Astérisque

A.-M. BERGÉ
J. MARTINET
F. SIGRIST

Une généralisation de l'algorithme de Voronoï pour les formes quadratiques

Astérisque, tome 209 (1992), p. 137-158
<http://www.numdam.org/item?id=AST_1992__209__137_0>

UNE GÉNÉRALISATION DE L'ALGORITHME DE VORONOÏ POUR LES FORMES QUADRATIQUES

par A-M. BERGÉ, J. MARTINET et F. SIGRIST

§ 1. **Introduction.** Soit n un entier > 0. On note $\mathcal{Q}_n$ l'espace vectoriel des formes quadratiques sur $\mathbb{R}^n$ que l'on identifie à l'espace vectoriel Sym_n des matrices symétriques d'ordre n à coefficients réels, en associant à $M \in \mathrm{Sym}_n$ la forme $Q(x) = {}^tXMX$ où, pour $x = (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$, X désigne la matrice-colonne de composantes $x_1, x_2, \ldots, x_n$ et la notation ${}^tA$ désigne la transposée de la matrice A. Pour une forme Q définie positive, on pose $m(Q) = \min_{x \in \mathbb{Z}^n \setminus \{0\}} Q(x)$ (*le minimum de* Q) et $S(Q) = \{x \in \mathbb{Z}^n \mid Q(x) = m(Q)\}$ (ensemble des *vecteurs minimaux de* Q), et l'on note $\det(Q)$ le déterminant $\det(M)$ de la matrice correspondant à Q (*le discriminant de* Q). *L'invariant d'Hermite de* Q est $\gamma_n(Q) = m(Q)(\det(Q))^{-1/n}$, et *la constante d'Hermite pour la dimension* n est $\gamma_n = \sup_Q \gamma_n(Q)$.

Afin de calculer la constante d'Hermite, Korkine et Zolotareff ont introduit la notion de *forme extrême* (forme qui réalise un maximum local de l'invariant d'Hermite) et démontré le résultat suivant ([K-Z]) :

1.1. Théorème (KORKINE ET ZOLOTAREFF, 1877). *Si Q est une forme extrême, les formes de matrices $Y {}^tY, Y \in S(Q)$ engendrent $\mathcal{Q}_n$. (En particulier, Q possède au moins $\frac{n(n+1)}{2}$ couples de vecteurs minimaux.)*

Les formes vérifiant cette propriété ont été appelées par la suite *formes parfaites* par Voronoï, qui a notamment démontré qu'elles sont en nombre fini à proportionalité et équivalence sous $\mathrm{Gl}_n(\mathbb{Z})$ près. C'est la notion de forme parfaite plutôt que celle de forme extrême qui est importante dans les applications.

mots-clés : Formes quadratiques réelles, Formes parfaites, Réseaux parfaits.

[Noter que, lorsque Y parcourt les vecteurs-colonnes à n composantes, les matrices $Y{}^tY$ parcourent l'ensemble des matrices positives de rang ≤ 1 de Sym_n, alors que ${}^tYY \in \mathbb{R}$ est le carré de la norme de Y.]

Korkine et Zolotareff, à l'aide de méthodes combinatoires, ont classé les formes parfaites jusqu'à la dimension 5, trouvant ainsi la valeur de γ_5 ([K-Z], 1877). L'étude des formes parfaites a été reprise 30 ans plus tard par Voronoï (dans [V], paru en 1908), qui a introduit une méthode entièrement nouvelle qui sera décrite en détail au § suivant. Indiquons simplement ici qu'il associe à toute forme parfaite Q de dimension $n \geq 2$ et de minimum m donné un cône polyédral d'intérieur non vide de $\mathcal{Q}_n$ et à toute face de ce cône une forme parfaite dite contiguë à Q, et qu'il démontre que le graphe de contiguïté ainsi obtenu est *connexe*. La relation de contiguïté étant compatible à l'équivalence, l'ensemble des classes de formes parfaites de minimum donné se trouve muni d'une structure de graphe qui est fini et connexe, ce qui entraîne la validité du procédé de calcul suivant :

1.2.Algorithme (VORONOÏ, 1908)

1. Choisir une forme parfaite Q_0 pour la dimension n.

2. Déterminer ses formes contiguës $Q_1, \ldots, Q_r$.

3. Supprimer de la liste toute forme équivalente à une forme déjà rencontrée.

4. Terminer si aucune forme nouvelle n'a été conservée.

5. Sinon, faire la liste de toutes les formes contiguës à l'une des formes nouvelles et aller en 3.

À l'aide de cet algorithme, Voronoï ([V]) a vérifié les résultats de Korkine et Zolotareff pour les dimensions ≤ 5. Son article indique qu'il a également commencé l'étude de la dimension 6 (et il y annonce aussi diverses autres recherches qu'il serait peut-être intéressant de reprendre). Son décès survenu en 1908 l'a empêché de poursuivre son programme. Le cas de la dimension 6 a été résolu un demi-siècle plus tard par Barnes ([Ba]), et celui de la dimension 7 vient d'être résolu par Jaquet ([J]). Cette dernière étude a nécessité des calculs considérables sur ordinateur, et il ne semble pas possible de traiter la dimension 8 selon les mêmes procédés.

Cela suggère de restreindre l'étude de l'invariant d'Hermite à certaines familles de formes quadratiques pour lesquelles on peut développer un algorithme analogue dans un sous-espace $\mathcal{T}$ de $\mathcal{Q}_n$ de dimension inférieure. Le paragraphe 2 est consacré à la description de cet algorithme. Voici deux exemples qui seront étudiés avec quelques détails dans cet article :

1.3. Exemple. Étant donnée une représentation intégrale $\rho : G \to \mathrm{Gl}_n(\mathbb{Z})$ d'un groupe fini G, on étudie l'ensemble $\mathcal{Q}_\rho$ des formes quadratiques définies positives invariantes par $\rho(G)$; dans ce cas, on peut prendre pour $\mathcal{T}$ l'espace de toutes les formes quadratiques invariantes par $\rho(G)$.

Cet exemple est étudié en détail aux §§ 3, où est justifié le choix fait pour $\mathcal{T}$ en même temps qu'est établi le lien avec la notion de G- réseau développée dans [B-M], et 4, consacré aux résultats effectifs obtenus à l'aide de l'algorithme de Voronoï.

1.4. Exemple. Soit $Q_0 = Q_0(x_1, x_2, \cdots, x_r)$ une forme quadratique définie positive à $r < n$ variables. On étudie les formes quadratiques définies positives $Q \in \mathcal{Q}_n$ de même minimum que Q_0 et telles que $Q(x_1, x_2, \cdots, x_r, 0, 0, \cdots, 0) = Q_0(x_1, x_2, \cdots, x_r)$. On se place alors dans l'espace $\mathcal{T}$ des formes $Q \in \mathcal{Q}_n$ telles que $Q(x_1, \cdots, x_r, 0, \cdots, 0) = 0$. Pour plus de détails, se reporter au § 5.

Le problème de développer un algorithme de Voronoï dans le cas des G-réseaux (exemple 1.3 ci-dessus) est posé dans [B-M]. Il a été résolu indépendamment de nous par Joseph Oesterlé, que nous remercions par ailleurs pour les discussions fructueuses que nous avons eues avec lui.

§ 2. Nouvel algorithme de Voronoï. On munit Sym_n du produit scalaire $\langle A, B\rangle = \mathrm{Tr}(AB)$. On en déduit un produit scalaire sur $\mathcal{Q}_n$, et par restriction sur tous les sous-espaces de Sym_n et de $\mathcal{Q}_n$. Pour $x \in \mathbb{R}^n$, on note P_x ou P_X la forme de matrice $X^tX \in \mathrm{Sym}_n$. On a alors, pour $x \in \mathbb{R}^n$ et $Q \in \mathcal{Q}_n$, $Q(x) = \langle Q, P_x\rangle = \langle A, P_x\rangle$, où A est la matrice représentant la forme quadratique Q.

2.1. Définition. Soit $\mathcal{T}$ un sous-espace vectoriel de $\mathcal{Q}_n$.

(1) Pour tout $x \in \mathbb{R}^n$ représenté par la matrice-colonne X, on note Ω_x (ou Ω_X) la projection orthogonale de $P_x = P_X$ sur $\mathcal{T}$.

(2) On dit qu'une forme quadratique définie positive Q est *$\mathcal{T}$-parfaite* (ou que la matrice de Q est *$\mathcal{T}$-parfaite*) si les matrices Ω_x engendrent $\mathcal{T}$ tout entier lorsque x décrit l'ensemble $S(Q)$ des vecteurs minimaux de Q.

Si $\mathcal{T}'$ est un sous-espace de $\mathcal{T}$, toute forme $\mathcal{T}$-parfaite est $\mathcal{T}'$-parfaite. Lorsque $\mathcal{T} = \mathcal{Q}_n$, on retrouve la notion de forme parfaite introduite par Voronoï. On montre facilement que les vecteurs minimaux d'une forme parfaite engendrent $\mathbb{R}^n$. Nous nous restreindrons aux sous-espaces $\mathcal{T}$ vérifiant une propriété analogue :

2.2. Hypothèse. Désormais, $\mathcal{T}$ désigne un sous-espace vectoriel de $\mathcal{Q}_n$

vérifiant la propriété suivante : *les vecteurs minimaux des formes $\mathcal{T}$-parfaites engendrent* $\mathbb{R}^n$.

La proposition suivante donne d'autres expressions de cette condition :

2.3. Proposition. *Soit Q une forme quadratique définie positive. Les conditions suivantes sont équivalentes :*

(1) *Il existe des coefficients positifs $\lambda_x, x \in S(Q)$ tels que la forme quadratique $\sum_{x\in S} \lambda_x P_x$ soit définie positive.*
(2) *Pour toute famille de coefficients positifs $\lambda_x, x \in S$, la forme quadratique $\sum_{x\in S} \lambda_x P_x$ est définie positive.*
(3) *$S(Q)$ engendre $\mathbb{R}^n$.*

Démonstration. Quel que soit le vecteur $u \in \mathbb{R}^n$ et les coefficients $\lambda_x > 0$, on a

$$\sum_{x\in S(Q)} \lambda_x \langle P_x, P_u\rangle = \sum_{x\in S(Q)} \lambda_x (x.u)^2 \geq 0\,,$$

et l'égalité a lieu si et seulement si u est orthogonal à x pour tout $x \in S(Q)$ (l'espace $\mathbb{R}^n$ étant muni de son produit scalaire canonique). On en déduit tout de suite les équivalences de (1) et (3) d'une part et de (2) et (3) d'autre part, **c.q.f.d.**

2.4. Définition. Soit Q une forme quadratique définie positive. *Le $\mathcal{T}$-domaine de Voronoï $\mathcal{D}_Q$ de Q* est l'enveloppe convexe dans $\mathcal{T}$ des demi-droites fermées portant les formes Ω_x pour $x \in S(Q)$. Si Q a pour matrice A, on écrit aussi $\mathcal{D}_A$ au-lieu de $\mathcal{D}_Q$.

Lorsque $\mathcal{T} = \mathcal{Q}_n$, on retrouve la notion de domaine de Q introduite par Voronoï. (En fait, le $\mathcal{T}$-domaine de Q est la projection sur $\mathcal{T}$ du domaine classique).

On a

$$\mathcal{D}_Q = \mathcal{D}_A = \{ \sum_{x\in S(Q)} \lambda_x \Omega_x \mid \lambda_x \geq 0\}\,,$$

et l'intérieur du $\mathcal{T}$-domaine de Voronoï de Q est

$$\mathrm{Int}(\mathcal{D}_Q) = \{ \sum_{x\in S(Q)} \lambda_x \Omega_x \mid \lambda_x > 0\}\,.$$

Dire que Q est $\mathcal{T}$-parfaite revient à dire que $\mathcal{D}_Q$ est d'intérieur non vide dans $\mathcal{T}$.

Dans la suite, on suppose que Q est $\mathcal{T}$-parfaite. (On pourrait se passer de cette restriction, à condition de remplacer dans les énoncés ci-dessous $\mathcal{T}$ par le sous-espace de $\mathcal{T}$ engendré par $\mathcal{D}_Q$.) Soit $\mathcal{F}$ une face de codimension 1 de $\mathcal{D}_Q$ dans $\mathcal{T}$. C'est un cône polyédral contenu dans $\mathcal{D}_Q$ qui engendre un hyperplan $\mathcal{H}$ de $\mathcal{T}$. On a $\mathcal{F} = \mathcal{H} \cap \mathcal{D}_Q$, et $\mathcal{D}_Q$ est contenu dans l'un des demi-espaces fermés définis par $\mathcal{H}$. Il existe une forme $Q_F \in \mathcal{T}$, unique à une homothétie positive près, vérifiant les deux conditions suivantes :

(1) $\langle Q_F, \Omega_x \rangle \geq 0$ quel que soit $x \in S(Q)$.
(2) $\langle Q_F, \Omega_x \rangle = 0 \iff \Omega_x \in \mathcal{F}$.

Une telle forme est appelée *forme de face de Q associée à $\mathcal{F}$*, et l'on note F la matrice correspondante. On a alors

$$\mathcal{D}_Q = \{Q' \in \mathcal{T} \mid \langle Q_F, Q' \rangle \geq 0 \text{ pour toute forme de face } Q_F \text{ de } Q\}.$$

Dans la pratique, on procède de la façon suivante : on commence par choisir une base $\mathcal{B} = (T_1, T_2, \ldots, T_k)$ de $\mathcal{T}$ (des choix commodes sont indiqués dans certains cas aux §§ 4 et 5) ; soit $\mathcal{B}^* = (T_1^*, T_2^*, \ldots, T_k^*)$ sa base duale dans $\mathcal{T}$. Pour tout $x \in S(Q)$, représenté par la matrice-colonne X, on détermine les composantes $\omega_{i,x}$ de Ω_x dans $\mathcal{B}^*$ à l'aide des formules

$$\omega_{i,x} = \langle \Omega_x, T_i \rangle = \langle P_X, T_i \rangle = {}^tXAX = Q_{T_i}(x).$$

La partie algorithmiquement difficile est l'établissement de la liste des faces de $\mathcal{D}_Q$. Comme il n'y a pas de différence de principe avec ce qui se fait dans le cas classique, nous renvoyons le lecteur à la thèse de Jaquet ([J]). La recherche d'une forme de face Q_F pour une face $\mathcal{F}$ se fait en résolvant le système linéaire suivant, qui donne les composantes f_i de Q_F dans la base $\mathcal{B}$:

$$\sum_i \omega_{i,x} f_i = 0 \qquad (x \in \mathcal{F})$$
$$\sum_i \omega_{i,x} f_i > 0 \qquad (x \notin \mathcal{F}).$$

On notera qu'il est inutile de déterminer $\mathcal{B}^*$.

Pour tout nombre réel $\theta \geq 0$, on pose $Q_\theta = Q + \theta Q_F$; c'est une forme quadratique de matrice $A_\theta = A + \theta F$. Les vecteurs X de $S(Q)$ dont l'image Ω_X est dans $\mathcal{F}$ sont de norme m, et ceux dont l'image n'est pas dans $\mathcal{F}$ sont de norme $m + \theta Q_F(X) > m$ dès que θ est > 0. Par ailleurs, les vecteurs

minimaux de Q_θ proviennent de ceux de Q lorsque θ est assez petit. Il en résulte que, pour $\theta > 0$ assez petit, Q_θ est une forme non $\mathcal{T}$-parfaite de même minimum m que Q.

2.5. Définition. On note $\rho \in]0, +\infty]$ la borne supérieure des $\theta \geq 0$ tels que Q_θ soit positive de minimum m. On dit que $\mathcal{F}$ (ou que F) est *une impasse* si $\rho = +\infty$. Lorsque $\mathcal{F}$ n'est pas une impasse, la forme Q_ρ s'appelle *la forme $\mathcal{T}$-contiguë à Q par $\mathcal{F}$* (ou *par F*).

2.6. Proposition.

(1) *Si $\mathcal{F}$ n'est pas une impasse, la forme Q_ρ est $\mathcal{T}$-parfaite.*
(2) *$\mathcal{F}$ est une impasse si et seulement si la forme Q_F est positive.*

Démonstration. Si Q_F est positive, on a $Q_\theta(x) \geq Q(x) \geq m$ pour tout $x \in \mathbb{Z}^n$ non nul, donc $\rho = +\infty$. Dans le cas contraire, il existe $x \in \mathbb{R}^n$ avec $Q_F(x) < 0$. Comme il existe des points de $\mathbb{Z}^n$ arbitrairement proches de la droite $\mathbb{R}x$, il existe $y \in \mathbb{Z}^n$ avec $Q_F(y) < 0$. Alors, $Q_\theta(y)$ est < 0 pour θ assez grand, et un tel θ est un majorant de ρ, d'où (2). En outre, on a $Q_\rho(x) \geq m$ pour tout $x \neq 0$ de $\mathbb{Z}^n$, mais, comme Q_θ prend sur $\mathbb{Z}^n \setminus \{0\}$ des valeurs $< m$ pour tout $\theta > \rho$, il existe $z \in \mathbb{Z}^n$ avec $Q_\rho(z) = m$ et $Q_F(z) < 0$. Le vecteur z est donc un vecteur minimal de Q_ρ qui n'est pas un vecteur minimal de Q. Comme le système des $\Omega_x \in \mathcal{F}$ $(x \in S(Q))$ est de rang $\dim \mathcal{T} - 1$, le système formé par $\Omega_x, x \in \mathcal{F}$ et Ω_z est de rang $\dim \mathcal{T}$, **c.q.f.d.**

Le lemme suivant est énoncé en termes de matrices.

2.7. Lemme. *Soient $A, B \in \mathrm{Sym}_n$ deux matrices définies positives de même minimum m avec $A - B \in \mathcal{T}$.*

(1) *Pour tout $C \in \mathcal{D}_A \cap \mathcal{D}_B$, on a $\langle C, A\rangle = \langle C, B\rangle$.*
(2) *Si $\mathrm{Int}(\mathcal{D}_A) \cap \mathcal{D}_B$ est non vide, alors $\mathcal{D}_A \subset \mathcal{D}_B$.*
(3) *Si de plus A est $\mathcal{T}$-parfaite, alors $B = A$.*

Démonstration. Posons $C = \sum_{x \in S(A)} \lambda_x \Omega_x$ avec des coefficients $\lambda_x \geq 0$. Comme
$A - B \in \mathcal{T}$, on a

$$\langle C, A - B\rangle = \sum_{x \in S(A)} \lambda_x \langle \Omega_x, A - B\rangle = \sum_{x \in S(A)} \lambda_x \langle P_x, A - B\rangle$$
$$= \sum_{x \in S(A)} \lambda_x (m - \langle P_x, B\rangle) \leq 0 .$$

On a de même $\langle C, B - A\rangle \leq 0$, d'où (1).

Lorsque $C \in \mathrm{Int}(A)$, on peut prendre les λ_x strictement positifs. Comme $m - \langle P_x, B\rangle$ est ≤ 0 pour tout $x \in S(A)$, l'égalité $\sum_{x\in S(A)} \lambda_x(m - \langle P_x, B\rangle) = 0$ entraîne que l'on a $\langle P_x, B\rangle = m$ pour tout $x \in S(A)$, d'où $S(A) \subset S(B)$, i.e. $\mathcal{D}_A \subset \mathcal{D}_B$.

Comme $A - B \in \mathcal{T}$, la condition $\langle P_x, A - B\rangle = 0$ pour tout $x \in S(A)$ équivaut à $\langle \Omega_x, A - B\rangle = 0$ pour tout $x \in S(A)$, ce qui, lorsque A est $\mathcal{T}$-parfaite, implique $A - B = 0$, **c.q.f.d.**

L'ensemble des formes $\mathcal{T}$-parfaites est l'ensemble des sommets d'un graphe non orienté dont les arêtes sont les couples de formes contiguës (la relation de contiguïté est clairement symétrique). On s'intéresse à la connexité de ce graphe, que l'on étudie à l'aide du résultat suivant, dont nous laissons comme Voronoï la démonstration au lecteur :

2.8. Lemme. *(VORONOÏ) Soit Φ une forme quadratique définie positive, soient m et K deux constantes. L'ensemble des vecteurs minimaux des formes définies positives Q de minimum m et telles que $\langle Q, \Phi\rangle \leq K$ est une partie finie de $\mathbb{Z}^n$.*

On rappelle que $\mathcal{T}$ désigne un sous-espace vectoriel de $\mathcal{Q}_n$ tel que les vecteurs minimaux de toute forme $\mathcal{T}$-parfaite engendrent $\mathbb{R}^n$.

2.9. Théorème. *Soit $Q_0 \in \mathcal{Q}_n$ et soit $\mathcal{E}$ l'ensemble des formes quadratiques Q de même minimum m que Q_0 et telles que $Q - Q_0 \in \mathcal{T}$. Alors, le graphe de $\mathcal{T}$-contiguïté des formes $\mathcal{T}$-parfaites de $\mathcal{E}$ est connexe.*

Démonstration. Soit Q une forme $\mathcal{T}$-parfaite de $\mathcal{E}$. Soient $\lambda_x, x \in S(Q)$ des nombres réels > 0, soit $\Phi_0 = \sum_{x\in S(Q)} \lambda_x \Omega_x$ et soit $\Phi = \sum_{x\in S(Q)} \lambda_x P_x$. Comme Q est $\mathcal{T}$-parfaite, l'hypothèse faite sur $\mathcal{T}$ implique que Φ est définie positive. Si Φ_0 est dans $\mathcal{D}_{Q_0}$, alors le lemme 2.7 montre que $Q_0 = Q$. Sinon, il existe une forme de face F de Q_0 avec $\langle \Phi_0, F\rangle < 0$, ce qui entraîne qu'il existe au moins un $x \in S(Q)$ vérifiant $\langle \Omega_x, F\rangle < 0$. Il existe donc une forme $\mathcal{T}$-contiguë Q_1 à Q_0 par F, et l'on a

$$\langle Q_1, \Phi_0\rangle = \langle Q_0, \Phi_0\rangle + \rho\langle F, \Phi_0\rangle < \langle Q_0, \Phi_0\rangle .$$

Si $\Phi_0 \notin \mathcal{D}_{Q_1}$, on contruit de même une forme $\mathcal{T}$-contiguë Q_2 à Q_1 telle que $\langle Q_2, \Phi_0\rangle < \langle Q_1, \Phi_0\rangle$. On construit ainsi une suite $Q_0, Q_1, \ldots, Q_i$ de formes $\mathcal{T}$-parfaites de même minimum m et telles que

$$\langle Q_0, \Phi\rangle > \langle Q_1, \Phi\rangle > \cdots > \langle Q_i, \Phi\rangle ,$$

car, comme $Q_{i+1} - Q_i$ appartient à $\mathcal{T}$, on a

$$\langle Q_{i+1}, \Phi\rangle - \langle Q_i, \Phi\rangle = \langle Q_{i+1}, \Phi_0\rangle - \langle Q_i, \Phi_0\rangle < 0 .$$

Comme Φ est définie positive, et comme, pour tout i, l'on a $\langle Q_i, \Phi\rangle < \langle Q_0, \Phi\rangle$, il existe une partie finie S de $\mathbb{Z}^n$ telle que, pour tout i, on ait $S(Q_i) \subset S$. La famille des $S(Q_i)$ est donc finie. Soient i et j deux indices tels que $S(Q_i) = S(Q_j)$. Pour tout $x \in S(Q_i)$, on a $\langle Q_i - Q_j, \Omega_x\rangle = \langle Q_i - Q_j, P_x\rangle$ (car $Q_i - Q_j \in \mathcal{T}$), et cette expression est nulle, puisque $\langle Q_i, P_x\rangle = \langle Q_j, P_x\rangle = m$. Comme Q_i est $\mathcal{T}$-parfaite, les $\Omega_x, x \in S(Q_i)$ engendrent $\mathcal{T}$, et les conditions $\langle Q_i - Q_j, \Omega_x\rangle = 0$ pour tout $x \in S(Q_i)$ entraînent donc $Q_i - Q_j = 0$. Par conséquent, la suite $Q_1, Q_2, \ldots$ est finie, et il existe un indice p tel que Φ appartienne à $\mathcal{D}_{Q_p}$, ce qui entraîne par le lemme 2.7 que $Q_p = Q$, **c.q.f.d.**

Dans la théorie classique de Voronoï, on exprime les résultats sur l'ensemble des classes d'équivalence modulo $\mathrm{Gl}_n(\mathbb{Z})$ de formes quadratiques (de minimum donné). Pour étendre la théorie, on doit introduire la définition suivante :

2.10. Définition. On dit que deux formes quadratiques Q et Q' de matrices respectives A et A' sont *$\mathcal{T}$-équivalentes* s'il existe $M \in \mathrm{Gl}_n(\mathbb{Z})$ vérifiant les deux conditions ${}^tMAM = A'$ et ${}^tM\mathcal{T}M \subset \mathcal{T}$.

2.11. Proposition. *La relation de contiguïté est compatible à la $\mathcal{T}$-équivalence.*

[Cela signifie qu'une $\mathcal{T}$-équivalence entre deux formes $\mathcal{T}$-parfaites met en bijection les ensembles de leurs formes contiguës. En particulier, à deux faces $\mathcal{T}$-équivalentes d'une même forme stable par cette équivalence sont associées des formes contiguës T-équivalentes.]

Démonstration. Rappelons que si deux formes quadratiques R et R' sont équivalentes par une transformation de matrice M, on a, pour tout vecteur-colonne X, $R(X) = R'(M^{-1}X)$.

Soit F une matrice de face du domaine D_Q de Q, et soit $F' = {}^tMFM$. C'est un élément de $\mathcal{T}$. Soit $X \in S(Q)$ tel que Ω_X soit dans la face orthogonale à F de $\mathcal{D}_D$. Alors, $M^{-1}X \in S(Q')$ vérifie

$$\langle F', \Omega_{M^{-1}X}\rangle = \langle F', P_{M^{-1}X}\rangle = \langle F, P_X\rangle = \langle F, \Omega_X\rangle = 0\,.$$

Donc, F' est une matrice de face pour $\mathcal{D}_{Q'}$. (Noter cependant que $\mathcal{D}_{Q'}$ est en général distinct de ${}^tM\mathcal{D}_QM$, car l'équivalence n'est pas une transformation orthogonale pour le produit scalaire $\langle .,.\rangle$.)

Pour tout $\theta \in \mathbb{R}$, soit Q_θ la forme de matrice $A_\theta = A + \theta F$. Soit $\rho \in \mathbb{R} \cup \infty$ la borne supérieure des $\theta \geq 0$ tels que Q_θ soit positive de minimum $m(Q)$ sur $\mathbb{Z}^n$, et soit Q'_θ la forme transformée de Q_θ par M. Sa matrice est $A'_\theta = A' + \theta F'$, et l'égalité $Q'_\theta(M^{-1}X)Q_\theta(X)$ montre que ρ est la borne supérieure des $\theta \geq 0$ tels que Q'_θ soit positive de minimum $m(Q) = m(Q')$ sur $\mathbb{Z}^n$, **c.q.f.d.**

La proposition ci-dessus justifie que l'on opère comme dans l'algorithme classique rappelé en 1.2 pour la recherche des formes $\mathcal{T}$-parfaites à partir d'une forme Q_0 donnée. Toutefois, on ne peut pas garantir la finitude du graphe à $\mathcal{T}$-équivalence près sans hypothèses supplémentaires. Du reste, la notion de $\mathcal{T}$-perfection est purement formelle lorsque l'on ne l'applique pas à des formes possédant des propriétés particulières liées à $\mathcal{T}$, comme dans les exemples 1.3 à 1.5.

2.12. Remarque. Dans le cas classique, Voronoï montre que les demi-droites portant les matrices Ω_x (x parcourant l'ensemble des vecteurs minimaux d'une forme parfaite Q) sont toutes des arêtes de de $\mathcal{D}_Q$, et qu'il n'y a pas d'impasse. Ceci ne se généralise pas : des contre-exemples sont signalés au § 4 (ex. 4.3 et 4.2).

§ 3. Actions de groupes. Soit G un groupe fini. Rappelons qu'une *représentation intégrale de rang n* du groupe G est un homomorphisme $\rho : G \to \mathrm{Gl}_n(\mathbb{Z})$; il revient au même de se donner une structure de $\mathbb{Z}[G]$-module sur $\mathbb{Z}^n$. On dit que deux représentations intégrales ρ et ρ' sont *équivalentes* s'il existe $M \in \mathrm{Gl}_n(\mathbb{Z})$ telle que, pour tous $s \in G$, on ait $M^{-1}\rho(s)M = \rho'(s)$.

Soit L un $\mathbb{Z}[G]$-module, libre de rang n sur $\mathbb{Z}$. On associe de façon naturelle à toute base de L une représentation intégrale de G, ce qui met en bijection les classes d'isomorphisme de $\mathbb{Z}[G]$-modules $\mathbb{Z}$-libres de rang n et les classes d'équivalence de représentations intégrales de rang n de G.

Soit E un espace euclidien et soit $\rho : G \to O(E)$ une représentation orthogonale de G. Un *G-réseau* ([B-M], §1) est un réseau stable par G. L'ensemble $\mathcal{R}_G$ des G-réseaux est non vide si et seulement si ρ est rationnelle sur $\mathbb{Q}$ ([B-M], § 2). Un réseau $\Lambda \in \mathcal{R}_G$ définit plus précisément une classe de représentations intégrales. La correspondance entre $\mathbb{Z}[G]$-modules à isomorphismes près et classes de représentations intégrales se traduit ainsi :

3.1. Proposition. *Pour que deux réseaux Λ et Λ' définissent la même classe de représentations intégrales, il faut et il suffit qu'il existe un élément f du commutant de ρ dans $\mathrm{Gl}(E)$ appliquant Λ sur Λ'.*

Pour déterminer les G-réseaux G-parfaits au sens de [B-M], déf. 2.3, à l'aide d'un algorithme de Voronoï du type du § précédent, il sera nécessaire de distinguer les diverses représentations intégrales définissant une même représentation sur $\mathbb{Q}$. Le problème de classification que cela soulève est en général difficile. Nous verrons en fin de § quelques exemples faciles, relatifs au cas d'un groupe G cyclique.

Étant donnés deux bases $\mathcal{B}$ et $\mathcal{B}'$ et un endomorphisme f de E, on note $\mathrm{Mat}(f, \mathcal{B}, \mathcal{B}')$ la matrice de f dans les bases $\mathcal{B}$ et $\mathcal{B}'$, et l'on écrit simplement $\mathrm{Mat}(f, \mathcal{B})$ lorsque $\mathcal{B} = \mathcal{B}'$. Rappelons que la *matrice de* Gram de $\mathcal{B} = (e_1, \ldots, e_n)$ est $\mathrm{Gram}(\mathcal{B}) = (e_i.e_j)$; on a aussi $\mathrm{Gram}(\mathcal{B}) = \mathrm{Mat}(\mathrm{Id}, \mathcal{B}, \mathcal{B}^*)$, où $\mathcal{B}^*$ désigne la base duale de $\mathcal{B}$ pour la structure euclidienne de E.

Soit $\Lambda \in \mathcal{R}_G$, soit $\mathcal{B}$ une base de Λ et soit $A = \mathrm{Gram}\,\mathcal{B}$. Au couple $(\Lambda, \mathcal{B})$, on associe la forme quadratique $Q(X) = {}^tXAX$, de matrice A, ce qui permet d'associer au réseau Λ la classe modulo $\mathrm{Gl}_n(\mathbb{Z})$ de la forme quadratique Q (n est le rang de Λ). Si l'on passe de la base $\mathcal{B}$ à une base $\mathcal{B}'$ à l'aide de la matrice de passage M, la forme Q devient la forme Q' de matrice $A' = {}^tMAM$. Le remplacement de Λ par un réseau qui lui est isométrique ne modifie pas la classe de formes associée à Λ.

Supposons maintenant que Λ soit dans $\mathcal{R}_G$. Au couple $(\Lambda, \mathcal{B})$ correspond alors la forme quadratique Q de matrice A et une représentation intégrale ρ que l'on peut définir par des matrices $U_s, s \in G$ telles que ${}^tU_sAU_s = A$ (ce qui ne fait que traduire l'appartenance de $\rho(s)$ à $O(E)$; on dit que Q (ou que A) est *invariante par* ρ).

Posons

$$\mathcal{T} = \{T \in \mathrm{Sym}_n(\mathbb{R}) \mid \forall s \in G, {}^tU_sTU_s = T\}.$$

3.2. Proposition. *Un G-réseau Λ' définit une représentation intégrale équivalente à $s \mapsto U_s$ si et seulement s'il possède une base dont la matrice de Gram appartient à $\mathcal{T}$.*

Démonstration. Si Λ' possède une base $\mathcal{B}'$ telle que $\mathrm{Mat}(\rho(s), \mathcal{B}') = U_s$, on a $\mathrm{Gram}(\mathcal{B}') = \mathrm{Gram}\,(\rho(s)(\mathcal{B}'))$ (parce que ρ est orthogonale), ce qui exprime l'appartenance de $\mathrm{Gram}(\mathcal{B}')$ à $\mathcal{T}$.

Réciproquement, soit Λ' un réseau et soit $\mathcal{B}'$ une base de Λ' telle que $A' = \mathrm{Gram}(\mathcal{B}')$ soit dans $\mathcal{T}$ (i.e., on a ${}^tU_sA'U_s = A'$ quel que soit $s \in G$). Montrons que Λ' est isométrique à un réseau Λ'' définisant la même classe de représentations intégrales que le réseau Λ de départ.

Soit $f \in \mathrm{Gl}(E)$ tel que $\Lambda' = f(\Lambda)$. Soit $\mathcal{B}$ une base de Λ telle que $\mathrm{Gram}(\mathcal{B}) = A$ et que $U_s = \mathrm{Mat}(s, \mathcal{B})$ (on a donc ${}^tU_sAU_s = A$), de base duale $\mathcal{B}^*$. On a

$$A' = \mathrm{Mat}({}^tff, \mathcal{B}, \mathcal{B}^*) \text{ et } {}^tU_sA'U_s = \mathrm{Mat}({}^t\rho(s){}^tff\rho(s), \mathcal{B}, \mathcal{B}^*).$$

La condition ${}^tU_sA'U_s = A'$ équivaut à ${}^t\rho(s){}^tff\rho(s) = {}^tff$. Comme ${}^t\rho(s) = \rho(s)^{-1}$ (parce que ρ est orthogonale), cela signifie que $\rho(s)$ et ${}^tff$

commutent. Il en est donc de même de $\sqrt{{}^t ff}$ et $\rho(s)$ ([B-M], dém. du lemme 2.1). Le réseau $\Lambda'' = \sqrt{{}^t ff}(\Lambda)$ est isométrique à $f(\Lambda)$ (on a $f/\sqrt{{}^t ff} \in O(E)$) et est en outre $\mathbb{Z}[G]$-isomorphe à Λ, **c.q.f.d.**

(Nous avons utilisé le fait qu'un endomorphisme symétrique u à valeurs propres ≥ 0 possède une unique racine carrée à valeurs propres ≥ 0 ; il est immédiat que ce résultat s'applique à ${}^t ff$ quel que soit $f \in \mathrm{End}(E)$.)

Soit $\Lambda \in \mathcal{R}_G$. Les G-réseaux voisins de Λ au sens de la topologie induite par celle de $\mathrm{Gl}(E)$ correspondent à la même classe de représentation intégrale de G que Λ, c'est-à-dire appartiennent à l'orbite de Λ sous l'action du commutant de G. Notons $\mathcal{S}_G$ le sous-espace vectoriel des endomorphismes symétriques de E commutant avec $\rho(s)$ pour tout $s \in G$. On montre dans [B-M] que, si le réseau est *G-extrême*, c'est-à-dire s'il réalise un maximum local de l'invariant d'Hermite dans $\mathcal{R}_G$, il est *G-parfait*, en ce sens que les formes linéaires sur $\mathcal{S}_G$

$$\varphi_x \ : \ h \mapsto h(x).x$$

engendrent, quand x décrit l'ensemble $S(\Lambda)$ des vecteurs minimaux de Λ, le dual $\mathcal{S}_G^*$ de $\mathcal{S}_G$.

3.3 Proposition. *Soit $\mathcal{B}$ une base du G-réseau Λ, soit $A = \mathrm{Gram}(\mathcal{B})$ et soit $\mathcal{T}$ l'espace des matrices invariantes par la représentation intégrale associée à $\mathcal{B}$. Alors le réseau Λ est G-parfait si et seulement si A est $\mathcal{T}$-parfaite.*

Démonstration. Comme on l'a remarqué au cours de la démonstration de la proposition 3.2, on a, pour tout endomorphisme h de E et tout $s \in G$,

$$\mathrm{Mat}\left(\rho(s)h\rho(s^{-1}), \mathcal{B}, \mathcal{B}^*\right) = {}^t U_s H U_s \,,$$

où $H = \mathrm{Mat}(h, \mathcal{B}, \mathcal{B}^*)$ et $U_s = \mathrm{Mat}(\rho(s), \mathcal{B})$, de sorte que l'endomorphisme h appartient à $\mathcal{S}_G$ si et seulement si sa matrice H appartient à $\mathcal{T}$.

Par ailleurs, si l'on suppose l'une de ces deux conditions vérifiée, on a, pour tout $x \in E$ représenté par la matrice colonne X dans $\mathcal{B}$:

$$\langle \Omega_X, H \rangle = \langle P_X, H \rangle = {}^t XHX = \varphi_x(h) \ ;$$

on voit ainsi que les $(\Omega_X)_{X \in S(A)}$ engendrent $\mathcal{T}$ si et seulement si les $(\varphi_x)_{x \in S(\Lambda)}$ engendrent $\mathcal{S}_G^*$, **c.q.f.d.**

Remarquons que Ω_X ne dépend que de l'orbite de X : cela résulte du calcul suivant (on a $\sigma \in G$ et $T \in \mathcal{T}$, donc ${}^t U_\sigma T = T U_\sigma^{-1}$)

$$\langle P_{\sigma X}, T \rangle = \langle U_\sigma P_X {}^t U_\sigma, T \rangle = \mathrm{Tr}(U_\sigma P_X (t U_\sigma T)) =$$
$$\mathrm{Tr}(U_\sigma P_X T U_\sigma^{-1}) = \mathrm{Tr}(P_X T) = \langle P_X, T \rangle.$$

Toutefois, on peut avoir $\Omega_X = \Omega_{X'}$ pour deux vecteurs minimaux n'appartenant pas à la même orbite. En outre, contrairement à ce qui se passe dans le cas classique, la demi-droite qui porte Ω_X peut ne pas être une arête du domaine de Voronoï pour $\mathcal{T}$, cf. ex. 4.3.

On montre dans [B-M] (prop. 2.9) que les vecteurs minimaux d'une forme G-invariante G-parfaite engendrent $\mathbb{R}^n$, ce qui assure la connexité du graphe de Voronoï (th. 2.9).

Examinons maintenant deux exemples de classifications de représentations intégrales d'un groupe G cyclique, correspondant à une représentation rationnelle ρ donnée de G.

Supposons d'abord que ρ soit $\mathbb{Q}$-irréductible. Soit m l'ordre de G (donc, ρ est de degré $n = \varphi(m)$). Les $\mathbb{Z}[G]$-modules L tels que $\mathbb{Q} \otimes_{\mathbb{Z}} L$ définisse une représentation isomorphe à ρ s'identifient à des $\mathbb{Z}[\zeta_m]$-modules de rang 1, ce qui met en bijection les classes de représentations intégrales associées à ρ et les classes d'idéaux du m-ième corps cyclotomique. (Pour tout entier $k > 0$, on note ζ_k une racine de l'unité d'ordre k dans une clôture algébrique de $\mathbb{Q}$.) En particulier, il n'y a qu'une classe de représentation intégrale lorsque m est < 23.

Supposons maintenant que G soit d'ordre ℓ premier, ρ étant la *représentation régulière*. Plongeons L dans $\mathbb{Q} \otimes_{\mathbb{Z}} L \simeq \mathbb{Q}[G]$, et soit $\mathfrak{O} = \{\lambda \subset \mathbb{Q}[G] \mid \lambda L \in L\}$ *l'ordre associé* à L. L'ordre $\mathfrak{O}$ est égal à $\mathbb{Z}[G]$ ou à l'ordre maximal $\mathfrak{M} \simeq \mathbb{Z} \times \mathbb{Z}[\zeta_l]$ de $\mathbb{Q}[G]$, puisque $[\mathfrak{M} : \mathfrak{O}] = \ell$. On montre (cf. ci-dessous) que, dans le premier cas, L est projectif sur $\mathfrak{O}$. Il en résulte que les représentations intégrales associées à ρ sont classées par deux invariants : leur ordre associé $\mathfrak{O}$ et une classe d'idéaux de $\mathbb{Q}[\zeta_\ell]$, puisque, lorsque $\mathfrak{O} = Z[G]$, le groupe des classes de $\mathbb{Z}[G]$ s'envoie injectivement dans celui de $\mathfrak{M}$ par extension des scalaires (théorème de Dock Sang Rim, [R]).

Indiquons une justification possible du fait qu'un réseau d'ordre associé $\mathbb{Z}[G]$ est $\mathbb{Z}[G]$-projectif, en revenant d'abord au cas général d'une représentation sur $\mathbb{Q}$ d'un groupe cyclique arbitraire G, définie par un $\mathbb{Q}[G]$-module V.

Pour tout sous-groupe H de G et tout sous-$\mathbb{Z}[G]$-module L de V de type fini engendrant V, le *quotient de Herbrand* $h(H, L)$ ([Se], ch. VIII, § 5) est défini et ne dépend que de H et de la classe d'isomorphisme de V : en effet, si L_1, L_2 et L' sont des sous-$\mathbb{Z}[G]$-modules de V de type fini et engendrant V avec $L' \subset L_1 \cap L_2$, on a $h(H, L_1) = h(H, L')$ et $h(H, L_2) = h(H, L')$, puisque L_1/L' et L_2/L' sont des groupes finis ; on le note $h(H, V)$.

3.4. Lemme. *Si V est libre de rang 1 sur $\mathbb{Q}[G]$, $h(H,V)=1$ quel que soit H.*

En effet, on peut calculer $h(H,V)$ en prenant $L=\mathbb{Z}[G]$, qui est libre sur H pour tout sous-groupe H de G.

3.5. Théorème. *Soit G un groupe cyclique, soit V un $\mathbb{Q}[G]$-module libre de rang 1, et soit L un sous-$\mathbb{Z}[G]$-module de V de type fini et engendrant V. Les conditions suivantes sont équivalentes :*

(1) *L'ordre $\mathfrak{O}$ associé à L est égal à $\mathbb{Z}[G]$.*
(2) *Pour tout sous-groupe H de G et tout entier $m>1$, $\frac{1}{m}\sum_{s\in H} s$ ne stabilise pas L.*
(3) *L est projectif sur $Z[G]$.*
(4) *L est localement libre sur $\mathbb{Z}[G]$.*

Démonstration. Il est clair que (1) entraîne (2), car on a l'implication $(\frac{1}{m}\sum_{s\in H} s)L\subset L \Longrightarrow \frac{1}{m}\sum_{s\in H} s\in\mathfrak{O}$. Si (2) est vérifiée, $\hat{H}^0(H,L)$ est nul pour tout sous-groupe H de G. Il en est donc de même de $\hat{H}^1(H,L)$ puisque $h(H,L)=1$. Le module L est alors cohomologiquement trivial, donc projectif sur $\mathbb{Z}[G]$ puisqu'il est libre sur $\mathbb{Z}$ ([Se], ch. IX, th. 6 et 7). L'implication (3)$\Longrightarrow$(4), qui résulte d'un théorème de Swan qui s'applique plus généralement à tous les groupes finis ([Sw]), est également un résultat standard d'algèbre comutative. Enfin, (4)$\Longrightarrow$(1) est immédiat une fois que l'on s'est ramené par localisation au cas d'un module libre, **c.q.f.d.**

§ 4. Algorithme de Voronoï pour un groupe donné. Nous avons au § 3 décrit les représentations intégrales d'un groupe cyclique lorsqu'il s'agit d'une représentation irréductible ou de la représentation régulière d'un groupe d'ordre premier ℓ. Nous explicitons d'abord l'espace $\mathcal{T}$, en nous limitant aux représentations fidèles, ce qui ne nuit pas à la généralité.

Dans tout ce §, G désigne un groupe cyclique d'ordre $m\geq 3$, σ un générateur de G et ζ une racine d'ordre m de l'unité (dans une clôture algébrique donnée de $\mathbb{Q}$). On se donne en outre une représentation intégrale de G de degré n définie par un réseau Λ muni d'une base $\mathcal{B}$. On se limite au cas où Λ est $\mathbb{Z}[G]$-monogène, et l'on écrit $\Lambda=\mathbb{Z}[G]x$.

L'espace $\mathcal{T}$ introduit au § 3 est constitué par les matrices $\mathrm{Mat}(v,\mathcal{B},\mathcal{B}^*)$ où v parcourt le commutant $\mathrm{End}_G^s(E)$ de G dans $\mathrm{End}^s(E)$. Les matrices de $\mathcal{T}$ s'écrivent $(a_{i,j})$ avec

$$a_{i,j}=v(\sigma^{i-1}x).\sigma^{j-1}x=\sigma^{i-j}v(x).x\,,$$

ce qui, en posant $\alpha_i = \frac{1}{2}(\sigma^i + \sigma^{-i})v(x).x$ $(i \bmod m)$, s'écrit encore $a_{i,j} = \alpha_{i-j}$ $(= \alpha_{j-i})$:

$$(*) \qquad (a_{i,j}) = \begin{pmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \dots & \dots & \alpha_{n-1} \\ \alpha_1 & \alpha_0 & \alpha_1 & \dots & \dots & \alpha_{n-2} \\ \alpha_2 & \alpha_1 & \alpha_0 & \ddots & \dots & \alpha_{n-3} \\ \dots & \dots & \ddots & \ddots & \ddots & \dots \\ \dots & \dots & \dots & \alpha_1 & \alpha_0 & \alpha_1 \\ \alpha_{n-1} & \alpha_{n-2} & \dots & \alpha_2 & \alpha_1 & \alpha_0 \end{pmatrix}.$$

Quant aux $\mathcal{T}$-équivalences, on les recherche entre matrices de $\mathcal{T}$ de la forme (*) associées à des suites α_i et α'_i en recherchant dans le module quadratique $\mathbb{Z}[G]x$ tel que $x.\sigma^i x = \alpha_i$ un élément x' vérifiant $x'.\sigma^i x' = \alpha'_i$. La matrice M correspondante est celle des vecteurs $(x', \sigma x', \dots, \sigma^{n-1}x')$ dans la base $(x, \sigma x, \dots, \sigma^{n-1}x)$; c'est une matrice de $\mathcal{T}$-équivalence, car on vérifie tout de suite qu'elle définit un élément du commutant dans $\mathrm{Gl}_n(\mathbb{Z})$ de la représentation considérée.

Occupons-nous d'abord du cas d'une *représentation $\mathbb{Q}$-irréductible* de G, donc de degré $n = \varphi(m)$ pair ; on pose $n = 2p$. Un choix possible pour Λ est alors $\mathbb{Z}[\zeta]$ plongé dans l'espace $\mathbb{R} \otimes \mathbb{Z}[\zeta]$ muni de la forme bilinéaire $1 \otimes \mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(x\overline{y})$, et rapporté à la base $(1, \zeta, \cdots, \zeta^{n-1}$. Le polynôme cyclotomique (qui est un polynôme réciproque) est de la forme

$$\begin{aligned} \Phi_m(X) &= X^n + a_1 X^{n-1} + \cdots + a_p X^p + \cdots + a_1 X + 1 \\ &= X^p[X^p + X^{-p} + a_1(X^{p-1} + X^{-(p-1)}) + \cdots + a_p], \end{aligned}$$

d'où l'on déduit la matrice représentant σ :

$$U_\sigma = \begin{pmatrix} 0 & 0 & \dots & 0 & -1 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -a_1 \end{pmatrix}.$$

On montre dans [B-M] que l'espace $\mathcal{T}$ (isomorphe à $\mathrm{End}^s_G(E)$) est dans ce cas de dimension p. Or, dans la forme générale des matrices de $\mathcal{T}$, les coefficients $\alpha_p, \alpha_{p+1}, \cdots, \alpha_{n-1}$ sont maintenant combinaisons linéaires des $p = \frac{n}{2}$ paramètres

$$\alpha_0, \alpha_1, \cdots \text{ et } \alpha_{p-1}.$$

On les calcule de proche en proche à l'aide du polynôme cyclotomique : on a

$$\sigma^p + \sigma^{-p} = -a_1(\sigma^{p-1} + \sigma^{-(p-1)}) - \cdots - a_{p-1}(\sigma + \sigma^{-1}) - a_p\,,$$

d'où

$$\alpha_p = -a_1\alpha_{p-1} - \cdots - a_{p-1}\alpha_1 - \frac{1}{2}a_p\alpha_0\,,$$

puis, pour $i = p+1, \cdots, n-1$, la formule de récurrence

$$\sigma^{i+1} + \sigma^{-(i+1)} = (\sigma^i + \sigma^{-i})(\sigma + \sigma^{-1}) - (\sigma^{i-1} + \sigma^{-(i-1)}).$$

On obtient donc ainsi une description complète de l'espace $\mathcal{T}$ des matrices G-invariantes.

Par exemple, pour $m = 3$, on a $\mathcal{T} = \left\{ \begin{pmatrix} \alpha_0 & -\alpha_0/2 \\ -\alpha_0/2 & \alpha_0 \end{pmatrix} \mid \alpha_0 \in \mathbb{R} \right\}$.

Pour $m = 9$, le polynôme cyclotomique est $\Phi_9(X) = X^3(X^3 + X^{-3} + 1)$, d'où l'on déduit les relations définissant $\mathcal{T}$:
$\alpha_3 = -\frac{1}{2}\alpha_0$ et $\alpha_5 = \alpha_4 = -\alpha_1 + \alpha_2$.

Les relations entre les paramètres α_i sont très faciles à expliciter dans le cas où $m = \ell$ est un nombre premier, et donc $n = \ell - 1$: on a alors
$\alpha_p = -\alpha_{p-1} - \alpha_{p-2} - \cdots - \alpha_1 - \frac{1}{2}\alpha_0$, et, pour $1 \leq i \leq p-1$, $\alpha_{p+i} = \alpha_{p-i+1}$.

Notons que l'étude de la représentation $\mathbb{Q}$-régulière de G représentée en dimension ℓ par l'ordre maximal $\mathbb{Z} \times \mathbb{Z}(\zeta)$ de $\mathbb{Q}[G]$, muni de la base $((1,0),(0,1),(0,\zeta),\cdots,(0,\zeta^{n-1}))$, se ramène directement à la précédente : il suffit de "border" la matrice U_σ et celles de $\mathcal{T}$ par une première ligne $(1,0,\cdots,0)$ et la première colonne transposée de celle-ci.

Considérons maintenant la représentation $\mathbb{Z}$-régulière de G. Cette représentation est donc de degré $n = m$, de polynôme caractéristique $X^m - 1$, et correspond au réseau $\mathbb{Z}[G]$ muni de sa base $(1, \sigma, \sigma^2, \cdots, \sigma^{n-1})$, qui conduit pour σ à la matrice suivante :

$$U_\sigma = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}.$$

L'espace $\mathcal{T}$ est constitué des matrices de la forme (*) où les coefficients α_i sont liés par les seules relations $\alpha_i = \alpha_{n-i}\,(= \alpha_{m-i})$: en effet, si l'on pose

$n = 2p$ si n est pair et $n = 2p + 1$ si n est impair, ces matrices dépendent des $p + 1$ paramètres $\alpha_0, \alpha_1, \cdots, \alpha_p$, alors que l'on a vu dans [B-M] que la dimension de $\mathrm{End}_G^s(E)$ est précisément égale à $p + 1$.

4.1. Exemple. $n = 4$, $m = 5$. La représentation s'identifie à celle du groupe G cyclique d'ordre 5 opérant sur $\mathbb{Z}[\zeta_4]$. L'espace $\mathcal{T}$ est de dimension 2. On en considère la base

$$T_1 = \begin{pmatrix} 2 & 0 & -1 & -1 \\ 0 & 2 & 0 & -1 \\ -1 & 0 & 2 & 0 \\ -1 & -1 & 0 & 2 \end{pmatrix} \quad \text{et} \quad T_2 = \begin{pmatrix} 0 & 1 & -1 & -1 \\ 1 & 0 & 1 & -1 \\ -1 & 1 & 0 & 1 \\ -1 & -1 & 1 & 0 \end{pmatrix}.$$

La matrice suivante (qui est la matrice de Gram du réseau A_4 associée au diagramme de Dynkin correspondant) définit une forme $\mathcal{T}$-parfaite :

$$A = T_1 - T_2 = \begin{pmatrix} 2 & -1 & 0 & 0 \\ -1 & 2 & -1 & 0 \\ 0 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{pmatrix}.$$

Les 10 vecteurs minimaux de A se répartissent en 2 orbites auxquelles correspondent les 2 vecteurs de face $F_1 = T_2$ et $F_2 = T_1 - 2T_2$ (il est inutile d'expliciter les faces elles-mêmes). Ces deux vecteurs sont $\mathcal{T}$-équivalents par la matrice

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

(trouvée comme matrice dans la base canonique de $\mathbb{R}^4$ d'un élément d'ordre 4 du normalisateur de G dans $\mathrm{Gl}_n(\mathbb{Z})$)).

On est ramené à étudier le premier vecteur de face $F_1 = T_2$. Pour $\rho = 1$, on obtient la forme de matrice $(T_1 - T_2) + 1 \times T_2 = T_1$, $\mathcal{T}$-équivalente à la forme de départ par la matrice

$$M' = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 1 & 1 & 0 & -1 \\ 0 & 1 & 1 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

qui correspond au changement de base
$(e_1, \sigma e_1, \sigma^2 e_1, \sigma^3 e_1) \mapsto (e_1+e_2, \sigma(e_1+e_2), \sigma^2(e_1+e_2), \sigma^3(e_1+e_2))$. Il n'y a donc

qu'une seule classe de $\mathcal{T}$-équivalence de formes parfaites (i.e., une seule classe de similitude de G-réseaux parfaits au sens de [B-M]) dans le cas d'un groupe $\mathbb{Q}$-irréductible d'ordre 5 en degré 4 (d'où le fait, trouvé antérieurement par Schoof et Washington, que A_4 réalise le maximum de la constante d'Hermite sur ces G-réseaux).

Le cas des groupes d'ordres 8 et 12 est analogue : on trouve encore une seule classe de réseaux parfaits, en l'occurence semblables à D_4, ce qui donne une nouvelle démonstration du th. 4.3 de [B-M].

4.2. Exemple. $n = 5$, $m = 5$. On s'intéresse dans cet exemple à la représentation régulière sur $\mathbb{Q}$ d'un groupe G cyclique d'ordre 5. Il y a deux classes de représentation intégrale sur $\mathbb{Z}$. L'une est définie par le $\mathbb{Z}$-module $\mathbb{Z} \times \mathbb{Z}[\zeta_4]$, et conduit donc d'après l'exemple précédent à une unique forme parfaite à similitude près, à savoir $A_1 \times A_4$, et l'autre est la représentation régulière sur $\mathbb{Z}$, que nous examinons maintenant.

L'espace $\mathcal{T}$ est de dimension 3 ; c'est l'ensemble de matrices suivant :

$$(\alpha,\beta,\gamma) = \begin{pmatrix} \alpha & \beta & \gamma & \gamma & \beta \\ \beta & \alpha & \beta & \gamma & \gamma \\ \gamma & \beta & \alpha & \beta & \gamma \\ \gamma & \gamma & \beta & \alpha & \beta \\ \beta & \gamma & \gamma & \beta & \alpha \end{pmatrix},$$

dont on définit une base (T_1, T_2, T_3) par l'égalité $(\alpha,\beta,\gamma) = \alpha T_1 + \beta T_2 + \gamma T_3$. On vérifie que les deux matrices suivantes

$$M = \begin{pmatrix} 1 & -1 & 1 & 0 & 0 \\ 0 & 1 & -1 & 1 & 0 \\ 0 & 0 & 1 & -1 & 1 \\ 1 & 0 & 0 & 1 & -1 \\ -1 & 1 & 0 & 0 & 1 \end{pmatrix} \quad \text{et} \quad M' = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

sont des matrices de $\mathcal{T}$-équivalence ; M, d'ordre infini, est dans le commutant de G dans $\mathrm{Gl}_n(\mathbb{Z})$, et M', d'ordre 2, dans son normalisateur. Dans la base (T_1, T_2, T_3), les transformations $\Gamma : X \mapsto {}^tMXM$ et $\Gamma' : X \mapsto {}^tM'XM'$ sont définies par les matrices

$$\Gamma : \begin{pmatrix} 3 & -4 & 2 \\ -2 & 4 & -1 \\ 1 & -1 & 1 \end{pmatrix} \quad \text{et} \quad \Gamma' : \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

La matrice de Gram du réseau A_5 dans une base de Korkine-Zolotareff est de la forme

$$A = (2,1,1) = \begin{pmatrix} 2 & 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 & 1 \\ 1 & 1 & 2 & 1 & 1 \\ 1 & 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 1 & 2 \end{pmatrix};$$

elle est parfaite donc $\mathcal{T}$-parfaite, et possède 15 vecteurs minimaux, répartis en trois orbites représentées par les vecteurs $(1,0,0,0,0)$, $(1,-1,0,0,0)$ et $(1,0,-1,0,0)$. Les projections sur $\mathcal{T}$ correspondantes ont pour composantes dans la base duale (T_1^*, T_2^*, T_3^*)

$$\Omega_1 = (1,0,0),\ \Omega_2 = (2,0,0) \text{ et } \Omega_3 = (2,0,-2).$$

Les matrices de face $F_{i,j}$ orthogonales aux matrices Ω_i et Ω_j ont pour composantes dans la base (T_1, T_2, T_3)

$$F_{1,2} = (0,0,-1), \quad F_{1,3} = (0,-1,0) \text{ et } F_{2,3} = (1,1,1).$$

Les faces $F_{1,2}$ et $F_{1,3}$ sont échangées par l'involution Γ', et $F_{2,3}$ est une impasse, la forme quadratique qui lui est associée étant $(x_1+x_2+x_3+x_4+x_5)^2$. La forme contiguë à A le long de $F_{1,2}$ est $B = A + F_{1,2}$ (on a $\rho = 1$), qui est équivalente à une matrice de Gram du réseau D_5 (réseau de racines de déterminant 4).

Par des calculs analogues que nous ne reproduirons pas faute de place, on trouve que B a 4 faces : une impasse, deux faces échangées par $\Gamma' \circ \Gamma^{-1}$ et $\mathcal{T}$-équivalentes à A, et une face dont la forme contiguë C s'interprète comme matrice de Gram du réseau A_5^3 de Coxeter, et est équivalente à la forme Z de Korkine-Zolotareff.

La forme C elle-même a 3 faces, dont l'une a pour forme contiguë B et les deux autres, qui se correspondent par $\Gamma' \circ \Gamma^{-1}$, ont pour formes contiguës des formes R et R' équivalentes à la forme notée Λ_5 dans [B-M], th. 5.3, laquelle est égale à $\frac{1}{5}(10T_1 - 5T_2 + T_3)$.

Enfin, la forme R a 3 faces, dont 2 sont $\mathcal{T}$-équivalentes et ont des formes contiguës $\mathcal{T}$-équivalentes à elle-même, et la troisième est bien sûr équivalente à C. Le graphe de contiguïté modulo $\mathcal{T}$-équivalence est le suivant (les formes soulignées ont une impasse, et la forme entourée est contiguë à elle-même) :

$$\boxed{R} \text{—} C \text{—} \underline{B} \text{—} \underline{A}.$$

Le diagramme de contiguïté complet peut se représenter en dimension 2 (dans une section plane du cône de Voronoï). En envoyant à l'infini dans la direction verticale le point $(5, 10, 10)$, sommet commun à toutes les formes équivalentes à R, on obtient la figure suivante limitée vers le bas par les impasses, dans laquelle Γ s'interprète comme la translation transformant $(2, 1, 0)$ en $(2, 0, 1)$, $(2, 1, 1)$ en $(4, -1, 2)$, ... et Γ' comme la symétrie par rapport à l'axe de symétrie vertical du domaine de $(2, 1, 1)$. Ce diagramme est reproduit à la fin du paragraphe.

4.3. Exemple. $n = 6$, $m = 7$ ou 9. Dans ces deux cas, que nous ne détaillons pas, l'espace $\mathcal{T}$ est de dimension 3 et les graphes de contiguïté à $\mathcal{T}$-équivalence près sont réduits à deux formes, que nous donnons dans les notations classiques des réseaux de dimension 6 :

$$A_6 \text{---} P_6 \qquad \text{et} \qquad E_6 \text{---} E_6^* .$$

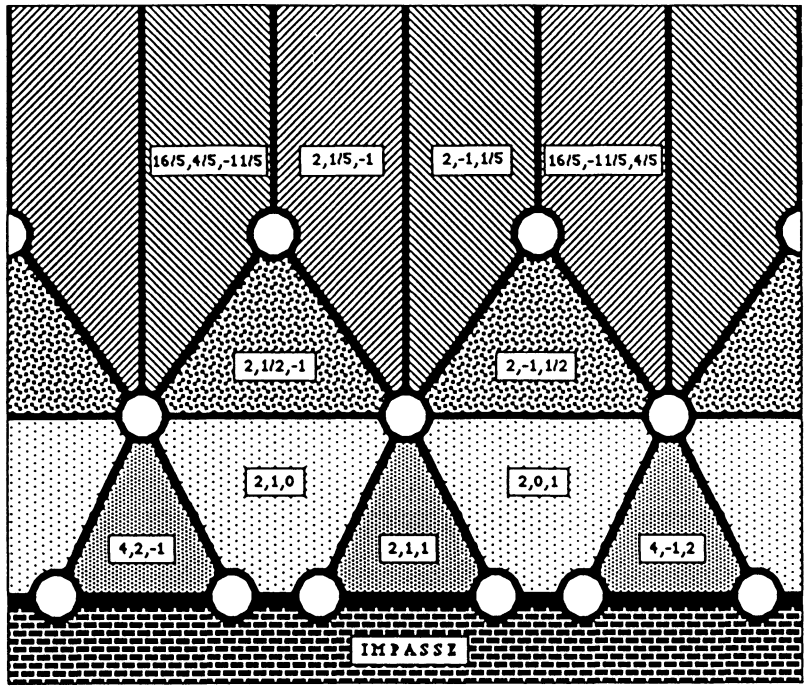
On retrouve encore les résultats de [B-M] (th. 4.6). Signalons que dans le cas de E_6 ($m = 9$), les 36 couples de vecteurs minimaux se répartissent en 4 orbites, mais que seulement 3 des projections associées sur $\mathcal{T}$ sont des arêtes du cône de Voronoï.

4.4 Exemple. $n = 8$, $m = 15$, 16, 20, 24. L'étude n'a été faite qu'à équivalence près, et non pas à $\mathcal{T}$-équivalence près. Les résultats corroborent ceux qui sont annoncés dans [B-M], § 6, et indiquent que dans le cas du groupe d'ordre 20 non traité dans [B-M], E_8 est probablement le seul réseau G-parfait.

[Une erreur typographique s'est glissée dans [B-M] ; dans les données numériques relative à $q = 15$, il faut remplacer $(-1, 0, 0)$ par $(1, 0, 0)$.]

4.5 Exemple. Les calculs effectués en dimension 12 pour le groupe $2A_4$ d'ordre 24 ont permis de trouver 8 réseaux G-parfaits. Parmi ceux-ci se trouve l'exemple connu de $\Lambda_{12}^{\max}$ ([C-S1], ch. 6, [C-S3], § 1), mais aussi un réseau de même déterminant possédant 312 couples de vecteurs minimaux, dont nous avons vérifié qu'il était isométrique à $\Lambda_{12}^{\min}$, prouvant l'existence pour ce réseau d'une structure de module sur l'ordre de Hurwitz. Ces réseaux ont été trouvés indépendamment par M. Laïhem par une méthode de balayage. Les réseaux G- parfaits ont probablement tous été trouvés, mais une démonstration de ce résultat nécessiterait des calculs peut-être trop importants.

Les domaines de Voronoï de l'exemple 4.2.



Dans la figure ci-dessus, les triangles au-dessus de l'impasse sont associés à la forme A, provenant du réseau A_5, et les trapèzes à la forme B, provenant du réseau D_5. Les triangles qui se trouvent au-dessus des domaines décrits ci-dessus sont associés à la forme C, provenant du réseau A_5^3 de Coxeter. Enfin, les domaines du haut de la figure, dont le sommet commun est rejeté à l'infini, sont associés à la forme R, provenant du réseau Λ_5 de [B-M].

§ 5. Indications sur l'algorithme à section donnée. On étudie dans ce § l'exemple 1.4 cité dans l'introduction.

Rappelons que l'on s'est donné une forme Q_0 définie positive à $r < n$ variables et que l'on étudie l'ensemble $\mathcal{E}$ des formes $Q \in \mathcal{Q}_n$ telles que $Q(x_1, \ldots, x_r, 0, \ldots, 0) = Q_0(x_1, \ldots, x_r)$ et $m(Q) = m(Q_0)$. (En termes de réseaux, cela revient à imposer la norme et la section par un sous-espace de dimension r.) On peut montrer que les formes qui réalisent dans $\mathcal{E}$ un maximum local de l'invariant d' Hermite sont $\mathcal{T}$-parfaites pour $\mathcal{T} = \{Q \in \mathcal{Q}_n \mid Q(x_1, \ldots, x_r, 0, \ldots, 0) = 0\}$. Les matrices de $\mathcal{T}$ sont de la

forme

$$\begin{pmatrix} O & M \\ {}^tM & N \end{pmatrix}, \text{ avec } N \text{ symétrique d'ordre } n-r,$$

et la projection Ω_X de

$$P_X = \begin{pmatrix} M_0 & M \\ {}^tM & N \end{pmatrix},$$

est

$$\Omega_X = \begin{pmatrix} O & M \\ {}^tM & N \end{pmatrix},$$

de sorte que les vecteurs minimaux de Q_0 ont une projection nulle. Notons que l'équivalence de deux matrices de $\mathcal{E}$ correspond en termes de réseaux à un endomorphisme de E qui stabilise le réseau et dont la restriction à la section donnée est une isométrie de cette section sur son image. La $\mathcal{T}$-équivalence exige de plus que l'endomorphisme stabilise la section.

On montre facilement que l'hypothèse 2.2 (qui entraîne la connexité du graphe de Voronoï) est vérifiée, et même un peu plus, à savoir que les vecteurs minimaux d'une forme $\mathcal{T}$-parfaite qui ne sont pas dans la section engendrent $\mathbb{R}^n$.

Le cas de la dimension $r = n-1$ est particulièrement simple. L'espace vectoriel euclidien $\mathcal{T}$ est alors de dimension n et peut être identifié à $\mathbb{R}^n$ par

$$\begin{pmatrix} 0 & 0 & \dots & 0 & a_1 \\ 0 & 0 & \dots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \\ a_1 & a_2 & \dots & 0 & a_n \end{pmatrix} \mapsto \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix},$$

muni du produit scalaire $X * Y = 2(x_1y_1 + \cdots + x_{n-1}y_{n-1}) + x_ny_n$. Ainsi, une forme $Q \in \mathcal{E}$ est $\mathcal{T}$-parfaite si et seulement si les vecteurs minimaux de Q dont la dernière composante n'est pas nulle engendrent $\mathbb{R}^n$. On montre en outre que s'il en est ainsi et si Q_0 est parfaite, alors Q est elle-même parfaite.

M. Laïhem ([L]) a entrepris à Bordeaux des calculs étendus concernant le cas où Q_0 est l'une des 33 formes parfaites de rang 7, Q elle-même étant de rang 8. Le nombre de classes de formes parfaites contenant une forme Q_0 donnée peut être très important (par exemple, 93 dans le cas de la forme P_7^{11} de [C-S2]). À l'opposé, dans le cas de $Q_0 = P_7^2 \sim E_7^*$ (l'unique forme parfaite entière de norme 3 en dimension 7), on trouve une seule forme parfaite Q, qui n'est entière que pour le minimum 6. Cela montre qu'une forme parfaite de dimension 8, entière et de minimum 3, s'il en existe, ne contient aucune section parfaite de norme 3 (sauf bien sûr en dimension 1).

BIBLIOGRAPHIE

[Ba] E.S. Barnes, *The complete enumeration of extreme senary forms*, Philos. Trans. Roy. Soc. London **249, A** (1957), 461–505.

[B-M] A.-M. Bergé et J. Martinet, *Réseaux extrêmes pour un groupe d'automorphismes*, Astérisque (1991), à *paraître*.

[C-S1] J. H. Conway et N.J.A. Sloane, *Sphere packings, lattices and groups*, Springer-Verlag, Heidelberg, 1988.

[C-S2] J. H. Conway et N.J.A. Sloane, *Low-dimensional lattices III. Perfect forms*, Proc. R. Soc. Lond. **A 418** (1988), 43–80.

[C-S3] J. H. Conway et N.J.A. Sloane, *Complex and Integral Laminated Lattices*, Trans. Amer. Math. Soc. **280** (1983), 463–490.

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

[J] D.-O. Jaquet, *thèse*, Université de Neuchâtel, 1991.

[L] M. Laïhem, *thèse*, en préparation.

[R] D.S. Rim, *Modules over finite groups*, Ann. of Math. **69** (1959), 700–712.

[Se] J.-P. Serre, *Corps locaux (troisième édition)*, Hermann, Paris, 1980.

[Sw] R.G. Swan, *Induced representations and projective modules*, Ann. of Maths. **71** (1960), 552–578.

[V] G. Voronoï, *Sur quelques propriétés des formes quadratiques positives parfaites*, J. reine angew. Math. **133** (1908), 97–178.

A.-M. B. *et* J.M.
CeReMaB
Université Bordeaux I
351, cours de la Libération
F-33405 Talence cedex

F.S.
Dépt. de Mathématiques
Université de Neuchâtel
Chantemerle 20
CH-2007 Neuchâtel