Journal de Théorie des Nombres
de Bordeaux **11** (1999), 149–159

Sur la classification des réseaux parfaits de dimension 5

par Jacques MARTINET

Résumé. En utilisant des méthodes de Watson, nous donnons une courte démonstration de la classification (due à Korkine et Zolotareff) des réseaux parfaits de dimension 5. Des considérations d'indice nous conduisent à nous intéresser à trois classes de réseaux, dont chacune contient précisément un réseau parfait.

Abstract. English title: *On the classification of* 5*-dimensional perfect lattices.* Using methods of Watson, we give a short proof of Korkine and Zolotareff's classification of 5-dimensional perfect lattices. Using a description of sub-lattices of rank 5 generated by minimal vectors, we are led to consider three classes of lattices, each of which containing exactly one perfect lattice.

L'exposé oral fait le 18 septembre 1997, sous le titre *les réseaux des espaces euclidiens*, avait consisté en un tour d'horizon de diverses questions liées à la propriété d'extrémalité. (Korkine et Zolotareff ont appelé *extrêmes* les réseaux sur lesquels la densité de de l'empilement de sphères asssocié atteint un maximum local.) On avait plus particulièrement fait le point sur les questions suivantes :

• Généralisations de la notion d'extrémalité et caractérisations à la façon de Voronoï par des propriétés de *perfection* et d'*eutaxie* convenables.
• Cas des réseaux *isoduaux* (i.e., semblables à leur dual), et en particulier des réseaux *symplectiques*, qui correspondent aux variétés abéliennes complexes principalement polarisées.
• Décomposition en *classes minimales* de l'espace des réseaux, et interprétation comme décomposition cellulaire de l'espace des formes quadratiques définies positives de minimum donné sur $\mathbb{Z}^n$.
• Réseaux modulaires au sens de Quebbemann. (Un réseau Λ est dit ℓ*-modulaire* s'il est entier et pair, et s'il existe une similitude de rapport $\sqrt{\ell}$ de Λ^* sur Λ.)
• Théorie de Venkov des réseaux *fortement parfaits*, et mise en évidence au moyen de formes modulaires à coefficients sphériques.

Mots-clefs. Réseaux euclidiens, réseaux parfaits.

En ce qui concerne le dernier point, j'ai écrit une rédaction provisoire de notes d'un cours intitulé "Réseaux et *designs* sphériques" fait à Bordeaux par Boris Venkov en 1996-1997, que je peux communiquer sur demande. Le trosième point est développé dans le chapitre IX de mon livre "Les réseaux parfaits des espaces euclidiens", paru chez Masson (Paris) en 1996.

Les autres points ont fait l'objet de deux "surveys" :

(1) "Algebraic Constructions of Lattices; Isodual Lattices", Actes du colloque d'Eger (Hongrie, 1996) ; *Number Theory*, Győry, Pethő, Sós éd., Walter de Gruyter GmbH & Co., Berlin - New York, 1998 ;

(2) "Perfect and Eutactic Lattices: Extensions of Voronoi's Theory", *in Voronoï's impact on modern science*, P. Engel et H. Syta éd., vol. 21 of Proc. Inst. Math. National Acad. Sc. Ukraine, Book 1, pages 186–198.

L'existence des références ci-dessus rend inutile la rédaction d'un compte rendu de mon exposé. Il m'a paru préférable de proposer aux organisateurs de publier une démonstration considérablement raccourcie (grâce à l'utilisation de méthodes de Watson) du théorème de classification des réseaux parfaits de dimension 5, dû à Korkine et Zolotareff, sous la forme forte que l'on peut extraire de leur article [K-Z3]. Le lecteur pourra vérifier que le cœur de la démonstration de [K-Z3] (qualifiée il est vrai de "prolixe" par Coxeter) occupe 20 pages, contre 9 pages dans [M], ch. VI, § 4, reposant sur les mêmes principes, et moins de 3 pages (§§ 3 et 4) ci-dessous. La démonstration présentée, du fait qu'elle se suffit à elle-même, occupe un peu plus de place ; dans les mêmes conditions, il en serait de même des autres démonstrations que nous avons évoquées (ainsi que de celles, radicalement différentes, fondées sur l'algorithme de Voronoï).

1. Énoncés, notations et inégalités classiques.

1.1. Théorème. *Un réseau de dimension* 5 *possédant une section minimale* $\mathbb{D}_4$ *et au moins* 5 *couples de vecteurs minimaux en-dehors de cette section est semblable à* $\mathbb{D}_5$.

1.2. Théorème. *Un réseau de dimension* $n = 5$ *sans section minimale* $\mathbb{D}_4$ *avec* $s \geq \frac{n(n+1)}{2} = 15$ *est semblable à* $\mathbb{A}_5$ *ou à* $\mathbb{A}_5^3$.

Ces résultats complètent ceux qui concernent les dimensions $n \leq 4$ dont nous rappelons ci-dessous l'énoncé (et dont nous indiquerons les grandes lignes d'une démonstration) :

1.3. Théorème. *Un réseau de dimension* $n \leq 4$ *avec* $s \geq \frac{n(n+1)}{2}$ *est semblable à l'un des réseaux* $\mathbb{Z}$, $\mathbb{A}_2$, $\mathbb{A}_3$, $\mathbb{D}_4$ *ou* $\mathbb{A}_4$.

Il s'agit de montrer que, pour $n \leq 3$ (resp. $n = 4$; resp. $n = 5$) il y a au plus un (resp. deux ; resp. trois) réseaux vérifiant les hypothèse des th. 1.1 à 1.3, des exemples étant connus *a priori* ; les démonstrations que nous donnerons conduiront du reste à des constructions explicites.

Le but de Korkine et Zolotareff était de classer les réseaux *extrêmes*, c'est-à-dire ceux sur lesquel l'invariant d'Hermite (ou la densité de l'empilement de sphère associé, cela revient au même) atteint un maximum local. Ils montrent que les réseaux extrêmes sont en particulier *parfaits*, une propriété qui, dans le langage géométrique des réseaux, s'exprime ainsi : les projections orthogonales sur l'ensemble des vecteurs minimaux du réseau engendrent l'espace $\mathrm{End}^s(E)$ des endomorphismes symétriques de l'espace euclidien E, et dans la traduction de celui plus classique des formes quadratiques : un réseau est parfait si et seulement s'il est déterminé à similitude près par la connaissance des composantes de ses vecteurs minimaux dans l'une de ses bases.

Les théorèmes 1.1 et 1.2 entraînent qu'il y a exactement 3 classes de similitude de réseaux parfaits de dimension 5, vu qu'un réseau parfait de dimension n contient nécessairement n vecteurs minimaux indépendants en-dehors de toute section hyperplane, et au moins $\frac{n(n+1)}{2}$ couples de vecteurs minimaux (en général, au moins $\frac{n(n+1)}{2} - \frac{r(r+1)}{2} = \frac{(n-r)(n+r+1)}{2}$ couples de vecteurs minimaux en-dehors de toute section de dimension r).

Notations : la norme d'un vecteur x est son carré scalaire $N(x) = x.x$, la norme d'un réseau Λ est $N(\Lambda) = \min_{x\in\Lambda\smallsetminus\{0\}} N(x)$, on pose $S(\Lambda) = \{x \in \Lambda \mid N(x) = N(\Lambda)\}$ (ensemble des *vecteurs minimaux* de Λ) et $s(\Lambda) = s = \frac{1}{2}|S(\Lambda)|$. La *matrice de Gram d'une base* $\mathcal{B} = (e_1, \ldots, e_n)$ de Λ est $\mathrm{Gram}(\mathcal{B}) = (e_i.e_j)$, et le *déterminant* $\det(\Lambda)$ *de* Λ est le déterminant de la matrice de Gram de l'une de ses bases. Enfin, l'*invariant d'Hermite de* Λ est $\gamma(\Lambda) = \dfrac{N(\Lambda)}{\det(\Lambda)}$ et la *constante d'Hermite pour la dimension* n est $\gamma_n = \sup_{\dim\Lambda=n} \gamma(\Lambda)$.

On utilisera l'*inégalité de Mordell* :

$$\textbf{(1.4)} \qquad \forall n \geq 3,\ \gamma_n \leq \gamma_n^{(n-1)/(n-2)},$$

qui contient comme cas particulier l'*inégalité d'Hermite*

$$\textbf{(1.5)} \qquad \forall n,\ \gamma_n \leq \left(\frac{4}{3}\right)^{(n-1)/2},$$

ainsi que la caractérisation suivante du réseau $\mathbb{A}_n$:

1.6. Théorème (Korkine et Zolotareff). *Un réseau de dimension n, contenant n vecteurs minimaux indépendants, engendré par n'importe quelle famille de n vecteurs minimaux indépendants, et vérifiant l'inégalité $s \geq \frac{n(n+1)}{2}$, est semblable à $\mathbb{A}_n$ (et l'on a alors $s = \frac{n(n+1)}{2}$),*
dont la démonstration jusqu'à la dimension 5 est un exercice de combinatoire.

Un des ingrédients de la démonstration de ce théorème est la notion de *déterminant caractéristique*, que nous allons aussi utiliser dans la suite. Considérons un réseau L de dimension n muni d'une base $\mathcal{B} = (e_1, \ldots, e_n)$ de vecteurs minimaux, et notons $\pm x_1, \ldots, \pm x_s$ les couples de vecteurs minimaux de L, en convenant de prendre $x_i = e_i$ pour $1 \leq i \leq n$.

1.7. Définition. On appelle *déterminant caractéristique du couple* $(L, \mathcal{B})$ tout déterminant extrait de la matrice des composantes dans $\mathcal{B}$ des vecteurs $x_{n+1}, \ldots, x_s$.

1.8. Lemme (Korkine et Zolotareff). *Si* $\Delta \neq 0$ *est un déterminant caractéristique de* $(L, \mathcal{B})$*,* L *possède un sous-réseau* L' *engendré par des vecteurs minimaux de* L *et d'indice* $|\Delta|$ *dans* L*.*

En effet, quitte à permuter les e_i et les x_j, on peut supposer qu'il s'agit du déterminant de la matrice M des composantes sur $e_1, \ldots, e_k$ du système $T = (x_{n+1}, \ldots, x_{n+k})$. En complétant T par adjonction de $e_{k+1}, \ldots, e_n$, on obtient un système T', engendrant un $\mathbb{Z}$-module $N \subset L$ tel que les diviseurs élémentaires de (N, L) sont ceux de la matrice M.

Démonstration de 1.3. Par récurrence à partir de la dimension 1, on voit de proche en proche qu'un réseau Λ de dimension $n \leq 4$ vérifiant l'inégalité $s(\Lambda) \geq \frac{n(n+1)}{2}$ possède n vecteurs minimaux indépendants. Vu la majoration $[\Lambda : \Lambda'] \leq \gamma_n^{n/2}$ s'appliquant à tout couple d'un réseau Λ de dimension n et d'un sous-réseau Λ' de Λ contenant n vecteurs minimaux de Λ (qui s'obtient tout de suite en minorant $\det(\Lambda)$ par (1.5) et en majorant $\det(\Lambda')$ par l'inégalité de Hadamard, cf. [M], ch. II, § 1 et prop. 2.7), on constate en utilisant (1.8) et (1.6) que la minoration $s(\Lambda) \geq \frac{n(n+1)}{2}$ entraîne que Λ est semblable à $\mathbb{A}_n$ pour tout $n \leq 3$. On a donc $\gamma_3 = \gamma(\mathbb{A}_3) = 2^{1/3}$, d'où $\gamma_4 \leq \sqrt{2}$, ce qui entraîne, pour $\dim \Lambda = 4$ et $s(\Lambda) \geq \frac{n(n+1)}{2} = 10$, l'alternative $\Lambda \sim \mathbb{A}_4$, ou, si $[\Lambda : \Lambda'] = 2$ est possible, $\Lambda \sim \mathbb{D}_4$, puisque l'inégalité de Hadamard étant alors une égalité, il n'y a pas d'autre choix pour Λ' et Λ qu'un réseau cubique et le réseau cubique centré correspondant, lequel est semblable au réseau de racines $\mathbb{D}_4$.

1.9. Proposition. *Un réseau de dimension* 5 *avec* $s \geq 15$ *possède* 5 *vecteurs minimaux indépendants.*

En effet, un réseau de dimension $n \leq 4$ possède au plus $s(\mathbb{D}_4) = 12$ couples de vecteurs minimaux.

Les démonstrations des théorèmes 1.1 et 1.2 occupent les §§ 2 à 5, qui sont suivis par un paragraphe de commentaires justifiant en particulier que nous n'avons pas triché en employant de façon cachée des résultats difficiles.

2. Préliminaires.

On utilisera le résultat suivant de Watson tant pour étudier des questions d'indices que pour préciser certaines proprétés des vecteurs minimaux des réseaux.

2.1. Proposition (Watson, [W]). *Si $e_1, \dots, e_n$ sont n vecteurs minimaux indépendants d'un réseau Λ contenant également un vecteur $e = \frac{1}{d}(\sum_{i=1}^n a_i e_i)$ avec $d > 1$ et $d, a_1, \dots, a_n$ premiers entre eux dans leur ensemble, on a $(\sum_i |a_i|) \geq 2d$.*

Cette inégalité est une conséquence immédiate de l'identité ci-dessous, que nous écrivons dans le cas particulier (auquel on se ramène facilement) des coefficients $a_i > 0$:

$$\textbf{(2.2)} \qquad \big((\sum_i a_i) - 2d\big)N(e) = \sum_i |a_i| \big(N(e - e_i) - N(e_i)\big)\,,$$

qui montre en outre que, en cas d'égalité, le vecteur $e - e_i$ est minimal chaque fois que a_i est non nul.

On considère uniquement des réseaux Λ de dimension n vérifiant la condition (WR) ci-dessous (pour *well rounded*) :

$$\textbf{(WR)} \qquad S(\Lambda) \text{ est de rang } n\,,$$

et l'on note alors Λ' un sous-réseau de Λ engendré par n vecteurs minimaux indépendants de Λ ; autrement dit, Λ' est un réseau de même norme que Λ vérifiant également la condition (WR).

En outre, *les calculs explicites de produits scalaires seront faits en supposant que Λ (et donc aussi Λ') est de norme* 1. Cette hypothèse entraîne en particulier l'inégalité $|x.y| \leq \frac{1}{2}$ quels que soient x, y minimaux, comme on le voit en considérant les minorations $(x \pm y).(x \pm y) \geq 1$.

2.3. Définition. On dit que Λ est *d'indice au plus d* si l'on a $[\Lambda : \Lambda'] \leq d$, et *d'indice d* si cette valeur est atteinte.

Lorsque $d = 2$, on peut écrire $\Lambda = \langle \Lambda', e \rangle$ avec $e = \dfrac{e_1 + \cdots + e_t}{2}$ pour un entier t convenable.

2.4. Définition. Soit Λ un réseau d'indice 2. La *2-longueur de* Λ est le minimum m des entiers t comme ci-dessus.

On a $4 \leq m \leq n$, la minoration $m \geq 4$ provenant du fait que seul l'indice 1 est possible en dimension $n \leq 3$. En outre, si $m = 4$, le réseau engendré par e, e_1, e_2, e_3, e_4 est semblable à $\mathbb{D}_4$.

2.5. Lemme. *Avec les notations des définitions 2.3 et 2.4, on a :*

(1) *Les vecteurs minimaux de* Λ' *sont des sommes* $\pm e_{i_1} \pm \cdots \pm e_{i_k}$.

(2) *Il n'y a pas dans* $S(\Lambda')$ *de doublets contenant* $e_i + e_j$ *et* $e_i - e_j$*, ni de triplets contenant* $e_i + e_j$, $e_i + e_k$ *et* $e_j + e_k$.

(3) *Il n'y a pas dans* $S(\Lambda')$ *de vecteurs* $\pm e_{i_1} \pm \cdots \pm e_{i_k}$ *avec* $k \geq 2$ *à support contenu dans* $\{1, \ldots, m\}$.

(4) *Les vecteurs de* $S(\Lambda) \cap (e + \Lambda)$ *sont de la forme* $x = e + \sum a_i e_i$ *avec* $a_i \in \{0, -1\}$ *si* $i \leq m$ *et* $a_i \in \{0, \pm 1\}$ *sinon.*

Démonstration. (1) Un sous-réseau d'indice d de Λ' étant d'indice $2d$ dans Λ, Λ' est un réseau d'indice 1. Si $x = \sum_i a_i e_i$ est minimal, chaque a_i est un déterminant caractéristique. On a donc $|a_i| \leq 1$ pour tout i.

(2) De la même façon, la présence dans $S(\Lambda')$ d'un doublet $(e_i + e_j + \ldots, e_i - e_j + \ldots)$ ou d'un triplet $(e_i + e_j + \ldots, e_i + e_k + \ldots, e_j + e_k + \ldots)$ est interdite par les égalités $\begin{vmatrix} 1 & 1 \\ 1 & -1 \end{vmatrix} = -2$ et $\begin{vmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{vmatrix} = -2$.

(3) Quitte à permuter et à changer les signes de certains vecteurs e_i, on peut supposer que $x = e_1 + \cdots + e_k$ est minimal. On peut alors écrire $e = \frac{(e_1 + \cdots + e_k) + e_{k+1} + \cdots + e_m}{2}$, ce qui contredit la définition de m.

(4) On écrit $x = \frac{b_1 e_1 + \cdots + b_n e_n}{2}$, avec $b_i = 1 + 2a_i$ ou $b_i = 2a_i$. Si b_1 (pour fixer les idées) est non nul, on a $e_1 = \frac{-2x + b_2 e_2 + \cdots + \beta_n e_n}{b_1}$, ce qui fait apparaître un indice $|b_1|$. On a donc $|b_i| \leq 2$ pour tout i.

2.6. Corollaire. *Si* $m = n$, $S(\Lambda')$ *est réduit à* $\{\pm e_1, \ldots, \pm e_n\}$.

2.7. Proposition. *Un réseau de dimension* 5 *est d'indice* 1 *ou* 2.

Démonstration. On a $\gamma_4 = \gamma(\mathbb{D}_4) = 2^{1/2}$ (Section 1), donc $\gamma_5 \leq 2^{2/3}$ par 1.4, d'où $[\Lambda : \Lambda'] \leq \lfloor 2^{5/3} \rfloor = 3$, et l'inégalité de Watson (2.1) montre que l'indice 3 est impossible.

Dans la suite, on considère un réseau Λ de dimension 5 et d'indice 2, et l'on note e_1, e_2, e_3, e_4, e_5 des vecteurs minimaux indépendants de Λ engendrant un sous-réseau Λ' d'indice 2 dans Λ. À similitude près, on peut supposer que Λ de norme 1.

3. Démonstration du théorème 1.1.

Quitte à permuter les e_i, on suppose que Λ contient le vecteur $e = \frac{e_1 + e_2 + e_3 + e_4}{2}$. Les réseaux $L' = \langle e_1, e_2, e_3, e_4 \rangle$ et $L = \langle L', e \rangle$ sont isométriques respectivement à $\mathbb{Z}^4$ et au réseau cubique centré correspondant.

Soit $x \in S(\Lambda'), x \notin L'$. On a $\pm x = e_5 + y$ avec $y \in L'$. Par permutation et changements de signes des e_i, on peut supposer que $x = e_5 + y$ et que y est l'un des vecteurs e_1, $e_1 + e_2$, $e_1 + e_2 + e_3$, $e_1 + e_2 + e_3 + e_4$. On doit exclure les deux derniers cas, car on aurait alors $e = \frac{x + e_4 - e_5}{2}$ ou $e = \frac{x - e_5}{2}$,

ce qui ferait apparaître un indice 2 en dimension 3 ou 2. Si $y = e_1 + e_2$, on peut écrire
$$e = \frac{(e_1 + e_2 + e_5) + e_3 + e_4 - e_5}{2},$$
ce qui entraîne que e_3 et e_4 sont orthogonaux à e_5, et que $e_5.(e_1+e_2+e_5) = 0$, donc $e_1.e_5+e_2.e_5 = -1$, d'où, vu les majorations $|e_i.e_5| \leq \frac{1}{2}$, $e_1.e_5 = e_2.e_5 = -\frac{1}{2}$. Ainsi, tous les produits scalaires $e_i.e_j$ sont fixés, ce qui prouve que Λ est unique à similitude près, et donc parfait. Comme $\sqrt{2}\Lambda$ est engendré par des vecteurs de norme 2, c'est un réseau de racines, qui ne peut être que $\mathbb{D}_5$ (et son identification est immédiate sur les matrices de Gram ci-dessous).

Si Λ n'est pas semblable à $\mathbb{D}_5$, les vecteurs minimaux de $S(\Lambda') \smallsetminus L'$ doivent être de la forme $\pm e_5$ ou $\pm e_i \pm e_5$. Mais $e_i + e_5$ et $e_i - e_5$ ne sont pas minimaux en même temps (lemme 2.5), non plus que $e_1 + e_5$ et $e_2 + e_5$, car on aurait alors $e_1.e_5 = e_2.e_5 = -\frac{1}{2}$ et $e_1 + e_2 + e_5$ serait minimal. Il y a donc alors au plus 2 couples de vecteurs minimaux dans $S(\Lambda') \smallsetminus L'$, et donc au moins 3 dans $S(\Lambda) \cap (e + \Lambda')$. Mais ce dernier cas se ramène au précédent en considérant le réseau $L'_1 = \langle e, e_2, e_3, e_4\rangle$ et en écrivant $L = \langle L'_1, e_1\rangle$.

3.1. Remarque. La démonstration précédente fournit 4 couples de vecteurs minimaux en-dehors de L dans chacune des classes Λ' et $e + \Lambda'$, représentés par e_5, $e_1 + e_5$, $e_2 + e_5$, $e_1 + e_2 + e_5$, $e + e_5$, $e - e_3 + e_5$, $e - e_4 + e_5$ et $e - e_3 - e_4 + e_5$, et les matrices de Gram suivantes de Λ' et Λ respectivement après remplacement de e_5 par $-e_5$:
$$A_1 = \begin{pmatrix} 2&0&0&0&1\\ 0&2&0&0&1\\ 0&0&2&0&0\\ 0&0&0&2&0\\ 1&1&0&0&2 \end{pmatrix} \qquad \text{et} \qquad B_1 = \begin{pmatrix} 2&1&1&1&1\\ 1&2&0&0&1\\ 1&0&2&0&0\\ 1&0&0&2&0\\ 1&1&0&0&2 \end{pmatrix}.$$

4. Démonstration du théorème 1.2.

Nous considérons maintenant un réseau Λ de dimension $n = 5$, d'indice 2, de 2-longueur 5, avec $s \geq 15$. En changeant éventuellement les signes des e_i, on peut supposer que e lui-même est minimal. Il résulte du corollaire 2.6 que les vecteurs minimaux de Λ autres que les $\pm e_i$ sont à chercher parmi les 16 couples $\pm e$, $\pm(e - e_i)$ et $\pm(e - e_j - e_k)$, $1 \leq j \leq k \leq 5$.

4.1. Lemme. *Soit s' le nombre de couples de vecteurs minimaux de Λ de la forme $e - e_j - e_k$, $j < k$. On a $s' \leq 6$, et, si $s' = 6$, à permutation près des e_i, il s'agit des vecteurs $e - e_j - e_k$, $j = 1, 2, 3$, $k = 4, 5$.*

Démonstration. Pour $1 \leq j \leq 5$, soit $p(j)$ le nombre d'indices k tels que $e - e_j - e_k$ soit minimal (on a $s' = \frac{1}{2}\sum_j p(j)$), et soit $p = \max_j p(j)$; on suppose $p = p(5)$. Si $p = 4$, le lemme 2.5, (2) majore s' par 4. Si $p = 2$ (resp. 1), on a évidemment $s' \leq \frac{1}{2}\binom{5}{2} = 5$ (resp. $s' \leq 2$). Si $p = 3$, on peut supposer que $e - e_5 - e_1, e - e_5 - e_2, e - e_5 - e_3$ sont minimaux, et 2.5, (2) entraîne que les autres vecteurs minimaux de la forme $e - e_j - e_k$ sont à chercher parmi les $e - e_4 - e_k$.

4.2. Lemme. *Λ possède exactement trois vecteurs minimaux de la forme $e - e_i$.*
Démonstration. Soit s'' le nombre de tels vecteurs minimaux. On a $s'' \geq 15 - 6 - s' \geq 3$, et l'égalité 2.2 : $N(e) = \sum_{i=1}^{5} N(e - e_i) - N(e_i)$ s'écrit ici $\sum_{N(e-e_i)>1} N(e - e_i) = 6 - s''$, et entraîne que l'on a $s'' \leq 4$.

Si $s'' = 4$, on peut supposer que $e - e_1$, $e - e_2$, $e - e_3$, $e - e_4$ sont minimaux, et que $e - e_5$ ne l'est pas, et l'égalité précédente se réduit à $N(e - e_5) = 2$, i.e. $e.e_5 = 0$. Alors, pour $1 \leq i \leq 4$, on a $N(e - e_i - e_5) = 2 + 2e.e_5 > 1$, ce qui entraîne tout de suite $s' \leq 4$, et donc $s \leq 6 + 4 + 4 < 15$.

4.3. Lemme. *Le réseau Λ possède 15 couples de vecteurs minimaux qui, à permutation et changements de signes près des e_i, peuvent être représentés par les 15 vecteurs e, e_i $(i \leq 5)$, $e - e_i$ $(i \leq 3)$ et $e - e_j - e_k$ $(j = 1, 2, 3,\ k = 4, 5)$.*
Démonstration. Par hypothèse, les e_i sont minimaux, et l'on a vu (lemmes 4.2 et 4.3) que l'on peut faire en sorte que $e, e - e_1, e - e_2, e - e_3$ le soient aussi. Alors, $e - e_4$ et $e - e_5$ ne le sont pas, ce qui impose (avec les notations du lemme 4.1) que l'on ait $s' \geq 6$, donc $s' = 6$ et $s = 15$, et aussi $p = 3$, valeur atteinte sur deux indices j dont il reste à montrer que ce sont $j = 4$ et $j = 5$. Sinon, on aurait par exemple $p(1) = 3$, et donc 3 vecteurs minimaux $e - e_1 - e_i$, $e - e_1 - e_j$, $e - e_1 - e_k$. Posons $e' = e - e_1$. On voit alors que les vecteurs e', $e' + e_1$, $e' - e_i$, $e' - e_j$, $e' - e_k$ sont minimaux, ce qui contredit le lemme 4.2.

L'énoncé suivant achève la démonstration du théorème 1.2 :

4.4. Théorème. *Un réseau de dimension 5, d'indice 2, de 2-longueur 5, avec $s \geq 15$ est parfait et possède exactement 15 couples de vecteurs minimaux. Il est entier et de déterminant 162 lorsqu'on le normalise au minimum 4.*
Démonstration. À similitude près, on peut supposer que Λ possède parmi ses vecteurs minimaux ceux dont la liste figure dans le lemme 4.3. On va montrer que ces conditions fixent les produits scalaires $e_i.e_j$, ce qui prouvera à la fois l'unicité de Λ à similitude près et sa perfection.

Posons $x_i = e.e_i$. On a $x_1 = x_2 = x_3 = \frac{1}{2}$ (car e, e_i et $e - e_i$ sont minimaux pour $i = 1, 2, 3$), et les 6 conditions $N(e - e_j - e_k) = 1$ pour $j = 1, 2, 3$ et $k = 4, 5$ entraînent les relations $e_j.e_k = x_k - \frac{1}{2}$. On obtient $x_4 + x_5 = 1$ par la relation $N(e) = 1$, d'où, pour $i = 1, 2, 3$, $e_i.e_4 + e_i.e_5 = x_4 + x_5 - 1 = -\frac{1}{2}$, puis, par le calcul de $e.e_i$, les relations $e_1.e_2 + e_1.e_3 = e_2.e_1 + e_2.e_3 = e_3.e_1 + e_3.e_2 = \frac{1}{2}$, d'où enfin $e_1.e_2 = e_1.e_3 = e_2.e_3 = \frac{1}{4}$. Par le calcul de $e.e_4$ et de $e.e_5$, on obtient $e_4.e_5 = \frac{1}{2} - x_4 = \frac{1}{2} - x_5$, d'où finalement $e_4.e_5 = x_4 = x_5 = \frac{1}{4}$ et $e_j.e_k = -\frac{1}{4}$ $(j = 1, 2, 3,\ k = 4, 5)$.

En changeant e_4 en $-e_4$ et e_5 en $-e_5$, et en posant $e' = \frac{e_1+e_2+e_3-e_4-e_5}{2}$, on obtient après multiplication par 2 les matrices de Gram suivantes de $\mathcal{B}' = (e_1, e_2, e_3, e_4, e_5)$ et de $\mathcal{B} = (e', e_2, e_3, e_4, e_5)$:

$$A_2 = \begin{pmatrix} 4&1&1&1&1\\ 1&4&1&1&1\\ 1&1&4&1&1\\ 1&1&1&4&1\\ 1&1&1&1&4 \end{pmatrix} \qquad \text{et} \qquad B_2 = \begin{pmatrix} 4&2&2&-1&-1\\ 2&4&1&1&1\\ 2&1&4&1&1\\ -1&1&1&4&1\\ -1&1&1&1&4 \end{pmatrix}.$$

Le système des valeurs propres de A est $(8^1, 3^4)$. On a donc $\det(A_2) = 2^3.3^4$ et $\det(B_2) = \frac{1}{4}\det(A_2) = 2.3^4 = 162$.

5. Commentaires.

Deux parties des travaux de Korkine et Zolotareff consacrés à la classification des réseaux extrêmes de dimension $n \le 5$ comportent des démonstrations très longues :

(1) L'obtention dans [K-Z2] de l'inégalité stricte $\gamma_5^{5/2} < 3$;

(2) La classification proprement dite des réseaux de dimension 5 vérifiant les hypothèses du théorème 1.1, qui occupe une grande partie de [K-Z3].

Les démonstrations simplifiées des résultats de Korkine et Zolotareff qui sont présentés dans [M], ch. II, § 8 et ch. VI, §§ 2, 4 sont dans l'esprit de celles de [K-Z2] et [K-Z3], et occupent encore beaucoup de place.

Watson suggère dans [W] que ses méthodes devraient permettre de simplifier les travaux de Korkine – Zolotareff, de Blichfeldt ([Bl], sur la constante d'Hermite dans les dimensions 6, 7 et 8) et de Barnes ([Bar], sur la classification des réseaux parfaits de dimension 6).

La démonstration du théorème 1.1 que nous avons donnée ici est comparable par la taille à celles de [K-Z3] (**19**) et de [M] (ch. VI, th. 4.1). Il en est de même de celle du théorème 1.3, dont une variante pour la dimension 4 consiste à remarquer que l'identité 2.2 de Watson est encore valable si l'on remplace e_i par $-e_i$ lorsque $a_i = \frac{d}{2}$. On voit alors directement que les vecteurs $\dfrac{\pm e_1 \pm e_2 \pm e_3 \pm e_4}{2}$ sont minimaux et l'on identifie le réseau cubique centré sans utiliser l'inégalité de Hadamard. C'est le point de vue de [C-S1], § 4.

La partie (1) est très raccourcie grâce aux majorations d'indices de Watson, dont nous avons donné des démonstrations complètes. L'inégalité de Mordell (qui figure du reste dans [K-Z1] pour $n = 3$) se démontre de façon très courte (cf. [Cas], Ch. X, § 3 ; la démonstration de [M], ch. II, § 3, qui analyse les cas d'égalité, est de ce fait plus longue). On aurait pu aussi se contenter de l'inégalité d'Hermite, à condition de modifier en conséquence la proposition 2.7 de façon à prouver l'impossibilité de l'indice 4, ce qui ne présente pas non plus de difficulté.

Il est surprenant que la partie (2) puisse être simplifiée dans de telles proportions. On peut invoquer le fait qu'elle conduit à une séparation naturelle en deux classes (celle de Λ' et celle de $e + \Lambda'$) des vecteurs de Λ, ainsi que la mise en évidence de symétries dans les calculs. De toute façon, ce procédé conduit à une caractérisation très agréable des trois réseaux parfaits de dimension 5 :

(1) $\mathbb{A}_5$ comme réseau d'indice 1 ;
(2) $\mathbb{D}_5$ comme réseaux d'indice 2 et de 2-longueur 4 ;
(3) $\mathbb{A}_5^3$ comme réseaux d'indice 2 et de 2-longueur 5.

Appelons *rang de perfection d'un réseau* Λ la dimension r du sous-espace de $\mathrm{End}^s(E)$ engendré par les p_x, $x \in S(\Lambda)$. On a $s \geq r$, et $r \leq \frac{n(n+1)}{2}$, l'égalité caractérisant les réseaux parfaits. Voronoï (cf. [M], ch. VII, prop. 2.6) a montré comment on peut déformer un réseau de façon à augmenter l'ensemble S jusqu'à ce que l'on obtienne un réseau parfait. Un résultat plus précis ([M], ch. IX, th. 1.9, (4)) est que l'on peut n'augmenter r que d'une unité à chaque étape, la différence $s - r$ croissant au sens large avec r.

Il résulte donc du th. 1.3 que l'on a $s = r$ pour $n \leq 4$, sauf dans le cas du réseau $\mathbb{D}_4$ pour lequel $s - r = 2$, et du th. 1.2 qu'il en est de même pour $n = 5$, sauf dans le cas des réseaux ayant une section hyperplane de même norme semblable à $\mathbb{D}_4$; il résulte alors du th. 1.1 que l'on a encore $s - r = 2$, sauf dans le cas du réseau $\mathbb{D}_5$, pour lequel $s - r = 5$.

Ainsi, les "relations de perfections" en dimension $n \leq 5$ proviennent toutes de l'existence des réseaux parfaits $\mathbb{D}_4$ et $\mathbb{D}_5$. Cette propriété ne subsiste pas au-delà : on montre en effet que, en dimension 6, il existe des réseaux avec $s = 12$ et $r = 11$, évidemment non parfaits, que l'on peut construire par le procédé de Watson décrit au § 1 : pour des choix convenables des produits scalaires $e_i.e_j$, le réseau engendré par $e_1, \dots, e_6$ et $e = \frac{e_1 + \cdots + e_6}{3}$ possède les 12 couples $\pm e_i, \pm(e - e_i)$ de vecteurs minimaux, et on a alors $r = 11 < s = 12$ ([M1], prop.. 3.2 et appendice).

Signalons pour terminer une erreur qui s'est glissée dans [W] à propos de la dimension 6. En appliquant l'inégalité de Mordell à la valeur de γ_5 déduite de la classification des réseaux parfaits de dimension 5, on obtient $[\Lambda : \Lambda'] \leq 4$ pour $n = 6$, et l'on montre facilement (Watson) que l'égalité n'a lieu que pour $(\Lambda, \Lambda') \sim (\mathbb{D}_6, \mathbb{A}_1^{\perp 6})$ (avec Λ/Λ' de type $(2, 2)$). Pour l'indice 3, l'affirmation de Watson ([W], p. 63, *I could show...*) selon laquelle il existe deux classes d'isométrie de réseaux parfaits de dimension 6 et d'indice 3 n'est pas correcte : il y en a trois, à savoir, dans la terminologie de [C-S1],

$P_6^1 \sim \mathbb{E}_6$, $P_6^2 \sim \mathbb{E}_6^*$ et P_6^4. Cela peut être vérifié informatiquement (Batut) en utilisant la classification de Barnes des réseaux parfaits de dimension 6. J'ai écrit (respectant en cela la "philosophie de Watson") une démonstration directe et "self-contained" de la classification des réseaux parfaits d'indice 3 ou 4, qui occupe environ 9 pages, trop longue pour être publiée ici, et qui demanderait à être complétée par l'étude de l'indice 2 afin de conduire au théorème de classification de Barnes sans utiliser ses difficiles calculs fondés sur l'algorithme de Voronoï.

Bibliographie

[Bar] E.S. Barnes, *The complete enumeration of extreme senary forms.* Phil. Trans. Roy. Soc. London Ser. A **249** (1957), 461–506.

[Bl] H.F. Blichfeldt, *The minimum value of positive.* quadratic forms in six, seven and eight variables, Math. Z. **39** (1935), 1–15.

[Cas] J.W.S. Cassels, *An Introduction to the Geometry of Numbers.* Springer-Verlag, Grundlehren **99**, Heidelberg, (1959).

[C-S] J.H. Conway et N.J.A. Sloane, *Sphere Packings, Lattices and Groups.* Springer-Verlag, Grundlehren **290** (1988), Heidelberg (seconde édition : 1993).

[C-S1] J.H. Conway et N.J.A. Sloane, *Low-dimensional lattices. III. Perfect forms.* Proc. Royal Soc. London Ser. A **418** (1988), 43–80.

[Cox] H.S.M. Coxeter, *Extreme forms.* Canad. J. Math. **3** (1951), 391–441.

[K-Z1] A. Korkine et G. Zolotareff, *Sur les formes quadratiques positives quaternaires.* Math. Ann. **5** (1872), 581–583.

[K-Z2] A. Korkine et G. Zolotareff, *Sur les formes quadratiques.* Math. Ann. **6** (1873), 366–389.

[K-Z3] A. Korkine et G. Zolotareff, *Sur les formes quadratiques positives.* Math. Ann. **11** (1877), 242–292.

[M] J. Martinet, *Les réseaux parfaits des espaces euclidiens.* Masson, Paris, (1996).

[M1] J. Martinet, *Une famille de réseaux dual-extrêmes.* **9** (1997), 169–181.

[W] G.L. Watson, *On the minimum points of a positive quadratic form.* Mathematika **18** (1971), 60–70.

Jacques Martinet
Laboratoire A2X
C.N.R.S. - UPRES A5465
Institut Mathématiques Bordeaux
351 cours de la Libération
F-33405 Talence Cedex
E-mail : `martinet@math.u-bordeaux.fr`