

# 6. ISODUALITÉ

Objektyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **41 (1995)**

Heft 3-4: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **13.09.2024**

## **Nutzungsbedingungen**

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern. Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden. Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

## **Haftungsausschluss**

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Posons, pour tout  $x \in S$ ,

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

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

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

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

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

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

Pour prouver (2), on suppose de plus que  $L'$  est  $\mathcal{C}$ -eutactique et dans la classe  $\mathcal{C}$  (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  $\text{Ker } v$ . Cela entraîne que  $v$  est nul: c'est clair si  $S$  engendre  $E$ , et, si  $L'$  est  $\mathcal{C}$ -parfait, cela résulte des égalités  $\varphi_x(v) = 0$  pour tout  $x \in S$ . On en déduit que l'on a  ${}^t u u = \text{Id}$ , donc que  $u$  est une isométrie.  $\square$

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

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

[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  $\sigma$ -isodual), l'égalité  ${}^t \sigma = \sigma^{-1}$  montre que  $\sigma$  applique  $L^*$  sur  $L$ , de sorte que  $\sigma^2$  est un automorphisme du réseau  $L$ . On peut préciser ce résultat en introduisant le groupe

$\text{Aut}^\#(L)$  des transformations orthogonales appliquant  $L$  sur  $L$  ou  $L^*$ ; ce groupe contient le groupe  $\text{Aut}(L)$  ( $= \text{Aut}(L^*)$ ) 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  $\tau = \sigma \circ u$ ,  $\sigma$  désignant l'une d'entre elles, et  $u$  parcourant le groupe d'automorphismes de  $L$ .

Un réseau  $\sigma$ -isodual est également  $\sigma'$ -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  $\sigma$  est d'ordre  $2^k m$ , avec  $m$  impair,  $\sigma^m$  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  $\sigma \in \mathcal{C}(E)$  et soit  $\mathcal{F}_\sigma$  la famille des réseaux  $\sigma$ -isoduaux.

6.1. PROPOSITION. Soit  $G_\sigma$  le sous-groupe de  $\text{Gl}(E)$  défini par

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

- (1) La composante connexe d'un réseau  $L \in \mathcal{F}_\sigma$  est contenue dans l'orbite de  $L$  sous l'action de  $G_\sigma$ .
- (2) Le groupe  $G_\sigma$  est stable par transposition.
- (3)  $G_\sigma$  est le groupe orthogonal de la forme bilinéaire

$$b_\sigma : (x, y) \rightarrow x \cdot \sigma y.$$

- (4) L'espace  $\mathcal{C}$  associé à  $\mathcal{F}_\sigma$  est

$$\mathcal{C} = \{v \in \text{End}^s(E) \mid \sigma v = -v \sigma\} \subset \text{Ker Tr}.$$

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

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

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

(2) La transformation  $\sigma$  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  $u \in \text{Gl}(E)$ ,  $x \in E$ ,  $y \in E$ ,

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

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

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

Etant donné 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  $\mathcal{C}$  est alors défini de façon analogue, par la formule  $\sigma v = \varphi(\sigma) v \sigma$ , où  $\varphi: G^\# \rightarrow \{\pm 1\}$  est le caractère de noyau  $G$ . La projection sur  $\mathcal{C}$  est donnée par la formule (cf. [B-M2], p. 45 dans le cas des  $G$ -réseaux):

$$\text{proj}_{\mathcal{C}}(v) = \frac{1}{|G^\#|} \sum_{s \in G^\#} \varphi(s) s v s^{-1}.$$

6.2. PROPOSITION. *S'il existe un réseau  $\sigma$ -isodual, la forme bilinéaire  $b_\sigma$  est de déterminant  $\pm 1$ , égal au déterminant de  $\sigma$ .*

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

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

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

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

6.3. DÉFINITION. Nous dirons que  $L$  est *orthogonal* (resp. *symplectique*) s'il possède une isométrie  $\sigma$  sur son dual pour laquelle  $b_\sigma$  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  $\pm \text{Id}$ .

Revenant au cas général, on remarque que, sur un réseau  $\sigma$ -isodual  $L$ , la forme  $b_\sigma$  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  $|x \cdot \sigma(y)| \leq N(x) = N(L) \leq \gamma_n$ , et donc pour  $n \leq 7$  ou  $n = 8$  et  $L \neq E_8$ ,  $b_\sigma(x, y)$  est égal à 0 ou  $\pm 1$ .

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  $(e_1, e_2, \dots, e_n)$  formée de  $n$  vecteurs minimaux de  $L$ . On a  $N(x) = 1$ , donc  $N(L') = N(L) = 1$ , ce qui entraîne les inégalités

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

La dernière inégalité est l'inégalité de Hadamard, qui est en fait une égalité, ce qui entraîne que les vecteurs  $e_1, e_2, \dots, e_n$  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  $\frac{1}{2} \leq t < 1$ . 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  $\text{Aut}^\#(L_t)$  est d'ordre 144 sur l'intervalle  $\left] \frac{1}{2}, 1 \right[$ , 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  $\text{Aut}^\#(L_t)$  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  $(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n)$ , on pose  $\varepsilon = \frac{1}{2}(\varepsilon_1 + \varepsilon_2 + \dots + \varepsilon_n)$  et  $\varepsilon' = \frac{1}{2}(-\varepsilon_1 + \varepsilon_2 + \dots + \varepsilon_n)$ , et l'on considère les réseaux  $D_n$ , définis dans  $\mathbf{Z}^n$  par la congruence  $\sum_i x_i \equiv 0 \pmod{2}$ , et  $D_n^+ = D_n \cup (\varepsilon + D_n)$ . Le groupe d'automorphismes  $\text{Aut}(D_n)$  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  $\varepsilon$  et  $\varepsilon'$  modulo  $D_n$ ). Pour  $n \equiv 2 \pmod{4}$  (resp.  $n \equiv 0 \pmod{4}$ ), on a  $D_n^{+*} = D_n \cup (\varepsilon' + D_n)$  (resp.  $D_n^{+*} = D_n^+$ ), et  $\text{Aut}^\#(D_n^+)$  s'identifie à  $\text{Aut}(D_n)$  pour  $n \equiv 2 \pmod{4}$  et est égal à  $\text{Aut}(D_n^+)$  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  $\varepsilon_i$ . Les réseaux  $D_n^+$  sont symplectiques, et également orthogonaux avec pour systèmes de valeurs propres possibles les combinaisons à  $k \equiv \frac{n}{2} \pmod{2}$  valeurs propres  $-1$ .

(4) Soit  $p \equiv 3 \pmod{4}$  premier. Les réseaux  $A_{\frac{p-1}{2}}^{((p+1)/4)}$  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  $\leq 7$  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  $\sigma$ -isodual pour une transformation  $\sigma$  de type symplectique. Cela se vérifie matriciellement par la formule  $A = {}^t S_1 (4A^{-1}) S_1$ , où  $S_1$  représente une isométrie  $\sigma_1$  dans le couple de bases  $(\mathcal{B}, \mathcal{B}^*)$  pour lequel on a  $\text{Gram}(\mathcal{B}) = A$ :

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

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

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

[Les principaux invariants de  $Wa_6$  sont  $s(Wa_6) = 16$ ,  $\det(Wa_6) = 64$ ,  $|\text{Aut}(Wa_6)| = 2^9 \cdot 3^2 \cdot 5$ . 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  $\lambda^2 = \frac{m^*}{m}$ , 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  $\leq 7$  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  $G_\sigma$ :

6.7. PROPOSITION. *Les éléments  $u$  de  $G_\sigma$  sont de la forme*

$$u = fv ,$$

où  $f$  est une isométrie qui commute avec  $\sigma$ , et  $\nu$  un automorphisme symétrique positif dont les valeurs propres  $\neq 1$  sont deux à deux inverses, et dont les sous-espaces propres  $E_\lambda$  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  $\geq 1$  (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  $\det(L) \leq \det(L') \leq N(e'_1)N(e'_2) \dots N(e'_n) = N(L)^n$ , soit  $\gamma(L) \geq 1$ ).

6.8. THÉORÈME. *Les réseaux de  $\mathcal{F}_\sigma$  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  $\mathcal{C}$ -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  $\mathcal{B}$  avec  $N(e_1) \dots N(e_n) \leq K_n \det(L)$ , 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  $N(L) \geq 1$ , donc  $N(e_i) \leq K_n$  pour tout  $i$ . La matrice  $B_\sigma$  de la forme  $b_\sigma$  dans la base  $\mathcal{B}$  est donc bornée (on a  $|b_\sigma(e_i, e_j)| = |\sigma(e_i) \cdot e_j| \leq \sqrt{N(e_i)N(e_j)} \leq K_n$ ). Ces matrices  $B_\sigma$  sont donc elles aussi en nombre fini. Soient alors  $L_1$  et  $L_2$  deux réseaux de  $\mathcal{F}_\sigma$  qui ont dans des bases convenables  $\mathcal{B}_1$  et  $\mathcal{B}_2$  même matrice  $B_\sigma$  et mêmes composantes de vecteurs minimaux. Soit  $u \in \text{Gl}(E)$  tel que  $\mathcal{B}_2 = u(\mathcal{B}_1)$ . La deuxième condition signifie que  $S(L_2)$  est égal à  $u(S(L_1))$ . Quant à la première, elle équivaut à  $u \in \text{O}(b_\sigma) = G_\sigma$  (prop. 6.1, (3)). Ainsi,  $L_1$  et  $L_2$  sont dans la même  $\sigma$ -classe.  $\square$

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  $\text{O}(E)$ , et dont les vecteurs minimaux engendrent l'espace.

Il suffit pour cela de remplacer la matrice  $B_\sigma = (\sigma(e_j) \cdot e_i)$  par les matrices  $B_g = (g(e_j) \cdot e_i^*)$   $g \in G$  des automorphismes  $g \in G$  dans la base  $\mathcal{B}$ . Puisque  $G$  opère sur le réseau de base  $\mathcal{B}$ , 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  $N(e_i^*) \leq \frac{K_n}{N(e_i)} \leq \frac{K_n}{N(L)}$  (voir [Ber], 2.7), et  $N(e_j)N(L)^{n-1} \leq K_n \det(L)$  par choix de la base «réduite»  $\mathcal{B}$ , d'où  $N(e_i^*)N(e_j) \leq \frac{K_n^2 \det(L)}{N(L)^n} = \frac{K_n^2}{\gamma(L)^n} \leq K_n^2$ . La démonstration s'achève comme ci-dessus, en remarquant que si les deux bases  $\mathcal{B}$  et  $u(\mathcal{B})$  de  $E$  fournissent la même représentation intégrale  $g \mapsto B_g$  du groupe  $G$ , le changement de base  $u$  appartient au commutant  $\mathcal{G}$  de  $G$  (comme on a  $g(u(e_j)) \cdot (u(e_i))^* = g(u(e_j)) \cdot {}^t u^{-1}(e_i^*) = (u^{-1}gu)(e_j) \cdot e_i^*$ , la condition sur  $u$  s'écrit  $u^{-1}gu = g$  pour tout  $g \in G$ ).  $\square$

*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  $\sigma$  un élément de  $O(E)$ . On rappelle que  $b_\sigma$  désigne la forme bilinéaire entière  $(x, y) \mapsto x \cdot \sigma y$ , et qu'un réseau  $\sigma$ -isodual est dit orthogonal (resp. symplectique) si  $b_\sigma$  est symétrique (resp. alternée). Il revient au même de dire que  $\sigma^2$  a pour carré  $+\text{Id}$  (resp.  $-\text{Id}$ ).

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

Nous allons tout d'abord examiner la structure de l'espace  $\mathcal{F}_\sigma$ . 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  $(x, y) \mapsto x \cdot y$  (resp.  $(x, y) \mapsto -x \cdot y$ ). On note  $U$  le module quadratique  $(\mathbf{Z}^2, 2x_1 x_2)$ . Enfin, pour  $p, q \geq 0$  entiers,  $pM + qN$  désigne la somme orthogonale de  $p$  copies de  $M$  et de  $q$  copies de  $N$ .