Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 41 (1995)
Heft: 3-4: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: DENSITÉ DANS DES FAMILLES DE RÉSEAUX. APPLICATION AUX RÉSEAUX ISODUAUX
Autor: Bergé, Anne-Marie / Martinet, Jacques
DOI: https://doi.org/10.5169/seals-61830

L'Enseignement Mathématique, t. 41 (1995), p. 335-365

DENSITÉ DANS DES FAMILLES DE RÉSEAUX. APPLICATION AUX RÉSEAUX ISODUAUX

par Anne-Marie BERGÉ et Jacques MARTINET[1]

RÉSUMÉ. On s'intéresse dans cet article à la densité des empilements de sphères associés à des familles de réseaux qui se déduisent de l'un d'entre eux par l'action d'un sous-groupe fermé du groupe linéaire. La théorie des groupes de Lie permet de donner une caractérisation à la Voronoï des maxima locaux de densité, recouvrant de très nombreuses situations étudiées auparavant. On applique ensuite ces méthodes à l'étude des réseaux isoduaux récemment définis par Conway et Sloane.

ABSTRACT. We study in this paper the density of sphere packings arising from families of lattices which consist in the orbit of one of them under the action of a closed subgroup of the linear group. The theory of Lie groups yields a characterization "à la Voronoï" of the local maxima of density which contains many previously known examples. These methods are then applied to isodual lattices, recently defined by Conway and Sloane.

1. INTRODUCTION

Soit E un espace euclidien de dimension n, et soit $\mathscr{R}$ l'espace des réseaux de E, muni de la topologie pour laquelle un système fondamental de voisinages d'un réseau L s'obtient en associant à tout voisinage $\mathscr{V}$ de Id dans $\mathrm{Gl}(E)$ l'ensemble des réseaux $u(L)$, $u \in \mathscr{V}$. Pour $x \in E$, la *norme de* x est $N(x) = x.x$ (le carré de la norme euclidienne). A toute base $\mathscr{B} = (e_1, e_2, \ldots, e_n)$ de E, on associe sa *matrice de Gram* $\mathrm{Gram}(\mathscr{B}) = ((e_i . e_j))$. L'invariant d'Hermite d'un réseau L est $\gamma(L) = N(L)\det(L)^{-1/n}$, où $N(L) = \inf_{x \in L, x \neq 0} N(x)$ est la *norme* ou *minimum* de L et $\det(L)$ est le *déterminant de* L (déterminant de la matrice de Gram d'une base de L); $\gamma(L)$ ne dépend que de la classe de similitude de L, et $\gamma^{n/2}(L)$ est proportionnel à la densité de l'empilement de sphères associé à L; $\gamma_n = \sup_{L \in \mathscr{R}} \gamma(L)$ est la *constante d'Hermite pour la dimension* n.

[1] Membres du laboratoire U.M.R. 9936 du C.N.R.S.

Nous étudions ici la densité dans des familles $\mathscr{F}$ de réseaux qui sont des orbites sous l'action d'un sous-groupe fermé $\mathscr{G}$ du groupe linéaire $\mathrm{Gl}(E)$, dont nous utilisons la structure de groupe de Lie. Un certain nombre de questions, classiques lorsqu'il s'agit de la famille $\mathscr{R}$ de tous les réseaux de E, se posent naturellement. La première est celle de la détermination des *réseaux extrêmes pour* $\mathscr{F}$, c'est-à-dire des réseaux de $\mathscr{F}$ sur lesquels l'invariant d'Hermite atteint un maximum local parmi les réseaux de $\mathscr{F}$, et en particulier la recherche des *réseaux critiques pour* $\mathscr{F}$, sur lesquels l'invariant d'Hermite atteint son maximum absolu $\gamma(\mathscr{F})$. L'existence de réseaux critiques n'est pas évidente *a priori,* mais se démontre souvent facilement en utilisant le théorème de compacité de Mahler, ce qui justifie que l'on entreprenne le calcul de $\gamma(\mathscr{F})$ en déterminant tous les réseaux extrêmes.

Il est utile de disposer d'une caractérisation commode des réseaux extrêmes pour $\mathscr{F}$, analogue à celle de Voronoï dans le cas classique, faisant intervenir les notions de réseaux «parfaits» et «eutactiques». On est amené à considérer une notion plus restrictive que l'extrémalité, à savoir celle de *réseaux strictement extrêmes pour* $\mathscr{F}$: il s'agit des réseaux L possédant un voisinage dans $\mathscr{F}$ sur lequel l'invariant d'Hermite est strictement inférieur à celui de L sauf lorsqu'il s'agit d'un réseau semblable à L. Cette propriété, qui est vérifiée dans le cas classique où l'on a $\mathscr{F} = \mathscr{R}$, n'est toutefois pas générale. Nous avons rencontré des contre-exemples dans certaines familles de réseaux isoduaux; un exemple est décrit à la fin du §4, dans lequel γ est constant sur une variété de réseaux (modulo similitude) de dimension 2.

Les notions de perfection et d'eutaxie que nous utilisons sont relatives, comme dans [B-M-S], à un sous-espace vectoriel $\mathscr{E}$ de l'espace $\mathrm{End}^s(E)$ des endomorphismes symétriques de E associé de façon naturelle à la famille $\mathscr{F}$.

On peut sans inconvénient faire la théorie dans le cas d'un groupe $\mathscr{G}$ connexe. Pour une telle famille, l'espace $\mathscr{E}$ se définit par le procédé suivant. Notons ${}^t u$ le transposé de $u \in \mathrm{Gl}(E)$. Comme $\mathscr{G}$ est un sous-groupe de Lie de $\mathrm{Gl}(E)$ (Bourbaki, Lie III. §8, th. 2), l'application $u \mapsto {}^t uu$ de $\mathscr{G}$ dans $\mathrm{Gl}(E)$ a pour image une sous-variété X à la fois de $\mathrm{Gl}(E)$ et de l'espace vectoriel $\mathrm{End}^s(E)$ des endomorphismes symétriques de E. L'espace tangent à X en l'identité est le sous-espace vectoriel $\mathscr{E}$ de $\mathrm{End}^s(E)$ cherché. Dans les applications, $\mathscr{G}$ est stable par transposition, et X est alors une sous-variété du groupe $\mathscr{G}$ lui-même.

Des exemples sont examinés au §2, concernant notamment les G-réseaux au sens de [B-M2] (exemple qui contient le cas usuel de tous les réseaux de E), les réseaux dual-extrêmes au sens de [B-M1], et les réseaux isoduaux

(notion introduite par Conway et Sloane dans l'appendice de [B-S], voir aussi [C-S3]).

La caractérisation des réseaux strictement extrêmes est l'objet des §§ 3 et 4.

Le § 5 est consacré à une classification des réseaux de la famille $\mathscr{F}$ selon la configuration de leurs vecteurs minimaux. On en déduit la finitude du nombre de réseaux extrêmes (modulo similitudes) dans le cas des G-réseaux (résultat obtenu antérieurement par Jaquet dans [Ja]) et dans celui des réseaux isoduaux.

Les réseaux isoduaux sont l'objet des §§ 6 à 8. On étudie plus particulièrement au § 7 les notions de réseaux isoduaux symplectiques et orthogonaux (la première notion est celle de [C-S2]), et l'on classe au § 8 jusqu'à la dimension 4 les réseaux symplectiques qui sont extrêmes en tant que réseaux isoduaux. La méthode utilisée repose sur l'introduction au § 6 de la notion plus générale de *réseau normal* (cf. déf. 6.5).

Les auteurs remercient Christophe Bavard pour ses remarques.

2. Exemples

Soit $\mathscr{G}$ un sous-groupe fermé de $\mathrm{Gl}(E)$ et soit L_0 un réseau de E. La constante d'Hermite prend les mêmes valeurs sur les images de L_0 par $\mathscr{G}$ et par le groupe $\mathbf{R}^*\mathscr{G}$ engendré par $\mathscr{G}$ et les homothéties positives. Si $\mathscr{G}$ contient les homothéties positives, soit $\mathscr{G}'$ son sous-groupe formé des éléments de déterminant ± 1. Alors, on a $\mathscr{G} = \mathbf{R}_+^*\mathscr{G}'$, et ce produit est direct, si bien que $\mathscr{G}$ est connexe si et seulement si $\mathscr{G}'$ l'est. Pour l'étude de l'invariant d'Hermite, il est indifférent de considérer $\mathscr{G}$ ou $\mathscr{G}'$, et ce dernier choix permet de se restreindre aux réseaux de déterminant 1.

L'une des formes du *théorème de compacité de Mahler* est l'assertion suivante: *une famille de réseaux de déterminants bornés et de normes minorées par une constante strictement positive est d'adhérence compacte.* Soit $\mathscr{F}$ une famille de réseaux de la forme $\mathscr{G}L_0$ pour un groupe comme ci-dessus et soit $\gamma = \sup_{L \in \mathscr{F}} \gamma(L)$. Soit L_p une suite de réseaux de $\mathscr{F}$ sur laquelle $\gamma(L_p)$ tend vers γ. Si $\mathscr{G}$ est de déterminant 1, le théorème de compacité de Mahler s'applique à la suite L_p, dont on peut extraire une sous-suite convergente dans $\mathscr{R}$, et le cas d'un groupe contenant les homothéties positives se ramène au précédent. Si la famille $\mathscr{F}$ est fermée dans $\mathscr{R}$, ce qui est le cas dans les exemples ci-dessous, puisque $\mathscr{G}$ est fermé dans $\mathrm{Gl}(E)$, la borne γ est alors atteinte sur $\mathscr{F}$ et l'existence de réseaux critiques pour $\mathscr{F}$ est assurée.

Dans de nombreux exemples, le groupe $\mathscr{G}$ est l'ensemble des éléments u d'une sous-algèbre A de $\mathrm{End}(E)$ munie d'une involution ι d'une algèbre d'endomorphismes qui vérifient l'égalité $uu^{\iota} = 1$. Dans ce cas, l'espace tangent $\mathscr{E}(\mathscr{G})$ en l'élément neutre du groupe $\mathscr{G}$ est donné par la formule

$$\mathscr{E}(\mathscr{G}) = \{v \in A \mid v^{\iota} = -v\}$$

(Bourbaki, Lie III, p. 145, prop. 37). La détermination de l'espace $\mathscr{E}$ se fait ensuite en observant que $\mathscr{E}$ est l'image de $\mathscr{E}(\mathscr{G})$ par l'application $v \mapsto {}^{t}v + v$.

2.1. EXEMPLE. L'ESPACE DES RÉSEAUX DE E. Ici, la famille $\mathscr{F}$ est l'ensemble $\mathscr{R}$ de tous les réseaux de E. On prend $\mathscr{G} = \mathrm{Gl}^{+}(E)$ et $\mathscr{E} = \mathrm{End}^{s}(E)$. Voronoï a montré que les réseaux extrêmes sont les réseaux parfaits et eutactiques, qu'ils sont strictement extrêmes, et que le nombre de classes de similitude de réseaux parfaits est fini. De plus, Korkine et Zolotareff ([K-Z]) ont montré que les réseaux parfaits sont rationnels (i.e. proportionnels à des réseaux entiers). Les questions soulevées dans l'introduction sont donc toutes résolues dans ce cas. En outre, Voronoï a donné un algorithme permettant de trouver tous les réseaux parfaits à partir de l'un d'entre eux.

2.2. EXEMPLE. L'ESPACE DES G-RÉSEAUX. On se donne un sous-groupe fini G du groupe orthogonal $\mathrm{O}(E)$, et l'on considère la famille $\mathscr{R}_G$ des réseaux stables par G. On peut prendre pour $\mathscr{G}$ le commutant de G dans $\mathrm{Gl}(E)$ (ou sa composante connexe neutre). L'espace $\mathscr{E}$ est le commutant de G dans $\mathrm{End}^{s}(E)$. La caractérisation des réseaux «G-extrêmes» comme réseaux $\mathscr{E}$-parfaits et $\mathscr{E}$-eutactiques est démontrée dans [B-M2] (th. 2.10), mais la démonstration de la finitude des classes de similitude de réseaux G-parfaits (prop. 3.12) est incorrecte. [Il n'est pas prouvé que les changements de bases utilisés dans la démonstration de 3.12 puissent se faire par des éléments de $\mathscr{G}$.] Une démonstration correcte vient d'être obtenue par Jaquet ([Ja]). Une autre démonstration en est proposée à la fin du §6. Un «algorithme de Voronoï» est exposé dans [B-M-S]. Les composantes connexes du graphe de Voronoï sont en bijection avec les classes de représentations intégrales de G ([B-M-S], th. 2.9).

2.3. EXEMPLE. LES RÉSEAUX DUAL-EXTRÊMES. Il s'agit d'une notion introduite dans [B-M1]. On définit un «invariant d'Hermite dual» γ' par $\gamma'(L) = (N(L)N(L^*))^{1/2}$ ($L^* = \{x \in E \mid \forall y \in E, x.y \in \mathbf{Z}\}$ est le *réseau dual de* L). On a la relation de moyenne $\gamma'(L) = (\gamma(L)\gamma(L^*))^{1/2}$ et l'égalité $\gamma'(L)$

$= \gamma'(L^*)$. On dit qu'un réseau est *dual-extrême* s'il réalise un maximum local de γ'. Considérons alors dans l'espace $E \times E$ de dimension $2n$ la famille $\mathscr{F}$ des sommes orthogonales $L \perp L^*$ dans lesquelles L parcourt l'ensemble $\mathscr{R}$ de tous les réseaux de E. Soit $\mathscr{G}$ le sous-groupe de $\mathrm{Gl}(E \times E)$ formé des couples $(u, {}^t u^{-1})$, $u \in \mathrm{Gl}^+(E)$. Les réseaux de la forme $L \perp L^*$ constituent une unique orbite sous l'action de $\mathscr{G}$. On a $\det(L \perp L^*) = 1$ et donc $\gamma(L \perp L^*) = \min[N(L), N(L^*)]$.

Supposons que l'on ait $N(L) \neq N(L^*)$, par exemple $N(L) < N(L^*)$ pour fixer les idées, et considérons les homothéties de rapport λ croissant de 1 à $(N(L)/N(L^*))^{1/2}$. Ces homothéties font croître strictement l'invariant d'Hermite. Donc, les maxima locaux de $\gamma(L \perp L^*)$ sont atteints sur le fermé d'équation $N(L) = N(L^*)$. Mais, sur cet ensemble, on a l'égalité $\gamma'(L) = \gamma(L \perp L^*)$. Les maxima locaux de l'invariant γ' sur les réseaux de E s'interprètent donc comme maxima locaux de l'invariant γ sur une sous-famille de réseaux de $E \times E$.

L'espace $\mathscr{E}$ est le sous-ensemble de $\mathrm{End}^s(E) \times \mathrm{End}^s(E)$ formé des couples $(v, -v)$. On vérifie facilement que les notions de dual-perfection et de dual-eutaxie ([B-M1], déf. 3.10, p. 24) coïncident avec celles de $\mathscr{E}$-perfection et de $\mathscr{E}$-eutaxie. La finitude de l'ensemble des classes de similitude de réseaux dual-extrêmes vient d'être démontrée par le premier auteur ([Ber]). La dual-perfection n'assure pas cette finitude (il existe des familles à 1 paramètre de réseaux dual-parfaits). On remédie à cet inconvénient en élargissant cette famille par homothétie, ce qui revient à remplacer $\mathscr{E}$ par $\mathscr{E} + \mathbf{R}\mathrm{Id}$.

On ne connaît pas d'adaptation de l'algorithme de Voronoï à cette situation.

2.4. EXEMPLE. LES RÉSEAUX ISODUAUX. Certains réseaux célèbres (A_2, D_4, E_8, réseaux de Coxeter-Todd, de Barnes-Wall, de Leech, diverses variantes du réseau de Quebbemann) sont semblables à leur dual, ce qui entraîne que les invariants γ et γ' prennent la même valeur sur ces réseaux. La normalisation $N(L) = N(L^*)$ déjà utilisée dans l'exemple 2.3 permet de se restreindre au cas des réseaux isométriques à leur dual; ce sont les réseaux *isoduaux*, notion introduite par Conway et Sloane dans [C-S2]. Nous devons préciser cette définition: étant donné un élément $\sigma \in \mathrm{O}(E)$, on dit qu'un réseau L est σ-*isodual* si l'on a $L^* = \sigma(L)$, cf. §§6-8. Alors, l'ensemble des réseaux σ-isoduaux (s'il n'est pas vide) constitue une orbite sous l'action d'un sous-groupe de Lie de $\mathrm{Gl}(E)$.

3. Perfection et eutaxie

Le but de ce § est d'étendre au sous-espace $\mathscr{E}$ les notions classiques de Voronoï, qui correspondent au cas où $\mathscr{E}$ est l'espace $\mathrm{End}^s(E)$ tout entier.

Pour tout $x \in E$, on note φ_x la forme linéaire sur $\mathrm{End}^s(E)$ définie par

$$\varphi_x(v) = v(x).x\ .$$

3.1. Définitions. Soit $\mathscr{E}$ un sous-espace vectoriel de $\mathrm{End}^s(E)$ et soit S un ensemble fini de vecteurs non nuls de E.

(1) S est *$\mathscr{E}$-parfait* si les restrictions à $\mathscr{E}$ des formes linéaires $\varphi_x, x \in S$, engendrent le dual $\mathscr{E}^*$ de $\mathscr{E}$, i.e. s'il n'existe pas dans $\mathscr{E}$ d'endomorphisme v non nul tel que $\varphi_x(v) = 0$ pour tout $x \in S$;

(2) S est *$\mathscr{E}$-eutactique* si la restriction à $\mathscr{E}$ de la forme linéaire trace (notée Tr) est combinaison linéaire à coefficients strictement positifs des restrictions à $\mathscr{E}$ des $\varphi_x, x \in S$.

On emploie la même terminologie pour un réseau en prenant pour ensemble S l'ensemble de ses vecteurs minimaux.

On remarque que, si S est parfait ou eutactique pour $\mathscr{E}$, il l'est également pour tout sous-espace vectoriel $\mathscr{E}'$ de $\mathscr{E}$.

De même, il est clair que tout ensemble fini de vecteurs de E contenant un ensemble $\mathscr{E}$-parfait est $\mathscr{E}$-parfait.

On peut montrer que la propriété «$\mathscr{E}$-eutactique et $\mathscr{E}$-parfait» se transmet également; cela résulte par exemple de la caractérisation suivante:

3.2. Proposition. *Soit $\mathscr{E}$ un sous-espace vectoriel de E, et soit S un ensemble fini de vecteurs non nuls de E. Alors, les conditions suivantes sont équivalentes:*

(1) *S est à la fois $\mathscr{E}$-parfait et $\mathscr{E}$-eutactique,*

(2) *$v = 0$ est l'unique solution dans $\mathscr{E}$ du système d'inéquations linéaires*

$$\varphi_x(v) \geqslant 0 \quad \textit{pour tout} \quad x \in S \quad \textit{et} \quad \mathrm{Tr}(v) \leqslant 0\ .$$

Démonstration. Supposons d'abord que S vérifie (1) et soit $v \in \mathscr{E}$ tel que

$$\varphi_x(v) \geqslant 0 \quad \text{pour tout} \quad x \in S \quad \text{et} \quad \mathrm{Tr}(v) \leqslant 0\ .$$

Dans la relation de $\mathscr{E}$-eutaxie appliquée à v

$$\mathrm{Tr}(v) = \sum_{x \in S} \rho_x \varphi_x(v), \quad \rho_x > 0 \text{ pour tout } x\ ,$$

le premier membre est donc $\leqslant 0$ et le second $\geqslant 0$, ils sont donc nuls, et puisque tous les $\rho_x \varphi_x(v)$ sont positifs ou nuls et les ρ_x positifs strictement, on obtient $\varphi_x(v) = 0$ pour tout $x \in S$, donc $v = 0$ puisque S est $\mathscr{E}$-parfait. La condition (2) est donc vérifiée.

Réciproquement, supposons (2) vérifiée, et montrons que S est $\mathscr{E}$-parfait. Soit donc $v \in \mathscr{E}$ tel que $\varphi_x(v) = 0$ pour tout $x \in S$; comme $-v$ vérifie cette même hypothèse, on peut, quitte à changer v en $-v$, supposer $\mathrm{Tr}(v) \leqslant 0$. Par (2), v est donc nul.

Pour montrer la $\mathscr{E}$-eutaxie, ce qui achèvera la preuve de la proposition, on utilise le théorème de programmation linéaire dû à Stiemke et exhumé par Barnes ([St]):

3.3. THÉORÈME (STIEMKE). *Soit V un espace vectoriel réel de dimenson finie, et soient $F_1, F_2, \cdots, F_m$ des formes linéaires sur V. Les propriétés suivantes sont équivalentes:*

(a) *Toute solution $v \in V$ du système d'inéquations*

$$F_i(v) \geqslant 0,\ i = 1, 2, \cdots m\ ,$$

est solution du système d'équations

$$F_i(v) = 0,\ i = 1, 2, \ldots, m\ .$$

(b) *Il existe des nombres réels $\rho_1, \rho_2, \cdots, \rho_m$ strictement positifs tels que $\rho_1 F_1 + \rho_2 F_2 + \cdots + \rho_m F_m = 0$.*

Appliquons ce résultat à $V = \mathscr{E}$, et aux restrictions à $\mathscr{E}$ des formes $-\mathrm{Tr}$ et $\varphi_x, x \in S$. La condition (b) ci-dessus est exactement la $\mathscr{E}$-eutaxie de S; quant à (a), elle est certainement vérifiée, puisque (2) dit que toute solution $v \in V$ du système d'inéquations est nulle. □

Dans le cas où $\mathscr{E}$ contient l'identité Id, on peut le remplacer par l'hyperplan $\mathscr{E}_0 \subset \mathscr{E}$, orthogonal à l'identité pour le produit scalaire $\langle v, v' \rangle = \mathrm{Tr}(vv')$,

$$\mathscr{E}_0 = \{v \in \mathscr{E} \mid \mathrm{Tr}(v) = 0\}\ .$$

3.4. PROPOSITION. *Soit $\mathscr{E}$ un sous-espace de $\mathrm{End}^s(E)$ contenant l'identité, soit $\mathscr{E}_0$ l'hyperplan de $\mathscr{E}$ formé des endomorphismes de trace nulle, et soit $S = \{x_1, \cdots, x_s\}$ un ensemble fini de vecteurs unitaires de E. On note φ^i la restriction à $\mathscr{E}$ de la forme linéaire φ_{x_i}, et φ_0^i sa restriction à $\mathscr{E}_0$. Alors:*

(1) *$\mathscr{E}$-eutaxie et $\mathscr{E}_0$-eutaxie sont équivalentes.*

(2) *Pour que* S *soit* $\mathscr{E}$*-parfait, il faut et il suffit qu'il soit* $\mathscr{E}_0$*-parfait et que les restrictions* φ_0^i *à* $\mathscr{E}_0$ *vérifient une relation*

$$\sum_{1 \leqslant i \leqslant s} \alpha_i \varphi_0^i = 0, \quad \textit{avec} \quad \sum_i \alpha_i \neq 0 .$$

(3) S *est* $\mathscr{E}$*-parfait et* $\mathscr{E}$*-eutactique si et seulement s'il est* $\mathscr{E}_0$*-parfait et* $\mathscr{E}_0$*-eutactique.*

Démonstration. (1) Supposons que S vérifie une relation $\sum_i \rho_i \varphi_0^i = 0$, $\rho_i > 0$, de $\mathscr{E}_0$-eutaxie. Alors il vérifie la relation de $\mathscr{E}$-eutaxie $\sum_i \frac{n\rho_i}{\sum \rho_i} \varphi^i = \mathrm{Tr}$. En effet, soit $v \in \mathscr{E}$ et soit $v_0 = v - \frac{1}{n}\mathrm{Tr}(v)\,\mathrm{Id}$ sa projection orthogonale sur $\mathscr{E}_0$. On a $\sum_i \rho_i \varphi^i(v_0) = 0$, c'est-à-dire

$$\sum_i \rho_i \varphi^i(v) = \frac{\sum_i \rho_i}{n} \mathrm{Tr}(v)\, \varphi^i(\mathrm{Id}) = \frac{\sum_i \rho_i}{n} \mathrm{Tr}(v) .$$

La réciproque est triviale.

(2) Si S est $\mathscr{E}$-parfait, il est trivialement $\mathscr{E}_0$-parfait; de plus, la restriction Tr à $\mathscr{E}$ de la forme trace s'écrit sur les φ^i (qui par hypothèse engendrent $\mathscr{E}^*$): $\mathrm{Tr} = \sum_i \alpha_i \varphi^i$, relation qui, appliquée à Id, donne $n = \sum_i \alpha_i$, et, par restriction à $\mathscr{E}_0$, $0 = \sum_i \alpha_i \varphi_0^i$.

Réciproquement, supposons qu'il existe une relation $\sum_{1 \leqslant i \leqslant s} \alpha_i \varphi_0^i = 0$, avec $\sum_i \alpha_i \neq 0$; soit $v = v_0 + \frac{1}{n}\mathrm{Tr}(v)\,\mathrm{Id}$, $v_0 \in \mathscr{E}_0$, un élément de $\mathscr{E}$ tel que $\varphi^i(v) = 0$ pour tout i. On a donc $\varphi_0^i(v_0) + \frac{1}{n}\mathrm{Tr}(v) = 0$ pour tout i, d'où l'on déduit $\sum_i \alpha_i \varphi_0^i(v_0) + \frac{\sum_i \alpha_i}{n}\mathrm{Tr}(v) = 0$, où $\sum_i \alpha_i \varphi_0^i(v_0) = 0$ et $\sum_i \alpha_i \neq 0$. Donc $\mathrm{Tr}(v) = 0$, et $v = v_0$ appartient à $\mathscr{E}_0$. Si S est $\mathscr{E}_0$-parfait, on déduit alors de la relation $\varphi^i(v) = 0$ pour tout i que v est nul. Ainsi, S est $\mathscr{E}$-parfait.

(3) se déduit immédiatement de (1) et (2), puisque toute relation de $\mathscr{E}_0$-eutaxie $\sum_i \rho_i \varphi_0^i = 0$, $\rho_i > 0$ est telle que $\sum \rho_i \neq 0$. □

Au produit scalaire $\langle v, w \rangle = \mathrm{Tr}(vw)$ dans l'espace $\mathrm{End}^s(E)$ est associée une identification de $\mathrm{End}^s(E)$ à son dual, transformant $v \in \mathrm{End}^s(E)$ en $\varphi : w \mapsto \langle v, w \rangle$. Cette dualité associe à l'application identique la forme linéaire trace, et, pour $x \neq 0 \in E$, à la projection orthogonale p_x de E sur $\mathbf{R}x$ la forme linéaire $\frac{1}{N(x)}\varphi_x$.

La dualité du sous-espace vectoriel $\mathscr{E}$ sur son dual $\mathscr{E}^*$ induite par l'identification précédente est

$$\mathrm{proj}_{\mathscr{E}}(v) \leftrightarrow \mathrm{restr}_{\mathscr{E}}(\varphi) ,$$

où $\mathrm{proj}_{\mathscr{E}}$ et $\mathrm{restr}_{\mathscr{E}}$ désignent respectivement la projection orthogonale sur $\mathscr{E}$ et la restriction à $\mathscr{E}$, comme on le voit en remarquant que, pour $w \in \mathscr{E}$, $\varphi(w) = \langle v, w \rangle = \langle \mathrm{proj}_{\mathscr{E}}(v), w \rangle$.

C'est ainsi que l'ensemble fini S est $\mathscr{C}$-parfait (resp. $\mathscr{C}$-eutactique) si et seulement si les $\mathrm{proj}_{\mathscr{C}}(p_x)$, $x \in S$, engendrent $\mathscr{C}$ (resp. s'il existe des coefficients ρ_x tous strictement positifs tels que $\mathrm{proj}_{\mathscr{C}}(\mathrm{Id}) = \sum_x \rho_x \mathrm{proj}_{\mathscr{C}}(p_x)$).

4. Extrémalité dans $\mathscr{F}$

Pour faire une étude locale de la fonction d'Hermite dans la famille $\mathscr{F}$, on établit quelques résultats préliminaires relatifs à l'espace $\mathrm{End}^s(E)$ des endomorphismes symétriques de E, dont on note $||\ .\ ||$ une norme.

On rappelle que l'on note exp l'application exponentielle de $\mathrm{End}(E)$ dans $\mathrm{Gl}(E)$; par restriction, elle induit un difféomorphisme de $\mathrm{End}^s(E)$ sur l'ensemble des automorphismes symétriques positifs de E.

Les deux énoncés suivants concernent le déterminant et la norme d'un réseau. Le premier, qui se démontre par un calcul de valeurs propres, est bien connu:

4.1. Lemme. *Pour tout* $v \in \mathrm{End}^s(E)$, *on a* $\det(\exp v) = e^{\mathrm{Tr}(v)}$.

4.2. Lemme.

(i) *Soit* $u \in \mathrm{Gl}(E)$ *et soit* $x \in E$. *On a* $N(u(x)) = N(x) + \varphi_x({}^t uu - \mathrm{Id})$.

(ii) *Pour tout* $v \in \mathrm{End}^s(E)$, *pour tout* $x \in E$, *on a* $\varphi_x(\exp(v) - \mathrm{Id}) \geqslant \varphi_x(v)$, *l'égalité ayant lieu si et seulement si* $v(x) = 0$ *(et alors les deux membres sont nuls).*

(iii) *Soit* S *un ensemble fini de vecteurs non nuls de* E *et soit* F *un cône fermé de* $\mathrm{End}^s(E)$ *tel que, pour tout* $v \neq 0$ *appartenant à* F, *le minimum* $\min_{x \in S} \varphi_x(v)$ *soit négatif. Alors, il existe* $\alpha > 0$ *tel que, pour tout* $v \in F$ *avec* $0 < ||v|| < \alpha$, *on ait* $\min_{x \in S} \varphi_x(\exp(v) - \mathrm{Id}) < 0$.

(iv) *Soit* L *un réseau et soit* S *l'ensemble de ses vecteurs minimaux. Pour* $u \in \mathrm{Gl}(E)$ *assez voisin de l'identité, on a* $N(u(L)) = N(L) + \min_{x \in S} \varphi_x({}^t uu - \mathrm{Id})$.

Démonstration. (i) On a

$$u(x) \,.\, u(x) - x \,.\, x = {}^t uu(x) \,.\, x - x \,.\, x = ({}^t uu - \mathrm{Id})\,(x) \,.\, x = \varphi_x({}^t uu - \mathrm{Id})\ .$$

On prouve (ii) et (iii) par un argument de convexité. On note Σ la sphère unité de $\mathrm{End}^s(E)$. Pour tout $w \in \Sigma$, pour tout $x \in E$, on remarque que la

fonction numérique $f_w : t \mapsto f_w(t) = \varphi_x(\exp(tw) - \mathrm{Id})$ est convexe, et que $f_w(0) = 0$, $f'_w(0) = \varphi_x(w)$.

En effet, en notant λ_i les valeurs propres de w et (ε_i) une base orthonormale de E formée de vecteurs propres de w, on a, en posant $x = \sum_i \xi_i \varepsilon_i$, $f_w(t) = \sum \xi_i^2 (e^{t\lambda_i} - 1)$, d'où les dérivées $f'_w(t) = \sum \xi_i^2 \lambda_i e^{t\lambda_i}$ et $f''_w(t) = \sum \xi_i^2 \lambda_i^2 e^{t\lambda_i} \geqslant 0$, avec égalité si et seulement si $w(x) = 0$.

(ii) Soient $x \in E$ et $v \neq 0$. On pose $||v|| = t$ et $w = \dfrac{v}{t} \in \Sigma$. La convexité de la fonction f_w précédente montre que $\varphi_x(\exp v - \mathrm{Id}) = \varphi_x(\exp(tw) - \mathrm{Id}) \geqslant t\varphi_x(w) = \varphi_x(v)$, l'égalité exigeant $w(x) = v(x) = 0$.

(iii) Soit $w \in F \cap \Sigma$. Par hypothèse, il existe $x \in S$ tel que $\varphi_x(w)$ soit < 0. La convexité de la fonction f_w correspondante montre qu'il existe $t_w > 0$ tel que $f_w(t)$ soit négative pour tout $t \in]0, t_w[$. Il en est donc de même de $M_w(t) = \min_x(\varphi_x(\exp(tw) - \mathrm{Id}))$, et, plus précisément, si M_w est négative en un point t_0, elle l'est sur tout l'intervalle $]0, t_0[$.

La fonction $w' \mapsto M_{w'}(t_w)$ étant continue sur $F \cap \Sigma$, il existe un voisinage ouvert $V(w)$ de w dans $F \cap \Sigma$ tel que, pour $w' \in V(w)$, $M_{w'}$ soit négatif en t_w, et donc aussi sur l'intervalle $]0, t_w]$. Du recouvrement $\cup_{w \in F \cap \Sigma} V(w)$ du compact $F \cap \Sigma$, on extrait un recouvrement fini $\cup_{1 \leqslant i \leqslant r} V(w_i)$, et l'on pose $\alpha = \min(t_{w_1} \cdots t_{w_r})$. Soit alors $v \in F$ tel que $0 < ||v|| < \alpha$ et soit $w = \frac{1}{||v||} v \in \Sigma$. Il existe i, $1 \leqslant i \leqslant r$, tel que w appartienne à $V(w_i)$ et donc $M_w(t)$ est < 0 sur l'intervalle $]0, \alpha[\subset]0, t_{w_i}]$.

(iv) Pour u suffisamment voisin de Id (modulo le groupe orthogonal), les vecteurs minimaux du réseau $u(L)$ proviennent de vecteurs minimaux de S, de sorte que $N(u(L)) = \min_{x \in S} N(u(x))$, d'où le résultat grâce à (i). □

4.3. LEMME. *Soit L un réseau, et soit $u \in \mathrm{Gl}(E)$ tel que $u(L)$ soit semblable à L. Alors, si u est assez voisin de l'identité, u lui-même est une similitude.*

Démonstration. Le rapport de similitude λ_u des deux réseaux est tel que $\lambda_u^{2n} = \frac{\det(u(L))}{\det(L)} = (\det u)^2$, et tend donc vers 1 quand u tend vers l'identité. Quitte à remplacer u par $\lambda_u^{-1} u$, on peut donc supposer les réseaux isométriques. Il existe alors une isométrie f avec $(fu)(L) = L$. Donc, fu appartient au sous-groupe discret $\mathrm{Gl}(L)$ de $\mathrm{Gl}(E)$, et ${}^t uu = {}^t(fu)(fu)$ appartient à l'ensemble discret des ${}^t vv$, $v \in \mathrm{Gl}(L)$. Pour u assez voisin de l'identité, on a donc ${}^t uu = \mathrm{Id}$, ce qui signifie que u est une isométrie. □

Soit $\mathscr{F}$ une famille de réseaux vérifiant les hypothèses et notations de l'introduction: il existe un sous-groupe fermé $\mathscr{G}$ de $\mathrm{Gl}(E)$ tel que les composantes connexes de $\mathscr{F}$ sont des orbites de la composante connexe neutre $\mathscr{G}^\circ$ de $\mathscr{G}$. On suppose que $\mathscr{G}$ est stable par transposition. L'espace tangent en l'identité à la variété des ${}^t uu$, $u \in \mathscr{G}$, est noté $\mathscr{E}$. *On suppose de plus que la famille $\mathscr{F}$ est stable par homothéties, ou bien constituée de réseaux de même déterminant.*

La proposition suivante permet si besoin est de ne considérer que des automorphismes symétriques de $\mathscr{G}$:

4.4. PROPOSITION. *Soit $u \in \mathscr{G}^\circ$ et soient f et s ses composantes orthogonale et symétrique. (On a $u = fs$ et s est défini positif.) Alors, f et s appartiennent aussi à $\mathscr{G}^\circ$.*

Démonstration. Comme ${}^t uu$ est défini positif, il existe $v \in \mathrm{End}^s(E)$ tel que ${}^t uu = \exp v$. Comme $\mathscr{G}$ est stable par transposition, v est dans l'espace tangent à $\mathscr{G}$ (et en fait dans $\mathscr{E}$). Alors, $t = \exp \frac{v}{2}$ est un endomorphisme symétrique positif appartenant à $\mathscr{G}^\circ$, et l'on a $t^2 = {}^t uu$, donc $t = s$. Ainsi, s, et par suite f, sont dans $\mathscr{G}^\circ$.

Nous sommes maintenant en mesure de démontrer un théorème à la Voronoï.

On rappelle qu'un réseau $L \in \mathscr{F}$ est dit *strictement extrême* s'il existe un voisinage $\mathscr{U}$ de L dans $\mathscr{F}$ dans lequel tout réseau L' *non semblable à* L vérifie l'inégalité stricte $\gamma(L') < \gamma(L)$.

4.5. THÉORÈME. *Soient $\mathscr{F}$, $\mathscr{G}$ et $\mathscr{E}$ comme ci-dessus. Soit L un réseau appartenant à $\mathscr{F}$ et soit S l'ensemble de ses vecteurs minimaux. Alors:*

(i) *L est strictement extrême dans $\mathscr{F}$ si et seulement s'il est $\mathscr{E}$-parfait et $\mathscr{E}$-eutactique.*

(ii) *Si L est extrême mais non strictement extrême, il existe dans $\mathscr{F}$ un arc d'origine L, formé de réseaux extrêmes deux à deux non semblables, de même invariant d'Hermite que L et qui, à l'exception de L, ont tous même ensemble de vecteurs minimaux engendrant un sous-espace strict de E.*

Démonstration. Pour étudier l'invariant d'Hermite au voisinage de L, on peut remplacer $\mathscr{F}$ par la famille normalisée $\mathscr{F}_0 = \{L' \in \mathscr{F} \mid \det(L') = \det(L)\}$, et donc, d'après 4.1, l'espace $\mathscr{E}$ par $\mathscr{E}_0 = \{v \in \mathscr{E} \mid \mathrm{Tr}(v) = 0\}$. L'invariant d'Hermite est alors proportionnel à la norme des réseaux.

Supposons d'abord que S soit $\mathscr{E}$-parfait et $\mathscr{E}$-eutactique. D'après le critère 3.2., on a donc, pour tout élément $v \neq 0$ de $\mathscr{E}_0$, $\min_{x \in S} \varphi_x(v) < 0$ (puisque $\mathrm{Tr}(v) = 0$). D'après le lemme 4.2,(iii) (appliqué à S et au cône $F = \mathscr{E}_0$), il existe $\alpha > 0$ tel que, pour $v \in \mathscr{E}_0$ avec $0 < ||v|| < \alpha$, on ait $\min_{x \in S} \varphi_x\left(\exp\left(\frac{1}{2}v\right) - \mathrm{Id}\right) < 0$. De même, il existe $\beta > 0$ tel que, pour $||v|| < \beta$, $N\left(\left(\exp\left(\frac{1}{2}v\right)(L)\right) - N(L) = \min_{x \in S} \varphi_x\left(\exp\left(\frac{1}{2}v\right) - \mathrm{Id}\right)\right.$ (4.2,(iv)). Soit $\varepsilon = \min(\alpha, \beta)$. Pour tout réseau L' appartenant au voisinage $\mathscr{U} = \{\exp\left(\frac{1}{2}v\right)(L), v \in \mathscr{E}_0, 0 < ||v|| < \varepsilon\}$ de L dans $\mathscr{F}_0$, on a $N(L') - N(L) < 0$, i.e. $\gamma(L') < \gamma(L)$: dans $\mathscr{U}$, $\gamma(L)$ est un maximum strict: L est strictement extrême.

Supposons inversement que $L \in \mathscr{F}$ réalise un maximum de la fonction d'Hermite dans un voisinage $\mathscr{U}$ de L dans $\mathscr{F}$, que l'on suppose assez petit pour que les vecteurs minimaux des réseaux qu'il contient proviennent de ceux de L, et soit $v \in \mathscr{E}_0$ tel que

$$\min_{x \in S} (\varphi_x(v)) \geqslant 0 \,. \tag{4.6}$$

Pour $t > 0$, on considère

$$u_t = \exp\left(\frac{t}{2} v\right) \in \mathscr{G}^+ \quad \text{et} \quad L_t = u_t(L) \in \mathscr{F}_0 \,. \tag{4.7}$$

On suppose t assez petit pour que L_t appartienne à $\mathscr{U}$, et pour que u_t vérifie la condition du lemme 4.3. Puisque $\mathrm{Tr}(v) = 0$, on a $\det u_t = 1$ (cf. 4.1), et donc $\det(L_t) = \det(L)$, et pour t assez petit (lemme 4.2,(iv) et (iii)), la condition (4.6) entraîne

$$\begin{aligned} \det(L)^{1/n}(\gamma(L_t) - \gamma(L)) &= N(L_t) - N(L) \\ &= \min_{x \in S} (\varphi_x(\exp(tv) - \mathrm{Id})) \geqslant t \min_{x \in S} \varphi_x(v) \geqslant 0 \,. \end{aligned}$$

Le caractère maximal de $\gamma(L)$ dans $\mathscr{U}$ implique que les inégalités ci-dessus sont des égalités, et donc que $\gamma(L_t) = \gamma(L)$. De plus, les vecteurs minimaux de L_t sont les vecteurs $u_t(x)$, avec $x \in S$ tel que $\varphi_x(\exp(tv) - \mathrm{Id})) = t\varphi_x(v) = 0$, c'est-à-dire, d'après 4.2,(ii), $v(x) = 0$ donc $u_t(x) = x$. On a donc

$$S(L_t) = S \cap \mathrm{Ker}(v) \,. \tag{4.8}$$

Si l'on suppose $\gamma(L)$ strictement maximal dans $\mathscr{U}$, la relation $\gamma(L_t) = \gamma(L)$ exige que L_t soit semblable à L, et donc (lemme 4.3) que u_t soit une isométrie (rappelons que $\det(u_t) = 1$), c'est-à-dire que v soit nul. Ainsi, sous cette hypothèse, la condition (4.6) implique $v = 0$: L est alors

$\mathscr{E}_0$-parfait et $\mathscr{E}_0$-eutactique, ce qui achève de prouver (i), compte tenu de 3.4.

Sinon, d'après l'étude de la partie directe, S n'est pas à la fois $\mathscr{E}_0$-parfait et $\mathscr{E}_0$-eutactique, et il existe bien dans $\mathscr{E}_0$ un élément $v \neq 0$ vérifiant les conditions (4.6). Les réseaux L_t construits à partir de v sont alors deux à deux non semblables, et vérifient les propriétés énoncées dans (ii). □

4.9. COROLLAIRE. *Si un réseau L est strictement extrême pour un groupe $\mathscr{G}$, le nombre s de couples $\pm x$ de ses vecteurs minimaux vérifie*

$$s \geqslant \dim(\mathscr{G}) ,$$

et même, dans le cas où $\mathscr{G}$ est formé d'éléments de déterminant ± 1,

$$s \geqslant \dim(\mathscr{G}) + 1 .$$

Démonstration. La $\mathscr{E}$-perfection de l'ensemble S des vecteurs minimaux implique $s \geqslant \dim(\mathscr{E}) = \dim(\mathscr{G})$; si de plus $\mathscr{G}$ est formé d'éléments de déterminant ± 1, $\mathscr{E}$ est contenu dans le noyau de la trace, de sorte que la relation de $\mathscr{E}$-eutaxie se traduit par une relation non triviale entre les φ_x, $x \in S(L)$, et l'on a donc $s \geqslant \dim(\langle \varphi_x, x \in S(L) \rangle) + 1$. □

[Remarquons que dans ce cas, L est aussi strictement extrême pour le groupe $\mathscr{G}' = \mathbf{R}^* \mathscr{G}$ de dimension $\dim(\mathscr{G}) + 1$.]

Sans hypothèse particulière sur $\mathscr{G}$, il peut exister des réseaux extrêmes qui ne le sont pas strictement. L'exemple suivant correspond à la famille isoduale réductible de dimension 3 considérée dans [C-S3].

Soit σ une rotation de $\mathbf{R}^3$ d'angle $\pi/2$ et d'axe une droite D dont on note P le plan orthogonal, et soit L un réseau σ- isodual. Il est en particulier stable par σ^2, ce qui entraîne que L contient avec l'indice 1 ou 2 la somme orthogonale $L \cap D \perp L \cap P$. On constate que l'indice 2 est impossible pour les réseaux σ-isoduaux, et que l'on a $L \cap D \simeq \mathbf{Z}$ (et $\det(L \cap P) = 1$). On a donc $\gamma(L) = N(L) \leqslant 1$, et les réseaux σ-extrêmes sont ceux pour lesquels $L \cap P$ est de norme $\geqslant 1$. Ils constituent modulo isométries une variété à bord de dimension 2. Aucun d'entre eux n'est strictement extrême, et leurs vecteurs minimaux peuvent se limiter à ceux de D.

5. Résultats de classification

On conserve les notations et hypothèses des paragraphes précédents. On suppose en outre que $\mathscr{G}$ est connexe.

On classe ci-dessous les réseaux selon la configuration de leurs vecteurs minimaux, généralisant des notions introduites dans [Ber] et [B-M3] (et auparavant de façon informelle dans [B-M1], §5).

5.1. Définition. Soient L et L' deux réseaux appartenant à la famille $\mathscr{F}$, et S et S' leurs ensembles de vecteurs minimaux. On définit les relations suivantes:

$L' \equiv L$ s'il existe $u \in \mathscr{G}$ tel que $L' = u(L)$ et $S' = u(S)$,

$L' \prec L$ s'il existe $u \in \mathscr{G}$ tel que $L' = u(L)$ et $S' \subset u(S)$.

La relation $\equiv$ est une relation d'équivalence dans $\mathscr{F}$, et la relation $\prec$ induit un ordre (encore noté $\prec$) sur l'ensemble des classes de $\equiv$-équivalence.

Le théorème suivant montre en particulier que les classes au sens de la déf. 5.1 contiennent au plus un réseau strictement $\mathscr{E}$-extrême.

5.2. Théorème. *Soit $\mathscr{C}$ une classe et soit $L \in \mathscr{C}$ un réseau $\mathscr{E}$-eutactique.*

(1) *L'invariant d'Hermite atteint sur L son minimum dans la réunion $\tilde{\mathscr{C}}$ des classes $\prec \mathscr{C}$.*

(2) *Si $S(L)$ engendre E, ou si L est $\mathscr{E}$-parfait, alors les réseaux eutactiques de $\mathscr{C}$ sont tous semblables à L.*

[Si le nombre de classes est fini (comme c'est le cas dans les exemples du §2), on obtient la finitude des réseaux strictement extrêmes pour le groupe $\mathscr{G}$, et même des réseaux $\mathscr{E}$-eutactiques possédant n vecteurs minimaux indépendants.]

Démonstration. On se ramène tout de suite au cas où $\mathscr{G}$ est de déterminant 1. Soit $L' = u(L) \in \mathscr{F}$, $u \in \mathscr{G}$, un réseau tel que $S' \supset u(S)$. On a donc $N(u(x)) = N(L')$ pour tout $x \in S$, c'est-à-dire (lemme 4.2,(i))

$$\varphi_x({}^t uu - \mathrm{Id}) = N(L') - N(L) \quad \text{pour tout} \quad x \in S .$$

De plus, comme $\mathscr{G}$ est connexe, il existe $v \in \mathscr{E}$ (de trace évidemment nulle) tel que ${}^t uu = \exp(v)$. On a donc

$$\varphi_x(\exp(v) - \mathrm{Id}) = N(L') - N(L) \quad \text{pour tout} \quad x \in S . \tag{5.3}$$

Posons, pour tout $x \in S$,

$$\psi_x(v) = \varphi_x(\exp(v) - \mathrm{Id}) - \varphi_x(v) .$$

D'après le lemme 4.2,(ii), on a l'inégalité $\psi_x(v) \geqslant 0$, avec égalité si et seulement si $v(x) = 0$. Par 5.3, on a

$$N(L') - N(L) = \varphi_x(v) + \psi_x(v) \quad \text{pour tout} \quad x \in S . \tag{5.4}$$

Puisque S est $\mathscr{E}$-eutactique, il existe des coefficients $\rho_x > 0$ tels que $\sum_{x \in S} \rho_x \varphi_x(v) = \mathrm{Tr}(v) = 0$, d'où l'on tire, par combinaison linéaire des relations 5.4:

$$\left(\sum_{x \in S} \rho_x \right) (N(L') - N(L)) = 0 + \sum_{x \in S} \rho_x \psi_x(v) \geqslant 0 , \tag{5.5}$$

et donc $N(L') - N(L) \geqslant 0$, d'où $\gamma(L') \geqslant \gamma(L)$, ce qui prouve (1).

Pour prouver (2), on suppose de plus que L' est $\mathscr{E}$-eutactique et dans la classe $\mathscr{C}$ (i.e., on a $S(L') = u(S)$). En échangeant les rôles de L' et de L, on voit que l'on a $N(L') - N(L) = 0$ (i.e., $\gamma(L') = \gamma(L)$), et donc (par 5.5) $\psi_x(v) = 0$ c'est-à-dire $v(x) = 0$ pour tout $x \in S$. Donc, S est inclus dans $\mathrm{Ker}\, v$. Cela entraîne que v est nul: c'est clair si S engendre E, et, si L' est $\mathscr{E}$-parfait, cela résulte des égalités $\varphi_x(v) = 0$ pour tout $x \in S$. On en déduit que l'on a ${}^t uu = \mathrm{Id}$, donc que u est une isométrie. □

5.6. COROLLAIRE. *Un réseau strictement $\mathscr{E}$-extrême est isolé (modulo similitude) dans sa classe $\mathscr{C}$; en particulier, lorsqu'il s'agit d'un maximum absolu (strict), ce réseau est unique modulo similitude dans la réunion $\tilde{\mathscr{C}}$ des classes qui contiennent $\mathscr{C}$.*

En effet, il réalise à la fois par définition même un maximum relatif (ou absolu) de γ dans $\mathscr{F}$, donc aussi dans $\mathscr{C}$, et d'après 5.2 un minimum absolu de γ dans $\mathscr{C}$.

[Une traduction du corollaire ci-dessus est qu'un tel réseau perd des vecteurs minimaux par toute déformation suffisamment petite.]

6. ISODUALITÉ

Soit L un réseau de E, et soit L^* son dual. Si $\sigma \in O(E)$ est une isométrie du réseau L sur son dual L^* (on dit alors que L est σ-*isodual*), l'égalité ${}^t\sigma = \sigma^{-1}$ montre que σ applique L^* sur L, de sorte que σ^2 est un automorphisme du réseau L. On peut préciser ce résultat en introduisant le groupe

$\mathrm{Aut}^{\#}(L)$ des transformations orthogonales appliquant L sur L ou L^*; ce groupe contient le groupe $\mathrm{Aut}(L)$ $(= \mathrm{Aut}(L^*))$ avec l'indice 1 ou 2, l'indice étant égal à 2 lorsque le réseau est isodual sans être unimodulaire. Dans ce cas, les isométries de L sur son dual sont de la forme $\tau = \sigma \circ u$, σ désignant l'une d'entre elles, et u parcourant le groupe d'automorphismes de L.

Un réseau σ-isodual est également σ'-isodual pour $\sigma' = \pm\sigma$, $\sigma' = \pm\sigma^{-1}$ et $\sigma' = \pm\sigma^m$ pour tout entier m impair. Il en résulte que, si l'isométrie σ est d'ordre $2^k m$, avec m impair, σ^m est encore une isométrie de L sur L^*, dont l'ordre est cette fois une puissance de 2; les isométries d'ordre une puissance de 2 présentent de ce fait un intérêt particulier.

Soit $\sigma \in \mathscr{O}(E)$ et soit $\mathscr{F}_\sigma$ la famille des réseaux σ-isoduaux.

6.1. PROPOSITION. *Soit* G_σ *le sous-groupe de* $\mathrm{Gl}(E)$ *défini par*

$$G_\sigma = \{u \in \mathrm{Gl}(E) \mid {}^t u \sigma u = \sigma\} .$$

(1) *La composante connexe d'un réseau* $L \in \mathscr{F}_\sigma$ *est contenue dans l'orbite de* L *sous l'action de* G_σ.

(2) *Le groupe* G_σ *est stable par transposition.*

(3) G_σ *est le groupe orthogonal de la forme bilinéaire*

$$b_\sigma : (x, y) \to x \,.\, \sigma y .$$

(4) *L'espace* $\mathscr{E}$ *associé à* $\mathscr{F}_\sigma$ *est*

$$\mathscr{E} = \{v \in \mathrm{End}^s(E) \mid \sigma v = -v\sigma\} \subset \mathrm{Ker}\,\mathrm{Tr} .$$

Démonstration. (1) Soient $L \in \mathscr{F}_\sigma$ et $u \in \mathrm{Gl}(E)$. On a les équivalences suivantes:

$$\begin{aligned} u(L) \in \mathscr{F}_\sigma &\Leftrightarrow (u(L))^* = \sigma(u(L)) \Leftrightarrow {}^t u^{-1}(L^*) = \sigma(u(L)) \\ &\Leftrightarrow {}^t u^{-1}(\sigma(L)) = \sigma(u(L)) \Leftrightarrow \sigma^{-1}\,{}^t u \sigma u \in \mathrm{Gl}(L) , \end{aligned}$$

d'où l'on déduit, lorsque u est suffisamment proche de l'identité, $\sigma^{-1}\,{}^t u \sigma u = \mathrm{Id}$.

(2) La transformation σ étant orthogonale, on a les équivalences $u \in G_\sigma \Leftrightarrow {}^t u^{-1} \in G_\sigma \Leftrightarrow {}^t u \in G_\sigma$.

(3) Cela résulte de l'équivalence, pour $u \in \mathrm{Gl}(E)$, $x \in E$, $y \in E$,

$$u(x) \,.\, \sigma u(y) = x \,.\, \sigma(y) \Leftrightarrow x \,.\, {}^t u \sigma u(y) = x \,.\, \sigma y .$$

(4) On utilise la proposition de Bourbaki citée au début du §2, avec pour involution l'application $u \mapsto u^\iota = \sigma\,{}^t u \sigma^{-1}$. On a en effet $(u^\iota)^\iota = \sigma^2 u \sigma^{-2}$,

et u commute à σ^2 (les réseaux σ-isoduaux sont des G-réseaux au sens de l'exemple 2.2 pour le groupe G engendré par σ^2). □

Etant donnés un sous-groupe fini $G^\#$ de $O(E)$ et un sous-groupe G d'indice 2 de $G^\#$, on pourrait plus généralement énoncer la proposition 6.1 pour des réseaux $(G^\#, G)$-isoduaux, c'est-à-dire stables par G et échangés avec leur dual par $G^\# \setminus G$. L'espace $\mathscr{E}$ est alors défini de façon analogue, par la formule $\sigma v = \varphi(\sigma) v \sigma$, où $\varphi : G^\# \to \{\pm 1\}$ est le caractère de noyau G. La projection sur $\mathscr{E}$ est donnée par la formule (cf. [B-M2], p. 45 dans le cas des G-réseaux):

$$\mathrm{proj}_{\mathscr{E}}(v) = \frac{1}{|G^\#|} \sum_{s \in G^\#} \varphi(s)\, svs^{-1} .$$

6.2. PROPOSITION. *S'il existe un réseau σ-isodual, la forme bilinéaire b_σ est de déterminant ± 1, égal au déterminant de σ.*

Démonstration. D'une façon générale, soient $\sigma \in \mathrm{Gl}(E)$, b_σ la forme bilinéaire associée comme ci-dessus à σ, et $\mathscr{B} = (e_1, \cdots, e_n)$ une base de E et $\mathscr{B}^*$ sa base duale. On a

$$\det_{\mathscr{B}} b_\sigma = \det_{\mathscr{B}^*} \sigma(\mathscr{B}) = \det_{\mathscr{B}} \sigma(\mathscr{B}) \det_{\mathscr{B}^*} \mathscr{B} = \det(\sigma) \det(\mathrm{Gram}(\mathscr{B})) .$$

Soit alors L un réseau σ-isodual et $\mathscr{B}$ une base L. On a alors $\det(\mathrm{Gram}(\mathscr{B})) = \det(L) = 1$, donc $\det(b_\sigma) = \det(\sigma)$. □

Il est immédiat que la forme b_σ est symétrique (resp. alternée) si et seulement si l'on a $\sigma^2 = +\mathrm{Id}$ (resp. $\sigma^2 = -\mathrm{Id}$), et que, dans le premier cas, si $+1$ (resp. -1) est valeur propre d'ordre p (resp. q) de σ, b_σ est alors de signature (p, q).

6.3. DÉFINITION. Nous dirons que L est *orthogonal* (resp. *symplectique*) s'il possède une isométrie σ sur son dual pour laquelle b_σ est symétrique (resp. alternée).

[Cette notion de réseau symplectique coïncide avec celle de [B-S] et de son appendice.]

Dans la suite, nous considérons essentiellement des réseaux isoduaux orthogonaux ou symplectiques. Notons que tout réseau unimodulaire est trivialement orthogonal pour les automorphismes $\pm \mathrm{Id}$.

Revenant au cas général, on remarque que, sur un réseau σ-isodual L, la forme b_σ ne prend que des valeurs entières. Précisons ses valeurs sur

l'ensemble $S(L)$ des vecteurs minimaux de L: soient x et $y \in S(L)$ des vecteurs minimaux de L; on a $|x.\sigma(y)| \leqslant N(x) = N(L) \leqslant \gamma_n$, et donc pour $n \leqslant 7$ ou $n = 8$ et $L \neq E_8$, $b_\sigma(x, y)$ est égal à 0 ou ± 1.

Il en résulte qu'*un tel réseau, si ses vecteurs minimaux engendrent E et s'il possède un vecteur minimal x appartenant également à son dual, est isométrique à $\mathbf{Z}^n$*. En effet, soit L' un sous-réseau de L ayant une base $(e_1, e_2, \ldots, e_n)$ formée de n vecteurs minimaux de L. On a $N(x) = 1$, donc $N(L') = N(L) = 1$, ce qui entraîne les inégalités

$$1 = \det(L) \leqslant \det(L') \leqslant N(e_1)N(e_2)\ldots N(e_n) = N(L)^n = 1 .$$

La dernière inégalité est l'inégalité de Hadamard, qui est en fait une égalité, ce qui entraîne que les vecteurs $e_1, e_2, \ldots, e_n$ sont deux à deux orthogonaux.

6.4. Exemples

(1) Tout réseau plan convenablement normalisé est appliqué sur son dual par les rotations $\pm\sigma$ d'ordre 4, donc est symplectique, cf. [C-S2, appendice de B-S].

(2) On trouve dans [B-M1], §5 la description d'une famille de réseaux L_t de dimension 4 ayant 9 vecteurs minimaux (la classe a_9) dépendant d'un paramètre modulo similitude, que l'on peut représenter dans une base (e_1, e_2, e_3, e_4) convenable par les matrices de Gram

$$A_t = \begin{pmatrix} 2 & -1 & -1 & t \\ -1 & 2 & 1-t & -1 \\ -1 & 1-t & 2 & -1 \\ t & -1 & -1 & 2 \end{pmatrix}$$

pour $\frac{1}{2} \leqslant t < 1$. Ce sont, comme le réseau hexagonal A_2, des réseaux sur l'anneau des entiers d'Eisenstein $\mathbf{Z}[\omega]$, $\omega^2 + \omega + 1 = 0$ et qui deviennent isoduaux par renormalisation, comme on le voit en vérifiant que l'application $\sigma : (e_1, e_2, e_3, e_4) \mapsto (-e_1^*, e_2^*, e_4^*, -e_3^*)$ est une similitude de L_t sur L_t^*. Le groupe $\mathrm{Aut}^{\#}(L_t)$ est d'ordre 144 sur l'intervalle $]\frac{1}{2}, 1[$, et d'ordre 288 (resp. 2304) pour $t = \frac{1}{2}$ (resp. $t = 1$), correspondant à un réseau semblable à $L_4^2 \simeq A_{4,0}$ (resp. à D_4). Ces réseaux sont symplectiques et non orthogonaux sauf L_4^2 et D_4 pour lesquels le groupe $\mathrm{Aut}^{\#}(L_t)$ contient des isodualités d'ordre 2 de signatures arbitraires.

Pour t croissant de $\frac{1}{2}$ à 1, l'invariant d'Hermite du réseau L_t, égal à $2[(t+1)(2-t)]^{-1/2}$, croît strictement de $\frac{4}{3}$ à $\gamma_4 = \sqrt{2}$.

(3) Dans $\mathbf{R}^n$, $n > 8$ pair, muni de sa base canonique $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n)$, on pose $\varepsilon = \frac{1}{2}(\varepsilon_1 + \varepsilon_2 + \cdots + \varepsilon_n)$ et $\varepsilon' = \frac{1}{2}(-\varepsilon_1 + \varepsilon_2 + \cdots + \varepsilon_n)$, et l'on considère les réseaux D_n, définis dans $\mathbf{Z}^n$ par la congruence $\sum_i x_i \equiv 0 \bmod 2$, et $D_n^+ = D_n \cup (\varepsilon + D_n)$. Le groupe d'automorphismes $\mathrm{Aut}(D_n)$ de D_n s'identifie au produit semi-direct $(\pm 1)^n \rtimes \mathfrak{S}_n$, celui de D_n^+ au groupe de Weyl du précédent (les automorphismes $(\varepsilon_i) \mapsto (\pm \varepsilon_i)$ de déterminant impair échangent ε et ε' modulo D_n). Pour $n \equiv 2 \bmod 4$ (resp. $n \equiv 0 \bmod 4$), on a $D_n^{+*} = D_n \cup (\varepsilon' + D_n)$ (resp. $D_n^{+*} = D_n^+$), et $\mathrm{Aut}^{\#}(D_n^+)$ s'identifie à $\mathrm{Aut}(D_n)$ pour $n \equiv 2 \bmod 4$ et est égal à $\mathrm{Aut}(D_n^+)$ sinon. Les isométries de D_n^+ sur son dual sont les automorphismes de D_n composés d'une permutation et d'un nombre impair (resp. pair) de changements de signes des ε_i. Les réseaux D_n^+ sont symplectiques, et également orthogonaux avec pour systèmes de valeurs propres possibles les combinaisons à $k \equiv \frac{n}{2} \bmod 2$ valeurs propres -1.

(4) Soit $p \equiv 3 \bmod 4$ premier. Les réseaux $A_{p-1}^{((p+1)/4)}$ de Craig ([C-S], ch. 8, §6) sont de norme $\frac{p+1}{2}$, isoduaux de type symplectique après renormalisation, eutactiques et conjecturalement parfaits, cf. [B-B], §3.

(5) Watson ([Wa]) a déterminé les valeurs maximales de l'invariant s pour les réseaux de dimension $\leqslant 7$ dépourvus de sections minimales de type A_2. Ce maximum est en particulier atteint sur un réseau unique (à isométrie près) entier pour le minimum 3, que nous notons Wa_n. Ces réseaux s'obtiennent comme sections de $\sqrt{2}E_7^*$. Le réseau Wa_6, défini par la matrice de Gram A ci-dessous, est proportionnel à un réseau σ-isodual pour une transformation σ de type symplectique. Cela se vérifie matriciellement par la formule $A = {}^tS_1(4A^{-1})S_1$, où S_1 représente une isométrie σ_1 dans le couple de bases $(\mathscr{B}, \mathscr{B}^*)$ pour lequel on a $\mathrm{Gram}(\mathscr{B}) = A$:

$$A = \begin{pmatrix} 3 & -1 & -1 & -1 & -1 & 1 \\ -1 & 3 & -1 & 1 & 1 & -1 \\ -1 & -1 & 3 & -1 & 1 & -1 \\ -1 & 1 & -1 & 3 & 1 & 1 \\ -1 & 1 & 1 & 1 & 3 & -1 \\ 1 & -1 & -1 & 1 & -1 & 3 \end{pmatrix}$$

$$S_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & -1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 1 & 0 & 1 \\ 1 & -1 & 0 & -1 & -1 & 0 \end{pmatrix}.$$

Le fait que Wa_6 soit symplectique se voit en contrôlant que $S = (AS_1^{-1})^3$ est telle que $S^2 = -64\,\mathrm{Id}$.

[Les principaux invariants de Wa_6 sont $s(Wa_6) = 16$, $\det(Wa_6) = 64$, $|\mathrm{Aut}(Wa_6)| = 2^9 . 3^2 . 5$. Signalons les similitudes $Wa_6 \sim D_6^+$, $Wa_5 \sim A_5^2 \sim (P_5^2)^*$ et $Wa_4 \sim A_3^*$.]

Dans l'étude des relations entre un réseau et son dual, il y a deux normalisations naturelles: celle qui donne aux deux réseaux le même déterminant (alors égal à 1, vu la formule $\det(L^*) = \det(L)^{-1}$) et celle qui leur donne la même norme.

6.5. DÉFINITION. Nous dirons qu'un réseau L est *normal* si ces deux normalisations coïncident. (Il revient au même de dire que les deux réseaux ont même invariant d'Hermite.)

Il est clair que tout réseau isodual est normal.

Soit L un réseau normal, de déterminant d et de norme m, et soient d^* et m^* les invariants analogues de L^*. (On a $dd^* = 1$.) Lorsque l'on effectue sur L une homothétie de rapport $\sqrt{\lambda}$, L^* subit une homothétie de rapport inverse. On transforme alors d en $D = \lambda^n d$, m en $M = \lambda m$, d^* en $D^* = \lambda^{-n} d^*$ et m^* en $M^* = \lambda^{-1} m^*$. L'égalité $M^* = M$ équivaut à $\lambda^2 = \dfrac{m^*}{m}$, d'où:

6.6. PROPOSITION. *Pour qu'un réseau soit normal, il faut et il suffit que ses invariants d, m, m^* vérifient l'égalité*

$$d^2 = \left(\frac{m}{m^*}\right)^n .$$

L'étude de la liste des réseaux parfaits jusqu'à la dimension 7 donnée dans [C-S1] montre que les seuls réseaux parfaits de dimension $\leqslant 7$ qui sont normaux sont (à similitude près) $P_1^1 \sim \mathbf{Z}$, $P_2^1 \sim A_2$, $P_4^1 \sim D_4$ et $P_6^5 \sim A_6^2 \sim P_6$. Il s'agit dans tous les cas de réseaux isoduaux. On vérifie de même que, parmi les réseaux de racines irréductibles, seuls $\mathbf{Z}$, A_2, D_4 et E_8 sont normaux.

La proposition suivante, dont nous ne donnerons pas la démonstration, précise la proposition 4.4 dans le cas du groupe G_σ:

6.7. PROPOSITION. *Les éléments u de G_σ sont de la forme*

$$u = fv ,$$

où f est une isométrie qui commute avec σ, et v un automorphisme symétrique positif dont les valeurs propres $\neq 1$ sont deux à deux inverses, et dont les sous-espaces propres E_λ vérifient $\sigma(E_\lambda) = E_{\lambda^{-1}}$.

Nous en venons aux résultats de finitude annoncés dans l'introduction: on se borne aux réseaux isoduaux de densité minorée. Rappelons que si l'ensemble S des vecteurs minimaux d'un réseau L engendre E, l'invariant d'Hermite de L est $\geqslant 1$ (reprenant dans un contexte plus général les remarques qui suivent la définition 6.3, on voit en effet que l'inégalité de Hadamard appliquée à un sous-réseau L' convenable de L donne $\det(L) \leqslant \det(L') \leqslant N(e'_1)N(e'_2)\ldots N(e'_n) = N(L)^n$, soit $\gamma(L) \geqslant 1$).

6.8. THÉORÈME. *Les réseaux de $\mathscr{F}_\sigma$ dont les vecteurs minimaux engendrent E se répartissent en un nombre fini de classes au sens de la définition 5.1.*

En utilisant le théorème 5.2, on en déduit (comparer avec [B-M3]):

6.9. COROLLAIRE. *A similitude près, il n'y a qu'un nombre fini de réseaux $\mathscr{C}$-eutactiques dont les vecteurs minimaux engendrent E.*

Démonstration de 6.8. On sait depuis Hermite qu'il existe une constante K_n telle que tout réseau L de dimension n admet une base $\mathscr{B}$ avec $N(e_1)\ldots N(e_n) \leqslant K_n \det(L)$, ce qui entraîne que les composantes des vecteurs minimaux dans cette base sont bornées (par $\sqrt{K_n}$, cf. [Ber], lemme 2.7) et donc en nombre fini. On a ici $\det(L) = 1$ et $N(L) \geqslant 1$, donc $N(e_i) \leqslant K_n$ pour tout i. La matrice B_σ de la forme b_σ dans la base $\mathscr{B}$ est donc bornée (on a $|b_\sigma(e_i, e_j)| = |\sigma(e_i) \,.\, e_j| \leqslant \sqrt{N(e_i)N(e_j)} \leqslant K_n$). Ces matrices B_σ sont donc elles aussi en nombre fini. Soient alors L_1 et L_2 deux réseaux de $\mathscr{F}_\sigma$ qui ont dans des bases convenables $\mathscr{B}_1$ et $\mathscr{B}_2$ même matrice B_σ et mêmes composantes de vecteurs minimaux. Soit $u \in \mathrm{Gl}(E)$ tel que $\mathscr{B}_2 = u(\mathscr{B}_1)$. La deuxième condition signifie que $S(L_2)$ est égal à $u(S(L_1))$. Quant à la première, elle équivaut à $u \in \mathrm{O}(b_\sigma) = G_\sigma$ (prop. 6.1,(3)). Ainsi, L_1 et L_2 sont dans la même σ-classe. □

REMARQUE. La démonstration peut être adaptée à la situation de l'exemple 2.2, c'est-à-dire celle des réseaux stables par un sous-groupe fini G donné de $\mathrm{O}(E)$, et dont les vecteurs minimaux engendrent l'espace.

Il suffit pour cela de remplacer la matrice $B_\sigma = (\sigma(e_j) \,.\, e_i)$ par les matrices $B_g = (g(e_j) \,.\, e_i^*)$ $g \in G$ des automorphismes $g \in G$ dans la base $\mathscr{B}$. Puisque G opère sur le réseau de base $\mathscr{B}$, ces matrices ont des coefficients entiers; ils sont de plus bornés, car les produits $N(e_i^*)N(e_j)$ sont

bornés: on a en effet $N(e_i^*) \leqslant \frac{K_n}{N(e_i)} \leqslant \frac{K_n}{N(L)}$ (voir [Ber], 2.7), et $N(e_j)N(L)^{n-1} \leqslant K_n \det(L)$ par choix de la base «réduite» $\mathscr{B}$, d'où $N(e_i^*)N(e_j) \leqslant \frac{K_n^2 \det(L)}{N(L)^n} = \frac{K_n^2}{\gamma(L)^n} \leqslant K_n^2$. La démonstration s'achève comme ci-dessus, en remarquant que si les deux bases $\mathscr{B}$ et $u(\mathscr{B})$ de E fournissent la même représentation intégrale $g \mapsto B_g$ du groupe G, le changement de base u appartient au commutant $\mathscr{G}$ de G (comme on a $g(u(e_j)) \,.\, (u(e_i))^* = g(u(e_j)) \,.\, {}^t u^{-1}(e_i^*) = (u^{-1}gu)(e_j) \,.\, e_i^*$, la condition sur u s'écrit $u^{-1}gu = g$ pour tout $g \in G$). □

Les G-réseaux dont les vecteurs minimaux engendrent l'espace se répartissent donc en un nombre fini de G-classes. C'est en particulier le cas des réseaux G-parfaits ([B-M2], prop. 2.9). Comme de plus une G-classe contient au plus un réseau G-parfait ([B-M2], prop. 2.9), on retrouve ainsi le résultat de finitude de [Ja].

7. Réseaux isoduaux orthogonaux et symplectiques

On conserve les notations du § précédent. On note σ un élément de $O(E)$. On rappelle que b_σ désigne la forme bilinéaire entière $(x, y) \mapsto x \,.\, \sigma y$, et qu'un réseau σ-isodual est dit orthogonal (resp. symplectique) si b_σ est symétrique (resp. alternée). Il revient au même de dire que σ^2 a pour carré $+\,\mathrm{Id}$ (resp. $-\,\mathrm{Id}$).

Le cas où $\sigma = \pm\,\mathrm{Id}$ est particulier: les réseaux σ-isoduaux sont les réseaux unimodulaires, et il est facile de vérifier que les composantes connexes de $\mathscr{F}_\sigma$ sont les classes d'isométrie de réseaux unimodulaires (cf. ci-dessous). Tous sont donc strictement σ-extrêmes. Sauf mention du contraire, nous supposons $\sigma \neq \pm\,\mathrm{Id}$.

Nous allons tout d'abord examiner la structure de l'espace $\mathscr{F}_\sigma$. Pour ce faire, nous rappelons deux résultats sur les formes bilinéaires entières de déterminant inversible. Le premier, dû à Milnor et Serre, est démontré dans [Se], le second (beaucoup plus facile) dans [M-H].

Rappelons qu'un $\mathbf{Z}$-module quadratique (sans torsion, de type fini) (M, b) est dit *pair* si $b(x, x)$ ne prend que des valeurs paires, et *impair* dans le cas contraire. Etant donné un réseau M, on note M^+ (resp. M^-) le module quadratique M muni de la forme bilinéaire $(x, y) \mapsto x \,.\, y$ (resp. $(x, y) \mapsto -x \,.\, y$). On note U le module quadratique $(\mathbf{Z}^2, 2x_1x_2)$. Enfin, pour $p, q \geqslant 0$ entiers, $pM + qN$ désigne la somme orthogonale de p copies de M et de q copies de N.

7.1. LEMME. *Un $\mathbf{Z}$-module quadratique indéfini impair (resp. pair) est isométrique à une somme $p\mathbf{Z}^+ + q\mathbf{Z}^-$ (resp. $pU + qE_8^+$ ou $pU + qE_8^-$). Sa signature (r, s) est égale à (p, q) (resp. à $(p + 8q, p)$ ou $(p, p + 8q)$). Un tel module est caractérisé à isométrie près par son type (pair ou impair) et sa signature, et il existe si et seulement si, dans le cas pair, on a $s \equiv r \bmod 8$.*

7.2. LEMME. *Soit A un anneau principal, et soit M un A-module de type fini, sans torsion, de rang n, muni d'une forme alternée de déterminant inversible dans A. Alors, n est pair, soit $n = 2m$, et M est isométrique à une somme orthogonale de m copies de A^2 muni de la forme $x_1y_2 - x_2y_1$.*

Nous en venons maintenant aux réseaux σ-isoduaux orthogonaux ou symplectiques, en supposant $\sigma \neq \pm \mathrm{Id}$, ce qui assure dans le premier cas que la forme b_σ est indéfinie.

7.3. THÉORÈME. *Soit $\sigma \in \mathrm{O}(E)$ de carré $\pm \mathrm{Id}$, $\sigma \neq \pm \mathrm{Id}$. Alors, la famille $\mathscr{F}_\sigma$ est composée d'une unique orbite sous G_σ (représentée par $\mathbf{Z}^n$ muni d'un automorphisme convenable), sauf dans le cas des réseaux orthogonaux de dimension paire, où il existe une seconde orbite représentée par des réseaux $\mathbf{Z}^n$ ou D_n^+ (selon la signature de b_σ).*

Démonstration. Comme G_σ est le groupe orthogonal de b_σ, deux réseaux appartiennent à la même orbite sous G_σ si et seulement si les formes b_σ qui leur sont associées sont isométriques. Les lemmes 7.1 et 7.2 montrent qu'il y a selon les cas au plus une ou deux orbites, et les exemples de $\mathbf{Z}^n$ et de D_{2m}^+ (cf. ex. 6.4, (3)) montrent que ces orbites existent effectivement. □

La proposition ci-dessous décrit les espaces $\mathscr{E}$ dans les cas orthogonaux et symplectiques. Sa démonstration découle tout de suite de la définition de $\mathscr{E}$ (prop. 6.1, (4)).

7.4. PROPOSITION.

(1) *Dans le cas orthogonal, soit $E = E^+ \perp E^-$ la décomposition de E en sous-espaces propres pour σ. On a alors*

$$\mathscr{E} = \{v \in \mathrm{End}^s(E) \mid v(E^+) \subset E^- \quad \text{et} \quad v(E^-) \subset E^+\},$$

et donc $\dim \mathscr{E} = \dim E^+ \cdot \dim E^-$.

(2) *Dans le cas symplectique, soit* $\mathscr{B}$ *une base orthonormée de* E *dans laquelle la matrice de* G_σ *est formée de blocs diagonaux de la forme* $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. *Alors, les éléments de* $\mathscr{E}$ *sont ceux qui ont pour matrices les matrices symétriques formées de blocs de la forme* $\begin{pmatrix} a & b \\ b & -a \end{pmatrix}$; *la dimension de* $\mathscr{E}$ *est donc* $m^2 + m$ *(on a posé* $n = 2m$*).*

[Dans le cas symplectique, la dimension du commutant de σ dans $\mathrm{End}^s(E)$ est m^2 ([B-M2], prop. 3.3), et l'on a bien $\frac{n(n+1)}{2} - m^2 = m^2 + m$.]

7.5. REMARQUE. Lorsque $\sigma = \pm \mathrm{Id}$, la dimension de $\mathscr{E}$, donc aussi celle de la sous-variété des automorphismes symétriques de G_σ, est nulle. Il en résulte que les composantes connexes de $\mathscr{F}_\sigma$ sont les classes d'isométrie de réseaux unimodulaires. La classification a été faite jusqu'à la dimension 25, cf. [C-S], ch. 16-18 et les références qui s'y trouvent. Le groupe G_σ est dans ce cas le groupe orthogonal $\mathrm{O}(E)$, qui a deux composantes connexes. Le nombre d'orbites de $\mathscr{F}_\sigma$ sous G_σ tend vers l'infini avec la dimension de E, ce qui montre que l'hypothèse «$\sigma \neq \pm \mathrm{Id}$» ne peut pas être supprimée de l'énoncé du th. 7.3.

7.6. THÉORÈME. *Dans le cas orthogonal (avec* $\sigma \neq \pm \mathrm{Id}$*) ou symplectique, les réseaux* σ*-extrêmes sont strictement extrêmes, et leurs vecteurs minimaux engendrent l'espace* E.

Démonstration. Compte tenu du th. 4.5,(ii), il suffit de prouver que, si $L \in \mathscr{F}_\sigma$ est un réseau σ-extrême, l'ensemble S de ses vecteurs minimaux engendre E. La démonstration se fera par l'absurde en utilisant le fait que, si $v \in \mathscr{E}$ est tel que $\varphi_x(v) \geqslant 0$ pour tout $x \in S$, il existe un réseau extrême (de la forme $(\exp(tv/2))(L)$ pour $t > 0$ assez petit) dont l'ensemble des vecteurs minimaux est $S \cap \mathrm{Ker}\, v$ (cf. 4.6-4.8). Dans tous les cas, on se ramène au cas où les vecteurs minimaux sont contenus dans un sous-espace σ-stable de E de codimension $\geqslant 2$.

Commençons par le cas symplectique. Si S est contenu dans un hyperplan H de E, soit $F = H \cap \sigma(H)$ le sous-espace σ-stable maximal de H. Dans une base $\mathscr{B}$ convenable de $P = F^\perp$, la matrice de la restriction de σ à P est $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. On considère l'endomorphisme $v \in \mathscr{E}$ nul sur F et dont la restriction à P a pour matrice $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ dans $\mathscr{B}$. Alors $x \mapsto \varphi_x(v)$ est nul ou

de signe constant sur l'hyperplan H, *a fortiori* sur S. En effet, soit $x = \lambda e + y$, $\lambda \in \mathbf{R}$, $y \in F$, l'écriture de $x \in H$ selon la décomposition $H = \mathbf{R}e \perp F$. On a $\varphi_x(v) = v(x) \,.\, x = \lambda v(e) \,.\, (\lambda e + y) = \lambda^2 v(e) \,.\, e$ (car $v(e) \,.\, y = e \,.\, v(y) = 0$); ainsi, quitte à remplacer v par $-v$, on peut supposer $\varphi_x(v) \geqslant 0$ pour tout $x \in H$. Il existe donc un réseau σ-extrême dont l'ensemble des vecteurs minimaux est $\operatorname{Ker} v \cap S$ contenu dans F. On peut donc supposer désormais S contenu dans F. Soit alors K un hyperplan de F disjoint de S, $G = K \cap \sigma(K)$ le sous-espace stable correspondant, et Q le plan orthogonal de G dans F, de sorte que l'on a $E = P \perp Q \perp G$. On considère $v \in \mathscr{E}$ nul sur G et qui échange les plans P et Q; dans une base de $P \perp Q$ convenable, on a

$$\mathscr{M}(\sigma) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}, \qquad \mathscr{M}(v) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}.$$

On a alors $\varphi_x(v) = 0$ pour tout $x \in F = Q \perp G$, car $v(x)$ appartient à $P = F^\perp$, donc cet endomorphisme v permet de construire un réseau (σ-extrême) dont l'ensemble des vecteurs minimaux est $S \cap \operatorname{Ker} v \subset S \cap G \subset S \cap K = \emptyset$, ce qui est absurde.

Supposons désormais $\sigma^2 = \mathrm{Id}$, $\sigma \neq \pm \mathrm{Id}$, notons E^+ et E^- les sous-espaces propres de σ pour les valeurs propres $+1$ et -1, et soit L un réseau σ-extrême dont l'ensemble S des vecteurs minimaux est inclus dans un hyperplan H de E. Il existe un hyperplan σ-stable F de H dont le plan orthogonal $P = F^\perp$ contient un vecteur propre e de σ pour la valeur $+1$ et un vecteur propre e' pour la valeur -1 (e et e' sont supposés unitaires). Si H n'est pas stable par σ, il suffit de prendre comme dans le cas symplectique $F = H \cap \sigma(H)$. En effet, si le plan $F^\perp$ était contenu dans E^+ par exemple, il en serait *a fortiori* de même pour la droite $H^\perp \subset F^\perp$, de sorte que H serait σ-stable. Ainsi la restriction de σ au plan stable $F^\perp$ est $\neq \pm \mathrm{Id}$. Si l'hyperplan H est stable, par exemple si $H^\perp$ est inclus dans E^+, on considère un plan P engendré par la droite $H^\perp$ et un vecteur non nul de E^- (par hypothèse il en existe). Le sous-espace σ-stable $F = P^\perp$ répond à la question. L'endomorphisme v qui est nul sur F et qui échange e et e' appartient à $\mathscr{E}$ et l'on peut supposer $\varphi_x(v) \geqslant 0$ pour tout $x \in H$ (même démonstration que dans le cas symplectique). Il permet donc de construire un réseau σ-extrême L' dont l'ensemble $S' = S \cap \operatorname{Ker} v$ de vecteurs minimaux est contenu dans F. Désormais, L désigne un réseau σ-extrême dont l'ensemble S des vecteurs minimaux est inclus dans un sous-espace σ-stable G de F de dimension minimale. Puisque G est stable par σ, et non nul, il contient au moins un vecteur

propre (unitaire) a pour σ, par exemple $a \in E^+$. L'endomorphisme v qui échange les vecteurs e' et a et qui est nul sur l'orthogonal du plan $\langle a, e' \rangle$ appartient à $\mathscr{E}$ (si a appartient à E^-, on remplace e' par e). De plus, $S \subset G$ est inclus dans l'hyperplan $\operatorname{Ker} v \perp \mathbf{R}a$ sur lequel $\varphi_x(v)$ est nul ou de signe constant (même démonstration que dans le cas symplectique). On peut donc construire à partir de v ou de $-v$ un nouveau réseau σ-extrême dont l'ensemble des vecteurs minimaux $S \cap \operatorname{Ker} v$ est contenu dans le sous-espace σ-stable $G \cap \operatorname{Ker} v$ strictement contenu dans G (puisque a n'appartient pas à $\operatorname{Ker} v$), ce qui est contraire au caractère minimal de G. □

8. Classification des réseaux isoduaux de petite dimension

Dans ce paragraphe on considère un élément $\sigma \in O(E)$, généralement tel que $\sigma^2 = \pm \mathrm{Id}$ (et $\sigma \neq \pm \mathrm{Id}$), et l'on recherche les réseaux σ-isoduaux strictement extrêmes pour σ. D'après le corollaire 4.9, le nombre s de couples $\pm x$ de vecteurs minimaux d'un tel réseau est $\geqslant \dim(\mathscr{G}_\sigma) + 1$, puisque le groupe de Lie $\mathscr{G}_\sigma$ est contenu dans le noyau du déterminant. Dans les cas orthogonal et symplectique, on déduit du th. 7.4 les minorations suivantes:

8.1. Proposition. *Soit L un réseau σ-isodual σ-extrême.*

(1) *Si L est σ-orthogonal, on a $s \geqslant pq + 1$, où p et q sont les multiplicités des valeurs propres $+1$ et -1 de σ $(p + q = n)$.*

(2) *Si L est σ-symplectique, on a $s \geqslant m^2 + m + 1$ $(n = 2m)$.*

Le cas de la dimension 2 est facile: les réseaux de déterminant 1 sont tous isoduaux pour une rotation d'ordre 4, et les réseaux extrêmes sont semblables à A_2. (Du reste, on a $s \geqslant 3$ par 8.1.) Ceux qui sont isoduaux pour une autre transformation sont semblables à $\mathbf{Z}^2$ ou à A_2.

Les réseaux isoduaux de dimension 3 ont été décrits par Conway et Sloane dans [C-S3], qui trouvent deux familles. L'une d'elle, qui correspond à une rotation d'ordre 4, est formée de réseaux réductibles, cf. la fin du §4. L'autre correspond au cas où $\pm\sigma$ est une rotation d'angle π. Pour cette famille, il y a un unique réseau σ-extrême, le réseau *ccc* de [C-S3].

On retrouve ce résultat en utilisant la classification (au sens de la déf. 5.1, appliquée à l'exemple 2.3) qui est faite dans [Ber]. On montre en effet

([Ber], 2.8) que les seules classes de réseaux de dimension 3 avec $s(L) = s(L^*) \geqslant 3$ sont représentées (modulo similitudes) par les matrices

$$\begin{pmatrix} 1 & t & t \\ t & 1 & t \\ t & t & 1 \end{pmatrix}, \; -1/3 < t < 1/2 \quad \text{et} \quad \begin{pmatrix} 1 & 2t-1 & -t \\ 2t-1 & 1 & -t \\ -t & -t & 1 \end{pmatrix}, \; 1/3 < t < 1/2 \; .$$

On voit facilement que les réseaux correspondants sont normaux (et en fait isoduaux) uniquement pour $t = 0$ dans le premier cas (il s'agit alors de $\mathbf{Z}^3$), et pour $t = \sqrt{2} - 1$ dans le second, ce qui correspond au réseau ccc.

Le but de la suite du § est d'obtenir une classification des réseaux isoduaux de dimension 4 ayant beaucoup de vecteurs minimaux. Nous nous appuierons sur la notion de réseau normal (déf. 6.5). Nous donnerons en passant des résultats un tout petit peu plus généraux.

8.2. THÉORÈME. *Un réseau normal de dimension* $\leqslant 8$ *possédant une section hyperplane critique (i.e. absolument extrême) est semblable à l'un des réseaux de racines* A_2, D_4, E_8.

Démonstration. Soit L un tel réseau, et M une section hyperplane critique de L, de norme $N(L)$; son déterminant est donné par la formule

$$\det(M) = \frac{N(L)^{n-1}}{\gamma_{n-1}^{n-1}} \; .$$

Le minimum de L^* est atteint sur les vecteurs primitifs de L^* orthogonaux à M, et l'on a donc

$$N(L^*) = \frac{\det(M)}{\det(L)} = \frac{1}{\det(L)} \frac{N(L)^{n-1}}{\gamma_{n-1}^{n-1}} \; .$$

Le réseau L étant normal, la proposition 6.6 entraîne l'égalité

$$N(L^*) = N(L) \det(L)^{-2/n}$$

En égalant ces deux expressions, on trouve la relation

$$\gamma(L)^{n-2} = \gamma_{n-1}^{n-1} \; .$$

Or, l'inégalité de Mordell (cf. [Cas], ch. X, § 3) s'écrit

$$\gamma_n^{n-2} \leqslant \gamma_{n-1}^{n-1} \; .$$

Le réseau L réalise donc le maximum γ_n de l'invariant d'Hermite, et ce dernier vérifie $\gamma_n^{n-2} = \gamma_{n-1}^{n-1}$, ce qui, pour les dimensions pour lesquelles sa valeur est connue, i.e. $n \leqslant 8$, ne se produit que pour $n = 2$, $n = 4$ et $n = 8$. □

8.3. THÉORÈME. *Soit L un réseau normal de dimension paire $n = 2m$, et soit M une section critique de dimension m de L, de même norme que L. Alors, l'orthogonal $M^\perp$ de M dans L^* est critique et de même norme que L^*.*

Dans le cas $m = 2$, si $\mathscr{B}$ est une base de L formée de vecteurs minimaux dont les m premiers engendrent M, les m derniers vecteurs de $\mathscr{B}^*$ sont minimaux et engendrent $M^\perp$.

Démonstration. De façon générale, pour toute section M de tout réseau L, on a $\det(M) = \det(L)\det(M^\perp)$. Dans le cas qui nous occupe, compte tenu de la proposition 6.6, on a $\frac{\det(M)}{\det(M^\perp)} = \frac{N(L)^m}{N(L^*)^m}$, et donc

$$\frac{\gamma(M^\perp)^m}{\gamma(M)^m} = \frac{\det(M)}{\det(M^\perp)} \cdot \frac{N(M^\perp)^m}{N(M)^m} = \frac{N(L)^m}{N(M)^m} \cdot \frac{N(M^\perp)^m}{N(L^*)^m} = \frac{N(M^\perp)^m}{N(L^*)^m} \geqslant 1 ;$$

puisque M réalise le maximum γ_m de l'invariant d'Hermite en dimension m, l'inégalité précédente est une égalité, et l'on a donc $\gamma(M^\perp) = \gamma(M) = \gamma_m$ et $N(M^\perp) = N(L^*)$, ce qui démontre la première partie de l'énoncé.

Considérons maintenant la base $\mathscr{B} = (e_1, \ldots, e_n)$. Pour tout vecteur minimal x' de L^*, les composantes dans $\mathscr{B}^*$ de x' sont les produits scalaires $x' . e_i$, entiers bornés par (utiliser l'inégalité de Schwarz)

$$\sqrt{N(x')N(e_i)} = \sqrt{N(L^*)N(L)} = \sqrt{\gamma(L^*)\gamma(L)} \leqslant \gamma_n < 2 ,$$

et donc éléments de $\{0, \pm 1\}$, quel que soit $n < 8$.

On applique ce qui précède à un vecteur $x' \in M^\perp$ et à ses composantes dans la base $(e^*_{m+1}, \ldots, e^*_n)$ de $M^\perp$.

Pour $m = 2$, $M^\perp$ est semblable à A_2 et possède donc 3 couples de vecteurs minimaux. Mais $x = e^*_3 + e^*_4$ et $y = e^*_3 - e^*_4$ ne peuvent être simultanément minimaux («méthode des déterminants caractéristiques» de Korkine et Zolotareff: (x, y) et (e^*_3, e^*_4) doivent engendrer le même réseau), donc e^*_3 et e^*_4 sont minimaux. □

Nous passons maintenant au cas de la dimension $n = 4$. On utilise la classification de [B-M$_1$], §5, où les réseaux engendrés par leurs vecteurs minimaux sont répartis en 18 classes (au sens du §5) $a_4, a_5, b_5, \ldots, a_9, b_9, a_{10}, a_{12}$, les deux dernières étant formées des classes de similitude de A_4 et de D_4; la classe a_9 est décrite dans l'exemple 6.4,(2).

8.4. THÉORÈME. *Les réseaux normaux de dimension 4 possédant au moins 7 couples de vecteurs minimaux sont les réseaux de la classe a_9 ou sont semblables à D_4.*

8.5. COROLLAIRE. *Les réseaux isoduaux symplectiques σ-extrêmes sont les réseaux semblables à* D_4.

Démonstration de 8.5. On sait (prop. 8.1) qu'un tel réseau possède au moins 7 couples de vecteurs minimaux, et, d'après l'exemple 6.4,(2), l'invariant d'Hermite ne possède pas de maximum relatif sur la classe a_9. □

Démonstration de 8.4. Le cas d'un réseau possédant une section hyperplane critique de même norme résulte du th. 8.2, ce qui résoud le cas des classes d_7, b_8, b_9, a_{10} et a_{12}.

Il reste à examiner les réseaux L de l'une des classes a_7, b_7, c_7, a_8.

Le cas de la classe b_7 est facile. Elle est caractérisée par l'existence de 7 vecteurs minimaux répartis dans 3 réseaux A_2 ayant un vecteur minimal e en commun. D'après le th. 8.3, le réseau orthogonal à e dans L^* possède 3 sections minimales de type A_2, et donc 6 vecteurs minimaux. Il est donc semblable à A_3, et l'on conclut par le th. 8.2 appliqué à L^*.

Pour traiter les trois derniers cas, nous avons utilisé le théorème 8.3 complété par des calculs explicites de matrices adjointes, conduits en s'aidant du système *PARI*. Nous illustrons le procédé en traitant ci-dessous le cas de la classe a_8.

Il résulte de [B-M1], §5, que ces réseaux peuvent être définis dans une base (e_1, e_2, e_3, e_4) convenable par les matrices de Gram ci-dessous:

$$\begin{pmatrix} 2 & -1 & -1 & t \\ -1 & 2 & u & -1 \\ -1 & u & 2 & -1 \\ t & -1 & -1 & 2 \end{pmatrix}.$$

On trouve $N(e_1^*) - N(e_2^*) = 2(u-t)(1-u-t)$, expression qui doit être nulle puisque $\langle e_3, e_4 \rangle$ est un réseau de type A_2, cf. th. 8.3. Si $u = 1 - t$, on obtient des matrices représentant a_9. Si $u = t$, on trouve $\frac{1}{2}N(e_1^*) - e_1^* . e_2^* = (2-t)(2t-1)$ et $\frac{1}{2}N(e_1^*) + e_1^* . e_2^* = 3(2-t)$, expressions qui ne peuvent s'annuler que pour $t = \frac{1}{2}$ ($|t|$ ne peut pas dépasser la valeur 1), cas dans lequel on obtient le réseau $L_4^2 \in a_9$. □

8.6. REMARQUE. Nous avons recherché les réseaux normaux dans les classes c_6 et d_6 (ce qui couvre tous les cas où il y a deux sections minimales de type A_2). La classe c_6 n'en contient pas. La classe d_6 contient une famille à deux paramètres de réseaux normaux, qui sont en fait isoduaux de type symplectique. Le bord de cette famille est la classe $\overline{a_9} = a_9 \cup a_{12}$. Elle contient des sous-variétés de dimension 1 formées de réseaux isoduaux de type orthogonal. En tant que réseaux σ-isoduaux de type orthogonal, L_4^2 et D_4

sont σ-extrêmes pour chacun des systèmes de valeurs propres possibles. Ce sont probablement les seuls.

Nous avons également recherché les réseaux σ-isoduaux pour un σ de valeurs propres $(+1, +1, -1, -1)$ admettant une base de vecteurs minimaux conforme au lemme 7.1. Outre la famille ci-dessus, on trouve une famille à deux paramètres à la fois symplectique et orthogonale avec $s = 4$. Son bord est contenu dans l'adhérence de la première famille.

Voici des matrices de Gram pour chacune de ces deux familles (renormalisées à la norme 2):

$$\begin{pmatrix} 2 & -1 & x & y \\ -1 & 2 & y & -x-y \\ x & y & 2 & -1 \\ y & -x-y & -1 & 2 \end{pmatrix} \qquad \begin{pmatrix} 2 & 0 & t & u \\ 0 & 2 & u & -t \\ t & u & 2 & 0 \\ u & -t & 0 & 2 \end{pmatrix}.$$

BIBLIOGRAPHIE

[B-B] BACHOC, C. et C. BATUT. Etude algorithmique de réseaux construits avec la forme trace. *Exp. Math. 1* (1992), 183-190.

[Bar] BARNES, E.S. On a theorem of Voronoï. *Proc. Cambridge Phil. Soc. 53* (1957), 537-539.

[Ber] BERGÉ, A.-M. Minimal Vectors of Pairs of Dual Lattices. *J. Number Theory, 52* (1995), 284-298.

[B-M1] BERGÉ, A.-M. et J. MARTINET. Sur un problème de dualité lié aux sphères en géométrie des nombres. *J. Number Theory 32* (1989), 14-42.

[B-M2] BERGÉ, A.-M. et J. MARTINET. Réseaux extrêmes pour un groupe d'automorphismes, *Astérisque 198-200* (1992), 41-66.

[B-M3] BERGÉ, A.-M. et J. MARTINET. Sur la classification des réseaux eutactiques. *J. London Math. Soc.* (à paraître).

[Bou] BOURBAKI, N. *Groupes et algèbres de Lie.* Chapitres 2 et 3. Hermann, Paris.

[B-M-S] BERGÉ, A.-M., J. MARTINET et F. SIGRIST. Une généralisation de l'algorithme de Voronoï pour les formes quadratiques. *Astérisque 209* (1992), 137-158.

[B-S] BUSER, P. and P. SARNAK. On the period matrix of a Riemann surface of large genus (with an Appendix by J.H. Conway and N.J.A. Sloane). *Invent. math. 117* (1994), 27-56.

[Cas] CASSELS, J.W.S. *An Introduction to the Geometry of Numbers.* Springer-Verlag, Grundlehren n° 99, Heidelberg, 1959.

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

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

[C-S2] CONWAY, J.H. and N.J.A. SLOANE. D_4, E_8, Leech and certain other lattices are symplectic. Appendix 2 to [B-S], 53-55.

[C-S3] CONWAY, J.H. and N.J.A. SLOANE. On Lattices Equivalent to Their Duals. *J. Number Theory, 48* (1994), 373-382.

[Ja] JAQUET, D.-O. Trois théorèmes de finitude pour les G-formes. *J. Théorie des Nombres Bordeaux (Actes des Journées Arithmétiques de septembre 1993)*. 12 pages, à paraître.

[K-Z] KORKINE, A. et G. ZOLOTAREFF. Sur les formes quadratiques positives. *Math. Ann. 11* (1877), 242-292.

[M-H] MILNOR, J. and D. HUSEMOLLER. *Symmetric Bilinear Forms*. Springer-Verlag, Heidelberg, 1973.

[Se] SERRE, J.-P. *Cours d'Arithmétique*. PUF, Paris, 1970.

[St] STIEMKE, E. Über positive Lösungen homogener linearer Gleichungen. *Math. Ann. 76* (1915), 340-342.

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

[Wa] WATSON, G.L. The number of minimum points of a positive quadratic form having no perfect binary section with the same minimum. *Proc. London Math. Soc. 24* (1972), 625-646.

(Reçu le 24 mars 1995)

A.-M. Bergé, J. Martinet

Laboratoire d'algorithmique arithmétique
Université Bordeaux I
351, cours de la Libération
33405 Talence Cedex
France

berge@math.u-bordeaux.fr, martinet@math.u-bordeaux.fr