbert : le cadre additif

II.4.1 Définitions et liens avec les formes quadratiques

Les formes de Humbert, introduites par Humbert dans [Hum39 ; Hum49] sous le nom de *systèmes de formes quadratiques définies positives*, sont une généralisation des formes quadratiques dans le contexte relatif de la théorie algébrique des nombres.

Définition II.4.1 *Une forme de Humbert de rang n sur K est une matrice symétrique $A \in \mathrm{H}_n(K_\mathbb{R})$ définie positive, c'est-à-dire telle que $\langle Ax \,|\, x\rangle > 0$ pour tout $x \in E$ non nul. L'ensemble des formes de Humbert de rang n sur K est noté $\mathrm{H}_n^{>0}(K_\mathbb{R})$.*

Exemple II.4.2 Lorsque $K = \mathbb{Q}$, les formes de Humbert de rang n sur K sont exactement les matrices symétriques définies positives à coefficients dans $\mathbb{R}$. Autrement dit, ce sont les formes quadratiques sur $\mathbb{R}^n$ définies positives.

Exemple II.4.3 Lorsque K un corps quadratique imaginaire, les formes de Humbert de rang n sur K sont exactement les matrices hermitiennes définies positives à coefficients dans $\mathbb{C}$. Autrement dit, ce sont les formes hermitiennes sur $\mathbb{C}^n$ définies positives.

Deux approches sont possibles concernant les formes de Humbert :

- une approche *multiplicative*, dans laquelle l'évaluation d'une forme de Humbert est définie en utilisant la *norme* du corps de nombres. C'est par exemple le cadre d'étude de [BI97 ; Ica97 ; Bae+01 ; Cou01 ; BC15].
- une approche *additive*, utilisant plutôt la *trace* du corps de nombres pour déterminer la valeur d'une forme de Humbert en un point. C'est le point de vue adopté dans [FP96 ; Lei05 ; OY10 ; FS10 ; WYH13].

Nous nous plaçons dans le cadre *additif* de cette théorie, plus propice à une étude algorithmique que le cadre multiplicatif. Le lecteur intéressé par une comparaison succincte entre les contextes additif et multiplicatif de la théorie des formes de Humbert pourra consulter [Cou04, §1.2, p.8–12].

Fixons $A \in \mathrm{H}_n^{>0}(K_{\mathbb{R}})$ une forme de Humbert de rang n sur K. Pour tous $x, y \in E$, on pose $A[x,y] := \langle Ax \,|\, y\rangle$ et $A[x] := A[x,x]$. À l'aide de la Proposition II.2.3, on montre que $\mathrm{H}_n^{>0}(K_{\mathbb{R}})$ s'identifie à $\mathrm{S}_n^{>0}(\mathbb{R})^r \times \mathrm{H}_n^{>0}(\mathbb{C})^s$ et

$$A[x,y] = \sum_{\sigma\in\Sigma} \sigma(x)^* \sigma(A) \sigma(y) \tag{II.9}$$

pour tous $x, y \in E$. En particulier, on retrouve ainsi la définition originale de Humbert, qui considère des systèmes constitués de r formes quadratiques définies positives et s formes hermitiennes définies positives.

À l'aide de la formule (II.9), nous allons construire une forme quadratique classique qui est, en un sens que nous préciserons, associée à la forme de Humbert A. Soient $\mathfrak{A} := (\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$ une famille d'idéaux fractionnaires de K et $\widetilde{A} \in \mathrm{GL}_{nd}(\mathbb{C})$ la matrice diagonale par blocs

$$\widetilde{A} := \begin{pmatrix} \sigma_1(A) & & \\ & \ddots & \\ & & \sigma_d(A) \end{pmatrix}.$$

Proposition II.4.4 *Pour tout $1 \leqslant i \leqslant n$, soit $(\omega_1^{(i)}, \ldots, \omega_d^{(i)})$ une $\mathbb{Z}$-base de $\mathfrak{a}_i$. Soit $B_{\mathfrak{A}} \in \mathrm{M}_{nd}(\mathbb{C})$ la matrice définie par blocs :*

$$B_{\mathfrak{A}} := \begin{pmatrix} B_{1,1} & \cdots & B_{1,d} \\ \vdots & \ddots & \vdots \\ B_{1,1} & \cdots & B_{d,d} \end{pmatrix},$$

où, pour tous $1 \leqslant i, j \leqslant n$, $B_{i,j} \in \mathrm{GL}_n(\mathbb{C})$ *est la matrice diagonale*

$$B_{i,j} := \mathrm{Diag}\left(\sigma_i(\omega_j^{(i)}), \ldots, \sigma_i(\omega_j^{(i)})\right).$$

La matrice $Q_{A,\mathfrak{A}} := B_{\mathfrak{A}}^* \widetilde{A} B_{\mathfrak{A}} \in \mathrm{M}_{nd}(\mathbb{C})$ *vérifie les propriétés suivantes :*

(i) $Q_{A,\mathfrak{A}}$ *est une matrice symétrique définie positive (réelle).*

(ii) Soit $x = (x_1, \ldots, x_n) \in E$. *Pour tout* $1 \leqslant i \leqslant n$, *soit* $y_i \in \mathbb{R}^d$ *le vecteur colonne des coordonnées de* x_i *dans la* $\mathbb{R}$*-base* $(\omega_1^{(i)}, \ldots, \omega_d^{(i)})$ *et soit* $y := (y_1, \ldots, y_n) \in \mathbb{R}^{nd}$. *On a l'égalité* $A[x] = Q_{A,\mathfrak{A}}[y]$.

Démonstration. Puisque $\widetilde{A}$ et $B_{\mathfrak{A}}$ sont données par blocs, on procède de même avec la matrice Q :

$$Q_{A,\mathfrak{A}} = \begin{pmatrix} Q_{1,1} & \cdots & Q_{1,d} \\ \vdots & \ddots & \vdots \\ Q_{1,1} & \cdots & Q_{d,d} \end{pmatrix},$$

où, pour tous $1 \leqslant i, j \leqslant d$ et $1 \leqslant k, l \leqslant n$, on obtient par un calcul direct que

$$Q_{i,j,k,l} = \sum_{\sigma \in \Sigma_K} \overline{\sigma}\left(\omega_i^{(k)}\right) \sigma\left(A_{k,l}\right) \sigma\left(\omega_j^{(l)}\right).$$

À l'aide de cette relation, on montre l'égalité $A[x] = Q_{A,\mathfrak{A}}[y]$ du point (ii). On en déduit que $Q_{A,\mathfrak{A}}$ est définie positive (puisque A l'est) et réelle (puisque $A[x] \in \mathbb{R}$ pour tout $x \in E$). □

II.4.2 Minimum et vecteurs minimaux

Dans la suite, on fixe $A \in \mathrm{H}_n^{>0}(K_{\mathbb{R}})$ une forme de Humbert de rang n sur K et $\mathfrak{A} := (\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$ une famille d'idéaux fractionnaires de K. Le $\mathfrak{A}$-minimum de A est défini de manière analogue au minimum d'une forme quadratique classique.

Définition II.4.5 *Le* $\mathfrak{A}$*-minimum de* A *est*

$$m_{\mathfrak{A}}(A) := \inf_{x \in \mathfrak{A} \setminus \{0\}} A[x].$$

Un élément $x \in \mathfrak{A}$ *tel que* $A[x] = m_{\mathfrak{A}}(A)$ *est appelé un vecteur* $\mathfrak{A}$*-minimal de* A. *L'ensemble des vecteurs* $\mathfrak{A}$*-minimaux de* A *est noté* $S_{\mathfrak{A}}(A)$.

Exemple II.4.6 Lorsque $K = \mathbb{Q}$, on ne considère généralement que le cas $\mathfrak{a}_i = \mathbb{Z}$ pour tout $1 \leqslant i \leqslant n$. Dès lors, le minimum d'une forme quadratique définie positive Q sera simplement noté $m(Q)$, et l'ensemble de ses vecteurs minimaux $S(Q)$.

Proposition II.4.7 *Soit* $Q_{A,\mathfrak{A}} \in S_{nd}^{>0}(\mathbb{R})$ *la forme quadratique associée à* A *et* $\mathfrak{A}$ *définie dans la Proposition II.4.4. On a l'égalité* $m(Q_{A,\mathfrak{A}}) = m_{\mathfrak{A}}(A)$. *De plus* $S(Q_{A,\mathfrak{A}})$ *et* $S_{\mathfrak{A}}(A)$ *sont en bijection.*

Démonstration. En reprenant les notations de la Proposition II.4.4, ces propriétés découlent de l'égalité $A[x] = Q_{A,\mathfrak{A}}[y]$ et du fait que $x \in \mathfrak{A}$ si et seulement si $y \in \mathbb{Z}^{nd}$. □

En particulier, on déduit de cette proposition que $S_{\mathfrak{A}}(A)$ est un ensemble fini et non vide. Plus généralement, si $c \in \mathbb{R}_{>0}$, l'ensemble

$$\{x \in \mathfrak{A} \,:\, 0 < A[x] \leqslant c\}$$

est lui aussi fini, et non vide si $c \geqslant m_{\mathfrak{A}}(A)$.

II.4.3 Discriminant

Rappelons que la norme de la $\mathbb{R}$-algèbre $K_{\mathbb{R}}$ est notée $\mathrm{N}_{K_{\mathbb{R}}}$.

Lemme II.4.8 *Soit $A \in \mathrm{H}_n^{>0}(K_{\mathbb{R}})$. La grandeur $\mathrm{N}_{K_{\mathbb{R}}}(\det(A))$ est un réel strictement positif.*

Démonstration. On a

$$\mathrm{N}_{K_{\mathbb{R}}}(\det(A)) = \prod_{\sigma \in \Sigma_K} \sigma(\det(A)) = \prod_{\sigma \in \Sigma_K} \det(\sigma(A))).$$

Puisque A est une forme de Humbert, $\sigma(A)$ est une matrice hermitienne (symétrique si σ est un plongement réel) définie positive, et donc en particulier $\det(\sigma(A)) > 0$. □

Définition II.4.9 *Le discriminant de $A \in \mathrm{H}_n^{>0}(K_{\mathbb{R}})$ est $\Delta(A) := \mathrm{N}_{K_{\mathbb{R}}}(\det(A))^{1/2}$.*

Exemple II.4.10 Le discriminant d'une forme quadratique définie positive (qui est une forme de Humbert sur $K = \mathbb{Q}$) est usuellement défini comme la racine carrée du déterminant de sa matrice [8]. Puisque $N_{\mathbb{Q}_{\mathbb{R}}} = \mathrm{id}$, cette définition est bien celle que nous avons donné dans un cadre général.

II.4.4 Équivalence intégrale et automorphisme

Soient $A \in \mathrm{H}_n^{>0}(K_{\mathbb{R}})$ et $\mathfrak{A} := (\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$ une famille d'idéaux fractionnaires de K.

Définition II.4.11 *Deux formes de Humbert $A, B \in \mathrm{H}_n^{>0}(K_{\mathbb{R}})$ sont dites $\mathfrak{A}$-équivalentes s'il existe $P \in \mathrm{GL}_n(\mathfrak{A})$ telle que $P^*AP = B$. On dit alors que P est une $\mathfrak{A}$-équivalence entre A et B. Une $\mathfrak{A}$-équivalence entre A et elle-même est appelée un $\mathfrak{A}$-automorphisme de A. On note $\mathrm{Aut}_{\mathfrak{A}}(A)$ le groupe des $\mathfrak{A}$-automorphismes de A.*

Exemple II.4.12 Pour $K = \mathbb{Q}$ et $\mathfrak{a}_i = \mathbb{Z}$ pour tout $1 \leqslant i \leqslant n$, on a $\mathrm{GL}(\mathfrak{A}) = \mathrm{GL}_n(\mathbb{Z})$. La $\mathfrak{A}$-equivalence entre formes de Humbert dans cette situation est donc l'équivalence intégrale usuelle entre formes quadratriques.

8. Notons que les notions de *discriminant* et de *déterminant* sont parfois confondues. Dans ce cas, le discriminant est égal au carré de la valeur que nous définissons.

Il est possible de prouver que $\mathrm{Aut}_{\mathfrak{A}}(A)$ est un groupe fini en utilisant le caractère discret des $\mathfrak{a}_i$ dans $K_{\mathbb{R}}$. Nous proposons ici une preuve légèrement différente.

Proposition II.4.13 *Soit $P \in \mathrm{Aut}_{\mathfrak{A}}(A)$. Notons $x_1, \dots, x_n$ les colonnes de P et $(e_1, \dots, e_n)$ la base standard de E. Pour tout $1 \leqslant i \leqslant n$, on a*

(i) $x_i \in \mathfrak{a}_1\mathfrak{a}_i^{-1} \oplus \cdots \oplus \mathfrak{a}_n\mathfrak{a}_i^{-1}$.

(ii) $A[x_i] = A[e_i]$.

En particulier, le groupe $\mathrm{Aut}_{\mathfrak{A}}(A)$ est fini.

Démonstration. Le premier point est une reformulation de la Proposition II.3.9. Soit $1 \leqslant i \leqslant n$. On a

$$\begin{aligned}(P^*AP)[e_i] &= \sum_{\sigma\in\Sigma_K} \sigma(e_i)^*\sigma(P^*AP)\sigma(e_i)\\ &= \sum_{\sigma\in\Sigma_K} \sigma(Pe_i)^*\sigma(A)\sigma(Pe_i)\\ &= A[Pe_i].\end{aligned}$$

Puisque $(e_1, \dots, e_n)$ est la base standard de E, $Pe_i = x_i$. D'où le second point.

En utilisant la forme quadratique associée à A et $(\mathfrak{a}_1\mathfrak{a}_i^{-1}, \dots, \mathfrak{a}_n\mathfrak{a}_i^{-1})$ définie dans la Proposition II.4.4, on montre que l'ensemble

$$\left\{x \in (\mathfrak{a}_1\mathfrak{a}_i^{-1}, \dots, \mathfrak{a}_n\mathfrak{a}_i^{-1}) \,:\, A[x] = A[e_i]\right\}$$

est fini. Ainsi, il n'y a qu'un nombre fini de possibilités pour chaque colonne de P, ce qui prouve la finitude de $\mathrm{Aut}_{\mathfrak{A}}(A)$. □

Remarquons que la condition $\det(P) \in \mathcal{O}_K^\times$ est automatiquement vérifiée lorsque P préserve une forme de Humbert :

Proposition II.4.14 *Soit $P \in \mathrm{M}_n(K_{\mathbb{R}})$ tel que $P_{i,j} \in \mathfrak{a}_i\mathfrak{a}_j^{-1}$ pour tous $1 \leqslant i, j \leqslant n$ et $P^*AP = A$. Alors $\det(P) \in \mathcal{O}_K^\times$.*

Démonstration. Le déterminant de P est un entier de K. En effet :

$$\det(P) = \sum_{\tau\in\mathfrak{S}_n} \varepsilon(\tau)\prod_{i=1}^n P_{i,\tau(i)} \in \sum_{\tau\in\mathfrak{S}_n}\prod_{i=1}^n \mathfrak{a}_i\mathfrak{a}_{\tau(i)}^{-1} = \sum_{\tau\in\mathfrak{S}_n}\prod_{i=1}^n \mathfrak{a}_i\mathfrak{a}_i^{-1} = \mathcal{O}_K.$$

Ainsi, pour montrer que $\det(P) \in \mathcal{O}_K^\times$, il suffit de montrer que $\mathrm{N}_{K/\mathbb{Q}}(\det(P)) = \pm 1$. Soit $\sigma \in \Sigma$. La relation $P^*AP = A$ entraîne que $\sigma(P)^*\sigma(A)\sigma(P) = \sigma(A)$, et donc que $|\sigma(\det(P))| = 1$. Dès lors,

$$|\mathrm{N}_{K/\mathbb{Q}}(\det(P))| = \prod_{\sigma\in\Sigma_K} |\sigma(\det(P))| = 1.$$

Ainsi, $\det(P)$ est bien une unité de $\mathcal{O}_K$. □

Il n'est pas difficile de vérifier que des formes de Humbert équivalentes partagent des propriétés similaires :

Proposition II.4.15 *Soient $P \in \mathrm{GL}_n(\mathfrak{A})$ et $B = P^*AP$.*

(i) A et B ont le même discriminant.

(ii) A et B ont le même $\mathfrak{A}$-minimum. De plus, $S_{\mathfrak{A}}(A)$ et $S_{\mathfrak{A}}(B)$ sont en bijection.

II.4.5 Constante de Hermite généralisée

Cette section est consacrée à l'extension de quelques définitions et résultats de [Lei05] sur la constante de Hermite généralisée. Les travaux de Leibak se restreignent au cas du $\mathfrak{A}$-minimum de formes de Humbert à coefficients dans K^n avec $\mathfrak{A} = (\mathcal{O}_K, \dots, \mathcal{O}_K)$. Nous les généralisons pour les formes de Humbert quelconques et toute famille d'idéaux fractionnaires. Nous utilisons le langage des formes de Humbert, mais il est tout à fait possible d'exprimer les notions de cette section en termes de réseaux algébriques à l'aide du dictionnaire développé dans le paragraphe suivant. Nous avons d'ailleurs étendu la notion classique de constante de Hermite dans le langage des réseaux algébriques sur $\mathbb{Q}(i\sqrt{D})$ avec $D \in \{1, 2, 3, 7, 11\}$ dans la Section I.2.3.2. Dans la suite, on fixe $\mathfrak{A} := (\mathfrak{a}_1, \dots, \mathfrak{a}_n)$ une famille d'idéaux fractionnaires de K.

Définition II.4.16 *Soit $A \in \mathrm{H}_n^{>0}(K_{\mathbb{R}})$ une forme de Humbert de rang n sur K. Le $\mathfrak{A}$-invariant de Hermite de A est*

$$\gamma_{\mathfrak{A},K}(A) := \frac{m_{\mathfrak{A}}(A)}{\Delta(A)^{2/nd}}.$$

La $\mathfrak{A}$-constante de Hermite de K est alors définie comme

$$\gamma_{\mathfrak{A},K} := \sup_{A \in \mathrm{H}_n^{>0}(K_{\mathbb{R}})} \gamma_{\mathfrak{A},K}(A).$$

Pour $K = \mathbb{Q}$ et $\mathfrak{a}_i = \mathbb{Z}$ pour tout $1 \leqslant i \leqslant n$, $\gamma_{\mathfrak{A},K}$ est la constante de Hermite usuelle, notée γ_n. Il est bien connu ([Mar03, §2.2, p.39–41] par exemple) que γ_n est finie pour tout $n \geqslant 1$ et vérifie $\gamma_n \leqslant (4/3)^{(n-1)/2}$. Néanmoins, la valeur exacte de γ_n n'est connue que pour $1 \leqslant n \leqslant 8$ et $n = 24$ (voir la Figure II.1). De plus, pour $K = \mathbb{Q}(i\sqrt{D})$ avec $D \in \{1, 2, 3, 7, 11\}$ et $\mathfrak{a}_i = \mathcal{O}_K$ pour tout $1 \leqslant i \leqslant n$, cette constante $\gamma_{\mathfrak{A},K}$ est égale à la constante $\gamma_{K,n}$ définie dans la Section I.2.3.2.

n	1	2	3	4	5	6	7	8	24
γ_n	1	$2/3^{1/2}$	$2^{1/3}$	$2^{1/2}$	$2^{3/5}$	$2/3^{1/6}$	$2^{6/7}$	2	4

Fig. II.1 – Valeurs connues de la constante de Hermite.

Il s'avère que la constante de Hermite généralisée est elle aussi finie. Il est même possible de la borner explicitement en utilisant l'inégalité de Hermite classique (voir par exemple [Mar03, thm.2.2.1, p.39]), dont nous avons démontrée une version « quadratique, euclidienne et imaginaire » dans le Théorème I.2.15.

Proposition II.4.17 *La constante de Hermite généralisée $\gamma_{\mathfrak{A},K}$ est finie. Plus précisément, on a*

$$\gamma_{\mathfrak{A},K} \leqslant \left(\frac{4}{3}\right)^{(nd-1)/2} D_{\mathfrak{A},K}^{2/nd},$$

où $D_{\mathfrak{A},K}$ est une constante (explicite) ne dépendant que de la famille d'idéaux fractionnaires $\mathfrak{A}$ et du corps K.

Démonstration. Soient $A \in \mathrm{H}_n^{>0}(K_{\mathbb{R}})$ et $Q_{A,\mathfrak{A}}$ la forme quadratique associée à A et $\mathfrak{A}$ définie dans la Proposition II.4.4. En reprenant les notations de cette proposition, on a $Q_{A,\mathfrak{A}} = B_{\mathfrak{A}}^* \widetilde{A} B_{\mathfrak{A}}$. Puisque $\Delta(A) = \det(\widetilde{A})^{1/2}$, on a

$$\det(Q_{A,\mathfrak{A}})^{1/2} = |\det(B_{\mathfrak{A}})| \Delta(A).$$

D'autre part, nous avons montrés dans la Proposition II.4.7 que $m_{\mathfrak{A}}(A) = m(Q_{A,\mathfrak{A}})$. Ainsi :

$$\gamma_{\mathfrak{A},K}(A) = \frac{m_{\mathfrak{A}}(A)}{\Delta(A)^{2/nd}} = \frac{m(Q_{A,\mathfrak{A}})}{\det(Q_{A,\mathfrak{A}})^{1/nd}} |\det(B_{\mathfrak{A}})|^{2/nd} \leqslant \gamma_{nd} |\det(B_{\mathfrak{A}})|^{2/nd}.$$

L'inégalité annoncée est démontrée avec $D_{\mathfrak{A},K} = |\det(B_{\mathfrak{A}})|$ à l'aide de l'inégalité de Hermite classique. □

II.5 Correspondance entre réseaux et formes

Le dictionnaire reliant les formes quadratiques et les réseaux euclidiens (détaillé par exemple dans [Mar03, §1.7, p.20–24]) est un outil puissant, que ce soit du point de vue théorique ou algorithmique : certaines questions sont plus faciles à traiter pour les réseaux que pour les formes quadratiques, et réciproquement. Nous démontrons dans cette section que les réseaux algébriques jouent le même rôle pour les formes de Humbert que les réseaux euclidiens pour les formes quadratiques.

Fixons $\Lambda_0 = \mathfrak{a}_1 b_1 \oplus \cdots \oplus \mathfrak{a}_n b_n$ un réseau algébrique de E. On note $\mathcal{B} := (b_1, \ldots, b_n)$ et $\mathfrak{A} := (\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$. Le stabilisateur de Λ_0 dans $\mathrm{GL}_n(K_{\mathbb{R}})$ s'identifie à $\mathrm{GL}_n(\mathfrak{A})$, qui agit par multiplication à droite sur $\mathrm{GL}_n(K_{\mathbb{R}})$. De plus, le groupe $\mathrm{O}_n(K_{\mathbb{R}})$ agit par multiplication à gauche sur $\mathrm{GL}_n(K_{\mathbb{R}})/\mathrm{GL}_n(\mathfrak{A})$. Dans la suite, si Λ et Λ' sont des réseaux algébriques de E, on note $\Lambda \sim \Lambda'$ si Λ et Λ' sont $K_{\mathbb{R}}$-isométriques.

Proposition II.5.1 *L'application*

$$\widetilde{\delta} : \{\Lambda \in \mathscr{L}_n(K_{\mathbb{R}}) \,:\, \Lambda \cong \Lambda_0\}/\sim \longrightarrow \mathrm{O}_n(K_{\mathbb{R}}) \backslash \mathrm{GL}_n(K_{\mathbb{R}}) / \mathrm{GL}_n(\mathfrak{A})$$

induite par

$$\begin{array}{rccc} \delta : & \{\Lambda \in \mathscr{L}_n(K_{\mathbb{R}}) \,:\, \Lambda \cong \Lambda_0\} & \longrightarrow & \mathrm{GL}_n(K_{\mathbb{R}})/\mathrm{GL}_n(\mathfrak{A}) \\ & u(\Lambda_0) & \longmapsto & [\mathrm{mat}_{\mathcal{B}}(u)] \end{array}$$

est une bijection.

Démonstration. L'identification usuelle entre l'orbite d'un élément et le quotient par son stabilisateur montre que δ est une bijection. Le fait que $\widetilde{\delta}$ soit aussi une bijection se déduit par passage au quotient. □

D'autre part, le groupe $\mathrm{GL}_n(\mathfrak{A})$ agit par conjugaison sur l'ensemble $\mathrm{H}_n^{>0}(K_{\mathbb{R}})$ des formes de Humbert de rang n sur K :

$$\begin{array}{ccc} \mathrm{GL}_n(\mathfrak{A}) \times \mathrm{H}_n^{>0}(K_{\mathbb{R}}) & \longrightarrow & \mathrm{H}_n^{>0}(K_{\mathbb{R}}) \\ (A, H) & \longmapsto & A^*HA \end{array} .$$

Proposition II.5.2 *L'application*

$$\widetilde{\eta} : \mathrm{O}_n(K_{\mathbb{R}}) \backslash \mathrm{GL}_n(K_{\mathbb{R}}) / \mathrm{GL}_n(\mathfrak{A}) \longrightarrow \mathrm{H}_n^{>0}(K_{\mathbb{R}}) / \mathrm{GL}_n(\mathfrak{A})$$

induite par

$$\begin{array}{rccc} \eta : & \mathrm{GL}_n(K_{\mathbb{R}}) & \longrightarrow & \mathrm{H}_n^{>0}(K_{\mathbb{R}}) \\ & A & \longmapsto & A^*A \end{array}$$

est une bijection.

Démonstration. Rappelons que si $B \in \mathrm{S}_n^{>0}(\mathbb{R})$ (resp. $B \in \mathrm{H}_n^{>0}(\mathbb{C})$), il existe $A \in \mathrm{GL}_n(\mathbb{R})$ (resp. $A \in \mathrm{GL}_n(\mathbb{C})$) telle que $B = A^*A$. En vertu des identifications démontrées dans la Proposition II.2.4 et la Proposition II.2.11 et de cette remarque, l'application δ est surjective. D'après le Corollaire II.2.8, si $A \in \mathrm{O}_n(K_{\mathbb{R}})$ et $B \in \mathrm{GL}_n(K_{\mathbb{R}})$, on a $(AB)^* = B^*A^*AB = B^*B$. Ainsi, l'application $\widetilde{\eta}$ induite par η est bien définie. La surjectivité de η entraînant celle de $\widetilde{\eta}$, il reste à démontrer que $\widetilde{\eta}$ est injective.

Soient $A, B \in \mathrm{GL}_n(K_{\mathbb{R}})$ telle que $A^*A = B^*B$ dans $\mathrm{H}_n^{>0}(K_{\mathbb{R}}) / \mathrm{GL}_n(\mathfrak{A})$. Il existe $U \in \mathrm{GL}_n(\mathfrak{A})$ telle que $A^*A = U^*B^*BU = (BU)^*(BU)$. Rappelons que si $P, Q \in \mathrm{GL}_n(\mathbb{R})$ (resp $P, BQ \in \mathrm{GL}_n(\mathbb{C})$) telles que $P^*P = Q^*Q$, alors il existe $V \in \mathrm{O}_n(\mathbb{R})$ (resp. $V \in \mathrm{U}_n(\mathbb{C})$) telle que $P = VQ$. En particulier, en utilisant les identifications établies dans la Proposition II.2.4 et la Proposition II.2.7, on en déduit l'existence d'une matrice $V \in \mathrm{O}_n(K_{\mathbb{R}})$ telle que $A = VBU$, ce qui entraîne que $A = B$ dans $\mathrm{O}_n(K_{\mathbb{R}}) \backslash \mathrm{GL}_n(K_{\mathbb{R}}) / \mathrm{GL}_n(\mathfrak{A})$. D'où l'injectivité de $\widetilde{\eta}$. □

En combinant ces deux propositions, nous obtenons l'identification suivante entre réseaux algébriques et formes de Humbert :

Théorème II.5.3 *L'application composée*

$$\{\Lambda \in \mathscr{L}_n(K_{\mathbb{R}}) \,:\, \Lambda \cong \Lambda_0\} / \sim \xrightarrow{\widetilde{\delta}} \mathrm{O}_n(K_{\mathbb{R}}) \backslash \mathrm{GL}_n(K_{\mathbb{R}}) / \mathrm{GL}_n(\mathfrak{A}) \xrightarrow{\widetilde{\eta}} \mathrm{H}_n^{>0}(K_{\mathbb{R}}) / \mathrm{GL}_n(\mathfrak{A})$$

est une bijection, où $\widetilde{\delta}$ est induite par

$$\begin{array}{rccc} \delta : & \{\Lambda \in \mathscr{L}_n(K_{\mathbb{R}}) \,:\, \Lambda \cong \Lambda_0\} & \longrightarrow & \mathrm{GL}_n(K_{\mathbb{R}}) / \mathrm{GL}_n(\mathfrak{A}) \\ & u(\Lambda_0) & \longmapsto & \left[\mathrm{mat}_{(b_1,\dots,b_n)}(u)\right] \end{array}$$

et $\widetilde{\eta}$ est induite par

$$\begin{array}{rccc} \eta : & \mathrm{GL}_n(K_{\mathbb{R}}) & \longrightarrow & \mathrm{H}_n^{>0}(K_{\mathbb{R}}) \\ & A & \longmapsto & A^*A \end{array}$$

Autrement dit, cette bijection fournit une correspondance entre les réseaux algébriques à $K_{\mathbb{R}}$-isométrie près et les formes de Humbert à équivalence près. Si Λ est un réseau algébrique de base $B \in \mathrm{GL}_n(K_{\mathbb{R}})$, alors B^*B est une forme de Humbert. Par abus de langage [9], nous dirons de B^*B que c'est la forme de Humbert associée à Λ. Réciproquement, si A est une forme de Humbert, il existe un réseau algébrique Λ de base $B \in \mathrm{GL}_n(K_{\mathbb{R}})$ tel que $B^*B = A$, que nous appellerons réseau algébrique associé à A.

Cette correspondance offre la possibilité de passer d'un langage à un autre suivant les notions manipulées. Fixons Λ un réseau algébrique de E de pseudo-base $(\mathfrak{a}_i, b_i)_{1\leqslant i\leqslant n}$ et $A := B^*B$ sa forme de Humbert associée (où B est la matrice de $(b_1, \dots, b_n)$). On note $\mathfrak{A} := (\mathfrak{a}_1, \dots, \mathfrak{a}_n)$.

- Soient $x, y \in E$, dont les coordonnées dans la base $(b_1, \dots, b_n)$ sont données respectivement par des vecteurs colonnes $X, Y \in K_{\mathbb{R}}^n$. On a $\langle x \,|\, y\rangle = A[X, Y]$. En effet, d'après le Corollaire II.2.9 :

$$A[X, Y] = \langle B^*BX \,|\, Y\rangle = \langle BX \,|\, BY\rangle = \langle x \,|\, y\rangle.$$

- En particulier, on en déduit que $m(\Lambda) = m_{\mathfrak{A}}(A)$ et que pour tout $c \in \mathbb{R}_{>0}$, l'application

$$\begin{array}{ccc} \{X \in \mathfrak{A} \,:\, 0 < A[X] \leqslant c\} & \longrightarrow & \{x \in \Lambda \,:\, 0 < \|x\|^2 \leqslant c\} \\ X & \longmapsto & BX \end{array}$$

  est une bijection.
- Il y a un isomorphisme de groupes

$$\begin{array}{ccc} \mathrm{Aut}(\Lambda) & \longrightarrow & \mathrm{Aut}_{\mathfrak{A}}(A) \\ u & \longmapsto & \mathrm{mat}_{(b_1,\dots,b_n)}(u) \end{array}.$$

  Soient $u \in \mathrm{Aut}(\Lambda)$ et $P := \mathrm{mat}_{(b_1,\dots,b_n)}(u)$. D'après la Proposition II.3.9, pour montrer que $P \in \mathrm{Aut}_{\mathfrak{A}}(A)$, il reste à montrer que $P^*AP = A$. Soit Q la matrice de u dans la base standard de E. Puisque u est un $K_{\mathbb{R}}$-endomorphisme orthogonal, on sait d'après le Corollaire II.2.8 que $Q^*Q = I_n$. Utilisée avec l'égalité $P = B^{-1}QB$, cette relation entraîne que $P^*AP = P^*B^*BP = B^*B = A$. Plus généralement, on montre que deux réseaux algébriques sont $K_{\mathbb{R}}$-isométriques si et seulement si les formes de Humbert correspondantes sont $\mathfrak{A}$-équivalentes.

Ces exemples ne sont pas exhaustifs : toute notion « raisonnable » sur les réseaux algébriques peut être traduite pour les formes de Humbert à l'aide de cette correspondance, et réciproquement.

9. Nous nous autorisons cet abus car la correspondance en question est principalement utilisée pour des propriétés ne dépendant pas des représentants choisis de part et d'autre.

III

EXTENSION DE L'ALGORITHME DE PLESKEN ET SOUVIGNIER

Sommaire

III.1 Introduction

La méthode la plus connue et la plus largement implantée à ce jour permettant de calculer le groupe d'automorphisme d'un réseau euclidien ou d'une forme quadratique définie positive est l'algorithme de Plesken et Souvignier [PS97], qui permet aussi de décider si deux réseaux euclidiens sont isométriques ou si deux formes quadratiques sont équivalentes. Ce chapitre est consacré à la généralisation de cet algorithme pour les réseaux algébriques. Nous nous concentrons dans un premier temps sur le problème de la détermination des $K_{\mathbb{R}}$-automorphismes d'un réseau algébrique. À l'aide de modifications mineures (détaillées dans la Section III.5), la méthode présentée permet aussi de décider si deux réseaux algébriques sont $K_{\mathbb{R}}$-isométriques. Notons que Braun, Coulangeon, Nebe et Schönnenbeck [Bra+15, §7.2] ont déjà considéré le problème de l'isométrie entre réseaux algébriques du point de vue des méthodes effectives, mais ils ont traité cette question en se ramenant à des réseaux euclidiens et en utilisant l'algorithme de Plesken et Souvignier classique. C'est une astuce que nous n'utilisons pas ici. Finalement, nous présentons dans le dernier paragraphe une adaptation de cet algorithme permettant de décider l'équivalence de formes quadratiques et de formes de Humbert modulo d'autres groupes que $\mathrm{GL}_n(\mathbb{Z})$ et $\mathrm{GL}_n(\mathcal{O}_K)$.

Dans tout ce chapitre, nous nous plaçons dans le cadre décrit dans le chapitre précédent. Soient K un corps de nombre de degré d et $K_{\mathbb{R}}^n := (K \otimes_{\mathbb{Q}} \mathbb{R})^n$. L'espace $K_{\mathbb{R}}^n$ est équipé du produit scalaire euclidien $\langle \cdot \,|\, \cdot \rangle$ issu de la norme T_2 (introduite dans la Section II.2.1). On note $\|\cdot\|$ la norme euclidienne associée.

III.2 Idée générale

Fixons Λ un réseau algébrique de $K_{\mathbb{R}}^n$. L'approche naïve pour calculer $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$ est d'identifier Λ à un réseau euclidien de $\mathbb{R}^{nd}$ à l'aide de la Proposition II.3.8, ce qui permet ensuite de calculer $\mathrm{Aut}_{\mathbb{R}}(\Lambda)$ avec l'algorithme de Plesken et Souvignier. Finalement, il ne reste plus qu'à filtrer les éléments $K_{\mathbb{R}}$-linéaires de ce groupe pour obtenir $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$. Cette approche est évidemment limitée :

- Le groupe $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$ peut être bien plus petit que $\mathrm{Aut}_{\mathbb{R}}(\Lambda)$, et la détermination de $\mathrm{Aut}_{\mathbb{R}}(\Lambda)$ peut donc entraîner de nombreux calculs superflus.
- Il est délicat d'obtenir une famille génératrice de $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$ à partir d'une famille génératrice de $\mathrm{Aut}_{\mathbb{R}}(\Lambda)$ sans passer par une énumération complète de $\mathrm{Aut}_{\mathbb{R}}(\Lambda)$.
- En identifiant Λ à un réseau euclidien, on passe d'un objet de dimension n sur $K_{\mathbb{R}}$ à un objet de dimension nd sur $\mathbb{R}$. Du point de vue de l'efficacité algorithmique, cette augmentation de la dimension est préjudiciable.

C'est pourquoi l'algorithme que nous présentons n'utilise pas directement [1] l'identification de Λ comme réseau euclidien. Notons tout de même qu'une manière plus raffinée d'utiliser l'algorithme classique pour les réseaux algébriques est présentée dans [Bra+15, §7.2], permettant

1. Mais cette identification reste en pratique nécessaire lors de la détermination d'un ensemble de la forme $\{x \in \Lambda : \|x\| \leqslant C\}$.

notamment d'éviter les écueils décrits dans les deux premiers points.

Exemple III.2.1 Prenons $K = \mathbb{Q}(i)$ et $\Lambda = \mathcal{O}_K^n \subset K_{\mathbb{R}}^n$. D'après la Proposition II.3.32, on a

$$\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda) \simeq \mu_K \wr \mathfrak{S}_n,$$

donc en particulier puisque $\mu_K = \{\pm 1, \pm i\}$

$$\left|\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)\right| = 4^n n!.$$

En prenant $(1, i)$ comme $\mathbb{Q}$-base de K, Λ est identifié au réseau euclidien $\mathbb{Z}^{nd} \subset \mathbb{R}^{nd}$. D'après [Mar03, thm.4.1.1, p.110], on a donc

$$|\mathrm{Aut}_{\mathbb{R}}(\Lambda)| = \left|\mathrm{Aut}(\mathbb{Z}^{nd})\right| = |\{\pm 1\} \wr \mathfrak{S}_{nd}| = 4^n (2n)!.$$

Le groupe $\mathrm{Aut}_{\mathbb{R}}(\Lambda)$ est donc $\frac{(2n)!}{n!}$ fois plus grand que le groupe $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$.

Soit $\mathscr{B}$ une pseudo-base de Λ donnée par $\mathcal{B} := (b_1, \ldots, b_n)$ une $K_{\mathbb{R}}$-base de $K_{\mathbb{R}}^n$ et $\mathfrak{A} := (\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$ une famille d'idéaux fractionnaires de K. Les $K_{\mathbb{R}}$-automorphismes de Λ sont caractérisés par la proposition suivante :

Proposition III.2.2 *Soit $(\omega_1, \ldots, \omega_d)$ une $\mathbb{Q}$-base de K. Un $K_{\mathbb{R}}$-endomorphisme $f : K_{\mathbb{R}}^n \longrightarrow K_{\mathbb{R}}^n$ est un $K_{\mathbb{R}}$-automorphisme de Λ si et seulement si :*

(i) $\langle f(\omega_k b_i) \,|\, f(\omega_l b_j)\rangle = \langle \omega_k b_i \,|\, \omega_l b_j\rangle$ *pour tous* $1 \leqslant i, j \leqslant n$ *et* $1 \leqslant k, l \leqslant d$.

(ii) $f(b_j) = \sum_{i=1}^n a_{i,j} b_i$ *avec* $a_{i,j} \in \mathfrak{a}_i \mathfrak{a}_j^{-1}$ *pour tous* $1 \leqslant i, j \leqslant n$. *Autrement dit, pour tout* $1 \leqslant j \leqslant n$, $f(b_j)$ *est un élément de* $\bigoplus_{i=1}^n \mathfrak{a}_i \mathfrak{a}_j^{-1} b_i$.

Démonstration. Puisque les $\omega_k b_i$ forment pour $1 \leqslant k \leqslant d$ et $1 \leqslant i \leqslant n$ une $\mathbb{R}$-base de $K_{\mathbb{R}}^n$, l'endomorphisme f est orthogonal si et seulement s'il vérifie le premier point.

D'après la Proposition II.3.9, un $K_{\mathbb{R}}$-automorphisme de Λ vérifie toujours le second point. Notons P la matrice de f dans la $K_{\mathbb{R}}$-base $\mathcal{B}$. Toujours en vertu de la Proposition II.3.9, pour conclure la démonstration, il suffit de montrer que si f est orthogonal et vérifie le second point, alors $\det(P) \in \mathcal{O}_K^\times$. En utilisant un argument similaire à celui utilisé pour prouver la Proposition II.4.14, cette propriété est démontrée. □

En nous appuyant sur ce résultat, nous reprenons et généralisons point par point l'algorithme de Plesken et Souvignier. Que ce soit dans le cas euclidien classique ou dans notre situation, la difficulté principale est l'obtention de $K_{\mathbb{R}}$-automorphismes particuliers (en un sens que nous préciserons plus loin) de Λ. En effet, une fois ces éléments particuliers calculables, le groupe $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$ est déterminé en adaptant des méthodes classiques issues de l'algorithmique des groupes de permutation. Nous nous concentrons donc dans un premier temps sur le problème de la détermination d'un $K_{\mathbb{R}}$-automorphisme de Λ.

Afin de déterminer un $f \in \mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$, l'idée est de calculer récursivement les images $f(b_1), f(b_2), \ldots, f(b_n)$ en tirant des éléments dans les ensembles donnés par la condition (ii) de la proposition précédente, et ceci en s'assurant à chaque étape que la condition (i) est satisfaite. La recherche d'un élément de $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$ peut donc être vue comme la recherche d'un chemin particulier de profondeur maximale dans un arbre ; la méthode employée est donc un algorithme de type *backtracking*.

III.3 Recherche d'un $K_{\mathbb{R}}$-automorphisme

Dans la suite, on fixe $\Omega := (\omega_1, \dots, \omega_d)$ une $\mathbb{Q}$-base de K. De plus, pour tout $1 \leqslant j \leqslant n$, on pose

$$\Lambda_j := \mathfrak{a}_1 \mathfrak{a}_j^{-1} b_1 \oplus \cdots \oplus \mathfrak{a}_n \mathfrak{a}_j^{-1} b_n.$$

III.3.1 Automorphisme partiel

Commençons par modifier la notion originale d'*automorphisme partiel* :

Définition III.3.1 *Soit $1 \leqslant m \leqslant n$. On appelle m-automorphisme partiel de Λ (suivant $\mathscr{B}$ et Ω) tout m-uplet $\mathcal{V} := (v_1, \dots, v_m)$ d'éléments de $K_{\mathbb{R}}^n$ tel que*

(i) $v_j \in \Lambda_j$ *pour tout* $1 \leqslant j \leqslant m$.

(ii) $\langle \omega_k v_i \,|\, \omega_l v_j \rangle = \langle \omega_k b_i \,|\, \omega_l b_j \rangle$ *pour tous* $1 \leqslant i, j \leqslant m$ *et* $1 \leqslant k, l \leqslant d$.

En particulier, en vertu de la Proposition III.2.2, un n-automorphisme partiel $\mathcal{V}$ de Λ définit un $K_{\mathbb{R}}$-automorphisme $f \in \mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$ en posant $f(b_i) = v_i$ pour tout $1 \leqslant i \leqslant n$. Réciproquement, un élément de $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$ définit de la même manière un n-automorphisme partiel de Λ. Nous déterminons donc un $K_{\mathbb{R}}$-automorphisme de Λ en complétant récursivement un 1-automorphisme partiel en un n-automorphisme partiel. Néanmoins, un m-automorphisme partiel ne peut pas toujours être complété en un n-automorphisme partiel. Ainsi, même s'il est raisonnablement aisé de tester si la complétion du rang m au rang $m+1$ est possible, il est souhaitable de disposer d'une méthode permettant d'éliminer rapidement les automorphismes partiels qui ne finiront pas par donner un élément de $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$. Avant d'introduire plusieurs invariants permettant d'effectuer de tels tests, remarquons que cette approche récursive est effectuée sur un nombre *fini* de possibilités :

Proposition III.3.2 *Pour tout $1 \leqslant m \leqslant n$, l'ensemble des m-automorphismes partiels de Λ est fini.*

Démonstration. Remarquons que puisque l'ensemble des n-automorphismes partiels de Λ est exactement $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$, nous avons déja démontré ce résultat de finitude pour $m = n$ dans la Proposition II.3.25. Pour tout $1 \leqslant j \leqslant n$ considérons

$$S_j(\Lambda, \mathscr{B}, \Omega) := \left\{ x \in \Lambda_j \,:\, \langle \omega_k x \,|\, \omega_l x \rangle = \langle \omega_k b_j \,|\, \omega_l b_j \rangle \ \forall\, 1 \leqslant k, l \leqslant d \right\}.$$

Par définition même, un m-automorphisme partiel de Λ a ses éléments dans

$$S_1(\Lambda, \mathscr{B}, \Omega) \times \cdots \times S_m(\Lambda, \mathscr{B}, \Omega),$$

et $S_j(\Lambda, \mathscr{B}, \Omega)$ est un ensemble fini pour tout $1 \leqslant j \leqslant n$. En effet, $\omega_1 \Lambda_j$ est un réseau algébrique de $K_{\mathbb{R}}^n$ et on a

$$S_j(\Lambda, \mathscr{B}, \Omega) \subset \omega_1^{-1} \cdot \left\{ y \in \omega_1 \Lambda_j \,:\, \|y\| = \|\omega_j b_j\| \right\}. \tag{III.1}$$

D'où le résultat annoncé. □

Comme nous le remarquerons dans le chapitre suivant (voir la Section IV.2.2), le calcul des ensembles $S_j(\Lambda, \mathscr{B}, \Omega)$ est une tâche difficile, qui est vraisemblablement la partie la plus coûteuse de l'algorithme. Notons que ces ensembles sont calculables en s'appuyant sur l'inclusion (III.1) puis en utilisant l'algorithme énumératif de Fincke et Pohst [FP85, §2] une fois le réseau $\omega_1\Lambda_j$ identifié à un réseau euclidien de $\mathbb{R}^{nd}$. Nous détaillons le calcul pratique de ces ensembles dans la Section V.4.1.1. Dans la suite, nous supposerons que ces ensembles ont été précalculés. Cette hypothèse est déjà présente dans l'algorithme original de Plesken et Souvignier, qui nécessite le précalcul des ensembles $\{x \in \Lambda \,:\, \|x\| = \|b_i\|\}$, où $(b_1, \ldots, b_n)$ est une base du réseau euclidien considéré.

III.3.2 Invariants pour le prolongement d'un automorphisme partiel

III.3.2.1 Empreinte d'une pseudo-base

Une première idée, connue dans le cas euclidien depuis les travaux de Plesken et Pohst [PP85, §3], est d'utiliser le résultat suivant :

Proposition III.3.3 *Soient $\mathcal{V}$ un m-automorphisme partiel de Λ (avec $1 \leqslant m < n$) et $f \in \mathrm{Aut}_{K_\mathbb{R}}(\Lambda)$. Le nombre d'éléments de Λ_{m+1} permettant de prolonger $\mathcal{V}$ en un $(m+1)$-automorphisme partiel est égal au nombre d'éléments de Λ_{m+1} permettant de prolonger $f(\mathcal{V}) := (f(v_1), \ldots, f(v_m))$ en un $(m+1)$-automorphisme partiel.*

Démonstration. Pour tout $x \in \Lambda_{m+1}$, $(\mathcal{V}, x)$ est un $(m+1)$-automorphisme partiel si et seulement si $(f(\mathcal{V}), f(x))$ en est un. □

Corollaire III.3.4 *Si un m-automorphisme partiel $\mathcal{V}$ se prolonge en un automorphisme de Λ, le nombre de prolongements de $\mathcal{V}$ en un $(m+1)$-automorphisme partiel est égal au nombre de prolongements de $(b_1, \ldots, b_m)$ en un $(m+1)$-automorphisme partiel.*

Cette propriété fournit un premier test pour vérifier si un automorphisme partiel est potentiellement prolongeable en un $K_\mathbb{R}$-automorphisme de Λ. Il est pour cela nécessaire de calculer le nombre de prolongements possibles de $(b_1, \ldots, b_m)$ en un $(m+1)$-automorphisme partiel pour tout $1 \leqslant m < n$. Cette donnée est appelée *empreinte de la pseudo-base $\mathscr{B}$ (suivant Ω)*.

Une permutation $\tau \in \mathfrak{S}_n$ de la pseudo-base $\mathscr{B}$ permettant de minimiser ces valeurs est également déterminée. Permuter les éléments de la pseudo-base initiale ne nécessite pas de recalculer les ensembles $S_j(\Lambda, \mathscr{B}, \Omega)$. En effet, si on note $\mathscr{B}^\tau$ la pseudo-base de Λ formée de $\mathcal{B}^\tau := (b_{\tau(1)}, \ldots, b_{\tau(n)})$ et $\mathfrak{A}^\tau := (\mathfrak{a}_{\tau(1)}, \ldots, \mathfrak{a}_{\tau(n)})$, on montre sans difficultés que

$$S_j(\Lambda, \mathscr{B}^\tau, \Omega) = S_{\tau(j)}(\Lambda, \mathscr{B}, \Omega)^\tau,$$

où τ agit sur $K_\mathbb{R}^n$ par permutation des coordonnées. Dans un souci de clarté et de lisibilité, nous supposerons dans la suite que la permutation τ est égale à l'identité. L'Algorithme III.1 implante les calculs de l'empreinte et de la permutation la minimisant.

Données :
- Une pseudo-base $\mathscr{B}$ de Λ.
- Une $\mathbb{Q}$-base Ω de K.
- Les ensemble $S_j(\Lambda, \mathscr{B}, \Omega)$ pour $1 \leqslant j \leqslant n$.

Résultat :
- L'empreinte $\mathcal{E}$ de $\mathcal{B}$ suivant Ω.
- La permutation τ minimisant l'empreinte.

calculer $\tau(1)$ tel que $\left|S_{\tau(1)}(\Lambda, \mathscr{B}, \Omega)\right| = \min_{1 \leqslant j \leqslant n} \left|S_j(\Lambda, \mathscr{B}, \Omega)\right|$.
$\mathcal{E}_1 := \left|S_{\tau(1)}(\Lambda, \mathscr{B}, \Omega)\right|$.
pour $2 \leqslant i \leqslant n$ faire
  pour $1 \leqslant j \leqslant n$ faire
    si $j \in \{\tau(1), \ldots, \tau(i-1)\}$ alors
      $\mathcal{F}_{i,j} := 0$.
    sinon
      $\mathcal{F}_{i,j} := \left|\left\{ x \in \mathcal{F}_{1,j} \,:\, \langle \omega_k x \,|\, \omega_l e_{\sigma(h)} \rangle = \langle \omega_k b_j \,|\, \omega_l e_{\sigma(h)} \rangle \quad \begin{array}{l} \forall\, 1 \leqslant k, l \leqslant d \\ \forall\, 1 \leqslant h < i \end{array} \right\}\right|$.
  calculer $\tau(i)$ tel que $\left|\mathcal{F}_{i,\tau(i)}\right| = \min_{\substack{1 \leqslant j \leqslant n \\ j \notin \{\tau(1), \ldots, \tau(i-1)\}}} \left|\mathcal{F}_{i,j}\right|$.
  $\mathcal{E}_i := \left|\mathcal{F}_{i,\tau(i)}\right|$.
retourner $\mathcal{E}$ et τ.

Algorithme III.1 - Calcul de l'empreinte d'une $K_{\mathbb{R}}$-base.

III.3.2.2 Combinaisons scalaires

Comme remarqué dans [PS97, §5], l'empreinte seule n'est parfois pas suffisante pour éliminer rapidement les automorphismes partiels qui ne définissent pas un $K_{\mathbb{R}}$-automorphisme de Λ. C'est pourquoi la notion de *combinaison scalaire* est introduite.

Soient $\mathcal{V}$ un m-automorphisme partiel de Λ et $s = (s_{k,l,j})_{1 \leqslant j \leqslant m}^{1 \leqslant k,l \leqslant d} \in \mathbb{R}^{md^2}$. On pose :

$$X_s(\mathcal{V}) := \left\{ x \in S_{m+1}(\Lambda, \mathscr{B}, \Omega) \,:\, \langle \omega_k x \,|\, \omega_l v_j \rangle = s_{k,l,j} \quad \begin{array}{l} \forall\, 1 \leqslant k, l \leqslant d \\ \forall\, 1 \leqslant j \leqslant m \end{array} \right\}$$

et

$$\widehat{X}_s(\mathcal{V}) := \sum_{x \in X_s(\mathcal{V})} x.$$

Puisque les $X_s(\mathcal{V})$ sont inclus dans $S_{m+1}(\Lambda, \mathscr{B}, \Omega)$, l'ensemble $\left\{ \widehat{X}_s(\mathcal{V}) \,:\, s \in \mathbb{R}^{md^2} \right\}$ est fini. On l'appelle l'ensemble des *sommes de combinaisons scalaires associées à $\mathcal{V}$ (suivant $\mathscr{B}$ et Ω)*. En utilisant la Proposition III.2.2, on montre que $f \in \mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$ préserve les ensembles $S_j(\Lambda, \mathscr{B}, \Omega)$. On en déduit la proposition suivante.

Données :
- Un m-automorphisme partiel $\mathcal{V}$ de Λ.
- Une $\mathbb{Q}$-base Ω de K.
- L'ensemble $S(\Lambda, \mathscr{B}, \Omega)$.

Résultat :
- Une K-base $\mathcal{X}$ extraite des $\widehat{X}_s(\mathcal{V})$, donnée par des indices $(s_1, \ldots, s_h)$.
- L'ensemble $\left\{ \langle \omega_k X_i \mid \omega_l X_j \rangle \ : \ \begin{array}{c} 1 \leqslant k, l \leqslant d \\ 1 \leqslant i, j \leqslant h \end{array} \right\}$.
- Les coordonnées des $\widehat{X}_s(\mathcal{V})$ dans la base $\mathcal{X}$.

pour $x \in S(\Lambda, \mathscr{B}, \Omega)$ faire
  pour $1 \leqslant k, l \leqslant d$ et $1 \leqslant j \leqslant m$ faire
    $s_{k,l,j} := \langle \omega_k x \mid \omega_l v_j \rangle$.
  soit $s = (s_{k,l,j})$. Ajouter x à $\widehat{X}_s(\mathcal{V})$.
extraire une K-base $\mathcal{X} = (X_1, \ldots, X_h)$ des $\widehat{X}_s(\mathcal{V})$.
déterminer les indices $(s_1, \ldots, s_h)$ tels que $X_i = \widehat{X}_{s_i}(v_1, \ldots, v_m)$ pour tout $1 \leqslant i \leqslant h$.
pour chaque $\widehat{X}_s(\mathcal{V})$ faire
  écrire $X_s(\mathcal{V}) = \sum_{i=1}^{h} \lambda_{s,i} X_i$ avec $\lambda_{s,i} \in K$.
pour $1 \leqslant k, l \leqslant d$ et $1 \leqslant i, j \leqslant h$ faire
  $G_{i,j,k,l} := \langle \omega_k X_i \mid \omega_l X_j \rangle$.
retourner $(s_1, \ldots, s_h)$, $(\lambda_{s,i})$ et G.

Algorithme III.2 - Calcul des combinaisons scalaires liées à un automorphisme partiel.

Proposition III.3.5 *Soit $f \in \mathrm{Aut}_{K_\mathbb{R}}(\Lambda)$. Pour tous $1 \leqslant m \leqslant n$ et $s \in \mathbb{R}^{md^2}$, l'application f induit une bijection entre $X_s(b_1, \ldots, b_m)$ et $X_s(f(b_1), \ldots, f(b_m))$. En particulier, on a*

$$f(\widehat{X}_s(b_1, \ldots, b_m)) = \widehat{X}_s(f(b_1), \ldots, f(b_m)).$$

Cette proposition fournira une seconde condition (détaillée dans la prochaine section) pour qu'un automorphisme partiel puisse être prolongé en un $K_\mathbb{R}$-automorphisme de Λ. Avant cela, il est nécessaire de précalculer pour tout $1 \leqslant m \leqslant n$ les combinaisons scalaires associées à $(b_1, \ldots, b_m)$ sous la forme suivante :

(a) On extrait une K-base $\mathcal{X} := (X_1, \ldots, X_h)$ de l'ensemble des $\widehat{X}_s(b_1, \ldots, b_m)$, donnée par des indices $(s_1, \ldots, s_h)$, de telle façon que $X_i = \widehat{X}_{s_i}(b_1, \ldots, b_m)$ pour tout $1 \leqslant i \leqslant h$. Notons que si $\mathcal{V}$ est un m-automorphisme partiel de Λ, pour tout $s \in \mathbb{R}^{md^2}$, $\widehat{X}_s(\mathcal{V})$ est un élément de $\mathrm{Vect}_K(\Lambda)$. En particulier, l'ensemble des combinaisons scalaires associées à un automorphisme partiel de Λ est de dimension au plus n sur K.

(b) On calcule l'ensemble $\left\{ \langle \omega_k X_i \mid \omega_l X_j \rangle \ : \ \begin{array}{c} 1 \leqslant k, l \leqslant d \\ 1 \leqslant i, j \leqslant h \end{array} \right\}$.

(c) On détermine les K-coordonnées des $\widehat{X}_s(b_1, \ldots, b_m)$ dans la base $\mathcal{X}$.

L'Algorithme III.2 détaille cette procédure.

III.3.3 Test d'un candidat et bilan

Soit $\mathcal{V}$ un m-automorphisme partiel de Λ. À partir des deux algorithmes précédents, nous construisons une méthode permettant de tester si $\mathcal{V}$ peut être prolongé en un $K_{\mathbb{R}}$-automorphisme de Λ. Soulignons néanmoins que les conditions que nous testons sont *nécessaires mais généralement non suffisantes* : il est possible qu'un automorphisme partiel passe ces tests sans finalement définir un $K_{\mathbb{R}}$-automorphisme de Λ. Soit C l'ensemble des éléments $x \in S_{m+1}(\Lambda, \mathscr{B}, \Omega)$ tels que $(\mathcal{V}, x)$ soit un $(m+1)$-automorphisme partiel.

(1) D'après le Corollaire III.3.4, si le cardinal de C n'est pas égal au nombre de prolongements de $(b_1, \dots, b_m)$ en un $(m+1)$-automorphisme partiel (précalculé par l'empreinte), alors $\mathcal{V}$ n'est pas prolongeable en un automorphisme de Λ.

(2) On calcule les $\widehat{X}_s(\mathcal{V})$ pour $s \in \mathbb{R}^{md^2}$. Si la base $\mathcal{X}$ du point (a) est donnée par des indices $(s_1, \dots, s_h)$, on pose ensuite $\widetilde{X}_i := \widehat{X}_{s_i}(\mathcal{V})$. Si $\mathcal{V}$ se prolonge en f un $K_{\mathbb{R}}$-automorphisme de Λ, en vertu de la Proposition III.3.5, $f(X_i) = \widetilde{X}_i$. Cependant, $f(X_i)$ n'est généralement pas calculable en connaissant seulement $\mathcal{V}$. C'est pourquoi on effectue plutôt les tests suivants :

   (i) On vérifie que $\langle \omega_k \widetilde{X}_i \,|\, \omega_l \widetilde{X}_j \rangle = \langle \omega_k X_i \,|\, \omega_l X_j \rangle$ pour tous $1 \leqslant i, j \leqslant h$ et $1 \leqslant k, l \leqslant d$ à l'aide des données du point (b). D'après la Proposition III.2.2, si $\mathcal{V}$ se prolonge en f, ces égalités sont vérifiées.

   (ii) En utilisant les données du point (c), chaque $\widehat{X}_s(b_1, \dots, b_m)$ s'écrit

$$\widehat{X}_s(b_1, \dots, b_m) = \sum_{i=1}^{h} \lambda_{s,i} X_i.$$

   On teste alors si $\widehat{X}_s(\mathcal{V}) = \sum_{i=1}^{h} \lambda_{s,i} \widetilde{X}_i$ pour tout $s \in \mathbb{R}^{nd^2}$. En effet, si $\mathcal{V}$ se prolonge en f, on obtient en utilisant Proposition III.3.5 :

$$f(\widehat{X}_s(b_1, \dots, b_m)) = \widehat{X}_s(\mathcal{V}) = \sum_{i=1}^{h} \lambda_{s,i} f(X_i) = \sum_{i=1}^{h} \lambda_{s,i} \widetilde{X}_i.$$

L'Algorithme III.3 implante cette phase de tests.

On en déduit enfin un algorithme permettant de déterminer un $K_{\mathbb{R}}$-automorphisme de Λ. On suppose que l'empreinte et les sommes de vecteurs de $\mathscr{B}$ sont précalculées à l'aide de l'Algorithme III.1 et de l'Algorithme III.2.

(1) On choisit un élément v_1 parmi l'ensemble $S_1(\Lambda, \mathscr{B}, \Omega)$ des 1-automorphismes partiels de Λ.

(2) Supposons déterminé $\mathcal{V}$ un m-automorphisme partiel de Λ. Si $m = n$, $\mathcal{V}$ définit un $K_{\mathbb{R}}$-automorphisme de Λ. Dans le cas contraire, on calcule l'ensemble C des éléments $x \in S_{m+1}(\Lambda, \mathscr{B}, \Omega)$ tels que $(\mathcal{V}, x)$ soit un $(m+1)$-automorphisme partiel, donné par

$$C := \left\{ x \in S_{m+1}(\Lambda, \mathscr{B}, \Omega) \,:\, \langle \omega_k x \,|\, \omega_l v_j \rangle = \langle \omega_k b_{m+1} \,|\, \omega_l b_j \rangle \quad \begin{matrix} \forall\, 1 \leqslant k, l \leqslant d \\ \forall\, 1 \leqslant j \leqslant m \end{matrix} \right\}.$$

On choisit $x \in C$ et on s'assure à l'aide de l'Algorithme III.3 que $(\mathcal{V}, x)$ est un bon candidat pour fournir un $K_{\mathbb{R}}$-automorphisme de Λ. Si $(\mathcal{V}, x)$ passe ce test avec succès, on pose $v_{m+1} = x$ et on passe à l'étape suivante. Sinon, un autre $x \in C$ est choisi. Si toutes les possibilités dans C sont épuisées, c'est que $\mathcal{V}$ ne peut pas être prolongé en un $K_{\mathbb{R}}$-automorphisme de Λ : on retourne donc à l'étape précédente.

Remarquons que cette méthode (Algorithme III.4) est aisément modifiable pour permettre le prolongement (si possible) d'un automorphisme partiel en un $K_{\mathbb{R}}$-automorphisme de Λ.

Données :
- Un m-automorphisme partiel $\mathcal{V}$ de Λ et l'ensemble C des candidats pour prolonger $\mathcal{V}$.
- L'ensemble $S(\Lambda, \mathscr{B}, \Omega)$.
- L'empreinte $\mathcal{E}$ de la pseudo-base $\mathscr{B}$ initiale de Λ donnée par l'Algorithme III.1.
- Les données $(s_1, \ldots, s_h)$, $(\lambda_{s,i})$ et G associées aux combinaisons scalaires de $(b_1, \ldots, b_m)$ renvoyées par l'Algorithme III.2.
- Une $\mathbb{Q}$-base Ω de K.

Résultat :
- Le résultat des tests de l'empreinte et des combinaisons scalaires sur $\mathcal{V}$.

```
1  si |C| ≠ E_m alors
2      retourner faux.
3  pour x ∈ S(Λ, B, Ω) faire
4      pour 1 ⩽ k, l ⩽ d et 1 ⩽ j ⩽ m faire
5          s_{k,l,j} := ⟨ω_k x | ω_l v_j⟩.
6      soit s = (s_{k,l,j}). Ajouter x à X̂_s(V).
7  pour 1 ⩽ i ⩽ h faire
8      X̃_i := X̂_{s_i}(V).
9      pour 1 ⩽ j ⩽ i et 1 ⩽ k, l ⩽ d faire
10         si ⟨ω_k X̃_i | ω_l X̃_j⟩ ≠ G_{i,j,k,l} alors
11             retourner faux.
12 pour chaque X̂_s(V) faire
13     si X̂_s(V) ≠ Σ_{i=1}^{h} λ_{s,i} X̃_i alors
14         retourner faux.
15 retourner vrai.
```

Algorithme III.3 - Test d'un prolongement : fonction `estCandidat`.

Données :
- Une pseudo-base $\mathscr{B}$ de Λ.
- Les ensemble $S_j(\Lambda, \mathscr{B}, \Omega)$ pour $1 \leqslant j \leqslant n$.
- L'empreinte $\mathcal{E}$ de pseudo-base initiale de Λ, donnée par l'Algorithme III.1.
- Les données des combinaisons scalaires de $(b_1, \dots, b_m)$ pour $1 \leqslant m < n$ renvoyées par l'Algorithme III.2.
- Une $\mathbb{Q}$-base Ω de K.

Résultat :
- Un $K_{\mathbb{R}}$-automorphisme de Λ.

1 $C_1 := S_1(\Lambda, \mathscr{B}, \Omega)$.
2 $i := 1$.
3 tant que $i \leqslant m-1$ faire
4 si $i = 1$ alors
5 choisir $v_1 \in C_1$.
6 $C_1 = C_1 \setminus \{v_1\}$.
7 $C_2 := \{x \in S_2(\Lambda, \mathscr{B}, \Omega) : \langle \omega_k x \,|\, \omega_l v_1 \rangle = \langle \omega_k b_2 \,|\, \omega_l b_1 \rangle \ \forall\, 1 \leqslant k, l \leqslant d\}$.
8 si estCandidat(v_1) (Algorithme III.3) alors
9 $i = i + 1$.
10 sinon
11 retourner à l'étape 5.
12 sinon
13 si $C_i = \emptyset$ alors
14 $i = i - 1$.
15 sinon
16 choisir $v_i \in C_i$.
17 $C_i = C_i \setminus \{v_i\}$.
18 $C_{i+1} := \left\{ x \in S_{i+1}(\Lambda, \mathscr{B}, \Omega) : \langle \omega_k x \,|\, \omega_l v_j \rangle = \langle \omega_k b_{i+1} \,|\, \omega_l b_j \rangle \ \begin{array}{l} \forall\, 1 \leqslant k, l \leqslant d \\ \forall\, 1 \leqslant j \leqslant i \end{array} \right\}$.
19 si estCandidat($v_1, \dots, v_i$) (Algorithme III.3) alors
20 $i = i + 1$.
21 sinon
22 retourner à l'étape 13.
23 choisir $v_m \in C_m$.
24 retourner $(v_1, \dots, v_m)$.

Algorithme III.4 - Calcul d'un $K_{\mathbb{R}}$-automorphisme.

III.4 Passage au groupe $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$

Dans [PS97, §8], Plesken et Souvignier ont montré qu'une fois connue une méthode pour calculer certains automorphismes d'un réseau euclidien, il est possible de passer au calcul du groupe d'automorphisme de ce réseau à l'aide de méthodes issues de l'algorithmique des groupes de permutation, notamment en adaptant l'algorithme de Schreier et Sims [But91, §13, p.129–142]. Cette stratégie est directement généralisable au cas des réseaux algébriques.

Dans la suite, on note G le groupe $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$. Pour tout $1 \leqslant k \leqslant n+1$, soit $G^{(k)}$ le stabilisateur de $b_1, \ldots, b_{k-1}$ dans G :

$$G^{(k)} := \{f \in G \,:\, f(b_i) = b_i \;\forall\, 1 \leqslant i < k\},$$

avec par convention $G^{(1)} = G$. On obtient ainsi une chaîne de stabilisateurs :

$$1 = G^{(n+1)} \leqslant G^{(m)} \leqslant \cdots \leqslant G^{(2)} \leqslant G^{(1)} = G,$$

où $G^{(i+1)}$ est le stabilisateur dans $G^{(i)}$ de b_i pour tout $1 \leqslant i \leqslant n$.

III.4.1 Famille génératrice forte

Par calculer le groupe G, nous entendons déterminer une famille génératrice de ce groupe. Plus précisément, nous allons déterminer une *famille génératrice forte* de G :

Définition III.4.1 *Une partie $\mathcal{G}$ de G est appelée une famille génératrice forte si $\mathcal{G} \cap G^{(k)}$ est une famille génératrice de $G^{(k)}$ pour tout $1 \leqslant k \leqslant n+1$.*

Puisque $G^{(1)} = G$, une famille génératrice forte est en particulier une famille génératrice de G. Ce concept est couramment utilisé en algorithmique des groupes de permutation (voir par exemple [But91, §10, p.78–97]), notamment dans le cadre de l'algorithme de Schreier et Sims. En remarquant que G s'identifie à un sous-groupe du groupe de permutation de l'ensemble $S(\Lambda, \mathscr{B}, \Omega)$, l'apparition de ce concept est naturelle. Commençons par remarquer qu'obtenir une famille génératrice forte de G permet de calculer à moindre frais l'ordre de G. En effet, pour calculer $|G|$, on peut se ramener au calcul $G^{(i)} \cdot b_i$ pour tout $1 \leqslant i \leqslant n$:

Proposition III.4.2 *L'ordre de G est donné par*

$$|G| = \prod_{i=1}^{n} \left|G^{(i)} \cdot b_i\right|.$$

Démonstration. Pour tout $1 \leqslant i \leqslant n$, puisque $G^{(i+1)}$ est le stabilisateur dans $G^{(i)}$ de b_i, on a

$$\left|G^{(i)}\right| = \frac{\left|G^{(i)} \cdot b_i\right|}{\left|G^{(i+1)}\right|}.$$

Une récurrence facile permet de conclure la démonstration. □

Ainsi, connaissant une famille génératrice de $G^{(i)}$ (donnée par une famille génératrice forte de G), le calcul de l'orbite de b_i sous $G^{(i)}$ est aisé en utilisant par exemple [But91, algo.1, p.57], et donc le calcul de l'ordre de G aussi.

Afin de déterminer une famille génératrice forte, nous allons nous appuyer sur le résultat suivant :

Proposition III.4.3 *Soit $\mathcal{G}$ une partie de G. Pour tout $1 \leqslant k \leqslant n+1$, notons $H^{(k)}$ le sous-groupe de $G^{(k)}$ engendré par $\mathcal{G} \cap G^{(k)}$. Si*

$$\left|H^{(k)} \cdot b_k\right| = \left|G^{(k)} \cdot b_k\right| \tag{III.2}$$

pour tout $1 \leqslant k \leqslant n+1$, alors $\mathcal{G}$ est une famille génératrice forte de G.

Démonstration. Soit $1 \leqslant k \leqslant n$. Puisque $G^{(k+1)}$ est le stabilisateur dans $G^{(k)}$ de b_k, $H^{(k+1)}$ est le stabilisateur dans $H^{(k)}$ de b_k. Ainsi par hypothèse :

$$\left|G^{(k)} \cdot b_k\right| = \frac{\left|G^{(k)}\right|}{\left|G^{(k+1)}\right|} = \left|H^{(k)} \cdot b_k\right| = \frac{\left|H^{(k)}\right|}{\left|H^{(k+1)}\right|}.$$

Par récurrence descendante sur k, il nous suffit donc de montrer que $G^{(n)} = H^{(n)}$. Puisqu'un élément de $G^{(n)}$ est complètement caractérisé par son image sur b_n, cette dernière égalité est vérifiée. □

Cette proposition suggère la méthode récursive que nous allons utiliser. Pour cela, on commence par définir la notion de *famille génératrice partielle* :

Définition III.4.4 *Soient $\mathcal{G}$ une partie de G et $1 \leqslant m \leqslant n+1$. Pour tout $1 \leqslant k \leqslant n+1$, notons $H^{(k)}$ le sous-groupe de $G^{(k)}$ engendré par $\mathcal{G} \cap G^{(k)}$. On dit que $\mathcal{G}$ est une m-famille génératrice partielle de G si*

$$\left|H^{(k)} \cdot b_k\right| = \left|G^{(k)} \cdot b_k\right|$$

pour tout $1 \leqslant k \leqslant m$.

D'après la proposition précédente, calculer une famille génératrice forte de G revient à calculer une $(n+1)$-famille génératrice partielle. On détermine une telle famille en commençant par construire une 1-famille génératrice partielle, que l'on complète ensuite récursivement jusqu'à obtention d'une $(n+1)$-famille génératrice partielle. L'Algorithme III.5 implante à la fois la construction d'une 1-famille génératrice partielle et la procédure permettant de passer du rang $m-1$ au rang m pour $m \geqslant 2$. L'idée est de détecter à l'aide de l'Algorithme III.4 les éléments $x \in S_m(\Lambda, \mathscr{B}, \Omega)$ tels que $(b_1, \ldots, b_{m-1}, x)$ soit prolongeable en un $K_{\mathbb{R}}$-automorphisme σ_x de Λ. Si c'est le cas, on ajoute σ_x à la famille $\mathcal{G}$ déjà calculée et on retire l'orbite de x sous $\mathcal{G}$ de la liste des candidats potentiels. Par ailleurs, garder en mémoire les « mauvais » candidats permet d'accélérer l'algorithme.

Données :
- Les données nécessaires au calcul d'un automorphisme de Λ.
- $\mathcal{G}$ une $(m-1)$-famille génératrice partielle de G (si $m > 1$).

Résultat :
- Une m-famille génératrice partielle de G contenant $\mathcal{G}$.

1 calculer C l'ensemble des $x \in S_m(\Lambda, \mathscr{B}, \Omega)$ tels que $(b_1, \ldots, b_{m-1}, x)$ soit un m-automorphisme partiel.
2 soit $C_0 := \emptyset$.
3 tant que $C \neq \emptyset$ faire
4 soit $x \in C$.
5 si $\exists f \in G^{(m)} : f(b_m) = x$, obtenu via l'Algorithme III.4 alors
6 Ajouter f à $\mathcal{G}$.
7 sinon
8 Ajouter x à C_0.
9 retirer $\langle \mathcal{G} \rangle \cdot x$ et $\langle \mathcal{G} \rangle \cdot C_0$ de C.
10 retourner $\mathcal{G}$.

Algorithme III.5 - Passage d'une $(m-1)$-famille génératrice à une m-famille génératrice.

III.4.2 Utilisation des stabilisateurs

S'il est possible de calculer une famille génératrice forte à l'aide de la méthode décrite dans le paragraphe précédent, il est en pratique judicieux de minimiser autant que possible le nombre d'appels à l'Algorithme III.4. C'est pour cela que le passage d'une $(m-1)$-famille génératrice partielle à une m-famille génératrice partielle est précédé par un calcul de stabilisateurs.

Soit $2 \leqslant m \leqslant n$. Supposons connues $\mathcal{G}$ une $(m-1)$-famille génératrice partielle, X une famille d'éléments de Λ et $\mathcal{H} := \{f_x : x \in X\}$ une famille d'éléments de $G^{(m)}$ indexée par X telle que pour tout $x \in X$, $f_x(x) = b_m$. Soient $x \in X$ et $g \in \mathcal{G} \cap G^{(m-1)}$. Si $g(x) \in X$, alors $h := f_{g(x)} \cdot g \cdot f_x^{-1}$ est un élément de $G^{(m)}$. Supposons sans perte de généralité que $h \neq \mathrm{id}$, et prenons $m \leqslant i \leqslant n$ maximal tel que $h \in G^{(i)}$. Notons $H^{(i)}$ le sous-groupe de $G^{(i)}$ engendré par $\mathcal{G} \cap G^{(i)}$ et $H_0^{(i)}$ le sous-groupe de $G^{(i)}$ engendré par $(\mathcal{G} \cup \{h\}) \cap G^{(i)}$. Puisque que l'on cherche à compléter $\mathcal{G}$ en une m-famille génératrice partielle, il est utile d'ajouter l'élément h à $\mathcal{G}$ si et seulement si l'orbite de b_i sous $H_0^{(i)}$ contient strictement plus de points que celle de b_i sous $H^{(i)}$. On évite ainsi d'ajouter des générateurs probablement superflus à la famille génératrice obtenue. Si $g(x) \notin X$, on l'ajoute à X et on ajoute $f_{g(x)} := f_x \cdot g$ à $\mathcal{H}$ et à $\mathcal{G}$.

L'heuristique montre que cette astuce, utilisée jusqu'à ce que $\mathcal{G} \cdot X \subset X$, permet obtenir des éléments de $G^{(m)}$ pour un coût moins élevé qu'en utilisant uniquement l'Algorithme III.4. Cette méthode est implantée par l'Algorithme III.6.

Données :
- Les données nécessaires au calcul d'un $K_{\mathbb{R}}$-automorphisme de Λ.
- $\mathcal{G}$ une $(m-1)$-famille génératrice partielle de G.

Résultat :
- $\mathcal{G}$ complétée avec des éléments de $G^{(m)}$.

soient $X := \{b_m\}$ et $\mathcal{H} = \{f_{b_m} := \mathrm{id}\}$.
tant que les points de X ne sont pas épuisés faire
  soit $x \in X$.
  pour $g \in \mathcal{G} \cap G^{(m-1)}$ faire
    soit $y := g(x)$.
    si $y \notin X$ alors
      ajouter y à X.
      ajouter $f_{g(x)} := f_x \cdot g$ à $\mathcal{H}$.
    sinon
      soient $h := f_{g(x)} \cdot g \cdot f_x^{-1}$ et i maximal tel que $h \in G^{(i)}$.
      si $i \leqslant n$ alors
        soient $H^{(i)} := \langle \mathcal{G} \rangle \cap G^{(i)}$ et $H_0^{(i)} := \langle \mathcal{G} \cup \{h\} \rangle \cap G^{(i)}$.
        si $\left|H^{(i)} \cdot b_i\right| < \left|H_0^{(i)} \cdot b_i\right|$ alors
          ajouter h à $\mathcal{G}$ et $f_y := h$ à $\mathcal{H}$.
retourner $\mathcal{G}$.

Algorithme III.6 - Calcul de stabilisateurs.

III.4.3 Calcul du groupe total

À partir de l'Algorithme III.5 et de l'Algorithme III.6, on construit l'Algorithme III.7 permettant de calculer une famille génératrice forte du groupe G. Remarquons que la m-ième valeur $\mathcal{E}_m$ de l'empreinte (définie dans la Section III.3.2.1) est une borne supérieure sur le cardinal de l'orbite de b_m sous $G^{(m)}$. En particulier, si l'orbite de b_m sous $\left\langle \mathcal{G} \cap G^{(m)} \right\rangle$ contient $\mathcal{E}_m$ éléments, alors $\left|\left\langle \mathcal{G} \cap G^{(m)} \right\rangle \cdot b_m\right| = \left|G^{(m)} \cdot b_m\right|$. Cette remarque permet d'éviter quelques appels aux deux algorithmes précédents.

III.5 $K_{\mathbb{R}}$-isométries, formes de Humbert et autres remarques

III.5.1 Isométries entre réseaux algébriques

Comme remarqué dans l'article original de Plesken et Souvignier [PS97, §9], il est possible de modifier l'Algorithme III.4 afin de décider si deux réseaux algébriques sont $K_{\mathbb{R}}$-isométriques. Soient Λ et Λ' deux réseaux algébriques de $K_{\mathbb{R}}^n$. Soit $\mathscr{B}$ une pseudo-base de Λ (resp. $\mathscr{B}'$ une pseudo-base de Λ') formée de $\mathcal{B}$ (resp. $\mathcal{B}'$) une $K_{\mathbb{R}}$-base de $K_{\mathbb{R}}^n$ et $\mathfrak{A}$ (resp. $\mathfrak{A}'$) une famille d'idéaux fractionnaires de K. En adaptant la preuve de la Proposition III.2.2, on montre que :

Données :
- Les données nécessaires au calcul d'un $K_{\mathbb{R}}$-automorphisme de Λ.

Résultat :
- Une famille génératrice forte $\mathcal{G}$ de G.

soit $\mathcal{G} := \{-\mathrm{id}\}$.
pour $m = 1$ à n faire
  si $\left|\left\langle \mathcal{G} \cap G^{(m)} \right\rangle \cdot b_m\right| < \mathcal{E}_m$ alors
    compléter $\mathcal{G}$ en une m-famille génératrice partielle à l'aide de Algorithme III.5.
  compléter $\mathcal{G}$ à l'aide de Algorithme III.6.
retourner $\mathcal{G}$.

Algorithme III.7 - Calcul du groupe $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$.

Proposition III.5.1 *Soit $(\omega_1, \ldots, \omega_d)$ une $\mathbb{Q}$-base de K. Un $K_{\mathbb{R}}$-endomorphisme de $f : K_{\mathbb{R}}^n \longrightarrow K_{\mathbb{R}}^n$ est une $K_{\mathbb{R}}$-isométrie de Λ vers Λ' si et seulement si :*

(i) $\langle f(\omega_k b_i) \,|\, f(\omega_l b_j)\rangle = \langle \omega_k b_i \,|\, \omega_l b_j\rangle$ *pour tous* $1 \leqslant i, j \leqslant n$ *et* $1 \leqslant k, l \leqslant d$.

(ii) $f(b_j) \in \bigoplus_{i=1}^n \mathfrak{a}'_i \mathfrak{a}_j^{-1} b'_i$ *pour tout* $1 \leqslant j \leqslant n$.

Les calculs d'empreinte et de combinaisons scalaires sont effectuées relativement à la pseudo-base $\mathscr{B}$ de Λ. Les images $f(b_j)$ pour $1 \leqslant j \leqslant n$ vérifiant la condition d'orthogonalité du premier point sont recherchées récursivement dans les ensembles

$$\left\{ x \in \bigoplus_{i=1}^n \mathfrak{a}'_i \mathfrak{a}_j^{-1} b'_i \;:\; \langle \omega_k x \,|\, \omega_l x\rangle = \langle \omega_k b_j \,|\, \omega_l b_j\rangle \;\; \forall\, 1 \leqslant k, l \leqslant d \right\}.$$

III.5.2 Équivalence de formes de Humbert

En utilisant la correspondance développée dans la Section II.5, décider si deux formes de Humbert sont équivalentes se ramène à décider si deux réseaux algébriques sont $K_{\mathbb{R}}$-isométriques. De même, le groupe d'automorphisme d'une forme de Humbert peut être déterminé en calculant le groupe des $K_{\mathbb{R}}$-automorphismes d'un réseau algébrique. Il est néanmoins très simple de modifier l'algorithme précédemment décrit de manière à ce qu'il prenne en charge les formes de Humbert. Nous détaillons ici ces modifications dans le cadre du calcul du groupe d'automorphisme d'une forme de Humbert.

Soient $A \in \mathrm{H}_n^{>0}(K_{\mathbb{R}})$ une forme de Humbert de rang n sur K et $\mathfrak{A} := (\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$ une famille d'idéaux fractionnaires de K. Rappelons que le groupe des $\mathfrak{A}$-automorphismes de A est

$$\mathrm{Aut}_{\mathfrak{A}}(A) = \{P \in \mathrm{GL}_n(\mathfrak{A}) \;:\; P^* A P = A\},$$

où $P \in \mathrm{GL}_n(\mathfrak{A})$ si et seulement si $\det(P) \in \mathcal{O}_K^\times$ et $P_{i,j} \in \mathfrak{a}_i \mathfrak{a}_j^{-1}$ pour tous $1 \leqslant i, j \leqslant n$. Nous avons montré dans la Proposition II.4.13 que la condition $\det(P) \in \mathcal{O}_K^\times$ est automatiquement vérifiée si P satisfait la relation $P^* A P = A$.

Dans cette situation, un m-automorphisme partiel de A est un m-uplet $(X_1, \ldots, X_m)$ tel que

$$X_i \in \mathfrak{a}_1\mathfrak{a}_i^{-1} \oplus \cdots \oplus \mathfrak{a}_n\mathfrak{a}_i^{-1}$$

et

$$X_i^* A X_j = A_{i,j}$$

pour tous $1 \leqslant i, j \leqslant m$. Déterminer un $\mathfrak{A}$-automorphisme de la forme A revient à en déterminer un n-automorphisme partiel. Les modifications à apporter aux différents objets et invariants introduits sont alors évidentes. Par exemple, les ensembles $S_j(\Lambda, \mathscr{B}, \Omega)$ sont remplacés par les ensembles

$$S_j(A, \mathfrak{A}) := \left\{ X \in \mathfrak{a}_1\mathfrak{a}_j^{-1} \oplus \cdots \oplus \mathfrak{a}_n\mathfrak{a}_j^{-1} \ : \ X^* A X = A_{j,j} \right\}.$$

Notons que seule la phase de calcul d'un automorphisme est modifiée ; le passage de cette étape au calcul du groupe total est utilisable pour les formes de Humbert telle qu'elle est présentée pour les réseaux algébriques.

III.5.3 Calcul des stabilisateurs

Heuristiquement, il est possible d'améliorer l'utilisation des stabilisateurs expliquée dans la Section III.4.2. En effet, itérer l'Algorithme III.6 jusqu'à ce que $\mathcal{G} \cdot X \subset X$ est généralement coûteux, mais en contrepartie, chaque générateur obtenu de cette manière évite des appels onéreux à l'Algorithme III.4. C'est pourquoi une condition d'arrêt heuristique est ajoutée à la condition $\mathcal{G} \cdot X \subset X$: après un certain nombre [2] de stabilisateurs « inutiles » calculés, des stabilisateurs supplémentaires sont déterminés et ajoutés à la famille génératrice (même s'ils semblent superflus), et l'algorithme est finalement arrêté. En contrepartie d'une augmentation de la taille de la famille génératrice obtenue, cet ajout de stabilisateurs permet en pratique d'accélérer le calcul du groupe total. Bien que non mentionnée dans l'article de Plesken et Souvignier, cette heuristique est déjà présente dans l'implantation originale de Souvignier. Nous renvoyons au code de la fonction `qfauto` [3] de la librairie `PARI/gp` [PARI/gp] pour plus de détails.

III.5.4 Certification des résultats

En utilisant l'Algorithme III.7, on obtient un groupe G décrit par une famille génératrice (forte) $\mathcal{G}$. Si s'assurer que ce groupe G est inclus dans $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$ est facile en utilisant la Proposition III.2.2, il est plus délicat de vérifier que $G = \mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$. Nous proposons dans ce paragraphe une méthode probabiliste permettant d'effectuer ce contrôle, sous l'hypothèse que les ensembles $S_j(\Lambda, \mathscr{B}, \Omega)$ sont correctement calculés.

Supposons que $G \neq \mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$. Puisque G est un sous-groupe strict de $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$, on a $|G| \leqslant \left|\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)\right|/2$. Dès lors, si un élément f est tiré de uniformément dans $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$, la

2. Cette valeur est déterminée expérimentalement.
3. Cette implantation est une adaptation directe du code original de Souvignier.

probabilité que f soit un élément de G est inférieure à 0.5. Finalement, en effectuant n tirages aléatoires indépendants uniformes dans $\mathrm{Aut}_{K_\mathbb{R}}(\Lambda)$, la probabilité de ne pas détecter que $G \neq \mathrm{Aut}_{K_\mathbb{R}}(\Lambda)$ est inférieure à 2^{-n}.

Des algorithmes sont connus pour tester l'appartenance d'un élément à un sous-groupe donné par une famille génératrice (voir [But91, algo.3, p.90]), et on peut obtenir une méthode de tirage aléatoire uniforme dans $\mathrm{Aut}_{K_\mathbb{R}}(\Lambda)$ en effectuant un tel tirage au moment de choisir un 1-automorphisme partiel initial et au moment de choisir le prolongement d'un n-automorphisme partiel en un $(n+1)$-automorphisme partiel dans l'Algorithme III.4.

III.6 Application à la G-équivalence de formes quadratiques

Nous détaillons dans cette section les modifications à apporter à l'algorithme de Plesken et Souvignier classique permettant de décider l'équivalence de formes quadratiques modulo d'autres groupes que $\mathrm{GL}_n(\mathbb{Z})$, notamment modulo certains groupes de congruence. Dans en second temps, nous présentons la généralisation aux formes de Humbert de ces aspects.

III.6.1 G-équivalence de formes quadratiques

Rappelons que deux formes quadratiques (définies positives) $A, B \in \mathrm{S}_n^{>0}(\mathbb{R})$ sont dites *équivalentes* s'il existe une matrice $P \in \mathrm{GL}_n(\mathbb{Z})$ telle que $P^\intercal AP = B$. Nous considérons dans cette section une version différente de cette notion d'équivalence, dans laquelle on demande à la matrice P de vérifier d'autres propriétés :

Définition III.6.1 *Soit G un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$. Deux formes quadratiques $A, B \in \mathrm{S}_n^{>0}(\mathbb{R})$ sont dites G-équivalentes s'il existe une matrice $P \in G$ telle que $P^\intercal AP = B$. Une G-équivalence de A sur elle-même est appelé un G-automorphisme de A.*

En particulier, la $\mathrm{GL}_n(\mathbb{Z})$-équivalence de formes quadratiques correspond à l'équivalence usuelle. De même, on peut voir l'équivalence de formes de Humbert définie dans la Section II.4.4 comme une $\mathrm{GL}_n(\mathcal{O}_K)$-équivalence des formes quadratiques sous-jacentes. Cette notion de G-équivalence n'est pas neuve ; Martinet propose par exemple dans [Mar03, §11, p.383–426] une étude des propriétés d'extrémalité des formes G-invariantes.

Définition III.6.2 *Soit G un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$. Une forme quadratique $A \in \mathrm{S}_n^{>0}(\mathbb{R})$ est dite G-invariante si $G \leqslant \mathrm{Aut}(A)$.*

Si G n'est ni fini, ni inclus dans $\mathrm{GL}_n(\mathbb{Z})$, il ne peut évidemment pas exister de forme quadratique G-invariante. Il s'avère que la réciproque est vraie :

Proposition III.6.3 *Soit G un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$. Il existe une forme quadratique G-invariante si et seulement si G est un sous-groupe fini de $\mathrm{GL}_n(\mathbb{Z})$.*

Démonstration. D'après [Mar03, thm.11.1.1, p.384-385], il existe $A \in \mathrm{S}_n^{>0}(\mathbb{R})$ une forme quadratique G-invariante si et seulement si G est fini et si sa représentation induite par l'inclusion

$G \subset \mathrm{GL}_n(\mathbb{R})$ est rationnelle sur $\mathbb{Q}$. Puisque $G \leqslant \mathrm{GL}_n(\mathbb{Z})$, la seconde condition est toujours vérifiée. Comme G est fini par hypothèse, le résultat est démontré. □

L'objectif du reste de cette partie est de montrer qu'il est possible d'utiliser l'algorithme de Plesken et Souvignier pour décider la G-équivalence de formes quadratiques pour une large famille de groupe G.

III.6.2 Groupes admissibles

III.6.2.1 Cas général

Nous ne savons pas l'heure actuelle traiter effectivement la G-équivalence de formes quadratiques sans conditions sur le groupe G. Puisque nous souhaitons utiliser l'algorithme de Plesken et Souvignier, il nous faut considérer une notion d'équivalence qui soit *plus forte* que l'équivalence classique. C'est pourquoi la première restriction que nous imposons est que G soit un groupe de $\mathrm{GL}_n(\mathbb{Z})$: dans ce cas, deux formes quadratiques G-équivalentes sont en particulier équivalentes au sens classique.

Définition III.6.4 *Un sous-groupe G de $\mathrm{GL}_n(\mathbb{Z})$ est dit admissible s'il existe des fonctions*

$$f_i : \mathbb{Z}^n \longrightarrow \{0, 1\}$$

calculables en temps polynomial et telles que pour toute matrice $P \in \mathrm{GL}_n(\mathbb{Z})$ dont les colonnes sont notées $p_1, \ldots, p_n$, on a

$$P \in G \iff f_i(p_i) = 1 \ \forall\, 1 \leqslant i \leqslant n.$$

Un sous-groupe de $\mathrm{SL}_n(\mathbb{Z})$ est dit admissible s'il est de la forme $G \cap \mathrm{SL}_n(\mathbb{Z})$, où G est un sous-groupe admissible de $\mathrm{GL}_n(\mathbb{Z})$.

Moins formellement, un groupe est admissible s'il est défini par un ensemble de conditions sur les *colonnes*, *deux-à-deux indépendantes* et *faciles à vérifier*.

Exemple III.6.5 Donnons quelques exemples simples de groupes admissibles :

- $\mathrm{GL}_n(\mathbb{Z})$ et $\mathrm{SL}_n(\mathbb{Z})$ sont admissibles : il suffit de prendre pour chaque f_i la fonction constante égale à 1.
- Le sous-groupe de $\mathrm{GL}_n(\mathbb{Z})$ formé des matrices diagonales est admissible. En effet, pour tout $1 \leqslant i \leqslant n$, il suffit prendre

$$f_i(p_i) = \begin{cases} 1 & \text{si } p_{i,j} = 0 \text{ pour tout } j \neq i, \\ 0 & \text{sinon.} \end{cases}$$

  De manière similaire, les matrices triangulaires (inférieures ou supérieures) de $\mathrm{GL}_n(\mathbb{Z})$ forment elles-aussi un sous-groupe admissible.

- Le sous-groupe de $\mathrm{GL}_n(\mathbb{Z}) \cap S_n(\mathbb{R})$ n'est pas admissible. En effet, la symétrie d'une matrice ne peut pas s'exprimer par un système convenable de conditions sur les colonnes : la condition de symétrie exprimée sur une colonne dépend des autres colonnes.

Il s'avère que les sous-groupes de congruence fournissent une grande quantité d'exemples de groupes admissibles.

III.6.2.2 Sous-groupes de congruence

Définition III.6.6 *Le sous-groupe de congruence principal de niveau $d \in \mathbb{N}_{>0}$ de $\mathrm{SL}_n(\mathbb{Z})$ est*

$$\Gamma(d) := \mathrm{Ker}\left(\pi_d : \mathrm{SL}_n(\mathbb{Z}) \longrightarrow \mathrm{SL}_n(\mathbb{Z}/d\mathbb{Z})\right),$$

où π_d est induit par l'application $\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ de réduction modulo d.

Les éléments de $\Gamma(d)$ sont donc les matrices $A \in \mathrm{SL}_n(\mathbb{Z})$ dont les éléments diagonaux sont congrus à 1 modulo d et les éléments non diagonaux sont congrus à 0 modulo d. En particulier, $\Gamma(d)$ est un groupe admissible : il est déterminé par les fonctions

$$f_i(p_i) = \begin{cases} 1 & \text{si } p_{i,j} \equiv \delta_{i,j} \mod d \text{ pour tout } 1 \leqslant j \leqslant n, \\ 0 & \text{sinon,} \end{cases}$$

où $\delta_{i,j}$ désigne le symbole de Kronecker en (i, j).

Définition III.6.7 *Un sous-groupe de congruence de $\mathrm{SL}_n(\mathbb{Z})$ est un sous-groupe $\Gamma \leqslant \mathrm{SL}_n(\mathbb{Z})$ pour lequel il existe un entier $d \in \mathbb{N}_{>0}$ tel que $\Gamma(d) \leqslant \Gamma \leqslant \mathrm{SL}_n(\mathbb{Z})$. Le plus petit commun multiple des entiers d tels que $\Gamma(d) \leqslant \Gamma$ est appelé le niveau de Γ.*

Bien évidemment, le sous-groupe de congruence principal $\Gamma(d)$ est un sous-groupe de congruence de niveau d de $\mathrm{SL}_n(\mathbb{Z})$ au sens de cette définition. La propriété fondamentale de ces groupes est d'être d'indice fini dans $\mathrm{SL}_n(\mathbb{Z})$:

Proposition III.6.8 *Un sous-groupe Γ de $\mathrm{SL}_n(\mathbb{Z})$ est de congruence si et seulement s'il existe $d \in \mathbb{N}_{>0}$ et un sous-groupe G de $\mathrm{SL}_n(\mathbb{Z}/d\mathbb{Z})$ tels que $\Gamma = \pi_d^{-1}(G)$. En particulier, les sous-groupes de congruence de $\mathrm{SL}_n(\mathbb{Z})$ sont d'indice fini.*

Démonstration. Si $\Gamma = \pi_d^{-1}(G)$, on a $\Gamma(d) = \pi_d^{-1}(1) \leqslant \pi_d^{-1}(G) = \Gamma$, donc Γ est bien un sous-groupe de congruence. Réciproquement, si Γ est de congruence, il existe $d \in \mathbb{N}_{>0}$ tel que $\Gamma(d) \leqslant \Gamma$. Puisque $\Gamma(d) = \mathrm{Ker}(\pi_d)$, $\pi_d(\Gamma)$ est un sous-groupe de $\mathrm{SL}_n(\mathbb{Z}/d\mathbb{Z})$ dont l'image réciproque par π_d est exactement Γ.

Si $\Gamma := \pi_d^{-1}(G)$ est un sous-groupe de congruence, on a $\mathrm{SL}_n(\mathbb{Z})/\Gamma \cong \mathrm{SL}_n(\mathbb{Z}/d\mathbb{Z})/G$, ce qui montre Γ est d'indice fini dans $\mathrm{SL}_n(\mathbb{Z})$. □

La question inverse est plus délicate à traiter. Citons tout de même le célèbre résultat de Bass, Lazard et Serre :

Théorème III.6.9 ([BLS64]) *Si $n \geqslant 3$, un sous-groupe de $\mathrm{SL}_n(\mathbb{Z})$ est d'indice fini si et seulement si c'est un sous-groupe de congruence.*

Notons que ce résultat est faux pour $n = 2$: il existe des sous-groupes de $\mathrm{SL}_2(\mathbb{Z})$ d'indice fini qui ne sont pas de congruence. En général, les sous-groupes de congruence ne sont pas admissibles ; on montre que $\Gamma := \pi_d^{-1}(G)$ est un sous-groupe admissible si et seulement si G l'est comme sous-groupe de $\mathrm{GL}_n(\mathbb{Z}/d\mathbb{Z})$. Quoi qu'il en soit, les deux familles de sous-goupes de congruence suivantes (en plus des sous-groupes de congruence principaux) fournissent un large panel d'exemples de groupes admissibles :

Définition III.6.10 *Soit $d \in \mathbb{N}_{>0}$.*

- *On désigne par $\Gamma_0(d)$ le sous-groupe de $\mathrm{SL}_n(\mathbb{Z})$ formé des matrices dont les éléments du triangle inférieur sont congrus à 0 modulo d. Ce groupe est appelé le sous-groupe de congruence de Hecke de niveau d.*
- *On désigne par $\Gamma_1(d)$ le sous-groupe de $\Gamma_0(d)$ formé des matrices dont les éléments diagonaux sont congrus à 1 modulo d.*

Puisqu'ils contiennent $\Gamma(d)$, les groupes $\Gamma_0(d)$ et $\Gamma_1(d)$ sont des sous-groupes de congruence de niveau d de $\mathrm{SL}_n(\mathbb{Z})$. De plus, il est clair que ces groupes sont admissibles.

III.6.3 Détermination effective de G-équivalences

Nous montrons dans cette section comment décider effectivement la G-équivalence de deux formes quadratiques pour un groupe G admissible. Puisque nous nous autorisons à considérer comme groupes admissibles des sous-groupes de $\mathrm{SL}_n(\mathbb{Z})$, nous expliquons dans un premier temps comment décider la $\mathrm{SL}_n(\mathbb{Z})$-équivalence de deux formes quadratiques.

III.6.3.1 Passage de $\mathrm{GL}_n(\mathbb{Z})$ à $\mathrm{SL}_n(\mathbb{Z})$

Nous expliquons dans ce paragraphe comment décider l'équivalence modulo $\mathrm{SL}_n(\mathbb{Z})$ de deux formes quadratiques à partir d'un algorithme permettant de décider de leur équivalence modulo $\mathrm{GL}_n(\mathbb{Z})$. Nous détaillons également cette construction dans le cadre du calcul des automorphismes d'une forme quadratique. Bien que ces méthodes ne soient pas nouvelles et semblent faire partie du folklore, elles n'ont à notre connaissance jamais été rédigées en détails dans une publication. Elles ont notamment été implantées dans le logiciel [PFPK] qui a permis d'effectuer les calculs modulo $\mathrm{SL}_n(\mathbb{Z})$ dans [EVGS02 ; EVGS13]. Ce passage de $\mathrm{GL}_n(\mathbb{Z})$ à $\mathrm{SL}_n(\mathbb{Z})$ repose essentiellement sur la proposition suivante. Dans la suite, si X et Y sont des sous-ensembles d'un même ensemble, on notera $X \setminus Y$ l'ensemble $X \setminus (X \cap Y)$.

Proposition III.6.11 *Soient $A, B \in \mathrm{S}_n^{>0}(\mathbb{R})$ deux formes quadratiques équivalentes modulo $\mathrm{GL}_n(\mathbb{Z})\backslash\mathrm{SL}_n(\mathbb{Z})$. Alors A et B sont équivalentes modulo $\mathrm{SL}_n(\mathbb{Z})$ si et seulement si $\mathrm{Aut}(A)\backslash\mathrm{SL}_n(\mathbb{Z}) \neq \emptyset$.*

Démonstration. Par hypothèse, il existe $P \in \mathrm{GL}_n(\mathbb{Z}) \setminus \mathrm{SL}_n(\mathbb{Z})$ tel que $P^\intercal AP = B$. S'il existe $Q \in \mathrm{Aut}(A)\backslash\mathrm{SL}_n(\mathbb{Z})$, la matrice QP est un élément de $\mathrm{SL}_n(\mathbb{Z})$ satisfaisant la relation $(QP)^\intercal A(QP) = B$.

Les formes A et B sont donc bien équivalentes modulo $\mathrm{SL}_n(\mathbb{Z})$. Réciproquement, s'il existe $Q \in \mathrm{SL}_n(\mathbb{Z})$ telle que $Q^\intercal AQ = B$, on vérifie que la matrice PQ^{-1} est un élément de $\mathrm{Aut}(A)\backslash\mathrm{SL}_n(\mathbb{Z})$. □

Le test de l'équivalence modulo $\mathrm{SL}_n(\mathbb{Z})$ de deux formes quadratiques découlant de cette proposition est implanté par l'Algorithme III.8. Nous supposons pour cela données les procédures :

- `equiv`, qui vérifie l'équivalence modulo $\mathrm{GL}_n(\mathbb{Z})$ de deux formes quadratiques (et renvoie une telle équivalence le cas échéant),
- `autom`, qui renvoie une famille génératrice du groupe des $\mathrm{GL}_n(\mathbb{Z})$-automorphismes d'une forme quadratique.

Notons qu'il est possible de tester la condition $\mathrm{Aut}(A) \setminus \mathrm{SL}_n(\mathbb{Z}) \neq \emptyset$ à partir d'une famille génératrice de $\mathrm{Aut}(A)$ et sans énumérer tous les éléments du groupe. En effet, si $\mathrm{Aut}(A) \setminus \mathrm{SL}_n(\mathbb{Z}) \neq \emptyset$, toute famille génératrice de $\mathrm{Aut}(A)$ doit contenir un élément de $\mathrm{Aut}(A) \setminus \mathrm{SL}_n(\mathbb{Z})$ (puisque $\mathrm{Aut}(A) \cap \mathrm{SL}_n(\mathbb{Z})$ est un sous-groupe de $\mathrm{Aut}(A)$).

Étant donné $A \in \mathrm{S}_n^{>0}(\mathbb{R})$, le passage de $\mathrm{Aut}(A)$ à $\mathrm{Aut}(A) \cap \mathrm{SL}_n(\mathbb{Z})$ est légèrement plus subtile. Supposons donnés $P_1, \ldots, P_\alpha \in \mathrm{SL}_n(\mathbb{Z})$ et $Q_1, \ldots, Q_\beta \in \mathrm{GL}_n(\mathbb{Z}) \setminus \mathrm{SL}_n(\mathbb{Z})$ les générateurs de $\mathrm{Aut}(A)$. Si $\beta = 0$, on a $\mathrm{Aut}(A) = \mathrm{Aut}(A) \cap \mathrm{SL}_n(\mathbb{Z})$ et il n'y a rien à calculer. Supposons donc que $\beta \geqslant 1$. Pour tous $1 \leqslant i \leqslant j \leqslant \beta$, soit $Q_{i,j} := Q_i Q_j$.

Proposition III.6.12 *Les P_k et les $Q_{i,j}$ pour $1 \leqslant k \leqslant \alpha$ et $1 \leqslant i \leqslant j \leqslant \beta$ forment une famille génératrice de* $\mathrm{Aut}(A) \cap \mathrm{SL}_n(\mathbb{Z})$.

Démonstration. Soit G le sous-groupe de $\mathrm{Aut}(A)$ engendré par les P_k et les $Q_{i,j}$. Par construction, G est un sous-groupe de $\mathrm{Aut}(A) \cap \mathrm{SL}_n(\mathbb{Z})$. On montre ensuite que

$$[\mathrm{Aut}(A) : \mathrm{Aut}(A) \cap \mathrm{SL}_n(\mathbb{Z})] = [\mathrm{Aut}(A) : G] = 2,$$

ce qui entraîne que $G = \mathrm{Aut}(A) \cap \mathrm{SL}_n(\mathbb{Z})$. □

En général, il y a beaucoup de générateurs redondants parmi ceux obtenus à l'aide de cette méthode. Obtenir une famille génératrice comportant moins d'éléments est parfois souhaitable. Il suffit pour cela de ne garder en mémoire que les $Q_{i,j}$ qui contribuent à élargir le groupe engendré. L'Algorithme III.9 utilise pour cela la procédure [But91, algo.3, p.90] qui permet de tester l'appartenance d'un élément à un groupe donné par une famille génératrice. Notons que l'algorithme présenté permet plus généralement de déterminer une famille génératrice de $G \cap \mathrm{SL}_n(\mathbb{Z})$ à partir d'une famille génératrice d'un sous-groupe fini quelconque G de $\mathrm{GL}_n(\mathbb{Z})$.

III.6.3.2 G-équivalence avec G admissible

Soit $G \leqslant \mathrm{GL}_n(\mathbb{Z})$ un groupe admissible. La stratégie présentée dans le chapitre précédent permet de traiter la $G \cap \mathrm{SL}_n(\mathbb{Z})$-équivalence si on dispose d'un algorithme permettant de traiter

Données :
- $A, B \in \mathrm{S}_n^{>0}(\mathbb{R})$.

Résultat :
- Une matrice $P \in \mathrm{SL}_n(\mathbb{Z})$ telle que $P^\intercal AP = B$ ou faux.

```
P ← equiv(A, B).
si P=faux ou det(P) = 1 alors
    retourner P.
sinon
    {Q_1, ..., Q_m} ← autom(A).
    pour 1 ⩽ i ⩽ m faire
        si det(Q_i) = −1 alors
            retourner Q_i P.
    retourner faux.
```

Algorithme III.8 - Équivalence de formes quadratiques modulo $\mathrm{SL}_n(\mathbb{Z})$.

Données :
- $P_1, \dots, P_\alpha \in \mathrm{SL}_n(\mathbb{Z})$ et $Q_1, \dots, Q_\beta \in \mathrm{GL}_n(\mathbb{Z}) \setminus \mathrm{SL}_n(\mathbb{Z})$ les générateurs de $\mathrm{Aut}(A)$, où $A \in \mathrm{S}_n^{>0}(\mathbb{R})$.

Résultat :
- Une famille génératrice de $\mathrm{Aut}(A) \cap \mathrm{SL}_n(\mathbb{Z})$.

```
F ← {P_1, ..., P_α}.
pour 1 ⩽ i ⩽ j ⩽ β faire
    si Q_i Q_j ∉ ⟨F⟩ alors
        ajouter Q_i Q_j à F.
retourner F.
```

Algorithme III.9 - Calcul de $\mathrm{Aut}(A) \cap \mathrm{SL}_n(\mathbb{Z})$.

la G-équivalence. Nous proposons ici un tel algorithme en modifiant celui de Plesken et Souvignier. Comme nous l'avons fait plus tôt dans ce chapitre, nous présentons ces modifications dans le cadre du calcul du groupe des G-automorphismes d'une forme quadratique ; les modifications à apporter pour la détermination d'une G-équivalence entre deux formes quadratiques s'en déduisent facilement.

Soit $A \in \mathrm{S}_n^{>0}(\mathbb{R})$ une forme quadratique. À partir des ensembles

$$S_i(A) := \{x \in \mathbb{Z}^n \,:\, x^\intercal A x = A_{i,i}\},$$

la méthode de Plesken et Souvignier consiste à déterminer récursivement $x_1, \dots, x_n$ formant les colonnes d'une matrice P tels que $x_i \in S_i(A)$ pour tout $1 \leqslant i \leqslant n$ et $P^\intercal AP = A$. En modifiant

les ensembles $S_i(A)$, on modifie les ensembles dans lesquels les colonnes des automorphismes de A sont tirées, et on s'assure ainsi que l'automorphisme calculé vérifie certaines propriétés.

Supposons que le groupe G est défini par des conditions sur les colonnes données par des fonctions $f_1, \ldots, f_n$. À la place des ensembles $S_i(A)$, on considère

$$T_i(A) := \{x \in S_i(A) \,:\, f_i(x) = 1\}.$$

En éxécutant l'algorithme de Plesken et Souvignier avec ces ensembles $T_i(A)$ au lieu des $S_i(A)$, on obtient $x_1, \ldots, x_n$ tels que $x_i \in T_i(A)$ pour tout $1 \leqslant i \leqslant n$ formant les colonnes d'une matrice P telle que $P^\intercal AP = A$. En particulier, on a $f_i(x_i) = 1$ pour tout $1 \leqslant i \leqslant n$, ce qui entraîne par définition de l'admissibilité que P est un élément du groupe G.

Remarque III.6.13 Si on relâche le critère d'admissibilité sur G en autorisant le fait que la condition sur une colonne puisse dépendre non seulement de cette colonne mais aussi des colonnes précédentes, il est encore possible de modifier l'algorithme de Plesken et Souvignier pour traiter la G-équivalence. Il suffit en effet d'ajouter une vérification des conditions à satisfaire à chaque prolongement d'un automorphisme partiel dans la phase de *backtracking*.

Remarque III.6.14 En fonction du groupe G considéré, il est possible d'ajouter plusieurs tests antérieurs à l'exécution de l'algorithme de Plesken et Souvignier. Par exemple, si $G = \Gamma(d)$, pour que deux formes quadratiques A, B soient G-équivalentes, il est nécessaire (mais non suffisant) que $A \equiv B \mod d$.

Exemple III.6.15 Considérons deux formes quadratiques $A, B \in \mathrm{S}_3^{>0}(\mathbb{R})$ données par

$$A := \begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 2 \end{pmatrix} \quad \text{et} \quad B := \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}.$$

Ces deux formes sont $\mathrm{GL}_3(\mathbb{Z})$-équivalentes puisque $P^\intercal BP = A$, où

$$P := \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & -1 \\ 1 & -1 & 0 \end{pmatrix} \in \mathrm{GL}_3(\mathbb{Z}).$$

A et B sont aussi $\mathrm{SL}_n(\mathbb{Z})$-équivalentes. En effet, $P \in \mathrm{GL}_3(\mathbb{Z}) \setminus \mathrm{SL}_3(\mathbb{Z})$ et $\mathrm{Aut}(A)$ est engendré par

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ -1 & 0 & 1 \\ 0 & -1 & 1 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & -1 \end{pmatrix} \in \mathrm{GL}_3(\mathbb{Z}) \setminus \mathrm{SL}_3(\mathbb{Z}).$$

Cependant, il n'existe pas $d \in \mathbb{N}_{>0}$ tel que A et B soient $\Gamma(d)$-équivalentes. En effet, si c'était le cas, on aurait $A \equiv B \mod d$, ce qui est impossible (il suffit de prêter attention au coefficient supérieur droit de A et B).

Exemple III.6.16 Considérons maintenant $A, B \in \mathrm{S}_3^{>0}(\mathbb{R})$ données par

$$A := \begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 2 \end{pmatrix} \quad \text{et} \quad B := \begin{pmatrix} 2 & 3 & 2 \\ 3 & 6 & 11 \\ 2 & 11 & 46 \end{pmatrix}.$$

Ces deux formes sont $\mathrm{GL}_3(\mathbb{Z})$-équivalentes puisque $P^{\intercal}BP = A$, où

$$P := \begin{pmatrix} 1 & 1 & 6 \\ -1 & 0 & -5 \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{GL}_3(\mathbb{Z}).$$

Il s'avère que A et B sont aussi $\Gamma(2)$-équivalentes puisque $Q^{\intercal}AQ = B$, où

$$Q := \begin{pmatrix} 1 & 2 & 4 \\ 0 & 1 & 6 \\ 0 & 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mod 2$$

Notons que A et B sont aussi $\Gamma_1(d)$-équivalentes pour tout $d \in \mathbb{N}_{>0}$ puisque Q est triangulaire inférieure et de coefficients diagonaux égaux à 1.

III.6.4 Extension aux formes de Humbert

Du point de vue théorique, la plupart des notions et résultats présentés s'étendent aux formes de Humbert. La notion de G-équivalence se généralise : si G est un sous-groupe de $\mathrm{GL}_n(K_{\mathbb{R}})$, deux formes de Humbert $A, B \in \mathrm{H}_n^{>0}(K_{\mathbb{R}})$ sont dites G-équivalentes s'il existe $P \in G$ tel que $P^*AP = B$. Cependant, l'existence d'une forme G-invariante si G est un sous-groupe fini de $\mathrm{GL}_n(\mathcal{O}_K)$ n'est pas clair, sauf si $\mathcal{O}_K$ est un anneau principal.

La notion d'admissibilité pour un sous-groupe de $\mathrm{GL}_n(\mathcal{O}_K)$ ou $\mathrm{SL}_n(\mathcal{O}_K)$ est inchangée, et des exemples de tels groupes sont une fois de plus donnés par les sous-groupes de congruence de $\mathrm{SL}_n(\mathcal{O}_K)$: un sous-groupe Γ de $\mathrm{SL}_n(\mathcal{O}_K)$ est appelé un sous-groupe de congruence s'il existe un idéal $\mathfrak{a}$ de $\mathcal{O}_K$ tel que

$$\Gamma(\mathfrak{a}) := \mathrm{Ker}\left(\mathrm{SL}_n(\mathcal{O}_K) \longrightarrow \mathrm{SL}_n(\mathcal{O}_K/\mathfrak{a})\right) \leqslant \Gamma.$$

Puisque pour tout idéal $\mathfrak{a}$ de $\mathcal{O}_K$ l'anneau $\mathcal{O}_K/\mathfrak{a}$ est fini, les sous-groupes de congruence de $\mathrm{SL}_n(\mathcal{O}_K)$ sont d'indice fini. Cependant, contrairement au cas de $\mathrm{SL}_n(\mathbb{Z})$, la réciproque de cette assertion est en général fausse (voir [BMS67]) : il existe généralement des sous-groupes de $\mathrm{SL}_n(\mathcal{O}_K)$ qui sont d'indice fini sans être de congruence.

L'extension des aspects algorithmiques présentés aux formes de Humbert est moins évidente. Si la méthode présentée pour décider la G-équivalence de formes de Humbert pour un sous-groupe G de $\mathrm{GL}_n(\mathcal{O}_K)$ reste valide, le passage *efficace* de $\mathrm{GL}_n(\mathcal{O}_K)$ à $\mathrm{SL}_n(\mathcal{O}_K)$ nous est à l'heure actuelle inaccessible. Si $A, B \in \mathrm{H}_n^{>0}(K_{\mathbb{R}})$ sont $\mathrm{GL}_n(\mathcal{O}_K)$-équivalentes par une matrice $P \in \mathrm{GL}_n(\mathcal{O}_K)$, alors A et B sont $\mathrm{SL}_n(\mathcal{O}_K)$-équivalentes si et seulement s'il existe $Q \in \mathrm{GL}_n(\mathcal{O}_K)$

telle que $Q^*AQ = A$ et $\det(Q) = \det(P)^{-1}$. Cependant, nous ne savons pas déterminer un tel élément Q sans passer par l'énumération complète de $\mathrm{Aut}_{\mathcal{O}_K}(A)$... Le même type de difficulté se présente d'ailleurs lors de la détermination de $\mathrm{Aut}_{\mathcal{O}_K}(A) \cap \mathrm{SL}_n(\mathcal{O}_K)$: comment associer à un générateur de $\mathrm{Aut}_{\mathcal{O}_K}(A)$ un potentiel générateur de $\mathrm{Aut}_{\mathcal{O}_K}(A) \cap \mathrm{SL}_n(\mathcal{O}_K)$?

IV

COMPLEXITÉ DU PROBLÈME DE L'ISOMÉTRIE DE RÉSEAUX

Sommaire

IV.1 Introduction

Les réseaux, qu'ils soient euclidiens ou algébriques, sont des sources fécondes de problèmes algorithmiques difficiles. Parmi ces questions, deux des moins bien connues sont les suivantes :

- le problème de l'isométrie : il s'agit de déterminer s'il existe une isométrie entre deux réseaux.
- le problème de la détermination du groupe des automorphismes d'un réseau.

À l'heure actuelle, peu de résultats de complexité ont été établis sur ces deux questions. Nous démontrons dans ce chapitre que, une fois connu des ensembles particuliers de vecteurs courts des réseaux considérés, les problèmes de l'isométrie et de la détermination des automorphismes sont réductibles en temps polynomial à des problèmes analogues sur les graphes. Ces problèmes sur les graphes étant bien mieux connus, cette réduction nous permet d'établir des résultats de complexité inédits. Elle est de plus généralisable au cas des réseaux algébriques. Cette transformation d'un réseau en un graphe n'est pas seulement d'un intérêt théorique : elle fournit un algorithme qui, une fois implanté, s'avère être parfois plus rapide que l'algorithme de Plesken et Souvignier [PS97], couramment utilisé (voir la Section V.5).

IV.2 Graphes, réseaux et problèmes algorithmiques

IV.2.1 Graphes et isomorphismes

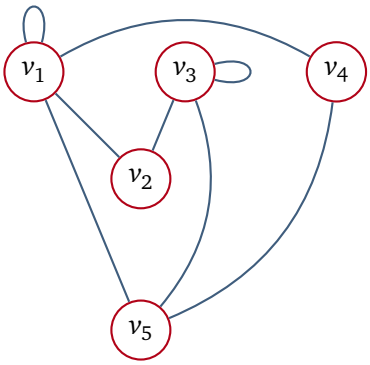
Le but de ce paragraphe est d'introduire la notion d'isomorphisme de graphes et les problèmes algorithmiques qui y sont reliés.

Définition IV.2.1 *Un graphe G est une paire (V, E) telle que :*

- *V est un ensemble fini, dont les éléments sont appelés les sommets de G.*
- *E est un sous-ensemble de $V \times V$ tel que pour tout couple $(v, w) \in E$, on a $(w, v) \in E$. Les éléments de E sont appelés les arrêtes de G.*

Les graphes que nous considérons sont donc *finis* et *non orientés*. De plus, ils peuvent contenir des boucles (c'est-à-dire des arrêtes de la forme (v, v) avec $v \in V$) mais pas d'arrêtes multiples (c'est-à-dire qu'il ne peut pas y avoir plusieurs arrêtes entre la même paire de sommets). Deux sommets d'un graphe sont dits *adjacents* ou *voisins* s'ils sont reliés par une arrête. Si G est un graphe dont les sommets sont $v_1, \ldots, v_N$, sa *matrice d'incidence* est la matrice symétrique de taille N dont le coefficient (i, j) vaut 1 si v_i et v_j sont adjacents et 0 sinon. La matrice d'incidence est un moyen pratique de représenter et manipuler les graphes. Un graphe $G := (V, E)$ est dit *complet* si $E = V \times V$, ce qui revient à dire que les sommets de G sont tous deux à deux adjacents.

La notion de densité d'un graphe est similaire à la notion de densité d'une matrice utilisée en algèbre linéaire :



$$\begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} \begin{array}{c} \begin{array}{ccccc} v_1 & v_2 & v_3 & v_4 & v_5 \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{pmatrix} \end{array}$$

Fig. IV.1 – Exemple de matrice d'incidence associée à un graphe.

Définition IV.2.2 *La densité d'un graphe $G := (V, E)$ est la grandeur $\rho(G) \in [0, 1]$ définie par*

$$\rho(G) := \frac{2|E|}{|V|(|V|+1)}.$$

Notons que pour un graphe sans boucle [1], la densité est plutôt définie comme la grandeur

$$\frac{2|E|}{|V|(|V|-1)}.$$

La densité de G quantifie le nombre de ses arrêtes relativement au nombre maximal d'arrêtes que peut posséder un graphe ayant le même nombre de sommet que G. Si $\rho(G)$ est proche de 0, on dit que G est *creux* ; au contraire, G est dit *dense* si $\rho(G)$ est proche de 1. La distinction entre le caractère creux ou dense d'un graphe est floue : dans certaines applications, un graphe peut être considéré comme creux si sa densité est inférieure à 0.50, alors que dans d'autres situations, un graphe ne sera creux que si sa densité est inférieure à 0.10. Rappelons que cette notion joue un rôle important dans les calculs pratiques : certains algorithmes sont pleinement optimisés pour les graphes creux mais peuvent être très lents sur des graphes denses, et réciproquement. Par exemple, le programme `nauty and Traces` [NAUTY] (qui est à ce jour l'un des plus efficaces pour résoudre le problème de l'isomorphisme de graphes) propose des implantations différentes suivant la densité des graphes considérés.

Exemple IV.2.3 Le graphe présenté sur la Figure IV.1 a 5 sommets et 8 arrêtes (dont 2 boucles). Sa densité est donc égale à $5/36 \approx 0.139$: il est plutôt creux. Un graphe avec le même nombre de sommets et plus de 27 arrêtes aurait une densité supérieure à 0.75 et pourrait légitimement être considéré comme dense.

La notion cruciale que nous étudions ici est celle d'isomorphisme entre graphes, c'est-à-dire une application d'un graphe à un autre qui préserve la relation d'adjacence :

1. Un tel graphe est dit *simple*.

Définition IV.2.4 *Un isomorphisme entre deux graphe $G := (V, E)$ et $G' := (V', E')$ est une bijection $f : V \longrightarrow V'$ telle que pour tous sommets $v, w \in V$, on a $(v, w) \in E$ si et seulement si $(f(v), f(w)) \in E'$.*

Un isomorphisme entre G et lui-même est appelé un *automorphisme* de G. L'ensemble des automorphismes de G est un groupe fini (puisque c'est un sous-groupe du groupe des permutations des sommets de G) , noté Aut(G).

Exemple IV.2.5 Les graphes présentés sur la Figure IV.2 sont isomorphes, et un isomorphisme est donné par $f(v_1) = w_4$, $f(v_2) = w_1$, $f(v_3) = w_3$ et $f(v_4) = w_2$.

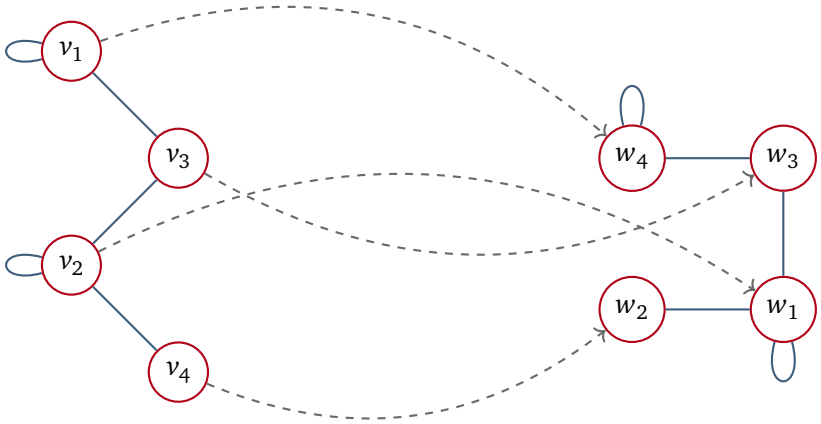


Fig. IV.2 – Exemple de graphes isomorphes.

Nous concentrons notre attention sur deux problèmes algorithmiques classiques liés à ces notions :

- *Graphs Isomorphism problem* (GI) : étant donné deux graphes, décider s'ils sont isomorphes.
- *Graph Automorphisms problem* (GA) : étant donné un graphe, déterminer une famille génératrice de son groupe d'automorphisme.

La réduction polynomiale de GI à GA est bien connue. Nous reprenons ici une preuve qui sera ensuite adaptée au cas des réseaux. Dans tout ce qui suit, par *calculer un groupe*, nous entendons *calculer une famille génératrice de ce groupe*.

Proposition IV.2.6 *Le problème GI est réductible en temps polynomial au problème GA. Plus précisément, décider si deux graphes à N sommets sont isomorphes est réductible au calcul du groupe d'automorphisme d'un graphe à $2N$ sommets.*

Démonstration. Soient G et G' deux graphes à N sommets. On peut supposer sans perte de généralité que G et G' sont connexes. Considérons $G \sqcup G'$ l'union disjointe de G et G'. Les graphes G et G' sont isomorphes si et seulement si $G \sqcup G'$ possède un automorphisme permutant G et G'. De plus, si un tel automorphisme de $G \sqcup G'$ existe, toute famille génératrice de $\mathrm{Aut}(G \sqcup G')$ doit en contenir un. □

Les problèmes GI et GA sont actuellement très étudiés. Il est bien connu que GI est un problème **NP**, qui n'est pas **NP**-complet à moins d'un effondrement de la hiérarchie polynomiale [AB09, §8.2.4, p.156–157]. Un tel effondrement implique en particulier que **P**=**NP**, et il est largement admis par la communauté que cette égalité n'a pas lieu [Gas02]. Le problème GI est résolu en temps polynomial pour de nombreuses classes spécifiques de graphes (citons par exemple les cas des arbres [Kel+57], des graphes planaires [HW74], des graphes de valence bornée [Luk82]...), mais l'existence d'un algorithme polynomial permettant de résoudre le problème GI général est encore à l'heure actuelle un problème ouvert. Jusqu'à récemment, le meilleur algorithme théorique connu était dû aux travaux de Babai et Luks [BL83] et Zemlyachenko, Korneenko et Tyshkevich [ZKT85], dont la complexité est en $2^{O\left(\sqrt{n \log n}\right)}$ pour un graphe à n sommets. Cependant, fin 2015, Babai [Bab15] a présenté un algorithme quasi-polynomial permettant de résoudre GI en temps $\exp\left(\log(n)^{O(1)}\right)$. Le problème GI est aussi relié à de nombreux autres problèmes algorithmiques concernant la notion d'isomorphisme entre des structures mathématiques variées (voir [ZKT85]). Il s'avère même que le problème de l'isomorphisme au sein d'une famille d'objets admettant une description raisonnable [2] est réductible en temps polynomial à GI (voir [Bus+11]).

Dans la suite, il nous sera pratique de considérer des graphes auxquels une donnée supplémentaire est ajoutée. On distingue les graphes étiquetés [3], auxquels une donnée sur les arrêtes est ajoutée, et les graphes colorés [4], auxquels c'est sur les sommets qu'une donnée est ajoutée.

Définition IV.2.7 *Un graphe étiqueté est un graphe $G := (V, E)$ muni d'une application*

$$c_G : E \longrightarrow M,$$

où M est un ensemble fini appelé ensemble des étiquettes de G. De manière similaire, un graphe coloré est un graphe $G := (V, E)$ muni d'une application

$$c_G : V \longrightarrow L,$$

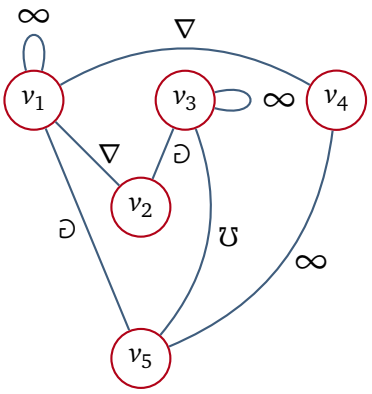
où L est un ensemble fini appelé ensemble des couleurs de G.

2. Plus précisément, il faut que la famille en question soit une classe de structures finies (au sens de [Mar06, §1.1, p.7–14]) sur un même vocabulaire fini, contenant des structures arbitrairement grandes, fermée par isomorphisme et reconnaissable en temps polynomial.

3. *Edge-labeled graph* en anglais.

4. *Vertex-labeled graph* en anglais.

La matrice d'incidence d'un graphe étiqueté contient en plus l'information des étiquettes : le coefficient (i, j) de cette matrice a pour valeur l'étiquette reliant les sommets v_i et v_j si ces sommets sont adjacents, et $\bullet$ (ou tout symbole n'appartenant pas à l'ensemble des étiquettes du graphe considéré) sinon. La Figure IV.3 présente un graphe étiqueté par l'ensemble $\{\infty, \mho, \ə, \nabla\}$ et la matrice d'incidence associée, avec $\bullet$ comme symbole de non-adjacence.



$$\begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} \begin{array}{c} \begin{array}{ccccc} v_1 & v_2 & v_3 & v_4 & v_5 \end{array} \\ \begin{pmatrix} \infty & \nabla & \bullet & \nabla & \ə \\ \nabla & \bullet & \ə & \bullet & \bullet \\ \bullet & \ə & \infty & \bullet & \mho \\ \nabla & \bullet & \bullet & \bullet & \infty \\ \ə & \bullet & \mho & \infty & 0 \end{pmatrix} \end{array}$$

Fig. IV.3 – Exemple de matrice d'incidence associée à un graphe étiqueté.

Dans le cas des graphes étiquetés ou colorés, on exige en plus que les isomorphismes préservent l'étiquetage ou la coloration des graphes :

Définition IV.2.8 *Un isomorphisme entre deux graphes étiquetés $G := (V, E, c_G)$ et $G' := (V', E', c_{G'})$ est un isomorphisme f entre les graphes sous-jacents tel que $e_G(v, w) = e'_G(f(v), f(w))$ pour toute arrête $(v, w) \in E$. De même, un isomorphisme entre deux graphes colorés $G := (V, E, c_G)$ et $G' := (V', E', c_{G'})$ est un isomorphisme f entre les graphes sous-jacents tel que $e_G(v) = e'_G(f(v))$ pour tout sommet $v \in V$.*

Notons que les conditions utilisées dans cette définition sont plus fortes que la simple préservation de la relation d'équivalence donnée par l'étiquetage ou la coloration, condition qui est parfois considérée lorsque la notion d'isomorphisme entre graphes colorés ou étiquetés est introduite. En particulier, deux graphes colorés ou étiquetés isomorphes ont nécessairement le même ensemble de couleurs ou d'étiquettes. Les versions des problèmes GI et GA pour les graphes colorés (resp. étiquetés) sont notées VLGI et VLGA (resp. ELGI et ELGA) [5]. Il est clair que les problèmes GI/GA sont réductibles en temps polynomial aux problèmes VLGI/VLGA et aux problèmes ELGI/ELGA (il suffit de considérer une coloration ou un étiquetage trivial). Comme nous le verrons plus loin, il s'avère que cette réduction est en fait une équivalence polynomiale. Utilisée conjointement avec la Proposition IV.2.6, cette équivalence permet de montrer que les problèmes VLGI et ELGI sont réductibles en temps polynomial aux problèmes VLGA et ELGA respectivement.

5. VLG pour *Vertex-Labeled Graph* et ELG pour *Edge-Labeled Graph*.

IV.2.2 Isométries entre réseaux euclidiens

Dans tout ce chapitre (excepté la Section IV.5), par *réseau*, nous entendons *réseau euclidien de rang maximal*. Nous nous plaçons donc dans le cadre de travail du Chapitre II avec $K = \mathbb{Q}$: pour tout $n \in \mathbb{N}_{>0}$, l'espace euclidien $\mathbb{R}^n$ est équipé du produit scalaire l_2, défini pour tous $x, y \in \mathbb{R}^n$ par $\langle x \,|\, y \rangle := \sum_{i=1}^{n} x_i y_i$. On note $\|\cdot\|$ la norme euclidienne associée.

Rappelons les notions d'isométrie et d'automorphisme introduites dans la Section II.3.5 : deux réseaux Λ et Λ' de $\mathbb{R}^n$ sont dits isométriques s'il existe une isométrie de $\mathbb{R}^n$ envoyant Λ sur Λ' ; une isométrie de Λ sur lui-même est appelée un automorphisme de Λ. L'ensemble $\mathrm{Aut}(\Lambda)$ des automorphismes de Λ est un groupe fini. Si $\mathcal{B}$ est une $\mathbb{R}$-base de $\mathbb{R}^n$, on note $\Lambda(\mathcal{B})$ le réseau de $\mathbb{R}^n$ engendré par cette base. On considère ici les analogues des problèmes GI et GA pour les réseaux :

- *Lattices Isometry problem* (LI) : étant données $\mathcal{B}$ et $\mathcal{B}'$ deux bases de $\mathbb{R}^n$, décider si les réseaux $\Lambda(\mathcal{B})$ et $\Lambda(\mathcal{B}')$ sont isométriques.
- *Lattice Automorphisms problem* (LA) : étant donnée une base $\mathcal{B}$ de $\mathbb{R}^n$, déterminer le groupe d'automorphisme du réseau $\Lambda(\mathcal{B})$.

Commençons par modifier la réduction de GI à GA afin d'obtenir une réduction de LI à LA :

Proposition IV.2.9 *Le problème LI est réductible en temps polynomial au problème LA. Plus précisément, décider si deux réseaux de $\mathbb{R}^n$ sont isométriques est réductible au calcul du groupe d'automorphisme d'un réseau de $\mathbb{R}^{2n}$.*

Démonstration. Soient Λ, Λ' deux réseaux de $\mathbb{R}^n$, de base respective $B, B' \in \mathrm{GL}_n(\mathbb{R})$. Considérons $\Lambda \oplus \Lambda'$ le réseau de $\mathbb{R}^{2n}$ de base $\begin{pmatrix} B & 0 \\ 0 & B' \end{pmatrix} \in \mathrm{GL}_{2n}(\mathbb{R})$. Les réseaux Λ et Λ' sont isométriques si et seulement si $\Lambda \oplus \Lambda'$ possède un automorphisme permutant Λ et Λ'. De plus, si un tel automorphisme de $\Lambda \oplus \Lambda'$ existe, toute famille génératrice de $\mathrm{Aut}(\Lambda \oplus \Lambda')$ doit en contenir un. □

Malgré le rôle important joué par ces problèmes dans de nombreux domaines, leur complexité est mal connue. Le meilleur algorithme connu et largement implanté pour attaquer les problèmes LI et LA est celui de Plesken et Souvignier [PS97], mais à notre connaissance, aucune analyse de complexité n'a été réalisée sur cette méthode. Haviv et Regev ont récemment présenté dans [HR14] un algorithme théorique qui énumère toutes les isométries entre deux réseaux de $\mathbb{R}^n$ en temps $n^{O(n)} s^{O(1)}$, où s est la taille des entrées. Cet algorithme est asymptotiquement optimal, mais le problème de l'énumération des isométries entre deux réseaux est bien différent du problème de décision de l'existence d'une telle isométrie.

Notons que similairement à GI, LI est un problème **NP**, qui n'est pas **NP**-complet à moins d'un effondrement de la hiérarchie polynomiale (essentiellement car il appartient à la classe de complexité **SZK**). Nous renvoyons à [Kaz15, §4.10.1, p.58–59] ou [HR14, §1 et §5.2] pour plus de détails sur ce résultat. Cependant, tous les algorithmes actuellement connus pour traiter les problèmes LI et LA (y compris celui de Plesken et Souvignier [PS97] et celui de Haviv et Regev

[HR14]) nécessitent le précalcul d'ensembles de la forme $\{x \in \Lambda \,:\, \|x\| = C\}$. Le comptage d'éléments de norme donnée dans un réseau est un problème ♯**P**-dur (voir [Cha07, §3]). De plus, les algorithmes d'énumération de $\{x \in \Lambda \,:\, \|x\| = C\}$ passent généralement par le calcul de $\{x \in \Lambda \,:\, \|x\| \leqslant C\}$, et il est bien connu que la détermination de tels ensembles est un problème **NP**-dur en norme l_2 sous des réductions probabilistes [Ajt96 ; Ajt98]. Même en tenant compte de ces calculs, très peu de résultats de complexité sont connus concernant LI et LA. C'est pourquoi nous introduisons des versions affaiblies de ces problèmes. Dans la suite, si Λ est un réseau de $\mathbb{R}^n$ et $X := (x_1, \ldots, x_k)$ est une famille d'éléments de $\mathbb{R}^n$, on note $S(\Lambda, X)$ l'ensemble fini :

$$S(\Lambda, X) := \bigcup_{i=1}^{k} \{x \in \Lambda \,:\, \|x\| = \|x_i\|\}\,.$$

Les versions affaiblies de LI et LA supposent données des ensembles de cette forme :

- *Weakened Lattices Isometry problem* (WLI) : étant données $\mathcal{B}$ et $\mathcal{B}'$ deux bases de $\mathbb{R}^n$ et les ensembles $S(\Lambda(\mathcal{B}), \mathcal{B})$ et $S(\Lambda(\mathcal{B}'), \mathcal{B})$, décider si les réseaux $\Lambda(\mathcal{B})$ et $\Lambda(\mathcal{B}')$ sont isométriques.
- *Weakened Lattice Automorphisms problem* (WLA) : étant donnée une base $\mathcal{B}$ de $\mathbb{R}^n$ et l'ensemble $S(\Lambda(\mathcal{B}), \mathcal{B})$, déterminer le groupe d'automorphisme du réseau $\Lambda(\mathcal{B})$.

Si $|S(\Lambda(\mathcal{B}), \mathcal{B})| \neq |S(\Lambda(\mathcal{B}'), \mathcal{B})|$, alors $\Lambda(\mathcal{B})$ et $\Lambda(\mathcal{B}')$ ne peuvent pas être isométriques. C'est pourquoi dans la suite, nous supposerons généralement que lorsqu'ils sont donnés, ces deux ensembles ont le même cardinal.

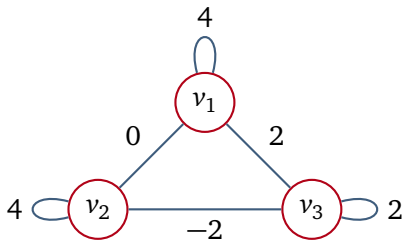
L'objectif des prochains paragraphes de ce chapitre est de montrer que les problèmes WLI et WLA sont réductibles en temps polynomial aux problèmes GI et GA respectivement. Nous passerons pour cela par des réductions au cas des graphes étiquetés puis au cas des graphes colorés. Notons que l'idée de relier les graphes et les réseaux par des problèmes d'isomorphisme n'est pas neuve : il est démontré dans [DSSV09, thm.3] que GI est réductible en temps polynomial à LI, et une approche « par les graphes » est présentée dans [BDSS09, §3.2] pour calculer certains isomorphismes entre cônes convexes provenant de réseaux.

IV.3 Transformation d'un réseau en un graphe

IV.3.1 De réseau à graphe étiqueté

Soit S un ensemble fini de points de $\mathbb{R}^n$. On associe à S un graphe complet étiqueté G_S, dont les sommets sont les éléments de S et l'étiquette de l'arrête entre x et y est $\langle x \,|\, y \rangle$. L'ensemble des étiquettes du graphe G_S est donc inclus dans $\mathbb{R}$. D'autre part, il n'est pas nécessaire de désigner un symbole de non-adjacence puisque ce graphe est complet.

Exemple IV.3.1 Considérons le sous-ensemble $S = \{(2,0), (0,-2), (1,1)\} = \{v_1, v_2, v_3\} \subset \mathbb{R}^2$. Le graphe étiqueté G_S associé est présenté sur la Figure IV.4.



$$\begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \end{array} \begin{array}{c} \begin{array}{ccc} v_1 & v_2 & v_3 \end{array} \\ \begin{pmatrix} 4 & 0 & 2 \\ 0 & 4 & -2 \\ 2 & -2 & 2 \end{pmatrix} \end{array}$$

Fig. IV.4 – Le graphe étiqueté G_S et sa matrice d'incidence.

Soient Λ un réseau de $\mathbb{R}^n$ de base $\mathcal{B} := (b_1, \dots, b_n)$. En prenant pour S l'ensemble $S(\Lambda, \mathcal{B})$ introduit dans la Section IV.2.2, on obtient un graphe complet étiqueté $G_{S(\Lambda,\mathcal{B})}$ à $|S(\Lambda, \mathcal{B})|$ sommets, qui sera noté $G(\Lambda, \mathcal{B})$ dans la suite. Remarquons qu'un automorphisme de Λ induit naturellement un automorphisme de $G(\Lambda, \mathcal{B})$. De plus, puisque $S(\Lambda, \mathcal{B})$ contient la base $\mathcal{B}$, deux automorphismes distincts de Λ induisent deux automorphismes distincts de $G(\Lambda, \mathcal{B})$. Il s'avère que tout automorphisme de $G(\Lambda, \mathcal{B})$ est de cette forme :

Proposition IV.3.2 *Soient Λ un réseau de $\mathbb{R}^n$ de base $\mathcal{B} := (b_1, \dots, b_n)$ et σ un automorphisme de $G(\Lambda, \mathcal{B})$. Il existe un unique automorphisme $u \in \mathrm{Aut}(\Lambda)$ tel que $u(x) = \sigma(x)$ pour tout $x \in S(\Lambda, \mathcal{B})$. En particulier, les groupes $\mathrm{Aut}(\Lambda)$ et $\mathrm{Aut}(G(\Lambda, \mathcal{B}))$ sont (explicitement) isomorphes.*

Démonstration. Pour tout $1 \leqslant i \leqslant n$, notons $b'_i := \sigma(b_i)$. Soient B et B' les matrices dont les colonnes sont formées par $(b_1, \dots, b_n)$ et $(b'_1, \dots, b'_n)$ respectivement. Puisque σ préserve les étiquettes des arrêtes de $G(\Lambda, \mathcal{B})$, on a $\langle b_i \,|\, b_j \rangle = \langle b'_i \,|\, b'_j \rangle$ pour tous $1 \leqslant i, j \leqslant n$, et donc $B^\intercal B = B'^\intercal B'$. Ceci entraîne que la matrice $Q := B'B^{-1}$ est orthogonale.

Montrons que $Qx = \sigma(x)$ pour tout $x \in S$. Soient $x \in S$ et $1 \leqslant i \leqslant n$. Par orthogonalité de Q, on a

$$b_i'^\intercal Q x = (Q^{-1} b'_i)^\intercal x$$

et donc

$$b_i'^\intercal Q x = b_i^\intercal x = b_i'^\intercal \sigma(x).$$

On obtient finalement l'égalité

$$b_i'^\intercal (Qx - \sigma(x)) = 0$$

pour tout $1 \leqslant i \leqslant n$. Puisque Q et B sont des matrices inversibles, B' l'est aussi. Ainsi, $(b'_1, \dots, b'_n)$ est une $\mathbb{R}$-base de $\mathbb{R}^n$ et l'égalité précédente entraîne que $Qx = \sigma(x)$. Comme $S(\Lambda, \mathcal{B})$ contient la base $\mathcal{B}$, l'endomorphisme u dont la matrice est Q dans la base standard de $\mathbb{R}^n$ est un automorphisme de Λ complètement déterminé par σ. □

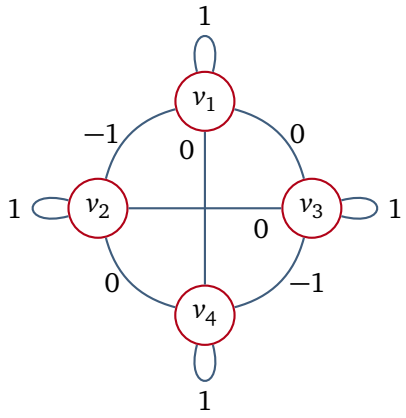
Il est aisé d'adapter la preuve précédente pour démontrer le résultat suivant :

Proposition IV.3.3 *Soient Λ et Λ' deux réseaux de $\mathbb{R}^n$ et $\mathcal{B} := (b_1, \dots, b_n)$ une base de Λ. Les réseaux Λ et Λ' sont isométriques si et seulement si les graphes étiquetés $G(\Lambda, \mathcal{B})$ et $G(\Lambda', \mathcal{B})$ sont isomorphes.*

Exemple IV.3.4 Considérons le réseau $\mathbb{Z}^2 \subset \mathbb{R}^2$ de base $\mathcal{B} := ((1,0),(0,1))$. On a

$$S(\mathbb{Z}^2, \mathcal{B}) = \{(1,0),(-1,0),(0,1),(0,-1)\} =: \{v_1, v_2, v_3, v_4\} \subset \mathbb{Z}^2.$$

Le graphe étiqueté $G(\mathbb{Z}^2, \mathcal{B})$ associé est présenté sur la Figure IV.5.



$$\begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{cccc} v_1 & v_2 & v_3 & v_4 \end{array} \\ \begin{pmatrix} 1 & -1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & -1 & 1 \end{pmatrix} \end{array}$$

Fig. IV.5 – Le graphe étiqueté $G(\mathbb{Z}^2, \mathcal{B})$ et sa matrice d'incidence.

Les groupes $\mathrm{Aut}(\mathbb{Z}^2)$ et $\mathrm{Aut}(G(\mathbb{Z}^2, \mathcal{B}))$ sont bien isomorphes. En effet, on a :

$$\mathrm{Aut}(\mathbb{Z}^2) = \left\langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle$$

et

$$\mathrm{Aut}(G(\mathbb{Z}^2, \mathcal{B})) = \langle (1\,2)(3\,4), (1\,3)(2\,4), (3\,4) \rangle .$$

Étant donné un graphe G et un ensemble fini $S \subset \mathbb{R}^n$, le graphe étiqueté G_S est calculable en un temps polynomial en le cardinal de S. On déduit de cette remarque une première réduction. Dans la suite, par *opérations arithmétiques*, nous désignons l'addition et la multiplication sur $\mathbb{Z}$, $\mathbb{Q}$ ou $\mathbb{R}$. Il faut noter que nous ignorons ici les problèmes liés à la précision des calculs. Il est aussi possible de se restreindre aux réseaux intégraux afin de ne considérer que des opérations sur $\mathbb{Z}$.

Théorème IV.3.5 *Les problèmes WLI et WLA sont réductibles en temps polynomial aux problèmes ELGI et ELGA respectivement. Plus précisément :*

- *Soient $\mathcal{B}$ et $\mathcal{B}'$ deux bases de $\mathbb{R}^n$. Supposons que les ensembles $S(\Lambda(\mathcal{B}), \mathcal{B})$ et $S(\Lambda(\mathcal{B}'), \mathcal{B})$ sont donnés et de même cardinal, noté s. Décider si $\Lambda(\mathcal{B})$ et $\Lambda(\mathcal{B}')$ sont isométriques est réductible en $O\left(ns^2\right)$ opérations arithmétiques à décider si deux graphes étiquetés à s sommets sont isomorphes.*
- *Soit $\mathcal{B}$ une base de $\mathbb{R}^n$. Supposons donné l'ensemble $S(\Lambda(\mathcal{B}), \mathcal{B})$ et notons s son cardinal. Le calcul de $\mathrm{Aut}(\Lambda(\mathcal{B}))$ est réductible en $O\left(ns^2\right)$ opérations arithmétiques au calcul du groupe d'automorphisme d'un graphe étiqueté à s sommets.*

Démonstration. Il s'agit de prouver que si S un sous-ensemble fini de $\mathbb{R}^n$, le graphe étiqueté G_S est calculable en $O\left(n|S|^2\right)$ opérations arithmétiques. Ceci est naïvement réalisable en calculant $\frac{|S|(|S|+1)}{2}$ produits scalaires, chacun nécessitant $2n-1$ opérations arithmétiques. □

Il est bon d'insister sur le fait que cette réduction est polynomiale *en le cardinal de* $S(\Lambda, \mathcal{B})$, et non en la dimension des réseaux considérés. Nous ne connaissons pas à l'heure actuelle de réduction de WLI/WLA à ELGI/ELGA en temps polynomial en la dimension. Ce constat est plus général : nous ne connaissons pas d'algorithme permettant de résoudre les problèmes WLI et WLA en temps polynomial en la dimension. Par exemple, la complexité de l'algorithme de Haviv et Regev [HR14] reste polynomiale seulement en la taille de $S(\Lambda, \mathcal{B})$, et ceci même en retirant la complexité du calcul de $S(\Lambda, \mathcal{B})$.

IV.3.2 De graphe étiqueté à graphe coloré

Nous détaillons dans cette section une méthode connue, suggérée par exemple dans la documentation de `nauty and Traces` [NAUTY, §14, p.60], permettant de transformer un graphe étiqueté en un graphe coloré tout en préservant le groupe d'automorphisme et la classe d'isomorphie du graphe considéré.

IV.3.2.1 Principe

Soit G un graphe étiqueté, dont les sommets sont notés $v_1, \dots, v_N$. Supposons dans un premier temps que les arrêtes de G sont étiquetées par $1, 2, 3, \dots, 2^d - 1$. Considérons le graphe coloré $G_\bullet$ tel que :

- $G_\bullet$ possède Nd sommets, notés v_i^j pour $1 \leqslant i \leqslant N$ et $1 \leqslant j \leqslant d$.
- Le sommet v_i^j de $G_\bullet$ est coloré par j. En particulier, il y a d couleurs différentes dans $G_\bullet$. Nous parlerons parfois de *niveau* j plutôt que de *couleur* j.
- Il y a une arrête entre v_i^j et v_k^l pour $j \neq l$ si et seulement si $i = k$ et $j = l \pm 1$. Ces arrêtes sont dites *verticales*.
- Il y a une arrête entre v_i^j et v_k^j si et seulement s'il y a une arrête dans G entre v_i et v_k d'étiquette $\alpha = \sum_{l=1}^{d} \alpha_l 2^{l-1}$ telle que $\alpha_j \neq 0$. Ces arrêtes sont appelées des arrêtes *horizontales*.

Avant de prouver que cette construction préserve les isomorphismes, illustrons-la par un exemple simple.

Exemple IV.3.6 Considérons le graphe étiqueté G et le graphe coloré associé présentés sur la Figure IV.6. Le graphe G possède $N = 3$ sommets et il faut $d = 3$ bits pour encoder ses 4 étiquettes. Ainsi, $G_\bullet$ possède 9 sommets repartis sur 3 niveaux. L'étiquette 1 est encodée par 001 et détermine donc des arrêtes entre les sommets de niveau 1. Par exemple, l'arrête d'étiquette 1 entre v_2 et v_3 dans G est convertie en une arrête entre v_2^1 et v_3^1 dans $G_\bullet$. De même, l'étiquette 3 est encodée par 011, et détermine donc des arrêtes entre les sommets de niveau 1 et 2. La boucle sur v_3 d'étiquette 3 est par conséquent convertie en des boucles sur v_3^1 et v_3^2.

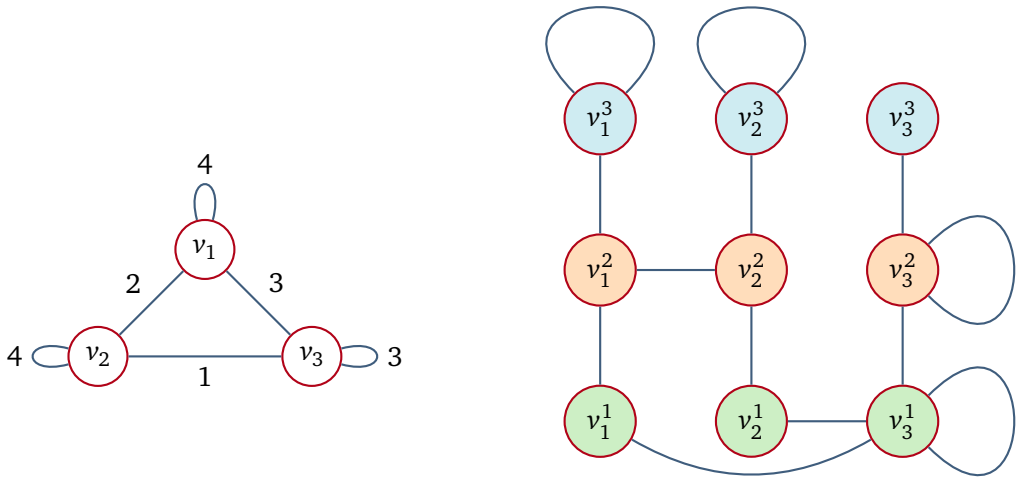


Fig. IV.6 – Le graphe étiqueté G et sa version colorée associée.

Si les étiquettes du graphe G considéré ne sont pas des entiers consécutifs, il est nécessaire de les ordonner avant d'appliquer la transformation précédemment décrite. Le graphe coloré $G_\bullet$ obtenu dépend du choix fait sur l'agencement de ces étiquettes, mais son groupe d'automorphisme est indépendant de ce choix (à un isomorphisme explicite près) puisqu'il est isomorphe à $\mathrm{Aut}(G)$, comme nous le verrons dans la prochaine section. De plus, puisque deux graphes étiquetés isomorphes ont nécessairement le même ensemble d'étiquettes, il suffit de choisir le même agencement de part et d'autre lors d'une instance de ELGI.

Exemple IV.3.7 On reprend le graphe étiqueté $G(\mathbb{Z}^2, \mathcal{B})$ de l'Exemple IV.3.4. Le graphe initial comporte $N = 4$ sommets, et puisque les étiquettes sont $\{-1, 0, 1\}$, seulement $d = 2$ bits sont nécessaires pour les encoder. La Figure IV.7 présente la version colorée de $G(\mathbb{Z}^2, \mathcal{B})$ obtenue pour l'agencement des étiquettes associé à l'ordre usuel sur $\mathbb{Z}$.

IV.3.2.2 Réduction du cas étiqueté au cas coloré

Nous montrons maintenant que la construction précédente préserve effectivement le groupe des automorphismes d'un graphe. Il sera ensuite aisé d'en déduire une preuve quant à la préservation des isomorphismes de graphes. On fixe G un graphe étiqueté, dont les sommets sont $v_1, \ldots, v_N$ et dont les étiquettes sont $1, 2, 3, \ldots, 2^d - 1$. Soit $G_\bullet$ le graphe coloré obtenu par la construction précédemment présentée.

Lemme IV.3.8 *Un automorphisme de $G_\bullet$ est complètement déterminé par son action sur $v_1^1, \ldots, v_N^1$.*

Démonstration. Soit $\sigma \in \mathrm{Aut}(G_\bullet)$. Puisque σ préserve la coloration des sommets de $G_\bullet$, il existe $\varphi \in \mathfrak{S}_N$ telle que $\sigma(v_i^1) = v_{\varphi(i)}^1$ pour tout $1 \leqslant i \leqslant N$. Montrons par récurrence sur

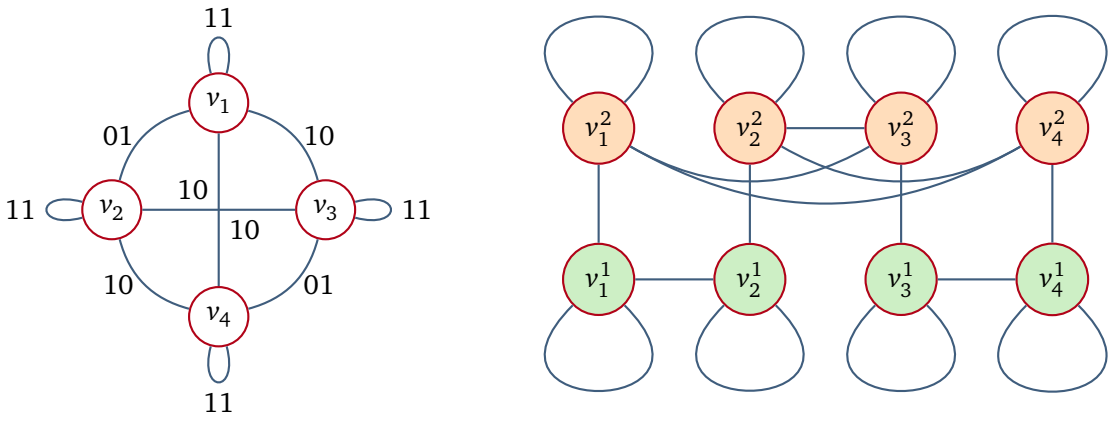


Fig. IV.7 – À gauche, le graphe $G(\mathbb{Z}^2, \mathcal{B})$ après réétiquetage binaire, à droite le graphe coloré associé.

$1 \leqslant j \leqslant d$ que $\sigma(v_i^j) = v_{\varphi(i)}^j$ pour tout $1 \leqslant i \leqslant N$.

Soient $1 \leqslant i \leqslant N$ et $2 \leqslant j \leqslant d$. Supposons que la relation précédente est vérifiée au rang $j-1$. Il existe un indice $1 \leqslant k \leqslant N$ tel que $\sigma(v_i^j) = v_k^j$. Les sommets v_i^{j-1} et v_i^j étant reliés par une arrête verticale, les sommets $\sigma(v_i^{j-1}) = v_{\varphi(i)}^{j-1}$ et $\sigma(v_i^j) = v_k^j$ le sont aussi. Par définition de $G_\bullet$, ceci n'est possible que si $k = \varphi(i)$. Ainsi, $\sigma(v_i^j) = v_{\varphi(i)}^j$ pour tous $1 \leqslant i \leqslant N$ et $1 \leqslant j \leqslant d$, ce qui prouve le résultat annoncé. □

Proposition IV.3.9 *Les groupes* $\mathrm{Aut}(G)$ *et* $\mathrm{Aut}(G_\bullet)$ *sont (explicitement) isomorphes.*

Démonstration. Soient $\sigma \in \mathrm{Aut}(G)$ et

$$\begin{array}{rccc} \widetilde{\sigma} : & G_\bullet & \longrightarrow & G_\bullet \\ & v_i^j & \longmapsto & \sigma(v_i)^j \end{array} .$$

Montrons que $\widetilde{\sigma}$ est un automorphisme de $G_\bullet$. Par définition, $\widetilde{\sigma}$ préserve la coloration des sommets de $G_\bullet$, et il est facile de voir que $\widetilde{\sigma}$ préserve les arrêtes verticales de $G_\bullet$. Soient v_i^k et v_j^k des sommets de $G_\bullet$ horizontalement adjacents. Par définition, il existe une arrête d'étiquette α reliant v_i et v_j dans G telle que le bit en position k de la décomposition binaire de α est non nul. Puisque σ est un automorphisme de G, $\sigma(v_i)$ et $\sigma(v_j)$ sont aussi reliés par une arrête d'étiquette α dans G, ce qui entraîne que $\widetilde{\sigma}(v_i^k) = \sigma(v_i)^k$ et $\widetilde{\sigma}(v_j^k) = \sigma(v_j)^k$ sont adjacents dans $G_\bullet$. Ainsi, $\widetilde{\sigma}$ est bien un automorphisme de $G_\bullet$.

Deux automorphismes distincts de G induisent par ce procédé deux automorphismes distincts de $G_\bullet$. Reste à montrer que tout automorphisme de $G_\bullet$ est de cette forme. Soient $\tau \in \mathrm{Aut}(G_\bullet)$ et $\varphi \in \mathfrak{S}_N$ la permutation induite par l'action de τ sur $v_1^1, \ldots, v_N^1$. L'application

$$\begin{array}{rccc} \sigma : & G & \longrightarrow & G \\ & v_i & \longmapsto & v_{\varphi(i)} \end{array}$$

est un automorphisme de G tel que $\widetilde{\sigma} = \tau$. En effet, $\widetilde{\sigma}$ coïncide par construction avec τ sur $v_1^1, \ldots, v_N^1$, ce qui entraîne l'égalité $\widetilde{\sigma} = \tau$ d'après le Lemme IV.3.8, et on en déduit par un argument analogue à celui du point précédent que σ est un automorphisme de G. □

Soient H un graphe étiqueté et $H_\bullet$ sa conversion en un graphe coloré par la méthode décrite plus haut. La démonstration précédente est aisément adaptable aux cas des isomorphismes entre graphes :

Proposition IV.3.10 *Les graphes étiquetés G et H sont isomorphes si et seulement si les graphes colorés $G_\bullet$ et $H_\bullet$ le sont.*

Finalement, on déduit des constructions présentées la réduction polynomiale de ELGI/ELGA à VLGI/VLGA :

Théorème IV.3.11 *Les problèmes ELGI et ELGA sont réductibles en temps polynomial aux problèmes VLGI et VLGA respectivement. Plus précisément :*

- *Soient G et H deux graphes étiquetés à N sommets et ayant les mêmes m étiquettes. Soit $d := \lfloor \log_2(m) \rfloor + 1$. Décider si G et H sont isomorphes se réduit en temps $O\left(dN^2\right)$ à décider si deux graphes colorés à dN sommets sont isomorphes.*
- *Soient G un graphe étiqueté à N sommets et m étiquettes. Soit $d := \lfloor \log_2(m) \rfloor + 1$. Le calcul de $\mathrm{Aut}(G)$ se réduit en temps $O(dN^2)$ au calcul du groupe d'automorphisme d'un graphe coloré à dN sommets.*

Démonstration. Par construction, le graphe étiqueté $G_\bullet$ possède bien dN sommets (puisqu'il faut d bits pour représenter les m étiquettes de G). De plus, ce graphe coloré est calculable en temps $O\left(dN^2\right)$: il suffit de parcourir les paires (v, w) de sommets de G et de calculer la décomposition binaire de l'étiquette de l'arrête reliant v et w (si elle existe). □

Notons que cette réduction est aussi polynomiale en le nombre de sommets N du graphe G initial : il y a au plus N^2 étiquettes distinctes dans G, donc au plus $N\left(2\lfloor \log_2(N) \rfloor + 1\right)$ sommets dans $G_\bullet$. L'intérêt de cette conversion n'est pas seulement théorique : la plupart des programmes permettant de traiter les problèmes GI et GA (dont `nauty and Traces` [NAUTY]) fonctionnent pour les graphes colorés et non les graphes étiquetés. Puisque ces programmes disposent généralement de routines différentes pour les graphes creux et les graphes denses, il est intéressant d'étudier la densité des graphes $G(\Lambda, \mathcal{B})_\bullet$.

IV.3.2.3 Densité de $G(\Lambda, \mathcal{B})_\bullet$

Comme remarqué précédemment, si G est un graphe étiqueté, la structure de $G_\bullet$ est dépendante de l'ordre choisi sur les étiquettes de G. En particulier, la densité de $G_\bullet$ dépend de ce choix. Il est aisé de déterminer un agencement des étiquettes minimisant la densité : il suffit d'affecter les étiquettes ayant le plus d'occurrence aux mots binaires de poids de Hamming minimal. Notons qu'en pratique, ordonner les étiquettes en fonction de leur nombre d'occurrence est coûteux, notamment lorsque le taille du graphe augmente. Quoi qu'il en soit, nous montrons

dans ce paragraphe que si Λ est un réseau de base $\mathcal{B}$, la densité du graphe coloré $G(\Lambda,\mathcal{B})_\bullet$ est inférieure à une quantité ne dépendant que la dimension de Λ, et ceci indépendamment de l'ordre choisi sur les étiquettes. En particulier, nous montrons que $G(\Lambda,\mathcal{B})_\bullet$ est toujours un graphe relativement creux.

Commençons par étudier le cas d'un graphe $G(\Lambda(\mathcal{B}),\mathcal{B})$ où $\mathcal{B}$ une base orthogonale dans laquelle tous les vecteurs ont la même norme. Ceci revient à demander que la matrice de Gram de $\mathcal{B}$ soit égale à αI_n pour un certain $\alpha \in \mathbb{R}_{>0}$.

Lemme IV.3.12 *Soient $\alpha \in \mathbb{R}_{>0}$ et $\mathcal{B} := (b_1,\dots,b_n)$ une base de $\mathbb{R}^n$ dont la matrice de Gram est αI_n. La densité de $G(\Lambda(\mathcal{B}),\mathcal{B})_\bullet$ dépend seulement de la dimension n :*

$$\rho(G(\Lambda(\mathcal{B}),\mathcal{B})_\bullet) = \begin{cases} \dfrac{2n+3}{8n+2} & \text{si l'ordre des étiquettes est } (\alpha,-\alpha,0) \text{ ou } (-\alpha,\alpha,0), \\ \dfrac{n+6}{8n+2} & \text{si l'ordre des étiquettes est } (-\alpha,0,\alpha) \text{ ou } (0,-\alpha,\alpha), \\ \dfrac{n+5}{8n+2} & \text{si l'ordre des étiquettes est } (\alpha,0,-\alpha) \text{ ou } (0,\alpha,-\alpha). \end{cases} \tag{IV.1}$$

Démonstration. Puisque la matrice de Gram de $\mathcal{B}$ est égale à αI_n, on a

$$S(\Lambda(\mathcal{B}),\mathcal{B}) = \{b_1,\dots,b_n,-b_1,\dots,-b_n\}.$$

Le graphe étiqueté $G(\Lambda(\mathcal{B}),\mathcal{B})$ possède donc $2n$ sommets et les étiquettes possibles sont $\pm\alpha$ et 0. On en déduit que $G(\Lambda(\mathcal{B}),\mathcal{B})_\bullet$ possède $4n$ sommets, répartis sur 2 niveaux de $2n$ sommets. Supposons que l'ordre des étiquettes de $G(\Lambda(\mathcal{B}),\mathcal{B})$ est $(-\alpha,0,\alpha)$ et énumérons les arrêtes de $G(\Lambda(\mathcal{B}),\mathcal{B})_\bullet$:

- Il y a $2n$ arrêtes verticales.
- Les arrêtes d'étiquette $-\alpha$ (associée au binaire 01) induisent n arrêtes dans le premier niveau de $G(\Lambda(\mathcal{B}),\mathcal{B})_\bullet$.
- Les arrêtes d'étiquette α (associée au binaire 11) induisent une boucle sur chaque sommet de $G(\Lambda(\mathcal{B}),\mathcal{B})_\bullet$, soit $4n$ boucles.
- Les arrêtes d'étiquettes 0 (associée au binaire 10) induisent $2n(n-1)$ arrêtes simples dans le second niveau de $G(\Lambda(\mathcal{B}),\mathcal{B})_\bullet$. En effet, un sommet $G(\Lambda(\mathcal{B}),\mathcal{B})$ est relié à tous les autres sommets excepté lui-même et son opposé par une arrête d'étiquette 0. En prenant soin de compter chaque arrête de ce type une unique fois, on en dénombre $\sum_{k=n-1}^{2n-2} k$ pour les n premiers sommets du second niveau de $G(\Lambda(\mathcal{B}),\mathcal{B})_\bullet$ associés à $b_1,\dots,b_n$, puis $\sum_{j=0}^{n-1} k$ pour les n sommets du second niveau restants, associés à $-b_1,\dots,-b_n$.

Le graphe $G(\Lambda(\mathcal{B}),\mathcal{B})_\bullet$ possède donc $2n+n+4n+2n(n-1)$ arrêtes. Finalement :

$$\rho(G(\Lambda(\mathcal{B}),\mathcal{B})_\bullet) = \frac{2(2n+n+4n+2n(n-1))}{(4n)(4n+1)} = \frac{n+6}{8n+2}.$$

Le résultat annoncé pour l'ordre $(-\alpha,0,\alpha)$ est démontré. Le même raisonnement pour les autres agencements permet de montrer les autres égalités. □

Proposition IV.3.13 *Soient Λ un réseau de $\mathbb{R}^n$ de base $\mathcal{B} := (b_1, \dots, b_n)$. La densité de $G(\Lambda, \mathcal{B})_\bullet$ est bornée indépendamment de la paire $(\Lambda, \mathcal{B})$ et de l'ordre choisi sur les étiquettes de $G(\Lambda, \mathcal{B})$:*

$$\rho\left(G(\Lambda, \mathcal{B})_\bullet\right) \leqslant \frac{2n+3}{6n+1}. \tag{IV.2}$$

En particulier,

$$\rho\left(G(\Lambda, \mathcal{B})_\bullet\right) \leqslant \frac{4}{13} + \frac{3}{6n+1}.$$

Démonstration. La seconde inégalité est une conséquence immédiate de la première puisque

$$\frac{2n+3}{6n+1} = \frac{2n}{6n+1} + \frac{3}{6n+1} \leqslant \frac{4}{13} + \frac{3}{6n+1}$$

dès que $n \geqslant 2$ (le cas trivial $n = 1$ est écarté), et ceci par décroissante de la fonction $x \mapsto \frac{2x}{6x+1}$ sur $\mathbb{R}_{>0}$. D'autre part, l'égalité (IV.1) entraîne l'inégalité (IV.2) : la comparaison de ces bornes se ramène à l'étude d'une paire d'inégalités quadratiques. Supposons donc qu'il n'existe pas $\alpha \in \mathbb{R}$ tel que la matrice de Gram de $\mathcal{B}$ soit égale à αI_n.

Notons d le nombre de bits nécessaires pour représenter les étiquettes des arrêtes de $G(\Lambda, \mathcal{B})$ et $s := |S(\Lambda, \mathcal{B})|$. Par construction, le graphe $G(\Lambda, \mathcal{B})_\bullet$ possède sd sommets et $s(d-1)$ arrêtes verticales. De plus, il y a dans chaque niveau de $G(\Lambda, \mathcal{B})_\bullet$ au plus $\frac{s(s+1)}{2}$ arrêtes horizontales (en incluant les boucles). On borne ainsi grossièrement la densité de $G(\Lambda, \mathcal{B})_\bullet$:

$$\rho\left(G(\Lambda, \mathcal{B})_\bullet\right) \leqslant \frac{2\left(s(d-1) + \frac{sd(s+1)}{2}\right)}{sd(sd+1)} \leqslant \frac{s+3}{sd+1}.$$

Puisque $S(\Lambda, \mathcal{B})$ contient $\pm b_1, \dots, \pm b_n$, on a $s \geqslant 2n$. De plus, la fonction $x \mapsto \frac{x+3}{xd+1}$ étant décroissante sur $\mathbb{R}_{>0}$, on a

$$\frac{s+3}{sd+1} \leqslant \frac{2n+3}{3nd+1}.$$

Pour conclure la preuve, il ne reste qu'à montrer que $d \geqslant 3$. Puisqu'il y a au moins deux étiquettes distinctes dans $G(\Lambda, \mathcal{B})$, on a $d \geqslant 2$. On raisonne par l'absurde et on suppose donc que $d = 2$, c'est-à-dire que $G(\Lambda, \mathcal{B})$ comporte 2 ou 3 étiquettes distinctes. Notons $\pm\alpha$ avec $\alpha \in \mathbb{R}_{>0}$ les deux étiquettes non nulles de $G(\Lambda, \mathcal{B})$. L'hypothétique troisième étiquette de $G(\Lambda, \mathcal{B})$ est nécessairement 0. On a $\|b_i\|^2 = \alpha$ pour tout $1 \leqslant i \leqslant n$, et puisque la matrice de Gram de $\mathcal{B}$ n'est pas égale à αI_n, il existe $1 \leqslant i < j \leqslant n$ tels que $\langle b_i \mid b_j \rangle \neq 0$. Quitte à changer b_j en $-b_j$, supposons que $\langle b_i \mid b_j \rangle = \alpha$. Alors

$$\|b_i - b_j\|^2 = -2\langle b_i \mid b_j \rangle + \|b_i\|^2 + \|b_j\|^2 = -2\alpha + \alpha + \alpha = 0,$$

ce qui est une contradiction évidente. Ainsi, $d \geqslant 3$ et l'inégalité annoncée est démontrée. □

L'inégalité (IV.2) montre que les graphes $G(\Lambda, \mathcal{B})_\bullet$ restent relativement creux indépendamment du réseau et de la base choisie. De plus, cette borne prévoit que la densité des graphes de la forme $G(\Lambda, \mathcal{B})$ est asymptotiquement inférieure à 0.30. Ce fait est expérimentalement

vérifié : les graphes les plus denses que nous avons obtenus sont issus de réseaux de petite dimension. Notons qu'en pratique, il est toujours possible d'utiliser les routines dédiées aux graphes creux du programme `nauty and Traces`. En effet, la borne (IV.2) est la plupart du temps assez éloignée de la densité réelle des graphes calculés : ils sont généralement bien plus creux que prévu. En guise d'exemple, considérons les bases des 10916 réseaux parfaits de dimension 8 données dans le catalogue LATTICES [LATT] maintenu par Nebe et Sloane. La partie gauche de la Figure IV.8 présente la distribution de la densité des graphes colorés obtenus. Ces graphes ont été calculés en considérant l'ordre des étiquettes associé à l'ordre usuel sur $\mathbb{R}$; les densités présentées ne sont donc pas optimales en général. Quoi qu'il en soit, la densité maximale obtenue est inférieure à 0.20. La partie droite de cette même figure présente le rapport entre la borne théorique (IV.2) et la densité obtenue. On remarque que la densité réelle des graphes considérés est au moins deux fois inférieure aux prédictions de la borne théorique.

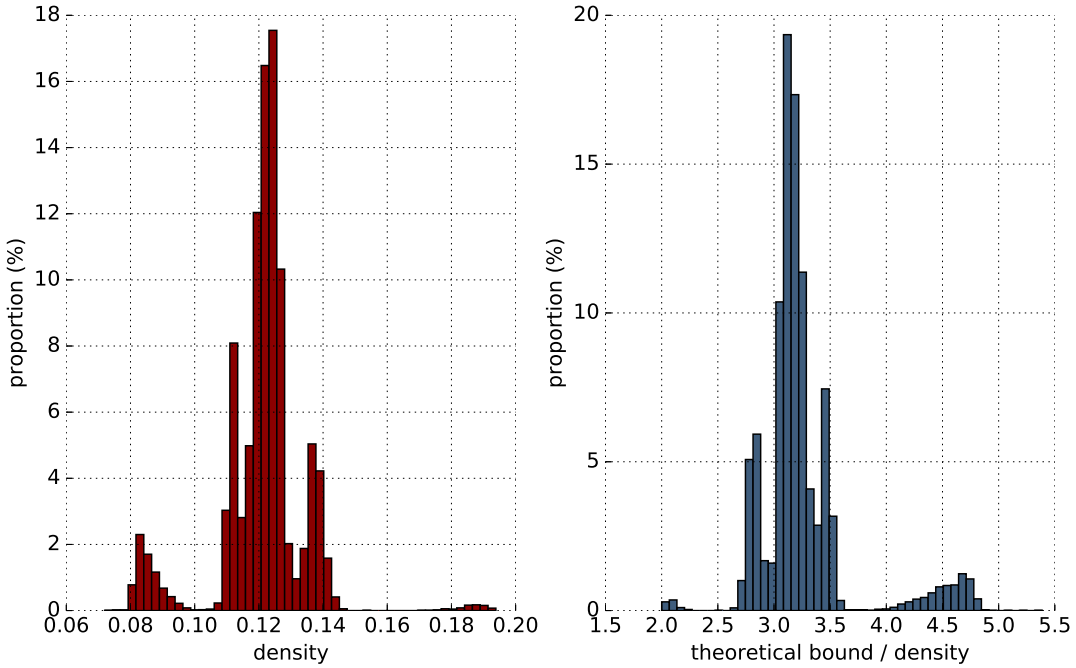


Fig. IV.8 – Densité des graphes associés aux 10916 réseaux parfaits de dimension 8 et comparaison avec la borne théorique (IV.2).

IV.3.3 Décoloration d'un graphe

La plupart des résultats de complexité sur les graphes concernent les graphes non colorés. C'est pourquoi nous rappelons ici un algorithme connu, très semblable à celui présenté dans le paragraphe précédent, permettant de « décolorer » un graphe tout en préservant ses

automorphismes et sa classe d'isomorphie.

IV.3.3.1 Principe

Pour tout $n \in \mathbb{N}$ dont la décomposition binaire est $n = \sum_{i=0}^{d} b_i 2^i$ avec $b_i \in \{0,1\}$, on note T_n l'arbre binaire de hauteur $d+1$ dans lequel, pour tout $0 \leqslant i \leqslant d$, chaque sommet de niveau i a $b_i + 1$ fils. La Figure IV.9 présente quelques exemples de tels arbres.

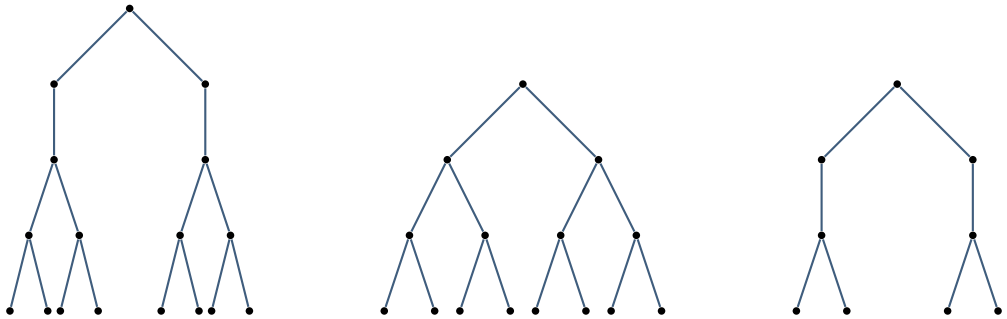


Fig. IV.9 – De gauche à droite, les arbres T_{13}, T_7 et T_6.

Soit G un graphe coloré. Comme dans le cas des graphes étiquetés, on suppose que, quitte à ordonner les couleurs de G, ces dernières sont $1, 2, \ldots, 2^d - 1$. Soit $G_\circ$ le graphe non coloré obtenu à partir de G en enracinant à chaque sommet de G de couleur i un arbre T_i. La Figure IV.10 présente un exemple de graphe $G_\circ$ obtenu à partir d'un graphe coloré G à 4 sommets et dont les couleurs sont $\{1,2,3\}$, ordonnées suivant l'ordre usuel sur $\mathbb{N}$.

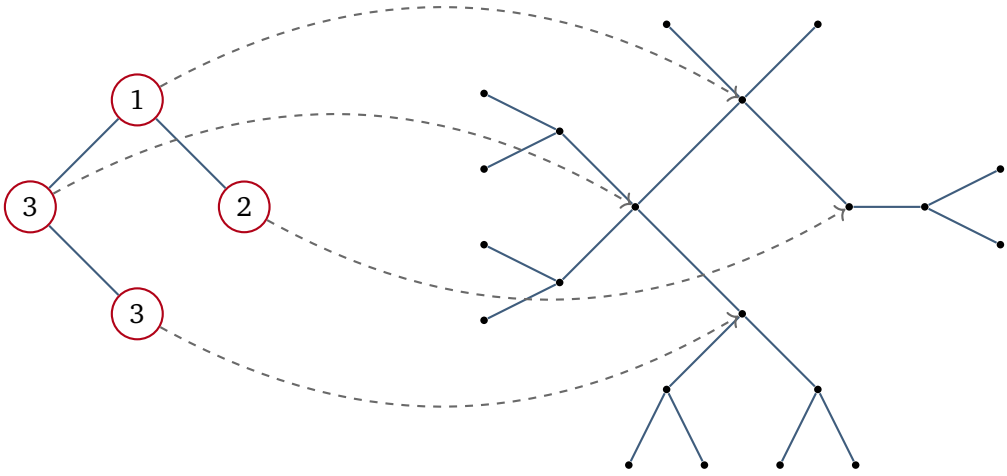


Fig. IV.10 – Exemple de décoloration d'un graphe.

IV.3.3.2 Réduction du cas coloré au cas général

En appliquant un raisonnement inductif sur la hauteur, on prouve que le passage de G à $G_\circ$ a les propriétés requises. Nous renvoyons le lecteur vers [Sch09, thm.1, p.21] pour une démonstration de ce résultat.

Proposition IV.3.14 *Soient G et H deux graphes colorés avec le même nombre de sommets et le même ensemble de couleurs.*

- *Les groupes* $\mathrm{Aut}(G)$ *et* $\mathrm{Aut}(G_\circ)$ *sont (explicitement) isomorphes.*
- *Les graphes colorés G et H sont isomorphes si et seulement si les graphes $G_\circ$ et $H_\circ$ le sont.*

La réduction recherchée entre le cas coloré et le cas général découle essentiellement du résultat précédent.

Théorème IV.3.15 *Les problèmes VLGI et VLGA sont réductibles en temps polynomial aux problèmes GI et GA respectivement. Plus précisément :*

- *Soient G et H deux graphes colorés à N sommets et ayant les mêmes m couleurs. Soit $d := \lfloor \log_2(m) \rfloor + 1$. Décider si G et H sont isomorphes se réduit en temps $O\left(dN^2\right)$ à décider si deux graphes à $O(Nm)$ sommets sont isomorphes.*
- *Soit G un graphe coloré à N sommets et m couleurs. Soit $d := \lfloor \log_2(m) \rfloor + 1$. Le calcul de* $\mathrm{Aut}(G)$ *se réduit en temps $O(dN^2)$ au calcul du groupe d'automorphisme d'un graphe à $O(Nm)$ sommets.*

Démonstration. L'algorithme suggéré dans la preuve du Théorème IV.3.11 permet de prouver les temps de réduction annoncés. Reste donc à montrer que si G est un graphe coloré à N sommets et m couleurs, le graphe $G_\circ$ possède $O(Nm)$ sommets. Le graphe $G_\circ$ est construit à partir de G en remplaçant chaque sommet de G par un arbre binaire de profondeur $d+1$. Cet arbre binaire possède au plus $2^{d+1}-1$ sommets, et ceci en comptant la racine, qui est un sommet du graphe initial. Le nombre de sommets du graphe $G_\circ$ est donc inférieur à

$$N(2^{d+1}-1) \leqslant N(2^{\log_2(m)+2}-1) = N(4m-1) = O(Nm),$$

ce qui termine la preuve. □

Cette réduction est une fois de plus polynomiale en le nombre de sommets du graphe initial : il ne peut pas y avoir plus de couleurs distinctes que de sommets.

IV.3.3.3 Densité de $G(\Lambda, \mathcal{B})_{\bullet\circ}$

Nous avons montré dans la Section IV.3.2.3 que si Λ est un réseau de $\mathbb{R}^n$ de base $\mathcal{B}$, le graphe étiqueté $G(\Lambda, \mathcal{B})_\bullet$ reste relativement creux, et ceci indépendamment de la paire $(\Lambda, \mathcal{B})$. Nous montrons dans ce paragraphe que cette propriété est préservée lors de la décoloration de $G(\Lambda, \mathcal{B})_\bullet$.

Lemme IV.3.16 *Soit $n \in \mathbb{N}$ dont la décomposition binaire est $n = \sum_{i=0}^{d} b_i 2^i$ avec $b_i \in \{0,1\}$ pour tout $0 \leqslant i \leqslant d$. Soit*

$$t_n := \sum_{i=0}^{d} \prod_{j=0}^{i-1} \big(b_j + 1\big).$$

L'arbre T_n possède t_n sommets et $t_n - 1$ arrêtes.

Démonstration. Par définition de l'arbre T_n, le résultat sur le nombre d'arrêtes est une conséquence de l'égalité sur le nombre de sommets. Pour tout $0 \leqslant i \leqslant d$, soit v_i le nombre de sommets au niveau i de T_n. Par construction, on a $v_0 = 1$ et $v_{i+1} = (b_i + 1)v_i$ pour tout $0 \leqslant i < d$. Une récurrence immédiate montre alors que

$$v_i = \prod_{j=0}^{i-1} \big(b_j + 1\big)$$

pour tout $0 \leqslant i \leqslant d$. Puisque le nombre de sommets T_n est égal à $\sum_{i=0}^{d} v_i$, le résultat est démontré. □

Dans un premier temps, on exprime de manière exacte mais peu explicite la densité de $G_\circ$. On déduit que lors du passage de G à $G_\circ$, la densité diminue forcément.

Proposition IV.3.17 *Soient G un graphe coloré et $G_\circ$ sa décoloration. On a $\rho(G_\circ) < \rho(G)$. Plus précisément, soient V l'ensemble des sommets de G et E l'ensemble de ses arrêtes. On suppose sans perte de généralité que les sommets de G sont colorés par une fonction $e_G : V \longrightarrow \mathbb{N}$. On a*

$$\rho(G_\circ) = \frac{2(|E| + t)}{(|V| + t)(|V| + t + 1)},$$

où

$$t := \sum_{v \in V} \big(t_{e_G(v)} - 1\big),$$

avec $t_{e_G(v)}$ la constante introduite dans le Lemme IV.3.16.

Démonstration. Soient $V_\circ$ l'ensemble des sommets de $G_\circ$ et $E_\circ$ l'ensemble de ses arrêtes. Le graphe $G_\circ$ est construit à partir de G en remplaçant chaque sommet $v \in V$ par l'arbre $T_{e_G(v)}$ qui comporte $t_{e_G(v)}$ sommets et $t_{e_G(v)} - 1$ arrêtes d'après le Lemme IV.3.16. Ainsi

$$|V_\circ| = \sum_{v \in V} t_{e_G(v)} = |V| + \sum_{v \in V} \big(t_{e_G(v)} - 1\big)$$

et, puisque les arrêtes de G sont conservées dans $G_\circ$,

$$|E_\circ| = |E| + \sum_{v \in V} \big(t_{e_G(v)} - 1\big).$$

Ainsi, la densité de $G_\circ$ est bien

$$\rho(G_\circ) = \frac{2|E_\circ|}{|V_\circ|(|V_\circ|+1)} = \frac{2(|E|+t)}{(|V|+t)(|V|+t+1)}.$$

Rappelons que la densité de G est donnée par

$$\rho(G) = \frac{2|E|}{|V|(|V|+1)}.$$

La fonction $x \mapsto \frac{2(|E|+x)}{(|V|+x)(|V|+x+1)}$ étant strictement décroissante sur $\mathbb{R}_{\geqslant 0}$, l'inégalité $\rho(G_\circ) < \rho(G)$ est démontrée. □

En particulier, on en déduit que les graphes $G(\Lambda, \mathcal{B})_{\bullet\circ}$ obtenus par conversion en graphe coloré puis décoloration des graphes étiquetés $G(\Lambda, \mathcal{B})$ restent relativement creux.

Corollaire IV.3.18 *Soit Λ un réseau de $\mathbb{R}^n$ de base $\mathcal{B} := (b_1, \dots, b_n)$. La densité de $G(\Lambda, \mathcal{B})_{\bullet\circ}$ est bornée indépendamment de la paire $(\Lambda, \mathcal{B})$, de l'ordre choisi sur les étiquettes de $G(\Lambda, \mathcal{B})$ et de l'ordre choisi sur les couleurs de $G(\Lambda, \mathcal{B})_\bullet$:*

$$\rho\left(G(\Lambda, \mathcal{B})_{\bullet\circ}\right) < \frac{2n+3}{6n+1}.$$

En particulier,

$$\rho\left(G(\Lambda, \mathcal{B})_{\bullet\circ}\right) < \frac{4}{13} + \frac{3}{6n+1}.$$

Démonstration. C'est une conséquence directe de la Proposition IV.3.13 et de la Proposition IV.3.17. □

IV.4 Quelques résultats de complexité

L'objectif de ce paragraphe est de rassembler les différentes réductions obtenues (résumées sur la Figure IV.11) afin d'obtenir une réduction des problèmes WLI/WLA aux problèmes GI/GA. Nous en déduisons des résultats de complexité inédits sur les problèmes WLI et WLA, ainsi que sur leur version non affaiblie. Puisque toutes les réductions obtenues sont exprimées en fonction du cardinal d'ensembles du type $S(\Lambda, \mathcal{B})$, nous présentons aussi des résultats sur la complexité du calcul de tels objets et des estimations de leur taille.

IV.4.1 Réduction de WLI/WLA à GI/GA et complexité

Rappelons que la complexité de la réduction du Théorème IV.3.5 est exprimée en nombre d'opérations arithmétiques. Dans tout ce qui suit, nous supposons que ces opérations sont effectués à temps constant, c'est-à-dire en temps $O(1)$. D'autre part, si $X := (x_1, \dots, x_k)$ est une famille d'éléments non nuls de $\mathbb{R}^n$, on note

$$\|X\|_\infty := \max_{1 \leqslant i \leqslant k} \|x_i\|,$$

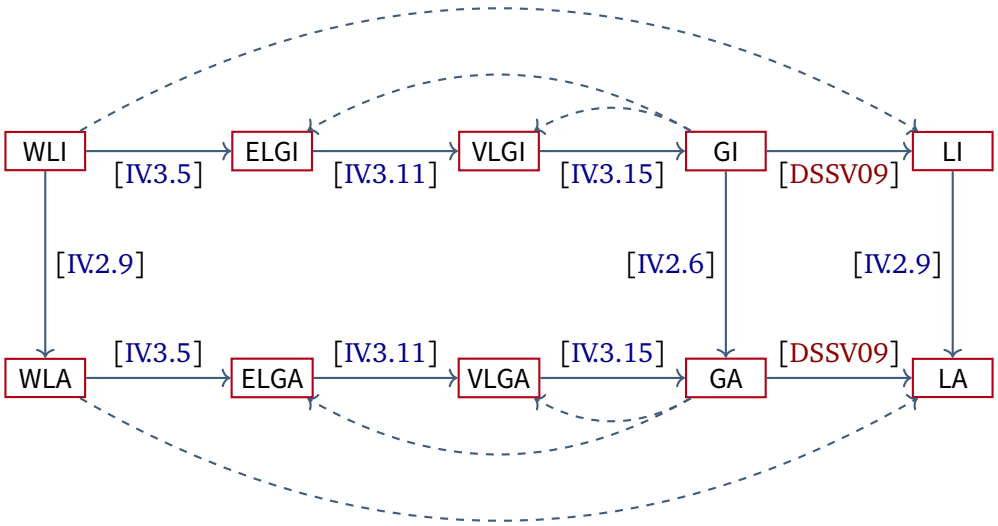


Fig. IV.11 – Résumé des réductions obtenues. Les flèches correspondent à des réductions polynomiales, les flèches en traits pointillés à des réductions triviales.

$$h(X) := \left\lfloor \log_2\left(2\|X\|_\infty^2 + 1\right)\right\rfloor + 1$$

et

$$h_2(X) := \left\lfloor \log_2(h(X))\right\rfloor + 1.$$

Théorème IV.4.1 *Les problèmes WLI et WLA sont réductibles en temps polynomial aux problèmes GI et GA respectivement. Plus précisément :*

- *Soient $\mathcal{B}$ et $\mathcal{B}'$ deux bases de $\mathbb{R}^n$. Supposons que les ensembles $S(\Lambda(\mathcal{B}), \mathcal{B})$ et $S(\Lambda(\mathcal{B}'), \mathcal{B})$ sont donnés et de même cardinal, noté s. Décider si $\Lambda(\mathcal{B})$ et $\Lambda(\mathcal{B}')$ sont isométriques est réductible en temps*

  $$O\left((n + h(\mathcal{B})h_2(\mathcal{B}))s^2\right)$$

  à décider si deux graphes à

  $$O\left(h(\mathcal{B})^2 s\right)$$

  sommets sont isomorphes.
- *Soit $\mathcal{B}$ une base de $\mathbb{R}^n$. Supposons donné l'ensemble $S(\Lambda(\mathcal{B}), \mathcal{B})$ et notons s son cardinal. Le calcul de $\mathrm{Aut}(\Lambda(\mathcal{B}))$ est réductible en temps*

  $$O\left((n + h(\mathcal{B})h_2(\mathcal{B}))s^2\right)$$

  au calcul du groupe d'automorphisme d'un graphe à

  $$O\left(h(\mathcal{B})^2 s\right)$$

  sommets.

Démonstration. On détaille la preuve pour WLA. Le même argument utilisé avec les problèmes WLI, ELGI, VLGI et GI permet de montrer la réduction de WLI à GI. En utilisant le Théorème IV.3.5, le Théorème IV.3.11 et le Théorème IV.3.15, le calcul du groupe d'automorphisme de Λ se réduit en temps

$$O\left(ns^2\right) + O\left(ns^2\right) + O\left(d'ds^2\right) = O\left((n + dd')s^2\right)$$

à celui de $G(\Lambda, \mathcal{B})_{\bullet\circ}$, un graphe à

$$O\left(d^2 s\right)$$

sommets, où d et d' sont respectivement le nombre de bits nécessaires pour représenter les étiquettes $G(\Lambda, \mathcal{B})$ et les couleurs de $G(\Lambda, \mathcal{B})_{\bullet}$. En vertu de l'inégalité de Cauchy-Schwarz, le nombre d'étiquettes distinctes dans $G(\Lambda, \mathcal{B})$ est inférieur à $2\|\mathcal{B}\|_\infty^2 + 1$, ce qui entraîne que $d \leqslant h(\mathcal{B})$. Par construction, il y a exactement d couleurs dans $G(\Lambda, \mathcal{B})_{\bullet}$, donc $d' = \lfloor \log_2(d) \rfloor + 1$. On a donc $d' \leqslant \lfloor \log_2(h(\mathcal{B})) \rfloor + 1 = h_2(\mathcal{B})$. Ces deux inégalités concluent la démonstration. □

Insistons encore une fois sur le fait que cette réduction n'est pas polynomiale en la dimension de Λ, mais en le cardinal de $S(\Lambda, \mathcal{B})$ et en $\|\mathcal{B}\|_\infty$. Une réduction polynomiale en la dimension est un résultat bien plus ardu à obtenir, qui nous est inaccessible à l'heure actuelle. En s'appuyant sur les travaux récent de Babai [Bab15] concernant la résolution du problème GI en temps quasi-polynomial , on déduit de la réduction précédente une borne de complexité pour le problème WLI :

Corollaire IV.4.2 *Le problème WLI est résoluble en temps quasi-polynomial. Plus précisément, soient $\mathcal{B}$ et $\mathcal{B}'$ deux bases de $\mathbb{R}^n$. Supposons que les ensembles $S(\Lambda(\mathcal{B}), \mathcal{B})$ et $S(\Lambda(\mathcal{B}'), \mathcal{B})$ sont donnés et de même cardinal, noté s. Il est possible de décider en temps*

$$O\left((n + h(\mathcal{B})h_2(\mathcal{B}))s^2\right) + \exp\left(\log\left(h(\mathcal{B})^2 s\right)^{O(1)}\right)$$

si $\Lambda(\mathcal{B})$ et $\Lambda(\mathcal{B}')$ sont isométriques.

Démonstration. Nous avons montré que WLI se ramène en temps $O\left((n + h(\mathcal{B})h_2(\mathcal{B}))s^2\right)$ à décider si deux graphes à $O\left(h(\mathcal{B})^2 s\right)$ sommets sont isomorphes. Puisque décider si deux graphes à N sommets sont isomorphes est possible en temps $\exp(\log(N)^{O(1)})$, le résultat est démontré. □

IV.4.2 Complexité du calcul de $S(\Lambda, \mathcal{B})$

Étant donnée une base $\mathcal{B} := (b_1, \ldots, b_n)$ d'un réseau Λ de $\mathbb{R}^n$, le calcul du graphe étiqueté $G(\Lambda, \mathcal{B})$ nécessite le calcul de l'ensemble

$$S(\Lambda, \mathcal{B}) = \bigcup_{i=1}^{n} \{x \in \Lambda \,:\, \|x\| = \|b_i\|\}.$$

Plusieurs algorithmes permettent de traiter ce problème, notamment l'algorithme énumératif de Fincke et Phost [FP85] et son amélioration par Kannan [Kan83], via le calcul de

$$\{x \in \Lambda \,:\, \|x\| \leqslant \|\mathcal{B}\|_\infty\}.$$

La meilleure analyse de complexité de ces algorithmes est due à Stehlé :

Théorème IV.4.3 ([Ste11, thm.8, p.35]) *Soient Λ un réseau de $\mathbb{R}^n$ de base $(b_1,\dots,b_n)$ et $C \in \mathbb{R}_{>0}$. L'ensemble $\{x \in \Lambda \,:\, \|x\| \leqslant C\}$ est calculable en moins de*

$$2^{O(n)} \prod_{i=1}^{n} \max\left(1, \frac{C}{\sqrt{n}\|b_i^*\|}\right)$$

opérations arithmétiques, où $(b_1^*,\dots,b_n^*)$ désigne l'orthogonalisation de Gram/Schmidt de $(b_1,\dots,b_n)$.

On déduit de ce résultat et du Théorème IV.4.1 des bornes de complexité pour LI et LA :

Corollaire IV.4.4

- *Soient $\mathcal{B} := (b_1,\dots,b_n)$ et $\mathcal{B}' := (b'_1,\dots,b'_n)$ deux bases de $\mathbb{R}^n$. Supposons que les ensembles $S(\Lambda(\mathcal{B}),\mathcal{B})$ et $S(\Lambda(\mathcal{B}'),\mathcal{B})$ sont de même cardinal, noté s. Décider si $\Lambda(\mathcal{B})$ et $\Lambda(\mathcal{B}')$ sont isométriques se réduit en temps*

$$2^{O(n)} \max\left(\prod_{i=1}^{n} \max\left(1, \frac{\|\mathcal{B}\|_\infty}{\sqrt{n}\|b_i\|}\right), \prod_{i=1}^{n} \max\left(1, \frac{\|\mathcal{B}\|_\infty}{\sqrt{n}\|b'_i\|}\right)\right) + O\left((n + h(\mathcal{B})h_2(\mathcal{B}))s^2\right)$$

  à décider si deux graphes à $O\left(h(\mathcal{B})^2 s\right)$ sommets sont isomorphes.
- *Soit Λ un réseau de $\mathbb{R}^n$ de base $\mathcal{B} := (b_1,\dots,b_n)$. Le calcul de $\mathrm{Aut}(\Lambda)$ se réduit en temps*

$$2^{O(n)} \prod_{i=1}^{n} \max\left(1, \frac{\|\mathcal{B}\|_\infty}{\sqrt{n}\|b_i\|}\right) + O\left((n + h(\mathcal{B})h_2(\mathcal{B}))s^2\right)$$

  au calcul du groupe d'automorphismes d'un graphe $O\left(h(\mathcal{B})^2 s\right)$ sommets, où $s := |S(\Lambda,\mathcal{B})|$.

IV.4.3 Estimations de $|S(\Lambda,\mathcal{B})|$

La plupart des bornes de complexité démontrées dans les paragraphes précédents sont exprimées en fonction de $|S(\Lambda,\mathcal{B})|$. Nous proposons ici plusieurs estimations de ces cardinaux.

Dans tout ce qui suit, on fixe Λ un réseau de $\mathbb{R}^n$ de base $\mathcal{B}$. On pose $s(\Lambda) := \frac{m(\Lambda)}{2}$, où $m(\Lambda)$ désigne le minimum de Λ. Pour tout $R > 0$ et tout $x \in \mathbb{R}^n$, on note $B_n(x,R)$ la boule fermée de $\mathbb{R}^n$ de centre x et rayon R, $\mathring{B}_n(x,R)$ son intérieur et $\partial B_n(x,R)$ son bord (c'est-à-dire la sphère de $\mathbb{R}^n$ de centre x et rayon R). Si μ_n est la mesure de Lebesgue n-dimensionnelle, on a

$$\mu_n(B_n(x,R)) = \mu_n(\mathring{B}_n(x,R)) = \frac{\pi^{n/2}R^n}{\Gamma\left(\frac{n}{2}+1\right)} \tag{IV.3}$$

et

$$\mu_{n-1}(\partial B_n(x,R)) = \frac{2\pi^{n/2}R^{n-1}}{\Gamma\left(\frac{n}{2}\right)}, \tag{IV.4}$$

où Γ est la *fonction gamma d'Euler*, définie pour $z \in \mathbb{C}$ tel que $\Re(z) > 0$ par

$$\Gamma(z) := \int_0^{+\infty} t^{z-1} e^{-t}\, dt.$$

Afin d'estimer une grandeur de la forme $|S(\Lambda, \mathcal{B})|$, deux approches sont possibles :

- En utilisant l'inégalité

$$|S(\Lambda, \mathcal{B})| \leqslant \sum_{i=1}^{n} |\Lambda \cap \partial B_n(0, \|b_i\|)|,$$

on se ramène au calcul du cardinal d'ensembles de la forme $\Lambda \cap \partial B_n(0,R)$ avec $R \geqslant 0$. Obtenir des estimations précises et explicites de ces cardinaux n'est pas une tâche facile, même pour le réseau $\mathbb{Z}^n$. C'est le problème de la *représentation d'entiers comme somme de carrés*. Citons par exemple le théorème de Hardy et Littlewood : pour $n \geqslant 5$ et $R \in \mathbb{Z}$, on a

$$|\mathbb{Z}^n \cap \partial B_n(0,R)| = \frac{\pi^{n/2} R^{n/2-1}}{\Gamma(\frac{n}{2})} \mathscr{S}(n,R) + O\left(R^{n/4}\right),$$

où $\mathscr{S}(n,R)$ est un terme appelé *série singulière*, définie par

$$\mathscr{S}(n,R) := \sum_{k=1}^{\infty} k^{-n} \sum_{h \in (\mathbb{Z}/k\mathbb{Z})^\times} G(h,k)^n e^{-2i\pi hR/k},$$

avec $G(h,k)$ une somme gaussienne :

$$G(h,k) := \sum_{l \in \mathbb{Z}/k\mathbb{Z}} e^{2i\pi hl^2/k}.$$

De plus, on a $|\mathbb{Z}^4 \cap \partial B_4(0,R)| = O(R)$, et des expressions exactes (mais complexes) sont connues en dimensions 2 et 3. Le lecteur intéressé par un panorama du problème de la représentation d'entiers comme somme de carrés pourra consulter [Gro12].

- Il est aussi possible de se ramener à l'étude de cardinaux du type $|\Lambda \cap B_n(0,R)|$ avec $R > 0$ en utilisant l'inclusion $S(\Lambda, \mathcal{B}) \subset \Lambda \cap B_n(0, \|\mathcal{B}\|_\infty)$. Encore une fois, même pour le réseau $\mathbb{Z}^n$, obtenir la meilleure approximation du cardinal de cet ensemble n'est pas aisé. Il s'agit de prouver la formule asymptotique

$$|\mathbb{Z}^n \cap B_n(0,R)| = \frac{\pi^{n/2} R^n}{\Gamma(\frac{n}{2}+1)} + O(R^{\varepsilon_n})$$

pour ε_n aussi petit que possible. Les cas 2-dimensionnel et 3-dimensionnel sont les plus étudiés. En effet, il est connu que $\varepsilon_n = n-2$ pour $n \geqslant 4$ et $\varepsilon_1 = 1$, mais il est conjecturé que $\varepsilon_2 = 1/2$ et $\varepsilon_3 = 1$. Les meilleurs bornes actuellement prouvées sont $\varepsilon_2 \leqslant 21/16$ et $\varepsilon_3 \leqslant 46/73$. Pour plus de détails sur ces résultats, voir par exemple [IL95 ; HB97].

Nous proposons dans ce paragraphe des estimations de $|\Lambda \cap B_n(0,R)|$ et de $|\Lambda \cap \partial B_n(0,R)|$ pour Λ un réseau arbitraire de $\mathbb{R}^n$ et $R > 0$. Dans un premier temps, évaluons $|\Lambda \cap B_n(0,R)|$ via une méthode géométrique naïve.

Proposition IV.4.5 *Soit $R \geqslant 0$. On a*

$$|\Lambda \cap B_n(0,R)| \leqslant \left(\frac{R}{s(\Lambda)} + 1\right)^n. \tag{IV.5}$$

En particulier, si $\mathcal{B}$ est une base de Λ :

$$|S(\Lambda, \mathcal{B})| \leqslant \left(\frac{\|\mathcal{B}\|_\infty}{s(\Lambda)} + 1\right)^n \tag{IV.6}$$

Démonstration. Les boules ouvertes $\mathring{B}_n(x, s(\Lambda))$ avec $x \in \Lambda \cap B_n(0,R)$ sont contenues dans $B_n(0, R + s(\lambda))$ et deux à deux disjointes par définition de $s(\Lambda)$. Ainsi :

$$\mu_n(B_n(0, R + s(\Lambda))) \geqslant \sum_{x \in \Lambda \cap B_n(0,R)} \mu_n(\mathring{B}_n(x, s(\Lambda))) = |\Lambda \cap B_n(0,R)| \mu_n(B_n(0, s(\Lambda))).$$

On en déduit l'inégalité annoncée à l'aide de (IV.3). □

Pour $R = m(\Lambda)$, la borne (IV.5) donne l'estimation $|S(\Lambda)| \leqslant 3^n - 1$ du nombre de vecteurs minimaux de Λ (une fois retiré le vecteur nul). Il s'avère qu'un raisonnement algébrique permet d'obtenir une meilleure estimation de $|S(\Lambda)|$. Nous reprenons ici la preuve de [Vor08, p.107–108].

Proposition IV.4.6 *Le nombre de vecteurs minimaux de Λ est borné par*

$$|S(\Lambda)| \leqslant 2^{n+1} - 2. \tag{IV.7}$$

Démonstration. Soient $x, y \in S(\Lambda)$. Supposons qu'il existe $t \in \Lambda$ tel que $y = x + 2t$. On a

$$\|y\|^2 = \|x + 2t\|^2 = \|x\|^2 + 4\|t\|^2 + 4\langle x \mid t \rangle,$$

ce qui entraîne que

$$\|x + t\|^2 + \|t\|^2 = \|x\|^2,$$

et donc en particulier, $\|x + t\|^2 \leqslant \|x\|^2$. Par définition du minimum de Λ, ceci n'est possible que si $x = -t$, c'est-à-dire si $y = -x$. Ainsi, deux éléments de $S(\Lambda)$ égaux dans $\Lambda/2\Lambda$ sont nécessairement opposés. Comme $S(\Lambda) \cap 2\Lambda = \emptyset$ et $|\Lambda/2\Lambda| = 2^n$, on a bien $|S(\Lambda)| \leqslant 2(2^n - 1) = 2^{n+1} - 2$. □

Nous proposons maintenant une estimation de $|\Lambda \cap \partial B_n(0,R)|$. Notons qu'elle est bien moins explicite que les précédentes puisqu'exprimée à l'aide d'une intégrale eulérienne.

Proposition IV.4.7 *Soit $R \geqslant 0$. On a*

$$|\Lambda \cap \partial B_n(0,R)| \leqslant \frac{2}{I\left(\eta_R; \frac{n-1}{2}, \frac{1}{2}\right)}, \tag{IV.8}$$

où :

- *$I(z;a,b)$ est la fonction bêta incomplète régularisée, définie pour tout $z \in \mathbb{R}$ et tous $a, b \in \mathbb{C}$ tels que $\Re(a) > 0$ et $\Re(b) > 0$ par*

$$I(z;a,b) := \frac{\int_0^z t^{a-1}(1-t)^{b-1}dt}{\int_0^1 t^{a-1}(1-t)^{b-1}dt}.$$

- *$\eta_R = \sin(\vartheta_R)^2$, où ϑ_R est la colattitude d'une calotte sphérique de la forme $B_n(x, s(\Lambda)) \cap \partial B_n(0,R)$ pour $x \in \partial B_n(0,R)$, donnée par*

$$\vartheta_R = \arccos\left(1 - \frac{s(\Lambda)^2}{2R^2}\right).$$

Démonstration. Par un argument similaire à celui employé pour prouver l'inégalité (IV.5), on montre que

$$|\Lambda \cap \partial B_n(0,R)| \leqslant \frac{\mu_{n-1}(\partial B_n(0,R))}{\mu_{n-1}(B_n(x,s(\Lambda)) \cap \partial B_n(0,R))}, \tag{IV.9}$$

où x est un point quelconque de $\partial B_n(0,R)$. En utilisant le fait que $y \in \partial B_n(0,R)$ est un élément de $B_n(x,s(\Lambda))$ si et seulement si $s(\Lambda)^2 \geqslant \|x-y\|^2 = \|x\|^2 + \|y\|^2 + 2\langle x \mid y\rangle = 2R^2 + 2\langle x \mid y\rangle$, on montre que

$$B_n(x,s(\Lambda)) \cap \partial B_n(0,R) = \left\{ y \in \partial B_n(0,R) \,:\, \frac{\langle x \mid y\rangle}{\|x\|\|y\|} \geqslant \cos(\vartheta_R) \right\}.$$

Ainsi, $B_n(x,s(\Lambda)) \cap \partial B_n(0,R)$ est une calotte sphérique de colattitude ϑ_R, et d'après [Li11, p.68], la mesure d'un tel ensemble est

$$\mu_{n-1}(B_n(x,s(\Lambda)) \cap \partial B_n(0,R)) = \frac{1}{2}\mu_{n-1}(\partial B_n(0,R)) I\left(\eta_R; \frac{n-1}{2}, \frac{1}{2}\right).$$

En utilisant cette égalité dans (IV.9), l'inégalité (IV.8) est démontrée. □

On déduit de ce résultat une borne sur $|S(\Lambda, \mathcal{B})|$:

Corollaire IV.4.8 *Si $\mathcal{B}$ est une base de Λ, on a*

$$|S(\Lambda,\mathcal{B})| \leqslant \frac{2n}{I\left(\eta_{\|\mathcal{B}\|_\infty}; \frac{n-1}{2}, \frac{1}{2}\right)}. \tag{IV.10}$$

Démonstration. La fonction $R \mapsto I(\eta_R; \frac{n-1}{2}, \frac{1}{2})$ est décroissante sur $\mathbb{R}_{\geqslant m(\Lambda)}$ pour tout $n \in \mathbb{N}_{>0}$. En effet, la fonction sinus est croissante sur $[0, \frac{\pi}{2}]$ et la fonction $R \mapsto \vartheta_R$ est décroissante sur $\mathbb{R}_{\geqslant m(\Lambda)}$ à valeur dans $[0, \arccos(\frac{7}{8})] \subset [0, \frac{\pi}{2}]$. Dès lors, on a d'après l'inégalité (IV.8)

$$|S(\Lambda, \mathcal{B})| \leqslant \sum_{i=1}^{n} |\Lambda \cap \partial B_n(0, \|b_i\|)| \leqslant \sum_{i=1}^{n} \frac{2}{I\left(\eta_{\|b_i\|}; \frac{n-1}{2}, \frac{1}{2}\right)} \leqslant \frac{2n}{I\left(\eta_{\|\mathcal{B}\|_\infty}; \frac{n-1}{2}, \frac{1}{2}\right)}.$$

Le résultat est démontré. □

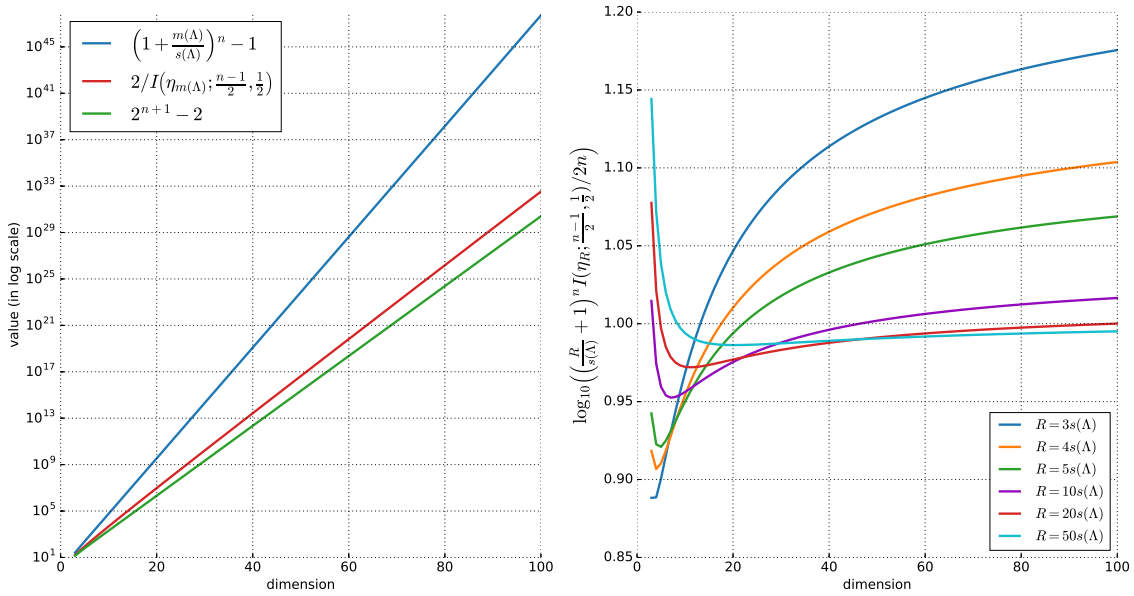


Fig. IV.12 – Comparaison des bornes obtenues. À gauche, les bornes (IV.5) et (IV.8) (pour $R = m(\Lambda)$), ainsi que la borne (IV.7) (échelle logarithmique). À droite, logarithme du rapport des bornes (IV.6) et (IV.10) pour différentes valeurs de $R = \|\mathcal{B}\|_\infty$.

La borne (IV.10) n'est pas complètement explicite ; il n'est pas évident de comparer théoriquement cette dernière avec la borne (IV.6). Néanmoins, les résultats expérimentaux présentés sur la Figure IV.12 permettent de tirer plusieurs conclusions :

- La borne (IV.8) fournit une estimation de $|S(\Lambda)|$ (*i.e.* pour $R = m(\Lambda)$) qui est proche de celle donnée par (IV.7), tout ayant l'avantage d'être valable pour tout $R \geqslant 0$. En revanche, la borne (IV.5) pour $R = m(\Lambda)$ est largement moins précise : le rapport entre (IV.5) et (IV.8) pour $n = 100$ et $R = m(\Lambda)$ est supérieur à 10^{20} ! Notons néanmoins que les bornes obtenues sont probablement très loin d'être optimales.
- Expérimentalement, on vérifie que la borne (IV.10) est meilleure que la borne (IV.6), et ceci indépendamment de la dimension sur réseau considéré et du rapport $\|\mathcal{B}\|_\infty / m(\Lambda)$.

IV.5 Extension aux réseaux algébriques

Le principe de la conversion d'un réseau euclidien en graphe étiqueté est adaptable au cas des réseaux algébriques. Nous détaillons cette adaptation dans le cadre du calcul des automorphismes d'un réseau algébrique et précisons ensuite les modifications à apporter afin de traiter le problème de l'isométrie pour les réseaux algébriques.

Le cadre de travail est celui introduit dans le Chapitre II : on fixe K un corps de nombres et on note $K_{\mathbb{R}}^n := (K \otimes_{\mathbb{Q}} \mathbb{R})^n$. Soit $\Omega := (\omega_1, \ldots, \omega_d)$ une $\mathbb{Q}$-base de K. Soient Λ un réseau algébrique de $K_{\mathbb{R}}^n$ et $\mathscr{B}$ une de ses pseudo-bases, donnée par $\mathcal{B} := (b_1, \ldots, b_n)$ une $K_{\mathbb{R}}$-base de $K_{\mathbb{R}}^n$ et $\mathfrak{A} := (\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$ une famille d'idéaux fractionnaires de K. Rappelons que d'après la Proposition III.2.2 démontrée dans le chapitre précédent, un $K_{\mathbb{R}}$-endomorphisme $f : K_{\mathbb{R}}^n \longrightarrow K_{\mathbb{R}}^n$ est un $K_{\mathbb{R}}$-automorphisme de Λ si et seulement si :

(i) $\langle f(\omega_k b_i) \,|\, f(\omega_l b_j)\rangle = \langle \omega_k b_i \,|\, \omega_l b_j\rangle$ pour tous $1 \leqslant i, j \leqslant n$ et $1 \leqslant k, l \leqslant d$.

(ii) $f(b_j) \in \Lambda_j$ pour tout $1 \leqslant j \leqslant n$, où $\Lambda_j = \bigoplus_{i=1}^n \mathfrak{a}_i \mathfrak{a}_j^{-1} b_i$.

La première condition impose l'orthogonalité de f. La seconde condition assure que f préserve Λ, et peut être reformulée par le fait que la colonne j de la matrice de f dans la base $(b_1, \ldots, b_n)$ est un élément de $\mathfrak{a}_1 \mathfrak{a}_j^{-1} \oplus \cdots \oplus \mathfrak{a}_n \mathfrak{a}_j^{-1}$. Comme dans la Section III.3.1, considérons pour tout $1 \leqslant j \leqslant n$ l'ensemble

$$S_j(\Lambda, \mathscr{B}, \Omega) := \left\{ x \in \Lambda_j \,:\, \langle \omega_k x \,|\, \omega_l x\rangle = \langle \omega_k b_j \,|\, \omega_l b_j\rangle \text{ pour tous } 1 \leqslant k, l \leqslant d \right\}.$$

Soit $S_j(\Lambda, \mathscr{B}, \Omega)$ l'union disjointe [6] :

$$S(\Lambda, \mathscr{B}, \Omega) := \bigsqcup_{j=1}^{n} S_j(\Lambda, \mathscr{B}, \Omega). \tag{IV.11}$$

C'est l'analogue de l'ensemble $S(\Lambda, \mathcal{B})$ de la situation euclidienne classique. L'importance d'utiliser ici une union *disjointe* sera expliquée plus loin. Nous avons déjà montré dans la Proposition III.3.2 que $S(\Lambda, \mathscr{B}, \Omega)$ est un ensemble fini.

On associe à l'ensemble $S(\Lambda, \mathscr{B}, \Omega)$ un graphe complet, étiqueté et coloré $G(\Lambda, \mathscr{B}, \Omega)$ dont les sommets sont les éléments de $S(\Lambda, \mathscr{B}, \Omega)$ et l'étiquette de l'arrête entre x et y est donnée par la matrice des produits scalaires $\langle \omega_k x \,|\, \omega_l y\rangle$ pour $1 \leqslant k, l \leqslant d$. Les sommets de $G(\Lambda, \mathscr{B}, \Omega)$ sont colorés suivant la décomposition (IV.11).

Théorème IV.5.1 *Les groupes* $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$ *et* $\mathrm{Aut}(G(\Lambda, \mathscr{B}, \Omega))$ *sont (explicitement) isomorphes.*

Démonstration. Le fait qu'un automorphisme de Λ induise un automorphisme de $G(\Lambda, \mathscr{B}, \Omega)$ résulte de la Proposition III.2.2. Comme l'ensemble $S(\Lambda, \mathscr{B}, \Omega)$ contient la $K_{\mathbb{R}}$-base $\mathcal{B}$, deux automorphismes distincts de Λ induisent deux automorphismes distincts de $G(\Lambda, \mathscr{B}, \Omega)$.

6. dans le sens de la somme dans la catégorie des ensembles.

Réciproquement, soit σ un automorphisme de $G(\Lambda, \mathscr{B}, \Omega)$. Soit f le $K_{\mathbb{R}}$-endomorphisme de $K_{\mathbb{R}}^n$ défini par $f(b_i) = \sigma(b_i)$ pour tout $1 \leqslant i \leqslant n$, où $\sigma(b_i)$ est calculé en considérant b_i comme élément de $S_i(\Lambda, \mathscr{B}, \Omega)$. Puisque σ préserve la coloration et les étiquettes de $G(\Lambda, \mathscr{B}, \Omega)$, f est un $K_{\mathbb{R}}$-automorphisme de Λ. Montrons que l'automorphisme de $G(\Lambda, \mathscr{B}, \Omega)$ induit par f coïncide avec σ. Soient $x \in S(\Lambda, \mathscr{B}, \Omega)$, $1 \leqslant i \leqslant n$ et $1 \leqslant k \leqslant d$. On note $b_i' = f(b_i) = \sigma(b_i)$. Puisque f est un $K_{\mathbb{R}}$-automorphisme orthogonal de $K_{\mathbb{R}}^n$, c'est en particulier un $\mathbb{R}$-automorphisme orthogonal du $\mathbb{R}$-espace euclidien $K_{\mathbb{R}}^n$, donc $f^{\intercal} = f^{-1}$. Ainsi

$$\langle f^{-1}(\omega_k b_i') \,|\, \omega_k x \rangle = \langle \omega_k b_i' \,|\, f(\omega_k x) \rangle = \langle \omega_k b_i' \,|\, \omega_k f(x) \rangle.$$

D'autre part, puisque σ préserve les étiquettes de $G(\Lambda, \mathscr{B}, \Omega)$, on a

$$\langle f^{-1}(\omega_k b_i') \,|\, \omega_k x \rangle = \langle \omega_k b_i \,|\, \omega_k x \rangle = \langle \omega_k b_i' \,|\, \omega_k \sigma(x) \rangle.$$

En remarquant que les $\omega_k b_i'$ forment pour $1 \leqslant i \leqslant n$ et $1 \leqslant k \leqslant d$ une $\mathbb{R}$-base de $K_{\mathbb{R}}^n$, on déduit de l'égalité $\langle \omega_k b_i' \,|\, \omega_k \sigma(x) \rangle = \langle \omega_k b_i' \,|\, \omega_k f(x) \rangle$ que $f(x) = \sigma(x)$. □

Considérons maintenant Λ' un autre réseau algébrique de $K_{\mathbb{R}}^n$. Deux réseaux algébriques $K_{\mathbb{R}}$-isométriques étant en particulier isomorphes, on suppose en vertu du Théorème II.3.12 que Λ et Λ' ont la même classe de Steinitz. Il existe donc une pseudo-base $\mathscr{B}'$ de Λ' formée de $\mathcal{B}' = (b_1', \ldots, b_n')$ une $K_{\mathbb{R}}$-base de $K_{\mathbb{R}}^n$ et de la famille d'idéaux fractionnaires $\mathfrak{A}$. Dès lors, on montre en adaptant la preuve précédente que :

Théorème IV.5.2 *Les réseaux algébriques Λ et Λ' sont $K_{\mathbb{R}}$-isométriques si et seulement si les graphes $G(\Lambda, \mathscr{B}, \Omega)$ et $G(\Lambda', \mathscr{B}', \Omega)$ sont isomorphes.*

Notons que le graphe $G(\Lambda, \mathscr{B}, \Omega)$ est à la fois coloré et étiqueté. Il faut donc prendre soin de conserver la coloration lors de la phase de désétiquetage. Il suffit pour cela de considérer une coloration donnée par le couple formée de la coloration initiale et du niveau des sommets dans $G(\Lambda, \mathscr{B}, \Omega)_\bullet$. La phase de décoloration est identique à celle du cas classique.

V

IMPLANTATIONS ET RÉSULTATS EXPÉRIMENTAUX

Sommaire

V.1 Introduction

La plupart des algorithmes que nous avons présentés dans les chapitres précédents ont été implantés ; nous partageons dans ce chapitre quelques détails sur ces implantations. Ces dernières ont été effectuées dans le langage C en utilisant de manière intensive la librairie PARI/gp [PARI/gp]. Nous prenons donc le soin de détailler quelques unes des structures et fonctions de cette librairie, notamment en ce qui concerne les corps de nombres, les réseaux et les formes quadratiques.

V.2 Corps de nombres et nombres algébriques dans PARI/gp

Nous rassemblons dans ce paragraphe quelques remarques et astuces concernant la représentation et la manipulation des corps de nombres et de leurs éléments dans PARI/gp. Nous renvoyons le lecteur avide de détails sur ces sujets vers la documentation officielle de PARI/gp, disponible à l'adresse `http://pari.math.u-bordeaux.fr/doc.html`.

V.2.1 Structures de corps de nombres

Soient $P \in \mathbb{Z}[X]$ un polynôme irréductible unitaire et $K := \mathbb{Q}[X]/(P)$ un corps de nombres. Il existe essentiellement deux [1] structures associées à K dans PARI/gp :

- La structure de corps de nombres standard, appelée `nf` et initialisée par `nfinit(P)`. Cette fonction calcule les données basiques du corps de nombres K, notamment sa signature, son discriminant, son anneau d'entiers $\mathcal{O}_K$ et les données nécessaires au calcul des plongements et de la norme T_2. La Figure V.2 présente les valeurs obtenues pour une telle structure associée à $\mathbb{Q}(i)$.
- La structure dite *de Buchmann*, appelée `bnf` et initialisée par `bnfinit(P)`. En plus de contenir toutes les données de la structure `nf`, `bnf` inclut en plus la structure des groupes Cl_K et $\mathcal{O}_K$. La Figure V.1 regroupe les informations sur ces groupes données par la structure `bnf` associée à $\mathbb{Q}(\sqrt{15})$.

Bien évidemment, la structure `bnf` est plus coûteuse à initialiser que la structure `nf`. N'ayant aucunement besoin de la structure de Cl_K ou de $\mathcal{O}_K^\times$ dans nos implantations, ni des autres invariants complexes associés à `bnf`, nous pouvons nous contenter de travailler avec des corps de nombres sous la forme `nf`. Précisons que si `K=nfinit(X^2+D)` avec $D \in \mathbb{N}_{>0}$, la base de $\mathcal{O}_K$ donnée par `K.zk` est $(1, \omega_D)$, où $\omega_D := i\sqrt{D}$ si $D \equiv 1, 2 \mod 4$ et $\omega_D := \frac{1-i\sqrt{D}}{2}$ sinon. Notons que PARI/gp propose aussi des fonctions et structures dédiées spécifiquement aux corps de nombres quadratiques, mais ces dernières sont plutôt à vocations arithmétiques qu'algébriques. En particulier, même dans le cadre de l'algorithme LLL que nous avons présenté dans le Chapitre I, nous préférons utiliser la structure `nf`.

1. Nous mettons de coté la structure associée aux corps de classes de rayons, bien plus générale.

```
? K = bnfinit(X^2-15);          // initialisation de la structure bnf
? K.nf == nfinit(X^2-15)        // structure nf sous-jacente
%2 = 1
? K.no                          // cardinal de Cl_K
%3 = 2
? K.cyc                         // diviseurs élémentaires de Cl_K
%4 = [2]
? K.gen                         // générateurs de Cl_K
%5 = [[2, 1; 0, 1]]
? K.tu[1]                       // cardinal de μ_K
%6 = 2
? K.tu[2]                       // générateur de μ_K
%7 = Mod(-1, X^2-15)
```

Fig. V.1 – Structure bnf associée à $\mathbb{Q}(\sqrt{15})$.

```
? K = nfinit(X^2+1);            // initialisation de la structure nf
? K.sign                        // signature
%2 = [0, 1]
? K.disc                        // discriminant
%3 = -4
? K.zk                          // base de O_K
%4 = [1, X]
? K[5][1]                       // valeurs des plongements des éléments de K.zk
%5 =
[1 0.E-38 + 1.00*I]
? K[5][2]                       // base du réseau associé à la forme T_2
%6 =
[1, 1.00; 1, -1.00]
? K[5][3]                       // matrice de Gram de T_2 sur K.zk
%7 =
[1, 1; 1, -1]
```

Fig. V.2 – Structure nf associée à $\mathbb{Q}(i)$.

PARI/gp ne dispose pas de structure ad-hoc destinée à la représentation et à la manipulation du produit tensoriel $K \otimes_{\mathbb{Q}} \mathbb{R}$. Ce n'est pas un réel problème : d'une part, un élément

$$\alpha = x_1 \otimes y_1 + \cdots + x_m \otimes y_m \in K \otimes_{\mathbb{Q}} \mathbb{R}$$

peut simplement être représenté par un vecteur `[[x1, y1], [x2, y2],...,[xm, ym]]` dans PARI/gp, et d'autre part, on peut tout simplement se ramener à ne manipuler que des éléments de K. En effet, tout au long de nos implantations, ce ne sont que des éléments des réseaux algébriques qui sont manipulés. En particulier, quitte à effectuer un changement de bases convenable, tous ces éléments peuvent être vus comme des vecteurs à coefficients dans K.

V.2.2 Nombres algébriques et idéaux fractionnaires

On considère toujours $K = \mathbb{Q}[X]/(P)$ avec $P \in \mathbb{Z}[X]$ irréductible et unitaire.

V.2.2.1 Représentations des éléments d'un corps de nombres

Soit $x \in K$. Le système PARI/gp propose deux représentations de x :

- x est représenté comme le vecteur colonne de ses coordonnées dans une $\mathbb{Q}$-base fixée de K, en l'occurrence la base `K.zk` calculée lors de l'initialisation de K à l'aide de la fonction `nfinit`. C'est la représentation en `t_COL`. Cette représentation est la plus pratique pour les calculs de plongements et de produit scalaire T_2 sur K. En effet, la structure `nf` contient la matrice de Gram de la forme T_2 sur la base `K.zk`, ainsi que les valeurs des plongements des éléments de cette base. Les calculs de la norme T_2 de x et de ses plongements se réduisent alors à de simples produits matriciels réels.
- x est vu comme un élément de $\mathbb{Q}[X]/(P)$ et il est représenté par un polynôme à coefficients rationnels modulo P. C'est la représentation en `t_POLMOD`. Cette forme est à privilégier pour les calculs d'algèbre linéaire sur K. En effet, les fonctions élémentaires d'algèbre linéaire de PARI/gp ne sont pas conçus pour manipuler des matrices dont les coefficients sont eux-mêmes des vecteurs (lignes ou colonnes), mais peuvent prendre en charge des matrices à coefficients polynomiaux [2]

Notons que PARI/gp dispose de fonctions de conversion (`nfbasistoalg` et `nfalgtobasis`) d'une représentation à l'autre. La Figure V.3 présente quelques exemples de conversion entre ces deux formes.

```
? K = nfinit(X^2+1);          // initialisation de la structure nf
? x = Mod(3*X+7, X^2+1);      // forme t_POLDMOD
? y = nfalgtobasis(K, x)      // conversion en forme t_COL
%3 = [7, 3]~
? nfbasistoalg(K, y)          // conversion en forme t_POLMOD
%4 = Mod(3*X+7, X^2+1)
? K.zk*y                      // y = coordonnées de x dans la base K.zk
%5 = 3*X+7
```

Fig. V.3 – Représentations des éléments de $\mathbb{Q}(i)$.

Il s'avère qu'appeler fréquemment ces fonctions ralentit considérablement les algorithmes. C'est pourquoi il est nécessaire de réduire au maximum le nombre de conversions effectués.

V.2.2.2 Représentations des idéaux fractionnaires

Il existe essentiellement trois représentations d'un idéal fractionnaire $\mathfrak{a}$ de K dans PARI/gp :

2. L'algèbre linéaire sur des matrices dont les coefficients sont des `t_COL` est néanmoins supportée dans une version de développement de PARI/gp.

- On représente $\mathfrak{a}$ par une matrice carrée de taille $[K : \mathbb{Q}]$, dont les colonnes sont des éléments de K au format `t_COL` formant une $\mathbb{Z}$-base de $\mathfrak{a}$. Cette matrice est toujours en forme normale de Hermite.
- Puisque $\mathcal{O}_K$ est un anneau de Dedekind, pour tout $x \in \mathfrak{a}$ non nul, il existe $y \in \mathfrak{a}$ tel que $\mathfrak{a} = (x, y) = \mathcal{O}_K x + \mathcal{O}_K y$. On peut donc représenter $\mathfrak{a}$ par la paire (x, y). Notons que même si $\mathfrak{a}$ est un idéal principal, y n'est pas forcément nul dans cette représentation ; `PARI/gp` dispose d'une fonction dédiée permettant de trouver un générateur (le cas échéant) d'un idéal principal, mais celle-ci nécessite l'utilisation de la structure de corps de nombres `bnf`.
- On représente $\mathfrak{a}$ par sa factorisation en produit d'idéaux premiers, tout comme on peut représenter un entier par sa factorisation en produit de nombres premiers.

La Figure V.4 présente quelques exemples de ces représentations et des fonctions de conversion associées.

```
? K = nfinit(X^2+1);          // initialisation de la structure nf
? x = Mod(3*X+7, X^2+1);
? a = idealhnf(K,x)           // forme normale de Hermite de a := (3i + 7)
%3 =
[58 41]                       // a = Z58 ⊕ Z(41 + i)
[ 0  1]
? idealtwoelt(K,a)            // représentation de a par deux éléments
%4 = [58, [41, 1]~]           // a = (58, 41 + i)
? idealfactor(K,a)            // factorisation de a
%5 =                          // a = (2, 1 + i)^2 · (29, 12 + i)
[      [2, [1, 1]~, 2, 1, [1, -1; 1, 1]] 1]
[[29, [12, 1]~, 1, 1, [-12, -1; 1, -12]] 1]
? K = bnfinit(X^2+1);         // initialisation de la structure bnf
? bnfisprincipal(K,a)         // a est-il principal ?
%7 [[]~, [7, 3]~]             // oui, et a = (3i + 7)
```

Fig. V.4 – Représentations des idéaux fractionnaires de $\mathbb{Q}(i)$.

Dans le cadre de l'algorithme de réduction LLL du Chapitre I, la question de la représentation des idéaux fractionnaires ne se pose pas. En effet, nous nous sommes limités à ne considérer que des réseaux algébriques libres (et généralement sur des corps de nombres dont l'anneau des entiers est principal), dans lesquels les seuls idéaux fractionnaires qui apparaissent sont triviaux. Au contraire, nous ne nous sommes pas restreints aux réseaux algébriques libres dans le cadre de la généralisation de l'algorithme de Plesken et Souvignier présentée dans le Chapitre III. Néanmoins, les idéaux fractionnaires n'y jouent qu'un rôle secondaire ; ils n'interviennent qu'au moment du calcul des vecteurs courts d'un réseau algébrique. En effet, afin d'effectuer ce calcul, nous identifions un réseau algébrique à un réseau euclidien (voir la Section V.4.1.1), ce qui nécessite de connaître une $\mathbb{Z}$-base des idéaux fractionnaires apparaissant dans la pseudo-base du réseau considéré. La représentation en forme normale de Hermite est donc la plus judicieuse

puisqu'elle fournit directement de telles bases. Quoi qu'il en soit, le surcoût engendré par la conversion des idéaux fractionnaires de n'importe quel format vers ce format matriciel est négligeable comparé au coût total de l'algorithme présenté.

V.3 Algorithme LLL sur $\mathbb{Q}(i\sqrt{D})$

Soit $K := \mathbb{Q}(i\sqrt{D})$ avec $D \in \{1, 2, 3, 7, 11\}$. L'implantation de l'algorithme LLL sur K que nous proposons est exactement celle décrite dans le Chapitre I. En particulier, cette implantation est élémentaire et est loin d'atteindre la sophistication et l'efficacité des versions actuellement utilisées dans le cas classique, comme le *Floating-point LLL* (voir [Ste09]), aujourd'hui exploité par les fonctions `qflll` et `qfllgram` de `PARI/gp`. Néanmoins, même dans le cadre de cette implantation naïve, deux points méritent d'être abordés : la gestion de l'identification $K \subset \mathbb{C}$ et le calcul de l'élément de $\mathcal{O}_K$ le plus proche d'un nombre complexe donné. Cette implantation a été réalisé dans le langage `C` à l'aide de la librairie `PARI`, et n'utilise donc pas l'interface gp de `PARI/gp`.

Fixons $\Lambda \subset \mathbb{C}^n$ un $\mathcal{O}_K$-réseau de base $\mathcal{B} := (b_1, \ldots, b_n)$.

V.3.1 Conversions entre K et $\mathbb{C}$

Le produit hermitien usuel de $\mathbb{C}^n$ est à valeurs dans K sur $K^n \times K^n$. En particulier, si $\Lambda \subset K^n$ (ce qui revient à demander que $b_i \in K^n$ pour tout $1 \leqslant i \leqslant n$), tous les calculs liés à l'algorithme LLL peuvent être effectués dans K. Ces calculs sont donc exécutés dans $\mathbb{Q}^n$ ou $\mathbb{Q}[x]/(X^2+D)$ par `PARI/gp` (suivant la représentation choisie). Au contraire, si $\Lambda \nsubseteq K^n$, les calculs sont effectués dans $\mathbb{C}$ (donc en particulier seulement à une précision fixée). Il est pour cela pratique de disposer de fonctions de conversion permettant de représenter un élément de K dans la $\mathbb{R}$-base $(1, i)$ et de représenter un élément de $\mathbb{C}$ dans la $\mathbb{R}$-base $(1, \omega_D)$ de $\mathbb{C}$ (qui est une $\mathbb{Q}$-base de K), où

$$\omega_D := \begin{cases} i\sqrt{D} & \text{si } D \equiv 1, 2 \mod 4, \\ \frac{1-i\sqrt{D}}{2} & \text{sinon.} \end{cases}$$

Ces fonctions de conversion (qui sont bien évidemment élémentaires) sont particulièrement utiles au moment de déterminer $\lfloor z \rceil \in \mathcal{O}_K$ avec $z \in \mathbb{C}$ (voir la prochaine section), essentiellement car il n'est pas complètement trivial de caractériser les éléments de $\mathcal{O}_K$ dans une base autre que celle de $\mathcal{O}_K$.

Soit $z := x + iy \in \mathbb{C}$ avec $x, y \in \mathbb{R}$. On a

$$z = \begin{cases} x + \omega_D \frac{y}{\sqrt{D}} & \text{si } D \equiv 1, 2 \mod 4, \\ \left(x - \frac{y}{\sqrt{D}}\right) + \omega_D \left(\frac{-2y}{\sqrt{D}}\right) & \text{sinon.} \end{cases}$$

Réciproquement, si $z := x + \omega_D y$ avec $x, y \in \mathbb{R}$, on a

$$z = \begin{cases} x + i(y\sqrt{D}) & \text{si } D \equiv 1,2 \mod 4, \\ \left(x + \frac{y}{2}\right) + i\left(\frac{-y\sqrt{D}}{2}\right) & \text{sinon.} \end{cases}$$

On déduit les procédures de conversion de ces deux égalités.

V.3.2 Approximations par les éléments de $\mathcal{O}_K$

L'opération permettant d'obtenir la première condition de LLL-réduction (LLL1) est de la forme $b_i \leftarrow b_i - \lfloor z \rceil b_j$, où $z \in \mathbb{C}$ et $\lfloor z \rceil$ désigne un élément de $\mathcal{O}_K$ tel que $|z - \lfloor z \rceil|^2 \leqslant \eta_K$. Cette opération est implantée par la fonction SWAP (Algorithme I.4). Déterminer $\lfloor z \rceil$ est plus aisé si z est exprimé dans la $\mathbb{R}$-base $(1, \omega_D)$ plutôt que dans la $\mathbb{R}$-base $(1, i)$, essentiellement car il est plus pratique d'exprimer les éléments de $\mathcal{O}_K$ dans la première base que dans la seconde. Supposons donc que $z = x + \omega_D y$ avec $x, y \in \mathbb{R}$.

Si $D \equiv 1,2 \mod 4$, on a $\lfloor z \rceil = \lfloor x \rceil + \omega_D \lfloor y \rceil$, où pour tout $t \in \mathbb{R}$, on désigne par $\lfloor t \rceil$ l'élément de $\mathbb{Z}$ le plus proche de t, c'est-à-dire [3] :

$$\lfloor t \rceil := \begin{cases} \lfloor t \rfloor & \text{si } \lfloor t \rfloor \leqslant t \leqslant \lfloor t \rfloor + \frac{1}{2}, \\ \lceil t \rceil & \text{si } \lfloor t \rfloor + \frac{1}{2} < t < \lceil t \rceil + 1. \end{cases}$$

En effet, dans ce cas, on a $\omega_D = i\sqrt{D}$ et

$$\left|(x - \lfloor x \rceil) + \omega_D (y - \lfloor y \rceil)\right|^2 = (x - \lfloor x \rceil)^2 + D(y - \lfloor y \rceil)^2 \leqslant \frac{D+1}{4} = \eta_K.$$

Si $D \equiv 3 \mod 4$, il est plus délicat de déterminer $\lfloor z \rceil$. Néanmoins, on vérifie que

$$\lfloor z \rceil \in \left\{\lfloor x \rfloor + \omega_D \lfloor y \rfloor, \lceil x \rceil + \omega_D \lfloor y \rfloor, \lfloor x \rfloor + \omega_D \lceil y \rceil, \lceil x \rceil + \omega_D \lceil y \rceil\right\}$$

Afin de déterminer $\lfloor z \rceil$, nous nous sommes contenté de déterminer les quatre éléments de cet ensemble, et de choisir celui qui est le plus proche de z.

V.4 Extension de l'algorithme de Plesken et Souvignier

Il est relativement aisé d'implanter naïvement les modifications de l'algorithme de Plesken et Souvignier que nous avons présentées dans le Chapitre III. Néanmoins, sans plusieurs astuces et optimisations, une telle implantation ne sera fonctionnelle et efficace que sur une proportion restreinte de réseaux algébriques. Ces optimisations sont ici détaillées dans le cadre de l'algorithme présenté dans la première partie du Chapitre III. Elles sont facilement adaptables dans le cadre de l'équivalence congruentielle de formes quadratiques et de formes de Humbert.

3. Il y a ambiguïté pour $t = \lfloor t \rfloor + \frac{1}{2}$; nous faisons le choix dans cette situation d'attribuer la valeur $\lfloor t \rfloor$ à $\lfloor t \rceil$.

Comme pour l'algorithme LLL, notre implantation a été effectuée dans le langage C à l'aide de la libraire PARI. En particulier, nous n'utilisons pas l'interface gp. Néanmoins, dans un objectif de simplicité et de lisibilité, les sections qui suivent sont illustrées d'exemples calculés avec l'interface gp.

Soient $\Lambda = \mathfrak{a}_1 b_1 \oplus \cdots \oplus \mathfrak{a}_n b_n$ un réseau algébrique de $K_{\mathbb{R}}^n$ et $\Omega := (\omega_1, \ldots, \omega_d)$ une $\mathbb{Q}$-base intégrale de K. On note $\mathscr{B}$ la pseudo-base formée des idéaux fractionnaires $\mathfrak{a}_i$ et des vecteurs b_i pour $1 \leqslant i \leqslant n$. Résumons sommairement le déroulement de l'algorithme dans le cadre du calcul du groupe $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$:

1. Précalcul des ensembles $S_j(\Lambda, \mathscr{B}, \Omega)$ pour $1 \leqslant j \leqslant n$ (Section III.3.1).
2. Précalcul de l'empreinte de la pseudo-base $\mathscr{B}$ (Section III.3.2.1).
3. Précalcul des combinaisons scalaires associées à $\mathscr{B}$ (Section III.3.2.2).
4. Réduction au calcul de certains $K_{\mathbb{R}}$-automorphismes de Λ par des méthodes issues de l'algorithmique des groupes de permutation (Section III.4).
5. Calcul individuel des $K_{\mathbb{R}}$-automorphismes de Λ : prolongement d'un candidat et méthodes de *backtracking* (Section III.3.3).

Nous détaillons l'implantation de certaines de ces étapes dans la suite de cette section.

V.4.1 Gestion des vecteurs courts d'un réseau algébrique

V.4.1.1 Calcul pratique

Afin d'utiliser la méthode de Plesken et Souvignier pour déterminer le groupe $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$, nous avons expliqué dans la Section III.3.1 qu'il est nécessaire de précalculer les ensembles $S_j(\Lambda, \mathscr{B}, \Omega)$, définis pour tout $1 \leqslant i \leqslant n$ par

$$S_j(\Lambda, \mathscr{B}, \Omega) := \left\{ x \in \Lambda_j \ : \ \langle \omega_k x \,|\, \omega_l x \rangle = \langle \omega_k b_j \,|\, \omega_l b_j \rangle \ \forall\, 1 \leqslant k, l \leqslant d \right\},$$

où $\Lambda_j := \mathfrak{a}_1 \mathfrak{a}_j^{-1} b_1 \oplus \cdots \oplus \mathfrak{a}_n \mathfrak{a}_j^{-1} b_n$ est un réseau algébrique de $K_{\mathbb{R}}^n$. Afin de calculer ces ensembles, on utilise l'inclusion (III.1) :

$$S_j(\Lambda, \mathscr{B}, \Omega) \subset \omega_1^{-1} \cdot \left\{ y \in \omega_1 \Lambda_j \ : \ 0 < \|y\|^2 \leqslant \|\omega_1 b_j\|^2 \right\}.$$

Notons qu'il est toujours possible de supposer que $\omega_1 = 1$, même en imposant des conditions de réduction sur la base Ω (voir [Bel04, §4.3, p.28–29]). De plus, la fonction `nfinit` de PARI/gp permettant d'initialiser un corps de nombres renvoie toujours une base intégrale LLL-réduite Ω telle que $\omega_1 = 1$. C'est pourquoi nous ferons l'hypothèse $\omega_1 = 1$ dans la suite de ce paragraphe.

Nous nous sommes finalement ramenés à la détermination d'ensembles de la forme

$$\{ x \in \Lambda \ : \ 0 < \|x\|^2 \leqslant c \}$$

avec $\Lambda \subset K_{\mathbb{R}}^n$ un réseau algébrique et $c \in \mathbb{R}_{>0}$. S'il est pour cela théoriquement possible d'adapter la méthode énumérative de Fieker et Pohst [FP96, algo.1, p.135], cet algorithme n'est actuellement pas implanté dans PARI/gp (ni dans MAGMA [MAGMA]). Il est donc nécessaire d'utiliser

la méthode classique permettant de résoudre ce problème pour les réseaux euclidiens : l'algorithme de Fincke et Pohst [FP85, algo.2.12, p.466], implanté notamment par la fonction `qfminim` dans `PARI/gp`.

La fonction `qfminim` prend en entrée une matrice $Q \in \mathrm{S}_n^{>0}(\mathbb{R})$ et un réel $c > 0$ et renvoie l'ensemble [4] $\{X \in \mathbb{Z}^n : 0 < X^\intercal Q X \leqslant c\}$. Pour l'utiliser, il nous faut donc identifier Λ à une matrice réelle symétrique définie positive. Pour cela, on utilise la Proposition II.3.8 : si $(\mathfrak{a}_i, b_i)_{1\leqslant i\leqslant n}$ une pseudo-base de Λ et si pour tout $1 \leqslant i \leqslant n$, $(\omega_1^{(i)}, \dots, \omega_d^{(i)})$ est une $\mathbb{Z}$-base de $\mathfrak{a}_i$, la famille $(\omega_j^{(i)} b_i)_{1\leqslant j\leqslant d}^{1\leqslant i\leqslant m}$ est une base de Λ vu comme réseau euclidien de $K_{\mathbb{R}}^n$. Dès lors, les image des $\omega_j^{(i)} b_i$ par l'isométrie Ψ introduite dans la Section II.2.1 forment une base $B \in \mathrm{GL}_{nd}(\mathbb{R})$ d'un réseau euclidien $\Lambda_{\mathbb{R}}$ de $\mathbb{R}^{nd}$ isométrique à Λ. La matrice de Gram P de la base standard de $\mathbb{R}^{nd}$ (pour le produit scalaire induit par la norme T_2 sur $K_{\mathbb{R}}^n$) est la matrice diagonale dont les nr premiers coefficients sont égaux à 1 et les $2ns$ suivant à 2. La matrice $Q := B^\intercal P B$ est symétrique définie positive. On calcule $\{X \in \mathbb{Z}^{nd} : X^\intercal Q X \leqslant c\}$ à l'aide de `qfminim`. Bien évidemment, il y a une bijection

$$\begin{array}{ccc} \{X \in \mathbb{Z}^{nd} : 0 < X^\intercal Q X \leqslant c\} & \longrightarrow & \{x \in \Lambda_{\mathbb{R}} : 0 < \|x\|^2 \leqslant c\} \\ X & \longmapsto & BX \end{array}$$

Finalement, l'ensemble $\{x \in \Lambda : 0 < \|x\|^2 \leqslant c\}$ est obtenu en calculant l'image réciproque par Ψ des éléments de $\{x \in \Lambda_{\mathbb{R}} : \|x\|^2 \leqslant c\}$.

Notons que dans cette situation, il est possible et intéressant de se passer du calcul de l'inverse de Ψ. En effet, un vecteur $X \in \mathbb{Z}^{nd}$ peut être vu comme le vecteur des coordonnées dans la base B d'un vecteur de $\Lambda_{\mathbb{R}}$. Ainsi, plutôt que de calculer $\Psi^{-1}(BX)$, on calcule $\Psi^{-1}(B)\widetilde{X}$, où $\widetilde{X}$ est obtenu par une réindexation convenable des composantes de X. La base $\Psi^{-1}(B)$ est connue : par construction, c'est la famille formée des $\omega_j^{(i)} b_i$. De plus, cette stratégie permet d'éviter le problème de précision lié au fait que la matrice B soit une matrice réelle : le résultat du produit BX est un vecteur réel, seulement représenté à précision fixée en machine. De plus, Ψ est généralement facile à inverser sur K^n, mais il est autrement plus délicat de l'inverser sur $K_{\mathbb{R}}^n$, toujours pour des problèmes de précision.

Exemple V.4.1 Le premier exemple présenté est très simple : les deux méthodes décrites précédemment fonctionnent et renvoient le même résultat. Prenons $K := \mathbb{Q}(i)$, $c := 4$ et

$$\Lambda := \mathcal{O}_K \begin{pmatrix} i \\ 0 \end{pmatrix} \oplus \mathcal{O}_K \begin{pmatrix} 0 \\ 2 \end{pmatrix} \subset \mathbb{Q}(i)^2.$$

L'isométrie Ψ est ici très facile à exprimer :

$$\begin{array}{rccc} \Psi : & \mathbb{Q}(i)_{\mathbb{R}}^2 & \longrightarrow & \mathbb{R}^4 \\ & \begin{pmatrix} x + iy \otimes \alpha \\ x' + iy' \otimes \alpha \end{pmatrix} & \longmapsto & \begin{pmatrix} \alpha x \\ \alpha y \\ \alpha' x' \\ \alpha' y' \end{pmatrix} \end{array}.$$

4. En réalité, un seul vecteur par paire de la forme $(+x, -x)$ est renvoyé par cette fonction.

En prenant $(1, i)$ comme $\mathbb{Q}$-base intégrale de K, on a

$$\Lambda = \mathbb{Z}\begin{pmatrix} i \\ 0 \end{pmatrix} \oplus \mathbb{Z}\begin{pmatrix} -1 \\ 0 \end{pmatrix} \oplus \mathbb{Z}\begin{pmatrix} 0 \\ 2 \end{pmatrix} \oplus \mathbb{Z}\begin{pmatrix} 0 \\ 2i \end{pmatrix}.$$

Ainsi, le réseau $\Lambda_{\mathbb{R}}$ de $\mathbb{R}^4$ associé à Λ a pour base

$$B := \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$

La signature de K étant $(0, 1)$, la matrice de Gram P de la base standard de $\mathbb{R}^4$ est

$$P := \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$

Ainsi, la matrice symétrique définie positive associée à Λ est

$$Q := B^{\intercal} P B = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 8 & 0 \\ 0 & 0 & 0 & 8 \end{pmatrix}.$$

Le résultat de `qfminim(Q,4)` est

$$\{X \in \mathbb{Z}^4 \,:\, 0 < X^{\intercal} Q X \leqslant 4\} = \pm \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

On obtient ainsi

$$\{x \in \Lambda_{\mathbb{R}} \,:\, 0 < \|x\|^2 \leqslant 4\} = B \cdot \{X \in \mathbb{Z}^4 \,:\, 0 < X^{\intercal} Q X \leqslant 4\} = \pm \begin{pmatrix} -1 & -1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

et finalement

$$\{x \in \Lambda \,:\, 0 < \|x\|^2 \leqslant 4\} = \Psi^{-1}\big(\{x \in \Lambda_{\mathbb{R}} \,:\, 0 < \|x\|^2 \leqslant 4\}\big) = \pm \begin{pmatrix} -1+i & -1 & 1+i & i \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

On peut se passer de calculer l'inverse de Ψ : à un vecteur $X := (x_1, x_2, x_3, x_4) \in \mathbb{Z}^n$, on associe directement l'élément $x_1 b_1 + i x_2 b_1 + x_3 b_2 + i x_4 b_2 \in \Lambda$.

Exemple V.4.2 Plaçons nous maintenant dans un cas moins trivial où des problèmes de précisions peuvent apparaître. Prenons pour K le corps quadratique $\mathbb{Q}(\zeta)$ avec $\zeta := \frac{-1+i\sqrt{3}}{2}$ et $c = \frac{5}{2}$. Soit

$$\Lambda := \mathcal{O}_K \begin{pmatrix} \zeta \otimes \pi \\ 1 \end{pmatrix} \oplus \mathcal{O}_K \begin{pmatrix} 1 \\ 0 \end{pmatrix} \subset \mathbb{Q}(\zeta)^2_{\mathbb{R}}.$$

En prenant $(1, \zeta)$ comme $\mathbb{Q}$-base intégrale de $\mathbb{Q}(\zeta)$, on a

$$\begin{aligned} \Lambda &= \mathbb{Z} \begin{pmatrix} \zeta \otimes \pi \\ 1 \end{pmatrix} \oplus \mathbb{Z} \begin{pmatrix} \zeta^2 \otimes \pi \\ \zeta \otimes 1 \end{pmatrix} \oplus \mathbb{Z} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \oplus \mathbb{Z} \begin{pmatrix} \zeta \otimes 1 \\ 0 \end{pmatrix} \\ &= \mathbb{Z} \begin{pmatrix} \zeta \otimes \pi \\ 1 \end{pmatrix} \oplus \mathbb{Z} \begin{pmatrix} -1-\zeta \otimes \pi \\ \zeta \otimes 1 \end{pmatrix} \oplus \mathbb{Z} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \oplus \mathbb{Z} \begin{pmatrix} \zeta \otimes 1 \\ 0 \end{pmatrix}. \end{aligned}$$

Dans cette situation, l'isométrie Ψ reste encore facile à décrire :

$$\begin{array}{rccc} \Psi : & \mathbb{Q}(\zeta)^2_{\mathbb{R}} & \longrightarrow & \mathbb{R}^4 \\ & \begin{pmatrix} x + \zeta y \otimes \alpha \\ x' + \zeta y' \otimes \alpha' \end{pmatrix} & \longmapsto & \begin{pmatrix} \alpha x - \frac{\alpha y}{2} \\ \frac{\sqrt{3}}{2} \alpha y \\ \alpha' x' - \frac{\alpha' y'}{2} \\ \frac{\sqrt{3}}{2} \alpha' y' \end{pmatrix} \end{array},$$

et le réseau $\Lambda_{\mathbb{R}}$ de $\mathbb{R}^4$ associé à Λ a pour base

$$B := \begin{pmatrix} -1.57 & -1.57 & 1.00 & -0.500 \\ 2.72 & -2.72 & 0 & 0.866 \\ 1.00 & -0.500 & 0 & 0 \\ 0 & 0.866 & 0 & 0 \end{pmatrix}.$$

Nous présentons cette matrice et les calculs qui suivent tels qu'ils sont effectués par l'interface gp de PARI/gp après appel à `default(realprecision,3)`, c'est-à-dire avec 19 chiffres significatifs (mais seulement 3 sont affichés). La signature de K étant $(0, 1)$, la matrice de Gram P de la base standard de $\mathbb{R}^4$ est

$$P := \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix},$$

et la matrice symétrique définie positive associée à B est

$$Q := B^{\mathsf{T}} P B = \begin{pmatrix} 21.7 & -10.9 & -3.14 & 6.28 \\ -10.9 & 21.7 & -3.14 & -3.14 \\ -3.14 & -3.14 & 2.00 & -1.00 \\ 6.28 & -3.14 & -1.00 & 2.00 \end{pmatrix}.$$

Le résultat de `qfminim(Q,2.50)` est

$$\left\{X \in \mathbb{Z}^4 \,:\, 0 < X^{\intercal} Q X \leqslant \frac{5}{2}\right\} = \pm \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 3 & 3 \\ 1 & 0 & 1 & -3 & 0 & 3 \end{pmatrix}.$$

En associant à un vecteur $X := (x_1, x_2, x_3, x_4) \in \mathbb{Z}^n$ l'élément $x_1 b_1 + \zeta x_2 b_1 + x_3 b_2 + \zeta x_4 b_2 \in \Lambda$, on obtient

$$\left\{x \in \Lambda \,:\, 0 < \|x\|^2 \leqslant \frac{5}{2}\right\} = \pm \begin{pmatrix} \zeta & 1 & 1+\zeta & \zeta \otimes \pi - 3 & 3+\pi & 1+\zeta \otimes 3 - \pi \\ 0 & 0 & 0 & 1 & 1+\zeta & 1+\zeta \end{pmatrix}.$$

Utilisons maintenant la méthode naïve qui ne fait pas appel à cette astuce. On a

$$\begin{aligned} \left\{x \in \Lambda_{\mathbb{R}} \,:\, 0 < \|x\|^2 \leqslant \frac{5}{2}\right\} &= B \cdot \left\{X \in \mathbb{Z}^4 \,:\, 0 < X^{\intercal} Q X \leqslant \frac{5}{2}\right\} \\ &= \pm \begin{pmatrix} -0.500 & 1.00 & 0.500 & -0.0708 & -0.142 & -0.0708 \\ 0.866 & 0 & 0.866 & 0.123 & 0.000 & -0.123 \\ 0 & 0 & 0 & 1.00 & 0.500 & -0.500 \\ 0 & 0 & 0 & 0 & 0.866 & 0.866 \end{pmatrix}. \end{aligned}$$

Afin de calculer l'inverse de Ψ, $\mathbb{Q}(\zeta)^2_{\mathbb{R}}$ est explicitement identifié à $\mathbb{R}^4$ *via* :

$$\begin{array}{rccc} \mu : & \mathbb{Q}(\zeta)^2_{\mathbb{R}} & \longrightarrow & \mathbb{R}^4 \\ & \begin{pmatrix} x + \zeta y \otimes \alpha \\ x' + \zeta y' \otimes \alpha' \end{pmatrix} & \longmapsto & \begin{pmatrix} \alpha x \\ \alpha y \\ \alpha' x' \\ \alpha' y' \end{pmatrix} \end{array}.$$

On a donc l'égalité $\Psi = \widetilde{\Psi} \circ \mu$, avec

$$\begin{array}{rccc} \widetilde{\Psi} : & \mathbb{R}^4 & \longrightarrow & \mathbb{R}^4 \\ & \begin{pmatrix} x \\ y \\ x' \\ y' \end{pmatrix} & \longmapsto & \begin{pmatrix} x - \frac{y}{2} \\ \frac{\sqrt{3}}{2} y \\ x' - \frac{y'}{2} \\ \frac{\sqrt{3}}{2} y' \end{pmatrix} \end{array},$$

qui a pour la matrice dans la base standard de $\mathbb{R}^4$:

$$M := \begin{pmatrix} 1.00 & -0.500 & 0 & 0 \\ 0 & 0.866 & 0 & 0 \\ 0 & 0 & 1.00 & -0.500 \\ 0 & 0 & 0 & 0.866 \end{pmatrix}.$$

On calcule l'inverse de M à l'aide de gp :

$$M^{-1} = \begin{pmatrix} 1.00 & 0.577 & 0 & 0 \\ 0 & 1.15 & 0 & 0 \\ 0 & 0 & 1.00 & 0.577 \\ 0 & 0 & 0 & 1.15 \end{pmatrix}.$$

Ainsi

$$\mu\left(\left\{x \in \Lambda \,:\, 0 < \|x\|^2 \leqslant \frac{5}{2}\right\}\right) = M^{-1} \cdot \left\{x \in \Lambda_{\mathbb{R}} \,:\, 0 < \|x\|^2 \leqslant \frac{5}{2}\right\}$$
$$= \pm \begin{pmatrix} 0.000 & 1.00 & 1.00 & -0.00000000000000000122 & -0.142 & -0.142 \\ 1.00 & 0 & 1.00 & 0.142 & 0.000 & -0.142 \\ 0 & 0 & 0 & 1.00 & 1.00 & 0.000 \\ 0 & 0 & 0 & 0 & 1.00 & 1.00 \end{pmatrix}.$$

Deux problèmes se présentent alors :

- Comment considérer le coefficient -0.00000000000000000122 ? Est-ce un coefficient nul qui, en pratique, n'est pas calculé comme nul par `PARI/gp` à cause d'erreurs d'arrondi ?
- Comment calculer l'image réciproque par μ du terme de droite de cette égalité ? La difficulté principale est de distinguer un réel d'un rationnel dans gp : le coefficient 0.142 est-il l'approximation rationnelle d'un réel, ou doit-il être considéré comme un rationnel ?

Les résultats de ces calculs dans gp sont présentés sur la Figure V.5.

V.4.1.2 Stockage des produits scalaires

Les invariants utilisés par l'algorithme présenté dans le Chapitre III utilisent de manière répétée les produits scalaires

$$\langle \omega_k x \,|\, \omega_l y \rangle, \tag{V.1}$$

où $x, y \in S(\Lambda, \mathscr{B}, \Omega)$ et $1 \leqslant k, l \leqslant d$. Il semble donc judicieux de stocker ces valeurs au moment du calcul des ensembles $S_j(\Lambda, \mathscr{B}, \Omega)$ dans une matrice. Cependant, la taille de l'ensemble $S(\Lambda, \mathscr{B}, \Omega)$ rend généralement le stockage de cette matrice impossible pour des questions de mémoire occupée. En effet, si $|S(\Lambda, \mathscr{B}, \Omega)| = 2S$, on montre en utilisant des arguments de symétrie que stocker cette matrice revient à stocker

$$\frac{dS(d+1)(S+1)}{4} = O\left(d^2 S^2\right)$$

coefficients réels.

Il est possible d'utiliser une stratégie intermédiaire entre le calcul complet des produits scalaires de la forme (V.1) et leur stockage. Le produit scalaire de $K_{\mathbb{R}}^n$ étant défini à partir de

```
? default(realprecision, 3)
? z = sqrt(3)/2
%2 = 0.866
? B = [-Pi/2,-Pi/2,1,-0.5;z*Pi,-z*Pi,0,z;1,-0.5,0,0;0,z,0,0]*1.0
    // ℤ-base de Λ_ℝ
%3 =
[-1.57  -1.57 1.00 -0.500]
[ 2.72  -2.72    0  0.866]
[ 1.00 -0.500    0      0]
[    0  0.866    0      0]
? P = matdiagonal([2,2,2,2]);
    // matrice de Gram de la base standard de ℝ^4
? Q = B~*P*B                    // forme quadratique associée à Λ_ℝ
%5 =
[ 21.7 -10.9 -3.14  6.28]
[-10.9  21.7 -3.14 -3.14]
[-3.14 -3.14  2.00 -1.00]
[ 6.28 -3.14 -1.00  2.00]
? S = qfminim(Q,2.50,,2)[3]
    // S = {X ∈ ℤ^4 : 0 < X^T Q X ⩽ 5/2}
%6 =
[0 0 0  1 1 0]
[0 0 0  0 1 1]
[0 1 1  0 3 3]
[1 0 1 -3 0 3]
? T = B*S                       // T = {x ∈ Λ_ℝ : 0 < ||x||^2 ⩽ 5/2}
%7 =
[-0.500 1.00 0.500 -0.0708 -0.142 -0.0708]
[ 0.866    0 0.866   0.123  0.000  -0.123]
[     0    0     0    1.00  0.500  -0.500]
[     0    0     0       0  0.866   0.866]
? M =[1,-0.5,0,0;0,z,0,0;0,0,1,-0.5;0,0,0,z]
    // matrice de Ψ̃ dans la base standard de ℝ^4
%8 =
[1 -0.500 0      0]
[0  0.866 0      0]
[0      0 1 -0.500]
[0      0 0  0.866]
? M^-1                          // matrice de Ψ̃^-1 dans la base standard de ℝ^4
%9 =
[1 0.577 0     0]
[0  1.15 0     0]
[0     0 1 0.577]
[0     0 0  1.15]
? M^-1*T                        // μ({x ∈ Λ : 0 < ||x||^2 ⩽ 5/2})
%10 =
[0.000 1.00 1.00 -0.00000000000000000122 -0.142 -0.142]
[ 1.00    0 1.00                  0.142  0.000 -0.142]
[    0    0    0                   1.00   1.00  0.000]
[    0    0    0                      0   1.00   1.00]
```

Fig. V.5 – Résultats de gp correspondant à l'Exemple V.4.2.

celui de $K_{\mathbb{R}}$, nous nous contentons de présenter cette stratégie dans le cas où Λ est un réseau algébrique de rang 1. Soient $x, y \in K_{\mathbb{R}}$. On peut écrire

$$x = x_1\omega_1 + \cdots + x_d\omega_d$$

et

$$y = y_1\omega_1 + \cdots + y_d\omega_d,$$

où $x_1, \ldots, x_d, y_1, \ldots, y_d \in \mathbb{R}$. Soient $X, Y \in \mathbb{R}^d$ les vecteurs colonnes formés des x_i et des y_i respectivement. On a

$$\langle \omega_k x \,|\, \omega_l y \rangle = \sum_{1 \leqslant i,j \leqslant d} x_i y_j \langle \omega_k \omega_i \,|\, \omega_l \omega_j \rangle = X^{\intercal} \Omega(k,l) Y, \tag{V.2}$$

où $\Omega(k,l) \in \mathrm{M}_d(\mathbb{R})$ est définie par $\Omega(k,l)_{i,j} := \langle \omega_k \omega_i \,|\, \omega_l \omega_j \rangle$ pour tous $1 \leqslant i, j \leqslant d$. Soulignons que la matrice $\Omega(k,l)$ n'est en général pas symétrique, mais que pour tout $1 \leqslant k, l \leqslant d$, on a $\Omega(k,l)^{\intercal} = \Omega(l,k)$. En particulier, on a donc

$$\langle \omega_l x \,|\, \omega_k y \rangle = X^{\intercal} \Omega(k,l) Y = (\Omega(l,k)X)^{\intercal} Y. \tag{V.3}$$

On stocke l'ensemble

$$\{\Omega(k,l)X \ : \ X \in S(\Lambda, \mathscr{B}, \Omega),\ 1 \leqslant k \leqslant l \leqslant d\}, \tag{V.4}$$

afin que le calcul d'un produit scalaire de la forme (V.1) se ramène simplement à un produit de la forme (V.2) ou (V.3). L'ensemble (V.4) est de cardinal au plus $\frac{Sd(d+1)}{2}$; il est ainsi stocké en mémoire sous la forme de

$$\frac{Sd^2(d+1)}{2} = O\left(Sd^3\right)$$

coefficients réels. La mémoire occupée est plus importante qu'avec le stockage complet des produits scalaire lorsque d augmente. Cependant, lorsque S est grand devant d (ce qui est généralement le cas), cette stratégie devient nettement plus économique en terme de mémoire occupée, tout en proposant une accélération intéressante lors du calcul des produits scalaires de la forme (V.1).

V.4.2 Empreinte et combinaisons scalaires

V.4.2.1 Empreinte et stockage des candidats

L'empreinte d'une pseudo-base, définie dans la Section III.3.2.1, est calculée en implantant directement l'Algorithme III.1. Rappelons simplement que les ensembles $S_j(\Lambda, \mathscr{B}, \Omega)$ sont en pratique calculés au signe près : un seul vecteur par paire de la forme $(+x, -x)$ est déterminé par la fonction `qfminim`. Il faut donc prendre soin de tester à la fois un vecteur et son opposé lorsque qu'un parcours de l'ensemble $S_j(\Lambda, \mathscr{B}, \Omega)$ est effectué. Que ce soit pour la détermination des ensembles $S_j(\Lambda, \mathscr{B}, \Omega)$, pour les calculs de l'empreinte et des combinaisons scalaires ou

pour la phase de *backtracking*, les tests sur un vecteur x consistent essentiellement à vérifier si les valeurs de produits scalaires de la forme (V.1) pour différents vecteurs y sont acceptables. En particulier, il est possible de combiner la phase de test d'un vecteur x et de son opposé sans avoir à recalculer tous ces produits scalaires.

Supposons que la base $(b_1, \dots, b_n)$ est déjà agencée de manière à minimiser l'empreinte. Rappelons que les valeurs de cette dernière sont données par le nombre de vecteurs x tels que $(b_1, \dots, b_{m-1}, x)$ soit un m-automorphisme partiel de Λ, et ceci pour tout $1 \leqslant m \leqslant n$. Or la méthode présentée dans la Section III.4 pour déterminer le groupe $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$ passe fréquemment par le prolongement de stabilisateurs de la famille $(b_1, \dots, b_m)$. Il est donc opportun lors du calcul de l'empreinte de garder en mémoire les vecteurs x tels que $(b_1, \dots, b_{m-1}, x)$ est un m-automorphisme partiel de Λ afin d'accélérer la génération du groupe $\mathrm{Aut}_{K_{\mathbb{R}}}(\Lambda)$.

V.4.2.2 Choix des invariants et paramètre de profondeur

Profondeur des combinaisons scalaires. Il s'avère que calculer les combinaisons scalaires telles que nous les avons décrites dans la Section III.3.2.2 est parfois très coûteux. En effet, au fur et à mesure qu'un m-automorphisme $\mathcal{V}$ est complété, on remarque souvent que la dimension sur K de l'espace engendré par les $\widehat{X}_s(\mathcal{V})$ augmente rapidement, ce qui complexifie les calculs associés aux combinaisons scalaires (que ce soit pendant la phase de précalcul ou le test d'un candidat). Nous présentons ici une forme affaiblie (qui généralise celle de [PS97, §5]) de cet invariant permettant en pratique de réduire cette dimension et qui reste d'une efficacité satisfaisante.

Soient $\mathcal{V} := (v_1, \dots, v_m)$ un m-automorphisme partiel de Λ et $s := (s_{k,l,j})_{1 \leqslant j \leqslant m}^{1 \leqslant k,l \leqslant d} \in \mathbb{R}^{md^2}$. Rappelons que les combinaisons scalaires sont définies comme

$$X_s(\mathcal{V}) := \left\{ x \in S_{m+1}(\Lambda, \mathscr{B}, \Omega) \,:\, \langle \omega_k x \,|\, \omega_l v_j \rangle = s_{k,l,j} \quad \begin{matrix} \forall\, 1 \leqslant k,l \leqslant d \\ \forall\, 1 \leqslant j \leqslant m \end{matrix} \right\}.$$

En pratique, on considère plutôt une version paramétrée par $0 \leqslant \vartheta \leqslant n$ des combinaisons scalaires :

$$X_s^{\vartheta}(\mathcal{V}) := \left\{ x \in S_{m+1}(\Lambda, \mathscr{B}, \Omega) \,:\, \langle \omega_k x \,|\, \omega_l v_j \rangle = s_{k,l,j} \quad \begin{matrix} \forall\, 1 \leqslant k,l \leqslant d \\ \forall \max(1, m+1-\vartheta) \leqslant j \leqslant m \end{matrix} \right\}.$$

On appelle ϑ le *paramètre de profondeur* des combinaisons scalaires. Il permet en pratique de réduire la dimension du K-espace vectoriel engendré par les $\widehat{X}_s(\mathcal{V})$:

- Si $m \leqslant \vartheta + 1$, on a $X_s^{\vartheta}(\mathcal{V}) = X_s(\mathcal{V})$ pour tout $s \in \mathbb{R}^{md^2}$. Les combinaisons scalaires ne sont donc pas modifiées avant le rang $\vartheta + 2$.
- Supposons maintenant que $m > \vartheta + 1$. Pour tout $s \in \mathbb{R}^{md^2}$, on a

  $$X_s^{\vartheta}(\mathcal{V}) = \bigsqcup_{t \in T_s} X_t(\mathcal{V})$$

  avec

  $$T_s := \left\{ t \in \mathbb{R}^{md^2} \,:\, t_i = s_i \;\forall\, m+1-\vartheta \leqslant i \leqslant m \right\}.$$

En particulier, cette égalité entraîne généralement [5] que

$$\dim_K\left(\left\{\widehat{X}_s^{\vartheta}(\mathcal{V}) \,:\, s\in\mathbb{R}^{md^2}\right\}\right) < \dim_K\left(\left\{\widehat{X}_s(\mathcal{V}) \,:\, s\in\mathbb{R}^{md^2}\right\}\right),$$

ce qui rend l'utilisation des combinaisons scalaires bien plus rapide.
Notons qu'utiliser la valeur $\vartheta = 0$ revient à n'utiliser que l'invariant associé à l'empreinte lors de la phase de *backtracking* (ce qui, comme remarqué précédemment, est parfois plus efficace). Pour $\vartheta = 1$, les combinaisons scalaires rejoignent la notion de *spectre* introduite dans [Mar03, def.1.4.3, p.12–13]. Enfin, les combinaisons scalaires « complètes » sont utilisées lorsque $\vartheta = n$.

Choix des invariants. Nous avons introduits dans le Chapitre III deux invariants (l'empreinte et les combinaisons scalaires) permettant d'accélérer la détection des automorphismes partiels non prolongeables (*i.e.* qui correspondent à des impasses dans l'arbre des possibilités). Cependant, le précalcul et l'utilisation de ces invariants peuvent avoir un coût non négligeable. Ce surcoût surpasse même parfois l'accélération apportée lors de la phase de *backtracking* ! Il est donc judicieux de ne pas toujours utiliser tous les invariants disponibles. Malheureusement, nous n'avons pas à l'heure actuelle de stratégie permettant de décider à l'avance quels invariants utiliser. Nous utilisons donc l'heuristique de [PS97, §10.(4)] :

1. L'empreinte seule est suffisante pour la majorité des réseaux algébriques. De plus, le gain apporté par cet invariant est en pratique toujours supérieur au surcoût engendré par son initialisation et son utilisation. En conclusion, l'empreinte est *toujours* utilisée.
2. Si aucun automorphisme n'est calculé par l'algorithme en un temps raisonnable (déterminé heuristiquement par le rang du réseau algébrique considéré, par la taille des ensembles $S_j(\Lambda, \mathscr{B}, \Omega)$ et par la puissance de calcul disponible), on recommence la phase de *backtracking* en ajoutant les combinaisons scalaires de faible profondeur.
3. Si l'algorithme ne détermine toujours pas d'automorphisme, on augmente graduellement la profondeur des combinaisons scalaires.

V.4.3 Résultats expérimentaux

Ce paragraphe présente quelques résultats issus des expérimentations menées concernant l'influence des combinaisons scalaires sur la vitesse de détermination du groupe des $K_{\mathbb{R}}$-automorphismes d'un réseau algébrique. Tous les tests ont été effectués sur un processeur Intel Core i7-4790 @ 3.60Ghz à l'aide de la librairie `PARI/gp 2.9.0`, compilés à l'aide de `gcc 5.4.0` sur un système Xubuntu 16.04.2 (64bits).

En dehors des réseaux algébriques « aléatoires », la plupart des exemples que nous avons considérés sont construits à l'aide de la proposition suivante :

5. En toute généralité, l'égalité précédente n'entraîne pas l'inégalité qui va suivre. Néanmoins, cette dernière est en pratique presque toujours vérifiée.

Proposition V.4.3 *Soient K un corps de nombres, $(\mathfrak{a}_1, \dots, \mathfrak{a}_n)$ une famille d'idéaux fractionaires de K et $(b_1, \dots, b_n)$ une $\mathbb{R}$-base de $\mathbb{R}^n$. L'ensemble*

$$\Lambda := \mathfrak{a}_1(1 \otimes b_1) \oplus \cdots \oplus \mathfrak{a}_n(1 \otimes b_n)$$

est un réseau algébrique de $K_{\mathbb{R}}^n$.

Démonstration. Il suffit de remarquer que si $(\omega_1^{(i)}, \dots, \omega_d^{(i)})$ est une $\mathbb{Z}$-base de $\mathfrak{a}_i$ pour tout $1 \leqslant i \leqslant n$, la famille formée des $\omega_j^{(i)} \otimes b_i$ avec $1 \leqslant i \leqslant n$ et $1 \leqslant j \leqslant d$ est une $\mathbb{R}$-base de $K_{\mathbb{R}}^n$ et une $\mathbb{Z}$-base de Λ. □

En particulier, on fabrique par ce procédé des réseaux algébriques de $K_{\mathbb{R}}^n$ à partir de ceux de $\mathbb{R}^n$; on dira alors qu'un réseau de $\mathbb{R}^n$ est *vu comme un réseau algébrique de $K_{\mathbb{R}}^n$*. En utilisant le catalogue [LATT] maintenu par Nebe et Sloane, nous avons ainsi construit une multitude d'exemples de réseaux algébriques issus de réseaux euclidiens particuliers. Les Figure V.6 et Figure V.7 présentent les résultats obtenus pour les réseaux $\mathbb{A}_7$, $\mathbb{A}_{20}$, BW_{16} et $\mathbb{A}_{24}^{\vee}$, vus respectivement comme réseaux algébriques de $\mathbb{Q}(i)_{\mathbb{R}}^7$, $\mathbb{Q}(i)_{\mathbb{R}}^{20}$, $\mathbb{Q}(i)_{\mathbb{R}}^{16}$, $\mathbb{Q}(i)_{\mathbb{R}}^{24}$, et ceci en utilisant les bases données par le catalogue [LATT] [6]. La Figure V.6 (resp. la Figure V.7) décrit l'évolution du rapport entre le temps calcul total (resp. du temps de précalcul) pour différentes valeurs de ϑ et le temps de calcul total (resp. le temps de précalcul) pour $\vartheta = 0$ (c'est-à-dire en n'utilisant que l'empreinte). Les valeurs présentées sont des valeurs moyennes obtenues sur un grand nombre de répétitions des tests.

- Pour le réseau $\mathbb{A}_7$, utiliser les valeurs $\vartheta \geqslant 1$ ne fait que ralentir l'algorithme. Ceci s'explique par le fait que le groupe des $K_{\mathbb{R}}$-automorphismes de $\mathbb{A}_7$ est « facile » à déterminer ; le surcoût engendré par le précalcul et l'utilisation des combinaisons scalaires surpasse largement la maigre accélération apportée.
- En utilisant la valeur $\vartheta = 1$ lors de la détermination de $\mathrm{Aut}_{K_{\mathbb{R}}}(\mathbb{A}_{20})$, le temps de calcul est divisé par 5 par rapport au temps de calcul obtenu pour $\vartheta = 0$! Notons que la réduction du temps de calcul diminue avec l'accroissement de ϑ (mais cette réduction reste importante). L'augmentation du temps de précalcul avec l'augmentation de ϑ est similaire à celle obtenue pour $\mathbb{A}_7$.
- Pour le réseau BW_{16} (le réseau de Barnes/Walls de dimension 16), ce n'est qu'à partir de la valeur $\vartheta = 2$ que l'algorithme est (considérablement) accéléré. À l'heure actuelle, nous n'avons pas d'explication précise quant aux oscillations de l'évolution du temps de précalcul avec l'accroissement de ϑ.
- Le temps de calcul du groupe des $K_{\mathbb{R}}$-automorphismes de $\mathbb{A}_{24}^{\vee}$ varie peu en fonction de ϑ, et ceci malgré une augmentation importante du temps de précalcul. Ceci s'explique par le fait que le temps de précalcul reste extrêmement faible en comparaison du temps de calcul total. De plus, l'accélération accordée par l'utilisation des combinaisons scalaires lors de la phase de *backtracking* doit compenser le surcoût de leur utilisation.

6. La base choisie a une influence essentielle sur les performances de l'algorithme, puisqu'elle modifie la taille des ensembles $S_j(\Lambda, \mathscr{B}, \Omega)$. En particulier, utiliser d'autres bases peut conduire à des résultats différents.

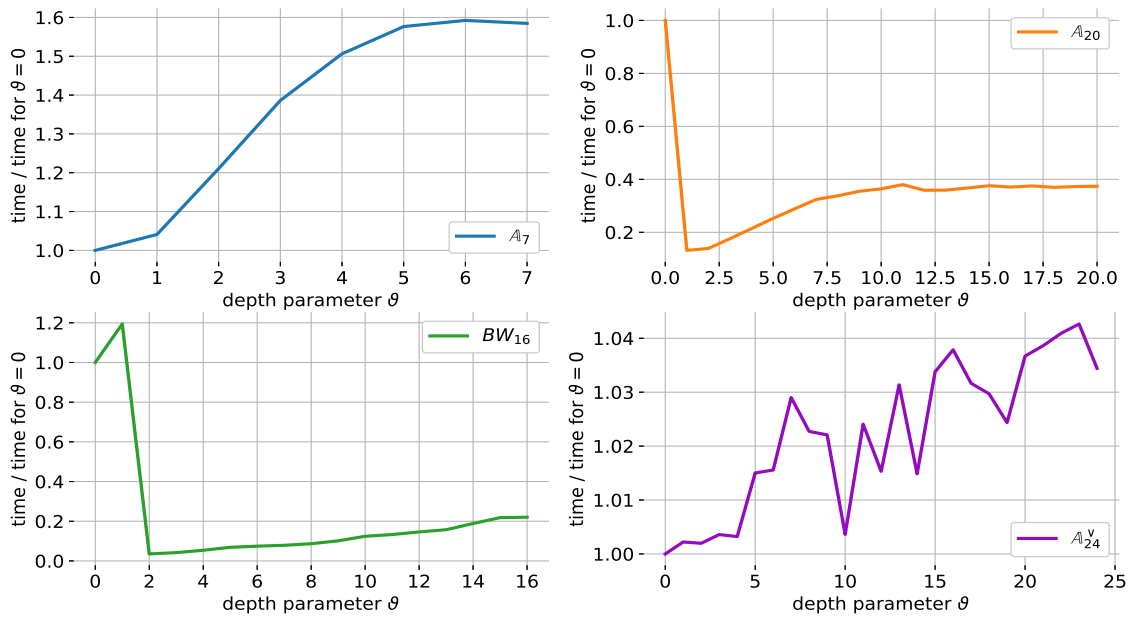


Fig. V.6 – Influence du paramètre de profondeur sur le temps de calcul total du groupe des $K_{\mathbb{R}}$-automorphismes de $\mathbb{A}_7$, $\mathbb{A}_{20}$, BW_{16} et $\mathbb{A}_{24}^{\vee}$ vus comme réseaux algébriques sur $\mathbb{Q}(i)^n_{\mathbb{R}}$.

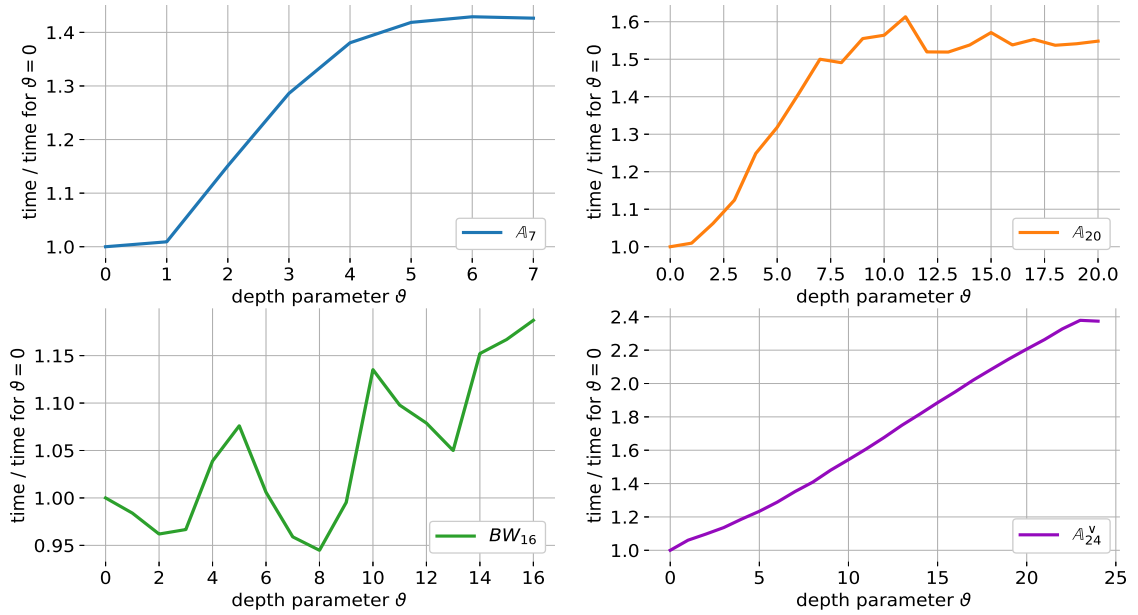


Fig. V.7 – Influence du paramètre de profondeur sur le temps de précalcul lors de la détermination du groupes des $K_{\mathbb{R}}$-automorphismes de $\mathbb{A}_7$, $\mathbb{A}_{20}$, BW_{16} et $\mathbb{A}_{24}^{\vee}$ vus comme réseaux algébriques sur $\mathbb{Q}(i)^n_{\mathbb{R}}$.

V.5 Utilisation des graphes pour les problèmes LI et LA

Nous avons implanté la conversion d'un réseau en un graphe décrite dans la Section IV.3 du Chapitre IV. Pour cela, nous avons principalement utilisé les librairies :

- `PARI` [PARI/gp] pour les calculs algébriques : manipulation des réseaux, gestion des vecteurs courts, algébre linéaire...
- `nauty and Traces` [NAUTY] pour tous les aspects liés aux graphes : initialisations, manipulations, calculs d'isomophismes et d'automorphismes...

Notons que comme `PARI` avec l'interface gp, `nauty and Traces` propose une interface nommée `dreadnaut` permettant d'accéder de manière simplifiée à toutes les fonctions de la librairie. Comme précédemment, les implantations ont été effectuées dans le langage `C` en utilisant les libraires citées et non les interfaces associées.

V.5.1 Graphes dans `nauty` et `Traces`

La libraire `nauty and Traces` contient essentiellement trois fonctions permettant de calculer le groupe d'automorphisme d'un graphe. Ces trois fonctions prennent en charge les graphes colorés ou non colorés, mais pas les graphes étiquetés. Pour plus de détails sur les fonctions et structures présentées, nous renvoyons le lecteur vers la documentation officielle [NAUTY].

V.5.1.1 Graphes denses pour `densenauty`

La fonction `densenauty` permet de calculer le groupe d'automorphisme d'un graphe dense. La structure associée à ces graphes est simplement appelée `graph`. Un `graph` représentant un graphe (non coloré et non étiqueté) dont les sommets sont $0, 1, \ldots, n-1$ est un tableau de taille n, dont l'entrée i contient les indices des sommets auxquels i est adjacent. La structure `graph` est donc essentiellement celle associée à la matrice d'adjacence d'un graphe. Deux routines d'allocation sont proposées pour cette structure :

- une allocation *statique*, qui requiert de connaître à l'avance une borne sur la taille des graphes considérés,
- une allocation *dynamique*, plus délicate à utiliser, mais qui ne nécessite pas de borner la taille des graphes.

L'initialisation statique n'est pas adaptée pour les graphes issus de réseaux : il est délicat d'estimer de manière raisonnable [7] la taille des graphes obtenus à partir des réseaux.

V.5.1.2 Graphes creux pour `sparsenauty` et `Traces`

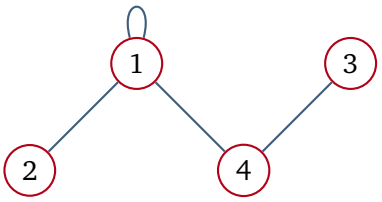
Deux fonctions sont conçues pour calculer les groupes d'automorphisme de graphes creux : `sparsenauty` et `Traces`. La structure destinée à représenter de tels graphes est appelée `sparsegraph`.

7. C'est-à-dire sans passer par une allocation mémoire gargantuesque. Par exemple, utiliser la borne $|G(\Lambda, \mathcal{B})_\bullet| \leqslant |S(\Lambda, \mathcal{B})|h(\mathcal{B})$ conduit à allouer plus de 80Go de mémoire pour le graphe coloré associé au réseau de Leech...

La représentation en `sparsegraph` d'un graphe (creux) dont les sommets sont $0, 1, \ldots, n-1$ est essentiellement la donnée de :

- un tableau `d` de taille n, tel que pour tout $0 \leqslant i < n$, `d[i]` est égal au nombre de sommets adjacents au sommet i,
- un tableau `v` de taille n et un tableau `e` (dont la taille est plus complexe à déterminer), tels que `e[v[i]]`, ..., `e[v[i]+d[i]-1]` désignent exactement les indices des sommets auxquels le sommet i est adjacent.

Exemple V.5.1 Considérons le graphe G et sa matrice d'incidence ci-dessous :



$$\begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}.$$

Une représentation possible de G en `sparsegraph` est donnée par

```
d = [3,1,1,2],
e = [1,2,4,1,3],
v = [0,0,2,3].
```

Au contraire de la structure `graph`, la structure `sparsegraph` ne propose que des routines d'allocation dynamiques. Il est possible de passer de la structure de graphe dense à celle de graphe creux à l'aide de la fonction `nauty_to_sg`. La fonction permettant la conversion inverse est appelée `sg_to_nauty`.

V.5.1.3 Coloration des sommets

Les structures `graph` et `sparsegraph` ne contiennent pas l'information sur la coloration des sommets du graphe considéré. La coloration des sommets d'un graphe est représentée par deux tableaux, habituellement appelés `lab` et `ptn`. Le tableau `lab` contient les indices des sommets du graphe, de manière à ce que les sommets de même couleur soient adjacents. Le tableau `ptn` est un tableau binaire qui sert à indiquer où commencent et finissent les classes de couleurs dans `lab`, l'indice `0` signifiant la fin d'une classe.

Exemple V.5.2 Considérons un graphe G à 10 sommets, dont la coloration des sommets est donnée par la partition $\{\{0\}, \{1\}, \{2, 3, 7\}, \{4, 9\}, \{5, 6, 8\}\}$. Cette coloration peut être encodée dans `nauty and Traces` par :

```
lab = [0,1,2,3,7,4,9,5,6,8],
ptn = [0,0,1,1,0,1,0,1,1,0].
```

V.5.2 Calcul du graphe associé à un réseau

Fixons $\mathcal{B} := (b_1, \dots, b_n)$ une base d'un réseau Λ de $\mathbb{R}^n$. Nous avons détaillé dans la Section IV.3 plusieurs transformations, qui préservent toutes la notion d'automorphisme :

- Le passage de l'ensemble $S(\Lambda, \mathcal{B})$ à un graphe étiqueté $G(\Lambda, \mathcal{B})$ (Section IV.3.1).
- Le passage du graphe étiqueté $G(\Lambda, \mathcal{B})$ à un graphe coloré $G(\Lambda, \mathcal{B})_\bullet$ (Section IV.3.2).
- Le passage du graphe coloré $G(\Lambda, \mathcal{B})_\bullet$ à un graphe $G(\Lambda, \mathcal{B})_{\bullet\circ}$ (Section IV.3.3).

Puisque les fonctions de `nauty and Traces` prennent en charge les graphes colorés, nous n'avons pas implanté la dernière transformation (la « décoloration »). De plus, puisque les graphes étiquetés ne sont pas gérés, nous avons choisi de calculer directement le graphe $G(\Lambda, \mathcal{B})_\bullet$, c'est-à-dire sans passer par le calcul de $G(\Lambda, \mathcal{B})$. Notons néanmoins que ce graphe est « implicitement calculé », puisque sa matrice d'incidence est exactement le matrice de Gram de $S(\Lambda, \mathcal{B})$. L'ensemble $S(\Lambda, \mathcal{B})$ est calculé à l'aide la fonction `qfminim` de `PARI/gp` (voir la Section V.4.1.1). Une fois cette étape effectuée, l'Algorithme V.1 permet de générer le graphe $G(\Lambda, \mathcal{B})_\bullet$.

```
Données :
    • L'ensemble S := S(Λ, B).
    • La grandeur h(B).
Résultat :
    • Le graphe G(Λ, B)• (sans sa coloration).
soient d := h(B), s := |S|, C := [] et A := [].
soit G le graphe sans arrêtes à sd sommets.
pour 0 ⩽ i < s et i ⩽ j < s faire
    si ⟨S[i]|S[j]⟩ ∉ C alors
        ajouter ⟨S[i]|S[j]⟩ à la fin de C.
        calculer α := [α_0, ..., α_{d-1}] tels que |C| = Σ_{i=0}^{d-1} α_i 2^i.
        ajouter α à la fin de A.
    sinon
        soient 1 ⩽ k ⩽ |C| tel que ⟨S[i]|S[j]⟩ = C[k] et α := A[k].
    pour 0 ⩽ l < d faire
        si α_l ≠ 0 alors
            ajouter une arrête dans G entre v_{i+ls} et v_{j+ls}.
supprimer les sommets de G à partir de v_{|A|s}.
pour 0 ⩽ i < s et 0 ⩽ j < |A| − 1 faire
    ajouter une arrête dans G entre v_{i+js} et v_{i+(j+1)s}.
retourner G.
```

Algorithme V.1 - Calcul du graphe $G(\Lambda, \mathcal{B})_\bullet$.

Plusieurs remarques peuvent être faites sur cet algorithme :

- Il est coûteux de déterminer à l'avance le nombre exact de couleurs (et donc le nombre

de sommets) du graphe $G(\Lambda, \mathcal{B})$; ceci revient à déterminer toutes les valeurs $\langle x \mid y \rangle$ pour $x, y \in S(\Lambda, \mathcal{B})$. Nous choisissons ici d'initialiser un graphe avec $|S(\Lambda, \mathcal{B})|h(\mathcal{B})$ sommets [8], et de supprimer *a posteriori* les sommets inutiles.

- Comme nous avons déjà pu le noter, il est complexe de déterminer un agencement des étiquettes de $G(\Lambda, \mathcal{B})$ permettant de minimiser le nombre d'arrêtes dans $G(\Lambda, \mathcal{B})_\bullet$. Nous nous contentons ici de l'agencement donné par l'ordre dans lequel les produits scalaires $\langle x \mid y \rangle$ apparaissent lors du parcours de $S(\Lambda, \mathcal{B})$. En particulier, la densité du graphe $G(\Lambda, \mathcal{B})_\bullet$ calculé par cet algorithme n'est en général pas optimale.
- Cet algorithme ne calcule pas la coloration du graphe $G(\Lambda, \mathcal{B})_\bullet$, mais elle est extrêmement simple à expliciter dans le format de `nauty and Traces`. En effet, si $G(\Lambda, \mathcal{B})_\bullet$ possède sd sommets répartis sur d niveaux, il suffit de prendre `lab = [0,1,2,...,sd-1]` et, pour tout $0 \leqslant i < sd - 1$, `ptn[i] = 0` si $i \equiv -1 \mod |S(\Lambda, \mathcal{B})|$ et `ptn[i] = 1` sinon.

En ayant en tête l'objectif de comparer les routines creuses et denses de `nauty and Traces`, nous avons utilisé cet algorithme pour initialiser la structure dense du graphe $G(\Lambda, \mathcal{B})_\bullet$ (afin de tester `densenauty`), qui est ensuite convertie en un graphe creux (afin de tester `sparsenauty` et `Traces`). Comme les expérimentations tendent à le prouver, il est en pratique plus judicieux d'initialiser un graphe creux et de ne pas utiliser les routines denses. Nous disposons ainsi de deux implantations : une implantation à vocation expérimentale, qui appelle les routines denses et creuses de `nauty and Traces`, et une implantation efficace, qui n'utilise que des routines creuses.

V.5.3 Résultat expérimentaux

Il s'avère que la conversion d'un réseau en graphe n'est pas seulement d'une utilité théorique. Les expérimentations menées nous ont permis d'exhiber des exemples pour lesquels utiliser l'approche par les graphes est plus efficace que l'approche classique. Les tests ont été effectués sur un processeur Intel Core i7-4790 @ 3.60Ghz et compilés à l'aide de `gcc 5.4.0` sur un système Xubuntu 16.04.2 (64bits). Les fonctions comparées sont :

- `qfauto` de la librairie `PARI/GP` version `2.9.0`. Cette fonction est une implantation de l'algorithme de Plesken et Souvignier [PS97]. Nous avons pris soin de précalculer séparément les ensembles $S(\Lambda, \mathcal{B})$ avant de l'appeler : les temps de calcul affichés pour `qfauto` ne prennent donc pas en compte de calcul.
- `densenauty` version `2.6r3`.
- `sparsenauty` version `2.6r3`.
- `Traces` version `2.6r3`.

Toutes les fonctions comparées ont été compilées à l'aide de `gcc 5.4.0`. Les temps de calcul présentés ne prennent pas en compte :

- Le calcul de l'ensemble $S(\Lambda, \mathcal{B})$.
- Le calcul du graphe $G(\Lambda, \mathcal{B})_\bullet$ à l'aide de l'Algorithme V.1.

8. C'est une borne établie dans la preuve du Théorème IV.4.1 sur le nombre de sommets de $G(\Lambda, \mathcal{B})_\bullet$.

En particulier, nous ne prenons en compte **que** les temps de calcul des groupes d'automorphisme des objets considérés. Les conversions entre réseaux et graphes, ainsi que les différents précalculs (en dehors de ceux intrinsèquement liés aux groupes d'automorphismes, comme l'empreinte, les combinaisons scalaires et les diffèrents invariants utilisés par les fonctions de `densenauty`, `sparsenauty` et `Traces`) ne sont pas pris en compte. Nous avons largement utilisé le catalogue [LATT] pour nos tests. Puisque l'ensemble $S(\Lambda, \mathcal{B})$ est dépendant de la base $\mathcal{B}$ choisie, considérer d'autres bases peut mener à des résultats différents.

La fonction `densenauty` s'est avérée être plus lente que `sparsenauty` et `Traces` sur l'ensemble des tests effectués. Elle est aussi généralement plus lente que `qfauto`. Ceci s'explique par la faible densité des graphes de la forme $G(\Lambda, \mathcal{B})_\bullet$, propriété étudiée dans la Section IV.3.2.3. Les résultats des comparaisons entre la méthode classique (c'est-à-dire l'algorithme de Plesken et Souvignier, implanté par la fonction `qfauto`) et l'approche par les graphes (les fonctions `densenauty`, `sparsenauty` et `Traces`) sont variables :

- La Figure V.8 et la Figure V.9 montrent que l'approche par les graphes est significativement plus rapide que l'approche classique pour les réseaux $\mathbb{A}_n$ et $\mathbb{D}_n$ respectivement. Le résultat est encore plus marqué pour les réseaux $\mathbb{Z}^n$: `sparsenauty` est environ 2000 fois plus rapide que `qfauto` pour déterminer le groupe d'automorphisme de $\mathbb{Z}^{40}$ (voir la Figure V.10).
- Au contraire, la Figure V.11 montre que la fonction `qfauto` reste la plus rapide sur les réseaux parfaits de dimension 8. Des résultats similaires ont été obtenus pour les réseaux parfaits de dimension $2 \leqslant n < 8$. De plus, les tests effectués sur des réseaux aléatoires (de dimension variable) montrent que l'approche classique est « génériquement plus efficace » que l'approche par les graphes. La Figure V.12 présente les résultats obtenus sur 10000 réseaux aléatoires de dimension 20.

En conclusion, nous pouvons retenir que l'approche par les graphes apporte un gain significatif par rapport à la méthode classique sur plusieurs familles d'exemples, mais semble être « en général » plus lente. Néanmoins, nous ne savons pas à l'heure actuelle distinguer les réseaux pour lesquels cette approche par les graphes est en pratique plus efficace, et de nombreux facteurs sont à prendre en compte avant de pouvoir tirer une conclusion définitive sur cette question. Notamment, la qualité des implantions des programmes comparés peut être un facteur crucial. Nous espérons que de plus amples expérimentations nous conduiront à affiner cette conclusion.

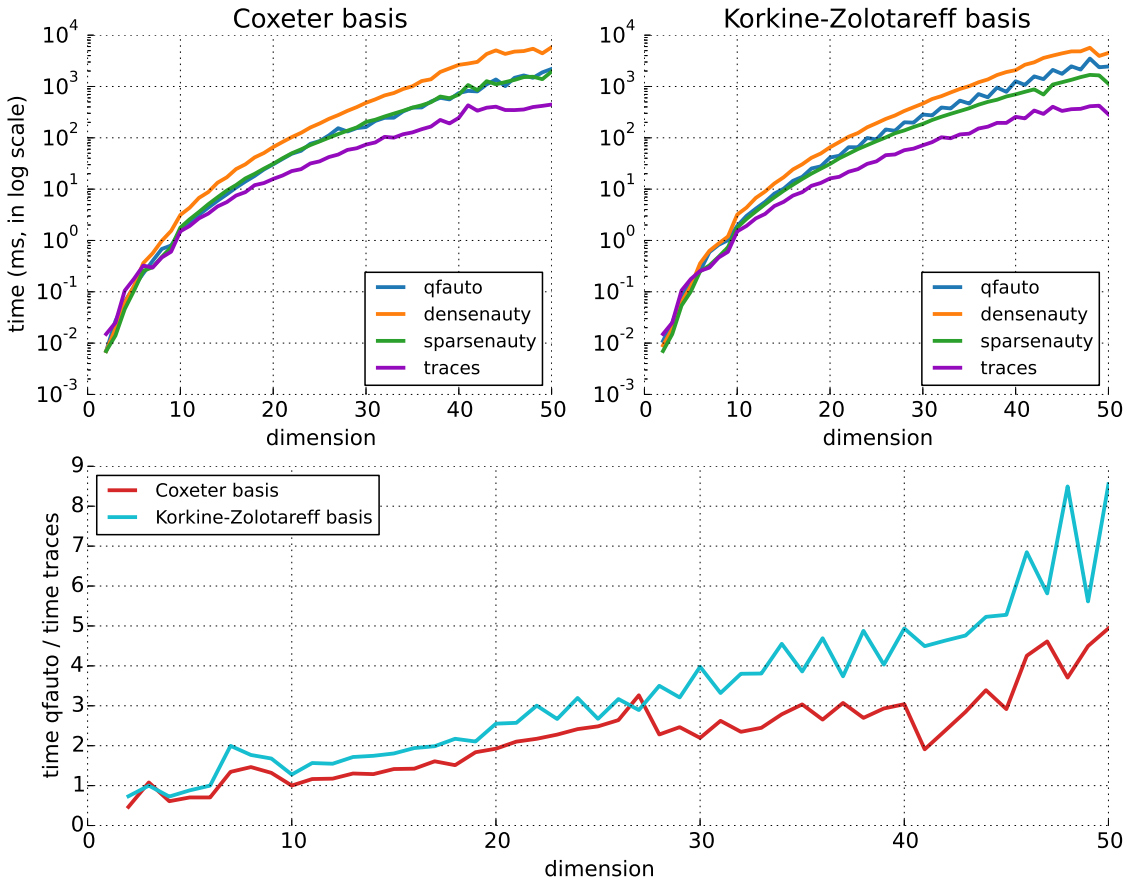


Fig. V.8 – Comparaison des temps de calculs sur deux bases différentes du réseau $\mathbb{A}_n$ pour $2 \leqslant n \leqslant 50$. Le graphe inférieur représente le rapport temps de calcul de `qfauto` / temps de calcul de `Traces`.

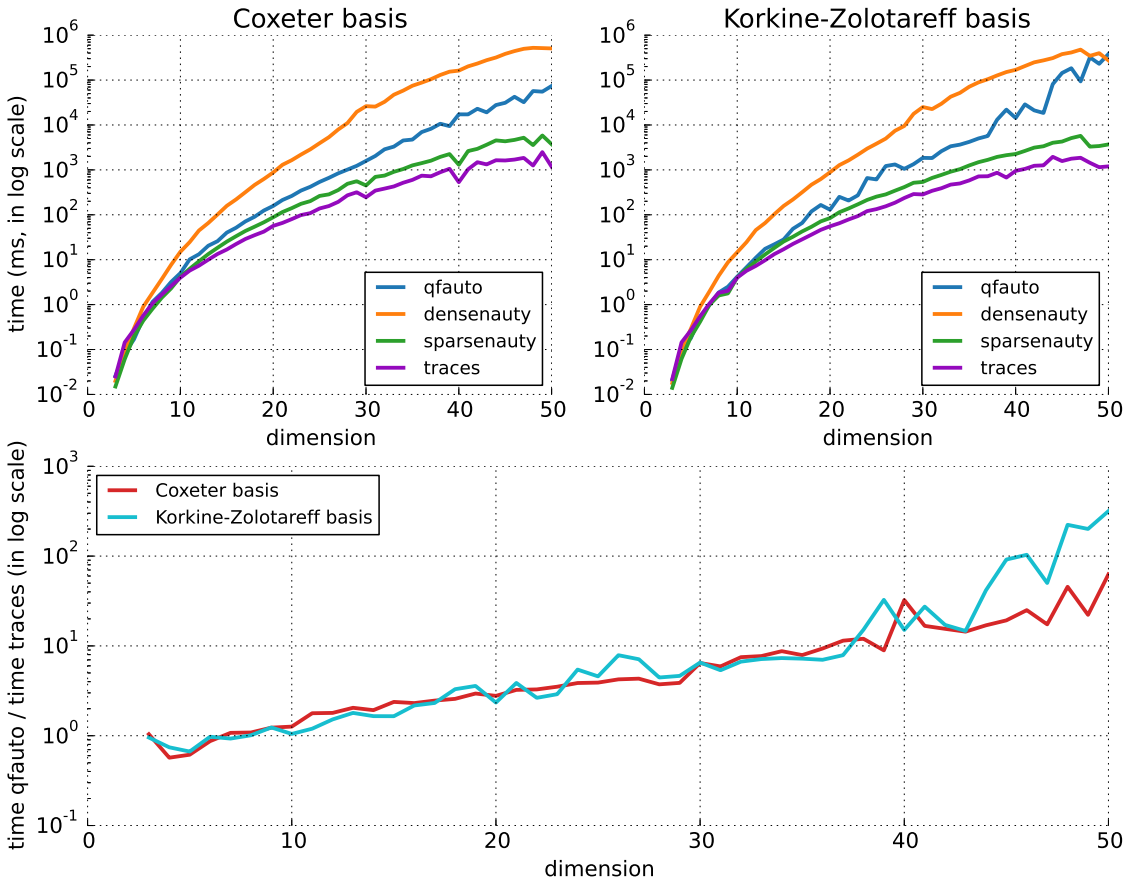


Fig. V.9 – Comparaison des temps de calculs sur deux bases différentes du réseau $\mathbb{D}_n$ pour $3 \leqslant n \leqslant 50$. Le graphe inférieur représente le rapport temps de calcul de `qfauto` / temps de calcul de `Traces`.

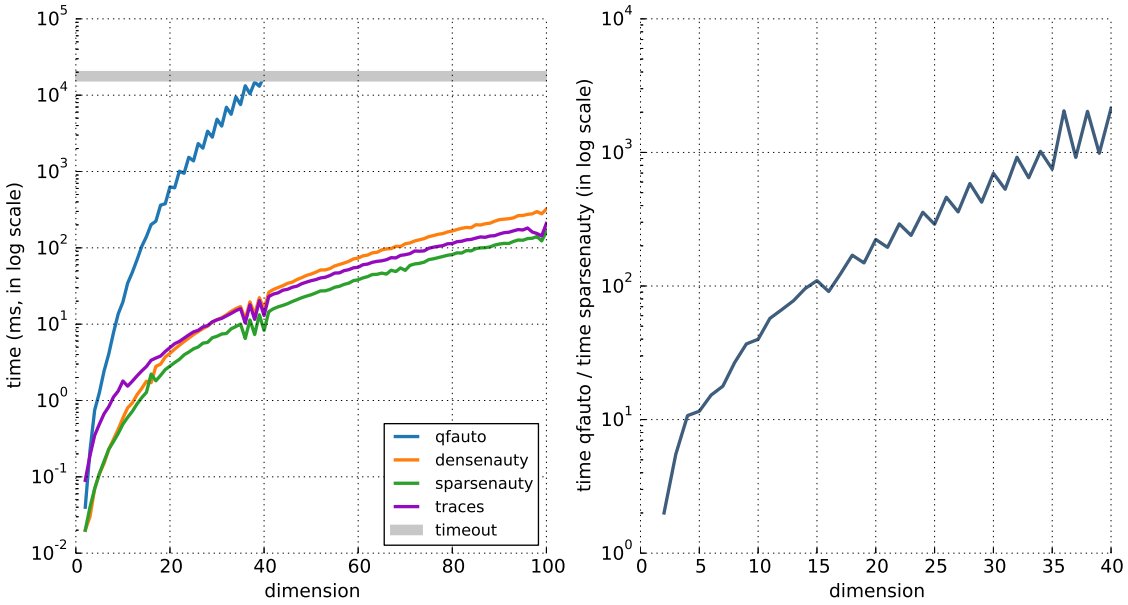


Fig. V.10 – Comparaison des temps de calculs sur les réseaux $\mathbb{Z}^n$ pour $2 \leqslant n \leqslant 100$. À droite, le rapport temps de calcul de `qfauto` / temps de calcul de `sparsenauty`.

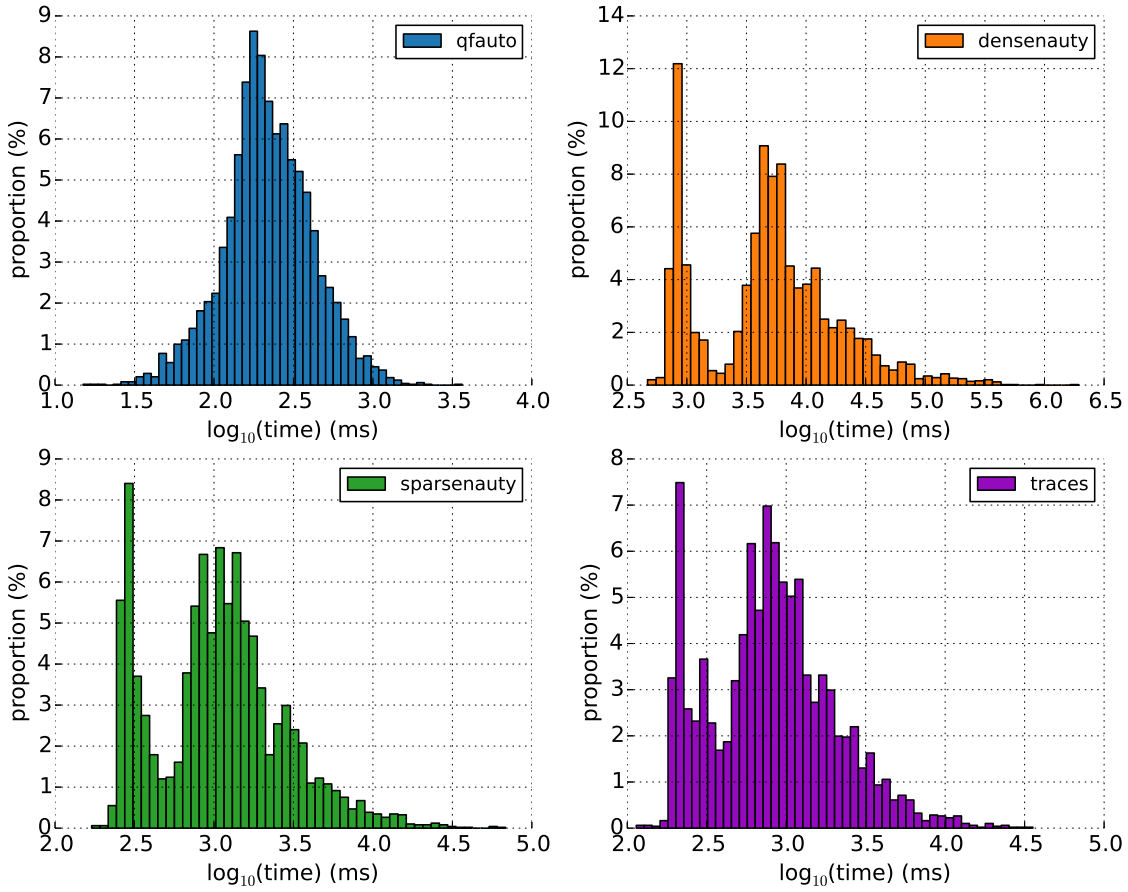


Fig. V.11 – Comparaison des temps de calculs sur les réseaux parfaits de dimension 8.

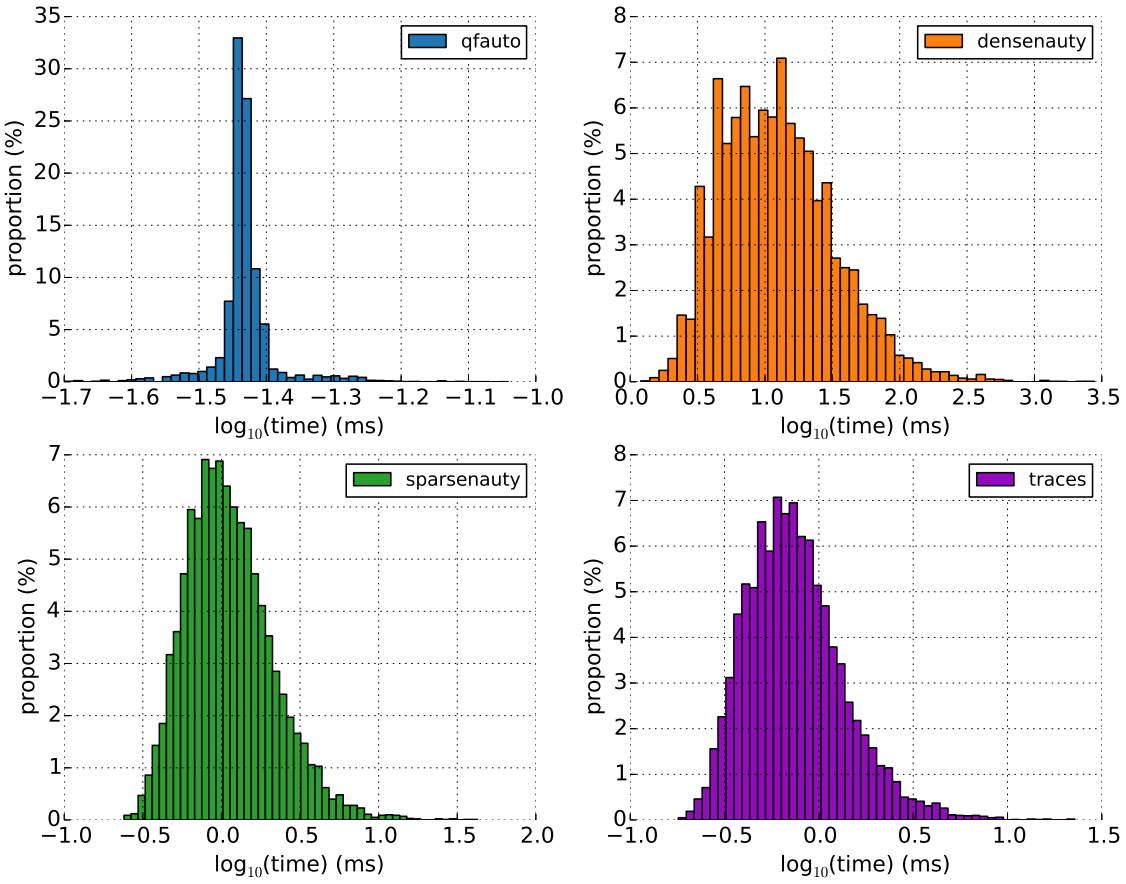


Fig. V.12 – Comparaison des temps de calculs sur 10000 réseaux aléatoires de dimension 20.

CONCLUSION ET PERSPECTIVES

TOUT au long de ce mémoire, nous avons étudié des généralisations de la théorie des réseaux euclidiens et des formes quadratiques, ainsi que des extensions de plusieurs algorithmes et problèmes algorithmiques classiques concernant ces objets. Nous avons notamment pris le soin de présenter ces travaux dans une optique effective. Parmi les algorithmes présentés, plusieurs nous ont permis de développer des implantations performantes.

Nous avons expliqué dans un premier temps comment la notion de réseau euclidien s'étend de manière élémentaire au cas des réseaux sur l'anneau des entiers d'un corps de nombres quadratique imaginaire et euclidien. Les résultats théoriques obtenus dans ce contexte nous ont conduit à généraliser et implanter un algorithme de réduction similaire à celui de Lenstra, Lenstra et Lovász. Nous avons notamment montré que cet algorithme permet de résoudre une variante approchée du problème du plus court vecteur pour ces réseaux, et que cette résolution est en moyenne plus efficace que ce que peut prévoir la théorie.

Plusieurs améliorations et prolongements sont envisageable concernant cet algorithme. Tout d'abord, une analyse de complexité poussée semble être une étape essentielle. Les analyses de complexité déjà menées sur l'algorithme original de Lenstra, Lenstra et Lovász sont probablement généralisables à celui que nous avons présenté. D'autre part, il serait intéressant d'adapter les implantations performantes de l'algorithme classique, comme le *Floating-point LLL*. Rappelons en effet que l'implantation que nous proposons reste élémentaire et est loin d'atteindre le niveau de technicité et d'efficacité des meilleures versions actuellement utilisées.

En ayant en tête l'objectif d'une généralisation aussi large que possible, nous avons introduit dans un second temps les notions de réseaux algébriques et de formes de Humbert. Nous avons montré que la théorie englobant ces objets est plus subtile et complexe que celle des réseaux euclidiens et des formes quadratiques. Néanmoins, de multiples résultats classiques s'étendent

avec plus ou moins de facilité et de précision à ces objets. Nous avons notamment établi la correspondance reliant les réseaux algébriques et les formes de Humbert, équivalent algébrique du dictionnaire échangeant réseaux euclidiens et formes quadratiques.

Nous nous sommes contenté de présenter les résultats élémentaires de la théorie des réseaux algébriques ; de nombreux pans de la théorie classiques restent à généraliser. Citons par exemple les aspects liés à la perfection et l'eutaxie, qui sont théoriquement bien compris mais dont les pendants effectifs sont encore lacunaires.

Nous avons dédié la troisième partie de ce mémoire aux modifications à apporter à l'algorithme de Plesken et Souvignier lui permettant de prendre en charge les réseaux algébriques. Ces changements nous fournissent un algorithme capable de déterminer le groupe des automorphismes algébriques d'un réseau algébrique. Avec quelques modifications, il est aussi capable d'exhiber (le cas échéant) une isométrie algébrique entre deux réseaux algébriques. Cet algorithme a été implanté avec succès dans le système `PARI/gp`. En guise d'application, nous avons montré son utilité pour la résolution du problème de l'équivalence congruentielle de formes quadratiques et de formes de Humbert.

Une analyse de complexité précise de l'algorithme de Plesken et Souvignier classique et de la version modifiée que nous avons présentée serait une avancée décisive vers la compréhension du problème de l'isométrie entre réseaux. D'autre part, notre implantation utilise des méthodes de *backtracking* classiques (tout comme l'algorithme original ou la version utilisée dans `PARI/gp`) ; utiliser certaines routines avancées (comme la méthode des partitions ordonnées, utilisée dans `nauty and Traces`) conduirait probablement à une amélioration substantielle des performances.

Dans un quatrième et dernier temps, nous avons étudié les problèmes de l'isométrie entre réseaux et de la détermination du groupe d'automorphisme d'un réseau. Si nous nous sommes restreint au cas des réseaux euclidiens, nous avons tout de même détaillé le passage du cas euclidien au cas algébrique général. À l'aide d'une série de réductions, nous avons montré que des variantes faibles de ces problèmes sont réductibles à des questions similaires sur les graphes. Ces dernières étant bien mieux comprises, nous en avons déduit des bornes de complexité inédites. Les réductions que nous avons détaillées nous ont permis de développer un nouvel algorithme, qui s'est avéré être parfois plus rapide que les implantations actuellement utilisées.

La réduction entre réseaux et graphes que nous avons présenté est polynomiale *en le nombre de vecteurs courts* du réseau considéré, et non en sa dimension. Obtenir une telle réduction serait un progrès significatif quant à la compréhension des liens qui unissent graphes et réseaux.

LISTE DES ALGORITHMES

LISTE DES FIGURES

A

REPRÉSENTATION DES IDÉAUX D'UN CORPS DE NOMBRES

Sommaire

A.1 Introduction

Un réseau algébrique sur un corps de nombres K est la donnée d'une $K \otimes_{\mathbb{Q}} \mathbb{R}$-base et d'une famille d'idéaux fractionnaires de K. Dans une approche algorithmique, il est naturel d'étudier la problématique de la *représentation* de ces idéaux fractionnaires. Étant donné un idéal fractionnaire non nul de K, comment le représenter dans une optique algorithmique, c'est-à-dire en respectant un compromis entre mémoire occupée et facilité de manipulation ?

Nous rappelons brièvement la représentation matricielle avant de nous concentrer sur la représentation via deux éléments. Nous présentons deux algorithmes permettant d'obtenir une telle représentation de taille réduite. Le second est essentiellement une version modifiée de l'algorithme de Fieker et Stehlé [FS10, fig.1, p.165], lui-même basé sur un algorithme de Belabas [Bel04, algo.6.21, p.51–52].

Dans toute cette annexe, on fixe K un corps de nombres de degré d et on note $\mathcal{O}_K$ son anneau d'entiers.

A.2 Représentation matricielle et forme normale de Hermite

Dans la suite on fixe $\mathfrak{a}$ un idéal fractionnaire de K. Quitte à multiplier $\mathfrak{a}$ par un entier convenable, on supposera généralement que $\mathfrak{a}$ est intégral. On fixe aussi $\Omega := (\omega_1, \dots, \omega_d)$ une base intégrale de K sur $\mathbb{Q}$.

A.2.1 Principe

Il est possible de représenter l'idéal $\mathfrak{a}$ par la matrice des coordonnées de l'une de ses bases dans la base Ω. Ainsi, si $\mathcal{A} := (a_1, \dots a_d)$ est une $\mathbb{Z}$-base de $\mathfrak{a}$ et si $a_j = \sum_{i=1}^{d} a_{i,j}\omega_i$ pour tout $1 \leqslant j \leqslant d$, $\mathfrak{a}$ est représenté par la matrice

$$\mathrm{mat}_\Omega(\mathcal{A}) = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix} \in \mathrm{M}_d(\mathbb{Z}) \cap \mathrm{GL}_d(\mathbb{Q}).$$

Cette représentation est unique modulo l'action de $\mathrm{GL}_d(\mathbb{Z})$, puisque les changements de bases d'un idéal fractionnaire se font par les éléments de $\mathrm{GL}_d(\mathbb{Z})$. Afin d'obtenir la matrice $\mathrm{mat}_\Omega(\mathcal{A})$, il est nécessaire de calculer une $\mathbb{Z}$-base de l'idéal $\mathfrak{a}$. Une méthode classique pour réaliser cette tâche est de partir d'une grande famille génératrice [1] de l'idéal $\mathfrak{a}$ puis d'appliquer un algorithme d'élimination afin d'en extraire une $\mathbb{Z}$-base. L'algorithme d'élimination typiquement utilisé est celui permettant d'obtenir la *forme normale de Hermite*. Notons qu'il est aussi possible d'utiliser un algorithme de réduction (tel que l'algorithme LLL [LLL82]), mais comme remarqué par Belabas dans [Bel04, §5.3.1, p.36], il est généralement possible d'éviter le surcoût entraîné par une réduction systématique des bases des idéaux considérés.

1. Typiquement, lorsque l'on cherche la représentation matricielle du produit d'idéaux, on considère la famille génératrice constituée de la réunion d'une base de chaque idéal impliqué dans le produit.

Définition A.2.1 *Une matrice* $A := (a_{i,j})_{1 \leqslant i,j \leqslant n} \in \mathrm{GL}_n(\mathbb{Z})$ *est dite en forme normale de Hermite si les conditions suivantes sont vérifiées :*

- *A est triangulaire supérieure : pour tous* $1 \leqslant j < i \leqslant n$, *on a* $a_{i,j} = 0$.
- *Les coefficients diagonaux de A sont strictement positifs : pour tous* $1 \leqslant i \leqslant n$, *on a* $a_{i,i} > 0$.
- *Les coefficients non-nuls d'une colonne de A sont tous inférieurs au coefficient de la diagonale correspondant à cette colonne : pour tous* $1 \leqslant i < j \leqslant n$, *on a* $a_{i,j} < a_{i,i}$.

Nous nous restreignons ici au cas des matrices *inversibles* ; la définition de la forme normale de Hermite se généralise néanmoins facilement au cas des matrices quelconques.

Théorème A.2.2 ([Coh93, thm.2.4.3, p.67]) *Soit* $A \in \mathrm{GL}_n(\mathbb{Z})$. *Il existe une unique matrice* $H \in \mathrm{GL}_n(\mathbb{Z})$ *en forme normale de Hermite pour laquelle il existe* $U \in \mathrm{GL}_n(\mathbb{Z})$ *(non-nécessairement unique) telle que* $A = UH$.

Définition A.2.3 *La matrice H du théorème précédent est appelée la forme normale de Hermite de A et est notée*[2] $\mathrm{HNF}(A)$.

On déduit notamment du Théorème A.2.2 une représentation matricielle *unique* (une fois fixée une base intégrale de K sur $\mathbb{Q}$) des idéaux fractionnaires de K.

Corollaire A.2.4 *Soient* Ω *une base intégrale de* K *sur* $\mathbb{Q}$ *et* $\mathfrak{a}$ *un idéal intégral de* K. *Soit A la matrice d'une base de* $\mathfrak{a}$ *dans la base* Ω. *La forme normale de Hermite de A ne dépends que de l'idéal* $\mathfrak{a}$ *et de la base intégrale* Ω *et caractérise complètement* $\mathfrak{a}$.

Démonstration. Soit $\mathfrak{a}$ un idéal de K. Considérons deux bases de $\mathfrak{a}$ de matrice respective A et A' dans la base Ω. Il existe $U, P \in \mathrm{GL}_d(\mathbb{Z})$ tels que $\mathrm{HNF}(A) = UA$ et $A = PA'$. En particulier, on a $\mathrm{HNF}(A) = PUA'$. Par unicité de la forme normale de Hermite et puisque $PU \in \mathrm{GL}_d(ZZ)$, cette égalité entraîne que $\mathrm{HNF}(A') = \mathrm{HNF}(A)$.

Montrons maintenant que deux idéaux avec la même forme normale de Hermite sont égaux. Soient $\mathfrak{a}, \mathfrak{b}$ des idéaux de K de base respective $A, B \in \mathrm{GL}_d(\mathbb{Q}) \cap \mathrm{M}_d(\mathbb{Z})$ (exprimées la base Ω) telles que $\mathrm{HNF}(A) = \mathrm{HNF}(B) = H$. Il existe $U, V \in \mathrm{GL}_d(\mathbb{Z})$ tels que $H = UA = VB$. En particulier, $A = U^{-1}VB$, ce qui montre que A est aussi une base de $\mathfrak{b}$, et donc que $\mathfrak{a} = \mathfrak{b}$. □

A.2.2 Calcul de la forme normale de Hermite

La matrice $\mathrm{mat}(\mathfrak{a})$ est obtenue en calculant la forme normale de Hermite de $\mathrm{mat}_\Omega(\mathcal{A})$ pour $\mathcal{A}$ une base quelconque de $\mathfrak{a}$. Nous renvoyons à [Coh93, §2.4.2, p.67–73] pour une présentation détaillée des algorithmes permettant d'obtenir la forme normale de Hermite d'une matrice.

Même si elle est efficace pour effectuer la plupart des opérations sur les idéaux fractionnaires, la représentation matricielle n'est pas la plus optimisée du point de vue de la mémoire occupée. C'est l'une des raisons qui nous pousse à introduire une méthode de représentation alternative par deux éléments. Notons que la motivation essentielle de cette dernière est le calcul efficace du produit de deux idéaux.

2. HNF pour *Hermite Normal Form*.

A.3 Représentation par deux éléments

A.3.1 Principe

Soit $\mathfrak{a}$ un idéal non nul de $\mathcal{O}_K$. Puisque $\mathcal{O}_K$ est un anneau de Dedekind, pour tout $x_1 \in \mathfrak{a}$ non nul, il existe $x_2 \in \mathfrak{a}$ tel que $\mathfrak{a} = (x_1, x_2)$. Il est ainsi possible de représenter $\mathfrak{a}$ par seulement deux éléments. Cette représentation est plus économique en terme de mémoire occupée que la représentation matricielle, mais elle peut être plus délicate à obtenir et à manipuler que cette dernière. Ce résultat repose sur le principe d'approximation faible (voir [Coh93, prop.4.7.7-8, p.192], dont la preuve est constructive : elle contient un algorithme naïf.

A.3.2 Algorithme naïf et amélioration

Comme remarqué dans [Coh00, algo.1.3.15, p.24], étant donné $x_1 \in \mathfrak{a}$ non nul, la recherche aléatoire est une méthode certes naïve, mais efficace, pour trouver $x_2 \in \mathfrak{a}$ tel que $(x_1, x_2) = \mathfrak{a}$. Dans la suite, on note $\mathrm{Sp}(\mathcal{O}_K)$ l'ensemble des idéaux premiers de $\mathcal{O}_K$. Une preuve du résultat suivant est présentée dans [Bel04, lem.6.14, p.51].

Proposition A.3.1 *Étant donné $x_1 \in \mathfrak{a}$ non nul, si x_2 est choisit uniformément dans $\mathfrak{a}/(x_1)$, alors :*

$$\mathbb{P}[(x_1, x_2) = \mathfrak{a}] = \prod_{\substack{\mathfrak{p} \in \mathrm{Sp}(\mathcal{O}_K) \\ v_\mathfrak{p}(x_1) > v_\mathfrak{p}(\mathfrak{a})}} \left(1 - \frac{1}{\mathcal{N}(\mathfrak{p})}\right) \geqslant \prod_{\substack{\mathfrak{p} \in \mathrm{Sp}(\mathcal{O}_K) \\ \mathfrak{p} \mid \mathfrak{a}}} \left(1 - \frac{1}{\mathcal{N}(\mathfrak{p})}\right).$$

À l'heure actuelle, nous ne connaissons pas de minoration de ce taux de réussite indépendante de $\mathfrak{a}$ et du corps K. L'Algorithme A.1 décrit une procédure utilisant cette recherche aléatoire naïve. Nous imposons à cet algorithme de se terminer en un temps t donné, et nous l'autorisons donc à échouer. Il est évidemment possible de construire un algorithme qui n'échoue jamais, mais dont le temps de calcul n'est pas maîtrisé. Une version plus évoluée de cette méthode est présentée par Belabas dans [Bel04, algo.6.15, p.51]. Elle est actuellement utilisée dans le système PARI/gp [PARI/gp].

```
Données :
    • Un élément non nul x_1 d'un idéal intégral a.
    • Un paramètre de succès t ⩾ 1.
Résultat :
    • x_2 ∈ a tel que (x_1, x_2) = a ou Échec.
pour i = 1 à t faire
    Choisir x_2 uniformément dans a/(x_1).
    si (x_1, x_2) = a alors
        retourner x_2.
retourner Échec.
```

Algorithme A.1 - Représentation par deux éléments : méthode naïve.

A.4 Représentation par deux éléments courts

La représentation par deux éléments occupe moins de mémoire que la représentation matricielle. Il est possible d'optimiser cette propriété en recherchant une représentation par deux éléments courts au sens de la norme T_2 (définie dans la Section II.2.1). Nous proposons deux algorithmes permettant d'obtenir une telle représentation. Le premier algorithme est théoriquement plus efficace que le second en terme de la taille des éléments obtenus, mais son taux de réussite est dépendant de l'idéal considéré, et plus généralement du corps de nombres dans lequel on se place.

A.4.1 Réduction forte, taux de réussite non maîtrisé

L'Algorithme A.2 est une adaptation de la méthode naïve par recherche aléatoire, détaillée dans le paragraphe précédent. Rappelons qu'en vertu de la Proposition II.3.8, un idéal fractionnaire de K s'identifie à un $\mathbb{Z}$-réseau de $K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R}$, donc à un $\mathbb{Z}$-réseau de $\mathbb{R}^d$. Dès lors, par *base réduite de* $\mathfrak{a}$, nous entendons une base réduite de $\mathfrak{a}$ vu comme $\mathbb{Z}$-réseau euclidien. De même, le *volume* de $\mathfrak{a}$, noté $\mathrm{vol}(\mathfrak{a})$, désigne le volume de $\mathfrak{a}$ vu comme réseau euclidien de $\mathbb{R}^d$. Nous avons fait le choix d'équiper $K_{\mathbb{R}}$ de la norme T_2, $\mathbb{R}^d$ n'est donc pas équipé de sa structure euclidienne classique et le volume de $\mathfrak{a}$ est calculé à l'aide de la mesure de Lebesgue multipliée par 2^s. En particulier, rappelons le résultat suivant :

Proposition A.4.1 ([Sam67, prop.2, p.69]) *Soit $\mathfrak{a}$ un idéal fractionnaire non nul de K. On a*

$$\mathrm{vol}(\mathfrak{a}) = |\Delta_K|^{1/2}\mathcal{N}(\mathfrak{a}),$$

où Δ_K désigne le discriminant de K.

Théorème A.4.2 *Fixons une base intégrale $\Omega := (\omega_1, \ldots, \omega_d)$ de K telle que $\omega_1 = 1$. Étant donné $\mathfrak{a}$ un idéal intégral non nul de K et un paramètre de succès $t \geqslant 1$, l'Algorithme A.2 renvoie avec une probabilité supérieure à*

$$1 - \left(1 - \prod_{\substack{\mathfrak{p} \in \mathrm{Sp}(\mathcal{O}_K) \\ \mathfrak{p} | \mathfrak{a}}} \left(1 - \frac{1}{\mathcal{N}(\mathfrak{p})}\right)\right)^t$$

et en temps polynomial deux éléments $x_1, x_2 \in \mathfrak{a}$ tels que $(x_1, x_2) = \mathfrak{a}$ et

$$\max\{\|x_1\|, \|x_2\|\} \leqslant \eta^{(d-1)/4} |\Delta_K|^{1/2d} \ell_1(\Omega) \mathcal{N}(\mathfrak{a})^{1/d}, \tag{A.1}$$

où :

- *$\eta := (\lambda - 0.25)^{-1}$, avec $0.25 < \lambda < 1$ la constante de Lovász pour la LLL-réduction.*
- *Δ_K est le discriminant de K.*
- *$\ell_1(\Omega) := \sum_{i=1}^{d} \|\omega_i\|$.*

Données :
- Un idéal intégral non nul $\mathfrak{a}$ de K, supposé distinct de $\mathcal{O}_K$.
- Un paramètre de succès $t \geqslant 1$.

Résultat :
- $x_1, x_2 \in \mathfrak{a}$ tels que $\mathfrak{a} = (x_1, x_2)$ ou Échec.

soit x_1 le premier vecteur d'une base réduite de $\mathfrak{a}$.
si $\mathfrak{a} = (x_1)$ alors
    retourner $(x_1, 0)$.
pour $i = 1$ à t faire
    choisir x_2 uniformément dans $\mathfrak{a}/(x_1)$.
    si $(x_1, x_2) = \mathfrak{a}$ alors
        aller à l'étape 9.
retourner Échec.
réduire fortement x_2 suivant $(x_1\omega_i)_{1\leqslant i\leqslant d}$.
retourner (x_1, x_2).

Algorithme A.2 - Représentation par deux éléments courts : version 1.

Remarque A.4.3 Comme mentionné dans [Bel04, §4.3, p.28–29], il est toujours possible de choisir une base intégrale de K comprenant l'unité de $\mathcal{O}_K$. Cette condition est essentiellement imposée afin d'assurer que $\ell_1(\Omega) \geqslant d \geqslant 1$.

Démonstration. Puisque x_1 est le premier vecteur d'une base LLL-réduite $\mathcal{X} := (x_1, \ldots, x_d)$ de $\mathfrak{a}$, en notant $(x_1^*, \ldots, x_d^*)$ la base orthogonale obtenue par application du procédé d'orthogonalisation de Gram/Schmidt à $\mathcal{X}$, on a par la Proposition A.4.1 :

$$\|x_1\|^{2d} \leqslant \prod_{i=1}^{d} \eta^{i-1}\|x_i^*\|^2 = \eta^{d(d-1)/2}\,\mathrm{vol}(\mathfrak{a})^2 = \eta^{d(d-1)/2}|\Delta_K|\mathcal{N}(\mathfrak{a})^2,$$

donc

$$\|x_1\|^2 \leqslant \eta^{(d-1)/2}|\Delta_K|^{1/d}\mathcal{N}(\mathfrak{a})^{2/d}. \tag{A.2}$$

L'opération de réduction forte suivant $(x_1\omega_i)_{1\leqslant i\leqslant d}$ consiste à remplacer

$$x_2 = \sum_{i=1}^{d} \alpha_i x_1 \omega_i$$

avec $\alpha_i \in \mathbb{Q}$ pour tout $1 \leqslant i \leqslant d$ par

$$\sum_{i=1}^{d} (\alpha_i - \lfloor \alpha_i \rceil) x_1 \omega_i.$$

Remarquons que puisque $\sum_{i=1}^{d} \lfloor \alpha_i \rceil x_1 \omega_i \in (x_1)$, la relation $\mathfrak{a} = (x_1, x_2)$ est préservée par la réduction forte. Après cette opération, on a

$$\|x_2\| \leqslant \sum_{i=1}^{d} |\alpha_i - \lfloor \alpha_i \rceil| \cdot \|x_1 \omega_i\| \leqslant \|x_1\| \ell_1(\Omega).$$

De l'inégalité (A.2) on déduit alors

$$\|x_2\| \leqslant \eta^{(d-1)/4} |\Delta_K|^{1/2d} \ell_1(\Omega) \mathcal{N}(\mathfrak{a})^{1/d}. \tag{A.3}$$

Puisque $\ell_1(\Omega) \geqslant 1$, on obtient finalement à partir de (A.2) et (A.3) l'inégalité (A.1) annoncée. L'Algorithme A.2 renvoie donc bien le résultat attendu. L'analyse de son taux de réussite découle directement de la Proposition A.3.1. □

Notons le taux de réussite de cet algorithme est conditionné par un paramètre de succès t, qui définit simplement le nombre maximal de tirages autorisés pour obtenir une relation du type $(x_1, x_2) = \mathfrak{a}$.

La quantité $\eta^{(d-1)/4} |\Delta_K|^{1/2d}$ ne dépend que du corps K. Si la base intégrale Ω est choisie LLL-réduite, il est de plus possible de majorer $\ell_1(\Omega)$ par une quantité ne dépendant elle aussi que du corps K (voir [FS10, lem.1]). Par conséquent :

Corollaire A.4.4 *Tout idéal intégral $\mathfrak{a}$ de K peut être représenté par deux éléments dont la taille en norme T_2 est en $\mathcal{O}(\mathcal{N}(\mathfrak{a})^{1/d})$.*

A.4.2 Réduction affaiblie, taux de réussite maîtrisé

Le taux de réussite variable de l'algorithme précédent peut être problématique. Nous proposons donc un autre algorithme dont la propension à échouer est mieux contrôlée, au prix d'un important affaiblissement de la borne théorique (A.1) et d'une forte complexification. C'est une version modifiée de l'algorithme de Fiecker et Stehlé [FS10, fig.1].

Dans un premier temps, nous avons besoin d'un algorithme permettant d'énumérer les idéaux premiers de $\mathcal{O}_K$ de petite norme. Dans la suite, pour $y \geqslant 1$, on note

$$\mathrm{Sp}_y(\mathcal{O}_K) := \{\mathfrak{p} \in \mathrm{Sp}(\mathcal{O}_K) \,:\, \mathcal{N}(\mathfrak{p}) \leqslant y\}.$$

Lemme A.4.5 *Étant donné un entier $y \geqslant 1$, l'Algorithme A.3 détermine correctement l'ensemble $\mathrm{Sp}_y(\mathcal{O}_K)$.*

Démonstration. Soit $\mathfrak{p} \in \mathrm{Sp}_y(\mathcal{O}_K)$. Il existe un unique nombre premier $p \in \mathrm{Sp}(\mathbb{Z})$ (divisible par $\mathfrak{p}$) tel que $\mathcal{N}(\mathfrak{p}) = p^\alpha$ pour un certain $\alpha \in \mathbb{N}_{>0}$. En particulier, on a nécessairement $p \leqslant y$. Ainsi, les éléments de $\mathrm{Sp}(\mathcal{O}_K)$ de norme inférieure à y sont parmi les diviseurs des nombres premiers inférieurs à y, ce qui prouve la correction de l'Algorithme A.3. □

Données :
- Un entier $y \geqslant 1$.

Résultat :
- L'ensemble $\mathrm{Sp}_y(\mathcal{O}_K)$.

soit $S := \emptyset$.
calculer $\mathrm{Sp}_y(\mathbb{Z}) := \{p \in \mathrm{Sp}(\mathbb{Z}) : 0 \leqslant p \leqslant y\}$.
pour chaque $p \in \mathrm{Sp}_y(\mathbb{Z})$ faire
    factoriser $p = \prod_{i=1}^{n} \mathfrak{p}_i^{e_i}$ dans $\mathcal{O}_K$.
    pour $i = 1$ à n faire
        si $\mathcal{N}(\mathfrak{p}_i) \leqslant y$ alors
            ajouter $\mathfrak{p}_i$ à S.
retourner S.

Algorithme A.3 - Calcul des idéaux premiers de petite norme.

Soit $p \leqslant y$ un nombre premier. Si l'algorithme de factorisation employé renvoie l'indice résiduel $f_{\mathfrak{p}}$ d'un diviseur $\mathfrak{p}$ de p (c'est par exemple le cas de l'algorithme utilisé dans PARI/gp), au lieu de vérifier que $\mathcal{N}(\mathfrak{p}) \leqslant y$, il suffit de vérifier que $p^{f_{\mathfrak{p}}} \leqslant y$, puisque $\mathcal{N}(\mathfrak{p}) = p^{f_{\mathfrak{p}}}$.

Théorème A.4.6 *Fixons une base intégrale $\Omega := (\omega_1, \ldots, \omega_d)$ de K telle que $\omega_1 = 1$. Étant donné $\mathfrak{a}$ un idéal intégral non nul de K et un paramètre de succès $t \geqslant 1$, l'Algorithme A.4 renvoie avec une probabilité supérieure à*

$$1 - \left(1 - \left(1 - \frac{1}{\alpha}\right)^{\alpha}\right)^{t}$$

et en temps polynomial deux éléments $x_1, x_2 \in \mathfrak{a}$ tels que $(x_1, x_2) = \mathfrak{a}$ et

$$\max\{\|x_1\|, \|x_2\|\} \leqslant \frac{4\eta^{7(d-1)/4} |\Delta_K|^{7/2d}}{d^{3/2}} \ell_1(\Omega)^4 \mathcal{N}(\mathfrak{a})^{4/d}, \tag{A.4}$$

où :

- $\alpha := e^{W(\log(2))}$, *où W désigne la fonction de Lambert.*
- $\eta := (\lambda - 0.25)^{-1}$, *avec $0.25 < \lambda < 1$ la constante de Lovász pour la LLL-réduction.*
- Δ_K *est le discriminant de K.*
- $\ell_1(\Omega) := \sum_{i=1}^{d} \|\omega_i\|$.

Remarque A.4.7 En pratique, à l'aide des fonctions de la librairie PARI/gp [PARI/gp] permettant d'approximer la fonction W de Lambert et la fonction exponentielle, on obtient la majoration $1 - \left(1 - \frac{1}{\alpha}\right)^{\alpha} \geqslant \frac{71}{89}$. De manière plus explicite, le taux de réussite de l'Algorithme A.4 est donc supérieur à $1 - \left(\frac{71}{89}\right)^{t} \approx 1 - 0,8^{t}$.

Démonstration. Nous reprenons la preuve proposée par Fiecker et Stehlé dans [FS10, p.164]. Nous renvoyons notamment à cet article en ce qui concerne l'analyse de la complexité de l'algorithme. Nous montrons dans un premier temps que l'algorithme est correct (en supposant qu'il n'échoue pas), puis nous étudions son taux de réussite.

Données :
- Un idéal intégral non nul $\mathfrak{a}$ de K.
- Un paramètre de succès $t \geqslant 1$.

Résultat :
- $x_1, x_2 \in \mathfrak{a}$ tels que $\mathfrak{a} = (x_1, x_2)$ ou Échec.

soit x_1 le premier vecteur d'une base réduite de $\mathfrak{a}$. Soit $\mathfrak{b} = (x_1)$.
si $\mathfrak{a} = \mathfrak{b}$ alors
    retourner $(x_1, 0)$.
soit y tel que $y \log(y) = \log(\mathcal{N}(\mathfrak{b}))$.
calculer $\mathrm{Sp}_y(\mathcal{O}_K)$ à l'aide de l'Algorithme A.3.
soient $\mathfrak{b}_0 := \prod_{\mathfrak{p} \in \mathrm{Sp}_y(\mathcal{O}_K)} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{b})}$, $\mathfrak{a}_0 := \prod_{\mathfrak{p} \in \mathrm{Sp}_y(\mathcal{O}_K)} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})}$, $\mathfrak{b}_1 := \mathfrak{b}\mathfrak{b}_0^{-1}$ et $\mathfrak{a}_1 := \mathfrak{a}\mathfrak{a}_0^{-1}$.
pour $i = 1$ à t faire
    choisir π_1 uniformément dans $\mathfrak{a}_1/\mathfrak{b}_1$.
    si $\mathfrak{a}_1 = \mathfrak{b}_1 + (\pi_1)$ alors
        Aller à l'étape 11.
retourner Échec.
si $\mathfrak{b}_0 = \mathcal{O}_K$ alors
    réduire fortement π_1 suivant $(x_1\omega_i)_{1 \leqslant i \leqslant d}$.
    retourner (x_1, π_1).
soit b le premier vecteur d'une base réduite de $\mathfrak{b}_1$.
réduire fortement π_1 suivant $(b\omega_i)_{1 \leqslant i \leqslant d}$.
si $\mathfrak{a}_0 = \mathcal{O}_K$ alors
    choisir $\pi_0 = 1$.
sinon
    calculer $S := \{\mathfrak{p} \in \mathrm{Sp}(\mathcal{O}_K) : \mathfrak{p} | \mathfrak{a}_0\}$.
    trouver $\pi_0 \in \mathcal{O}_K$ tel que $v_\mathfrak{p}(\pi_0) = v_\mathfrak{p}(\mathfrak{a}_0)$ pour tout $\mathfrak{p} \in S$.
    soit b le premier vecteur d'une base réduite de $\prod_{\mathfrak{p} \in S} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a}_0)+1}$.
    réduire faiblement π_0 suivant $(b\omega_i)_{1 \leqslant i \leqslant d}$.
trouver $\beta_0 \in \mathfrak{b}_0$ et $\beta_1 \in \mathfrak{b}_1$ tels que $\beta_0 + \beta_1 = 1$.
soit b le premier vecteur d'une base réduite de $\mathfrak{b}$.
réduire fortement β_0 et β_1 suivant $(b\omega_i)_{1 \leqslant i \leqslant d}$.
soit $x_2 = (\pi_0\beta_1 + \beta_0)(\pi_1\beta_0 + \beta_1)$.
retourner (x_1, x_2).

Algorithme A.4 - Représentation par deux éléments courts : version 2.

Correction de l'algorithme. Soient x_1 le premier vecteur d'une base réduite de $\mathfrak{a}$ et $\mathfrak{b} := (x_1)$. On calcule y tel que $y\log(y) = \log(\mathcal{N}(\mathfrak{b}))$ en évaluant :

$$y = e^{W(\log(\mathcal{N}(\mathfrak{b}))},$$

où W désigne la fonction de Lambert. Dans la suite, on pose

$$\mathfrak{b}_0 := \prod_{\mathfrak{p}\in \mathrm{Sp}_y(\mathcal{O}_K)} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{b})},$$

$$\mathfrak{a}_0 := \prod_{\mathfrak{p}\in \mathrm{Sp}_y(\mathcal{O}_K)} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})},$$

$\mathfrak{b}_1 := \mathfrak{b}\mathfrak{b}_0^{-1}$ et $\mathfrak{a}_1 := \mathfrak{a}\mathfrak{a}_0^{-1}$.

Le cas $\mathfrak{b}_0 = \mathcal{O}_K$ est traité par le Théorème A.4.2, puisque dans cette situation, $\mathfrak{a}_0 = \mathcal{O}_K$, $\mathfrak{a}_1 = \mathfrak{a}$ et $\mathfrak{b}_1 = \mathfrak{b} = (x_1)$. Remarquons néanmoins que puisque $\ell_1(\Omega) \geqslant d$ et

$$\eta^{(d-1)/4}|\Delta_K|^{1/2d}\ell_1(\Omega) \leqslant 4\frac{4eta^{7(d-1)/4}|\Delta_K|^{4/d}}{d^{3/2}}\ell_1(\Omega)^4,$$

l'inégalité (A.1) entraîne l'inégalité (A.4).

Nous supposons donc dans la suite que $\mathfrak{b}_0 \neq \mathcal{O}_K$. Puisque π_1 est fortement réduit suivant $(b\omega_i)_{1\leqslant i\leqslant d}$, où b est le premier vecteur d'une base réduite de $\mathfrak{b}_1$, on montre par la méthode employée pour prouver l'inégalité (A.3) que

$$\|\pi_1\| \leqslant \eta^{(d-1)/4}|\Delta_K|^{1/2d}\ell_1(\Omega)\mathcal{N}(\mathfrak{b}_1)^{1/d} \tag{A.5}$$

après la ligne 16, tout en préservant la relation

$$\mathfrak{a}_1 = \mathfrak{b}_1 + (\pi_1). \tag{A.6}$$

Si $\mathfrak{a}_0 = \mathcal{O}_K$, on pose $\pi_0 = 1$. Dans ce cas $\mathfrak{a}_0 = \mathfrak{b}_0 + (\pi_0)$. Montrons que $\pi_0 = 1$ vérifie

$$\|\pi_0\| \leqslant \ell_1(\Omega) \leqslant 2^{-s/2d}\eta^{(d-1)/4}|\Delta_K|^{1/2d}\ell_1(\Omega)\mathcal{N}(\mathfrak{a}_0)^{2/d}.$$

Sachant que $\|\pi_0\| \leqslant \ell_1(\Omega)$ et $\mathcal{N}(\mathfrak{a}_0)^{2/d} = 1$, il suffit pour cela de montrer que

$$\eta^{(d-1)/4}|\Delta_K|^{1/2d} \geqslant 1.$$

Excluons le cas trivial $K = \mathbb{Q}$ et supposons que $d \geqslant 2$. En vertu de la borne de Minkowski [Neu13, prop.2.14, p.204], on a

$$|\Delta_K|^{1/2d} \geqslant \left(\left(\frac{\pi}{4}\right)^s \frac{d^d}{d!}\right)^{1/d} \geqslant \frac{d}{(d!)^{1/d}} \geqslant \frac{2}{2^{1/2}}.$$

Utilisée avec $\eta^{(d-1)/2} \geqslant (4/3)^{1/4}$, cette dernière inégalité montre le résultat attendu.

Supposons maintenant que $\mathfrak{a}_0 \neq \mathcal{O}_K$, et posons $S := \{\mathfrak{p} \in \mathrm{Sp}(\mathcal{O}_K) \ : \ \mathfrak{p} | \mathfrak{a}_0\} \subset \mathrm{Sp}_y(\mathcal{O}_K)$. Un élément $\pi_0 \in \mathcal{O}_K$ tel que $v_\mathfrak{p}(\pi_0) = v_\mathfrak{p}(\mathfrak{a}_0)$ pour tout $\mathfrak{p} \in S$ est déterminé via le principe d'approximation faible, en utilisant par exemple [Bel04, algo. 6.8, p. 49]. Notons

$$\mathfrak{a}_0' := \prod_{\mathfrak{p} \in S} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a}_0)+1}$$

et considérons b le premier vecteur d'une base réduite de $\mathfrak{a}_0'$.

Si ε_1 désigne la réduction forte de π_1 suivant $(b\omega_i)_{1 \leqslant i \leqslant d}$, nous appelons réduction faible de π_1 suivant $(b\omega_i)_{1 \leqslant i \leqslant d}$ le remplacement de π_1 par ε_1 si $\varepsilon_1 \neq 0$, et b sinon. Notons $\widetilde{\pi}_0$ la valeur ainsi obtenue. On peut écrire $\widetilde{\pi}_0 = \pi_0 + \tau$ avec $\tau \in \mathfrak{a}_0'$. Ainsi[3], pour tout $\mathfrak{p} \in S$, puisque $v_\mathfrak{p}(\tau) \geqslant v_\mathfrak{p}(\mathfrak{a}_0') > v_\mathfrak{p}(\mathfrak{a}_0) = v_\mathfrak{p}(\pi_0)$, on a $v_\mathfrak{p}(\widetilde{\pi}_0) = v_\mathfrak{p}(\pi_0) = v_\mathfrak{p}(\mathfrak{a}_0)$, ce qui entraîne l'égalité

$$v_\mathfrak{p}(\mathfrak{b}_0 + (\widetilde{\pi}_0)) = \min\{v_\mathfrak{p}(\mathfrak{b}_0)\,;\, v_\mathfrak{p}(\widetilde{\pi}_0)\} = \min\{v_\mathfrak{p}(\mathfrak{b})\,;\, v_\mathfrak{p}(\mathfrak{a}_0)\} = v_\mathfrak{p}(\mathfrak{a}_0).$$

Ceci permet de conclure que $\mathfrak{b}_0 + (\widetilde{\pi}_0) = \mathfrak{a}_0$. D'autre part, en utilisant un analogue de l'inégalité (A.3) pour b et $\mathfrak{a}_0'$ (le cas $\widetilde{\pi}_0 = b$ étant trivial) :

$$\|\widetilde{\pi}_0\| \leqslant \eta^{(d-1)/4} |\Delta_K|^{1/2d} \ell_1(\Omega) \mathcal{N}(\mathfrak{a}_0')^{1/d} \leqslant \eta^{(d-1)/4} |\Delta_K|^{1/2d} \ell_1(\Omega) \mathcal{N}(\mathfrak{a}_0)^{2/d},$$

la dernière inégalité découlant de $0 < v_\mathfrak{p}(\mathfrak{a}_0') = v_\mathfrak{p}(\mathfrak{a}_0) + 1 \leqslant 2v_\mathfrak{p}(\mathfrak{a}_0)$ pour tout $\mathfrak{p} \in S$.

Finalement, nous avons montré qu'en arrivant à la ligne 24 de l'algorithme

$$\|\pi_0\| \leqslant \eta^{(d-1)/4} |\Delta_K|^{1/2d} \ell_1(\Omega) \mathcal{N}(\mathfrak{a}_0)^{2/d} \tag{A.7}$$

et

$$\mathfrak{a}_0 = \mathfrak{b}_0 + (\pi_0). \tag{A.8}$$

Par construction, $\mathfrak{b}_0$ et $\mathfrak{b}_1$ sont des idéaux premiers entre eux. Il est donc possible (en utilisant par exemple [Coh00, algo.1.3.2, p.17]) de trouver $\beta_0 \in \mathfrak{b}_0$ et $\beta_1 \in \mathfrak{b}_1$ tels que $\beta_0 + \beta_1 = 1$. Notons b le premier vecteur d'une base réduite de $\mathfrak{b}$. La réduction forte de β_j suivant $(b\omega_i)_{1 \leqslant i \leqslant d}$ entraîne comme vu dans l'inégalité (A.3) que :

$$\|\beta_j\| \leqslant \eta^{(d-1)/4} |\Delta_K|^{1/2d} \ell_1(\Omega) \mathcal{N}(\mathfrak{b})^{1/d} \qquad j \in \{0, 1\}. \tag{A.9}$$

Posons $x_2 = (\pi_0\beta_1 + \beta_0)(\pi_1\beta_0 + \beta_1)$. On montre en utilisant le même argument que [FS10, p.166] et via les relations (A.6) et (A.8) que

$$\mathfrak{a} = (x_1, x_2).$$

Ainsi, l'algorithme renvoie bien une représentation de $\mathfrak{a}$ par deux éléments. Reste à montrer que ces deux éléments sont courts. Puisque $\ell_1(\Omega) \geqslant d$, l'inégalité (A.2) entraîne

$$\|x_1\| \leqslant \frac{4\eta^{7(d-1)/4} |\Delta_K|^{7/2d}}{d^{3/2}} \ell_1(\Omega)^4 \mathcal{N}(\mathfrak{a})^{4/d}.$$

3. Nous avons pris soin d'imposer $\widetilde{\pi}_0 \neq 0$; nous pouvons donc légitimement considérer les valuations $\mathfrak{p}$-adiques de $\widetilde{\pi}_0$.

D'autre part, en utilisant les inégalités (A.5), (A.7) et (A.9) et en posant $\kappa := \eta^{(d-1)/4}|\Delta_K|^{1/2d}\ell_1(\Omega)$, on montre que

$$\begin{aligned}
\|x_2\| &\leqslant (\|\pi_0\| \cdot \|\beta_1\| + \|\beta_0\|) \cdot (\|\pi_1\| \cdot \|\beta_0\| + \|\beta_1\|) \\
&\leqslant \left(\kappa^2 \mathcal{N}(\mathfrak{a}_0)^{2/d} \mathcal{N}(\mathfrak{b})^{1/d} + \kappa \mathcal{N}(\mathfrak{b})^{1/d}\right)\left(\kappa^2 \mathcal{N}(\mathfrak{b}_1)^{1/d} \mathcal{N}(\mathfrak{b})^{1/d} + \kappa \mathcal{N}(\mathfrak{b})^{1/d}\right) \\
&= \kappa^4 \mathcal{N}(\mathfrak{b})^{2/d}\left(\mathcal{N}(\mathfrak{a}_0)^{2/d} + 1\right)\left(\mathcal{N}(\mathfrak{b}_1)^{1/d} + 1\right) \\
&\leqslant 4\kappa^4 \mathcal{N}(\mathfrak{b})^{2/d} \mathcal{N}(\mathfrak{a}_0)^{2/d} \mathcal{N}(\mathfrak{b}_1)^{1/d} \\
&\leqslant 4\kappa^4 \mathcal{N}(\mathfrak{b})^{2/d} \mathcal{N}(\mathfrak{a}_0)^{2/d} \left(\frac{\mathcal{N}(\mathfrak{b})}{\mathcal{N}(\mathfrak{a}_0)}\right)^{1/d} \\
&\leqslant 4\kappa^4 \mathcal{N}(\mathfrak{b})^{3/d} \mathcal{N}(\mathfrak{a})^{1/d}
\end{aligned}$$

Or en utilisant l'inégalité arithmético-géométrique et l'inégalité (A.2), on peut borner $\mathcal{N}(\mathfrak{b})$ en fonction de $\mathcal{N}(\mathfrak{a})$:

$$\mathcal{N}(\mathfrak{b})^{1/d} = |N_{K/\mathbb{Q}}(x_1)|^{1/d} \leqslant \frac{1}{d^{1/2}}\|x_1\| \leqslant \frac{\eta^{(d-1)/4}|\Delta_K|^{1/2d}}{d^{1/2}} \mathcal{N}(\mathfrak{a})^{1/d}.$$

Finalement :

$$\|x_2\| \leqslant \frac{4\eta^{7(d-1)/4}|\Delta_K|^{7/2d}}{d^{3/2}} \ell_1(\Omega)^4 \mathcal{N}(\mathfrak{a})^{4/d}.$$

L'inégalité (A.4) est vérifiée, et l'Algorithme A.4 renvoie donc bien le résultat annoncé.

Analyse du taux de réussite. En adaptant la preuve de la Proposition A.3.1, on montre que la probabilité de réussite de l'algorithme est :

$$\mathbb{P}[\text{réussite}] \geqslant 1 - \left(1 - \prod_{\substack{\mathfrak{p} \in \mathrm{Sp}(\mathcal{O}_K) \\ \mathfrak{p} | \mathfrak{b}_1}} \left(1 - \frac{1}{\mathcal{N}(\mathfrak{p})}\right)\right)^t.$$

Mais puisque $\mathfrak{p}|\mathfrak{b}_1$ entraîne que $\mathcal{N}(\mathfrak{p}) \geqslant y$, on a

$$\prod_{\substack{\mathfrak{p} \in \mathrm{Sp}(\mathcal{O}_K) \\ \mathfrak{p} | \mathfrak{b}_1}} \left(1 - \frac{1}{\mathcal{N}(\mathfrak{p})}\right) \geqslant \left(1 - \frac{1}{y}\right)^{\#\{\mathfrak{p} \in \mathrm{Sp}(\mathcal{O}_K) : \mathfrak{p} | \mathfrak{b}_1\}}.$$

Pour la même raison, on a $\mathcal{N}(\mathfrak{b}) \geqslant \mathcal{N}(\mathfrak{b}_1) \geqslant y^{\#\{\mathfrak{p} \in \mathrm{Sp}(\mathcal{O}_K) : \mathfrak{p} | \mathfrak{b}_1\}}$, donc $\#\{\mathfrak{p} \in \mathrm{Sp}(\mathcal{O}_K) : \mathfrak{p}|\mathfrak{b}_1\} \leqslant \log_y(\mathcal{N}(\mathfrak{b}))$. Ainsi :

$$\prod_{\substack{\mathfrak{p} \in \mathrm{Sp}(\mathcal{O}_K) \\ \mathfrak{p} | \mathfrak{b}_1}} \left(1 - \frac{1}{\mathcal{N}(\mathfrak{p})}\right) \geqslant \left(1 - \frac{1}{y}\right)^{\#\{\mathfrak{p} \in \mathrm{Sp}(\mathcal{O}_K) : \mathfrak{p} | \mathfrak{b}_1\}} \geqslant \left(1 - \frac{1}{y}\right)^{\log_y(\mathcal{N}(\mathfrak{b}))}.$$

Puisque la relation $y\log(y) = \log(\mathcal{N}(\mathfrak{b}))$ entraîne que $y = \log_y(\mathcal{N}(\mathfrak{b}))$, on obtient finalement

$$\mathbb{P}[\text{réussite}] \geqslant 1 - \left(1 - \left(1 - \frac{1}{y}\right)^y\right)^t.$$

La fonction W de Lambert étant croissante,

$$y = e^{W(\log(\mathcal{N}(\mathfrak{a})))} \geqslant e^{W(\log 2)} \geqslant 1$$

et donc par croissance de la fonction $x \mapsto \left(1-\frac{1}{x}\right)^x$ sur $[1,+\infty[$, en posant $\alpha := e^{W(\log(2))}$

$$\left(1-\frac{1}{y}\right)^y \geqslant \left(1-\frac{1}{\alpha}\right)^\alpha,$$

ce qui justifie le taux de réussite annoncé. □

La quantité $\frac{4\eta^{7(d-1)/4}|\Delta_K|^{7/2d}}{d^{3/2}}$ ne dépend encore une fois que du corps K. Comme remarqué précédemment, si la base intégrale Ω est choisie réduite (au sens LLL), on peut majorer $\ell_1(\Omega)^4$ par une quantité ne dépendant elle aussi que du corps K. On obtient ainsi une représentation de $\mathfrak{a}$ par des éléments de taille en $\mathcal{O}(\mathcal{N}(\mathfrak{a})^{4/d})$. Cette représentation est en théorie moins courte que celle décrite au paragraphe précédent, mais son obtention est plus sûre. De plus, cet algorithme est généralement plus lent que le précédent.

Remarque A.4.8 Plusieurs différences sont à noter entre notre version et celle de Fiecker et Stehlé :

- La borne (A.4) est originellement exprimée en fonction de $\ell_\infty(\Omega) := \max_{1\leqslant i\leqslant d}\|\omega_i\|$ plutôt qu'avec $\ell_1(\Omega)$. Exprimée en termes de $\ell_\infty(\Omega)$, la relation (A.4) devient

  $$\max\{\|x_1\|,\|x_2\|\} \leqslant 4\eta^{7(d-1)/4}|\Delta_K|^{7/2d}d^{5/2}\ell_\infty(\Omega)^4\mathcal{N}(\mathfrak{a})^{4/d}.$$

  Les exposants dans la constante $4\eta^{7(d-1)/4}|\Delta_K|^{7/2d}d^{5/2}$ sont plus faibles que ceux de la version originale. Ceci provient de la majoration légèrement plus fine de $\|x_2\|$ obtenue et de l'utilisation de la borne

  $$\|x_1\|^2 \leqslant \eta^{(d-1)/2}|\Delta_K|^{1/d}\mathcal{N}(\mathfrak{a})^{2/d}$$

  plutôt que

  $$\|x_1\|^2 \leqslant \eta^{d/2}|\Delta_K|^{1/d}\mathcal{N}(\mathfrak{a})^{2/d}.$$

  Par ailleurs, dans notre version, un facteur $d^{5/2}$ est ajouté. En effet, nous avons choisi d'effectuer les opérations de réduction sans passer par le GSOP. Au prix d'une borne théorique moins fine, se passer du GSOP permet de considérablement accélérer l'algorithme.
- L'estimation originale du taux d'échec de l'algorithme est erronée. En effet, l'inégalité $\left(1-\frac{1}{y}\right)^y \geqslant e^{-1}$ annoncée pour $y \geqslant 1$ n'est pas vérifiée.

BIBLIOGRAPHIE

[Ajt03] M. AJTAI. “The worst-case behavior of schnorr’s algorithm approximating the shortest nonzero vector in a lattice”. In : *Proceedings of the thirty-fifth annual ACM symposium on Theory of computing*. ACM. 2003, p. 396–406. [39]

[AKS01] M. AJTAI, R. KUMAR et D. SIVAKUMAR. “A sieve algorithm for the shortest lattice vector problem”. In : *Proceedings of the thirty-third annual ACM symposium on Theory of computing*. ACM. 2001, p. 601–610. [3, 5]

[Ajt96] M. AJTAI. “Generating hard instances of lattice problems”. In : *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*. ACM, 1996, p. 99–108. [8, 110]

[Ajt98] M. AJTAI. “The shortest vector problem in L 2 is NP-hard for randomized reductions”. In : *Proceedings of the thirtieth annual ACM symposium on Theory of computing*. ACM, 1998, p. 10–19. [3, 8, 110]

[AB09] S. ARORA et B. BARAK. *Computational complexity : a modern approach*. Cambridge University Press, 2009. [107]

[AGM02] A. ASH, P. GUNNELLS et M. MCCONNELL. “Cohomology of congruence subgroups of $\mathrm{SL}(4, \mathbb{Z})$”. In : *Journal of Number Theory* 94.1 (2002), p. 181–212. [1]

[AGM08] A. ASH, P. GUNNELLS et M. MCCONNELL. "Cohomology of congruence subgroups of SL(4, $\mathbb{Z}$). II". In : *Journal of Number Theory* 128.8 (2008), p. 2263–2274. [1]

[AGM10] A. ASH, P. GUNNELLS et M. MCCONNELL. "Cohomology of congruence subgroups of SL(4, $\mathbb{Z}$). III". In : *Mathematics of Computation* 79.271 (2010), p. 1811–1831. [1]

[AGM11] A. ASH, P. GUNNELLS et M. MCCONNELL. "Torsion in the cohomology of congruence subgroups of SL(4, $\mathbb{Z}$) and Galois representations". In : *Journal of Algebra* 325.1 (2011), p. 404–415. [1]

[AGM12] A. ASH, P. GUNNELLS et M. MCCONNELL. "Resolutions of the Steinberg module for GL(n)". In : *Journal of Algebra* 349.1 (2012), p. 380–390. [1]

[AGM15] A. ASH, P. GUNNELLS et M. MCCONNELL. "Mod 2 homology for GL(4) and Galois representations". In : *Journal of Number Theory* 146 (2015), p. 4–22. [1]

[BL83] L. BABAI et E. M. LUKS. "Canonical labeling of graphs". In : *Proceedings of the fifteenth annual ACM symposium on Theory of computing*. ACM. 1983, p. 171–183. [4, 107]

[Bab15] L. BABAI. "Graph Isomorphism in Quasipolynomial Time". In : http://arxiv.org/abs/1512.03547 (2015). [4, 6, 107, 125]

[BI97] R. BAEZA et M. I. ICAZA. "On Humbert-Minkowski's constant for a number field". In : *Proceedings of the American Mathematical Society* 125.11 (1997), p. 3195–3202. [2, 68]

[Bae+01] R. BAEZA et al. "Hermite's constant for quadratic number fields". In : *Experimental Mathematics* 10.4 (2001), p. 543–551. [2, 68]

[Bar57] E. S. BARNES. "The complete enumeration of extreme senary forms". In : *Philosophical Transactions of the Royal Society of London A : Mathematical, Physical and Engineering Sciences* 249.969 (1957), p. 461–506. [3]

[BLS64] H. BASS, M. LAZARD et J.-P. SERRE. "Sous-groupes d'indice fini dans SL(n, $\mathbb{Z}$)". In : *Bulletin of the American mathematical society* 70.3 (1964), p. 385–392. [96]

[BMS67] H. BASS, J. MILNOR et J.-P. SERRE. “Solution of the congruence subgroup problem for $\mathrm{SL}_n (n \geqslant 3)$ and $\mathrm{Sp}_{2n} (n \geqslant 2)$”. In : *Publications mathématiques de l'IHÉS* 33 (1967), p. 59–137. [100]

[BFEH13] E. BAYER-FLUCKIGER, V. EMERY et J. HOURIET. “Hermitian lattices and bounds in K-theory of algebraic integers”. In : *Documenta Math.* (2013). [1]

[Bel04] K. BELABAS. “Topics in computational algebraic number theory”. In : *Journal de Théorie des Nombres de Bordeaux* 16.1 (2004), p. 19–63. [67, 140, 172, 174, 176, 181]

[BFH17] J.-F. BIASSE, C. FIEKER et T. HOFMANN. “On the computation of the HNF of a module over the ring of integers of a number field”. In : *Journal of Symbolic Computation* 80 (2017), p. 581–615. [55]

[MAGMA] W. BOSMA, J. CANNON et C. PLAYOUST. “The Magma algebra system. I. The user language”. In : *Journal of Symbolic Computation* 24.3-4 (1997), p. 235–265. [4, 55, 140]

[BP91] W. BOSMA et M. POHST. “Computations with finitely generated modules over Dedekind rings”. In : *Proceedings of the 1991 international symposium on Symbolic and algebraic computation*. ACM. 1991, p. 151–156. [4, 54]

[BC15] O. BRAUN et R. COULANGEON. “Perfect lattices over imaginary quadratic number fields”. In : *Mathematics of Computation* 84.293 (2015), p. 1451–1467. [2, 53, 68]

[Bra+15] O. BRAUN et al. “Computing in arithmetic groups with Voronoï's algorithm”. In : *Journal of Algebra* 435 (2015), p. 263–285. [5, 6, 78]

[BDSS09] D. BREMNER, M. DUTOUR SIKIRIĆ et A. SCHÜRMANN. “Polyhedral representation conversion up to symmetries”. In : *CRM proceedings*. T. 48. 2009, p. 45–72. [110]

[Bus+11] S. BUSS et al. “Strong isomorphism reductions in complexity theory”. In : *The Journal of Symbolic Logic* 76.04 (2011), p. 1381–1402. [107]

[But91] G. BUTLER. *Fundamental algorithms for permutation groups*. T. 559. Springer-Verlag Berlin, Heidelberg, New York, 1991. [87, 88, 93, 97]

[Cha83] J. CHALK. “Algebraic lattices”. In : *Convexity and its applications*. Springer, 1983, p. 97–110. [2]

[Cha07] D. X. CHARLES. “Counting lattice vectors”. In : *Journal of Computer and System Sciences* 73.6 (2007), p. 962–972. [110]

[NIST16] L. CHEN et al. “Report on post-quantum cryptography”. In : *National Institute of Standards and Technology Internal Report* 8105 (2016). [1]

[Coh93] H. COHEN. *A course in computational algebraic number theory*. T. 138. Springer, 1993. [53, 173, 174]

[Coh96] H. COHEN. “Hermite and Smith normal form algorithms over Dedekind domains”. In : *Mathematics of Computation of the American Mathematical Society* 65.216 (1996), p. 1681–1699. [4, 55]

[Coh00] H. COHEN. *Advanced topics in computational number theory*. T. 193. Springer, 2000. [53, 54, 57, 174, 181]

[Cou01] R. COULANGEON. “Voronoï theory over algebraic number fields”. In : *Monographies de l’Enseignement Mathématique* 37 (2001), p. 147–162. [2, 68]

[Cou04] R. COULANGEON. “Invariants d’Hermite, théorie de Voronoï et designs sphériques”. Habilitation à diriger des recherches. Université de Bordeaux, 2004. [68]

[DL73] J. L. DE LAGRANGE. *Recherches d’Arithmétique*. Nouveaux mémoires de l’Académie royale des sciences et belles-lettres de Berlin, 1773. [2, 3]

[DW90] R. DIJKGRAAF et E. WITTEN. “Topological gauge theories and group cohomology”. In : *Communications in Mathematical Physics* 129.2 (1990), p. 393–429. [1]

[Dir89] P. G. L. DIRICHLET. *Werke, vol. 1*. 1889. [1]

[DSES11] M. DUTOUR SIKIRIĆ, G. ELLIS et A. SCHÜRMANN. “On the integral homology of $PSL_4(\mathbb{Z})$ and other arithmetic groups”. In : *Journal of Number Theory* 131.12 (2011), p. 2368–2375. [1]

[DSSV07] M. DUTOUR SIKIRIĆ, A. SCHÜRMANN et F. VALLENTIN. “Classification of eight-dimensional perfect forms”. In : *Electronic research announcements of the american mathematical society* 13.3 (2007), p. 21–32. [3]

[DSSV09] M. DUTOUR SIKIRIĆ, A. SCHÜRMANN et F. VALLENTIN. "Complexity and algorithms for computing Voronoi cells of lattices". In : *Mathematics of computation* 78.267 (2009), p. 1713–1731. [4, 110, 124]

[PFPK] P. ELBAZ-VINCENT. "PFPK : a tool for working with perfect forms and the geometry of the Voronoï space". In : *ICM 2006 - Mathematical Software. Abtracts, p.14–16*. URL : http://icm2006.mathunion.org/v_f/AbsDef/Globals/MathSoft.pdf. [96]

[EV15] P. ELBAZ-VINCENT. "Computational geometry of numbers, cohomology of modular groups and applications". In : *Lectures at the Workshop on computational problems in number theory Chern Institute of Mathematics, Nankai University*. 2015. URL : https://www-fourier.ujf-grenoble.fr/~pev/CIM2015/. [1]

[EVGS02] P. ELBAZ-VINCENT, H. GANGL et C. SOULÉ. "Quelques calculs de la cohomologie de $\mathrm{GL}_N(\mathbb{Z})$ et de la K-théorie de $\mathbb{Z}$". In : *Comptes Rendus Mathematique* 335.4 (2002), p. 321–324. [1, 96]

[EVGS13] P. ELBAZ-VINCENT, H. GANGL et C. SOULÉ. "Perfect forms, K-theory and the cohomology of modular groups". In : *Advances in Mathematics* 245 (2013), p. 587–624. [1, 96]

[EB81] P. van EMDE BOAS. *Another NP-complete partition problem and the complexity of computing short vectors in a lattice*. Universiteit van Amsterdam. Mathematisch Instituut, 1981. [3]

[FP96] C. FIEKER et M. POHST. "On lattices over number fields". In : *Algorithmic Number Theory*. Springer, 1996, p. 133–139. [4, 49, 53, 57, 68, 140]

[FS10] C. FIEKER et D. STEHLÉ. "Short bases of lattices over number fields". In : *Algorithmic number theory*. Springer, 2010, p. 157–173. [4, 46, 48, 53, 68, 172, 177, 178, 181]

[FP85] U. FINCKE et M. POHST. "Improved methods for calculating vectors of short length in a lattice, including a complexity analysis". In : *Mathematics of computation* 44.170 (1985), p. 463–471. [4, 81, 125, 141]

[GM05] Y. H. GAN et W. H. MOW. "Complex lattice reduction algorithms for low-complexity MIMO detection". In : *Global Telecommunications Conference, 2005. GLOBECOM'05. IEEE*. T. 5. IEEE. 2005. [21, 24, 28]

[Gas02] W. I. GASARCH. “The P= ?NP poll”. In : *Sigact News* 33.2 (2002), p. 34–47. [107]

[GM03] D. GOLDSTEIN et A. MAYER. “On the equidistribution of Hecke points”. In : *Forum Mathematicum*. T. 15. 2. Berlin ; New York : De Gruyter, c1989-. 2003, p. 165–190. [39]

[Gro12] E. GROSSWALD. *Representations of integers as sums of squares*. Springer Science & Business Media, 2012. [127]

[HR14] I. HAVIV et O. REGEV. “On the lattice isomorphism problem”. In : *Proceedings of the Twenty-Fifth Annual ACM-SIAM Symposium on Discrete Algorithms*. Society for Industrial et Applied Mathematics. 2014, p. 391–404. [4, 6, 109, 110, 113]

[HB97] D. HEATH-BROWN. “Lattice points in the sphere”. In : *Number theory in progress* 2 (1997), p. 883–892. [127]

[HV98] B. HEMKEMEIER et F. VALLENTIN. “On the decomposition of lattices”. In : *Electronic Colloquium on Computation and Complexity TR98-52*. Citeseer. 1998. [63]

[HPS98] J. HOFFSTEIN, J. PIPHER et J. H. SILVERMAN. “NTRU : A ring-based public key cryptosystem”. In : *Algorithmic number theory*. Springer, 1998, p. 267–288. [24]

[HW74] J. E. HOPCROFT et J.-K. WONG. “Linear time algorithm for isomorphism of planar graphs (preliminary report)”. In : *Proceedings of the sixth annual ACM symposium on Theory of computing*. ACM. 1974, p. 172–184. [107]

[Hum39] P. HUMBERT. “Théorie de la réduction des formes quadratiques définies positives dans un corps algébrique K fini”. In : *Commentarii Mathematici Helvetici* 12.1 (1939), p. 263–306. [2, 46, 67]

[Hum49] P. HUMBERT. “Réduction de formes quadratiques dans un corps algébrique fini”. In : *Commentarii Mathematici Helvetici* 23.1 (1949), p. 50–63. [2, 46, 67]

[Ica97] M. I. ICAZA. “Hermite constant and extreme forms for algebraic number fields”. In : *Journal of the London Mathematical Society* 55.01 (1997), p. 11–22. [68]

[IL95] H. IWANIEC et F. C. LORENTE. “On the sphere problem”. In : *Revista matemática iberoamericana* 11.2 (1995), p. 417–430. [127]

[JC93] D.-O. JAQUET-CHIFFELLE. “Énumération complete des classes de formes parfaites en dimension 7”. In : *Annales de l'institut Fourier*. T. 43. 1. 1993, p. 21–55. [3]

[Kan83] R. KANNAN. “Improved algorithms for integer programming and related lattice problems”. In : *Proceedings of the fifteenth annual ACM symposium on Theory of computing*. ACM, 1983, p. 193–206. [3, 5, 125]

[Kaz15] R. A. KAZMI. “Cryptography from Post-Quantum Assumptions”. Thèse de doct. McGill University, 2015. [109]

[Kel+57] P. J. KELLY et al. “A congruence theorem for trees”. In : *Pacific J. Math* 7.1 (1957), p. 961–968. [107]

[KZ77] A KORKINGE et G ZOLOTAREFF. “Sur les formes quadratiques positives”. In : *Mathematische Annalen* 11.2 (1877), p. 242–292. [2, 3]

[LLN09] M. LACA, N. S. LARSEN et S. NESHVEYEV. “On Bost–Connes type systems for number fields”. In : *Journal of Number Theory* 129.2 (2009), p. 325–338. [54]

[LS76] R. LEE et R. SZCZARBA. “The group K3 (Z) is cyclic of order forty-eight”. In : *Annals of Mathematics* (1976), p. 31–60. [1]

[LS78] R. LEE et R. SZCZARBA. “On the torsion in $K_4(\mathbb{Z})$ and $K_5(\mathbb{Z})$”. In : *Duke Mathematical Journal* 45.1 (1978), p. 101–129. [1]

[Lei05] A. LEIBAK. “On additive generalization of Voronoi's theory to algebraic number fields”. In : *Proceedings of the Estonian Academy of Science Physics/Mathematics* 54.4 (2005), p. 195–212. [2, 5, 46, 68, 72]

[LLL82] A. K. LENSTRA, H. W. LENSTRA et L. LOVÁSZ. “Factoring polynomials with rational coefficients”. In : *Mathematische Annalen* 261.4 (1982), p. 515–534. [2, 8, 15, 21, 23, 24, 28, 172]

[Lez12] P. LEZOWSKI. “Questions d'Euclidianité”. Thèse de doct. Université Sciences et Technologies-Bordeaux I, 2012. [13]

[Li11] S. LI. “Concise formulas for the area and volume of a hyperspherical cap”. In : *Asian Journal of Mathematics and Statistics* 4.1 (2011), p. 66–70. [129]

[Luk82] E. M. LUKS. “Isomorphism of graphs of bounded valence can be tested in polynomial time”. In : *Journal of computer and system sciences* 25.1 (1982), p. 42–65. [107]

[Mar06] D. MARKER. *Model theory : an introduction*. T. 217. Springer Science & Business Media, 2006. [107]

[Mar03] J. MARTINET. *Perfect lattices in Euclidean spaces*. T. 327. Springer, 2003. [16, 46, 48, 60, 62, 63, 67, 72, 73, 79, 93, 149]

[MW01] M MASANORI et T WATANABE. "Adele geometry of numbers, Class field theory—its centenary and prospect (Tokyo, 1998)". In : *Math. Soc. Japan, Tokyo (2001)* (2001), p. 509–536. [2]

[NAUTY] B. D. MCKAY et A. PIPERNO. *Nauty and Traces user's guide (Version 2.5)*. 2013. [105, 113, 116, 152]

[Min96] H. MINKOWSKI. *Geometrie der Zahlen*. Leipzig Und Berlin : R. G. Teubner, 1896. [1, 3]

[Min07] H. MINKOWSKI. *Diophantische approximationen : eine einfü hrung in die zahlentheorie*. Leipzig Und Berlin : R. G. Teubner, 1907. [2]

[Nap96] H. NAPIAS. "A generalization of the LLL-algorithm over euclidean rings or orders". In : *Journal de théorie des nombres de Bordeaux* 8.2 (1996), p. 387–396. [5, 8, 16, 21, 28, 53]

[LATT] G. NEBE et N. SLOANE. *LATTICES - A Catalogue of Lattices*. URL : http://www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES/. [119, 150, 156]

[Neu13] J. NEUKIRCH. *Algebraic number theory*. T. 322. Springer Science & Business Media, 2013. [46, 48, 180]

[Ngu07] P. Q. NGUYEN. "Théorie et Pratique de la Cryptanalyse à Clef Publique". Habilitation à diriger des recherches. Université Paris 7, 2007. [3, 40]

[NV10] P. Q. NGUYEN et B. VALLÉE. *The LLL Algorithm. Survey and Applications*. Springer-Verlag, 2010. [3, 24]

[OY10] K. OKUDA et S. YANO. "A generalization of Voronoï's Theorem to algebraic lattices". In : *Journal de Théorie des Nombres de Bordeaux* 22.3 (2010), p. 727–740. [2, 46, 53, 54, 61, 68]

[O'M73] O. T. O'MEARA. *Introduction to quadratic forms*. T. 117. Springer, 1973. [46]

[PP85] W. PLESKEN et M POHST. "Constructing integral lattices with prescribed minimum. I". In : *mathematics of computation* 45.171 (1985), p. 209–221. [81]

[PS97] W. PLESKEN et B. SOUVIGNIER. "Computing isometries of lattices". In : *Journal of Symbolic Computation* 24.3 (1997), p. 327–334. [4–6, 78, 82, 87, 90, 104, 109, 148, 149, 155]

[Rob04] X.-F. ROBLOT. "Polynomial factorization algorithms over number fields". In : *Journal of Symbolic Computation* 38.5 (2004), p. 1429–1443. [24]

[RSD58] K ROGERS et H. SWINNERTON-DYER. "The Geometry of Numbers over algebraic number fields". In : *Transactions of the American Mathematical Society* 88.1 (1958), p. 227–242. [2]

[Rot08] J. ROTMAN. *An introduction to homological algebra*. Springer Science & Business Media, 2008. [48, 49]

[Sam67] P. SAMUEL. *Théorie algébrique des nombres*. Hermann, 1967. [8–10, 46, 67, 175]

[SBL10] M. SCHNEIDER, J. BUCHMANN et R. LINDNER. "Probabilistic analysis of LLL reduced bases". In : *Western European Workshop on Research in Cryptology (WEWoRC)*. T. 6429. 2010. [5, 8, 38–40]

[Sch09] P. SCHWEITZER. "Problems of unknown complexity". In : *Graph isomorphism and Ramsey theoretic numbers. Diss. University of Saarlandes* (2009). [121]

[Scilab] SCILAB ENTERPRISES. *Scilab : Le logiciel open source gratuit de calcul numérique*. Disponible sur http://www.scilab.org. Orsay, France, 2012. [40]

[Sil13] A. SILVERBERG. "Fully Homomorphic Encryption for Mathematicians". In : *IACR Cryptology ePrint Archive* 2013 (2013), p. 250. [24]

[Sou78] C. SOULÉ. "The cohomology of $SL_3(\mathbb{Z})$". In : *Topology* 17.1 (1978), p. 1–22. [1]

[Ste09] D. STEHLÉ. "Floating-point LLL : theoretical and practical aspects". In : *The LLL Algorithm*. Springer, 2009, p. 179–213. [138]

[Ste11] D. STEHLÉ. "Réseaux Euclidiens : Algorithmes et Cryptographie". Habilitation à diriger des recherches. École Normale Supérieure de Lyon, 2011. [126]

[PARI/gp] THE PARI GROUP. *PARI/GP version 2.9.1*. available from http ://pari.math.u-bordeaux.fr/. Université de Bordeaux, 2016. [4, 6, 55, 92, 134, 152, 174, 178]

[VZGG03] J. VON ZUR GATHEN et J. GERHARD. *Modern computer algebra*. Cambridge University Press, 2003. [20, 28, 36]

[Vor08] G. VORONOI. "Nouvelles applications des paramètres continus à la théorie des formes quadratiques. Premier mémoire. Sur quelques propriétés des formes quadratiques positives parfaites." In : *Journal für die reine und angewandte Mathematik* 133 (1908), p. 97–178. [1–3, 5, 128]

[Wat00] T. WATANABE. "On an analog of Hermite's constant". In : *J. Lie Theory* 10.1 (2000), p. 33–52. [2]

[WYH13] T. WATANABE, S. YANO et T. HAYASHI. "Voronoï's reduction theory of GL_n over a totally real number field". In : *Diophantine Methods, Lattices, and Arithmetic Theory of Quadratic Forms* 587 (2013), p. 213. [2, 5, 53, 68]

[Gnuplot] T. WILLIAMS, C. KELLEY et MANY OTHERS. *Gnuplot 4.4 patchlevel 3 : an interactive plotting program*. Disponible sur http://gnuplot.info. 2011. [40]

[ZKT85] V. ZEMLYACHENKO, N. KORNEENKO et R. TYSHKEVICH. "Graph isomorphism problem". In : *Journal of Mathematical Sciences* 29.4 (1985), p. 1426–1481. [4, 107]

Résumé

Les travaux présentés dans ce mémoire concernent les réseaux, qui sont des objets mathématiques fondamentaux pour de nombreux domaines tel que théorie des nombres et la cryptographie.

Nous proposons dans un premier temps une généralisation et une implantation de l'algorithme de réduction de Lenstra, Lenstra et Lovász (algorithme LLL) dans le cadre algébrique simple des réseaux sur les anneaux d'entiers quadratiques, imaginaires et euclidiens.

Nous nous attachons ensuite à présenter les notions de réseaux algébriques et de formes de Humbert, qui sont des généralisations dans un cadre algébrique aussi large que possible des notions classiques de réseaux euclidiens et de formes quadratiques. L'introduction de ces objets nous permet de présenter une adaptation et une implantation de l'algorithme de Plesken et Souvignier permettant de traiter efficacement les problèmes de l'isométrie et de la détermination des automorphismes pour les réseaux algébriques.

Nous proposons finalement une étude détaillée de la complexité de ces deux problèmes. Nous montrons notamment qu'ils sont intiment reliés à des problèmes similaires sur les graphes. Cette réduction nous permet d'exhiber des bornes de complexité inédites.

Mots-clés : Méthodes algorithmiques • Réseaux algébriques • formes de Humbert • Isométrie • Automorphisme

---

Abstract

This thesis deals with lattices, which are fundamental objects in many fields, such as number theory and cryptography.

As a first step, we propose a generalization and an implementation of the Lenstra, Lenstra and Lovász algorithm (LLL algorithm) in the simple algebraic setting of lattices over quadratic imaginary and euclidean ring of integers.

Then, we present the notions of algebraic lattices and Humbert forms, which are extensions of euclidean lattices and quadratic forms in a large algebraic setting. Introducing these objects leads us to develop and implement modifications of the Plesken and Souvignier algorithm. This algorithm efficiently solves the isometric lattices problem and the automorphism group computation problem for algebraic lattices.

Finally, we analyze in depth the complexity of these two algorithmic problems. We show that they are intimately related to similar problems for graphs. This reduction leads us to express new complexity bounds.

Keywords : Algorithmic methods • Algebraic lattices • Humbert forms • Isometry • Automorphism