Document de synthèse en vue de l'Habilitation à Diriger des Recherches

Renaud Coulangeon

9 février 2005

Introduction

Les travaux présentés dans ce document de synthèse relèvent de la “Géométrie des Nombres”. Cette branche de la théorie des nombres initiée par Minkowski à la fin du XIXème siècle a été très active durant toute la première moitié du XXième siècle. Une notion classique, antérieure à la Géométrie des Nombres de Minkowski et dont il sera question, en filigrane, dans tout ce qui suit, est la notion de “constante d'Hermite”. L'application qu'en fit Minkowski aux classes d'idéaux des corps de nombres est sans doute l'exemple le plus populaire d'utilisation des méthodes de la géométrie des nombres en arithmétique. Néanmoins, l'étude de la constante d'Hermite (et de constantes analogues dont il sera question plus loin) présente un intérêt en dehors même de toute application à la théorie des nombres. Ainsi, dans sa présentation géométrique classique, la constante d'Hermite en dimension n correspond à la densité maximale d'un empilement de sphères régulier dans cette dimension. A cette question sont liés, plus ou moins directement, de nombreux problèmes de théorie de l'information, en particulier ceux relevant de la théorie des codes correcteurs d'erreurs. Plus généralement, il existe une très grande variété de mathématiques reliées d'une façon ou d'une autre à cette question d'apparence anodine : théorie des groupes, formes modulaires, courbes elliptiques etc ; (voir, par exemple, l'excellent survey de N. Elkies dans les Notices de l'AMS [20], ou le livre de référence [17] de Conway et Sloane).

J'ai souhaité privilégier dans la présentation qui suit, une certaine cohérence thématique de mes travaux, autour de l'extension de la théorie de Voronoï. Pour cette raison, je n'ai pas adopté une démarche strictement chronologique.

J'ai regroupé dans une première partie ceux de mes travaux qui concernent la théorie de Voronoï.

Dans une seconde partie, j'expose les résultats obtenus en collaboration avec C. Bachoc, E. Bannai et G. Nebe, et qui relèvent davantage de la “combinatoire algébrique”.

La troisième et dernière partie traite de travaux antérieurs, effectués juste après ma thèse, portant sur les propriétés du produit tensoriel de réseaux.

Par ailleurs, j'ai souhaité mettre l'accent sur les relations entre mes travaux et ceux d'autres chercheurs, et sur les diverses collaborations entreprises ces dernières années avec C. Bachoc (Bordeaux), G. Nebe (Ulm, Allemagne), E. Bannai (Fukuoaka, Japon), R. Baeza, M.I Icaza et M. O'Ryan (Talca, Chili) et T. Watanabe (Osaka, Japon).

Chapitre 1

Invariants d'Hermite généralisés.

Une part importante des travaux présentés dans ce premier chapitre ainsi que dans le suivant, concerne la constante d'Hermite et ses généralisations. Nous allons rappeler brièvement dans un premier paragraphe quelques notions classiques sur l'invariant d'Hermite d'une forme quadratique définie positive, ou d'un réseau.

1.1 L'invariant d'Hermite.

Rappelons pour commencer la définition de cet invariant classique : on note $S_n(\mathbb{R})$ l'espace des matrices réelles symétriques de taille n, identifié à l'espace des formes quadratiques en n variables, à l'intérieur duquel on distingue le cône $P_n = S_n(\mathbb{R})_{>0}$, correspondant aux formes quadratiques définies positives. Un élément A de P_n définit une fonction sur $\mathbb{R}^n$: $X \mapsto A[X] = XAX'$ [1], valeur en X de la forme quadratique correspondant à A. L'ensemble des valeurs prises par une forme quadratique définie positive sur $\mathbb{Z}^n$, ou plus généralement sur un sous-ensemble discret de $\mathbb{R}^n$, admet un minimum, atteint en un nombre fini de points. On définit donc

$$m(A) = \min_{X \in \mathbb{Z}^n \setminus \{0\}} A[X], \tag{1.1}$$

que l'on homogénéise en

$$\gamma(A) = \frac{m(A)}{(\det A)^{\frac{1}{n}}} \quad \textit{invariant d'Hermite de } A. \tag{1.2}$$

L'ensemble (fini) de vecteurs *minimaux* de A (ceux sur lesquels est atteint le minimum) est noté $S(A)$.

La constante d'Hermite en dimension n est définie comme

$$\gamma_n := \sup_{A \in P_n} \gamma(A). \tag{1.3}$$

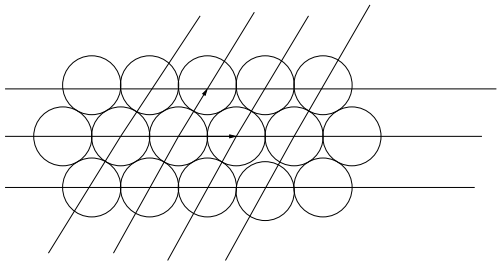
[1] dans la suite, on note M' la transposée d'une matrice M

La valeur exacte de γ_n n'est connue que jusqu'à la dimension 8. Au-delà, il y a des conjectures très vraisemblables dans certaines dimensions particulières, mais qui ne sont probablement pas démontrables avec les méthodes appliquées jusqu'en dimension 8.

Attardons-nous un instant sur la signification géométrique de l'invariant (*resp.* de la constante) d'Hermite. Toute matrice A de P_n peut se décomposer sous la forme $A = PP'$, où $P \in \mathrm{GL}_n(\mathbb{R})$ est essentiellement unique modulo $O_n(\mathbb{R})$. On associe alors à A le *réseau* $L = \mathbb{Z}^n P$ dans R^n (on fait opérer $\mathrm{GL}_n(\mathbb{R})$ à gauche sur $\mathbb{Z}^n$), ou plus exactement la classe d'isométrie de ce réseau (P n'est défini que modulo $O_n(\mathbb{R})$). Le nombre $\gamma(A)$ précédemment défini est donc un invariant de la classe d'isométrie du réseau L, que l'on peut définir directement comme :

$$\gamma(L) = \frac{\min_{l \in L \setminus \{0\}} ||l||^2}{\det L^{1/n}} \tag{1.4}$$

On constate alors que la quantité $\gamma(L)^{n/2}$ est proportionnelle à la densité de l'empilement de sphères associé à L.



Le calcul de γ_n est donc équivalent à la détermination de la densité maximale d'un empilement de sphère régulier[2]. Une idée naturelle pour élucider cette question, est d'étudier les maxima locaux de la fonction $A \mapsto \gamma(A)$. En 1873, Korkine et Zolotareff ont, les premiers, exploité cette idée ([31],[32]), et ont introduit le terme de formes

[2] Par empilement de sphères régulier on entend empilement de sphères disjointes de même rayon centrées aux points d'un réseau.

extrêmes pour désigner ces maxima locaux. C'est Voronoï qui donnera, trente ans après leurs travaux ([41]), une caractérisation complète des formes extrêmes, *via* les notions de forme parfaite et eutactique, dont nous rappelons maintenant la définition.

Definition 1.1.1 *(i) Une forme A est* parfaite *si les matrices $X'X$, $X \in S(A)$, engendrent $S_n(\mathbb{R})$.*

(ii) Une forme A est eutactique *si la matrice A^{-1} appartient à l'enveloppe convexe des matrices $X'X$, $X \in S(A)$.*

Une autre façon de formuler la perfection est de dire qu'une forme quadratique définie positive A est parfaite si elle est complètement déterminée par l'ensemble des équations $A[X] = m(A), X \in S(A)$. En d'autres termes, si $B[X] = m(A)$ pour tout $X \in S(A)$, alors $B = A$. Le théorème fondamental de Voronoï s'énonce alors ainsi

Théorème 1.1.1 (Voronoï 1908) *Une forme A est* **extrême** *si et seulement si elle est à la fois parfaite et eutactique.*

Une conséquence remarquable est que la constante γ_n est atteinte sur une forme rationnelle, et que $\gamma_n^n \in \mathbb{Q}$.

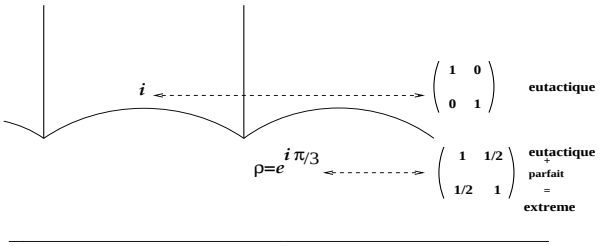
La théorie de Voronoï offre en fait beaucoup plus que cela : dans l' article [41] où figure le théorème ci-dessus, est également développé un algorithme qui conduit à une décomposition cellulaire $GL_n(\mathbb{Z})$-invariante de l'espace P_n, et dont les cellules de dimension 0 correspondent exactement aux formes parfaites. Ceci permet en principe de déterminer systématiquement les formes parfaites dans une dimension donnée, et de calculer par conséquent la constante d'Hermite de cette dimension. En pratique, la complexité de l'algorithme le rend inaccessible aux moyens de calculs actuels dès la dimension 8. Signalons cependant, que l'utilisation de ce complexe cellulaire fourni par l'algorithme de Voronoï, permet en principe de calculer l'homologie de $GL_n(\mathbb{Z})$ et la K-théorie de $\mathbb{Z}$. Les travaux les plus récents dans ce domaine sont dus à Elbaz-Vincent, Gangl et Soulé ([21]).

Dans le cas des formes en deux variables, une autre interprétation géométrique fournit une image pour les notions de perfection et d'eutaxie. Il y a en effet dans ce cas une bijection naturelle entre le demi-plan de Poincaré $\mathfrak{H} := \{z \in \mathbb{C} : \Im(z) > 0\}$ et le cône P_2 modulo homothétie :

$$\begin{array}{ccc} \mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H} & \longleftrightarrow & \mathbb{R}_{>0}\backslash P_2/\mathrm{SL}_2(\mathbb{Z}) \\ z = x + iy & \longleftrightarrow & \begin{pmatrix} 1 & x \\ x & x^2+y^2 \end{pmatrix} \end{array}$$

Pour $z = x + iy \in \mathfrak{H}$, la quantité $\frac{1}{y}$ mesure la distance à l'infini Ainsi, du côté droit du schéma ci-dessus, une forme avec un invariant d'Hermite élevé correspond à un point de $\mathfrak{H}$ de partie imaginaire petite, c'est à dire de distance à l'infini élevée. Ceci est illustré par la figure ci-dessous :

Le fait que le point $\rho = e^{\frac{2i\pi}{3}}$ soit à l'intersection des cercles $|z| = 1$ et $|z - 1| = 1$ est relié à la perfection de la forme correspondante. De même, la propriété qu'a le point i de réaliser un minimum local sur le cerle $|z| = 1$ pour la distance à l'infini, peut s'interpréter en termes d'eutaxie de la forme correspondante.



[h]

Dans les années récentes, différentes variantes de la constante d'Hermite ont été étudiées, parmi lesquelles la constante de Bergé-Martinet ([6]), la constante des G-réseaux ([7], [8]), la constante de Rankin ([13]), la constante de Humbert dont il sera question au paragraphe suivant ([26], [16]). Dans tous ces cas, un analogue du théorème de Voronoï a été établi. Les résultats les plus généraux quant aux extensions du théorème de Voronoï sont dus à Bavard ([5]).

1.2 Invariant d'Hermite-Humbert.

Il y a eu plusieurs tentatives pour développer une "géométrie des nombres dans un contexte relatif", *i.e.* où le corps des rationnels serait remplacé par un corps de nombres arbitraire (voir par exemple [38]). Dans les années 40, P. Humbert écrit deux longs articles sur la "théorie de la réduction des formes quadratiques sur un corps de nombres" ([24],[25]). Ces travaux, quelque peu méconnus, ont été exhumés en 1997 par Maria Ines Icaza ([26])[3]. En fait, les objets considérés dans cette théorie de la réduction ne sont pas exactement des formes quadratiques, mais plutôt ce que nous

[3]Signalons également l'article [43] d'Hermann Weyl qui reprend, de manière un peu plus synthétique, les résultats de Humbert.

appellerons dans la suite des "formes de Humbert", selon la terminologie introduite par Icaza. Ces dernières sont définies comme suit : tout d'abord, on considère un corps de nombres k, avec $[k : \mathbb{Q}] = d$. On note $\{v_1, \ldots, v_r\}$ l'ensemble des *places réelles*, correspondant aux plongements réels de k, et $\{v_{r+1}, \ldots, v_{r+s}\}$ l'ensemble des *places complexes*, correspondant aux couples de plongements complexes 2 à 2 conjugués de k, de sorte que $d = r + 2s$. Comme dans le cas classique détaillé dans le premier paragraphe, on doit définir un espace de formes $S_{n,k}$ ainsi qu'un cône $P_{n,k}$ d'éléménts positifs. On procède de la façon suivante :

$$\begin{aligned} S_{n,k} &:= S_n(\mathbb{R})^r \times H_n(\mathbb{C})^s \\ &\cup \\ P_{n,k} &:= S_n(\mathbb{R})^r_{>0} \times H_n(\mathbb{C})^s_{>0}. \end{aligned}$$

Definition 1.2.1 *Une forme de Humbert de rang n sur k est un $(r+s)$-uplet $\mathcal{A} = (A_1, \ldots, A_r, A_{r+1}, \ldots, A_{r+s})$ dans $P_{n,k}$.*

La valeur d'une forme de Humbert $\mathcal{A}$ en un vecteur u de k^n est définie comme suit : à $u \in k^n$ on associe ses conjugués $u^{(1)}, \ldots, u^{(r+s)}$ et on pose

$$\begin{aligned} \mathcal{A}[u] &:= \prod_{i=1}^{r+s} A_i[u^{(i)}]^{d_i} \text{ avec } d_i = \begin{cases} 1 \text{ si } v_i \text{ réel} \\ 2 \text{ si } v_i \text{ complexe} \end{cases} \\ &= \prod_{i=1}^{r} A_i[u^{(i)}] \prod_{i=r+1}^{r+s} A_i[u^{(i)}]^2. \end{aligned}$$

Cette définition de la valeur d'une forme en un vecteur diffère de celle adoptée par la plupart des auteurs ayant abordé ces questions([38], [30],[34], [1]) : dans les références que nous venons de citer, en effet, on définit la valeur d'un $(r+s)$-uplet de formes $\mathcal{A} = (A_1, \ldots, A_r, A_{r+1}, \ldots, A_{r+s})$ dans $P_{n,k}$ en $u \in k^n$ comme

$$\mathcal{A}(u) = \sum_{i=1}^{r+s} d_i A_i[u^{(i)}].$$

Ce point de vue "additif" a plusieurs avantages sur le point de vue "multiplicatif" que nous proposons, notamment celui de permettre un extension presque sans changement de la théorie de Voronoï exposée au paragraphe précédent, algorithme compris. Il présente néanmoins un certain nombre d'inconvénients. Tout d'abord, comme on le verra au paragraphe suivant, si l'on veut inclure cette théorie dans le cadre général défini par Watanabe, c'est le point de vue multiplicatif qui s'impose. Par ailleurs, un certains nombres de propriétés "naturelles" sont mises en défaut si l'on fait le choix de la définition additive. En voici deux exemples :

- *Invariance par multiplication par une unité* : l'analogue naturel de la propriété $A[-u] = A[u]$ dans le cas classique, est $A[\xi u] = A[u], \xi \in \mathcal{O}_k^\times$, ce qui est vérifié avec la définition multiplicative, mais pas avec le définition additive.

- *Homogénéité* : si k est totalement réel, avec $[k : \mathbb{Q}] = r$, l'exemple type de forme de Humbert est fourni par les r-uplets de la forme $(A^{(1)}, \ldots, A^{(r)})$, où les $A^{(i)}$ sont les conjugués d'une matrice symétrique totalement définie positive A à coefficients dans k. Dans ce cas, il est naturel de vouloir "identifier" A et tous ses multiples de la forme αA, avec $\alpha \in k$ totalement positif. Pour cela, il est nécessaire qu'il y ait une relation simple entre les valeurs prises par A et αA en un même vecteur u, ce qui est le cas avec la définition "multiplicative" ($\alpha A[u] = \mathrm{N}_{K/\mathbb{Q}}(\alpha) A[u]$), mais pas avec la définition "additive".

Soit $\mathcal{O}_k$ l'anneau des entiers de k. À partir de maintenant nous supposerons, pour simplifier l'exposition, que le nombre de classes h_k de k est 1, *i.e.* que $\mathcal{O}_k$ est principal (le cas général est traité en annexe).

Definition 1.2.2 *Le minimum d'une forme de Humbert $\mathcal{A} \in P_{n,k}$ est defini par*

$$m(\mathcal{A}) = \min\{\mathcal{A}[u] \ : \ u \in \mathcal{O}_k^n \setminus \{0\}\}.$$

L'invariant d'Hermite-Humbert de $\mathcal{A}$ est

$$\gamma(\mathcal{A}) = \frac{m(\mathcal{A})}{(\det \mathcal{A})^{1/n}},$$

où $\det \mathcal{A} = \prod_i \det A_i^{d_i} = \prod_{i=1}^{r} \det A_i \prod_{i=r+1}^{r+s} (\det A_i)^2$

Remarque *(i) Si $k = \mathbb{Q}$, alors$P_{n,k} = P_n$, et l'invariant d'Hermite-Humbert coïncide avec l'invariant d'Hermite classique.*

(ii) Quand $h_k > 1$, on doit considérer simultanément h_k invariants d'Hermite-Humbert distincts pour une forme de Humbert$\mathcal{A}$ donnée, indéxés par les classes d'idéaux $\{[\mathfrak{a}_1], \cdots, [\mathfrak{a}_{h_k}]\}$, et définis en remplaçant $\mathcal{O}_k^n$ par les réseaux $\mathfrak{a}_i \oplus \mathcal{O}_k^{n-1}$, $i = 1, \cdots, h_k$ dans la définition ci-dessus, voir l'annexe 1.6.

Les vecteurs de $\mathcal{O}_k^n$ réalisant le minimum $m(\mathcal{A})$ sont dits *minimaux*. Noter, qu'ils sont *a priori* en nombre infini, puisque si u est minimal, alors ξu est minimal pour tout ξ appartenant au groupe des unités $\mathcal{O}_k^\times$ de $\mathcal{O}_k$. Cependant, modulo multiplication par les unités, on obtient un ensemble fini.On pose

$$S(\mathcal{A}) := \{u \in \mathcal{O}_k^n \text{ minimal pour} \mathcal{A}\}/\mathcal{O}_k^\times$$

Dans [26]), Icaza établit le théorème suivant :

Théorème 1.2.1 (Icaza, 1997) $\gamma_{n,k} := \sup_{\mathcal{A} \in P_{n,k}} \{\gamma(\mathcal{A})\} < \infty$*et est atteint.*

En s'inspirant de la terminologie de Korkine et Zolotareff, nous appellerons *extrêmes* les formes de Humbert réalisant un maximum local de l'invariant γ. Ces formes extrêmes peuvent être caractérisées par un théorème de type Voronoï. Cela nécessite quelques définitions supplémentaires.

À un vecteur $u \in \mathcal{O}_k^n$, on associe le $r+s$-uplet

$$u' u_{\mathcal{A}} := \left(d_1 \frac{\overline{u^{(1)}}' u^{(1)}}{A_1[u^{(1)}]}, \ldots, d_{r+s} \frac{\overline{u^{(r+s)}}' u^{(r+s)}}{A_{r+s}[u^{(r+s)}]} \right) \in S_{n,k}.$$

Definition 1.2.3 *Une forme de Humbert $\mathcal{A} = (A_1, \ldots, A_{r+s})$ est parfaite si*

$$\dim_{\mathbb{R}} \sum_{u \in S(\mathcal{A})} \mathbb{R} u' u_{\mathcal{A}} = r\frac{n(n+1)}{2} + sn^2 - (r+s-1).$$

Definition 1.2.4 *Une forme de Humbert$\mathcal{A} = (A_1, \ldots, A_{r+s})$ est eutactique si sa forme adjointe $\overline{\mathcal{A}^{-1}} = (\overline{A_1^{-1}}, \ldots, \overline{A_{r+s}^{-1}})$ appartient à l'intérieur de l'enveloppe convexe des $(r+s)$-tuples $u' u_{\mathcal{A}},\ u \in S(\mathcal{A})$. En d'autres termes, $\mathcal{A}$ est eutactique si il existe $\rho_u > 0$, $u \in S(\mathcal{A})$ tels que :*

$$\overline{A_i^{-1}} = \sum_{u \in S(\mathcal{A})} \rho_u d_i \frac{\overline{u^{(i)}}' u^{(i)}}{A_i[u^{(i)}]} \text{ pour } i = 1, \ldots, r+s.$$

Bien sûr,quand $k = \mathbb{Q}$,ces définitions coïncident avec les notions classiques de perfection et d'eutaxie mentionnées au paragraphe précédent. Dans [16], on obtient une caractérisation des formes de Humbert extrêmes :

Théorème 1.2.2 ([16]) *Une forme de Humbert $\mathcal{A}$ est extrême si et seulement si elle est à la fois eutactique et parfaite.*

Bien que l'énoncé de ce théorème soit en tous points similaire au théorème de Voronoï, sa démonstration est sensiblement plus compliquée.Un outil général pour obtenir ce genre de résultats est la condition (C) de Bavard (voir [5]).

Comme conséquence, on obtient également les propriétés suivantes :

Théorème 1.2.3 ([16]) *(i) (Algebricité) Toute forme de Humbert parfaite $\mathcal{A}$ de dimension n est équivalente, modulohomothétie,à une forme de Humbert $\mathcal{B}$ définie sur une extension finie de k.*

(ii) (Finitude) L'ensemble des formes de Humbert parfaites de dimension n sur un corps de nombres k donné, modulo homothétie et $GL_n(\mathcal{O}_k)$-équivalence, est fini.

Malheureusement, il n'y a pas d'algorithme de Voronoï général pour déterminer toutes les formes parfaites dans une dimension donnée. Néanmoins, en dimension 2, nous avons pu calculer quelques constantes d'Hermite-Humbert sur des corps quadratiques réels de petit discriminant. Il s'agit d'un travail commun [4] avec M.I. Icaza, R. Baeza et M. O'Ryan de l'Université de Talca (Chili).

Théorème 1.2.4 ([4]) *La valeur de $\gamma_{2,k}$ pour les corps quadratiques réels $k = \mathbb{Q}(\sqrt{d})$, $d = 2, 3, 5$ est donnée dans le tableau suivant :*

d	2	3	5
$\gamma_{2,\mathbb{Q}(\sqrt{d})}$	$\frac{4}{2\sqrt{6}-3}$	4	$4/\sqrt{5}$

La démonstration repose de façon cruciale sur le théorème (1.2.2), ainsi que sur la théorie de la réduction des formes de Humbert.

Ces résultats en dimension 2 peuvent être interprétés en termes de surfaces modulaires de Hilbert (voir [4] pour les details). En effet, si k est un corps de nombres totalement réel avec $[k : \mathbb{Q}] = r$, il y a une action naturelle de $\mathrm{SL}_2(\mathcal{O}_k)$ sur $\mathfrak{H}^r$, induite

par le plongement diagonal de $\mathrm{SL}_2(\mathcal{O}_k)$ dans $\mathrm{SL}_2(\mathbb{R})^r$ et l'action standard de $\mathrm{SL}_2(\mathbb{R})$ sur $\mathfrak{H}$. Le quotient $\mathrm{SL}_2(\mathcal{O}_k)\backslash\mathfrak{H}^r$ est, par définition, une surface modulaire de Hilbert. Comme dans le premier paragraphe, on obtient une bijection

$$\mathrm{SL}_2(\mathcal{O}_k)\backslash\mathfrak{H}^r \longleftrightarrow \mathbb{R}^r_{>0}\backslash P_{2,k}/\mathrm{SL}_2(\mathcal{O}_k)$$

Si l'on suppose à nouveau, pour simplifier, que $h_k = 1$, alors l'invariant de Hermite-Humbert d'une forme $\mathcal{A} \in P_{2,k}$ peut être interprété comme la distance à l'infini du point correspondant de $\mathrm{SL}_2(\mathcal{O}_k)\backslash\mathfrak{H}^r$:

$$\begin{aligned} \text{“distance à } \infty\text{”} &\longleftrightarrow \text{“}\gamma(\mathcal{A})\text{”} \\ \text{“maximum local”} &\longleftrightarrow \text{“forme de Humbert extrême”} \end{aligned}$$

Le problème de trouver les points d'une surface modulaire de Hilbert de distance à l'infini maximale a été étudié par H. Cohn dans les années 60 (voir [11]). Pour les corps quadratiques réels $\mathbb{Q}(\sqrt{d})$, $d = 2, 3, 5$, il formule quelques conjectures qui, une fois traduites dans le language approprié, apparaissent comme conséquences de notre théorème.

Remarque *Si $h_k > 1$, alors il y a h_k "pointes", en bijection avec les classes d'idéaux de $\mathcal{O}_k$, et h_k invariants de Humbert, correspondant à la distance à ces différentes pointes.*

1.3 Une application à l'approximation diophantienne.

On a rappelé, au premier paragraphe de ce chapitre, l'interprétation classique de la constante d'Hermite en termes de densité d'empilements de sphères. Une telle interprétation, pour ce qui concerne la constante d'Hermite-Humbert sur un corps de nombres arbitraire est moins évidente. Néanmoins, cette constante apparait assez naturellement dans diverses questions. Nous en développons brièvement un exemple dans ce paragraphe, qui a trait au "lemme de Siegel" en approximation diophantienne. Dans sa formulation usuelle, ce lemme affirme l'existence d'une solution non nulle de petite hauteur pour tout système de m équations linéaires homogènes en n variables, $n > m$. Dans un article très récent [40], J.D. Vaaler établit la version "optimale" suivante du lemme de Siegel sur un corps de nombres :

Théorème 1.3.1 *Soit k un corps de nombres, $n > m$ deux entiers naturels et $M \in M_{m,n}(k)$ de rang m. Alors il existe $0 \neq \xi \in k^n$ such that $M\xi = 0$ et*

$$H(\xi) \leq \gamma_{n-m}(k)^{1/2} H(M)^{1/(n-m)}, \tag{1.5}$$

où $\gamma_{n-m}(k)$ désigne la constante d'Hermite-Humbert de k en dimension $n-m$ (pour la définition précise de la hauteur H, voir [40]).

Le résultat ci-dessus est optimal, en ce sens que Vaaler démontre que l'on ne peut pas remplacer $\gamma_{n-m}(k)^{1/2}$ dans ([40]) par une constante plus petite[4].

[4]Ceci s'applique en particulier pour $k = \mathbb{Q}$, et c'est alors la constante d'Hermite classique qui apparait.

1.4 Constantes d'Hermite généralisées (d'après T. Watanabe).

Dans ses travaux récents, T. Watanabe (Osaka) a proposé une vaste généralisation de la géométrie des nombres "classique" dans un cadre adélique (voir [42],[33]).

Le cadre général est le suivant : on considère un corps de nombres k, et un groupe algébrique connexe réductif G défini sur k. Soit $\mathfrak{V} = \mathfrak{V}_f \cup \mathfrak{V}_\infty$ l'ensemble des places de k, et $\mathbb{A}$ l'anneau des adèles de k . On fixe ensuite une représentation $\rho : G \longrightarrow GL(V)$ fortement k-rationnelle et absolument irréductible, dans un k-espace vectoriel V (voir [42],[33] pour les détails). Soit D le sous-espace de plus haut poids ("highest weight space") de ρ, et P son stabilisateur (c'est un sous-groupe parabolique.Alors $X = G/P$ est une variété projective lisse, plongée dans $\mathbb{P}(V)$ via ρ. Sur chaque localisation $V_v = V \otimes_k k_v$, $v \in \mathfrak{V}$, on fixe une norme $||\cdot||_v$. On doit ensuite choisir un sous-groupe compact maximal K dans$G(\mathbb{A})$, assujetti à certaines conditions techniques. Pour $x \in GL(V(\mathbb{A}))V(k)$, on pose$||x||_{\mathbb{A}} := \prod_{v\in\mathfrak{V}} ||x_v||_v$. L'une des conditions à satisfaire pour K est que $||.||_{\mathbb{A}}$ soit K-invariante. Finalement, $||.||_{\mathbb{A}}$ est normalisée par la condition $||x_0||_{\mathbb{A}} = 1$ pour $x \in D(k) \setminus \{0\}$ (ce qui peut être obtenu moyennant un choix convenable des normes locales $||\cdot||_v$).

Pour tout $g \in G(\mathbb{A})^1 := \{g \in G(\mathbb{A}) : \forall \chi \in X_k(G) \quad |\chi(g)|_{\mathbb{A}} = 1\}$, définissons $H_g(x) := ||\rho(g\gamma)x_0||_{\mathbb{A}}^{1/[k:\mathbb{Q}]}$, où $x = \rho(\gamma)x_0$. Alors,

Théorème 1.4.1 ([42])

$$K \setminus G(\mathbb{A})^1/G(k) \longrightarrow \mathbb{R}_+$$
$$g \mapsto \min_{x\in X(k)} H_g(x)$$

est une fonction continue bornée. La constante d'Hermite généralisée associée à $(\rho, ||.||_{\mathbb{A}})$ *est*

$$\mu(\rho, ||.||_{\mathbb{A}}) := \max_{g\in G(\mathbb{A})^1} \min_{x\in X(k)} H_g(x)^2.$$

EXEMPLES : $G = GL_n$

(i) $k = \mathbb{Q}$,
   (a) si ρ est la représentation naturelle dans $\mathbb{Q}^n$, alors $\mu(\rho, ||.||_{\mathbb{A}}) = \gamma_n$, la constante d'Hermite classique.
   (b) si ρ_d est la représentation naturelle dans $\bigwedge^d \mathbb{Q}^n$, alors $\mu(\rho, ||.||_{\mathbb{A}}) = \gamma_{n,d}$ constante de Rankin (voir [37],[13]).

(ii) $k =$ corps de nombres,
   (a) si ρ est la représentation naturelle dans k^n, alors $\mu(\rho, ||.||_{\mathbb{A}}) = \gamma_{n,k}$ constante d'Hermite-Humbert .
   (b) si ρ_d est la représentation naturelle dans $\bigwedge^d k^n$, alors $\mu(\rho, ||.||_{\mathbb{A}}) = \gamma_{n,d}$ constante de Rankin-Thunder (voir [39]).

Il est naturel de se demander s'il existe une théorie de Voronoï générale pour caractériser les maxima locaux de $\mu(\rho, ||.||_{\mathbb{A}})$. Nous conjecturons, avec T. Watanabe, que cela devrait être le cas au moins pour les groupes classiques. Nous traitons, dans un travail en cours (voir [18]), le cas du groupe linéaire sur un corps de quaternions.

1.5 Perspectives.

En dehors de la "conjecture" mentionnée ci-dessus, de nombreuses pistes de travail sont ouvertes. Ainsi, l'adaptation de l'algorithme de Voronoï sur un corps quadratique imaginaire, ou bien un corps de quaternions sur $\mathbb{Q}$, ne pose pas de problèmes théoriques, ce qui ouvre la voie à de nombreuses exploitations numériques. Au-delà, les applications connues de l'algorithme de Voronoï au calcul de l'homologie de $GL_n(\mathbb{Z})$ et à la K-théorie de $\mathbb{Z}$ devraient, de la même façon produire des résultats au niveau de la K-théorie de l'anneau des entiers d'un corps quadratique imaginaire.

Par ailleurs, nous poursuivons avec M.I. Icaza et M. O'Ryan l'étude (plus difficile) des formes de Humbert sur un corps quadratique réel. Signalons également le travail récent de M. Pohst et M. Wagner [35], qui reprennent les méthodes que nous avons introduites dans [4] pour traiter de nouveaux exemples.

Enfin, nous comptons entreprendre l'étude des constantes d'Hermite généralisés pour d'autres groupes que le groupe linéaire, en particulier pour le groupe symplectique.

1.6 Annexe.

Au paragraphe 1.2, nous avons donné une définition simplifiée de l'invariant d'Hermite-Humbert (il s'agit de la définition introduite par Icaza dans [26], reprise par la suite dans [16] et [4]). A posteriori, il apparait que cette définition n'est pas la plus naturelle quand le nombre de classes du corps de nombres considéré est supérieur à 1, car elle ne coïncide pas avec la définition adélique de Watanabe. Nous donnons donc dans cette annexe une définition plus complète, qui prend en compte le cas d'un nombre de classes supérieur à 1.

Comme précédemment, k est un corps de nombres, $\mathcal{O}_k$ son anneau d'entiers, $\mathcal{C}l_k$ son groupe des classes d'idéaux, de cardinal h_k. Pour des raisons techniques, notamment la formule 1.11 ci-desous, on fixe dans chaque classe d'idéaux un représentant $\mathfrak{a}_i$ entier, de norme minimale parmi les idéaux entiers de même classe, en convenant par exemple que $\mathfrak{a}_1 = \mathcal{O}_k$.

Soit $L \subset k^n$ un $\mathcal{O}_k$-réseau, *i.e.* L un sous-module projectif de type fini de k^n tel que $kL = k^n$. Il est bien connu qu'un tel réseau est isomorphe à une somme directe $I_1 \oplus \cdots \oplus I_n$ d'idéaux fractionnaires, et que la classe du produit $I_1 \cdots I_n$ dans $\mathcal{C}l_k$ est un invariant complet de la classe d'isomorphisme de L, dite "classe de Steinitz de L, est notée $St(L)$. La principale différence entre le cas $h_k = 1$ et le cas $h_k > 1$ est que dans le second cas, on doit évaluer une forme de Humbert donnée $\mathcal{A}$ non seulement sur les $\mathcal{O}_k$-réseaux libres (ceux dont la classe de Steinitz est triviale), mais sur tous les $\mathcal{O}_k$-réseaux de k^n. Cela conduit à définir h_k invariants distincts , correspondants aux différentes classes.

Soient donc $\mathcal{A}$ une forme de Humbert et $L \subset k^n$ un $\mathcal{O}_k$-réseau, de classe de Steinitz $St(L) = [\mathfrak{a}_i]$, autrement dit $L = I_1 e_1 \oplus \cdots \oplus I_n e_n$, et $[I_1 \cdots I_n] = [\mathfrak{a}_i]$. À $x = \sum x_i e_i \in L$, on associe l'idéal entier $\mathfrak{a}_x = x_1 I_1^{-1} + \cdots + x_n I_n^{-1}$. On définit le

minimum de $\mathcal{A}$ relativement à L comme

$$m_L(\mathcal{A}) = \min_{x \in L \setminus \{0\}} \frac{\mathcal{A}[x]}{N(\mathfrak{a}_x)^2}, \tag{1.6}$$

son *déterminant* relativement à L comme

$$\det_L \mathcal{A} = N(I_1 \cdots I_n)^2 \det \mathcal{A}, \tag{1.7}$$

et son invariant d'Hermite-Humbert relativement à L

$$\gamma_L(\mathcal{A}) = \frac{m_L(\mathcal{A})}{(\det_L \mathcal{A})^{\frac{1}{n}}}. \tag{1.8}$$

La *constante* d'Hermite-Humbert relativement à L est alors définie par :

$$\gamma_L = \sup_{\mathcal{A} \in P_{n,k}} \gamma_L(\mathcal{A}). \tag{1.9}$$

Clairement, $\gamma_L = \gamma_{L'}$ si $St(L) = St(L')$. Il est donc suffisant de considérer les réseaux $L_i := \mathfrak{a}_i \oplus \mathcal{O}_k^{n-1}$, $1 \leq i \leq h$ et les constantes d'Hermite-Humbert associées $\gamma_i := \gamma_{L_i}$.

Finalement, on pose

$$\gamma_{n,k} := \max_{1 \leq i \leq h} \gamma_i. \tag{1.10}$$

Quand $h_k = 1$, on retrouve bien entendu la définition donnée au paragraphe 1.2. Pour déterminer $\gamma_{n,k}$, on calcule séparément chacun des $\gamma_i = \sup_{\mathcal{A} \in P_{n,k}} \gamma_{L_i}(\mathcal{A})$. Pour une forme donnée $\mathcal{A}$, on a $m_i(\mathcal{A}) := m_{L_i}(\mathcal{A}) = min_{1 \leq j \leq h} m_{i,j}(\mathcal{A})$, où

$$m_{i,j}(\mathcal{A}) = \min_{\substack{x \in L_i \setminus \{0\} \\ [\mathfrak{a}_x] = [\mathfrak{a}_j]}} \frac{\mathcal{A}[x]}{N(\mathfrak{a}_x)^2} = \min_{\substack{x \in L_i \setminus \{0\} \\ \mathfrak{a}_x = \mathfrak{a}_j}} \frac{\mathcal{A}[x]}{N(\mathfrak{a}_j)^2} \tag{1.11}$$

Les résultats de [16] peuvent s'étendre sans difficulté, à condition de traiter séparément chacune des constantes γ_i. On peut définir ainsi des notions de γ_i-extremalité, γ_i-perfection et γ_i-eutaxie, et obtenir l'analogue du théorème 1.2.2, en remplaçant dans tous les énoncés l'ensemble $S(\mathcal{A})$ des vecteurs minimaux de $\mathcal{A}$ par l'ensemble $S_i(\mathcal{A})$ des vecteurs minimaux de $\mathcal{A}$ relativement à L_i, c'est-à-dire :

$$S_i(\mathcal{A}) := \{u \in L_i \setminus \{0\} \mid \frac{\mathcal{A}[x]}{N(\mathfrak{a}_x)^2} = m_i(\mathcal{A})\}/\mathcal{O}_k^\times$$

Chapitre 2

Combinatoire algébrique et designs.

Les travaux présentés dans cette seconde partie relèvent de la combinatoire algébrique. Ils ont donné lieu à deux articles, l'un en collaboration avec C. Bachoc (Bordeaux) et G. Nebe (Ulm, Allemagne), et le second en collaboration avec C. Bachoc et E. Bannai (Fukuoka, Japon). On y traite de notions généralisées de "design sphérique" et de "code sphérique". Nous commençons, dans le paragraphe suivant, par un bref rappel sur ces deux notions, avant d'aborder nos propres résultats.

2.1 Designs et codes sphériques

Une référence classique pour ces questions est l'article fondateur de Delsarte, Goethals et Seidel ([19]). On note S^{n-1} la sphère unité dans $\mathbb{R}^n$, munie de sa mesure $O(n)$-invariante canonique dx, normalisée en sorte que $\int_{S^{n-1}} dx = 1$.

Definition 2.1.1 *Un sous ensemble fini X de S^{n-1} est un t-design, t étant un entier positif, si pour tout polynôme homogène f de degré au plus t on a*

$$\int_{S^{n-1}} f(x)dx = \frac{1}{|X|} \sum_{x \in X} f(x) \tag{2.1}$$

On voit aisément l'intérêt de cette notion pour des applications à l'intégration numérique : un t-design fournit en effet une méthode de quadrature d'ordre t pour le calcul approché d'intégrales sur la sphère. En vue de ce type d'applications, il est naturel de rechercher de tels t-design de cardinal aussi petit que possible. Une question cruciale est donc de trouver une borne inférieure pour la taille d'un t-design.

Definition 2.1.2 *Un sous ensemble fini X de S^{n-1} est un A-code, si les produits scalaires de vecteurs 2 à 2 distincts de X appartiennent à un ensemble fixé $A \subset [-1, 1]$.*

À l'inverse du problème précédent, il est naturel ici de chercher une borne supérieure pour la taille d'un A-code : quand $A = [-1, 1/2]$, trouver une telle borne est équivalent au problème du "kissing number" (pour $n = 3$, il s'agit du classique "problème des 13 sphères").

Une variante de la notion de A-code est celle de s-code :

Definition 2.1.3 *Un sous ensemble fini X de S^{n-1} est un s-code, s étant un entier positif, si les produits scalaires de vecteurs 2 à 2 distincts de X prennent au plus s valeurs*

$$|\{x \cdot y, x \neq y \in X\}| \leq s \tag{2.2}$$

Delsarte, Goethals et Seidel ont introduit une méthode générale, utilisant l'analyse harmonique sur le groupe orthogonal, pour étudier simultanément la question d'une borne inférieure pour la taille d'un t-design, et d'une borne supérieure pour la taille d'un s-code, mettant en évidence une sorte de dualité entre les deux problèmes.

Designs et réseaux.

La théorie des réseaux euclidiens fournit de nombreux exemples de designs : si L est un réseau de $\mathbb{R}^n$, *i.e.* un sous-groupe discret de $\mathbb{R}^n$ de rang maximal, $S(L)$ l'ensemble de ses vecteurs minimaux (*i.e.* l'ensemble fini des vecteurs non nuls de L de longueur minimale), on peut voir $S(L)$, convenablement renormalisé, comme un sous ensemble fini S^{n-1}. Dans de nombreux cas, on obtient ainsi un t-design, pour des valeurs de t variables. Qui plus est, et c'est là l'une des motivations principales pour notre travail sur les designs généralisées, le fait que l'ensemble des vecteurs minimaux d'un réseau possède cette propriété de design a une incidence sur l'invariant d'Hermite du réseau, grâce au remarquable théorème suivant, dû à B. Venkov :

Théorème 2.1.1 ([41]) *Si $S(L)$ est un 4-design, alors L réalise un maximum local pour l'invariant d'Hermite $\gamma(L) = \frac{\min L}{(\det L)^{1/n}}$.*

Une généralisation de ce résultat est exposée au paragraphe suivant.

2.2 Designs et codes dans les grassmanniennes.

Les problèmes d"'empilements" dans les grassmanniennes $\mathcal{G}_{m,n}$ et des questions combinatoires connexes ont été soulevées récemment dans une série d'articles (voir [12], [10]). Ce sont ces articles qui ont motivés nos propres travaux, que nous résumons dans les paragraphes qui suivent.

2.3 Grassmannniennes.

La grassmannienne $\mathcal{G}_{m,n}$ (*resp.* la grassmanienne orientée $\mathcal{G}^{\circ}_{m,n}$) est l'ensemble des sous-espaces (*resp.* des sous-espaces orientés) de dimension m de $\mathbb{R}^n$. Ce sont des espaces homogènes isomorphes, respectivement, à $O(n)/O(m) \times O(n-m)$ et $O(n)/SO(m) \times O(n-m)$, de sorte que $\mathcal{G}^{\circ}_{m,n}$ est un revêtement 2 feuillets de $\mathcal{G}_{m,n}$.

$$\begin{array}{c} \mathcal{G}^{\circ}_{m,n} \simeq O(n)/SO(m)\times O(n-m) \\ {\scriptstyle (2:1)}\big\downarrow \\ \mathcal{G}_{m,n} \simeq O(n)/O(m)\times O(n-m) \end{array}$$

EXEMPLE : $m=1$

$$\begin{array}{c} \mathcal{G}^{\circ}_{1,n} = S^{n-1} \\ {\scriptstyle (2:1)}\big\downarrow \\ \mathcal{G}_{1,n} = \mathbb{P}^{n-1} \end{array}$$

Une première difficulté est de caractériser les positions relatives de deux sous-espaces de dimension m de $\mathbb{R}^n$, ou, en termes plus sophistiqués, de caractériser l'orbite sous $O(n)$ d'un couple $(p,q)\in {\mathcal{G}_{m,n}}^2$. Dans le cas $m=1$, la position relative de deux droites issues de l'origine dans $\mathbb{R}^n$ est simplement déterminée par leur angle. En général, on définit un m-uplet d'*angles principaux* de la façon suivante : on fixe un point base p_0, par exemple $p_0 :=$ le sous-espace engendré par les m premiers vecteurs de la base canonique de $\mathbb{R}^n$. Chaque couple $(p,q)\in {\mathcal{G}_{m,n}}^2$ peut alors être écrit sous la forme $(p,q)=(g.p_0,h.p_0)$ pour des éléments g et h convenables dans $O(n)$. On décompose la matrice $g^{-1}h$ en blocs

$$g^{-1}h=\begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

avec $A\in M_m(\mathbb{R})$, et on note $1\geq y_1\geq y_2\geq\cdots\geq y_m\geq 0$ les valeurs propres dela matrice symétrique réelle AA^t. Finalement, on pose $t_i:=\sqrt{y_i}=\cos\theta_i\in[0,1]$. C'est un résultat classique qu'alors, l'orbite sous $O(n)$de (p,q) est caractérisée par le m-uplet $(t_1,\cdots,t_m)$.

$$O(n).(p,q)\leftrightarrow(t_1,\cdots,t_m). \tag{2.3}$$

Pour ce qui concerne les orbites sous $O(n)$ d'un ouple $(\tilde{p},\tilde{q})\in {\mathcal{G}^{\circ}_{m,n}}^2$, on a besoin d'un invariant suppléméntaire, à savoir $\epsilon:=\frac{\det A}{|\det A|}$:

$$O(n).(\tilde{p},\tilde{q})\leftrightarrow(\epsilon,t_1,\cdots,t_m). \tag{2.4}$$

2.4 Un peu d'analyse harmonique. Fonctions zonales.

L'espace des fonctions de carré intégrable sur $\mathcal{G}_{m,n}$, resp $\mathcal{G}^{\circ}_{m,n}$, se décompose comme somme directe de $O(n)$-modules irréductibles $H^{\mu}_{m,n}$, indéxés par les partitions $\mu=\mu_1\geq\cdots\geq\mu_m$ d'un entier k en au plus m parts non nulles, de la façon suivante (voir.[23] p. 546 ou [3]) : on dit qu'une partition $\mu=\mu_1\geq\cdots\geq\mu_m\geq 0$ d'un entier k est *admissible* si

$$\mu_i\equiv\mu_j \mod 2 \text{ pour tout } (i,j), \tag{2.5}$$

et que μ est *paire* (resp. *impaire*), si ses composantes sont paires (resp. impaires). L'entier $k = \sum \mu_i$, aussi noté $|\mu|$, est le *degré* de μ. On a alors :

$$\begin{array}{ccc} L^2(\mathcal{G}^\circ_{m,n}) & = & \bigoplus_{\mu \text{ admissible}} H^\mu_{m,n} \\ \uparrow & & \\ L^2(\mathcal{G}_{m,n}) & = & \bigoplus_{\substack{\mu \text{admissible} \\ \text{et paire}}} H^\mu_{m,n} \end{array}$$

EXEMPLE : $m = 1$, $\mu = k$, $H^k_{1,n} = \mathrm{Harm}_k[X_1, \cdots, X_n]$, l'espace des polynômes harmoniques de degré k.

Il est à noter que $H^\mu_{m,n}$ ne dépend que de n et μ, c'est-à-dire que si $m \leq m'$ et μ est une partition en au plus m parts non nulles, alors $H^\mu_{m,n} \simeq H^\mu_{m',n}$.

À chaque composante irréductible $H^\mu_{m,n}$ est associée une fonction *zonale* P_μ définie sur $\mathcal{G}^\circ_{m,n} \times \mathcal{G}^\circ_{m,n}$ et caractérisée par :

(i) $P_\mu(p, .) \in H^\mu_{m,n}$ pour tout $p \in \mathcal{G}^\circ_{m,n}$, $P_\mu(., q) \in H^\mu_{m,n}$ pour tout $q \in \mathcal{G}^\circ_{m,n}$

(ii) $P_\mu(\sigma p, \sigma q) = P_\mu(p, q)$ pour tout $\sigma \in O(n)$, $(p, q) \in {\mathcal{G}^\circ_{m,n}}^2$.

Si μ est paire, on a

$$P_\mu(p, q) = p_\mu(y_1(p, q), \cdots, y_m(p, q)),$$

où $p_\mu(Y_1, \cdots, Y_m)$ est un polynôme symétrique de degré $\frac{|\mu|}{2}$, tandis que si μ est impaire

$$P_\mu(p, q) = (\epsilon t_1 \cdots t_m) p_\mu(y_1, \cdots, y_m),$$

où $p_\mu(Y_1, \cdots, Y_m)$ est un polynôme symétrique de degré $\frac{|\mu|-m}{2}$.

À partir de maintenant, on normalise les fonctions zonales de sorte que :

$$P_\mu(p, p) = 1.$$

On a alors les propriétés suivantes :

(i) $\langle P_\mu(p, .), P_\lambda(q, .)\rangle = \frac{\delta_{\lambda,\mu}}{d_\mu} P_\mu(p, q)$,
où $d_\mu = \dim H^\mu_{m,n}$.

(ii) $P_\lambda P_\mu = \sum_\tau c_{\lambda,\mu}(\tau) P_\tau$, avec $c_{\lambda,\mu}(\tau) \geq 0$.

2.5 Designs.

Pour tout entier $k \geq 1$, on définit

$$H^+_k := \bigoplus_{\substack{|\mu| \leq k \\ \mu \text{paire}}} H^\mu_{m,n} \subset L^2(\mathcal{G}_{m,n}) \subset L^2(\mathcal{G}^\circ_{m,n})$$

$$\text{et } H^-_k := \bigoplus_{\substack{|\mu| \leq k \\ \mu \text{impaire}}} H^\mu_{m,n} \subset L^2(\mathcal{G}_{m,n})^\perp \subset L^2(\mathcal{G}^\circ_{m,n}).$$

Venons-en à la définition des designs généralisés :

Definition 2.5.1 ([3]) *Un sous-ensemble$\mathcal{D} \subset \mathcal{G}_{m,n}$ est un $2k$-design si*

$$\forall \varphi \in H_{2k}^{+}\ ,\ \int_{\mathcal{G}_{m,n}} \varphi(p)dp = \frac{1}{|\mathcal{D}|}\sum_{p\in\mathcal{D}} \varphi(p)$$

Il est à noter que, puisque la définition est donnée en termes de grassmannienness *non orientées* , ce que l'on obtient pour $m = 1$ n'est pas exactement la définition d'un design sphérique donnée au paragraphe précédent, mais, de façon plus restrictive, la notion de design *antipodal* (voir [19]).

Il y a plusieurs critères pour déterminer si un sous ensemble donné d'une grassmannienne est un design. Le premier met en jeu les fonctions zonales P_μ.

Proposition 2.5.1 ([3]) *Les propriétés suivantes, pour un sous-ensemble fini $\mathcal{D} \subset \mathcal{G}_{m,n}$, sont équivalentes :*

(i) *$\mathcal{D}$ est un $2k$-design.*

(ii) *$\forall \mu$ avec $2 \leq |\mu| \leq 2k$, $\sum_{p\in\mathcal{D}} P_\mu(p,\cdot) = 0$.*

(iii) *$\forall \mu$ avec $2 \leq |\mu| \leq 2k$, $\sum_{(p,q)\in\mathcal{D}^2} P_\mu(p,q) = 0$.*

Pour pouvoir appliquer effectivement ce critère, on doit savoir calculer explicitement les polynômes P_μ. Cela est fait dans [27]. Pour $m = 1$, les P_μ ne sont autres que les polynômes de Gegenbauer classiques [19].

On dispose également de critères d'une toute autre nature, relevant de la théorie des groupes. Le groupe orthogonal $O(n)$ agit sur l'espace SM_n des matrices symétriques $n \times n$ selon la formule $g.S = (g^t)^{-1}Sg^{-1}$, ce qui induit une représentation de $O(n)$ dans $\mathrm{Hom}_k(SM_n)$, espace des polynômes homogènes de degré k en la variable $S = (S_{i,j}) \in SM_n$

$$g.P(S) := P(g^{-1}.S) = P(g^tSg). \tag{2.6}$$

On a alors le théorème suivant :

Théorème 2.5.1 ([3]) *Soit G un sous-groupe fini de $O(n)$. Alors, les propriétés suivantes sont équivalentes :*

(i) *$\forall m \leq \frac{n}{2},\ \forall p \in \mathcal{G}_{m,n},\ G \cdot p$ est un $2k$-design.*

(ii) $\mathrm{Hom}_k(SM_n)^G = \mathrm{Hom}_k(SM_n)^{O(n)}$.

Ce théorème s'applique en particulier quand $G = \mathrm{Aut}L$ est le groupe des automorphismes d'un réseau L. Par exemple, si $L = \mathbb{D}_4, \mathbb{E}_6$ ou $\mathbb{E}_7$, le théorème (2.5.1) s'applique avec $k = 2$, si $L = \mathbb{E}_8$, il s'applique avec $k = 3$, et si $L = \Lambda_{24}$ (réseau de Leech), avec $k = 5$ (voir [3]).

2.6 Invariants de Rankin.

À côté du classique invariant d'Hermite γ ($= \gamma_1$ dans ce qui suit), Rankin [37] a défini une collection d'invariants γ_m, de la façon suivante : soit L un réseau dans $\mathbb{R}^n$, muni du produit scalaire usuel, noté $x \cdot y$, et $1 \leq m \leq \dim L$ un entier. On définit

$$\delta_m(L) = \inf_{p\in L(m)} \det p, \tag{2.7}$$

où $L(m)$ désigne l'ensemble des sous-réseaux de dimension m de L, et

$$\gamma_m(L) = \delta_m(L)/(\det L)^{\frac{m}{n}} \tag{2.8}$$

Pour $m = 1$, $\gamma_1(L)$ est l'invariant d'Hermite de L. De manière générale, la fonction γ_m est bornée sur l'ensemble des réseaux de dimension n ([37]), et sa borne supérieure, qui se trouve être un maximum, est notée $\gamma_{m,n}$. Les réseaux réalisant un maximum local pour γ_m sont dits m-extrêmes (voir [13] pour une caractérisation de ces réseaux m-extrêmes en termes de m-perfection et m-eutaxie).

On définit l'ensemble (fini) des m-sections minimales de L comme

$$\mathcal{S}_m(L) = \{p \in L(m) \mid \det p = \delta_m(L)\}. \tag{2.9}$$

L'application $p \mapsto \mathbb{R}p$ (le sous-espace engendré par p) induit une injection de $\mathcal{S}_m(L)$ dans $\mathcal{G}_{m,n}$ (parce que $\mathbb{R}p/p$ est sans torsion, de par la minimalité de p). Ainsi, on peut voir $\mathcal{S}_m(L)$ comme un sous-ensemble de $\mathcal{G}_{m,n}$. On a alors le théorème suivant, analogue au théorème de Venkov mentionné plus haut :

Théorème 2.6.1 ([3]) *Si $\mathcal{S}_m(L)$ est un 4-design, alors L est m-extrême.*

La preuve repose sur la caractérisation évoquée ci-dessus des réseaux m-extrêmes en termes de m-perfection et m-eutaxie. Ce théorème, joint au théorème 2.5.1, permet de vérifier que certains réseaux "classiques" sont extrêmes relativement à *tous* les invariants de Rankin :

Proposition 2.6.1 *Si $L = \mathbb{D}_4, \mathbb{E}_6, \mathbb{E}_7, \mathbb{E}_8$ ou Λ_{24}, alors L est m-extrême pour tout m, $1 \leq m \leq \frac{\dim L}{2}$.*

Ce qui fait tout l'intérêt de cette proposition est que ce genre de résultat serait hors de portée sans les théorèmes 2.5.1 et 2.6.1.

2.7 Codes dans les variétés grassmanniennes. Bornes.

Definition 2.7.1 ([2]) *Soit $f(Y_1, \cdots, Y_m)$ polynôme symétrique, normalisé par la condition*

$$f(1, \cdots, 1) = 1.$$

Un sous-ensemble $\mathcal{D} \subset \mathcal{G}_{m,n}$ est un f-code si pour tout (p, q) dans $\mathcal{D}^2$, $p \neq q$ on a

$$f(y_1(p, q), \cdots, y_m(p, q)) = 0.$$

REMARQUE. Pour $m = 1$, on retrouve bien sûr la définition usuelle d'un s-code sur la sphère mentionnée précédemment.

Soit $d_k^+ = \dim H_k^+$ et $d_k^- = \dim H_k^-$. Ces dimensions peuvent être calculées facilement à partir des dimensions d_n^μ des composantes irréductibles $H_{m,n}^\mu$, que l'on trouve par exemple dans [22], chapitre 24. Elles interviennent dans les deux théorèmes suivants, qui donnent des bornes pour la taille d'un design et d'un code dans $\mathcal{G}_{m,n}$.

Théorème 2.7.1 ([2]) *Soit $\mathcal{D} \subset \mathcal{G}_{m,n}$ un $2k$-design. Alors*

$$|\mathcal{D}| \geq \max(d_k^+, d_k^-).$$

De plus, si cette borne est atteinte, alors $\mathcal{D}$ est un f-code relativement à

$$f = \frac{1}{d_k^+} \sum_{\substack{|\mu| \leq k \\ \mu \text{ paire}}} d_\mu p_\mu \quad \textit{ou} \quad \frac{y_1 \cdots y_m}{d_k^-} \sum_{\substack{|\mu| \leq k \\ \mu \text{ impaire}}} d_\mu p_\mu$$
$$(d_k^+ > d_k^-) \qquad (d_k^- > d_k^+)$$

Definition 2.7.2 ([2]) *Un f-code est de type 1 si $Y_1 \cdots Y_m$ divise f, de type 0 sinon.*

Théorème 2.7.2 ([2]) *Tout f-code $\mathcal{D} \subset \mathcal{G}_{m,n}$ satisfait*

$$|\mathcal{D}| \leq d_k^+,$$

où $k = 2 \deg f$. Si de plus f est de type 1, alors $\mathcal{D} \subset \mathcal{G}_{m,n}$ vérifie

$$|\mathcal{D}| \leq d_k^-,$$

où $k = 2 \deg f - m$.

Qui plus est, si cette borne est atteinte, alors

$$f = \frac{1}{d_k^+} \sum_{\substack{|\mu| \leq k \\ \mu \text{ paire}}} d_\mu p_\mu \textit{ (type 0)},$$

resp.

$$f = \frac{y_1 \cdots y_m}{d_k^-} \sum_{\substack{|\mu| \leq k \\ \mu \text{ impaire}}} d_\mu p_\mu \textit{ (type 1)}$$

et $\mathcal{D}$ est un $2k$-design.

Les designs, resp. les codes, réalisant la borne du théorème 2.7.1, resp. 2.7.2, quand ils existent, sont appelés *tight*-designs (“designs serrés”).

EXEMPLE. Dans [10], §5, une famille infinie $\mathcal{D}_p$ d’empilements dans $\mathcal{G}_{\frac{p-1}{2},p}$ est définie, où p est un nombre premier soit égal à 3 soit congru à -1 modulo 8. Chacun de ces empilement est constitué de $\frac{p(p+1)}{2} = d_{[0,\cdots,0]} + d_{[2,0,\cdots,0]} = d_2^+$ sous-espaces ayant deux à deux même *distance chordale* $d^2 = \frac{(p+1)^2}{4(p+2)}$. Comme $d^2 = \sum \sin^2 \theta_i = \frac{p-1}{2} - \sum y_i$, $\mathcal{D}_p$ est un f-code, avec $f = \frac{4(p+2)(\sum Y_i) - (p^2-5)}{p^2-5}$, et le théorème 2.7.2 s’applique, de sorte que :

Proposition 2.7.1 ([2]) *Pour tout nombre premier soit égal à 3 soit congru à -1 modulo 8, $\mathcal{D}_p$ est un tight 4-design dans $\mathcal{G}_{\frac{p-1}{2},p}$.*

2.8 Perspectives.

La recherche d'autres exemples de "tight"-designs est une question largement ouverte. Néanmoins, les bornes mentionnées au paragraphe précédent sont vraisemblablement très loin d'être optimales en général, ce qui limite les possibilités d'existence de tels exemples. Un prolongement naturel de nos travaux serait donc de s'efforcer d'affiner ces bornes, quand cela est possible.

Une autre suite à donner à ces travaux, serait de dégager une notion de *perfection forte* dans d'autres situations, par exemple, relativement aux invariants d'Hermite généralisés de Watanabe, et d'obtenir des résultats du type de 2.1.1, 2.6.1.

Chapitre 3

Produit tensoriel et puissances extérieures de réseaux.

Nous présentons brièvement dans cette dernière partie les résultats contenus dans [14] et [15]. On s'est efforcé, dans ces deux articles, d'étudier, un tant soit peu systématiquement, la question des vecteurs minimaux d'un produit tensoriel de réseaux et du carré extérieur d'un réseau.

3.1 Produit tensoriel.

Les propriétés des réseaux euclidiens relativement au produit tensoriel ont été étudiées dans une série d'articles de Kitaoka (voir notamment [29] ainsi que le chapitre 7 de [28]). Une question assez naturelle étudiée, entre autres, par Kitaoka, est la détermination des vecteurs minimaux du produit tensoriel $L \otimes M$ de deux réseaux euclidiens L et M. Il démontre par exemple que jusqu'en dimension 43, ces vecteurs minimaux sont *scindés*, comme on peut s'y attendre, c'est-à-dire de la forme $l \otimes m$ où l et m sont des vecteurs minimaux de L et M respectivement.

Dans [15], on étudie l'analogue de ce problème pour le produit tensoriel de réseaux *hermitiens* sur l'anneau des entiers d'un corps quadratique imaginaire, ou sur un ordre maximal d'un corps de quaternions. La principale motivation pour ce travail est l'étude des réseaux *modulaires*, selon la définition de Quebbemann ([Q]), c'est-à-dire les réseaux pairs semblables à leur dual. C. Bachoc et G. Nebe ont montré ([9]) comment le produit tensoriel sur l'anneau des entiers d'un corps quadratique imaginaire peut-être utilisé pour passer d'un *niveau* de modularité à un autre (par définition, le *niveau* d'un réseau modulaire L est le carré du rapport de similitude appliquant L^* sur L). Elles utilisent cette idée pour construire un réseau unimodulaire *extrêmal*[1] en dimension 80 à partir d'un réseau 7-modulaire extrêmal en dimension 20. On voit donc l'intérêt qu'il

[1] L'aspect le plus important de la théorie de Quebbemann est le fait que la série theta de ces réseaux modulaires est soumise à des contraintes très fortes, qui, font que leur minimum ne peut pas dépasser une certaine borne, explicite. Quand cette borne est atteinte, on dit que le réseau est *extrêmal* (à ne pas confondre avec la notion de réseau extrême mentionnée précédemment).

peut y avoir à connaître *a priori* le comportement des vecteurs minimaux sous l'effet du produit tensoriel : il est en effet hors de question, du moins avec les moyens de calcul actuels, de déterminer numériquement la norme minimale d'un réseau en dimension 80 ! L'un des buts de l'article [15] est de donner une preuve sensiblement plus simple du résultat de Bachoc et Nebe.

3.2 Puissances extérieures.

Dans [14], ont étudie les vecteurs minimaux du carré extérieur d'un réseau. La motivation première pour l'étude de cette question est liée à l'étude, évoquée au chapitre précedent, des invariants de Rankin dans [13]. Les puissances extérieures $\bigwedge^m E$ d'un espace euclidien E de dimension n héritent d'une structure euclidienne canonique induite par le produit scalaire original E, qui est définie pour les vecteurs *scindés* , c'est-à-dire, les vecteurs de la forme $x_1 \wedge \cdots \wedge x_m$) par :

$$(x_1 \wedge \cdots \wedge x_m) \cdot (y_1 \wedge \cdots \wedge y_m) := \det(x_i \cdot y_j)_{1 \leq i,j \leq m} \ .$$

Ainsi, la *norme* (c'est-à-dire le carré de la longueur) d'un vecteur scindé $x_1 \wedge \cdots \wedge x_m$ relativement à ce produit scalaire coïncide avec le déterminant du sous-réseau engendré par $x_1, \cdots, x_m$. Par conséquent, une question naturelle, est de se demander si la norme minimale usuelle de $\bigwedge^m L$, vu comme réseau dans $\bigwedge^m E$, est atteinte sur les vecteurs *scindés* , ou, de façon équivalente, si $\delta_m(L) = \mathrm{N}(\bigwedge^m L)$.

On donne dans[14] une réponse partielle à cette question, dans le cas du *carré extérieur* ($m = 2$), à l'aide d'arguments similaires à ceux de Kitaoka pour le cas du produit tensoriel. En particulier, on montre qu'en petite dimension, la réponse à la question initiale est toujours positive. Mais on donne également des contre-exemples explicites en dimension 24 et 48, et on montre qu'asymptotiquement, la réponse est en général négative (pour tout m).

Bibliographie

[1] A. Ash et M. McConnell, *Cohomology at infinity and the well-rounded retract for general linear groups*, Duke Math. J. **90** (1997), no. 3, 549–576.

[2] C. Bachoc, E. Bannai et R. Coulangeon, *Codes and designs in Grassmannian spaces*, Discrete Mathematics **277** (2004), 15–28.

[3] C. Bachoc, R. Coulangeon et G. Nebe, *Designs in Grassmannian spaces and lattices*, J. Algebraic Combin.

[4] R. Baeza, R. Coulangeon, M.I. Icaza et M. O'Ryan (2001), *Hermite's constant for quadratic number fields*, Experimental Mathematics **10**, no. 4, 543–551.

[5] C. Bavard (1997), *Systole et invariant d'Hermite.* J. Reine Angew. Math., **482**, 93–120.

[6] A.-M.Bergé et J. Martinet, *Densité dans des familles de réseaux. Application aux réseaux isoduaux*, Enseign. Math. (2), **41**, (1995), No. 3-4, 335– 365.

[7] A.-M.Bergé et J. Martinet, *Réseaux extrêmes pour un groupe d'automorphismes*, Journées Arithmétiques, 1989 (Luminy, 1989), Astérisque, No. 198-200 (1991), 41– 66 (1992).

[8] A.-M. Bergé, J. Martinet et F. Sigrist, *Une généralisation de l'algorithme de Voronoĭpour les formes quadratiques.* Journées Arithmétiques, 1991 (Genève). Astérisque No. 209 (1992) **12**, 137–158.

[9] C. Bachoc et G. Nebe, *Extremal lattices of minimum* 8 *related to the Mathieu group* M_{22}, J. Reine Angew. Math. **494** (1998),155–171.

[10] A. R. Calderbank, R. H. Hardin, E. M. Rains, P. W. Shor et N. J. A. Sloane, *A group-theoretic framework for the construction of packings in Grassmannian spaces*, J. Algebraic Combin. **9** (1999), no. 2, 129–140.

[11] H. Cohn (1965), *A numerical survey of the floors of various Hilbert fundamental domains*, Math. Comp., **19**, 594-605.

[12] J. H. Conway, R. H. Hardin et N. J. A. Sloane, *Packing Lines, Planes, etc., Packings in Grassmannian Spaces*, Experimental Mathematics, Vol. 5 (1996), 139-159.

[13] R. Coulangeon, (1996) *Réseaux k-extrêmes.*, Proc. London Math. Soc. (3), **73** , no. 3, 555–574.

[14] R. Coulangeon, *Minimal vectors in the second exterior power of a lattice*, J. Algebra **194** (1997), no. 2, 467-476.

[15] R. Coulangeon, *Tensor products of Hermitian lattices*, Acta Arithmetica **92** (2000), 115-130.

[16] R. Coulangeon (2001), *Voronoï theory over algebraic number fields*, Monographies de l'Enseignement Mathématique, **no 37**, 147-162.

[17] J. H. Conway et N. J. A. Sloane, *Sphere packings, lattices and groups*, Third edition. With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], **290**. Springer-Verlag, New York, 1999.

[18] R. Coulangeon et T. Watanabe, *Hermite constant and Voronoï theory over a quaternion skew field*, soumis.

[19] Ph. Delsarte, J.M. Goethals et J.J. Seidel, *Spherical codes and designs*, Geom. Dedicata (6) (1977), 363-388.

[20] N. D. Elkies, *Lattices, linear codes, and invariants. I*, Notices Amer. Math. Soc. **47** (2000), no. 10, 1238–1245.

[21] P. Elbaz-Vincent, H. Gangl, C. Soulé, *Quelques calculs de la cohomologie de* $\mathrm{GL}_N(\mathbb{Z})$ *et de la* K*-théorie de* $\mathbb{Z}$, C. R. Math. Acad. Sci. Paris **335** (2002), no. 4, 321–324.

[22] W. Fulton et J. Harris, *Representation Theory, a first course*, GTM 129 Springer 1991

[23] R. Goodman et N. R. Wallach, *Representations and invariants of the classical groups*, Encyclopedia of Mathematics and its Applications 68, Cambridge University Press, 1998.

[24] P. Humbert (1940), *Théorie de la réduction des formes quadratiques définies positives dans un corps algébrique K fini*, Comment. Math. Helv., **12**, 263–306.

[25] P. Humbert (1949), *Réduction de formes quadratiques dans un corps algébrique fini*, Comment. Math. Helv., **23**, 50–63.

[26] M.I. Icaza (1997), *Hermite constant and extreme forms for algebraic number fields*, J. London Math. Soc. (2), **55**, (1997), 11–22.

[27] A.T. James et A.G. Constantine, *Generalized Jacobi polynomials as spherical functions of the Grassmann manifold*, Proc. London Math. Soc. (3) **29** (1974), 174-192.

[28] Y. Kitaoka, *Arithmetic of quadratic forms*, Cambridge University Tracts (1993).

[29] Y. Kitaoka, *Scalar extension of quadratic lattices II*, Nagoya Math. J. **67** (1977), 159–164

[30] M. Koecher, *Beiträge zu einer Reduktionstheorie in Positivitätsbereichen. I.* Math. Ann. **141** (1960) 384–432.

[31] A. Korkine et G. Zolotareff, *Sur les formes quadratiques*, Math. Ann, **6** (1873), 366–389.

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

[33] M. Masanori et T. Watanabe, *Adèle geometry of numbers*, Class field theory—its centenary and prospect (Tokyo, 1998), Math. Soc. Japan, Tokyo (2001), 509–536.

[34] H. E. Ong, *Perfect quadratic forms over real-quadratic number fields*, Geom. Dedicata **20** (1986), no. 1, 51–77.

[35] M. Pohst et M. Wagner, *On the computation of hermite-Humbert constants for real quadratic number fields*, prépublication.

[36] H.-G. Quebbemann, *Modular Lattices in Euclidean Spaces*, J. Number Theory **54** (1995), 190–202.

[37] R. A. Rankin, *On positive definite quadratic forms*, J. London Math. Soc., **28** (1953), 309–314.

[38] K. Rogers et H. P. F. Swinnerton-Dyer, *The geometry of numbers over algebraic number fields*, Trans. Amer. Math. Soc., **88** (1958), 227–242

[39] J. L. Thunder, *Higher-dimensional analogs of Hermite's constant*, Michigan Math. J., **45** (1998), no. 2, 301–314.

[40] J.D. Vaaler, *The best constant in Siegel's lemma*, Monatsh. Math. **140** (2003), no. 1, 71–89.

[41] G. Voronoï, *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.

[42] T. Watanabe, *On an analog of Hermite's constant.*, J. Lie Theory, **10** (2000), no. 1, 33–52.

[43] H. Weyl, *Theory of reduction for arithmetical equivalence. II*, Trans. Amer. Math. Soc. **51**, (1942). 203–231.