7. RÉSEAUX ISODUAUX ORTHOGONAUX ET SYMPLECTIQUES

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