# SUR L'INDICE D'UN SOUS-RÉSEAU

par Jacques MARTINET
(avec un appendice de Christian BATUT)

RÉSUMÉ. Nous étudions l'indice dans un réseau euclidien du sous-réseau engendré par ses minima successifs. Nous obtenons en particulier une classification complète de toutes les possibilités qui peuvent se présenter en dimension $n \leq 8$. Ce travail complète et précise sur divers points des travaux antérieurs de Watson, Ryškov et Zahareva.

ABSTRACT. English title: The index of a sublattice.
We study the index in a Euclidean lattice of the sublattice generated by its successive minima. We obtain in particular a complete classification of all the possibilities which may occur in dimensions $n \leq 8$. This work completes previous work by Watson, Ryškov, and Zahareva.

## INTRODUCTION

Soit $E$ un espace euclidien, de dimension $n$, et soit $\Lambda$ un réseau de $E$, c'est-à-dire un sous-groupe discret de rang $n$ de $E$. On note $x\,.\,y$ le produit scalaire de deux vecteurs $x, y \in E$, et l'on appelle *norme de $x$* le carré scalaire $N(x) = x\,.\,x$, carré de la norme au sens usuel $\|x\|$.

Considérons la suite croissante $m_1 \leq \cdots \leq m_n$ des nombres réels positifs tels que, pour $1 \leq k \leq n$, $m_k$ est le plus petit entier pour lequel l'ensemble des vecteurs de $\Lambda$ de norme $\leq m_k$ est de rang au moins $k$. Ce sont les *minima successifs*, ou *minima de $\Lambda$*.

Choisissons pour tout $k$ un vecteur $e_k$ avec $N(e_k) = m_k$. On obtient ainsi un sous-réseau $\Lambda'$ de $\Lambda$, et l'on s'intéresse aux valeurs que peuvent

Laboratoire A2X, UPRES A 5465 C.N.R.S. — Université Bordeaux 1

Mots-clés : *Réseaux euclidiens, vecteurs minimaux, minima successifs.*

prendre l'indice $[\Lambda : \Lambda']$, et, plus précisément, aux structures possibles du quotient $\Lambda/\Lambda'$.

Le travail fondateur est l'article [W] de Watson. Nous en rendons compte ici, tout en le précisant sur quelques points. Surtout, nous le présentons dans le langage géométrique des réseaux, mieux adapté aux questions d'indice que celui des formes quadratiques utilisé par Watson, dont la lecture est parfois difficile.

Ses travaux ont été ensuite poursuivis par des membres de l'école Russe, en particulier par Ryškov ([Ry], qui règle le cas des dimensions $n \leq 7$), puis par Zahareva ([Za]). Cette dernière a donné une classification des quotients possibles jusqu'à la dimension $8$, et introduit divers compléments théoriques utiles, dans un langage mixte formes quadratiques—réseaux. Nous préciserons le sens qu'il convient de donner à cette classification, et la relierons à la décomposition cellulaire de l'espace des formes quadratiques définies positives.

J'ai entrepris cette étude après avoir lu le travail de Watson, sans connaître l'existence des articles [Ry] et [Za]; la lecture de l'article [Ry] m'a suggéré que Ryškov a peut-être eu le même problème vis-à-vis de Watson.

Il m'a semblé opportun de mettre à la disposition de ceux qui s'intéressent à la géométrie des nombres une rédaction synthétique de cette théorie, écrite intégralement dans le langage des réseaux (le langage des formes quadratiques n'intervient qu'à propos de décomposition cellulaire), étendant certains des résultats des auteurs qui m'ont précédé, en particulier sur ce qui concerne la perfection d'une part, et les réalisations minimales (pour le "kissing number") de chacun des types au sens du § 7. En outre, nous corrigeons quelques erreurs. Par exemple, l'assertion de Watson sur les réseaux parfaits de dimension $6$ ([W], p. 63, I could show ... that there are exactly two $6$-dimensional perfect lattices with a possible index $3$) n'est pas correcte – il y a trois réseaux possibles. Cela a été vérifié informatiquement par Batut sur la classification de Barnes des réseaux parfaits; j'ai écrit une démonstration directe (disponible sur demande) de ce résultat, trop longue pour être reproduite ici.

Plus important, la classification de [Za] est incomplète en dimension $8$ : d'une part, au sens de sa classification (qui sera précisé au § 7), il manque trois classes – celles qui sont associées à un quotient de type $(4,2)$ ; d'autre part, sa démonstration de l'impossibilité des quotients cycliques d'ordre $8$ n'est pas correcte (un dénominateur $2$ se transforme en $4$ en cours de route). [J'ai appris de Ryškov lors du "Voronoï memorial" qui a eu lieu à

Kiev au mois de septembre 1998 que Mme Zahareva connaissait l'existence de certains "trous" dans ses démonstrations qui, à sa connaissance, n'ont jamais été comblés.]

Nous avons simplifié certaines démonstrations de [Za], rectifié les résultats incorrects, corrigé les démonstrations insuffisantes, et enfin complété sa classification à la lumière de la décomposition cellulaire de l'espace des formes quadratiques (ou des classes minimales de réseaux selon la terminologie de [M], chapitre IX).

L'énoncé suivant, dont une forme beaucoup plus précise dera donnée ultérieurement au cours des différents paragraphes et que l'on peut trouver résumé dans le tableau du §11, fournit un élément de classification pour les dimensions $n \le 8$ :

THÉORÈME. *La liste des structures possibles non triviales de* $\Lambda/\Lambda'$ *pour un couple* $(\Lambda, \Lambda')$ *formé d'un réseau* $\Lambda$ *de dimension* $n \le 8$ *et de l'un de ses sous-réseaux engendré par des vecteurs représentant ses minima successifs est contenue dans le tableau suivant:*

$n \ge 4$ : (2) ;

$n \ge 6$ : (3), (2, 2) ;

$n \ge 7$ : (4), (2, 2, 2) ;

$n \ge 8$ : (5), (6), (4, 2), (3, 3), (2, 2, 2, 2) .

*Toutes ces structures sont réalisables en prenant pour* $\Lambda$ *l'un des réseaux de racines* $\mathbb{D}_4$ , $\mathbb{D}_5$ , $\mathbb{D}_6$ , $\mathbb{E}_6$ , $\mathbb{E}_7$ *ou* $\mathbb{E}_8$ . *En outre, pour* $n = 4,\ 6,\ 7,\ 8$, *on a* $[\Lambda : \Lambda'] \le 1,\ 3,\ 4,\ 8$ *respectivement sauf si* $\Lambda$ *est l'un des réseaux* $\mathbb{D}_4$ , $\mathbb{D}_6$ , $\mathbb{E}_7$ *ou* $\mathbb{E}_8$ .

Nous rappelons au §1 le théorème de Minkowski sur les minima successifs (théorème 1.3) et en donnons une version "locale" (théorème 1.4), fondamentale pour la suite, montrant, à l'aide de déformations, que l'on peut se ramener au cas des réseaux dont les minima successifs sont égaux. De ce fait, cette théorie de l'indice peut être faite en se limitant aux réseaux possédant $n$ vecteurs minimaux indépendants, propriété notée (WR) dans la suite (*well rounded lattices* dans la terminologie de Ash et McConnell).

Nous donnons au §2 (avec quelques compléments) les inégalités fondamentales de Watson, et expliquons au §3 ses principes généraux. Ces principes sont appliqués au §4 à l'étude des quotients 2-élémentaires (qui se ramène à la théorie des codes binaires) et au §5 à la description des indices possibles en dimension 6 et 7. On s'occupe des réseaux de racines au § 6, puis on revient aux §§ 7 et 8 à des questions plus théoriques liées à la décomposition cellulaire de l'espace des formes quadratiques définies positives. La description de toutes les possibilités en dimension 8 est complétée au § 9, consacré aux quotients cycliques qui n'existent pas en dimension inférieure, et au § 10, où l'on s'occupe de quotients non cycliques.

Nous avons regroupé au § 11 les principaux résultats obtenus au cours des 10 paragraphes précédents, sous forme d'un tableau analogue à la table 1 de [Za]. Outre les corrections, notre tableau diffère de celui de [Za] par la présence de l'indication du minimum de l'invariant $s(\Lambda)$ (nombre de couples de vecteurs minimaux de $\Lambda$), et des invariants $r(\Lambda)$ et $s(\Lambda')$ correspondants ($r$ désigne le rang de perfection, dont la définition est rappelée au § 1; dans tous les cas rencontrés dans cette étude, $r(\Lambda')$ et $s(\Lambda')$ coïncident). Le fait que l'on puisse avoir $s(\Lambda) = n$ (ou $r(\Lambda) = n$, cela revient au même) figure dans la table de [Za] (mention *free*, et mention *not* dans le cas contraire).

Une étude complète de la dimension 9 nécessiterait un travail considérable, et n'est guère envisageable sans utilisation systématique par voie informatique d'algorithmes de programmation linéaire. Nous ne l'avons pas entreprise. Signalons seulement l'article [M1] dans lequel est étudié en vue d'application à la notion de *réseau dual-extrême* une famille d'indice $d$ et de dimension $n = 2d$ pour tout $d \geq 3$.

Un appendice de Christian Batut présente quelques uns des résultats qu'il a obtenus à l'aide d'un programme écrit en langage $C$.

À des modifications mineures près, cet article est la version disponible depuis novembre 1998 sur ma page WEB, forme révisée d'une version préliminaire de mai 1997.

## 1. Les minima successifs

On rappelle que $E$ désigne un espace euclidien de dimension $n$ et $\Lambda$ un réseau de $E$, dont on note $m_1(\Lambda), \dots, m_n(\Lambda)$ les minima successifs, définis en début d'introduction.

La *norme* ou *minimum de* $\Lambda$ est le premier minimum $m_1$, le plus souvent noté $N(\Lambda)$. La *sphère de* $\Lambda$ est $S(\Lambda) = \{x \in \Lambda \mid N(x) = N(\Lambda)\}$. On pose $s(\Lambda) = \frac{1}{2}|S(\Lambda)|$ ($2s$ est le *kissing number de* $\Lambda$); on écrit souvent $S$ et $s$ au lieu de $S(\Lambda)$ et $s(\Lambda)$.

La *matrice de Gram d'une base* $\mathcal{B} = (e_1, \dots, e_n)$ *de* $E$ est $\mathrm{Gram}(\mathcal{B}) = (e_i \,.\, e_j)$. Le *déterminant* $\det(\Lambda)$ *de* $\Lambda$ est le déterminant de la matrice de Gram de l'une de ses bases, et son *invariant d'Hermite* est $\gamma(\Lambda) = \dfrac{N(\Lambda)}{\det(\Lambda)^{1/n}}$. C'est un invariant de similitude. La *constante d'Hermite pour la dimension* $n$ est $\gamma_n = \sup_{\dim \Lambda = n} \gamma(\Lambda)$. Son existence résulte de majorations de l'invariant $\gamma$, par exemple de celle de Minkowski, qui consiste à majorer par $1$ la densité de l'empilement de sphères associé au réseau. Les valeurs de $\gamma_n$ sont connues jusqu'à la dimension $8$ ; elles sont reproduites par exemple dans [M], chapitre XIV, tableau 4.1 (et sous d'autres formes dans [C-S] et dans [Cas]).

Il est utile de connaître la majoration de $\gamma_n$ découverte par Korkine et Zolotareff pour la dimension $4$, et démontrée en toute dimension par Mordell (la démonstration, très courte, peut être lue dans [Cas], ch. X, §3) :

$$\forall\, n \geq 3\,,\ \gamma_n \leq \gamma_{n-1}^{(n-1)/(n-2)}\,, \tag{1.1}$$

qui permet par récurrence à partir du cas $n = 2$ de retrouver l'inégalité d'Hermite

$$\gamma_n \leq (\frac{4}{3})^{(n-1)/2}\,. \tag{1.2}$$

Vu la difficulté que présentent le calcul de $\gamma_6$ et $\gamma_7$ et la détermination des réseaux critiques correspondants, et afin de préserver la possibilité d'en obtenir des démonstrations simplifiées en utilisant les résultats de cet article, nous adopterons la "philosophie de Watson", consistant à ne pas utiliser les valeurs précises de $\gamma_6$ et de $\gamma_7$, mais seulement les majorations qui se déduisent de l'égalité $\gamma_5 = 2^{3/5}$, due à Korkine et Zolotareff. (En déduire les résultats analogues pour la dimension $8$ est en revanche assez simple, cf. [M], ch. VI, §6, où est reproduite une démonstration due à Anne-Marie Bergé ; pour la dimension $5$, voir [M2].)

Nous allons maintenant énoncer deux théorèmes, le premier dû à Minkowski, permettant de majorer les produit des minima successifs et de préciser les réseaux sur lesquels une fonction qui leur est liée (notée $\Phi$ ci-dessous) atteint un maximum relatif. Le premier théorème est énoncé et démontré dans [M], chapitre II (théorème 6.8) ; la démonstration de [M], fondée sur un argument de déformation, prouve en fait le second théorème, dont le premier se déduit très facilement. Avant de les énoncer, introduisons sur l'espace des réseaux la fonction

$$\Phi(\Lambda) = \frac{m_1(\Lambda)\dots m_n(\Lambda)}{\det(\Lambda)}\,,$$

et rappelons qu'un réseau réseau $\Lambda$ est dit *extrême* s'il réalise un maximum local de l'invariant d'Hermite. Il est alors *strictement extrême*, en ce sens que ce maximum est strict modulo similitudes, et il vérifie la condition (WR) (pour *well rounded*), cf. [M], ch. III, §4, que nous rappelons cidessous :

(WR) *$\Lambda$ possède $n$ vecteurs minimaux indépendants.*

[Cette notion est très utile, en particulier parce que l'espace des réseaux "well rounded" modulo homothéties est compact.]

THÉORÈME 1.3. (Minkowski). *Quel que soit $\Lambda$, on a $\Phi(\Lambda) \le \gamma_n^n$.*

THÉORÈME 1.4. *Les réseaux sur lesquels la fonction $\Phi$ atteint un maximum local sont les réseaux extrêmes, et ce maximum est un maximum strict sur les classes de similitude de réseaux.*

*Indication sur les démonstration des théorèmes 1.3 et 1.4.* Nous donnons seulement le principe de la démonstration utilisé dans [M] pour démontrer le théorème de Minkowski, de façon à permettre au lecteur de s'assurer que la démonstration de [M] prouve effectivement l'énoncé 1.4. Considérons un réseau $\Lambda$ dont les minima successifs ne sont pas tous égaux, et soit $k$ un indice pour lequel on a $m_k(\Lambda) < m_{k+1}(\Lambda)$. On montre que l'on peut déformer $\Lambda$ de façon à augmenter strictement $\Phi(\Lambda)$ et à diminuer strictement le rapport $m_k(\Lambda)/m_{k+1}(\Lambda)$. Par passage à la limite, on construit ainsi un réseau $\Lambda'$ pour lequel on a $\Phi(\Lambda') > \Phi(\Lambda)$ et $m_k(\Lambda) = m_{k+1}(\Lambda)$, diminuant par ce procédé le nombre de minima distincts du réseau de départ. En itérant, on construit finalement un réseau $L$ avec $\Phi(L) > \Phi(\Lambda)$ et $m_1(L) = \cdots = m_n(L)$. Cela prouve que les maxima locaux de la fonction $\Phi$ sont les mêmes que ceux de l'invariant $\gamma$, donc qu'ils sont stricts modulo similitude et atteints exactement sur les réseaux extrêmes. Le théorème 1.4 en résulte, et le théorème 1.3 s'en déduit, vu que l'on a $\gamma(L) \le \gamma_n$ par définition de $\gamma_n$. $\square$

Venons-en maintenant à l'étude des quotients $\Lambda/\Lambda'$ d'un réseau $\Lambda$ par un sous-réseau $\Lambda'$ engendré par des vecteurs qui représentent les minima successifs de $\Lambda$. La notion de réseau extrême s'avérant trop restrictive, nous rappelons d'abord quelques résultats concernant des notions voisines.

Voronoï a caractérisé les réseaux extrêmes comme étant les réseaux qui sont à la fois *parfaits* et *eutactiques*. Ces notions sont étudiées en détail dans [M], ch. III, §§2 et 4; le théorème de Voronoï est le théorème 4.6. Voici des définitions géométriques de ces notions: le *rang de perfection d'un réseau* $\Lambda$ est la dimension du sous-espace de l'espace $\mathrm{End}^s(E)$ des endomorphismes symétriques de $E$ engendré par les projections orthogonales $p_x$ sur les droites portées par les vecteurs minimaux $x$ de $\Lambda$. On dit qu'un réseau $\Lambda$ est *parfait* si son rang de perfection est maximum (i.e., égale à la dimension $\frac{n(n+1)}{2}$ de $\mathrm{End}^s(E)$, autrement dit, si les $p_x$, $x \in S(\Lambda)$ engendrent $\mathrm{End}^s(E)$), et qu'il est *eutactique* s'il existe une relation $\mathrm{Id}_E = \sum_{x \in S(\Lambda)/\{\pm 1\}} \rho_x p_x$ à coefficients $\rho_x$ strictement positifs. Les réseaux parfaits et les réseaux eutactiques vérifient la propriété (WR). En outre, dans une dimension donnée, les classes de similitude de réseaux parfaits ou eutactiques sont en nombre fini.

On peut caractériser les réseaux parfaits par la propriété suivante: il existe un voisinage $\mathcal{V}$ de l'identité dans $\mathrm{End}(E)$ tel que, pour tout $u \in \mathcal{V}$ qui n'est pas une similitude, $u(\Lambda)$ possède moins de vecteurs minimaux que $\Lambda$. *A contrario*, un procédé de Voronoï permet de "perfectionner" un réseau non parfait en le déformant au moyen de transformations $u \in \mathrm{GL}(E)$, tout en conservant l'égalité $u(S(\Lambda)) = S(u(\Lambda))$ au cours des transformations, cf. [M], ch. VII, proposition 2.6.

Les déformations qui interviennent dans les démonstrations des théorèmes 1.3 et 1.4 ainsi que dans le processus de perfectionnement ci-dessus, du fait qu'il s'agit de transformations continues, conservent la classe d'isomorphisme de $\Lambda/\Lambda'$, et permettent donc de construire un couple $(L, L')$ de réseaux avec $L/L' \simeq \Lambda/\Lambda'$ tel que $L$ soit parfait. On en déduit:

THÉORÈME 1.5. *Soit $A$ un groupe abélien fini. S'il existe un couple $(\Lambda, \Lambda')$ d'un réseau $\Lambda$ et d'un sous-réseau $\Lambda'$ de $\Lambda$ ayant une base formée de vecteurs représentant les minima successifs de $\Lambda$ et tel que $\Lambda/\Lambda'$ soit isomorphe à $A$, il existe un couple $(L, L')$ possédant les mêmes propriétés, et tel que $L$ soit parfait.*
[ Noter que, puisque $A$ est fini, $\Lambda'$ et $L'$ vérifient la condition (WR).] □

[En revanche, les transformations qu'il faudrait utiliser pour transformer ensuite $L$ en un réseaux extrême peuvent ne pas conserver l'ensemble des vecteurs minimaux de $L$ (la perfection est une propriété d'algèbre linéaire, alors que l'eutaxie fait intervenir une propriété de convexité). La question de savoir si l'on peut remplacer “parfait” par “extrême” dans cet énoncé est ouverte. Il n'y a aucune raison pour qu'il en soit ainsi. Toutefois, nous verrons en classant les indices possibles que c'est le cas dans toutes les dimensions $n \leq 8$.]

Nous allons maintenant donner une majoration de l'indice $[\Lambda : \Lambda']$. Nous aurons besoin de l'inégalité de Hadamard, dont la démonstration ne présente aucune difficulté, et dont nous rappelons ci-dessous l'énoncé (le déterminant est relatif à une base orthonormée) :

LEMME 1.6 (Inégalité de Hadamard). *Quels que soient les vecteurs $e_1, \dots, e_n$ de $E$, on a la majoration $|\det(e_1, \dots, e_n)| \leq \|e_1\| \dots \|e_n\|$, et l'égalité a lieu si et seulement si les vecteurs $e_i$ sont deux à deux orthogonaux ou si l'un d'eux est nul.* □

THÉORÈME 1.7. *Avec les notation du théorème 1.5, on a*

$$[\Lambda : \Lambda'] \leq \gamma_n^{n/2}.$$

*Démonstration.* Le calcul de l'indice se fait au moyen d'un calcul de déterminants, grâce à la formule $\det(\Lambda') = \det(\Lambda)\,[\Lambda : \Lambda']^2$. En appliquant le théorème 1.5, on se ramène au cas où $\Lambda'$ est engendré par $n$ vecteurs de $S(\Lambda)$. En outre, quitte à remplacer $\Lambda$ par un réseau proportionnel, on peut le supposer de norme $1$. On a l'inégalité $\det(\Lambda') \leq 1$ par 1.4 ainsi que l'égalité $\det(\Lambda) = \gamma(\Lambda)^{-n}$ provenant de la définition même de l'invariant d'Hermite, et donc

$$\frac{\det(\Lambda')}{\det(\Lambda)} \leq \gamma(\Lambda)^n \leq \gamma_n^n. \qquad \square$$

REMARQUE 1.8. Nous verrons que l'inégalité $[\Lambda : \Lambda'] \leq \lfloor \gamma_n^{n/2} \rfloor$ est optimale jusqu'à la dimension $8$. Il n'y a aucune raison pour qu'il en soit toujours ainsi au-delà. Probablement, l'inégalité est stricte en dimension $9$.

## 2. INÉGALITÉS DE BASE

À partir de ce §, et sauf mention expresse du contraire, on ne s'occupe que de réseaux vérifiant la condition (WR). On considère un couple de réseaux $\Lambda$ et $\Lambda' \subset \Lambda$ de même norme. Pour étudier les structures possibles des quotients $\Lambda/\Lambda'$, on commence par examiner le cas crucial d'un quotient cyclique d'ordre $d > 1$, en suivant l'étude faite par Watson dans [W2].

On considère ainsi $n$ vecteurs $e_1, \dots, e_n$ indépendants de même norme de $E$. On note $\Lambda'$ le réseau qu'ils engendrent, et l'on suppose que $\Lambda$ est engendré sur $\Lambda'$ par un vecteur

$$e = \frac{a_1 e_1 + \cdots + a_n e_n}{d}$$

où les $a_i$ sont des entiers, que l'on peut supposer premiers entre eux dans leur ensemble, condition qui assure que l'indice $[\Lambda : \Lambda']$ n'est pas un diviseur strict de $d$.

LEMME 2.1. *Désignons par* $\operatorname{sgn}(x)$ *le signe du nombre réel* $x$ *(*$0$ *si* $x = 0$*). Alors, on a*

$$\Big(\big(\sum_{i=1}^{n} |a_i|\big) - 2d\Big) N(e) = \sum_{i=1}^{n} |a_i| \big(N(e - \operatorname{sgn}(a_i) e_i) - N(e_i)\big)\,.$$

*Démonstration.* Quitte à remplacer $e_i$ par $-e_i$ lorsque $a_i$ est négatif, on peut supposer tous les $a_i \geq 0$. On a $N(e - e_i) - N(e_i) = N(e) - 2e \,.\, e_i$. En multipliant les deux membre de cette identité par $a_i$ et en ajoutant, on obtient tout de suite l'égalité de l'énoncé. $\square$

THÉORÈME 2.2. (Watson). *Avec les notations ci-dessus, on a*

$$\sum_{i-1}^{n} |a_i| \geq 2d\,,$$

*et l'égalité a lieu si et seulement si* $e - \operatorname{sgn}(a_i) e_i$ *est minimal pour tout indice* $i$ *avec* $a_i \neq 0$.

*De plus, si l'un au moins des* $a_j$ *est égal à* $\frac{d}{2}$*, alors* $e$ *et tous les vecteurs déduits de* $e$ *ou d'un vecteur* $e - e_i$ *avec* $a_i \neq \frac{d}{2}$ *en remplaçant par leurs opposés certains des vecteurs* $e_j$ *avec* $a_j = \frac{d}{2}$ *sont aussi minimaux.*

*Démonstration.* L'inégalité et la caractérisation des cas d'égalité sont des conséquences immédiates du lemme 2.1.

Prouvons la dernière assertion. Si, par exemple, on a $a_n = \frac{d}{2}$, on peut appliquer le lemme en remplaçant $e$ par $e' = e - e_n$, ce qui revient à changer le signe de $e_n$. $\square$

Le résultat suivant s'applique en particulier au cas où il y a égalité dans le théorème 2.2, cas qui présente une grande importance pratique.

PROPOSITION 2.3.

(1) *Si les vecteurs* $e - e_i$ *et* $e - e_j$ $(j \neq i)$ *sont minimaux, on a* $e_i \,.\, e_j \geq 0$, *et ce produit scalaire est nul si et seulement si* $e$ *et* $e - e_i - e_j$ *sont minimaux. Dans ces conditions, les* 6 *vecteurs* $e, e_i, e_j, e - e_i, e - e_j, e - e_i - e_j$ *et leurs opposés constituent une configuration semblable à celle de* $S(\mathbb{A}_3)$.

(2) *Si les vecteurs* $e - e_i$, $e - e_j$ *et* $e - e_k$ $(i, j, k$ *distincts) sont minimaux, le vecteur* $e - e_i - e_j - e_k$ *est minimal si et seulement si les trois vecteurs* $e - e_i - e_j$, $e - e_i - e_k$ *et* $e - e_j - e_k$ *le sont. Dans ces conditions, les* 12 *vecteurs* $e, e_i, e_j, e_k, e - e_i, e - e_j, e - e_k, e - e_i - e_j, e - e_i - e_k, e - e_j - e_k, e - e_i - e_j - e_k, 2e - e_i - e_j - e_k$ *et leurs opposés constituent une configuration semblable à celle de* $S(\mathbb{D}_4)$. *En particulier,* 10 *quelconques d'entre eux forment une famille de rang de perfection* 10.

*Démonstration.* On utilise les identités

$$N(e) + N(e - e_i - e_j) - N(e - e_i) - N(e - e_j) = 2e_i \,.\, e_j \tag{2.4}$$

et

$$\begin{aligned} &N(e) + N(e - e_i - e_j) + N(e - e_i - e_k) + N(e - e_j - e_k) = \\ &N(e - e_i) + N(e - e_j) + N(e - e_k) + N(e - e_i - e_j - e_k), \end{aligned} \tag{2.5}$$

ainsi que le fait que, en dimension 3 (resp. 4), l'inégalité $s \geq 6$ (resp. $s \geq 11$) caractérise le réseau $\mathbb{A}_3$ (resp. $\mathbb{D}_4$). $\square$

[Le fait que l'inégalité $s \geq \frac{n(n+1)}{2}$ caractérise les réseaux parfaits en dimension $n \leq 4$, qui peut être extrait des travaux de Korkine et Zolotarev, est démontré dans [M], ch. VI, théorème 2.1. Une preuve directe du fait qu'il s'agit ici de l'un des réseaux $\mathbb{A}_3$ ou $\mathbb{D}_4$ peut s'obtenir en construisant les matrices de Gram correspondantes.]

Les résultats précédents ne disent rien sur la norme de $e$ lui-même. La proposition suivante donne quelques indications sur des cas où $e$ est minimal. (En général, il ne l'est pas.) Pour alléger les notations, nous supposons que $\Lambda$ *est de norme* 1.

PROPOSITION 2.6. *Supposons vérifiée la condition $\sum_i a_i = 2d$, avec des coefficients $a_i > 0$. Alors, la valeur des produits scalaires $e\,.\,e_i$ ne dépend pas du choix de $i$. On a $e\,.\,e_i \geq \frac{1}{2}$, et l'égalité a lieu si et seulement si $e$ est minimal. En outre, cette dernière condition est vérifiée chaque fois qu'il existe un indice $i$ avec $a_i = \frac{d}{2}$.*

*Démonstration.* La relation $N(e) - N(e-e_i) = 2e\,.\,e_i - 1$ montre que, lorsque les vecteurs $e - e_i$ sont minimaux, on a $e\,.\,e_i = \frac{1}{2}N(e)$, si bien que les produits scalaires $e\,.\,e_i$ ne dépendent pas de $i$ et valent au moins $\frac{1}{2}$, avec égalité si et seulement si $e$ est minimal. La dernière assertion de la proposition est contenue dans le théorème 2.2. $\square$

## 3. COMPLÉMENTS SUR LES QUOTIENTS CYCLIQUES

On conserve les notations du §2 : on a $\Lambda = \langle \Lambda', e\rangle$ avec $\Lambda' = \langle e_1, \dots, e_n\rangle$ et $e = \frac{a_1 e_1 + \cdots + a_n e_n}{d}$. Nous expliquons certaines techniques de Watson que nous utiliserons plus loin.

En ajoutant à $e$ des multiples convenables des $e_i$, on peut supposer que l'on a $-\frac{d}{2} < a_i \leq \frac{d}{2}$ pour tout $i$, et même, quitte à remplacer certains vecteurs $e_i$ par leurs opposés, que l'on a $0 \leq a_i \leq \frac{d}{2}$. Notons $m$ le nombre de coefficients $a_i$ non nuls. Quitte à permuter les vecteurs $e_i$, on peut supposer que l'on a

$$(3.1) \qquad 1 \leq a_1 \leq \cdots \leq a_m \leq \left\lfloor \frac{d}{2} \right\rfloor \quad \text{et} \quad a_i = 0 \quad \text{pour } m+1 \leq i \leq n\,,$$

*conditions que l'on suppose systématiquement satisfaites dans la suite.*

Posons $t = \lfloor \frac{d}{2} \rfloor$, et, pour $1 \leq k \leq t$, soit

$$m_k = |\{i \mid a_i = k\}|\,.$$

Les conventions de 3.1 et le théorème 2.2 se traduisent par les conditions

$$(3.2) \quad m_1 + m_2 + \cdots + m_t = m \leq n \quad \text{et} \quad m_1 + 2m_2 + \cdots + tm_t \geq 2d\,.$$

Pour tout entier $a$ premier à $d$, on a aussi $\Lambda = \langle \Lambda', ae\rangle$. On en déduit une opération du groupe $(\mathbb{Z}/d\mathbb{Z})^\times/\{\pm 1\}$ sur les suites $a_1, \dots, a_n$ et donc aussi sur les suites $(m_1, \dots, m_t)$ susceptibles de définir $\Lambda$ comme extension de $\Lambda'$, opération qui permute entre eux les indices $k$ ayant avec $d$ un P.G.C.D. donné. Explicitement, l'opération s'obtient de la façon suivante : pour $a \in \mathbb{Z}$ premier à $d$, on remplace le coefficient $a\,a_i$ qui apparaît au numérateur de $a\,e$ par l'unique reste modulo $d$ de $\pm a\,a_i$ qui appartient à l'intervalle $[0,t]$. L'appartenance à une même orbite pour cette opération sera notée

$$(m_1,\dots,m_t)\sim(m'_1,\dots,m'_t)\,.$$

En pratique, on cherchera à minimiser la somme $\sigma=\sum_{k=1}^t km_k$ avant d'appliquer 3.2.

Exemple 3.3. Soit $n=8$, $d=5$, et $e=\dfrac{e_1+\cdots+e_6+2e_7+2e_8}{2}$. On peut représenter $(\mathbb{Z}/5\mathbb{Z})^\times/\{\pm1\}$ par les entiers $1$ et $2$. On a

$$2e-e_7-e_8=\frac{2e_1+\cdots+2e_6-e_7-e_8}{2}\,.$$

En remplaçant $e_7,e_8$ par leurs opposés $e'_7,e'_8$, on obtient

$$2e-e_7-e_8=\frac{e'_7+e'_8+2e_1+\cdots+2e_6}{2}\,,$$

expression qui montre l'équivalence $(6,2)\sim(2,6)$. Bien entendu, les opérations de $a$ et de $d-a\equiv a \mod d$ consuisent au même résultat.

À l'opposé, pour tout diviseur $d'$ de $d$, soit $\Lambda_1=\langle\Lambda',d'e\rangle$. On peut appliquer les remarques précédentes au couple $(\Lambda_1,\Lambda')$, pour lequel le quotient $\Lambda_1/\Lambda'$ est cyclique d'ordre $\frac{d}{d'}$.

Soit maintenant $e'=\dfrac{b_1e_1+\cdots+b_me_m}{d}$ un vecteur minimal de $\Lambda$, et supposons les $b_j$ premiers entre eux. Soit $i\le m$ un indice, et soit $\Lambda'_i$ le réseau de base $(e',e_1,\dots,e_{i-1},e_{i+1},\dots,e_n)$. On a $\Lambda=\langle\Lambda'_i,-e_i\rangle$ et

$$-e_i=\frac{-de'+b_1e_1+\cdots+b_{i-1}e_{i-1}+b_{i+1}e_{i+1}+b_me_m}{b_i}\,, \tag{3.4}$$

ce qui met en évidence un couple $(\Lambda,\Lambda'_1)$ à quotient cyclique d'ordre $|b_i|$. (Noter que la congruence $b_i\equiv a_i \mod d$ montre que $b_i$ n'est pas nul.)

Appliqué à $e-e_i$ supposé minimal, la formule 3.4 prend la forme explicite

$$e_i=\frac{-d(e-e_i)+\sum_{j\ne i}a_je_j}{d-a_i}\,. \tag{3.5}$$

Voici deux applications de ces remarques :

- En majorant pour un entier $m$ donné les dénominateurs possibles dans l'écriture de $e$, on obtient une majoration efficace des coefficients $b_i$

provenant d'un vecteur minimal; on peut en particulier appliquer la majoration donnée par le théorème 1.7.

• Lorsqu'il y a égalité dans l'inégalité du théorème 2.2, les vecteurs $e-e_i$ sont minimaux. On en déduit que les coefficients $a_i$ apparaissent comme indices de sous-réseaux engendrés par $n$ vecteurs minimaux (y compris l'indice 1 si $a_1=1$, ce qui signifie simplement que $\Lambda$ possède une base de vecteurs minimaux).

EXEMPLE 3.6. Illustrons ce qui précède par l'exemple de la dimension 6 avec l'indice 3. On peut prendre les $a_i$ égaux à 0 ou 1, et, par 3.2 (ou par 2.2), on a nécessairement $m=n=6$ et $a_i=1$ pour tout $i$. La majoration du théorème 1.7 ($[\Lambda:\Lambda'] \le \gamma_6^3 < 5$) montre que les coefficients $b_i$ d'un vecteur minimal $e'$ de $\Lambda \smallsetminus \Lambda'$ ne peuvent pas dépasser 4 (nombre que l'on peut même exclure, cf. *infra*, théorème 5.2). Par ailleurs, comme il y a égalité dans 2.2, on voit que, lorsque l'indice $[\Lambda:\Lambda']=3$ est possible pour un réseau $\Lambda$ de dimension 6, les indices 2 et 1 sont aussi possibles.

## 4. LES QUOTIENTS 2-ÉLÉMENTAIRES

On conserve les notations du § 1. On suppose que $\Lambda/\Lambda'$ est un 2-groupe abélien élémentaire d'ordre $2^r$. Pour faire les calculs, on normalise $\Lambda$ à la norme 1. On commence par le cas $r=1$, ce qui rend compte de l'unique indice non trivial possible en dimension 5.

PROPOSITION 4.1. *Si $[\Lambda:\Lambda']=2$, on a $n\ge 4$, et l'égalité a lieu si et seulement si $(\Lambda,\Lambda')$ est semblable à $(\mathbb{D}_4, \mathbb{A}_1^{\perp 4})$.*

*Démonstration.* Il résulte du théorème 2.2 que l'on a $n \ge 4$, et qu'il ne peut y avoir égalité que si tous les vecteurs $\dfrac{\pm e_1 \pm e_2 \pm e_3 \pm e_4}{2}$ sont minimaux. La proposition 2.3 entraîne alors que les produits scalaires $e_i \,.\, e_j$ ($j \ne i$) sont tous nuls, si bien que $\Lambda'$ (resp. $\Lambda$) est un réseau cubique (resp. un réseau cubique centré, semblable à $\mathbb{D}_4$). □

REMARQUE 4.2. La majoration $\gamma_5^{5/2} < 3$ montre que, en dimension 5, l'indice $\Lambda/\Lambda'$ ne dépasse pas 2, et qu'il est égal à 2 si et seulement si l'une des conditions suivantes est vérifiée :

• ou bien $(\Lambda,\Lambda') \sim (\mathbb{D}_4 \bigoplus \mathbb{A}_1, \mathbb{A}_1^{\perp 4} \bigoplus \mathbb{A}_1)$ ;

• ou bien $\Lambda$ n'a pas de section de même norme semblable à $\mathbb{D}_4$, et est de la forme $\langle \Lambda', \frac{e_1+e_2+e_3+e_4+e_5}{2}\rangle$, les $e_i$ étant des vecteurs minimaux de $\Lambda$ constituant une base de $\Lambda'$.

Supposons maintenant l'indice au moins égal à $4$. En utilisant ce que l'on sait du cas $d=2$ et quelques résultats faciles de théorie des codes, on obtient le résultat suivant concernant les dimensions $6$, $7$ et $8$ :

THÉORÈME 4.3. *Supposons que $\Lambda/\Lambda'$ soit $2$-élémentaire d'ordre $2^r$. Alors, si $r=2$ (resp. $r=3$, resp. $r=4$), on a $n\ge 6$ (resp. $n\ge 7$, resp. $n\ge 8$), et l'égalité a lieu si et seulement si le couple $(\Lambda,\Lambda')$ est semblable à $(\mathbb{D}_6, \mathbb{A}_1^{\perp 6})$ (resp. à $(\mathbb{E}_7, \mathbb{A}_1^{\perp 7})$, resp. à $(\mathbb{E}_8, \mathbb{A}_1^{\perp 8})$).*

*Démonstration.* On obtient $\Lambda$ à partir de $\Lambda'$ par adjonction de $r$ vecteurs convenables de la forme $\dfrac{a_1e_1+a_2e_2+\cdots+a_ne_n}{2}$, avec $a_i\in\{0,1\}$. Considérés comme vecteurs de $\mathbb{F}_2^n$, ces suites $(a_1,a_2,\dots,a_n)$ définissent un code binaire de longueur $n$ qui, par hypothèse, est de dimension $r=\dim_{\mathbb{F}_2}\Lambda/\Lambda'$. La proposition 2 montre que ce code doit être de poids au moins 4. Or, il est bien connu, et facile à vérifier, que, pour $r=2$ (resp. $r=3$, resp. $r=4$), de tels codes n'existent que si l'on a $n\ge 6$ (resp. $n\ge 7$, resp. $n\ge 8$), et que, lorsqu'il y a égalité, les codes sont isomorphes aux sections de longueurs $6,7,8$ du *code de Hamming étendu*, de matrice génératrice

$$\begin{pmatrix} 1&1&1&1&0&0&0&0\\ 0&0&1&1&1&1&0&0\\ 1&0&1&0&1&0&1&0\\ 0&0&0&0&1&1&1&1 \end{pmatrix}.$$

Les réseaux obtenus en relevant ces codes, après homothéties de rapport $\sqrt{2}$, sont visiblement engendrés par des vecteurs de norme $2$. Ce sont donc des réseaux de racines qui, vu leurs déterminants ($4$, $2$ et $1$), s'identifient à $\mathbb{D}_6$, $\mathbb{E}_7$ et $\mathbb{E}_8$ respectivement. $\square$

En longueur $7$, il existe trois autres codes de poids $w\ge 4$. Ils sont de dimension $2$ et de poids $4$, les poids des mots non nuls étant respectivement $(4^4)$ (provenant de la dimension $6$), $(4^2,6)$ et $(4,5^2)$. Les réseaux correspondants contiennent donc tous une section $\mathbb{D}_4$, avec $s\ge 31$, $s\ge 22$ et $s\ge 14$ respectivement.

En longueur $8$, on trouve un unique code de poids $w>4$ ; son système de poids est $(5^2,6)$, et les réseaux associés sont de la forme $\langle\Lambda',e,e'\rangle$ avec

$$e = \frac{e_1 + e_2 + e_3 + e_4 + e_5}{2} \quad \text{et} \quad e' = \frac{e_4 + e_5 + e_6 + e_7 + e_8}{2}\,.$$

Lorsque l'on prend les $e_i$ deux à deux orthogonaux, on obtient un réseau avec $s = 8$.

Une vérification facile, mais un peu fastidieuse, montre que les autres codes de longueur $8$ sont de poids $4$ et de dimension $2$ ($4$ codes) ou $3$ ($3$ codes). Leurs systèmes de poids non nuls sont $(4^2, 8)$, $(4, 6^2)$, $(4, 5, 7)$ et $(5^2, 6)$ dans le premier cas, $(4^6, 8)$, $(4^5, 6^2)$ et $(4^3, 5^4)$ dans le second cas.

On montre de même que les codes de dimension $5$ et de poids $w \geq 4$ n'existent qu'à partir de la longueur $10$. Donc, en dimension $9$, un quotient $2$-élémentaire est d'ordre au plus $16$, comme en dimension $8$. En dimension $10$, le couple $(\mathbb{D}_{10}^+, \mathbb{A}_1{}^{10})$ est à quotient $2$-élémentaire d'ordre $32$ ; ce n'est pas le seul. (Pour $n \geq 8$ pair, on pose $\mathbb{D}_n^+ = \mathbb{D}_n \cup \left(\frac{1}{2}(1, \dots, 1) + \mathbb{D}_n\right)$ ; c'est un réseau de minimum $2$, égal à $\mathbb{E}_8$ lorsque $n = 8$, cf. §6.)

## 5. Quotients cycliques d'ordre 4 en dimension 6 et 7

Dans ce §, dans lequel on conserve les notations générales des §§2 et 3, on écrit $\Lambda = \langle \Lambda', e \rangle$ et

$$e = \frac{e_1 + \cdots + e_p + 2e_{p+1} + \cdots + 2e_{p+q}}{4} = \frac{e' + e_{p+1} + \cdots + e_{p+q}}{2}$$
$$\text{avec} \;\; e' = \frac{e_1 + \cdots + e_p}{2}\,.$$

Proposition 5.1. *Avec les notations ci-dessus, les entiers $p$ et $q$ vérifient les conditions $7 \leq p + q = m \leq n$, $p \geq 4$, $q \geq 3$ si $p = 4$, et $p \in \{4, 5, 6\}$ si $m = 7$.*

*Démonstration.* On a $e' \in \Lambda$, donc $p \geq 4$ (proposition 4.1). Si $p = 4$, $e'$ est minimal, et, comme $e = \frac{e' + e_{p+1} + \cdots + e_{p+q}}{2}$, on a $q \geq 3$ et $m = p + q \geq 7$.

Sinon, on a $p \geq 5$, et l'on déduit de 3.2 l'inégalité $p + 2(m - p) \geq 8$, donc $m \geq \frac{8+p}{2} > 6$, et $p \leq 2m - 8$, donc $p \leq 6$ si $m = 7$. $\square$

THÉORÈME 5.2. *Si $\Lambda$ est de dimension $n = 6$, le quotient $\Lambda/\Lambda'$ possède l'une des structures* (1), (2), (3) *ou* (2,2), *ce dernier cas n'étant possible que si $(\Lambda, \Lambda') \sim (\mathbb{D}_6, \mathbb{A}_1^{\perp 6})$. En outre, si $\Lambda$ contient un réseau d'indice 3, il contient aussi des réseaux d'indice 2 et d'indice 1.*

*Démonstration.* On a $\gamma_6^3 \leq \gamma_5^{15/4} = 2^{9/4} < 5$ par 1.1, et donc $[\Lambda : \Lambda'] \leq 4$ par 1.7. S'il y a égalité, le quotient est non cyclique (proposition 5.1), et on conclut à l'aide du théorème 4.3. Enfin, si l'indice 3 est possible, les indices 2 et 1 le sont aussi par l'exemple 3.6. □

PROPOSITION 5.3. *Si $[\Lambda : \Lambda'] = 8$, on a $n = 7$ et $(\Lambda, \Lambda') \sim (\mathbb{E}_7, \mathbb{A}_1^{\perp 7})$, ou $n \geq 8$.*

*Démonstration.* Si $\Lambda/\Lambda'$ est de type $(2, 2, 2)$, c'est une conséquence du théorème 4.3.

Supposons maintenant que $\Lambda/\Lambda'$ soit cyclique d'ordre 8. Si $n = 7$, on a $m_4 = 0$, faute de quoi les quotients cycliques d'ordre 4 existeraient en dimension 6, donc $m_1 + m_2 + m_3 = 7$ et $m_1 + 2m_2 + 3m_3 \geq 16$ par 3.2. En éliminant $m_2$, cette inégalité devient $m_3 - m_1 \geq 2$, ce qui contredit la possibilité d'imposer l'inégalité $m_1 \geq m_3$ résultant de l'opération de $(\mathbb{Z}/8\mathbb{Z})^\times$ (qui échange $m_1$ et $m_3$).

Supposons enfin que $\Lambda/\Lambda'$ soit de type $(4, 2)$. Écrivons $\Lambda = \langle \Lambda', e, f \rangle$ avec $e$ (resp. $f$) d'ordre 4 (resp. 2) modulo $\Lambda'$, et adoptons pour $e$ la notation $(p, q)$ de la proposition 5.1 ainsi que la notation analogue $(p_1, q_1)$ pour $e + f$. Soit $q'$ le nombre d'indices $i > p$ tels que $e_i$ figure au numérateur de $f$. On a $p_1 = p$; si $p + q = n$, ce qui est le cas lorsque $n = 7$ (proposition 5.1), on a $q_1 = q - q'$, et donc $q' = 0$ si $n = 7$. Le code binaire de dimension 2 engendré par $2e$ et $f$ est donc de longueur $p$, ce qui entraîne $p \geq 6$ (cf. §4) et en fait $p = 6$ par 5.1, ce qui est impossible, car $2e$ définit un mot de poids 6. □

[Si l'on admet l'égalité $\gamma_7 = \gamma(\mathbb{E}_7)$, l'inégalité de Hadamard est une égalité en cas d'indice 8, ce qui entraîne tout de suite la proposition 5.3.]

THÉORÈME 5.4. *Si $\Lambda$ est de dimension $n = 7$, le quotient $\Lambda/\Lambda'$ possède l'une des structures* (1), (2), (3), (4), (2,2) *ou* (2,2,2), *ce dernier cas n'étant possible que si $(\Lambda, \Lambda') \sim (\mathbb{E}_7, \mathbb{A}_1^{\perp 7})$.*

*Démonstration.* On a $\gamma_7^{7/2} \leq \gamma_6^{21/5} \leq 2^{63/20} < 9$ par 1.1, et donc $[\Lambda' : \Lambda'] \leq 8$ par 1.7. Si $[\Lambda : \Lambda'] = 8$, on a $(\Lambda, \Lambda') \sim (\mathbb{E}_7, \mathbb{A}_1^{\perp 7})$ par 5.3.

Il n'est pas difficile de démontrer que toutes les structures décrites dans l'énoncé existent effectivement; on peut utiliser des réseaux de racines (cf. §6 ci-après), ou utiliser les résultats plus fins décrits au §7.

Il reste à montrer l'impossibilités des indices $5$, $6$ et $7$.

Dans le cas de l'indice $5$, on a $m_1 + m_2 = 7$ et $m_1 + 2m_2 \geq 10$, et, en imposant l'inégalité $m_1 \geq m_2$, on obtient l'unique possibilité $m_1 = 4, m_2 = 3$, qui entraîne par 3.2 que les vecteurs $e - e_i$ sont minimaux. En écrivant $e$ sous la forme

$$\begin{aligned} e &= \frac{(e_1 - e) + e_2 + e_3 + e_4 + 2e_5 + 2e_6 + 2e_7}{4} \\ &= \frac{\frac{(e_1-e)+e_2+e_3+e_4}{2} + e_5 + e_6 + e_7}{2}, \end{aligned}$$

et en permutant $e_1, e_2, e_3, e_4$, on voit que les produits scalaires $e_i \,.\, e_j$ et $(e - e_i) \,.\, e_j$ sont nuls pour $j \neq i$, $1 \leq i, j \leq 4$. On a alors $e_i \,.\, e = 0$, ce qui contredit le fait que $e - e_i$ soit minimal.

[La démonstration de Watson paraît insuffisante; celle de Ryshkov est correcte.]

Dans le cas de l'indice $6$, la considération des vecteurs $2e$ (resp. $3e$) permet d'appliquer 3.2 avec $d = 3$ (resp. $d = 2$). On obtient alors les inégalités $m_1 + m_2 \geq 6$, i.e. $m_3 \leq 1$ (resp. $m_1 + m_3 \geq 4$, i.e. $m_2 \leq 3$), et l'on vérifie que les relations supplémentaires $m_1 + m_2 + m_3 = 7$ et $m_1 + 2m_2 + 3m_3 \geq 12$ imposent que l'on ait $m_1 = m_2 = 3$ et $m_3 = 1$, donc en particulier $m_1 + 2m_2 + 3m_3 = 12$, ce qui entraîne que les vecteurs $e - e_i$ sont minimaux. En utilisant 3.5, on construit un couple $(\Lambda, \Lambda'')$ avec l'indice $5$, ce qui est impossible.

Enfin, dans le cas de l'indice $7$, l'application de 3.2 avec la contrainte $m_1 = \max(m_2, m_3)$ impose que l'on ait $(m_1, m_2, m_3) = (3, 1, 3)$, triplet équivalent à $(3, 3, 1)$, dont l'existence contredit 3.2. $\square$

## 6. Les réseaux de racines

On considère dans ce § le cas où $\Lambda$ est un réseau de racines irréductible de norme $2$. Donc, $\Lambda$ est isométrique à l'un des réseaux $\mathbb{A}_n$ $(n \geq 1)$, $\mathbb{D}_n$ $(n \geq 4)$, $\mathbb{E}_6$, $\mathbb{E}_7$ or $\mathbb{E}_8$, dont nous rappelons brièvement les définitions.

L'espace vectoriel $\mathbb{R}^{n+1}$ (resp. $\mathbb{R}^n$) est muni de sa base orthonormale canonique $(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_n)$ (resp. $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n)$).

Pour $n \geq 1$ (resp. $n \geq 2$), soit $\mathbb{A}_n = \{x \in \mathbb{Z}^{n+1} \mid x_0 + x_1 + \cdots + x_n = 0\}$ (resp. $\mathbb{D}_n = \{x \in \mathbb{Z}^n \mid x_1 + x_2 + \cdots + x_n \equiv 0 \mod 2\}$; on a les isométries $\mathbb{D}_2 \simeq \mathbb{A}_1 \perp \mathbb{A}_1$ et $\mathbb{D}_3 \simeq \mathbb{A}_3$.

Pour $n = 8$, soit $e = \dfrac{\varepsilon_1+\varepsilon_2+\varepsilon_3+\varepsilon_4+\varepsilon_5+\varepsilon_6+\varepsilon_7+\varepsilon_8}{2}$. Soit $\mathbb{E}_8 = \mathbb{D}_8 \cup (e + \mathbb{D}_8)$, et soit $\mathcal{B}$ sa base formée des 8 vecteurs $e_1 = e$, $e_2 = -\varepsilon_1 - \varepsilon_2$, $e_i = \varepsilon_{i-2} - \varepsilon_{i-1}$ $(3 \le i \le 8)$. Soit $\mathbb{E}_7$ (resp. $\mathbb{E}_6$) l'orthogonal dans $\mathbb{E}_8$ de $\varepsilon_7 - \varepsilon_8$ (resp. de $\varepsilon_6 - \varepsilon_7$ et $\varepsilon_7 - \varepsilon_8$); on obtient des bases de $\mathbb{E}_7$ et de $\mathbb{E}_6$ en supprimant le dernier ou les deux derniers vecteurs de $\mathcal{B}$.

Tous ces réseaux sont engendrés par leurs vecteurs de norme 2, qui constituent des systèmes de racines de type $\boldsymbol{A}_n$, $\boldsymbol{D}_n$ et $\boldsymbol{E}_n$ respectivement, et les bases précédentes définissent le diagramme de Dynkin du système. Il résulte de la classification des systèmes de racines que les sous-réseaux de $\Lambda$ engendrés par des vecteurs de norme 2 sont somme orthogonale de réseaux de racines irréductibles.

Considérons d'abord un autre réseau de racines irréductible $L$, de rang $m < n$. Les plongements $L \subset \Lambda$ sont possibles si et seulement si $L$ et $\Lambda$ respectent la relation d'ordre $\mathbb{A} \prec \mathbb{D} \prec \mathbb{E}$, et, lorsque $\Lambda$ est de type $\mathbb{A}_n$ ou $\mathbb{D}_n$, sont classés à un automorphisme près de $\Lambda$ de la façon suivante :

Si $\Lambda = \mathbb{A}_n$ $(n \ge 2)$, il y a un unique plongement $L \subset \Lambda$, et $L^\perp$ n'est pas un réseau de racines.

Si $\Lambda = \mathbb{D}_n$ $(n \ge 4)$, il y a encore un unique plongement $L \subset \Lambda$, sauf si $L = \mathbb{A}_3$ et $n \ge 5$, où il y a deux orbites, $L = \langle \varepsilon_1 - \varepsilon_2, \varepsilon_2 - \varepsilon_3, \varepsilon_3 - \varepsilon_4 \rangle$ et $L = \langle \varepsilon_1 - \varepsilon_2, \varepsilon_2 - \varepsilon_3, \varepsilon_3 - \varepsilon_1 \rangle$, que nous distinguons en les notant respectivement $\mathbb{A}_3$ et $\mathbb{D}_3$ ; pour $n = 4$, nous notons $\mathbb{A}_3$ l'unique orbite.

De façon analogue, pour $n \ge 5$, il y a deux orbites de $L = \mathbb{A}_1 \perp \mathbb{A}_1$ dans $\mathbb{D}_n$, équivalentes à $\langle \varepsilon_1 - \varepsilon_2, \varepsilon_1 + \varepsilon_2 \rangle$ et $\langle \varepsilon_1 - \varepsilon_2, \varepsilon_3 - \varepsilon_4 \rangle$, que nous distinguons en les notant respectivement $\mathbb{D}_2$ et $\mathbb{A}'_2$ ; pour $n = 4$, nous notons $\mathbb{D}_2$ l'unique orbite.

Alors, le sous-réseau de $\mathbb{D}_n$ orthogonal à $\mathbb{D}_m$ $(2 \le m \le n-2)$ où à $\mathbb{A}_1$ est un réseau de racines (en l'occurence, $\mathbb{D}_{n-m}$ ou $\mathbb{A}_1 \perp \mathbb{D}_{n-2}$), tandis que $\mathbb{A}_m^\perp$ $(m \ge 2)$ et ${\mathbb{A}'_2}^\perp$ ne le sont pas.

De cette discussion découle tout de suite le théorème suivant, dont la première assertion remonte à Korkine et Zolotareff :

THÉORÈME 6.1. *Le réseau $\mathbb{A}_n$ ne contient aucun sous-réseau de même rang autre que lui même qui soit engendré par des vecteurs de norme $2$. Les sous-réseau de $\mathbb{D}_n$ $(n \geq 4)$ de même rang engendrés par des vecteurs de norme $2$ sont isométriques à des sommes orthogonales $\mathbb{D}_{m_1} \perp \cdots \perp \mathbb{D}_{m_r}$ avec $2 \leq m_1 \cdots \leq m_r$ et $\sum m_i = n$ ; ils sont définis de façon unique par les $m_i$ à un automorphisme près de $\mathbb{D}_n$. Les quotients $\mathbb{D}_m/(\perp_i \mathbb{D}_{m_i})$ sont $2$-élémentaires de rang $r-1$, et la valeur maximale de $r$ est $\left\lfloor \dfrac{n-3}{2} \right\rfloor$.* □

On peut développer une théorie analogue pour les réseaux exceptionnels. Les démonstrations se ramènent au cas de $\Lambda = \mathbb{E}_8$. (Toutefois, l'étude directe est plus facile dans le cas de $\mathbb{E}_6$.)

Un réseau exceptionnel peut contenir strictement un réseau irréductible de même rang. C'est le cas des trois couples $(\mathbb{A}_7, \mathbb{E}_7)$, $(\mathbb{A}_8, \mathbb{E}_8)$, et $(\mathbb{D}_8, \mathbb{E}_8)$. (Dans les notations de Coxeter, ces plongements correspondent aux isomorphismes $\mathbb{E}_7 \simeq \mathbb{A}_7^2$, $\mathbb{E}_8 \simeq \mathbb{D}_8^2 = \mathbb{D}_8^+$ et $\mathbb{E}_8 \simeq \mathbb{A}_8^3$.)

À automorphisme près, il existe un unique plongement $\mathbb{A}_m \subset \mathbb{E}_8$ si $m \neq 7$ (y compris pour $m = 3$ et $m = 8$) et deux si $m = 7$, et $\mathbb{A}_m^\perp$ est un réseau de racines pour $m \neq 6$ ainsi que pour l'une des deux orbites dans le cas $m = 7$. En outre, les deux orbites de $\mathbb{A}_1 \perp \mathbb{A}_1$ dans $\mathbb{D}_8$ se réunissent dans $\mathbb{E}_8$. En conséquence, nous revenons aux notations usuelles $\mathbb{A}_1^{\perp 2}$ et $\mathbb{A}_3$ au lieu de $\mathbb{A}_2'$ et $\mathbb{D}_3$.

De même, pour $4 \leq m \leq 8$, il y a une unique orbite de $\mathbb{D}_m$ dans $\mathbb{E}_8$, et $\mathbb{D}_m^\perp$ est un réseau de racines sauf $\mathbb{D}_7^\perp \simeq 2\mathbb{Z}$.

Le théorème suivant, qui tient compte du théorème 6.1, est une conséquence des remarques ci-dessus. Nous n'en donnerons pas de démonstration détaillée, renvoyant le lecteur à l'article [B-S] de Borel et de Siebenthal. Nous nous contenterons pour utilisation ultérieure de quelques précisions dans le cas du plongement $\mathbb{A}_3^{\perp 2} \perp \mathbb{A}_1^{\perp 2} \subset \mathbb{E}_8$, qui met en évidence un quotient de type $(4,2)$.

THÉORÈME 6.2. *Soit $\Lambda$ un réseau de racines irréductible. Alors, tout sous-réseau $\Lambda'$ de $\Lambda$ engendré par des vecteurs de norme $2$ est bien défini modulo un automorphisme de $\Lambda$ par sa classe d'isométrie. De plus, pour $n \leq 8$, les différentes possibilités pour le quotient $\Lambda/\Lambda'$ supposé non trivial sont les suivantes :*

$(2,2,2,2)$ : $(\mathbb{E}_8\,, \mathbb{A}_1^{\perp 8})$

$(3,3)$ : $(\mathbb{E}_8\,, \mathbb{A}_2^{\perp 4})$

$(4,2)$ : $(\mathbb{E}_8\,, \mathbb{A}_3^{\perp 2} \perp \mathbb{A}_1^{\perp 2})$

$(2,2,2)$ : $(\mathbb{E}_7\,, \mathbb{A}_1^{\perp 7})$ ; $(\mathbb{D}_8\,, \mathbb{A}_1^{\perp 8})$, $(\mathbb{E}_8\,, \mathbb{D}_4 \perp \mathbb{A}_1^{\perp 4})$

$(6)$ : $(\mathbb{E}_8\,, \mathbb{A}_5 \perp \mathbb{A}_2 \perp \mathbb{A}_1)$

$(5)$ : $(\mathbb{E}_8\,, \mathbb{A}_4^{\perp 2})$

$(4)$ : $(\mathbb{E}_7\,, \mathbb{A}_3^{\perp 2} \perp \mathbb{A}_1)$ ; $(\mathbb{E}_8\,, \mathbb{A}_7 \perp \mathbb{A}_1)$, $(\mathbb{E}_8\,, \mathbb{D}_5 \perp \mathbb{A}_3)$

$(2,2)$ : $(\mathbb{D}_6\,, \mathbb{A}_1^{\perp 6})$ ; $(\mathbb{D}_7\,, \mathbb{A}_3 \perp \mathbb{A}_1^{\perp 4})$, $(\mathbb{E}_7\,, \mathbb{D}_4 \perp \mathbb{A}_1^{\perp 3})$ ;

: $(\mathbb{D}_8\,, \mathbb{D}_4 \perp \mathbb{A}_1^{\perp 4})$, $(\mathbb{D}_8\,, \mathbb{A}_3^{\perp 2} \perp \mathbb{A}_1^{\perp 2})$, $(\mathbb{E}_8\,, \mathbb{D}_6 \perp \mathbb{A}_1^{\perp 2}$, $(\mathbb{E}_8\,, \mathbb{D}_4^{\perp 2})$

$(3)$ : $(\mathbb{E}_6\,, \mathbb{A}_2^{\perp 3})$ ; $(\mathbb{E}_7\,, \mathbb{A}_5 \perp \mathbb{A}_2)$ ; $(\mathbb{E}_8\,, \mathbb{A}_8)$, $(\mathbb{E}_8\,, \mathbb{E}_6 \perp \mathbb{A}_2)$

$(2)$ : $(\mathbb{D}_4\,, \mathbb{A}_1^{\perp 4})$ ; $(\mathbb{D}_5\,, \mathbb{A}_3 \perp \mathbb{A}_1^{\perp 2})$ ; $(\mathbb{D}_6\,, \mathbb{D}_4 \perp \mathbb{A}_1^{\perp 2})$,

: $(\mathbb{D}_6\,, \mathbb{A}_3 \perp \mathbb{A}_3)$, $(\mathbb{E}_6\,, \mathbb{A}_5 \perp \mathbb{A}_1)$ ; $(\mathbb{D}_7\,, \mathbb{D}_5 \perp \mathbb{A}_1^{\perp 2})$,

: $(\mathbb{D}_7\,, \mathbb{D}_4 \perp \mathbb{A}_3)$, $(\mathbb{E}_7\,, \mathbb{A}_7)$, $(\mathbb{E}_7\,, \mathbb{D}_6 \perp \mathbb{A}_1)$ ; $(\mathbb{D}_8\,, \mathbb{D}_6 \perp \mathbb{A}_1^{\perp 2})$,

: $(\mathbb{D}_8\,, \mathbb{D}_5 \perp \mathbb{A}_3)$, $(\mathbb{D}_8\,, \mathbb{D}_4^{\perp 2})$, $(\mathbb{E}_8\,, \mathbb{D}_8)$, $(\mathbb{E}_8\,, \mathbb{E}_7 \perp \mathbb{A}_1)$. □

Les plongements à quotient de type $(4,2)$ sont obtenus de la façon suivante : on considère les 8 vecteurs $e_1 = \varepsilon_1 - \varepsilon_2$, $e_2 = \varepsilon_2 - \varepsilon_3$, $e_3 = \varepsilon_1 + \varepsilon_3$, $e_4 = \varepsilon_4 - \varepsilon_5$, $e_5 = \varepsilon_5 - \varepsilon_6$, $e_6 = \varepsilon_4 + \varepsilon_6$, $e_7 = \varepsilon_7 + \varepsilon_8$ et $e_8 = \varepsilon_7 - \varepsilon_8$, ainsi que

$$e = \frac{-e_1 + e_2 - e_3 - e_4 + e_5 - e_6 + 2e_7}{4} \quad \text{et} \quad f = \frac{e_1 + e_2 + e_3 + e_7 + e_8}{2} \ ;$$

Les vecteurs $e_i$ engendrent un réseau $\Lambda' \simeq \mathbb{A}_3^{\perp 2} \perp \mathbb{A}_1^{\perp 2}$, et $\Lambda', e, f$ engendrent un réseau isométrique à $\mathbb{E}_8$ ; $e$ (resp. $f$) est d'ordre 4 (resp. 2) modulo $\Lambda'$, et $f$ n'est pas congru à $2e$ modulo $\Lambda'$ ; explicitement,

$$e = \frac{-\varepsilon_1 + \varepsilon_2 - \varepsilon_3 - \varepsilon_4 + \varepsilon_5 - \varepsilon_6 + \varepsilon_7 + \varepsilon_8}{2} \quad \text{et} \quad f = \varepsilon_1 + \varepsilon_7\,.$$

Le théorème 6.2 justifie l'existence jusqu'à la dimension 8 des différentes structures de $\Lambda/\Lambda'$ citées dans l'énoncé du théorème de l'introduction, et montre, compte tenu des résultats des §§ 4 et 5, que, jusqu'à la dimension 7, ces structures sont réalisables par des réseaux de racines.

Toutefois, on ne trouve pas tous les types (pour une définition formelle, cf. *infra*, définition 7.4) décrits dans les §§ 4 et 5; c'est évident *a priori* dans le cas des quotients 2-élémentaires, les réseaux de racines ne pouvant visiblement être obtenus qu'à partir de codes doublement pairs.

## 7. La décomposition cellulaire de l'espace des formes quadratiques

La relation entre réseaux $L$ et $L'$ de $E$ : il existe $u \in \mathrm{GL}(E)$ avec $u(L) = L'$ et $u(S(L)) = S(L')$ est une relation d'équivalence compatible avec les similitudes, qui partage l'ensemble des réseaux en classes d'équivalence, que nous appellerons *cellules* plutôt que *classes minimales* comme dans [B-M] ou [M], ch. IX, bien qu'il s'agisse en fait de quotients de cellules par des groupes finis (on emploie parfois le mot anglais *orbifold*) : à partir d'une décomposition cellulaire de l'espace des formes quadratiques de minimum donné, on peut, par un choix judicieux de représentants des classes modulo $\mathrm{GL}_n(\mathbb{Z})$, construire un complexe cellulaire fini au sens de la topologie, mais il n'est pas possible de conserver une seule cellule par classe sans passer aux "orbifolds". Nous conserverons néanmoins le point de vue des réseaux, mieux adapté à l'étude des questions d'indice que celui des formes quadratiques.

Les réseaux dont les vecteurs minimaux n'engendrent pas $E$ appartiennent à des cellules provenant d'espaces de dimension inférieure, ce qui permet de se limiter aux réseaux WR, lesquels constituent un espace compact modulo les homothéties. Comme deux réseaux semblables sont équivalents, l'invariant d'Hermite possède alors une borne inférieure sur chaque cellule.

Dans la suite du §, on se limite aux réseaux WR, et on renvoie à [M], ch. IX, §1 pour la démonstration des résultats énoncés sans justification.

Le premier travail sur le sujet semble être l'article [St] de Štogrin (ou Shtogrin), qui a démontré que les cellules sont en nombre fini et que le minimum de l'invariant d'Hermite dans une cellule (s'il existe) est atteint sur une unique classe de similitude, et a décrit ces réseaux en dimension $n \leq 4$. Ses résultats ont été retrouvés dans [B-M] et complétés sur le point suivant : les réseaux sur lesquels l'invariant d'Hermite atteint son minimum sont les réseaux *faiblements eutactiques*, c'est-à-dire ceux qui sont tels que l'identité appartienne au sous-espace de $\mathrm{End}^s(E)$ engendré par les projections sur les droites qui portent leurs vecteurs minimaux.

Ces résultats se démontrent en identifiant l'ensemble des réseaux modulo similitudes à l'ensemble des classes de formes quadratiques définies positives de minimum donnné, et en utilisant la convexité des sous-ensembles constitués des formes ayant pour vecteurs minimaux une partie finie donnée de $\mathbb{Z}^n$.

On définit une relation d'ordre entre cellules en écrivant $\mathcal{C} \prec \mathcal{C}'$ s'il existe $L \in \mathcal{C}$ et $L' \in \mathcal{C}'$ avec $S(L) \subset S(L')$. Rappelons (§ 1) que le *rang de perfection d'un réseau* $L$ est la dimension $r = r(L)$ du sous-espace de $\mathrm{End}^s(E)$ engendré par les projections sur les droites portant les vecteurs minimaux de $L$. On a $r \leq \frac{n(n+1)}{2}$, l'égalité caractérisant les réseaux parfaits. Le *corang* ou *défaut de perfection* de $L$ est $\frac{n(n+1)}{2} - r$. On montre que $r(L)$, de même que $s(L)$, ne dépend que de la cellule contenant $L$. Le *défaut de perfection d'une cellule* $\mathcal{C}$ est la dimension de $\mathcal{C}$ modulo les similitudes de $E$, autrement dit le nombre de paramètres dont dépendent affinement les réseaux de $\mathcal{C}$. Les cellules de dimension 0 sont celles qui se réduisent à l'ensemble des réseaux semblables à un même réseau, qui est alors parfait.

L'adhérence d'une cellule $\mathcal{C}$ est la réunion des cellules $\mathcal{C}' \succ \mathcal{C}$. Les cellules parfaites sont donc les cellules maximales de l'espace des réseaux. En affinant le procédé de Voronoï de “perfectionnement de réseaux” signalé pour justifier le théorème 1.5, on montre que deux cellules $\mathcal{C}$ et $\mathcal{C}' \succ \mathcal{C}$ peuvent être jointes par une chaîne de cellules dont le rang de perfection croît exactement d'une unité à chaque étape ([M], chapitre IX, théorème 1.9).

Venons-en maintenant aux questions d'indices. Soient $\Lambda$ et $\Lambda' \subset \Lambda$ deux réseaux WR de même minimum, et soit $\mathcal{C}$ la cellule contenant $\Lambda$. Posons $A = \Lambda/\Lambda'$. Si $\Lambda_1$ est un autre réseau de $\mathcal{C}$, et si $u \in \mathrm{GL}(E)$ applique $\Lambda$ sur $\Lambda_1$, soit $\Lambda_1' = u(\Lambda')$. Alors, $\Lambda_1'$ est un réseau WR de même minimum que $\Lambda_1$, et le quotient $\Lambda_1/\Lambda_1'$ est isomorphe à $A$. Ainsi, l'ensemble des structures possibles pour les quotients $\Lambda/\Lambda'$ entre réseaux WR de même minimum ne dépend que de la cellule de $\Lambda$. En outre, par passage à la limite, on voit que $A$ peut être réalisé dans toute classe $\mathcal{C}' \succ \mathcal{C}$. Il en résulte que tout groupe abélien fini $A$ réalisable en dimension $n$ comme quotient $\Lambda/\Lambda'$ de réseaux WR de même minimum est réalisable sur des cellules minimales pour la relation $\prec$.

Cette remarque justifie la possibilité de donner la définition suivante :

DÉFINITION 7.1. Soit $A$ un groupe abélien fini. On dit qu'une cellule $\mathcal{C}$ est *$A$-minimale* s'il existe un couple $(\Lambda, \Lambda')$ de réseaux WR avec $\Lambda \in \mathcal{C}$ et $\Lambda/\Lambda' \simeq A$, et si un tel couple n'existe pas sur les cellules $\mathcal{C}' \prec \mathcal{C}$ distinctes de $\mathcal{C}$.

À côté de la liste des structures possibles de $A$ et des entiers $r$ et $s$, un autre invariant important d'une classe $\mathcal{C}$ est la structure du quotient $M(\mathcal{C})$ de $\Lambda \in \mathcal{C}$ par son sous-réseau engendré par $S(\Lambda)$. Pour $\mathcal{C}_1 \succ \mathcal{C}$, $\Lambda \in \mathcal{C}$ et $\Lambda_1 \in \mathcal{C}_1$, $S(\Lambda)$ s'identifie à un sous-ensemble de $S(\Lambda_1)$, et donc $M(\mathcal{C}_1)$ à un quotient de $M(\mathcal{C})$. En conséquence, les groupes $M(\mathcal{C})$ maximaux sont atteints sur les cellules $A$-minimales associées aux groupes $A$ maximaux.

À deux cellules de dimensions $p$ et $q$, soit $\mathcal{C} \subset \mathbb{R}^p$ et $\mathcal{D} \subset \mathbb{R}^q$, on associe la *cellule somme directe $\mathcal{C} \oplus \mathcal{D}$ de $\mathcal{C}$ et de $\mathcal{D}$*, à savoir la cellule de $\mathbb{R}^{p+q}$ contenant les sommes orthogonales d'un réseau $\Lambda$ de $\mathcal{C}$ et d'un réseau $M$ de $\mathcal{D}$ de même norme. C'est l'ensemble des réseaux sommes directes $\Lambda \oplus M$ qui n'ont pas d'autres vecteurs minimaux que ceux de $\Lambda$ et de $M$. Ses invariants $s$ et $r$ sont sommes des invariants correspondants de $\mathcal{C}$ et de $\mathcal{D}$, et les quotients sont sommes directes des quotients qui existent pour $\mathcal{C}$ et $\mathcal{D}$.

Le procédé précédent permet d'associer à toute cellule $\mathcal{C}$ de dimension $n$ une *cellule étendue* de dimension $n'$ pour tout entier $n' > n$, en prenant comme réseau $M$ un réseau semblable à $\mathbb{Z}^{n'-n}$.

DÉFINITION 7.2. On dit qu'une cellule est *primitive* si elle n'est pas l'extension à la dimension $n$ d'une cellule de dimension inférieure.

Voici quelques exemples de cellules primitives minimales, permettant en particulier de les exhiber toutes jusqu'à la dimension 7.

• <u>INDICE 1</u>. La seule cellule primitive est celle de $\mathbb{Z}$, de dimension 1.

• <u>INDICE 2</u>. Il y a une cellule primitive minimale par dimension $n \geq 4$. Pour $n = 4$, c'est la classe de similitude de $\mathbb{D}_4$, avec $s = 12$ et $r = 10$. Pour $n \geq 5$, elle est représentée par $\langle \mathbb{Z}^n, \frac{1}{2}(\varepsilon_1 + \cdots + \varepsilon_n) \rangle$, avec $s = r = n$.

• <u>QUOTIENTS 2-ÉLÉMENTAIRES</u>. Lorsque $A$ est 2-élémentaire d'ordre $2^r$, ce que nous avons dit à propos de l'indice 2 se généralise ainsi : on attache à $\mathcal{C}$ un code $C$, engendré par des mots $\mu_1, \dots, \mu_r$ de poids $\omega \geq 4$, de supports $\sigma_1, \dots, \sigma_r$, et l'on représente $\mathcal{C}$ par le réseau $\langle \mathbb{Z}^n, f_1, \dots, f_r \rangle$ avec $f_i = \frac{1}{2} \sum_{k \in \sigma_i} \varepsilon_k$. Soit $t$ le nombre de mots de poids 4 de $C$. On a alors $s = 8t + n$. Le rang de perfection $r$ dépend de la disposition des supports des mots de poids 4 de $C$. Quant à la primitivité, elle s'exprime par l'absence d'une coordonnée nulle pour tous les mots du code.

Pour $r = 2$, on a $n \geq 6$. Si $n = 6$, il s'agit de la cellule de $\mathbb{D}_6$, avec $s = 30$ et $r = 21$. Si $n = 7$, il y a deux codes possibles, avec les poids $(4, 4, 6)$ (et alors $s = 23$, $r = 19$) et $(4, 5, 5)$ (et alors $s = 15$ et $r = 13$).

Pour $r = 3$, on a $n \geq 7$. Si $n = 7$, il s'agit de la cellule de $\mathbb{E}_7$, avec $s = 63$ et $r = 28$ ; $C$ est alors une section du code de Hamming étendu.

• <u>Indice 3</u>. Il y a une cellule primitive minimale par dimension $n \geq 6$. Le théorème 2.2 montre que l'on a $n \geq 6$, et $s \geq 12$ si $n = 6$. Si $n = 6$, on a $s = 12$ et $r = 11$ ; c'est un cas particulier de la proposition A.1 de [M1]. (En normalisant par $e_i \,.\, e_i = 1$, on peut prendre les $e_i \,.\, e_j$ égaux à un même nombre réel $t \in ]\frac{1}{10}, \frac{1}{4}[$.) On verra au prochain § que l'on peut prendre $s = r = n$ pour tout $n \geq 7$.

• <u>Indice 4</u>. Le cas des quotients de type $(2, 2)$ a déjà été discuté. Dans le cas cyclique, on a défini au §5 des entiers $p$ et $q$ avec $p + q = n$. Si $n = 7$, on a $p = 4$, 5 ou 6.

Si $p = 4$, $S(\Lambda)$ contient les vecteurs minimaux des deux réseaux de type $\mathbb{D}_4$ engendrés par $e', e_1, e_2, e_3$ et $e, e_5, e_6, e_7$, ce qui entraîne $s \geq 23$ et $r \geq 19$, et les deux égalités sont vérifiées lorsque les vecteurs $e_i$ sont deux à deux orthogonaux, exemple dû à Watson.

Si $p = 5$, en prenant $e_i \,.\, e_j = \frac{1}{6}$ pour $1 \leq i < j \leq 5$ et $e_i \,.\, e_j = 0$ pour $1 \leq i < j = 6, 7$, on obtient un exemple avec $s = r = 7$.

Si $p = 6$, le théorème 2.2 montre que l'on doit avoir $s \geq 21$ ($S(\Lambda)$ doit contenir les vecteurs $e_1, e - e_i, e - e_i - e_7$, $i \leq 6$ ainsi que $e, e_7, e - e_7$). On vérifie que l'on a $s = 21$ et $r = 19$ lorsque $e_i \,.\, e_j = \frac{1}{5}$ pour $1 \leq i < j \leq 6$ et $e_k \,.\, e_7 = 0$ pour $k \leq 6$.

• <u>Indice 8</u>. Ce n'est possible que pour $n \geq 7$, et, si $n = 7$, la cellule est celle de $\mathbb{E}_7$, avec $s = 63$ et $r = 28$ et quotient de type $(2, 2, 2)$.

On a donc fait la liste exhaustive de toutes les cellules $A$-minimales jusqu'à la dimension 7, puisque l'on a réalisé toutes les possibilités qui n'avaient pas été exclues aux §§3, à 5. On en déduit :

Proposition 7.3. *Pour tout $n \leq 7$, et pour tout couple $(\Lambda, \Lambda')$ d'une cellule minimale, on a $s(\Lambda') = n$.* $\square$

Ce résultat ne subsiste pas en dimension $8$. On verra en effet que les quotients de type $(3,3)$ ne sont possibles qu'avec un couple $(\Lambda, \Lambda') \sim (\mathbb{E}_8, \mathbb{A}_2^{\perp 4})$, pour lequel $s(\Lambda') = 12$, cet exemple n'étant du reste pas unique.

La classification utilisée dans [Ry] et dans [Za] ne se réfère pas à la décomposition cellulaire, mais correspond à une notion de *type de quotient* qu'il semble raisonnable de décrire ainsi.

Soit $A$ un groupe abélien fini, d'ordre $a$, d'annulateur $d$ et de nombre minimum de générateurs $t$. On caractérise $A$ à isomorphisme près par ses diviseurs élémentaires, famille $d_1, \dots, d_t$ d'entiers vérifiant les conditions $d_1 = d,\ d_t > 1,\ d_{i+1} \mid d_i\,(i < t)$, et $\prod_i d_i = a$.

On utilise ces notations dans le cas de deux réseaux $\Lambda$ et $\Lambda' \subset \Lambda$ engendré par $n$ vecteurs minimaux de $\Lambda$, avec $\Lambda/\Lambda' \simeq A$. Le groupe $A$ est un $\mathbb{Z}/d\mathbb{Z}$-module, et l'on associe au couple $(\Lambda, \Lambda')$ le code sur $\mathbb{Z}/d\mathbb{Z}$ dont les mots sont les suites $a_1, \dots, a_n$ d'entiers modulo $d$ telles que $\frac{1}{d}\sum_i a_i e_i$ soit un élément de $\Lambda$. C'est un code de longueur $d$ et de "dimension" $t$.

Définition 7.4. Le *type du couple* $(\Lambda, \Lambda')$ est la classe d'équivalence du code associé à $(\Lambda, \Lambda')$ pour la relation suivante entre deux codes, c'est-à-dire entre deux sous-modules $A$ et $A'$ de $(\mathbb{Z}/d\mathbb{Z})^n$ : il existe un isomorphisme de $A$ sur $A'$ induit par des *matrices monomiales* de $\mathcal{M}_n(\mathbb{Z}/d\mathbb{Z})$ (matrices ayant un unique coefficient non nul dans chaque ligne et chaque colonne, qui est en outre inversible).

Dans le cas d'un dénominateur $d$ premier, on retrouve la notion utilisée en théorie des codes.

Étant donné un réseau $M$, notons $\mathrm{GL}(M)$ le stabilisateur de $M$ dans $\mathrm{GL}(E)$ ; c'est un sous-groupe discret de $\mathrm{GL}(E)$, que le choix d'une base de $M$ permet d'identifier à $\mathrm{GL}_n(\mathbb{Z})$.

Lorsque $s(\Lambda') = n$, les automorphismes du code associé à $(\Lambda, \Lambda')$ proviennent des éléments de $\mathrm{GL}(\Lambda')$ qui stabilisent $\Lambda$, et le type de $(\Lambda, \Lambda')$ définit une unique cellule minimale associée à $(\Lambda, \Lambda')$.

Pour autant, deux cellules de types différents ne sont pas nécessairement distinctes : on peut vérifier que les types avec $s = 48$ du tableau 11.1, partie 2 contiennent chacun une unique cellule $A$-minimale au sens de la définition 7.1, $A$ étant le groupe abélien $C_4 \times C_2$ et $C_2 \times C_2 \times C_2$

respectivement (cela se fait en identifiant les réseaux qui leurs sont attachés par l'argument de moyenne décrit au paragraphe suivant) ; en conséquence, les cellules $A$-minimales correspondant à ces deux types sont identiques, mais il est possible de trouver pour tout réseau $\Lambda$ de cette cellule des sous-réseaux $\Lambda'$ et $\Lambda''$ engendrés par $8$ vecteurs minimaux de $\Lambda$ de façon à obtenir des quotients $\Lambda/\Lambda'$ et $\Lambda/\Lambda''$ isomorphes à $C_4 \times C_2$ et $C_2 \times C_2 \times C_2$ respectivement.

Il peut y avoir également des *inclusions entre types*, en ce sens que toute cellule de l'un soit majorée par une cellule associée à l'autre pour la relation "$\prec$". C'est le cas des types à des quotients $C_4 \times C_2$ avec $s = 75$ et $s = 120$ : la cellule considérée se réduit à la classe de similitude de $\mathbb{E}_8$ dans le cas $s = 120$ et à une arête du graphe de Voronoï reliant deux copies de $\mathbb{E}_8$ dans le cas $s = 75$.

Nous reviendrons à la fin du § 10 sur les deux phénomènes signalés ci-dessus, qui ne se produisent pas avant la dimension $8$.

## 8. Déformations

Dans ce paragraphe, on indique divers procédés permettant de minimiser $S(\Lambda)$ en conservant la structure du quotient $\Lambda/\Lambda'$, et même le type de ce quotient (au sens de la définition 7.4) lorsque l'on conserve la dimension. Pour ce faire, on utilise le plus souvent des déformations de la structure euclidienne.

On conserve les notations antérieures. En particulier, $(\Lambda, \Lambda')$ désigne un couple de réseaux WR de même minimum, avec $\Lambda \supset \Lambda'$, $\Lambda'$ possédant une base $\mathcal{B} = (e_1, \dots, e_n)$ formée de vecteurs minimaux de $\Lambda$.

Les deux énoncés suivants, dont le second n'est pas utilisé dans la suite, montrent comment l'on peut dans certaines conditions transformer un couple $(\Lambda, \Lambda')$ en un couple $(L, L')$ avec $s(L) = s(L')$, tout en conservant certains des invariants associés à $(\Lambda, \Lambda')$. Le premier concerne le passage d'une dimension a une dimension supérieure dans le cas d'un code monogène; il pourrait être étendu à des codes de dimension $t > 1$, en remplaçant $n$ par une dimension $n' \leq n + t$ convenable.

PROPOSITION 8.1. *Supposons que l'on ait* $\Lambda = \langle \Lambda', e\rangle$ *avec* $e = \dfrac{a_1e_1 + \cdots + a_ne_n}{d}$, $d > 1$ *et* $(d, a_1, \ldots, a_n) = 1$. *Soit* $a \in [1, \frac{d}{2}]$ *un entier premier à* $d$. *Il existe alors en dimension* $n+1$ *un couple* $(L, L')$, *de type* $(a, a_1, \ldots, a_n)$, *avec* $L/L' \simeq \Lambda/\Lambda'$ *et* $s(L) = s(L') = s(\Lambda') + 1$.

*Démonstration.* On munit $\mathbb{R} \times E$ de la base formée des vecteurs $f_0 = (1, 0)$, $f_1 = (0, e_1)$, ... , $f_n = (0, e_n)$. Posons

$$L' = \mathbb{Z} f_0 \perp \Lambda',\ f = \frac{af_0 + a_1f_1 + a_2f_2 + \cdots + a_nf_n}{d} \quad \text{et} \quad L = \langle L', f\rangle\,.$$

On a $L = \cup_{c \bmod d}\, cf + L'$, et les éléments de $cf + L'$ sont de la forme

$$x = \frac{ac}{d}\, f_0 + ce + \lambda\, f_0 + y',\ \ \lambda \in \mathbb{Z}, y' \in \Lambda'\,,$$

ce qui s'écrit $x = (\lambda + \frac{ac}{d})\, f_0 + z$ avec $z = y' + ce$. Lorsque $c$ n'est pas divisible par $d$, on a $z \in \Lambda \smallsetminus \Lambda'$ et $N(x) > N(y) \geq N(\Lambda)$, d'où $s(L) = s(L')$, puis $s(L') = s(\Lambda') + 1$. □

PROPOSITION 8.2. *Supposons la condition* $s(\Lambda) - r(\Lambda) = s(\Lambda') - r(\Lambda')$ *satisfaite. Alors, dans tout voisinage de l'identité dans* $\mathrm{End}^s(E)$, *il existe un automorphisme* $u$ *de* $E$ *tel que* $(u(\Lambda), u(\Lambda'))$ *soit du même type que* $(\Lambda, \Lambda')$ *et que* $u(\Lambda)$ *et* $u(\Lambda')$ *aient les mêmes vecteurs minimaux.*

*Démonstration.* On munit l'espace $\mathrm{End}^s(E)$ des endomorphismes symétriques de $E$ du *produit scalaire de Voronoï* $\langle u, v\rangle = \mathrm{Tr}(v \circ u)$. Notant toujours $p_x \in \mathrm{End}^s(E)$ la projection sur la droite portant le vecteur non nul $x$ de $E$, on a la formule $\langle u, p_x\rangle = x \,.\, u(x)$.

Dans $\mathrm{End}^s(E)$, soit $H$ (resp. $H'$) le sous-espace engendré par les $p_x$, $x \in S(\Lambda)$ (resp. $x \in S(\Lambda')$). L'hypothèse signifie que $H$ est engendré par $H'$ et les projections $p_1, \ldots, p_{s-s'}$ sur les $s - s'$ droites portant les vecteurs minimaux de $\Lambda \smallsetminus \Lambda'$. Pour tout $i$, soit $H_i$ l'hyperplan de $H$ engendré par $H'$ et les $p_j$, $j \neq i$, et soit $v_i$ un vecteur non nul porté par la droite de $H$ orthogonale à $H_i$. Le produit scalaire $\langle p_i, v_i\rangle$ est non nul ; quitte à changer le signe de $v_i$, on peut le supposer positif. Soit $v = v_1 + \cdots + v_n$.

Pour $u \in \mathrm{End}^s(E)$ assez voisin de l'identité, on a $S(u(\Lambda)) \subset u(S(\Lambda))$ (*les vecteurs minimaux de* $u(\Lambda)$ *proviennent de ceux de* $\Lambda$). Pour $|\lambda|$ assez petit, $\mathrm{Id} + \lambda v$ est défini positif. On peut donc considérer $u_\lambda = (\mathrm{Id} + \lambda v)^{1/2}$ qui, pour $|\lambda|$ assez petit, applique $S(\Lambda)$ dans $S(u_\lambda(\Lambda))$. On choisit $\lambda$ ainsi, et de plus positif et tel que $u_\lambda(\Lambda)$ soit encore dans la cellule de $\Lambda$ et $u_\lambda(\Lambda')$ dans celle de $\Lambda'$. Le calcul de normes

$$N(u_\lambda(x)) = u_\lambda(x)\,.\,u_\lambda(x) = x\,.\,u_\lambda^2(x) = N(x) + \lambda \sum_i x\,.\,v_i(x)$$

montre alors que l'on a $N(u_\lambda(x)) \geq N(x)$ pour tout $x \in S(\Lambda)$, avec égalité sur $S(\Lambda')$ et inégalité stricte sur $S(\Lambda) \smallsetminus S(\Lambda')$. $\square$

En général, il n'est pas possible de déformer $(\Lambda, \Lambda')$ en un couple $(L, L')$ avec $s(L) = s(L')$ sans l'hypothèse sur $S(\Lambda)$. Par exemple, pour $n = 4$, $[\Lambda : \Lambda'] = 2$ n'est possible que pour $(\Lambda, \Lambda') \sim (\mathbb{D}_4, \mathbb{A}_1^4)$. On a alors dans ce cas $s(\Lambda) = 12 > s(\Lambda') = 4$, et $s(\Lambda) - r(\Lambda) = 2 > s(\Lambda') - r(\Lambda') = 0$.

De même, il est en général impossible de déformer $\Lambda'$ en un réseau avec seulement $n$ vecteurs minimaux. Des exemples existent en dimension 8 avec des quotients $\Lambda/\Lambda'$ de type $(4,2)$ ou $(3,3)$. Il n'y en a pas en dimension $n \leq 7$. En outre, aucun exemple avec un quotient $\Lambda/\Lambda'$ cyclique n'est connu.

Nous introduisons maintenant d'autres déformations, obtenues par un procédé de moyenne analogue à celui qui permet d'associer une représentation orthogonale à toute représentation réelle d'un groupe fini, donnant une forme générale à une technique utilisée par Zahareva dans des cas particuliers.

DÉFINITION 8.3. Étant donné un réseau $L$, on pose

$$\mathrm{GL}(L) = \{u \in \mathrm{GL}(E) \mid u(L) = L\}$$

et

$$\mathcal{G}(L) = \{u \in \mathrm{GL}(L) \mid u(S(L)) = S(L)\}\,.$$

Le choix d'une base de $L$ identifie $\mathrm{GL}(L)$ à $\mathrm{GL}_n(\mathbb{Z})$. Quant au groupe $\mathcal{G}(L)$, il contient le groupe $\mathrm{Aut}(L)$ des automorphismes de $L$, et il est fini lorsque $L$ vérifie la condition (WR), puisqu'il est alors isomorphe à un sous-groupe du groupe symétrique de $S(L)$.

Pour tout $\sigma \in \mathrm{GL}(E)$, $(x,y) \mapsto \sigma x\,.\,\sigma y$ est un produit scalaire sur $E$.

DÉFINITION 8.4. Pour tout sous-groupe fini $H$ de $\mathrm{GL}(E)$, soit $E_H$ l'espace vectoriel $E$ muni du produit scalaire

$$(x,y)_H = \frac{1}{|H|} \sum_{\sigma \in H} \sigma x\,.\,\sigma y\,.$$

Il est clair que tout réseau $L$ de $E$ peut être considéré comme un réseau de $E_H$, noté $L_H$, ce qui donne un sens à l'énoncé suivant, généralisation d'un résultat de Zahareva ([Za], lemme 7) :

PROPOSITION 8.5. *Soit $L$ un réseau de $E$ et soit $H$ un sous-groupe fini de* $\mathrm{GL}(L)$. *Alors :*

*(1) On a $N(L_H) \geq N(L)$, et l'égalité a lieu si et seulement s'il existe une orbite de $H$ contenue dans $S(L)$.*

*(2) Si $N(L_H) = N(L)$, $S(L_H)$ est contenu dans $S(L)$, et lui est égal si et seulement si $H$ est un sous-groupe de $\mathcal{G}(L)$.*

*(3) Si $M$ et $L \subset M$ sont deux réseaux de même norme vérifiant la condition (WR), si $N(L_H) = N(L)$, et si $H$ stabilise $M$, alors $M_H$ et $L_H$ vérifient aussi la condition (WR), et les couples $(M_H, L_H)$ et $(M, L)$ sont du même type.*

*Démonstration.* (1) Pour tout $x \in L$ non nul et tout $\sigma \in H$, on a $\sigma x \,.\, \sigma x \geq N(L)$, donc $N(x) \geq N(L)$, et l'inégalité est stricte sauf si $S(L)$ contient $Hx$.

(2) Si $N(L_H) = N(L)$, on a l'équivalence

$$S(L_H) = S(L) \Longleftrightarrow \forall\, x \in S(L), \forall\, \sigma \in H, \sigma x \,.\, \sigma x = N(L)\,.$$

(3) Comme $N(M) = N(L)$, on a $S(M_H) \cap L = S(L_H) = S(L)$. Par conséquent, $M_H$ et $L_H$ ont même norme et vérifient encore la condition (WR). Qu'ils soient du même type résulte du fait qu'une famille génératrice de $M$ sur $L$ est aussi une famille génératrice de $M_H$ sur $L_H$. □

Cette proposition permet de simplifier la recherche des cellules minimales de type donné, en se restreignant à des familles de réseaux dépendant d'un nombre réduit de paramètres, et de prouver éventuellement l'impossibilité de certains types. En l'appliquant à des sous-groupes $H$ de $\mathcal{G}(\Lambda')$, on conserve $\Lambda'$, ce qui permet de rechercher les minima de $s(\Lambda)$ pour une classe de $\Lambda'$ fixée.

Partons d'un couple $(\Lambda, \Lambda')$ pour lequel on note $d = d_1, d_2, \ldots, d_t$ la suite (décroissante) de ses diviseurs élémentaires ; on peut écrire $\Lambda = \langle \Lambda', e^{(1)}, \ldots, e^{(t)} \rangle$, les vecteurs $e^{(i)}$ étant de la forme

$$e^{(i)} = \frac{a_1^{(i)} e_1 + \cdots + a_n^{(i)} e_n}{d_i}\,, \quad \text{avec} \quad -\frac{d_i}{2} < a_j^{(i)} \leq \frac{d_i}{2}\,.$$

Nous devons chercher des éléments de $\mathrm{GL}(\Lambda')$ qui induisent par passage au quotient des automorphismes du code sur $\mathbb{Z}/d\mathbb{Z}$ défini par $\Lambda/\Lambda'$.

Voici deux exemples particulièrement utiles. (D'autres transformations, dépendant étroitement du code, seront utilisées dans la suite, voir par exemple l'étude des quotients de type $(4,2)$ en dimension $8$.)

Exemple 8.6.. Supposons que pour une famille $T = \{j_1, \dots, j_k\}$ d'indices, les $kt$ coefficients $a_j^{(i)}, j \in T, 1 \le i \le t$ soient égaux. Les permutations de $j_1, \dots, j_k$ conservent alors le code. Il en résulte d'une part que l'on peut choisir les $\frac{k(k-1)}{2}$ produits scalaires $e_j \,.\, e_{j'}$, $j, j' \in T$ égaux, et d'autre part que, pour tout $i \notin T$, on peut aussi choisir les $k$ produits scalaires $e_i \,.\, e_j$, $j \in T$ égaux.

Exemple 8.7.. Supposons que, pour un indice $j$ donné, les $t$ coefficients $a_j^{(i)}$ soient égaux à $0$ ou à $\frac{d_1}{2}$. Alors, l'opération consistant à changer le signe de $e_j$ conserve le code. Il en résulte que $e_j$ peut être choisi orthogonal à tous les autres vecteurs $e_i$.

Lors de l'utilisation dans les calculs explicites de l'exemple 8.6, nous adoptons la notation suivante :

Notation 8.8. Soit $t = \lfloor \frac{d}{2} \rfloor$. On note $x_1, \dots, x_t$ les produits scalaires $e_i \,.\, e_j$ pour $a_i = a_j = 1, \dots, t$, et $y_1, \dots, y_{t(t-1)/2}$ ceux qui correspondent aux couples $(1,2), (1,3), \dots, (t-1,t)$.

On fera en outre la convention suivante, justifiée par l'exemple 8.7 :

Convention 8.9. *On suppose que les $y_k$ correspondant aux produit scalaires $e_i \,.\, e_j$ avec $a_j = \frac{d}{2}$ sont nuls.*

Appliquée aux quotients 2-élémentaires, la proposition 8.5 montre simplement qu'un tel quotient existe si et seulement s'il existe sur des réseaux dont les vecteurs $e_i$ sont deux à deux orthogonaux. En combinant la proposition 8.1 avec l'existence de l'indice 3 en dimension 6 (exepmple 3.6), on voit que $s = r = n$ est possible avec l'indice 3 pour tout $n \ge 7$.

L'étude générale de l'indice 4 se fait de façon analogue, en utilisant l'existence des trois types de dimension $7$, celle de la répartition $(8,0)$ en dimension 8 (prendre $e_i \,.\, e_j = t$ quels que soient $i$ et $j \ne i$ avec $\frac{1}{7} < t < \frac{1}{3}$,

[M1], formule 2.2), et l'écriture $e = \dfrac{\frac{e_1+\cdots+e_p}{2} + e_{p+1} + \cdots + e_n}{2}$, et conduit au résultat suivant :

Proposition 8.10. *Pour qu'il existe un couple $(\Lambda, \Lambda')$ à quotient cyclique d'ordre $4$ avec $s = r = n$, il faut et il suffit que l'on ait $n \geq 9$, ou $n = 8, p = 7$, ou $n \geq 7$, $5 \leq p \leq n-2$. Les autres possibilités à quotients cycliques d'ordre $4$ sont $n = 7, p = 4$ $(s = 23, r = 19)$, $n \geq 8, p = 4$ $(s = n+8, r = n+6)$, $n = 7, p = 6$ $(s = 21, r = 19)$ et $n = p = 8$ $(s = 16, r = 15)$.* □

## 9. Indices 5, 6, 7, 8, 9 en dimension 8

Les travaux de Watson pour les indices compris entre $10$ et $15$, et les résultats antérieurs concernant les indices $3$ et $4$ laissent en suspens dans le cas de la dimension $8$, d'une part les quotients cycliques d'ordre $5, 6, 7, 8, 9$, qui sont l'objet de ce §, et d'autre part les quotients non cycliques, qui seront examinés au § suivant.
On considère en dimension $8$ un couple $(\Lambda, \Lambda')$ avec $\Lambda/\Lambda' \simeq \mathbb{Z}/d\mathbb{Z}$, $d \in \{5, 6, 7, 8, 9\}$. On examine d'abord les répartitions $(m_1, \ldots, m_t)$ $(t = \lfloor \frac{d}{2} \rfloor)$ possibles modulo l'action de $(\mathbb{Z}/d\mathbb{Z})^\times$. On pose $\sigma = \sum_{i=1}^{t} i m_i$, et l'on détermine les invariants $s$ et $r$ des réseaux $\mathbb{Z}/d\mathbb{Z}$-minimaux.

<u>$d = 5$</u>.

On a les contraintes $t = 2$, $m_1 + m_2 = 8$ et $m_1 + 2m_2 \geq 10$, et l'on peut échanger $m_1$ et $m_2$, donc imposer l'inégalité $m_1 \geq m_2$. Cela laisse à échange près de $m_1$ et $m_2$ les $3$ répartitions suivantes :

$(6,2)$ $(\sigma = 10)$; $(5,3)$ $(\sigma = 11)$; $(4,4)$ $(\sigma = 12)$, qui, d'après [Za], existent toutes.

<u>$d = 6$</u>.

On a les contraintes $t = 3$, $m_1 + m_2 + m_3 = 8$ et, en considérant $e$, $2e$ et $3e$, $m_1 + 2m_2 + 3m_3 \geq 12$, $m_1 + m_3 \geq 4$, et $m_1 + m_2 \geq 6$, i.e. $m_3 \geq 2$. En envisageant les $3$ valeurs *a priori* possibles pour $m_3$, on trouve les $9$ répartitions suivantes :

$(4,4,0)$, $(5,2,1)$, $(6,0,2)$ $(\sigma = 12)$; $(4,3,1)$, $(5,1,2)$ $(\sigma = 13)$; $(3,4,1)$, $(4,2,2)$ $(\sigma = 14)$; $(3,3,2)$ $(\sigma = 15)$; $(2,4,2)$ $(\sigma = 16)$.

La première est impossible, car on pourrait écrire

$$e = \frac{\frac{e_1+e_2+e_3+e_4}{2} + e_5 + e_6 + e_7 + e_8}{3},$$

introduisant un indice 3 en dimension 5. On prouve de façon analogue l'impossibilité de la répartition $(5,1,2)$ : soit $f = \frac{e_1+e_2+e_3+e_4+e_5-e_6}{3}$ ; alors, $f + e_6$ est minimal, et l'on a $e = \frac{(f+e_6)+e_7+e_8}{2}$, ce qui introduit un indice 2 en dimension 3. On élimine enfin la répartition $(6,0,2)$ en posant $f = \frac{e_1+e_2+e_3+e_4+e_5+e_6}{3}$ et $f' = f - e_6$ ; on a $e = \frac{f'+e_6+e_7+e_8}{2}$ avec $f'$ minimal, donc $e_6 \,.\, f' = 0$, et de même $f'.e_i = 0$ pour $1 \le i \le 6$, d'où $6N(f') = e_1 \,.\, f' + \cdots + e_5 \,.\, f' - 2e_6 \,.\, f' = 0$.

Il reste 6 possibilités, qui en fait existent toutes, résultat dû à Zahareva.

$\underline{d = 7}$.

On a les contraintes $t = 3$, $m_1+m_2+m_3 = 8$ et $m_1+2m_2+3m_3 \ge 14$, et l'on peut permuter circulairement $m_1, m_2, m_3$, ce qui permet dans une première étape d'imposer que l'on ait $m_1 = \max(m_2, m_3)$, puis d'affiner la liste trouvée en minimisant $\sigma$. On constate alors que les répartitions doivent être équivalentes par permutation circulaire des $m_i$ à l'une des trois suivantes :

$(3,4,1)$, $(4,2,2)$ $(\sigma = 14)$; $(3,3,2)$ $(\sigma = 15)$.

$\underline{d = 8}$.

À côté des contraintes $t = 4$, $m_1 + m_2 + m_3 + m_4 = 8$ et $m_1 + 2m_2 + 3m_3 + 4m_4 \ge 16$, on a $m_1 + m_2 + m_3 \ge 7$, i.e. $m_4 \le 1$ et $m_1 + m_3 \ge 4$, parce que $\langle \Lambda', 2e \rangle / \Lambda'$ est cyclique d'ordre 4, et l'action de $(\mathbb{Z}/8\mathbb{Z})^\times$ permet d'échanger $m_1$ et $m_3$, et donc de supposer $m_1 \ge m_3$.

Si $m_4 = 0$, les deux premières conditions entraînent $-m_1 + m_3 \ge 0$, donc $m_3 = m_1$, ce qui laisse les 3 répartitions $(2,4,2,0)$, $(3,2,3,0)$ et $(4,0,4,0)$ avec $\sigma = 16$.

Si $m_4 = 1$, l'examen des diverses possibilités, en tenant compte de ce que l'on sait sur l'indice 4, laisse la liste suivante de répartitions *a priori* possibles :

$(3,3,1,1)$, $(4,1,2,1)$ $(\sigma = 16)$; $(3,2,2,1)$ $(\sigma = 17)$; $(2,3,2,1)$, $(3,1,3,1)$ $(\sigma = 18)$.

$\underline{d = 9}$.

On peut permuter circulairement $m_1, m_2, m_4$, et ce que l'on sait de l'indice 3 entraîne la minoration $m_1 + m_2 + m_4 \geq 6$, i.e. $m_3 \geq 2$. L'examen des 3 valeurs que peut prendre $m_3$ ne laisse que les 3 possibilités suivantes :

$(3,2,1,2)$, $(2,3,2,1)$ $(\sigma = 18)$; $(2,2,2,2)$ $(\sigma = 20)$,

Quotients d'ordre 5.

Proposition 9.1. *Les valeurs minimales de $s$ et de $r$ sont $s = 16$ et $r = 15$ dans le cas des répartitions $(6,2)$ et $(4,4)$, et $s = r = 8$ dans le cas de la répartition $(5,3)$.*

*Démonstration.* Pour construire les exemples. on se limitera à des produits scalaires $e_i \,.\, e_j$, $i < j$ prenant au plus trois valeurs, $x_1$ pour $i, j \leq p$, $x_2$ pour $i, j > p$ et $y_1$ pour $i \leq p$ et $j > p$, avec $p \in \{4, 5, 6\}$.

Dans le cas de la répartition $(5,3)$, il suffit de constater que l'on a $s = 8$ si $(x_1, x_2, y_1) = (1/4, 1/8, 1/16)$. [La valeur $y_1 = 1/8$ proposée dans [Za] entraîne $s = r = 13$, et ne réalise donc pas les minima possibles pour $s$ et $r$.]

On vérifie que l'on obtient des exemples avec $s = 16$ dans les cas des répartitions $(4,4)$ et $(6,2)$ en utilisant les valeurs données par Zahareva, à savoir $(x_1, x_2, y_1) = (1/4, 1/4, 0)$ et $(x_1, x_2, y_1) = (3/10, 1/8, 1/8)$ respectivement, et que l'on a $r = 15$ dans les deux cas.

Il reste à prouver que $s = 16$ est le minimum possible. Dans le second cas, cela résulte du théorème 2.2. Dans le premier cas, on utilise une identité de Zahareva : en posant $f = e_1 + e_2 + e_3 + e_4$ et $g = e_5 + e_6 + e_7 + e_8$, d'où $e = \frac{f+2g}{5}$, et $e' = 2e - g = \frac{2f-g}{5}$, on a

$$\begin{aligned}
&\sum_{i=5}^{8}(N(e-e_i)-1) + \sum_{i=1}^{4}(N(e'-e_i)-1) \\
&= 4N(e) - 2e\,.\,g + 4N(e') - 2e'\,.\,f \\
&= 4N(e) + 4N(e') - \frac{4}{5}(N(f)+N(g)),
\end{aligned}$$

$N(e) = \frac{1}{25}(N(f) + 4N(g) + 4f\,.\,g)$, $N(e') = \frac{1}{25}(N(g) + 4N(f) - 4f\,.\,g)$, ce qui entraîne $N(e) + N(e') = \frac{1}{5}(N(f) + N(g))$, et donc $\sum_{i=5}^{8}(N(e-e_i) - 1) + \sum_{i=1}^{4}(N(e'-e_i) - 1) = 0$. Comme il s'agit d'une somme de termes non négatifs, chacun d'eux est nul, ce qui prouve que les 8 vecteurs $e - e_i$ $(i = 5,6,7,8)$ et $e' - e_i$ $(i = 1,2,3,4)$ sont minimaux. $\square$

Quotients d'ordre 6.

Nous examinons les 6 répartitions $(5,2,1)$, $(4,3,1)$, $(3,4,1)$, $(4,2,2)$, $(3,3,2)$ et $(2,4,2)$, avec au plus 3 valeurs des produits scalaires $e_i\,.\,e_j$, $i<j$, notées $x_1, x_2$, si $i,j$ correspondent à $m_1, m_2$ respectivement, et $y_1$ s'ils correspondent à $(m_1,m_2)$. (Les autres produits scalaires peuvent être pris égaux à 0 d'après 8.7.)

On s'occupe d'abord des 5 répartitions pour lesquelles le théorème de Watson appliqué à $e$, $2e$ ou $3e$ fournit des vecteurs minimaux supplémentaires.

$(5,2,1)$. Dans ce cas, on a $\sigma = 12$. Des égalités $N(e) = N(e-e_6) = 1$, on déduit $x_1 = \frac{4x_2+3}{10}$ et $y_1 = \frac{-2x_1+1}{5}$. De $N(e-e_1-e_6-e_7) \geq 1$, on déduit alors que l'on a $x_2 \geq \frac{1}{2}$, i.e. $x_2 = \frac{1}{2}$, donc $x_1 = \frac{1}{2}$ et $y_1 = 0$. Ainsi, $\Lambda$ est semblable à un réseau de racines, qui ne peut être que $\mathbb{E}_8$, et $\Lambda'$ est semblable à $\mathbb{A}_5 \perp \mathbb{A}_2 \perp \mathbb{A}_1$, pour lequel on a $r' = s' = 19 > 8$. Les écritures

$$\begin{aligned} e &= \frac{(e_1-e_2)+e_3+e_4+e_5+2e_2+2e_6+2e_7+3e_8}{6} \\ &= \frac{(e_1-e_2)+(e_3-e_4)+e_5+2e_2+2e_4+2e_6+2e_7+3e_8}{6} \end{aligned}$$

montrent que $(\mathbb{E}_8, \mathbb{A}_5 \perp \mathbb{A}_2 \perp \mathbb{A}_1)$ réalise aussi les répartitions $(4,3,1)$ et $(3,4,1)$.

$(4,2,2)$. En écrivant $e = \dfrac{\frac{e_1+e_2+e_3+e_4+2e_5-e_6}{3}+e_6+e_7+e_8}{2}$, on voit que l'on doit avoir $4y_1+2x_2 = 1$. Soit $e' = 2e-e_5-e_6-e_7-e_8$. Les minorations $N(e') \geq 1$ et $N(e'-e_1) \geq 1$ s'écrivent alors $12x_1+10x_2 \geq 7$ et $-12x_1+8x_2 \geq 2$, d'où $x_2 \geq \frac{1}{2}$, i.e. $x_2 = \frac{1}{2}$, puis $x_1 = \frac{1}{6}$. On trouve un unique réseau $\Lambda$, avec $s = 36$ et $r = 28$, et l'on a $r' = s' = 9$ (le vecteur $e_5 - e_6$ est minimal).

$(3,3,2)$. Le réseau $\Lambda$ contient $e' = \frac{e_1+e_2+e_3-e_4-e_5-e_6}{3}$, auquel sont associés 6 vecteurs minimaux, dont l'existence impose que l'on ait $x_2 = x_1$ et entraîne les minorations $s \geq 14$ et $r \geq 13$. On réalise $s = 14$ (et donc $r = 13$) en prenant par exemple $x_1 = x_2 = \frac{1}{5}$ et $y_1 = -\frac{1}{24}$.
[Ici encore, l'exemple de [Za] (forme 38) ne minimise pas $s$.]

$(2,4,2)$. Le réseau $\Lambda$ contient les deux vecteurs $e' = \frac{e_1+e_2+e_3-e_4-e_5-e_6}{3}$ et $e'' = \frac{e_1+e_2+e_7+e_8}{2}$, auxquels sont associés respectivement 6 et 8 vecteurs minimaux, d'où $s \geq 22$, et dont l'existence impose les relations $3x_2+2y_1 = x_1 = 0$, ce qui permet de calculer les produits scalaires $e_i\,.\,e_j$ en fonction d'un unique paramètre $t$, par $x_2 = 2t$ et $y_1 = -3t$. On trouve alors $N(\frac{e_1+e_2-e_3-e_4-e_5-e_6}{3}) = \frac{2+24t}{3}$, d'où $t \geq \frac{1}{24}$, et $N(\frac{2e_1+2e_2+e_3+e_4+e_5+e_6}{3}) = \frac{4-24t}{3}$, d'où $t \leq \frac{1}{24}$. Il y a donc au plus un réseau qui, en plus des 22 vecteurs signalés et des deux précédents, doit contenir les vecteurs minimaux $e$, $e-e_8$, $e-e_7$ et $e-e_7-e_8$, d'où $s \geq 28$. On vérifie qu'il existe, et que l'on a $s=28$ et $r=22$.

<u>$(3,4,1)$</u>. Le vecteur $e'' = \frac{e_1+e_2+e_3+e_8}{2}$ est minimal ce qui impose $x_1 = 0$, et l'écriture $e = \frac{e''+e_4+e_5+e_6+e_7+e_8}{3}$ montre que les vecteurs $e-e_i$ et $e-e_i-e_8$ sont minimaux pour $i = 4,5,6,7$. Les égalités $N(e) = N(e-e_4) = 1$ s'écrivent $12x_2+12y_1 = 2$ et $-6x_2+3y_1 = -1$, i.e. $y_1 = 0$ et $x_2 = 1/6$. Il y a un unique réseau possible, pour lequel on vérifie que l'on a $s=31$ et $r=26$.

<u>$(4,3,1)$</u>. On considère les vecteurs $e$,
$e' = 2e-e_5-e_6-e_7-e_8 = \frac{e_1+e_2+e_3+e_4-e_5-e_6-e_7}{3}$ et
$e'' = 3e-e_5-e_6-e_7-e_8 = \frac{e_1+e_2+e_3+e_4e+e_8}{2}$. On a $N(e''-e_3-e_4) = \frac{5-4x_1}{4} \geq 1$, d'où $x_1 \leq \frac{1}{4}$, puis $N(e-e_5) = \frac{12x_1-24x_2+37}{36} \geq 1$, d'où $x_2 \leq \frac{1+12x_1}{24} \leq \frac{1}{6}$, puis $N(e) = \frac{12x_1+24x_2+48y_1+25}{36}$, d'où $y_1 \geq \frac{11-12x_1-24x_2}{48} \geq \frac{4}{48} = \frac{1}{12}$. On en déduit la majoration $N(e') = \frac{12x_1+6x_2-24y_1+7}{9} \leq 1$, et l'égalité $N(e') = 1$ n'est possible que pour $x_1 = \frac{1}{4}$, $x_2 = \frac{1}{6}$ et $y_1 = \frac{1}{12}$. On trouve un unique réseau possible, dont on vérifie qu'il a les invariants $s=27$ et $r=25$.

On constate que, dans tous les cas, $s$ et $r$ dépassent la valeur $n=8$, et que les valeurs minimales de $s'$ et de $r'$ sont $r'=s'=8$, sauf dans le cas des répartitions $(5,2,1)$ et $(4,2,2)$.

<u>QUOTIENTS D'ORDRE 7</u>.

Nous montrons maintenant l'impossibilité de l'indice 7, et vérifions essentiellement que les démonstrations de Zahareva sont correctes. Nous devons examiner les 3 répartitions $(3,4,1)$, $(4,2,2)$ et $(3,3,2)$. Les deux premières, pour lesquelles $\sigma = 14$, sont facilement traitées par la méthode de Watson. Pour la troisième, on utilise une identié de Zahararova.

<u>$(3,4,1)$</u>. Soit $e'_1 = e_1 - e$. On a $e = \frac{e'_1+e_2+e_3+2e_4+2e_5+2e_6+2e_7+3e_8}{6}$, si bien que $e'' = \frac{e'_1+e_2+e_3+e_8}{2}$ est un vecteur minimal de $\Lambda$. On a donc $e_8 \,.\, e_2 = e_8 \,.\, e_3 = 0$, et de même $e_8 \,.\, e_1 = 0$, et aussi $e_8 \,.\, e'_1 = 0$, d'où $e_8 \,.\, e = e_8 \,.\, e_1 - e_8 \,.\, e'_1 = 0$ et donc $N(e-e_8) \geq 2$, alors que l'écriture $e = \frac{e''+e_4+e_5+e_6+e_7+e_8}{3}$ entraîne que $e-e_8$ est minimal.

$\underline{(4,2,2)}$. Soit encore $e_1' = e_1 - e$, et soit $f = \frac{e_1'+e_2+e_3+e_4-e_5-e_6}{3}$. Alors, $f+e_5$ est minimal, et l'on a $e = \frac{(f+e_5)+e_6+e_7+e_8}{2}$, donc $e_7 \,.\, e_6 = e_7 \,.\, e_8 = 0$, i.e. $y_3 = x_3 = 0$. Parmi les $2 \times 36$ vecteurs minimaux associés à la répartition $(4,2,2)$ pour l'indice 6 figurent $e_5 - e_6$, d'où $x_2 = \frac{1}{2}$, ainsi que $f$ et $e$, d'où $e \,.\, e_i = \frac{1}{2}$ pour tout $i$. Appliquées avec $i = 1,5,7$, ces dernières conditions s'écrivent
$$\frac{1}{2} = \frac{1}{7}(1+3x_1+4y_1+6y_2) = \frac{1}{7}(4y_1+2+2x_2++6y_3) = \frac{1}{7}(4y_2+4y_3+3+3x_3)\,.$$
L'unique possibilité est alors $x_1 = \frac{5}{12}$, $x_2 = \frac{1}{2}$, $y_1 = y_2 = \frac{1}{8}$, $x_3 = y_3 = 0$. Comme $f$ et donc aussi $f - e_2$ et $f + e_6$ sont des vecteurs minimaux, on a $f \,.\, e_2 = -f \,.\, e_6 = \frac{1}{2}$, et finalement $N(f - e_2 + e_6) = 1 - 2y_1 = \frac{3}{4} < 1$.

$\underline{(3,3,2)}$. Posons $f = e_1 + e_2 + e_3$, $g = e_4 + e_5 + e_6$ et $h = e_7 + e_8$. Alors, $\Lambda$ contient les vecteurs $e = \frac{f+2g+3h}{7}$, $e' = \frac{2f-3g-h}{7}$ et $e'' = \frac{3f-g+2h}{7}$. Par des calculs analogues à ceux qui ont été faits pour étudier la répartition $(6,2)$ dans le cas de l'indice 5, on montre l'identité
$$N(e) + \sum_{i=7}^{8} N(e - e_i) + \sum_{i=4}^{6} N(e' + e_i) + \sum_{i=1}^{3} N(e'' - e_i) = 8\,,$$
qui est impossible car le premier membre est la somme des normes de 9 vecteurs non nuls.

<u>Quotients d'ordre 9</u>.

Il est maintenant facile de démontrer l'impossibilité des quotients cycliques d'ordre 9. Il suffit pour cela de prouver que les vecteurs $e-e_i$ sont minimaux lorsque $a_i = 2$, car on en déduit alors (vu que $m_2$ n'est jamais nul) un quotient $\Lambda/L$ d'ordre 7. C'est clair dans le cas des répartitions $(3,2,1,2)$ et $(2,3,2,1)$, pour lesquelles $\sigma = 18$, et cela se vérifie dans le cas de la répartition $(2,2,2,2)$ en écrivant
$$e = \frac{(f + e_3) + e_4 + e_5 + e_6 + e_7 + e_8}{3}$$
avec
$$f = \frac{e_1 + e_2 - e_3 - e_4 + e_7 + e_8}{3}\,.$$

<u>Quotients d'ordre 8</u>.

Il reste à traiter le cas délicat de l'indice 8, pour lequel les démonstrations de [Za] ne sont pas correctes (page 132, ligne 7, apparaît un dénominateur 4 dans l'expression de $4e$ alors que $8e$ est un vecteur de $\Lambda'$). En outre, nous donnerons des versions très simplifiées de certaines démonstrations de [Za].

Parmi les 8 répartitions *a priori* possibles, on doit exclure les 5 répartitions avec $\sigma = 16$, qui (vu que $m_1$ n'est jamais nul) entraîneraient l'existence d'un quotient d'ordre $7$. Il reste donc à examiner les 3 répartitions $(3,2,2,1)$, $(2,3,2,1)$ et $(3,1,3,1)$. Parmi les 6 paramètres $x_1$, $x_2$, $x_3$, $y_1$, $y_2$, $y_4$ qu'il faut considérer (sauf que $x_2$ n'intervient pas dans le dernier cas), on a les restrictions supplémentaires $y_1 = y_4 = 0$ dans le cas des deux dernières répartitions, car $(e_1,e_2,e_3,e_4,e_5,e_6,e_7,e_8) \mapsto (e_6,e_7,-e_3,-e_4,-e_5,e_1,e_2,e_8)$ échange $e$ et $3e$ modulo $\Lambda'$.

$\underline{(2,3,2,1)}$. On peut représenter $e$ sous la forme

$$f = \frac{e_1+e_2-e_6-e_7}{2}\,,\ g = \frac{f+e_3+e_4+e_5}{2} \quad \text{et} \quad e = \frac{g+e_6+e_7+e_8}{2}\,,$$

ce qui entraîne les relations d'orthogonalité supplémentaires $x_1 = x_2 = x_3 = y_2 = 0$. On a aussi $e_6\,.\,g = 0$, d'où $y_4 = -\frac{1}{3}e_6\,.\,f = \frac{1}{6}$, qui contredit la possibilité de choisir $y_4$ nul.

$\underline{(3,1,3,1)}$. Soit $f = \frac{e_1+e_2+e_3-e_5-e_6-e_7+2e_4}{4}$. Comme $f$ et $f+e_6$ sont minimaux, on a $e_6\,.\,f = \frac{1}{2}$. Mais on a $e = \frac{(f+e_5)+e_6+e_7+e_8}{2}$, d'où, comme $f+e_5$ est aussi minimal, les relations $e_6\,.\,e_7 = 0$, i.e. $x_3 = 0$, et $e_6\,.\,f = -e_6\,.\,e_5 = -x_3 = 0$.

$\underline{(3,2,2,1)}$. Ici, les inégalités de Watson ne suffisent pas à prouver l'impossibilité de cette répartition. Nous allons rechercher une contradiction entre diverses inégalités provenant de minorations de norme de vecteurs en nous plaçant dans le cas où les produits scalaires dépendent des 6 paramètres $x_1 = e_1\,.\,e_2 = e_1\,.\,e_3 = e_2\,.\,e_3$, $x_2 = e_4\,.\,e_5$, $x_3 = e_6\,.\,e_7$, $y_1 = e_1\,.\,e_4 = e_2\,.\,e_4 = e_3\,.\,e_4 = e_1\,.\,e_5 = e_2\,.\,e_5 = e_3\,.\,e_5$, $y_2 = e_1\,.\,e_6 = e_2\,.\,e_6 = e_3\,.\,e_6 = e_1\,.\,e_7 = e_2\,.\,e_7 = e_3\,.\,e_7$ et $y_4 = e_4\,.\,e_6 = e_5\,.\,e_6 = e_4\,.\,e_7 = e_5\,.\,e_7$, vérifiant comme toujours le double encadrement $-\frac{1}{2} \le x_i, y_j \le +\frac{1}{2}$.

On a $e = \dfrac{e_1+e_2+e_3+2e_4+2e_5+3e_6+3e_7+4e_8}{8}$. On pose

$$g = \frac{e_1+e_2+e_3-e_6-e_7}{2} \quad \text{et} \quad f = \frac{e_1+e_2+e_3-e_6-e_7+2e_4+2e_5}{4}\ ;$$

on a $f = \frac{g+e_4+e_5}{2}$ et $e = \frac{f+e_6+e_7+e_8}{2}$. On considère en outre

$$\begin{aligned} e' &= \frac{3e_1+3e_2+3e_3-2e_4-2e_5+e_6+e_7+4e_8}{8} \\ &= 3e-e_4-e_5-e_6-e_6-e_8 \equiv 3e \mod \Lambda'\,. \end{aligned}$$

En utilisant les 4 inégalités $N(\frac{g\pm e_4\pm e_5}{2}) \geq 1$, on voit que l'on a $N(g) \geq 2$. En minorant par 2 la norme de $g$ et par 1 les normes de $g+e_6+e_7$, $g+e_6$, $g+e_6-e_1$, $g-e_1-e_2$, on obtient les 5 inégalités

(g1) $$6x_1+2x_3-12y_2 \geq +3$$

(g2) $$6x_1+2x_3+12y_2 \geq -1$$

(g3) $$6x_1-2x_3 \geq -1$$

(g4) $$-2x_1-2x_3 \geq -1$$

(g5) $$-2x_1+2x_3+4y_2 \geq -1$$

dont nous allons montrer qu'elles entraînent les suivantes :

$$x_1 \geq 0\,, \quad ax_1+bx_2 \leq \frac{1}{2}\max(a,b)\ (\forall\, a,\, b \geq 0)\,, \quad y_2 \leq 0\,, \quad x_3 \geq 0\,.$$

En effet, on a $6x_1+2x_3 \geq 0$ par (g1) et (g2), puis $x_1 \geq 0$ par (g3) ; on a ensuite $x_1+x_2 \leq \frac{1}{2}$ par (g4) et donc $ax_1+bx_2 = (a-b)x_1+b(x_1+x_2) = (b-a)x_3+b(x_1+x_2) \leq \max(a,b)(x_1+x_3)$ ; (g1) entraîne alors la majoration $12y_2 \leq -3+6x_1+2x_3 \leq 0$, et la combinaison (g1)+3(g5) s'écrit $x_3 \geq 0$.

En minorant par 1 les normes de $f$, $e$, $e'$, $e-e_4$, $f-e_4-e_5$ et $f-e_1$, on obtient

(f1) $$6x_1+8x_2+2x_3+24y_1-12y_2-16y_4 \geq 3$$

(e1) $$6x_1+8x_2+18x_3+24y_1+36y_2+48y_4 \geq 19$$

(e'1) $$54x_1+8x_2+2x_3-72y_1+36y_2-16y_4 \geq 11$$

(e2) $$6x_1-24x_2+18x_3-24y_1+36y_2-48y_4 \geq -13$$

(f2) $$6x_1+8x_2+2x_3-24y_1-12y_2+16y_4 \geq 3$$

(f3) $$-10x_1+8x_2+2x_3-8y_1+4y_2-16y_4 \geq 3$$

La combinaison $\frac{1}{2}$(f1)+$\frac{1}{4}$(e1)+$\frac{1}{4}$(e'1) conduit à $18x_1+8x_2+6x_3+12y_2 \geq 9$, d'où $8x_2 \geq 9-(18x_1+6x_3)-12y_2 \geq 0$, alors que la combinaison $\frac{1}{2}$(e1)+$\frac{1}{2}$(e2)+3(g1) conduit à $24x_1-8x_2+24x_3 \geq 12$, d'où $8x_2 \leq 24(x_1+x_3)-12 \leq 0$. On en déduit les deux égalités $x_2=0$ et $x_1+x_3=\frac{1}{2}$, et l'inégalité $18x_1+8x_2+6x_3+12y_2 \geq 9$ peut maintenant s'écrire $12x_1+12y_2 \geq 9-6(x_1+x_3)=6$, i.e. $x_1-|y_2| \geq \frac{1}{2}$, ce qui n'est possible que pour $x_1=\frac{1}{2}$ et $y_2=0$. Finalement, on trouve

$$x_1 = \frac{1}{2} \quad \text{et} \quad x_2=x_3=y_2=0\,.$$

En remplaçant $x_1,x_2,x_3,y_2$ dans par les valeurs ci-dessus dans (f1) et (f2), il vient $24y_1-16y_4 \geq 0$ et $-24y_1+16y_4 \geq 0$, donc $24y_1=16y_4$, et en procédant de même avec les identités (e1) et (e2), on obtient la relation $24y_1 + 48y_4 = 16$, ce qui impose que l'on ait $y_1 = \frac{1}{6}$ et $y_4 = \frac{1}{4}$, valeurs qui contredisent l'identité (f3).

Cela prouve que la repartition $(3,1,3,1)$ n'existe pas , complétant ainsi la classification en dimension 8 des types de couples $(\Lambda,\Lambda')$ à quotients cycliques.

Remarque 9.2. Les quotients cycliques d'ordres $d = 7$ et $d = 8$ existent en dimension $9$.

Pour $d = 7$, on peut utiliser la répartition $(3,3,3)$, avec des produits scalaires vérifiant les conditions $x_1 = x_2 = x_3$ et $y_2 = y_3 = -y_1$, par exemple $x_1 = 1/4$ et $y_1 = 0$. On a alors $s = 18$ et $r = 17$, valeurs minimales pour cette répartition.

Pour $d = 8$, on peut utiliser la répartition $(2,3,2,2)$. En prenant les produits scalaires $e_i \,.\, e_j$ nuls, on obtient $s = 33$ et $r = 27$, valeurs également minimales pour cette répartition.

## 10. Quotients non cycliques en dimension 8

Vu la majoration de l'indice par $\gamma_n^{n/2}$ et les classifications faites dans les cas cycliques, 2-élémentaires et de dimension $n \le 7$, il n'y a plus à considérer que les quotients de type $(3,3)$, $(4,2)$ ou $(4,4)$ en dimension $8$. Ce dernier cas est clairement impossible si l'on admet que, en dimension $8$, l'invariant d'Hermite atteint son maximum seulement sur le réseau $\mathbb{E}_8$, et, si l'on veut se contenter de la majoration $\gamma_8^4 < 17$, la démonstration ne présente aucune difficulté une fois classés les quotients de type $(4,2)$.

Commençons par l'indice $9$.

Théorème 10.1. *Si $n = 8$ et $[\Lambda : \Lambda'] = 9$, alors $\Lambda/\Lambda' \simeq (3,3)$ et $(\Lambda,\Lambda') \sim (\mathbb{E}_8, \mathbb{A}_2^{4\perp})$.*

*Démonstration.* Que $\Lambda/\Lambda'$ ne soit pas cyclique a été démontré au §9. Considérons donc le cas d'un quotient $\Lambda/\Lambda'$ de type $(3,3)$.

On peut engendrer $\Lambda$ par adjonction à $\Lambda'$ de deux vecteurs de la forme $\frac{1}{3}\sum_{i=0}^{8} a_i e_i$, avec $a_i \in \{0,\pm 1\}$. Les suites $(a_i)$ mod 3 attachées à ces deux vecteurs engendrent un code ternaire dont le poids doit être au moins $6$, puisque l'indice $3$ n'apparaît pas avant la dimension $6$. On voit tout de suite qu'un tel code est équivalent au code de matrice génératrice

$\left(\begin{smallmatrix} 1&1&1&1&1&1&0&0\\ 0&0&1&1&-1&-1&1&1 \end{smallmatrix}\right)$ (*code de répétition du tétracode*). On peut donc écrire $\Lambda = \langle \Lambda', e, f\rangle$ avec

$$e = \frac{e_1+e_2+e_3+e_4+e_5+e_6}{2} \quad \text{et} \quad f = \frac{e_3+e_4-e_5-e_6+e_7+e_8}{2}\,.$$

Divisons l'ensemble $\{1,2,\dots,8\}$ en les quatre blocs $\{1,2\}$, $\{3,4\}$, $\{5,6\}$, $\{7,8\}$, et considérons les deux vecteurs

$$g = \frac{e_1+e_2-e_3-e_4+e_7+e_8}{3} \quad \text{et} \quad h = \frac{e_1+e_2-e_5-e_6-e_7-e_8}{3}\,,$$

congrus respectivement à $e+f$ et $e-f$ modulo $\Lambda'$.

En appliquant la proposition 2.3, (1) à $e$ (resp. à $f$), on obtient les inégalités $e_i\,.\,e_j \geq 0$ pour $1 \leq i < j \leq 6$ (resp. $e_i\,.\,e_j \leq 0$ pour $i \in \{2,3,7,8\}$ et $j \in \{5,6\}$). En considérant plus généralement chacun des six couples de deux vecteurs pris parmi $\{e,f,g,h\}$, on voit que les produits scalaires $e_i\,.\,e_j$ sont nuls chaque fois que $i$ et $j$ appartiennent à des blocs distincts. Puisque les vecteurs $e$ et $e-e_i$ ($i \leq 6$) sont minimaux, on a $e\,.\,e_i = \frac{1}{2}$ pour tout $i \leq 6$ (exemple 3.6). Ainsi, pour tout bloc $\{i,i'\}$ avec $i,i' \leq 6$, on a $\frac{1}{2} = e\,.\,e_i = e\,.\,e_{i'} = \frac{1+e_i\,.\,e_{i'}}{3}$, et donc $e_i\,.\,e_{i'} = \frac{1}{2}$. En raisonnant de la même façon avec $f$, on obtient le même résultat pour $i,i' \geq 3$.

En identifiant chacun des plans défini par l'un des quatre blocs à l'anneau des entiers d'Eisenstein, on reconnaît la construction de $\mathbb{E}_8$ par le tétracode ternaire. $\square$

Nous passons maintenant à l'indice $8$. On sait que le quotient ne peut pas être cyclique. La classification des quotients $2$-élémentaires ayant été discutée au § 4, nous nous restreignons au cas des quotients de type $(4,2)$, pour lesquels nous donnons d'abord des conditions d'existence s'appliquant à une dimension $n$ arbitraire.

On note $m$ le plus petit entier tel qu'il existe $L \subset \Lambda$ de rang $m$ vérifiant les quatre conditions : $L' = L \cap \Lambda$ est engendré par $n-m$ des vecteurs $e_i$, que l'on suppose (quitte à permuter les $e_i$) être $e_1,\dots,e_m$, $L/L' \simeq \Lambda/\Lambda'$, $N(L) = N(\Lambda)$ et $S(\Lambda) = S(L) \cup \{e_{m+1},\dots,e_n\}$.

Il existe deux vecteurs $e,f \in L$ avec $4e \in L'$, $2f \in L'$, $f \not\equiv 2e$ mod $L'$ et $L = \langle L', e, f\rangle$. Comme $e$ est d'ordre 4 modulo $\Lambda'$, on peut, après permutation éventuelle de $e_1,\dots,e_m$, le supposer de la forme $e = \dfrac{e_1+\cdots+e_p+2e_{p+1}+\cdots+2e_{p+q}}{4}$. Le lemme suivant résulte tout de suite de la proposition 5.1 :

LEMME 10.2. *Les entiers* $p,q,m,n$ *vérifient les inégalités* $7 \leq p+q \leq m \leq n$, $p \geq 4$, *et* $p \leq 6$ *if* $p+q=7$. $\square$

En combinant ce lemme avec les résultats concernant les quotients de type $(2,2)$, nous démontrons maintenant :

PROPOSITION 10.3. *Supposons* $\Lambda/\Lambda'$ *de type* $(4,2)$. *Alors, il existe des générateurs de* $\Lambda$ *sur* $\Lambda'$ *de la forme*

$$e = \frac{e_1 + \cdots + e_\mu + 2(e_{\mu+1} + \cdots + e_{\mu+\nu})}{4} \qquad et$$
$$f = \frac{e_1 + \cdots + e_{\mu'} + e_{\mu+1} + \cdots + e_{\nu'} + e_{\mu+\nu+1} + \cdots + e_{\mu+\nu+\pi'}}{2}$$

*tels que les entiers* $n,m,\mu,\nu,\mu',\nu',\pi'$ *satisfassent les conditions* $m = \mu+\nu+\pi' \leq n$, $\mu' \leq \frac{\mu}{2}$, $\nu' \leq \nu$ *et* $\nu' \leq \pi'$. *De plus, ces 7 entiers sont des invariants du code associé au couple* $(\Lambda,\Lambda')$.

*Démonstration.* On choisit $e$ et $f$ d'ordres respectifs 4 et 2 modulo $L'$. Le lemme précédent prouve que l'on peut permuter les $e_i$ de façon que $e$ ait la forme voulue, et une permutation supplémentaire permet de faire en sorte qu'il en soit de même de $f$. On a alors évidemment $\mu' \leq \mu$, $\nu' \leq \nu$ et $\mu+\nu+\pi' \leq n$.

Les classes de $\Lambda$ d'ordre 4 modulo $\Lambda'$ sont alors $\pm e+\Lambda'$ et $\pm(e+f)+\Lambda'$, et l'on a

$$e+f \equiv \frac{-e_1 - \cdots - e_{\mu'} + e_{\mu'+1} + \cdots + e_\mu + 2(e_{\mu+\nu'+1} + \cdots + e_{\mu+\nu+\pi'})}{4}.$$

En changeant les signes des $\mu'$ premiers $e_i$, on voit tout de suite que $\mu$ est un invariant du couple $(\Lambda,\Lambda')$, et que l'on peut en outre supposer que l'on a $\nu \leq \nu+\pi'-\nu'$, i.e. $\nu' \leq \pi'$.

Les classes de $\Lambda$ d'ordre 2 modulo $\Lambda'$ sont représentées par $2e$, $f$ et $f+2e$, Échanger les classes de $f$ et de $f+2e$ revient à remplacer $e_1 + \cdots + e_{\mu'}$ par $e_{\mu'+1} + \cdots + e_\mu$, ce qui nous permet de supposer que l'on a $\mu' \leq \mu - \mu'$, i.e. $\mu' \leq \frac{\mu}{2}$. $\square$

LEMME 10.4. *Si* $\Lambda/\Lambda'$ *est de type* $(4,2)$, *on a* $n \geq m \geq 8$, *et* $\nu' = \pi' = 1$ *si* $n = 8$.

*Démonstration.* On a $\mu+\nu \geq 7$, donc $m \geq \pi'+7$, et par conséquent $m \geq 8$ ou $\pi' = 0$, et $\pi' = 0$ entraîne $\nu' = 0$, donc $\mu' \geq 4$, et par suite $m \geq \mu \geq 2\mu' \geq 8$.

Supposons maintenant que l'on ait $n = 8$.

Si $\pi' = 0$, on a $e = \frac{e_1+\cdots+e_8}{4}$, ce qui entraîne que les vecteurs

$$f = \frac{e_1+e_2+e_3+e_4}{2} \quad \text{et} \quad 2e-f = \frac{e_5+e_6+e_7+e_8}{2}$$

sont tous deux minimaux, ce qui est impossible, car $e = \frac{f+(2e-f)}{2}$.

Nous pouvons donc supposer que $\pi' = 1$. Alors, $\nu' = 0$ ou $\nu' = 1$. Si $\nu' = 0$, alors $\mu' \geq 3$, donc $\mu \geq 6$, i.e. $\mu = 6$. Mais $f$, $f' = \frac{e_4+e_5+e_6-e_8}{2}$ et $e_7$ sont alors minimaux, et ceci est encore impossible, vu la relation $e = \frac{f+f'-e_7}{2}$. $\square$

Dans l'énoncé du théorème suivant, $f'$ désigne le vecteur de $\Lambda$ congru à $2e+f$ modulo $\Lambda'$ qui est la demi-somme de certains des vecteurs $e_i$.

THÉORÈME 10.5. *Si $n = 8$ et si $\Lambda/\Lambda'$ est de type $(4,2)$, on peut écrire $\Lambda = \langle \Lambda', e, f\rangle$ avec $e$ et $f$ de l'une des formes suivantes:*

*(a):* $(\mu,\nu,\mu',\nu',\pi') = (4,3,2,1,1)$.

$$e = \frac{e_1+e_2+e_3+e_4+2e_5+2e_6+2e_7}{4}$$
$$f = \frac{e_1+e_2+e_5+e_8}{2}$$
$$e-f = \frac{-e_1-e_2+e_3+e_4+2e_6+2e_7-2e_8}{4}$$
$$f' = \frac{e_3+e_4+e_5+e_8}{2}\,.$$

*(b):* $(\mu,\nu,\mu',\nu',\pi') = (5,2,2,1,1)$.

$$e = \frac{e_1+e_2+e_3+e_4+e_5+2e_6+2e_7}{4}$$
$$f = \frac{e_1+e_2+e_6+e_8}{2}$$
$$e-f = \frac{-e_1-e_2+e_3+e_4+e_5+2e_7-2e_8}{4}$$
$$f' = \frac{e_3+e_4+e_5+e_6+e_8}{2}\,.$$

*(c):* $(\mu,\nu,\mu',\nu',\pi') = (6,1,3,1,1)$.

$$e = \frac{e_1+e_2+e_3+e_4+e_5+e_6+2e_7}{4}$$
$$f = \frac{e_1+e_2+e_3+e_7+e_8}{2}$$
$$e-f = \frac{-e_1-e_2-e_3+e_4+e_5+e_6-2e_8}{4}$$
$$f' = \frac{e_4+e_5+e_6+e_7+e_8}{2}\,.$$

*Ces trois possibilités se présentent avec* $\Lambda = \mathbb{E}_8$ *et* $\Lambda' = \mathbb{A}_3 \perp \mathbb{A}_3 \perp \mathbb{A}_1 \perp \mathbb{A}_1$ .

*Démonstration.* Le lemme précédent montre que l'on a $\nu' = \pi' = 1$, donc $\mu' \geq 2$, i.e. $\mu' = 2$ ou $\mu' = 3$. On voit facilement que cette condition ne permet que les trois possibilités énoncées dans le théorème ainsi qu'une quatrième, à savoir

(d) : $(\mu, \nu, \mu', \nu', \pi') = (6, 1, 2, 1, 1)$

$$e = \frac{e_1 + e_2 + e_3 + e_4 + e_5 + e_6 + 2e_7}{4}$$
$$f = \frac{e_1 + e_2 + e_7 + e_8}{2}$$
$$e - f = \frac{-e_1 - e_2 + e_3 + e_4 + e_5 + e_6 - 2e_8}{4}$$
$$f' = \frac{e_3 + e_4 + e_5 + e_6 + e_7 + e_8}{2}\ .$$

L'exemple donné à la fin du §6, avec $\Lambda = \mathbb{E}_8$ , correspond à la structure (c). En y remplaçant $e_1$ par $e_1' = e_1 + e_2$ (resp. $e_1$ par $e_1'$ et $e_5$ par $e_5' = e_5 + e_6$), on obtient la structure (b) (resp. (a)).

Il reste à prouver l'impossibilité de la structure (d). Pour cela, nous remarquons que le groupe $H$ des automorphismes du code sur $\mathbb{Z}/4\mathbb{Z}$ défini par $\Lambda/\Lambda'$ contient la transposition $(e_1, e_2)$, les permutations de $\{e_3, e_4, e_5\}$, les changements de signe de $e_7$ et de $e_8$, et la transformation $(e_1, e_2, e_7, e_8) \mapsto (-e_1, -e_2, -e_8, -e_7)$. On peut donc exprimer les produits scalaires $e_i \,.\, e_j$, $i < j$ en fonction des deux paramètres $x = e_1 \,.\, e_2$ et $y = e_3 \,.\, e_4 = e_3 \,.\, e_5 = e_4 \,.\, e_5$, les autres produits scalaires $e_i \,.\, e_j$, $i < j$ étant nuls. Comme $f \in \Lambda$, on a $x = 0$, et donc $N(e) = \frac{10+6y}{16} \leq \frac{13}{16} < 1$. $\square$

Nous déterminons maintenant l'ensemble $S(\Lambda)$ dans chacun des cas (a), (b), (c).

Dans le cas (a), on connaît *a priori* 48 couples de vecteurs minimaux, 8 pour chacun des ensembles $\Lambda'$, $f + \Lambda'$, $f' + \Lambda'$, $2e + \Lambda'$, $\pm e + \Lambda'$ et $\pm(e + f) + \Lambda'$. Il est immédiat qu'en prenant tous les produits scalaires $e_i \,.\, e_j$, $i < j$ nuls, on obtient un réseau avec $s = 48$ (et $r' = s' = 8$). On contrôle que son rang de perfection est $r = 32$.

L'étude du cas (b) est tout à fait analogue : on se ramène au cas où les produits scalaires $e_i \,.\, e_j$ sont nuls pour $i < j$, sauf $e_3 \,.\, e_4$, $e_3 \,.\, e_5$ et $e_4 \,.\, e_5$, égaux à un même paramètre $y$. On a alors $N(e) = \frac{13+6y}{16} \geq 1$, donc $y \geq \frac{1}{2}$, i.e. $y = \frac{1}{2}$. Cela détermine complètement $\Lambda$ à isométrie près. On vérifie que le réseau obtenu est entier pour la norme 4, et possède les invariants $s = 75$ et $r = 35$. Les réseaux réalisant la structure (b) sont donc ceux de la famille à un paramètre (modulo similitude) de réseaux non parfaits de dimension 8 que Watson a caractérisés par l'inégalité $s \geq 75$ ([W2], théorème 1), ainsi que le réseau $\mathbb{E}_8$. (Pour $y \in [0,1]$, ils décrivent un chemin de Voronoï reliant deux copies de $\mathbb{E}_8$ ; ils contiennent tous une section $\mathbb{E}_7$ ; pour $y = \frac{1}{2}$, $\sqrt{2}\,\Lambda$ est le réseau décrit à la fin des notes du ch. VI de [M].)

Dans le cas (c), on montre que l'on peut se ramener aux deux paramètres $x = e_1 . e_2 = e_1 . e_3 = e_2 . e_3$ et $y = e_4 . e_5 = e_4 . e_6 = e_5 . e_6$, les autres produits scalaires étant nuls. On a alors $N(e) = \frac{10+6x+6y}{16}$, et l'inégalité $N(e) \geq 1$ s'écrit $x + y \geq 1$ et entraîne $x = y = \frac{1}{2}$. On constate sans peine que $\Lambda$ doit être proportionnnel à un réseau de racines, qui ne peut être que $\mathbb{E}_8$ (et l'on a alors $\Lambda' \simeq \mathbb{A}_3 \perp \mathbb{A}_3 \perp \mathbb{A}_1 \perp \mathbb{A}_1$). $\square$

Remarque 10.6. Il résulte des §§4, 5, 9, 10 que toutes les structures de groupes abéliens qui sont réalisables en dimension $n \leq 8$ comme quotient $\Lambda/\Lambda'$ de deux réseaux WR de même norme le sont avec $r' = s'$ (et même $r' = s' = n$ pour $n \leq 7$). Du fait que l'égalité $r' = s'$ est vraie en toute dimension $n \leq 8$, nous n'avons pas mentionné la valeur de $r'$ dans le tableau 11.1.

Nous terminons ce § en donnant quelques compléments sur les couples $(\Lambda, \Lambda')$ de dimension 8 et d'indice multiple de 8. Il y a 8 types à considérer, que nous notons $T_1, \dots, T_8$, définis ainsi : $T_1$ est l'extension à $n = 8$ au moyen de la proposition 8.1 du type $\mathbb{E}_7$ du tableau 11.1, formé des réseaux de la classe de $\mathbb{E}_7 \bigoplus \mathbb{A}_1$, pour lesquels on a $\Lambda/\Lambda' \simeq C_2 \times C_2 \times C_2$ ; les types $T_2, T_3, T_4$ (resp. $T_5, T_6, T_7$) sont ceux du tableau 11.1, partie 2, avec $\Lambda/\Lambda' \simeq C_4 \times C_2$ (resp. $\Lambda/\Lambda' \simeq C_2 \times C_2 \times C_2$), dans l'ordre où ils apparaissent ; le type $T_8$ correspond à l'indice 16 (dernière ligne du tableau). On note $\mathcal{C}_1, \dots, \mathcal{C}_8$ les cellules correspondantes ; $\mathcal{C}_5$ (resp. $\mathcal{C}_4$ et $\mathcal{C}_8$) se réduisent à la classe de similitude de $\mathbb{D}_8$ (resp. de $\mathbb{E}_8$).

Les résultats de Watson rappelés à propos de l'étude du cas (b) du théorème 10.5 démontrent que $\mathcal{C}_3$ a pour adérence $\mathcal{C}_3 \cup \mathcal{C}_4$. En vérifiant que le réseau avec $e_i . e_j = 0$ utilisé pour illustrer le cas (a) du théorème 10.5 représente également le type $T_3$, on prouve que l'ahérence de $\mathcal{C}_2$ contient $\mathcal{C}_3$. Cela justifie les résultats énoncés à la fin du §7.

Pour approfondir l'étude des réseaux parfaits des types $T_1$ à $T_8$, nous aurons besoins des résultats suivants de Baril ([Br]), s'appliquant à un réseau parfait $L$ de dimension 8 et de norme 2 :

(a) Si $L$ possède une section hyperplane isométrique à $\mathbb{E}_7$ (resp. à $\mathbb{D}_7$), il est isométrique à $\mathbb{E}_8$ ou au réseau de Barnes $\mathbb{A}_8^2$ (resp. à $\mathbb{E}_8$ ou à $\mathbb{D}_8$);

(b) Si $L$ est isométrique à une somme directe $\mathbb{D}_6 \bigoplus \mathbb{A}_2$, il possède une section hyperplane isométrique à $\mathbb{E}_7$ ou à $\mathbb{D}_7$.

L'examen du code servant à définir le type $T_2$ montre tout de suite que les réseaux de l'adhérence de la cellule $\mathcal{C}_2$ sont de la forme $\mathbb{D}_6 \bigoplus \mathbb{A}_2$. Il en résulte que les réseaux parfaits de type $T_2$ sont semblable à l'un des trois réseaux $\mathbb{E}_8, \mathbb{A}_8^2, \mathbb{D}_8$. Comme il n'y a pas de quotient $C_4 \times C_2$ dans les deux derniers cas, nous avons démontré :

PROPOSITION 10.7. *Un réseau* parfait $\Lambda$ *de dimension* $n \leq 8$ *possédant un sous-réseau* $\Lambda'$ *engendré par des vecteurs minimaux de* $S(\Lambda)$ *avec* $\Lambda/\Lambda' \simeq C_4 \times C_2$ *est semblable à* $\mathbb{E}_8$. $\square$

Les réseaux parfaits (de dimension $n \leq 8$) associés à un quotient $C_2 \times C_2 \times C_2$ que nous avons rencontrés (à savoir $\mathbb{E}_7$, $\mathbb{E}_8$, $\mathbb{A}_8^2$ et $\mathbb{D}_8$) possèdent tous une section $\mathbb{D}_6$. Il est probable, mais non démontré, que tout réseau à quotient $C_2 \times C_2 \times C_2$ possède une telle section, et que ceux de ces réseaux qui sont parfaits sont semblables à $\mathbb{E}_7$, $\mathbb{E}_8$, $\mathbb{A}_8^2$ ou $\mathbb{D}_8$.

## 11. RÉSULTATS

Nous présentons sous forme de tableau la classification des types de cellules *primitives* de dimension $n \leq 8$. Rappelons (proposition 8.1) que les cellules non primitives sont représentées par des sommes directes, que l'on peut supposer orthogonales, de la forme $\Lambda \bigoplus N(\Lambda)\mathbb{Z}^{n-\dim(\Lambda)}$, $\Lambda$ représentant une cellule primitive.

Le tableau fait apparaître 42 types au sens de la définition 7.4. (Aux 39 types figurant dans [Za], il faut ajouter 3 types, représentés par des réseaux de dimension 8, à quotients $C_4 \times C_2$.)

Les sept colonnes des deux partie du tableau contiennent les données suivantes :

- la dimension $n$ de $\Lambda$.
- l'ordre $a$ du quotient $A = \Lambda/\Lambda'$.
- L'invariant de Smith de $A$ (suite des diviseurs élémentaires de $A$), la notation $d_1^{m_1} \cdot d_2^{m_2} \cdots d_t^{m_t}$ signifiant que $A$ est isomorphe à un produit

direct $(\mathbb{Z}/d_1\mathbb{Z})^{m_1} \times (\mathbb{Z}/d_2\mathbb{Z})^{m_2} \times \cdots \times (\mathbb{Z}/d_\imath\mathbb{Z})^{m_\imath}$ ; on a $a = d_1^{m_1} \ldots d_\imath^{m_\imath}$, et $d_j$ divise $d_{j-1}$ pour $2 \leq j \leq \imath$.

• des générateurs de $\Lambda$ sur $\Lambda'$, décrits ainsi : on trouve un, deux ou trois vecteurs à $n$ composantes (disons $e^{(1)}$, $e^{(2)}$, $e^{(3)}$ pour fixer les idées), en nombre égal au nombre de termes non triviaux de l'invariant de Smith ; si celui-ci est $d_1 \cdot d_2 \cdot d_3$, on doit adjoindre à $\Lambda'$ les vecteurs $\dfrac{e^{(1)}}{d_1}, \dfrac{e^{(2)}}{d_2}, \dfrac{e^{(3)}}{d_3}$.

On constate que, pour tout $n \leq 8$, il y a une unique cellule minimale associée à chacun des types permis. Il s'ensuit qu'il y a une configuration $S$ de vecteurs minimaux qui est minimale pour l'inclusion. Pour cette configuration, nous donnons

• le nombre $s$ de couples $\pm x$ vecteurs de $S$ ;

• le rang de perfection $r$ de $S$ ;

• le nombre $s'$ de couples de vecteurs de $S \cap \Lambda'$ ; jusqu'à la dimension $8$, c'est aussi le rang de perfection $r'$ de $S \cap \Lambda'$.

Tableau 11.1. Les types de couples $(\Lambda, \Lambda')$ (partie 1)

| $n$ | $a$ | Smith | Générateurs | $s$ | $r$ | $s'$ |
|---|---|---|---|---|---|---|
| 1 | 1 | 1 | | 1 | 1 | 1 |
| 4 | 2 | 2 | $(1,1,1,1)$ | 12 | 10 | 4 |
| 5 | 2 | 2 | $(1,1,1,1,1)$ | 5 | 5 | 5 |
| 6 | 2 | 2 | $(1,1,1,1,1,1)$ | 6 | 6 | 6 |
| 6 | 3 | 3 | $(1,1,1,1,1,1)$ | 12 | 11 | 6 |
| 6 | 4 | $2^2$ | $(1,1,1,1,0,0),(0,0,1,1,1,1)$ | 30 | 21 | 6 |
| 7 | 2 | 2 | $(1,1,1,1,1,1,1)$ | 7 | 7 | 7 |
| 7 | 3 | 3 | $(1,1,1,1,1,1,1)$ | 7 | 7 | 7 |
| 7 | 4 | 4 | $(1,1,1,1,2,2,2)$ | 23 | 19 | 7 |
| 7 | 4 | 4 | $(1,1,1,1,1,2,2)$ | 7 | 7 | 7 |
| 7 | 4 | 4 | $(1,1,1,1,1,1,2)$ | 21 | 19 | 7 |
| 7 | 4 | $2^2$ | $(1,1,1,1,0,0,0),(0,0,0,1,1,1,1)$ | 23 | 19 | 7 |
| 7 | 4 | $2^2$ | $(1,1,1,1,0,0,0),(0,0,1,1,1,1,1)$ | 15 | 13 | 7 |
| 7 | 8 | $2^3$ | $(1,1,1,1,0,0,0),(0,0,1,1,1,1,0),(1,0,1,0,1,0,1)$ | 63 | 28 | 7 |
| 8 | 2 | 2 | $(1,1,1,1,1,1,1,1)$ | 8 | 8 | 8 |
| 8 | 3 | 3 | $(1,1,1,1,1,1,1,1)$ | 8 | 8 | 8 |
| 8 | 4 | 4 | $(1,1,1,1,2,2,2,2)$ | 16 | 14 | 8 |
| 8 | 4 | 4 | $(1,1,1,1,1,2,2,2)$ | 8 | 8 | 8 |
| 8 | 4 | 4 | $(1,1,1,1,1,1,2,2)$ | 8 | 8 | 8 |
| 8 | 4 | 4 | $(1,1,1,1,1,1,1,2)$ | 8 | 8 | 8 |
| 8 | 4 | 4 | $(1,1,1,1,1,1,1,1)$ | 16 | 15 | 8 |

Tableau 11.1. Les types de couples $(\Lambda, \Lambda')$ (partie 2)

| $n$ | $a$ | Smith | Générateurs | $s$ | $r$ | $s'$ |
|---|---|---|---|---|---|---|
| 8 | 4 | $2^2$ | $(1,1,1,1,0,0,0,0), (0,0,0,0,1,1,1,1)$ | 24 | 20 | 8 |
| 8 | 4 | $2^2$ | $(1,1,1,1,0,0,0,0), (0,0,0,1,1,1,1,1)$ | 16 | 14 | 8 |
| 8 | 4 | $2^2$ | $(1,1,1,1,0,0,0,0), (0,0,1,1,1,1,1,1)$ | 16 | 14 | 8 |
| 8 | 4 | $2^2$ | $(1,1,1,1,1,0,0,0), (0,0,0,1,1,1,1,1)$ | 8 | 8 | 8 |
| 8 | 5 | 5 | $(1,1,1,1,2,2,2,2)$ | 16 | 15 | 8 |
| 8 | 5 | 5 | $(1,1,1,1,1,2,2,2)$ | 8 | 8 | 8 |
| 8 | 5 | 5 | $(1,1,1,1,1,1,2,2)$ | 16 | 15 | 8 |
| 8 | 6 | 6 | $(1,1,1,2,2,2,2,3)$ | 31 | 26 | 8 |
| 8 | 6 | 6 | $(1,1,1,1,2,2,2,3)$ | 27 | 25 | 8 |
| 8 | 6 | 6 | $(1,1,1,1,1,2,2,3)$ | 120 | 36 | 19 |
| 8 | 6 | 6 | $(1,1,2,2,2,2,3,3)$ | 28 | 22 | 8 |
| 8 | 6 | 6 | $(1,1,1,2,2,2,3,3)$ | 14 | 13 | 8 |
| 8 | 6 | 6 | $(1,1,1,1,2,2,3,3)$ | 36 | 28 | 9 |
| 8 | 8 | 4.2 | $(1,1,1,1,2,2,2,0), (1,1,0,0,1,0,0,1)$ | 48 | 32 | 8 |
| 8 | 8 | 4.2 | $(1,1,1,1,1,2,2,0), (1,1,0,0,0,1,0,1)$ | 75 | 35 | 8 |
| 8 | 8 | 4.2 | $(1,1,1,1,1,1,2,0), (1,1,1,0,0,0,1,1)$ | 120 | 36 | 14 |
| 8 | 8 | $2^3$ | $(1,1,1,1,0,0,0,0),(0,0,1,1,1,1,0,0),(0,0,0,0,1,1,1,1)$ | 56 | 36 | 8 |
| 8 | 8 | $2^3$ | $(1,1,1,1,0,0,0,0),(0,0,1,1,1,1,0,0),(0,0,0,1,0,1,1,1)$ | 48 | 32 | 8 |
| 8 | 8 | $2^3$ | $(1,1,1,1,0,0,0,0),(0,0,1,1,1,1,0,0),(0,1,0,1,0,1,1,1)$ | 32 | 23 | 8 |
| 8 | 9 | $3^2$ | $(1,1,1,1,1,1,0,0), (0,0,1,1,-1,-1,1,1)$ | 120 | 36 | 12 |
| 8 | 16 | $2^4$ | Code de Hamming étendu | 120 | 36 | 8 |

## APPENDICE : CALCUL DE L'INDICE D'UN SOUS-RÉSEAU

par Christian BATUT

On considère un réseau $\Lambda$ dans l'espace euclidien $E$, que l'on suppose "well rounded", c'est-à-dire tel que ses vecteurs minimaux engendrent $E$ (condition notée (WR) au § 1). Un système $S$ de $n$ vecteurs minimaux indépendants de $\Lambda$ engendre un sous-réseau $\Lambda'$ de $\Lambda$, et le quotient $\Lambda/\Lambda'$ est un groupe abélien fini. Nous avons écrit un programme calculant, pour chaque structure de groupe abélien fini, le nombre de systèmes $S$ pour lesquels $\Lambda/\Lambda'$ possède précisément cette structure.

Ce programme aboutit pourvu que $\binom{s}{n}$ ne soit pas trop grand. En pratique, on atteint la dimension 8 à l'exception du réseau $\mathbb{E}_8$ pour lequel $s = 120$ (et pour lequel le résultat a été obtenu au § 6 grâce à la classification des systèmes de racines). D'après Watson ([W2]), si l'on exclut $\mathbb{E}_8$, on a alors $s \leq 75$ pour $n = 8$ (et probablement $s \leq 71$ si $\Lambda$ est de surcroît parfait, valeur atteinte sur le réseau de Barnes $\mathbb{A}_8^2$). Le résultat pour ce réseau a nécessité trois jours de calcul environ sur une machine SUN Sparc 3. Les structures qui interviennent sont les mêmes que pour $\mathbb{E}_7 \sim \mathbb{A}_7^2$ :

- $\mathbb{A}_8^2$ : (1), (2), (3), (4), (2, 2), (2, 2, 2).

Les réseaux parfaits jusqu'à la dimension 7 se traitent sans difficulté. Voici les listes de quotients qui apparaissent, donnés avec les notations $P_n^i$ introduites par Conway et Sloane dans [C-S1] et utilisées dans [M], chapitre VI; par un théorème de Korkine et Zolotareff, dans le cas où 1 est l'unique indice possible, il n'y a pour tout $n$ que le réseau $\mathbb{A}_n$ :

- (1) : $P_1^1$ ; $P_2^1$ ; $P_3^1$ ; $P_4^2$ ; $P_5^3$ ; $P_6^7$ ; $P_7^{33}$.
- (1), (2) : $P_4^1$ ; $P_5^1$, $P_5^2$ ; $P_6^5$, $P_6^6$ ; $P_7^{32}$.
- (1), (2), (3) : $P_6^1$, $P_6^2$, $P_6^4$ ; $P_7^2$, $P_7^5$, $P_7^{11}$–$P_7^{16}$, $P_7^{18}$–$P_7^{31}$.
- (1), (2), (2, 2) : $P_6^3$ ; $P_7^4$.
- (1), (2), (3), (4) : $P_7^3$, $P_7^6$–$P_7^9$, $P_7^{17}$.
- (1), (2), (3), (4), (2, 2) : $P_7^{10}$.
- (1), (2), (3), (4), (2, 2), (2, 2, 2) : $P_7^1$.

L'examen des 1171 réseaux parfaits (classés par Laïhem dans [Lh]) contenant une section hyperplane parfaite de même norme qui n'est pas un réseau de racines (restriction qui n'écarte que les 4 réseaux $\mathbb{E}_8$, $\mathbb{A}_8^2$, $\mathbb{D}_8$ et $\mathbb{A}_8$ examinés par ailleurs) ne fait apparaître que des indices variant de 1 à 6. En fait, à trois exceptions près, les quotients de type $1, 2, 3, 4, 2^2$ existent pour tous ces réseaux.

[Avec les notations de [Lh], les exceptions concernent le réseau numéro 1171 (quotients $1, 2, 2^2$) et les réseaux numéros 1154 et 1164 (quotients $1, 2, 3$).]

Des calculs d'indice portant sur tous les réseaux parfaits de dimension 8 connus à ce jour (il y en a 10916) figurent dans des pages WEB réalisées avec Martinet (consultation sur http: //www.math.u-bordeaux.fr/~martinet). Ici encore, les 5 structures $1, 2, 3, 4, 2^2$ sont possibles pour la plupart des réseaux.

## BIBLIOGRAPHIE


[A-MC] Ash, A. et McConnel, M. Mod $p$ cohomology of $\mathrm{SL}(n, \mathbb{Z})$. *Topology l31* (1992), 349–355.

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

[Bt] Batut, C. Classification of quintic eutactic forms. *Math. Comp.*, to appear.

[B-M] Bergé, A.-M. et Martinet, J. Sur la classification des réseaux eutactiques. *J. London Math. Soc. l53* (1996), 417–432.

[B-S] Borel, A. et de Siebenthal, J. Sur les sous-groupes fermés connexes d'un groupe de Lie clos. *Comm. Mat. Helv. 25* (1951), 210–256.

[Cas] Cassels, J. W. S. *An Introduction to the Geometry of Numbers.* Grundlehren n° 99, Springer-Verlag (Heidelberg), 1959. (Deuxième édition : 1997.)

[C-S] Conway, J. H. et Sloane, N. J. A. *Sphere Packings, Lattices and Groups.* Grundlehren n° 290, Springer-Verlag (Heidelberg), 1993. (Troisième édition : 1999.)

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

[C-S2] Conway, J. H. et Sloane, N. J. A A lattice without a basis of minimal vectors. *Mathematika 42* (1995), 175–177.

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

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

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

[M2] Martinet, J. Sur la classification des réseaux parfaits de dimension 5. *J. Théorie des Nombres de Bordeaux 11* (1999), 149–159. (Actes des Journées Arithmétiques de Limoges de 1997.)

[Ry] Ryškov, S. S. On the problem of the determination of quadratic forms in many variables. *Proc. Steklov Inst. Math. 142* (1979), 233–259; original en russe : 1976.

[St] Štogrin (= Shtogrin). Locally quasi-densest lattice packings of spheres. *transl. from Dokl. Akad. Nauk SSSR 218* (1974), 62–65; original en russe : 1974.

[W] WATSON, G. L. On the minimum points of a positive quadratic form. *Mathematika l18* (1971), 60–70.

[W1] WATSON, G. L. On the minimum of a positive quadratic forms in $n$ ($\leq 8$) variables (verification of Blichfeldt's calculation). *Proc. Camb. Phil. Soc l62*, (1966), p. 719.

[W2] WATSON, G. L. The number of minimum points of a positive quadratic form. *Dissertationes Math. l84*, (1971), 1–46.

[Za] ZAHAREVA, N. V. Centerings of 8-dimensional lattices that preserve a frame of successive minima. *Proc. Steklov Inst. Math. 152*, (1982), 107–134; original en russe : 1980.

Jacques Martinet

A2X, Institut de Mathématiques
Université Bordeaux 1
351, cours de la Libération
33405 Talence cedex
France
*e-mail :* martinet@math.u-bordeaux.fr