Astérisque

A.-M. BERGÉ
J. MARTINET

Réseaux extrêmes pour un groupe d'automorphismes

Astérisque, tome 198-199-200 (1991), p. 41-66
<http://www.numdam.org/item?id=AST_1991__198-199-200__41_0>

© Société mathématique de France, 1991, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

RÉSEAUX EXTRÊMES POUR UN GROUPE D'AUTOMORPHISMES

par A-M. BERGÉ et J. MARTINET

1. Introduction. Soit V un espace vectoriel euclidien dont la dimension est notée n. Étant donné un réseau Λ de V, on note $\|\Lambda\| = \inf_{x\in\Lambda-\{0\}} \|x\|$ la norme du réseau, et $\Delta(\Lambda)$ son discriminant ($\Delta^2(\Lambda)$ est le déterminant de la matrice de Gram d'une base du réseau). On pose alors

$$\gamma_n(\Lambda) = \frac{\|\Lambda\|^2}{\Delta(\Lambda)^{\frac{2}{n}}}.$$

C'est un invariant de la classe de similitude de Λ. La *constante d'Hermite* pour la dimension n est

$$\gamma_n = \sup_{\Lambda} \gamma_n(\Lambda) \ ;$$

ses valeurs sont connues pour $n \leq 8$, et l'on dispose au-delà des majorations de Rogers.

Cette constante intervient dans de nombreuses inégalités utilisant la géométrie des nombres, par exemple dans les minorations à la Remak des régulateurs, ce qui a été le point de départ de cette étude (cf. [5], § 7 où est résumée une partie des résultats de cet article).

Soit maintenant G un sous-groupe fini du groupe orthogonal $O(V)$ de V. Si l'on se restreint aux réseaux Λ stables par G (les *G-réseaux*), on définit naturellement une "G-constante d'Hermite" $\gamma_{n,G}$. On peut alors améliorer la majoration classique chaque fois que les groupes d'automorphismes des *réseaux critiques* (i.e. qui réalisent γ_n) ne fournissent pas par restriction la représentation donnée de G. C'est ainsi que les minorations géométriques des régulateurs peuvent être améliorées pour certains types d'extensions galoisiennes.

Dans cet article, nous nous intéressons à la détermination des *maxima locaux* de $\gamma_n(\Lambda)$ sur les G-réseaux pour un groupe G donné (plus généralement, il est utile de se donner plutôt une représentation de G dans $O(V)$) ; les maxima globaux s'en déduisent : c'est le principe qui a été utilisé par Korkine et Zolotareff en 1877 pour calculer γ_5. Par analogie avec la situation classique, on introduit la notion de *réseau G-extrême*, qui se réduit à la notion habituelle de *réseau extrême* lorsque G est réduit à $\{\mathrm{Id}\}$ ou à $\{\pm\mathrm{Id}\}$, et, comme dans

le cas classique traité par Voronoï, on caractérise les réseaux G-extrêmes comme étant G-parfaits et eutactiques. C'est l'objet du § 2, où nous nous inspirons de la méthode qui a permis à Barnes de simplifier considérablement la démonstration de Voronoï.

Des résultats du § 2, on déduit dans le § 3 une minoration du nombre d'orbites de vecteurs minimaux sous l'action de G pour tout réseau G-parfait. C'est cette minoration qui est à la base de la détermination des réseaux G-parfaits (et donc des réseaux G-extrêmes) pour certaines représentations $G \to O(V)$ examinées au cours des §§ 4 et 5 : groupes cycliques irréductibles lorsque $\dim V = 4$ ou 6, puis, pour $\ell = 3$ ou 5, groupes cycliques d'ordre $\ell = \dim V$. En particulier, dans le cas d'un groupe cyclique irréductible d'ordre 5 ou 7, nous obtenons une majoration non triviale de la constante d'Hermite des G-réseaux, retrouvant dans le cas de l'ordre 5 un résultat obtenu par Schoof et Washington ([14]) à l'aide d'un calcul d'extremum. Un court § 6 est consacré à l'énoncé de quelques résultats obtenus postérieurement à l'exposé.

Il est à noter que, en établissant la liste des réseaux G-extrêmes dans les cas couverts par le § 4,nous retrouvons 4 des 5 constructions "cyclotomiques" trouvées par Craig ([10]) pour des réseaux extrêmes de dimension 6. L'idée d'utiliser des groupes d'automorphismes donnés *a priori* intervient également dans un travail d'Eva Bayer ([3]) dans lequel l'auteur s'intéresse à des formes quadratiques entières unimodulaires possédant un automorphisme de polynôme caractéristique donné.

2. Caractérisation des réseaux G-extrêmes . Dans tout ce §, on adoptera les notations suivantes : V désigne un espace *euclidien* de dimension $n > 0$, $\mathrm{Gl}(V)$ et $\mathrm{O}(V)$ ses groupes *linéaire* et *orthogonal*, $\mathcal{S}(V) = \mathcal{S}$ (resp. $\mathcal{S}^+(V) = \mathcal{S}^+$) l'ensemble des endomorphismes symétriques (resp. symétriques et à valeurs propres ≥ 0) de V. Rappelons que dans $\mathcal{S}^+$ tout élément a une unique racine carrée, d'où l'on déduit :

2.1 LEMME. *(i) Tout $u \in Gl(V)$ s'écrit de façon unique $u = sf$, avec $s \in \mathcal{S}^+$ et $f \in O(V)$.*

(ii) Soient $s \in \mathcal{S}^+$ et $g \in O(V)$. Alors on a l'équivalence : $s^{-1}gs \in O(V) \Leftrightarrow sg = gs$.

Démonstration. (i) : on prend pour s la racine carrée positive de ${}^t uu \in \mathcal{S}^+$. (ii) : on a les équivalences $s^{-1}gs \in \mathrm{O}(V) \Leftrightarrow {}^t(s^{-1}gs) = (s^{-1}gs)^{-1} \Leftrightarrow sg^{-1}s^{-1} = s^{-1}g^{-1}s \Leftrightarrow s^2 = (g^{-1}sg)^2 \Leftrightarrow s = g^{-1}sg$.

On note $\mathcal{R}$ l'ensemble des *réseaux de* V. Il est muni d'une *topologie naturelle* que l'on peut décrire ainsi : les sous-ensembles $\mathcal{V}'$ de $\mathcal{R}$ de la forme $\mathcal{V}\Lambda$ (=$\{ s\Lambda, s \in \mathcal{V}\}$) où $\mathcal{V}$ est un voisinage de l'identité dans $\mathrm{Gl}(V)$ constituent un système fondamental de voisinages d'un réseau Λ. Alors, l'application $s \mapsto s\Lambda$

de $\mathcal{V}$ dans $\mathcal{V}'$ ci-dessus est bijective si on se limite à des voisinages de l'identité assez petits, puisque le *stabilisateur* $\mathrm{Gl}(\Lambda)$ *de* Λ *dans* $\mathrm{Gl}(V)$ est discret. (La condition "assez petit" dépend du réseau Λ.) L'ensemble des *classes d'isométrie* de réseaux est également muni d'une topologie naturelle, à savoir la topologie quotient de $\mathcal{R}$ par l'action du groupe orthogonal.

Soit Λ un réseau de V ; son groupe d'automorphismes $\mathrm{Aut}(\Lambda) = \{u \in \mathrm{O}(V) \mid u\Lambda \subset \Lambda\}$ est un sous-groupe compact donc fini de $\mathrm{Gl}(\Lambda)$, dont l'espace vectoriel $W = \mathbb{Q}\Lambda$ est une représentation rationnelle. Inversement, soit G un groupe fini tel que V provienne d'une représentation W de G dans $\mathrm{O}(V)$ rationnelle sur $\mathbb{Q}$. Le sous-ensemble $\mathcal{R}_G$ de $\mathcal{R}$ formé des réseaux stables par G ("*G-réseaux*") n'est pas vide. (Si $e_1, e_2, ..., e_n$ est une $\mathbb{Q}$-base de W, le sous-groupe Λ de W engendré par les $s(e_i), s \in G, i = 1, 2, ..., n$ est un réseau de $\mathcal{R}_G$.) *Nous supposons désormais que les couples (V, G) vérifient les hypothèses ci-dessus.* Notons que l'on peut se ramener facilement au cas où la représentation W est fidèle, ce qui revient à supposer que G est un sous-groupe de $\mathrm{O}(V)$.

On munit $\mathcal{R}_G$ de la topologie induite par celle de $\mathcal{R}$. Soit $\Lambda \in \mathcal{R}_G$ et soit $\mathcal{V}'$ un voisinage de Λ dans $\mathcal{R}$ provenant d'un voisinage $\mathcal{V}$ de Id dans $\mathrm{Gl}(V)$. Si $\mathcal{V}$ est assez petit, les éléments u de $\mathcal{V}$ qui s'appliquent sur $\mathcal{V}' \cap \mathcal{R}_G$ par la bijection $u \mapsto u\Lambda$ sont ceux qui commutent avec G (puisque, pour tout $g \in G$, ils doivent vérifier $gug^{-1}\Lambda = u\Lambda$). D'après 2.1., la composante symétrique $s \in \mathcal{S}^+$ d'un tel u doit aussi commuter avec G. Notons $\mathcal{S}_G$ (resp. $\mathcal{S}_G^+$) le *commutant de G dans $\mathcal{S}$* (resp. *dans $\mathcal{S}^+$*). Les images canoniques des ensembles $\{s\Lambda \mid s \in \mathcal{V} \cap \mathcal{S}_G^+\}$ forment, quand $\mathcal{V}$ décrit l'ensemble des voisinages de Id dans $\mathrm{Gl}(V)$, un système fondamental de voisinages de la classe d'isométrie de Λ.

2.2 DÉFINITION. Un G-réseau est dit *G-extrême* (resp. *G-critique*) s'il réalise un maximum local (resp. absolu) de la fonction γ_n dans $\mathcal{R}_G$.

Notons que cette notion ne dépend que de la classe de similitude du réseau.

Rappelons quelques notions et notations relatives à la *méthode de Korkine et Zolotareff* (cf. [11], [1] et [4]) ; on note $S(\Lambda)$, ou simplement S, l'ensemble des *vecteurs minimaux* de Λ.

Pour $x \neq 0$, on note φ_x la forme linéaire $u \mapsto x.u(x)$ sur $\mathcal{S}$ et p_x la projection orthogonale de V sur la droite $\mathbb{R}x$. Un réseau de V est dit *parfait* si le dual $\mathcal{S}^*$ de $\mathcal{S}$ est engendré par les formes φ_x, $x \in S$, et *eutactique* si l'endomorphisme Trace est combinaison linéaire à coefficients *strictement* positifs des φ_x, $x \in S$.

En termes de projections, "parfait" signifie que les $(p_x)_{x \in S}$ engendrent $\mathcal{S}$, et "eutactique" que l'identité est combinaison linéaire à coefficients > 0 des p_x (la traduction se fait par dualité par rapport à la forme quadratique définie positive $u \mapsto \mathrm{Tr}(u^2)$ sur $\mathcal{S}$, cf. [4], rem. 3.12).

2.3 DÉFINITION. On dit qu'un G-réseau est *G-parfait* si le dual $\mathcal{S}_G^*$ de $\mathcal{S}_G$ est engendré par les restrictions à $\mathcal{S}_G$ des formes linéaires φ_x, $x \in S$, et qu'il est *G-eutactique* si la restriction à $\mathcal{S}_G$ de la forme linéaire Trace est combinaison linéaire à coefficients positifs des restrictions à $\mathcal{S}_G$ des φ_x.

Notons que ces notions ne font intervenir que l'ensemble S des vecteurs minimaux du G-réseau. Le groupe G opère sur cet ensemble, et les restrictions à $\mathcal{S}_G$ des formes linéaires φ_x, $x \in S$ sont constantes sur les orbites de S sous G : on a en effet, pour tous $x \in S$, $g \in G$ et $u \in \mathcal{S}$, $\quad \varphi_{gx}(u) = \varphi_x(g^{-1}ug)$. On en déduit immédiatement :

2.4 PROPOSITION. *Le nombre d'orbites sous G de couples $\{\pm x\}$ de vecteurs minimaux d'un réseau G-parfait est au moins égal à la dimension de l'espace $\mathcal{S}_G$ des endomorphismes symétriques de V commutant avec G.*

(Quitte à grossir G en le remplaçant par $G \cup -G$, on pourrait supposer que deux vecteurs opposés sont toujours dans une même orbite.)

Remarquons que la G- perfection peut s'écrire ainsi : le système

$$\forall x \in S, \qquad \varphi_x(u) = 0$$

n'a pas de solution non triviale $u \in \mathcal{S}_G$. Cela permet d'obtenir pour les G-réseaux parfaits une caractérisation par *rigidité* analogue au mystérieux

"Toute forme extrême a au moins $\frac{n(n+1)}{2}$ représentations de son minimum qui déterminent complètement cette forme, en supposant que son minimum soit donné"

de Korkine et Zolotareff (Math. Annalen 11 (1877), p. 252) :

2.5 PROPOSITION. *Tout réseau G-parfait a au moins* $\dim \mathcal{S}_G$ *orbites de couples $\{\pm x\}$ de vecteurs minimaux, dont la configuration par rapport au réseau le détermine complètement à isométrie près. En particulier, $\gamma_{n,G}^n \in \mathbb{Q}$.*

[Précisons le sens que nous donnons dans le cas des G-réseaux au mot configuration : étant donnés deux réseaux Λ et Λ' *munis de bases $\mathcal{B}$ et $\mathcal{B}'$*, on dit que leurs ensembles S et S' de vecteurs minimaux ont *mêmes configurations par rapport à ces bases* s'il existe une bijection de $S(\Lambda)$ sur $S(\Lambda')$ *respectant les orbites sous G* telle que la matrice de S dans $\mathcal{B}$ ait pour image la matrice de S' dans $\mathcal{B}'$.]

Comme dans le cas classique, cette propriété d'unicité assure réciproquement la G-perfection. Comme la perfection (et du reste également l'eutaxie) ne dépend que du sous-réseau engendré par les vecteurs minimaux, on en déduit :

2.6 PROPOSITION. *Pour qu'un G-réseau Λ soit G-parfait, il faut et il suffit qu'une matrice de Gram d'une base de Λ soit déterminée de façon unique par les composantes dans cette base des vecteurs minimaux de Λ.*

Nous reviendrons sur cette question d'unicité au paragraphe suivant (prop. 3.12).

Remarquons que si H est un sous-groupe de G, tout réseau H-parfait (resp. H-eutactique, resp. H-extrême) est G-parfait (resp. G-eutactique, G-extrême), et que pour $G = \{\mathrm{Id}\}$ ou $\{\pm\mathrm{Id}\}$, on retrouve les notions usuelles. En fait, pour un G-réseau, les notions de G-eutaxie et d'eutaxie sont équivalentes :

2.7 LEMME. *Pour qu'un G-réseau soit G-eutactique, il faut et il suffit qu'il soit eutactique.*

Démonstration. Que la condition soit suffisante résulte des remarques ci-dessus. Pour la réciproque, on observe qu'à tout $u \in \mathcal{S}$ on peut associer de façon naturelle un endomorphisme symétrique u_G commutant avec G : on pose

$$u_G = \frac{1}{\operatorname{card} G} \sum_{g \in G} gug^{-1}.$$

On a alors $\mathrm{Tr}(u_G) = \mathrm{Tr}(u)$, et $\varphi_x(u_G) = \frac{1}{\operatorname{card} G} \sum_{g \in G} \varphi_x(u)$, d'où l'équivalence

$$\mathrm{Tr}(u_G) = \sum_{x \in S} \rho_x \varphi_x(u_G) \Leftrightarrow \mathrm{Tr}(u_G) = \sum_{x \in S} \alpha_x \varphi_x(u)$$

avec $\alpha_x = \frac{1}{\operatorname{Card} G} \sum_{g \in G} \rho_{gx}$. On en déduit immédiatement 2.4.

Par dualité, la G-perfection peut être caractérisée ainsi :

2.8 PROPOSITION. *Un G-réseau est G-parfait si et seulement si les endomorphismes $p_{x,G} = \frac{1}{\operatorname{card} G} \sum_{g \in G} gp_x g^{-1} = \frac{1}{\operatorname{card} G} \sum_{g \in G} p_{gx}$ engendrent $\mathcal{S}_G$.*

Comme conséquence immédiate des définitions, on obtient le résultat important suivant :

2.9 PROPOSITION. *Les vecteurs minimaux d'un réseau G-parfait ou G-eutactique engendrent l'espace vectoriel V.*

Démonstration. Soit V' le sous-espace de V orthogonal à tous les vecteurs minimaux du réseau. Il est stable par G, donc la projection orthogonale u de V sur V' appartient à $\mathcal{S}_G$, et l'on a $\varphi_x(u) = 0$ pour tout $x \in S$, d'où, si le réseau est G-parfait (resp. eutactique), u=0 (resp. $\mathrm{Tr}(u)$=0), donc $V' = \{0\}$.

Les notions introduites ci-dessus permettent une caractérisation des réseaux G-extrêmes analogue à celle obtenue par Voronoï et dont la démonstration que nous donnons est inspirée par la démonstration très simple donnée par Barnes ([1]) dans le cas classique :

2.10 THÉORÈME. *Pour qu'un G-réseau soit G-extrême, il faut et il suffit qu'il soit G-parfait et eutactique.*

On démontre d'abord le lemme suivant :

2.11 LEMME. *Soit Λ un G-réseau.*
1. Les conditions suivantes sont équivalentes :
(i) Λ est G-extrême ;
(ii) dans $\mathcal{S}_G$, le système d'inégalités

$$(1) \qquad \begin{cases} x.u(x) \geq 0 \ \textit{pour tout } x \in S(\Lambda) \\ \quad Tru \leq 0 \end{cases}$$

n'a pas d'autre solution que $u = 0$.
2. Si Λ est G-extrême, on a $\gamma_n(\Lambda') < \gamma_n(\Lambda)$ pour tout G-réseau Λ' suffisamment voisin de Λ et non semblable à Λ.

Démonstration du lemme. Soit Λ' un G-réseau voisin de Λ et non semblable à Λ ; il peut s'écrire

$$\Lambda' = v\Lambda, \qquad \text{avec } v = \mathrm{Id} + \epsilon u,\ \epsilon > 0, u \neq 0 \ \in \mathcal{S}_G.$$

Il s'agit de comparer les constantes d'Hermite donc les normes et les discriminants de Λ et $v\Lambda$. On suppose ϵ assez petit pour que les vecteurs minimaux de $v\Lambda$ proviennent de ceux de Λ. Soit $x \in V$; avec les notations ci-dessus, la relation

$$\|v(x)\|^2 - \|x\|^2 = 2\epsilon x.u(x) + \epsilon^2\|u(x)\|^2 \qquad (x \in V)$$

montre l'équivalence

$$\|v(x)\|^2 \geq \|x\|^2 \iff x.u(x) \geq 0\,,$$

d'où aussi

$$(2) \qquad \|v\Lambda\| \geq \|\Lambda\| \iff \forall x \in S(\Lambda),\ \varphi_x(u) \geq 0.$$

Notons $X^n - T_1(u)X^{n-1} + T_2(u)X^{n-2} + ... + (-1)^n T_n(u) = \prod_i (X - \lambda_i)$ le polynôme caractéristique de u, où T_1 est la forme linéaire Trace, et où $T_2(u) = \frac{1}{2}(T_1(u)^2 - \sum \lambda_i^2)$ est $< \frac{1}{2}T_1(u)^2$. Le développement

$$\frac{\Delta(v\Lambda)}{\Delta(\Lambda)} - 1 = \epsilon T_1(u) + \epsilon^2 T_2(u) + ...$$

fournit les implications (pour $u \neq 0 \in \mathcal{S}$)

$$(3) \qquad \begin{aligned} T_1(u) > 0 &\Rightarrow \Delta(v\Lambda) > \Delta(\Lambda) \\ T_1(u) \leq 0 &\Rightarrow \Delta(v\Lambda) < \Delta(\Lambda). \end{aligned}$$

Supposons alors que Λ ne vérifie pas la conditon (ii) du lemme, et soit $u \in \mathcal{S}_G$ une solution non triviale de (1). Le réseau $v\Lambda$ correspondant vérifie $\|v\Lambda\| \geq \|\Lambda\|$ d'après (2) et $\Delta(v\Lambda) < \Delta(\Lambda)$ d'après (3), d'où $\gamma_n(v\Lambda) > \gamma_n(\Lambda)$: le réseau Λ n'est pas G-extrême. Réciproquement, supposons (ii) vérifiée par Λ et soit Λ' un G-réseau voisin de Λ, non semblable à Λ, que l'on peut supposer de même norme que Λ (quitte à le remplacer par un réseau homothétique). L'endomorphisme non nul $u \in \mathcal{S}_G$ correspondant à Λ' vérifie alors les inégalités $\varphi_x(u) \geq 0$ pour tout $x \in S$ d'après (2) ; comme il ne peut vérifier (1) (condition (ii)), on a $\mathrm{Tr}u > 0$ d'où, par (3), $\Delta(\Lambda') > \Delta(\Lambda)$ et $\gamma_n(\Lambda') < \gamma_n(\Lambda)$, ce qui prouve que Λ est G-extrême et démontre aussi 2.

La caractérisation des réseaux G-extrêmes à l'aide de la condition (ii) du lemme 2.11 repose sur un théorème de Stiemke très utile en programmation linéaire et que Barnes ([1]) a eu l'idée d'exhumer pour l'étude de la situation classique :

2.12 LEMME (STIEMKE, 1915). *Soit E un espace vectoriel réel de dimension finie et soient $\varphi_1, ..., \varphi_p$ des formes linéaires sur E. Les conditions suivantes sont équivalentes :*
(i) Il existe des nombres réels $\rho_1, ..., \rho_p$ positifs tels que $\rho_1\varphi_1 + ... + \rho_p\varphi_p = 0$;
(ii) Toute solution $v \in E$ au système d'inéquations $\varphi_j(v) \geq 0$, $j = 1, ..., p$ vérifie les égalités $\varphi_j(v) = 0$ pour $j = 1, ..., p$.

Démonstration du théorème. On applique 2.11 aux formes linéaires φ_x, $x \in S$ et $-\mathrm{Tr}$ sur $E = \mathcal{S}_G$, de sorte que la condition (i) du lemme exprime l'eutaxie du G-réseau.

Notons, pour $u \in \mathcal{S}_G$, (1) la condition "$\forall x \in S$, $\varphi_x(u) \geq 0$ et $-\mathrm{Tr}u \geq 0$", et (2) la condition "$\forall x \in S$, $\varphi_x(u) = 0$".

Par 2.11, "Λ G-extrême " équivaut à "(1) implique $u = 0$ ". Par définition, "Λ G-parfait " équivaut à "(2) implique $u = 0$ ". Par 2.11., "Λ eutactique " équivaut à "(1) implique (2) et $-\mathrm{Tr}u \geq 0$".

Supposons le réseau G-extrême, et soit $u \in \mathcal{S}_G$ vérifiant (2); u ou $-u$ vérifie (1), donc est nul. Si $u \in \mathcal{S}_G$ vérifie (1), il est nul, donc vérifie (2) et $-\mathrm{Tr}u \geq 0$.

Réciproquement, supposons Λ G-parfait et eutactique, et soit $u \in \mathcal{S}_G$ vérifiant (1) ; il vérifie aussi (2), donc $u = 0$, **c.q.f.d.**

3. Calculs de dimensions. Dans ce §, nous déterminons la dimension de l'espace vectoriel $\mathcal{S}_G$ des endomorphismes symétriques de V qui commutent

avec G. Nous donnons en outre la structure des G-réseaux extrêmes qui sont sommes directes orthogonales de sous-réseaux stables. Nous conservons les notations du § 2.

Soit $V = V_1 \perp V_2 \perp \ldots \perp V_r$ une décomposition de V en somme directe orthogonale de sous-espaces stables par G. Pour tout i, soit p_i la projection orthogonale de V sur V_i. Soit $u \in \mathrm{End}(V)$. Il se décompose de manière unique en somme $\sum u_{ij}$ où $u_{ij} \in \mathrm{End}(V)$ est nul sur les V_k pour $k \neq i$ et a une image contenue dans V_j : on a en fait $u_{ij} = p_j \circ u \circ p_i$. On identifiera souvent $u_{ij} \in \mathrm{End}(V)$ avec l'homomorphisme de V_i dans V_j qu'il définit. Pour tout couple (i,j), on a ${}^t(u_{ij}) = ({}^tu)_{ji}$, et, en particulier, u est symétrique si et seulement si les u_{ij} vérifient les relations ${}^tu_{ij} = u_{ji}$. De même, u commute avec G si et seulement tous les u_{ij} commutent avec G. Par ailleurs, pour tout $x \in V_i$, $\varphi_x(u_{jk})$ est nul sauf peut-être si $i = j = k$ (cf. § 2 après 2.2 pour la définition de φ_x). En particulier :

3.1 PROPOSITION. *Soit i, $1 \leq i \leq r$, soit $x \in V_i$ et soit $u = \sum_{jk} u_{jk} \in$ End(V). Alors, $\varphi_x(u) = \varphi_x(u_{ii})$.*

Pour tout caractère $\mathbb{R}$-irréductible χ de G, et pour tout sous-espace stable V' de V, notons V'_χ la somme des sous-espaces de V' de caractère χ. L'espace V' est somme directe orthogonale de ses sous-espaces stables V'_χ. En particulier, on a $V = \perp_\chi V_\chi$. Comme $\mathrm{Hom}_{\mathbb{R}[G]}(V_\chi, V_{\chi'})$ est réduit à zéro pour $\chi \neq \chi'$, on a

$$\mathcal{S}_G(V) = \oplus_\chi \mathcal{S}_G(V_\chi)\,, \tag{3.2}$$

d'où en particulier

$$\dim_{\mathbb{R}} \mathcal{S}_G(V) = \sum_\chi \dim_{\mathbb{R}} \mathcal{S}_G(V_\chi)\,.$$

Rappelons (cf. [12], § 13.2, pp. 122-123) qu'*un caractère $\mathbb{R}$-irréductible* (i.e. le caractère d'une représentation irréductible de G sur $\mathbb{R}$) χ est de l'un des trois types suivants : (I) χ est un caractère "réel", i.e. le caractère d'une représentation $\mathbb{C}$-irréductible de G réalisable sur $\mathbb{R}$; (II) $\chi = \varphi + \bar{\varphi}$, où φ est un caractère $\mathbb{C}$-irréductible qui prend au moins une valeur non réelle ; (III) $\chi = 2\varphi$ où φ est à valeurs réelles, mais n'est pas le caractère d'une représentation réalisable sur $\mathbb{R}$. Les commutants de ces trois types de caractères sont isomorphes respectivement à $\mathbb{R}$, $\mathbb{C}$ et $\mathbb{H}$ ($\mathbb{H}$ désigne le corps des quaternions de Hamilton). Notons maintenant a_χ le nombre de fois que le caractère de V_χ contient χ, $K_\chi = K$ le commutant de χ, et soit $b_\chi = [K_\chi : \mathbb{R}]$ (donc, $b_\chi = 1$, 2 ou 4).

3.3 PROPOSITION. *On a :*

$$\dim_{\mathbb{R}} \mathcal{S}_G(V_\chi) = \begin{cases} \dfrac{a_\chi(a_\chi+1)}{2} & si\ K=\mathbb{R}\ ; \\ a_\chi^2 & si\ K=\mathbb{C}\ ; \\ a_\chi(2a_\chi-1) & si\ K=\mathbb{H}\ . \end{cases}$$

Démonstration. Écrivons V_χ sous la forme d'une somme directe de sous-espaces irréductibles stables W_i, $1 \leq i \leq a_\chi$, chacun des W_i étant isomorphe à un même espace W irréductible sur $\mathbb{R}$. Alors, $\mathrm{End}_{\mathbb{R}[G]}(V_\chi)$ est isomorphe à $\mathcal{M}_{a_\chi}(\mathrm{End}_{\mathbb{R}[G]}(W)) = \mathcal{M}_{a_\chi}(K)$, et son sous-espace $\mathrm{End}^s(V_\chi)$ formé des endomorphismes symétriques s'identifie au sous-espace de $\mathcal{M}_{a_\chi}(\mathrm{End}_{\mathbb{R}[G]}(W))$ dont les éléments diagonaux sont symétriques, c'est-à-dire réels, et tels que deux éléments symétriques par rapport à la diagonale soient transposés l'un de l'autre. (Dans l'identification à une algèbre de matrices $\mathcal{M}_m(K)$ du facteur simple associé à une représentation irréductible, la transposée d'une matrice P est ${}^t\bar{P}$, où $^-$ désigne la conjugaison dans K.) On a donc $\dim_{\mathbb{R}} \mathcal{S}_G(V_\chi) = a_\chi + b_\chi \frac{a_\chi(a_\chi-1)}{2}$, ce qui est bien la formule de la prop. 3.3. Revenons maintenant à des décompositions orthogonales plus générales que la décomposition canonique.

3.4 PROPOSITION. *Soit $V = V_1 \perp V_2 \perp \ldots \perp V_r$ une décomposition de V en somme directe orthogonale de sous-espaces stables par G. Alors, $\mathcal{S}_G(V)$ contient la somme des $\mathcal{S}_G(V_i)$, et l'égalité a lieu si et seulement si les V_i sont sans composantes irréductibles communes.*

Démonstration. L'inclusion $\mathcal{S}_G(V) \supset \oplus\mathcal{S}_G(V_i)$ est évidente. Si les V_i sont sans composantes irréductibles communes, alors, pour tout χ, V_χ est égal à l'un des $V_{i,\chi}$, et l'inclusion est une égalité par 3.2. Dans le cas contraire, il existe un couple (i,j) pour lequel $\mathrm{Hom}_{\mathbb{R}[G]}(V_i, V_j)$ contient un élément $v \neq 0$. Alors, l'élément $u \in \mathrm{End}_{\mathbb{R}[G]}(V)$ défini par $u_{ij} = v$, $u_{ji} = {}^t v$ et $u_{kl} = 0$ pour $\{k,l\} \neq \{i,j\}$ appartient à $\mathcal{S}_G(V)$ mais pas à $\oplus\mathcal{S}_G(V_k)$.

Nous appliquons maintenant ce qui précède à l'étude des G-réseaux décomposables.

3.5 PROPOSITION. *Soit Λ un réseau, somme directe orthogonale de réseaux relatifs $\Lambda_1, , \Lambda_2, \ldots, \Lambda_r$. Alors :*

(i) *$S(\Lambda)$ est égal à la réunion des $S(\Lambda_i)$ pour les i tels que $\|\Lambda_i\|$ soit minimal.*

(ii) *Λ est eutactique si et seulement si les réseaux Λ_i sont eutactiques et ont même norme.*

Démonstration. L'assertion (i) est évidente, et elle entraîne que l'endomorphisme identité de V, qui est somme des projections p_{V_i} sur les V_i, ne peut s'écrire comme combinaison des p_x, $x \in S(\Lambda)$ que si $S(\Lambda)$ contient tous les $S(\Lambda_i)$, ce qui donne la condition d'égalité des normes dans l'assertion (ii). Lorsque cette condition est satisfaite, comme la restriction de p_{V_i} à V_i est l'identité de V_i pour tout i, il est clair que Λ est eutactique si et seulement si tous les Λ_i le sont.

3.6 THÉORÈME. *Soit Λ un G-réseau, somme directe orthogonale de G-réseaux relatifs $\Lambda_1, \Lambda_2, ..., \Lambda_r$. Pour que le réseau Λ soit G-parfait (resp. G-extrême), il faut et il suffit que les trois conditions suivantes soient satisfaites :*

(i) *Les réseaux Λ_i ont même norme ;*
(ii) *Les réseaux Λ_i sont G-parfaits (resp. G-extrêmes) ;*
(iii) *Les restrictions aux sous-espaces V_i de la représentation définie par V sont sans composantes irréductibles communes.*

Démonstration. Étudions d'abord la perfection du réseau Λ. Un argument analogue à celui qui a été utilisé pour démontrer 3.5 montre tout de suite que les conditions (i) et (ii) sont vérifiées lorsque Λ est G-parfait. Lorsqu'elles sont vérifiées, on a, quel que soit $x \in S$ et $u_{ij} \in \mathrm{Hom}_{\mathbb{R}[G]}(V_i, V_j)$ avec $i \neq j$, $\varphi_x(u_{ij}) = 0$ (cf. 3.1 et 3.5, (i)). La proposition 3.4 montre que le sous-espace de $\mathrm{End}(V)^*$ engendré par les φ_x, $x \in S(\Lambda)$ est somme directe de ses sous-espaces engendrés par les φ_x , $x \in S(\Lambda_i)$ si et seulement si la condition (iii) est satisfaite.

Comme Λ est G-extrême si et seulement s'il est G-parfait et eutactique (th. 2.10), l'assertion relative au caractère extrémal de Λ est une conséquence immédiate de la prop. 3.5.

Le cas où V est $\mathbb{R}$-irréductible est particulièrement simple : en effet, il résulte de la proposition 3.3 que $\mathcal{S}_G(V)$ est alors de dimension 1 sur $\mathbb{R}$ (et la réciproque est du reste exacte). La description de la topologie de $\mathcal{R}_G$ faite au début du § 2 montre alors tout de suite le résultat suivant :

3.7 PROPOSITION. *Lorsque V est $\mathbb{R}$-irréductible, tous les G-réseaux de V sont G-extrêmes.*

C'est en particulier le cas en dimension 2 pour le réseau hexagonal lorsque G est cyclique d'ordre 3 ou 6 et pour le réseau carré lorsque G est cyclique d'ordre 4 ; de façon générale, cela se produit chaque fois que le groupe G est "gros" relativement à la dimension de V.

La proposition 2.4 se réduit dans le cas classique où $G = \{\mathrm{Id}\}$ à l'inégalité $s \geq n(n+1)/2$ de Korkine et Zolotareff que doit vérifier le nombre s de couples $\{\pm x\}$ de vecteurs minimaux de tout réseau parfait. C'est cette inégalité qui

est à la base de leur détermination des réseaux parfaits de dimension ≤ 5. Une analyse de leurs démonstrations montre qu'ils ont en fait prouvé le résultat plus fort suivant :

3.8 THÉORÈME (KORKINE ET ZOLOTAREFF, 1877). *Un réseau parfait de dimension $n \leq 5$ est extrême, et est semblable à l'un des réseaux A_1, A_2, A_3, D_4, A_4, D_5, A_5^3 ou A_5. En outre, pour $n \leq 4$, l'inégalité $s \geq n(n+1)/2$ assure la perfection.*

Rappelons brièvement les notations (cf. [6]).

Pour tout $n \geq 1$, A_n désigne la section du réseau cubique $\mathbb{Z}^{n+1} \subset \mathbb{R}^{n+1}$ par l'hyperplan orthogonal au vecteur $(1, 1, ..., 1)$. C'est un réseau extrême ; on a $\|A_n\|^2 = 2$, $s(A_n) = n(n+1)/2$ et $\Delta^2(A_n) = n+1$. Il possède une base $e_1, ..., e_n$ de vecteurs minimaux pour laquelle on a $e_i.e_j = 1$ pour $j \neq i$. Son dual A_n^*, pour lequel $s = n+1$, n'est pas parfait lorsque n est ≥ 3. L'opération de $\mathrm{Aut}(A_n) = \mathrm{Aut}(A_n^*)$ sur $S(A_n^*)$ permet d'identifier ce groupe à $\{\pm\mathrm{Id}\} \times S_{n+1}$. En particulier, pour ℓ premier, A_ℓ possède un automorphisme de polynôme caractéristique $X^\ell - 1$, et $A_{\ell-1}$ possède un automorphisme $\mathbb{Q}$-irréductible d'ordre ℓ.

Le réseau A_n^t (notation de Coxeter) est défini pour $1 \leq t \leq n+1$, $t|(n+1)$, en ajoutant à la base précédente de A_n le vecteur $\frac{e}{t}$ où $e = e_1 + ... + e_n$. Il est stable par $\mathrm{Aut}(A_n)$. Son dual est semblable à $A_n^{t'}$ où $tt' = n+1$. (Le réseau A_n^t est noté $A_n[t']$ dans [6], ch. 4, § 6.6, et A_n^{+t} dans [7], § 5.)

Pour tout $n \geq 4$, D_n désigne le sous-réseau de $\mathbb{Z}^n$ formé des points dont la somme des coordonnées est paire. C'est un réseau extrême ; on a $\|D_n\|^2 = 2$, $s = n(n-1)$, et $\Delta^2(D_n) = 4$. Le dual de D_n est un réseau cubique centré. Pour $n \geq 5$, il n'est pas parfait, car $s(D_n^*) = n$, et l'opération de $\mathrm{Aut}(D_n)$ sur D_n^* identifie ce groupe à $\{\pm\mathrm{Id}\}^n \times S_n$. Pour $n = 4$, D_4 et D_4^* sont semblables, et leur groupe d'automorphismes est une extension du groupe précédent par un groupe d'ordre 3. En particulier, si ℓ est premier, $\mathrm{Aut}(D_\ell)$ contient un automorphisme de polynôme caractéristique $X^\ell - 1$, et D_4 possède des automorphismes irréductibles d'ordre 8 et 12.

La détermination des réseaux parfaits de dimension 6 a été effectuée par Barnes ([2]) en 1957, qui a prouvé qu'il existe à similitude près exactement 7 réseaux parfaits, dont 6 extrêmes. La démonstration de Barnes utilise l'algorithme de Voronoï, et ne permet pas de prouver la perfection des réseaux ayant suffisamment de vecteurs minimaux. Du reste, l'énoncé analogue à 3.8 est faux en dimension $n \geq 6$, comme le montre l'exemple de la somme othogonale $D_{n-1} \perp A_1$, qui est un réseau non parfait possédant $(n-1)(n-2)+1 \geq n(n+1)/2$ vecteurs minimaux. (En dimension 5, l'énoncé est correct à condition de se limiter aux réseaux ne possédant pas de section hyperplane isométrique à D_4.)

Nous décrivons maintenant ceux de ces réseaux que nous aurons à utiliser dans la suite. Deux d'entre eux, dont le réseau non extrême, ont un groupe d'automorphismes réductible. Les 5 autres sont A_6, D_6, le réseau critique E_6 (cf. ci-dessous), son dual E_6^*, et le réseau P_6 de Barnes (noté $A_6^{(2)}$ dans [7]), qui est le sous-réseau de A_6 formé des points de $\mathbb{Z}^7$ dont les coordonnées vérifient la congruence $\sum_i ix_i \equiv 0 \mod 7$. Il est semblable à son dual, et possède un automorphisme d'ordre 7. Les réseaux E_6 et E_6^* (ce dernier est semblable au réseau appelé L_6^3 par Barnes et noté $A_{6,0}$ dans [7]) possèdent un automorphisme d'ordre 9.

On note E_8 le réseau A_8^3 (autre construction : E_8 est le réseau D_8^+ engendré par D_8 et le vecteur de composantes $\frac{1}{2}$). En coupant E_8 par un sous-espace orthogonal à un vecteur minimal (resp. à un plan hexagonal de vecteurs minimaux), on obtient E_7 (resp. E_6) ; E_7 est semblable à A_7^2, et possède donc un automorphisme d'ordre 7.

Dans la suite, les évaluations de $\dim \mathcal{S}_G$ que nous avons données seront utilisées comme minorations des nombres d'orbites de vecteurs minimaux des réseaux G-parfaits. L'énoncé suivant, facile mais d'usage constant, apporte quelques précisions sur ces vecteurs minimaux :

3.9 PROPOSITION. *Soit Λ un réseau G-parfait engendrant l'espace vectoriel V.*

(i) *Si V est $\mathbb{Q}$-irréductible, l'orbite d'un vecteur non nul de Λ engendre V ;*

(ii) *Si en outre G est abélien et fidèle, le nombre de couples $\{\pm x\}$ de vecteurs contenus dans l'orbite d'un vecteur non nul de Λ est égal à l'ordre de G si $-Id$ n'appartient pas à G, et à la moitié de l'ordre de G sinon.*

Démonstration. L'assertion (i) résulte de la définition même de l'irréductibilité. Pour prouver (ii), il suffit de remarquer que la seule réalisation comme groupe de permutations fidèle d'un groupe abélien est la permutation régulière.

Pour terminer ce §, nous donnons, en suivant Korkine et Zolotareff, des résultats concernant l'indice dans un réseau Λ d'un sous-réseau Λ' de même norme ($S(\Lambda)$ et $S(\Lambda')$ engendrant tous deux l'espace V). On supposera dans la suite que les deux réseaux sont de norme 1, ce que l'on peut faire sans restreindre la généralité.

3.10 PROPOSITION.

(i) *L'indice $[\Lambda : \Lambda']$ est majoré par $\{\gamma_n/\gamma_n(\Lambda')\}^{n/2}$, avec égalité si et seulement si Λ est critique ; en particulier, on a la majoration $[\Lambda : \Lambda'] \leq \gamma_n^{n/2}$ indépendante de Λ.*

(ii) *On suppose que Λ possède une base e_1, e_2, ..., e_n formée de vecteurs de $S(\Lambda)$. Soient e'_1, e'_2, ..., e'_r $(r \leq n)$ des vecteurs de $S(\Lambda)$. Alors, les déterminants d'ordre $\leq r$ extraits de la matrice des composantes des e'_j dans la base e_i de V sont $\leq \gamma_n^{n/2}$.*

En effet, $\gamma_n(\Lambda)^{-n/2}$ est égal au discriminant $\Delta(\Lambda)$ du réseau Λ, ce qui prouve les deux assertions de (i), compte tenu de l'inégalité $\Delta(\Lambda) \leq 1$ valable pour tout réseau engendré par des vecteurs de norme 1, qui découle de l'inégalité de Hadamard appliquée à un sous-réseau de Λ ayant une base formée de tels vecteurs. L'assertion (ii) est évidente lorsque les e'_i sont dépendants. Dans le cas contraire, on complète cet ensemble de vecteurs en une base de V par $n-r$ vecteurs convenablement choisis parmi les e_i. Le déterminant de ce système de vecteurs dans la base (e_i) est alors précisément le déterminant extrait que l'on cherche, **c.q.f.d.**

Compte tenu des valeurs de la constante d'Hermite, connues pour $n \leq 8$, on obtient les majorations suivantes pour $[\Lambda : \Lambda']$:

3.11 PROPOSITION. *Avec les notations de 3.10, l'indice $[\Lambda : \Lambda']$ est majoré par 1 pour $n \leq 3$, par 2 pour $n = 4$, 5 , par 4 pour $n = 6$, par 8 pour $n = 7$ et par 16 pour $n = 8$. En outre, pour $n = 4$ (resp. 8), on peut remplacer 2 par 1 (resp. 16 par 15) si Λ n'est pas critique.*

Combinés avec les résultats du § 2, les majorations d'indice permettent de démontrer une assertion de finitude :

3.12 PROPOSITION. *L'ensemble des classes de similitude de réseaux G-parfaits est fini.*

Démonstration. Soit Λ un réseau G-parfait de V et soit Λ' le sous-réseau de Λ engendré par les vecteurs de $S(\Lambda)$. L'indice $m = [\Lambda : \Lambda']$ ne prend qu'un nombre fini de valeurs (prop. 3.10, (i)), et la double inclusion $\Lambda' \subset \Lambda \subset \frac{1}{m}\Lambda'$ montre que, pour Λ' fixé, il n'y a qu'un nombre fini de réseaux Λ possibles. On est donc ramené au cas où Λ est engendré par ses vecteurs minimaux.

Comme Λ est engendré par des vecteurs minimaux, son discriminant est borné. Il existe donc (Hermite) une borne B_n telle que Λ possède une base $\mathcal{B}$ constituée de vecteurs de norme $\leq B_n$. En raisonnant comme dans 3.10 (ii), on montre qu'il existe une constante C_n majorant les composantes dans une telle base des vecteurs de $S(\Lambda)$. Le nombre de vecteurs de $S(\Lambda)$ (le *kissing number*) étant majoré par une fonction qui ne dépend que de n, la proposition 2.6 permet de conclure.

3.13 REMARQUE. La démonstration précédente s'applique en particulier dans le cas des réseaux parfaits au sens ordinaire. Il serait intéressant de trouver un "G-algorithme de Voronoï" produisant un graphe connexe pour l'ensemble

des faces associées aux G-réseaux G-parfaits (mais il faut –remarque de Sigrist–considérer les familles de réseaux *appartenant à une classe donnée de représentations intégrales* (i.e. sur $\mathbb{Z}$) de G). Par ailleurs, il est vraisemblable que des énoncés analogues (algorithme de Voronoï compris) s'appliquent aux réseaux "dual-extrêmes" au sens de [4] stables sous l'action d'un sous-groupe fini de $\mathrm{O}(V)$.

4. Groupes cycliques irréductibles. On conserve dans ce § les notations du § 3, mais on suppose maintenant que G est cyclique et que V provient d'une représentation $\mathbb{Q}$-irréductible et fidèle de G. On note q l'ordre de G, σ un générateur de G, et l'on suppose que q est ≥ 3 (si $q = 1$ ou 2, V est de dimension 1, et l'unique réseau à similitude près est A_1, semblable à $\mathbb{Z}$). Si l'ordre de G est congru à 2 mod 4, G est produit direct de $\{\pm\mathrm{Id}\}$ par un groupe G' d'ordre moitié. Comme les notions de G- et de G'-réseaux coïncident, on peut supposer, ce que nous ferons dans la suite, que q est impair ou divisible par 4.

Soit ζ une racine de l'unité d'odre q. Un G-réseau Λ de V possède une structure de module (de rang 1, sans torsion) sur l'anneau des entiers $\mathbb{Z}[\zeta]$ du corps cyclotomique $K_q = \mathbb{Q}(\zeta)$, définie par la règle $\zeta x = \sigma x$ (il y a $\varphi(q)$ structures de module possibles, dépendant du choix de ζ). On note K'_q le sous-corps réel maximal de K_q. Lorsque q est une puissance de nombre premier et est ≤ 19, ce qui est le cas dans les applications que nous avons en vue, l'anneau $\mathbb{Z}[\zeta]$ est principal et ses unités sont de la forme $\zeta^i\eta$ où η est une unité de K'_q.

Comme G est irréductible, les vecteurs minimaux de Λ engendrent V. Soit Λ' un sous-réseau de Λ engendré par des vecteurs de $S(\Lambda)$. On a vu précédemment (prop. 3.10) comment majorer l'indice $[\Lambda : \Lambda']$; en particulier, on a $[\Lambda : \Lambda'] = 1$ pour $n \leq 3$, et même pour $n = 4$ si Λ n'est pas critique, $[\Lambda : \Lambda'] \leq 2$ pour $n \leq 5$ et $[\Lambda : \Lambda'] \leq 4$ pour $n = 6$. Lorsque l'on suppose en outre que Λ' est lui aussi un G-réseau, on a $[\Lambda : \Lambda'] = N_{K_q/\mathbb{Q}}(\mathfrak{a})$ où $\mathfrak{a}$ désigne le $\mathbb{Z}[\zeta]$-indice (au sens de [13], ch. III, § 1) de Λ' dans Λ. Le fait que $[\Lambda : \Lambda']$ soit une norme permet de limiter les valeurs possibles de cet indice. En particulier, on a :

4.1 PROPOSITION. *Soit Λ un G-réseau, et soit Λ' un sous-G-réseau de Λ engendré par des vecteurs minimaux de Λ. Alors :*

(i) *Si Λ' est strictement contenu dans Λ, $[\Lambda : \Lambda']$ est au moins égal au plus petit diviseur premier de q ;*
(ii) *Si q est une puissance d'un nombre premier p, $[\Lambda : \Lambda']$ est une puissance de p ou est $\geq q + 1$;*
(iii) *Si $q = 5$ ou 7, on a $\Lambda' = \Lambda$;*
(iv) *Si $q = 9$, $[\Lambda : \Lambda'] = 1$ ou 3.*

Démonstration. La norme minimale d'un idéal de K_q est évidemment une puissance de nombre premier. La loi de décomposition des nombres premiers dans les corps cyclotomiques montre que les idéaux premiers non ramifiés ont une norme $\equiv 1 \mod q$, d'où (i) et (ii). Les assertions (iii) et (iv) sont des conséquences immédiates de (i) et (ii) et des majorations d'indices rappelées au début de ce §.

La dimension de V est $n = \varphi(q)$. Comme q est ≥ 3, n est pair. On pose $m = n/2$. L'espace V contient m sous-espaces $\mathbb{R}$-irréductibles, qui sont des plans deux à deux non isomorphes que nous notons $P_1, P_2, ..., P_m$, P_i étant caractérisé par le fait que σ induit sur P_i une rotation d'angle $\pm 2i\pi/q$ (l'angle n'est défini qu'au signe près) ; l'indexation des P_i dépend du choix de σ.

Chaque plan P_i est un $\mathbb{C}$-espace vectoriel de dimension 1, et les calculs de dimension effectués au § 3 montrent tout de suite l'égalité $\dim_{\mathbb{R}} \mathcal{S}_G = m$. En utilisant la prop. 2.5, on en déduit une minoration du nombre de vecteurs minimaux des réseaux G-parfaits :

4.2 LEMME. *Pour tout réseau G-parfait, on a $s \geq q\varphi(q)/2$ si q est impair, et $s \geq q\varphi(q)/4$ si q est pair.*

Lorsque q est égal à 3 ou à 4, on est dans le cas évoqué en 3.7 dans lequel V est $\mathbb{R}$-irréductible. Sinon, m est ≥ 2, et les classes de similitude de G-réseaux ne sont pas isolées. C'est le cas dès la dimension 4, pour laquelle les valeurs possibles pour q sont 5, 8 et 12. On a vu (cf. prop. 2.4) qu'un réseau G-parfait possède au moins $m = 2$ orbites de vecteurs minimaux dans le cas de la dimension 4. Cette condition caractérise en fait les réseaux parfaits, et même extrêmes, comme dans le cas du théorème 3.8 de Korkine et Zolotareff :

4.3 THÉORÈME. *Soit V un $\mathbb{R}$-espace vectoriel de dimension 4, soit G un sous-groupe cyclique irréductible de $O(V)$, et soit Λ un G-réseau possédant au moins deux orbites de vecteurs minimaux. Alors, Λ est G-extrême, et :*

(i) *Si G est d'ordre 5, Λ est semblable à A_4 ;*
(ii) *Si G est d'ordre 8 ou 12, Λ est semblable à D_4 .*

4.4 COROLLAIRE (SCHOOF ET WASHINGTON, [14]). *Si Λ est un réseau de dimension 4 muni d'un automorphisme d'ordre 5, on a $\gamma_4(\Lambda)^4 \leq \frac{16}{5}$ ($< \gamma_4^4 = 4$).*

En effet, $\gamma_4(A_5)^4 = \frac{16}{5}$.

Démonstration de 4.4. D'après le lemme 4.2, pour $q = 5$ (resp. 8, resp. 12), $s(\Lambda)$ est ≥ 10 (resp. 8, resp. 12). Le théorème 3.8 montre tout de suite que pour q=5 et q=12, le réseau Λ est extrême. Comme 5 ne divise pas $s(D_4)$, Λ est semblable à A_4 lorsque q=5, et, pour q=12, l'inégalité $s(\Lambda) \geq 12$ montre

que Λ est semblable à D_4. Comme on sait qu'il existe des G-réseaux admettant ces groupes comme groupes d'automorphismes (cf. § 2, après le th. 3.8)), il est clair que, réciproquement, ces réseaux conviennent.

Il reste à traiter le cas $q = 8$; c'est une conséquence immédiate du lemme suivant :

4.5 LEMME. *Un G-réseau non critique a une seule orbite de couples $\{\pm x\}$ de vecteurs minimaux.*

En effet, tout vecteur minimal constitue alors une base de Λ sur $\mathbb{Z}_{\mathbb{Q}(\zeta)}$, de sorte que si x et y sont deux vecteurs minimaux de Λ, on a

$$(1) \qquad y = \lambda x, \ \lambda \text{ unité de } \mathbb{Q}(\zeta),$$

où, quitte à échanger les rôles de x et y et à remplacer y par un de ses conjugués, on peut supposer $\lambda = \epsilon^k$, ϵ désignant l'unité fondamentale $1 + \zeta + \zeta^{-1}$ de $\mathbb{Q}(\zeta)$, et k un entier ≥ 0. Posant alors $x_k = \epsilon^k x$, où x est minimal, on voit immédiatement les relations

$$(2) \quad \|x_{k+1}\|^2 = 3\|x_k\|^2 + 4x_k.\zeta x_k \quad \text{et} \quad x_{k+1}.\zeta x_{k+1} = 2\|x_k\|^2 + 3x_k.\zeta x_k \ .$$

On en tire d'abord, puisque $x_0 = x$ est minimal, que $x_0.\zeta x_0$ est $\geq -\frac{1}{2}$, l'égalité équivalant à $\|x_1\| = 1$, mais aussi à $\|x + \zeta x\| = 1$, impossible d'après (1), puisque $1 + \zeta$ est de norme 2 : x_1 n'est donc pas minimal. Les relations (2) montrent aussi par récurrence que, pour $k \geq 1$, on a $x_k.\zeta x_k \geq \frac{1}{2}$ et donc $\|x_{k+1}\|^2 \geq 5$. Ainsi, les vecteurs minimaux de Λ se répartissent sur une seule orbite, celle de $x = x_0$, **c.q.f.d.**

Par des arguments de nature combinatoire analogues à ceux qui ont permis de démontrer le théorème précédent dans le cas $q = 8$, on peut trouver tous les réseaux G-parfaits pour $n = 6$, ce qui impose $q = 7$ ou 9. Ici encore, la minoration de s donnée par 3.3 suffit :

4.6 THÉORÈME. *Soit V un espace vectoriel euclidien de dimension 6, soit G un sous-groupe cyclique irréductible de $O(V)$, d'ordre $q \not\equiv 2 \mod 4$, et soit Λ un G-réseau contenant au moins 3 orbites de couples $\pm x$ de vecteurs minimaux. Alors, Λ est extrême, et l'on est dans l'un des deux cas suivants :*

(i) *$q = 7$, et Λ est semblable à A_6 ou à P_6 ;*
(ii) *$q = 9$, et Λ est semblable à E_6 ou à E_6^*.*

4.7 COROLLAIRE. *Un réseau de dimension 6 invariant sous l'action d'un sous-groupe cyclique d'ordre 7 de $O(V)$ vérifie l'inégalité*

$$\gamma_6(\Lambda)^6 \leq \frac{2^{12}}{7^3} < 11,942 \ (< \gamma_6^6 = \frac{64}{3} = 21,333...)$$

En effet, on a $\gamma_6(A_6)^6 = \frac{2^6}{7} < \gamma_6(P_6) = \frac{2^{12}}{7^3}$.

Démonstration de 4.6. Soit Λ un réseau vérifiant les hypothèses du théorème. En combinant les prop. 3.11 et 4.1, on voit tout de suite que le réseau Λ' engendré par les vecteurs minimaux de Λ est égal à Λ lorsque $q = 7$, et est d'indice 1 ou 3 lorsque $q = 9$. Pour faire la démonstration, on supposera d'abord que Λ est engendré par ses vecteurs minimaux, ce qui est loisible puisque Λ' satisfait aussi aux hypothèses du théorème.

Dans les deux cas $q = 7$ et $q = 9$, le corps $\mathbb{Q}(\zeta)$ est cyclique de degré 6 et possède deux unités fondamentales e et f, que l'on peut prendre égales à $\zeta+\zeta^{-1}$ et $\zeta^2+\zeta^{-2}$ respectivement. Ce sont deux éléments conjugués du sous-corps réel maximal K'_q de $\mathbb{Q}(\zeta)$; on note g le conjuqué autre que f de e. On a $g = \zeta^4 + \zeta^{-4}$ $(= \zeta^3 + \zeta^{-3}$ si $q = 7)$. Les unités e, f, g vérifient les relations $efg = 1$ et $e+f+g = -1$ lorsque $q = 7$, et $efg = -1$ et $e+f+g = 0$ lorsque $q = 9$.

Dans l'énoncé du lemme ci-dessous, lorsque q=9, on note π l'élément $\zeta-\zeta^{-1}$ de $\mathbb{Z}[\zeta]$; c'est un générateur de l'unique idéal premier au-dessus de 3 de $\mathbb{Z}[\zeta]$.

4.8 LEMME. *Il existe trois vecteurs minimaux x, y, z de Λ appartenant à des orbites distinctes de $\pm G$ et des unités η et η' de K'_q telles l'une des conditions suivantes soit vérifiée :*

(i) $y = \eta x$ *et* $z = \eta' x$;
(ii) $y = \eta x$ *et* $z = \eta'\pi x$;
(iii) $y = \eta\pi x$ *et* $z = \eta'\pi x$;

Démonstration. On a vu que Λ possède au moins trois orbites de vecteurs minimaux. On prend pour x, y, z des représentants de ces orbites. On a vu également que Λ est un module libre sur $\mathbb{Z}[\zeta]$. Soit a une $\mathbb{Z}[\zeta]$-base de Λ. Il existe des éléments λ, μ et ν de $\mathbb{Z}[\zeta]$ tels que $x = \lambda a$, $y = \mu a$ et $z = \nu a$. Quitte à permuter x, y, z, on peut supposer λ, μ, ν rangés par normes croissantes. La proposition 4.1 montre que ces éléments sont de la forme ε ou $\varepsilon\pi$, ε désignant une unité de K_q. Vu les propriétés de K_q rappelées au début du §, ces unités sont de la forme $\zeta^i\eta$ où η est une unité de K'_q. Il est alors clair que l'on est dans le cas (i) si π divise 0 ou 3 des éléments λ, μ, ν, dans le cas (ii) si π en divise 2, et dans le cas 3 si π en divise 1.

Nous allons maintenant étudier de plus près ce que peuvent être η et η'.

4.9 LEMME. *Soient x et y deux vecteurs minimaux indépendants de Λ et soit η une unité de K'_q telle que $y = \eta x$. Alors, $\pm\eta$ ou $\pm\eta^{-1} \in \{e, f, g\}$.*

Démonstration. Écrivons $\eta = u + ve + wf$, u, v, $w \in \mathbb{Z}$ avec $(v, w) \neq (0,0)$. On sait (cf. § 3) que tous les déterminants formés par 2 composantes sur la base ζ^i, $-2 \leq i \leq 3$ de 2 vecteurs $\zeta^j y$, $\zeta^k y$ sont ≤ 4. On vérifie que l'on peut faire apparaître les valeurs w^2, v^2, et $u^2 - v^2$ de ces déterminants. Par exemple, si $q = 7$, il suffit d'utiliser successivement $(j,k) = (0,1)$ avec $i \in \{-2,3\}$, $(1,3)$ avec $i \in \{1,2\}$ et $(3,-3)$ avec $i \in \{1,3\}$. On en déduit que les valeurs absolues de u, v, w sont ≤ 2. Les triplets (u', v', w') obtenus à partir d'un triplet (u, v, w) en faisant opérer $\mathrm{Gal}(K'_q/\mathbb{Q})$ doivent vérifier les mêmes propriétés, ainsi que ceux obtenus par les transformations $\eta \mapsto \eta^{-1}$ (car $x = \eta^{-1} y$) et $\eta \mapsto -\eta$. Les triplets admissibles se répartissent donc en orbites de 12 éléments sous l'action d'un groupe abélien de type $(6,2)$. On vérifie alors facilement que ces contraintes limitent les valeurs de η à deux orbites, à savoir celles de e et de $e^2 f$, pour $q = 7$ comme pour $q = 9$.

Pour simplifier l'écriture des calculs qui vont suivre, nous normalisons Λ par la condition $\|\Lambda\| = 1$. Nous allons calculer les normes de certains vecteurs de Λ en fonction des produits scalaires $\alpha = x.\zeta x$, $\beta = x.\zeta^2 x$ et $\gamma = x.\zeta^4 x$ ($\gamma = x.\zeta^3 x$ si $q = 7$). La somme $\alpha + \beta + \gamma$ est égale à $-\frac{1}{2}$ si $q = 7$ et à 0 si $q = 9$; en outre, $x.\zeta^3 x = -\frac{1}{2}$ si $q = 9$: cela se voit simplement en utilisant l'égalité $\|x\|^2 = 1$. En écrivant les inégalités $\|z\| \geq 1$ pour $z = x \pm \zeta^i x$, on obtient $-\frac{1}{2} \leq \alpha, \beta, \gamma \leq \frac{1}{2}$, d'où, pour $q = 7$ (resp. 9), $\alpha + \beta \leq 0$ (resp. $-\frac{1}{2} \leq \alpha + \beta \leq \frac{1}{2}$).

Occupons-nous maintenant du cas $q = 7$. En calculant $\|efx\|$ par l'égalité $ef = -1 - f$, on obtient $\alpha - \beta \leq \frac{1}{2}$. On trouve enfin $\|e^2 fx\|^2 = \|(1 - e + f)x\|^2 = 6 - 6\alpha + 8\beta = 6 + 2\beta - 6(\alpha - \beta) \geq 3 - 2\beta \geq 2$, inégalité qui prouve que $e^2 fx$ ne peut pas être un vecteur minimal.

Lorsque $q = 9$, on obtient par un calcul analogue $\|efx\|^2 = \|(1 - e)x\|^2 = 3 - 4\alpha + 2\beta \geq 1$, d'où $2\alpha - \beta \leq 1$, puis $\|e^2 fx\|^2 = \|(2 - e + f)x\|^2 = 10 - 14\alpha + 8\beta = 10 + \beta - 7(2\alpha - \beta) \geq 3 + \beta > 2$, ce qui achève la démonstration du lemme 4.9.

4.10 LEMME. *Si Λ vérifie l'hypothèse (i) du lemme 4.8, on peut choisir x, y, z de façon que $(\eta, \eta') = (ef, f)$ ou (ef, e).*

Démonstration. Écrivons $\eta = \pm e^a f^b$ et $\eta' = \pm e^c f^d$. En examinant l'effet des 6 permutations de $\{x, y, z\}$ sur le quadruplet (a, b, c, d), on voit tout de suite que l'on peut se limiter aux cas où l'on a $a \geq c \geq 0$ et $d \geq 0$ lorsque $c = 0$. Il suffit alors de considérer les couples $(\eta, \eta') = (ef, e)$, (ef, f), et (e, f). Or, on a $\|ex\|^2 = 2 + \beta$ et $\|fx\|^2 = 2 + \gamma$. Donc, si ex et fx sont minimaux, on a $\beta = \gamma = -\frac{1}{2}$. Cela entraîne l'égalité absurde $\alpha = 1$ lorsque $q = 9$ et, pour $q = 7$, l'égalité $\alpha = \frac{1}{2}$ qui entraîne à son tour l'égalité absurde $\|efx\| = 0$.

Fin de la démonstration de 4.6, (i). Il résulte du lemme 4.10 qu'un réseau

vérifiant les hypothèses du th. 4.6, (i) est semblable à un réseau possédant 3 orbites de vecteurs minimaux de la forme x, efx, ex ou x, efx, fx. Ces données fixent le système α, β, γ une fois que l'on a imposé $\|x\|$. Donc, à similitude près, au plus 2 réseaux conviennent. Or, nous connaissons deux réseaux acceptables, à savoir A_6 et P_6. Ce sont donc certainement ces 2 réseaux, **c.q.f.d.**

(Pour $\|x\| = 1$, les valeurs respectives du triplet (α, β, γ) sont $(0, -\frac{1}{2}, \frac{1}{2})$ et $(\frac{1}{4}, -\frac{1}{4}, -\frac{1}{2})$. La forme quadratique $t \mapsto 2\|t\|^2$ étant entière pour le premier réseau mais non pour le second, le premier réseau est semblable à A_6 et le second à P_6.)

Nous devons maintenant examiner les autres possibilités prévues par le lemme 4.8. Nous supposons donc que $q = 9$. Toutefois, vu l'absence d'application comparable au cor. 4.7, nous n'écrirons pas tous les détails.

4.11 LEMME. *Si Λ possède un couple de vecteurs minimaux $(x, \eta\pi x)$, alors η est l'une des unités ± 1, $\pm e$, $\pm(1-e)$, pour lesquelles on a respectivement $\beta = \frac{1}{2}$, $\gamma = \frac{1}{2}$, $\alpha = \frac{1}{2}$.*

Démonstration. On écrit $\eta = u + ve + wf$. Par des considérations analogues à celles qui ont été utilisées dans la démonstration de 4.9, on montre les majorations $|u| \leq 3$, $|v| \leq 2$, $|w| \leq 1$, et, en utilisant la conjugaison dans K_9', on limite les triplets (u, v, w) à 4 orbites de 3 éléments (au signe près). En écrivant les inégalités $\|t\| \geq 1$ pour quelques vecteurs bien choisis, on trouve finalement qu'une seule orbite convient, en l'occurence $\{\pm 1, \pm e, \pm(1-e)\}$; la fin du lemme est évidente.

Fin de la démonstration de 3.6, (ii). On remarque d'abord que le cas (iii) du lemme 4.8 ne se produit pas, car 2 des α, β, γ ne peuvent prendre la valeur $\frac{1}{2}$ à cause de la relation $\alpha + \beta + \gamma = 0$. On essaie alors les diverses possibilités provenant du cas (ii) de ce lemme, et on constate que, compte tenu des inégalités $|\alpha|$, $|\beta|$, $|\gamma| \leq \frac{1}{2}$ et $\|x - \zeta^i x - \zeta^{-i} x\| \geq 1$, les orbites de vecteurs minimaux doivent être de l'une des formes

$$(x, efx, (1-e)\pi x),\ (x, ex, e\pi x),\ (x, fx, (1-e)\pi x).$$

Dans les 3 cas, on retrouve le réseau rencontré dans le lemme 4.10, réseau qui possède en fait 4 orbites de vecteurs minimaux.

On obtient donc un résultat analogue à celui que nous avons démontré dans le cas $q = 7$: il y a au plus 2 classes de similitude de G-réseaux engendrés par leurs vecteurs minimaux. Or, on connaît *a priori* deux réseaux de ce type, à savoir E_6 et son dual E_6^*. Ce sont donc ces deux réseaux que nous avons trouvés. Comme le premier est critique, et que le quotient des discriminants de E_6^* et E_6 (ramenés à la norme 1) est < 2, il n'existe pas pour $q = 9$ de

G-réseau qui ne soit pas engendré par ses vecteurs minimaux. Cela achève la démonstration du th. 4.6.

4.12 REMARQUE. Pour n=8, les groupes cycliques irréductibles sont d'ordre 15 (ou 30), 16, 20, 24. En examinant la table des caractères donnée par l'Atlas ([8]) pour les groupes liés à $\mathrm{O}_8^+(2)$, on voit que E_8 fournit des représentations $\mathbb{Q}$-irréductibles pour les groupes cycliques d'ordre 15, 20 et 24, ce qui résulte aussi du travail d'Eva Bayer ([3], exemple 5.8). En revanche, E_8 ne possède pas d'automorphisme d'ordre 16 ; en conséquence, la classification des G-réseaux possédant un tel automorphisme permettrait d'améliorer la G-constante d'Hermite correspondante.

Une remarque analogue peut être faite en dimension 10 avec un groupe cyclique d'ordre 11, le réseau conjecturalement critique ne possédant pas d'automorphisme d'ordre 11 (les vecteurs minimaux de son dual engendrent un réseau plan hexagonal, cf. [4], rem. 4.8).

Nous reviendrons sur les réseaux de dimension 8 dans un article ultérieur. (Voir aussi l'appendice (§ 6) ci-dessous.)

5. Autres groupes cycliques. Dans ce §, pour lequel nous conservons les notations des § précédents, nous étudions quelques exemples dans lesquels le groupe G est un sous-groupe cyclique de $O(V)$ dont la représentation associée n'est pas irréductible, et classons complètement les réseaux G-parfaits lorsque G est cyclique d'ordre 3 ou 5 et V de dimension égale à l'ordre de G . Toutefois, comme les réseaux critiques font partie des listes que nous dressons, nous ne reproduirons pas tous les détails des démonstrations.

Soit ℓ un nombre premier impair, et supposons que l'on ait $\operatorname{Card} G = \dim V = \ell$. Une représentation rationnelle fidèle de G est unique à isomorphisme près, et le polynôme caractéristique d'un générateur σ de G est alors $X^\ell - 1$. Notons toujours ζ une racine de l'unité d'ordre ℓ, et soit $T \in \mathbb{Z}[G]$ la "trace" $\sum_{i=0}^{\ell-1} \sigma^i$. L'algèbre $\mathbb{Q}[G]$ s'identifie au produit $\mathbb{Q} \times \mathbb{Q}(\zeta)$, le premier facteur étant associé à l'idempotent $e = \frac{T}{\ell}$ et le second à l'idempotent orthogonal $1 - e$. Plus précisemment, on identifie l'élément

$$\sum_{i \bmod \ell} a_i \sigma^i \text{ de } \mathbb{Q}[G] \text{ au couple } \Big(\sum_{i \bmod \ell} a_i, \sum_{i \bmod \ell} a_i \zeta^i \Big) \text{ de } \mathbb{Q} \times \mathbb{Q}(\zeta).$$

L'espace V est somme directe de l'image de T, qui est une droite stable notée D, et du noyau de T, qui est l'hyperplan H orthogonal à cette droite.

L'anneau $\mathbb{Z}[G]$ est contenu dans l'unique ordre maximal $\mathfrak{M}$ de $\mathbb{Q}[G]$, engendré par $\mathbb{Z}[G]$ et e. Le quotient $\mathfrak{M}/\mathbb{Z}[G]$ est un groupe cyclique d'ordre ℓ. Comme Λ est de rang 1, l'une des deux conditions suivantes est réalisée : ou

bien Λ possède une structure de $\mathfrak{M}$-module, ou bien il est projectif sur $\mathbb{Z}[G]$, et donc libre pour $\ell \leq 19$.

5.1 PROPOSITION. *Si Λ est un $\mathfrak{M}$-module, ses vecteurs minimaux sont dans l'image ou le noyau de e.*

Démonstration. Soit $x \in S(\Lambda)$. Si $\sigma x = x$, on a $ex = x$. Sinon, on a $\|x \pm \sigma x\| \geq 1$, d'où $|x.\sigma x| \leq \frac{1}{2}$, ce qui entraîne $\|\sum \sigma^i x\|^2 \leq \frac{\ell(\ell+1)}{2}$, d'où $\|ex\|^2 \leq \frac{(\ell+1)}{2\ell} < 1$. (On a normalisé Λ par $\|\Lambda\| = 1$.) Cette somme est donc nulle, **c.q.f.d.**

La représentation de G définie par V est somme de $\frac{\ell+1}{2}$ représentations $\mathbb{R}$-irréductibles (une de dimension 1, la droite D, et $\frac{\ell-1}{2}$ de dimension 2). Il en résulte (cf. 2.4) que, si Λ est G-parfait, $S(\Lambda)$ contient au moins $\frac{\ell+1}{2}$ orbites de couples $\{\pm x\}$ de vecteurs minimaux, formées de ℓ vecteurs sauf au plus une qui peut être réduite à un élément. Nous allons voir que pour $\ell = 3$ ou 5, cette condition est suffisante. Le cas $\ell = 3$ est facile :

5.2 THÉORÈME. *Si G est d'ordre 3 et opère fidèlement sur V, les réseaux Λ possédant deux orbites de vecteurs minimaux sont G-extrêmes, et semblables à $A_1 \perp A_2$, A_3 ou A_3^*.*

Démonstration. Le cas d'un réseau réductible est une conséquence immédiate du th. 3.6. Par ailleurs, si les orbites de vecteurs minimaux ont 3 éléments, le th. 3.8 montre que Λ est semblable à A_3. Il reste à considérer le cas où $S(\Lambda)$ contient un vecteur x fixe par G et une orbite Gy non contenue dans H. Alors, l'orbite de y engendre V, donc aussi Λ (prop. 3.11). Écrivons $x = ay + b\sigma y + c\sigma^2 y$, avec $a, b, c \in \mathbb{Z}$. On a $a = b = c$ (car $\sigma x = x$), puis $a = \pm 1$ (car x est minimal). Les produits scalaires $y.\sigma^{\pm 1} y$ sont égaux, et valent $-\frac{1}{3}$, comme on le voit en calculant $\|y\|$. On reconnaît alors le réseau A_3^*. On vérifie sans peine l'indépendance de φ_x et de φ_y, ce qui prouve que le réseau est G-parfait. Comme les réseaux A_n^* sont eutactiques ([9], 12.7), A_3^* est G-extrême. Les deux autres le sont également (th. 3.6 pour $A_1 \perp A_2$ et th. 3.8 pour A_3), **c.q.f.d.**

Passons maintenant au cas où $\ell = 5$.

5.3 THÉORÈME. *Si G est d'ordre 5 et opère fidèlement sur V, et si $S(\Lambda)$ contient 3 orbites de vecteurs minimaux, Λ est G-extrême, et semblable à l'un des 5 réseaux suivants : D_5, A_5^3, A_5, Λ_5 ou $A_1 \perp A_4$, où Λ_5, normé par*

$\|\Lambda_5\|^2 = 10$, *a pour déterminant 19602 et est défini par la matrice de Gram*

$$\begin{pmatrix} 10 & -5 & 1 & 1 & -5 \\ -5 & 10 & -5 & 1 & 1 \\ 1 & -5 & 10 & -5 & 1 \\ 1 & 1 & -5 & 10 & -5 \\ -5 & 1 & 1 & -5 & 10 \end{pmatrix}.$$

Démonstration. Rappelons (prop. 3.11) que le sous-réseau de Λ engendré par l'orbite d'un vecteur minimal qui n'est ni dans D ni dans H est d'indice 1 ou 2, et que sa projection sur H engendre la projection de Λ sur H (cf. prop. 4.1).

5.4 LEMME. *Soient x et y deux vecteurs minimaux d'un G-réseau Λ engendrant des orbites distinctes, avec $x \notin H$. Alors, quitte à remplacer y par l'un des vecteurs $\pm\sigma^i y$, on peut supposer que l'une des relations suivantes est vérifiée :*

(i) *Gx et Gy engendrent des réseaux de même indice dans Λ, $y = (\sigma + \sigma^{-1} - 1)x$ ou $y = (\sigma^2 + \sigma^{-2} - 1)x$ (on passe d'un cas à l'autre en échangeant x et y) ;*

(ii) *Gy engendre un réseau d'indice 2 et Gx un réseau d'indice 1, $y = (1 + \sigma^i)x$, avec $i = 1$ ou 2 (à l'échange près de x et de y) ;*

(iii) *$y \in H$, $y = (\sigma - 1)x$, $(\sigma^2 - 1)x$, $(1 - \sigma + \sigma^{-1} - \sigma^2)x$ ou $(1 - \sigma - \sigma^{-1} + \sigma^2)x$.*

Démonstration (indications). (i) En utilisant l'isomorphisme de $\mathbb{Z}[G]/T\mathbb{Z}$ sur $\mathbb{Z}[\zeta]$, on montre que les unités de $\mathbb{Z}[G]$ sont de la forme $\pm\sigma^i(\sigma + \sigma^{-1} - 1)^m$, $m \in \mathbb{Z}$. Un argument d'indice déjà utilisé montre que l'on doit choisir m pour que les coefficients de y sur la base $\{\sigma^i x\}$ soient bornés par 2, ce qui impose $m = \pm 1$. Pour (ii), on montre de même que les éléments de $\mathbb{Z}[G]$ de norme ± 2 sont de la forme $\pm\sigma^i(\sigma + \sigma^{-1})(\sigma + \sigma^{-1} - 1)^m$, et on limite les valeurs de m à 0, -1 par un argument d'indice. Pour (iii), on écrit $y = \lambda x$, avec λ dans l'idéal d'augmentation de $\mathbb{Z}[G]$. Un argument d'indice montre encore que les coefficients de λ sont bornés par 1, ce qui permet de conclure facilement.

Soit maintenant Λ un G-réseau avec 3 orbites de vecteurs minimaux. Comme un réseau de dimension 4 a au plus 12 vecteurs minimaux, une au moins de ces orbites n'est pas contenue dans H. On note x, y, z des vecteurs engendrant chacune de ces orbites, en supposant que x n'est pas dans H, et l'on discute selon le nombre d'orbites contenues dans H. On pose $\alpha = x.\sigma x$ et $\beta = x.\sigma^2 x$.

Si y et z sont dans H, on utilise 5.4, (iii). On trouve *a priori* pour (α, β) ou (β, α) l'une des possibilités $(\frac{1}{2}, \frac{1}{2})$, $(\frac{1}{2}, 0)$ et $(\frac{1}{2}, \frac{2}{3})$. La dernière est clairement impossible, et les deux premières correspondent pour le réseau engendré par les

orbites de x, y, z à A_5 et D_5 respectivement. L'indice 2 est alors impossible, les discriminants de A_5 et de D_5 étant trop petits. On a donc $\Lambda \sim A_5$ ou $\Lambda \sim D_5$.

Si z est dans H mais non y, on utilise 5.4, (i) et (iii) si Gx et Gy engendrent le même réseau, et 5.4, (ii) et (iii) sinon. En échangeant éventuellement α et β, on se ramène à $\alpha = -\frac{1}{2}$ et $\beta \in \{0, \frac{1}{2}, \frac{1}{3}\}$. L'inégalité $\|x\| \geq 1$ ne laisse plus que la possibilité $\alpha = -\frac{1}{2}$, $\beta = 0$, qui correspond à D_5, Gx et Gy engendrant toutes les deux Λ.

(Compte tenu des échanges de α et de β, D_5 est apparu quatre fois, ce qui correspond à l'existence pour ce réseau de 4 orbites de vecteurs minimaux, dont 2 dans H.)

Enfin, si Λ ne possède aucune orbite dans H, on peut, compte tenu du lemme 5.4, supposer que Gx engendre Λ et que Gz engendre un sous-réseau d'indice 2, Gy étant d'indice 1 ou 2 dans Λ. Un très petit nombre d'essais permet de voir que le réseau cherché peut être défini par $\alpha = -\frac{1}{2}$ et $\beta = \frac{1}{4}$. L'unique réseau que nous avons trouvé ne peut être alors que le réseau A_5^3, ce qui qui n'est pas difficile à vérifier directement.

Ainsi, lorsque le nombre de vecteurs minimaux du G-réseau Λ est un multiple de 5, Λ est semblable à l'un des 3 réseaux extrêmes qui existent en dimension 5.

Nous étudions maintenant le cas où $s(\Lambda)$ est congru à 1 modulo 5. Il y a alors un vecteur minimal stable par G, que nous notons x, et deux vecteurs minimaux y et z ayant des orbites à 5 éléments. Si y et z sont dans H, les vecteurs minimaux engendrent un réseau semblable à $A_1 \perp A_4$, qui est égal à Λ tout entier vu son discriminant, et qui est G-extrême d'après le th. 3.6.

Sinon, on suppose que y n'est pas dans H. L'indice $Q = [\Lambda : Gy]$ vaut 1 ou 2, et l'on peut supposer que l'indice $[\Lambda : Gz]$ est $\geq Q$ si z n'est pas dans H. On pose maintenant $\alpha = y.\sigma y$ et $\beta = y.\sigma^2 y$. Du fait que x est minimal, on a $\alpha + \beta = \frac{Q^2-5}{10}$. Nous avons alors examiné les trois possibilités $z \in H$, $z \notin H$ et $[\Lambda : Gz] = Q$, et enfin $z \notin H$, $Q = 1$ et $[\Lambda : Gz] = 2$, et avons éliminé les réseaux de discriminant trop petit (ce qui signifie que x, y, z ne sont en fait pas minimaux). Seule a subsisté la possibilité (α, β) (ou (β, α)) $= (-\frac{1}{2}, \frac{1}{10})$, qui donne la matrice de Gram annoncée. Nous avons alors vérifié que x, y, z sont effectivement des vecteurs minimaux, et contrôlé que l'équation

$$\mathrm{Tr} = a\varphi_x + b\varphi_y + c\varphi_z$$

possède pour unique solution le triplet $(\frac{15}{33}, \frac{50}{33}, \frac{100}{33})$.

L'unicité confirme que Λ_5 est G-parfait, et Λ_5 est même G-extrême, puisque a, b, c sont > 0, **c.q.f.d.**.

5.5 REMARQUE. L'étude du cas $\ell = 7$ semble possible avec des calculs limités. Toutefois, le réseau critique E_7 possédant un automorphisme d'ordre 7, on ne

peut pas espérer améliorer la majoration classique de $\gamma_7(\Lambda)$ sur les G-réseaux Λ. (6 des 33 réseaux parfaits figurant dans [7], à savoir $p_7^1 \sim E_7$, $p_7^2 \sim E_7^*$, $p_7^4 \sim D_7$, p_7^{15}, p_7^{30} et $p_7^{33} \sim A_7$, possèdent un automorphisme d'ordre 7.)

De même, l'étude des automorphismes de polynôme minimal X^2+X+1 ou X^2+1 en dimensions n =4, 6 ou 8 n'améliore pas $\gamma_n(\Lambda)$, les réseaux critiques D_4, E_6 et E_8 possédant des automorphismes de ce type.

6. Compléments (mai 1990). Nous décrivons brièvement dans ce § quelques résultats concernant le degré 8 qui ont été obtenus postérieurement à l'exposé fait aux journées arithmétiques.

Nous avons déterminé les réseaux G-parfaits pour les groupes cycliques $\mathbb{Q}$-irréductibles d'ordres 15,16 et 24, ce qui couvre trois des quatre possibilités en dimension 8. (Le cas des groupes d'ordre 20 reste en suspens ; il est probable (mais non démontré) que le seul réseau G-parfait est dans ce cas E_8.) Ces réseaux sont engendrés en tant que $\mathbb{Z}[G]$-modules par un vecteur minimal convenable x et sont déterminés à isométrie près par les 4 produits scalaires $\alpha_i(x) = x.\sigma^i(x)$, $i = 0, 1, 2, 3$. Pour les décrire, nous les normalisons de façon que que $\alpha_0(x) = \|x\|^2$ soit le plus petit entier qui rende le réseau entier. Pour $q = 15$ (resp. 16, resp. 24), on trouve à similitude près 1 (resp. 3, resp. 2) réseaux G-parfaits, qui sont tous G-extrêmes, donc en particulier eutactiques, mais seuls D_8 (trouvé pour $q = 16$) et E_8 (trouvé pour $q = 15$ et $q = 24$) sont parfaits au sens usuel du terme.

Voici ces six réseaux, pour lesquels nous donnons α_0, un triplet $(\alpha_1, \alpha_2, \alpha_3)$, et le déterminant noté det.

$q = 15$: 2 ; (-1, 0, 0) ; det=1 (E_8).
$q = 16$: 8 ; (-2,-4, 3) ; det=$(2.241)^2$.
$q = 16$: 2 ; (-1,-0,-0) ; det=4 (D_8).
$q = 16$: 4 ; (-2, 0, 1) ; det=$(2.17)^2$).
$q = 24$: 2 ; (-1,-0,-0) ; det=1 (E_8).
$q = 24$: 4 ; (0,-1,-2) ; det=5^4.

Les constantes d'Hermite des trois réseaux G-parfaits trouvés pour $|G| = 16$, arrondies aux deux décimales les plus proches, sont respectivement 72,21 ; 64,00 et 56,69 . On en déduit :

THÉORÈME. *Soit Λ un réseau d'un espace euclidien de dimension 8, invariant sous l'action d'un groupe cyclique ($\mathbb{Q}$-irréductible) d'ordre 16. Alors, la constante d'Hermite de Λ vérifie l'inégalité*

$$\gamma_8(\Lambda)^8 \leq 2^{22}241^{-2} = 72,214... \quad (< \gamma_8^8 = 256).$$

On peut également montrer (M. Laïhem) que les seuls réseaux de dimension 8 parfaits pour le groupe quaternionien d'ordre 8 sont (à similitude près) D_8 et E_8.

Signalons enfin que François Sigrist a calculé les "G-voisins" d'un certain nombre de G-réseaux considérés dans cet article pour l'adaptation naturelle aux G-réseaux de l'algorithme classique de Voronoï. Bien que l'on n'ait pas encore de résultats de connexité au sens de la remarque 3.13 qui permettraient d'effectuer des classifications, on a dès à présent un procédé intéressant de construction de G-réseaux. En outre, les résultats de Sigrist corroborent ceux de notre article dans le cas des groupe cycliques $\mathbb{Q}$-irréductibles d'ordre 5 et 7 (th. 4.3 et 4.6) ainsi que dans le cas des groupes d'ordre 5 en dimension 5, où il y a une composante connexe de 4 classes de G-réseaux (correspondants à ceux qui sont projectifs sur $\mathbb{Z}[G]$) et une composante réduite à la classe de $A_1 \perp A_4$, conformément à ce que laissait prévoir le th. 5.3. Enfin, dans le cas $|G| = n = 7$, il trouve à partir de A_7 les 6 réseaux évoqués dans la remarque 5 et deux réseaux supplémentaires analogues au réseau Λ_5 du th. 5.3.

BIBLIOGRAPHIE

[1] E.S. Barnes, *On a theorem of Voronoï*, Proc. Cambridge Phil. Soc. **53** (1957), 537–539.

[2] E.S. Barnes, *The perfect and extreme senary forms*, Canad. J. Math. **9** (1957), 235–242.

[3] E. Bayer-Fluckiger, *Definite unimodular lattices having an automorphism of given characteristic polynomial*, Comm. Math. Helvet. **59** (1984), 509-538.

[4] A-M. Bergé et J. Martinet, *Sur un problème de dualité lié aux sphères en géométrie des nombres*, J. Number Theory **32** (1989), 14–42.

[5] A-M. Bergé et J. Martinet, *Sur les minorations géométriques des régulateurs*, "Séminaire de Théorie des Nombres de Paris," Birkhäuser, Bâle, 1989, pp. 23–50.

[6] J.H. Conway et N.J.A. Sloane, "Sphere Packings, Lattices and Groups," Springer-Verlag, Grundlehren no 290, Heidelberg, 1988.

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

[8] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker et R.A. Wilson, "ATLAS of Finite Groups," Oxford Univ. Press, 1988.

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

[10] M. Craig, *Extreme Forms ans Cyclotomy*, Mathematika **25** (1978), 44–56.

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

[12] J-P. Serre, "Représentations linéaires des groupes finis (2ième édition)," Hermann, Paris, 1971.

[13] J-P. Serre, "Corps locaux (3ième édition)," Hermann, Paris, 1980.

[14] R. Schoof et L. Washington, *Quintic Polynomials and Real Cyclotomic Fields with Large Class Numbers*, Math. Comp. **50** (1988), 543–556.

mots clés : automorphismes, réseaux, géométrie des nombres

Laboratoire de Mathématiques
351, cours de la Libération
F-33405 TALENCE cedex

(Reçu le 3 novembre 1989)