RÉSEAUX ET "DESIGNS" SPHÉRIQUES

par Boris VENKOV
(notes de Jacques Martinet)

RÉSUMÉ. La théorie classique de Korkine et Zolotareff, approfondie au début du 20-ième siècle par Voronoï, a trouvé un relais dans la notion de design sphérique : le fait que l'ensemble des vecteurs minimaux d'un réseau euclidien soit un 2- ou un 4-design sphérique est une forme restrictive de la propriété d'eutaxie ou d'extrémalité. Après quelques rappels sur la notion de t-design sphérique, on étudie sa traduction en termes de réseaux, puis on résoud certains problèmes de classification (réseaux de petite dimension ou de petit "kissing number", réseaux entiers de petit minimum). On étudie pour terminer les applications de la théorie des formes modulaires à coefficients harmoniques (sphériques) ainsi que certaines constructions par sections.

ABSTRACT. ENGLISH TITLE : Lattices and Spherical Designs.
New methods in the study of the classical theory of Korkine and Zolotareff, refined by Voronoï at the beginnning of the twentieth century, have arised in connection with the notion of a spherical design : that the set of minimal vectors of a lattice be a spherical 2- or 4-design is a restrictive form of the properties of eutaxy or extremality. After having recalled some basic facts about spherical t-designs, we study the translation of this theory in terms of lattices, then we solve some classification questions (small dimensional lattices, lattices with a small kissing number, integral lattices with a small minimum). We finish with some applications to this theory of the theory of modular forms with harmonic (spherical) coefficients as well as some constructions of designs by means of sections of lattices.

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

Mots-clés : *Réseaux, designs sphériques, perfection, formes modulaires.*

L'auteur remercie le C.N.R.S. et l'Université Bordeaux 1 qui, en lui offrant la possibilité d'effectuer deux séjours de six mois à Bordeaux, ont permis la réalisation de cet article, ainsi que le Fonds National Suisse de la Recherche Scientifique, qui a financé plusieurs séjours à l'Université de Genève. L'auteur remercie également les universités d'Aix-la-Chapelle et de Dortmund qui ont organisé plusieurs séjours de l'auteur, lui donnant l'occasion d'y exposer diverses parties de ce cours.

Introduction.

L'origine de cet article est un cours professé à Bordeaux par son auteur pendant le premier semestre de l'année 1997-1998. Le but du cours était l'étude des connexions qui existent entre la théorie des designs sphériques d'une part, et la théorie des réseaux euclidiens d'autre part. Au départ, il y a la remarque suivante : si les vecteurs minimaux d'un réseau forment un 4-design sphérique, alors le réseau est parfait (et même extrême) au sens de la théorie de Korkine-Zolotareff et Voronoï, cf. §6. Ces réseaux sont donc *a priori* intéressants du point de vue de la géométrie des nombres.

Les méthodes développées dans cet article permettent de prouver l'extrémalité des réseaux de certaines familles qui n'ont pas encore été classées, par exemple la famille des réseaux unimodulaires pairs de minimum 4 et de dimension 32. Dans ce cas précis, le résultat est obtenu en exploitant des propriétés modulaires des fonctions Thêta à coefficients harmoniques de ces réseaux, une méthode qui apparaît pour la première fois dans [V2].

Rappelons la définition d'un design sphérique. Dans l'espace $\mathbb{R}^n$ muni de son produit scalaire canonique $(\,,\,)$, considérons une partie finie X de S^{n-1} (*sphère unité de* $\mathbb{R}^n$). En *analyse numérique*, on s'intéresse à l'estimation de l'intégrale d'une fonction $f : S^{n-1} \to \mathbb{R}$. On a l'approximation

$$(*) \qquad \int_{S^{n-1}} f\,dx \sim \frac{1}{|X|}\sum_{x\in X} f(x)\,.$$

Définition. Soit t un entier positif. On dit que X est un *t-design (sphérique)* s'il y a égalité dans $(*)$ pour tout polynôme f de degré au plus t.

Exemple. Soit Λ_{24} le réseau de Leech (renormé à la norme 1), et soit X l'ensemble de ses vecteurs minimaux. (On a $|X| = 196560$.) Alors, X est un 11-design.

Définition. Un réseau dont les vecteurs minimaux portent une structure de 4-design est dit *fortement parfait*.

Il y a une très importante littérature sur les designs sphériques, provenant de sources varées, notamment de la combinatoire (écoles de Seidel et de Bannai) et de l'analyse numérique (école de Sobolev).

La classification des t-designs sphériques devient vite impossible, lorsque l'invariant t ou la cardinalité est élevé. Or, les designs portés par les vecteurs minimaux d'un réseau jouissent de propriétés particulières qui ouvrent la voie à des résultats de classification.

EXEMPLE. En dimension 10, il existe (à similitude près) exactement deux réseaux fortement parfaits (i.e., dont les vecteurs minimaux forment un 4-design).

Dans cet article, on démontrera plusieurs résultats de classification de réseaux fortement parfaits. Par exemple, la classification des réseaux fortement parfaits est connue jusqu'à la dimension 11 ; ces réseaux sont au nombre de 10. Outre quelques réseaux de racines et leurs duals, on trouve seulement les deux réseaux de dimension 10 de l'exemple précédent. De même, nous avons classé les réseaux fortement parfaits qui sont entiers et de minimum 3 ; il y en a cinq, de dimensions 1, 7, 16, 22, 23.

L'article est organisé de la façon suivante. On discute les généralités sur le laplacien et les polynômes harmoniques dans les deux premiers §§, puis sur les designs sphériques au §3, notion illustrée au §4 sur l'exemple des designs de dimension 2. On considère ensuite les systèmes de racines du point de vue des designs sphériques. La notion de *réseau fortement parfait* est introduite au §6, où l'on démontre qu'il s'agit de configurations extrêmes au sens de Korkine et Zolotareff. Les réseaux fortement parfaits de minimum 3 sont classés au §7, ceux de dimensions 8, 9 et 11 le sont aux §§11 et 12. Nous donnons au §8 une caractérisation numérique des designs sphériques qui semble être nouvelle, et qui caractérise les t-designs comme minima absolus pour la norme ℓ^t de leur matrices de Gram. (Une application à l'analyse fonctionnelle figure au §15.) La connexion de cette théorie avec le problème de Waring pour les polynômes est discutée au §14. Les §§16 et 17 sont consacrés à l'étude des réseaux extrémaux au sens des formes modulaires et de certains réseaux qui leur sont proches. Un §18 est consacré à la célèbre famille des réseaux de Barnes-Wall, seule famille infinie connue de réseaux fortement parfaits. Enfin, nous terminons par un §19, de nature numérique.

Je remercie Jacques Martinet qui a rédigé cet article à partir de notes prises à mon cours de Bordeaux, et qui a par ailleurs amelioré quelques unes de mes démonstrations ainsi que la présentation de l'ensemble.

Je remercie également Thierry Vust pour sa lecture détaillée de la première version transmise à *L'Enseignement Mathématique*, ainsi que pour sa participation à la rédaction des paragraphes 17 et 18.

Je remercie aussi Christian Batut pour son importante participation à la confection des tables du paragraphe 19.

Je remercie enfin les auditeurs de mes cours à Bordeaux, Aix-la-Chapelle et Dortmund (C. Batut, C. Bachoc, C. Bavard, A.-M. Bergé, H. Cohen, R. Coulangeon, J. Martinet, G. Nebe, W. Plesken, R. Scharlau) pour leur intérêt stimulant.

Voici le plan de l'article :

1. Fonctions polynomiales et laplacien.

L'espace $\mathbb{R}^n$ est muni de son produit scalaire canonique $(\,,\,)$, et l'on note $(e_1,\dots,e_n)$ sa base (orthonormale) canonique. On identifie à l'aide de cette base l'anneau $\mathbb{R}[X_1,\dots,X_n]$ des polynômes réels à n indéterminées à l'ensemble $\mathcal{F}$ des fonctions polynomiales sur $\mathbb{R}^n$. On note $\mathcal{F}_{n,m}$, ou parfois simplement $\mathcal{F}_m$, la partie homogène de degré m de $\mathcal{F}$.

Étant donné un multi-indice $i=(i_1,\dots,i_n)\in\mathbb{Z}_+^n$, on pose

$$|i|=\sum_{k=1}^n i_k\,,\quad X^i=X_1^{i_1}\dots X_n^{i_n}\quad\text{et}\quad T_m=\{i\mid |i|=m\}\,;$$

le *coefficient multinomial* correspondant est

$$c(i)=\frac{|i|!}{i_1!\dots i_n!}\,.$$

Noter que l'on a $\dim\mathcal{F}_{n,m}=|T_m|=\binom{n+m-1}{n-1}$.

Pour définir un produit scalaire sur l'espace $\mathcal{F}_{n,m}$, nous introduisons le coefficient $c(i)$ dans la représentation des éléments f de $\mathcal{F}$: pour $f(x)=\sum_{i=1}^n c(i)a(i)x^i$ et $g(x)=\sum_{i=1}^n c(i)b(i)x^i$, on pose

$$[f,g]=\sum_{|i|=m} c(i)a(i)b(i);$$

c'est bien un produit scalaire euclidien.

Voici encore deux notations: on pose $\omega(x)=(x,x)$ et, pour tout $\alpha\in\mathbb{R}^n$, $\rho_\alpha^{(m)}(x)=(x,\alpha)^m$. Nous considérerons le plus souvent des polynômes homogènes de degré m *pair*. Alors, les deux fonctions $\omega^{m/2}$ et $\rho_\alpha^{(m)}$ sont des polynômes homogènes de degré m.

Proposition 1.1. *Pour tout $f\in\mathcal{F}_m$ et tout $\alpha\in\mathbb{R}^n$, on a $[f,\rho_\alpha^{(m)}]=f(\alpha)$.* [On dit parfois que $\rho_\alpha^{(m)}$ est un "noyau reproduisant".]

Démonstration. On écrit ρ sous forme canonique:

$$\begin{aligned}\rho_\alpha^{(m)}=(\alpha_1x_1+\dots+\alpha_nx_n)^m&=\sum_{i_1+\dots+i_n=m}\frac{m!}{i_1!\dots i_m!}\alpha_1^{i_1}x_1^{i_1}\dots\alpha_n^{i_n}x_n^{i_n}\\&=\sum_{|i|=m}c(i)\alpha^ix^i\,,\end{aligned}$$

ce qui entraîne tout de suite l'égalité

$$[f,\rho_\alpha^{(m)}]=\sum_{|i|=m}c(i)\alpha^i\,a(i)=f(\alpha)\,.\qquad\square$$

À $f \in \mathcal{F}_m$, on associe un opérateur différentiel, obtenu en remplaçant le vecteur $(x_1, \dots, x_n)$ par le vecteur formel $\nabla = (\frac{\partial}{\partial x_1}, \dots, \frac{\partial}{\partial x_n})$, noté $f(\nabla)$. (∇ se lit *nabla*.) Avec cette notation, on a :

PROPOSITION 1.2. $m!\,[f, g] = f(\nabla)g$.

Démonstration. On a en effet $\nabla^j x^i = 0$ si $j \neq i$ et $\nabla^i x^i = i_1! \dots i_n!$, comme on le voit sur l'expression $\nabla^j = \frac{\partial^{j_1}}{\partial x_1^{j_1}} \cdots \frac{\partial^{j_n}}{\partial x_n^{j_n}}$. □

On rappelle que l'on a posé $\omega(x) = (x, x)$. Il en résulte que

$$\omega(\nabla) = \frac{\partial^2}{\partial x_1^2} + \cdots + \frac{\partial^2}{\partial x_n^2}$$

est l'*opérateur Δ de Laplace*. Il est invariant par le groupe orthogonal de $\mathbb{R}^n$, et applique $\mathcal{F}_{n,m}$ dans $\mathcal{F}_{n,m-2}$. Son noyau est l'ensemble des polynômes harmoniques :

$$\ker \Delta = \mathrm{Harm}_{n,m}\,(= \mathrm{Harm}_m)\,.$$

PROPOSITION 1.3. *L'opérateur Δ est surjectif.*

Démonstration. Soit $g \in (\mathrm{Im}\,\Delta)^\perp \subset \mathcal{F}_{n,m-2}$. Alors, ωg est un élément de $\mathcal{F}_{n,m}$ et, pour tout $f \in \mathcal{F}_{n,m}$, on a les égalités

$$\begin{aligned} m!\,[\omega g, f] = (\omega g)(\nabla)\, f &= \omega(\nabla) g(\nabla)\, f \\ &= \Delta g(\nabla)\, f = g(\nabla)\Delta f = (m-2)!\,[g, \Delta f] = 0\,. \end{aligned}$$

Il en résulte que ωg, donc g lui-même, est nul. □

REMARQUE 1.4. Cette démonstration par orthogonalité ne permet pas de construire explicitement un relèvement dans $\mathcal{F}_{n,m}$ d'un élément donné de $\mathcal{F}_{n,m-2}$. Une telle construction peut être obtenue en utilisant les *polynômes orthogonaux de Gegenbauer*, cf. [Vi].

Terminons ce § par quelques exemples de calculs de laplaciens, dont les détails sont laissés au lecteur ; α désigne un élément de $\mathbb{R}^n$; la notation Δ_y signifie que l'on dérive par rapport à la variable y.

EXEMPLE 1.5.

$$\Delta_x(\alpha,x)^m = m(m-1)(\alpha,\alpha)(\alpha,x)^{m-2}\,.$$
$$\Delta(x,x)^\ell = 2\ell(2\ell+n-2)(x,x)^{\ell-1}\,.$$
$$\Delta_\alpha\left[(\alpha,\alpha)^\ell(x,\alpha)^k\right] =$$
$$2\ell(2\ell+2k+n-2)(\alpha,\alpha)^{\ell-1}(x,\alpha)^k + k(k-1)(x,x)(\alpha,\alpha)^\ell(\alpha,x)^{k-2}\,.$$

Voici deux exemples en degrés 2 et 4. Pour $\alpha\in\mathbb{R}^n$, posons

$$P_\alpha^{(2)}(x) = (x,\alpha)^2 - \frac{1}{n}(\alpha,\alpha)(x,x)$$

et

$$P_\alpha^{(4)}(x) = (x,\alpha)^4 - \frac{6}{n+4}(x,\alpha)^2(x,x)(\alpha,\alpha) + 3\frac{(x,x)^2(\alpha,\alpha)^2}{(n+4)(n+2)}\,.$$

Alors, $P_\alpha^{(2)}$ et $P_\alpha^{(4)}$ sont des polynômes harmoniques de degrés respectifs 2 et 4.

2. POLYNÔMES HARMONIQUES.

On a vu que le Laplacien est une application linéaire de $F_{n,m}$ sur $F_{n,m-2}$, et que l'application $f\mapsto\omega f$ est une application linéaire en sens inverse.

THÉORÈME 2.1.

(1) On a une décomposition en somme directe orthogonale

$$\mathcal{F}_{n,m} = \mathrm{Harm}_m \perp \omega\,\mathrm{Harm}_{m-2} \perp \omega^2\,\mathrm{Harm}_{m-4} \perp \dots\,.$$

(2) Chacun des sous-espaces ci-dessus est stable par $\mathrm{SO}(n)$.

(3) Ces sous-espaces sont irréductibles. [Cela signifie qu'ils ne contiennent pas de sous-espaces non triviaux stables par $\mathrm{SO}(n)$.]

(4) Un polynôme harmonique divisible par $\omega=(x,x)$ *est nul.*

(5) Un polynôme invariant de degré m *est nul si* m *est impair, et est proportionnel à* $\omega^{m/2}$ *si* m *est pair.*

Démonstration. Nous renvoyons à la fin du § la démonstration de la troisième assertion.

Le fait qu'il s'agisse dans (1) d'une somme orthogonale provient de l'égalité $[\omega g, f] = 0$ rencontrée au cours de la démonstration de la proposition 1.3. Cette proposition entraîne aussi l'égalité $\dim \mathrm{Harm}_m = \dim \mathcal{F}_m - \dim \mathcal{F}_{m-2}$. On en déduit par récurrence à partir des cas évidents $m \leq 1$ l'égalité des dimensions des deux membres. Les assertions (2), (4) et (5) sont faciles. □

DÉFINITION 2.2. On dit qu'un espace métrique $(\mathcal{E}, d)$ est 2-*homogène* si, quels que soient les couples (x_1, y_1) et (x_2, y_2) de points de $\mathcal{E}$ tels que $d(x_1, y_1) = d(x_2, y_2)$, il existe une isométrie σ de $\mathcal{E}$ avec $x_2 = \sigma(x_1)$ et $y_2 = \sigma(y_1)$.

EXEMPLE 2.3. La sphère $S^{n-1} \subset \mathbb{R}^n$ est 2-homogène pour tout $n \geq 2$.

Autres exemples: $P^n(\mathbb{R})$, $P^n(\mathbb{C})$, $P^n(\mathbb{H})$, $P^2(\mathbb{O})$ (le plan projectif de Cayley); il y a aussi de nombreux ensembles finis intéressants, par exemples des graphes. Voici encore un exemple: on considère un espace vectoriel V de dimension finie sur un corps fini K et la grassmannienne $\mathrm{Gr}_m(V)$ des sous-espaces de V de dimension m sur K; on prend comme distance de deux sous-espaces $d(W_1, W_2) = m - \dim W_1 \cap W_2$.

Revenons au cas de $\mathcal{E} = S^{n-1}$, muni du groupe d'isométries $\mathrm{SO}(n)$. Soit $M = M(S^{n-1}, \mathbb{R})$ l'espace des fonctions réelles sur S^{n-1}. Considérons un sous-espace V de M de dimension finie, non réduit à $\{0\}$, et invariant par $\mathrm{SO}(n)$.
[Le groupe $\mathrm{SO}(n)$ opère sur M par $(\sigma.f)(x) = f(\sigma^{-1}x)$; on suppose que l'on a $\sigma.f \in V$ quels que soient $f \in V$ et $\sigma \in \mathrm{SO}(n)$.]

Il existe sur V un produit scalaire $(\ ,\ )$ invariant par $\mathrm{SO}(n)$, comme on le voit en prenant la moyenne des transformés par le groupe compact $\mathrm{SO}(n)$ d'un produit scalaire arbitraire. Alors, $\forall\, \sigma \in \mathrm{SO}(n)$, $\forall\, f, g \in V$, $(\sigma f, \sigma g) = (f, g)$.

Soit $N = \dim V$ et soit $(f_1, \ldots, f_N)$ une base orthonormale de V. Pour $x_1, x_2 \in S^{n-1}$, posons

$$\alpha(x_1, x_2) = \sum_{i=1}^{N} f_i(x_1) f_i(x_2)\,.$$

PROPOSITION 2.4.

(1) α *ne dépend pas du choix de la base orthonormale* $(f_1, \ldots, f_N)$.

(2) $\alpha(x_1, x_2)$ *ne dépend que de la distance de* x_1 *à* x_2.

Démonstration. (1) Soit $(g_1, \ldots, g_N)$ une autre base orthonormale. Exprimons les g_i sur la base $(f_1, \ldots, f_N)$: $\forall\, i,\ g_i = \sum_j \alpha_{j,i} f_j$. Le fait que la seconde base soit orthonormale se traduit par les relations $\sum_i \alpha_{j,i}\alpha_{k,i} = \delta_{j,k}$. On a alors

$$\begin{aligned}\sum_i g_i(x_1)g_i(x_2) &= \sum_{i,j,k} \alpha_{j,i}\alpha_{k,i} f_j(x_1) f_k(x_2) \\ &= \sum_{j,k} \big(\sum_i \alpha_{j,i}\alpha_{k,i}\big) f_j(x_1) f_k(x_2) \\ &= \sum_j f_j(x_1) f_k(x_2)\,.\end{aligned}$$

(2) Soient $x_1, x_2, y_1, y_2 \in S^{n-1}$ avec $d(x_1, x_2) = d(y_1, y_2)$. Il existe $\sigma \in \mathrm{SO}(n)$ avec $y_1 = \sigma x_1$ et $y_2 = \sigma x_2$. On a alors

$$\alpha(y_1, y_2) = \alpha(\sigma x_1, \sigma x_2) = \sum_i f_i(\sigma x_1) f_i(\sigma x_2)\,.$$

Mais, en notant g_i la transformée de f_i par σ^{-1}, on a $f_i(\sigma x) = g_i(x)$ quel que soit $x \in S^{n-1}$, et donc $\alpha(y_1, y_2) = \alpha(x_1, x_2)$ par (1). □

Fixons maintenant un point $e \in S^{n-1}$. Appelons *fonction zônale sphérique* une fonction $f(x)$ définie sur S^{n-1} qui ne dépend que de la distance de x à e. Par exemple, la fonction $x \mapsto \alpha(e, x)$ est une fonction zônale sphérique.

Montrons que V contient une fonction zônale sphérique non nulle. En effet, on aurait sinon $\alpha(e, e) = \sum_i f_i^2(e) = 0$, ce qui entraînerait que toutes les fonctions f_i, et par conséquent toutes les fonctions de V, s'annulent en e ; vu que V est invariant et que l'opération de SO_n sur S^{n-1} est transitive , cela entraînerait que les fonctions de V s'annulent en tout point de S^{n-1}, ce qui est absurde.

LEMME 2.5. *Si l'espace des fonctions zônales sphériques de* V *est de dimension* 1, V *est irréductible pour l'action de* $\mathrm{SO}(n)$.

Démonstration. Sinon, soit W' un sous-espace stable non trivial de V, et soit W'' son orthogonal. C'est un sous-espace stable de V, qui est

un supplémentaire de W. La construction d'une fonction $\alpha(e,x) \neq 0$ peut être faite dans W' et dans W''. Dans les deux cas, ce sont des fonctions zônales sphériques de V. L'hypothèse faite sur la dimension montre qu'elles sont proportionnelles, ce qui contredit $W' \cap W'' = \{0\}$. □

Fin de la démonstration du théorème 2.1. On va appliquer ce lemme à l'espace Harm_m, en choisissant $e \in S^{n-1}$, et en montrant qu'il existe une unique fonction $f \in \mathrm{Harm}_m$, dont la restriction à S^{n-1} est zônale sphérique, et qui est telle que $f(e) = 1$. Sur S^{n-1}, elle ne dépendra que de la distance de x à e, donc que de la valeur du produit scalaire (x,e), et pourra donc se mettre sous la forme $f(x) = F((x,e),(x,x))$, où F est un polynôme à deux indéterminées.

Soit $f = \sum a_{i,j}(x,e)^i(x,x)^j$. Il existe deux constantes c_1, c_2 pour lesquelles on a

$$\Delta\,(x,x)^j(x,e)^i = c_1(x,x)^{j-1}(x,e)^i + c_2(x,x)^j(x,e)^{i-2}\,.$$

Ainsi, Δ devient un opérateur différentiel d'ordre 2 sur l'espace des polynômes à deux indéterminées.

On doit montrer que l'espace des fonctions f comme ci-dessus est de dimension 1. Comme un polynôme harmonique non nul ne peut pas être divisible par (x,x) (théorème 2.1, (4)), s'il existait deux fonctions f et g, on pourrait écrire

$$f = (x,e)^m + \alpha_1(x,x)(x,e)^{m-1} + \dots$$

et

$$g = (x,e)^m + \beta_1(x,x)(x,e)^{m-1} + \dots,$$

et $g-f$ serait un polynôme harmonique divisible par (x,x), donc nul. Cela prouve que l'espace ci-dessus est de dimension au plus 1. En fait, cette dimension est égale à 1, car il existe un unique polynôme harmonique de terme dominant $(x,e)^m$, à savoir le *polynôme de Gegenbauer* G_m, voir [Vi] pour la définition. [Par exemple, on a $G_2(x) = (x,e)^2 - \frac{1}{n}\,(x,x)\,(e,e)$.] Cela achève la démonstration du théorème 2.1. □

3. Généralités sur les designs sphériques.

Rappelons la définition suivante de l'introduction :

DÉFINITION 3.1. Soit $X \subset S^{n-1}$ un ensemble fini. On dit que X est un *t-design sphérique* si on a l'égalité

$$(*) \qquad \int_{S^{n-1}} f(x)\,dx = \frac{1}{|X|}\sum_{x\in X} f(x)$$

quel que soit le polynôme homogène f de degré $\leq t$.
[Comme toujours, on normalise la mesure par $\int_{S^{n-1}} dx = 1$.]

Dans l'énoncé suivant, étant donné un entier $t > 0$, on note p (resp. i) le plus grand entier pair (resp. impair) qui est $\leq t$ (le plus grand des deux est donc égal à t.)

THÉORÈME 3.2. *On suppose $n \geq 2$. Alors, les conditions suivantes sont équivalentes :*

(1) X est un t-design sphérique.

(2) Quels que soient le polynôme f homogène de degré $\leq t$ et $\sigma \in \mathrm{SO}(n)$, on a

$$\sum_{x\in X} f(x) = \sum_{x\in X} (\sigma f)(x)\,.$$

(3) Pour tout polynôme harmonique homogène non constant de degré $\leq t$, on a $\sum_{x\in X} f(x) = 0$.

(4) Il existe une constante $c = c_p$ telle que, quel que soit $\alpha \in \mathbb{R}^n$, on a les deux égalités

$$\sum_{x\in X} (x,\alpha)^p = c(\alpha,\alpha)^{p/2} \quad \textit{et} \quad \sum_{x\in X} (x,\alpha)^i = 0\,.$$

Démonstration. (1) $\Rightarrow$ (2). Cela résulte de l'invariance de la mesure par $\mathrm{SO}(n)$.

(2) $\Rightarrow$ (3). Considérons pour $m \leq t$ l'application $f \mapsto \sum_{x\in X} f(x)$ de Harm_m dans $\mathbb{R}$. Son noyau est un sous-espace invariant par $\mathrm{SO}(n)$, non trivial, car $\dim \mathrm{Harm}_m > 1$. C'est donc l'espace Harm_m tout entier.

(3) $\Rightarrow$ (4). On peut compléter $(x,\alpha)^p$ par des termes degré inférieur de façon à obtenir un polynôme harmonique

$$h = (x,\alpha)^p + \lambda(\alpha,\alpha)(x,\alpha)^{p-2}(\alpha,\alpha) + \dots\,.$$

Par différence, on se ramène à un polynôme sans terme en $(x,\alpha)^p$, et, en répétant le procédé, on arrive à un polynôme de degré 0 ou 1, pour lequel le résultat cherché est évident.

(4) $\Rightarrow$ (1). On remarque d'abord que si l'assertion (4) est vérifiée, la valeur de c est celle écrite en 3.6 ci-dessous. Cela se voit par récurrence en utilisant les calculs de laplacien qui se trouvent dans la eexemple 1.5. En outre, toujours par itération du laplacien, on aura les formules

$$\sum_{x\in X}(x,\alpha)^k = c(\alpha,\alpha)^{k/2} \quad \text{et} \quad \sum_{x\in X}(x,\alpha)^\ell = 0$$

pour tout $k \leq p$ pair et tout $\ell \leq i$ impair. Enfin, les polynômes $\rho_\alpha^{(m)} = (x,\alpha)^m$, quand α parcourt $\mathbb{R}^n$, engendrent l'espace $\mathcal{F}_{n,m}$ des polynômes en x homogènes de degré m : cela peut se voir en remarquant que $\mathrm{GL}_n(\mathbb{R})$ opère irréductiblement sur $\mathcal{F}_{n,m}$ et que l'espace engendré par les $\rho_\alpha^{(m)}$ est invariant, donc égal à $\mathcal{F}_{n,m}$ tout entier; on peut aussi utiliser le produit scalaire $[\,,\,]$ introduit au §1, en remarquant que si F est dans l'orthogonal du sous-espace engendré par les $\rho_\alpha^{(m)}$, on a

$$0 = [F, \rho_\alpha^{(m)}] = F(\alpha)$$

(proposition 1.1), c'est-à-dire $F(\alpha) = 0$ quel que soit $\alpha \in \mathbb{R}^n$.

On procède maintenant à la démonstration proprement dite. On veut démontrer que l'égalité

$$\int_{S^{n-1}} f(x)\,dx = \frac{1}{|X|}\sum_{x\in X} f(x)$$

est satisfaite par tous les polynômes homogènes f de degré au plus t. Cette égalité étant linéaire en f, il suffit de considérer les fonctions $f = \rho_\alpha^{(m)}$ pour tout $m \leq t$ et tout $\alpha \in \mathbb{R}^n$. Dans ce cas, on connaît le second membre, et la formule à démontrer devient

$$\int_{S^{n-1}} (x,\alpha)^m\,dx = \frac{c_m}{|X|}\,(\alpha,\alpha)^{m/2}$$

lorsque m est pair, et

$$\int_{S^{n-1}} (x,\alpha)^m\,dx = 0$$

lorsque m est impair. Or, l'intégrale, en tant que fonction de α, est un polynôme homogène de degré m invariant par l'action de SO_n. Ce polynôme est donc nul si m est impair, et de la forme $c'_m\,(\alpha.\alpha)^{m/2}$ pour une certaine constante c'_m lorsque m est pair (théorème 2.1, (5)). En appliquant le laplacien aux deux membres de l'égalité, on voit que les constantes c'_m vérifient les mêmes relations de récurrence que les constantes c_m ; on conclut en observant que l'on a $c'_0 = \dfrac{1}{|X|}\,c_0 = 1$.

REMARQUE 3.3. Le plus souvent, on ne considère que des ensembles X symétriques (i.e., on a $-X = X$). Alors, la condition $\sum_{x\in X}(x,\alpha)^i = 0$ est automatiquement vérifiée.

REMARQUE 3.4. Pour tout $\sigma \in \mathrm{O}(n)$, σX est encore un t-design sphérique.

REMARQUE 3.5. Si X_1 et X_2 sont deux t-designs sphérique de même dimension *disjoints*, $X_1 \cup X_2$ est aussi un t-design sphérique.

Rappelons pour utilisation ultérieure que la constante c qui intervient dans l'énoncé 3.2, (4) est

$$c = c_p = \frac{1.3.5\ldots(p-1)}{n(n+2)\ldots(n+p-2)}\,|X|\,. \tag{3.6}$$

4. LES DESIGNS DE DIMENSION 2.

Dans ce §, nous identifions $\mathbb{R}^2$ à $\mathbb{C}$; on a alors $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$, et X est un ensemble fini $\{z_1, \ldots, z_N\}$ de nombres complexes de module 1. L'espace $\mathcal{F}_m$ est de dimension $m+1$, de base $x^m, x^{m-1}y, \ldots, y^m$. On peut remplacer (x,y) par $(z,\overline{z})$ (avec $z = x+iy$). Les polynômes harmoniques homogènes de degré m forment un espace de dimension 2, engendré par $\Re(z^m)$ et $\Im(z^m)$, qui constituent une base de Harm_m. La condition pour X d'être un t-design, qui s'écrit $\sum_{x\in X} f(x) = 0$ pour tout polynôme harmonique de degré $\leq t$, est simplement $z_1^m + z_2^m + \cdots + z_N^m = 0$ pour $m = 1, 2, \ldots, t$.

En particulier, les racines N-ièmes de l'unité sont un t-design sphérique à N éléments pour tout $t < N$.

PROPOSITION 4.1. *Les $(N-1)$-designs sphériques sont les polygones réguliers à N côtés.*

Démonstration. Considérons le polynôme $f(X) = (z-z_1)\ldots(z-z_N)$. Il se développe sous la forme $z^N + \sum_{i=1}^{N-1} a_i X^{N-i} + c$. Les formules de Newton montrent que les relations $z_1^m + z_2^m + \cdots + z_N^m = 0$ sont satisfaites pour $1 \leq m \leq N-1$ si et seulement si les coefficients α_i sont nuls pour $1 \leq i \leq N-1$. Dans ces conditions, les racines de $f(X) = X^N - c$ sont les sommets d'un polygone régulier. La réciproque est évidente. □

De façon générale, on construit des t-design sphériques en observant que l'image par une rotation d'un t-design sphérique est encore un t-design sphérique, et qu'un t-design sphérique est un t_1-design sphérique pour $t_1 \leq t$.

THÉORÈME 4.2 (Hong). *Soit X un t-design sphérique.*

(1) Si $t+1 \leq |X| \leq 2t+1$, X est un polygone regulier.

(2) Si $|X| = 2t+2$, X est réunion de deux polygones réguliers.

Démonstration. On écrit encore $X = \{x_1, \ldots, z_N\}$ et $f(X) = \prod_{i=1}^{N}(X - z_i)$.

(1) On sait que les t coefficients de $z_1, \ldots, z_t$ sont nuls. Comme les racines de $z^N f(\frac{1}{z})$ sont les inverses, et donc les conjuguées, de celles de f, les formules de Newton montrent encore que les coefficients de $z^{N-1}, \ldots, z^{N-t}$ sont également nuls, donc que f est de la forme $X^N - c$, $|c| = 1$.

(2) Le même argument montre maintenant seulement que f est de la forme $f(X) = X^{2t+2} - AX^{t+1} + c$. Par rotation, on se ramène au cas où $c = 1$, si bien que f est alors de la forme $f(X) = (X^{t+1} - B)(X^{t+1} - \overline{B})$, polynôme dont les racines sont les sommets d'une réunion de deux polygones réguliers. □

REMARQUE 4.3. On peut montrer qu'il existe des familles de t-designs X dépendant (à isométrie près) d'un paramètre continu pour lesquels $|X|$ prend n'importe quelle valeur donnée $s \geq 2t+3$.

Les constructions de designs en dimension $n \geq 3$ sont plus difficiles. D'après un théorème non constructif de Seymour et Zaslavsky ([S-Z]), il existe des t-design sphériques dans $\mathbb{R}^n$ pour toutes les valeurs de n et de t. On ne dispose pas de bonnes estimations de la taille de X. Nous verrons dans la suite que la situation est beaucoup plus simple si X est l'ensemble des vecteurs courts d'un réseau euclidien.

5. Designs associés aux systèmes de racines.

On suppose dorénavant que X est l'ensemble des vecteurs minimaux d'un réseau Λ d'un espace euclidien E dont nous notons n la dimension et (x, y) le produit scalaire. Pour alléger certaines notations, on ne suppose

plus que la sphère qui contient X soit de rayon 1. Comme $X = -X$, la seconde condition de 3.2, (4) est automatiquement vérifiée, et l'existence d'une constante c pour laquelle on a l'identité

$$\sum_{x\in X}(x,\alpha)^{2k} = c(\alpha,\alpha)^k \tag{5.1}$$

pour tout $\alpha \in E$ suffit à assurer que X est un $(2k+1)$-design sphérique. (Il y a identité entre $2k$- et $(2k+1)$-designs.)

On rappelle que si X est un t-design sphérique, c'est aussi un t'-design sphérique pour tout $t' \leq t$, si bien qu'il existe une identité de la forme $\sum_{x\in X}(x,\alpha)^{2\ell} = c_\ell(\alpha,\alpha)^\ell$ pour tout $\ell < k$.

On s'intéresse maintenant aux 5-designs. On a alors deux identités

$$\sum_{x\in X}(x,\alpha)^2 = c(\alpha,\alpha) \quad \text{et} \quad \sum_{x\in X}(x,\alpha)^4 = d(\alpha,\alpha)^2\,,$$

dont la première est conséquence de la seconde. En calculant Δ_α à partir des formules 1.5, on détermine tout de suite c et d ; on obtient

$$c = \frac{(x,x)|X|}{n} \quad \text{et} \quad d = \frac{3(x,x)^2|X|}{n(n+2)}\,.$$

En résumé, on a les deux identités

$$\sum_{x\in X}(x,\alpha)^2 = \frac{(x,x)|X|}{n}\,(\alpha,\alpha) \tag{5.2 a}$$

$$\sum_{x\in X}(x,\alpha)^4 = \frac{3(x,x)^2|X|}{n(n+2)}\,(\alpha,\alpha)^2\,. \tag{5.2 b}$$

On va maintenant considérer le cas des systèmes de racines, dont nous rappelons ci-dessous la définition et quelques propriétés. Pour $x \in E$ non nul, soit σ_x la réflexion orthogonale d'hyperplan orthogonal à x.

DÉFINITION 5.3. Un *système de racines* est une partie R d'un espace euclidien E, telle que:

(1) R est finie, engendre E et ne contient pas 0.

(2) Pour tout $r \in R$, R est stable par σ_r.

(3) Quels que soient $x, y \in R$, $2\dfrac{(x,y)}{(x,x)} \in \mathbb{Z}$.

La dimension n de E s'appelle le *rang de* R.

On ne considère dans la suite que des systèmes à une seule norme ("simply laced systems"), que l'on normalise à la norme 2.

Les systèmes de racines sont évidemment stables par $x \mapsto -x$; le nombre de racines est donc pair, soit $|R| = 2s$. Le *groupe d'automorphismes* d'un système R est $\mathrm{Aut}(R) = \{\sigma \in \mathrm{O}(E) \mid \forall\, r \in R,\, \sigma(r) \in R\}$, et le *groupe de Weyl de* R est le sous-groupe $W(R)$ du précédent engendré par les σ_r, $r \in R$; ce sont des groupes finis.

Les systèmes *irréductibles* (ceux qui ne sont pas réunion de deux systèmes d'une somme directe orthogonale de sous-espaces de E) se répartissent alors en *deux séries infinies* et *trois systèmes exceptionnels*, à savoir

$$\boldsymbol{A}_n\ (n \geq 1)\,, \quad \boldsymbol{D}_n\ (\geq 4)\,, \quad \boldsymbol{E}_n\ (n = 6, 7, 8)\,,$$

systèmes que nous décrivons ci-dessous.

Pour définir la première série, on prend pour E l'hyperplan d'équation $\sum_{i=0}^{n} x_i = 0$ de $\mathbb{R}^{n+1}$. Notant $(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_n)$ la base canonique de $\mathbb{R}^{n+1}$, on pose

$$\boldsymbol{A}_n = \{\pm(\varepsilon_i - \varepsilon_j),\ 0 \leq i < j\}\,.$$

Dans les autres cas, on prend $E = \mathbb{R}^n$, muni de sa base canonique $(\varepsilon_1, \ldots, \varepsilon_n)$. On pose

$$\boldsymbol{D}_n = \{\pm(\varepsilon_i \pm \varepsilon_j),\ 1 \leq i < j \leq n\}\,,$$

puis

$$\boldsymbol{E}_8 = \boldsymbol{D}_8 \cup \left\{\tfrac{\pm\varepsilon_1 \pm \cdots \pm \varepsilon_8}{2}\right\}$$

en se limitant ci-dessus aux sommes ayant un nombre pair de signes $-$,

et l'on définit enfin $\boldsymbol{E}_7$ et $\boldsymbol{E}_6$ comme sections de $\boldsymbol{E}_8$ par

$$\boldsymbol{E}_7 = \boldsymbol{E}_8 \cap (\varepsilon_7 - \varepsilon_8)^{\perp} \quad \text{et} \quad \boldsymbol{E}_6 = \boldsymbol{E}_7 \cap (\varepsilon_6 - \varepsilon_7)^{\perp}\,.$$

Dans tous les cas, on constate que R est un ensemble de vecteurs de norme 2, dont les produits scalaires mutuels sont à valeurs dans $\{\pm 2, \pm 1, 0\}$. Il en résulte que le sous-groupe de E engendré par un système de racines R du type ci-dessus est un réseau (pair) dont R est l'ensemble des vecteurs minimaux (on dit que c'est un *réseau de racines*), et que n divise $2s$, ce qui justifie la définition suivante :

DÉFINITION 5.4. Le *nombre de Coxeter de* R, supposé irréductible, est l'entier $h = \dfrac{2s}{n}$.

[Plus intrinsèquement, on pourrait définir h comme l'ordre d'une classe de conjugaison de $W(R)$, cf. [Bou], ch. V, § 6, n° 1.]

On vérifie sur la classification que $W(R)$ opère transitivement sur R. Il en résulte que, étant donnnée une racine r, les nombres n_0 et n_1 de racines r' avec respectivement $(r,r')=0$ et $(r,r')=1$ sont indépendants de r. On a évidemment la relation $n_0+2n_1=2s-2$, mais on peut aussi faire intervenir le nombre de Coxeter, comme le montre la proposition suivante bien connue (cf. Bourbaki ([Bou]), Lie VI, §1.11, prop. 3.2), que l'on peut également vérifier cas par cas:

PROPOSITION 5.5. *Soit R un système de racines (à une seule norme) irréductible. Alors:*

(1) $n_1=2h-4$.

(2) Pour tout $x\in E$, $\sum_{r\in R}\dfrac{(x,r)^2}{(r,r)}=h\,(x,x)$.

Tableau 5.6. Invariants des systèmes de racines

nom	rang	$\lvert R\rvert=2s$	n_0	n_1	h	$\lvert W\rvert$
$\boldsymbol{A}_n$	$n\geq 1$	$n(n+1)$	$(n-1)(n-2)$	$2(n-1)$	$n+1$	$(n+1)!$
$\boldsymbol{D}_n$	$n\geq 4$	$2n(n-1)$	$2(n^2-5n+7)$	$4(n-2)$	$2(n-1)$	$2^{n-1}.n!$
$\boldsymbol{E}_6$	6	72	30	20	12	$2^7.3^4.5$
$\boldsymbol{E}_7$	7	126	60	32	18	$2^{10}.3^4.5.7$
$\boldsymbol{E}_8$	8	240	126	56	30	$2^{14}.3^5.5^2.7$

La proposition 5.5, (2) montre (en utilisant 5.2 a) que les systèmes de racines "sphériques" irréductibles sont des 3-designs. L'énoncé suivant précise ceux qui sont des 5-designs (ou des 4-designs, cela revient au même):

THÉORÈME 5.7. *Les systèmes de racines qui sont des 5-designs sont irréductibles, et semblables à $\boldsymbol{A}_1$, $\boldsymbol{A}_2$, $\boldsymbol{D}_4$, $\boldsymbol{E}_6$, $\boldsymbol{E}_7$, $\boldsymbol{E}_8$. En outre, $\boldsymbol{E}_8$ est un 7-design.*

Démonstration. Soit R un système de racines qui est un 5-design. Le point crucial est la démonstration de l'irréductibilité. Il s'agit là d'un résultat qui s'applique à tous les réseaux parfaits (voir §6), et qui se

démontre en utilisant l'identité 6.5, que nous admettons provisoirement :

$$(*) \qquad \sum_{x\in X}(x,\alpha_1)^2(x,\alpha_2)^2 = \frac{(x,x)^2|X|}{n(n+2)}\left[2(\alpha_1,\alpha_2)^2+(\alpha_1,\alpha_1)(\alpha_2,\alpha_2)\right].$$

Si $R = R_1 \perp R_2$, on applique $(*)$ en prenant $\alpha_1 \in R_1$ et $\alpha_2 \in R_2$. Le membre de gauche est alors nul, alors que celui de droite ne l'est pas, étant égal à $\frac{2^4|R|}{n(n+2)}$.

Le système R est donc irréductible. Si l'on prend pour α dans 5.2 a une racine r_0, on voit en utilisant 5.5 (1) que le nombre de Coxeter h de R est tel que $|X| = nh$. Toujours en utilisant 5.5, (1), on voit que le premier membre de 5.2 b vaut $2(2^4 + n_1) = 4(h+6)$. En remplaçant $|X|$ par nh dans le second membre, on obtient la relation

$$(10-n)h = 6(n+2)\,, \tag{5.8}$$

qui entraîne la majoration $n \leq 9$, et montre l'impossibilité des valeurs $n = 3$ et $n = 5$ (parce que $10 - n$ ne divise alors pas $6(n+2)$), ainsi que celle de $n = 9$, qui entraînerait $h = 66$, alors que l'on a $h(\boldsymbol{A}_9) < h(\boldsymbol{D}_9) = 16$. Ainsi, n doit prendre l'une des valeurs de l'énoncé, et la valeur de h fournie par 5.8 impose que le système soit celui qui est décrit dans l'énoncé.

Il faut maintenant vérifier l'identité 5.2 b dans chacun des 6 cas de l'énoncé.

C'est évident dans le cas de $\boldsymbol{A}_1$, et c'est une conséquence de la proposition 4.2 dans le cas de $\boldsymbol{A}_2$.

Dans le cas de $\boldsymbol{D}_4$, cela résulte de l'identité

$$6(X_1^2+X_2^2+X_3^2+X_4^2)^2 = \sum_{1\leq i<j\leq 4}(X_i \pm X_j)^4\,,$$

utilisée par Liouville en 1859 pour prouver la majoration $g(4) \leq 53$ dans le problème de Waring[1]) (cf. Hardy and Wright, *An introduction to the theory of numbers*, Clarendon Press, Oxford, section 21.1; fifth edition: 1979), puis plus tard par Lucas en 1876.

Les calculs explicites dans le cas des systèmes exceptionnels sont beaucoup plus compliqués; on les évite en utilisant la théorie des invariants dans les cas de la représentation (absolument irréductible) de $W(R)$ opérant sur E. Les polynômes invariants sont engendrés dans chacun des trois cas

[1]) Des travaux récents sur $g(4)$ et $G(4)$ ont utilisé des identités associées aux structures de 5-design portées par $\boldsymbol{A}_2$, $\boldsymbol{D}_4$ et $\boldsymbol{E}_6$.

par n *polynômes homogènes fondamentaux*, dont les degrés (les *degrés fondamentaux*) sont les suivants:

$\boldsymbol{E}_6$: $2, 5, 6, 8, 9, 12$;

$\boldsymbol{E}_7$: $2, 6, 8, 10, 12, 14, 18$;

$\boldsymbol{E}_8$: $2, 8, 12, 14, 18, 20, 24, 30$.

[Le degré 2 provient du polynôme (α, α) ; le plus grand degré est le nombre de Coxeter.]

Vu que les polynômes $\sum_{x \in R}(x, \alpha)^{2k}$ sont invariants par $W(R)$, l'absence du degré 4 dans les listes ci-dessus entraîne que les polynômes invariants de degré 4 sont proportionnels à $(\alpha, \alpha)^2$, ce qui montre que les systèmes exceptionnels définissent des 4-designs, donc des 5-designs, et l'absence du degré 6 dans le cas de $\boldsymbol{E}_8$ montre de même que $\boldsymbol{E}_8$ est un 7-design. □

[Variantes de démonstration: le fait que la liste des systèmes qui sont des 5-designs soit limitée aux 6 systèmes de l'énoncé peut se voir en utilisant l'invariant γ', cf. définition 10.2 et théorème 10.4; le fait que les systèmes de l'énoncé soient effectivement des 5-designs, mais non des 6-designs (sauf dans le cas de $\boldsymbol{E}_8$) peut se faire "à la main" en utilisant le corollaire 8.3 et les données contenues dans le tableau 5.6. Le calcul explicite conduit à des formules du type de la formule 5.10 ci-dessous.]

REMARQUE 5.9. Écartons le cas trivial de la dimension 1. Les valeurs $t = 5$ (dans les cas $R \neq \boldsymbol{E}_8$) et la valeur $t = 7$ dans le cas $R = \boldsymbol{E}_8$ sont les plus grandes possibles. Pour $R \neq \boldsymbol{E}_8$, cela se voit en cherchant une relation de la forme $\sum_{x \in X}(x, \alpha)^6 = e(\alpha, \alpha)^3$. En appliquant Δ_α selon les formules de l'exemple 1.5, on transforme le premier membre en $30 \sum_{x \in X}(x, x)(x, \alpha)^4$. En remplaçant $\sum(x, \alpha)^4$ par sa valeur tirée de 5.2 b, on en déduit e, obtenant finalement la formule

$$(*) \qquad \sum_{x \in X}(x, \alpha)^6 = \frac{15(x, x)^3 |X|}{n(n+2)(n+4)}(\alpha, \alpha)^3 .$$

En évaluant $(*)$ en un élément $\alpha = r \in R$ et en utilisant l'égalité $|R| = nh$, on obtient la relation

$$(5.10) \qquad h + 30 = \frac{240h}{(n+2)(n+4)} ,$$

qui n'est correcte que pour $n = 8$ (et $n = 1$). On montre de façon analogue que $\boldsymbol{E}_8$ n'est pas un 8-design; voir aussi [M1], où sont classés les réseaux qui définissent des 7-designs.

6. Les réseaux fortement parfaits.

La notion de réseau fortement parfait introduite dans ce § est un renforcement de notions étudiées par l'école russe entre 1873 et 1908, dont les deux contributions les plus importantes pour ce qui nous concerne ici sont les articles de Korkine et Zolotareff ([K-Z], 1877) et de Voronoï ([Vo], 1908).

Étant donné un réseau L dans un espace euclidien E de dimension n, on appelle *norme* (ou) *minimum de* L le nombre $N(L) = \min_{x \in L \smallsetminus \{0\}}(x, x)$ et *déterminant de* L le déterminant $\det(L)$ de la matrice de Gram d'une base de L ; l'*invariant d'Hermite de* L est $\gamma(L) = \dfrac{N(L)}{\det(L)^{1/n}}$. Les vecteurs $x \in L$ tels que $N(x) = N(L)$ sont appelés *vecteurs minimaux* ou *vecteurs courts* de L. Leur ensemble est noté $S(L)$, ou S, ou parfois X, et l'on pose $s(L) = s = \frac{1}{2}|S(L)|$.

Rappelons (Korkine et Zolotareff, [K-Z2], [K-Z3]) qu'un réseau L est dit *extrême* s'il réalise un maximum local de l'invariant d'Hermite. Les réseaux extrêmes ont été caractérisés par Voronoï comme les réseaux parfaits et eutactiques. Ces notions possèdent de nombreuses définitions équivalentes, cf. [M], ch. III, § 3, dont nous retiendrons les suivantes, qui sont les mieux adaptées à notre sujet : soit L un réseau, dont on note X l'ensemble des vecteurs minimaux. On dit que L est *eutactique* s'il existe des *coefficients d'eutaxie* λ_x, $x \in X$, strictement positifs tels que l'on ait la relation

$$N(\alpha) = \sum_{x \in X/\{\pm 1\}} \lambda_x (x, \alpha)^2$$

quel que soit $\alpha \in E$, et que L est *parfait* si l'ensemble des polynômes $\rho_x^{(2)} : \alpha \mapsto (x, \alpha)^2$, $x \in X$ engendre $\mathcal{F}_{n,2}$.

Définition 6.1. On dit qu'un réseau est *fortement eutactique* s'il est eutactique avec des coefficients d'eutaxie égaux.

C'est par exemple le cas des réseaux qui possédent des coefficients d'eutaxie et dont le groupe des automorphismes opère transitivement sur

l'ensemble des vecteurs minimaux, ou encore dont la représentation du groupe d'automorphismes opérant sur E est $\mathbb{R}$-irréductible. Ces réseaux font l'objet d'un étude détaillée dans [M-V] (ce volume).

PROPOSITION 6.2. *Pour qu'un réseau L soit fortement eutactique, il faut et il suffit que l'ensemble X de ses vecteurs minimaux soit un 3-design (ou un 2-design, cela revient au même). Les coefficients d'eutaxie sont alors égaux à* $\dfrac{n}{N(L)\,|X|}$.

Démonstration. En effet, il résulte du théorème 3.2 que les 3-design sphériques sont précisément les ensembles X pour lesquels (α,α) est proportionnel à $\sum_{x\in X}(x,\alpha)^2$, le coefficient de proportionalité étant donné par la formule 5.2 a. □

Nous en venons maintenant à la notion centrale de ce cours :

DÉFINITION 6.3. On dit qu'un réseau est *fortement parfait* si l'ensemble X de ses vecteurs minimaux est un 5-design sphérique.

Il revient au même de dire que X est un 4-design sphérique, ou encore que X satisfait la formule 5.2 b.

THÉORÈME 6.4. *Un réseau fortement parfait est extrême et fortement eutactique.*

Démonstration. Soit L un tel réseau. L'ensemble X de ses vecteurs minimaux vérifie la formule 5.2 b, donc aussi la formule 5.2 a, dont la proposition 6.2 montre qu'elle entraîne l'eutaxie forte. Compte tenu du théorème de Voronoï rappelé au début du §, il suffit maintenant de prouver que L est parfait.

On considère l'espace $V = \mathcal{F}_{n,2}$ muni du produit scalaire $[\,,\,]$ défini au début du §1. On a $[\rho^{(2)}_{x_1}, P] = P(x_1)$ quel que soit le polynôme P de degré 2 ; appliquée à $P = \rho^{(2)}_{x_2}$, cette formule devient $[\rho^{(2)}_{x_1}, \rho^{(2)}_{x_2}] = (x_1,x_2)^2$. On est donc ramené à montrer que la matrice G (de taille $|X|\times|X|$) ayant pour coefficients $g_{i,j} = (x_i,x_j)^2$ est de rang $\frac{n(n+1)}{2}$. On va démontrer ce résultat en prouvant que les valeurs propres non nulles de G (comptées avec leurs multiplicités) sont au nombre de $\frac{n(n+1)}{2}$.

Dans les calculs qui suivent, F désigne la matrice de taille $|X|\times|X|$ dont tous les coefficients sont égaux à 1.

Soient $\alpha_1, \alpha_2 \in \mathbb{R}^n$. Considérons les vecteurs de la forme $\alpha' = \xi\alpha_1 + \eta\alpha_2$, $\xi, \eta \in \mathbb{R}$, et appliquons-leur l'identité 5.2 b. Le coefficient de $\xi^2\eta^2$ est $\frac{4!}{2!2!}\sum(x,\alpha_1)^2(x,\alpha_2)^2$ dans le membre de gauche et le produit $\frac{3(x,x)^2|X|}{n(n+2)}\cdot\left(2^2(\alpha_1,\alpha_2)^2+2(\alpha_1,\alpha_1)(\alpha_2,\alpha_2)\right)$ dans le membre de droite, d'où l'on déduit l'identité

$$\sum_{x\in X}(x,\alpha_1)^2(x,\alpha_2)^2 = \frac{(x,x)^2|X|}{n(n+2)}\left[2(\alpha_1,\alpha_2)^2+(\alpha_1,\alpha_1)(\alpha_2,\alpha_2)\right]. \tag{6.5}$$

En choisissant alors $\alpha_1 = x_1$ et $\alpha_2 = x_2$, $x_1, x_2 \in X$, on obtient l'équation

$$G^2 = aG + bF \tag{6.6}$$

dans laquelle on a posé

$$a = \frac{2(x,x)^2|X|}{n(n+2)} \quad \text{et} \quad b = \frac{(x,x)^4|X|}{n(n+2)}. \tag{6.6'}$$

En exprimant F en fonction de G par 6.6, on obtient les relations

$$GF = FG = cF \quad \text{avec} \quad c = \frac{(x,x)^2|X|}{n}. \tag{6.7}$$

Comme F et G commutent, on peut les "diagonaliser simultanément", obtenant des matrices

$$F' = \begin{pmatrix} |X| & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix} \quad \text{et} \quad G' = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_{|X|} \end{pmatrix}.$$

L'équation 6.7 entraîne la relation $\lambda_1 = c$. En utilisant 6.5, on obtient $\lambda_i^2 = a\lambda_i$ pour $2 \le i \le |X|$, donc $\lambda_i = 0$ ou $\lambda_i = a$. Notons t le nombre d'indices $i \ge 2$ pour lesquels $\lambda_i = a$. En comparant les valeurs de la trace de G calculées avec la définition de G et avec la forme diagonale ci-dessus, on obtient l'égalité $(x,x)^2|X| = c + ta$ qui, en remplaçant a et c par leurs valeurs tirées de 6.6' et de 6.7, devient $1 = \frac{1}{n} + \frac{2t}{n(n+2)}$, d'où $t = \dfrac{(n-1)(n+2)}{2}$. Le nombre de valeurs propres non nulles de G est donc $t+1 = \dfrac{n(n+1)}{2}$. $\square$

La démonstration matricielle donnée ci-dessus sert de modèle pour certaines démonstrations à venir. Voici une démonstration plus directe du théorème 6.7, due à Thierry Vust.

Il s'agit de prouver qu'un réseau fortement parfait est parfait. Pour cela, on démontre qu'un polynôme P orthogonal à tous les $\rho_x^{(2)}$, $x \in X$, est nul. Pour $x \in X$, on a $P(x) = [\rho_x^{(2)}, P] = 0$. Si maintenant X est un 4-design, on a

$$\int_{S^{n-1}} P^2 \, dx = \frac{1}{|X|} \sum_{x \in X} P(x)^2 = 0$$

d'où $P = 0$, puisque P est une fonction continue.

REMARQUE 6.8. Les notions de perfection et d'eutaxie fortes, tout comme les notions usuelles, ne font intervenir que l'ensemble des vecteurs minimaux du réseau. Ainsi, si L est fortement parfait, tout réseau $L' \supset L$ ayant même ensemble de vecteurs minimaux que L est également fortement parfait.

REMARQUE 6.9. Comme les réseaux parfaits dont ils sont un cas particulier, les réseaux fortement parfaits possèdent les trois propriétés suivantes :

(1) $S(L)$ engendre E.

(2) L est irréductible.

(3) L est rationnel, c'est-à-dire proportionnel à un réseau entier.

Commentaires.

(1) Découle de la simple existence de coefficients d'eutaxie, sans restriction sur le signe, et est en particulier vérifiée par les réseaux fortement eutactiques.

(2) Résulte simplement du fait que la dimension de l'espace engendré par les $\rho_x^{(2)}$, $x \in S(L)$ est strictement inférieure à $\dim \mathcal{F}_{n,2} = \frac{n(n+1)}{2}$ dans le cas d'un réseau réductible. Ce *n'est pas* une conséquence de la forte eutaxie.

(3) Il s'agit d'un théorème de Korkone et Zolotareff. On démontre dans [M-V] que cette propriété est vérifiée par les réseaux fortement eutactiques. (Toutefois, elle n'est pas entraînée par l'eutaxie.)

On montre (Bergé et Martinet, cf. [M], chapitre IX) que les classes de similitude de réseaux *faiblement eutactiques* (c'est-à-dire possédant des coefficients d'eutaxie) sont en nombre fini, résultat dû à Voronoï dans le cas des réseaux parfaits et à Ash dans le cas des réseaux eutactiques. Cette propriété suggère d'essayer de classer les réseaux fortement parfaits entiers

de dimension donnée, une question sur laquelle nous reviendrons dans la suite.

La propriété (3) ci-dessus suggère de classer également les réseaux fortement parfaits de minimum donné.

Le cas du minimum 1 est évident, le seul réseau entier irréductible de minimum 1 étant $\mathbb{Z}$; c'est en effet un résultat général qu'un plongement isométrique $L \mapsto L'$ avec L unimodulaire induit une isométrie $L' \simeq L \perp L^{\perp}$, et, dans le cas de $L = \mathbb{Z}$, c'est évident en utilisant le lemme suivant, facile, mais d'usage constant :

LEMME 6.10. *Soit L un réseau et soient x et y deux vecteurs non nuls et non proportionnels de L. Alors,*

(1) Si x est minimal, on a $|(x,y)| \leq \frac{1}{2}N(y)$.

(2) Si x et y sont minimaux, on a $|(x,y)| \leq \frac{1}{2}N(L)$.

Démonstration. On a $N(x \pm y) - N(x) = N(y) \pm 2(x,y) \geq 0$, d'où $\mp(x,y) \leq \frac{1}{2}N(y)$. □

Les résultats du § précédent permettent de résoudre tout de suite le cas du minimum 2 (on note $\mathbb{A}_n$, $\mathbb{D}_n$, $\mathbb{E}_n$ le réseau engendré par le système de racines respectifs $\boldsymbol{A}_n$, $\boldsymbol{D}_n$, $\boldsymbol{E}_n$) :

THÉORÈME 6.11. *Un réseau entier fortement parfait de minimum 2 est isométrique à l'un des réseaux de racines $\mathbb{A}_1$, $\mathbb{A}_2$, $\mathbb{D}_4$, $\mathbb{E}_6$, $\mathbb{E}_7$ ou $\mathbb{E}_8$.*

Démonstration. Soit Λ un tel réseau. Le sous-réseau L' de L engendré par $S(L)$ est lui aussi fortement parfait et de même rang n que L. Étant engendré par par des vecteurs de norme 2, L' est un réseau de racines, dont le théorème 5.7 montre qu'il est isométrique à l'un des six réseaux $\mathbb{A}_1$, $\mathbb{A}_2$, $\mathbb{D}_4$, $\mathbb{E}_6$, $\mathbb{E}_7$ ou $\mathbb{E}_8$. On a $\det(L') = \det(L)\,[L : L']^2$. Comme $[L''L']^2$ doit diviser $\det(L')$, les seules possibilités sont $L = L'$, ou $n = 4$, $L' = \mathbb{D}_4$ et $[L : L'] = 2$. On exclut ce dernier cas en observant que L devrait être alors unimodulaire, donc isométrique au réseauréductible $\mathbb{Z}^4$.

Le cas du minimum 3 est l'objet du § suivant. La classification n'est pas connue au-delà; voir toutefois [M1] pour le cas de certains designs supérieurs.

En examinant la liste des 48 réseaux parfaits (dont 44 sont extrêmes) de dimension $n \leq 7$, on démontre :

THÉORÈME 6.12. *Un réseau fortement parfait de dimension $n \leq 7$ est semblable à l'un des 7 réseaux $\mathbb{A}_1 \sim \mathbb{Z}$, $\mathbb{A}_2$, $\mathbb{D}_4$, $\mathbb{E}_6$, $\mathbb{E}_6^*$, $\mathbb{E}_7$ ou $\mathbb{E}_7^*$.* □

La liste des réseaux parfaits ainsi que celle de leurs principaux invariants peut être lue dans [C-S1] ou dans [M], chapitre VI; la confirmation du caractère exhaustif de cette liste a été faite par Jaquet dans sa thèse, résumée dans [J].

La démonstration du théorème 6.12 est grandement facilitée par deux résultats que nous prouverons plus loin :

(1) Une condition nécessaire pour qu'un réseau L soit fortement parfait est que l'inégalité $N(L)N(L^*) \geq \frac{n+2}{3}$ soit satisfaite (théorème 10.4 et proposition 10.8 ci-après). L'examen des 48 réseaux parfaits de dimension $n \leq 7$ prouve que seuls les 7 réseaux ci-dessus vérifient cette condition. (Il y a même égalité; on dit alors que ces réseaux fortement parfaits sont *de type minimal*, cf. § 10.)

(2) Les méthodes du § 8 permettent de laisser à un ordinateur le soin de déterminer les valeurs de t pour lesquelles un réseau donné est un t-design sphérique (tout au moins, si la dimension n'est pas excessive). Comme les groupes d'automorphismes des 7 réseaux ci-dessus opèrent transitivement sur leurs ensembles de vecteurs minimaux, il suffit ici d'appliquer le corollaire 8.3, ce qui peut se faire facilement "à la main".

En outre, du fait que ces réseaux sont de type minimal, la proposition 10.12 entraîne que leurs ensembles de vecteurs minimaux ne sont pas des 6-designs.

7. Les réseaux fortement parfaits de minimum 3.

Pour décrire la classification de ces réseaux, nous devons décrire pour certaines dimensions $n \leq 23$ des réseaux, que nous notons O_n, notation qui n'est classique que pour $n = 23$. Le lemme suivant peut être extrait de [M], ch. 5, § 7:

LEMME 7.1. *Soit Λ un réseau entier pair de dimension $n \geq 2$ et de minimum 4, et soit e un vecteur minimal de Λ. Notons p la projection orthogonale sur l'hyperplan $H = e^\perp$, posons $\Lambda'_e = \{x \in \Lambda \mid (e,x) \equiv 0 \mod 2\}$, et soit $\Lambda_e = p(\Lambda'_e)$. Supposons vérifiée l'une des deux hypothèses suivantes :*

(1) Il existe $x \in \Lambda$ *avec* $(e,x) \equiv 1 \mod 2$ *;*

(2) On a $(y,e) \equiv 0 \mod 2$ *pour tout* $y \in \Lambda$*, et* Λ *contient un vecteur* x *avec* $(e,x) \equiv 2 \mod 4$*. Alors,* Λ_e *est un réseau entier impair de minimum au moins* 3*, et l'on a* $\det(\Lambda_e) = \det(\Lambda)$ *sous l'hypothèse (1) et* $\det(\Lambda_e) = \frac{1}{4}\det(\Lambda)$ *sous l'hypothèse (2).*

Démonstration. Comme $x \in E$ se projette sur $\mathbb{R}e$ en $\dfrac{(e,x)}{(e,e)}e$, on a $p(x) = x - \dfrac{(e,x)}{(e,e)}e$, d'où, quels que soient $x, y \in E$,

$$(p(x),p(y)) = (x,y) - \frac{(e,x)(e,y)}{(e,e)} = (x,y) - \frac{(e,x)(e,y)}{4} \tag{7.2}$$

Comme les produits scalaires (x,e) sont pairs pour $x \in \Lambda'_e$, Λ_e est entier. En outre, Λ'_e contient des vecteurs x avec $(e,x) \equiv 2 \mod 4$ (sous l'hypothèse (1), prendre $x = 2y$ avec (y,e) impair), et, pour un tel vecteur, $N(p(x)) = N(x) - \dfrac{(e,x)^2}{4}$ est impair. Le lemme 6.10 montre que l'on a $|(e,x)| \leq \frac{1}{2}N(x)$ pour tout $x \in \Lambda$ non colinéaire à e, d'où $N(p(x)) = N(x) - \dfrac{(e,x)^2}{4} \geq \dfrac{3}{4}N(x) \geq 3$.

Il reste à calculer le déterminant de Λ_e. Or, vu que l'on obtient Λ_e en projetant Λ'_e parallèlement à e, on a $\det(\Lambda'_e) = \det(\mathbb{Z}e)\det(\Lambda_e)$, donc $\det(\Lambda_e) = \dfrac{\det(\Lambda'_e)}{4}$, ce qui est bien le résultat annoncé, car Λ'_e est d'indice 2 dans Λ sous l'hypothèse (1) et égal à Λ sinon. □

En pratique, on considère des réseaux Λ tels que Λ'_e contient un vecteur x minimal avec $(e,x) = 2$, et l'on a alors $N(\Lambda_e) = 3$. C'est ce qui se passe dans le cas des *réseaux laminés* de Conway et Sloane ([C-S], ch. 6; voir aussi plus loin, §19) pour $2 \leq n \leq 24$. Rappelons que ces réseaux sont de minimum 4, uniques à isométrie près sauf en dimensions $11, 12, 13$, que Λ_n est isométrique à $\sqrt{2}\,\mathbb{E}_n$ pour $n = 6, 7, 8$, que Λ_{24} est le *réseau de Leech*, l'unique réseau unimodulaire de dimension 24 et de minimum 4 (théorème de Conway), et que Λ_8 se plonge dans Λ_{24} de façon unique à automorphisme près de Λ_{24}. Son orthogonal est alors le réseau Λ_{16}, isométrique au réseau BW_{16} de Barnes-Wall (l'orthogonal dans Λ_{24} de Λ_n est isométrique à Λ_{24-n}). Ce dernier réseau est 2-*modulaire* (i.e. il existe une similitude de rapport $\sqrt{2}$ de Λ_{16}^* sur Λ_{16}).

Pour $n \leq 8$, $n = 16$ et $n = 24$ (entre autres), le groupe $\mathrm{Aut}(\Lambda_n)$ opère transitivement sur l'ensemble des vecteurs minimaux. Il en résulte

que le réseau Λ_e qui lui est associé est défini à isométrie près par la donnée de Λ_n.

Notons enfin que le plongement de $\Lambda_8 \simeq \sqrt{2}\,\mathbb{E}_8$ dans Λ_{24} définit un plongement des réseaux projetés Λ_e correspondants.

DÉFINITION 7.3. On pose $O_1 = \sqrt{3}\,\mathbb{Z}$. On note O_7 (resp. O_{23}) le projeté Λ_e associé à Λ_8 (resp. à Λ_{24}). On note enfin O_{22} (resp. O_{16}) l'orthogonal de O_1 (resp. O_7) dans O_{23}.

Ce que l'on sait des réseaux laminés garantit que les réseaux de la définition 7.3 sont uniques à isométrie près. Le lemme 7.1 montre que ces réseaux sont entiers de minimum 3, que O_{23} est unimodulaire et que O_7 est de déterminant 64 ; on a donc aussi $\det(O_{16}) = 64$.

On peut être plus précis.

La règle selon laquelle "la projection du dual est le dual de la section" (cf. [M], ch. I, prop. 3.4) montre que l'on a

$$O_7^* = p(\Lambda_8)^* = \Lambda_8^* \cap H = \frac{1}{2}\Lambda_8 \cap H = \frac{1}{2}\Lambda_7 \simeq \frac{1}{\sqrt{2}}\,\mathbb{E}_7\,.$$

On a donc $O_7 \simeq \sqrt{2}\,\mathbb{E}_7^*$, et O_7 s'obtient à partir de $\sqrt{2}\,\mathbb{E}_7 \simeq \Lambda_7$ par adjonction d'un vecteur de norme 3 de Λ_7^*.

De la même façon, O_{16} s'obtient par adjonction à Λ_{16} d'un vecteur de norme 3 de Λ_{16}^*. Comme Λ_8 et Λ_{16} sont 2-modulaires, les quotients O_n/O_n^* sont 2-élémentaires pour $n = 7$ et $n = 16$, alors que O_{22} est de déterminant 3. En fait, Λ_7, Λ_{16}, Λ_{22} et Λ_{23} sont les réseaux pairs associés respectivement à O_7, O_{16}, O_{22} et O_{23}.

[Toutefois, contrairement à ce qui est écrit dans la préface à la deuxième édition de [C-S], on n'obtient pas un réseau de déterminant 64 par projection de Λ_{17}.]

Il est important de connaître le nombre de vecteurs minimaux de chacun de ces réseaux. On a $s(O_1) = 1$, $s(O_7) = 28$, $s(O_{16}) = 256$, $s(O_{22}) = 1408$ et $s(O_{23}) = 2300$.

Signalons que les réseaux O_n construits par Rains et Sloane dans [R-S] ne sont pas les réseaux O_n ci-dessus.

THÉORÈME 7.4. *Les réseaux fortement parfaits qui sont entiers et de minimum 3 sont O_1, O_7, O_{16}, O_{22} et O_{23}.*

Démonstration. Soit Λ un réseau entier de minimum 3, et soit X l'ensemble de ses vecteurs minimaux. On va appliquer les identités 5.2

en prenant $\alpha = x_0 \in X$. Soit $n_i = |\{x \in X \mid (x_0, x) = i\}|$; on a $|X| = 2 + n_0 + 2n_1$. Les identités 5.2 s'écrivent

$$3^2 + n_1 = \frac{3^2|X|}{2n} \tag{7.5 a}$$

$$3^4 + n_1 = \frac{3^5|X|}{2n(n+2)}\,, \tag{7.5 b}$$

d'où, par différence,

$$\frac{25-n}{2n(n+2)}|X| = 8\,. \tag{7.6}$$

On a donc $n \leq 24$, et les relation de divisibilité imposées par 7.6 et 7.5 a permettent de restreindre n à la liste

$$n = 1, 7, 13, 16, 17, 19, 21, 22, 23, 24\,, \tag{7.7}$$

valeurs pour lesquelles les équations 7.5 ont une solution en entiers $n, |X|, n_1 > 0$. On constate que

$$\frac{|X|}{2n} = \frac{8(n+2)}{25-n} \quad \text{et} \quad n_1 = 81\frac{n-1}{25-n} \tag{7.8}$$

sont bien dans tous les cas des entiers positifs.

Notons Y l'ensemble des vecteurs de Λ de norme 4.

Lemme 7.9.

(1) Quels que soient $x \in X$ et $y \in Y$, on a $(x, y) \in \{0, \pm 1, \pm 2\}$.

(2) Soit $y_0 \in Y$. Alors, le nombre d'éléments $x \in X$ avec $(x, y_0) = 2$ est

$$m_2 = \frac{34-n}{n+2}\,\frac{|X|}{2n} = 8\,\frac{34-n}{25-n}\,.$$

(3) On a $n_1|X| = m_2|Y|$.

Démonstration. (1) est une conséquence immédiate du lemme 6.10.

(2) Pour $i = 0, 1, 2$, soit $m_i = |\{x \in X \mid (y_0, x) = i\}|$. Les équations 5.2, appliquées avec $\alpha = y_0 \in Y$, expriment m_1 et m_2 comme solutions d'un système de Cramer permettant de vérifier tout de suite que m_2 a la valeur donnée dans (2).

(3) Le nombre de couples d'éléments $x_0, x_1 \in X$ avec $(x_0, x_1) = 1$ est égal à $n_1|X|$. Mais, si $(x_0, x_1) = 1$, pour $y = x_0 - x_1$, on a $(y, y) = 4$ et $(x_0, y) = 2$. Réciproquement, si $y \in Y$ et si $x_0 \in X$ est tel que $(x_0, y) = 2$, alors, pour $x_1 = x_0 - y$, on a $(x_0, x_1) = 1$. On a ainsi mis en bijection l'ensemble des couples x, x' de $X \times X$ vérifiant $(x, x') = 1$ avec l'ensemble des couples x, y de $X \times Y$ vérifiant $(x, y) = 2$. □

En tirant n_1 et $|X|$ de 7.8 et m_2 de 7.9, (2), on déduit de 7.9, (3) l'égalité

$$|Y| = 2.3^4 \frac{n(n-1)(n+2)}{(25-n)(34-n)}.$$

Comme $|Y|$ doit être entier, on élimine de la liste 7.7 les valeurs $n = 13, 19, 21, 24$, restreignant les dimensions *a priori* possibles à

$$n = 1, 7, 16, 17, 22, 23. \tag{7.10}$$

LEMME 7.11. *Si Λ n'est pas unimodulaire, on a $n \equiv 1 \mod 3$, et Λ^* est de minimum $\dfrac{n+2}{9}$.*

Démonstration. Par hypothèse, l'inclusion $\Lambda^* \supset \Lambda$ est stricte. Considérons une classe non nulle c de Λ^* modulo Λ, et choisissons dans c un élément t de norme minimale. L'argument utilisé pour démontrer le lemme 6.10 montre que, pour tout $x \in X$, on a $|(t,x)| \leq \dfrac{(x,x)}{2} = \dfrac{3}{2}$. Soit $p_1 = |\{x \in X \mid (t,x) = 1\}|$. Les formules 5.2 s'écrivent alors

$$2p_1 = 6\frac{|X|}{2n}(t,t) \quad \text{et} \quad 2p_1 = 54\frac{|X|}{2n}\frac{(t,t)^2}{n+2}$$

et ont pour unique solution

$$(t,t) = \frac{n+2}{9}, \quad p_1 = \frac{n+2}{3}\frac{|X|}{2n} = \frac{8(n+2)^2}{3(25-n)}.$$

Le fait que p_1 soit entier équivaut à $n \equiv 1 \mod 3$. □

On sait ([C-S], ch. 16) que O_{23} est l'unique réseau unimodulaire de minimum 3 et de dimension $n \leq 23$. Par ailleurs, si Λ est imprimitif, $\frac{1}{\sqrt{3}}\Lambda$ est entier de minimum 1, donc isométrique à $\mathbb{Z}$, et Λ lui-même est isométrique à O_1.

Pour démontrer le théorème 7.4, on est maintemant ramené à prouver que, dans chacune des dimensions $n = 7, 16, 22$, un réseau Λ primitif non unimodulaire fortement parfait est nécessairement isométrique à un réseau O_n, et que les cinq réseaux O_n de l'énoncé sont effectivement fortement parfaits. On se contentera d'une vérification informatique de ce dernier point (en fait nécessaire seulement pour $n = 16, 22, 23$).

LEMME 7.12. *Si $n = 7$ ou $n = 16$, Λ^*/Λ est 2-élémentaire; si $n = 22$, Λ^*/Λ est 3-élémentaire.*

Démonstration. Le réseau Λ^* est engendré par les vecteurs de la forme $t + x$, x parcourant Λ et t l'ensemble des vecteurs minimaux des classes non nulles de Λ^*/Λ. On a vu au cours de la démonstration du lemme 7.11 que l'on a $(t,t) = \frac{n+2}{9}$, d'où $(t+x, t+x) = (t,t) + 2(t,x) + (x,x) \equiv (t,t) \equiv \frac{n+2}{9} \mod \mathbb{Z}$.

Si $n = 7$ ou $n = 16$, $(t + x, t + x)$ est entier quels que soient t et x, si bien que les produits scalaires sont entiers ou demi-entiers sur Λ^*. On a donc $2\Lambda^* \subset \Lambda$ dans ce cas.

Si $n = 22$, on a $(t,t) = \frac{8}{3}$, donc $6(t + x, t + x) \in 2\mathbb{Z}$. Cela prouve que $\sqrt{6}\,\Lambda^*$ est un réseau pair; en particulier, on a $\sqrt{6}\,\Lambda^* \subset (\sqrt{6}\,\Lambda^*)^* = \frac{1}{\sqrt{6}}\,\Lambda$, d'où l'inclusion $6\Lambda^* \subset \Lambda$, qui montre que l'exposant du groupe Λ^*/Λ divise 6. Cet exposant divise 3 (et est en fait égal à 3) : sinon, il existerait un élément u d'ordre 2 dans Λ^*/Λ (on aurait $u \in \Lambda^*$, $u \notin \Lambda$, $2u \in \Lambda$); un tel u serait encore de la forme $u = t_1 + x$, avec $(t_1, t_1) = \frac{8}{3}$ et $x \in \Lambda$; modulo Λ, on pourrait supposer que $u = t_1$ avec $2t_1 \in \Lambda$, et $4\,(t_1, t_1) = \frac{32}{3}$ serait entier. Cela prouve que Λ^*/Λ est 3-élémentaire. □

Il résulte de ce lemme que le déterminant de Λ est de la forme 2^k (resp. 3^k) avec $0 \leq k \leq n$. Les inégalités sont en fait strictes puisque Λ n'est ni unimodulaire, ni imprimitif. En outre, $\sqrt{2}\,\Lambda^*$ est de minimum 2 pour $n = 7$ et 4 pour $n = 16$, alors que $\sqrt{3}\,\Lambda^*$ est de minimum 8 pour $n = 22$.

Pour achever la démonstration du théorème 7.4, nous allons devoir préciser les valeurs du déterminant de Λ, puis utiliser divers résultats de classification.

Démonstration du Théorème 7.4 pour $n = 7$. On a vu que $\det(\Lambda) = 2^k$ pour un entier $k \in [1, 6]$. Mais on n'a pas $k \leq 5$, car Λ serait alors plus dense que $\mathbb{E}_7$. Par ailleurs, chaque classe de Λ^*/Λ contient un couple $\pm t$ de vecteurs de norme 1. Il y a donc $2(2^k - 1) = 2.63$ vecteurs de norme 1 dans Λ^*. Soient Λ' le réseau qu'ils engendrent. Par $x \mapsto \sqrt{2}\,x$, on transforme L' en un réseau de racines L contenant 2.63 racines. On a donc $L \simeq \mathbb{E}_7$, donc aussi $\sqrt{2}\,\Lambda^* \simeq \mathbb{E}_7$ (car $\det(\Lambda^*)$ doit être entier, et $\det(\mathbb{E}_7) = 2$), ce qui prouve que Λ est semblable à $\mathbb{E}_7^*$.

Démonstration du Théorème 7.4 pour $n = 16$. Posons $\det(\Lambda) = 2^k$. Soit Λ_0 le réseau pair associé à Λ. On a $\Lambda_0 \subset \Lambda \subset \Lambda^* \subset \Lambda_0^*$, et

$[\Lambda : \Lambda_0] = [\Lambda_0^* : \Lambda] = 2$, donc $\det(\Lambda_0) = 2^{k+2}$. On remarque que

$$\forall\, \xi \in \Lambda_0^* \smallsetminus \Lambda^*,\ \forall\, x \in \Lambda \smallsetminus \Lambda_0,\ (\xi, x) \in \frac{1}{2} + \mathbb{Z}\,.$$

En effet, pour $\xi \in \Lambda_0^* \smallsetminus \Lambda^*$, $2(\xi, x) = (2\xi, x)$ est entier pour tout $x \in \Lambda$, d'ou $(\xi, x) \in \mathbb{Z} \cup \frac{1}{2} + \mathbb{Z}$, et (ξ, x) est demi-entier pour au moins un $x \in \Lambda$, qui n'est certainement pas dans Λ_0. Si y est un autre élément de $\Lambda \smallsetminus \Lambda_0$, on a $y - x \in \Lambda_0$, et donc $(\xi, x) - (\xi, y) = (\xi, x - y)$ est entier.

Soit maintenant $\xi \in \Lambda_0^* \smallsetminus \Lambda^*$ de norme minimum dans sa classe modulo Λ^*. Pour $x \in X$ (ensemble des vecteurs courts de Λ), on a $|(\xi, x)| \leq \frac{1}{2}(x, x) = \frac{3}{2}$, soit $(\xi, x) \in \{\pm\frac{1}{2}, \pm\frac{3}{2}\}$. Les trois nombres (ξ, ξ), $n_{1/2}$ et $n_{3/2}$ (nombres de $x \in X$ avec respectivement $(\xi, x) = \frac{1}{2}, \frac{3}{2}$ vérifient les trois équations $|X| = 2(n_{1/2} + n_{3/2})$ et les deux équations fournies par 5.2, ce qui conduit au système

$$(*) \qquad n_{1/2} + n_{3/2} = 256\,;$$

$$(**) \qquad n_{1/2} + 9n_{3/2} = 192(\xi, \xi)\,;$$

$$(***) \qquad n_{1/2} + 81n_{3/2} = 384(\xi, \xi)^2\,.$$

En éliminant $n_{1/2}$ et $n_{3/2}$, on obtient l'équation du second degré

$$(\xi, \xi)^2 - 5(\xi, \xi) + 6 = 0$$

qui prouve que (ξ, ξ) est l'un des entiers 2 ou 3, et entraîne que $\sqrt{2}\,\Lambda_0^*$ est un réseau (entier) pair. On en déduit que le quotient Λ_0^*/Λ_0 est 2-élémentaire.

Or, les réseaux de dimension 16 qui sont pairs et 2-élémentaires ainsi que leur dual renormalisé ont été classés par Scharlau et Venkov [S-V]. (Pour tenir compte à la fois du fait que Λ_0 n'a pas de vecteurs de norme 2 et que son dual renormalisé n'a pas de vecteur de norme 2, on dit dans [S-V] que le *système de racines généralisé* est trivial.) Parmi ces réseaux, un seul est de minimum ≥ 4, à savoir le réseau de Barnes-Wall Λ_{16}. Par conséquent, Λ est bien le réseau O_{16} décrit au début du paragraphe.

Démonstration du Théorème 7.4 pour $n = 22$. On a vu que $\det(\Lambda) = 3^k$ pour un entier $k \in [1, 21]$; on montre que $k = 1$. Pour cela, on observe que, quel que soit $y \in \Lambda^* \smallsetminus \Lambda$, on a $(y, y) \equiv -\frac{1}{3} \mod \mathbb{Z}$, car y est de la forme $t + x$ avec $x \in \Lambda$ et t minimal dans sa classe, et l'on a alors $(y, y) \equiv (t, t) \equiv \frac{8}{3} \mod \mathbb{Z}$. Si $k > 1$, on peut trouver $t_1, t_2 \in \Lambda^* \smallsetminus \Lambda$ tels que $t_1 + t_2$ et $t_1 - t_2$ soient tous deux dans $\Lambda^* \smallsetminus \Lambda$. On en déduit que

l'on a $4(t_1,t_2) \equiv (t_1+t_2,t_1+t_2) - (t_1-t_2,t_1-t_2) \equiv 0 \mod \mathbb{Z}$, donc $(t_1+t_2,t_1+t_2) \equiv -\frac{2}{3} \mod \frac{1}{2}\mathbb{Z} \not\equiv -\frac{1}{3} \mod \mathbb{Z}$.

Ainsi, Λ est un réseau entier, de minimum 3, de dimension 22, de déterminant 3, et les éléments non nuls de Λ^*/Λ sont de norme au moins $\frac{8}{3}$ et congrus à $-\frac{1}{3}$ modulo $\mathbb{Z}$. Dans $\Lambda \perp O_1$, considérons l'élément $x = (y, \frac{1}{3}z)$ où y est un vecteur minimal de Λ^* et z engendre O_1. On a $(x,x) = \frac{8}{3} + \frac{1}{3} = 3$, et on voit tout de suite que le réseau engendré par $\Lambda \perp O_1$ et x est entier, de minimum 3 et de déterminant 1. Il est donc isométrique à O_{23}, et Λ lui-même est donc isométrique à O_{22}.

Cela achève la démonstration du théorème 7.4. □

Des techniques utilisant des calculs de crochets (au sens du §1) de polynômes convenablement choisis permettent d'obtenir des majorations fines de l'invariant s ("demi kissing number") d'un réseau entier de norme 3. Voici un énoncé, de portée en fait plus générale, s'appliquant aux dimensions $n \leq 24$, et fournissant en particulier une démonstration de l'inégalité 7.6 sous des hypothèses moins restrictives.

THÉORÈME 7.13. *Soit S une partie finie symétrique de $\mathbb{R}^n$ formée de $2s$ vecteurs de norme 3, de produits scalaires mutuels $0, \pm 1, \pm 3$. Alors, on a les majorations suivantes de s :*

(1) Pour tout $n \leq 24$, $s \leq \dfrac{8n(n+2)}{25-n}$.

(2) Pour tout $n \leq 8$, $s \leq \dfrac{8n}{9-n}$.

Signalons la majoration universelle suivante, due à Seidel ([S]) :

$$s \leq \binom{n+2}{3} = \frac{n(n+1)(n+2)}{6}, \tag{7.13'}$$

dont le théorème 7.13 montre qu'elle n'est optimale pour aucune valeur de $n \leq 24$ sauf $n = 1$ et $n = 23$.

Avant de procéder à la démonstration du théorème 7.13, nous démontrons des inégalités faisant intervenir les polynômes de Gegenbauer, cf. [Vi], ainsi que [Bc-V], §5. Pour tout entier $d \geq 1$ et tout $\alpha \in \mathbb{R}^n$, il s'agit de l'unique polynôme harmonique de la forme

$$P_d^{(\alpha)}(x) = (x,\alpha)^d + a_1(\alpha,\alpha)\,(x,x)\,(x,\alpha)^{d-2} + \dots .$$

Voici ces polynômes dans les cas $d = 2$ et $d = 4$:

$$P_2^{(\alpha)}(x) = (x,x)^2 - \frac{1}{n}\,(\alpha,\alpha)\,(x,x)\,;$$
$$P_4^{(\alpha)}(x) = (x,x)^4 - \frac{6}{n+4}\,(\alpha,\alpha)\,(x,x)\,(x,\alpha)^2 + \frac{3(\alpha,\alpha)^2(x,x)^2}{(n+4)(n+2)}\,.$$

PROPOSITION 7.13 a. *Soit X un sous-ensemble fini de $\mathbb{R}^n$. Pour tout $d \geq 1$, on a*

$$\sum_{x_1,x_2\in X} P_d^{(x_1)}(x_2) \geq 0\,.$$

Démonstration. Considérons le polynôme $F(x) = \sum_{y\in X} P_d^{(y)}(x)$. Calculons $[F,F]$. On a

$$[F,F] = \sum_{y_1,y_2\in X} [P_d^{(y_1)}, P_d^{(y_2)}] = \sum_{y_1,y_2\in X} [(x,y_1)^d, P_d^{(y_2)}] = \sum_{y_1,y_2\in X} P_d^{(y_2)}(y_1)\,.$$

(La dernière égalité provient de la proposition 1.1 ; la précédente se justifie en utilisant l'égalité $[\omega f, h] = 0$, valable pour tout h harmonique ; on a posé $\omega = (x,x)$.) Cela démontre la proposition, puisque $[F,F]$ est positif ou nul quel que soit F. □

Démonstration du théorème 7.13. On revient aux notations du théorème, en notant en outre S' un système de représentants des couples $\pm x$ de S. (On a $|S'| = s$.) On note a le nombre de couple $(x_1,x_2) \in S' \times S'$ tels que $(x_1,x_2) = \pm 1$. On utilise la proposition précédente pour $d = 2$ et $d = 4$, avec $X = S'$.

Pour $d = 2$, on obtient

$$\sum_{x_1,x_2\in S'} P_2^{(x_1)}(x_2) = \sum_{x_1,x_2\in S'} \big((x_2,x_1)^2 - \frac{1}{n}\,3^2\big) = 9n + a - \frac{9}{n}\,s^2 \geq 0\,,$$

d'où

$$(*) \qquad a \geq \frac{9s(s-n)}{n}$$

.

Pour $d = 4$, on obtient

$$\sum_{x_1,x_2\in S'} P_4^{(x_1)}(x_2)$$
$$= \sum_{x_1,x_2\in S'} \big((x_1,x_2)^4 - \frac{6}{n+4}\,3^2(x_1,x_2)^2 + \frac{3.3^4}{(n+4)(n+2)}\big)$$
$$= a + 3^4 s - \frac{6.3^2}{n+4}\,(a+3^2 s)\frac{3^5 s^2}{(n+4)(n+2)} \geq 0\,.$$

On vérifie facilement que pour $n \leq 50$, cette inégalité se transforme en

$$(**) \qquad a \leq \frac{3^4 s\,(n^2-4+3s)}{(n+2)(50-n)}\,.$$

En éliminant a entre les inégalités $(*)$ et $(**)$, on obtient

$$\frac{s-n}{n} \leq \frac{3^2(n^2-4+3s)}{(n+2)(50-n)}\,.$$

Lorsque l'on suppose en outre que l'on a $n \leq 24$, l'inégalité précédente se met sous la forme

$$s \leq \frac{8n(n+2)}{25-n}\,,$$

qui est précisément l'assertion (1) du théorème.

Pour démontrer l'assertion (2), on utilise $(*)$ ainsi que l'inégalité évidente $a \leq s(s-1)$. En éliminant a, on obtient

$$\frac{9s(s-n)}{n} \leq s(s-1)\,,$$

qui, pour $n \leq 8$ est précisément l'assertion (2). □

Voici une démonstration de l'inégalité $s \leq \binom{n+2}{3} = \frac{n(n+1)(n+2)}{6}$ énoncée ci-dessus. Il convient de noter que le nombre $m = \binom{n+2}{3}$ intervient comme dimension de l'espace $\mathcal{F}_{n,3}$ des polynômes homogènes de degré 3 à n indéterminées. On conserve les notations de la démonstration du théorème 7.13.

Soient G et F les matrices $s \times s$ dont les éléments sont les produits scalaires respectifs (x,y) et $(x,y)^3$ avec $x, y \in S'$. On a $(x,y) = 3$ si $y = x$ et $(x,y) = 0, \pm 1$ si $y \neq x$, d'où $(x,y)^3 = (x,y)$ si x et y sont distincts, et $(x,x)^3 - (x,x) = 3^3 - 3 = 24$ sinon, ce qui entraîne la relation

$$F - G = 24\,I_n\,.$$

On remarque que G est la matrice de Gram de S'. C'est donc une matrice positive, de valeurs propres $\lambda_1, \ldots, \lambda_s \geq 0$, et de rang $\leq n$. Par conséquent, les valeurs propres de F, égales à $24 + \lambda_i$, sont strictement positives.

Nous allons maintenant interpréter F comme une matrice de Gram dans $\mathbb{R}^m$. À $x \in S'$, on associe (cf. §1) la forme $\rho_x^{(3)} : \alpha \mapsto (x,\alpha)^3$. Alors, F est la

matrice de Gram associée aux produits scalaires $\left[\rho_x^{(3)}, \rho_y^{(3)}\right]$. Son rang est donc au plus m, dimension de l'espace $\mathcal{F}_{n,3}$, et aussi égal à s, puisque F possède exactenent s valeurs propres non nulles. □

La majoration par 24 de la dimension que nous avons utilisée dans la démonstration du théorème 7.4 possède la généralisation suivante:

PROPOSITION 7.14. *Un réseau fortement parfait entier de norme* $m \geq 2$ *est de dimension* $n \leq 3(m^2-1)$.

Démonstration. On applique comme précédemment les relations 5.2 à un vecteur minimal α de L. Les sommes du membre de gauche ont pour termes dominants respectivement m^2 et $m^4 > m^2$, et l'on a pour tous les autres termes les inégalités larges $(x,\alpha)^4 \geq (x,\alpha)^2$. En faisant la différence des seconds membres, on en déduit l'inégalité stricte

$$\frac{m^2}{n}\,|X|(\frac{3m^2}{n+2}-1) > 0\,,$$

i.e. $n < 3m^2 - 2$. □

8. UNE CARACTÉRISATION DES DESIGNS SPHÉRIQUES.

Dans ce §, on considère un sous-ensemble fini $X = \{x_1, \ldots, x_N\}$ d'une sphère de $\mathbb{R}^n$, dont le carré du rayon est noté m. Pour simplifier, on suppose que X est *symétrique* (on a $-X = X$). On note k un entier positif pair, soit $k = 2\ell$, et l'on s'intéresse à la propriété pour X d'être un k-design (ou un $(k+1)$-design; vu la symétrie de X, cela revient au même).

THÉORÈME 8.1. *On a*

$$\sum_{x,y\in X} (x,y)^{2\ell} \geq \frac{1.3.5\ldots(2\ell-1)}{n(n+2)\ldots(n+2(\ell-1))} m^{2\ell}|X|^2\,,$$

et l'égalité a lieu si et seulement si X *est un* $2\ell+1$*-design.*

Démonstration. On suppose pour faire la démonstration que $m = 1$, et l'on pose

$$c = \frac{1.3.5\ldots(2\ell-1)}{n(n+2)\ldots(n+2(\ell-1))}\,|X|\,. \tag{8.2}$$

Rappellons que X est un 2ℓ-design si et seulement s'il vérifie la condition

$$\sum_{x\in X}(x,\alpha)^{2\ell} = c(\alpha,\alpha)^{\ell}$$

quel que soit $\alpha \in \mathbb{R}^n$; c'est une identité polynomiale. Rappelons également quelques notations du §1 : on pose $\omega(\alpha) = (\alpha,\alpha)$, et $\rho_z^{(2\ell)}$ est l'application $x \mapsto (z,x)^{2\ell}$. La démonstration va découler du calcul de la norme dans l'espace des polynômes (le *crochet*, défini au début du §1) de la différence $\sum_{x\in X}\rho_x^{(2\ell)} - c\omega^{\ell}$. On a en effet

$$(*) \qquad \left[\sum_{x\in X}\rho_x^{(2\ell)} - c\omega^{\ell}, \sum_{x\in X}\rho_x^{(2\ell)} - c\omega^{\ell}\right] \geq 0\,,$$

et l'égalité caractérise les 2ℓ-designs.

Le calcul du crochet se fait en utilisant les règles suivantes démontrées au §1 (F et G désignent deux polynômes homogènes de degré 2ℓ sur $\mathbb{R}^n$) :

(1) $[\rho_z^{(2\ell)}, F] = F(z)\,;$

(2) $[F,G] = \dfrac{1}{(2\ell)!}\,F(\nabla)\,G\,.$

On trouve pour le crochet l'expression

$$\sum_{x_1,x_2\in X}[\rho_{x_1}^{(2\ell)},\rho_{x_2}^{(2\ell)})] - 2c\sum_{x\in X}[\omega^{\ell},\rho_x^{(2\ell)})] + c^2[\omega^{\ell},\omega^{\ell}]$$

dont on voit tout de suite que les deux premiers termes valent respectivement

$$\sum_{x_1,x_2\in X}(x_1,x_2)^{2\ell} \quad \text{et} \quad -2c|X|\,.$$

Quant au dernier terme, on le calcule par l'identité $[\omega^{\ell},\omega^{\ell}] = \dfrac{1}{(2\ell)!}\Delta^{\ell}(\omega^{\ell})$ (exemple 1.5). On a $\Delta((\alpha,\alpha)^{\ell}) = 2\ell(2\ell+n-2)\omega^{\ell-1}$, d'où, en itérant,

$$\begin{aligned}\frac{1}{(2\ell)!}\Delta^{\ell}(\omega^{\ell}) &= \frac{1}{(2\ell)!}(2\ell)(2\ell-2)\ldots 2\,.\,(2\ell+n-2)(2\ell+n-4)\ldots n\\ &= \frac{2^{\ell}\,\ell!}{(2\ell)!}n(n+2)\ldots(n+2\ell-2)\\ &= \frac{n(n+2)(n+4)\ldots(n+2\ell-2)}{1.3.5\ldots(2\ell-1)}\,.\end{aligned}$$

Finalement, on obtient $\sum_{x,y\in X}(x,y)^{2\ell} \geq 2c|X| - c^2\frac{|X|}{c} = c|X|$. □

Pour appliquer le théorème 8.1, on a intérêt à utiliser le groupe des automorphismes de X (transformations orthogonales conservant X). En effet, la somme $\sum_{y\in X}(x,y)^{2\ell}$ ne dépend que de l'orbite de x sous $\mathrm{Aut}(X)$. En notant Ω l'ensemble des orbites, on obtient

$$\sum_{x,y\in X}(x,y)^{2\ell}=\sum_{o\in\Omega}|o|\sum_{y\in X}(x_o,y)^{2\ell}\,,$$

où x_o désigne un élément arbitraire de l'orbite o.

Dans le cas particulier d'une opération transitive, on obtient (c est défini en 8.2) :

COROLLAIRE 8.3. *Supposons que* $\mathrm{Aut}(X)$ *opère transitivement sur* X. *Alors,* X *est un* $(2\ell+1)$*-design si et seulement si , pour un* $x\in X$*, on a* $\sum_{y\in X}(x,y)^{2\ell}=m^{2\ell}c|X|$.

L'inégalité du théorème 8.1 s'interprète comme une inégalité matricielle portant sur la matrice de Gram $G=((x_i,x_j))$ des vecteurs de X. Elle est particulièrement intéressante dans le cas des matrices G semi-positives, qui sont fortement dégénérées, c'est-à-dire dont la taille est très supérieure au rang.

À un réseau Λ, on associe ainsi une série de fonctions de degrés $2,4,\ldots$, associées à l'ensemble X de ses vecteurs minimaux, dont la plus importante dans l'étude de la perfection forte est

$$\varphi_4(\Lambda)=\sum_{x,y\in X}(x,y)^4-\frac{3|X|^2}{n(n+2)}(x,x)^4\,,$$

ou sa normalisée $\widetilde{\varphi}_4(\Lambda)=\dfrac{\varphi_4(\Lambda)}{(x,x)^4}$. Cette dernière fonction est définie sur les classes de similitude de réseaux. C'est une fonction positive, dont les zéros sont les classes de similitude de réseaux fortement parfaits. Ces réseaux sont donc des points critiques de $\widetilde{\varphi}_4$.

Les points critiques de l'invariant d'Hermite $\gamma(\Lambda)=\frac{\min\Lambda}{\det(\Lambda)^{1/n}}$, sont les classes de similitude de réseaux eutactiques, liés à la cohomologie de $\mathrm{SL}_n(\mathbb{Z})$ (cf. [Ash]) ; on s'attend à ce qu'il y en ait beaucoup.

En revanche, dans le cas de $\widetilde{\varphi}_4$, on cherche des minima absolus (en l'occurence, la valeur 0). La complexité de la cohomologie de $\mathrm{SL}_n(\mathbb{Z})$ n'intervient pas ici, et l'on s'attend en conséquence à ce qu'il n'existe que peu de réseaux fortement parfaits.

9. Réseaux fortement parfaits et familles équiangulaires de droites.

Comme c'est le cas pour tous les réseaux parfaits, l'ensemble X des vecteurs mininaux d'un réseau fortement parfait possède au moins $2s = n(n+1)$ vecteurs minimaux (on doit avoir $s = \frac{1}{2}|X| \geq \dim \mathcal{F}_{n,2} = \frac{n(n+1)}{2}$). On s'intéresse aux cas où il y a égalité. Nous avons déjà rencontré trois exemples de tels réseaux, à savoir $\mathbb{Z}$, $\mathbb{A}_2$ et $\mathbb{E}_7^*$. Dans ces trois exemples, les directions des vecteurs minimaux forment une famille *équiangulaire* de droites. C'est là un fait général:

Théorème 9.1. *Soit Λ un réseau fortement parfait avec $|X| = n(n+1)$. Alors:*

(1) Quels que soient $x \in X$ et $y \in X$ non proportionnel à x, on a $\pm\cos\widehat{x,y} = \dfrac{1}{\sqrt{n+2}}$.

(2) Si Λ est de dimension $n > 2$, $n+2$ est le carré d'un entier impair.

Démonstration. Choisissons un système X' de représentants des couples $\pm x$ de vecteurs de X. Le nombre d'éléments de X' est $s = \frac{n(n+1)}{2}$. Comme Λ est parfait, les polynômes homogènes de degré 2 sont combinaison linéaire des $\rho_x^{(2)}$, $x \in X'$, et cette représentation est unique, car $|X'| = s$. Cela s'applique en particulier aux polynômes de la forme $\rho_z^{(2)}$ pour $z \in \mathbb{R}^n$, pour lesquels on trouve la représentation explicite

$$\rho_z^{(2)} = \sum_{x \in X'} \frac{1}{(x,x)^2} \left(\frac{n(n+2)}{|X|}(z,x)^2 - \frac{n}{|X|}(z,z)(x,x) \right) \rho_x^{(2)} . \tag{9.2}$$

(Cela se voit en calculant la norme de la différence des deux membres, par un calcul analogue à celui qui a permis de caractériser les 2ℓ-designs en 8.1.)

Appliquons cette formule à un élément $z = x_0 \in X'$. Le coefficient de $\rho_{x_0}^{(2)}$ s'écrit

$$\frac{1}{(x_0,x_0)^2} \left(\frac{n(n+2)}{|X|}(x_0,x_0)^2 - \frac{n}{|X|}(x_0,x_0)^2 \right) = \frac{n+2}{n+1} - \frac{1}{n+1} = 1$$

comme il se doit, et les autres coefficients doivent être nuls, ce qui impose que l'on ait pour tout $x \neq x_0$ de X' les égalités

$$\frac{n(n+2)}{|X|}(x_0,x)^2 = \frac{n}{|X|}(x_0,x_0)(x,x) \iff \frac{(x,x_0)^2}{(x_0,x_0)^2} = \frac{1}{n+2} ,$$

ce qui est précisément l'assertion (1) du théorème.

Prouvons maintenant l'assertion (2) (en supposant $n \geq 3$), et normalisons Λ au minimum 1, ce qui ne restreint pas la généralité. Comme tout réseau parfait est rationnel (cf. 6.9), les produits scalaires $(x,y)^2$ sont rationnels quels que soient $x, y \in X$, ce qui prouve tout de suite que $n+2$ est le carré d'un entier pour tout $n > 1$. Il nous faut prouver que cet entier est impair.

Posons $\alpha = \dfrac{1}{\sqrt{n+2}}$. Notons G la matrice de Gram de X' (peu importe la façon dont on ordonne les vecteurs de X'); soit I la matrice unité d'ordre $|X'| = \frac{n(n+1)}{2}$, soit J la matrice de même ordre dont tous les coefficients valent 1, et soit $H = \frac{1}{\alpha}(G - I)$. Ces matrices sont de la forme

$$G = \begin{pmatrix} 1 & \pm\alpha & \dots & \pm\alpha \\ \pm\alpha & 1 & \dots & \pm\alpha \\ \vdots & \vdots & \ddots & \vdots \\ \pm\alpha & \pm\alpha & \dots & 1 \end{pmatrix}, \quad H = \begin{pmatrix} 0 & \pm 1 & \dots & \pm 1 \\ \pm 1 & 0 & \dots & \pm 1 \\ \vdots & \vdots & \ddots & \vdots \\ \pm 1 & \pm 1 & \dots & 0 \end{pmatrix} \quad \text{et} \quad J = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & 1 & \dots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \dots & 1 \end{pmatrix}.$$

Le rang de G est égal au rang de X, soit n. La multiplicité de 0 comme valeur propre de G est donc $N - n \geq 3$. Les valeurs propres de J sont 0 et s, avec les multiplicités respectives $N-1$ et 1. Il en résulte que les sous-espaces propres associés à la valeur propre 0 de G et de J ont une intersection non réduite à $\{0\}$. Soit x un vecteur propre commun à G et à J. On a $Gx = 0$, donc $Hx = -\frac{1}{\alpha}x$. Considérons alors la matrice $K = \frac{1}{2}(H + J - I)$. On a $Kx = -\frac{1}{2}(\frac{1}{\alpha} + 1)\, x$. Comme les coefficients de K sont entiers (égaux à 0 ou 1), $\frac{1}{2}(\frac{1}{\alpha} + 1)$ est un entier algébrique, et sa norme est un entier rationnel. Finalement, $\dfrac{1}{4}(1 - \dfrac{1}{\alpha^2}) = -\dfrac{n+1}{4}$ est entier, d'où $n \equiv -1 \mod 4$. □

Après les dimensions $1, 2, 7$ que nous connaissons, la prochaine dimension *a priori* possible pour laquelle les conditions de 9.1 sont satisfaite est $n = 23$. Il existe effectivement desdn réseaux fortement parfait de dimension 23 avec $|X| = 23.24 = 552$, cf. §19.

10. Relations avec le réseau dual.

Très souvent, le dual d'un réseau fortement parfait est lui-même fortement parfait. En fait, le seul contre-exemple connu est celui du réseau K'_{21} défini au §19, dont le dual est seulement fortement eutactique. (On a $s({K'_{21}}^*) = 112 < \frac{21.22}{2} = 231$.)

QUESTION 10.1. *Le dual d'un réseau fortement parfait est-il toujours fortement eutactique ?*

Nous allons maintenant nous intéresser à la variante duale γ' de l'invariant d'Hermite.

DÉFINITION 10.2. L'invariant de *Bergé-Martinet* d'un réseau Λ est

$$\gamma'(\Lambda) = (N(\Lambda)N(\Lambda^*))^{1/2} = (\gamma(\Lambda)\gamma(\Lambda^*))^{1/2}$$

La *constante de Bergé-Martinet* est $\gamma'_n = \sup_\Lambda \gamma'(\Lambda)$.

[L'égalité qui figure dans 10.2 résulte de définition même de l'invariant d'Hermite: on a $\gamma(\Lambda) = \frac{N(\Lambda)}{\det(\Lambda)^{1/n}}$ et $\det(\Lambda^*) = \det(\Lambda)^{-1}$. On a évidemment $\gamma'(\Lambda^*) = \gamma'(\Lambda) \leq \gamma_n$.]

Les réseaux sur lesquels γ' atteint un maximum local ont été étudiés sous le nom de *réseaux dual-extrêmes*, et caractérisés comme réseaux *dual-parfaits* et *dual-eutactiques*, cf. [M], ch. III, §§3 et 8. Il résulte de ces caractérisations qu'une réponse positive à la question 10.1 entraînerait que les réseaux fortement parfaits sont dual-extrêmes.

Soit Λ un réseau. Notons X' un demi-système de vecteurs minimaux de Λ. Appliquée à un vecteur minimal ρ de Λ^*, et vu que l'on a $(x,x)(\rho,\rho) = \gamma'(\Lambda)^2$ quel que soit $x \in X$, la relation 5.2a peut s'écrire sous la forme

$$\sum_{x\in X'} (x,\rho)^2 = \frac{s}{n}\gamma'(\Lambda)^2 . \tag{10.3}$$

Le membre de gauche de 10.3 étant entier, on en déduit que $\gamma'(\Lambda)^2$ est un nombre rationnel chaque fois que Λ est fortement eutactique.

THÉORÈME 10.4. *Si Λ est fortement parfait, on a $\gamma'(\Lambda)^2 \geq \dfrac{n+2}{3}$.*

Démonstration. En faisant la différence des relations 5.2 appliquées en prenant $\alpha = \rho$, on obtient l'égalité

$$\sum_{x\in X'} (x,\rho)^2\big((x,\rho)^2 - 1\big) = \frac{s}{n}\,\gamma'(\Lambda)^2\big(\frac{3}{n+2}\gamma'(\Lambda)^2 - 1\big)\,, \tag{10.5}$$

dans laquelle le premier membre est un entier ≥ 0, ce qui entraîne immédiatement la minoration $\gamma'(\Lambda)^2 \geq \frac{n+2}{3}$. □

DÉFINITION 10.5. On dit qu'un réseau fortement parfait Λ est de *type minimal* si $\gamma'(\Lambda)^2 = \dfrac{n+2}{3}$ et de *type général* sinon.

De l'examen du membre de gauche de 10.6, on déduit :

PROPOSITION 10.7. *Pour qu'un réseau fortement parfait Λ soit de type minimal, il faut et il suffit que les produits scalaires (x,ρ) avec x minimal dans Λ et ρ minimal dans Λ^* soient égaux à 0 ou ± 1.* □

L'invariant γ' est utile pour majorer le premier membre de 10.5. En effet, l'inégalité de Schwarz entraîne

$$|(x,\rho)| \leq (x,x)^{1/2}(\rho,\rho)^{1/2} = \gamma'(\Lambda) \leq \gamma'_n .$$

Pour $n \leq 8$, on a $|(x,\rho)| \leq \gamma'_n \leq \gamma_n \leq \gamma_8 = 2$, et l'égalité $|(x,\rho)| = 2$ a lieu si et seulement si $n = 8$, $\Lambda \sim \mathbb{E}_8$ et ρ est proportionnel à x. L'énoncé suivant résulte tout de suite de ces remarques et des inégalités $\gamma_3^2 < \frac{5}{3}$ et $\gamma_5^2 < \frac{7}{3}$:

PROPOSITION 10.8. *Un réseau fortement parfait de dimension $n \leq 8$ et non semblable à $\mathbb{E}_8$ est de type minimal. En outre, sa dimension n'est ni 3, ni 5.* □

En revanche, les réseaux unimodulaires fortement parfaits de dimension $n > 1$ ne sont jamais de type minimal : un tel réseau est en effet de norme $m \geq 2$. En prenant alors $\rho = x \in X$, on obtient $(x,\rho) = m > 1$, ce qui entraîne que le premier membre de 10.5 est dans ce cas strictement spérieur à 1. On remarque toutefois que le lemme 6.10 entraîne l'inégalité meilleure $|(x,\rho)| \leq \lfloor \frac{m}{2} \rfloor$ lorsque x et ρ ne sont pas proportionnels. Il serait intéressant d'améliorer la majoration de $|(x,\rho)|$ pour x et ρ non proportionnels dans d'autres cas que celui des réseaux unimodulaires.

PROPOSITION 10.9. *Un réseau de type minimal de dimension $n \geq 2$ n'est un t-design pour aucune valeur de $t \geq 6$.*

Démonstration. Soit L un tel réseau. La propriété pour l'ensemble S de ses vecteurs minimaux d'être un 2ℓ-design se traduit par l'identité

$$\sum_{x \in S/\pm} (x,\alpha)^{2\ell} = c_\ell \, \gamma'(L)^{2\ell} ,$$

la constante c_ℓ étant celle du second membre de 3.6 et de 8.2 On applique cette formule en prenant pour α un vecteur minimal de L^*. La proposition 10.7 montre que les premiers membres de ces identités sont indépendants de ℓ (parce que $(x,\alpha) \in \{0, \pm 1\}$). En écrivant que les seconds membres sont égaux pour $\ell = 2$ et $\ell = 3$, on obtient l'égalité $\gamma'(L) = \frac{n+4}{5}$. En comparant avec la définition 10.6, on obtient l'égalité $\frac{n+4}{5} = \frac{n+2}{3}$, c'est-à-dire $n = 1$. □

REMARQUE 10.10. La relation 10.3, par sommation sur ρ, entraîne l'identité

$$\sum_{x \in X', \rho \in X'^*} (x,\rho)^2 = \frac{ss^*}{n} \gamma'(\Lambda)^2 ,$$

qui est symétrique entre Λ et Λ^*. (On a posé $s^* = s(\Lambda^*)$.)

Nous donnons maintenant pour utilisation ultérieure une autre forme des relations fondamentales 5.2 adaptée au cas où α est un élément λ de Λ^*. Soit $\theta(\lambda) = (x,x)(\lambda,\lambda)$. Les produits scalaires $|(x,\lambda)|$ sont des entiers majorés par $\sqrt{\theta(\lambda)}$. Posons $k = \lfloor \sqrt{\theta(\lambda)} \rfloor$, et pour $0 \leq j \leq k$, soit m_j le nombre d'éléments $x \in X'$ (demi-système de vecteurs minimaux) avec $|(x,\lambda)| = j$. Notons A_λ et B_λ les demi-premiers membres de 5.2. On a

$$A_\lambda = m_1 + 2^2 m_2 + \cdots + k^2 m_k = \frac{s}{n}\,\theta(\lambda) \quad \text{et} \tag{10.11 a}$$

$$B_\lambda = m_1 + 2^4 m_2 + \cdots + k^4 m_k = \frac{3}{n+2}\,\frac{s}{n}\,\theta(\lambda)^2 . \tag{10.11 b}$$

Comme les différences $j^4 - j^2$ sont divisibles par 12,

$$C_\lambda = \frac{1}{12}(B_\lambda - A_\lambda)$$

est entier, et la relation 10.5 prend la forme

$$C_\lambda = m_2 + \cdots + \frac{k^4 - k^2}{12} m_k = \frac{s\,\theta(\lambda)}{12\,n(n+2)} \big(3\theta(\lambda) - (n+2)\big) . \tag{10.12}$$

Nous convenons d'omettre la référence à λ lorsque λ est minimal dans Λ^*. On a alors $\theta = \gamma'(\Lambda)^2$, et l'on obtient une majoration de l'entier C en majorant d'abord θ par γ_n^2, puis γ_n et s par les bornes supérieures que l'on connaît, et que l'on peut trouver notamment dans [C-S], chapitre 1, table 1.2 (à utiliser avec la formule (47)) et table 1.5. Ces majorations sont indiquées dans le tableau 10.13 ci-dessous, reposant sur le tableau 1.2 de

[C-S], dans lequel la majoration C_{conj} correspond aux choix pour $\gamma_n(\Lambda)$ et $s(\Lambda)$ des plus grandes valeurs connues (qui peuvent du reste correspondre à des réseaux distincts). Les valeurs de C_{conj} mettent en évidence la relative faiblesse des meilleurs majorations connues des invariants γ et s.

Tableau 10.13

n	10	11	12	13	14	15	16
$\gamma_n^2 \leq$	5,177	5,799	6,453	7,140	7,852	8,597	9,373
$s \leq$	297	457	708	1116	1716	2715	4156
$C \leq$	3	6	12	21	37	67	114
$C_{\text{conj}} \leq$	0	0	2	1	4	10	30

En explicitant C_λ à partir de 10.12, on trouve (de façon générale, quelque soit $\lambda \in \Lambda^*$) que $\theta(\lambda)$ est racine de l'équation du second degré

$$3s\theta(\lambda)^2 - (n+2)s\theta(\lambda) - 12n(n+2)C_\lambda = 0 \tag{10.14}$$

que l'on étudie dans le cas particulier de $\lambda \in S(\Lambda^*)$ en essayant pour C les valeurs autorisées par la table 10.13. Écartons le cas $C = 0$, qui correspond à un réseau de type minimal. On écrit que le discriminant

$$\Delta_\lambda = (n+2)\, s\big((n+2)s + 144\, n\, C_\lambda\big) \tag{10.15}$$

est un carré, on calcule ensuite la racine positive θ de 10.14, on écarte les cas où θ ne respecte pas la majoration de γ_n donnée dans la table 10.13 ou la minoration stricte $\theta > \frac{n+2}{3}$, ainsi que ceux pour lesquels $A = \theta\frac{s}{n}$ n'est pas entier.

On obtient ainsi d'importantes restrictions quant aux valeurs possibles du couple (θ, s) susceptibles de conduire à un réseau de type général. C'est cette stratégie qui sera utilisée dans l'étude des dimensions 8 à 11.

Notons que la majoration $\theta \leq \gamma_n$ jointe à l'inégalité de Schwarz $|(x,y)| \leq N(x)N(y)$ entraîne la majoration $|(x,y)| \leq \gamma_n$ quels que soient $x \in S(\Lambda)$ et $y \in S(\Lambda^*)$. Pour $n \leq 8$, on trouve $(x,y) = 0, \pm 1$ sauf lorsque x et y sont des vecteurs proportionnels d'un réseau semblable à $\mathbb{E}_8$ ([M], ch. VI, lemme 3.3 et les commentaires qui suivent). Le tableau 10.13 montre que la majoration $|(x,y)| \leq 2$ est valable au moins jusqu'à la dimension 15 (et sans doute aussi en dimension 16). Il en résulte que pour $n \leq 15$, C est le nombre d'éléments $x \in S(\Lambda)/\{\pm 1\}$ ayant avec un élément donné y de $S(\Lambda^*)$ un produit scalaire égal à ± 2.

11. Les dimensions 8 et 9.

La liste complète des réseaux fortement parfaits de dimension $n \leq 7$ est donnée par le théorème 6.11. Le but de ce § est de prouver que, dans les dimensions 8 et 9, seul $\mathbb{E}_8$ est fortement parfait, ce qui prouve que, à similitude près, il y a exactement 8 réseaux fortement parfaits de dimension $n \leq 9$, dont des représentants primitifs sont $\mathbb{Z}, \mathbb{A}_2, \mathbb{D}_4, \mathbb{E}_6, \sqrt{3}\,\mathbb{E}_6^*, \mathbb{E}_7, \sqrt{2}\,\mathbb{E}_7^*, \mathbb{E}_8$.

Nous commençons par la dimension 9, pour laquelle le résultat était *a priori* probable, car on ne connaît aucun réseau Λ avec $\gamma'(\Lambda)^2 \geq \dfrac{11}{3}$.

Théorème 11.1. *Il n'existe pas de réseau fortement parfait de dimension* 9.

Démonstration. Sinon, soit Λ un tel réseau. Nous allons utiliser les relations 10.11 et 10.12 en prenant d'abord pour λ un vecteur minimal de Λ^*. On a alors $\theta = \gamma'(\Lambda)^2$. Nous utiliserons les majorations $\gamma'(\Lambda) \leq \gamma_9 < 2,142$ (Rogers; cf. [C-S], ch. 1, table 1.2 et formule (47)) et $s(\Lambda) \leq 136$ (Watson, [W]).

Il en résulte la majoration $\theta \leq \gamma_9^2 < 4,59\ldots$, et 10.12 s'écrit

$$C = \frac{136\theta}{1188}\,(3\theta - (n+2)) < 2\,,$$

d'où $C = 1$ (type général) ou $C = 0$ (type minimal).
[On aurait pu se contenter de la majoration moins précise $s \leq 190$ donnée dans [C-S], table 1.5, à condition de montrer également l'impossibilité du cas $C = 2$.]

Réseaux de type général. On a $C = 1$, i.e. $s\theta(3\theta - 11) = 12.9.11 = 1188$, d'où

$$\frac{A^2}{B} = \frac{s(n+2)}{3n} = \frac{11s}{27} \quad \text{et} \quad B - A = 12\,,$$

donc $\dfrac{A^2}{A+12} = \dfrac{11s}{27}$, équation du second degré en A, de discriminant

$$\frac{1}{3^6}\,(11s)(11s + 6^4)\,.$$

En écrivant que le numérateur est un carré, on constate que s doit être un multiple de 11 de l'intervalle $[45, 190]$, soit $s = 11t$ avec $5 \leq t \leq 17$, et un petit nombre de vérifications montre que ce n'est pas possible.

Réseaux de type minimal. On a $C = 0$, $\theta = \gamma'(\Lambda)^2 = \frac{11}{3}$ et $A = \frac{11s}{27}$. En normalisant, on peut supposer que $N(\Lambda) = 1$, donc que $N(\Lambda^*) = \frac{11}{3}$. Les formules 10.11, en posant $s = 27t$ et $w = (\lambda, \lambda)$, s'écrivent

$$A_\lambda = \frac{s}{n}\, w = 3tw \quad \text{et} \quad B_\lambda = \frac{3}{n+2}\, \frac{s}{n}\, w^2 = \frac{9t}{11}\, w^2 .$$

Posons $w = \dfrac{p}{q}$, où p et q sont des entiers premiers entre eux. On a $B_\lambda = \dfrac{9tp^2}{11q^2}$. Donc, q^2 divise $9t$. Comme t est ≤ 7, cela entraîne $q \in \{1, 2, 3, 6\}$. On a aussi

$$\frac{B_\lambda - A_\lambda}{12} = \frac{tp(3p - 11q)}{4.11.q^2} \in \mathbb{Z} ,$$

ce qui entraîne $p \equiv 0 \mod 11$, soit $p = 11p'$, puis $\dfrac{11p'(q - 3p')}{4q^2} \in \mathbb{Z}$, d'où l'on déduit que q est impair (faute de quoi, t devrait être divisible par 16). Ainsi, on a $q = 1$ ou $q = 3$, et w est de la forme $\dfrac{11\ell}{3}$ avec $\ell \in \mathbb{Z}$. Autrement dit, les normes des vecteurs de Λ^* sont des multiples *entiers* de $N(\Lambda^*)$.

Soit $\Gamma = \sqrt{\frac{6}{11}}\, \Lambda^*$; ses vecteurs ayant pour norme des entiers pairs, c'est un réseau pair, et en particulier entier. Par conséquent, $d = \det(\Gamma)$ est entier. Mais $\Gamma^* = \sqrt{\frac{11}{6}}\, \Lambda$ est de norme $\frac{11}{6}$ et de déterminant $\frac{1}{d}$. La majoration de Rogers de γ_9 fournit alors l'inégalité $\frac{11}{6}\, d^{1/9} \leq 2,141$, d'où $d \leq 4$. Comme $N(\Gamma^*) = \frac{11}{6}$, l'annulateur de Γ^*/Γ est un multiple de 6, ce qui impose que d soit multiple de 6, et contredit l'inégalité $d \leq 4$. □

Passons maintenant à la dimension 8.

THÉORÈME 11.2. *Les réseaux fortement parfaits de dimension* 8 *sont semblables à* $\mathbb{E}_8$.

Démonstration. Soit Λ un réseau fortement parfait de dimension 8. La proposition 10.8 montre que Λ est semblable à $\mathbb{E}_8$ (et est alors de type général), ou qu'il est de type minimal. Nous devons montrer que ce dernier cas est impossible.

Soit Λ un tel réseau. Quitte à le remplacer par un réseau proportionel, on peut le supposer de minimum 1. On a alors $N(\Lambda^*) = \gamma'(\Lambda)^2 = \frac{10}{3}$. On note X' un demi-système de vecteurs minimaux de Λ.

Appliquée à un vecteur minimal α de Λ^*, la relation 10.11 a s'écrit $\frac{s}{n}(\alpha,\alpha) = \frac{10s}{24} = A_\alpha \in \mathbb{Z}$, qui montre que s est divisible par 12, soit $s = 12s_1$. On sait (Watson, [W]) que l'on a $s \leq 75$ pour tout réseau de dimension 8 non semblable à $\mathbb{E}_8$. On a donc $s_1 \leq 6$. (Comme on le verra, l'inégalité $s_1 < 9$ nous suffit.)

Comme dans le cas de la dimension 9, on considère maintenant un vecteur λ arbitraire de Λ^* ; on pose $(\lambda,\lambda) = w$ et $w = \frac{p}{q}$, $(p,q) = 1$.

Les relations 10.11 montrent que

$$\frac{s_1 w}{2} = \frac{s_1 p}{2q} \quad \text{et} \quad \frac{3^2 s_1 w^2}{2^2.5} = \frac{3^2 s_1 p^2}{2^2.5q^2}$$

sont entiers. Nous distinguons maintenant deux cas.

cas 1 : $s_1 \neq 5$. On a alors $p \equiv 0 \mod 5$, soit $p = 5p_1$, et la relation 10.12 entraîne que $\dfrac{5s_1p_1(3p_1 - 2q)}{16q^2}$ est entier, donc que p_1 est pair (faute de quoi, s_1 serait divisible par 16). De ce fait, q est impair, et donc égal à 1 ou 3, et w est de la forme $\frac{5}{3}m$, m entier. Ainsi, $\Gamma = \sqrt{\frac{3}{5}}\,\Lambda^*$ est un réseau dont tous les vecteurs sont de norme paire. C'est en particulier un réseau entier, donc de déterminant d entier. Le réseau $\Gamma^* = \sqrt{\frac{5}{3}}\,\Lambda$ est de minimum $\frac{5}{3}$, de déterminant $\frac{1}{d}$, et l'on a $\gamma(\Gamma^*) = \frac{5}{3}d^{1/8} < 2$, donc $d < (\frac{6}{5})^8 < 5$, i.e. $d \in \{1,2,3,4\}$. On doit exclure les valeurs $1,2,4$, parce que l'annulateur de Γ^*/Γ est un multiple de 3. Un théorème de Conway et Sloane ([C-S], table 15.9), montre qu'il n'existe pas de réseau pair de dimension 8 et de déterminant 3.

cas 2 : $s_1 = 5$. C'est le cas $s = 60$, plus délicat que le précédent. On a $A_\lambda = \dfrac{15p}{2q}$ et $B_\lambda = \dfrac{3.60p^2}{8.10q^2} = \dfrac{9p^2}{4q^2}$, ce qui entraîne encore que p est pair, soit $p = 2p_1$, et que q est égal à 1 ou 3.

• Si $q = 3$, on a $A_\lambda = 5p_1$, $B_\lambda = p_1^2$, et $C_\lambda = \dfrac{p_1(p_1-5)}{12}$ ne peut être entier que si $p_1 \equiv 5 \mod 3$. Posons $p_1 - 5 = 3p_2$. On a $(3p_2+5)p_2 \equiv 0 \mod 4$, d'où $p_2 \equiv 0$ ou $1 \mod 4$. Donc, dans cette situation, w est de l'une des formes $w = \dfrac{24p_3 + 10}{3}$ ou $w = \dfrac{24p_4 + 16}{3}$.

• Si $q = 1$, on a cette fois $A_\lambda = 15p_1$, $B_\lambda = 9p_1^2$ et $C_\lambda = \dfrac{p_1(3p_1-5)}{4}$, et w est de l'une des formes $w = 8p_5$ ou $w = 8p_6 + 6$.

Finalement, il y a *a priori* quatre formes possibles pour w, ce qui montre que les normes des vecteurs non nuls de Λ^* font partie de la suite $\frac{10}{3}$, $\frac{16}{3}$, 6, 8, $\frac{34}{3}$, $\frac{40}{3}$, 14, 16, ... Le réseau $\Gamma = \sqrt{3}\,\Lambda^*$ est donc (entier) pair.

Quels que soient α et β dans $\mathbb{R}^n$, on a l'identité (formule 6.5) :

$$\sum_{x\in X'}(x,\alpha)^2(x,\beta)^2 = \frac{s}{n(n+2)}\big(2(\alpha,\beta)^2+(\alpha,\alpha)(\beta,\beta)\big)$$

$$= \frac{3}{4}\big(2(\alpha,\beta)^2+(\alpha,\alpha)(\beta,\beta)\big)\ . \tag{11.3}$$

Appliquons-la à des éléments α et β de Γ. On a $(\alpha,\alpha)(\beta,\beta)\equiv 0 \mod 4$. Comme le premier membre de 11.3 est entier, (α,β) est pair. Donc, $M=\frac{1}{\sqrt{2}}\Gamma$ est entier, et les normes de ses vecteurs non nuls sont 5, 8, 9, 12, ...

Nous allons maintenant montrer que

$$M_0=\{m\in M \mid (m,m)\equiv 0 \mod 3\}$$

est un sous-réseau d'indice 3 de M.

Prenons en effet $\alpha,\beta\in\Gamma$, soit $\alpha=\sqrt{3}\,\alpha'$ et $\beta=\sqrt{3}\,\beta'$ avec $\alpha',\beta'\in\Lambda^*$. La formule 11.3 montre alors que l'on a

$$2(\alpha,\beta)^2+(\alpha,\alpha)(\beta,\beta)=12\sum_{x\in X'}(x,\alpha')^2(x,\beta')^2\equiv 0 \mod 12\,,$$

et donc que deux éléments arbitraires m,m' de M satisfont la congruence

$$(m,m')^2\equiv(m,m)(m',m') \mod 3\,. \tag{11.4}$$

Il en résulte que M_0 est un sous-groupe de M. En outre, la formule 11.4 montre que si m et m' sont deux éléments de $M\smallsetminus M_0$, on a $(m\pm m',m\pm m')=(m,m)+(m',m')\pm 2(m,m')\equiv 0 \mod 3$ pour un choix de signe convenable, d'où la majoration $[M:M_0]\le 3$, et donc l'égalité $[M:M_0]=3$, vu que M contient des éléments de norme 5.

Soit d l'entier $\det(M)$. On a $\det(M^*)=\frac{1}{d}$, et $N(M^*)=\frac{2}{3}$ puisque $N(M)=5$, d'où $\gamma(M^*)=\frac{2}{3}d^{1/8}$. De $\gamma_8\le 2$, on déduit $d\le 3^8$.

Par ailleurs, la norme de M_0 étant minorée par la plus petite norme d'un vecteur de M qui soit divisible par 3, on a $N(M_0)\ge 9$. En majorant par 2 l'invariant d'Hermite de M_0, on obtient $9/\det(M_0)^{1/8}\le 2$, i.e. $\det(M_0)\ge(\frac{9}{2})^8$, d'où la minoration

$$d=\det(M)=\det(M_0)/3^2\ge 3^{14}2^{-8}=3^8\Big(\frac{27}{16}\Big)^2\,,$$

qui contredit la majoration $d\le 3^8$. □

12. La dimension 11.

Dans cette dimension, comme dans le cas de la dimension 9, les réseaux Λ connus vérifient l'inégalité $\gamma'(\Lambda)^2 \leq 4 < \frac{n+2}{3} = \frac{13}{3}$. (La valeur 4 est atteinte sur plusieurs réseaux, en particulier sur le réseau K_{11}, sur lequel est aussi atteinte la plus grande valeur connue de l'invariant d'Hermite.)

Par des arguments analogues à ceux qui ont été utilisés dans l'étude des dimensions 8 et 9, nous démontrons en fait :

Théorème 12.1. *Il n'existe pas de réseaux fortement parfaits de dimension 11.*

Démonstration. Nous aurons besoin de majorations des invariants γ' et s pour appliquer les formules 10.11 et 10.12. Rappelons celles qui apparaissent dans la table 10.13 : la borne de Rogers en dimension 11 est $\gamma_{11} < 2,408106$, qui entraîne ${\gamma'_{11}}^2 \leq \gamma_{11}^2 < 5,799$. Le nombre de contacts des empilements de sphères généraux est quant à lui majoré par 915 (cf. [C-S], table 1.5), d'où $s \leq 457$, estimation certainement très au-delà de la réalité.

Comme précédemment, nous considérons séparément les réseaux de type général et ceux de type minimal. Dans les deux cas, on considère un réseau Λ de minimum 1 ; on a donc $N(\Lambda^*) = \gamma'(\Lambda)^2$.

Pour tout $\alpha \in \mathbb{R}^{11}$, les relations 5.2 s'écrivent

$$\sum_{x \in X'} (x,\alpha)^2 = \frac{s}{11}(\alpha,\alpha) \quad \text{et} \quad \sum_{x \in X'} (x,\alpha)^4 = \frac{3s}{11.13}(\alpha,\alpha)^2 . \tag{12.2}$$

Lorsqu'on les applique à des vecteurs α de Λ^*, on obtient des premiers membres $A(\alpha)$ et $B(\alpha)$ qui sont entiers, ainsi que

$$C(\alpha) = \frac{B(\alpha) - A(\alpha)}{12} = \frac{s\,(\alpha,\alpha)}{11.12.13}(3\,(\alpha,\alpha) - 13) . \tag{12.3}$$

Réseaux de type général. C'est le cas $\gamma'(\Lambda)^2 > \frac{13}{3}$. Nous appliquons 12.2 et 12.3 en choisissant α minimal dans Λ^*. Le fait que Λ soit de type général se traduit alors par $C > 0$, et les majorations de $\gamma'(\Lambda)$ et de s que nous avons rappelées montrent que l'on a $C \leq 6,79\ldots$, i.e. $C \leq 6$. Il en résulte que (α,α) est racine de l'une des équations

$$3sX^2 - 13sX - 11.12.13\,C = 0\,, \quad C = 1,2,3,4,5,6\,,$$

pour lesquelles s est limité par l'encadrement $\frac{n(n+1)}{2} = 66 \leq s \leq 457$. Comme (α,α) doit être rationnel, le discriminant de l'équation doit être

un carré ce qui impose $s \equiv 0 \mod 13$, et un nombre modeste d'essais, que l'on peut confier à un ordinateur (et que l'on pourrait du reste restreindre par des congruences modulo 13) montre qu'aucune de ces équations ne possède de racine rationnelle dans les intervalles où doivent se trouver s et C.

Réseaux de type minimal. C'est le cas $\gamma'(\Lambda)^2 = \frac{13}{3}$. En appliquant 12.2 à un vecteur minimal α de Λ^*, on voit que $A(\alpha) = \dfrac{s}{n}(\alpha,\alpha) = \dfrac{13s}{3.11}$ doit être entier, d'où $s \equiv 0 \mod 33$, soit $s = 33s_1$; on a alors $2 \leq s_1 \leq 13$ (et $s \leq 439$).

Nous appliquons maintenant 11.2 et 11.3 à un vecteur α arbitraire de Λ^*. On pose $(\alpha,\alpha) = w$ et $w = \frac{p}{q}$, $(p,q) = 1$. En écrivant que $C(\alpha)$ est entier, on obtient la condition

$$\frac{s_1 p(3p - 13q)}{2^2.13.q^2} \in \mathbb{Z}\,,$$

d'où l'on déduit, compte tenu de la majoration $s_1 \leq 13$, que q est impair (sinon, s_1 serait divisible par 16) et que q^2 divise $3s_1$, d'où $q = 1$ ou $q = 3$.

Nous distinguons maitenant deux cas.

Cas 1 : $s_1 \not\equiv 13$. Alors, on a $s_1 \not\equiv 0 \mod 13$, donc $p \equiv 0 \mod 13$. Les normes des vecteurs de Λ^* sont donc des multiples entiers de $\frac{13}{3}$, et le réseau $\Gamma = \dfrac{\sqrt{2}}{\sqrt{13/3}}\Lambda^*$ est entier et pair, de minimum

$$N(\Gamma) = \frac{6}{13}N(\Lambda^*) = \frac{6}{13}\gamma'(\Lambda)^2 = 2\,.$$

Soit $d = \det(\Gamma)$. On a $N(\Gamma^*) = \frac{13}{6}$ (car Γ^* et Λ ont même invariant γ') et $\det(\Gamma^*) = \frac{1}{d}$, donc $\gamma(\Gamma)^* = \frac{13}{6}d^{1/11}$, et la majoration de Rogers entraîne $\frac{13}{6}d^{1/11} < 2,4082$, i.e. $d < 3,2$, soit $d \in \{1,2,3\}$. On doit écarter la possibilité $d = 1$, car les réseaux unimodulaires pairs n'existent que dans les dimensions multiples de 8. Les tables 15.8 et 15.9 de [C-S] montrent que les seules possibilités sont que Γ soit isométrique à l'orthogonal d'un vecteur de norme 2 ou 3 du réseau unimodulaire $\mathbb{D}_{12}^+$. Cela laisse *a priori* deux réseaux M_2 et M_3 possibles, tous deux de minimum 2, dont les réseaux duals ont pour minima respectifs $\frac{3}{2}$ et $\frac{5}{3}$. On a donc $\gamma'(M_2)^2 = 3 < \frac{13}{3}$ et $\gamma'(M_3)^2 = \frac{10}{3} < \frac{13}{3}$, ce qui prouve que ces réseaux ne sont pas fortement parfaits.

[Le réseau M_3 est isométrique au réseau $\mathbb{A}_{11}^2$ de Coxeter.]

Cas 2: $s_1 = 13$, et donc, $s = 3.11.13 = 429$. La qualité médiocre des majorations connues en dimension 11 tant de la constante d'Hermite que du "kissing number" complique considerablement la démonstration qui suit.

On a $q = 3$ ou $q = 1$, donc

$$A = 13p,\ B = p^2,\ C = \frac{p(p-13)}{12}$$
ou
$$A = 3.13p,\ B = 3^2p^2,\ C = \frac{p(3p-13)}{4},$$

ce qui fait que les normes des vecteurs non nuls de Λ^* font partie de la suite $\frac{13}{3}$, $\frac{16}{3}$, 7, 8, $\frac{25}{3}$, $\frac{28}{3}$, 11, 12,... formée des nombres rationnels de l'une des formes $\frac{12m+1}{3}$, $\frac{12m+4}{3}$, $4m-1$, $4m$, commençant par $\frac{13}{3} = N(\Lambda^*)$.

On raisonne maintenant comme dans le cas de la dimension 8. On pose $\Gamma = \sqrt{6}\,\Lambda^*$; c'est un réseau (entier) pair. Le calcul de la somme $\sum_{x\in X'}(x,\alpha)^2(x,\beta)^2$ fait lors de la démonstration de la formule 11.3 conduit à une congruence analogue à 11.4, à savoir

$$\forall\,\omega_1,\omega_2 \in \Gamma,\ 2(\omega_1,\omega_2)^2 + (\omega_1,\omega_1)(\omega_2,\omega_2) \equiv 0 \mod 12, \tag{12.4}$$

qui prouve que les produits scalaires (ω_1,ω_2) sont tous pairs, et donc que $M = \frac{1}{\sqrt{2}}\,\Gamma = \sqrt{3}\,\Lambda^*$ est un réseau entier de minimum 13, dont les normes des vecteurs non nuls appartiennent à la suite $13, 16, 21, 24, \ldots$

Il résulte aussi de 12.4 que

$$M_0 = \{x \in M \mid (x,x) \equiv 0 \mod 3\}$$

est un sous-réseau de M, d'indice 3, et dont toutes les normes sont multiples de 3. Le réseau pair

$$M_1 = \{x \in M_0 \mid (x,x) \equiv 0 \mod 2\}$$

associé à M_0 ne contient que des vecteurs dont les normes sont multiples de 6.

LEMME 12.5. *L'entier* $d = \det(M)$ *satisfait la double inégalité* $7,19537 < d^{1/11} < 7,22432$.

Démonstration. On utilise la majoration de γ_{11} rappelée au début du §.

Le réseau M^* a pour déterminant $\frac{1}{d}$ et pour minimum $\frac{1}{3}$. On a donc $\gamma(M^*) = \frac{d^{1/11}}{3}$, d'où $d^{1/11} \leq 3\gamma_{11} < 7,22432$.

On a par ailleurs $\det(M_1) = 6^2 d$ et $N(M_1) \geq 24$, d'où $\gamma(M_1) \geq \frac{24}{(d^2 d)^{1/11}}$, ce qui entraîne $d^{1/11} \geq \frac{24}{6^{2/11}.\gamma_{11}} \geq 7,19537\ldots$ □

Posons $\Delta = \frac{1}{\sqrt{6}} M_1$ et $\delta = \det(\Delta)$.

LEMME 12.6. *Δ est un réseau pair de minimum 4, et δ est l'un des entiers*

$$267 = 3.89,\ 270 = 2.3^3.5,\ 273 = 3.7.13,\ 276 = 2^2.3.23\,.$$

Démonstration. Soient $\omega_1, \omega_2 \in M_1$. En leur appliquant la relation 12.4, on voit d'abord que l'on a $2(\omega_1, \omega_2)^2 \equiv 0 \mod 12$, donc que $\frac{1}{6}(\omega_1, \omega_2)$ est entier, puis que $(\omega, \omega) \equiv 0 \mod 8$ pour tout $\omega \in M$. Alors, Δ est un réseau pair. Comme M_1 est de minimum au moins 24, on a $N(\Delta) \geq 4$, et en fait $N(\Delta) = 4$, vu la majoration de Rogers de γ_{11}.

On a $\det(M_1) = 6^2 \det(M) = 6^2 d$, et aussi $\det(M_1) = 6^{11}\delta$, d'où $d = 6^9\delta$. Le lemme 12.5 montre que δ vérifie la double inégalité $266 \leq \delta \leq 277$, et tout revient à démontrer que δ est divisible par 3.

Pour ce faire, nous revenons au réseau M, et appliquons 12.4 avec $\omega_2 \in M$ et $\omega_1 \in M_0$. On a $(\omega_1.\omega_1) \equiv 0 \mod 3$ et $(\omega_2, \omega_2) \in \mathbb{Z}$, donc $(\omega_1, \omega_2) \equiv 0 \mod 3$, i.e. $\frac{1}{3}\omega_2 \in M_0^*$. L'inclusion $M_0^* \subset M_1^* = \frac{1}{\sqrt{6}}\Delta^*$ montre qu'il existe $\omega \in \Delta^*$ avec $\frac{1}{3}\omega_2 = \frac{1}{\sqrt{6}}\omega$. En prenant ω_2 minimal dans M, on obtient $(\omega, \omega) = \frac{2}{3}(\omega_2, \omega_2) = \frac{26}{3}$, ce qui prouve bien que le déterminant de Δ est divisible par 3. □

Fin de la démonstration du Théorème 12.1. On peut sans diminuer la généralité supposer que Λ est engendré par l'ensemble X de ses vecteurs minimaux. Posons $X_1 = \sqrt{2}X$. On a

$$M_1 = \sqrt{6}\,\Delta \subset M \subset M^* \subset \frac{1}{\sqrt{6}}\,\Delta^*$$

et $\Lambda = \sqrt{3}\,M^*$, donc $\sqrt{2}\,\Lambda \subset \Delta^*$. En particulier, X_1 est un sous-ensemble de Δ^*.

Pour $x \in X_1$, posons $\Delta_x = \langle \Delta, x \rangle$. On a $\Delta \subset \Delta_x \subset \Delta^*$, et la première inclusion est stricte, car $(x, x) = 2$ n'est pas la norme d'un vecteur de Δ. D'autre part, du fait que Δ est un réseau pair et que x est de norme paire, Δ_x est pair, et en particulier entier. Il en résulte que $\det(\Delta_x)$ est entier,

et de la forme $\frac{\delta}{\ell^2}$ où $\ell = [\Delta_x : \Delta]$ est un entier ≥ 2. Par 12.6, on a le choix entre seulement les deux possibilités

$$\ell = 2 \text{ et } \delta = 2^2.3.23 \qquad \text{ou} \qquad \ell = 3 \text{ et } \delta = 2.3^3.5\,,$$

au sujet desquelles nous remarquons que l'entier ℓ ne dépend pas du choix de x, puisqu'il est déterminé par la valeur de δ.

Posons $V = \Delta^*/\Delta$, et soit V_ℓ ($\ell = 2$ ou $\ell = 3$) le sous-groupe des éléments de V annulés par une puissance de ℓ. On a $\sqrt{6}\,M^* = \sqrt{2}\,\Lambda = \langle X_1 \rangle \subset V_\ell$, mais $\sqrt{6}\,M^*$ est d'indice 6 dans Δ^*, ce qui, si $\ell = 2$ (resp. si $\ell = 3$) contredit le fait que δ soit divisible par 23 (resp. par 5). □

13. Indications sur la dimension 10.

On connaît les séries Λ_n, K_n et K'_n pour $1 \leq n \leq 24$. Il s'agit de réseaux entiers de minimum 4 contenus dans le réseau de Leech Λ_{24}, dont les définitions sont brièvement rappelées au §19. Les deux premières sont classiques; toutes trois sont définies de façon précise dans [M], ch. III, § 7 et ch. VIII, §§ 5, 7.

Dans le cas $n = 10$ qui nous concerne ici, ce sont des réseaux extrêmes, ainsi que ${K'_{10}}^*$, mais ni Λ^*_{10}, ni K^*_{10} ne sont parfaits, vu l'inégalité $s < \frac{n(n+1)}{2}$. Les valeurs de l'invariant γ' sont $\gamma'(\Lambda_{10}) = \frac{8}{3}$, $\gamma'(K_{10}) = \frac{32}{9}$ et $\gamma'(K'_{10}) = 4$. On a donc l'inégalité stricte $\gamma'(L) < \frac{n+2}{3}$ pour $L \sim \Lambda_{10}$ et pour $L \sim K_{10}$, alors qu'il y a égalité dans le cas de K'_{10}. Ainsi, aucun des quatre réseaux Λ_{10}, Λ^*_{10}, K_{10}, K^*_{10} ne peut être fortement parfait. En revanche, un calcul sur machine utilisant le théorème 8.1 prouve:

Proposition 13.1. *Les réseaux K'_{10} et ${K'_{10}}^*$ sont fortement parfaits de type minimal.* □

On obtient ainsi deux réseaux fortement parfaits de dimension 10 ayant respectivement 135 et 120 couples de vecteurs minimaux.

On ne connaît pas de réseaux de dimension 10 d'invariant $\gamma' > 4$. En-dehors de K'_{10} et ${K'_{10}}^*$, l'égalité $\gamma'(L) = 4$ est connue seulement dans le cas des réseaux semblables à l'un des deux réseaux isoduaux $\mathbb{D}^+_{10}$ et Q_{10} (noté F_5 par Souvignier), dont on vérifie qu'ils ne sont pas fortement parfaits; c'est clair pour $\mathbb{D}^+_{10}$, qui a même ensemble de vecteurs minimaux que $\mathbb{D}_{10}$, et se vérifie à l'aide du corollaire 8.3 dans le cas de Q_{10}.

Le théorème et la conjecture ci-dessous ont été indiqués dans le cours:

THÉORÈME 13.2. *Un réseau fortement parfait de dimension* 10 *est de type minimal et d'invariant s égal à* 120 *ou à* 135.

CONJECTURE 13.3 [2]). *Un réseau fortement parfait de dimension* 10 *est semblable à* K'_{10} *ou à* ${K'_{10}}^*$.

14. Designs sphériques et problème de Waring. Le cas du réseau de Leech.

Nous traitons dans ce § la question suivante, mentionnée dans l'introduction: on cherche à représenter le polynôme homogène de degré 10 en n variables $(t_1^2+\cdots+t_n^2)^5$ comme somme de puissances 10-èmes de formes linéaires réelles (ou complexes), soit

$$(t_1^2+\cdots+t_n^2)^5 = \sum_{i=1}^{k} \lambda_i (x_{i,1}t_1+\cdots+x_{i,n}t_n)^{10}\,, \tag{14.1}$$

l'entier k étant le plus petit possible. On pose $x_i = (x_{i,1},\ldots,x_{i,n})$, et l'on suppose que les vecteurs ont tous la même longueur. On démontre alors:

THÉORÈME 14.2. *Pour* $n = 24$, *une telle représentation n'est possible que si l'on a* $k \geq 98280$, *et, s'il y a égalité, alors les coefficients* λ_i *sont égaux et les vecteurs* $\pm x_i$ *forment une configuration semblable à la configuration des vecteurs minimaux du réseau de Leech* Λ_{24}.

COROLLAIRE 14.3. *Les vecteurs minimaux du réseau de Leech forment un* 11*-design sphérique.* □

Démonstration du théorème 14.2. Nous étudions d'abord le cas d'une dimension n arbitraire, puis nous spécialiserons l'étude à la dimension $n = 24$. On note X l'ensemble des vecteurs x_i. L'hypothèse signifie que l'on a l'identité

$$\forall\, \alpha \in \mathbb{R}^n\,,\ \sum_{x\in X} \lambda_x (x,\alpha)^{10} = (\alpha,\alpha)^5\,. \tag{14.4 a}$$

Par applications successives de l'opérateur Δ_α aux deux membres de 14.4 a (cf. 1.5), on obtient les identités suivantes, que l'on utilisera avec $n = 24$

[2]) Cette conjecture vient d'être démontrée par Nebe et Venkov ([Ne-V1])

(14.4 b)
$$\sum_{x\in X}\lambda_x(x,\alpha)^8=\frac{n+8}{9}(\alpha,\alpha)^4\,,$$

(14.4 c)
$$\sum_{x\in X}\lambda_x(x,\alpha)^6=\frac{(n+8)(n+6)}{9.7}(\alpha,\alpha)^3\,,$$

(14.4 d)
$$\sum_{x\in X}\lambda_x(x,\alpha)^4=\frac{(n+8)(n+6)(n+4)}{9.7.5}(\alpha,\alpha)^2\,,$$

(14.4 e)
$$\sum_{x\in X}\lambda_x(x,\alpha)^2=\frac{(n+8)(n+6)(n+4)(n+2)}{9.7.5.3}(\alpha,\alpha)\,,$$

(14.4 f)
$$\sum_{x\in X}\lambda_x=\frac{(n+8)(n+6)(n+4)(n+2)n}{9.7.5.3.1}\,,$$

Rappelons la notation suivante, introduite au début du §1 : pour $x\in\mathbb{R}^n$, on note $\rho_x^{(m)}$ la forme linéaire $\alpha\mapsto(x,\alpha)^m$.

LEMME 14.5. *Supposons que l'on ait une identité de la forme 14.4 a, à savoir*
$$(\alpha,\alpha)^5=\sum_{x\in X}\lambda_x(x,\alpha)^{10}\,.$$
Alors, pour tout $v\in\mathbb{R}^n$, on a l'identité
$$\rho_v^{(5)}=\sum_{x\in X}\lambda_x(A(x,v)^5+B(x,v)^3(v,v)+C(x,v)(v,v)^2)\rho_x^{(5)}\,,$$
avec $A=\dfrac{3^2.7}{2^3}$, $B=-\dfrac{5.7.9}{4(n+8)}$, *et* $C=\dfrac{3.5.7.9}{2^3(n+8)(n+6)}$.

Admettons provisoirement ce lemme, et poursuivons la démonstration de 14.2. Le fait que tout polynôme homogène de degré 5 soit combinaison linéaire des $\rho_v^{(5)}$ et le lemme 14.5 entraînent la minoration $|X|\geq\dim\mathcal{F}_{n,5}=\binom{n+4}{n-1}$, cf. §1. Pour $n=24$, cette dimension est précisément 98280.

Nous démontrons maintenant un peu plus qu'il n'est nécessaire, en prouvant en plus que l'égalité $|X|=\dim\mathcal{F}_{n,5}=\binom{n+4}{5}$ n'est possible que pour $n=24$. Supposons donc l'égalité ci-dessus vérifiée. Alors, les $\rho_x^{(5)}$ forment une base de $\mathcal{F}_{n,5}$, et la décomposition du lemme est unique.

En appliquant le lemme à un vecteur $v = x_0 \in X$, on constate que λ_x ne dépend pas de x (on note alors λ la valeur commune), et que, pour $x_1 \neq x_0$ dans X, on a $\lambda(A(x_1,x_0)^5 + B(x_1,x_0)^3 + C(x_1,x_0))\rho^{(5)} = 0$. Cela signifie que (x_0,x_1) est nul ou que $(x_0,x_1)^2$ est racine du trinome AX^2+BX+C.

Soient η et η' les racines de ce trinome, et soit u (resp. u') le nombre d'éléments $x \in X$ avec $(x,x_0) = \eta$ (resp. $(x,x_0) = \eta'$). Les équations 14.4 a à 14.4 e prennent la forme d'un système linéaire de 5 équations en les 3 inconnues λ, $\mu = \lambda u$, $\mu' = \lambda u'$, de la forme $\lambda + \eta^i\mu + \eta'^i\mu' = \nu_i$ $(1 \leq i \leq 5)$. La compatibilité des équations s'écrit en annulant des déterminants d'ordre 4. Comme les vecteurs-colonne des second membres ne sont pas proportionnels pour deux valeurs distinctes de n, il y a au plus une possibilité pour n. On essaie alors $n = 24$, qui conduit à $\eta = \frac{1}{4}$ et $\eta' = \frac{1}{16}$, et l'on constate que, pour $n = 24$, il y a une unique solution en (λ,μ,μ'). En normalisant X à la norme 4, on voit par le calcul de η et de η' que les produits scalaires (x,x_0), $x \neq \pm x_0$ valent au signe près 0, 1 ou 2, et par le calcul de u et de u' que les nombres de vecteurs respectifs de X sont 46576, 47104 et 4600 (et l'on vérifie par le calcul de λ (on trouve $\lambda = \frac{512}{2835}$) la compatibilité avec 14.4 f).

On reconnaît là les multiplicités des valeurs des produits scalaires entre vecteurs minimaux du réseau de Leech, et nous allons prouver que X engendre effectivement un réseau isométrique à Λ_{24}.

Soit $\Gamma = \{\sum_{x\in X} n_x x \mid n_x \in \mathbb{Z}\}$ le sous-groupe de $\mathbb{R}^{24}$ engendré par X. Comme les produits scalaires entre vecteurs de Γ sont entiers, c'est un groupe discret, donc un réseau d'un sous-espace de $\mathbb{R}^{24}$. C'est même un réseau de $\mathbb{R}^{24}$, faute de quoi, pour le choix d'un vecteur α non nul dans $\Gamma^\perp$, le premier membre de 14.4 a serait nul, alors que le second ne le serait pas. C'est en outre un réseau entier, car il est engendré par des vecteurs de norme paire. On a donc l'inclusion $\Gamma \subset \Gamma^*$, et nous allons montrer qu'il s'agit en fait d'une égalité.

Sinon, soit $c \in \Gamma^* \smallsetminus \Gamma$ de norme minimale dans sa classe modulo Γ. On a alors $|(c,x)| \leq \frac{1}{2}(x,x) = 2$. (Sinon, en changeant x en $-x$, on peut supposer que l'on a $(c,x) > 2$; pour $c' = c - x$, on a $(c',c') - (c,c) = 4 - 2(c,x) < (c,c)$.) En notant m_1 (resp. m_2) le nombre de vecteurs $x \in X$ avec $(c,x) = 1$ (resp. $(c,x) = 2$), on obtient en substituant c à α dans 14.4 un nouveau système de 5 équations à 3 inconnues m_1, m_2 et t de la forme $m_1 + 2^{2i}m_2 = c_i t^i$ $(1 \leq i \leq 5)$, dont on vérifie cette fois qu'il est impossible. Par conséquent, un tel vecteur c n'existe pas, ce qui prouve que Γ est unimodulaire.

Explicitement, en posant $t = 2^2(c,c)$, on obtient le système $m_1 + 2^{10}m_2 = 5670t^5$, $m_1 + 2^8 m_2 = 5040t^4$, $m_1 + 2^6 m_2 = 5400t^5$, $m_1 + 2^4 m_2 = 7560t^5$, $m_1 + 2^2 m_2 = 16380t^5$.

L'équation 14.4 a, appliquée en prenant pour α un vecteur de norme 2 de Γ, s'écrit $\sum_{x\in X}(x,\alpha)^{10} = 2^5\lambda^{-1}$, égalité impossible, car le second membre n'est pas entier.

Par conséquent, Γ est un réseau unimodulaire pair de dimension 24 et de minimum $m \geq 4$. D'après un théorème de Conway (cf. [C-S], chapitre 12), Γ est isométrique au réseau de Leech. □

Démonstration du lemme 14.5. Supposons donc que l'on ait une identité de la forme 14.4 a:

$$(\alpha,\alpha)^5 = \sum_{x\in X} \lambda_x (x,\alpha)^{10}\,.$$

En l'appliquant à un élément $\alpha = \xi v + \eta t$ avec $\xi, \eta \in \mathbb{R}$, v (resp. t) désignant un vecteur fixe (resp. indéterminé) de $\mathbb{R}^n$, on obtient l'identité

$$(14.6)\qquad \left((v,v)\xi^2 + 2(v,t)\xi\eta + (t,t)\eta^2\right)^5 = \sum_{x\in X} \lambda_x \left((x,v)\xi + (x,t)\eta\right)^{10}\,,$$

dont les deux membres sont des polynômes de degré 10. En comparant les coefficients des termes en $\xi^5\eta^5$, on obtient après simplification la nouvelle identité

$$\sum_x \lambda_x (x,v)^5\,(x,t)^5 =$$

$$(*)\qquad \frac{2^3}{9.7}(v,t)^5 + \frac{2^3.5}{9.7}(v,t)^3(v,v)(t,t) + \frac{5}{3.7}(v,t)(v,v)^2(t,t)^2\,.$$

En appliquant à 14.4 b le procédé qui a permis de déduire 14.6 de 14.4 a, on obtient l'identité

$$(14.7)\qquad \left((v,v)\xi^2 + 2(v,t)\xi\eta + (t,t)\eta^2\right)^4 = \sum_{x\in X} \lambda_x \left((x,v)\xi + (x,t)\eta\right)^8\,,$$

dont les deux membres sont des polynômes de degré 8. En comparant les coefficients des termes en $\xi^3\eta^5$, il vient

$(**)$

$$\sum_x \lambda_x (x,v)^3\,(x,t)^5 = \frac{(n+8)}{3.7}(v,t)(v,v)(t,t)^2 + \frac{2^2(n+8)}{9.7}(v,t)^3(t,t)\,.$$

La même méthode, mais en partant cette fois de 14.4 c, entraîne l'identité

$$(14.8) \qquad \left((v,v)\xi^2 + 2(v,t)\xi\eta + (t,t)\eta^2\right)^3 = \sum_{x\in X} \lambda_x \left((x,v)\xi + (x,t)\eta\right)^6 ,$$

dont les deux membres sont des polynômes de degré 6. En comparant les coefficients des termes en $\xi\eta^5$, il vient

$$(***) \qquad \sum_x \lambda_x(x,v)\,(x,t)^5 = \frac{(n+8)(n+6)}{9.7}(v,t)(t,t)^2$$

Effectuons maintenant la combinaison

$$(14.9) \qquad \frac{9.7}{2^3}\,(*) - \frac{5.7.9}{4(n+8)}\,(v,v)\,(**) + \frac{3.5.7.9}{2^3(n+8)(n+6)}\,(v,v)^2\,(***)\,.$$

On voit tout de suite que le membre de gauche est égal au second membre de la formule de 14.5. Quant au membre de droite, on voit qu'il contient d'une part un terme en $(v,v)^5$ provenant de $(*)$ et affecté du coefficient 1, et d'autre part deux termes en $(v,t)^3(v,v)(v,t)$ et trois termes $(v,t)(v,v)^2(v,t)^2$, dont on vérifie qu'ils se détruisent. Le second membre de 14.9 est donc bien égal à $\rho_v^{(5)}$. □

15. Applications à l'analyse fonctionnelle.

On rappelle qu'un *espace de Banach (réel)* est un espace vectoriel normé complet sur $\mathbb{R}$. Nous nous intéressons ici à des espaces de suites. On note ℓ_p (ou ℓ_p^∞) l'espace des suites réelles $x = (x_1, \ldots, x_n, \ldots)$ de puissance p-ième absolument sommable, que l'on munit de la norme $\|x\|_p = (\sum_{i=1}^\infty |x_i|^p)^{1/p}$. On note ℓ_p^N le sous-espace de ℓ_p^∞ formée des suites dont tous les termes sont nuls à partir du rang $N+1$, espace que l'on identifie à $\mathbb{R}^N$.

Le cas $p = 2$ est particulièrement intéressant, puisqu'il s'agit d'un espace de Hilbert, de produit scalaire $(x,y) = \sum_{i=1}^\infty x_i y_i$.

Soient deux espaces ℓ_p^N et ℓ_q^M. On s'intéresse à l'existence d'*immersions* $\ell_p^N \hookrightarrow \ell_q^M$, c'est-à-dire d'applications linéaires injectives conservant la norme.

Un théorème non constructif de Dvoretski (cf. [L-V]) affirme l'existence d'immersions de ℓ_2^∞ dans ℓ_q^∞ pour tout q. Il est intéressant d'obtenir des résultats explicites pour les dimensions finies.

L'étude de l'ensemble X des vecteurs minimaux du réseau de Leech permet de considérer le cas des paramètres $p = 2$, $N = 24$, $q = 10$,

$M = 98280$: le fait que les polynômes $(\alpha,\alpha)^5$ et $\sum_{x\in X}(x,\alpha)^{10}$ soient proportionnels entraîne l'existence d'une constante réelle c telle que l'on ait l'identité

$$(\alpha,\alpha) = c\left(\sum_{x\in X}(x,\alpha)^{10}\right)^{1/10},$$

ce qui prouve l'existence du plongement.

La situation est analogue dans le cas du réseau $\mathbb{E}_8$, avec les paramètres $p=2,\ N=8,\ q=8,\ M=120$.

16. Réseaux unimodulaires et formes modulaires.

Les *formes modulaires* sont des fonctions complexes définies sur le demi-plan supérieur et qui, outre certaines propriétés régularité, vérifient certaines formules de transformation sous l'action homographique d'un sous-groupe Γ d'indice fini de $\mathrm{SL}_2(\mathbb{Z})$. Ici, nous n'utiliserons que les formes pour lesquelles Γ est le groupe $\mathrm{SL}_2(\mathbb{Z})$ tout entier. De ce fait, le lecteur trouvera l'essentiel de ce dont il a besoin dans le livre de Serre ([Se], chapitre VII); nous renvoyons également à celui de Ogg ([Ogg]; voir en particulier le chapitre VI) pour quelques compléments.

La plupart des résultats de ce § se trouvent déjà dans l'article [V2], datant de 1984.

On considère un réseau Λ de $\mathbb{R}^n$, dont on note S l'ensemble des vecteurs minimaux, et l'on suppose que Λ est fortement parfait, autrement dit que S est un 5-design sphérique, ce qui revient à dire que, pour tout polynôme homogène harmonique non constant P sur $\mathbb{R}^n$ de degré $\deg(P)\leq 5$, on a $\sum_{x\in S}P(x)=0$.

On sait (§6) qu'un tel réseau est *rationnel*, c'est-à-dire proportionnel à un réseau entier. Nous normalisons Λ de façon qu'il soit pair. Pour tout entier k, on note Λ_k l'ensemble des éléments de Λ de norme k, ensemble qui ne peut être non vide que si k est pair. On pose alors

$$a_k(P) = \sum_{x\in\Lambda_{2k}} P(x),$$

et l'on associe à Λ et à P la *série génératrice de la suite* (a_k), à savoir la série formelle

$$\Theta_{\Lambda,P} = \sum_{k\in\mathbb{N}} a_k(P)q^k \in \mathbb{R}[[q]].$$

Si $p = 1$, il s'agit alors de la *série* Θ usuelle du réseau Λ.

Soit $D = \Lambda^*/\Lambda$, groupe que l'on munit de la forme quadratique $x \mapsto d(x) = \frac{1}{2}(x,x)$ à valeurs dans $\mathbb{Q}/\mathbb{Z}$. Soit ℓ l'annulateur de D ; c'est aussi le plus petit entier pour lequel ℓd est la forme quadratique nulle; on l'appelle le *niveau de* Λ. Nous intéresserons ici aux réseaux de niveau 1 ; ce sont les réseaux unimodulaires pairs.

On fait de la série Θ définie ci-dessus une fonction d'une variable complexe z définie sur le demi-plan supérieur (ou demi-plan de Poincaré) $\mathcal{H}$ en posant $q = e^{2i\pi z}$. Noter que la condition $z \in \mathcal{H}$ équivaut à $|q| < 1$, et assure la convergence de la série thêta, cf. [Ogg].

Rappelons qu'une *forme modulaire de poids* ϖ *(pour le groupe* $\Gamma = \mathrm{SL}_2(\mathbb{Z})$*)* est une fonction f holomorphe sur $\mathcal{H}$, se transformant sous l'action des homographies associées aux éléments $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ de Γ par la formule

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^{\varpi} f(z)\,,$$

et qui est en outre "holomorphe aux pointes de Γ", ce qui signifie ici simplement qu'elle est bornée sur les bandes verticales. On dit que f est *parabolique* si elle s'annule "aux pointes de Γ", c'est-à-dire si elle tend vers 0 à l'infini dans les directions verticales. L'holomorphie aux pointes se traduit par l'existence d'un développement en série de Fourier de la forme

$$f(z) = \sum_{p=0}^{\infty} a_p(f)\, e^{2i\pi x}\,;$$

les formes paraboliques sont alors caractérisées par la condition $a_0(f) = 0$.

L'ensemble des formes modulaires (resp. paraboliques) de poids ϖ, auquel on adjoint le forme nulle, est un espace vectoriel complexe, noté $\mathcal{M}_\varpi$ (resp. $\mathcal{S}_\varpi$).

THÉORÈME 16.1 (Schoeneberg; cf. [Ogg]). *Soit* Λ *un réseau unimodulaire pair de dimension* n*, et soit* P *un polynôme harmonique homogène. Alors,* $\Theta_{\Lambda,P}$ *est une forme modulaire de poids* $\frac{n}{2} + \deg(P)$*. C'est une forme parabolique si* $\deg(P) > 0$. □

On montre (cf. [Se], chapitre VII, théorème 4 et son corollaire 1; toutefois, Serre note k ce que nous notons $2k$) que le poids est un entier $2k \geq 0$ pair, et que l'on a la *formule de dimension*

$$\dim \mathcal{M}_{2k}(\mathrm{SL}_2(\mathbb{Z})) = \left\lfloor \frac{2k}{12} \right\rfloor \quad \text{ou} \quad \left\lfloor \frac{2k}{12} \right\rfloor + 1$$

selon que l'on a $2k \equiv 2 \mod 12$ ou $2k \not\equiv 2 \mod 12$. (Le poids 2 est impossible.) Nous aurons besoin aussi du résultat classique suivant :

THÉORÈME 16.2. *La dimension d'un réseau unimodulaire pair est un multiple de* 8. □

[Ce théorème peut se démontrer à l'aide de la théorie des formes modulaires. On trouvera dans [Se], ch. V, une démonstration purement algébrique de ce résultat, consistant à en généraliser l'énoncé de façon à y inclure les "réseaux indéfinis" non nécessairement pairs, puis à traiter le cas indéfini à l'aide d'un théorème de classification.]

En exhibant une base de l'espace des formes modulaires de poids ϖ donné ([Se], corollaire 2 au théorème 4 du chapitre VII), on montre qu'il existe une unique forme modulaire pour $\mathrm{SL}_2(\mathbb{Z})$ de poids ϖ donné dont les coefficients $a_0, \ldots, a_{r-1}$ ($r = \dim \mathcal{M}_\varpi(\mathrm{SL}_2(\mathbb{Z}))$ ont une valeur donnée. On montre en outre que, pour le choix $a_1 = \cdots = a_{r-1} = 0$ (et $a_0 = 1$), le coefficient a_r est non nul. Il en résulte que, si Λ est un réseau unimodulaire pair dépourvu de vecteurs de norme $2, \ldots, 2r-2$, alors le nombre de vecteurs de norme k donnée de Λ est déterminé de façon unique quelque soit k.
[Le fait que le coefficient a_r soit non nul, et même strictement positif, peut être extrait de l'article [Sg], dans lequel Siegel démontre l'existence pour toute forme de poids $2r$ d'une relation de dépendance $c_0 a_0 + \cdots + c_r a_r = 0$ à coefficients c_i entiers ([Sg], théorème 1), avec en outre $c_r = 1$ ([Sg], formules (5) et (10)) et $c_0 < 0$ ([Sg], fin de la démonstration du théorème 2).]

DÉFINITION 16.3. Un réseau unimodulaire pair de minimum $2r$ est dit *extrémal*.

En dimension 8 et 16, les réseaux extrémaux sont les réseaux $\mathbb{D}_8^+ = \mathbb{E}_8$, $\mathbb{E}_8 \perp \mathbb{E}_8$ et $\mathbb{D}_{16}^+$, de minimum 2 (notations de [C-S] ou [M], chapitre 4). En dimension 24, le minimum passe à 4 (les sauts de dimension de l'espace des formes modulaires ont lieu pour les dimensions de Λ multiples de 24). L'unique réseau extrémal est alors le réseau de Leech (théorème de Conway, cf. [C-S], chapitre 12). Le minimum est encore 4 en dimension 32 et 40, puis devient 6 en dimension 48 (où 3 réseaux sont connus), 56, 64, etc. On

connaît des réseaux extrémaux seulement dans les dimensions 8 à 64 et 80, le premier cas ouvert se présentant en dimension 72 (pour le minimum 8). On sait par ailleurs ([M-O-S], [V2]) qu'il n'existe pas de réseaux extrémaux de dimension arbitrairement grande. (À isométrie près, il n'existe donc qu'un nombre fini de réseaux unimodulaires pairs extrémaux.)

Le rôle des multiples de 24 apparaît dans l'énoncé suivant (que nous connaissons déjà jusqu'à la dimension 24), qui nous oblige à distinguer trois cas, selon que $n = \dim \Lambda$ est congru à 0, 8 ou 16 modulo 24.

THÉORÈME 16.4. *Soit Λ un réseau (unimodulaire, pair) extrémal, d'ensemble de vecteurs minimaux S.*

(1) Si $n \equiv 0 \mod 24$, S est un 11-design sphérique.

(2) Si $n \equiv 8 \mod 24$, S est un 7-design sphérique.

(3) Si $n \equiv 16 \mod 24$, S est un 3-design sphérique. En particulier, ces réseaux sont tous fortement eutactiques, et ceux de dimension non congrue à 16 modulo 24 sont fortement parfaits.

REMARQUE 16.5. On peut être un peu plus précis: les valeurs $t = 3$, $t = 7$, $t = 11$ qui apparaissent dans l'énoncé ne peuvent pas être en général améliorées (nous le savons jusqu'à la dimension 24; voir aussi la remarque 16.8 ci-dessous), mais les sommes $\sum_{x \in S} P(x)$ sont encore nulles lorsque P est harmonique de degré $t+3$, et aussi évidemment $t+2$ et $t+4$. On dit alors que S est un $(t+\frac{1}{2})$-*design sphérique*.

Démonstration. Avant de passer à la démonstration proprement dite du théorème et de la remarque qui suit, nous rappelons quelques propriétés de l'algèbre des formes modulaires sur $\mathrm{SL}_2(\mathbb{Z})$. C'est une algèbre graduée (par le poids), qui s'identifie en tant qu'algèbre graduée à l'algèbre des polynômes $\mathbb{C}[E_4, E_6]$, où E_4, E_6, de poids respectifs 4 et 6, sont les deux premières *séries d'Eisenstein*

$$E_4 = 1 + 240q + \dots \quad \text{et} \quad E_6 = 1 - 504q + \dots ,$$

normalisées pour prendre la valeur 1 à la pointe ∞, cf. [Se], chapitre VII, corollaire 2 au théorème 4 et n° 4.2. (Noter que E_4 est la série thêta du réseau $\mathbb{E}_8$, cf. [Se], chapitre VII, n° 6.6, mais que E_6, qui possède des coefficients négatifs, n'est pas la série thêta d'un réseau.) Une forme modulaire de poids ϖ est donc un polynôme isobare de poids ϖ en E_4, E_6, somme de monomes $E_4^\alpha E_6^\beta$ avec $4\alpha + 6\beta = \varpi$. En particulier, une forme

parabolique est de poids multiple de 12, les formes paraboliques de poids 12 étant proportionnelles à

$$\Delta = \frac{1}{1728}(E_4^3 - E_6^2) = q - 24q^2 + \cdots = \sum_{n=1}^{\infty} \tau(n) q^n \,.$$

(On a $1728 = 12^3$; $n \mapsto \tau(n)$ est la *fonction de Ramanujan.*)

Plus généralement, les formes $\sum a_n q^n$ avec $a_0 = \cdots = a_k = 0$ sont les multiples de Δ^{k+1}.

On considère donc un réseau Λ de dimension $n = 24k + \varepsilon$, $\varepsilon = 0$, 8 ou 16, qui est extrémal, ce qui équivaut à la condition $N(\Lambda) = 2k + 2$. Sa série thêta est une forme modulaire de poids $12k + \frac{\varepsilon}{2}$, qui s'exprime comme la valeur d'un polynôme isobare Q en E_4 et E_6 : on a

$$\Theta_\Lambda = Q(E_4, E_6) = 1 + a_{k+1} q^{k+1} + a_{k+2} q^{k+2} \ldots ,$$

et les coefficients $a_m = |\Lambda_{2m}|$ ne dépendent pas de Λ, étant déterminés par les $k + 1$ conditions $a_0 = 1$, $a_1 = \cdots = a_k = 0$. Rappelons que le coefficient a_{k+1} est non nul, et même strictement positif.

Au réseau Λ et à un polynôme harmonique P, on associe la fonction thêta

$$\Theta_{\Lambda,P} = \sum_{p=1}^{\infty} \Big(\sum_{x \in \Lambda_{2p}} P(x) \Big) q^p \ ; \tag{16.6}$$

si elle est non nulle, c'est une forme modulaire de poids $\frac{n}{2} + \deg P$. Si en outre P est non constant, ses coefficients a_i, $i \leq k$ sont nuls (a_0 parce que $P(0) = 0$, les autres parce que Λ_i est vide). Il en résulte qu'elle est de la forme $\Delta^{k+1} h$, où h est une forme modulaire dont nous notons ϖ le poids lorsqu'elle n'est pas nulle. Ainsi, si la série (16.6) est non nulle, on a

$$12k + \varepsilon/2 + \deg P = 12(k+1) + \varpi \,. \tag{16.7}$$

Posons $t = 11, t = 7, t = 3$ selon que l'on a $\varepsilon = 0, \varepsilon = 8, \varepsilon = 16$. On a $t + 1 = 12 - \varepsilon/2$; la relation 16.7 prend alors la forme

$$\deg P = t + 1 + \varpi \,,$$

qui entraîne l'alternative

$$\deg P > t \quad \text{ou} \quad \forall\, p > 0, \sum_{x \in \Lambda_{2p}} P(x) = 0 \,.$$

En particulier, la somme $\sum_{x\in\Lambda_{2k+2}} P(x)$ est nulle pour tout polynôme harmonique non constant de degré au plus t, ce qui est l'assertion du théorème 16.4. En outre, comme il n'existe pas de forme modulaire de poids 2, l'égalité 16.7 est impossible avec $\deg P = t+3$. En conséquence, la somme $\sum_{x\in\Lambda_{2k+2}} P(x)$ est également nulle pour $\deg P = t+3$, ce qui justifie la remarque 16.5. □

REMARQUE 16.8. La question de savoir s'il est possible qu'un réseau extrémal soit un $(t+1)$-design ($t \in \{11, 7, 3\}$ comme ci-dessus) est ouverte pour la plupart des dimensions. Quelques résultats d'impossibilité figurent dans [Mar1], § 4. En particulier, en dimension 40, S n'est jamais un 4-design sphérique; autrement dit, les réseaux extrémaux de dimension 40 ne sont pas fortement parfaits. Cela n'empêche pas que certains d'entre eux soient parfaits.

REMARQUE 16.9. Des résultats analogues au théorème 16.4 existent dans le cas de certains réseaux *ℓ-modulaires* au sens de Quebbemann (réseaux L entiers pairs tels qu'il existe une similitude de rapport $\sqrt{\ell}$ appliquant L^* sur L), en particulier lorsque $\ell = 2$ ou $\ell = 3$ (le cas $\ell = 1$ est celui des réseaux unimodulaires). Cela s'applique par exemple avec $\ell = 2$ au réseau de Barnes-Wall Λ_{16} et aux réseaux de Bachoc, de Nebe, et de Quebbemann de dimension 32 et de minimum 6, et avec $\ell = 3$ au réseau K_{12} de Coxeter-Todd. Pour les détails, nous renvoyons le lecteur à l'article [Bc-V] de C. Bachoc et B. Venkov.

17. SECTIONS FORTEMENT PARFAITES DE RÉSEAUX UNIMODULAIRES.

Le théorème 16.4 ne concerne que des réseaux extrémaux. On peut cependant construire des réseaux fortement parfaits par section à partir de réseaux unimodulaires pairs non extrémaux. Un des cas les plus intéressants est le suivant :

THÉORÈME 17.1. *Soit Λ un réseau unimodulaire pair de dimension 32 dont l'ensemble $\mathcal{R}$ des racines constitue un système irréductible de l'un des types $\varnothing$, $\boldsymbol{A}_1$, $\boldsymbol{A}_2$, $\boldsymbol{D}_4$, $\boldsymbol{E}_6$, $\boldsymbol{E}_7$, $\boldsymbol{E}_8$. On note E le sous-espace de $\mathbb{R}\bigotimes\Lambda \simeq \mathbb{R}^{32}$ engendré par $\mathcal{R}$ et $\Gamma = E^\perp \cap \Lambda$ la section de Λ par l'orthogonal $E^\perp$ de E. Alors, Γ est un réseau fortement parfait.*

Avant de commencer la démonstration proprement dite, nous faisons quelques rappels. Désignons par Λ_m l'ensemble des vecteurs de Λ de norme m. Alors, Λ_2 est l'ensemble des *racines de* Λ (vecteurs indivisibles de Λ tels que la réflexion orthogonale qu'ils définissent stabilise Λ). On note $Q(\mathcal{R})$ le sous-réseau de Λ engendré par $\mathcal{R}$ (de dimension en général plus petite que celle de Λ) et $P(\mathcal{R}) = Q(\mathcal{R})^*$ le réseau dual de $Q(\mathcal{R})$ dans $\mathbb{R}\bigotimes Q(\mathcal{R})$; c'est le *réseau des poids*. Rappelons aussi qu'un poids $\lambda \in P(\mathcal{R})$ est dit *minuscule* si les produits scalaires (λ, r) ne prennent que les valeurs $0, \pm 1$ sur $\mathcal{R}$.

On remarque que la liste des systèmes de racines non vides qui intervient dans l'énoncé du théorème est exactement la liste des systèmes de racines dont les poids minuscules non nuls ont une même norme. En fait, 0 est l'unique poids minuscule de $\boldsymbol{E}_8$; dans le cas des sytèmes $\boldsymbol{A}_1$, $\boldsymbol{A}_2$, $\boldsymbol{D}_4$, $\boldsymbol{E}_6$, $\boldsymbol{E}_7$, ces normes sont $\frac{1}{2}$, $\frac{2}{3}$, 1, $\frac{4}{3}$, $\frac{3}{2}$ respectivement, cf. [Bou], chapitre VI, § 1, exercice 24 et § 4, exercice 15.

Démonstration du théorème 17.1. Nous allons utiliser les formules suivantes, qui se trouvent dans [V3] et [V4], valables pour n'importe quel réseau unimodulaire pair de dimension 32 ; dans ces formules, on a $X = \Lambda_4$, $\mathcal{R} = \Lambda_2$, et α est arbitraire dans $\mathbb{R}^{32}$:

$$\sum_{x\in X}(x,\alpha)^4 = (2^2.3^2\,|R| + 2^4.3^4.5)\,(\alpha,\alpha)^2$$
$$+ 2^3.3.19\sum_{r\in R}(r,\alpha)^4 - 2^3.3^2.7\,(\alpha,\alpha)\sum_{r\in R}(r,\alpha)^2\,; \tag{17.2}$$

$$\sum_{x\in X}(x,\alpha)^6 = (2.3.5\,|R| + 2^4.3^2.5^2)\,(\alpha,\alpha)^3 - 2^6.3^2\sum_{r\in R}(r,\alpha)^6$$
$$+ 2^2.3^2.5^2\,(\alpha,\alpha)\sum_{r\in R}(r,\alpha)^4 - 2^2.3^3.5\,(\alpha,\alpha)^2\sum_{r\in R}(r,\alpha)^2\,. \tag{17.3}$$

[Ces formules, qui peuvent être considérées comme une extension par l'adjonction de termes correctifs des formules plus simples du cas extrémal, s'obtiennent ainsi: pour $\alpha \in \mathbb{R}^{32}$ donné, on considère les polynômes de Gegenbauer

$$P^\alpha_{2m}(x) = (x,\alpha)^{2m} + c_1(x,x)\,(\alpha,\alpha)\,(x,\alpha)^{2m-2} + \dots$$

relatifs à α, c'est-à-dire les polynômes harmoniques de degré $2m$ de terme dominant $(x,\alpha)^{2m}$; les séries thêta de Λ à coefficients P^α_{2m} sont des formes modulaires paraboliques de poids $16+2m$ pour le groupe $\mathrm{SL}_2(\mathbb{Z})$; pour $m = 2, 3$, l'espace des formes paraboliques de poids $16+2m$ est de dimension 1 ; les formules 17.2 et 17.3 en résultent.]

Posons $F = E^{\perp}$ (orthogonal de E dans $\mathbb{R}^{32}$) (on a donc une décomposition orthogonale $\mathbb{R}^{32} = E \perp F$). Pour tout $\alpha \in \mathbb{R}^{32}$, notons α_1 et α_2 les projections orthogonales respectives de α sur E et sur F. Posons

$$X_E = X \cap E \quad \text{et} \quad X_F = X \cap F$$

(on rappelle que $X = \Lambda_4$ est l'ensemble des vecteurs de norme 4 de Λ), et soit $X_\xi = X \smallsetminus (X_E \cup X_F)$, ensemble des vecteurs de norme 4 de X qui ne sont ni dans E, ni dans F. Tout $x \in X_\xi$ définit un poids sur $\mathcal{R}$, qui est non nul, puisque $x \notin F$. C'est un poids minuscule: en effet, il existerait sinon $r \in \mathcal{R}$ avec $|(x,r)| \geq 2$, donc $|(x,r)| = 2$, vu la majoration $(x,r)^2 \leq (x,x)\,(r,r) = 8$; mais si $(x,r) = \pm 2$, alors $x \mp r$ est une racine; il s'en suit que $x = \pm r + (x \mp r)$ est somme de deux racines (orthogonales), d'où $x \in E$, i.e., $x \in X_E$, contrairement à l'hypothèse $x \in X_\xi$.

Comme dans notre situation tous les poids minuscules non nuls sont de même norme, que nous notons ξ (d'où la notation X_ξ), on a

$$(x_1, x_1) = \xi \qquad \text{pour tout } x \in X_\xi\,,$$

et donc

$$(x_2, x_2) = 4 - \xi \qquad \text{pour tout } x \in X_\xi\,.$$

Appliquons maintenant les formules 17.2 et 17.3 en prenant α dans F. On a alors $(x,\alpha) = (x_2,\alpha)$ et $(\alpha, r) = 0$ pour tout $r \in \mathcal{R}$, ce qui donne les deux relations

$$\sum_{x \in X} (x_2,\alpha)^4 = c_1\,(\alpha,\alpha)^2 \tag{17.4}$$

et

$$\sum_{x \in X} (x_2,\alpha)^6 = c_2\,(\alpha,\alpha)^3 \tag{17.5}$$

dans lesquelles c_1 et c_2 sont deux constantes qu'il est inutile d'expliciter. Si $x \in X_E$, on a $x_2 = 0$, si bien que les éléments de X_2 ne donnent pas de contribution aux sommes précédentes, que l'on peut de ce fait écrire en mettant en évidence les parties X_F et X_ξ de notre partition de X :

$$\sum_{x \in X_F} (x,\alpha)^4 + \sum_{x \in X_\xi} (x_2,\alpha)^4 = c_1(\alpha,\alpha)^2\,; \tag{17.6}$$

$$\sum_{x \in X_F} (x,\alpha)^6 + \sum_{x \in X_\xi} (x_2,\alpha)^6 = c_2(\alpha,\alpha)^3\,. \tag{17.7}$$

[Noter que $x = x_2$ si $x \in F$.]

Transformons maintenant la formule 17.7 en lui appliquant l'opérateur de Laplace relatif à F par raport à x : on obtient (cf. exemple 1.5) l'identité

$$6.5.4 \sum_{x\in X_F}(x,\alpha)^4 + 6.5.(4-\xi)\sum_{x\in X_\xi}(x_2,\alpha)^4 = c_3(\alpha,\alpha)^2 \tag{17.8}$$

de degré 4, dans laquelle c_3 désigne une nouvelle constante.

Les identités 17.6 et 17.8 peuvent s'interpréter comme un système linéaire dont les inconnues sont les sommes sur X_F et sur X_ξ. Comme $\xi \neq 0$, c'est un système de Cramer. On en déduit en particulier l'existence d'une identité de la forme

$$\sum_{x\in X_F}(x,\alpha)^4 = d\,(\alpha,\alpha)^4$$

où d est une nouvellle constante, ce qui démontre que $\Gamma = \Lambda \cap F$ est fortement parfait. □

Remarque 17.9. De la démonstration ci-dessus, on déduit également l'existence d'une formule

$$\sum_{x\in X_\xi}(x,\alpha)^4 = e\,(\alpha,\alpha)^4 \tag{17.10}$$

dans laquelle e est une constante, mais cela ne suffit pas à démontrer que la projection $pr_F(X_\xi)$ de X_ξ sur F est un 4-design sphérique, à cause de la présence possible de multiplicités dans le premier membre de 17.10. Toutefois, une étude cas par cas permet de vérifier d'une part que les multiplicités sont constantes, et d'autre part que $pr_F(X_\xi)$ est l'ensemble des vecteurs minimaux du réseau dual de $\Gamma = \Lambda \cap F$, ce qui montre que le réseau dual de Γ est aussi fortement parfait.

Commentaires.

(1) Lorsque $\mathcal{R} = \boldsymbol{D}_4, \boldsymbol{E}_6, \boldsymbol{E}_7, \boldsymbol{E}_8$, les réseaux Γ du théorème 17.1 sont connus. En fait, il s'agit de réseaux pairs de minimum 4, de dimensions $28, 26, 25, 24$ et de déterminants $4, 3, 2, 1$.

Lorsque $\mathcal{R} = \boldsymbol{D}_4$, on montre que ce sont exactement les parties paires des réseaux unnimodulaires de dimension 28 sans racine et de *type général* (i.e., sans vecteur caractéristique de norme 4). Ces réseaux on été classés par Bacher et Venkov ([Ba-V]) ; il y en a 31 parmi les 33 réseaux énumérés dans [Ba-V].

Lorsque $\mathcal{R} = \boldsymbol{E}_6$, Γ est un réseau pair sans racine de déterminant 3. Borcherds a montré dans sa thèse ([Bo]) qu'il existe un unique réseau de ce type.

Lorsque $\mathcal{R} = \boldsymbol{E}_7$, Γ est un réseau pair sans racine de déterminant 2. Borcherds a montré dans sa thèse qu'il n'existe pas de tels réseaux; il n'existe donc pas de réseaux unimodulaires pairs de dimension 32 de système de racines $\boldsymbol{E}_7$.

Lorsque $\mathcal{R} = \boldsymbol{E}_8$, Γ est évidemment le réseau de Leech Λ_{24}.

(2) En revanche, le cas où $\mathcal{R}$ est l'un des systèmes $\boldsymbol{A}_1$ ou $\boldsymbol{A}_2$ conduit à des réseaux qui ne sont pas classés, et qui sont assez nombreux.

Le cas de $\mathcal{R} = \boldsymbol{A}_1$ est le plus intéressant. En effet, $\Gamma = \Lambda \cap F$ est un réseau pair de dimension 31, de déterminant 2 et de minimum 4, et les réseaux Γ et Γ^* sont tous deux fortement parfaits. On montre que l'on peut munir l'ensemble des couples $\pm x$ de vecteurs minimaux des réseaux Γ^* d'une structure de graphe, qui est un graphe fortement régulier possédant les mêmes paramètres que les graphes géométriques construits à partir de systèmes de sextuples de Steiner sur 496 points. Pour plus de détails, nous renvoyons le lecteur à [V1].

18. Les réseaux de Barnes-Wall.

Il s'agit de réseaux de dimensions $n = 2^d$, $d \geq 3$, notés BW_{2^d}, dont la définition est rappelée ci-dessous. Dans une normalisation convenable, ils sont alternativement unimodulaires et 2-modulaires. Le début de la série a déjà été rencontré: on a $\mathrm{BW}_8 \simeq \mathbb{E}_8$, BW_{16} est le réseau laminé Λ_{16}, et BW_{32} est un réseau unimodulaire pair extrémal.

J. Nottebaum a montré dans son *Diplomarbeit* ([Nt]) que ces réseaux sont fortement parfaits. Le théorème ci-dessous est un peu plus précis que son résultat:

Théorème. *Les ensembles de vecteurs minimaux des réseaux de Barnes-Wall de dimension $n \geq 8$ sont des 7-designs sphériques.*

Le théorème ci-dessus montre qu'il s'agit d'une famille *infinie* de réseaux fortement parfaits. Pour l'instant, c'est la seule famille connue de réseaux fortement parfaits de dimensions non bornées. On notera que, en tant que réseaux 1- ou 2-modulaires, les réseaux de Barnes-Wall ne sont

extrémaux que jusqu'à la dimension 32. Les méthodes modulaires du §16 ne s'appliquent donc pas au-delà de la dimension 32.

Soit $d \geq 3$ un entier; on note m la partie entière de $\frac{d}{2}$. Dans l'espace euclidien E^{2^d} de dimension $n = 2^d$, on considère une base orthogonale (e_a) indexée par $\mathbb{F}_2^d$ et normalisée par $(e_a, e_a) = 2^{-m}$; en interprétant e_a comme la fonction caractéristique de $\{a\} \subset \mathbb{F}_2^d$, on identifie $\mathbb{F}_2^{2^d}$ à l'ensemble des applications $\mathbb{F}_2^d \to \mathbb{F}_2$.

On désigne par $\mathcal{G}_{d,\ell}$ l'ensemble des sous-espaces <u>affines</u> de dimension ℓ de $\mathbb{F}_2^d$ et par $\mathcal{R}(d,\ell)$ le sous-espace de $\mathbb{F}_2^d$ engendré par $\mathcal{G}_{d,\ell}$; c'est le *code de Reed-Muller*. Pour d fixé, les $\mathcal{R}(d,\ell)$ forment une suite emboîtée de codes linéaires binaires de longueur 2^d.

Pour un sous-ensemble v de $\mathbb{F}_2^d$, soit

$$[v] = \sum_{a \in v} e_a \in E^{2^d}.$$

DÉFINITION 18.1. Le *réseau de Barnes-Wall* BW_n est le réseau de E^{2^d} engendré par les $2^{m-k}[v]$, où $v \in \mathcal{R}(d, 2k)$ et $k = 0, \ldots, m$ $(m = \lfloor \frac{d}{2} \rfloor)$.

On notera que, pour $v \in \mathcal{G}_{d,2k}$, la norme de $2^{m-k}[v]$ est égale à $2^{2(m-k)}\, 2^{2k}\, 2^{-m} = 2^m$.

Voici quelques propriétés des réseaux de Barnes-Wall; pour plus de détails, voir l'article [B-E] de Broué et Enguehard.

Le réseau $BW_n = BW_{2^d}$ est pair de norme 2^m et son groupe d'automorphismes opère transitivement sur l'ensemble S_d de ses éléments de norme 2^m. La structure de S_d est connue. En fait, pour $A \subset \mathbb{F}_2^d$, soit

$$\begin{aligned} \varepsilon_a : E^{2^d} &\to E^{2^d} \\ e_a &\to \begin{cases} e_a \text{ si } a \notin A \\ -e_a \text{ si } a \in A \end{cases}, \end{aligned}$$

et, pour $v \in \mathcal{G}_{d,\ell}$, désignons par $S_d(v)$ l'ensemble des éléments de S_d de la forme $2^{m-k}\varepsilon_A[v]$ où A est tel que ε_A est un automorphisme de BW_d. Alors, on a $S_d(v) \subset S_d$, et

$$|S_d(v)| = 2^{1+2k+(2k-1)k} \tag{18.2}$$

est indépendant de $v \in \mathcal{G}_{d,2k}$. De plus,

$$S_d = \bigcup_{k=0}^{m} \bigcup_{v \in \mathcal{G}_{d,2k}} S_d(v) \tag{18.3}$$

et par conséquent

$$|S_d| = \sum_{k=0}^{m} 2^{1+2k+(2k-1)k} \begin{bmatrix} d \\ 2k \end{bmatrix}_2 2^{d-2k} = 2^{d+1} \sum_{k=0}^{m} 2^{(2k-1)k} \begin{bmatrix} d \\ 2k \end{bmatrix}_2 , \tag{18.4}$$

où

$$\begin{bmatrix} d \\ \ell \end{bmatrix}_2 = \frac{(2^d - 1) \dots (2^{d-\ell+1} - 1)}{(2^\ell - 1) \dots (2 - 1)}$$

est le nombre de sous-espaces vectoriels de dimension ℓ de $\mathbb{F}_2^d$.

THÉORÈME 18.5. *L'ensemble S_d des vecteurs minimaux de BW_{2^d}, $d \geq 3$, est un 7-design sphérique.*

Démonstration. On sait que BW_{2^d} est de norme 2^m, $m = \lfloor \frac{d}{2} \rfloor$. D'après le théorème 8.1, il suffit de montrer que pout tout $y \in S_d$, on a l'identité

$$\sum_{x \in S_d} (x, y)^6 = \frac{1.3.5}{2^d \, (2^d + 2) \, (2^d + 4)} \, (2^m)^6 \, |S_d| . \tag{18.6}$$

Comme le groupe $\mathrm{Aut}(BW_{2^d})$ opère transitivement sur $S_d = S(BW_{2^d})$, il suffit de vérifier l'identité ci-dessus pour un élément y de S_d. Puisque $0 \in \mathcal{G}_{d,0}$, l'élément $2^m[0] = 2^m e_0$ appartient à S_d. C'est lui que nous choisissons comme élément y du membre de gauche de 18.6.

Pour $v \in \mathcal{G}_{d,2k}$, on a

$$(2^{m-k}[v], 2^m e_0)^{2p} = \begin{cases} (2^{m-k} \, 2^m \, 2^{-m})^{2p} = 2^{2p(m-k)} \\ \text{si } v \text{ est un sous-espace vectoriel de } \mathbb{F}_2^d , \\ 0 \text{ sinon,} \end{cases}$$

puis, d'après 18,2,

$$\sum_{x \in S_d(v)} (x, 2^m e_0)^{2p} = \begin{cases} 2^{2p(m-k)+1+2k+(2k-1)k} \\ \text{si } v \text{ est un sous-espace vectoriel de } \mathbb{F}_2^d , \\ 0 \text{ sinon,} \end{cases}$$

et enfin, d'après 18,3,

$$\sum_{x\in S_d(v)} (x,2^m e_0)^{2p} = 2^{2pm}\sum_{k=0}^{m} 2^{-2pk+1+2k+k(2k-1)} \begin{bmatrix} d \\ 2k \end{bmatrix}_2$$
$$= 2^{2pm+1}\sum_{k=0}^{m} 2^{(2k-1)k} \begin{bmatrix} d \\ 2k \end{bmatrix}_2 \Big(\frac{1}{2^{p-1}}\Big)^{2k}$$
$$= 2^{2pm+1}\, h_d\Big(\frac{1}{2^{p-1}}\Big)\,, \tag{18.7}$$

où

$$h_d(z) = \sum_{k=0}^{m} 2^{(2k-1)k} \begin{bmatrix} d \\ 2k \end{bmatrix}_2 z^{2k} \in \mathbb{Z}[z]\,.$$

Pour calculer $h_d(z)$, il est commode d'introduire le polynôme

$$g_d(z) = \sum_{\ell=0}^{d} 2^{\ell(\ell-1)/2} \begin{bmatrix} d \\ \ell \end{bmatrix}_2 z^{\ell} \in \mathbb{Z}[z]\,,$$

de sorte que $2h_d(z) = g_d(z) + g_d(-z)$.

LEMME 18.8. *Pour tout $d \geq 1$, on a*

$$g_d(z) = (1+z)\,(1+2z)\ldots(1+2^{d-1}z)\,.$$

Démonstration de 18.8. La formule est vraie pour $d = 1$, et l'on conclut par récurrence à l'aide de l'identité

$$\begin{bmatrix} d+1 \\ \ell \end{bmatrix}_2 = \begin{bmatrix} d \\ \ell \end{bmatrix}_2 + 2^{d-\ell+1} \begin{bmatrix} d \\ \ell-1 \end{bmatrix}_2 .$$

Fin de la démonstration de 18.6. Il résulte du lemme ci-dessus que l'on a $g_d(-\frac{1}{2^2}) = 0$ pour tout $d \geq 3$. Par conséquent, la formule 18.7 peut s'écrire

$$\sum_{x\in S_d} (x,2^m e_0)^6 = 2^{6m} g_d(\tfrac{1}{2^2})$$
$$= 2^{6m}(1+\frac{1}{2^2})\,(1+\frac{2}{2^2})\ldots(1+\frac{2^{d-1}}{2^2})$$
$$= 2^{6m}\frac{5.3}{2^2.2}(1+1)\ldots(1+2^{d-3})$$
$$= 2^{6m}\frac{1.3.5}{2\,(2^{d-1}+1)\,2^2\,(2^{d-2}+1)} \times (1+1)\ldots(1+2^{d-3})\,(1+2^{d-2})\,(1+2^{d-1})$$
$$= \frac{2^{6m}\,1.3.5\,2^d\,g_d(1)}{2^d\,(2^d+2)\,(2^d+4)}\,.$$

En utilisant la définition de h_d et la description de S_d donnée en 18.3, on obtient

$$|S_d| = 2^{d+1}h_d(1) = 2^d\big(g_d(1) + g_d(-1)\big) = 2^d g_d(1)$$

(puisque $g_d(-1) = 0$), ce qui achève la démonstration de la formule 18.6 et donc aussi celle du théorème 18.5. □

REMARQUE 18.9. Une démonstration en tous points analogue à la précédente permet de prouver que l'ensemble des vecteurs minimaux des réseaux de Barnes-Wall BW_{2^d}, $d \geq 3$ forme un $7\frac{1}{2}$-design au sens de la remarque 16.5, c'est-à-dire que les sommes $\sum_{x\in S_d} P(x)$ sont nulles lorsque P est un polynôme harmonique homogène de degré 10, mais que, en revanche, cet ensemble n'est pas un 8-design, autrement dit que ces sommes sont non nulles lorsque P est de degré 8. La vérification de ces assertions est laissée au lecteur.

REMARQUE 18.10. Le groupe d'automorphismes de BW_{2^d}, calculé par Broué et Enguehard ([B-E]), est pour $d \geq 4$ un sous-groupe d'indice 2 dans un "groupe de Clifford $2_+^{1+2d} \cdot \mathrm{O}^+(2^d, 2)$", qui apparaît dans divers contextes (codes quantiques, "spreads" orthogonaux, codes binaires). Les invariants des groupes de Clifford sont notamment liés aux codes binaires, voir à ce sujet le travail récent [N-R-S] de Nebe, Rains et Sloane, ainsi que les articles de Runge ([Ru]) et de Sidel´nikov ([Si]). En particulier, le groupe $2_+^{1+2d} \cdot \mathrm{O}^+(2^d, 2)$ n'a pas d'invariants harmoniques dans les degrés 2, 4, 6, 10. Cela entraîne que les diverses couches de la réunion d'un réseau de Barnes-Wall et de son dual renormalisés au même minimum sont des $7\frac{1}{2}$-designs sphériques.

19. RÉSULTATS NUMÉRIQUES.

Les tableaux 19.1 et 19.2 ci-après, construits avec l'aide de Christian Batut, contiennent la liste de tous les réseaux fortement parfaits connus jusqu'à la dimension $n = 24$, à cela près que nous n'avons donné qu'un réseau par couple (Λ, Λ^*). En fait, avec la seule exception de ${K'_{21}}^*$ qui est fortement eutactique mais non fortement parfait, le réseau dual d'un réseau fortement parfait est fortement parfait dans tous les cas connus de dimension $n \leq 24$.

Rappelons qu'un réseau Λ est dit *ℓ-modulaire* (ℓ désignant un entier positif) s'il existe une similitude de rapport $\sqrt{\ell}$ transformant Λ^* en Λ,

et *modulaire* s'il est ℓ-modulaire pour un entier ℓ. On ne considère ici que les cas où $\ell = 1, 2, 3, 5$, et l'on suppose en outre que Λ et $\sqrt{\ell}\,\Lambda^*$ sont tous deux des réseaux pairs, conformément à la définition originelle de Quebbemann. On vérifie facilement qu'un réseau proportionnel à un réseau entier est semblable à son dual si et seulement s'il est modulaire. Ainsi, en dimensions 6 (resp. 10), par exemple, il y a chaque fois deux réseaux fortement parfaits, à savoir $\mathbb{E}_6$ et $K_6' \sim \mathbb{E}_6^*$ (resp. K_{10}' et ${K_{10}'}^*$).

Les *réseaux laminés* Λ_n ont été définis par Conway et Sloane ([C-S], chapitre 6). Étant donné un réseau Λ_0 de dimension n_0, on construit les réseaux *faiblement laminés au-dessus de* Λ_0 en considérant d'abord les réseaux de dimension $n_0 + 1$ de déterminant minimum parmi ceux qui contiennent Λ_0 comme section hyperplane de même norme, puis en faisant la même construction au-dessus de ces réseaux de dimension $n_0 + 1$, etc. À partir de la dimension $n_0 + 2$, les déterminants peuvent ne plus être uniques. Pour chaque dimension $n \geq n_0$, les réseaux *fortement laminés* sont les réseaux faiblement laminés dont le déterminant est minimum. Enfin, les *réseaux laminés* sont les réseaux fortement laminés au-dessus du réseau $\{0\}$ de dimension 0 auquel on a attribué la norme 4. Ce sont donc des réseaux de norme 4. Ils sont entiers jusqu'à la dimension 24, et uniques à isométrie près sauf pour $n = 11, 12, 13$, dimensions qui ne nous intéressent pas ici. On les note Λ_n. Pour $1 \leq n \leq 8$, ce sont des renormalisations des réseaux de racines $\mathbb{A}_1 \sim \mathbb{Z}$, $\mathbb{A}_2$, $\mathbb{A}_3$, $\mathbb{D}_4$, $\mathbb{D}_5$, $\mathbb{E}_6$, $\mathbb{E}_7$, $\mathbb{E}_8$; pour $9 \leq n \leq 24$, ils sont primitifs; on a $\Lambda_{16} \simeq \mathrm{BW}_{16}$ et Λ_{24} est le réseau de Leech.

Le réseau K_{12} de Coxeter-Todd (cf. [M], ch. VIII, § 5) est un réseau de dimension 12 qui est unimodulaire *en tant que réseau sur l'anneau A des entiers d'Eisenstein*, et de ce fait 3-modulaire. Les "antilaminations fortes" de ce réseau constituent une suite descendante $K_{12} \supset K_{11} \supset \cdots \supset K_0 = \{0\}$. On peut munir Λ_{24} d'une structure de réseau sur A et y plonger K_{12}. Par orthogonalité, on en déduit une suite croissante $K_{12} \subset K_{13} \subset \cdots \subset K_{24} = \Lambda_{24}$. La série K_n a été découverte par Leech.

Il y a deux orbites de réseaux hexagonaux dans $K_{12}^* \simeq \dfrac{1}{\sqrt{3}}\,K_{12}$, dont une seule porte une A-structure naturelle. Par orthogonalité dans K_{12}^*, celle qui n'en porte pas définit K_{10} et l'autre un réseau de même déterminant noté K_{10}'. Par antilaminations, on définit une suite descendante $K_{10}' \supset K_9' \supset \cdots \supset K_0' = \{0\}$, que l'on complète par $K_{12}' = K_{12}$ et $K_{11}' = K_{11}$. Par orthogonalité dans Λ_{24}, on définit une suite croissante

$K'_{12} \subset K'_{13} = K_{13} \subset \cdots \subset K'_{24} = \Lambda_{24}$; pour n pair, les K'_n sont des A-réseaux.

Entre les séries Λ_n, K_n et K'_n existent les coïncidences suivantes :

- $K_n = \Lambda_n$ pour $0 \leq n \leq 6$ et $18 \leq n \leq 24$.
- $K'_n = K_n$ pour $n = 11, 12, 13$.
- $K'_n = \Lambda_n$ pour $n = 0, 1, 2, 22, 23, 24$.
- Les réseaux ci-dessus qui sont modulaires sont Λ_1, Λ_2, Λ_4, Λ_8, K_{12}, Λ_{16} et Λ_{24} (autrement dit, si Λ est l'un des réseaux Λ_n, K_n, K'_n, $n \leq 24$, il est semblable à son dual si et seulement s'il appartient à cette liste).

Les réseaux O_n ($n = 7, 16, 22, 23$) sont définis au §7; O_{23} est unimodulaire, les autres ne sont pas modulaires.

Le réseau modulaire extrémal Q_{14} a été découvert par Souvignier, et les réseaux modulaires extrémaux N_{16}, N_{20}, N'_{20}, N''_{20} et N_{24} par Nebe, dans les deux cas à Aix-la-Chapelle, comme réseaux stabilisant un sous-groupe fini maximal de $\mathrm{GL}_n(\mathbb{Z})$. On démontre dans [B-N-V] qu'il y a exactement 1 réseau 5-modulaire extrémal de de dimension 16, et dans [Bc-V] qu'il y a exactement 3 réseaux 2-modulaires extrémaux de dimension 20.

On connaît deux réseaux fortement parfaits en dimension 24, à savoir le réseau de Leech Λ_{24} et le réseau 3-modulaire N_{24}, extrémal et donc de norme 6. On ignore s'il existe d'autres réseaux 3-modulaires extrémaux de dimension 24.

L'existence en dimension 24 du réseau de Leech, dont l'ensemble des vecteurs minimaux constitue un 11-design sphérique, permet de trouver par sections de petites codimension plusieurs réseaux fortement parfaits. Leur description est facilitée par l'introduction de la notion de *dual partiel* d'un réseau entier : si Λ est entier, et si m désigne l'annulateur de Λ^*/Λ, on considère les réseaux $\Lambda[a] = \Lambda + a\Lambda^*$ où a divise m. On a clairement $\Lambda[1] = \Lambda^*$ et $\Lambda[m] = \Lambda$; on vérifie que l'égalité $\Lambda[a]^* = \Lambda[b]$ a lieu chaque fois que l'on a une décomposition $m = ab$ de m avec a, b premiers entre eux. Un tel réseau est appelé un *dual partiel de* Λ. (Noter que $\Lambda[a]$ peut être semblable à Λ pour un $a \neq 1, m$; un tel exemple, avec $m = 6$ et $a = 3$, est fourni par K'_{10}.)

En coupant Λ_{24} par l'orthogonal d'un vecteur de norme 4 (resp. 6) de $\Lambda^*_{24} \simeq \Lambda_{24}$, on obtient le réseau laminé Λ_{23} (resp. un réseau M_{23})

pour lequel $m = 4$ (resp. $m = 6$). On a $\Lambda_{23}[2] \simeq O_{23}$. Les 4 réseaux $M_{23}[a]$, $a = 1, 2, 3, 6$ sont fortement parfaits; les droites portant les vecteurs minimaux de $M_{23}[1]$ et de $M_{23}[3]$ constituent toutes deux la famille équiangulaire signalée au §9. (Rendus entiers et primitifs, les minima de ces deux réseaux sont respectivement 15 et 5, et leurs réseaux pairs associés sont proportionnels à $M_{22}[2]$ et $M_{22}[4]$.)

Les deux premières normes du réseau Λ_{23}^* rendu entier sont 12 et 15, et définissent par orthogonalité le réseau Λ_{22} et un réseau M_{22} (qui est aussi une section de M_{23}), avec respectivement $m = 6$ et $m = 15$. Les 8 réseaux $\Lambda_{22}[a]$, $a = 1, 2, 3, 6$ et $M_{22}[a]$, $a = 1, 3, 5, 15$ sont fortement parfaits et deux à deux non semblables. Les droites portant les vecteurs minimaux de $M_{22}[1]$ et de $M_{22}[3]$ constituent une famille de 275 droites, qui est projection orthogonale de la configuration equiangulaire de dimension 23 du §9.

Les travaux de Koch et Venkov ([K-V]) ont produit de nombreux exemples de réseaux unimodulaires de dimension 32 et de norme 4, qui sont donc fortement parfaits par le théorème 16.4. Le théorème 17.1 permet alors de construire des exemples de réseaux fortement parfaits de norme 4 dans chacune des dimensions 31, 30, 28 et 26. On connaît en outre en dimension 32 quatre réseaux 2-modulaires extrémaux (de norme 6), qui sont de ce fait fortement parfaits, découverts par Quebbemann (2), Bachoc et Nebe.

Au-delà de la dimension 32, on connaît en particulier les réseaux de Barnes-Wall ($n = 64, 128, \ldots$, cf. §18) et les réseaux ℓ-modulaires extrémaux pour $\ell = 1$ ($n = 48, 56, 80$, normes 6, 6 et 8; les deux exemples de dimension 80 ont été découverts récemment par Bachoc et Nebe) et $\ell = 2$ ($n = 48$, norme 8, trouvé par Quebbemann). Le fait que les réseaux ℓ-modulaires pour $\ell = 2, 3, 5$ que nous avons cités dans ce paragraphe soient fortement parfaits est justifié dans [Bc-V].

La théorie des groupes finis est une autre source de réseaux fortement parfaits. Nous renvoyons à l'article récent [L-S-T] pour la construction de réseaux à groupe d'automorphismes liés à des groupes sporadiques. Par exemple, le réseau de Thompson-Smith est un réseau unimodulaire pair de dimension 248, dont les vecteurs ayant une norme donnée non nulle forment un 7-design, par la théorie des invariants du groupe de Thompson. On ignore si le minimum de ce réseau est 12 ou 10.

Les notations employées dans les tableaux 19.1 et 19.2 sont les suivantes: on trouve dans les 3 premières colonnes successivement la dimension n, le nom et le déterminant d'un réseau entier et primitif fortement parfait, dont le demi-kissing number s et le minimum m sont donnés dans les colonnes 4 et 5; les invariants analogues pour le réseau dual renormalisé, notés s^* et m^*, figurent dans les colonnes 6 et 7. L'*invariant de Smith du réseau* est la suite $(a_1, \ldots, a_n)$ des diviseurs élémentaires du couple (Λ^*, Λ), en notation abrégée: dans la ligne 7, par exemple, la notation $6^2.3^3$ signifie que l'invariant de Smith est la suite $(6, 6, 3, 3, 3, 1, 1, 1, 1, 1)$ (le nombre de 1 se calcule à l'aide de la dimension; ici, c'est $12 - 2 - 3 = 5$). Noter que a_1 est l'annulateur de Λ^*/Λ, et que le minimum de Λ^* est

$$N(\Lambda^*) = \frac{m^*}{a_1}\,.$$

Le type (minimal ou général) se réfère à la définition 10.6.

Dans la colonne "Rem." (pour "Remarques"), "mod." signifie "modulaire", "equig." signifie "équiangulaire" (cf. §9; ici, seul le réseau dual possède cette propriété), et la mention "non f.p." est utilisée pour rappeler que ${K'_{21}}^*$ *n'est pas* fortement parfait, mais seulement fortement eutactique, alors que, dans tous les autres cas, les duals des réseaux du tableau sont aussi fortement parfaits.

Les tables ci-dessous contiennent les **39** réseaux fortement parfaits de dimension $n \leq 24$ connus à ce jour, répartis ainsi:

- **14** réseaux modulaires (dont 3 en dimension 20);
- Le réseau K'_{21};
- **12** couples (Λ, Λ^*) de réseaux tous deux fortement parfaits.

Cette liste est exhaustive pour $n \leq 11$ [3]). Nous pensons en outre qu'il n'existe pas de réseaux fortement parfaits dans les dimensions 13, 17, 19, du fait qu'aucun réseau connu dans ces dimensions ne satisfait l'inégalité du théorème 10.4.

---

[3]) Le cas de la dimension 10 vient d'être résolu dans [Ne-V1]

Tableau 19.1. Réseaux fortement parfaits connus ($1 \leq n \leq 20$).

dim	nom	det	s	m	s^*	m^*	Smith	Type	Rem.
1	$\mathbb{Z}$	1	1	1	1	1	1	min.	$1-$mod.
2	$\mathbb{A}_2$	3	3	2	3	2	3	min.	$3-$mod.
4	$\mathbb{D}_4$	4	12	2	12	2	2^2	min.	$2-$mod.
6	$\mathbb{E}_6$	3	36	2	27	4	3	min.	
7	$\mathbb{E}_7$	2	63	2	28	3	2	min.	Λ^* equiang.
8	$\mathbb{E}_8$	1	120	2	120	2	1	gén.	$1-$mod.
10	K'_{10}	972	135	4	120	6	$6^2.3^3$	min.	
12	K_{12}	729	378	4	378	4	3^6	gén.	$3-$mod.
14	Q_{14}	2187	378	4	378	4	3^7	min.	$3-$mod.
16	Λ_{16}	256	2160	4	2160	4	2^8	gén.	$2-$mod.
–	O_{16}	64	256	3	1008	4	2^6	min.	
–	N_{16}	390625	1200	6	1200	6	5^8	gén.	$5-$mod.
18	K'_{18}	243	3240	4	1080	6	3^5	gén.	
20	$N_{20}, ', ''$	1024	1980	4	1980	4	2^{10}	gén.	$2-$mod.

Tableau 19.2. Réseaux fortement parfaits connus ($21 \leq n \leq 24$).

dim	nom	det	s	m	s^*	m^*	Smith	Type	Rem.
21	K'_{21}	36	13041	4	112	27	12.3	gén.	${K'}^*_{21}$ non f.p.
22	Λ_{22}	12	24948	4	891	16	6.2	gén.	
22	$\Lambda_{22[2]}$	$2^{20}.3$	4224	6	891	8	6.2^{19}	min	
–	O_{22}	3	1408	3	891	8	3	min.	
–	M_{22}	15	22275	4	275	36	15	gén.	
–	$M_{22}[5]$	$3^{21}.5$	7128	10	275	12	15.3^{20}	min.	
23	Λ_{23}	4	46575	4	2300	12	4	gén.	
–	O_{23}	1	2300	3	2300	3	1	gén.	$1-$ mod.
–	M_{23}	6	37950	4	276	15	6	gén.	Λ^* equiang.
–	$M_{23}[2]$	2.3^{22}	11178	10	276	5	6.3^{21}	min.	Λ^* equiang.
24	Λ_{24}	1	98280	4	98280	4	1	gén.	$1-$ mod.
–	N_{24}	3^{12}	13104	6	13104	6	3^{12}	gén.	$3-$ mod.

BIBLIOGRAPHIE

[Ash] Ash, A. On eutactic forms. *Can. J. Math. 29* (1977), 1040–1054.

[Ba-V] Bacher, R. et Venkov, B. B. Réseaux entiers unimodulaires sans racine en dimension 27 et 28. *Ce volume.*

[Bc-V] Bachoc, C. et Venkov, B. B. Modular forms, lattices and spherical designs, *Ce volume.*

[B-N-V] Bachoc C.,Nebe, G. et Venkov, B. B. Appendix to [Bc-V].

[Bo] Borcherds, R. *The Leech lattice and other lattices.* Ph.D. thesis, Trinity College (Cambridge, U.K.), 1984.

[Bou] Bourbaki, N. *Groupes et algèbres de Lie.* Masson (Paris), 1981.

[B-E] Broué, M. et Enguehard, M. Une famille infinie de formes quadratiques entières; leurs groupes d'automorphismes. *Ann. Sci. École Norm. Sup., (4) 6* (1973), 17–51.

[C-S] Conway, J.H. et Sloane, N.J.A. *Sphere Packings, Lattices and Groups.* Springer-Verlag, Grundlehren no. 290 (Heidelberg), 1988. (Troisième édition : 1999.)

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

[D-G-S] Delsarte, P., Goethals, J.M. et Seidel, J.J. Spherical codes and designs. *Geometriae Dedicata 6* (1977), 363–388.

[H-S1] Hardin, R.H. et Sloane, N.J.A. New spherical 4-designs. *Discr. Math. 106–107* (1992), 255–264.

[H-S2] Hardin, R.H. et Sloane, N.J.A. Mc Laren's improved snub cube and other spherical designs in three dimensions. *Discr. Comp. Geometry 15* (1996), 429–441.

[Ho] Hong, Y. On spherical t-designs in $\mathbb{R}^2$. *Eur. J. Comb. l3* (1982), 255–258.

[J] Jaquet-Chiffelle, D.-O. Énumération complète des classes de formes parfaites en dimension 7. *Ann. Inst. Fourier 43,1* (1993), 21–55.

[K-V] Koch, H. and Venkov, B.B. Über gerade unimodulare Gitter der Dimension 32, III. *Math. Nachr. (152)* (1991), 191-213.

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

[L-S] Lemmens, P.W.H. et Seidel, J.J. Equiangular lines. *J. Algebra 24* (1973), 494–512.

[L-S-T] Lempken, W, Schröder, B. et Tiep, P.H. Symmetric squares and lattice minima. *Preprint, Essen.*

[L-V] Lyubich, Y.I. et Vasserstein, L.N. Isometric embeddings between classical Banach spaces, cubature formulas and spherical designs. *Geometriae Dedicata 47* (1993), 327–362.

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

[M1] Martinet, J. Sur certains designs sphériques liés à des réseaux entiers. *Ce volume.*

[M-V] Martinet, J. et Venkov, B.B. Les réseaux fortement eutactiques. *Ce volume.*

[M-O-S] Mallows, C.L., Odlyzko, A.M. et Sloane. N.J.A. Upper Bounds for Modular Forms, Lattices and Codes. *J. Algebra 36.* (1975), 68–76.

[Ne-V1] Nebe, G. et Venkov, B.B. The strongly perfect lattices of dimension 10. *Journal de Théorie des Nombres de Bordeaux*, à paraître.

[N-R-S] Nebe, G., Rains, E.M. et Sloane, N.J.A. The invariants of the Clifford group. *Preprint.*

[Nt] Nottebaum, J. *Sphärische 4-designs in Gittern.* Universität Oldenburg, Diplomarbeit, 1995.

[Ogg] Ogg, A. *Modular Forms and Dirichlet Series.* Benjamin (New-York), 1969.

[R-S] Rains, E.M. et Sloane, N.J.A. The Shadow Theory of Modular and Unimodular Lattices. AT& T Labs-Research, preprint, 1998.

[Rz] REZNICK, B. Sums of even powers of real linear forms. *Mem. Amer. Math. Soc. 463* (1992), 155 pages.

[Rog] ROGERS, C.A. *Packing and covering.* Cambridge Univerity Press (Cambridge, U.K.), 1964.

[Ru] RUNGE, B. Codes and Siegel modular forms. *Discrete Math. 148* (1995), 175–205

[S] SEIDEL, J. J. Geometry and combinatorics. In: *Selected Works of J. J. Seidel*, Academic Press (New York), 1991.

[Se] SERRE, J.-P. *Cours d'Arithmétique.* P.U.F. (Paris), 1970.

[S-V] SCHARLAU, R. et VENKOV, B. B. The genus of the Barnes-Wall lattice. *Comment. Math. Helvet. 169* (1994), 322–333.

[S-Z] SEYMOUR, P.D. et ZASLAVSKY,T. Averaging sets: a generalization of mean values and spherical designs. *Adv. Math. 152* (1984), 213–240.

[Sg] SIEGEL, C. L. Berechnung von Zetafunktionen an ganzzahligen Stellen. *Gött. Nachrichten 10* (1969), 87–112
(= *Ges. Abh. IV, 89* 82–97).

[Si] SIDEL'NIKOV, V. M. Orbital spherical 11-designs whose initial point is a root of an invariant polynomial. *St. Petersburg Math. J. 11, 4* (2000), (En russe.)

[So] SOBOLEV, S. L. *Einführung in die Theorie der Kubaturformeln (Vvedenie v teoriju kubaturnyh formul).* (En russe.) Hauptredaktion für physikalisch-mathematische Literatur 808 S.R. 3.03, Verlag "Nauka" (Moskau), 1974.

[V1] VENKOV, B. B. Unimodular lattices and strongly regular graphs. *J. Soviet Math. 29* (1985), 1121–1127. (Original en russe: 1983.)

[V2] VENKOV, B. B. Even unimodular extremal lattices. *Proc. Steklov Inst. Math. 165* (1984), 47–52. (Original en russe: 1984.)

[V3] VENKOV, B. B. On even unimodular Euclidean lattices of dimension 32. *J. Soviet math. 26* (1984), 1860–1867. (Original en russe: 1982.)

[V4] VENKOV, B. B. On even unimodular Euclidean lattices of dimension 32, II. *J. Soviet math. 36* (1987), 21–38. (Original en russe: 1984.)

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

[Vi] VILENKIN, N. J. Special Functions and the Theory of Group Representations. *Translations of Mathematical Monographs 22* AMS editors (1968).

[W] WATSON, G. L. The number of minimum points of a positive quadratic

form. *Dissertationes Math. 84* (1971), 1–46.

Boris Venkov

Fontanka 27, POMI
191011 St.Petersbourg
Russie
e-mail: bvenkov@pdmi.ras.ru