N° d'ordre : 1454

THESE

PRESENTEE A

L'UNIVERSITE BORDEAUX I

ECOLE DOCTORALE DE MATHEMATIQUES ET INFORMATIQUE

PAR **Huguette NAPIAS**

POUR OBTENIR LE GRADE DE

DOCTEUR

SPECIALITE : MATHEMATIQUES PURES

ETUDE EXPERIMENTALE ET ALGORITHMIQUE DE RESEAUX EUCLIDIENS

Soutenue le : 25 Janvier 1996

Après avis de : M. F. SIGRIST (Univ. Neuchâtel) **Rapporteurs**
Mme B. VALLÉE (Univ. Caen)

Devant la commission d'examen formée de :

M.	Ch. BATUT	Maître de Conférences (Univ. Bordeaux I)
Mme	A-M. BERGÉ	Professeur (Univ. Bordeaux I)
M.	A. JOUX	Ingénieur Armement (CELAR Rennes)
M.	J. MARTINET	Professeur (Univ. Bordeaux I)
Mme	G. NEBE	Maître de Conférences (Univ. d'Aix-La-Chapelle)
M.	F. SIGRIST	Professeur (Univ. de Neuchâtel)
Mme	B. VALLÉE	Professeur (Univ. de Caen)

- 1996 -

$\mathcal{A}$ tout seigneur, tout honneur ! En premier lieu, je tiens à exprimer ma reconnaissance à Jacques $\mathcal{M}$artinet qui, tout au long de ces trois années, a toujours su m'orienter dans la bonne direction, avec une infinie patience. Ce "puits de sciences" possède non seulement un immense savoir mathématique, mais aussi les qualités humaines nécessaires pour "encadrer" un doctorant et guider ses premiers pas vers la recherche.

$\mathcal{B}$ien que pris par d'autres activités, comme la direction du laboratoire d'algorithmique et d'arithmétique expérimentales, il a toujours aménagé son planning de manière à m'accorder beaucoup de temps.

$\mathcal{J}$e remercie aussi François $\mathcal{S}$igrist et Brigitte $\mathcal{V}$allée qui ont bien voulu rapporter cette thèse et me faire l'honneur d'être membres du jury.

$\mathcal{C}$hristian $\mathcal{B}$atut m'a "pilotée" pour le côté algorithmique de ce travail, notamment pour le troisième chapitre. Je lui sais gré du temps qu'il a bien voulu me consacrer et aussi d'être l'un des jurés. Son nom est associé à ceux des concepteurs du système PARI, à savoir Dominique $\mathcal{B}$ernardi, Henri $\mathcal{C}$ohen et Michel $\mathcal{O}$livier. La plupart de mes programmes informatiques utilise ce logiciel de calculs, bien utile pour les arithméticiens et devenu indispensable pour le laboratoire.

$\mathcal{J}$e remercie Anne-Marie $\mathcal{B}$ergé et Gabriele $\mathcal{N}$ebe d'avoir accepté d'être parmi les membres du jury.

$\mathcal{J}$'ai pu discuter maintes fois avec Christine $\mathcal{B}$achoc et m'enrichir de ses connaissances sur les réseaux hermitiens. Je l'en remercie chaleureusement.

$\mathcal{J}$'ai emprunté des tables de corps de nombres à Francisco $\mathcal{D}$iaz y $\mathcal{D}$iaz et à Michel $\mathcal{O}$livier. Qu'ils en soient ici remerciés.

$\mathcal{A}$ntoine $\mathcal{J}$oux, mon lien avec le CELAR de Rennes, a manifesté de l'intérêt pour mon travail et c'est avec joie qu'il a accepté de se joindre aux autres membres du jury. Je lui exprime ici ma reconnaissance.

$\mathcal{J}$e n'oublie pas les ingénieurs système Paul $\mathcal{C}$rubillé et Christian $\mathcal{L}$abesse qui s'évertuent à rendre l'emploi du réseau informatique plus convivial pour les "non-informaticiens" que nous sommes.

$\mathcal{J}$e remercie aussi La secrétaire du laboratoire Véronique $\mathcal{S}$aint-$\mathcal{M}$artin pour tous les services qu'elle m'a rendus ainsi que pour son accueil chaleureux dans l'équipe de théorie des nombres.

$\mathcal{J}$e salue mes amis Jean-Luc $\mathcal{B}$aril, Isabelle $\mathcal{C}$halendar, Andreas $\mathcal{H}$artmann, Arnaud $\mathcal{J}$ehanne, Jean-Marc $\mathcal{M}$ercier, Thierry $\mathcal{S}$ageaux, Anne $\mathcal{S}$errie, Florence $\mathcal{S}$oriano, Hervé $\mathcal{T}$homas, Marie-Thérèse $\mathcal{T}$ogni et Emmanuel $\mathcal{T}$ollis qui ont participé de près ou de loin à l'élaboration de cette thèse.

$\mathcal{E}$nfin, je remercie Mauricette $\mathcal{J}$aubert et Daniel $\mathcal{Y}$nbourg, pour leur gentillesse et pour avoir bien voulu assurer la réalisation matérielle de ce travail.

Sommaire.

Introduction.

Cette thèse comporte quatre parties :

Elle débute par un chapitre concernant les réseaux de Leech et de Ch. Bachoc (réseaux les plus denses connus au sens de la constante d'Hermite, dans les dimensions 24 et 32). On s'est plus particulièrement intéressé aux sections ayant des invariants d'Hermite duals [B-M] élevés. On retrouve les bornes données par N.J.A. Sloane, et dans les dimensions 18 et 21, on améliore les valeurs de ces bornes.

Par lamination faible au-dessus du réseau K_{12} (réseau le plus dense connu en dimension 12), W. Plesken et M. Pohst dans [Pl-P] retrouvent les séries des K_n, Λ_n et K'_n. Cependant, en dimension 16, ils fournissent deux réseaux non isométriques : à l'aide d'un programme informatique, nous avons déterminé celui qui est isométrique à l'orthogonal de K'_8 dans le réseau de Leech.

Ch. Bachoc a construit un réseau en dimension 32 sur l'ordre de Hurwitz (ordre maximal de l'algèbre non commutative des quaternions de Hamilton ramifiée en 2 et l'infini). Il s'agit d'un réseau isodual de même densité que les deux réseaux construits antérieurement par H-G. Quebbemann. Cet ordre, muni de la forme trace réduite, peut être considéré comme isométrique au réseau de racines $\mathbb{D}_4$ (réseau critique en dimension 4). Nous avons recherché dans le réseau de Ch. Bachoc, un réseau isométrique au réseau de racines $\mathbb{E}_8$, toujours avec ce même programme informatique. On peut dire que le réseau de Ch. Bachoc contient les réseaux les plus denses de rang inférieur ou égal à 8. Par sections de ce réseau, nous avons aussi trouvé un réseau parfait en dimension 8 sans section hyperplane parfaite non connu jusque là.

Cette première partie a fait l'objet d'une note publiée aux Comptes Rendus de l'Académie des Sciences en Octobre 1994. Toutefois, on ne donne pas cette version mais une autre complétée par quelques réseaux de W. Plesken et M. Pohst. Le titre du dernier paragraphe a été renommé, car on sait aujourd'hui que les trois réseaux qui étaient appelés réseaux de H-G. Quebbemann lors de la parution de la note, ne sont pas isométriques entre eux.

Le chapitre suivant traite de voisinages au sens de Voronoï des formes quadratiques parfaites définies positives. G. Voronoï a donné un algorithme permettant de trouver, à

partir d'une forme parfaite donnée, dans une dimension n, toutes les formes parfaites. Dans une dimension donnée et à isométrie près, celles-ci sont en nombre fini. Il a introduit la notion de réseaux contigus et montré que la relation de contiguïté entraîne la connexité de son graphe. Nous avons recherché, essentiellement, les formes "voisines" des formes de Coxeter $\mathbb{A}_n^{\frac{n+1}{2}}$ et $\mathbb{A}_n^2$ (les réseaux de Coxeter sont construits à partir du réseau de racines $\mathbb{A}_n$). Lorsque le groupe d'automorphismes du réseau est transitif sur la sphère de ses vecteurs minimaux et que celle-ci a pour demi-cardinal $\frac{n(n+1)}{2}$, il n'y a qu'un seul réseau contigu, à isométrie près. C'est le cas pour les réseaux de Coxeter. Pour chaque dimension n impaire, à partir d'une matrice de Gram d'une base du réseau Coxeter, nous donnons la forme générale, dépendant de n, d'une matrice de Gram du réseau contigu. On montre aussi que le nombre de couples de vecteurs minimaux du réseau contigu vaut $\frac{n(n+1)}{2}$.

Cette partie se termine par des calculs de voisinages de réseaux parfaits de rang 8, dont le "kissing number" $2s$ vaut $n(n+1)$, et ceci grâce à l'algorithme de Voronoï. En 1992, dans sa thèse, M. Laïhem avait obtenu 1 171 réseaux parfaits (ils possèdent une section hyperplane parfaite). On peut leur ajouter les quatre réseaux $\mathbb{A}_8$, $\mathbb{D}_8$, $\mathbb{A}_8^2$, $\mathbb{E}_8$ au-dessus des réseaux de racines en dimension 7, les 53 réseaux construits par J-L. Baril par *patchwork* (i.e. somme directe d'un réseau parfait en dimension 6 et du réseau de racines $\mathbb{A}_2$, renormalisés à la même norme), dont un déjà trouvé par D-O. Jaquet, et celui décrit dans le premier chapitre. A partir de 340 réseaux (329 de la liste de M. Laïhem et 11 de celle de J-L. Baril), ayant 36 paires de vecteurs minimaux, l'algorithme de Voronoï a fourni 9 541 nouveaux réseaux parfaits. On connaissait ainsi 1 229 réseaux parfaits en dimension $n = 8$. On en connaît maintenant 10 770 ! On peut noter que tous ces réseaux sont de norme minimale paire.

Le troisième chapitre concerne la réduction de bases de réseaux et plus particulièrement l'algorithme LLL. Trouver une base réduite est un vieux problème qui remonte à C.F. Gauss. Ce dernier a donné un algorithme dans le cas de la dimension 2 qui trouve une base formée de vecteurs de "petites" normes. Plus récemment, en 1986, B. Vallée a résolu le cas de la dimension 3. En 1982, dans [LLL], A.K. Lenstra, H.W. Lenstra et L. Lovász ont introduit une nouvelle forme de réduction : *une base est dite "LLL-réduite" lorsqu'elle est composée de vecteurs de "petites" normes et "presque orthogonaux".*

Une version de leur algorithme utilise les nombres entiers ; nous l'avons généralisé à des anneaux euclidiens. Il trouve une base formée de vecteurs de "petites" normes d'un réseau possédant une structure algébrique sur un anneau ou un ordre euclidien (par exemple, l'anneau d'entiers d'un corps quadratique imaginaire ou un ordre maximal d'une algèbre non commutative de quaternions), tout en conservant cette structure. Les calculs se font dans l'anneau (ou l'ordre) euclidien. A partir d'une matrice de produits hermitiens, on peut reconstituer une matrice de Gram sur $\mathbb{Z}$. Cet algorithme a été, en particulier, appliqué à des réseaux construits à l'aide de codes et sur l'ordre de Hurwitz, par Ch. Bachoc en dimensions 32, 40, 48 (dimensions relatives 8, 10, 12). Il a permis de trouver des bases formées de vecteurs minimaux sur $\mathbb{Z}$, que l'algorithme LLL usuel ne trouve pas toujours, et ceci en peu de temps.

La dernière partie traite des minima successifs. On sait d'après un théorème de Minkowski et l'inégalité de Hadamard que l'on peut majorer l'indice d'un réseau engendré par des vecteurs représentant les minima successifs d'un réseau, dans ce réseau, par la constante d'Hermite en dimension n à la puissance $\frac{n}{2}$. Par conséquent, des vecteurs réalisant les minima forment une base jusqu'à la dimension $n < 4$ (en dimension $n = 4$, si l'on exclut le réseau de racines $\mathbb{D}_4$, cet indice vaut toujours 1).

L'algorithme de recherche des minima a été appliqué aux anneaux d'entiers de corps de nombres, $K = \mathbb{Q}(\theta)$, totalement réels, en degrés 3, 4, 5, construits par M. Olivier, J. Buchmann, D. Ford, M. Pohst, F. Diaz y Diaz et A. Schwarz. En dimension 5, des vecteurs représentant les minima successifs engendrent un réseau avec un indice 1 ou 2 dans le réseau de départ. Cependant, dans cette dimension, on a toujours trouvé un indice égal à 1 (il faut noter qu'un système de vecteurs réalisant les minima successifs n'est *a priori* pas unique). En degré 3, dans le cas galoisien, si 1 et θ sont deux "vecteurs" représentant les deux premiers minima, on montre que l'on peut prendre un conjugué de θ par un élément du groupe de Galois comme "vecteur" réalisant le troisième minimum.

Afin de "vérifier" une conjecture de J. Martinet, cette partie se termine par quelques exemples de minima successifs d'anneaux d'entiers de corps de nombres cycliques de degrés 5, 7, 11 et 13.

Chapitre 1

Sur quelques réseaux contenus dans les réseaux de Leech et de Ch. Bachoc.

Le but de ce chapitre est de rechercher quelques réseaux de petites dimensions qui sont denses (au sens usuel de la constante d'Hermite et surtout au sens de la constante γ'_n de Bergé-Martinet). Nous avons pour cela, étudié des sections des réseaux de Leech et de Ch. Bachoc et utilisé les réseaux faiblement laminés de W. Plesken et M. Pohst.

1.1 INTRODUCTION.

On considère l'espace euclidien de dimension n, $\mathbb{R}^n$. Pour tout vecteur x de $\mathbb{R}^n$, on note $N(x) = x.x$ la norme de x. (C'est aussi le carré de la norme euclidienne $\|x\|$.) On définit un réseau L de $\mathbb{R}^n$ comme étant un sous-groupe discret de $\mathbb{R}^n$ de rang maximum.

La norme minimale de L, $N(L)$ et la sphère des vecteurs minimaux de L, $S(L)$ sont définies de la manière suivante : $N(L) = \min_{x \in L, x \neq 0} N(x)$, $S(L) = \{x \in L \mid N(L) = N(x)\}$. On pose $s = s(L) = \frac{1}{2}|S(L)|$. La quantité $2s$ est aussi appelée "kissing number" de L : c'est le nombre de points de contacts avec la sphère de rayon $\frac{1}{2}\sqrt{N(L)}$ centrée à l'origine, des sphères de mêmes rayons centrées aux autres points du réseau.

Le déterminant $\det(L)$ de L est le déterminant d'une matrice de Gram d'une base de L (matrice des produits scalaires deux à deux des vecteurs de la base). On dira que le réseau L est *entier* lorsqu'une de ses matrices de Gram est à coefficients entiers, *unimodulaire* lorsqu'il est entier et de déterminant égal à 1 et *pair* s'il est entier et si les produits scalaires $x.x$ sont tous pairs.

On note $L^* = \{x \in \mathbb{R}^n \mid \forall y \in L,\ x.y \in \mathbb{Z}\}$ le réseau dual de L. On peut montrer que le réseau L est entier lorsqu'il est contenu dans son dual et unimodulaire lorsqu'il est égal à son dual.

On définit le *groupe d'automorphismes* du réseau L et on le note $Aut(L)$, l'ensemble des isométries de $\mathbb{R}^n$ qui applique L sur lui-même. C'est un groupe fini. Dire que deux réseaux L et L' de $\mathbb{R}^n$ sont isométriques signifie qu'étant données une matrice de Gram A de L

dans une base de L et une matrice de Gram A' de L' dans une base de L', il existe une matrice de passage $P \in Gl_n(\mathbb{Z})$ (i.e. à coefficients entiers et inversible) telle que l'on ait la relation $A' = {}^tPAP$ où ${}^tP$ désigne la transposée de P.

L'invariant d'Hermite de L est $\gamma_n(L) = N(L)/\det(L)^{1/n}$, la constante d'Hermite pour la dimension n est $\gamma_n = \sup_L \gamma_n(L)$ ($\gamma_n^{n/2}$ est proportionnel à la densité de l'empilement de sphères défini par les réseaux). A-M. Bergé et J. Martinet ont défini la constante $\gamma'_n = \sup_L \gamma'_n(L)$ où $\gamma'_n(L) = (N(L).N(L^*))^{1/2}$ est "l'invariant d'Hermite dual" de L.

Un réseau L est dit *parfait* si les projections sur les directions des vecteurs minimaux engendrent l'espace $\mathrm{End}^s(\mathbb{R}^n)$ des endomorphismes symétriques de $\mathbb{R}^n$, *eutactique* si l'identité de $\mathbb{R}^n$ est combinaison linéaire à coefficients strictement positifs de ces projections. G. Voronoï a montré qu'un réseau est extrême (i.e. qu'il réalise un maximum local de l'invariant d'Hermite) si, et seulement si, il est parfait et eutactique.

On introduit aussi la notion de dual-extrémalité, c'est-à-dire de réalisation d'un maximum local de l'invariant d'Hermite dual. A-M. Bergé et J. Martinet [B-M] ont montré que lorsqu'un réseau est extrême et son dual eutactique alors il est dual-extrême.

1.2 LES SÉRIES Λ_n, K_n, K'_n.

1.2.1 Réseaux fortement laminés (ou plus simplement laminés).

Définition [C-S 2 Chap 6].

On pose $\Lambda_0 = \{0\}$. Pour $n \geq 1$, on considère tous les réseaux de dimension n, de norme minimale 4 contenant le réseau Λ_{n-1} et l'on se restreint aux réseaux dont le déterminant est minimum.

De tels réseaux sont dits laminés.

On les note Λ_n, avec un exposant éventuel pour en distinguer deux non isométriques. En dimension 24, on trouve le réseau de Leech et pour $n \leq 8$, les réseaux de racines $\mathbb{A}_1$, $\mathbb{A}_2$, $\mathbb{A}_3$, $\mathbb{D}_4$, $\mathbb{D}_5$, $\mathbb{E}_6$, $\mathbb{E}_7$, $\mathbb{E}_8$ renormalisés à la norme 4. On remarque que pour $12 \leq n \leq 24$, Λ_n est isométrique à l'orthogonal dans Λ_{24} de Λ_{24-n}, d'où la formule $\det(\Lambda_n) = \det(\Lambda_{24-n})$ pour $0 \leq n \leq 24$ en posant $\det(\Lambda_0) = 1$. Il y a exactement un réseau laminé pour chaque dimension $n \leq 24$ sauf pour les dimensions 11, 12, 13 pour lesquelles on trouve respectivement 2, 3, 3 réseaux non isométriques que l'on distingue par leurs nombres de vecteurs minimaux avec les exposants min, mid, max.

Pour $1 \leq n \leq 8$, $n = 15, 16$ et $19 \leq n \leq 24$, les réseaux Λ_n sont extrêmes et leurs duals sont eutactiques. Par conséquent ils sont dual-extrêmes. Il en est de même de $\Lambda_{12}^{\max}, \Lambda_{13}^{\max}$. Pour tout $n \leq 24$, les réseaux laminés sont parfaits.

1.2.2 Les réseaux K_n ($0 \leq n \leq 24$).

Ils ont été définis par Leech pour toute dimension $n \leq 24$. Nous rappelons ici brièvement la construction de [M 1].

Soit F un sous-espace de $\mathbb{R}^n$ de dimension m coupant un réseau de $\mathbb{R}^n$ suivant L_F un réseau de F. Alors, $F^\perp$ coupe L^* suivant $L_F^\perp$ un réseau de $F^\perp$. Lorsque $\sigma : L \mapsto L^*$ est une similitude, on associe à L_F le réseau $L_{F,\sigma} = \sigma(L_F)^\perp \cap L_F$.

H.S.M. Coxeter et J.A. Todd ont défini leur réseau noté K_{12} à l'aide de congruences sur $\mathbb{Z}[\omega]^6$ ($\mathbb{Z}[\omega]$, ω tel que $\omega^2 + \omega + 1 = 0$, étant l'anneau des entiers d'Eisenstein). En utilisant la similitude $x : \mapsto \frac{x}{1-\omega}$ de K_{12} sur son dual, on construit une suite de réseaux $K_{11} \supset K_{10} \supset \cdots \supset K_0 = \{0\}$. On peut construire les K_n, $n \geq 12$ comme réseaux isométriques aux orthogonaux dans le réseau de Leech des K_n. On a ainsi (comme pour les réseaux laminés) la formule $\det(K_{24-n}) = \det(K_n)$ pour tout $n \leq 24$. Les réseaux K_n sont entiers et de norme minimale 4. On remarque la coïncidence entre les K_n et les Λ_n pour $0 \leq n \leq 6$ et $18 \leq n \leq 24$.

Ils sont parfaits sauf pour $n = 7,\ 8$; K_{11} et K_{12} sont extrêmes et dual-extrêmes. Pour $0 \leq n \leq 10$ et $14 \leq n \leq 24$, les réseaux laminés sont les plus denses connus alors que pour $n = 11, 12, 13$, ce sont les K_n.

1.2.3 Les réseaux $\mathbf{K'_n}$ ($\mathbf{0 \leq n \leq 24}$).

On utilise la même méthode de construction que pour les réseaux K_n. Pour n pair, $n \leq 12$, les réseaux K'_n sont munis d'une structure sur l'anneau des entiers d'Eisenstein compatible avec celle de K_{12} et pour n impair on prend le réseau le plus dense parmi ceux qui sont contenus dans K'_{n+1} et qui contiennent K'_{n-1}. On définit K'_n pour $13 \leq n \leq 24$ en prenant les réseaux isométriques aux orthogonaux dans le réseau de Leech des K'_{24-n} plongés dans K_{12}. On a de même la formule $\det(K'_{24-n}) = \det(K'_n)$ pour tout $n \leq 24$ et $K'_n = \Lambda_n$ (resp. K_n) pour $n = 0,\ 1,\ 2,\ 22,\ 23,\ 24$ (resp. $n = 11,\ 12,\ 13$).

Pour $0 \leq n \leq 12$, les réseaux K'_n sont extrêmes sauf pour $n = 3,\ 4$. Ils sont dual-extrêmes pour $n = 5,\ 6,\ 8,\ 10,\ 11,\ 12,\ 16,\ 18,\ 20,\ 21$.

1.2.4 Les réseaux faiblement laminés de W. Plesken et M. Pohst.

Définition.

On considère $(L_n)_{n\in\mathbb{N}}$, $L_0 = \{0\} \subset L_1 \subset L_2 \subset \ldots$ des réseaux entiers en dimension n de norme minimale 4 satisfaisant les propriétés :

1) L_n est engendré par ses vecteurs minimaux.

2) L_{n-1} étant donné, L_n a un déterminant minimum parmi tous les réseaux entiers en dimension n de norme minimale 4 contenant L_{n-1}.

De tels réseaux sont dits faiblement laminés.

W. Plesken et M. Pohst ont construit les réseaux faiblement laminés au-dessus des réseaux Λ_n et K_n pour $n \geq 12$. Ils en déduisent des réseaux qu'ils notent L_{na}, L_{nb}, L_{nc}, L_{nd} (les réseaux L_{na} sont les réseaux laminés). Leurs familles contiennent les familles Λ_n, K_n, K'_n pour $n \geq 12$. Pour $n \geq 12$, nous avons utilisé les matrices de Gram de W. Plesken et M. Pohst [PL-P] obtenues par laminations faibles au-dessus de K_{12}. Ils retrouvent la série des K'_n sauf pour la dimension 16 où ils trouvent deux réseaux distingués par leurs nombres de couples de vecteurs minimaux 1218 et 1224 et dont un seul est isométrique à l'orthogonal de K'_8 dans $\Lambda_{24} = K'_{24}$. L'autre réseau sera noté K''_{16}.

Proposition. *[M 1]*
Le réseau K'_{16} est celui d'invariant $s = 1224$.

Preuve
On cherche le réseau K'_{21} dans le réseau de Leech, on reconstitue la chaîne décroissante des K'_n jusqu'à la dimension 17 puis on différencie les sections K'_{16} et K''_{16} par leurs orthogonaux. *(Parmi les 37 vecteurs minimaux de K'^*_{17}, un seul a pour orthogonal K'_{16} dans K'_{17}, résultat déjà observé pour K^*_{11} et K'^*_9.)* ■

Nous nous sommes préoccupés plus particulièrement de rechercher les grandes valeurs de la constante de Bergé-Martinet.

1.3 SUR LA CONSTANTE DE BERGÉ-MARTINET.

On rappelle qu'il s'agit de $\gamma'_n = \sup_L \gamma'_n(L)$ avec $\gamma'_n(L) = (N(L).N(L^*))^{1/2}$.
Dans [S], N.J.A. Sloane signale pour chaque dimension n, $1 \leq n \leq 24$, une borne inférieure pour γ'^2_n, complétant les valeurs données dans [B-M] pour $n \leq 9$ (pour $1 \leq n \leq 8$, on trouve les réseaux laminés, le réseau $\mathbb{A}^2_9$ de Coxeter pour $n = 9$ et aussi le réseau $\mathbb{A}^3_5$ en dimension $n = 5$). Nous avons amélioré ces résultats en dimensions $n = 18$ où $\gamma'^2_n \geq 8$ ($\gamma'^2_{18}(K'_{18}) = 8$) et $n = 21$ où $\gamma'^2_n \geq 9$ ($\gamma'^2_{21}(K'_{21}) = 9$) ; les réseaux K'_{17} et L_{17d} de W. Plesken M. Pohst donnent pour γ'^2_{17} la valeur de [S].

Remarques : Pour $n = 10$, γ'^2_{10} atteint la valeur 4 sur les trois réseaux K'_{10}, Q_{10} (réseau isodual décrit dans [C-S 1]) et $\mathbb{D}^+_{10}$ (également isodual). Pour $n = 11,\ 12$ (resp. $n = 13,\ 14,\ 15,\ 16,\ 22,\ 23,\ 24$) les plus grandes valeurs connues sont atteintes sur K_n (resp. sur Λ_n). Pour $n = 19,\ 20$, les réseaux Λ_n et K_n fournissent tous deux la meilleure borne connue. On peut noter que le résultat n'est certainement pas optimal pour $n = 17, 19$, les réseaux K'_{17}, Λ_{17d}, Λ_{19} et K_{19} n'étant pas dual-extrêmes. Signalons que γ'^2_{14} prend sur le réseau Q_{14} de [C-S 3] la même valeur que sur Λ_{14}.
[G. Nebe et W. Plesken ont construit un réseau isodual (retrouvé par H-G. Quebbemann) ayant une constante $\gamma'^2_{20} = \frac{64}{7} = 9,14...$ supérieure à celle de Λ_{20}, cf. [Ne-Pl] §IX, réseau $\lfloor 2.M_{22}.2 \rfloor_{20}$.]

1.4 RÉSULTATS NUMÉRIQUES.

Dans les tableaux suivants, nous utilisons les abréviations : E pour extrême, p pour parfait (ce qui n'exclut pas l'extrémalité), e pour eutactique, D pour dual-extrême, s-e pour semi-eutactique (i.e. analogue à eutactique mais avec des coefficients positifs ou nuls), DP lorsque le réseau est dual-parfait (i.e. les projections sur les directions des vecteurs minimaux du réseau et de son dual engendrent l'espace $\mathrm{End}^s(\mathbb{R}^n)$ des endomorphismes symétriques de $\mathbb{R}^n$), ce qui n'exclut pas la dual-extrémalité lorsque s^*, le nombre de paires de vecteurs minimaux du dual est au moins égal à n, R pour "rien" et ? lorsque les résultats ne sont pas connus.

Nous avons calculé les invariants suivants : le déterminant $\det(L)$, la norme minimale N' du dual rendu entier, le carré de l'invariant d'Hermite dual $\gamma_n'^2(L)$, le couple $(s,\ s^*)$ où s est le nombre de couples de vecteurs minimaux de L et s^* celui de L^* rendu entier, $(L,\ L^*)$ désigne les propriétés de L et de L^*, l'annulateur $\mathrm{ann}(L^*/L)$ et la norme minimale N de L.

Il est probable quoique peut-être non vérifié en toute dimension n, que les réseaux Λ_n $(0 \leq n \leq 24)$, K_n $(n \neq 7,\ 8)$ et K'_n $(n \neq 3,\ 4)$ sont extrêmes. Nous avons aussi cherché les invariants du réseau K_{q9} qui est parfait, contenu dans K_{10} et non dans K'_{10}, de même déterminant que K'_9 mais avec $s = 82$ au lieu de 81, ainsi que ceux de K_{q15}, un réseau isométrique à son orthogonal dans le réseau de Leech. Nous avons vérifié l'eutaxie lorsque les coefficients sont égaux ou lorsqu'elle provient d'une représentation irréductible du groupe d'automorphismes. Par exemple, Λ_{23} et Λ_{23}^* sont extrêmes puisqu'ils définissent la représentation irréductible de degré 23 du groupe Co_2 [ATLAS].

n	L	$\det(L)$	N'	$\gamma_n'^2(L)$	$(s,\ s^*)$	$(L,\ L^*)$	$\mathrm{ann}(L^*/L)$	N
1	$\mathbb{Z}$	1	1	1	$(1,1)$	$(E,E)\ D$	1	1
2	$\mathbb{A}_2$	3	2	4/3	$(3,3)$	$(E,E)\ D$	3	4
3	$\mathbb{A}_3$	4	3	3/2	$(6,4)$	$(E,e)\ D$	4	4
4	$\mathbb{D}_4$	4	2	2	$(12,12)$	$(E,E)\ D$	2	4
5	$\mathbb{D}_5$	4	4	2	$(20,5)$	$(E,e)\ D$	4	4
	$\mathbb{A}_5^3$	162	3	2	$(15,10)$	$(E,e)\ D$	6	4
6	$\mathbb{E}_6$	3	4	8/3	$(36,27)$	$(E,E)\ D$	3	4
7	$\mathbb{E}_7$	2	3	3	$(63,28)$	$(E,E)\ D$	2	4
	K_7	384	12	2	$(46,1)$	$(e,R)\ DP$	24	4
8	$\mathbb{E}_8$	1	2	4	$(120,120)$	$(E,E)\ D$	1	4
	K_8	576	8	8/3	$(66,6)$	$(s\text{-}e,R)\ DP$	12	4
	K'_8	729	6	8/3	$(54,12)$	$(E,e)\ D$	9	4
9	Λ_9	512	4	2	$(136,1)$	$(E,R)\ DP$	8	4
	K_9	864	16	8/3	$(90,3)$	$(p,R)\ DP$	24	4
	K'_9	972	27	3	$(81,13)$	$(E,s\text{-}e)\ D$	36	4
	K_{q9}	972	27	3	$(82,4)$	$(p,R)\ DP$	36	4
	$\mathbb{A}_9^5$	781 250	4	16/5	$(45,45)$	$(E,E)\ D$	10	8
10	Λ_{10}	768	8	8/3	$(168,3)$	$(p,R)\ DP$	12	4
	K_{10}	972	16	32/9	$(138,27)$	$(p,R)\ DP$	18	4
	K'_{10}	972	6	4	$(135,120)$	$(E,E)\ D$	6	4
	$\mathbb{D}_{10}^+$	1 024	4	4	$(90,90)$	$(E,E)\ D$	4	4
	Q_{10}	1 024	4	4	$(130,130)$	$(E,E)\ D$	4	4
11	$\Lambda_{11}^{\min}$	1 024	12	3	$(216,4)$	$(p,R)\ DP$	16	4
	$\Lambda_{11}^{\max}$	1 024	3	3	$(219,4)$	$(p,R)\ DP$	4	4
	K_{11}	972	12	4	$(216,41)$	$(E,e)\ D$	12	4
	$\mathbb{A}_{11}^3$	236 196	8	4	$(66,66)$	$(E,E)\ D$	12	6

n	L	$\det(L)$	N'	$\gamma_n'^2(L)$	$(s,\ s^*)$	$(L,\ L^*)$	$\mathrm{ann}(L^*/L)$	N
12	$\Lambda_{12}^{\min}$	1024	8	4	(312, 12)	$(p,R)\ DP$	8	4
	$\Lambda_{12}^{\mathrm{mid}}$	1024	4	4	(316, 20)	(p,R)	4	4
	$\Lambda_{12}^{\max}$	1024	4	4	(324, 36)	$(E,e)\ D$	4	4
	K_{12}	729	4	16/3	(378, 378)	$(E,E)\ D$	3	4
13	$\Lambda_{13}^{\min}$	1 024	16	4	(444, 5)	$(p,R)\ DP$	16	4
	$\Lambda_{13}^{\mathrm{mid}}$	1 024	4	4	(445, 5)	$(p,R)\ DP$	4	4
	$\Lambda_{13}^{\max}$	1 024	4	4	(453, 13)	$(E,e)\ D$	4	4
	K_{13}	972	9	3	(459, 1)	$(p,R)\ DP$	12	4
14	Λ_{14}	768	16	16/3	(711, 75)	$(p,?)$	12	4
	L_{14b}	1 024	4	4	(614, 6)	(p,R)	4	4
	L_{14c}	1 024	4	4	(606, 6)	(p,R)	4	4
	L_{14d}	1 024	16	4	(605, 2)	$(p,R)\ DP$	16	4
	K'_{14}	972	1	4	(624, 3)	$(p,R)\ DP$	6	4
	K_{14}	972	18	4	(621, 3)	$(p,R)\ DP$	18	4
15	Λ_{15}	512	12	6	(1 170, 140)	$(E,E)\ D$	8	4
	L_{15b}	768	12	4	(936, 1)	$(p,R)\ DP$	12	4
	L_{15c}	1 024	4	4	(815, 7)	$(p,R)\ DP$	4	4
	L_{15d}	1 024	16	4	(798, 3)	$(p,R)\ DP$	16	4
	K_{15}	864	27	9/2	(873, 4)	$(p,R)\ DP$	24	4
	K'_{15}	972	36	4	(822, 2)	$(p,R)\ DP$	36	4
	K_{q15}	972	36	4	(819, 2)	$(p,R)\ DP$	36	4
16	Λ_{16}	256	4	8	(2 160, 2 160)	$(E,E)\ D$	2	4
	L_{16b}	512	8	4	(1 491, 1)	$(p,R)\ DP$	8	4
	L_{16c}	768	12	4	(1 201, 2)	$(p,R)\ DP$	12	4
	L_{16d}	768	32	16/3	(1 182, 1)	$(p,R)\ DP$	24	4
	K_{16}	576	16	16/3	(1 386, 6)	$(p,R)\ DP$	12	4
	K''_{16}	729	36	16/3	(1 218, 9)	$(p,R)\ DP$	27	4
	K'_{16}	729	12	16/3	(1 224, 36)	$(E,e)\ D$	9	4
17	Λ_{17}	256	4	4	(2 673, 1)	$(p,R)\ DP$	4	4
	L_{17b}	512	8	4	(1 860, 2)	$(p,R)\ DP$	8	4
	L_{17c}	512	44	11/2	(1 827, 8)	$(p,R)\ DP$	32	4
	L_{17d}	512	12	6	(1 818, 24)	(p,R)	8	4
	K_{17}	384	32	16/3	(2 133, 3)	$(p,R)\ DP$	24	4
	K'_{17}	486	6	6	(1 872, 37)	(p,R)	18	4
18	Λ_{18}	192	8	16/3	(3 699, 3)	$(p,R)\ DP$	6	4
	L_{18b}	256	4	4	(3 250, 2)	$(p,R)\ DP$	4	4
	L_{18c}	256	12	6	(3 168, 8)	$(p,R)\ DP$	8	4
	K'_{18}	243	6	8	(3 240, 1 080)	$(E,E)\ D$	3	4
19	Λ_{19}	128	12	6	(5 334, 4)	$(p,R)\ DP$	8	4
	K'_{19}	162	9	6	(4 698, 1)	$(p,R)\ DP$	6	4
20	Λ_{20}	64	8	8	(8 700, 60)	$(E,e)\ D$	4	4
	K'_{20}	81	18	8	(7 695, 30)	$(E,e)\ D$	9	4
21	Λ_{21}	32	16	8	(13 860, 21)	$(E,e)\ D$	8	4
	K'_{21}	36	27	9	(13 041, 112)	$(E,e)\ D$	12	4
22	Λ_{22}	12	16	32/3	(24 948, 891)	$(E,E)\ D$	6	4
23	Λ_{23}	4	12	12	(46 575, 2 300)	$(E,E)\ D$	4	4
24	Λ_{24}	4	4	16	(98 280, 98 280)	$(E,E)\ D$	1	4

Les 13 vecteurs minimaux de $\Lambda_{13}^{\max *}$ sont orthogonaux deux à deux. Il en est de même pour les 21 vecteurs minimaux de Λ_{21}^{*} ainsi que pour les cinq vecteurs minimaux de $\mathbb{D}_5^*$.

1.5 A PROPOS DU RÉSEAU DE CH. BACHOC.

On considère l'algèbre non commutative des quaternions de Hamilton. Elle sera notée $\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$ où $i,\ j,\ k$ vérifient les relations $i^2 = j^2 = k^2 = -1$ et $ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j$. Elle est ramifiée en 2 et à l'infini. Elle possède un unique ordre maximal $\mathfrak{M}$, l'ordre de Hurwitz, de base $(1,\ i,\ j,\ \omega)$ avec $\omega = \frac{-1+i+j+k}{2}$.

Ch. Bachoc a construit sur cet ordre un réseau noté BC_{32} de norme minimale 6, de déterminant 2^{16}, ayant 2.130 560 vecteurs minimaux, c'est-à-dire ayant les mêmes invariants que celui de Quebbemann ([Q] ; [C-S 2 chap. 8, p. 220]). Il existe à ce jour trois réseaux de rang 32 ayant les mêmes invariants (i.e. de déterminant 2^{16} et avec 2.130 560 vecteurs minimaux). Ils sont semblables à leurs duals dans une similitude de rapport $\sqrt{2}$, mais ils ne sont pas isométriques entre eux. Dans [Pl-S], W. Plesken et B. Souvignier ont montré que les groupes d'automorphismes de ces trois réseaux n'ont pas le même cardinal. Nous utilisons ici celui de Ch. Bachoc.

Ch. Bachoc a donné une matrice d'ordre 8 des produits scalaires hermitiens et a écrit un programme transformant les matrices de ce type en des matrices de Gram usuelles d'ordre 32 ; ces dernières ont sur la diagonale 8 blocs d'ordre 4 correspondant à des $\mathfrak{M}$-modules de rang 1.

Partant de sa matrice, nous avons échangé les blocs 1 et 8, obtenant une matrice notée A, équivalente à la matrice $B = 2A^{-1}$. On construit les matrices $B_{32} = B$, B_{31}, B_{30}, B_{29} en supprimant quatre fois de suite les dernières colonnes et lignes. Nous avons recherché dans B_{29} des systèmes de quatre vecteurs minimaux de façon que, par orthogonalité dans A, apparaisse un réseau semblable à $\mathbb{E}_8$ renormalisé à la norme minimale de BC_{32}. Comme $\mathbb{E}_8$ et ses sections $\mathbb{E}_7$, $\mathbb{E}_6$, $\mathbb{D}_5$, $\mathbb{D}_4$, $\mathbb{A}_3$, $\mathbb{A}_2$, $\mathbb{A}_1$ sont les réseaux les plus denses jusqu'à la dimension 8, on en déduit par orthogonalité des sections de BC_{32} qui sont de densité maximale. Nous n'avons pas vérifié leur unicité à automorphisme près de BC_{32}. Notons également que nous ne pouvons pas garantir que le modèle de $\mathbb{E}_8$ trouvé soit une section de BC_{32} compatible avec la $\mathfrak{M}$-structure.

La table ci-dessous donne les principaux invariants des réseaux L trouvés, de norme minimale 6, notés BC_n : le déterminant $\det(L)$, $(s,\ s^*)$ où s est le nombre de couples de vecteurs minimaux et s^* celui de L^*, l'annulateur $\mathrm{ann}(L^*/L)$, la norme N' du réseau L^* rendu entier, l'invariant d'Hermite $\gamma_n(L)$ et le carré de l'invariant d'Hermite dual $\gamma_n'^2(L)$:

L	$\det(L)$	$(s,\ s^*)$	$\mathrm{ann}(L^*/L)$	N'	$\gamma_n(L)$	$\gamma_n'^2(L)$
BC_{32}	65 536	(130 560, 130 560)	2	6	4.24	18
BC_{31}	196 608	(67 860, 760)	12	27	4.05	13.5
BC_{30}	442 368	(40 083, 144)	18	36	3.89	12
BC_{29}	884 736	(24 774, 5)	24	36	3.74	9
BC_{28}	1 327 104	(17 376, 12)	12	18	3.62	9

L	$\det(L)$	$(s,\ s^*)$	$\mathrm{ann}(L^*/L)$	N'	$\gamma_n(L)$	$\gamma_n'^2(L)$
BC_{27}	1 990 656	(12 165, 4)	24	27	3.50	6.75
BC_{26}	2 239 488	(9 591, 3)	18	18	3.41	6
BC_{25}	2 239 488	(7 917, 1)	12	9	3.34	4.50
BC_{24}	1 679 616	(7 080, 1 440)	6	10	3.30	10
BC_{23}	2 799 360	(4 629, 23)	60	75	3.14	7.5
BC_{22}	3 499 200	(2 913, 4)	90	100	3.02	6.66...
BC_{21}	3 888 000	(2 063, 4)	120	128	2.91	6.4
BC_{20}	4 147 200	(1 473, 1)	960	868	2.80	5.42
BC_{19}	3 749 760	(1 115, 1)	104 160	80 475	2.70	4.63
BC_{18}	2 897 100	(887, 2)	96 570	74 772	2.62	4.64
BC_{17}	2 243 160	(688, 1)	186 930	121 203	2.53	3.89
BC_{16}	1 454 436	(561, 6)	1 206	934	2.47	4.64

Nous avons également donné les invariants de réseaux de dimensions 23, 22, 21, 20, 19, 18, 17, 16 obtenus par sections successives de densité maximale. Notons que nous ne pouvons pas montrer que les réseaux de dimensions 23 à 16 trouvés, soient des sections de BC_{32} de densité maximale (la situation est la même que pour le réseau de Leech pour lequel il n'est pas démontré que les réseaux Λ_n (resp. K_n) soient les sections les plus denses dans les dimensions 9, 10, 14, 15 (resp. 11, 12, 13 cf. [C-S 2 chap. 6]).

On peut remarquer que, pour $16 \leq n \leq 29$, on a $\gamma_n(\Lambda_n) > \gamma_n(BC_n)$ et que pour $n = 30,\ 31,\ 32$, c'est le contraire. Les réseaux BC_n sont parfaits pour $16 \leq n \leq 32$.

Le groupe d'automorphismes de BC_{32} n'opère pas transitivement sur les sections semblables à $\mathbb{A}_3$. Nous avons en effet trouvé une section de dimension 29 orthogonale à une section minimale dont une suite de sections hyperplanes successives les plus denses produit les déterminants $1\ 658\ 880 = 2^{12}.3^4.5$, $243\ 3024 = 2^{13}.3^3.11$, $3\ 345\ 408 = 2^{10}.3^3.11^2$, $4\ 561\ 920 = 2^{10}.3^4.5.11$ alors que l'on trouve $1\ 327\ 104 = 2^{14}.3^4$, $1\ 990\ 656 = 2^{13}.3^5$, $2\ 239\ 488 = 2^{10}.3^7$, 2 239 488 lorsque l'orthogonal est une section minimale de type $\mathbb{D}_4$.

Voici les invariants d'une suite de sections de densité maximale de ce réseau de dimension 29, notés BC_n' pour $16 \leq n \leq 29$, de norme minimale 6 :

L	$\det(L)$	$(s,\ s^*)$	$\mathrm{ann}(L^*/L)$	N'	$\gamma_n(L)$	$\gamma_n'^2(L)$
BC'_{29}	884 736	(24 684, 168)	24	45	3.74	11.25
BC'_{28}	1 658 880	(15 445, 2)	270	396	3.59	8.79...
BC'_{27}	2 433 024	(10 728, 1)	264	363	3.48	8.25
BC'_{26}	3 345 408	(7 547, 1)	198	270	3.36	8.18
BC'_{25}	4 561 920	(5 251, 2)	1 980	2 597	3.24	7.86
BC'_{24}	5 983 488	(3 644, 1)	15 582	17 204	3.13	6.62

L	$\det(L)$	$(s,\ s^*)$	$\mathrm{ann}(L^*/L)$	N'	$\gamma_n(L)$	$\gamma_n'^2(L)$
BC'_{23}	6 606 336	(2 698, 1)	103 224	113 219	3.03	6.58
BC'_{22}	7 246 016	(1 953, 1)	226 438	245 200	2.92	6.49
BC'_{21}	7 846 400	(1 390, 1)	490 400	448 525	2.81	5.48
BC'_{20}	7 176 400	(1 065, 1)	897 050	812 978	2.72	5.43
BC'_{19}	6 503 824	(795, 1)	1 625 956	1 375 860	2.62	5.07
BC'_{18}	5 503 440	(597, 1)	1 375 860	1 103 474	2.53	4.81
BC'_{17}	4 413 896	(449, 1)	4 413 896	3 317 145	2.43	4.51
BC'_{16}	3 317 145	(339, 1)	3 317 145	2 201 700	2.34	3.98

On peut noter le même phénomène en ce qui concerne l'invariant d'Hermite des réseaux laminés Λ_n et des réseaux BC'_n que précédemment. Les réseaux BC'_n sont parfaits pour $16 \leq n \leq 32$.

L'orthogonal de BC'_{24} dans BC_{32} est un nouveau réseau extrême de dimension 8, de norme minimale 6 dont l'invariant d'Hermite vaut 1.7063..., ne contenant aucune section hyperplane parfaite. Il possède une base de vecteurs minimaux. Le tableau ci-dessous fournit certains de ses invariants : la notation DP signifie que ce réseau est dual-parfait et E qu'il est extrême.

$\det(L)$	N'	$\gamma_8'^2(L)$	$(s,\ s^*)$	$(L,\ L^*)$	$\mathrm{ann}(L^*/L)$	N
23 373	2 970	2.2872...	(44, 1)	$(E,\ R)\ DP$	7 791	6

Ce réseau ne peut pas être dual-extrême car son dual ne posséde que deux vecteurs minimaux. On donne ci-après une matrice de Gram de ce réseau dans une base de vecteurs minimaux.

$$\begin{pmatrix} 6 & 3 & -3 & 2 & -3 & -3 & 3 & 1 \\ 3 & 6 & -3 & 3 & -3 & -3 & 3 & -1 \\ -3 & -3 & 6 & 0 & 3 & 2 & -2 & -2 \\ 2 & 3 & 0 & 6 & -3 & 0 & 1 & -1 \\ -3 & -3 & 3 & -3 & 6 & 0 & -3 & -2 \\ -3 & -3 & 2 & 0 & 0 & 6 & -3 & 2 \\ 3 & 3 & -2 & 1 & -3 & -3 & 6 & -1 \\ 1 & -1 & -2 & -1 & -2 & 2 & -1 & 6 \end{pmatrix}$$

N.B : Deux erreurs ont été corrigées : dans le tableau de la page 11, la norme minimale du réseau $\mathbb{A}_9^5$ n'est pas 4, mais 8 et de même dans le tableau de la page 13, la constante $\gamma_{29}(BC_{29})$ vaut 3.74 et non 3.80 comme il est écrit dans [Na].

BIBLIOGRAPHIE

[**ATLAS**] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, R.A. Wilson, *ATLAS of Finite Groups*, Oxford Univ. Press, Oxford, 1985.

[**Ba**] Ch. Bachoc, *Voisinage au sens de Kneser pour les réseaux quaternioniens*, Comm. Math. Helvet. 70 (1995), 350–374.

[**B-M**] A-M. Bergé, J. Martinet, *Sur un problème de dualité lié aux sphères en géométrie des nombres*, J. Number Theory 32 (1989), 14–42.

[**C-S 1**] J.H. Conway, N.J.A. Sloane, *On Lattices Equivalent to Their Duals*, J. Number Theory 48 (1994), 373–382.

[**C-S 2**] J.H. Conway, N.J.A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, Grundlehren n°290, Heidelberg, 1988.

[**C-S 3**] J.H. Conway, N.J.A. Sloane, *Low-dimensional lattices. II. Subgroups of* $Gl(n, \mathbb{Z})$, Proc. Royal Soc. London **A** 419 (1988), 29–68.

[**M 1**] J. Martinet, *Structures algébriques sur les réseaux*, Number Theory, S. David éd. (Séminaire de Théorie des Nombres de Paris, 1992 – 93), Cambridge University Press, Cambridge, 1995, pp. 167–186.

[**M 2**] J. Martinet, *Les réseaux parfaits des espaces euclidiens*, livre en préparation.

[**Na**] H. Napias, *Sur quelques réseaux contenus dans les réseaux de Leech et de Quebbemann*, Comptes Rendus Acad. Sc. Paris 319, **série I** (1994), 653–658.

[**Ne-Pl**] W. Plesken, G. Nebe, *Finite rational matrix groups*, *Memoirs A.M.S.*, vol. 116, number 556, pp. 1–144.

[**Pari**] Ch. Batut, D. Bernardi, H. Cohen and M. Olivier, User's Guide to PARI-GP.

[**Pl-P**] W. Plesken, M. Pohst, *Constructing Integral Lattices With Prescribed Minimum. II*, Math. Comp. 60 (1993), 817–825.

[**Pl-S**] W. Plesken, B. Souvignier, *Computing isometries of lattices*, J. Symbolic Computation, à paraître.

[**Q**] H-G. Quebbemann, *Lattices with theta-functions for* $G(\sqrt{2})$ *and linear codes*, J. Algebra 105 (1987), 443–450.

[**S**] N.J.A. Sloane, *Lettre à J. Martinet du* 11 *Mai* 1992.

Chapitre 2

Des voisinages de réseaux.

Soit Λ un réseau donné par une matrice de Gram A dans une base. On dira que la forme quadratique associée à L est la forme q admettant A pour matrice. Elle est définie positive et par abus de langage, on dira aussi que A est définie positive. Deux formes quadratiques q et q' seront dites équivalentes s'il existe une matrice P de $\mathrm{Gl}_n(\mathbb{Z})$ telle que $A' = {}^tPAP$ où les matrices A et A' correspondent respectivement à q et q'.

Dans ce chapitre, on cherche les formes parfaites contiguës à une forme parfaite donnée, à isométrie près. Ceci se fera grâce à l'algorithme de Voronoï.

Par abus de langage, on parlera aussi bien de réseaux que de formes quadratiques définies positives (qui leur sont associées) et de matrices symétriques définies positives.

2.1 LES FORMES CONTIGUËS.

On se place dans l'espace vectoriel des formes quadratiques définies positives (resp. des endomorphismes symétriques) sur $\mathbb{R}^n$ muni du produit scalaire $\langle Q, R\rangle = \mathrm{Tr}(AB)$ ((resp. $\langle u, v\rangle = \mathrm{Tr}(uv)$) où A et B sont les matrices correspondant à Q et R respectivement (resp. u et v sont deux endomorphismes symétriques) et $\mathrm{Tr}(A)$ désigne la trace de la matrice A (resp. $\mathrm{Tr}(u)$ désigne la trace de l'endomorphisme u). Cet espace euclidien est appelé espace de Voronoï et noté $\mathcal{V}or$, de l'ensemble $\mathcal{Q}$ des formes quadratiques définies positives (resp. $\mathcal{L}$ des endomorphismes symétriques) sur $\mathbb{R}^n$. Il a pour dimension $N = \frac{n(n+1)}{2}$.

A tout élément $x = (x_i)_{1\leq i\leq n}$ de $\mathbb{R}^n$ est associé le vecteur colonne X dont les composantes sont les x_i. Le produit scalaire $X{}^tX$ est la matrice symétrique d'ordre n

$$\begin{pmatrix} x_1^2 & x_1x_2 & \dots & x_1x_n \\ x_2x_1 & x_2^2 & \dots & x_2x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_nx_1 & x_nx_2 & \dots & x_n^2 \end{pmatrix}.$$

On appelle domaine de Voronoï de la forme Q de $\mathcal{Q}$ associée au réseau Λ, l'enveloppe convexe dans l'espace $\mathcal{V}or$ des demi-droites issues de l'origine et contenant les projections

sur les vecteurs minimaux du réseau Λ (i.e. les $X{}^tX$ où le vecteur colonne X correspond à un vecteur minimal de Λ). Il sera noté $\mathcal{D}_Q$ ou $\mathcal{D}_\Lambda$. Un réseau Λ est parfait lorsque son domaine de Voronoï est d'intérieur non vide (ou lorsque son domaine de Voronoï n'est pas contenu dans un hyperplan de l'espace de Voronoï).

On rappelle qu'étant donné un convexe C, un hyperplan d'appui de C est un hyperplan affine H qui rencontre C et qui est tel que C soit contenu dans l'un des deux demi-espaces définis par H. On note $\mathcal{F}$, une face du domaine $\mathcal{D}_\Lambda$ c'est-à-dire l'intersection de $\mathcal{D}_\Lambda$ avec un de ses hyperplans d'appui. Il lui est associé un vecteur R de l'espace $\mathcal{V}or$ (autrement dit une matrice symétrique réelle d'ordre n), orthogonal à $\mathcal{F}$ et orienté vers l'extérieur de $\mathcal{F}$. Le vecteur R est appelé vecteur de face associé à $\mathcal{F}$.

On peut donc dire que $\mathcal{D}_\Lambda = \{Y \mid \langle R, Y\rangle \geq 0\}$.

Définition et proposition.

Étant donnés une forme quadratique définie positive Q parfaite sur $\mathbb{R}^n$ et un vecteur de face R associé à la face $\mathcal{F}$ du domaine $\mathcal{D}_Q$, on appelle forme contiguë à (ou voisine de) Q le long de la face $\mathcal{F}$, l'unique forme quadratique parfaite $Q_\rho = Q + \rho R$ où ρ est un nombre réel strictement positif (et en fait rationnel), de même minimum que Q, différente de Q et ayant la face $\mathcal{F}$ en commun avec Q.

Pour tout $\theta \in \mathbb{R}$, si $0 < \theta < \rho$ alors la forme quadratique $Q + \theta R$ est non parfaite et de même minimum que Q et si $\theta > \rho$ ou $\theta < 0$, elle est ou bien indéfinie ou bien de norme minimale inférieure à celle de Q. Si $0 < \theta < \rho$, les vecteurs minimaux de $Q + \rho R$ sont les vecteurs minimaux de Q d'image dans $\mathcal{F}$.

Remarque : Si A et B sont deux matrices symétriques réelles d'ordre n correspondant à deux formes quadratiques équivalentes Q_A et Q_B, il existe une matrice de passage P de $\mathrm{Gl}_n(\mathbb{Z})$ telle que $A = {}^tP\ B\ P$. Si $\mathcal{F}_A$ est une face de $\mathcal{D}_{Q_A}$ de vecteur de face R_A alors $\mathcal{F}_B = P^{-1}\ \mathcal{F}_A\ {}^tP^{-1}$ est une face de Q_B de vecteur de face R_B (image de R_A par l'application envoyant Q_A sur Q_B). On peut donc dire que si $Q_A + \rho R_A$ est la forme contiguë à Q_A le long de la face $\mathcal{F}_A$ alors $Q_B + \rho R_B$ est la forme contiguë à Q_B le long de la face $\mathcal{F}_B$. Par conséquent, la relation de contiguïté est définie modulo les classes d'équivalence de formes quadratiques définies positives (ou des réseaux).

Lorsque le nombre de couples de vecteurs minimaux du réseau vaut N, on peut associer à un représentant de chaque orbite de vecteurs minimaux du réseau Λ, la face du domaine $\mathcal{D}_\Lambda$ qui ne la contient pas (sa face opposée). Toutefois, on peut obtenir plusieurs formes équivalentes suivant des faces ne correspondant pas à la même orbite de vecteurs minimaux : c'est le cas dans le quatrième paragraphe, pour des réseaux voisins du réseau de racines $\mathbb{E}_8$. Lorsque le groupe des automorphismes du réseau Λ est transitif sur la sphère de ses vecteurs minimaux $S(\Lambda)$ et que cette sphère a pour demi-cardinal N, on n'obtiendra qu'une seule forme contiguë, à isométrie près (c'est le cas pour les réseaux de Coxeter).

On note $s(\Lambda)$ ou s le demi-cardinal de la sphère des vecteurs minimaux d'un réseau Λ et s^* le nombre de paires de vecteurs minimaux du réseau dual Λ^*. On rappelle que le "kissing number" est la quantité $2s$.

Description de l'algorithme de voisinages utilisé.

Donnée : une matrice de Gram A d'un réseau parfait en dimension n et un représentant de chaque orbite de vecteurs minimaux.
Sortie : une matrice de Gram C de chaque réseau contigu.

On se place dans le cas où $s = \frac{n(n+1)}{2}$. Les représentants des vecteurs minimaux sont donnés en ligne.

Étape 1 : Pour un représentant v_k d'une orbite de vecteurs minimaux, trouver un vecteur de face correspondant (i.e. une matrice symétrique d'ordre n notée B telle que $\langle B, {}^t v_k v_k \rangle > 0$ et $\langle B, {}^t v_j v_j \rangle = 0$ pour tout $j \neq k$).

Étape 2 : Trouver le rationnel $\rho > 0$ tel que la forme $A + \rho B$ soit parfaite, de même norme minimale que A et sortir $C = A + \rho B$.

Étape 3 : Passer au vecteur suivant (s'il en reste) et revenir à l'étape 1.

Remarque : La recherche du rationnel ρ s'effectue de la manière suivante : on l'encadre entre un entier naturel m et son successeur (i.e. l'entier m est la borne supérieure des réels θ tels que la forme $A + \theta B$ soit de même norme minimale que A mais pas parfaite et $m+1$ est la borne inférieure des réels θ tels que la forme $A + \theta B$ soit ou bien indéfinie ou bien de norme minimale inférieure à celle de A). Ensuite, on écrit ρ sous la forme $m + \frac{p}{q}$ où p et q sont deux entiers naturels non nuls tels que $p < q$. On fait parcourir à p et q l'ensemble $\mathbb{N} \setminus \{0\}$ jusqu'à ce que la forme $A + (m + \frac{p}{q})B$ soit parfaite et de même minimum que A et on donne à ρ cette valeur. C'est cette recherche qui coûte le plus de temps dans l'algorithme.

Dans les deux paragraphes suivants, on recherche les réseaux contigus à des réseaux de "kissing number" égal à $n(n+1)$ (i.e. aux réseaux de Coxeter dont le groupe d'automorphismes est transitif sur l'ensemble de leurs vecteurs minimaux et à certains des réseaux parfaits ayant une section hyperplane parfaite ou pas, en dimension $n = 8$).

2.2 LES RÉSEAUX DE COXETER $\mathbb{A}_n^r$.

Soit $n \geq 0$ un entier. On rappelle que le réseau de racines $\mathbb{A}_n$ est l'intersection de $\mathbb{Z}^{n+1}$ avec l'hyperplan $E = (\varepsilon_0 + \varepsilon_1 + \cdots + \varepsilon_n)^{\perp}$. Les vecteurs $e_i = \varepsilon_0 - \varepsilon_i, 1 \leq i \leq n$, en constituent une base.

Définition.

Soit $e = e_1 + \cdots + e_n$. Pour tout nombre rationnel r positif on note $\mathbb{A}_n^r$ le réseau de $\mathbb{R}^n$ de base $(e_1, e_n, \ldots, e_{n-1}, \frac{1}{r}e)$ et on pose $q = \frac{n+1}{r}$.

Lorsque r est un entier qui divise $n+1$, ces réseaux sont appelés réseaux de Coxeter.

La matrice de Gram $(a_{i,j})$ du réseau $\mathbb{A}_n^r$ dans la base $(e_1, e_n, \ldots, e_{n-1}, \frac{1}{r}e)$ a pour coefficients :

$a_{i,i} = 2$ pour $1 \leq i \leq n-1$, $a_{i,j} = a_{j,i} = 1$ pour $1 \leq i,\ j \leq n-1$, $a_{i,n} = a_{n,i} = \frac{n+1}{r}$ pour $1 \leq i \leq n-1$ et $a_{n,n} = \frac{n(n+1)}{r^2}$.

Le réseau de Coxeter $\mathbb{A}_n^r$ est l'unique sous-réseau de $\mathbb{A}_n^*$ contenant $\mathbb{A}_n$ avec l'indice r. Dans ce cas, on a $(\mathbb{A}_n^r)^* = \mathbb{A}_n^q$.

On ne va s'intéresser qu'aux réseaux de Coxeter (i.e. r est un entier positif divisant $n+1$).

On rappelle que la constante d'Hermite duale (ou constante de Bergé-Martinet) en dimension n est la quantité $\gamma_n' = \sup_L \gamma_n'(L)$ avec $\gamma_n'(L) = \sqrt{N(L)N(L^*)}$ et qu'un réseau est dual-extrême lorsqu'il réalise un maximum local de cet invariant.

Théorème (COXETER).

1) Les réseaux $\mathbb{A}_n^r$ sont extrêmes sauf si $r = n+1$, $n \geq 3$, ou $n = 3$ ou 5 et $r = 2$, cas dans lesquels ils sont eutactiques mais non parfaits.

2) $\mathbb{A}_n^r$ est de norme 2 et on a $S(\mathbb{A}_n^r) = S(\mathbb{A}_n)$ sauf si $r = n+1$, $r = \frac{n+1}{2}$ ou $r = 2$ et $n = 5$ ou $r = 2$ et $n = 7$ ($\mathbb{A}_7^2$ est isométrique à $\mathbb{E}_7$) ou $r = 3$ et $n = 8$ ($\mathbb{A}_8^3$ est isométrique à $\mathbb{E}_8$).

3) Lorsque n est impair et $r = \frac{n+1}{2}$, $s = \frac{n(n+1)}{2}$, $N(\mathbb{A}_n^r) = \frac{2(n-1)}{n+1}$ sauf pour $n = 3$ où $s(\mathbb{A}_3^2) = 3$. Si $r = n+1$ on a $s(\mathbb{A}_n^{n+1}) = n+1$ et $N(\mathbb{A}_n^{n+1}) = \frac{n}{n+1}$, $s(\mathbb{A}_5^2) = 10$ et $N(\mathbb{A}_5^2) = \frac{3}{2}$.

4) On a $\mathrm{Aut}(\mathbb{A}_n^r) = \mathrm{Aut}(\mathbb{A}_n)$ si $\mathbb{A}_n^r$ est de norme minimale 2 auquel cas le groupe des automorphismes de $\mathbb{A}_n^r$ est transitif sur l'ensemble de ses vecteurs minimaux. Pour $n \geq 5$ et $n \neq 7$ le groupe des automorphismes de $\mathbb{A}_n^{\frac{n+1}{2}}$ est transitif sur la sphère de ses vecteurs minimaux.

5) Les réseaux $\mathbb{A}_n^r$ sont dual-extrêmes, sauf $\mathbb{A}_3^2$ qui est semblable à $\mathbb{Z}^3$.

6) On a $\gamma_n'^2(\mathbb{A}_n^r) = 4$ pour $3 \leq r \leq \frac{n+1}{3}$, $\gamma_n'^2(\mathbb{A}_n^2) = \gamma_n'^2(\mathbb{A}_n^{\frac{n+1}{2}}) = \frac{4(n-1)}{n+1}$ pour n impair et $n \geq 7$, $\gamma_5'^2(\mathbb{A}_n^2) = 2$ et $\gamma_n'^2(\mathbb{A}_n^{n+1}) = \gamma_n'^2(\mathbb{A}_n) = \frac{2n}{n+1}$ pour tout $n \geq 1$.

On trouvera une preuve de ce théorème dans [M].

2.3 LES VOISINS DES RÉSEAUX DE COXETER $\mathbb{A}_n^r$.

Dans ce paragraphe, on va chercher les réseaux contigus aux réseaux de Coxeter $\mathbb{A}_n^2$ et $\mathbb{A}_n^{\frac{n+1}{2}}$. Pour cela, on définit d'autres réseaux liés aux réseaux de racines $\mathbb{D}_n$.

2.3.1 Les réseaux $\mathbb{D}_{n,t}$.

Soient $n \geq 4$ et $t > 0$ deux entiers. On suppose t pair. On rappelle que le réseau de racines $\mathbb{D}_n$ est $\{\sum_1^n x_i\varepsilon_i \in \mathbb{Z}^n \mid \sum x_i \equiv 0 \pmod 2\}$.

Définition.

Soit $f = \sum_1^t \varepsilon_i \in \mathbb{D}_n$. On note $\mathbb{D}_{n,t}$ le réseau engendré par $\mathbb{D}_n$ et $\frac{1}{2}f$.

Proposition.

$\mathbb{D}_{n,t}$ a pour déterminant 1 ; on a $s = n(n-1)$ pour $t > 8$ et $s(\mathbb{D}_{n,8}) = n(n-1)+64$. Il est extrême si et seulement si $t \geq 8$. Lorsque $t = n$ (donc pour n pair), $\mathbb{D}_{n,t}$ est l'empilement $\mathbb{D}_n^+$. Le réseau $\mathbb{D}_{n,t}$ est demi-entier et n'est entier que si $t = n$ et $n \equiv 0$ (mod 4).

2.3.2 Cas où $n \geq 9$ et $r = 2$.

Théorème.

Pour n impair et $n \geq 9$ (resp. pour n pair et $n \geq 10$), le voisin de $\mathbb{A}_n^2$ est le réseau $\mathbb{D}_{n,n-1}$ (resp. $\mathbb{D}_{n,n-2}$).

Preuve

On suppose n impair. On est dans le cas où $s(\mathbb{A}_n^2) = \frac{n(n+1)}{2} = N$ et le groupe des automorphismes de $\mathbb{A}_n^2$ est transitif sur la sphère de ses vecteurs minimaux. Il suffit donc de chercher le voisin de $\mathbb{A}_n^2$ pour un vecteur minimal quelconque, par exemple le vecteur $\varepsilon_1 - \varepsilon_2$.

On note A la matrice de Gram de $\mathbb{A}_n^2$ dans la base $(e_1, e_2, \ldots, e_{n-1}, e'_n = \frac{1}{2}e)$. Les vecteurs minimaux de $\mathbb{A}_n^2$ sont les $\pm(\varepsilon_i - \varepsilon_j)$ pour $0 \leq i < j \leq n$. On pose $X_{i,j} = \varepsilon_i - \varepsilon_j$. Les matrices des $X_{i,j}{}^tX_{i,j}$ ont pour coefficients, si i ou $j \neq n$, $q_{i,i} = q_{j,j} = 1$, $q_{i,j} = q_{j,i} = -1$ et $q_{k,l} = 0$ pour $(k,l) \neq (i,j)$.

Pour traiter le cas i ou $j = n$, on suppose que c'est j qui est égal à n. Alors $X_{i,n}$ est un vecteur colonne ayant pour composantes -1 suivant les vecteurs e_j pour $1 \leq j \leq n-1$ et $j \neq i$, -2 suivant e_i et 2 suivant e'_n. On peut ainsi calculer les coefficients de $X_{i,n}{}^tX_{i,n}$. On cherche une matrice B, symétrique, orthogonale à $X_{1,2}{}^tX_{1,2}$. On voit que l'on peut se ramener à la matrice $(b_{i,j})$ telle que $b_{1,2} = -1$, $b_{k,l} = 0$ si $(k,l) \neq (1,2)$ et (k ou $l \neq n$), $b_{1,n} = b_{2,n} = -\frac{1}{2}$, $b_{k,n} = 0$ pour $3 \leq k \leq n-1$ et $b_{n,n} = -\frac{1}{2}$. On vérifie que $\langle B, X_{1,2}{}^tX_{1,2}\rangle = 2$. En ajoutant les matrices A et B, on trouve la matrice de Gram du réseau $\mathbb{D}_{n,n-1}$ correspondant à la base $f_1 = \varepsilon_1 + \varepsilon_2$, $f_2 = \varepsilon_1 - \varepsilon_2$, $f_3 = \varepsilon_1 - \varepsilon_3$, ...,

$f_{n-1} = \varepsilon_1 - \varepsilon_{n-1}$, $f_n = -\frac{1}{2}\sum_1^{n-1} \varepsilon_i + \frac{n+1}{2}\varepsilon_1 + \frac{1}{2}(\varepsilon_2 \pm \varepsilon_n)$ ('+' si $n \equiv 1 \pmod 4$ et '−' si $n \equiv 3 \pmod 4$).

Comme $\mathbb{D}_{n,n-1}$ est un réseau parfait, c'est le réseau contigu à $\mathbb{A}_n^2$ le long de la face B pour $n \geq 9$ et n impair.

Lorsque n est pair, le réseau $\mathbb{A}_n^2$ est demi-entier (ce n'est pas un réseau de Coxeter). On le rend entier. On a $S(\mathbb{A}_n^2) = S(\mathbb{A}_n)$ si $n \geq 10$ et son groupe d'automorphismes est transitif sur la sphère de ses vecteurs minimaux. On note A la matrice de Gram de $\mathbb{A}_n^2$ multipliée par deux. Comme précédemment, en ajoutant les matrices A et B on trouve la matrice de Gram
du réseau $\mathbb{D}_{n,n-2}$ correspondant à la base $f_1 = \varepsilon_1 + \varepsilon_2$, $f_2 = \varepsilon_1 - \varepsilon_2$, $f_3 = \varepsilon_1 - \varepsilon_3$, ...,
$f_{n-1} = \varepsilon_1 - \varepsilon_{n-1}$, $f_n = -\frac{1}{2}\sum_1^{n-2} \varepsilon_i + \frac{n+1}{2}\varepsilon_1 + \frac{1}{2}(\varepsilon_2 + \varepsilon_{n-1} \pm \varepsilon_n)$ ('+' si $n \equiv 0 \pmod 4$ et '−' si $n \equiv 2 \pmod 4$).

Pour $n \geq 10$ et n pair, le réseau $\mathbb{D}_{n,n-2}$ est le réseau contigu à $\mathbb{A}_n^2$ le long de la face B car il est parfait. ■

2.3.3 Cas où n est impair, n ≥ 9 et r = $\frac{n+1}{2}$.

Pour $n \equiv 1 \pmod 4$ (resp. $n \equiv 3 \pmod 4$) le multiplicateur rendant entier $\mathbb{A}_n^{\frac{n+1}{2}}$ est $\frac{n+1}{2}$ (resp. $\frac{n+1}{4}$) et le réseau $\tilde{\mathbb{A}}_n^{\frac{n+1}{2}}$ ainsi obtenu a pour norme minimale $n-1$ (resp. $\frac{n-1}{2}$).

Pour $n = 5$ et $n = 7$, on sait déjà que les voisins de $\mathbb{A}_5^3$ et de $\mathbb{A}_7^4$ sont respectivement $\mathbb{D}_5$ et $\mathbb{E}_7$. On suppose donc que l'on a $n \geq 9$.

On a $s(\mathbb{A}_n^{\frac{n+1}{2}}) = \frac{n(n+1)}{2} = N$. Les vecteurs minimaux de $\mathbb{A}_n^{\frac{n+1}{2}}$ sont les $\pm e_{i,j}$ avec $e_{i,j} = \frac{n-1}{n+1}(\varepsilon_i + \varepsilon_j) - \frac{2}{n+1}\sum_{k \neq i,j} \varepsilon_k$ pour $0 \leq i < j \leq n$. Comme précédemment, on cherche le voisin de $\mathbb{A}_n^{\frac{n+1}{2}}$ pour un seul vecteur minimal, le vecteur $-e_{1,n}$.
Cependant, on n'utilise pas la base donnée dans la définition des $\mathbb{A}_n^r$ mais une autre formée de $e_{0,1}$ et de ses images par le cycle $\sigma = (0,\ 1,\ 2,\ \ldots,\ n-2,\ n-1)$. Elle sera notée (f_k). On note A la matrice de Gram correspondante du réseau $\tilde{\mathbb{A}}_n^{\frac{n+1}{2}}$.

Dans cette base $e_{1,n} = -\sum_1^{\frac{n-1}{2}} f_{2k+1}$. ($-e_{1,n}$ est le premier vecteur trouvé par la fonction **minim** du système PARI). On pose $v = -e_{1,n}$ et on cherche B un vecteur de face opposé à v.

On peut prendre comme matrice $B = (b_{i,j})$ avec $b_{i,i} = 0$, $b_{1,2} = 1$, $b_{1,i} = -\frac{n-5}{2}$ pour $3 \leq i \leq n-1$, $b_{1,n} = b_{2,3} = -\frac{n-3}{2}$, $b_{2,i} = -\frac{n-5}{2}$ pour $4 \leq i \leq n$, $b_{i,i+1} = 1$ pour $3 \leq i \leq n-1$ et $b_{i,j} = 2$ sinon.

En effet : si u est un vecteur de la base, comme B a ses coefficients diagonaux nuls, on a bien $\langle B, u^t u\rangle = 0$. Puisque v a des composantes nulles suivant f_1 et f_2, pour calculer $\langle B, v^t v\rangle$, on ne s'intéresse qu'aux coefficients $b_{i,j}$ pour $i, j \geq 3$ et on peut voir que l'on a $\langle B, v^t v\rangle = \frac{(n-3)(n-1)}{2} > 0$.

On donne ci-dessous les décompositions des vecteurs minimaux dans la base (f_k).

Pour i pair, j pair et $0 \leq i < j$ on a : $e_{i,j} = \sum_{1}^{i}(-1)^k f_k + \sum_{j+1}^{n}(-1)^{k+1} f_k$.

Pour i impair, j pair, $i < j$ et $i < n$, on a : $e_{i,j} = \sum_{i+1}^{j}(-1)^k f_k$.

Pour i impair, j impair et $i < j < n$, on a : $e_{i,j} = \sum_{1}^{i}(-1)^{k+1} f_k + \sum_{j+1}^{n}(-1)^k f_k$.

Pour i pair, j impair et $i < j < n$, on a : $e_{i,j} = \sum_{i+1}^{j}(-1)^{k+1} f_k$.

Si i est impair et $i < n$, on a : $e_{i,n} = -(\sum_{1}^{\frac{i-1}{2}} f_{2k} + \sum_{\frac{i+1}{2}}^{\frac{n-1}{2}} f_{2k+1})$.

Si i est pair et $i \geq 0$, on a : $e_{i,n} = -(\sum_{0}^{\frac{i-2}{2}} f_{2k+1} + \sum_{\frac{i+2}{2}}^{\frac{n-1}{2}} f_{2k})$.

On peut ainsi calculer les $e_{i,j}{}^t e_{i,j}$, vérifier que l'on a bien $\langle B, e_{i,j}{}^t e_{i,j}\rangle = 0$ si $(i,j) \neq (1,n)$ et donc B est un vecteur de face.

Il faut maintenant calculer le rationnel $\rho > 0$ tel que la matrice $A + \rho B$ soit parfaite et ait même minimum que A. On note k le numéro du réseau $\mathbb{A}_n^{\frac{n+1}{2}}$ compté à partir de $\mathbb{A}_9^5$ (i.e. $\mathbb{A}_9^5$ correspond à $k = 1$, $\mathbb{A}_{11}^6$ à $k = 2$ etc.). On peut remarquer que $k = r - 4 = \frac{n-7}{2}$.

Proposition 1.

i) Pour $n \equiv 1 \ (mod\ 4)$, on a $\frac{1}{\rho} = \frac{n+1}{2}(k-1) + 5 = \frac{n^2-8n+11}{4}$.

ii) Pour $n \equiv 3 \ (mod\ 4)$, on a $\frac{1}{\rho} = nk - (k-2) = \frac{n^2-8n+11}{2}$.

Remarque : Le trinôme $n^2 - 8n + 11$ est bien strictement positif pour $n \geq 9$. Pour $n \equiv 1 \pmod 4$ ou $n \equiv 3 \pmod 4$, le trinôme $n^2 - 8n + 11$ est divisible par 4. Par conséquent, le rationnel ρ est de la forme $\frac{1}{m}$ avec $m \in \mathbb{N} \setminus \{0\}$.

Preuve de la proposition 1.

On traite le cas $n \equiv 1 \pmod 4$ (l'autre cas étant analogue). On note $C = (c_{i,j})$ la matrice $A + \frac{4}{n^2-8n+11} B$.

Elle a pour coefficients :

$c_{i,i} = n-1$, $\quad c_{1,2} = \frac{(n-1)(n-5)^2}{2(n^2-8n+11)}$, $\quad c_{i,i+1} = \frac{(n-1)(n-5)^2}{2(n^2-8n+11)}$ $\quad$ pour $3 \leq i \leq n-1$,

$c_{1,n} = c_{2,3} = \frac{(n-1)(n-3)(n-7)}{2(n^2-8n+11)}$, $\quad c_{1,i} = \frac{-2(n-1)(n-6)}{n^2-8n+11}$ $\quad$ pour $3 \leq i \leq n-1$,

$c_{2,i} = \frac{-2(n-1)(n-6)}{n^2-8n+11}$ $\quad$ pour $4 \leq i \leq n$ $\quad$ et $\quad c_{i,j} = \frac{-2(n-1)(n-7)}{n^2-8n+11}$ $\quad$ sinon

(si $n \equiv 3 \pmod 4$, les coefficients de C sont les moitiés des précédents).

On montre d'abord que C est une matrice de Gram d'un réseau. Pour cela, on fait un changement de base sur le réseau $\tilde{\mathbb{A}}_n^{\frac{n+1}{2}}$. On remplace la base (f_i) par la base (f'_i) où : $f'_n = f_n$ et pour $1 \leq i \leq n-1$, $f'_i = f_i - f_{i+1}$. On obtient comme nouvelle matrice de Gram de $\tilde{\mathbb{A}}_n^{\frac{n+1}{2}}$ la matrice ${}^tPAP = A'$ où P est la matrice de passage de la base (f_i) à (f'_i). (Les coefficients de $P = (p_{i,j})$ sont : $p_{i,i} = 1$ et pour $1 \leq j \leq n-1$ $p_{j+1,j} = -1$, tous les autres étant nuls.) On doit aussi changer B, le vecteur de face, en ${}^tPBP = B'$. Tout ceci sert à remplacer la matrice C par la matrice ${}^tPCP$ que l'on notera $C' = (c'_{i,j})$ et dont les coefficients sont :

$c'_{1,1} = c'_{j,j} = \frac{(n-1)(n^2-6n-3)}{n^2-8n+11}$ $\quad$ pour $3 \leq j \leq n-1$, $\quad c'_{1,n} = \frac{(n-1)(n^2-6n-3)}{2(n^2-8n+11)}$,

$c'_{2,2} = \frac{(n-1)(n^2-6n+1)}{n^2-8n+11}$, $\quad c'_{n,n} = n-1$, $\quad c'_{2,n} = -\frac{2(n-1)}{n^2-8n+11}$,

$c'_{j,j+2} = c'_{1,n-1} = c'_{n-1,n} = -\frac{(n-1)(n^2-6n-3)}{2(n^2-8n+11)}$ $\quad$ pour $1 \leq j \leq n-2$

et $\quad c'_{i,j} = 0$ $\quad$ sinon.

On note $\tilde{C}$ la matrice $\frac{n^2-8n+11}{n-1}\, C'$ et on cherche la décomposition en carrés de Gauss de la forme quadratique associée à $\tilde{C}$ qui sera encore appelée $\tilde{C}$ par abus de langage. On notera les coefficients de décomposition, d_i (i.e. $\tilde{C}(x_1, x_2, \ldots, x_n) = d_1\phi_1(x_1, x_2, \ldots, x_n)^2 + d_2\phi_2(x_2, x_3, \ldots, x_n)^2 + \cdots + d_n\phi_n(x_n)^2$ où les ϕ_i sont des formes linéaires linéairement indépendantes).

Il s'agit de montrer qu'ils sont tous strictement positifs.

Les nouveaux coefficients de la matrice $\tilde{C}$ sont les suivants :

$\tilde{c}_{1,1} = \tilde{c}_{j,j} = n^2 - 6n - 3$ $\quad$ pour $\quad 3 \leq j \leq n-1$, $\quad \tilde{c}_{1,n} = \frac{n^2-6n-3}{2}$, $\quad \tilde{c}_{2,n} = -2$,

$\tilde{c}_{n,n} = n^2 - 8n + 11$, $\quad \tilde{c}_{2,2} = n^2 - 6n + 1$,

$\tilde{c}_{j,j+2} = \tilde{c}_{1,n-1} = \tilde{c}_{n-1,n} = -\frac{n^2-6n-3}{2}$ $\quad$ pour $1 \leq j \leq n-2$ $\quad$ et $\quad \tilde{c}_{i,j} = 0$ $\quad$ sinon.

On a $d_1 = n^2 - 6n - 3 > 0$, $d_2 = n^2 - 6n + 1 > 0$ et $d_k = (n^2 - 6n - 3)(1 - \frac{n^2-6n-3}{4d_{k-2}})$ pour $3 \leq k \leq n-2$. On peut voir que si k est impair alors $d_k = \frac{1}{2}\frac{k+3}{k+1}d_1$ pour $3 \leq k \leq n-2$, et que si k est pair, $d_k = \frac{d_1}{2}\left(\frac{(k+2)d_1+8k}{kd_1+8(k-2)}\right)$ pour $2 \leq k \leq n-3$, donc d_k est strictement positif

pour tout $1 \leq k \leq n-2$.

Il reste à calculer d_{n-1} et d_n.

$$\text{On a } d_{n-1} = d_1 - \tfrac{d_1}{2^2} - \tfrac{d_3}{3^2} - \tfrac{d_5}{4^2} - \tfrac{d_7}{5^2} - \cdots - \tfrac{d_{2j+1}}{(j+2)^2} - \cdots - \tfrac{4d_{n-4}}{(n-1)^2} - \tfrac{d_1^2}{4d_{n-3}} - \tfrac{(n+1)d_1}{2(n-1)}\tfrac{4}{(n+1)^2},$$

$$= d_1 - \sum_{0}^{\frac{n-5}{2}} \tfrac{d_{2j+1}}{(j+2)^2} - \tfrac{d_1^2}{4d_{n-3}} - \tfrac{2d_1}{n^2-1},$$

$$= d_1(1 - \tfrac{1}{2}\tfrac{n-3}{n-1}) - \tfrac{d_1}{2}\left(\tfrac{(n-3)d_1+8(n-5)}{(n-1)d_1+8(n-3)}\right) - \tfrac{2d_1}{n^2-1},$$

$$= \tfrac{d_1}{2}\left(\tfrac{n+3}{n+1} - \tfrac{(n-3)d_1+8(n-5)}{(n-1)d_1+8(n-3)}\right).$$

On a $\frac{(n-3)d_1+8(n-5)}{(n-1)d_1+8(n-3)} < 1 < \frac{n+3}{n+1}$ donc d_{n-1} est strictement positif.

Passons maintenant au coefficient d_n.

$$d_n = n^2 - 8n + 11 - \tfrac{d_1}{2^2} - \tfrac{d_3}{3^2} - \tfrac{d_5}{4^2} - \tfrac{d_7}{5^2} - \cdots - \tfrac{d_{2j+1}}{(j+2)^2} - \cdots - \tfrac{4d_{n-4}}{(n-1)^2} - d_{n-2}\left(\tfrac{3-n}{n+1}\right)^2 - \tfrac{4d_1^2}{d_{n-1}}\left(\tfrac{1}{n+1} + \tfrac{2}{8(n-3)+(n-1)d_1}\right)^2 - \left(\tfrac{4}{d_2} + \tfrac{d_1^2}{d_2^2 d_4} + \tfrac{d_1^4}{4d_2^2 d_4^2 d_6} + \cdots + \tfrac{d_1^{n-5}}{2^{n-7}\prod_{1}^{\frac{n-3}{2}} d_{2j}^2}\right),$$

$$d_n = n^2 - 8n + 11 - \tfrac{d_1}{2}\tfrac{n-3}{n-1} - \tfrac{d_1}{2}\tfrac{(3-n)^2}{n^2-1} - \tfrac{4d_1^2}{d_{n-1}}\left(\tfrac{1}{n+1} + \tfrac{2}{8(n-3)+(n-1)d_1}\right)^2 - \sum_{k=1}^{\frac{n-3}{2}} \frac{d_1^{2(k-1)}}{d_{2k}2^{2(k-2)}\prod_{j=1}^{k-1} d_{2j}^2},$$

$$= n^2 - 8n + 11 - d_1\tfrac{n-3}{n+1} - \tfrac{4d_1^2}{d_{n-1}}\left(\tfrac{1}{n+1} + \tfrac{2}{8(n-3)+(n-1)d_1}\right)^2 - \sum_{k=1}^{\frac{n-3}{2}} \frac{d_1^{2(k-1)}}{d_{2k}2^{2(k-2)}\prod_{j=1}^{k-1} d_{2j}^2}.$$

On peut remarquer que pour $1 \leq k \leq \frac{n-3}{2}$ on a l'égalité :

$\frac{d_1^{2(k-1)}}{d_{2k}2^{2(k-2)}\prod_{j=1}^{k-1} d_{2j}^2} = \frac{8d_1}{((k+1)d_1+8k)(kd_1+8(k-1))}$ et donc la somme

$\sum_{k=1}^{\frac{n-3}{2}} \frac{d_1^{2(k-1)}}{d_{2k}2^{2(k-2)}\prod_{j=1}^{k-1} d_{2j}^2}$ vaut $1 - \frac{(n-1)d_1}{(n-1)d_1+8(n-3)}$.

On trouve ainsi une formule plus simple pour d_n qui est :

$$d_n = n^2 - 8n + 10 - d_1\tfrac{n-3}{n+1} - \tfrac{4d_1^2}{d_{n-1}}\left(\tfrac{1}{n+1} + \tfrac{2}{8(n-3)+(n-1)d_1}\right)^2 + \tfrac{(n-1)d_1}{(n-1)d_1+8(n-3)}.$$

Après calculs, on trouve $d_n = \frac{2n^3-26n^2+102n-110}{n^3-6n^2+5n-8}$.

Le dénominateur et le numérateur étant strictement positifs pour $n \geq 9$, d_n est strictement positif.

On donne ci-dessous la forme générale de $\tilde{C}$.

$$\tilde{C}(x_1,x_2,\ldots,x_n) = d_1(x_1 - \tfrac{1}{2}x_3 - \tfrac{1}{2}x_{n-1} + \tfrac{1}{2}x_n)^2 + d_2(x_2 - \tfrac{d_1}{2d_2}x_4 - \tfrac{2}{d_2}x_n)^2 +$$
$$\tfrac{3}{4}d_1(x_3 - \tfrac{2}{3}x_5 - \tfrac{1}{3}x_{n-1} + \tfrac{1}{3}x_n)^2 + d_4(x_4 - \tfrac{d_1}{2d_4}x_6 - \tfrac{d_1}{d_2d_4}x_n)^2 +$$
$$\tfrac{2}{3}d_1(x_5 - \tfrac{3}{4}x_7 - \tfrac{1}{4}x_{n-1} + \tfrac{1}{4}x_n)^2 + d_6(x_6 - \tfrac{d_1}{2d_6}x_8 - \tfrac{d_1^2}{2d_2d_4d_6}x_n)^2 +$$
$$\tfrac{5}{8}d_1(x_7 - \tfrac{4}{5}x_9 - \tfrac{1}{5}x_{n-1} + \tfrac{1}{5}x_n)^2 + d_8(x_8 - \tfrac{d_1}{2d_8}x_{10} - \tfrac{d_1^3}{2^2d_2d_4d_6d_8}x_n)^2 + \ldots\ldots\ldots +$$

$$d_{n-3}(x_{n-3} - \tfrac{d_1}{2d_{n-3}}x_{n-1} - \frac{d_1^{\frac{n-5}{2}}}{2^{\frac{n-7}{2}}\prod_1^{\frac{n-3}{2}} d_{2j}}x_n)^2 + \tfrac{n+1}{2(n-1)}d_1(x_{n-2} - \tfrac{2}{n+1}x_{n-1} + \tfrac{3-n}{n+1}x_n)^2 +$$

$$d_{n-1}\left(x_{n-1} - (\tfrac{2d_1}{d_{n-1}(n+1)} + \tfrac{d_1}{d_{n-1}}\tfrac{4}{(n-1)d_1+8(n-3)})x_n\right)^2 + d_nx_n^2.$$

Comme chaque coefficient d_i est strictement positif, la forme $\tilde{C}$ est définie positive.

On donne comme exemples les décompositions en carrés de Gauss pour $n = 9$ et $n = 13$:

$$\tilde{C}_9^5(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8,x_9) = 24(x_1 - \tfrac{1}{2}x_3 - \tfrac{1}{2}x_8 + \tfrac{1}{2}x_9)^2 +$$
$$28(x_2 - \tfrac{3}{7}x_4 - \tfrac{1}{14}x_9)^2 + 18(x_3 - \tfrac{2}{3}x_5 - \tfrac{1}{3}x_8 + \tfrac{1}{3}x_9)^2 + \tfrac{132}{7}(x_4 - \tfrac{7}{11}x_6 - \tfrac{1}{22}x_9)^2 +$$
$$16(x_5 - \tfrac{3}{4}x_7 - \tfrac{1}{4}x_8 + \tfrac{1}{4}x_9)^2 + \tfrac{180}{11}(x_6 - \tfrac{11}{15}x_8 - \tfrac{1}{30}x_9)^2 + 15(x_7 - \tfrac{1}{5}x_8 - \tfrac{3}{5}x_9)^2 +$$
$$\tfrac{28}{5}(x_8 - \tfrac{13}{14}x_9)^2 + \tfrac{4}{7}x_9^2.$$

$$\tilde{C}_{13}^7(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8,x_9,x_{10},x_{11},x_{12},x_{13}) = 88(x_1 - \tfrac{1}{2}x_3 - \tfrac{1}{2}x_{12} + \tfrac{1}{2}x_{13})^2 +$$
$$92(x_2 - \tfrac{11}{23}x_4 - \tfrac{1}{46}x_{13})^2 + 66(x_3 - \tfrac{2}{3}x_5 - \tfrac{1}{3}x_{12} + \tfrac{1}{3}x_{13})^2 +$$
$$\tfrac{1540}{23}(x_4 - \tfrac{23}{35}x_6 - \tfrac{1}{70}x_{13})^2 + \tfrac{176}{3}(x_5 - \tfrac{3}{4}x_7 - \tfrac{1}{4}x_{12} + \tfrac{1}{4}x_{13})^2 +$$
$$\tfrac{2068}{35}(x_6 - \tfrac{35}{47}x_8 - \tfrac{1}{94}x_{13})^2 + 55(x_7 - \tfrac{4}{5}x_9 - \tfrac{1}{5}x_{12} + \tfrac{1}{5}x_{13})^2 +$$
$$\tfrac{2596}{47}(x_8 - \tfrac{47}{59}x_{10} - \tfrac{1}{118}x_{13})^2 + \tfrac{264}{5}(x_9 - \tfrac{5}{6}x_{11} - \tfrac{1}{6}x_{12} + \tfrac{1}{6}x_{13})^2 +$$
$$\tfrac{3124}{59}(x_{10} - \tfrac{59}{71}x_{12} - \tfrac{1}{142}x_{13})^2 + \tfrac{154}{3}(x_{11} - \tfrac{1}{7}x_{12} - \tfrac{5}{7}x_{13})^2 + \tfrac{6820}{497}(x_{12} - \tfrac{291}{310}x_{13})^2 +$$
$$\tfrac{152}{155}x_{13}^2.$$

On cherche maintenant la norme minimale de C. On peut voir qu'elle est inférieure ou égale à $n-1$ (car si u est un vecteur minimal de A, orthogonal à B, alors on a la relation ${}^tuAu + \rho^tuBu = {}^tuCu = n-1$). Il faut montrer que c'est exactement $n-1$.
Les suites $(d_{2j})_{1\leq j\leq \frac{n-3}{2}}$ et $(d_{2j+1})_{1\leq j\leq \frac{n-3}{2}}$ sont décroissantes, $d_{2j} > d_{2j+1}$ et d_{n-1} est le plus petit des d_k pour $1 \leq k \leq n-1$.

On compare d_{n-1} et d_n. Par le calcul, on trouve

$$d_{n-1} - d_n = \frac{2n^8 - 38n^7 + 268n^6 - 898n^5 + 1724n^4 - 2442n^3 + 1276n^2 + 754n - 2694}{x^7 - 12n^6 + 45n^5 - 72n^4 + 107n^3 + 44n^2 - 25n + 168}.$$

Là aussi, le numérateur et le dénominateur sont strictement positifs et donc $d_{n-1} > d_n$.

On cherche un vecteur minimal de $\tilde{C}$, $v = (x_1,\ x_2,\ \ldots,\ x_{n-1},\ x_n)$. On va minimiser chaque $d_i\phi_i^2$ en "remontant" (i.e. $i = n,\ n-1,\ n-2,\ \ldots,\ 2,\ 1$).
Comme d_n est le plus petit des d_i, on peut prendre $x_n = \pm 1$; on choisit $x_n = 1$.
Ensuite on minimise $d_{n-1}\phi_{n-1}(x_{n-1},\ x_n)^2$. On a

$d_{n-1}\phi_{n-1}(x_{n-1},\ x_n)^2 = \frac{d_{n-1}}{b_{n-1}^2}(b_{n-1}x_{n-1} - a_{n-1}x_n)^2$ avec $a_{n-1} = n^3 - 7n^2 + 13n - 19 > 0$, $b_{n-1} = n^3 - 6n^2 + 5n - 8 > 0$ et $a_{n-1} < b_{n-1}$. La plus petite valeur de x_{n-1} que l'on doit prendre est $x_{n-1} = x_n = 1$.
On a $d_{n-2}\phi_{n-2}(x_{n-2}, x_{n-1}, x_n)^2 = \frac{d_{n-2}}{(n+1)^2}((n+1)x_{n-2} - (n-1)x_n)^2$. Là aussi on doit avoir $x_{n-2} = x_n = 1$.
Pour $0 \leq k \leq \frac{n-5}{2}$, on a $d_{2k+1}\phi_{2k+1}(x_{2k+1}, x_{2k+3}, x_{n-1}, x_n)^2 = \frac{d_{2k+1}}{(k+2)^2}((k+2)x_{2k+1} - (k+1)x_{2k+3})^2$ et on minimise $\frac{d_{2k+1}}{(k+2)^2}\phi_{2k+1}(x_{2k+1}, x_{2k+3}, x_{n-1}, x_n)^2$ en prenant $x_{2k+1} = x_{2k+3} = 1$.
On traite maintenant le cas des $d_{2k}\phi_{2k}^2$. On a aussi $d_{n-3}\phi_{n-3}(x_{n-3}, x_{n-1}, x_n)^2 = \frac{d_{n-3}}{b_{n-3}^2}(b_{n-3}x_{n-3} - a_{n-3}x_n)^2$ avec $a_{n-3} = \frac{(n-3)d_1 + 8(n-4)}{2}$, $b_{n-3} = \frac{(n-1)d_1 + 8(n-3)}{2}$ et $a_{n-3} < b_{n-3}$. On doit prendre $x_{n-3} = x_n = 1$.
Pour $1 \leq k \leq \frac{n-5}{2}$, on a $d_{2k}\phi_{2k}(x_{2k}, x_{2k+2}, x_n)^2 = \frac{d_{2k}}{b_{2k}^2}(b_{2k}x_{2k} - a_{2k}x_n)^2$ avec $a_{2k} = kd_1 + 8(k - \frac{1}{2})$, $b_{2k} = (k+1)d_1 + 8k$ et $a_{2k} < b_{2k}$. On minimise en prenant $x_{2k} = x_n = 1$.

On obtient comme vecteur $v = (1,\ 1,\ 1,\ \ldots,\ 1,\ 1)$.

On a ainsi :

$v.\tilde{C} = [\frac{n^2-6n-3}{2}, n^2-6n+1-2-\frac{n^2-6n-3}{2}, 0, 0, \ldots, 0, -\frac{n^2-6n-3}{2}, -\frac{n^2-6n-3}{2} - 2 + n^2 - 8n + 11]$ et donc v a pour norme $\frac{n^2-6n-3}{2} + n^2 - 6n + 1 - 2 - \frac{n^2-6n-3}{2} - \frac{n^2-6n-3}{2} - \frac{n^2-6n-3}{2} - 2 + n^2 - 8n + 11 = n^2 - 8n + 11$. La norme minimale de C est alors $(n^2 - 8n + 11)\frac{n-1}{n^2-8n+11} = n - 1$.

On revient au réseau C de départ.
Soient (g_i) une base du réseau correspondant à C et w le vecteur de C de composantes $(1, 1, 0, 1, 0, 1, \ldots, 1, 0, 1, 0)$ dans cette base.

On calcule $\langle B, w^t w\rangle$. C'est égal à $-\frac{(n^2-8n+11)}{2} < 0$ (lorsque $n \equiv 3 \pmod 4$ on trouve un produit scalaire aussi égal à $-\frac{(n^2-8n+11)}{2} < 0$).

On cherche ensuite la norme du vecteur w. On a $w.C = [\frac{n-1}{2},\ \frac{n-1}{2},\ 0,\ 0,\ \ldots,\ 0]$ et donc w a pour norme $n - 1$ (si $n \equiv 3 \pmod 4$, on a $w.C = [\frac{n-1}{4},\ \frac{n-1}{4},\ 0,\ 0,\ \ldots,\ 0]$, et donc la norme de w est $\frac{n-1}{2} = N(\tilde{\mathbb{A}}_n^{\frac{n+1}{2}})$).

De ce calcul, on déduit que le vecteur w est un vecteur minimal de C et que la face associée à la matrice symétrique B est commune aux deux formes quadratiques A et C.

Ceci montre que la forme associée à la matrice C est parfaite et qu'elle est de même minimum que A. C'est donc la forme contiguë à A. ■

Proposition 2.

Le nombre de couples de vecteurs minimaux de la forme contiguë à $\tilde{\mathbb{A}}_n^{\frac{n+1}{2}}$ *est* $s = \frac{n(n+1)}{2}$.

Preuve (dans le cas $n \equiv 1 \pmod 4$).
Comme C est une forme parfaite, on sait que $s \geq \frac{n(n+1)}{2}$. On montre que c'est exactement $\frac{n(n+1)}{2}$.

On donne les vecteurs minimaux (au signe près) de $\tilde{C}$ dans la base $(h_i)_{1\leq i\leq n}$ correspondant à la matrice de Gram de $\tilde{C}$ (celle dont on a donné la décomposition en carrés de Gauss). Ils sont de l'une des formes suivantes :

$\sum_{k=0}^{\frac{i-1}{2}} h_{2k+1} - \sum_{k=\frac{j-1}{2}}^{\frac{n-1}{2}} h_{2k+1}$ pour i impair, $1 \leq i \leq n-4$, j impair et $i+4 \leq j \leq n$

(ce qui en donne $\frac{(n-3)(n-1)}{8}$) ;

$\sum_{k=i}^{\frac{n-1}{2}} h_{2k+1}$ pour $1 \leq i \leq \frac{n-1}{2}$ (ce qui en donne $\frac{n-1}{2}$) ;

$\sum_{k=1}^{i-1} h_{2k} + \sum_{k=j}^{n} h_k$ pour i impair, $3 \leq i \leq \frac{n+1}{2}$ et $2i-1 \leq j \leq 2i < n$ (ce qui en donne

$\frac{n-3}{2}$) ;

$\sum_{k=i}^{n} h_k$ pour $1 \leq i \leq n-1$ (ce qui en donne $n-1$) ;

$\sum_{k=i}^{\frac{j-2}{2}} h_{2k+1} + \sum_{k=j}^{n} h_k$ pour j pair, $4 \leq j \leq n-1$ et $0 \leq i < \frac{j-4}{2}$ (ce qui en donne

$\frac{(n-1)(n-3)}{8}$) ;

$\sum_{k=i}^{\frac{j-2}{2}} h_{2k} + \sum_{k=j}^{n} h_k$ pour $2 \leq i \leq \frac{n-3}{2}$, j pair et $2i+2 \leq j \leq n-1$ (ce qui en donne

$\frac{(n-5)(n-3)}{8}$) ;

Les vecteurs précédents, au nombre de $\frac{3(n-1)(n+1)}{8}$, sont ceux ayant pour composantes ± 1 et 0.

Les vecteurs suivants sont ceux ayant pour composantes 0, ± 1 et ± 2 :

$\sum_{k=1}^{n} h_k + \sum_{k=i}^{\frac{n-1}{2}} h_{2k}$ pour $2 \leq i \leq \frac{n-1}{2}$ (ce qui en donne $\frac{n-3}{2}$) ;

$\sum_{k=0}^{\frac{i-1}{2}} h_{2k+1} + \sum_{k=i+1}^{n} h_k + \sum_{k=j}^{\frac{n-1}{2}} h_{2k}$ pour $3 \leq i \leq n-2$, i impair, $\frac{3+i}{2} \leq j \leq \frac{n-1}{2}$

(ce qui en donne $\frac{(n-3)(n-5)}{8}$) ;

On a ainsi $\frac{(n-1)(n-3)}{8}$ vecteurs de cette forme.

Les vecteurs suivants sont ceux ayant pour composantes 0, ± 1, ± 2, ..., $\pm \frac{n+1}{2}$:

$h_1 + \sum_{\substack{k=4 \\ k\text{pair}}}^{n+1} \frac{k}{2}(h_{k-1} + h_{k-2})$ (ce qui en donne 1) ;

$\sum_{\substack{k=2 \\ k\text{pair}}}^{n-1} \frac{k}{2}(h_k + h_{k+1})$ (ce qui en donne 1) ;

$\sum_{\substack{2 \leq j < 2k \\ j\text{pair}}} \frac{j}{2}(h_{j-1}+h_j) + k(h_{2k-1}+h_{2k}+h_{2k+1}) + \sum_{\substack{2k < j \leq n-1 \\ j\text{pair}}} \frac{j}{2}(h_j+h_{j+1})$ pour $1 \leq k \leq \frac{n-1}{2}$

(ce qui en donne $\frac{n-1}{2}$) ;

$\sum_{\substack{2 \leq j < 2k \\ j\text{pair}}} \frac{j}{2}(h_j+h_{j+1}) + k(h_{2k}+h_{2k+1}+h_{2k+2}) + \sum_{\substack{2k < j \leq n-3 \\ j\text{pair}}} \frac{j}{2}(h_{j+1}+h_{j+2}) + \frac{n+1}{2}h_n$ pour

$1 \leq k \leq \frac{n-3}{2}$ (ce qui en donne $\frac{n-3}{2}$).

De tels vecteurs sont au nombre de n.

En faisant la somme, $\frac{3(n+1)(n-1)}{8} + \frac{(n-1)(n-3)}{8} + n$, on trouve $s = \frac{n(n+1)}{2}$.

(Un vecteur minimal de $\mathbb{A}_n^{\frac{n+1}{2}}$ qui est orthogonal à B donne un vecteur minimal de C (ce qui donne $\frac{n(n+1)}{2} - 1$ vecteurs minimaux) et le vecteur $(1,1,0,1,0,1,\ldots,1,0,1,0)$ est aussi un vecteur minimal de C.) ■

2.4 DE NOUVEAUX RÉSEAUX PARFAITS EN DIMENSION 8 OBTENUS PAR VOISINAGES.

En 1992, dans sa thèse [Lah], M. Laïhem a trouvé 1 171 réseaux parfaits en dimension 8 ayant une section hyperplane parfaite au-dessus de 30 réseaux parfaits de dimension 7. J-L. Baril [Ba] a complété cette liste en traitant le cas des réseaux de racines $\mathbb{E}_7$, $\mathbb{D}_7$ et $\mathbb{A}_7$. Il a ainsi montré qu'à la liste de M. Laïhem s'ajoutent les quatre réseaux $\mathbb{A}_8$, $\mathbb{A}_8^2$, $\mathbb{D}_8$, $\mathbb{E}_8$. Il existe donc 1 175 réseaux parfaits en dimension 8 ayant une section hyperplane parfaite au-dessus des 33 réseaux parfaits de dimension 7. A ceux-ci s'ajoutent les 53 réseaux parfaits construits par J-L. Baril (ils s'écrivent sous la forme d'une somme directe du réseau de racines $\mathbb{A}_2$ et d'un réseau parfait de dimension 6, renormalisés à la même norme) et celui décrit dans le premier chapitre. On connaissait ainsi 1 229 réseaux parfaits en dimension $n = 8$.

Nous avons cherché les réseaux contigus aux 329 réseaux de M. Laïhem avec $s = 36$. Nous avons obtenu 10 115 formes parfaites dont 789 nouvelles (i.e. non isométriques aux 1 229 formes connues jusque là). Parmi toutes ces formes, on retrouve 10 des 48 voisines de $\mathbb{D}_8$ de D-O. Jaquet-Chiffelle [Ja]. (Toutes les formes contiguës à $\mathbb{D}_8$ font partie des 1 171 formes de M. Laïhem sauf une qui est une des 53 formes de J-L. Baril.) On a aussi retrouvé un voisin d'un réseau de J-L. Baril, deux du réseau $\mathbb{A}_8^2$. Le réseau $\mathbb{E}_8$ admet comme réseaux voisins les 329 réseaux de M. Laïhem possédant 36 couples de vecteurs minimaux. On peut remarquer que pour chaque cas la constante ρ est entière (elle vaut 1 ou 2). On peut aussi noter que $\mathbb{E}_8$ admet un même voisin suivant plusieurs faces ne correspondant pas à la même orbite de vecteurs minimaux. A ce niveau, le nombre de réseaux parfaits connus en dimension $n = 8$ vaut 2 018.

Puis on a considéré parmi les 789 réseaux ceux ayant 36 couples de vecteurs minimaux. Il y en a 733, dont on a cherché les voisins. On en obtient 24 396 dont 3 287 nouveaux (i.e. non isométriques aux 2 018), ce qui amène le nombre de réseaux parfaits connus en dimension 8 à 5 305.

On trouve 80 nouveaux voisins du réseau $\mathbb{A}_8^2$ pour lesquels le rationnel ρ prend les valeurs $1, \frac{1}{2}$ ou $\frac{1}{3}$, 95 voisins des 53 réseaux de J-L. Baril (ρ est égal à 1, $\frac{1}{2}$, $\frac{1}{3}$ ou $\frac{1}{4}$) et 34 du réseau obtenu par sections dans le réseau de Ch. Bachoc. Pour ces derniers, la constante ρ vaut 1 ou $\frac{1}{3}$. Parmi les 789 réseaux, 733 sont des voisins de $\mathbb{E}_8$. La valeur de ρ est en général entière (c'est 1 voire 2 pour 4 réseaux), cependant pour 11 réseaux elle est non entière : c'est $\frac{1}{4}$ ou $\frac{1}{3}$. On obtient par conséquent 1 062 réseaux non isométriques, contigus au réseau de racines $\mathbb{E}_8$ (sans compter $\mathbb{D}_8$ et $\mathbb{A}_8^2$).

Le nombre de couples de vecteurs minimaux des duals des 4 076 nouveaux réseaux est presque toujours 1 (c'est 2 pour 288 réseaux, 3 pour cinq réseaux, 4 pour sept réseaux, 6 pour un seul et 8 pour un autre). Ce n'est pas 1 dans environ 7.4% des cas. Tous ces réseaux ne sont pas dual-extrêmes (même celui ayant exactement 8 couples de vecteurs minimaux dans son dual).

Parmi les 4 076 formes, 177 ne sont pas données dans une base de vecteurs minimaux. Nous leur avons appliqué un algorithme de réduction LLL (cf. chap. 3). Lorsque cette

réduction n'a pas donné de matrice de Gram dans une base de vecteurs minimaux, on a utilisé une autre forme de réduction : les minima successifs (cf. chap. 4). Pour seulement deux formes, aucun des deux algorithmes de réduction n'a fourni de matrice de Gram dans une base de vecteurs minimaux (les vecteurs trouvés réalisant les minima successifs engendrent, dans les deux cas, un réseau d'indice 2 dans le réseau de départ). Pour chacune d'entre elles, un seul des vecteurs de la base n'est pas minimal. Cependant, en le remplaçant par un vecteur minimal convenable on obtient une matrice de Gram dans une base de vecteurs minimaux.

Nous avons vérifié une autre propriété de ces nouvelles formes : l'extrémalité. Environ 16% sont extrêmes.

Nous donnons ci-dessous quelques invariants du réseau trouvé parmi les 4 076 ayant la constante d'Hermite la plus élevée. Les notations sont les suivantes : $\det(\Lambda)$ représente le déterminant du réseau Λ, N' la norme minimale de son dual rendu entier, $\gamma_n'^2(\Lambda)$ le carré de la constante d'Hermite duale, $\gamma_n(\Lambda)$ la constante d'Hermite, $(s,\ s^*)$ le nombre de couples de vecteurs minimaux du réseau et de son dual, $\mathrm{ann}(\Lambda^*/\Lambda)$ l'annulateur et N la norme minimale du réseau.

$\det(\Lambda)$	N'	$\gamma_n'^2(\Lambda)$	$\gamma_n(\Lambda)$	$(s,\ s^*)$	$\mathrm{ann}(\Lambda^*/\Lambda)$	N
21 681	2 574	2.1369...	1.7242...	$(47,1)$	7 227	6

Parmi les 3 287 formes parfaites trouvées précédemment, un peu moins de la moitié, soit 1 491, ont 36 couples de vecteurs minimaux. Dans la liste des 53 formes de J-L. Baril, seulement 11 ont un "kissing number" de 72. Nous avons cherché les formes contiguës de ces 1 502 formes. Nous en obtenons 49 814 dont 2 854 nouvelles, i.e. non isométriques aux 5 305 connues jusque là (29 sont des voisins des réseaux de J-L. Baril). Le nombre de formes parfaites en dimension 8 devient 8 159.

Aucun des 2 854 réseaux n'est dual-extrême car le nombre de paires de vecteurs minimaux des réseaux duals est strictement inférieur à 8 (c'est 2 pour 204 réseaux, 3 pour un seul, 6 pour un autre et 1 pour tous les autres).

Environ 85.9% d'entre eux ne sont pas extrêmes.

Par contre, ils admettent tous une base formée de vecteurs minimaux (obtenue par LLL-réduction ou avec l'algorithme des minima successifs ou bien en remplaçant les vecteurs non minimaux par des vecteurs minimaux convenables).

Les 11 réseaux de J-L. Baril ayant 36 couples de vecteurs minimaux fournissent dix nouveaux voisins du réseau de racines $\mathbb{E}_8$ (la valeur de ρ est 1 dans tous les cas), un même voisin pour $\mathbb{D}_8$ et $\mathbb{A}_8^2$, mais pas suivant le même vecteur de face (la valeur de ρ est respectivement 4 et $\frac{1}{2}$), 11 voisins des 53 réseaux s'écrivant sous la forme d'une somme directe du réseau de racines $\mathbb{A}_2$ et d'un réseau parfait de dimension 6, renormalisés à la même norme (ρ valant 1, 2, $\frac{1}{4}$ ou $\frac{1}{2}$).

Parmi les 3 287 formes, 1 491 sont des contiguës de $\mathbb{E}_8$: ρ peut prendre les valeurs

1, 2, $\frac{1}{2}$, $\frac{1}{3}$, $\frac{2}{3}$, $\frac{4}{3}$, $\frac{1}{4}$, $\frac{1}{5}$, $\frac{2}{5}$, $\frac{3}{5}$, $\frac{1}{6}$, $\frac{1}{7}$, $\frac{2}{7}$ ou $\frac{1}{9}$ (avec les 1 075 précédents, on trouve 2 566 voisins de $\mathbb{E}_8$ non isométriques deux à deux). Le réseau $\mathbb{A}_8^2$ admet 336 réseaux voisins supplémentaires (ρ valant 1, 2 ou $\frac{1}{2}$) et le réseau décrit dans le premier chapitre en admet 56 (ρ valant 1, $\frac{1}{3}$ ou $\frac{2}{3}$). On trouve 193 nouveaux réseaux contigus aux 53 réseaux de J-L. Baril (ρ est égal à 1, $\frac{1}{2}$, $\frac{1}{3}$, $\frac{1}{4}$, $\frac{3}{4}$ ou $\frac{1}{6}$).

Plus de la moitié des 2 825 formes, soit 1 634, ont 36 couples de vecteurs minimaux. Nous avons cherché leurs formes contiguës et en avons obtenu 54 547 dont 1 560 nouvelles.

Le nombre de formes parfaites en dimension 8 devient par conséquent 9 719.

Un seul des 1 560 nouveaux réseaux a 8 paires de vecteurs minimaux dans son dual. Cependant, il n'est pas dual-extrême. Les autres ne le sont pas non plus car les réseaux duals n'ont pas assez de vecteurs minimaux (s^*, le nombre de couples de vecteurs minimaux du réseau dual, vaut 1 pour 1 413 réseaux, 2 pour 135 réseaux, 3 pour quatre réseaux, 4 pour six réseaux, 6 pour deux réseaux). Ils admettent tous une base formée de vecteurs minimaux. Environ 83% d'entre eux ne sont pas extrêmes.

On trouve 1 633 réseaux qui sont des voisins de $\mathbb{E}_8$ (ρ peut prendre les valeurs 1, 2, $\frac{1}{2}$, $\frac{1}{3}$, $\frac{2}{3}$, $\frac{1}{4}$, $\frac{3}{4}$, $\frac{1}{5}$, $\frac{2}{5}$, $\frac{3}{5}$, $\frac{1}{6}$, $\frac{1}{7}$ ou $\frac{1}{8}$), 260 voisins de $\mathbb{A}_8^2$ (ρ vaut 1, 2 ou $\frac{1}{2}$), 236 voisins des 53 réseaux de J-L. Baril (ρ est égal à 1, 2, $\frac{1}{2}$, $\frac{1}{3}$, $\frac{2}{3}$, $\frac{1}{4}$, $\frac{3}{4}$ ou $\frac{1}{6}$) et 76 du réseau décrit dans le premier chapitre (ρ valant 1, $\frac{1}{3}$ ou $\frac{2}{3}$).

Parmi les 1 560 réseaux, 1 102 ont 36 paires de vecteurs minimaux. Nous avons cherché leurs contigus et trouvé 36 377 réseaux dont 702 nouveaux. Le nombre de réseaux parfaits en dimension $n = 8$ est maintenant 10 421.

Les 702 formes trouvées ne sont pas dual-extrêmes car s^* est strictement inférieur à 8 (c'est 7 pour une forme, 3 pour trois formes, 2 pour 76 formes et 1 pour les 626 autres). Environ 78.6% d'entre elles ne sont pas extrêmes. Toutes admettent une base formée de vecteurs minimaux (obtenue ou bien par une réduction LLL ou bien grâce à l'algorithme des minima successifs ou bien lorsque les deux méthodes précédentes n'ont pas donné de matrice de Gram dans une base de vecteurs minimaux, en remplaçant les vecteurs non minimaux par des vecteurs minimaux convenables).

On trouve 1 100 nouveaux voisins du réseau de racines $\mathbb{E}_8$ pour lesquels la constante ρ vaut 1, 2, $\frac{1}{2}$, $\frac{1}{3}$, $\frac{2}{3}$, $\frac{1}{4}$, $\frac{1}{5}$, $\frac{2}{5}$, $\frac{1}{6}$, $\frac{1}{7}$, $\frac{1}{8}$, $\frac{3}{8}$ ou $\frac{1}{10}$. Le réseau $\mathbb{A}_8^2$ possède 72 nouveaux voisins (ρ vaut 1, 2, $\frac{1}{2}$ ou $\frac{1}{6}$), les 53 réseaux de J-L. Baril en possèdent 193 nouveaux (ρ est égal à 1, 2, $\frac{1}{2}$, $\frac{1}{3}$, $\frac{1}{4}$, $\frac{1}{5}$ ou $\frac{1}{6}$) et le réseau obtenu par sections successives dans le réseau de Ch. Bachoc de dimension 32, en admet 41 nouveaux pour lesquels ρ vaut 1, $\frac{1}{3}$ ou $\frac{2}{3}$.

Parmi les 702 réseaux, 546 ont un "kissing number" égal à 72. Nous avons appliqué une nouvelle fois l'algorithme de Voronoï et trouvé 17 654 formes dont 240 nouvelles. Le nombre de réseaux parfaits de rang 8 est par conséquent 10 661.

Aucun des 240 nouveaux réseaux n'est dual-extrême car s^* est inférieur ou égal à 7 (c'est 1 pour 211 réseaux, 2 pour 25 réseaux, 3 pour un autre, 4 pour deux réseaux et 7 pour un dernier). Seulement 49 d'entre eux sont extrêmes. Ils possèdent tous une base formée de vecteurs minimaux.

Le réseau $\mathbb{E}_8$ admet 545 autres réseaux voisins (la constante ρ est toujours entière, c'est 1 en général et 2 pour quelques cas), le réseau $\mathbb{A}_8^2$ en admet 22 nouveaux (ρ vaut 1, 2 ou $\frac{1}{2}$), les 53 réseaux de J-L. Baril en admettent 117 (ρ vaut 1, 2, $\frac{1}{2}$, $\frac{1}{3}$, $\frac{1}{4}$ ou $\frac{1}{6}$) et le réseau construit dans le premier chapitre en admet 19 pour lesquels ρ peut prendre les valeurs 1, $\frac{1}{3}$ ou $\frac{2}{3}$.

Parmi les 240 nouvelles formes, 203 ont 36 couples de vecteurs minimaux. Nous avons cherché leurs formes voisines et en avons trouvé 6 097 dont 73 nouvelles, et en particulier 57 de "kissing number" 72. On obtient ainsi 10 734 réseaux parfaits en dimension $n = 8$.

Aucun des 73 réseaux n'est dual-extrême, les réseaux duals n'ayant pas assez de vecteurs minimaux (s^* vaut 1 pour 58 réseaux, 2 pour 13, 4 pour un réseau et 7 pour un autre). Ils admettent tous une base constituée de vecteurs minimaux et seulement 22 d'entre eux sont extrêmes.

On constate que le réseau de racines $\mathbb{E}_8$ admet 203 autres réseaux voisins pour lesquels ρ prend les valeurs entières 1 ou 2, le réseau $\mathbb{A}_8^2$ en admet 9 (ρ vaut 1, 2 ou $\frac{1}{2}$), les 53 réseaux de J-L. Baril en admettent 59 pour lesquels ρ est égal à 1, $\frac{1}{2}$, $\frac{1}{3}$, $\frac{2}{3}$, $\frac{1}{4}$ ou $\frac{1}{6}$, et le réseau contenu dans BC_{32} en admet 6 (ρ vaut $\frac{1}{3}$ ou $\frac{2}{3}$).

Nous avons utilisé l'algorithme de voisinages avec les 57 réseaux et obtenu 1 535 réseaux dont 18 nouveaux (i.e. non isométriques aux 10 734 déjà connus) et parmi ces derniers, 16 ont 36 paires de vecteurs minimaux. On connaît maintenant 10 752 réseaux parfaits en dimension 8.

Parmi ces 18 réseaux, cinq sont extrêmes. Ils ne sont pas pas dual-extrêmes (s^* vaut 1 pour 14 réseaux, 2 pour trois autres et 3 pour un dernier). A ceux qui n'etaient pas donnés dans une base de vecteurs minimaux, on a appliqué une réduction LLL qui a fournit une matrice de Gram dans une base de vecteurs minimaux.

Les 57 réseaux sont tous des réseaux voisins de $\mathbb{E}_8$, la constante ρ est entière (elle vaut 1 ou 2), seulement quatre sont des réseaux contigus à $\mathbb{A}_8^2$ (ρ a pour valeur 1, 2 ou $\frac{1}{2}$), quatre autres sont des voisins du réseau décrit dans le premier chapitre (ρ est égal à 1 ou $\frac{1}{3}$) et dix sont contigus aux 53 réseaux de J-L. Baril (ρ vaut 1, $\frac{1}{2}$, $\frac{1}{3}$, $\frac{2}{3}$ ou $\frac{1}{4}$).

Nous avons cherché les réseaux contigus aux 16 réseaux et en avons obtenu 426 dont seulement quatre nouveaux (ces derniers ont tous un "kissing number" de 72). Le nombre de réseaux parfaits de rang 8 devient 10 756.

Ces quatre réseaux ne sont ni extrêmes, ni dual-extrêmes (s^*, le nombre de paires de vecteurs minimaux vaut 1 pour un réseau, 2 pour deux autres et 4 pour un dernier) et admettent tous une base formée de vecteurs minimaux.

Les 16 réseaux sont tous voisins de $\mathbb{E}_8$ (ρ valant 1 ou 2), quatre sont des voisins des 53 réseaux de J-L. Baril (ρ est égal à 1 ou $\frac{1}{3}$) et un seul est contigu au réseau trouvé par sections dans le réseau de Ch. Bachoc, pour lequel ρ vaut $\frac{1}{3}$. Néanmoins, aucun n'est contigu au réseau $\mathbb{A}_8^2$.

Par voisinages des quatre réseaux, on obtient 87 formes dont quatre nouvelles, toutes ayant 36 couples de vecteurs minimaux. Le nombre de réseaux parfaits de rang 8 est maintenant 10 760.

Parmi ces quatre nouveaux, un seul est extrême. Ils ne sont pas dual-extrêmes (s^* vaut 1 pour trois d'entre eux et 2 pour l'autre). On peut toujours trouver une base constituée de vecteurs minimaux.

Le réseau de racines $\mathbb{E}_8$ admet pour voisins les quatre réseaux dont on a cherché les réseaux contigus (ρ vaut toujours 1), le réseau $\mathbb{A}_8^2$ en admet un seul, pour lequel $\rho = 1$ et un seul des 53 réseaux de J-L. Baril en admet un autre ($\rho = 1$ aussi). Mais, le réseau décrit dans le premier chapitre n'en admet aucun.

On a appliqué une nouvelle fois l'algorithme de voisinages de Voronoï aux quatre formes et trouvé 100 autres formes dont trois nouvelles. En dimension 8, on connaît 10 763 réseaux parfaits.

Les trois réseaux ne sont ni extrêmes, ni dual-extrêmes (leurs réseaux duals admettent une ou deux paires de vecteurs minimaux) et possèdent tous une base formée de vecteurs minimaux.

Le réseau $\mathbb{E}_8$ admet quatre nouveaux voisins et $\mathbb{A}_8^2$ en admet un seul. Dans tous les cas, ρ prend la valeur 1. Mais ni les 53 réseaux de J-L. Baril ni le réseau construit par sections successives dans le réseau de Ch. Bachoc ne possèdent de nouveaux contigus.

Parmi les trois réseaux trouvés précédemment, deux ont 36 couples de vecteurs minimaux. Nous avons cherché leurs voisins et obtenu 30 réseaux dont un seul non isométrique aux 10 763. Ce dernier a un "kissing number" égal à 72. Le nombre de réseaux parfaits de rang 8 devient maintenant 10 764.

Ce nouveau réseau n'est ni dual-extrême ($s^* = 1$), ni extrême. Il admet une base formée de vecteurs minimaux.

Le réseau de racines $\mathbb{E}_8$ admet un nouveau voisin pour lequel ρ vaut 1. C'est le seul parmi $\mathbb{A}_8^2$, $\mathbb{E}_8$, les 53 réseaux de J-L. Baril et le réseau décrit dans le premier chapitre, qui possède de nouveaux voisins.

Nous avons une dernière fois utilisé l'algorithme de Voronoï avec le dernier réseau trouvé et obtenu 21 réseaux. Mais tous sont déjà connus. Par conséquent, on a épuisé la "source prolifique" des réseaux construits par voisinages des réseaux de M. Laïhem.

Parmi les 29 réseaux obtenus par voisinages des 53 réseaux de J-L. Baril (voir p. 31), 17 ont un "kissing number" de 72. Nous avons cherché leurs réseaux contigus et trouvé 597 réseaux dont seulement cinq non encore connus. Le nombre de réseaux parfaits de rang 8 devient 10 769.

Ces cinq réseaux ne sont ni dual-extrêmes ($s^* = 1$ pour chacun), ni extrêmes. Ils admettent tous une base constituée de vecteurs minimaux.

On trouve 17 réseaux contigus à $\mathbb{E}_8$ (ρ vaut 1 ou 2), deux voisins de $\mathbb{A}_8^2$ (ρ vaut 1 ou $\frac{1}{2}$) et 17 voisins des 53 réseaux de J-L. Baril (ρ vaut 1, $\frac{1}{2}$, $\frac{1}{3}$, $\frac{2}{3}$, $\frac{1}{4}$ ou $\frac{1}{6}$), mais aucun du réseau obtenu par sections successives dans BC_{32}.

Parmi les cinq réseaux trouvés ci-dessus, quatre possèdent 36 paires de vecteurs minimaux. Nous leur avons appliqué l'algorithme de Voronoï et obtenu 129 réseaux dont un seul nouveau. Ce dernier a 36 couples de vecteurs minimaux. Le nombre de réseaux parfaits de rang 8 devient 10 770. Ce nouveau réseau n'est ni dual-extrême car $s^* = 1$, ni extrême.

On trouve quatre nouveaux réseaux contigus au réseau $\mathbb{E}_8$, pour lesquels ρ vaut 1, deux réseaux voisins des 53 réseaux de J-L. Baril pour lesquels ρ vaut $\frac{1}{2}$ ou $\frac{1}{4}$, mais aucun de $\mathbb{A}_8^2$ ni du réseau décrit dans le premier chapitre.

Nous avons utilisé l'algorithme de voisinages une dernière fois avec le nouveau réseau trouvé ci-dessus. Il a fourni 24 formes mais toutes font partie de la liste des 10 770. Ce réseau est un voisin du réseau de racines $\mathbb{E}_8$ (ρ prend la valeur 1). C'est le seul parmi $\mathbb{A}_8^2$, $\mathbb{E}_8$, les 53 réseaux de J-L. Baril et le réseau construit dans le premier chapitre à posséder de nouveaux voisins.

Dans le cas des réseaux de J-L. Baril, après la troisième utilisation de l'algorithme de voisinages, ce dernier ne trouve plus que des réseaux parfaits déjà connus.

Remarque : Aucun des 10 770 réseaux parfaits de rang 8 n'est de norme minimale impaire.

En résumé :

- Nous connaissons maintenant 10 770 réseaux parfaits de dimension 8.
- Tous ces réseaux sont de norme minimale paire.
- Ils admettent tous une base formée de vecteurs minimaux.
- On a dénombré :

  6 149 réseaux contigus au réseau de racines $\mathbb{E}_8$,

  791 réseaux contigus au réseau $\mathbb{A}_8^2$,

  931 réseaux contigus aux 53 réseaux de J-L. Baril,

  243 réseaux contigus au réseau construit dans le premier chapitre.

Les normes minimales possibles de tous ces réseaux sont

$$\{2,\ 4,\ 6,\ 8,\ 10,\ 12,\ 14,\ 16,\ 18,\ 20,\ 22,\ 24,\ 26,\ 30,\ 32\}.$$

Quant aux nombres de paires de vecteurs minimaux, ils prennent toutes les valeurs comprises entre 36 et 58 excepté 53, 55, 56, 57. On a compté 6 145 réseaux ayant 36 paires de vecteurs minimaux. Les réseaux duals de 9 764 parmi les 10 770 possèdent une seule paire de vecteurs minimaux. Il n'y a que 11 réseaux ayant plus de huit paires de vecteurs minimaux dans leurs duals.

Les réseaux dual-extrêmes sont très rares : en effet, il n'y en a que six (les trois réseaux de racines $\mathbb{E}_8$, $\mathbb{A}_8$, $\mathbb{D}_8$, et trois réseaux de M. Laïhem). On a dénombré 1 974 réseaux extrêmes.

Pour 6 898 réseaux, le groupe d'automorphismes est $\{\pm \mathrm{Id}\}$.

BIBLIOGRAPHIE

[Ba] J-L. Baril, *Autour de l'algorithme de Voronoï : construction de réseaux euclidiens*, Thèse, Univ. Bordeaux I (1996).

[Ja] D-O. Jaquet-Chiffelle, *Description des voisines de* $\mathbb{E}_7$, $\mathbb{D}_7$, $\mathbb{D}_8$ *et* $\mathbb{D}_9$, Sém. Th. Nombres de Bordeaux 4 (1992), 273–374.

[Lah] M. Laïhem, *Construction algorithmique de réseaux parfaits*, Thèse, Univ. Bordeaux I (1992).

[M] J. Martinet, *Les réseaux parfaits des espaces euclidiens*, livre en préparation.

[Pari] Ch. Batut, D. Bernardi, H. Cohen and M. Olivier, User's Guide to PARI-GP.

[Vo] G. Voronoï, *Nouvelles applications des paramètres continus à la théorie des formes quadratiques : 1 Sur quelques propriétés des formes quadratiques positives parfaites*, J. reine angew. Math 133 (1908), 97–178.

Chapitre 3

L'algorithme LLL sur des anneaux euclidiens.

Nous décrivons dans ce chapitre une généralisation d'un algorithme de réduction de bases et donnons quelques exemples d'applications. Sur certains réseaux de Ch. Bachoc, cet algorithme fournit des bases réduites que l'algorithme usuel ne trouve pas toujours, et ceci en peu de temps.

3.1 INTRODUCTION.

Trouver un algorithme qui cherche une base formée de vecteurs de petites normes, en un temps relativement court, est un vieux problème (résolu en dimension $n = 2$ par C.F. Gauss et plus récemment en 1986 par B. Vallée en dimension $n = 3$). Un grand pas en avant a été fait en 1982 par A. K. Lenstra, H.W. Lenstra et L. Lovász. Dans [LLL], ils donnent un algorithme, qui sera appelé **algorithme LLL** et qui fournit une base presque orthogonale et formée de "petits" vecteurs.

On peut généraliser l'algorithme LLL à des anneaux euclidiens, comme les cinq anneaux des entiers des corps quadratiques imaginaires, $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(j)$, $\mathbb{Q}(\sqrt{-5})$, $\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-11})$, ainsi qu'aux ordres maximaux des algèbres des quaternions ramifiées en 2 (resp. 3) et l'infini (qui sont euclidiens à droite et à gauche). Ceci permettra, pour un réseau, possédant une structure sur un de ces anneaux (ou ordres), de trouver une base formée de vecteurs de petites normes, tout en conservant la structure. Nous décrivons cette généralisation dans le deuxième paragraphe. Dans la troisième partie, on traitera comme exemples, les anneaux $\mathbb{Z}[i]$, $\mathbb{Z}[j]$ et $\mathfrak{M}$, l'ordre de Hurwitz (unique ordre maximal du corps des quaternions de Hamilton, ramifié en 2 et l'infini) et on finira avec quelques résultats numériques et des applications de la LLL-réduction.

Ce travail a été fait alors que l'auteur bénéficiait du contrat DGA 04/94/SA.AR. Je remercie le CELAR pour son aide.

Je remercie également Ch. BATUT qui m'a mis "le pied à l'étrier" sur ce sujet et qui par sa compétence en programmation du langage C, m'a permis de progresser dans ce domaine.

3.2 L'ALGORITHME LLL SUR UN ANNEAU EUCLIDIEN.

On note A l'anneau euclidien contenu dans un corps $\mathbb{K}$: corps de nombres ou corps de quaternions sur un corps de nombres, pouvant s'identifier à un $\mathbb{R}^m$ et doté d'une involution $\sigma : x \mapsto \bar{x}$. On munit $\mathbb{K}^n$ d'un produit hermitien noté $x.y = \sum_{p=1}^{n} x_p\ \bar{y}_p$. On suppose que l'application $N : x \mapsto \mid x \mid = x\sigma(x)$ envoie $\mathbb{K}$ sur $\mathbb{R}$ (resp. A sur $\mathbb{Z}$). On traite le cas où le corps $\mathbb{K}$ est commutatif.

Remarque : Lorsque le corps $\mathbb{K}$ est gauche, l'analogue du déterminant d'une matrice M est la norme réduite. On note r, le rang du corps $\mathbb{K}$ sur son centre $\mathbb{D}$ et $\mathrm{Nrd}(M)$ la norme réduite de M. Si M est à coefficients dans $\mathbb{D}$, on a $\mathrm{Nrd}(M) = \det(M)^r$. Si elle est triangulaire, sa norme réduite est le produit des normes réduites des éléments diagonaux. Sinon, en multipliant à gauche (ou à droite) par une matrice triangulaire avec des 1 sur la diagonale, on se ramène à une matrice triangulaire.

On a d'abord besoin du procédé d'orthogonalisation de Gram-Schmidt, qui permet de trouver une base orthogonale.

3.2.1 L'orthogonalisation de Gram-Schmidt.

Soient $b_1, b_2, \ldots, b_n$ une base d'un réseau Λ de $\mathbb{K}^n$ (i.e. Λ est l'ensemble des combinaisons A-linéaires de $b_1, b_2, \ldots, b_n$).
On définit par récurrence les vecteurs b_r^* et les scalaires $\mu_{r,s}$ de la façon suivante :

$$b_1^* = b_1 ,$$

$$b_r^* = b_r - \sum_{1 \le p < r} \mu_{r,s} b_s^* \quad \text{pour } 2 \le r \le n ,$$

$$\text{avec } \mu_{r,s} = \frac{b_r.b_s^*}{b_s^*.b_s^*} \quad \text{pour } 1 \le s < r \le n.$$

Les vecteurs b_r^* sont orthogonaux deux à deux et forment une base de $\mathbb{K}^n$, b_r^* est le projeté orthogonal de b_r sur le supplémentaire orthogonal de $\sum_{s=1}^{r-1} \mathbb{K} b_s = \sum_{s=1}^{r-1} \mathbb{K} b_s^*$. De plus, la matrice exprimant les coordonnées des b_r^* en fonction des b_r est triangulaire supérieure et les termes diagonaux sont égaux à 1. Enfin, si on note $\det(\Lambda)$ le déterminant du réseau Λ, alors on a $\det(\Lambda) = \prod_{1 \le s \le n} b_s^*.b_s^*$.

Dans la suite, la notation $\| b_r \|^2$ (resp. B_r) désignera la quantité $b_r.b_r$ (resp. $b_r^*.b_r^*$).

Proposition (Inégalité de Hadamard).
Soit Λ un réseau de base $(b_p)_{1 \le p \le n}$, de déterminant $\det(\Lambda)$.

Alors $\det(\Lambda) \le \prod_{1 \le p \le n} \mid b_p \mid$.

Preuve.

En effet, on a d'après l'orthogonalité des b_r^*, $\| b_r \|^2 = B_r + \sum_{1\leq s<r} | \mu_{r,s} | B_s$ et donc

$$\det(\Lambda) = \prod_{1\leq r\leq n} B_r \leq \prod_{1\leq r\leq n} \| b_r \|^2.$$ ■

3.2.2 Description de l'algorithme LLL sur A.

Une base A-LLL-réduite est "presque orthogonale" et formée de vecteurs de petites normes.

Définition.

Avec les notations de 1), *on dira que la base* $(b_p)_{1\leq p\leq n}$ *est A-LLL-réduite si les deux conditions suivantes sont satisfaites :*

a) $| \mu_{r,s} | \leq C_1 \quad$ *pour* $1 \leq s < r \leq n$,

b) $\| b_r^* + \mu_{r,r-1} b_{r-1}^* \|^2 \geq C_2 \| b_{r-1}^* \|^2 \quad$ *pour* $2 \leq r \leq n$,

où C_1 *et* C_2 *sont des réels tels que* $0 < C_1 < C_2 < 1$.

Remarques : La condition *a)* sera appelée condition de réduction en taille et la condition *b)* condition de Lovász. Cette dernière est équivalente à $B_r \geq (C_2 - | \mu_{r,r-1} |) B_{r-1}$. La constante C_2 dépend de C_1. Elle peut prendre n'importe quelle valeur strictement supérieure à C_1, mais elle doit être strictement inférieure à 1, pour assurer la convergence de l'algorithme. La constante C_1 est égale au $\sup\{\inf\{N(y-x) \mid x \in A\} \mid y \in \mathbb{K}\}$ et dépend du corps $\mathbb{K}$.

Les vecteurs $b_r^* + \mu_{r,r-1} b_{r-1}^*$ et b_{r-1}^* sont les projetés orthogonaux respectifs de b_r et b_{r-1} sur le supplémentaire orthogonal de $\sum_{s=1}^{r-2} \mathbb{K} b_s$.

On a les propriétés suivantes :

Propriétés.

Soit $(b_p)_{1\leq p\leq n}$ *une base A-LLL-réduite d'un réseau* Λ. *Alors*

i) $\det(\Lambda) \leq \prod_{1\leq p\leq n} \| b_p \|^2 \leq (C_2 - C_1)^{\frac{-n(n-1)}{2}} \det(\Lambda)$.

ii) $\| b_p \|^2 \leq (C_2 - C_1)^{1-r} B_r \quad$ *pour* $1 \leq p \leq r \leq n$.

iii) $\| b_1 \|^2 \leq (C_2 - C_1)^{\frac{1-n}{2}} \det(\Lambda)^{\frac{1}{n}}$.

iv) Pour tout $x \in \Lambda, x \neq 0$, *on a* $\| b_1 \|^2 \leq (C_2 - C_1)^{1-n} \| x \|^2$.

v) Plus généralement, pour tout système de vecteurs linéairement indépendants $x_1, x_2, \ldots, x_t$ *de* Λ, *on a* $\| b_r \|^2 \leq (C_2 - C_1)^{1-n} \max(\| x_1 \|^2, \| x_2 \|^2, \ldots, \| x_t \|^2)$ *pour* $1 \leq r \leq t$.

Preuve.
i) $\det(\Lambda) \leq \prod_{1\leq p\leq n} \| b_p \|^2$ (c'est l'inégalité de Hadamard).

D'après la condition de Lovász, on a $\| b_r^* \|^2 \geq (C_2 - C_1) \| b_{r-1}^* \|^2$ et par conséquent

$\| b_s^* \|^2 \leq (C_2 - C_1)^{s-r} \| b_r^* \|^2$ pour tout s tel que $s \leq r$ et donc

$\| b_r \|^2 \leq (\frac{1-C_2}{1-(C_2-C_1)} + \frac{C_1(C_2-C_1)^{1-r}}{1-(C_2-C_1)}) B_r \leq (C_2 - C_1)^{1-r} B_r$.

On en déduit facilement que $\prod_{1\leq p\leq n} \| b_p \|^2 \leq (C_2 - C_1)^{\frac{-n(n-1)}{2}} \det(\Lambda)$.

ii) En utilisant les deux inégalités, $\| b_s \|^2 \leq (\frac{1-C_2}{1-(C_2-C_1)} + \frac{C_1(C_2-C_1)^{1-s}}{1-(C_2-C_1)}) B_s$ et

$\| b_s^* \|^2 \leq (C_2 - C_1)^{s-r} \| b_r^* \|^2$, on majore $\| b_s \|^2$ par $(C_2 - C_1)^{1-r} B_r$.

iii) En prenant $p = 1$ dans *ii)* et en faisant le produit pour $s = 1$ jusqu'à n de ces inégalités, on en déduit $\| b_1 \|^{2n} \leq (C_2 - C_1)^{\frac{-n(n-1)}{2}} \det(\Lambda)^2$.

iv) Il existe un entier r_0, $1 \leq r_0 \leq n$ tel que $x = \sum_{1\leq p\leq r_0} s_p b_p = \sum_{1\leq p\leq r_0} t_p b_p^*$ avec $s_{r_0} \neq 0$,

$s_p \in A$ et $t_p \in \mathbb{K}$. On a alors $s_{r_0} = t_{r_0} \in A$ (par la définition des b_p^*).

On en déduit, $\| x \|^2 \geq | s_{r_0} | B_{r_0} = | t_{r_0} | B_{r_0} \geq B_{r_0}$.

Comme d'après *ii)*, $B_{r_0} \geq \| b_1 \|^2 (C_2 - C_1)^{r_0-1} \geq \| b_1 \|^2 (C_2 - C_1)^{n-1}$, on a *iv)*.

v) On écrit $x_r = \sum_{1\leq p\leq n} t_{p,r} b_p$ avec $t_{p,r} \in A$ pour tout $1 \leq r \leq t$.

Pour un r fixé, on note $p(r)$, le plus grand entier tel que $t_{p,r} \neq 0$. On a $\| x_r \|^2 \geq \| b_{p(r)}^* \|^2$ pour tout $r \leq t$.

On renumérote les x_r pour avoir $p(1) \leq p(2) \leq \cdots \leq p(t)$. On a alors $r \leq p(r)$. Sinon, $x_1, x_2, \ldots, x_r$ appartiennent à $\mathbb{K}b_1 + \mathbb{K}b_2 + \cdots + \mathbb{K}b_{r-1}$, ce qui est contraire à l'hypothèse d'indépendance linéaire.

On en déduit $\| b_r \|^2 \leq (C_2 - C_1)^{1-p(r)} \| b_{p(r)}^* \|^2 \leq (C_2 - C_1)^{1-n} \| x_r \|^2$ pour tout $r \leq t$.
■

Description de l'algorithme LLL.

On procède par récurrence. On suppose que les vecteurs b_1, b_2, ..., b_{r-1} sont A-LLL-réduits. (On commence la récurrence avec $r = 2$.) On doit vérifier $| \mu_{r,s} | \leq C_1$ pour tout $s < r$. On suppose que l'on a $| \mu_{r,p} | \leq C_1$ pour tout s tel que $p < s < r$. On pose $q = \lfloor \mu_{r,p} \rceil$ (i.e. un entier le plus proche au sens de l'application N de $\mu_{r,p}$) . On remplace le vecteur b_r par $b_r - qb_p$ et $\mu_{r,p}$ par $\mu_{r,p} - q$ et ainsi le "nouveau" $\mu_{r,p}$ satisfait $| \mu_{r,p} | \leq C_1$.

Pour $t > p$, les $\mu_{r,t}$ ne sont pas modifiés (car les vecteurs b_t^* et b_p^* sont orthogonaux). On a ainsi $| \mu_{r,p} | \leq C_1$ pour tout $p \leq s < r$.
Ensuite, le vecteur b_r doit aussi satisfaire la condition b). Si oui, on passe au vecteur suivant (i.e. on incrémente r de 1). Sinon, on échange b_r et b_{r-1} et on décrémente r de 1, puisque seuls les vecteurs $b_1, b_2, \ldots, b_{r-2}$ sont A-LLL-réduits.

On peut améliorer cet algorithme de la façon suivante :
Avant de tester la condition b), on a seulement besoin d'avoir $| \mu_{r,r-1} | \leq C_1$. Il est donc inutile de réduire les autres $\mu_{r,p}$ pour $p < r-1$. On pourrait aussi calculer tous les coefficients d_r et $\mu_{r,s}$ au départ et ensuite les changer chaque fois que cela est nécessaire. Mais cela est inutile car ils seront probablement modifiés avant que l'on teste si $r \leq n$. On les calcule donc au fur et à mesure, tout en gardant dans une variable r_{max} le maximum de la valeur de r que l'on a atteint.

On va maintenant donner l'algorithme.
Donnée : une matrice de produits hermitiens ($b_{r,s} = b_r.b_s$) d'ordre n.
Sortie : une matrice de produits hermitiens dont les vecteurs sont A-LLL-réduits.

Étape 1

$r \leftarrow 2$;
$r_{max} \leftarrow 1$;
$B_1 \leftarrow b_{1,1}$;

Étape 2

tant que $r \leqslant n$ faire
{ si $r > r_{max}$
{ $r_{max} \leftarrow r$;
pour $s = 1, 2, \ldots, r-1$
{ $a_{r,s} \leftarrow b_{r,s}$;
pour $t = 1, 2, \ldots, s-1$ $a_{r,s} \leftarrow a_{r,s} - a_{r,t}\, \bar{\mu}_{s,t}$;
$\mu_{r,s} \leftarrow \frac{a_{r,s}}{B_s}$;
}
$B_r \leftarrow b_{r,r}$;
pour $t = 1, 2, \ldots, r-1$ $B_r \leftarrow B_r - a_{r,t}\bar{\mu}_{r,t}$;
}

Étape 3

RED(r, r-1) ;
tant que $B_r < (C_2 - | \mu_{r,r-1} |)\, B_{r-1}$ faire
{ SWAP(r) ;
$r \leftarrow \max(r, 2)$;
RED(r, r-1) ;
}
pour $s = r-2, r-3, \ldots, 1$

{ RED(r, s) ;
$r \leftarrow r + 1$;
}
}
sortir b ■

Sous-Algorithme RED(r, s)

{ $q \leftarrow \lfloor \mu_{r,s} \rceil$;
$b_{r,r} \leftarrow b_{r,r} + q b_{s,s} \bar{q} - q b_{s,r} - b_{r,s} \bar{q}$;
pour $t = 1, 2, \ldots, n$ si $t \neq r$ $\{b_{t,r} \leftarrow b_{t,r} - b_{t,s} \bar{q}$; $b_{r,t} \leftarrow \bar{b}_{t,r}$;}
commentaire : $b_r \leftarrow b_r - q\, b_s$
$\mu_{r,s} \leftarrow \mu_{r,s} - q$;
pour $t = 1, 2, \ldots, s-1$ $\mu_{r,t} \leftarrow \mu_{r,t} - q\, \mu_{s,t}$;
sortir ■
}

Sous-Algorithme SWAP(r)

pour $t = 1, 2, \ldots, n$
si $t \neq r$ et $t \neq r-1$
$\{ v \leftarrow b_{r,t}$; $b_{r,t} \leftarrow b_{r-1,t}$; $b_{r-1,t} \leftarrow v$; $b_{t,r} \leftarrow \bar{b}_{r,t}$; $b_{t,r-1} \leftarrow \bar{b}_{r-1,t}$;}
$v \leftarrow b_{r,r}$; $b_{r,r} \leftarrow b_{r-1,r-1}$; $b_{r-1,r-1} \leftarrow v$;
$v \leftarrow b_{r,r-1}$; $b_{r,r-1} \leftarrow b_{r-1,r}$; $b_{r-1,r} \leftarrow v$;
commentaire : échange des vecteurs b_r et b_{r-1}
pour $s = 1, 2, \ldots, r-2$ $\{ v \leftarrow \mu_{r,s}$; $\mu_{r,s} \leftarrow \mu_{r-1,s}$; $\mu_{r-1,s} \leftarrow v;\}$
commentaire : échange des $\mu_{r,s}$ et $\mu_{r-1,s}$
$\mu \leftarrow \mu_{r,r-1}$;
$B \leftarrow B_r + |\mu|\, B_{r-1}$;
$\mu_{r,r-1} \leftarrow \frac{\bar{\mu}\, B_{r-1}}{B}$;
$B_r \leftarrow \frac{B_{r-1}\, B_r}{B}$;
$B_{r-1} \leftarrow B$;
pour $t = r+1, 2, \ldots, r_{max}$
{ $\nu \leftarrow \mu_{t,r}$;
$\mu_{t,r} \leftarrow \mu_{t,r-1} - \nu\, \mu$;
$\mu_{t,r-1} \leftarrow \nu + \mu_{t,r}\, \mu_{r,r-1}$;
}
sortir ■

Preuve de l'algorithme.

Comme on ne fait que des opérations du type, "échange de deux vecteurs" et "remplacement d'un vecteur par la différence de ce vecteur avec un autre vecteur multiplié par un scalaire", on reste toujours dans le réseau de départ (i.e. on fait des opérations unimodulaires). On peut voir facilement qu'au cours de l'algorithme, juste avant de tester si $r \leq n$, les vecteurs $b_1, b_2, \ldots, b_{r-1}$ sont A-LLL-réduits.
Il nous reste à montrer que l'algorithme se termine effectivement.

Pour cela, on utilise les scalaires d_r définis précédemment et on pose $D = \prod_{1\leq p\leq n-1} d_p$. Le scalaire $D > 0$ est modifié lorsque les d_p le sont, c'est-à-dire lors des échanges des vecteurs b_r et b_{r-1} (dans le sous-algorithme SWAP). Dans ce cas, seul d_{r-1} est modifié. Il est multiplié par un facteur au plus égal à C_2 et par conséquent D aussi.
On note Λ_r le sous-réseau de Λ engendré par les b_p pour $1 \leq p \leq r$ et $N(\Lambda_r)$ sa norme minimale. On a

$$d_r \geq N(\Lambda_r)^r \gamma_r^{-r} \geq N(\Lambda)^r \gamma_r^{-r}$$

où $N(\Lambda)$ est la norme minimale de Λ et γ_r, la constante d'Hermite en dimension r. Cette expression ne dépend que de r et donc d_r est minoré par une constante ne dépendant que de r et du réseau Λ. Par conséquent, D est minoré par une constante ne dépendant que de Λ. Ceci montre que le sous-algorithme SWAP n'est exécuté qu'un nombre fini de fois. ■

Comme nous n'utilisons que des réseaux dont le produit hermitien est à valeurs dans A, nous allons aussi décrire l'algorithme LLL qui ne travaille qu'avec des éléments de A. Pour cela, on a besoin des deux propositions suivantes (cf. [Co]).

Proposition 1.
On considère la matrice $(b_r.b_s)$ *et on pose* $d_p = \det((b_r.b_s)_{1\leq r,s\leq p}) = \prod_{1\leq s\leq p} B_s$ *pour* $1 \leq p \leq n$ *et* $d_0 = 1$. *Alors,*

i) Pour tout p *et* r *tels que* $r < p$, *on a* $d_{p-1}B_p \in \mathbb{Z}$ *et* $\mu_{p,r}d_r \in A$.

ii) Pour tout p, r, t *tels que* $r < t \leq p$, *on a* $d_r \sum_{1\leq s\leq r} \mu_{p,s}\bar{\mu}_{t,s}B_s \in A$.

Preuve.
i) On a l'égalité suivante $d_{r-1}B_r = d_r$, donc $d_r \in \mathbb{Z}$ (et même $\in \mathbb{N}$). Pour la seconde assertion, on considère pour $s < r$ le vecteur $v = b_r - \sum_{1\leq p\leq s} \mu_{r,p}b_p^* = b_r^* - \sum_{s<p<r} \mu_{r,p}b_p^*$.

Pour tout p tel que $1 \leq p \leq s$, on a $v.b_p^* = 0$, ou de manière équivalente $v.b_p = 0$

(puisque $\sum_{1\leq p\leq s} \mathbb{K}b_p^* = \sum_{1\leq p\leq s} \mathbb{K}b_p$). On a alors $v = b_r - \sum_{1\leq p\leq s} x_p b_p$ avec $x_p \in \mathbb{K}$.

Les relations $v.b_p = 0$ peuvent être écrites sous la forme matricielle

$$\begin{pmatrix} b_1.b_1 & \dots & \dots & b_1.b_s \\ \dots & \dots & \dots & \dots \\ & & & \\ & & & \\ \dots & \dots & \dots & \dots \\ b_s.b_1 & \dots & \dots & b_s.b_s \end{pmatrix} \begin{pmatrix} x_1 \\ \dots \\ \\ \\ \dots \\ x_s \end{pmatrix} = \begin{pmatrix} b_1.b_r \\ \dots \\ \\ \\ \dots \\ b_s.b_r \end{pmatrix}.$$

Le déterminant de la matrice est, par définition, d_s et en inversant la matrice, on voit que les x_p sont de la forme $\frac{m_p}{d_s}$ avec $m_p \in A$.

L'égalité $\sum_{1\leq p\leq s} x_p b_p = \sum_{1\leq p\leq s} \mu_{r,p} b_p^*$ montre par projection sur b_s^* que $x_s = \mu_{r,s} = \frac{m_r}{d_s}$.

On en déduit alors l'assertion.

ii) Par *i)*, $d_s\mu_{r,s}$ est un élément de A pour tout $s < r$, donc $d_s v$ est une combinaison A-linéaire des b_p ; par conséquent $d_r v.b_t \in A$ pour tout $1 \leq t \leq n$.

On en déduit alors $d_s \sum_{1\leq p\leq s} \mu_{r,p}\bar{\mu}_{t,p} B_p \in A$. ■

Proposition 2.

Avec les mêmes notations que la proposition précédente, on pose $\lambda_{r,s} = \mu_{r,s} d_s$ *pour* $s < r$ $(\lambda_{r,s} \in A)$ *et* $\lambda_{r,r} = d_r$.

Pour $s \leq r$ *fixés, on définit la suite* u_p *par* $u_0 = b_r.b_s$ *et pour tout* p *tel que* $1 \leq p < s$,

$u_p = \frac{d_p u_{p-1} - \lambda_{r,p}\bar{\lambda}_{s,p}}{d_{p-1}}$.

Alors $u_p \in A$ *et* $u_{s-1} = \lambda_{r,s}$.

Preuve

Par récurrence sur p, on montre que

$$u_p = d_p\,(b_r.b_s - \sum_{1\leq t\leq p} \frac{\lambda_{r,t}\bar{\lambda}_{s,t}}{d_t d_{t-1}}) = d_p\,(b_r.b_s - \sum_{1\leq t\leq p} \mu_{r,t}\bar{\mu}_{s,t} B_t),$$

ce qui montre (grâce à *ii)*) de la proposition 1) que $u_p \in A$.

On a ensuite les égalités :

$$\begin{aligned} u_{s-1} &= d_{s-1}\,(b_r.b_s - \sum_{1\leq p\leq s-1} \mu_{r,p}\bar{\mu}_{s,p} B_p), \\ &= d_{s-1}\,(b_r^* + \sum_{1\leq t<r} \mu_{r,t} b_t^*).(b_s^* + \sum_{1\leq q<s} \mu_{s,q} b_q^*) - d_{s-1} \sum_{1\leq p\leq s-1} \mu_{r,p}\bar{\mu}_{s,p} B_p, \\ &= \mu_{r,s}\; d_{s-1}\; B_s, \\ &= d_s\; \mu_{r,s}, \\ &= \lambda_{r,s}. \end{aligned}$$

■

On obtient ainsi deux nouvelles conditions de A-LLL-réduction qui sont les suivantes :

a') $\quad | \lambda_{r,s} | \leq C_1 d_s^2 \quad$ pour $1 \leq s < r$,

b') $\quad d_r d_{r-2} + | \lambda_{r,r-1} | \geq C_2 d_{r-1}^2 \quad$ pour $2 \leq r \leq n$.

On donne aussi l'algorithme ne travaillant qu'avec des éléments de A.
Donnée : une matrice de produits hermitiens ($b_{r,s} = b_r.b_s$) d'ordre n.
Sortie : une matrice de produits hermitiens dont les vecteurs sont A-LLL-réduits.

Étape 1

$r \leftarrow 2$;
$r_{max} \leftarrow 1$;
$d_0 \leftarrow 1$; $\quad d_1 \leftarrow b_{1,1}$;

Étape 2

tant que $r \leq n$ faire
{ si $r > r_{max}$
{ $r_{max} \leftarrow r$;
pour $p = 1, 2, \ldots, r$
{ $u \leftarrow b_{p,r}$;
pour $s = 1, 2, \ldots, p-1 \quad u \leftarrow \frac{d_s \, u - \lambda_{r,s} \, \bar{\lambda}_{p,s}}{d_{s-1}}$;
si $p < r \quad \lambda_{r,p} \leftarrow u$;
si $p \leftarrow r \quad d_r \leftarrow u$;
}
}

Étape 3

REDI(r, r-1) ;
tant que $\quad d_r \, d_{r-2} + | \lambda_{r,r-1} | < C_2 \, {d_{r-1}}^2$
{ SWAPI(r) ;
$r \leftarrow \max(r, 2)$;
REDI(r, r-1) ;
}
pour $\quad t = r-2, r-3, \ldots, 1$
{ REDI(r, t) ;
$r \leftarrow r + 1$;
}
}
sortir b ■

Sous-Algorithme REDI(r, s)

{ $q \leftarrow \lfloor \frac{\lambda_{r,s}}{d_s} \rceil$;
$b_{r,r} \leftarrow b_{r,r} + q \, b_{s,s} \, \bar{q} - b_{r,s} \, \bar{q} - q \, b_{s,r}$;
pour $\quad p = 1, 2, \ldots, n$
si $\quad p \neq r \quad \{ b_{p,r} \leftarrow b_{p,r} - b_{p,s} \, \bar{q}$; $\quad b_{r,p} \leftarrow \bar{b}_{p,r}$; }

commentaire : $b_r \leftarrow b_r - q\, b_s$
$\lambda_{r,s} \leftarrow \lambda_{r,s} - q\, d_s$;
pour $p = 1, 2, \ldots, s-1$ $\lambda_{r,p} \leftarrow \lambda_{r,p} - q\, \lambda_{s,p}$;
sortir ■
}

Sous-Algorithme SWAPI(r)
{ pour $p = 1, 2, \ldots, n$ si $p \neq r$ et $p \neq r-1$
$\{v \leftarrow b_{r,p}$; $b_{r,p} \leftarrow b_{r-1,p}$; $b_{r-1,p} \leftarrow v$; $b_{p,r} \leftarrow \bar{b}_{r,p}$; $b_{p,r-1} \leftarrow \bar{b}_{r-1,p}$; $\}$
$v \leftarrow b_{r,r}$; $b_{r,r} \leftarrow b_{r-1,r-1}$; $b_{r-1,r-1} \leftarrow v$;
$v \leftarrow b_{r,r-1}$; $b_{r,r-1} \leftarrow b_{r-1,r}$; $b_{r-1,r} \leftarrow v$;
commentaire : échange des vecteurs b_r et b_{r-1}
pour $p = 1, 2, \ldots, r-2$ $\{ v \leftarrow \lambda_{r,p}$; $\lambda_{r,p} \leftarrow \lambda_{r-1,p}$; $\lambda_{r-1,p} \leftarrow v$; $\}$
$\lambda \leftarrow \lambda_{r,r-1}$;
$\lambda_{r,r-1} \leftarrow \bar{\lambda}_{r,r-1}$;
pour $s = r+1, 2, \ldots, r_{max}$
$\{ l_1 \leftarrow \lambda_{s,r}$; $l_2 \leftarrow \lambda_{s,r-1}$;
$\lambda_{s,r} \leftarrow \frac{l_2\, d_r - l_1\, \lambda}{d_{r-1}}$;
$\lambda_{s,r-1} \leftarrow \frac{l_1\, d_{r-2} + \bar{\lambda}\, l_2}{d_{r-1}}$;
$\}$
$d_{r-1} \leftarrow \frac{d_{r-2}\, d_r + |\lambda|}{d_{r-1}}$;
sortir ■
}

Remarque : La preuve de cet algorithme est la même que celle de l'algorithme travaillant avec des éléments de $\mathbb{K}$.

On va maintenant traiter les exemples, $A = \mathbb{Z}[i]$, l'anneau des entiers de Gauss, avec $i^2 = -1$, $A = \mathbb{Z}[j]$, l'anneau des entiers d'Eisenstein, avec $j^2 + j + 1 = 0$ et $A = \mathfrak{M}$, l'ordre de Hurwitz.

3.3 L'ALGORITHME LLL SUR $\mathbb{Z}[i]$, $\mathbb{Z}[j]$, $\mathfrak{M}$.

3.3.1 Sur $\mathbb{Z}[i]$, $\mathbb{Z}[j]$.

Dans cette partie, les réseaux sont définis sur $\mathbb{Z}[i]$ (resp. $\mathbb{Z}[j]$) et on considère le produit hermitien $x.y = \sum_{1\leq p\leq n} x_p\bar{y}_p$ où $\bar{y}_p$ est le conjugué complexe de y_p sur $\mathbb{Z}[i]$ (resp. $\mathbb{Z}[j]$).

Ces anneaux sont euclidiens pour la norme de corps de nombres $N : x \mapsto x\bar{x}$. Lorsque $x = a + ib$ (resp. $a + bj$), $N(x) = a^2 + b^2$ (resp. $a^2 + b^2 - 2ab$).

Les notations sont les mêmes que celles du paragraphe précédent et pour un complexe α, $|\alpha|^2 = \alpha\bar{\alpha}$ représente le carré de son module. Pour tout réel x, la quantité $\lfloor x \rceil$ désigne un entier le plus proche (i.e. $\lfloor x \rceil = \lfloor x + \frac{1}{2} \rfloor$).

Définition.

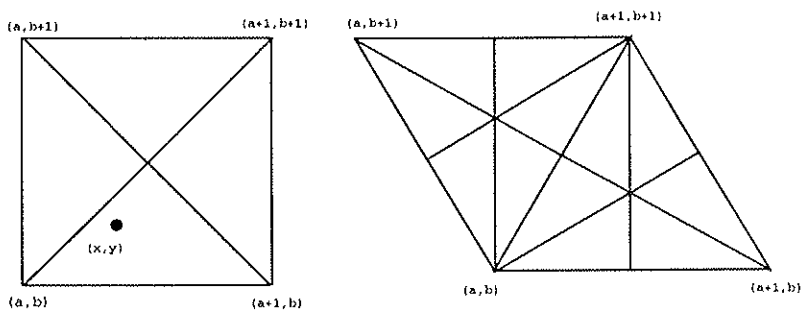
On dira que la base $(b_p)_{1\leq p\leq n}$ *est* $\mathbb{Z}[i]$ *(resp.* $\mathbb{Z}[j]$*)-LLL-réduite lorsque :*

a) $C_1 = \frac{1}{2}$ *(resp.* $\frac{1}{3}$*),*

b) $C_2 = \frac{3}{4}$ *(resp.* $\frac{2}{3}$*).*

Remarques : Tout élément z de $\mathbb{Q}[i]$ (resp. $\mathbb{Q}[j]$) peut se représenter comme un point se trouvant à l'intérieur d'un carré (resp. d'un losange) dont les sommets sont des éléments de $\mathbb{Z}[i]$ (resp. de $\mathbb{Z}[j]$) de côté 1. On rapproche l'élément $z = x + i\,y$ (resp. $z = x + j\,y$) du coin $c = a + i\,b$ (resp. $a + j\,b$) avec $a = \lfloor x \rceil$ et $b = \lfloor y \rceil$. Dans le cas $\mathbb{Z}[i]$, c'est le centre du carré qui fournit la plus grande distance ($\frac{1}{2}$) avec un des sommets.

Dans le cas $\mathbb{Z}[j] = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$, il est bien connu que $C_1 = \frac{1}{3}$ (cf. [L]). Les points les plus éloignés de $\mathbb{Z}[j]$ au sens de la norme de $\mathbb{Q}[j]$, sont les points congrus à $\frac{2+j}{3}$ (mod $\mathbb{Z}[j]$) ou à $\frac{1+2j}{3}$ (mod $\mathbb{Z}[j]$). (Dans le losange ci-dessous, ils correspondent aux deux centres des triangles équilatéraux.)



Remarques : A partir de la matrice des produits hermitiens sur $\mathbb{Z}[i]$ (resp. $\mathbb{Z}[j]$), on peut construire la matrice de Gram sur $\mathbb{Z}$ en utilisant, comme produit scalaire,
$< x, y >= \mathrm{Tr}(x.y)$, avec pour tout $z \in \mathbb{Z}[i]$ (resp. $\mathbb{Z}[j]$), $\mathrm{Tr}(z) = z + \bar{z}$.

Autrement dit, le coefficient $a_{r,s} + b_{r,s}i$ (resp. $a_{r,s} + b_{r,s}j$) d'indices $\{r, s\}$, explose en le bloc 2x2,

$$\begin{pmatrix} 2a_{r,s} & 2b_{r,s} \\ -2b_{r,s} & 2a_{r,s} \end{pmatrix} \text{ (resp. } \begin{pmatrix} 2a_{r,s} - b_{r,s} & 2b_{r,s} - a_{r,s} \\ -a_{r,s} - b_{r,s} & 2a_{r,s} - b_{r,s} \end{pmatrix}).$$

3.3.2 Sur $\mathfrak{M}$.

On peut écrire l'algèbre non commutative des quaternions de Hamilton $\mathbb{H}$ sous la forme, $\mathbb{H} = \mathbb{R}[i, j, k]$ avec $ij = -ji = k$, $i^2 = j^2 = -1$. Soit $y = y_0 + iy_1 + jy_2 + ky_3$, un quaternion de Hamilton, on définit son conjugué $\bar{y}$ par $\bar{y} = y_0 - iy_1 - jy_2 - ky_3$. On pose $\mathrm{Nrd}(y) = y\bar{y} = y_0^2 + y_1^2 + y_2^2 + y_3^2$ et $\mathrm{Nrd}(y)$ est appelée la norme réduite de y. On peut aussi définir la trace réduite de y par $\mathrm{Trd}(y) = y + \bar{y} = 2y_0$. L'ordre de Hurwitz ($\mathfrak{M} = \mathbb{Z}[i, j, \omega]$ avec $\omega = \frac{-1+i+j+k}{2}$) est euclidien (à droite ou à gauche) pour la norme réduite (cf. [H-W]). On le considère comme module à gauche.

Pour tout entier de Hurwitz, $x = x_0 + ix_1 + jx_2 + \omega x_3$, on notera $x = (x_0,\ x_1,\ x_2,\ x_3)$. On utilisera le symbole $\lfloor \alpha \rceil$ pour désigner un entier le plus proche du réel α.

Les réseaux considérés sont entiers sur $\mathfrak{M}$ et on utilise le produit hermitien $x.y = \sum_{1 \le p \le n} x_p \bar{y}_p$ où $\bar{y}_p$ est le conjugué quaternionien de y_p. Toutes les notations, ainsi que les définitions de la suite $(u_p)_{1 \le p \le n}$ sont les mêmes que dans la partie précédente sauf pour $d_r, r \ge 1$ qui n'est plus défini que par $\prod_{1 \le s \le r} B_s$ (car la notion de déterminant n'a pas de sens dans une algèbre non commutative). La preuve de l'algorithme va donc changer dans ce cas, ainsi que la preuve de la proposition 1 (celle de la proposition 2 n'est pas modifiée).

Remarque : A l'aide de la matrice des produits hermitiens, on récupère la matrice de Gram sur $\mathbb{Z}$, en utilisant le produit scalaire, $< x, y >= \mathrm{Trd}(x.y)$. Le coefficient $a + ib + jc + \omega d$ d'indices $\{r, s\}$, explose en le bloc 4x4,

$$\begin{pmatrix} 2a-d & 2b+d & 2b+2c-d & -a+b+c+2d \\ -2b-d & 2a-d & -d & a+b+c \\ -2c-d & d & 2a-d & a-b+c \\ -a-b-c-d & a-b-c-d & a+b-c-d & 2a-d \end{pmatrix}$$

Définition.

On dira que la base $(b_p)_{1 \le p \le n}$ est $\mathfrak{M}$-LLL-réduite lorsque :

a) $C_1 = \frac{1}{2}$,

b) $C_2 = \frac{3}{4}$.

Remarques : Si on considère le quaternion $y = y'_0 + iy'_1 + jy'_2 + ky'_3$, on cherche un élément de Hurwitz $x = x_0 + ix_1 + jx_2 + \omega x_3$, proche pour la norme réduite. On écrit

$y = y_0 + iy_1 + jy_2 + \omega y_3$ et on pose $\hat{x} = (x_0,\ x_1,\ x_2,\ x_3)$ avec $x_3 = \lfloor y_3 \rceil$,

$x_2 = \lfloor y_2 + \frac{y_3 - x_3}{2} \rceil$, $x_1 = \lfloor y_1 + \frac{y_3 - x_3}{2} \rceil$, $x_0 = \lfloor y_0 - \frac{y_3 - x_3}{2} \rceil$.

On a ainsi $\mathrm{Nrd}(y - \hat{x}) = (y_0 - x_0 - \frac{1}{2}(y_3 - x_3))^2 + (y_1 - x_1 + \frac{1}{2}(y_3 - x_3))^2 +$

$(y_2 - x_2 + \frac{1}{2}(y_3 - x_3))^2 + \frac{1}{4}(y_3 - x_3)^2 \leq \frac{13}{16} = 0.8125$.

Mais, on peut trouver un entier de Hurwitz plus proche de y.

Pour cela, on calcule d'abord la différence entre y et $\hat{x}$ (les trois premières coordonnées sont comprises entre $-\frac{3}{4}$ et $\frac{3}{4}$ et la quatrième entre $-\frac{1}{2}$ et $\frac{1}{2}$). Elle sera notée z. On effectue les différences $z - (t_0,\ t_1,\ t_2,\ t_3)$ avec $t_p \in \{-1,\ 0,\ 1\}$, de même signe que z_p, pour $p = 0,\ 1,\ 2,\ 3$. On prend alors un élément de Hurwitz, $x = \hat{x} + (t_0,\ t_1,\ t_2,\ t_3)$ où $(t_0,\ t_1,\ t_2,\ t_3)$ est tel que $\mathrm{Nrd}(z - (t_0,\ t_1,\ t_2,\ t_3))$ est la plus petite. En général, cet élément est unique. Cependant, pour des quaternions y congrus à $\frac{1+i}{2} \pmod{\mathfrak{M}}$, ou $\frac{1+j}{2} \pmod{\mathfrak{M}}$, ou $\frac{i+j}{2} \pmod{\mathfrak{M}}$, ce procédé exhibe 8 entiers de Hurwitz x avec $\mathrm{Nrd}(y - x)$ la plus petite possible. Par exemple, pour $y = \frac{1+i}{2}$, les éléments $x \in \{0,\ 1,\ i,\ 1 + i\ ,\ 1 + \omega,\ i - w,\ 1 - j + \omega,\ i + j - \omega\}$ réalisent le maximum de la norme réduite. D'autres ont 2 entiers de Hurwitz les plus proches.

On peut identifier $\mathfrak{M}$ au réseau de racines $\mathbb{D}_4$ par $\mathfrak{M} = \{(x_0,\ x_1,\ x_2,\ x_3) \in \mathbb{Z}^4 \mid x_0 + x_1 + x_2 + x_3 \equiv 0 \pmod 2\}$. La base de $\mathbb{D}_4$, $((-1,\ 1,\ 0,\ 0)\,;\ (1,\ 1,\ 0,\ 0)\,;\ (0,\ 0,\ 1,\ 1)\,;\ (1,\ 0,\ 0,\ 1))$ correspond à la base de Hurwitz $(1,\ i,\ j,\ \omega)$. Dans le cube $\mathbb{D}_4$, il y a exactement 24 éléments z de $\mathbb{R}^4$ dont la distance $d(z,\ \mathbb{D}_4) = \inf\{N(z - x) = \sum_{p=0}^{3}(z_p - x_p)^2 \mid x \in \mathbb{D}_4\}$ vaut $\frac{1}{2}$. Les 24 éléments de $\mathfrak{M}$ correspondants sont de la forme $\frac{1-i}{2}u$ où u est une unité de $\mathfrak{M}$ (i.e. un élément de $\{\pm 1,\ \pm i,\ \pm j,\ \pm k, \frac{\pm 1 \pm i \pm j \pm \omega}{2}\}$).

Le maximum de la norme, $\frac{1}{2}$, est atteint lorsque $y_3 \in \mathbb{Z}$, une des trois autres composantes de y est entière et les deux autres sont demi-entières.

Preuve de la proposition 1.
i) La première assertion est évidente et on montre par récurrence sur s que $\mu_{r,s}d_s$ est un élément de l'ordre de Hurwitz pour tout s tel que $1 \leq s < r$.

ii) Un calcul explicite de la somme donne *ii)* pour toute valeur de s. On donne le résultat pour $s = 1$ et $s = 2$.

Pour $s = 1$, $\quad d_1\mu_{p,1}\bar{\mu}_{t,1}B_1 = B_1\frac{b_p.b_1}{B_1}\frac{b_1.b_t}{B_1}B_1 \quad \in \mathfrak{M}$.

Pour $s = 2$, $\quad d_2(\mu_{p,1}\bar{\mu}_{t,1}B_1 + \mu_{p,2}\bar{\mu}_{t,2}B_2) = (b_2.b_2)(b_p.b_1)(b_1.b_t) + B_1(b_p.b_2)(b_2.b_t) -$
$(b_p.b_2)(b_2.b_1)(b_1.b_t) - (b_p.b_1)(b_1.b_2)(b_2.b_t) \quad \in \mathfrak{M}$. ■

Preuve de l'algorithme.
Dans la preuve de l'algorithme, on utilisait auparavant une inégalité due à Hermite,

$$d_r \geq N(\Lambda_r)^r \gamma_r^{-r} \geq N(\Lambda)^r \gamma_r^{-r}.$$

Ici, on utilise la formule $\det_{\mathbb{Z}}(\Lambda_r) = d_r^4.\mathrm{disc}(\mathfrak{M})^n$, où le déterminant d'une matrice de Gram de $\mathfrak{M}$ (en tant que réseau sur $\mathbb{Z}$) $\mathrm{disc}(\mathfrak{M})$ vaut $\frac{1}{4}$ si on prend comme produit scalaire sur $\mathbb{Z}$, $< x, y >= \frac{1}{2}\,\mathrm{Trd}(x.y)$ et $\det_{\mathbb{Z}}(\Lambda_r)$ est le déterminant du réseau Λ_r sur $\mathbb{Z}$.

On a alors comme inégalité

$$d_r^4 \geq N(\Lambda)^{4r} \gamma_r^{-4r} 4^n.$$

Le scalaire d_r est minoré par une constante ne dépendant que de r et du réseau et par conséquent D est minoré par une constante ne dépendant que du réseau Λ. Ceci montre que le sous-algorithme SWAPI n'est exécuté qu'un nombre fini de fois. ■

3.4 QUELQUES EXEMPLES NUMÉRIQUES.

Dans chaque exemple, on donne les bases des réseaux et les matrices des produits hermitiens sur $\mathbb{Z}[j]$ (resp. $\mathfrak{M}$).

Exemple 1 : le réseau K_{12}, dans une base de vecteurs minimaux, en tant que $\mathbb{Z}[j]$-module.
On construit la matrice $B = (b_p.b_r)$ des produits hermitiens des vecteurs minimaux de K_{12}, à partir de la base donnée dans [M], $b_1 = (0,\ 0,\ 0,\ 0,\ -1,\ 1)$; $b_2 = (0,\ 0,\ 0,\ -1,\ 1,\ 0)$; $b_3 = \frac{1}{1-j}\ (1,\ 1,\ 1,\ 1,\ 1,\ 1)$; $b_4 = (0,\ -1,\ 0,\ 1,\ 0,\ 0)$; $b_5 = (0,\ -j,\ 1,\ 0,\ 0,\ 0)$; $b_6 = (0,\ 0,\ -1,\ 1,\ 0,\ 0)$. On obtient la matrice suivante :

$$\begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 \\ -1 & 2 & 0 & -1 & 0 & -1 \\ 0 & 0 & 2 & 0 & j+1 & 0 \\ 0 & -1 & 0 & 2 & -j-1 & 1 \\ 0 & 0 & -j & j & 2 & -1 \\ 0 & -1 & 0 & 1 & -1 & 2 \end{pmatrix}$$

Après $\mathbb{Z}[j]$-LLL-réduction, on obtient la matrice suivante,

$$\begin{pmatrix} 2 & 1 & 1 & -j-1 & j & -j-1 \\ 1 & 2 & -j & -j-1 & j & 0 \\ 1 & j+1 & 2 & -j & 0 & -j-1 \\ j & j & j+1 & 2 & -j & -j \\ -j-1 & -j-1 & 0 & j+1 & 2 & 0 \\ j & 0 & j & j+1 & 0 & 2 \end{pmatrix}$$

Exemple 2 : le réseau K_{12} en tant que $\mathbb{Z}[j]$-module.

On reprend la même matrice B et on considère U, une matrice de $Gl_6(\mathbb{Z})$, de déterminant 1. Puis, on construit la matrice ${}^tUBU$ de K_{12}. Ce qui donne la matrice

$$\begin{pmatrix} 73 & 2j-66 & -2j+63 & -2j+117 & -4j+221 & 5j-279 \\ -2j-68 & 65 & -2j-62 & -2j-112 & -4j-212 & 5j+268 \\ 2j+65 & 2j-60 & 60 & 106 & 201 & -254 \\ 2j+119 & 2j-110 & 106 & 194 & 366 & -463 \\ 4j+225 & 4j-208 & 201 & 366 & 692 & -874 \\ -5j-284 & -5j+263 & -254 & -463 & -874 & 1106 \end{pmatrix}$$

A la fin du programme, on obtient la matrice

$$\begin{pmatrix} 2 & -j-1 & j & j & 1 & -j-1 \\ j & 2 & -j & -j-1 & j & 0 \\ -j-1 & j+1 & 2 & -j & -j-1 & 0 \\ -j-1 & j & j+1 & 2 & -j & 0 \\ 1 & -j-1 & j & j+1 & 2 & 0 \\ j & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

On peut remarquer que les termes diagonaux sont tous égaux à 2.

Remarques : Dans les deux exemples précédents, on a donné à la constante C_2, les valeurs 0.75, 0.8, 0.85, 0.9, 0.95, 0.99. Dans le premier exemple, lorsque la constante est ≥ 0.8, on obtient dans chaque cas, la même matrice. Pour chacune de ces valeurs, les matrices obtenues ont une diagonale de 2. Dans le deuxième exemple, on obtient les mêmes matrices pour 0.8 et 0.85 et pour $C_2 \geq 0.9$, mais une matrice différente lorsque $C_2 = 0.75$. Là aussi, toutes les matrices ont une diagonale de 2.

Exemple 3 : le réseau $\mathbf{BW}_{16}$ en tant $\mathfrak{M}$-module, dans une base de vecteurs minimaux.

On a pris comme $\mathfrak{M}$-base : $b_1 = (1,\ 1,\ 1,\ 1)$; $b_2 = (0,\ 1+i,\ 1+i,\ 0)$; $b_3 = (1+i,\ 1+i,\ 0,\ 0)$; $b_4 = (2,\ 0,\ 0,\ 0)$.
La matrice des produits hermitiens, après division par 2, est la suivante,

$$\begin{pmatrix} 2 & 1-i & 1-i & 1 \\ 1+i & 2 & 1 & 0 \\ 1+i & 1 & 2 & 1+i \\ 1 & 0 & 1-i & 2 \end{pmatrix}$$

Après $\mathfrak{M}$-réduction, on obtient

$$\begin{pmatrix} 2 & -1+i & -1+i & -1 \\ -1-i & 2 & 1 & i \\ -1-i & 1 & 2 & i \\ -1 & -i & -i & 2 \end{pmatrix}$$

Exemple 4 : le réseau de Leech en tant que $\mathfrak{M}$-module.

On considère la $\mathfrak{M}$-base : $b_1 = (1,\ 1,\ 1,\ 1,\ 0,\ 1,\ 1+2\omega)$; $b_2 = (0,\ 1+i,\ 0, -1+j,\ 1+i,\ -1+j)$; $b_3 = (0,\ 0,\ 1+i,\ -1+j,\ -1+j,\ 1+i)$; $b_4 = (0,\ 0,\ 0,\ 2,\ 0,\ -2)$; $b_5 = (0,\ 0,\ 0,\ 0,\ 2,\ -2)$; $b_6 = (0,\ 0,\ 0,\ 0,\ 0,\ 2+2i)$.

Elle correspond à la matrice des produits hermitiens, après division par 2,

$$\begin{pmatrix} 4 & -2\omega & 1-i-2j+2\omega & -2\omega & -2\omega & 3-i-2j+4\omega \\ 2+\omega & 4 & 0 & 0 & 2+i-j & 2\omega \\ -1+i+2j-2\omega & 0 & 4 & -2-i+j & -2-i+j & 2 \\ 2+2\omega & 0 & -2+i-j & 4 & 2 & -2+2i \\ 2+2\omega & 2-i+j & -2+i-j & 2 & 4 & -2+2i \\ -1+i+2j-4\omega & -2-2\omega & 2 & -2-2i & -2-2i & 4 \end{pmatrix}$$

Le programme sort comme matrice des produits hermitiens,

$$\begin{pmatrix} 4 & 1-i+2j & -1+2i+j & 2-i+j & 2i+2j & -1+3i-2\omega \\ 1+i-2j & 4 & 2-i-j+2\omega & 0 & 2-2i-2j+4\omega & -i-j \\ -1-2i-j & i+j-2\omega & 4 & -2-2\omega & 2-i-j & 3-i-2j+2\omega \\ 2+i-j & 0 & 2\omega & 4 & 2+2\omega & -2+2i \\ -2i-2j & -2+2i+2j-4\omega & 2+i+j & -2\omega & 4 & 1-j+2\omega \\ 1-3i+2\omega & i+j & 1+i+2j-2\omega & -2-2i & -1+j-2\omega & 4 \end{pmatrix}$$

Exemple 5 : les réseaux de Ch. Bachoc sur l'ordre de Hurwitz en dimensions 32, 40, 48.

On notera ces réseaux BC_{32}, BC_{40} et BC_{48} (ils sont construits à partir de codes [B 1] et [B 2]). Pour ces réseaux , qui au départ ne sont pas dans une base de vecteurs minimaux, on a appliqué la $\mathfrak{M}$-LLL-réduction. Ensuite, on a permuté les vecteurs de la base réduite afin de classer la diagonale (qui correspond aux normes hermitiennes des vecteurs) par ordre croissant et on a réduit la matrice ainsi obtenue. Enfin, on a recommencé les deux opérations précédentes jusqu'à ce que l'on "tombe sur" une base de vecteurs minimaux (que l'on obtient après une itération pour BC_{32}, deux pour BC_{40} et trois pour BC_{48}, lorsque la constante dans la condition de Lovász est 0.85).

Les deux matrices suivantes sont les bases des réseaux BC_{32} (resp. BC_{40}). Les vecteurs sont donnés en colonnes et la partie supérieure de chacune de ces matrices est formée de 0.

$$\begin{pmatrix}
1-i & & & & & & & \\
1-i & 2 & & & & & & \\
1-i & 0 & 2 & & & & & \\
1-i & 2 & 2 & 2+2i & & & & \\
1-i & 2-2i+2\omega & 2\omega & 0 & 2+2i & & & \\
1-i & 2+2\omega & 2i-2\omega & 2+2j & 2+2i & 4 & & \\
-1+i & 2i+2j-2\omega & 2i-2\omega & 2+2j & 2+2i & 0 & 4 & \\
-1+i-4\omega & 6j-2\omega & 2-2\omega & 2+2i & 2+2i & -4 & -4 & 4+4i
\end{pmatrix}$$

$$\begin{pmatrix}
1 & & & & & & & & & \\
1 & 0 & 1+i & & & & & & & \\
1 & -1+j & 1+i & & & & & & & \\
1 & -i-j & 1+i & 2i & & & & & & \\
1 & 0 & 1+i & 0 & 2i & & & & & \\
1 & 0 & -1+j & 2i & 2i & 2-2i-2j+2\omega & & & & \\
1 & 1+i & 1+i & 2i & 2i & 2i & 2i & & & \\
1 & -1+j & -1+j & 2i & 2i & 2i & -2+2j-2\omega & -2+2i & & \\
1 & -i-j & -i-j & 0 & 2i & 2i & 2-2i-2j+2\omega & 0 & -2+2i & \\
1+2\omega & 0 & -i-j & 0 & 2i & -2+2j-2\omega & 0 & -2+2i & -2+2i & 4
\end{pmatrix}$$

Voici les 12 vecteurs de $\mathfrak{M}$-base de BC_{48} :
$b_1 = (1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ -1+2j-4\omega)$,
$b_2 = (0,\ 1+i,\ 0,\ -1+j,\ 1+i,\ -1+j,\ 0,\ 1+i,\ 0,\ -1+j,\ 1+i,\ -1+j)$,
$b_3 = (0,\ 0,\ 1+i,\ -1+j,\ -1+j,\ 1+i,\ 0,\ 0,\ 1+i,\ -1+j,\ -1+j,\ 1+i)$,
$b_4 = (2i,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1+3i,\ 1+i,\ 1+i,\ 1+i,\ 1+i,\ 1+i)$,
$b_5 = (0,\ 0,\ 0,\ 2i,\ 0,\ 2i,\ 0,\ 0,\ 0,\ 2i,\ 0,\ 2i)$,
$b_6 = (0,\ 0,\ 0,\ 0,\ 2i,\ 2i,\ 0,\ 0,\ 0,\ 0,\ 2i,\ 2i)$,
$b_7 = (0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 2i,\ 0,\ 2-2i-2j+2\omega,\ 2i,\ 2-2i-2j+2\omega)$,
$b_8 = (0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 2i,\ 2-2i-2j+2\omega,\ 2-2i-2j+2\omega,\ 2i)$,
$b_9 = (0,\ 0,\ 0,\ 0,\ 0,\ -2+2i,\ 0,\ 0,\ 0,\ 0,\ 0,\ -2+2i)$,
$b_{10} = (0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ -2+2i,\ 0,\ -2+2i)$,
$b_{11} = (0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ -2+2i,\ -2+2i)$,
$b_{12} = (0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,4)$.

On donne seulement la diagonale des produits hermitiens, après division par 4 (resp. 2) pour BC_{32} et BC_{40} (resp. BC_{48}) et avant $\mathfrak{M}$-LLL-réduction, [6, 12, 8, 8, 8, 8, 8, 8] (resp. [3, 3, 4, 4, 6, 5, 3, 4, 4, 4], [10, 8, 8, 12, 8, 8, 8, 8, 8, 8, 8, 8]). Le tableau suivant contient les diagonales des produits hermitiens après chaque itération.

BC_{32}	BC_{40}	BC_{48}
[6, 6, 6, 6, 6, 6, 6, 6]	[3, 3, 3, 3, 3, 3, 3, 3, 4, 4]	[8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 12, 12]
	[3, 3, 3, 3, 3, 3, 3, 3, 3, 3]	[8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 12, 12]
		[8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8]

Remarques : Pour les trois réseaux de Ch. Bachoc, on a appliqué le procédé précédent à l'algorithme LLL sur $\mathbb{Z}$. On trouve une base de vecteurs minimaux de BC_{32} au bout de quatre itérations, mais pas pour BC_{40}, ni pour BC_{48}. Lorsqu'on ne fait qu'une seule $\mathfrak{M}$-LLL-réduction, les calculs sont beaucoup plus rapides que dans le cas de la $\mathbb{Z}$-LLL-réduction.

On a mis l'accent au début de cette partie, sur le fait que pour tout quaternion y, il n'existe pas qu'un seul entier de Hurwitz, x, tel que $\mathrm{Nrd}(y-x)$ soit la plus petite possible. Le programme prend le premier x qu'il trouve. Cela semble avoir beaucoup d'importance car pour les trois réseaux précédents, on ne trouve pas forcément une base de vecteurs minimaux (il faut modifier la constante C_2 dans la condition de Lovász).

BIBLIOGRAPHIE

[**Ba 1**] Ch. Bachoc, *Voisinage au sens de Kneser pour les réseaux quaternioniens*, Comm. Math. Helvet. 70 (1995), 350–374.

[**Ba 2**] Ch. Bachoc, *Codes et réseaux 2-modulaires extrémaux, en préparation.*

[**Co**] H. Cohen, *A course in computational algebraic number theory*, Springer-Verlag, Graduate Texts in Mathematics, n°138, 1995.

[**H-W**] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers*, Oxford university press.

[**L**] F. Lemmermeyer, *The euclidean algorithm in algebraic number fields, preprint.*

[**LLL**] A.K. Lenstra, H.W. Lenstra, Jr and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. 261 (1982), 515–534.

[**M**] J. Martinet, *Les réseaux parfaits des espaces euclidiens*, livre en préparation.

[**Pari**] Ch. Batut, D. Bernardi, H. Cohen and M. Olivier, User's Guide to PARI-GP.

Chapitre 4

A propos des minima successifs.

Ce chapitre traite d'une forme de réduction de bases de réseaux. Nous donnons un algorithme de recherche des minima successifs et l'appliquons aux anneaux d'entiers de corps de nombres de degrés 3, 4, 5, 7, 11 et 13.

4.1 GÉNÉRALITÉS.

Définition.
Soit Λ un réseau. Les minima successifs de Λ sont les n nombres réels $m_1, m_2, \ldots, m_n$ tels que pour $1 \leq r \leq n$, m_r est la borne inférieure des nombres réels λ tels qu'il existe r vecteurs indépendants de norme inférieure ou égale à λ.

Le premier minimum m_1 est égal à la norme minimale du réseau. Un système de vecteurs de normes les minima successifs n'est pas unique. Le théorème de Minkowski donne une majoration du produit des minima successifs.

Théorème (Minkowski).
Les minima successifs d'un réseau Λ de dimension n vérifient, pour tout $r \leq n$, l'inégalité $m_1 m_2 \ldots m_r \leq \gamma_n^r \det(\Lambda)^{\frac{r}{n}}$ où γ_n est la constante d'Hermite en dimension n et $\det(\Lambda)$ le déterminant du réseau Λ.

Grâce à ce théorème et à l'inégalité de Hadamard, on en déduit le corollaire suivant :

Corollaire.
L'indice d'un sous-réseau engendré par des vecteurs réalisant les minima successifs d'un réseau Λ est majoré par $\gamma_n^{\frac{n}{2}}$.

Preuve.
Soient Λ un réseau et Λ' le sous-réseau engendré par des vecteurs réalisant les minima successifs $m_1, m_2, \ldots, m_n$.
L'inégalité de Hadamard nous donne $\det(\Lambda') \leq m_1 m_2 \ldots m_n$ et celle du théorème de Minkowski, $\det(\Lambda) \geq m_1 m_2 \ldots m_n \gamma_n^{-n}$. On obtient donc $\frac{\det(\Lambda')}{\det(\Lambda)} \leq \gamma_n^n$. Comme le carré

de l'indice $[\Lambda : \Lambda']$ du réseau Λ' dans Λ est égal au quotient $\frac{\det(\Lambda')}{\det(\Lambda)}$, on a bien l'inégalité annoncée dans le corollaire. ■

La constante d'Hermite en dimension 3, γ_3, est strictement inférieure à 2. Ceci permet de dire qu'un réseau de dimension 3 possède toujours une base formée de vecteurs réalisant les minima successifs. En dimension 4, la constante d'Hermite vaut 2 et est réalisée par le réseau de racines $\mathbb{D}_4$. L'indice du réseau engendré par des vecteurs réalisant les minima successifs vaut donc 1 sauf peut-être si le réseau est isométrique à $\mathbb{D}_4$. En dimension 5, l'indice est majoré par 2, un système de vecteurs de normes les minima successifs n'est pas nécessairement une base du réseau. L'indice est 2 dans le cas du réseau cubique centré $\mathbb{D}_5$. Pour les dimensions supérieures, la majoration de l'indice croît assez vite. On trouve 4 pour la dimension $n = 6$, 8 pour $n = 7$ et 16 pour $n = 8$. On voit donc que trouver une base de vecteurs réalisant les minima successifs est en général limité aux dimensions $n \leq 4$. Par conséquent, on doit chercher d'autres formes de réduction de bases comme par exemple la LLL-réduction.

Description de l'algorithme de recherche de vecteurs réalisant les minima successifs.
Donnée : une matrice de Gram d'un réseau Λ *entier* de dimension n.
Sortie : une matrice de Gram du réseau Λ' engendré par un système de vecteurs réalisant les minima successifs de Λ et la matrice de passage de Λ à Λ'.
On notera $(m_i)_{1 \leq i \leq n}$ les minima successifs.
En pratique, on commence par remplacer la matrice de Gram donnée par une réduite LLL, et on reviendra en fin d'algorithme à la matrice de départ.

- $k = 1$.
- Chercher un vecteur minimal v_1 du réseau L.
- Tant que $k \leq n$

  Étape 1 : Vérifier que le nombre de vecteurs de norme m_k est supérieur ou égal à k.

  Si oui, prendre un vecteur v_{k+1} de norme m_k,
  vérifier que les vecteurs $v_1, v_2, \ldots, v_{k+1}$ sont linéairement indépendants. S'ils sont dépendants, choisir un autre vecteur de norme m_k et faire cela jusqu'à ce que l'on en trouve un tel que $v_1, v_2, \ldots, v_{k+1}$ soient linéairement indépendants.

  Sinon, incrémenter m_k de 1 et revenir à l'étape 1.

  Étape 2 : Si tous les vecteurs v_{k+1} de norme m_k sont tels que le système $\{v_1, v_2, \ldots, v_{k+1}\}$ est linéairement dépendant, incrémenter m_k de 1 et revenir à l'étape 1.
  Sinon, stocker v_{k+1}, poser $m_{k+1} = m_k$ et incrémenter k de 1.

- Construire la matrice de Gram du réseau engendré par les v_k.

Cet algorithme est basé sur la recherche de vecteurs de normes données et en particulier de norme minimale. Lorsque le réseau n'est pas entier, on travaille avec les nombres réels et on n'obtient qu'une approximation des normes. En 1982, dans [LLL], A.K. Lenstra,

H.W. Lenstra, Jr et L. Lovász exhibent un algorithme, qui sera appelé algorithme LLL, polynomial en temps, qui permet de trouver des vecteurs de normes assez petites et très souvent de norme minimale. La recherche des minima successifs peut être considérée comme une application de l'algorithme LLL.

Nous avons implanté l'algorithme des minima successifs afin de chercher des "bases plus agréables" des anneaux d'entiers de corps de nombres. Les matrices de Gram sont entières et par conséquent tous les calculs sont exacts. L'expression "base plus agréable" signifie ici base composée de vecteurs de normes plus petites que celles de départ.

4.2 APPLICATIONS AUX BASES D'ENTIERS DE CORPS DE NOMBRES.

Nous allons maintenant examiner le cas des réseaux formés par les anneaux d'entiers des corps de nombres totalement réels de degrés 3, 4, 5, 7, 11 et 13. Il est à noter que pour tout automorphisme σ d'un corps $K = \mathbb{Q}(\theta)$, si θ représente un minimum m_i, $\sigma(\theta)$ représente le même minimum. On pourra ainsi réaliser les minima m_i, m_{i+1}, ... par un certain nombre de relations de dépendance liant les conjugués de θ et les représentants des minima précédents.

On considère un corps de nombres K, de degré n, de signature $(r_1,\ r_2)$ $(r_1 + 2r_2 = n)$. On note $\sigma_1, \ldots, \sigma_n$ les n plongements de K dans $\mathbb{C}$, indexés de façon que σ_k soit réel pour $1 \leq k \leq r_1$ et que $\sigma_{r_1+r_2+k}$ soit le conjugué complexe de σ_{r_1+k} pour $1 \leq k \leq r_2$. On plonge K dans la $\mathbb{R}$-algèbre $\mathbb{C}^n$, que l'on munit du produit scalaire $\mathbb{C}$-hermitien défini positif $z.z' = \sum_{k=1}^{n} \sigma_k(z)\overline{\sigma}_k(z')$.

Proposition.
On a $m_1 = n$, et ce premier minimum est atteint exactement sur les racines de l'unité de K.

Preuve
On a en effet les deux inégalités

$$\left(\frac{\sum_{k=1}^{n} \sigma_k(\theta)\overline{\sigma}_k(\theta)}{n} \right)^n \geq \prod_{k=1}^{n} \sigma_k(\theta)\overline{\sigma}_k(\theta) = \mathrm{N}_{K/\mathbb{Q}}(\theta)^2 \geq 1$$

et l'égalité a lieu si et seulement si les $|\sigma_j(\theta)|^2$ sont tous égaux et de produit égal à 1. Ces conditions entraînent que les conjugués de θ sont tous de module 1, et donc, par le lemme de Kronecker, que θ est une racine de l'unité.
Réciproquement, il est clair que les racines de l'unité sont des vecteurs dont la longueur est de carré n. ■

Ainsi, dans le cas des corps cycliques de degré l premier, les minima successifs sont représentés par 1, puis par $l - 1$ conjugués d'un représentant de m_2.

4.2.1 Les corps cubiques.

Soit K un corps cubique cyclique. On peut trouver un entier algébrique θ tel que $K = \mathbb{Q}(\theta)$. On notera $P(X) = X^3 - SX^2 + TX - N$, le polynôme minimal de θ. Comme K est galoisien, il est totalement réel. On notera $G = \mathrm{Gal}(K/\mathbb{Q}) =< \sigma >\simeq \mathbb{Z}/3\mathbb{Z}$, son groupe de Galois. On considère $\zeta = \exp(\frac{2i\pi}{3})$ une racine cubique de l'unité. Ce n'est pas un élément de K car K est totalement réel. Le corps $K(\zeta)$ est de degré 6 sur $\mathbb{Q}$, galoisien, de groupe de Galois engendré par le prolongement de σ en $\sigma(\zeta) = \zeta$ (noté encore σ) et la conjugaison complexe τ.

On a le lemme suivant :

Lemme 1.
Soient $\nu = \theta + \zeta^2\sigma(\theta) + \zeta\sigma^2(\theta)$ et $\beta = \frac{\nu^2}{\tau(\nu)}$ ($\nu,\ \beta \in K(\zeta)$).

Alors $P(X) = X^3 - SX^2 + \frac{S^2-e}{3}X - \frac{S^3-3Se+eu}{27}$ où $e = \beta\tau(\beta)$ et $u = \beta + \tau(\beta)$ (i.e. e et u sont la norme et la trace de β considéré comme élément de $\mathbb{Q}(\zeta)$).

Par la théorie de Galois, on montre que β est un élément de $\mathbb{Q}(\zeta)$. Il peut donc s'écrire sous la forme $\frac{u+v\sqrt{-3}}{2}$ où u et v sont deux rationnels. D'après le lemme précédent, on a $e = \frac{u^2+3v^2}{4}$.

Le lemme suivant donne une forme bien pratique du polynôme P.

Lemme 2.
Pour tout corps cubique cyclique K, il existe une unique paire d'entiers $(e,\ u)$ tels que e est un produit de nombres premiers distincts congrus à 1 modulo 3, u est congru à 2 modulo 3 et $K = \mathbb{Q}(\theta')$ où θ' est une racine du polynôme $Q(X) = X^3 - \frac{e}{3}X - \frac{eu}{27}$ de $\mathbb{Z}[X]$ ou de manière équivalente $K = \mathbb{Q}(\theta)$ où θ est une racine du polynôme $P(X) = 27Q(X/3) = X^3 - 3eX - eu$.

Le lemme 3 va nous donner une base d'entiers et le discriminant du corps K.

Lemme 3.
Soit $K = \mathbb{Q}(\theta)$ un corps cubique cyclique où θ est racine du polynôme $P(X) = X^3 - 3eX - eu$, $e = \frac{u^2+3v^2}{4}$ avec $u \equiv 2\ (mod\ 3)$ et e est un produit de nombres premiers distincts congrus à 1 modulo 3.
a) Supposons $3 \nmid v$. Alors $(1,\ \theta,\ \sigma(\theta))$ et $(1,\ \theta,\ \sigma^2(\theta))$ sont des bases d'entiers de K et le discriminant d_K de K est $(9e)^2$.
b) Supposons $3 \mid v$. On pose $\theta' = \frac{1+\theta}{3}$. Alors $(1,\ \theta',\ \sigma(\theta'))$ et $(1,\ \theta',\ \sigma^2(\theta'))$ sont des bases d'entiers de K et le discriminant d_K de K est e^2.
De telles bases sont dites normales.

A partir de ces lemmes, on obtient le théorème suivant :

Théorème 1.

Tout corps cubique cyclique K est donné (à isomorphisme près) par

1) si 3 est ramifié dans K, alors $K = \mathbb{Q}(\theta)$ où θ est racine du polynôme à coefficients entiers, $P(X) = X^3 - \frac{e}{3}X - \frac{eu}{27}$ avec $e = \frac{u^2+27v^2}{4}$, $u \equiv 6 \pmod 9$, $3 \nmid v$, $v > 0$,

$u \equiv v \pmod 2$ et $\frac{e}{9}$ est un produit de nombres premiers distincts congrus à 1 modulo 3.

2) Si 3 n'est pas ramifié dans K, alors $K = \mathbb{Q}(\theta)$ où θ est racine du polynôme de $\mathbb{Z}[X]$, $P(X) = X^3 - X^2 + \frac{1-e}{3}X - \frac{1-3e+eu}{27}$ avec $e = \frac{u^2+27v^2}{4}$, $u \equiv 2 \pmod 3$, $v > 0$,

$u \equiv v \pmod 2$ et e est un produit de nombres premiers distincts congrus à 1 modulo 3.

Dans les deux cas, le discriminant de P, $disc(P)$ est e^2v^2 et celui du corps K, $d_K = e^2$.

3) Inversement, si e est égal à 9 multiplié par un produit de $(t-1)$ nombres premiers distincts congrus à 1 modulo 3 (resp. e est un produit de t nombres premiers distincts congrus à 1 modulo 3) alors il existe, à isomorphisme près, exactement 2^{t-1} corps cubiques cycliques de discriminants e^2 définis par un polynôme donné dans 1) (resp. 2)).

On pourra trouver une démonstration des trois lemmes ainsi que du théorème dans [Co].

Nous avons cherché les minima successifs des corps cubiques K totalement réels accessibles par ftp sur **megrez.math.u-bordeaux.fr** (147.210.16.17). Nous avons utilisé la table des 112 444 corps de nombres de discriminant inférieur ou égal à 2 000 000, construite par M. Olivier. On s'est plus particulièrement intéressé aux corps cycliques. On associe le produit scalaire $\langle x,\ y\rangle = \sum_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \sigma(x)\sigma(y) = \mathrm{Tr}_{K/\mathbb{Q}}(xy)$ au corps K.

Muni de ce produit scalaire, l'anneau des entiers $\mathbb{Z}_K$ est un réseau. Comme K est totalement réel, $\mathbb{Z}_K$, en tant que réseau, est entier. On a traité le cas des corps réels car on a employé la fonction **minim** du système PARI, pour chercher des vecteurs de normes données. Cette dernière utilise la version avec des calculs entiers de l'algorithme LLL.

On a obtenu le résultat suivant :

Théorème 2.

Soit $K = \mathbb{Q}(\theta)$ un corps cubique cyclique. On peut trouver une base d'entiers formée du "vecteur" 1 réalisant le premier minimum et de deux vecteurs conjugués, réalisant le deuxième, ces deux vecteurs étant définis par les polynômes qui interviennent dans le théorème 1.

Preuve.

On utilise les notations du théorème 1 et des lemmes précédents. D'après le lemme 3, tout élément de l'anneau d'entiers $\mathbb{Z}_K$ peut s'écrire sous la forme $a + b\theta + c\sigma(\theta)$ où a, b, c sont des entiers et σ un générateur de $\mathrm{Gal}(K/\mathbb{Q})$.

a) Cas où 3 est ramifié dans K.
Le polynôme minimal de θ est de la forme $P(X) = X^3 - 3eX - eu$. La trace $\mathrm{Tr}_{K/\mathbb{Q}}(\theta)$ est nulle et celle de θ^2 vaut $6e$. Il s'agit de trouver les minima successifs de la forme quadratique $\mathrm{Tr}_{K/\mathbb{Q}}(x^2)$. On pose $f(a,\ b,\ c) = \mathrm{Tr}_{K/\mathbb{Q}}((a + b\theta + c\sigma(\theta))^2)$.

On a $f(a,\ b,\ c) = \mathrm{Tr}_{K/\mathbb{Q}}(a^2 + b^2\theta^2 + c^2\sigma^2(\theta) + 2ab\theta + 2ac\sigma(\theta) + 2bc\theta\sigma(\theta))$,
$= 3a^2 + 6b^2e + 6c^2e - 6ebc$,
$= 3a^2 + 6e[(b - \frac{c}{2})^2 + \frac{3}{4}c^2]$.

Comme e est strictement positif, on a $f(a,\ b,\ c) \geq 3a^2 \geq 3$ si $a \neq 0$ avec l'égalité si $a = \pm 1$.

Si a est nul, la quantité $6e((b - \frac{c}{2})^2 + \frac{3}{4}c^2)$ ne peut pas être strictement inférieure à 3 sauf si b et c sont nuls.

Le premier minimum vaut donc 3 et est réalisé par les "vecteurs" ± 1.

Cherchons maintenant le deuxième minimum.

Supposons que a ne soit pas nul. On a $f(a,\ b,\ c) \geq 3a^2 \geq 3$. Il faut chercher le minimum de la forme $g(b,\ c) = 6e[(b - \frac{c}{2})^2 + \frac{3}{4}c^2]$.

Si c est nul, $g(b,\ 0) \geq 6eb^2$ et b ne peut pas être nul (car on cherche le deuxième minimum). Donc $g(b,\ 0) \geq 6e$ avec l'égalité si $b = \pm 1$.

Si c est non nul et b est nul, $g(0,\ c) \geq 6e$ avec l'égalité si $c = \pm 1$.

Si b et c sont non nuls, deux cas se présentent :

- $b \neq \frac{c}{2}$ et alors $g(b,\ c) \geq 6e(\frac{1}{4} + \frac{3}{4}c^2) \geq 6e$ avec l'égalité si $c = b = \pm 1$.
- $b = \frac{c}{2}$ et alors $g(\frac{c}{2},\ c) \geq \frac{9}{2}ec^2$. Mais dans ce cas, c est pair et $\mid c \mid \geq 2$, donc $g(\frac{c}{2},\ c) \geq 18e$.

Dans tous les cas, $g(b,\ c) \geq 6e$ et donc $f(a,\ b,\ c) \geq 3 + 6e$.

Si on suppose a nul, $f(0,\ b,\ c) \geq 6e$.
Par conséquent, le deuxième minimum est $6e$ et il est atteint lorsque ($a = c = 0$ et $b = \pm 1$) ou ($a = b = 0$ et $c = \pm 1$) ou ($a = 0$ et $b = c = \pm 1$). Il est réalisé par les six "vecteurs" $\pm\theta,\ \pm\sigma(\theta),\ \pm(\theta + \sigma(\theta)) = \mp\sigma^2(\theta)$.
Comme $(1,\ \theta,\ \sigma(\theta))$ est une base d'entiers, c'est aussi une base de vecteurs réalisant les deux premiers minima.

b) Cas où 3 n'est pas ramifié dans K.
Le polynôme minimal de θ est de la forme $P(X) = X^3 - X^2 + \frac{1-e}{3}X - \frac{1-3e+eu}{27}$. La trace de θ vaut 1 et celle de θ^2 vaut $\frac{2e+1}{3}$ et est supérieure ou égale à 5.

On a $f(a,\ b,\ c) = \mathrm{Tr}_{K/\mathbb{Q}}((a + b\theta + c\sigma(\theta))^2)$,
$= 3a^2 + b^2\frac{2e+1}{3} + c^2\frac{2e+1}{3} + 2ab + 2bc + 2bc\frac{1-e}{3}$.

On pose $E = \frac{2e+1}{3} \geq 5$.

Alors, $f(a,\ b,\ c) = 3(a + \frac{b+c}{3})^2 + (E - \frac{1}{3})[(b - \frac{c}{2})^2 + \frac{3}{4}c^2]$.

Cherchons le premier minimum.

On a $f(a,\ b,\ c) \geq 3(a + \frac{b+c}{3})^2$. Si $b = c = 0$, $f(a,\ 0,\ 0) \geq 3a^2 \geq 3$ si a n'est pas nul et l'égalité a lieu lorsque a vaut ± 1.

Si $b = 0$ et $c \neq 0$

- si $a = \frac{-c}{3}$ alors $f(\frac{-c}{3},\ 0,\ c) = (E - \frac{1}{3})c^2 \geq \frac{14}{3} > 3$,
- si $a \neq \frac{-c}{3}$ alors $f(a,\ 0,\ c) \geq 3 + (E - \frac{1}{3})c^2 > 3$.

On obtient les mêmes résultats si on suppose $c = 0$ et $b \neq 0$.

La quantité $(E - \frac{1}{3})[(b - \frac{c}{2})^2 + \frac{3}{4}c^2]$ est toujours supérieure à 3 sauf si $b = c = 0$.
Le premier minimum vaut 3 et est atteint par les "vecteurs" ± 1.

On cherche maintenant le deuxième minimum. Pour cela, on suppose d'abord que a est nul.

Si $c = 0$, $f(0,\ b,\ 0) = Eb^2 \geq E$ avec l'égalité si $b = \pm 1$ (car b ne peut pas être nul).

Si $c \neq 0$ et $b = 0$, $f(0,\ 0,\ c) = Ec^2 \geq E$ avec l'égalité si $c = \pm 1$.

Si b et c sont non nuls et si $b = \frac{c}{2}$, $f(0,\ \frac{c}{2},\ c) = \frac{1}{2}c^2 + \frac{3}{4}Ec^2 > E$ car c est pair et $\mid c \mid \geq 2$.

Si b et c sont non nuls et si $b \neq \frac{c}{2}$, $f(0,\ b,\ c) \geq \frac{1}{3}(b + c)^2 + (E - \frac{1}{3})(1 + \frac{3}{4}c^2)$,

- si $b = -c$, $f(0,\ -c,\ c) \geq \frac{7}{4}(E - \frac{1}{3}) > E$,
- si $b \neq -c$, $f(0,\ b,\ c) > \frac{1}{3} + \frac{7}{4}(E - \frac{1}{3}) \geq E$.

Lorsque $a = 0$, on a $f(0,\ b,\ c) \geq E$.
Supposons maintenant que a ne soit pas nul.

- Si $b = 0$, $f(a,\ 0,\ c) = 3(a + \frac{c}{3})^2 + (E - \frac{1}{3})c^2$,
  c doit être non nul car on cherche le deuxième minimum,
  - si $a = \frac{-c}{3}$, $f(\frac{-c}{3},\ 0,\ c) = (E - \frac{1}{3})c^2 \geq 9(E - \frac{1}{3})$ car c divisible par 3,
    donc $f(\frac{-c}{3},\ 0,\ c) > E$,
  - si $a \neq \frac{-c}{3}$, $f(a,\ 0,\ c) \geq \frac{1}{3} + (E - \frac{1}{3})c^2 > E$.

On a des résultats analogues si c est nul.

Si b et c sont tous deux non nuls,

- si $b = \frac{c}{2}$, $f(a,\ \frac{c}{2},\ c) = 3(a + \frac{c}{2})^2 + (E - \frac{1}{3})\frac{3}{4}c^2$,
  - si $a = \frac{-c}{2}$, $f(\frac{-c}{2},\ \frac{c}{2},\ c) = (E - \frac{1}{3})\frac{3}{4}c^2 \geq 3(E - \frac{1}{3})$ car c est pair et $\mid c \mid \geq 2$,
    d'où $f(\frac{-c}{2},\ \frac{c}{2},\ c) > E$,
  - si $a \neq \frac{-c}{2}$, $f(a,\ \frac{c}{2},\ c) \geq \frac{1}{2} + \frac{3}{4}Ec^2 > E$ car c est pair,
- si $b \neq \frac{c}{2}$, $f(a,\ b,\ c) \geq 3(a + \frac{b+c}{3})^2 + (E - \frac{1}{3})(\frac{1}{4} + \frac{3}{4}c^2)$,
  - si $b = -c$, $f(a,\ -c,\ c) \geq \frac{8}{3} + E > E$,
  - si $b \neq -c$, $f(a,\ b,\ c) \geq \frac{1}{3} + (E - \frac{1}{3}) \geq E$ avec l'égalité lorsque $a = 1$,
    $b = c = -1$ ou $a = -1$, $b = c = 1$.

Quelle que soit la valeur de a, le deuxième minimum est E et il est atteint lorsque $a = c = 0$ et $b = \pm 1$ (i.e. en $\pm\theta$) ou $a = b = 0$ et $c = \pm 1$ (i.e. en $\pm\sigma(\theta)$) ou $a = 1$, $b = c = -1$ (i.e. en $\sigma^2(\theta)$) ou $a = -1$, $b = c = 1$ (i.e. en $-\sigma^2(\theta)$).

Comme $(1,\ \theta,\ \sigma(\theta))$ est une base d'entiers, c'est aussi une base de vecteurs réalisant les deux premiers minima. ■

Remarque : On peut éviter tout calcul en observant que, étant donné un $\mathbb{Z}[G]$-module Λ de rang 1 (avec $G = \{1,\ \sigma,\ \sigma^2\}$ cyclique d'ordre 3), Λ/Λ^G est un module de rang 1 sur l'anneau des entiers d'Eisenstein, donc libre, la base étant unique au produit près par un élément $\pm\sigma^j$. Un élément θ de $\mathbb{Z}_K$ engendrant une base normale et de trace dans $[-1,\ +1]$ est donc unique au signe près et à conjugaison près, et, comme le second minimum engendre aussi une base normale, il coïncide avec l'un des $\pm\sigma^j(\theta)$.

4.2.2 Les corps de nombres de degré 4.

Nous avons utilisé la table des 13 073 corps de nombres, de discriminants inférieurs à 1 000 000, totalement réels de degré 4 construite par J. Buchmann, D. Ford, M. Pohst. Elle est aussi accessible par ftp sur **megrez.math.u-bordeaux.fr.**

Nous avons calculé ci-dessous dans la limite de la table utilisée tous les minima successifs pour les corps imprimitifs totalement réels de degré 4. Le type galoisien est $C_4 = \mathbb{Z}/4\mathbb{Z}$ ou $C_2 \times C_2 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. On traite aussi le cas diédral D_4. Pour chacun, on donne le plus petit discriminant et les possibilités rencontrées.

- C_4.

Premier cas : les deuxième, troisième et quatrième vecteurs représentant le deuxième minimum ont un polynôme minimal de degré 4. Ils sont alors nécessairement conjugués. Le premier corps quartique rencontré a pour discriminant $4\ 913 = 17^3$.

Deuxième cas : le deuxième vecteur a un polynôme minimal quadratique et les deux suivants un polynôme minimal quartique. Ces deux derniers sont conjugués et le premier corps rencontré a pour discriminant $1\ 125 = 3^2.5^3$.

Troisième cas : les deuxième, troisième et quatrième vecteurs ont même longueur, mais deux d'entre eux ont un polynôme minimal de degré 4 et le troisième un polynôme minimal de degré 2. Comme ce cas est assez rare, on donne la liste par ordre croissant, de tous les discriminants d_K des corps quartiques vérifiant cette propriété, ainsi que le discriminant du corps quadratique d_k défini par le polynôme minimal du troisième vecteur représentant le deuxième minimum.

$d_K = 2\ 048 = 2^{11}$ et $d_k = 8$,
$d_K = 256\ 000 = 2^{11}.5^3$ et $d_k = 40$,
$d_K = 256\ 000 = 2^{11}.5^3$ et $d_k = 40$.
Ces deux derniers corps ne sont pas isomorphes.

- $C_2 \times C_2$

Premier cas : les deuxième et troisième vecteurs ont un polynôme minimal quadratique. Le discriminant du corps défini par le polynôme minimal du deuxième vecteur est strictement inférieur au discriminant du corps défini par le polynôme minimal du troisième. Le

quatrième vecteur a un polynôme minimal de degré 4. Le premier corps quartique pour lequel cette situtation se produit a pour discriminant $1\ 600 = 2^6.5^2$.

Deuxième cas : les deuxième et quatrième vecteurs ont un polynôme minimal quadratique. Le discriminant du corps défini par le polynôme minimal du deuxième vecteur est strictement inférieur au discriminant du corps défini par le polynôme minimal du quatrième. Le troisième vecteur a un polynôme minimal de degré 4. Le plus petit discriminant est $2\ 304 = 2^8.3^2$.

Troisième cas : les deuxième et troisième vecteurs ont un polynôme minimal quartique. Ils sont conjugués. Le quatrième vecteur a un polynôme minimal de degré 2. Le premier corps quartique rencontré a pour discriminant $7\ 056 = 2^4.3^2.7^2$.

Quatrième cas : les troisième et quatrième vecteurs ont un polynôme minimal quartique. Ils sont conjugués. Le deuxième vecteur a un polynôme minimal de degré 2. Le premier corps quartique rencontré a pour discriminant $53\ 361 = 3^2.7^2.11^2$.

- D_4

Premier cas : le premier vecteur réalisant le deuxième minimum a un polynôme minimal quadratique et les deux suivants un polynôme minimal quartique. Le plus petit discriminant est $725 = 5^2.29$.

Deuxième cas : les deuxième et troisième vecteurs ont un polynôme minimal quartique. Ils ne sont pas conjugués. Le quatrième vecteur est quadratique. Le plus petit discriminant est $9\ 248 = 2^5.17^2$.

Troisième cas : les deuxième et quatrième vecteurs ont un polynôme minimal quartique. Ils ne sont pas conjugués. Le troisième vecteur est quadratique. Le plus petit discriminant est $4\ 752 = 2^4.3^3.11$.

Quatrième cas : les deuxième, troisième et quatrième vecteurs ont un polynôme minimal de degré 4. Ils ne sont pas nécessairement conjugués. Le plus petit discriminant est $4\ 205 = 5.29^2$. (Le corps correspondant a la même clôture galoisienne que celui du premier cas.)

4.2.3 Les corps de nombres de degré 5.

Nous avons cherché les minima successifs des 22 740 corps quintiques, de discriminant inférieur à 20 000 000, de la table construite par F. Diaz y Diaz, M. Pohst, A. Schwarz. Cette table est disponible sur **megrez.math.u-bordeaux.fr**. Le résultat le plus étonnant est le suivant :

Théorème 3.
Pour les 22 740 *anneaux d'entiers des corps quintiques totalement réels de discriminant inférieur à* 20 000 000, *les vecteurs réalisant les minima successifs constituent une base d'entiers.*

Théorème 4.
Soit K un corps galoisien de degré 5, *totalement réel, de discriminant $d_k \leq$ 20 000 000. On peut trouver, une base d'entiers formée de* 1, *vecteur réalisant le premier minimum*

et de quatre autres éléments conjugués, réalisant le deuxième. Ces vecteurs sont la trace sur K d'une racine de l'unité d'ordre f minimum tel que K soit un sous-corps de $\mathbb{Q}(\zeta_f)$. Le discriminant de K, d_K vaut f^4.

Preuve.
Il existe seulement 5 corps quintiques $K = \mathbb{Q}(\theta)$ cycliques galoisiens totalement réels de discriminant inférieur à 20 000 000. Pour chacun d'eux, on donne le discriminant de K, une base d'entiers, les conjugués de θ sous l'action du groupe de Galois $G = \mathrm{Gal}(K/\mathbb{Q}) = < \sigma > \simeq \mathbb{Z}/5\mathbb{Z}$ donnés dans l'ordre θ, $\sigma(\theta)$, $\sigma^2(\theta)$, $\sigma^3(\theta)$, $\sigma^4(\theta)$, la matrice de Gram des éléments de la base d'entiers, la matrice de passage de la base de départ à la base des vecteurs réalisant les minima successifs, la matrice des produits scalaires des vecteurs réalisant les minima successifs, l'expression des vecteurs réalisant le deuxième minimum en fonction des conjugués de θ, le polynôme minimal d'un vecteur réalisant le deuxième minimum et une valeur de θ.

- Corps 1 : $d_K = 11^4$,

base d'entiers : $[1,\ \theta,\ \theta^2,\ \theta^3,\ \theta^4]$,

conjugués de θ : $[\theta,\ \theta^3 - 3\theta,\ -\theta^2 + 2,\ -\theta^4 + 4\theta^2 - 2,\ \theta^4 - \theta^3 - 3\theta^2 + 2\theta + 1]$,

matrice de Gram : $\begin{pmatrix} 5 & 1 & 9 & 4 & 25 \\ 1 & 9 & 4 & 25 & 16 \\ 9 & 4 & 25 & 16 & 78 \\ 4 & 25 & 16 & 78 & 64 \\ 25 & 16 & 78 & 64 & 257 \end{pmatrix}$,

matrice de passage : $\begin{pmatrix} 1 & 2 & 1 & 0 & -2 \\ 0 & 0 & 2 & -3 & 0 \\ 0 & -4 & -3 & 0 & 1 \\ 0 & 0 & -1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix}$,

matrice de Gram des minima successifs : $\begin{pmatrix} 5 & -1 & 1 & 1 & -1 \\ -1 & 9 & 2 & 2 & -2 \\ 1 & 2 & 9 & -2 & 2 \\ 1 & 2 & -2 & 9 & 2 \\ -1 & -2 & 2 & 2 & 9 \end{pmatrix}$,

expression des vecteurs réalisant le deuxième minimum en fonction des conjugués de θ : $2 - 4\theta^2 + \theta^4 = -\sigma^3(\theta)$, $1 + 2\theta - 3\theta^2 - \theta^3 + \theta^4 = \sigma^4(\theta)$, $-3\theta + \theta^3 = \sigma(\theta)$, $-2 + \theta^2 = -\sigma^2(\theta)$,

polynôme minimal d'un vecteur réalisant le deuxième minimum : $x^5 - x^4 - 4x^3 + 3x^2 + 3x - 1$,

on peut prendre $\theta = -2\cos(\frac{2\pi}{11})$.

- Corps 2 : $d_K = 25^4$,

base d'entiers : $[1,\ \theta,\ \theta^2,\ \theta^3,\ 1/7\theta^4 - 3/7\theta^3 - 1/7\theta^2 - 2/7\theta + 2/7]$,

conjugués de θ : $[\theta,\ -1/7\theta^4+3/7\theta^3+8/7\theta^2-19/7\theta-9/7,\ 3/7\theta^4-2/7\theta^3-24/7\theta^2-6/7\theta+6/7,\ 2/7\theta^4+1/7\theta^3-23/7\theta^2-18/7\theta+25/7,\ -4/7\theta^4-2/7\theta^3+39/7\theta^2+36/7\theta-22/7]$,

matrice de Gram : $\begin{pmatrix} 5 & 0 & 20 & 15 & 15 \\ 0 & 20 & 15 & 160 & -40 \\ 20 & 15 & 160 & 255 & 80 \\ 15 & 160 & 255 & 1475 & -250 \\ 15 & -40 & 80 & -250 & 175 \end{pmatrix}$,

matrice de passage : $\begin{pmatrix} 1 & 2 & 0 & 3 & 1 \\ 0 & -4 & 0 & -2 & 3 \\ 0 & -5 & -3 & -3 & -1 \\ 0 & 2 & 1 & 1 & 0 \\ 0 & 4 & 3 & 2 & 1 \end{pmatrix}$,

matrice de Gram des minima successifs : $\begin{pmatrix} 5 & 0 & 0 & 0 & 0 \\ 0 & 20 & 5 & 5 & -5 \\ 0 & 5 & 20 & -5 & 5 \\ 0 & 5 & -5 & 20 & 5 \\ 0 & -5 & 5 & 5 & 20 \end{pmatrix}$,

expression des vecteurs réalisant le deuxième minimum en fonction des conjugués de θ :
$2 - 4\theta - 5\theta^2 + 2\theta^3 + 4(1/7\theta^4 - 3/7\theta^3 - 1/7\theta^2 - 2/7\theta + 2/7) = -\sigma^4(\theta)$,
$-3\theta^2 + \theta^3 + 3(1/7\theta^4 - 3/7\theta^3 - 1/7\theta^2 - 2/7\theta + 2/7) = \sigma^2(\theta)$,
$3 - 2\theta - 3\theta^2 + \theta^3 + 2(1/7\theta^4 - 3/7\theta^3 - 1/7\theta^2 - 2/7\theta + 2/7) = \sigma^3(\theta)$,
$1 + 3\theta - \theta^2 + 1/7\theta^4 - 3/7\theta^3 - 1/7\theta^2 - 2/7\theta + 2/7 = -\sigma(\theta)$,

polynôme minimal d'un vecteur réalisant le deuxième minimum : $x^5 - 10x^3 - 5x^2 + 10x - 1$,

on peut prendre $\theta = -2(\cos(\frac{2\pi}{25}) + \cos(\frac{14\pi}{25}))$.

- Corps 3 : $d_K = 31^4$,

base d'entiers : $[1,\ \theta,\ \theta^2,\ \theta^3,\ 1/5\theta^4 + 2/5\theta^3 - 1/5\theta^2 - 2/5\theta]$,

conjugués de θ : $[\theta,\ 2/5\theta^4 - 1/5\theta^3 - 22/5\theta^2 + 31/5\theta,\ -1/5\theta^4 - 2/5\theta^3 + 6/5\theta^2 + 2/5\theta + 2,\ 2/5\theta^4 + 4/5\theta^3 - 17/5\theta^2 - 14/5\theta + 2,\ -3/5\theta^4 - 1/5\theta^3 + 33/5\theta^2 - 24/5\theta - 3]$,

matrice de Gram : $\begin{pmatrix} 5 & 1 & 25 & -26 & 34 \\ 1 & 25 & -26 & 249 & -18 \\ 25 & -26 & 249 & -564 & 325 \\ -26 & 249 & -564 & 2950 & -586 \\ 34 & -18 & 325 & -586 & 442 \end{pmatrix}$,

matrice de passage : $\begin{pmatrix} 1 & 0 & -3 & 2 & -2 \\ 0 & -7 & -6 & -2 & 0 \\ 0 & 4 & 6 & -3 & -1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & -2 & -3 & 2 & 1 \end{pmatrix}$,

matrice de Gram des minima successifs : $\begin{pmatrix} 5 & -1 & 1 & 1 & -1 \\ -1 & 25 & 6 & 6 & -6 \\ 1 & 6 & 25 & -6 & 6 \\ 1 & 6 & -6 & 25 & 6 \\ -1 & -6 & 6 & 6 & 25 \end{pmatrix}$,

expression des vecteurs réalisant le deuxième minimum en fonction des conjugués de θ :
$-7\theta + 4\theta^2 + \theta^3 - 2(1/5\theta^4 + 2/5\theta^3 - 1/5\theta^2 - 2/5\theta) = -\sigma(\theta)$,
$-3 - 6\theta + 6\theta^2 + \theta^3 - 3(1/5\theta^4 + 2/5\theta^3 - 1/5\theta^2 - 2/5\theta) = \sigma^4(\theta)$,
$2 - 2\theta - 3\theta^2 + 2(1/5\theta^4 + 2/5\theta^3 - 1/5\theta^2 - 2/5\theta) = \sigma^3(\theta)$,
$-2 - \theta^2 + 1/5\theta^4 + 2/5\theta^3 - 1/5\theta^2 - 2/5\theta = -\sigma^2(\theta)$,

polynôme minimal d'un vecteur réalisant le deuxième minimum : $x^5 - x^4 - 12x^3 + 21x^2 + x - 5$,

on peut prendre $\theta = -2(\cos(\frac{2\pi}{31}) + \cos(\frac{10\pi}{31}) + \cos(\frac{12\pi}{31}))$.

- Corps 4 : $d_K = 41^4$,

base d'entiers : $[1,\ \theta,\ \theta^2,\ 1/3\theta^3 - 1/3\theta,\ 1/9\theta^4 - 1/9\theta^3 - 1/9\theta^2 - 5/9\theta - 1/3]$,

conjugués de θ : $[\theta,\ -1/9\theta^4 + 4/9\theta^3 + 10/9\theta^2 - 34/9\theta - 2/3,\ -1/9\theta^4 + 1/9\theta^3 + 19/9\theta^2 - 4/9\theta - 11/3,\ 4/9\theta^4 - 7/9\theta^3 - 58/9\theta^2 + 19/9\theta + 20/3,\ -2/9\theta^4 + 2/9\theta^3 + 29/9\theta^2 + 10/9\theta - 4/3]$,

matrice de Gram : $\begin{pmatrix} 5 & 1 & 33 & 21 & 44 \\ 1 & 33 & 64 & 160 & 99 \\ 33 & 64 & 513 & 524 & 766 \\ 21 & 160 & 524 & 941 & 808 \\ 44 & 99 & 766 & 808 & 1158 \end{pmatrix}$,

matrice de passage : $\begin{pmatrix} 1 & 8 & 2 & 4 & 1 \\ 0 & 4 & 0 & 1 & 4 \\ 0 & -6 & -3 & -2 & -1 \\ 0 & -1 & 0 & 0 & -1 \\ 0 & 4 & 2 & 1 & 1 \end{pmatrix}$,

matrice de Gram des minima successifs : $\begin{pmatrix} 5 & 1 & -1 & -1 & -1 \\ 1 & 33 & 8 & 8 & 8 \\ -1 & 8 & 33 & -8 & -8 \\ -1 & 8 & -8 & 33 & -8 \\ -1 & 8 & -8 & -8 & 33 \end{pmatrix}$,

expression des vecteurs réalisant le deuxième minimum en fonction des conjugués de θ :
$8 + 4\theta - 6\theta^2 - (1/3\theta^3 - 1/3\theta) + 4(1/9\theta^4 - 1/9\theta^3 - 1/9\theta^2 - 5/9\theta - 1/3) = \sigma^3(\theta)$,
$2 - 3\theta^2 + 2(1/9\theta^4 - 1/9\theta^3 - 1/9\theta^2 - 5/9\theta - 1/3) = -\sigma^4(\theta)$,
$4 + \theta - 2\theta^2 + 1/9\theta^4 - 1/9\theta^3 - 1/9\theta^2 - 5/9\theta - 1/3 = -\sigma^2(\theta)$,
$1 + 4\theta - \theta^2 - (1/3\theta^3 - 1/3\theta) + 1/9\theta^4 - 1/9\theta^3 - 1/9\theta^2 - 5/9\theta - 1/3 = -\sigma(\theta)$,

polynôme minimal d'un vecteur réalisant le deuxième minimum : $x^5 - x^4 - 16x^3 - 5x^2 + 21x + 9$,

on peut prendre $\theta = -2(\cos(\frac{2\pi}{41}) + \cos(\frac{6\pi}{41}) + \cos(\frac{18\pi}{41}) + \cos(\frac{28\pi}{41}))$.

- Corps 5 : $d_K = 61^4$,

base d'entiers : $[1,\ \theta,\ \theta^2,\ \theta^3,\ 1/29\theta^4 - 12/29\theta^3 - 8/29\theta^2 - 11/29\theta - 12/29]$,

conjugués de θ : $[\theta,\ 25/29\theta^4 - 39/29\theta^3 - 577/29\theta^2 + 740/29\theta + 599/29,\ -11/29\theta^4 + 16/29\theta^3 + 262/29\theta^2 - 314/29\theta - 332/29,\ -8/29\theta^4 + 9/29\theta^3 + 180/29\theta^2 - 173/29\theta - 136/29,\ -6/29\theta^4 + 14/29\theta^3 + 135/29\theta^2 - 282/29\theta - 102/29]$,

matrice de Gram : $\begin{pmatrix} 5 & 1 & 49 & 22 & 10 \\ 1 & 49 & 22 & 1017 & -425 \\ 49 & 22 & 1017 & 606 & 220 \\ 22 & 1017 & 606 & 22618 & -9289 \\ 10 & -425 & 220 & -9289 & 4046 \end{pmatrix}$,

matrice de passage : $\begin{pmatrix} 1 & -16 & -31 & 8 & -6 \\ 0 & -15 & -35 & 9 & -12 \\ 0 & 6 & 13 & -4 & 3 \\ 0 & -4 & -9 & 3 & -2 \\ 0 & -11 & -25 & 8 & -6 \end{pmatrix}$,

matrice de Gram des minima successifs : $\begin{pmatrix} 5 & 1 & -1 & -1 & 1 \\ 1 & 49 & 12 & 12 & -12 \\ -1 & 12 & 49 & -12 & 12 \\ -1 & 12 & -12 & 49 & 12 \\ 1 & -12 & 12 & 12 & 49 \end{pmatrix}$,

expression des vecteurs réalisant le deuxième minimum en fonction des conjugués de θ :
$-16 - 15\theta + 6\theta^2 - 4\theta^3 - 11(1/29\theta^4 - 12/29\theta^3 - 8/29\theta^2 - 11/29\theta - 12/29) = \sigma^2(\theta)$,
$-31 - 35\theta + 13\theta^2 - 9\theta^3 - 25(1/29\theta^4 - 12/29\theta^3 - 8/29\theta^2 - 11/29\theta - 12/29) = -\sigma(\theta)$,
$8 + 9\theta - 4\theta^2 + 3\theta^3 + 8(1/29\theta^4 - 12/29\theta^3 - 8/29\theta^2 - 11/29\theta - 12/29) = -\sigma^3(\theta)$,
$-6 - 12\theta + 3\theta^2 - 2\theta^3 - 6(1/29\theta^4 - 12/29\theta^3 - 8/29\theta^2 - 11/29\theta - 12/29) = \sigma^4(\theta)$,

polynôme minimal d'un vecteur réalisant le deuxième minimum : $x^5 - x^4 - 24x^3 + 17x^2 + 41x + 13$,

on peut prendre $\theta = 2(\cos(\frac{2\pi}{61}) + \cos(\frac{22\pi}{61}) + \cos(\frac{26\pi}{61}) + \cos(\frac{28\pi}{61}) + \cos(\frac{42\pi}{61}) + \cos(\frac{58\pi}{61}))$. ■

4.2.4 Les corps de nombres de degré supérieur ou égal à 5.

Nous énonçons la conjecture suivante :

Conjecture (J. Martinet).
Soit K un corps cyclique de degré premier $l \geq 5$ et de conducteur f (le plus petit entier tel que K soit un sous-corps du corps $\mathbb{Q}(\zeta)$, où ζ est une racine d'ordre f de l'unité). Soit $\theta = \mathrm{Tr}_{\mathbb{Q}(\zeta)/K}(\zeta)$. Alors, θ et ses conjugués représentent les minima d'indice > 1 de $\mathbb{Z}_K$.

Afin de tester cette conjecture, nous avons calculé des polynômes correspondant à des corps quintiques totalement réels cycliques de discriminant f^4 pour $f < 2\ 000$. Ce dernier est soit un produit de nombres premiers distincts deux à deux, congrus à 1 modulo 5, soit 25 multiplié par un produit de nombres premiers distincts deux à deux, congrus à 1 modulo 5. On a ainsi trouvé 132 corps deux à deux non isomorphes et pour chacun d'eux la conjecture s'est révélée vraie.

Nous avons aussi cherché des polynômes correspondant à des corps de degré 7 totalement réels cycliques de discriminant f^6 lorsque f est un produit de nombres premiers distincts deux à deux, congrus à 1 modulo 7 et $f < 1\ 000$. Nous avons obtenu 28 corps deux à deux non isomorphes. Pour chacun d'eux, 1, θ et ses conjugués réalisent les minima successifs et ils forment une base d'entiers.

Nous nous sommes intéressés à des polynômes associés à des corps de degré 11 (resp. 13) totalement réels cycliques de discriminant f^{10} (resp. f^{12}) lorsque f est un produit de nombres premiers congrus à 1 modulo 11 (resp. 13) et $f < 1\ 500$ (resp. $f < 2\ 000$). Nous avons ainsi trouvé 22 (resp. 24) corps deux à deux non isomorphes et avons vérifié que pour chacun d'eux, 1, θ et ses conjugués représentent les minima successifs et qu'ils constituent une base d'entiers.

BIBLIOGRAPHIE

[B] B.C. Berndt and R.J. Evans, *The Determination of Gauss Sums*, Bull. Amer. Math. Soc. 5 (1981), 107 – 129.

[C] J.W.S. Cassels, *Rational Quadratic Forms*, Academic Press, London, 1978.

[Co] H. Cohen, *A course in computational algebraic number theory*, Springer-Verlag, Graduate Texts in Mathematics, 1995.

[LLL] A.K. Lenstra, H.W. Lenstra, Jr and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. 261 (1982), 515 – 534.

[M] J. Martinet, *Les réseaux parfaits des espaces euclidiens*, livre en préparation.

[**Pari**] Ch. Batut, D. Bernardi, H. Cohen and M. Olivier, User's Guide to PARI-GP.

[**Si**] C.L. Siegel, *The trace of totally positive and real algebraic integers*, Ann Math. 46 (1945), 302 – 312.

[V] B. Vallée, *Algorithmique en géométrie des nombres. Applications à la cryptographie et à la factorisation des entiers*, Dossier en vue de l'obtention de l'habilitation à diriger des recherches, 1989.

Résumé.

Cette thèse se compose de quatre parties qui sont toutes consacrées à l'étude des réseaux euclidiens, et qui plus est sous un aspect résolument algorithmique. Ces quatre chapitres traitent des questions suivantes : sections de quelques réseaux importants, algorithme de voisinages de Voronoï, réduction des réseaux par une variante de l'algorithme LLL et enfin réduction et minima successifs des anneaux d'entiers algébriques.

Abstract.

This thesis contains four sections which are all devoted to the study of euclidean lattices especially from an algorithmic point of view. These four chapters deal with the following questions: sections of some important lattices, algorithm of Voronoï's neighbourhood, reduction of the lattices with a new version of the LLL algorithm and at last, reduction and successive minima for the algebraic rings of the integers.

Mots-clés.

Réseaux euclidiens, de Leech, de Ch. Bachoc, de Coxeter, voisinages de Voronoï, LLL-réduction, algorithme des minima successifs pour les anneaux d'entiers de corps de nombres.