Journal de Théorie des Nombres
de Bordeaux **7** *(1995), 165–176*

Trois théorèmes de finitude pour les G-formes

par David-Olivier Jaquet-Chiffelle*

Résumé – Dans cet article, nous allons démontrer qu'étant donné G, un sous-groupe fini de $Gl_n(\mathbb{Z})$, il n'y a, à G-équivalence près, qu'un nombre fini de formes G-parfaites (resp. G-eutactiques, G-extrêmes).

Abstract – In this paper, we want to prove that, given G, a finite subgroup of $Gl_n(\mathbb{Z})$, there is, up to G-equivalence, only a finite number of G-perfect (resp. G-eutactic, G-extreme) forms.

1. Rappels

Soit n, un entier positif et q, une forme quadratique réelle définie positive à n variables. On associe à q, de façon canonique, une matrice réelle symétrique définie positive $A_q \in Sym_n(\mathbb{R})$ telle que $\forall x \in \mathbb{R}^n, q(x) = x^t A_q x$. Plus généralement, cette correspondance permet d'identifier l'espace vectoriel des formes quadratiques sur $\mathbb{R}^n$, à l'espace vectoriel $Sym_n(\mathbb{R})$ des matrices symétriques réelles. On rend cet espace euclidien via le produit scalaire induit par la trace : $< A|B >= Trace(AB)$.

On appelle minimum de q, noté $m(q)$ ou $m(A_q)$, le nombre positif suivant :

$$m(q) = m(A_q) = \min_{\substack{x\in\mathbb{Z}^n \\ x\neq 0}} q(x) = \min_{\substack{x\in\mathbb{Z}^n \\ x\neq 0}} x^t A_q x = \min_{\substack{x\in\mathbb{Z}^n \\ x\neq 0}} < A_q | x x^t > .$$

Les vecteurs minimaux de q (ou de A_q) sont les vecteurs $x \in \mathbb{Z}^n$ qui vérifient $q(x) = m(q)$. On note $M(q)$ (ou $M(A_q)$) l'ensemble des vecteurs minimaux de q.

$$M(q) = M(A_q) = \{x \in \mathbb{Z}^n | q(x) = m(q)\}$$

L'invariant d'Hermite de q, noté $\gamma_n(q)$, est défini par $\gamma_n(q) = \frac{m(A_q)}{\sqrt[n]{det A_q}}$. Les formes qui réalisent un maximum local de l'invariant d'Hermite sont dites *extrêmes*.

Manuscrit reçu le 25 janvier 1994, version corrigée le 7 mai 1994.
* L'auteur remercie le "Fonds national suisse de la recherche scientifique" pour son soutien financier, ainsi que le rapporteur pour sa lecture attentive de la version initiale, ses remarques et ses suggestions .

Dans $Sym_n(\mathbb{R})$, regardons les points $xx^t, x \in M(q)$. L'enveloppe convexe des demi-droites fermées issues de l'origine et passant par ces points est appelée *domaine de Voronoï* de la forme q, noté $\mathcal{D}_q$ ou $\mathcal{D}_{A_q}$. Si $\lambda \in \mathbb{R}^+$, il est clair que $\mathcal{D}_{\lambda q} = \mathcal{D}_q$. Une forme q est dite *parfaite* si son domaine est de dimension maximale, c'est-à-dire si $dim\mathcal{D}_A = \frac{n(n+1)}{2}$.
On dit qu'une forme q est *eutactique* si A_q^{-1}, la matrice inverse de A_q, est un point intérieur de $\mathcal{D}_q$.
Voronoï relie ces définitions dans un théorème maintenant classique (Cf [9]) :

THÉORÈME 1.1 (VORONOÏ). *Une forme quadratique réelle définie positive est extrême si et seulement si elle est parfaite et eutactique.*

2. Trois actions de $Gl_n(\mathbb{Z})$

Considérons les trois actions suivantes :

1) α_1 : action de $Gl_n(\mathbb{Z})$ sur $Sym_n(\mathbb{R})$.
Pour $g \in Gl_n(\mathbb{Z})$ et $X \in Sym_n(\mathbb{R})$, on définit :

$$g \cdot X = (g^{-1})^t X g^{-1}$$

2) α_2 : action de $Gl_n(\mathbb{Z})$ sur l'ensemble des domaines de Voronoï.
Pour $g \in Gl_n(\mathbb{Z})$ et $\mathcal{D}$ un domaine de Voronoï, on définit :

$$\begin{aligned} g \cdot \mathcal{D} &= g\mathcal{D}g^t \\ &= \{Y \in Sym_n(\mathbb{R}) | Y = gXg^t, X \in \mathcal{D}\} \end{aligned}$$

3) α_3 : action de $Gl_n(\mathbb{Z})$, par conjugaison, sur l'ensemble de ses sous-groupes.
Pour $g \in Gl_n(\mathbb{Z})$ et H un sous-groupe de $Gl_n(\mathbb{Z})$, on définit :

$$g \cdot H = gHg^{-1}$$

DÉFINITION 2.1. *On appelle* groupe des automorphismes de A, *noté* $Aut(A)$, *le stabilisateur de* A *sous* α_1.

$$\begin{aligned} Aut(A) &= \{g \in Gl_n(\mathbb{Z}) | g \cdot A = A\} \\ &= \{g \in Gl_n(\mathbb{Z}) | (g^{-1})^t A g^{-1} = A\} = \{g \in Gl_n(\mathbb{Z}) | g^t A g = A\} \end{aligned}$$

Définition 2.2. *On appelle* groupe des symétries d'un domaine $\mathcal{D}$, *noté* $\mathcal{S}(\mathcal{D})$, *le stabilisateur de* $\mathcal{D}$ *sous* α_2.

$$\begin{aligned}\mathcal{S}(\mathcal{D}) &= \{g \in Gl_n(\mathbb{Z}) | g \cdot \mathcal{D} = \mathcal{D}\} \\ &= \{g \in Gl_n(\mathbb{Z}) | g\mathcal{D}g^t = \mathcal{D}\}\end{aligned}$$

Les actions α_1, α_2 et α_3 sont compatibles entre elles. En effet, considérons
$X = A$, la matrice d'une forme quadratique réelle définie positive,

$\mathcal{D} = \mathcal{D}_A$, le domaine de Voronoï associé à A,
$Aut(A) < Gl_n(\mathbb{Z})$, le groupe des automorphismes de A,
$\mathcal{S}(\mathcal{D}_A) < Gl_n(\mathbb{Z})$, le groupe des symétries de $\mathcal{D}_A$.

On vérifie sans peine que :
(i) $g \cdot \mathcal{D}_A = \mathcal{D}_{g \cdot A}$ (compatibilité de α_1 et α_2)
(ii) $g \cdot Aut(A) = Aut(g \cdot A)$ (compatibilité de α_1 et α_3)
(iii) $g \cdot \mathcal{S}(\mathcal{D}_A) = \mathcal{S}(g \cdot \mathcal{D}_A)$ (compatibilité de α_2 et α_3)

On dira que deux formes (dont les matrices respectives sont) A et B sont équivalentes si elles sont positivement proportionnelles à deux formes qui appartiennent à la même orbite sous α_1. Donc A et B sont équivalentes si et seulement si

$$\exists \lambda \in \mathbb{R}^+ \text{ et } g \in Gl_n(\mathbb{Z}) \text{ tels que } g \cdot A = \lambda B.$$

L'invariant d'Hermite est constant sur les classes d'équivalence.
On dira que deux domaines sont équivalents s'ils appartiennent à la même orbite sous α_2. La compatibilité des actions α_1 et α_2 nous permet de vérifier sans peine qu'à deux formes équivalentes correspondent deux domaines équivalents (la réciproque est fausse !); si $g \cdot A = \lambda B$, alors $g \cdot \mathcal{D}_A = \mathcal{D}_{g\ A} = \mathcal{D}_{\lambda B} = \mathcal{D}_B$.

3. G-formes

3.1 Résultats classiques à généraliser

Voronoï a montré que pour n fixé, il n'existe, à équivalence près, qu'un nombre fini de formes parfaites. Par 1.1, on conclut qu'à équivalence près toujours, il n'existe qu'un nombre fini de formes extrêmes. Ash dans [1] montre qu'à équivalence près, il n'y a qu'un nombre fini de formes eutactiques.

Le but de notre article est de généraliser ces résultats dans le cas des G-formes.

3.2 Définitions et propriétés fondamentales

Soit G, un sous-groupe fini de $Gl_n(\mathbb{Z})$. On dira d'une forme quadratique réelle définie positive q qu'elle est une *G-forme* si $G < Aut(A_q)$.
L'action α_1 induit une action de G sur $Sym_n(\mathbb{R})$. L'ensemble des points fixes par cette action est un sous-espace vectoriel de $Sym_n(\mathbb{R})$ noté $\mathcal{T}(G)$.

$$\mathcal{T}(G) = \{X \in Sym_n(\mathbb{R}) | \forall g \in G, g \cdot X = X\}$$

En particulier, toute G-forme appartient à $\mathcal{T}(G)$.
On définit le groupe de Bravais de G (Cf, par exemple, [7] et [8]), noté $\mathcal{B}(G)$, comme étant le fixateur de $\mathcal{T}(G)$ sous α_1.

$$\mathcal{B}(G) = \{h \in Gl_n(\mathbb{Z}) | h \cdot X = X, \forall X \in \mathcal{T}(G)\}$$

Remarques :

(i) G est un sous-groupe de $\mathcal{B}(G)$,

(ii) toute G-forme est une $\mathcal{B}(G)$-forme (et réciproquement !),

(iii) $\mathcal{B}(\mathcal{B}(G)) = \mathcal{B}(G)$,

(iv) la correspondance $G \to \mathcal{T}(G)$ n'est pas biunivoque. En effet, plusieurs groupes G peuvent définir le même espace $\mathcal{T}(G)$. Par contre, la correspondance $\mathcal{B}(G) \leftrightarrow \mathcal{T}(G)$, elle, est biunivoque.

Une forme q est dite *G-extrême* si elle réalise dans $\mathcal{T}(G)$ un maximum local de l'invariant d'Hermite.
On appelle *G-domaine* d'une G-forme q, la projection orthogonale de son domaine usuel $\mathcal{D}_q$ sur $\mathcal{T}(G)$.
Une forme q est dite *G-parfaite* si q est une G-forme dont le G-domaine est de dimension maximale dans $\mathcal{T}(G)$. On voit facilement que toute G-forme parfaite est G-parfaite (la réciproque est fausse !).
Une forme q est dite *G-eutactique* si q est une G-forme eutactique et s'il existe des coefficients d'eutaxie constants sur les orbites de vecteurs minimaux sous G. Il est facile de voir, en prenant les moyennes sur les orbites, qu'une G-forme eutactique est toujours G-eutactique (Cf, par exemple, [3]).
On a, pour les G-formes, un théorème analogue au théorème 1.1.

Théorème 3.1 (Bergé-Martinet). *Une G-forme est G-extrême si et seulement si elle est G-parfaite et (G-)eutactique.*

On dira qu'une matrice $h \in Gl_n(\mathbb{Z})$ est une *matrice de G-équivalence* si $h^t\ \mathcal{T}(G)\ h \subset \mathcal{T}(G)$. Il est facile de voir que cette condition équivaut à

$h^t\ \mathcal{T}(G)\ h = \mathcal{T}(G)$. L'ensemble $\mathcal{N}(G)$ des matrices de G-équivalence est le plus grand sous-groupe de $Gl_n(\mathbb{Z})$ pour lequel on peut définir une action sur $\mathcal{T}(G)$ par restriction de α_1.
On dira que deux G-formes A et B sont *G-équivalentes* s'il existe $\lambda \in \mathbb{R}^+$ et h, une matrice de G-équivalence, tels que $h \cdot A = \lambda B$. La notion de G-équivalence est plus forte que la notion d'équivalence. Deux G-formes G-équivalentes sont équivalentes ; par contre, il arrive que deux G-formes équivalentes ne soient pas G-équivalentes.

LEMME 3.2. *Le groupe $\mathcal{N}(G)$ est le normalisateur, dans $Gl_n(\mathbb{Z})$, du groupe de Bravais $\mathcal{B}(G)$, c'est-à-dire*

$$\mathcal{N}(G) = N_{Gl_n(\mathbb{Z})}(\mathcal{B}(G)).$$

Preuve : Soit $h \in Gl_n(\mathbb{Z})$; les énoncés suivants équivalent à dire que h est une matrice de G-équivalence.

$$\begin{aligned}
h \in \mathcal{N}(G) &\Leftrightarrow \forall X \in \mathcal{T}(G), h^{-1} \cdot X \in \mathcal{T}(G)\\
&\Leftrightarrow \forall X \in \mathcal{T}(G), \forall g \in G, g \cdot (h^{-1} \cdot X) = (h^{-1} \cdot X)\\
&\Leftrightarrow \forall X \in \mathcal{T}(G), \forall g \in \mathcal{B}(G), g \cdot (h^{-1} \cdot X) = (h^{-1} \cdot X)\\
&\Leftrightarrow \forall X \in \mathcal{T}(G), \forall g \in \mathcal{B}(G), (hgh^{-1}) \cdot X = X\\
&\Leftrightarrow \forall g \in \mathcal{B}(G), hgh^{-1} \in \mathcal{B}(G)\\
&\Leftrightarrow h \in N_{Gl_n(\mathbb{Z})}(\mathcal{B}(G))
\end{aligned}$$

■

4 Quelques exemples

4.1 $G = \{Id_n\}$ ou $\{\pm Id_n\}$

Lorsque $G = \{Id_n\}$ ou $\{\pm Id_n\}, \mathcal{T}(G) = Sym_n(\mathbb{R})$ et l'on retrouve les notions habituelles de formes parfaites, eutactiques, extrêmes et de domaines de Voronoï. Dans cet exemple, les notions d'équivalence et de G-équivalence coïncident. En effet, $\mathcal{B}(G) = \{\pm Id_n\}$ et $\mathcal{N}(G) = N_{Gl_n(\mathbb{Z})}(\{\pm Id_n\}) = Gl_n(\mathbb{Z})$.
Il y a une infinité de formes parfaites (resp. eutactiques, extrêmes). Mais, nous savons qu'il y a qu'un nombre fini de classes de formes parfaites (resp. eutactiques, extrêmes).

4.2 $G = Aut(A_n), Aut(D_n), Aut(E_6), Aut(E_7), Aut(E_8)$, etc.

Lorsque G est le groupe des automorphismes d'une forme parfaite q et que G agit transitivement sur les vecteurs minimaux de q (une seule orbite), toutes les G-formes sont positivement proportionnelles à q.
De façon générale, deux vecteurs minimaux qui sont dans la même orbite sous G définissent deux arêtes dans $Sym_n(\mathbb{R})$ qui ont même projection sur $\mathcal{T}(G)$. On en conclut que, dans le cas qui nous intéresse, la dimension de la projection de $\mathcal{D}_q$ sur $\mathcal{T}(G)$ est au plus 1. Comme q est une G-forme parfaite, elle est G-parfaite et la dimension de la projection de $\mathcal{D}_q$ sur $\mathcal{T}(G)$ est égale à la dimension de $\mathcal{T}(G)$. Mais cette dernière est toujours supérieure ou égale à 1 ($A = \Sigma_{g\in G} g^t g$ est une matrice symétrique réelle définie positive qui appartient toujours à $\mathcal{T}(G)$). Ainsi, la dimension de $\mathcal{T}(G)$ vaut 1 et on conclut en remarquant que la matrice de Gram associée à q est un élément non-nul de $\mathcal{T}(G)$.
Dans cet exemple, il y a donc, à homothétie près, une seule G-forme. Elle est par conséquent, G-extrême et G-eutactique, donc eutactique.
Il est clair que G est égal à son groupe de Bravais : cela est vrai dès que G est le groupe des automorphismes d'une forme quadratique réelle définie positive. Mais ici, on a mieux ; du fait que la dimension de $\mathcal{T}(G)$ vaut 1, on déduit facilement que G est aussi égal au normalisateur, dans $Gl_n(\mathbb{Z})$, de son groupe de Bravais. Ainsi, on a dans cet exemple $G = \mathcal{B}(G) = \mathcal{N}(G)$.

5 Théorèmes de finitude à G-équivalence près

Nous allons maintenant démontrer trois théorèmes de finitude pour les G-formes, à savoir :

Théorème 5.1. [1] *A G-équivalence près, il n'y a qu'un nombre fini de formes G-parfaites.*

Théorème 5.2. *A G-équivalence près, il n'y a qu'un nombre fini de G-formes eutactiques.*

Théorème 5.3. *A G-équivalence près, il n'y a qu'un nombre fini de formes G-extrêmes.*

Le théorème 5.3 est une conséquence directe des théorèmes 3.1 et 5.1 ou 5.2. Pour démontrer les théorèmes 5.1 et 5.2, nous avons besoin de certains résultats intermédiaires.

[1] Dans [3], A.-M. Bergé et J. Martinet énoncent que *l'ensemble des classes de similitudes de réseaux G-parfaits est fini* (Prop. 3.12). Le théorème 5.1 est plus fort que cette proposition puisqu'il montre la finitude du nombre de classes de formes G-parfaites à $\underline{G}$-équivalence près (et non pas seulement à équivalence près). De plus, comme les auteurs me l'ont signalé, la démonstration qu'ils donnent de leur proposition 3.12 n'est pas correcte.

Lemme 5.4. *Soit A, la matrice d'une forme quadratique réelle définie positive ; $Aut(A)$ est un sous-groupe de $\mathcal{S}(\mathcal{D}_A)$.*

Preuve : Dire que g appartient à $Aut(A)$ revient à dire que $g \cdot A = A$. Par compatibilité des actions α_1 et $\alpha_2, g \cdot \mathcal{D}_A = \mathcal{D}_{g \cdot A} = \mathcal{D}_A$; cela équivaut à dire que g appartient au groupe des symétries de $\mathcal{D}_A$.

■

En général, $\mathcal{S}(\mathcal{D}_A)$ est plus grand que $Aut(A)$; il arrive même que $\mathcal{S}(\mathcal{D}_A)$ soit infini. Mais :

Lemme 5.5. *Si A est la matrice d'une forme parfaite, $Aut(A)$ et $\mathcal{S}(\mathcal{D}_A)$ coïncident.*

Preuve : Soit $g \in \mathcal{S}(\mathcal{D}_A)$; $\mathcal{D}_A = g \cdot \mathcal{D}_A = \mathcal{D}_{g \cdot A}$. On en conclut que A et $g \cdot A$ ont les mêmes vecteurs minimaux. Comme il est clair que $m(A) = m(g \cdot A)$, la perfection de A implique l'égalité $A = g \cdot A$; d'où, $g \in Aut(A)$.

■

Lemme 5.6 (Voronoï). *Tout domaine de Voronoï est soit le domaine d'une forme parfaite, soit une facette de codimension ≥ 1 d'un tel domaine.*

On en déduit,

Lemme 5.7 (Voronoï). *A équivalence près, il n'y a qu'un nombre fini de domaines de Voronoï.*

On a vu dans la démonstration du lemme 5.5 que deux formes parfaites de même minimum et de même domaine sont égales. Cette propriété classique reste vraie pour les G-formes. Plus exactement :

Proposition 5.8. *Deux formes G-parfaites de même minimum et de même G-domaine sont égales.*

Cette proposition est une conséquence immédiate du lemme 2.7 dans [4].

En général, $A \notin \mathcal{D}_A$ et il se peut qu'un domaine $\mathcal{D}$ ne contienne aucune forme quadratique définie positive. Les domaines qui contiennent des formes quadratiques réelles définies positives ont des propriétés particulières.

Lemme 5.9 (Voronoï). *Soit $\mathcal{D}$, un domaine contenant f, une forme quadratique réelle définie positive. Le domaine $\mathcal{D}$ n'est contenu que dans un nombre fini de domaines de formes parfaites.*

Preuve : Il suffit de constater que si A est une forme parfaite dont le domaine contient $\mathcal{D}$ (donc f),

$$< A|f >= \lambda \ m(A) \text{ où } \lambda > 0 \text{ ne dépend pas de } A.$$

Si l'on fixe le minimum, disons $m(A) = 1$, on sait que le nombre de formes parfaites A vérifiant $< A|f >= \lambda$ est fini ; cette propriété, énoncée dans [9], est démontrée de façon détaillée dans [5] (p. 39).

∎

PROPOSITION 5.10. *Soit $\mathcal{D}$, un domaine contenant f, une forme quadratique réelle définie positive. $\mathcal{S}(\mathcal{D})$, le groupe des symétries de $\mathcal{D}$ est un sous-groupe fini de $Gl_n(\mathbb{Z})$.*

Preuve : Soit $\mathcal{V}(\mathcal{D})$, l'ensemble des domaines de formes parfaites contenant $\mathcal{D}$. Le lemme 5.9 montre que $\mathcal{V}(\mathcal{D})$ est un ensemble fini. $\mathcal{S}(\mathcal{D})$ agit sur $\mathcal{V}(\mathcal{D})$ par restriction de α_2. Le fixateur de $\mathcal{V}(\mathcal{D})$ est toujours fini. En effet,

$$\begin{aligned} Fixateur\ (\mathcal{V}(\mathcal{D})) &= \{g \in \mathcal{S}(\mathcal{D}) | g \cdot \mathcal{D}_X = \mathcal{D}_X,\ \forall \mathcal{D}_X \in \mathcal{V}(\mathcal{D})\} \\ &\subset \mathcal{S}(\mathcal{D}_X), \forall \mathcal{D}_X \in \mathcal{V}(\mathcal{D}). \end{aligned}$$

Comme X est une forme parfaite, le lemme 5.5 montre que $\mathcal{S}(\mathcal{D}_X) = Aut(X)$; en particulier, c'est un groupe fini.
Du fait que $\mathcal{V}(\mathcal{D})$ et son fixateur sont tous deux finis, on déduit que $\mathcal{S}(\mathcal{D})$ est, dans ce cas, un groupe fini.

∎

LEMME 5.11. *Soit G, un sous-groupe fini de $Gl_n(\mathbb{Z})$ et h, un élément de $Gl_n(\mathbb{Z})$. Une forme A est G-parfaite si et seulement si $(h \cdot A)$ est $(h \cdot G)$-parfaite.*

Preuve : Il suffit de montrer l'implication dans un sens.
La compatibilité des actions α_1 et α_3 montre que si A est une G-forme, $(h \cdot A)$ est stable par $(h \cdot G)$. Cela a donc un sens de vérifier la $(h \cdot G)$-perfection de $(h \cdot A)$. Remarquons que $\mathcal{T}(h \cdot G) = (h^{-1})^t\, \mathcal{T}(G) h^{-1}$; si $\beta = \{T_1, T_2, ..., T_d\}$ forme une base de $\mathcal{T}(G)$, $h \cdot \beta = \{(h^{-1})^t\, T_1 h^{-1}, (h^{-1})^t\, T_2 h^{-1}, ..., (h^{-1})^t\, T_d h^{-1}\}$ forme une base de $\mathcal{T}(h \cdot G)$; $\mathcal{T}(G)$ et $\mathcal{T}(h \cdot G)$ ont donc la même dimension. Si v est un vecteur minimal de A, hv est un vecteur minimal de $h \cdot A = (h^{-1})^t A h^{-1}$. Calculons la projection orthogonale de $(hv)(hv)^t$ sur $\mathcal{T}(h \cdot G)$, exprimée dans la base duale de $h \cdot \beta$. La i-ème coordonnée est donnée par

$$\begin{aligned} < (h^{-1})^t\, T_i h^{-1} | h v v^t h^t > &= Trace((h^{-1})^t\, T_i h^{-1} h v v^t h^t) \\ &= Trace(T_i v v^t) = < T_i | v v^t > \end{aligned}$$

On retrouve la i-ème coordonnée de la projection orthogonale de vv^t sur $\mathcal{T}(G)$, exprimée dans la base duale de β.

Ainsi, la dimension du G-domaine de A et celle du $(h \cdot G)$-domaine de $h \cdot A$ peuvent se calculer via le rang de la même matrice. Ces dimensions sont donc égales. Par conséquent, si A est G-parfaite, c'est-à-dire si ce rang est maximal, $h \cdot A$ est $(h \cdot G)$-parfaite.

■

La proposition suivante décrit une propriété fondamentale des formes G-parfaites, propriété qui joue un rôle essentiel dans la démonstration du théorème 5.1.

PROPOSITION 5.12. *Soit G, un sous-groupe fini de $Gl_n(\mathbb{Z})$ et q, une forme G-parfaite. Alors, $\mathcal{S}(\mathcal{D}_q)$ est fini ; en particulier, $\mathcal{S}(\mathcal{D}_q)$ ne contient qu'un nombre fini de sous-groupes conjugués, par un élément de $Gl_n(\mathbb{Z})$, au groupe de Bravais $\mathcal{B}(G)$.*

Preuve : Dans [3], la proposition 2.8 montre que si q est une forme G-parfaite, les vecteurs minimaux de q engendrent $\mathbb{R}^n$. Par la proposition 2.3 de [4], on sait que $\mathcal{D}_q$ contient alors au moins une forme quadratique réelle définie positive. Par la proposition 5.10, on en déduit que $\mathcal{S}(\mathcal{D}_q)$ est un groupe fini.

■

Soit G_1, G_2 et G_3, trois groupes tels que $G_1 < G_2 < G_3$. On notera $\mathcal{C}(G_1, G_2, G_3)$, l'ensemble des sous-groupes de G_2, conjugués à G_1 par un élément de G_3. Le groupe G_2 agit naturellement sur $\mathcal{C}(G_1, G_2, G_3)$ par conjugaison. On notera $\mathcal{K}(G_1, G_2, G_3)$, le nombre d'orbites pour cette action.

PROPOSITION 5.13. *Soit G, un sous-groupe fini de $Gl_n(\mathbb{Z})$ et q, une forme G-parfaite. Il y a au plus $\mathcal{K}(\mathcal{B}(G), \mathcal{S}(\mathcal{D}_q), Gl_n(\mathbb{Z})) < \infty$ classes de G-équivalence de formes G-parfaites dont les domaines sont équivalents à $\mathcal{D}_q$.*

Preuve : La proposition 5.12 montre que $\mathcal{C}(\mathcal{B}(G), \mathcal{S}(\mathcal{D}_q), Gl_n(\mathbb{Z}))$ est un ensemble fini ; *a fortiori*, $\mathcal{K}(\mathcal{B}(G), \mathcal{S}(\mathcal{D}_q), Gl_n(\mathbb{Z}))$ est fini.

Soit q_1 et q_2, deux formes G-parfaites dont les domaines usuels sont équivalents à $\mathcal{D}_q$. Il existe g_1 et g_2 dans $Gl_n(\mathbb{Z})$ tels que $\mathcal{D}_q = g_i \cdot \mathcal{D}_{q_i}$, $(i = 1, 2)$. On peut supposer, sans perdre de généralité, que q_1 et q_2 ont le même minimum. Par compatibilité des actions α_2 et α_3,

$$\mathcal{B}(G) \subset \mathcal{S}(\mathcal{D}_{q_i}) \Rightarrow g_i \cdot \mathcal{B}(G) \subset g_i \cdot \mathcal{S}(\mathcal{D}_{q_i}) = \mathcal{S}(\mathcal{D}_q).$$

Les $g_i \cdot \mathcal{B}(G)$ sont des sous-groupes de $\mathcal{S}(\mathcal{D}_q)$ conjugués, par un élément de $Gl_n(\mathbb{Z})$, au groupe de Bravais $\mathcal{B}(G)$.

On peut montrer que les formes q_1 et q_2 sont G-équivalentes si et seulement si $g_1 \cdot \mathcal{B}(G)$ et $g_2 \cdot \mathcal{B}(G)$ sont dans la même orbite de $\mathcal{C}(\mathcal{B}(G), \mathcal{S}(\mathcal{D}_q), Gl_n(\mathbb{Z}))$ sous l'action de $\mathcal{S}(\mathcal{D}_q)$ par conjugaison. Pour achever la démonstration de notre proposition, seul un sens de cette équivalence nous importe, à savoir, si $g_1 \cdot \mathcal{B}(G)$ et $g_2 \cdot \mathcal{B}(G)$ sont dans la même orbite alors q_1 et q_2 sont dans la même classe de G-équivalence.

Dire que $g_1 \cdot \mathcal{B}(G)$ et $g_2 \cdot \mathcal{B}(G)$ sont dans la même orbite équivaut à dire qu'il exite $g \in \mathcal{S}(\mathcal{D}_q)$ tel que $g \cdot (g_1 \cdot \mathcal{B}(G)) = g_2 \cdot \mathcal{B}(G)$. Comme $(gg_1) \cdot \mathcal{D}_{q_1} = g \cdot \mathcal{D}_{g_1 \cdot q_1} = g \cdot \mathcal{D}_q = \mathcal{D}_q$, on peut supposer, quitte à remplacer g_1 par gg_1, que $g_1 \cdot \mathcal{B}(G) = g_2 \cdot \mathcal{B}(G)$.
Posons

$$H = g_1 \cdot \mathcal{B}(G) = g_2 \cdot \mathcal{B}(G) \quad (1)$$

Comme les q_i $(i = 1, 2)$ sont G-parfaites, le lemme 5.11 affirme que les $g_i \cdot q_i$ $(i = 1, 2)$ sont H-parfaites. Elles ont le même domaine $\mathcal{D}_q$, donc le même H-domaine (projection de $\mathcal{D}_q$ sur $\mathcal{T}(H)$) et le même minimum. Par la proposition 5.8, on conclut que

$$g_1 \cdot q_1 = g_2 \cdot q_2 \quad (2)$$

La relation (2) montre que $g_2^{-1} g_1$ fournit une équivalence entre q_1 et q_2. La relation (1) montre que c'est une G-équivalence ; en effet, cette relation équivaut à dire que $g_2^{-1} g_1$ appartient au normalisateur de $\mathcal{B}(G)$ dans $Gl_n(\mathbb{Z})$.

■

Preuve du théorème 5.1 : A toute G-forme correspond un domaine classique de Voronoï. Le lemme 5.7 garantit qu'il n'existe qu'un nombre fini de domaines inéquivalents. *A fortiori*, l'ensemble des domaines $\mathcal{D}_q$, où q est une forme G-parfaite, se décompose aussi en un nombre fini de classes d'équivalence.

La proposition 5.13 montre qu'à G-équivalence près, il n'y a qu'un nombre fini de formes G-parfaites dont les domaines usuels sont équivalents.

Ensemble, ces deux résultats de finitude montrent qu'à G-équivalence près, il n'y a qu'un nombre fini de formes G-parfaites.

■

Proposition 5.14. *Soit G, un sous-groupe fini de $Gl_n(\mathbb{Z})$ et q, une G-forme. Il y a au plus $\mathcal{K}(\mathcal{B}(G), Aut(q), Gl_n(\mathbb{Z})) < \infty$ classes de G-équivalence de G-formes équivalentes à q.*

Preuve : La finitude de $\mathcal{K}(\mathcal{B}(G), Aut(q), Gl_n(\mathbb{Z}))$ découle de la finitude de $Aut(q)$.

Les énoncés des propositions 5.13 et 5.14 présentent une grande similitude. Cette analogie se retrouve partiellement dans la démonstration. En effet, soit q_1 et q_2, deux G-formes équivalentes à q (une G-forme quelconque, cette fois-ci) ; on peut reprendre la première partie de la preuve de 5.13 en faisant jouer à q (resp. q_1, q_2) le rôle de $\mathcal{D}_q$ (resp. $\mathcal{D}_{q_1}, \mathcal{D}_{q_2}$). De façon naturelle, il s'agit de remplacer $\mathcal{S}(\mathcal{D}_q)$ (resp. $\mathcal{S}(\mathcal{D}_{q_1})$, $\mathcal{S}(\mathcal{D}_{q_2})$) par $Aut(q)$ (resp. $Aut(q_1)$, $Aut(q_2)$).

On conclut toutefois plus rapidement que précédemment puisque l'égalité entre domaines $(gg_1) \cdot \mathcal{D}_{q_1} = g_2 \cdot \mathcal{D}_{q_2} = \mathcal{D}_q$ – dans la preuve de 5.13 – se traduit, ici, directement par une égalité entre formes quadratiques : $(gg_1) \cdot q_1 = g_2 \cdot q_2 = q$. La matrice $g_2^{-1} g g_1$ est une matrice de G-équivalence qui envoie q_1 sur q_2.

■

Preuve du théorème 5.2 : Ash dans [1] montre qu'à équivalence près, il n'y a qu'un nombre fini de formes eutactiques. La proposition 5.14 prouve que chaque classe de formes eutactiques ne contient au plus qu'un nombre fini de classes de G-équivalence de G-formes eutactiques.

■

6. Conclusion

Dans [4], les auteurs définissent aussi les notions plus générales de formes $\mathcal{T}$-parfaites, $\mathcal{T}$-extrêmes, etc. où $\mathcal{T}$ est un sous-espace quelconque de Sym_n ($\mathbb{R}$). Le cas des G-formes correspond au cas particulier où $\mathcal{T} = \mathcal{T}(G)$.
Les résultats de finitude de cet article ne sont plus toujours vrais dans le cas des $\mathcal{T}$-formes. En effet, François Sigrist et moi-même venons de construire, en dimension 2, un exemple pour lequel il y a, à $\mathcal{T}$-équivalence près, une infinité de formes $\mathcal{T}$-parfaites (Cf [6]).
Cela souligne l'intérêt des trois théorèmes précédents de finitude pour le cas des G-réseaux, c'est-à-dire lorsque $\mathcal{T} = \mathcal{T}(G)$ provient d'un sous-groupe fini de $Gl_n(\mathbb{Z})$.

Références

[1] A. Ash, *On eutatic forms*, Can. J. Math., Vol. **XXIX, No. 5** (1977), 1040–1054.

[2] A. Ash, *On the existence of eutactic forms*, Bull. London Math. Soc. **12** (1980), 192–196.

[3] A.-M. Bergé et J. Martinet, *Réseaux extrêmes pour un groupe d'automorphismes*, Astérisque ** **200** (1991), 41–66.

[4] A.-M. Bergé, J. Martinet et F. Sigrist, *Une généralisation de l'algorithme de Voronoï*, Astérisque **209** (1992), 137–158.

[5] D.-O. Jaquet-Chiffelle, *Enumération complète des classes de formes parfaites en dimension 7*, Thèse de doctorat, Annales de l'Institut Fourier **Tome 43, Fasc. 1** (1993), 21–55.

[6] D.-O. Jaquet-Chiffelle et F. Sigrist, *Classification des formes quadratiques réelles : un contre-exemple à la finitude*, Acta Arithmetica **LXVIII.3** (1994), 291–294.

[7] W. Plesken, *The Bravais group and the normalizer of a reducible finite subgroup of* $Gl_n(\mathbb{Z})$, Communications in algebra **5 (4)** (1977), 375–396.

[8] S. S. Ryškov, *Maximal finite groups of integral* $n \times n$ *matrices and full groups of integral automorphims of positive quadratic forms (Bravais models)*, Trudy Mat. Inst. Steklov, Proc. Steklov Inst. Math. **128** (1972), 217–250.

[9] G. Voronoï, *Sur quelques propriétés des formes quadratiques positives parfaites*, J. reine angew. Math **33** (1908), 97–178.

David-Olivier Jaquet-Chiffelle
Confédération suisse
Section fédérale de cryptologie
Hofweg 11 CH-3013 Berne
Suisse