HAL open science

Constantes d'Hermite et théorie de Voronoï

Bertrand Meyer

To cite this version:

Bertrand Meyer. Constantes d'Hermite et théorie de Voronoï. Mathématiques [math]. Université Sciences et Technologies - Bordeaux I, 2008. Français. NNT : . tel-00346870

HAL Id: tel-00346870

https://theses.hal.science/tel-00346870v1

Submitted on 12 Dec 2008

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

N° d'ordre : 3676

THÈSE

présentée à

L'UNIVERSITÉ BORDEAUX 1

Ecole doctorale de mathématiques et d'informatique

par M. Bertrand Fabien Meyer

pour obtenir le grade de

DOCTEUR

Spécialité : Mathématiques pures

Constantes d'Hermite et théorie de Voronoï

Soutenue publiquement le 28 novembre 2008,

Après avis de

MM.	Bannai Eiichi, professeur, université de Kyushu, Fukuoka,	Rapporteur
	Vaaler Jeffrey, professeur, université du Texas, Austin,	Rapporteur

Devant la commission d'examen formée de

Mme	Bachoc Christine, professeur, université de Bordeaux 1, Talence,	Rapporteur
MM.	Bavard Christophe, professeur, université de Bordeaux 1, Talence,	Examinateur
	Coulangeon Renaud, maître de conférences, université de Bordeaux 1, Talence,	Directeur
Mme	Nebe Gabriele, professeur, école polytechnique de Rhénanie–Westphalie, Aix-La-Chapelle,	Examinatrice
MM.	Lachaud Gilles, directeur de recherches, centre national de la recherche scientifique, Marseille	Président
	Watanabe Takao, professeur, université d'Osaka, Toyonaka,	Co-directeur.

Institut de mathématiques de Bordeaux – U.M.R. 5251
Université Bordeaux 1
351, cours de la Libération - F 33405 Talence cedex

A ceux qui m'ont fait grandir.

Car, dès ma prime jeunesse et jusques à présent, embrasé sans mesure d'une très haute et noble amour, qui semblerait peut-être, à la conter moi-même, beaucoup plus élevé qu'il n'appartient à ma basse condition, encore qu'elle ne m'ait valu, auprès des gens sages qui en eurent connaissance, que des louanges et un surcroît de considération, à très grand-peine néanmoins j'endurai cette amour, non certes du fait d'une quelconque cruauté de la dame aimée, mais à cause plutôt du feu immodéré conçu en mon esprit par un appétit peu réglé ; et ce feu, parce qu'il ne me permettait pas de me donner contentement dans les limites de la convenance, me causait trop souvent un ennui plus profond qu'il m'était besoin. — Boccace, « Le Décaméron », proême.

Remerciements

À l'orée de cette thèse, je souhaiterais exprimer toute ma gratitude à Renaud Coulangeon, le cicerone de mes premiers pas dans les mathématiques des grands. En limier perspicace, il a su me faire emprunter des pistes fertiles et me guider avec justesse sans jamais ne rien retrancher à ma liberté d'explorer les chemins par mes propres et faibles moyens. Je souhaiterais également remercier Takao Watanabe, qui m'a accueilli avec empressement et attention durant un semestre à Osaka, auprès de qui j'ai eu l'occasion de valider et de consolider mes travaux et mes connaissances[1].

Je remercie les rapporteurs Eiichi Bannaï et Jeffrey Vaaler pour leur concours et leurs encouragements ; ils ont effectué avec zêle une tâche d'autant moins facile que le manuscrit n'était pas écrit dans leur langue. Cette thèse a été relue également par de nombreuses personnes[2], certaines étrangères à ses mathématiques ; je recueille avec estime leurs commentaires, leurs conseils et leurs leçons de grammaire.

Gabriele Nebe et Gilles Lachaud ont pris le temps de se déplacer jusqu'à Bordeaux, rejoints sur place par Christine Bachoc et Christophe Bavard, pour compléter mon jury. Je me vois très honoré de leur présence et leur sait gré de l'intérêt porté à mon travail ainsi que de leurs recommandations pour les extensions à venir.

J'ai bénéficié pour mon plus grand profit de la proximité avec un groupe de mathématiciens nourri et dynamique constitué autour du noyeau « codes et réseaux » et plus largement des équipes de théorie des nombres et de combinatoire. J'ai aussi eu maintes occasions de rencontrer la communauté des codes, réseaux, formes quadratiques, empilements de sphères et théorie des nombres, tant à Bordeaux qu'à l'extérieur, ce qui a grandement stimulé mon activité et a façonné ma compréhension de ce sujet. Qu'ils trouvent ici l'expression de ma gratitude.

Parmi les témoins de cette thèse en gésine, je souhaiterai encore remercier tout particulièrement les jeunes chercheurs de mon couloir et de notre institut de mathématiques dont la compagnie a cultivé un chaleureux esprit de travail, toujours enthousiasmant et motivant. J'ai également été reçu avec prévenance

[1] Ce voyage n'aurait pas été possible sans l'appui du collège doctoral franco-japonais.

[2] Je pense en particulier à Etienne Bernard, Jean Creignou ou Jean-Tarcise Meyer.

par mes collègues à Osaka, je mesure tout le confort et toutes les découvertes que j'ai pu vivre grâce à eux au Japon.

Le travail à l'institut de mathématiques a été allégé par une qualité des équipements remarquable et surtout grâce à la diligence des équipes du personnel de la bibliothèque, du secrétariat et de la cellule informatique.

Cette thèse a été très abondante en rencontres au travers d'activités associatives et para-universitaires ; je voudrais remercier toutes les personnes croisées sur ce chemin pour la richesse et l'équilibre qu'elles m'ont apportées.

Plus lointainement, je ne peux qu'avoir une pensée reconnaissante envers la totalité de mes maîtres, enseignants et professeurs qui ont formé la personne que je suis aujourd'hui.

Mes parents, mon frère, ma famille et mes amis comptent beaucoup pour moi et m'ont toujours témoigné avec compréhension l'amour et le soutien qui m'a permis de m'épanouir. Grand merci à eux.

Qu'ils partagent la fierté que j'emporte en ce moment.

Bordeaux, le 30 novembre 2008.

Préface

Si l'art de garnir l'espace à peu de perte fut depuis longtemps la quête des décorateurs de palais fastueux et la distraction de princes esthètes à la poursuite de motifs délassants, il fallut attendre la seconde moitié du dix-neuvième siècle pour que la vision de disques proprement ordonnés fît florès en mathématiques et inspirât aux théoriciens des nombres des idées des plus fécondes. Ainsi naquit du génie de Minkowski et de ses pairs la géométrie des nombres ou *Geometrie der Zahlen* qui consista à dire dans le langage de l'espace ce qui jusque-là résistait à l'aridité de lignes de calculs. Pour simple que fût l'idée, elle ne pénétrait pas moins de façon lumineuse et inédite des objets que l'esprit humain sondait alors avec obstination sans succès et partant ouvrait un champ d'exploration nouveau qui fut soigneusement cultivé pendant le demi-siècle qui suivit. En effet, quoi de plus enfantin que de vouloir quarrer la proportion de terrain que se dispute une troupe de boules en rang qui s'entrechoquent mais ne se mordent pas, trop rondes pour pouvoir s'ajuster ? On convoqua Hermite pour arbitrer la bataille — après tout, il fut le premier à l'avoir provoquée — et on appela en son honneur la constante entrée de la sorte en faveur auprès des spécialistes. Devenu de conserve sujet de recherches autonome, un nouvel objet d'étude était né et ne se lasserait plus de connaître des développements et de trouver des ramifications et des liens avec d'autres questions comme nous allons le raconter dans notre *premier chapitre*.

Dans les traces et les sillons d'une longue cohorte de mathématiciens, cette thèse s'efforce à caractériser et à toucher de près une forme généralisée de la constante, introduite par T. Watanabe, qui mêle ingrédients issus de la théorie des nombres – juste retour aux origines –, adèles et théorie des représentations des groupes classiques. Pour nous autoriser à formuler nos résultats d'un ton aussi clair et assuré que possible, nous reprenons tout d'abord au *chapitre deux*, dans un traitement autonome écrit selon notre guise, les définitions, lemmes et théorèmes des objets mathématiques que les années ont charriés jusqu'à nous et que nous utilisons dans ce qui suivra sans autre forme de procès. Après avoir fixé quelques conventions, nous présentons notamment les représentations du groupe linéaire et les hauteurs de la variété drapeau.

Cette thèse ne serait rien si le spectre indulgent d'un prestidigitateur des formes quadratiques n'avait accompagné de sa bienveillante paternité sa patiente élaboration. Malheureusement souvent connue uniquement pour ses diagrammes qui partagent l'espace en zones d'influences, l'œuvre de G. Voronoï, qui renforça et acheva les travaux de ses prédécesseurs A. Korkine et I. Zolotareff, inspire

et dirige le contenu du *chapitre trois*, où une généralisation des deux qualités — eutaxie et perfection — qui caractérisent les formes extrêmes est détaillée. Précisément, nous exposons comment la constante d'Hermite généralisée a été définie initialement, nous en avançons une formulation équivalente en terme de formes de Humbert et nous établissons une théorie de la caractérisation des extrêmes semblable à celle de G. Voronoï en nous appuyant sur les travaux de Ch. Bavard. Il en découle notamment la finitude du cardinal des classes de formes parfaites et l'algébricité de la constante.

Le *chapitre quatre* est consacrée à la description des relations qui peuvent être démontrées à l'image des inégalités déjà connues (celles de dualité, de Mordell, ou de Bergé–Martinet) et des inégalités ou majorations que l'on peut obtenir à partir de résultats de la littérature (réinterprétation de la réduction de Korkine et Zolotareff, recours aux minima successifs, exploitation du changement de corps de base). Des valeurs explicites de ces constantes sont occasionnellement obtenues par l'exploitation des inégalités et le truchement de méthodes variées.

Si le sujet recèle de connexions inattendues, c'est aussi parce que de collections finies de points — les designs — dont la moyenne fournit une quadrature particulièrement précise, on peut tirer des configurations spécialement avantageuses, comme l'a mis au jour B. Venkov. Ainsi que l'ont démontré Ch. Bachoc, R. Coulangeon et G. Nebe dans un cas intermédiaire étayé par des considérations de théorie des groupes, nous introduisons au *chapitre cinq* une nouvelle notion de design qui concourt à caractériser certaines configurations spéciales dans le cas général. À cet égard, nous passons en revue les fonctions zonales de la variété drapeau et nous définissons les réseaux fortement parfaits relativement à notre cadre : ces derniers sont systématiquement extrêmes. Ce critère nous permet de qualifier de nombreux exemples.

Nous consacrons les annexes à la détermination des valeurs de la constante d'Hermite. Le *chapitre premier* présente une recension des diverses sources dans lesquelles des constantes d'Hermite ont été calculées à ce jour.

La part la plus spectaculaire et fascinante des résultats de G. Voronoï est non seulement la mise à jour de la caractérisation des formes extrêmes par les propriétés de perfection et d'eutaxie mais surtout l'exhibition d'un algorithme parfaitement limpide et au fonctionnement principalement linéaire qui détermine la configuration optimale d'une dimension donnée. Nous rappelons au *chapitre second* comment le principe de cet algorithme a été étendu par M. Koecher au cas des corps quadratiques imaginaires et donnons quelques résultats de son exécution en dimension trois.

Table des matières

Remerciements **v**

Préface **vii**

1 Prodromes **1**
1.1 Les constantes d'Hermite 1
1.1.1 La constante classique 1
1.1.2 Généralisations de la constante *sui generis* 2
1.1.3 Approximation diophantienne 3
1.2 La théorie et l'algorithme de Voronoï 5
1.2.1 Caractérisation des formes extrêmes 5
1.2.2 Interprétation 7
1.3 Les designs 8
1.3.1 Les designs sphériques 8
1.3.2 Les designs grassmanniens 8

2 Notations, structures et objets mis en jeu **11**
2.1 Conventions 11
2.1.1 Objets combinatoires 11
2.1.2 Algèbre linéaire et affidés 15
2.1.3 Théorie algébrique des nombres 19
2.1.4 Les adèles 22
2.2 Les représentations des groupes linéaire et orthogonal 23
2.2.1 Considérations générales 23
2.2.2 Le module de Schur par les tableaux 25
2.2.3 Les plongements projectifs de la variété drapeau 27
2.2.4 Le module de Schur par les polynômes 28
2.2.5 Décomposition de l'espace des polynômes 28
2.2.6 Représentations du groupe orthogonal 29
2.3 Hauteurs et géométrie arithmétique 30
2.3.1 La hauteur de Weil 30
2.3.2 La hauteur d'Arakelov 33

3 Théorie de Voronoï **37**
3.1 La constante d'Hermite généralisée 37
3.2 La constante d'Hermite des formes de Hermite–Humbert 38
3.2.1 Formes de Hermite–Humbert 38
3.2.2 Équivalence des constantes généralisées et de Humbert . . 40
3.3 Eutaxie et perfection 41
3.3.1 Reformulation géométrique 42
3.3.2 Un théorème à la Voronoï 45
3.3.3 Algébricité de la constante 46

4 Inégalités et calculs exacts **49**
4.1 Relations entre les constantes 49
4.1.1 Une égalité de dualité 49
4.1.2 L'inégalité de Mordell 50
4.1.3 Des inégalités avec la constante de Bergé–Martinet 51
4.2 Calculs exacts et approximations 55
4.2.1 Détermination de quelques constantes sur $\mathbb{Q}$ 55
4.2.2 Majoration par les minima successifs 59
4.2.3 Majoration par changement de corps de base 60
4.2.4 Trace dyadique et exploitation des inégalités de Bergé–Martinet 65

5 Réseaux extrêmes et designs vexillaires **71**
5.1 Fonctions de la variété drapeau et designs 71
5.1.1 Fonctions de carré intégrable sur la variété drapeau . . . 71
5.1.2 Fonctions zonales 73
5.1.3 Définition des designs vexillaires 75
5.2 Réseaux fortement parfaits 78
5.3 Calculs 80

A Table des valeurs connues **83**
A.1 Sur le corps des rationnels 83
A.1.1 Constante d'Hermite traditionnelle 83
A.1.2 Meilleurs invariants connus 83
A.2 Formes binaires sur les corps de nombres 84
A.2.1 Quelques corps quadratiques imaginaires principaux . . . 84
A.2.2 Quelques corps quadratiques réels 86
A.2.3 Un corps cubique 86

B Algorithme de Voronoï des corps quadratiques imaginaires **87**
B.1 L'algorithme de Voronoï d'après Kœcher 87
B.1.1 Présentation 87
B.1.2 L'équivalence arithmétique dans les corps imaginaires . . 89
B.1.3 Implémentation 91
B.2 Résultats en dimension 3 93
B.2.1 Énumération des formes parfaites ternaires de $\mathbb{Q}[\sqrt{-1}]$ . . 93
B.2.2 Énumération des formes parfaites ternaires de $\mathbb{Q}[\sqrt{-2}]$ . . 94
B.2.3 Énumération des formes parfaites ternaires de $\mathbb{Q}[\sqrt{-3}]$ . . 95
B.2.4 Énumération des formes parfaites ternaires de $\mathbb{Q}[\sqrt{-7}]$ . . 96
B.2.5 Énumération des formes parfaites ternaires de $\mathbb{Q}[\sqrt{-11}]$. 97

Table des figures **101**

Liste des tableaux **101**

Index **103**

Bibliographie **107**

Prodromes 1

Nous entamons cette thèse par un panorama sur le sujet, bien que certaines définitions et notations employées ne soient introduites qu'au chapitre suivant, en espérant que ce qu'elle perd en rigueur dans la progression de l'exposition gagne en vivacité et en intérêt.

1.1 Les constantes d'Hermite

1.1.1 La constante classique

On appelle classiquement *constante d'Hermite* la quantité

$$\gamma_n = \max_{L} \min_{x \in L \smallsetminus \{0\}} \|x\| = \max_{A} \min_{x \in \mathbb{Z}^n \smallsetminus \{0\}} A[x]. \tag{1.1}$$

où L parcourt l'ensemble des réseaux euclidiens unimodulaires[1] d'une dimension n donnée et A l'ensemble des formes quadratiques définies positives de déterminant 1 et de dimension n. En notant δ_n la densité optimale d'un empilement de boules régulier dans $\mathbb{R}^n$ (voir figure 1.1), on peut relier γ_n et δ_n par

$$\delta_n = {\gamma_n}^{n/2} \frac{\omega_n}{2^n}, \tag{1.2}$$

où ω_n représente le volume de la boule unité, c'est-à-dire $\omega_n = \pi^{n/2}/\Gamma(1+n/2)$. En exprimant qu'une densité n'excède jamais 1, on dispose alors de la majoration $\gamma_n \leqslant 4\,{\omega_n}^{-2/n}$, ce qui, combiné avec un argument de compacité de Mahler, justifie très facilement l'existence de la constante γ_n.

Du point de vue des formes quadratiques, Ch. Hermite a été le premier à établir l'existence de la constante en prouvant que pour tout entier n supérieur à 2, la constante vérifie $\gamma_{n+1} \leqslant {\gamma_n}^{\frac{n-1}{n-2}}$, ce qui l'a conduit, par récurrence, à prouver que le minimum était borné par la quantité $\left(2/\sqrt{3}\right)^{n-1}$, mais le travail de majoration est demeuré beaucoup plus ardu, tant que H. Minkowski ne s'est pas rendu compte qu'estimer le minimum de formes quadratiques sur un réseau donné revenait à estimer le minimum de réseaux pour une forme quadratique donnée.

H. Minkowski [MH67] l'a conjecturé également et E. Hlawka [Hla43] a prouvé en utilisant un argument de moyenne que $\left(2\,\zeta(n)\,/\,\omega_n\right)^n \leqslant \gamma_n$. La borne de Minkowski alliée avec celle de Hlawka montre que la constante d'Hermite croît

[1] c'est-à-dire de déterminant 1

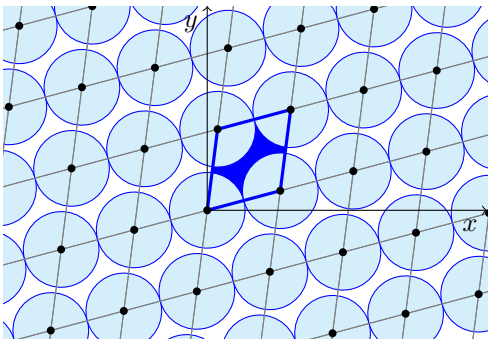


Fig. 1.1 – Empilement régulier de sphères quelconque en dimension 2

linéairement selon n. Diverses améliorations de ces bornes ont été obtenues ; on pourra consulter §19 de [GL87] pour un compte rendu plus détaillé. Par un résultat de Korkine et Zolotareff [KZ73], on sait également que ${\gamma_n}^n$ est rationnel.

Pour plus de détails sur les techniques et des résultats « historiques » obtenus dans ce domaine, on pourra lire la traduction [RB79] du russe vers l'anglais d'une très complète recension opérée par S. S. Ryshkov et E. P. Baranovski.

Les champs disciplinaires parmi lesquels des occurrences de la constante d'Hermite ont été identifiées sont nombreux. On peut citer, pêle-mêle, notamment des questions de *mathématiques des télécommunications*, de *physique*, de *chimie*, de *biologie*, de *conception d'antennes*, de *tomographie* (*cf.* chap. 1 §1.4 de [CS99]). La constante d'Hermite possède également des avatars dans d'autres champs mathématiques, notamment en géométrie riemannienne où elle est appelée *systole*. En général, la systole d'une variété riemannienne compacte est la longueur minimale d'une courbe non contractile, si bien que l'invariant d'Hermite d'un réseau n'est rien d'autre que le carré de la systole du tore obtenu par quotient de l'espace par le réseau.

1.1.2 Généralisations de la constante sui generis

La constante d'Hermite a été étendue en tant que telle dans deux directions avant que T. Watanabe ne propose une définition encore plus générale qui les unisse et dont nous reportons la présentation au chapitre trois.

La *constante de Rankin* [Ran53] consiste en le nombre

$$\gamma_{n,m} = \max_{L} \min_{\Lambda} \frac{\text{dét}\,\Lambda}{(\text{dét}\,L)^{m/n}}, \tag{1.3}$$

où L décrit toujours l'ensemble des réseaux euclidiens d'une dimension donnée n et Λ parcourt l'ensemble de ses sous-réseaux de dimension m. Par dualité, on peut vérifier que $\gamma_{n,m} = \gamma_{n,n-m}$. D'autre part, R. Rankin a prouvé que

$$\gamma_{n,d} \leqslant \gamma_{m,d}\, \gamma_{n,m}^{d/m}. \tag{1.4}$$

Nous reviendrons sur ces résultats au cours de cette thèse. L'algébricité de $\gamma_{n,m}$ a été prouvée par Ch. Bavard [Bav97].

La *constante de Hermite–Humbert* $\gamma_n(k)$ a été introduite par M. I. Icaza [Ica97] ; elle consiste à remplacer une forme quadratique par une forme de Humbert définie sur un certain corps de nombre k (*cf.* section 3.2 pour les détails concernant ces formes et la constante). Son algébricité a été établie dans [Cou01] par le recours à une théorie de Voronoï.

1.1.3 Approximation diophantienne

La constante d'Hermite se manifeste également dans des questions d'approximation diophantienne. Partant d'un espace vectoriel de dimension n défini sur un corps de nombre k et considérant des problèmes de majoration de hauteurs minimales sur l'espace des grassmanniennes $\mathscr{G}_{n,m}(k)$, c'est-à-dire des sous-espaces rationnels de dimension fixée m de k^n, J. L. Thunder a défini dans [Thu98] la constante d'Hermite $\gamma_{n,m}(k)$ comme la plus petite constante C telle que pour tout automorphisme adèlique A, il existe un espace V de $\mathscr{G}_{n,m}(k)$ dont la taille observe l'inégalité

$$H_A(V) \leqslant C^{1/2} \ |\text{dét}\, A|_{k_{\mathbb{A}}}^{m/n}. \tag{1.5}$$

Dans cette inégalité, $H_A(\cdot)$ représente une hauteur tordue par un automorphisme A du groupe linéaire adélique, ces termes feront l'objet d'une définition précise dans la partie 2.3.1.1. Lorsque le corps de nombre est le corps des rationnels, la constante coïncide avec celle de Rankin.

Théorème 1.1 (Thunder). — *Reprenant les résultats déjà attestés pour la constante d'Hermite classique ou la constante de Rankin, J. L. Thunder montre encore que*

1. *L'inégalité* $\gamma_{n,d}(k) \leqslant \gamma_{m,d}(k) \ (\gamma_{n,m}(k))^{d/m}$ *est vérifiée.*
2. *La constante peut être majorée par un théorème des minima successifs analogue à celui de Minkowski*

$$\gamma_{n,m}(k)^{\frac{1}{2m}} \leqslant \frac{2^r \ |D_k|^{1/2}}{\omega_n^{r_1/n}\, \omega_{2n}^{r_2/n}}. \tag{1.6}$$

   Les notations seront précisées au chapitre 2.

3. *La constante peut être minorée de façon analogue à la minoration de Hlawka :*

$$\frac{w_k\, n}{h_k R_k} \cdot \frac{\displaystyle\prod_{j=n-m+1}^{n} \frac{\zeta_k(j) \ |D_k|^{j/2}}{j^r\, 2^{jr_2}\, {\omega_j}^{r_1}\, {\omega_{2j}}^{r_2}}}{\displaystyle\prod_{l=2}^{d} \frac{\zeta_k(l) \ |D_k|^{l/2}}{l^r\, 2^{lr_2}\, {\omega_l}^{r_1}\, {\omega_{2l}}^{r_2}}} \leqslant \gamma_{n,d}(k)^{\frac{n}{2}}, \tag{1.7}$$

   en utilisant le discriminant D_k du corps de nombre k, son nombre de classe h_k, son régulateur R_k, le cardinal de ses racines de l'unité w_k et la fonction ζ_k de Dedekind.

4. *En conséquence, lorsque le corps k et l'entier m sont fixés,*

$$\log \gamma_{n,m}(k) = r\, m \, \log n + \mathcal{O}(1). \tag{1.8}$$

J. D. Vaaler s'est intéressé au sens que pouvait prendre cette constante et a montré dans l'article [Vaa03] que la constante ainsi définie satisfaisait d'une part que :

Théorème 1.2 (Vaaler). — *Étant donné un sous-espace rationnel V de dimension m, il en existe une base $(\eta_i)_{1\leqslant i\leqslant m}$ de vecteurs rangés par hauteur croissante dont la taille est contrôlée par*

$$\prod_{l=1}^{m} H(\eta_l) \leqslant \gamma_{n,1}(k)^{m/2} H(V). \tag{1.9}$$

— ce type de résultats est généralement appelé *lemme de Siegel* (*cf.* [BV83]) — et d'autre part que

Théorème 1.3 (Vaaler). — *Cette constante est optimale dans le sens où dans l'inégalité sous-jacente $H(\eta_1) \leqslant \gamma_{n,1}(k)^{1/2} H(V)$, la constante ne peut être remplacée par une constante plus petite.*

Exemple 1.4. — Dans le cas du plan, cette inégalité revient à dire que la constante d'Hermite fixe le plus petit volume garantissant la présence d'un point à coordonnées entières dans une ellipse quelconque dudit volume (*cf.* figure 1.2).

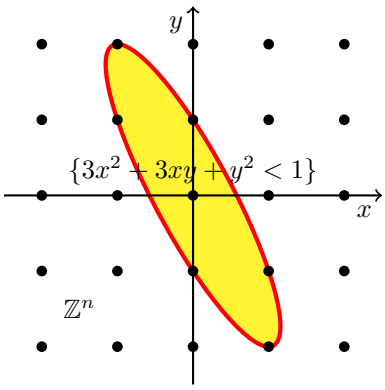


Fig. 1.2 – Illustration du lemme de Siegel

D'autre part, on peut observer que ces constantes générales conservent leur signification dans un contexte « relatif », autrement dit, lorsque l'on compare les hauteurs tordues d'un sous-espace emboîté dans un autre et non plus plongé dans l'espace ambiant. Cette constatation a été d'abord avisée par I. Aliev, A. Schinzel et W. M. Schmidt [ASS05] dans le cas des rationnels ($k = \mathbb{Q}$) puis par T. Watanabe [Wat06] dans le cas général. Nous donnons le résultat dans sa forme générale.

Théorème 1.5 (A., S. & S. sur $\mathbb{Q}$, puis W.). — *Supposons que des entiers $m < n < N$ sont donnés, on se place dans le grand espace k^N.*

1. *Pour tout automorphisme adélique A et tout sous-espace vectoriel rationnel $\mathscr{X}$ de dimension fixée n, il existe un sous-espace $\mathscr{Y}$ de dimension m*

contenu dans $\mathscr{X}$ tel que

$$H_A(\mathscr{Y}) \leqslant \gamma_{n,m}(k)^{1/2} H_A(\mathscr{X})^{m/n}. \tag{1.10}$$

De plus, cette constante est la meilleure possible dans le sens où elle ne peut pas être remplacée par une constante plus petite pour au moins un automorphisme A.

2. *Pour tout automorphisme adélique A et tout sous-espace vectoriel rationnel $\mathscr{X}'$ de dimension fixée $N-n$, il existe un sur-espace vectoriel $\mathscr{Y}'$ de dimension $N-m$ contenant $\mathscr{X}'$ tel que*

$$H_A(\mathscr{Y}') \leqslant \gamma_{n,m}(k)^{1/2} H_A(\mathscr{X})^{m/n}. \tag{1.11}$$

Ici encore, $\gamma_{n,m}(k)$ est la meilleure constante possible.

Dans le cas rationnel, Aliev *et al.* ont montré qu'en vérité la constante était même atteinte lorsque l'automorphisme A est l'identité. Cette question demeure cependant ouverte dans le cas général.

1.2 La théorie et l'algorithme de Voronoï

1.2.1 Caractérisation des formes extrêmes

La caractérisation des formes extrêmes a été entreprise par A. Korkine et I. Zolotareff, qui ont dégagé la notion de perfection, et a été achevée par G. Voronoï, qui, en introduisant la notion d'eutaxie ou de « bonne disposition » selon l'étymologie du terme, a énoncé et prouvé le théorème de caractérisation des formes extrêmes ci-dessous [Vor08]. La notion de perfection seule est insuffisante à caractériser l'extrêmalité d'une forme.

Définition 1.6. — On dit qu'une forme A est *parfaite* si les projections $p_u = uu'$ associées à ses vecteurs minimaux u engendrent l'espace des endomorphismes symétriques.
On dit qu'une forme A est *eutactique* si son inverse A^{-1} est une combinaison linéaire à coefficients strictement positifs des mêmes projections.
On dit qu'une forme est *extrême* si elle réalise un maximum local de l'invariant d'Hermite.

Théorème 1.7 (Voronoï). — *Les formes extrêmes sont les formes parfaites et eutactiques.*

Définition 1.8. — On appelle *domaine de Ryshkov* l'ensemble des formes quadratiques définies positives de minimum supérieur à 1.

Ce domaine est l'intersection d'une infinité de demi-espaces affines définis par les inégalités $A[u] \geqslant 1$ quand u décrit $\mathbb{Z}^n \smallsetminus \{0\}$; localement il prend l'allure d'un cône polyèdral puisqu'un compact de cet espace ne rencontre qu'un ensemble fini de tels hyperplans. Les formes parfaites de minimum 1 en constituent les extrémités. (Voir chap 3. [Sch08a])

Définition 1.9. — On appelle *graphe de Voronoï* le graphe dont les sommets sont les extrémités du domaine de Ryshkov et les arêtes les bords de dimension 1.

Ce graphe est encore défini à équivalence arithmétique près, c'est-à-dire modulo transformation de la forme A en la forme $P'AP$ par un élément P de $\mathbf{GL}_n(\mathbb{Z})$.

Théorème 1.10 (Voronoï). — *À équivalence arithmétique près, le graphe de Voronoï est un graphe fini et connexe.*

Comme le fait de construire les formes contiguës à un sommet ou de tester l'équivalence arithmétique de deux formes sont des procédés totalement effectifs, ce résultat a une conséquence considérable.

Théorème 1.11 (Voronoï). — *Il existe un algorithme effectif qui calcule la constante d'Hermite d'une dimension donnée.*

Démonstration. — Nous esquissons les principaux traits de cet algorithme. À partir d'un point du domaine de Ryshkov, il suffit de rechercher un sommet du domaine en se déplaçant vers les bords, puis d'énumérer les formes parfaites par un parcours du graphe de Voronoï, les arêtes issues d'un sommet étant définie par une famille de codimension 1 de projecteurs p_u indicés par les vecteurs minimaux u de la forme du sommet. La constante d'Hermite est le maximum des invariants d'Hermite des formes trouvées. Pour plus de détails, on pourra consulter [Mar03]. □

Toutefois, l'explosion du nombre de formes parfaites avec la dimension et surtout la quantité astronomique de voisins de certaines formes particulières ne permettent à cet algorithme de ne fonctionner à ce jour que jusqu'en dimension 8 et laisse peu d'espoir de le voir parvenir à bout du graphe de Voronoï en dimension supérieure. On connaît d'ores et déjà plusieurs centaines de milliers de formes parfaites en dimension 9.

Le principe de caractérisation des formes extrêmes a été étendu par R. Coulangeon au cas de la constante de Rankin [Cou96] et de la constante d'Hermite–Humbert[Cou01]. Il a également été étendu par Ch. Bavard [Bav97, Bav05] dans un cadre géométrique plus général, que nous aurons l'occasion d'emprunter au chapitre 3.

Signalons aussi que la théorie de Voronoï fonctionne encore lorsque l'on se restreint à des réseaux invariants sous l'action d'un groupe G, ce que l'on appelle G-réseau. La constante d'Hermite associée est le maximum des invariants d'Hermite des G-réseaux. Les notions de G-perfection et de G-eutaxie peuvent être définies relativement à l'espace des endomorphismes symétriques stables sous l'action de G. Elles caractérisent de manière semblable les formes G-extrêmes [BM91]. L'algorithme de Voronoï fonctionne toujours [BMS92] : cela revient à trancher le domaine de Ryshkov par l'espace des endomorphismes symétriques stables sous l'action de G.

L'algorithme de Voronoï a été étendu ensuite par M. Koecher [Kœc60], notamment dans le cas des formes quadratiques définies sur un corps de nombres à la manière de P. Humbert, et plus récemment par J. Opgenorth [Opg01]. M. Dutour-Sikirić, A. Schürmann et F. Vallentin en ont élaboré la version la plus efficace à ce jour [DSSV07, Sch08b]. Les fondements théoriques de l'algorithme de Voronoï fournissent par ailleurs une théorie de la réduction, c'est-à-dire un moyen de décrire un domaine fondamental de l'espace des formes définies positives sous l'action du groupe $\mathbf{GL}_n(\mathbb{Z})$. La décomposition cellulaire de l'espace des formes quadratiques qu'elle suscite est un ingrédient fréquemment utilisé pour le

calcul de groupes de K-théorie [LS78, Sta79, EVGS02]. Cette décomposition a également été utilisée dans le contexte de compactification d'espaces de module [AMRT75, SB06].

1.2.2 Interprétation

D'un point de vue plus moderne, la théorie de Voronoï peut se mettre sous la forme du programme d'optimisation suivant :
Minimiser : $f(A) = \ln \operatorname{dét} A$
Sous les contraintes : $\forall u \in \mathbb{Z}^n \smallsetminus \{0\}, \qquad g_u(A) = 1 - A[u] \leqslant 0$

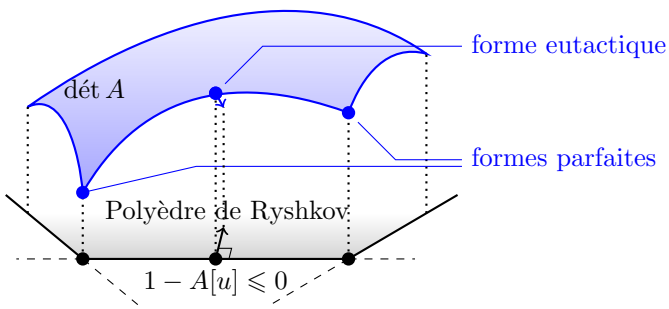


FIG. 1.3 – Vue des formes parfaites et eutactiques

Attention, il ne s'agit pas d'un programme d'optimisation convexe puisque f est concave et non convexe. Toutefois, on peut observer que les conditions différentielles d'optimalité gardent leur sens. Rappelons que dans ce cas le gradient de f est $\nabla f = \dfrac{\text{Com A}}{\operatorname{dét} A} = A^{-1}$ et que le gradient de g_u est $\nabla g_u = -uu'$. L'ensemble des éléments réalisables est le domaine de Ryshkov. Dire qu'une forme réalisable $A^\star$ est eutactique revient à écrire, en complétant pour tout $u \in \mathbb{Z}^n$ les coefficients d'eutaxie ρ_u par des zéros, que

$$\nabla f(A^\star) + \sum_{u \in \mathbb{Z}^n \smallsetminus \{0\}} \rho_u \nabla g_u(A^\star) = 0 \tag{1.12a}$$

et que

$$\forall u \in \mathbb{Z}^n \smallsetminus \{0\}, \quad \min(\rho_u, g_u(A^\star)) = 0. \tag{1.12b}$$

Ces deux conditions sont les fameuses *conditions de Karush-Kuhn-Tucker* qui dictent le cône dans lequel le gradient de f est autorisé à prendre ses valeurs en fonction des contraintes saturées, la première condition s'appelant généralement condition de stationnarité et la seconde condition de relâchement supplémentaire (ou « complementary slackness » en anglais). Les coefficients d'eutaxie s'appellent aussi dans ce cadre *multiplicateurs de Lagrange*. La condition de perfection de $A^\star$ signifie que le maximum de contraintes doivent être activées, autrement dit, que $A^\star$ est situé « dans les coins du domaine de Ryshkov », condition que l'on peut par exemple rapprocher de celle de la méthode du simplexe de la programmation linéaire.

1.3 Les designs

La notion de design recouvre l'idée que l'on approche un espace par un ensemble fini de points de cet espace ; elle apparaît dans des contextes aussi variés que les statistiques, la théorie des graphes ou les géométries finies. Concernant la sphère, la notion de design a été introduite par Ph. Delsarte, J. M. Goethals et J. J. Seidel dans [DGS77].

1.3.1 Les designs sphériques

Définition 1.12. — On dit qu'un ensemble fini de points $\mathcal{D}$ de la sphère unité $\mathscr{S}^{n-1}$ de $\mathbb{R}^n$ forme un *t-design sphérique* si pour tout polynôme f de degré inférieur à t, l'intégrale de f sur la sphère est égale à la moyenne des valeurs de f sur $\mathcal{D}$.

$$\forall f \in \mathbb{R}_t[X_1, \ldots, X_n], \qquad \int_{\mathscr{S}^{n-1}} f(x)\,\mathrm{d}x = \frac{1}{|\mathcal{D}|} \sum_{x \in \mathcal{D}} f(x). \tag{1.13}$$

B. Venkov a montré [Ven01] que les réseaux dont les vecteurs minimaux portent une structure de 4-design au moins forment une classe aux propriétés de densité particulièrement intéressantes. Il les appelle réseaux *fortement parfaits*.

Théorème 1.13 (Venkov). — *Les réseaux fortement parfaits sont extrêmes.*

Les propriétés combinatoires dont jouissent les réseaux fortement parfaits ont permis d'engager leur classification [BV01].

Par ailleurs, W. Lempken, B. Schroeder et Ph. H.Tiep [LST01] ont développé un mécanisme de construction de t-designs portés par l'orbite d'un point sous l'action d'un sous-groupe fini du groupe orthogonal.

Théorème 1.14 (L., Sch. & T.). — *Soit G un sous-groupe fini de $\mathbf{O}(\mathbb{R}^n)$, t un entier, l'orbite $G \cdot x$ d'un point x de la sphère $\mathscr{S}^{n-1}$ forme un t-design sphérique pour tout vecteur x si et seulement s'il n'existe pas de polynôme harmonique non constant de degré inférieur à t et invariant sous G.*

Ce mécanisme est particulièrement adapté à la classe des réseaux possédant un groupe d'automorphismes substantiel, puisque celui-ci agit notamment sur l'ensemble des vecteurs minimaux. Il permet de démontrer en utilisant la théorie des caractères, et particulièrement les caractères des puissances symétriques, l'extrêmalité d'une large classe d'exemples pour lesquels des calculs directs sont actuellement impensables et hors de portée, incluant des réseaux tels que le réseau de Thomson–Smith[2] dont on ne connaît pas à ce jour ni le minimum ni la valeur de la constante d'Hermite.

1.3.2 Les designs grassmanniens

Ch. Bachoc, R. Coulangeon et G. Nebe ont ensuite adapté cette procédure dans le cas de l'invariant de Rankin [BCN02, Bac05]. La notion de *design grassmannien* est définie dans le premier de ces articles. On y rencontre encore le résultat suivant.

[2] réseau unimodulair pair de rang 248 dont le groupe d'automorphisme est, au facteur $\mathbb{Z}/2\mathbb{Z}$ près, le groupe sporadique de Thomson issu de la classification des groupes finis simples.

Théorème 1.15 (B., C. & N.). — *Les réseaux fortement parfaits au sens des designs grassmanniens sont extrêmes relativement à l'invariant de Rankin.*

Parallèlement, toujours dans [BCN02], des critères d'obtention de designs par la théorie des groupes sont développés sur le modèle du cas sphérique, ce qui permet de détailler toute une classe d'exemples de réseaux extrêmes relativement à l'invariant de Rankin, parmi lesquels figurent certains réseaux de racines ou le réseau de Leech. Le second article [Bac05] en passe encore en revue une large collection et étudie en particulier les réseaux de Barnes–Wall.

Signalons par ailleurs que la méthode de Delsarte *et al.* a également fait l'objet d'investigations par Ch. Bachoc, E. Bannai et R. Coulangeon dans le cadre des grassmanniennes dans [BBC04]. L'étude des groupes qui présentent un 4-designs a été effectuée dans [Tie06].

Mentionnons également les travaux de C. Pache [Pac08] qui a proposé très récemment un cadre général pour les designs qui englobe le cas grassmannien mais qui permet aussi de définir une notion de perfection forte pour des formes de Humbert.

Un et un font deux ; deux et deux font quatre . . . —
Y. Mishima, « Cinq Nô modernes ».

Notations, structures et objets mis en jeu

2

2.1 Conventions

Les lettres $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ désignent respectivement l'ensemble des entiers naturels[1], des entiers relatifs, des nombres rationnels, des nombres réels et des nombres complexes, éventuellement munis de leur structure de semi-groupe, d'anneau ou de corps[2] habituelle. La partie réelle et la partie imaginaire sont notées $\Re$ et $\Im$ respectivement. Le symbole $\mathbb{F}_q$ désigne le corps fini à q éléments. La lettre $\mathbb{K}$ désigne un corps quelconque.

2.1.1 Objets combinatoires

2.1.1.1 Partitions

Partager un entier strictement positif consiste à le décomposer en une somme d'entiers strictement positifs dans laquelle l'ordre n'importe pas.

Définition 2.1. — On appelle *partition* toute suite d'entiers $\lambda = (\lambda_i)_{i\in\mathbb{N}^\times}$ décroissante et cofinale à zéro. Les éléments non-nuls de la suite λ sont appelés les *parts*. On appelle *degré* et on note $|\lambda|$ la somme des parts ; on appelle *profondeur* et on note $\lfloor\lambda\rfloor$ le nombre de parts non-nulles. Lorsque m est le degré de la partition λ, on dit que λ est une partition de m et on note $\lambda \vdash m$.

Plutôt que d'énumérer les indices des parts, nous signifierons par la notation $q \in \lambda$ que q est l'une des parts $(\lambda_i)_{i\in\mathbb{N}^\times}$ non-nulles.

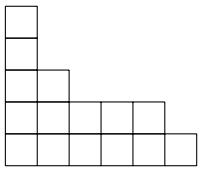
Définition 2.2. — Une partition λ est représentée dans le premier quadrant du plan par un diagramme, dit *diagramme de Ferrer*, formé d'une superposition de barres horizontales alignées à gauche et d'une longueur indiquée par les parts de λ. Les boîtes qui constituent le diagramme sont repérées par leur coordonnées cartésiennes, la boîte du coin bas gauche étant la boîte $(1, 1)$. Les lettres s et $\check{s}$ feront références à la largeur et à la hauteur du diagramme de λ.

[1] Il s'agit de l'ensemble $\{0, 1, \ldots\}$ conformément à la tradition française. Signalons également à cet égard que les termes « positif », « négatif », « croissant » et « décroissant » s'entendent au sens large.

[2] Sans plus de précision, les corps que nous envisagerons seront tous *commutatifs*.

Définition 2.3. — La notation $\breve{\lambda}$ désigne la *partition transposée* de λ, dont le diagramme de Ferrer est, par définition, l'image de celui λ par la symétrie orthogonale d'axe la première bissectrice.

Exemple 2.4. — Soit $\lambda = (6, 5, 2, 1, 1)$ la partition de l'entier 15. Son degré est $|\lambda| = 6 + 5 + 2 + 1 + 1 = 15$ et sa profondeur est $\lfloor \lambda \rfloor = 5$.

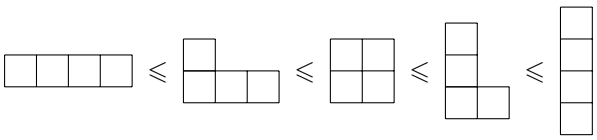
$\lambda =$  .

Dans cet exemple, on a $s = 6$ et $\breve{s} = 5$. Enfin, la partition transposée est $\breve{\lambda} = (5, 3, 2, 2, 2, 1)$.

Notons $\varkappa_t(\lambda) = \sum_{i=t}^{\infty} \lambda_i$ le total des boîtes de λ situées au dessus de la $t^{\text{ième}}$ ligne.

Définition 2.5. — On définit sur l'ensemble des partitions deux notions d'*ordre*. Le premier, noté $\subset$, correspond à l'*inclusion* dans le plan des diagrammes de Ferrer ; le second, noté $\leqslant$, raffine le premier et se définit par $\lambda \leqslant \mu$ si et seulement si pour tout entier t, $\varkappa_t(\lambda)$ est inférieur à $\varkappa_t(\mu)$.

Exemple 2.6. — Les partitions de degré 4 sont ordonnées comme suit



2.1.1.2 Tableaux

Définition 2.7. — On appelle *tableau* T la donnée d'un diagramme de Ferrer inscrit d'entiers naturels, $T(i, j)$ étant l'entier placé à l'abscisse i et l'ordonnée j.
On dit qu'un tableau est *standard* si les entiers qui le composent sont strictement croissants le long des colonnes et croissants le long des lignes. On note f_λ^n le cardinal de l'ensemble des tableaux standards de forme λ à valeurs entre 1 et n.
On appelle *contenu* d'un tableau et on note C_T le compte pour tout entier de son nombre d'occurrence dans T.

Exemple 2.8. — Le tableau

$$U(\lambda) = \begin{array}{|c|c|c|c|c|c|} \hline \breve{s} \\ \cline{1-1} \\ \cline{1-2} \\ \cline{1-2} 2 & 2 & \cdot & \cdot & 2 \\ \hline 1 & 1 & \cdot & \cdot & \cdot & 1 \\ \hline \end{array} \tag{2.1}$$

est un tableau standard. Il est parfois appelé *tableau initial* et jouera un rôle particulier dans la suite.

2.1.1.3 Bitableaux

Définition 2.9. — On appelle *bitableau* et on note $\{T, \Theta\}$ tout couple, ordonné, de tableaux T et Θ de même forme donnée.
Un bitableau $\{T, \Theta\}$ est dit *standard* si les deux tableaux T et Θ qui le constituent le sont.
Le *contenu* d'un bitableau $C_{\{T,\Theta\}}$ est le couple des contenus (C_T, C_Θ).

Dans cette thèse, pour des entiers n et m précisés plus tard, on considérera principalement des bitableaux dont les coefficients du tableau gauche T sont compris entre 1 et n tandis que ceux du tableau de droite Θ sont compris entre 1 et m.

Définition 2.10. — Un bitableau $\{T, \Theta\}$ est dit *initial à gauche*, respectivement *initial à droite*, si le tableau de gauche T, respectivement le tableau de droite Θ, est égal au tableau initial $U(\lambda)$.

2.1.1.4 Polynômes multivariés

Pour $m = \check{s}$, la lettre Z désignera toujours la matrice suivante

$$Z = \begin{pmatrix} z_{1,1} & \cdots & z_{1,m} \\ z_{2,1} & & \vdots \\ \vdots & & \vdots \\ z_{n,1} & \cdots & z_{n,m} \end{pmatrix} \tag{2.2}$$

dont les coefficients $(z_{i,j})_{1\leqslant i\leqslant n,\ 1\leqslant j\leqslant m}$ sont des indéterminées. La notation $\mathbb{K}[Z]$ fait référence à l'*espace des polynômes* en les $n \cdot m$ variables à coefficient dans $\mathbb{K}$.

Définition 2.11. — Lorsque $\mathbb{K}$ est le corps des réels ou des complexes, cet espace de polynômes $\mathbb{K}[Z]$ est muni du *produit scalaire* $[\cdot, \cdot]$ suivant. Le monôme $z^\alpha = z_{1,1}^{\alpha_{1,1}} \cdot z_{1,2}^{\alpha_{1,2}} \cdots z_{n,\check{s}}^{\alpha_{n,\check{s}}}$ a pour norme

$$[z^\alpha, z^\alpha] = \frac{\alpha!}{|\alpha|!} = \frac{\alpha_{1,1}! \cdot \alpha_{1,2}! \cdots \alpha_{n,\check{s}}!}{|\alpha|!} \tag{2.3}$$

et deux monômes distincts sont orthogonaux.

Notons $\underline{\partial}$ la matrice des opérateurs de dérivation

$$\underline{\partial} = \begin{pmatrix} \partial_{z_{1,1}} & \partial_{z_{2,1}} & \cdots & \partial_{z_{n,1}} \\ \vdots & & & \vdots \\ \partial_{z_{\check{s},1}} & \cdots & \cdots & \partial_{z_{\check{s},n}} \end{pmatrix}.$$

On dispose d'un morphisme évident entre l'algèbre des polynômes $\mathbb{K}[Z]$ et l'algèbre des opérateurs différentiels $\mathbb{K}[\underline{\partial}]$ qui consiste à envoyer $z_{i,j}$ sur $\partial_{z_{i,j}}$ et à transformer la multiplication en une composition ; nous noterons $P(\underline{\partial})$ l'image de $\underline{\partial}$ par un polynôme P.

Proposition 2.12. — *Lorsque P et $Q \in \mathbb{K}[Z]$ sont des polynômes homogènes de degré t, le produit scalaire que nous venons de définir vérifie*

$$t!\ [P, Q] = L_0\left(P(\underline{\partial}) \cdot \overline{Q}(Z)\right),$$

où $\overline{Q}$ est le conjugué complexe du polynôme Q et L_0 est l'opérateur qui évalue les polynômes en zéro.

Exemple 2.13. — Considérons les polynômes $P(Z) = z_{1,1} + z_{2,2}$ et $Q(Z) = z_{1,1}^2 + z_{2,2}$, alors $P(\underline{\partial}) \cdot \overline{Q}(Z) = (\partial_{1,1} + \partial_{2,2}) \cdot (z_{1,1}^2 + z_{2,2}) = 2z_{1,1} + 1$ et leur produit scalaire est $[P, Q] = \dfrac{1}{1!} = 1$.

Définition 2.14. — D'un bitableau $\{T, \Theta\}$ de forme μ, on peut construire le *monôme déterminantal*, dit de *forme* μ,

$$\mathscr{M}_{\{T,\Theta\}} = \prod_{i=1}^{u} \text{dét}\, \left(z_{T(i,j),\, \Theta(i,j')}\right)_{1 \leqslant j,\, j' \leqslant \breve{\mu}_i} \tag{2.4}$$

qui est un produit de mineurs de Z, où le choix des colonnes extraites est piloté par l'une des colonnes du tableau de gauche T et le choix des lignes extraites est commandé par la colonne concomitante du tableau de droite Θ, le degré total du monôme coïncidant avec le degré de la forme du bitableau.

Les monômes déterminantaux héritent de la terminologie déjà définie au sujet des partitions, tableaux et bitableaux.

Proposition 2.15. — *La collection des monômes non-nuls $\mathscr{M}_{\{T,\Theta\}}$ constitue une base vectorielle de l'espace des polynômes $\mathbb{K}[Z]$ lorsque $\{T, \Theta\}$ parcourt l'ensemble des bitableaux standards de forme quelconque.*

Démonstration. — On démontre ce fait par un procédé de réécriture des monômes non-standards comme combinaison linéaire de monômes indicés par des bitableaux, de forme éventuellement différente, supérieurs au sens de l'ordre $\geqslant$ induit par $\varkappa$, la transformation préservant le degré et le contenu des bitableaux. Comme il n'y a qu'un nombre fini de bitableaux de degré donné, ce procédé s'arrête et achoppe à la fin sur une configuration où tous les bitableaux sont standards. Ce processus est connu dans la littérature sous le nom de loi de rectification de Doubilet *et al.* [DRS74]. □

Définition 2.16. — On note $I_t(Z)$ l'idéal engendré par les mineurs de taille t de Z. Par extension, si $\breve{\mu}$ est une partition de profondeur u, nous noterons encore $I^{(\mu)}(Z)$ le produit des idéaux

$$I^{(\mu)}(Z) = I_{\breve{\mu}_1}(Z) \cdots I_{\breve{\mu}_u}(Z). \tag{2.5}$$

Enfin, nous noterons $I_{>}^{(\mu)}(Z)$ l'idéal engendré par les idéaux $I^{(\lambda)}(Z)$ indexés par des partitions λ qui contiennent strictement μ au sens de l'inclusion des diagrammes de Ferrer.

L'appartenance d'un monôme déterminantal $\mathscr{M}$ de forme λ à l'idéal $I^{(\mu)}(Z)$ dépend d'un critère purement combinatoire. Un monôme de forme λ appartient à $I^{(\mu)}(Z)$ si et seulement si la forme λ est supérieure à μ au sens de l'ordre $\geqslant$ induit par $\varkappa$ sur les partitions.

Proposition 2.17. — *L'idéal $I^{(\mu)}(Z)$ admet pour base l'ensemble des monômes déterminantaux standards de forme supérieure à μ.*

2.1.2 Algèbre linéaire et affidés

2.1.2.1 Espaces vectoriels et matrices

Dans l'ensemble de cette thèse, un entier n est fixé ; il désigne génériquement la dimension de l'espace vectoriel ambiant. La notation E^n désigne le produit cartésien de n copies de l'ensemble E.

Soit $\mathbb{K}$ un corps ou un anneau, le produit cartésien $\mathbb{K}^n$ sera systématiquement muni de sa base canonique, notée $(e_i)_{1\leqslant i\leqslant n}$. L'ensemble des matrices de taille $n\times m$ à coefficient dans $\mathbb{K}$ est noté $\mathcal{M}_{n,m}(\mathbb{K})$; l'ensemble des matrices carrées de taille n et à coefficient dans $\mathbb{K}$ est noté $\mathcal{M}_n(\mathbb{K})$. La matrice identité est notée I_n .

Selon l'habitude, on note $\mathbf{GL}_n(\mathbb{K})$ et $\mathbf{SL}_n(\mathbb{K})$ le groupe linéaire et le groupe spécial linéaire sur le corps $\mathbb{K}$. On note $\mathbf{O}_n(\mathbb{R})$ le groupe orthogonal et $\mathbf{U}_n(\mathbb{C})$ le groupe unitaire.

On note M' la *matrice transposée* de M. Lorsque M est une matrice à coefficients complexes, la *conjuguée de la matrice transposée* de M est notée M^*. L'ensemble des matrices réelles symétriques définies positives de taille n est noté $\mathcal{S}_n^{>0}$; l'ensemble des matrices complexes hermitiennes définies positives est noté $\mathcal{H}_n^{>0}$.

2.1.2.2 Drapeaux

Définition 2.18. — Soit $\mathrm{d} = (d_1, \ldots, d_\ell)$ une partition de profondeur ℓ aux parts strictement décroissantes. On appelle *drapeau* de l'espace vectoriel $\mathbb{K}^n$ de forme d et on note Δ toute suite de sous-espaces emboîtés

$$\Delta : \quad \{0\} \subsetneq V_\ell \subsetneq \cdots \subsetneq V_i \subsetneq \cdots \subsetneq V_1 \subsetneq \mathbb{K}^n \tag{2.6}$$

dont la dimension $d_i = \dim V_i$ a été fixée une fois pour toutes. L'ensemble des drapeaux de forme d forme une variété, notée $\mathscr{D}_\mathrm{d}$ et appelée *variété drapeau* .

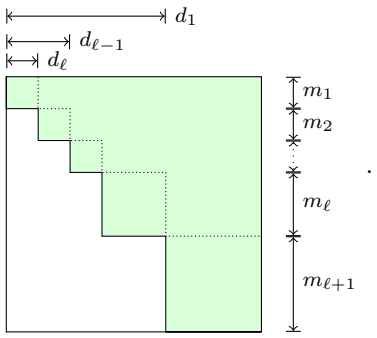
Posons $m = d_1$, $m_1 = d_\ell$, $m_2 = d_{\ell-1} - d_\ell$, $m_i = d_{\ell+1-i} - d_{\ell+2-i}$ lorsque i est compris entre 2 et ℓ et $m_{\ell+1} = n - d_1$. On appelle drapeau canonique le drapeau dont l'espace de dimension d_i est engendré par les d_i premiers vecteurs de la base canonique.

On note $P_\mathrm{d}(\mathbb{K})$ le sous-groupe parabolique[3] de $\mathbf{GL}_n(\mathbb{K})$ qui stabilise le drapeau canonique. Il s'agit de l'ensemble des matrices triangulaires par bloc supérieures, dont les blocs sont de taille $(m_i)_{1\leqslant i\leqslant m+1}$. La variété des drapeaux sur $\mathbb{K}$ s'identifie alors au quotient $\mathbf{GL}_n(\mathbb{K})/P_\mathrm{d}(\mathbb{K})$.

Exemple 2.19. — Soit d la forme de drapeau $\mathrm{d} = (5, 3, 2, 1)$, les matrices de P_d

[3] *i. e.* tel que le quotient du groupe par P soit une variété projective. Les sous-groupes de Borel sont les sous-groupes paraboliques minimaux.

prennent l'allure suivante



Lorsque $\mathbb{K}$ est le corps des réels, la variété drapeau $\mathscr{D}_{\mathrm{d}}$ s'identifie au quotient $\mathbf{O}_n(\mathbb{R})/\mathbf{O}_{m_1}(\mathbb{R}) \times \cdots \times \mathbf{O}_{m_{\ell+1}}(\mathbb{R})$. On repérera par la suite un drapeau réel Δ par une des matrices aux colonnes orthonormées $X_\Delta \in \mathcal{M}_{n,m}(\mathbb{R})$, dont les d_i premières colonnes engendrent l'espace V_i ; celles-ci se déduisent l'une de l'autre par multiplication à droite de $\mathbf{O_m}(\mathbb{R}) = \mathbf{O}_{m_1}(\mathbb{R}) \times \cdots \mathbf{O}_{m_\ell}(\mathbb{R})$.

Lorsque la partition d ne comporte qu'une seule part égale à d, la variété $\mathscr{D}_{\mathrm{d}}$ s'appelle encore *variété grassmannienne* que nous noterons $\mathscr{G}_d$. Lorsqu'en outre $\mathrm{d} = \square$, la variété $\mathscr{D}_{\mathrm{d}}$ s'identifie à l'espace projectif $\mathbb{P}(\mathbb{K})$.

2.1.2.3 Réseaux euclidiens

Définition 2.20. — On appelle *réseau euclidien* tout sous-groupe discret et co-compact d'un espace euclidien.
On appelle *sous-réseau* tout sous-groupe d'un réseau[4].

Un réseau euclidien L peut toujours se mettre sous la forme

$$L = \mathbb{Z}u_1 \oplus \cdots \oplus \mathbb{Z}u_n,$$

où $(u_i)_{1\leqslant i\leqslant n}$ est une famille libre de vecteurs de L. On dit alors que $(u_i)_{1\leqslant i\leqslant n}$ est une *base* de L. La base de L n'est pas unique, deux bases se déduisent l'une de l'autre par une transformation de $\mathbf{GL}_n(\mathbb{Z})$.

La matrice des produits scalaires $A = (\langle u_i, u_j\rangle)_{1\leqslant i,j\leqslant n}$ s'appelle la *matrice de Gram* de L. Il s'agit d'une matrice symétrique définie positive. Elle n'est pas unique ; deux matrices de Gram A et B sont néanmoins semblables ou arithmétiquement équivalentes, c'est-à-dire reliées l'une à l'autre par une relation de la forme $B = P'AP$ où P appartient à $\mathbf{GL}_n(\mathbb{Z})$.

On appelle *déterminant* d'un réseau euclidien le déterminant de l'une de ses matrices de Gram. Le déterminant s'interprète comme le carré du volume d'un parallélotope construit le long des vecteurs d'une base du réseau.

On appelle *minimum* d'un réseau le minimum de la norme carrée des vecteurs non-nuls du réseau. On appelle *vecteur minimal* d'un réseau L tout vecteur non-nul de norme minimale. On notera $\mathscr{S}(L)$ leur ensemble.

On notera $\mathrm{Aut}(L)$ le *groupe des isométries* qui appliquent le réseau L sur lui-même. Il s'agit d'un sous-groupe fini du groupe orthogonal.

[4] sans condition sur le rang.

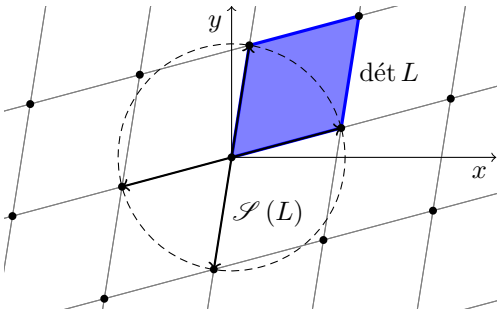


FIG. 2.1 – Déterminant et pairs de vecteurs minimaux d'un réseau L

Définition 2.21. — Le quotient $\gamma_n(L) = \dfrac{\min L}{(\text{dét}\, L)^{1/n}}$ s'appelle, au sens classique du terme, l'*invariant d'Hermite* du réseau L. La *constante d'Hermite* quant à elle est définie par

$$\gamma_n = \sup_{L \text{ réseau}} \gamma_n(L). \tag{2.7}$$

Exemple 2.22. — Les *réseaux de racines* sont des réseaux particuliers, nommés selon le système de racine que porte leur ensemble de vecteurs minimaux. Ils comptent deux familles infinies, notées $(\mathbb{A}_n)_{n\geqslant 1}$ et $(\mathbb{D}_n)_{n\geqslant 2}$ et trois réseaux particuliers $\mathbb{E}_6$, $\mathbb{E}_7$ et $\mathbb{E}_8$.

- Le réseau $\mathbb{A}_n$ est un réseau de rang n, défini par l'intersection de $\mathbb{Z}^{n+1}$ avec l'hyperplan H de $\mathbb{R}^{n+1}$ d'équation $\sum_{i=0}^{n} x_i = 0$. Son déterminant est $\text{dét}\,(\mathbb{A}_n) = n+1$, il possède $n(n+1)/2$ paires de vecteurs minimaux.
- Le réseau $\mathbb{D}_n$ est un réseau de rang n, formé des vecteurs de $\mathbb{Z}^n$ dont la somme des coordonnées est paire. Le déterminant de $\mathbb{D}_n$ est toujours 4, le réseau possède $n(n-1)$ paires de vecteurs minimaux.
- Le réseau $\mathbb{E}_8$ peut être construit à partir de $\mathbb{D}_8$ en le complétant d'un translaté de $\mathbb{D}_8$ par le vecteur $\frac{1}{2}\sum_{i=1}^{8} e_i$. Le réseau $\mathbb{E}_8$ a pour déterminant 1 et possède 120 paires de vecteurs minimaux de norme 2.
- Le réseau $\mathbb{E}_7$, respectivement $\mathbb{E}_6$, est l'orthogonal dans le réseau $\mathbb{E}_8$ du vecteur $e_7 + e_8$, respectivement des vecteurs $e_7 + e_8$ et $e_6 + e_8$. Le réseau $\mathbb{E}_7$ possède 63 paires de vecteurs minimaux, le réseau $\mathbb{E}_6$ en possède 36.

Exemple 2.23. — Le *réseau de Leech* Λ_{24} est un réseau de dimension 24 qui regorge de propriétés particulièrement fabuleuses. Il possède 196560 vecteurs minimaux de norme 4. Pair signifiant ici que ses vecteurs sont tous de norme entière paire et unimodulaire signifiant de déterminant 1, on peut par exemple caractériser le réseau de Leech comme l'unique réseau unimodulaire pair de dimension 24 dépourvu de vecteur de norme 2 ; de tels réseaux sont au nombre de vingt-quatre, dont vingt-trois admettent des vecteurs de norme 2 pour minimum. D'autres constructions totalement explicites sont possibles notamment à partir du code de Golay.

Exemple 2.24. — Soit k un entier, $n = 2^k$ et $\mathbb{R}^n$ l'espace euclidien muni de la base orthonormée $(e_u)_{u\in\mathbb{F}_2^k}$. Le *réseau de Barnes–Wall* BW_n est le réseau engendré sur $\mathbb{Z}$ par les vecteurs $2^{\lfloor \frac{k-d+1}{2} \rfloor} \sum_{u\in U} e_u$ lorsque U décrit l'ensemble des sous-

espaces affines de $\mathbb{F}_2^k$ et d représente la dimension de U.
Cette suite de réseaux démarre par les réseaux $\mathrm{BW}_4 = \mathbb{D}_4$, $\mathrm{BW}_8 = \mathbb{E}_8$ et $\mathrm{BW}_{16} = \Lambda_{16}$ qui est le réseau laminé de dimension 16. Il s'agit d'un des rares exemples de famille infinie de réseaux dont l'invariant d'Hermite croît significativement avec la dimension, même si sa croissance, logarithmique, est asymptotiquement loin d'atteindre celle linéaire de la constante d'Hermite et sa borne inférieure par Hlawka.

Définition 2.25. — Une partition λ étant donnée, on appelle *drapeau minimal* toute chaîne de sous-réseaux $\Lambda = (\Lambda_1, \ldots, \Lambda_{\breve{s}})$ emboîtés et satisfaisant la condition $\mathrm{rg}(\Lambda_i) = \breve{\lambda}_i$ pour tout $1 \leqslant i \leqslant \breve{s}$ tels que le produit suivant

$$\text{dét}\,(\Lambda_1) \cdot \text{dét}\,(\Lambda_2) \cdots \text{dét}\,(\Lambda_{\breve{s}}) \tag{2.8}$$

soit minimal.
On note $\mathscr{S}(L)$ l'ensemble des drapeaux minimaux ; il est de cardinal fini.

Exemple 2.26. — Dans le réseau $\mathbb{A}_3 = \mathbb{D}_3$, les drapeaux minimaux de forme $\boxplus$ sont dirigés par un couple de vecteurs minimaux (*cf.* illustration 2.2).

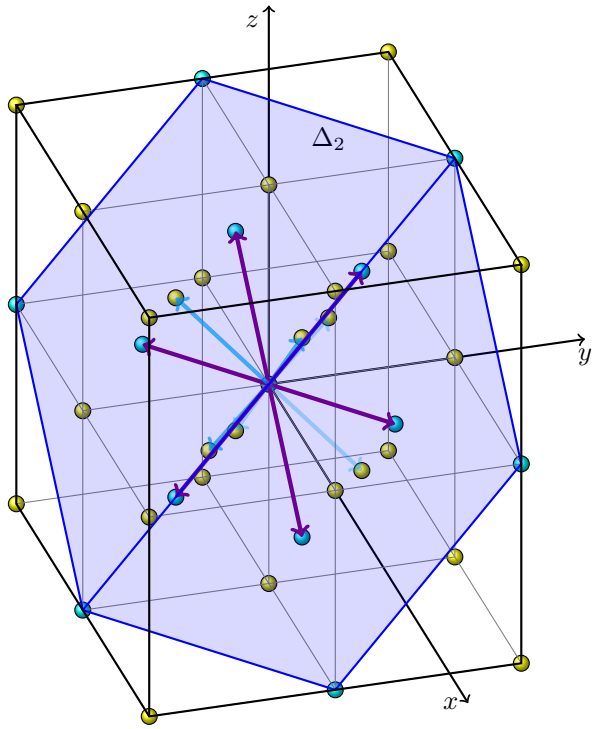


Fig. 2.2 – Drapeau minimal dans le réseau cubique face centrée ($\mathbb{D}_3$)

2.1.2.4 Correspondance entre réseaux euclidiens et formes quadratiques définies positives

Les questions relatives aux réseaux euclidiens peuvent être intégralement reformulées en terme de formes quadratiques définies positives auscultées sous le rapport des entiers et *vice versa*. Nous avons déjà vu comment on peut associer à un réseau sa matrice de Gram. Réciproquement, par une décomposition de Sylvester de la forme en une somme de carrés on peut retrouver une base du réseau et, partant, reconstituer tout le réseau L. Le tableau 2.1 résume les principales correspondances.

Tab. 2.1 – Correspondance entre réseaux euclidiens et formes quadratiques

Réseau	Forme quadratique
réseau L muni d'une base	forme quadratique Q
$\min\limits_{\substack{x\in L\\ x\neq 0}} \|x\|^2$	$\min\limits_{\substack{x\in Z^n\\ x\neq 0}} Q[x]$
dét L	dét Q
invariant d'Hermite du réseau	invariant d'Hermite de la forme
changement de base	équivalence arithmétique
réseau dual	forme de matrice inverse Q^{-1}
réseau à similitude près	forme à équivalence et constante près

Exemple 2.27. — On associe généralement au réseau hexagonal $\mathbb{A}_2$ la base $u_1 = e_1 - e_0$ et $u_2 = e_2 - e_0$ dont la forme quadratique associée est $2x^2 + 2y^2 + 2xy$, mais en choisissant plutôt la base $(u_1 + u_2, u_2)$ on obtiendrait $6x^2 + 2y^2 + 6xy$ qui est le double de la forme représentée dans la figure 1.2.

2.1.3 Théorie algébrique des nombres

2.1.3.1 Corps globaux

La lettre k réfère à un *corps de nombre*, c'est-à-dire une extension algébrique du corps des rationnels $\mathbb{Q}$, de degré $d = r_1 + 2r_2$, où r_1 compte le nombre de plongements réels de k et r_2 compte le nombre de plongements complexes. Nous appellerons parfois r la somme $r_1 + r_2$. Nous noterons D_k le discriminant de k.

L'anneau des entiers du corps k est noté $\mathfrak{o}_k$ ou plus simplement $\mathfrak{o}$ s'il n'y a pas de confusion possible. Le corps k comporte h classes d'idéaux distincts, dont nous fixons des représentants une fois pour toutes : $\mathfrak{a}_1 = \mathfrak{o}$, $\mathfrak{a}_2$, …, $\mathfrak{a}_h$. La norme d'un idéal est notée $\mathcal{N}(\mathfrak{a})$.

Exemple 2.28. — On appelle *entier de Gauß*, et on note $\mathfrak{G}$ leur ensemble, les entiers du corps de nombre quadratique imaginaire $\mathbb{Q}[\mathrm{i}]$ (où $\mathrm{i}^2 = -1$). Ces entiers se mettent tous sous la forme

$$z = a + b\,\mathrm{i},$$

où a et b appartiennent à $\mathbb{Z}$. Du reste, le discriminant de $\mathbb{Q}[\mathrm{i}]$ vaut $D_{\mathbb{Q}[\mathrm{i}]} = -4$.

Exemple 2.29. — On appelle *entier d'Eisenstein*, et on note $\mathfrak{E}$ leur ensemble, les entiers du corps de nombre quadratique imaginaire $\mathbb{Q}[\sqrt{-3}]$. Notons j une racine cubique primitive de l'unité, c'est-à-dire $\mathrm{j} = \frac{-1+\sqrt{-3}}{2}$ ou $\mathrm{j}^2+\mathrm{j}+1 = 0$. Ces entiers s'écrivent alors sous la forme

$$z = a + b\,\mathrm{j},$$

où a et b appartiennent à $\mathbb{Z}$. De plus, le discriminant de $\mathbb{Q}[\sqrt{-3}]$ vaut $D_{\mathbb{Q}[\mathrm{j}]} = -3$.

2.1.3.2 Corps locaux

L'ensemble des places de k est noté $\mathfrak{V}$ et se décompose en deux parties : l'ensemble $\mathfrak{V}_\infty$ des places infinies ou archimédiennes d'une part et l'ensemble $\mathfrak{V}_f$ des places finies ou ultramétriques d'autre part. Les plongements de k dans le corps des réels $\mathbb{R}$ ou dans le corps des nombres complexes $\mathbb{C}$ seront notés $(\sigma_v)_{v\in\mathfrak{V}_\infty}$. La complétion de k, respectivement de $\mathfrak{o}$, à la place v (où v appartient à $\mathfrak{V}$), est notée k_v, respectivement $\mathfrak{o}_v$; lorsque v est une place ultramétrique de $\mathbb{Q}$, $\mathbb{Q}_v$ désigne ainsi le corps des nombres v-adiques selon la notation usuelle et $\mathbb{Z}_v$ l'anneau des entiers v-adiques.

Nous appellerons d_v le *degré local* $[k_v : \mathbb{Q}_v]$. La complétion k_v est munie de deux valeurs absolues que nous distinguons. La valeur absolue, notée $\|\cdot\|_v$, est l'unique extension de la valeur absolue usuelle du corps des réels $\mathbb{Q}_\infty$ lorsque v est une place archimédienne ou du corps p-adique $\mathbb{Q}_p$ lorsque v divise p (nous entendons ainsi que $\|p\|_v = p^{-1}$). La seconde valeur absolue est définie en référence à la première par $|\cdot|_v = \|\cdot\|^{d_v}$ et offre l'avantage de satisfaire à la formule du produit pour tout rationnel $\alpha \in k^\times$, à savoir l'égalité $\prod_{v\in\mathfrak{V}} |\alpha|_v = 1$. Nous pourrions plus directement définir $|x|_v$ comme l'unique coefficient de proportionnalité entre la mesure de Haar d'un compact de k_v et celle du même compact dilaté par une homothétie de rapport x.

2.1.3.3 Réseaux d'un corps de nombre

Définition 2.30. — On appelle *réseau* de l'espace vectoriel k^n tout sous-module sur $\mathfrak{o}_k$ projectif de type fini et de rang maximal[5].

Un réseau L peut toujours se mettre sous la forme

$$L = \mathfrak{c}_1\, u_1 \oplus \cdots \oplus \mathfrak{c}_{n-1}\, u_{n-1} \oplus \mathfrak{c}_n\, u_n, \tag{2.9}$$

où $(u_i)_{1\leqslant i\leqslant n}$ est une base vectorielle de k^n et $(\mathfrak{c}_i)_{1\leqslant i\leqslant n}$ est une suite d'idéaux fractionnaires de k (*cf.* [O'M00]). En particulier, lorsque n vaut 1, la notion de réseau se confond avec la notion d'idéal fractionnaire non nul. On observe que la classe du produit $[\mathfrak{c}_1 \cdot \mathfrak{c}_2 \cdots \mathfrak{c}_n]$ ne dépend pas de l'écriture choisie et s'appelle classe de Steinitz du réseau L.

Sous l'action de conjugaison par un automorphisme de k^n, il y a exactement h classes d'équivalences de réseaux, chaque classe se trouvant caractérisée par sa classe de Steinitz. Au surplus, chaque classe contient un représentant de la forme

$$L_\iota : \quad \mathfrak{o}\, u_1 \oplus \cdots \oplus \mathfrak{o}\, u_{n-1} \oplus \mathfrak{a}_\iota\, u_n. \tag{2.10}$$

[5] Il nous arrivera parfois d'omettre cette dernière condition, nous parlons alors de *sous-réseau*.

Définition 2.31. — Les réseaux de $\mathbb{Q}[\mathfrak{i}]$, respectivement de $\mathbb{Q}[\mathfrak{j}]$ sont appelés réseaux *gaussiens*, respectivement *eisensteiniens* (voir [CS99] p52, chap 2 §2.6).

Soit L un réseau gaussien ou eisensteinien de rang n, ou plus généralement un réseau défini sur un corps de nombre quadratique imaginaire, on note $\Lambda_{\text{réel}}$ le réseau euclidien de rang $2n$ formé des vecteurs

$$(\Re(z_1), \ldots, \Re(z_n), \Im(z_1), \ldots, \Im(z_n)),$$

pour $(z_1, \ldots, z_n) \in L$.

Alors

$$\text{dét}\, L_{\text{réel}} = |D_k|^n\, 4^{-n} (\text{dét}\, L)^2, \tag{2.11}$$

où dét L désigne le déterminant d'une matrice de Gram d'une base de L en tant que module sur l'anneau des entiers $\mathfrak{o}_k$.

Plusieurs réseaux classiques possèdent une structure de réseau gaussien ou eisensteinien :

Exemple 2.32 (Réseau $\mathbb{D}_4$). — Le réseau gaussien engendré par les vecteurs $(1, 1)$ et $(0, 1 + \mathfrak{i})$ détermine un réseau réel isomorphe à $\mathbb{D}_4$ (*cf.* exemple 13a p202 chap7 [CS99]).

Exemple 2.33 (Réseau $\mathbb{E}_6$). — Soit $\theta = \mathfrak{j} - \bar{\mathfrak{j}} \in \mathfrak{E}$, soit L le réseau eisensteinien engendré par les vecteurs $u_1 = (\theta, 0, 0)$, $u_2 = (0, \theta, 0)$ et $u_3 = (1, 1, 1)$, alors $L_{\text{réel}}$ est le réseau de racine $\mathbb{E}_6$.

Exemple 2.34 (Réseau $\mathbb{D}_8$). — Le réseau gaussien engendré par des vecteurs dont les produits scalaires forment la matrice de Gram suivante

$$\begin{pmatrix} 2 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 \\ 1 & 1 & 2 & 1-\mathfrak{i} \\ 1 & 1 & 1+\mathfrak{i} & 2 \end{pmatrix}$$

détermine un réseau réel isomorphe au réseau de racine $\mathbb{D}_8$.

Exemple 2.35 (Réseau $\mathbb{E}_8$). — Le réseau formé des éléments $x = (x_1, \ldots, x_4)$ de $\mathfrak{G}^4$ satisfaisant à $x \mod (1 + \mathfrak{i}) = (0, 0, 0, 0)$ ou $(1, 1, 1, 1)$ et dont la somme des coordonnées est divisible par 2 fournit une structure gaussienne du réseau $\mathbb{E}_8$ (*cf.* exemple 13b p 202 chap 7 de [CS99]). Une matrice de Gram est donnée par

$$\begin{pmatrix} 2 & 1 & -\mathfrak{i} & \mathfrak{i} \\ 1 & 2 & -\mathfrak{i} & \mathfrak{i} \\ \mathfrak{i} & \mathfrak{i} & 2 & -\mathfrak{i} \\ -\mathfrak{i} & -\mathfrak{i} & \mathfrak{i} & 2 \end{pmatrix}.$$

Un construction semblable à partir du tétracode[6] modulo $\sqrt{-3}$ produit le réseau $\mathbb{E}_8$ en tant que réseau eisensteinien (exemple 11b p 200 chap 7 de [CS99]). Une matrice de Gram est donnée par

$$\begin{pmatrix} 2 & \frac{2}{3}(2-\mathfrak{j}) & \frac{2}{3}(2-\mathfrak{j}) & \frac{2}{3}(2-\mathfrak{j}) \\ \frac{2}{3}(1+\mathfrak{j}) & 2 & \frac{2}{3}(2-\mathfrak{j}) & \frac{2}{3}(2-\mathfrak{j}) \\ \frac{2}{3}(1+\mathfrak{j}) & \frac{2}{3}(1+\mathfrak{j}) & 2 & \frac{2}{3}(2-\mathfrak{j}) \\ \frac{2}{3}(1+\mathfrak{j}) & \frac{2}{3}(1+\mathfrak{j}) & \frac{2}{3}(1+\mathfrak{j}) & 2 \end{pmatrix}.$$

[6] code de paramètres [4,2,3] engendré sur $\mathbb{F}_3$ par les vecteurs $(1, 1, 1, 0)$ et $(0, 1, -1, 1)$

Le réseau $\mathbb{E}_8$ possède aussi une structure sur $\mathbb{Q}[\sqrt{-7}]$ explicitement donnée par la matrice de Gram

$$\begin{pmatrix} 2 & 1+\frac{3\sqrt{-7}}{7} & 1+\frac{\sqrt{-7}}{7} & 1+\frac{\sqrt{-7}}{7} \\ 1-\frac{3\sqrt{-7}}{7} & 2 & 0 & 0 \\ 1-\frac{\sqrt{-7}}{7} & 0 & 2 & 1+\frac{\sqrt{-7}}{7} \\ 1-\frac{\sqrt{-7}}{7} & 0 & 1-\frac{\sqrt{-7}}{7} & 2 \end{pmatrix}.$$

Exemple 2.36 (Réseau de Leech). — Le réseau de Leech Λ_{24} possède également une structure de réseau gaussien et eisensteinien dont on trouvera la description détaillée au chapitre 7 de [CS99].

2.1.4 Les adèles

L'arithmétique classique, du moins celle que pratiquaient les mathématiciens du XIXème siècle, rencontre une obstruction bien connue des théoriciens des nombres : très peu d'anneaux de corps de nombre sont principaux. Si la parade classique consiste à étudier d'abord le problème dans l'ensemble des complétés v-adiques puis de remonter dans le corps global initial, un objet permet de travailler simultanément dans l'ensemble des complétions : il s'agit de l'anneau des adèles.

2.1.4.1 Anneau des adèles

Définition 2.37. — On appelle *adèle* un élément $a = (a_v)_{v\in\mathfrak{V}}$ du produit $\prod_{v\in\mathfrak{V}} k_v$ soumis à la condition que a_v appartienne à l'anneau local $\mathfrak{o}_v$ pour presque toute place finie $v \in \mathfrak{V}_f$. L'ensemble des adèles est noté $k_{\mathbb{A}}$. Il est muni d'une structure d'anneau, l'addition et la multiplication étant définies composante par composante.

L'anneau des adèles peut se voir comme la limite inductive des ensembles

$$k_{\mathbb{A}}(S) = \prod_{v\in S} k_v \times \prod_{v\notin S} \mathfrak{o}_v, \tag{2.12}$$

où S est une collection finie de places contenant notamment toutes les places archimédiennes. Chacun des $k_{\mathbb{A}}(S)$ est muni de la topologie produit naturelle ; l'anneau des adèles $k_{\mathbb{A}}$ hérite de cette topologie par passage à la limite. On dit que $k_{\mathbb{A}}$ est un produit topologique restreint. Une base d'ouverts pour la topologie de ce produit est donnée par des ensembles de la forme

$$W = \prod_{v\in\mathfrak{V}} W_v,$$

où W_v est égal au compact $\mathfrak{o}_v$ pour presque tout $v \in \mathfrak{V}_f$.

L'anneau $k_{\mathbb{A}}$ est par construction un anneau *localement compact*[7]. Le plongement de k dans $k_{\mathbb{A}}$ par plongement diagonal est *continu*.

Remarque 2.38. — On peut démontrer que l'image de k dans $k_{\mathbb{A}}$ est discrète et co-compacte. En quelque sorte, on peut voir k dans $k_{\mathbb{A}}$ comme un analogue d'un

[7] alors que le seul produit topologique des $(k_v)_{v\in\mathfrak{V}}$ ne le serait pas.

réseau de dimension 1 dans l'espace euclidien de dimension 1. Cette analogie s'étend à la théorie de la dualité de Pontryagin, le quotient $k_{\mathbb{A}}/k$ pouvant se voir comme le dual $\hat{k}$ de k, c'est-à-dire l'ensemble des homophismes continus de k dans le cercle unité, de la même façon que le quotient $\mathbb{R}/\mathbb{Z}$ peut se comprendre comme le dual de $\mathbb{Z}$.

2.1.4.2 Espaces adéliques attachés à une variété algébrique

Nous serons amenés à considérer de nombreux objets géométriques sur l'anneau des adèles, notamment le groupe général linaire ou bien la variété des drapeaux. Nous précisons ici une fois pour toutes ce que nous entendons ainsi et rappelons quelques faits classiques [Wei82].

Soit $\mathcal{V}$ une variété algébrique définie sur k et soit K un sur-corps de k. On note $\mathcal{V}(K)$ les points de $\mathcal{V}$ rationnels sur K. La variété $\mathcal{V}$ possède un recouvrement fini par des ouverts, eux-même isomorphes à des variétés affines disons $(\mathcal{V}_i)_{1\leqslant i\leqslant p}$ définies sur k :

$$\mathcal{V} = \bigcup_{1\leqslant i\leqslant p} \psi_i(\mathcal{V}_i)$$

où les applications ψ_i sont définies elles aussi sur k.

Définition 2.39. — On appelle espace adélique associé à la variété $\mathcal{V}$ et on note $\mathcal{V}(k_{\mathbb{A}})$ la limite inductive des ensembles

$$\mathcal{V}(k_{\mathbb{A}}(S)) = \prod_{v\in S} \mathcal{V}(k_v) \times \prod_{v\notin S} \bigcup_{1\leqslant i\leqslant p} \psi_i(\mathcal{V}_i(\mathfrak{o}_v))$$

où S est une collection finie de places contenant notamment toutes les places archimédiennes. L'espace $\mathcal{V}(k_{\mathbb{A}})$ hérite de la topologie limite.

Proposition 2.40. — *Soient $\mathcal{V} = \bigcup_{1\leqslant i\leqslant p} \psi_i(\mathcal{V}_i)$ et $\mathcal{V}' = \bigcup_{1\leqslant i\leqslant p'} \psi'_i(\mathcal{V}'_i)$ deux variétés définies sur k et soit $F : \mathcal{V} \to \mathcal{V}'$ un morphisme défini sur k. Alors il existe un ensemble de places S fini et contenant les places archimédiennes, tel que l'image de $\bigcup_{1\leqslant i\leqslant p} \psi_i(\mathcal{V}_i(\mathfrak{o}_v))$ par F est incluse dans $\bigcup_{1\leqslant i\leqslant p'} \psi'_i(\mathcal{V}'_i(\mathfrak{o}_v))$ pour toute place v hors de S.*
En particulier, lorsque F est un isomorphisme, il s'agit d'une égalité.

Exemple 2.41. — Pour qu'un élément $g = (g_v)_{v\in\mathfrak{V}}$, où g_v est dans $\mathbf{GL}_n(k_v)$, appartienne à $\mathbf{GL}_n(k_{\mathbb{A}})$ il faut et il suffit que g_v appartienne à $\mathbf{GL}_n(\mathfrak{o}_v)$ pour presque toute place finie $v \in \mathfrak{V}_f$.

2.2 Les représentations polynomiales du groupe linéaire et du groupe orthogonal

2.2.1 Considérations générales

Rappelons que par *représentation de groupe*, on entend la donnée d'une action du groupe, disons G, sur un espace vectoriel E qui préserve la loi de groupe, ou encore un morphisme de groupe π entre le groupe initial G et le groupe des automorphismes dudit espace vectoriel E. La dimension de E est aussi appelée *dimension* de la représentation. Lorsque la dimension vaut 1, on parle également de *caractère* du groupe G.

Une représentation (E, π) est dite *irréductible* si l'espace E n'admet pas de sous-espace vectoriel E propre qui soit stable sous l'action de G ; elle est dite de surcroît *complètement réductible* si l'espace E peut se décomposer en somme directe de sous-représentations irréductibles[8].

Lorsque le groupe en question possède une richesse aussi étendue que celle du groupe linéaire, il importe de préciser quelles propriétés supplémentaires sont attendues de la représentation : qu'elle soit par exemple continue, holomorphe, rationnelle, polynomiale[9], *etc.* Du reste, les représentations rationnelles du groupe linéaire ne diffèrent des représentations polynomiales que par un produit d'une puissance entière relative du déterminant. En vertu de la formule du produit, il nous sera ainsi loisible de ne travailler qu'avec des représentations polynomiales du groupe $\mathbf{GL}_n(k)$. Signalons par ailleurs que les représentations rationnelles du groupe linéaire sur k sont toutes complètement réductibles.

La classification des représentations des groupes classiques procède d'une théorie exposée pour la première fois dans son unité par Weyl son célèbre ouvrage « The classical groups » [Wey97] puis étendue aux corps algébriquement clos par Chevalley et enfin à des corps quelconques par Tits [Tit71] lorsque le groupe est déployé sur son corps de base. Dans ce qui suit, nous notons $G = \mathbf{G}(k)$ les points rationnels sur k d'un groupe algébrique $\mathbf{G}$ défini sur k, connexe, réductif et déployé sur k. Ses k-représentations irréductibles sont caractérisées par les poids dominants du groupe G, caractères d'un tore[10] maximal de G, tout poids dominant relativement à un sous-groupe de Borel[11] $B = \mathbf{B}(k)$ étant poids dominant χ d'une représentation irréductible.

Plus précisément, la théorie générale assure que l'action du tore de G sur E peut être diagonalisée et que E se décompose en sous-espaces propres, appelés aussi *espaces de poids*, indicés par un poids, c'est-à-dire un caractère du tore, qui précise la valeur propre associée. Parmi ces espaces, une droite se distingue : elle s'appelle *droite de poids dominant* et est constituée par les vecteurs $v^\star$ tels que $\pi(B) \cdot v^\star \subset k\, v^\star$. De tels vecteurs $v^\star$ sont encore dits *vecteurs de poids dominant* ; si h appartient au tore, alors $\pi(h) \cdot v^\star = \chi(h) v^\star$.

En ce qui concerne le groupe linéaire, les *poids dominants* relativement au sous-groupe de Borel formé par les matrices triangulaires supérieures sont en correspondance bijective avec les partitions à moins de n parts. Le poids — ou ici caractère du groupe des matrices diagonales — associé à la partition λ sera noté χ_λ et se définit par

$$\chi_\lambda : \quad \mathrm{Diag}(x_1, \ldots, x_n) \mapsto x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_n^{\lambda_n}. \tag{2.13}$$

Nous noterons $\left(\mathbb{S}^\lambda(\mathbb{K}^n), \pi_\lambda\right)$ un représentant de la *représentation irréductible* associée à λ. Notons d'ores et déjà f_λ^n la *dimension* de la représentation de poids

[8] Toutes les représentations de $\mathbf{GL}_n(\mathbb{R})$ ne sont pas complètement irréductibles, comme l'atteste la représentation continue de dimension deux suivante

$$g \in \mathbf{GL}_n(\mathbb{R}) \mapsto \begin{pmatrix} 1 & \ln \text{dét}\, g \\ 0 & 1 \end{pmatrix} \in \mathbf{GL}(\mathbb{R}^2),$$

qui laisse stable la droite $\mathbb{R}e_1$ et elle uniquement.

[9] On veut dire par là que les coordonnées de ρ s'expriment en terme de fonctions continues, holomorphes, rationnelles, polynomiales une fois une base arrêtée.

[10] Rappelons qu'un groupe algébrique T est un *tore* s'il est connexe et vérifie au choix : (i) T est formé d'éléments semi-simples ; (ii) T est diagonalisable ; (iii) T est isomorphe sur $\overline{k}$ au produit de n copies du groupe multiplicatif $\overline{k}^\times$ où $\overline{k}$ est la clôture algébrique de k.

[11] Autrement dit, un sous-groupe fermé résoluble connexe maximal.

λ du groupe linéaire d'ordre n. On dit parfois que $\mathbb{S}^\lambda(\,\cdot\,)$ s'appelle le *foncteur de Schur*. Nous nous employons à le décrire de deux manières dans les deux prochains paragraphes. Les références classiques sur ce sujet sont [FH91, GW98].

2.2.2 Le module de Schur par les tableaux

Le contenu de ce paragraphe résume le chapitre 8 de [Ful97].

Soit A un anneau commutatif et E un A-module quelconque. Nous nous proposons de décrire dans ce paragraphe le A-module de Schur $\mathbb{S}^\lambda(E)$ sous la forme d'une solution à un problème universel puis par une construction recourant à des tableaux de forme λ.

Nous désignons par $E^{\times\lambda}$ le produit cartésien de $|\lambda|$ copies de E, chacune étant indexée par une boîte du diagramme de Ferrer de la partition λ.

Définition 2.42. — Un élément $\mathbf{v}$ de $E^{\times\lambda}$ est ainsi un diagramme de Ferrer inscrit d'éléments de E. On dit qu'un échange d'inscriptions dans le diagramme λ est licite s'il permute le contenu d'un nombre arbitraire de boîtes dans une colonne avec le contenu du même nombre de boîtes d'une seconde colonne en conservant l'ordre vertical, le contenu des autres boîtes demeurant inchangé. Étant donné un A-module F et un morphisme $\varphi : E^{\times\lambda} \to F$, on dit que φ a la propriété $(\star)$ si pour tout $\mathbf{v} \in E^{\times\lambda}$, $\varphi(\mathbf{v}) = \sum_{\mathbf{w}} \varphi(\mathbf{w})$, où la somme porte sur tous les $\mathbf{w}$ obtenus à partir de $\mathbf{v}$ par échange licite entre deux colonnes et un choix de boîtes dans la colonne de droite précisées à l'avance.

Exemple 2.43. — Soit $\lambda = (3,3,1)$, pour que la propriété $(\star)$ s'impose à φ, il faut par exemple que, choisissant la première et la dernière colonne et l'unique boîte de la dernière colonne,

$$\varphi\left(\begin{array}{|c|c|c|}\hline \mathbf{c} & r & \\ \hline \mathbf{b} & q & \\ \hline \mathbf{a} & p & \mathbf{z} \\ \hline\end{array}\right) = \varphi\left(\begin{array}{|c|c|c|}\hline \mathbf{z} & r & \\ \hline b & q & \\ \hline a & p & \mathbf{c} \\ \hline\end{array}\right) + \varphi\left(\begin{array}{|c|c|c|}\hline c & r & \\ \hline \mathbf{z} & q & \\ \hline a & p & \mathbf{b} \\ \hline\end{array}\right) + \varphi\left(\begin{array}{|c|c|c|}\hline c & r & \\ \hline b & q & \\ \hline \mathbf{z} & p & \mathbf{a} \\ \hline\end{array}\right)$$

ou que, en choisissant les deux premières colonnes et les boîtes extrêmes de la seconde,

$$\varphi\left(\begin{array}{|c|c|c|}\hline \mathbf{c} & \mathbf{r} & \\ \hline \mathbf{b} & q & \\ \hline \mathbf{a} & \mathbf{p} & z \\ \hline\end{array}\right) = \varphi\left(\begin{array}{|c|c|c|}\hline \mathbf{r} & \mathbf{c} & \\ \hline \mathbf{p} & q & \\ \hline a & \mathbf{b} & z \\ \hline\end{array}\right) + \varphi\left(\begin{array}{|c|c|c|}\hline c & \mathbf{b} & \\ \hline \mathbf{r} & q & \\ \hline \mathbf{p} & \mathbf{a} & z \\ \hline\end{array}\right) + \varphi\left(\begin{array}{|c|c|c|}\hline \mathbf{r} & \mathbf{c} & \\ \hline b & q & \\ \hline \mathbf{p} & \mathbf{a} & z \\ \hline\end{array}\right)$$

ou même que, en choisissant les deux premières colonnes et les trois boîtes de la deuxième,

$$\varphi\left(\begin{array}{|c|c|c|}\hline \mathbf{c} & \mathbf{r} & \\ \hline \mathbf{b} & \mathbf{q} & \\ \hline \mathbf{a} & \mathbf{p} & z \\ \hline\end{array}\right) = \varphi\left(\begin{array}{|c|c|c|}\hline \mathbf{r} & \mathbf{c} & \\ \hline \mathbf{q} & \mathbf{b} & \\ \hline \mathbf{p} & \mathbf{a} & z \\ \hline\end{array}\right).$$

Définition 2.44. — Pour tout A-module E, le module de Schur $\mathbb{S}^\lambda(E)$ est le A-module équipé d'un morphisme de projection $\rho_\lambda : E^{\times\lambda} \to \mathbb{S}^\lambda(E)$ tel que pour toute application linéaire φ de $E^{\times\lambda}$ vers un A module F jouissant des propriétés suivantes :

1. φ est multilinéaire,

2. la restriction de φ à une colonne quelconque est alternée,
3. φ possède la propriété $(\star)$,

il existe un unique homomorphisme de A-modules $\widetilde{\varphi}$ de sorte que pour tout $|\lambda|$-upplet de vecteurs $\mathbf{v} \in E^{\times\lambda}$, l'application $\varphi(\mathbf{v})$ se factorise au travers de ρ_λ par $\varphi(\mathbf{v}) = \widetilde{\varphi}\,(\rho_\lambda(\mathbf{v}))$.

Cette construction se résume au travers du diagramme commutatif suivant.

$$\begin{tikzcd} E^{\times\lambda} \arrow[r, "\varphi"'] \arrow[d, "\rho_\lambda"'] & \mathrm{F} \\ \mathbb{S}^\lambda(E) \arrow[ur, dashed, "\widetilde{\varphi}"'] & \end{tikzcd}$$

Remarque 2.45. — Lorsque $\lambda = \square$, les trois conditions sont automatiquement satisfaites et $\mathbb{S}^\square(E)$ est égal à E.
Lorsque λ n'a qu'une part, la condition 2 n'impose rien tandis que la condition 3 exprime la commutativité des coefficients dans $\mathbf{v}$: $\mathbb{S}^{\square\square\square\square}(E)$ est l'espace des puissances symétriques $|\lambda|^{\text{ièmes}}$ de E, encore noté $\mathrm{Sym}^{|\lambda|}E$.
Lorsque $\check{\lambda}$ n'a qu'une part, la condition 3 au contraire ne contraint rien tandis que la condition 2 exprime l'alternativité des coefficients $\mathbf{v}$: $\mathbb{S}^{\begin{smallmatrix}\square\\\square\\\square\\\square\end{smallmatrix}}(E)$ est l'espace des puissances extérieures $|\lambda|^{\text{ièmes}}$ de E, encore noté $\bigwedge^{|\lambda|} E$.

Une construction de $\mathbb{S}^\lambda(E)$ peut être tirée facilement de la définition 2.44. La condition 1 suggère de partir du produit tensoriel de λ copies de E puis de quotienter par le sous-module engendré par les relations décrites par les conditions 2 et 3. Nous pourrons ainsi représenter les éléments de $\mathbb{S}^\lambda(E)$ par des combinaisons de *vecteurs tableaux*, c'est-à-dire de la forme

$$V = \begin{array}{|c|c|c|c|c|c|}
\cline{1-1} x_{1,\check{\lambda}} & & & & & \\
\cline{1-1} & & & & & \\
\cline{1-2} & & & & & \\
\cline{1-6} x_{1,2} & x_{2,2} & \cdot & \cdot & x_{\lambda_2,2} & \\
\cline{1-6} x_{1,1} & x_{2,1} & \cdot & \cdot & \cdot & x_{\lambda_1,1} \\
\cline{1-6}
\end{array}$$

où les éléments $\big(x_{(i,j)}\big)_{(i,j)\in\lambda}$ appartiennent chacun à E. Évidemment, de même que $x\wedge y$ et $x\wedge(x+y)$ représentent le même vecteur dans $\bigwedge^2 E$, la représentation par des vecteurs tableaux n'est pas unique en général.

Définition 2.46. — Étant donné un tableau T, on définit e_T le vecteur de $\mathbb{S}^\lambda(E)$ représenté par

$$e_T = \begin{array}{|c|c|c|c|c|c|}
\cline{1-1} e_{T_{1,\check{\lambda}}} & & & & & \\
\cline{1-1} & & & & & \\
\cline{1-2} & & & & & \\
\cline{1-6} e_{T_{1,2}} & e_{T_{2,2}} & \cdot & \cdot & e_{T_{\lambda_2,2}} & \\
\cline{1-6} e_{T_{1,1}} & e_{T_{2,1}} & \cdot & \cdot & \cdot & e_{T_{\lambda_1,1}} \\
\cline{1-6}
\end{array}$$

Proposition 2.47. — *Supposons que E soit un A-module libre et que $(e_i)_{1\leqslant i\leqslant n}$ en soit une base, alors $\mathbb{S}^\lambda(E)$ est encore un A-module libre engendré par les*

générateurs libres (e_T) *quand* T *parcourt l'ensemble des tableaux standards de forme* λ *à valeur comprise entre 1 et* n.

Exemple 2.48. — Supposons que $E = \mathbb{R}^3$ soit muni de la base $\mathcal{B} = (\vec{i}, \vec{j}, \vec{k})$, le module de Schur $\mathbb{S}^{\boxplus}(\mathbb{R}^3)$ admet pour base vectorielle

$$\left\{ \begin{array}{|c|c|}\hline \vec{j} & \\ \hline \vec{i} & \vec{i} \\ \hline \end{array}, \begin{array}{|c|c|}\hline \vec{k} & \\ \hline \vec{i} & \vec{i} \\ \hline \end{array}, \begin{array}{|c|c|}\hline \vec{j} & \\ \hline \vec{i} & \vec{j} \\ \hline \end{array}, \begin{array}{|c|c|}\hline \vec{k} & \\ \hline \vec{i} & \vec{j} \\ \hline \end{array}, \begin{array}{|c|c|}\hline \vec{j} & \\ \hline \vec{i} & \vec{k} \\ \hline \end{array}, \begin{array}{|c|c|}\hline \vec{k} & \\ \hline \vec{i} & \vec{k} \\ \hline \end{array}, \begin{array}{|c|c|}\hline \vec{k} & \\ \hline \vec{j} & \vec{j} \\ \hline \end{array}, \begin{array}{|c|c|}\hline \vec{k} & \\ \hline \vec{j} & \vec{k} \\ \hline \end{array} \right\}.$$

Remarque 2.49. — Dans le cas des produits extérieurs ou des puissances symétriques, ce résultat n'est rien d'autre qu'un fait bien connu, à savoir que les vecteurs $e_{i_1} \wedge \cdots \wedge e_{i_{|\lambda|}}$ et $e_{i_1} \odot \cdots \odot e_{i_{|\lambda|}}$ en forment une base quand $1 \leqslant i_1 < \cdots < i_{|\lambda|} \leqslant n$ et $1 \leqslant i_1 \leqslant \cdots \leqslant i_{|\lambda|} \leqslant n$ respectivement.

À présent, remarquons que par construction, le module de Schur $\mathbb{S}^\lambda(E)$ est naturellement un $\mathbf{GL}_n(E)$-module. En effet, l'action de $\mathbf{GL}_n(E)$ sur $E^{\times\lambda}$ passe au quotient : si V est un vecteur tableau, l'action d'un élément g à V revient à appliquer g à chacune de ses composantes. On vérifie aussitôt que les vecteurs e_T sont des vecteurs de poids, associés au caractère défini par le contenu de T. De plus, on s'assure que $e_{U(\lambda)}$ est l'unique *vecteur de poids dominant* de $\mathbb{S}^\lambda(\mathbb{K}^n)$ à multiplication par un scalaire près.

Théorème 2.50. — *Soit* λ *une partition à moins de* n *parts, le module de Schur* $\mathbb{S}^\lambda(k^n)$ *construit par la définition 2.44 est bel et bien une représentation irréductible du groupe linéaire sur* k *de poids dominant* λ. *De plus toute représentation irréductible polynomiale est décrite par un de ces modules.*

Démonstration. — Voir [Ful97]. □

2.2.3 Les plongements projectifs de la variété drapeau

Définition 2.51. — Soit $(x_i)_{1 \leqslant i \leqslant \check{s}}$ une famille libre de vecteurs de k^n. On dit que le vecteur V représenté par

$$V = \begin{array}{|c|c|c|c|c|c|}\hline x_{\check{s}} & & & & & \\ \hline & & & & & \\ \hline & & & & & \\ \hline x_2 & x_2 & \cdot & \cdot & x_2 & \\ \hline x_1 & x_1 & \cdot & \cdot & \cdot & x_1 \\ \hline \end{array} \tag{2.14}$$

s'appelle un *vecteur drapeau* et on note $\mathbb{S}^\lambda_\sharp(k^n)$ leur ensemble.

Théorème 2.52. — *[Ful97] On suppose que les parts* $(\check{\lambda}_i)_{1 \leqslant i \leqslant s}$ *prennent exactement les valeurs de* $\mathrm{d} = (d_i)_{1 \leqslant i \leqslant \ell}$. *Soit* $(x_i)_{1 \leqslant i \leqslant \check{s}}$ *une famille libre de vecteurs de* k^n. *L'application qui au drapeau de forme* d *et engendré par les vecteurs* $(x_i)_{1 \leqslant i \leqslant \check{s}}$ *associe le vecteur drapeau correspondant définit un plongement projectif de la variété drapeau* $\mathscr{D}_{\mathrm{d}}$ *dans l'espace* $\mathbb{P}\left(\mathbb{S}^\lambda(k^n)\right)$

Exemple 2.53. — Si $\check{\lambda}$ n'a qu'une part, ceci n'est rien d'autre que le plongement habituel de Plücker de l'espace des grassmaniennes $\mathscr{G}_{|\lambda|}$ dans les puissances

extérieures. Si λ n'a qu'une seule part, il s'agit du plongement de Veronese vers les puissances symétriques.

2.2.4 Le module de Schur par les polynômes

Nous rappelons dans cette partie une autre construction du module de Schur $\mathbb{S}^\lambda(\mathbb{K}^n)$, obtenue cette fois-ci comme sous-espace de $\mathbb{K}[Z]$. On pourra lire le chapitre 11 de [BV88] ou consulter directement [dCEP80] pour plus de détails.

On suppose que la profondeur $\lfloor\lambda\rfloor$ est inférieure aux entiers n et m.

Définition 2.54. — On note $\mathbb{D}^\lambda(\mathbb{K}^n)$ le sous-espace de $\mathbb{K}[Z]$ généré par l'ensemble des bitableaux initiaux à droite.

D'après le lemme suivant, $\mathbb{D}^\lambda(\mathbb{K}^n)$ est un $\mathbf{GL}_n(\mathbb{K})$ module.

Lemme 2.55. — *Soit T_0 un tableau quelconque, alors il existe des coefficients (a_T) uniques et tels que le monôme déterminantal $\mathscr{M}_{\{T_0,U(\lambda)\}}$ d'un bitableau initial à droite possède l'écriture*

$$\mathscr{M}_{\{T_0,U(\lambda)\}} = \sum_T a_T \mathscr{M}_{\{T,U(\lambda)\}} \tag{2.15}$$

où la somme porte sur l'ensemble des tableaux T standards.

Preuve. — On utilise le fait que les règles de réécriture — le processus de rectification de Doubilet *et al.* [DRS74] esquissé dans la justification de la proposition 2.15 — du monôme $\mathscr{M}_{\{T_0,U(\lambda)\}}$ dans la base des bitableaux standards conserve le contenu. Or $U(\lambda)$ est le seul tableau standard de contenu λ. □

Théorème 2.56. — *La représentation $\mathbb{D}^\lambda(\mathbb{K}^n)$ du groupe linéaire est une représentation irréductible de poids dominant λ. De plus, l'isomorphisme entre le module de Schur $\mathbb{S}^\lambda(\mathbb{K}^n)$ défini précédemment et $\mathbb{D}^\lambda(\mathbb{K}^n)$ est exactement accompli par l'application qui envoie le vecteur e_T sur le monôme $\mathscr{M}_{\{T,U(\lambda)\}}$.*

Remarque 2.57. — Ces résultats restent valable si l'on remplace « à droite » par « à gauche » et que l'on note ${}^\lambda\mathbb{D}(\mathbb{K}^m)$ le module correspondant.

2.2.5 Décomposition de l'espace des polynômes

L'espace des polynômes $\mathbb{K}[Z]$ est naturellement muni de l'action de multiplication à droite et à gauche de la variable Z par $G = \mathbf{GL}_n(\mathbb{K}) \times \mathbf{GL}_m(\mathbb{K})$. On observe aussitôt que les idéaux $I^{(\mu)}(Z)$ sont stables sous cette action.

Lemme 2.58. — *Soient (a_T) et (α_Θ) les coordonnées des monômes $\mathscr{M}_{\{T_0,U(\lambda)\}}$ et $\mathscr{M}_{\{U(\lambda),\Theta_0\}}$ de forme λ tels que figurés au lemme 2.55, alors*

$$\mathscr{M}_{\{T_0,\Theta_0\}} = \sum_{T,\Theta} a_T\, \alpha_\Theta\, \mathscr{M}_{\{T,\Theta\}} + I_>^{(\lambda)}(Z), \tag{2.16}$$

où la somme porte sur l'ensemble des tableaux standards T à valeur inférieure à n et Θ à valeur inférieure à m.

On tire aussitôt du lemme la proposition suivante

Proposition 2.59. — *L'application* $\mathbb{S}^\lambda(\mathbb{K}^n) \otimes \mathbb{S}^\lambda(\mathbb{K}^m) \to I^{(\lambda)}(Z)/I^{(\lambda)}_>(Z)$ *définie par*

$$e_T \otimes e_\Theta \mapsto \mathscr{M}_{\{T,\Theta\}} + I^{(\lambda)}_>(Z) \tag{2.17}$$

est un isomorphisme de représentations du groupe $\mathbf{GL}_n(\mathbb{K}^n) \times \mathbf{GL}_(\mathbb{K}^m)$.

Compte tenu de la filtration de $\mathbb{K}[Z]$ par les idéaux déterminantaux, on peut en déduire la structure de l'anneau $\mathbb{K}[Z]$ sous l'action de G.

Théorème 2.60. — *Soit* $\mathbb{K}$ *un corps de caractéristique nulle, alors, sous l'action de* $\mathbf{GL}_n(\mathbb{K}) \times \mathbf{GL}_m(\mathbb{K})$*, l'espace des polynômes* $\mathbb{K}[Z]$ *se décompose en une somme directe de composantes irréductibles sous* G

$$\mathbb{K}[Z] = \bigoplus_{\substack{\lambda,\\ \lfloor\lambda\rfloor \leqslant \min m,n}} M^\lambda \tag{2.18}$$

où M^λ *est l'unique complément invariant par* G *de l'idéal* $I^{(\lambda)}_>(Z)$ *dans* $I^{(\lambda)}(Z)$*. De plus,* M^λ *est la composante isotypique de poids* λ *pour l'action de* $\mathbf{GL}_n(\mathbb{K})$ *ou de* $\mathbf{GL}_m(\mathbb{K})$.

Le module M^λ est isomorphe à $\mathbb{S}^\lambda(\mathbb{K}^n) \otimes \mathbb{S}^\lambda(\mathbb{K}^m)$ selon un isomorphisme ψ décrit dans la proposition 2.59 précédente.

Compte tenu du paragraphe précédent, M^λ contient notamment l'ensemble des monômes initiaux à droite ou à gauche de forme λ. Par contre, tous les monômes de forme λ n'appartiennent pas à M^λ : autrement dit, il n'est pas systématiquement avéré que $\psi(e_T \otimes e_\Theta) = \mathscr{M}_{\{T,\Theta\}}$, comme on peut en juger par l'exemple ci-après. Posons

$$T_1 = \begin{array}{|c|c|}\hline 2 & \\ \hline 1 & 3 \\ \hline\end{array}, \quad T_2 = \begin{array}{|c|c|}\hline 3 & \\ \hline 1 & 2 \\ \hline\end{array}, \quad T_3 = \begin{array}{|c|c|}\hline 2 & \\ \hline 3 & 1 \\ \hline\end{array}, \quad \Theta_1 = \begin{array}{|c|c|}\hline 3 & \\ \hline 1 & 2 \\ \hline\end{array}, \quad B^\sharp = \left\{ \begin{array}{|c|}\hline 3 \\ \hline 2 \\ \hline 1 \\ \hline\end{array}, \begin{array}{|c|}\hline 3 \\ \hline 2 \\ \hline 1 \\ \hline\end{array} \right\}.$$

Les tableaux T_1, T_2 et Θ_1 sont standards mais T_3 ne l'est pas. Alors

$$\mathscr{M}_{\{T_3,\Theta_1\}} = \mathscr{M}_{\{T_1,\Theta_1\}} - \mathscr{M}_{\{T_2,\Theta_1\}} + \mathscr{M}_{B^\sharp}$$

et $\mathscr{M}_{B^\sharp} \in I^{\boxplus}(Z) \subseteq I^{\boxplus}_>(Z)$.

En se restreignant aux polynômes homogènes de degré fixé, un lecteur initié fera le lien avec la construction habituelle des représentations irréductibles du groupe linéaire de poids du degré déjà dit comme sous-représentation d'une puissance tensorielle de $\mathbb{K}^n$ et qui paraissent ici sous des traits cachés.

2.2.6 Représentations du groupe orthogonal

L'objectif de ce paragraphe est de décrire comment le module $\mathbb{S}^\lambda(\mathbb{R}^n)$ se décompose en sous-représentations irréductibles sous l'action du groupe orthogonal $\mathbf{O}_n(\mathbb{R})$.

Définition 2.61. — On désigne par $\mathbb{S}^{[\lambda]}(\mathbb{R}^n)$ la représentation irréductible du groupe orthogonal $\mathbf{O}_n(\mathbb{R})$ de poids λ. On note encore $f^n_{[\lambda]}$ la dimension de cette représentation.

Proposition 2.62. — *Supposons que la profondeur $\lfloor\lambda\rfloor$ soit inférieure strictement à $n/2$. En tant que représentation du groupe orthogonal, le module $\mathbb{S}^{\lambda}(\mathbb{R}^n)$ se fractionne en plusieurs parties*

$$\mathbb{S}^{\lambda}(\mathbb{R}^n) = \mathbb{S}^{[\lambda]}(\mathbb{R}^n) \oplus J^{\lambda}. \tag{2.19}$$

Toutefois la multiplicité de la représentation irréductible de poids λ est toujours 1 et son complément J^{λ} n'est constitué que de représentations de poids inférieur à λ.

Le complément J^{λ} est engendré par les sommes $V \in \mathbb{S}^{\lambda}(\mathbb{R}^n)$ de tableaux inscrits de vecteurs construits à partir d'un premier vecteur $V_0 \in \mathbb{S}^{\lambda}(\mathbb{R}^n)$ comme suit : on sélectionne d boîtes dans deux colonnes distinctes, alors V est la somme des vecteurs tableaux V_0 dans lesquels pour tout multi-indice $i_1 < i_2 < \cdots < i_d$ d'entiers choisis entre 1 et n a été substitué, en respectant l'ordre, le contenu des boîtes selectionnées par la suite des vecteurs $e_{i_1}, \ldots, e_{i_d}$.

D'autre part, pour obtenir une base $\mathbb{S}^{[\lambda]}(\mathbb{R}^n)$, on peut procéder comme suit. On dit qu'un tableau (de nombre) T contient une *violation* si lorsque le même entier v apparaît dans deux colonnes distinctes, il y a plus d'indices strictement inférieurs à v répétés dans les deux colonnes qu'il n'y a d'indices strictement inférieurs à v absent des deux colonnes. On note $[e_T]$ la projection[12] sur $\mathbb{S}^{[\lambda]}(\mathbb{R}^n)$ de e_T parallèlement à J^{λ}. L'ensemble des vecteurs $[e_T]$ indexés par des tableaux standards sans violations fournit une base de $\mathbb{S}^{\lambda}(\mathbb{R}^n)$ (voir [LT85]).

2.3 Hauteurs et géométrie arithmétique

2.3.1 La hauteur de Weil

2.3.1.1 Définition

Définition 2.63. — [God63] Soit $(|\cdot|_v)_{v\in\mathfrak{V}}$ une famille de valeurs absolues de k telle que définie au paragraphe (2.1.3.2), c'est-à-dire respectant la formule du produit. On appelle *hauteur*[13] du k-espace vectoriel E toute fonction $H(\cdot)$ à valeur strictement positive obtenue comme suit : pour chaque place $v \in \mathfrak{V}$, on choisit sur $E \otimes_k k_v$ une norme $H_v(\,\cdot\,)$ compatible avec la valeur absolue $|\cdot|_v$ de k_v de sorte que pour presque toute place finie v et pour tout $x \in E \otimes_k k_v$, $H_v(x)$ soit le maximum des coordonnées des valeurs absolues de x par rapport à une base de E fixée une fois pour toutes. La norme $H_v(\cdot)$ est encore appelée *hauteur locale*. Ceci fait, on définit la hauteur globale comme le produit des hauteurs locales par une constante de normalisation h_0 arrêtée selon son goût.
Compte tenu de la formule du produit, la hauteur $H(\cdot)$ est en réalité définie sur l'espace projectif $\mathbb{P}(E)$.

Afin de simplifier les notations, nous noterons $|x|_{k_{\mathbb{A}}}$ la hauteur d'un adèle $x \in k_{\mathbb{A}}$. Il s'agit du produit des valeurs absolues de x pour l'ensemble des places de k.

Définition 2.64. — Soient E un espace vectoriel sur k et A un automorphisme de

[12] Nous verrons par la suite qu'il s'agit même d'une projection orthogonale.
[13] Je remercie F. Pazuki pour les discussions fructueuses que nous avons eues sur le sujet.

$\mathbf{GL}_n\left(E(k_{\mathbb{A}})\right)$, on appelle *hauteur tordue* par A la hauteur définie par

$$\forall x \in E, \qquad H_A\left(x\right) = H\left(Ax\right). \tag{2.20}$$

Les hauteurs ont été introduites et sont utilisées à cause de la propriété suivante :

Théorème 2.65 (Propriété de Northcott). — *Il n'y a qu'un nombre fini d'éléments sur k de hauteur bornée.*

2.3.1.2 Hauteurs de $\mathbb{S}^\lambda\left(k^n\right)$

Hauteurs locales de $\mathbb{S}^\lambda\left({k_v}^n\right)$ lorsque $v \in \mathfrak{V}_\infty$. D'après le paragraphe 2.2.4, l'espace $\mathbb{S}^\lambda\left({k_v}^n\right)$ peut être vu comme un sous-espace des fonctions polynômiales $k_v[Z]$ muni du produit scalaire euclidien ou hermitien $[\cdot,\cdot]$.

Définition 2.66. — Lorsque $v \in \mathfrak{V}_\infty$ est un place archimédienne, on définit la hauteur locale $H_v\left(\cdot\right)$ sur $\mathbb{S}^\lambda\left({k_v}^n\right)$ par

$$\forall Z \in \mathbb{S}^\lambda\left({k_v}^n\right), \qquad H_v(Z) = f_\lambda^n \cdot [Z,Z]^{d_v/2} \tag{2.21}$$

Lemme 2.67. — *Lorsque v est une place réelle, respectivement lorsque v est une place complexe, l'action du groupe orthogonal $\mathbf{O}_n(\mathbb{R})$ sur $\mathbb{S}^\lambda\left(\mathbb{R}^n\right)$, respectivement du groupe unitaire $\mathbf{U}_n(\mathbb{C})$ sur $\mathbb{S}^\lambda\left(\mathbb{C}^n\right)$, est orthogonale, respectivement unitaire.*

Preuve. — Nous traitons le cas réel ; le cas complexe se démontre de façon identique. Si ω est un élément de $\mathbf{O}_n(\mathbb{R})$, et P, Q deux polynômes de $k[Z]$ appartenant au sous-espace $\mathbb{S}^\lambda\left(\mathbb{R}^n\right)$, comme l'action d'une isométrie commute avec la dérivation par rapport à un polynôme d'opérateurs différentiels, on a l'égalité

$$\big((\omega\cdot P)(\underline{\partial})\big)\big((\omega\cdot Q)(Z)\big) = \omega\cdot\big(P(\underline{\partial})\big)\big(Q(Z)\big) \tag{2.22}$$

En effet, par linéarité, il est suffisant de montrer ce résultat sur les monômes. Nous procédons par une démonstration par récurrence. Notons $\omega = (\!(\omega_{i,j})\!)_{1\leqslant i,j\leqslant n}$ les coefficients de la transformation orthogonale ω.

– Si P et Q sont réduits à une variable, disons $P = z_{i,j}$ et $Q = z_{i',j'}$, alors $\omega\cdot P(\underline{\partial}) = \sum_{k=1}^n \omega_{k,j}\partial_{z_{i,k}}$ et $\omega\cdot Q = \sum_{k=1}^n z_{i',k}\omega_{k,j'}z_{i',k}$. Ainsi

$$(\omega\cdot P(\underline{\partial}))(\omega\cdot Q) = \begin{cases} 0 & \text{si } i \neq i', \\ \displaystyle\sum_{k=0}^n \omega_{k,j}\omega_{k,j'} = 0 & \text{si } i = i' \text{ et } j \neq j', \\ \displaystyle\sum_{k=0}^n \omega_{k,j}\omega_{k,j'} = 1 & \text{si } i = i' \text{ et } j = j'. \end{cases}$$

– Si $P = z_{i,j}$ est encore de degré 1, et si nous supposons avoir démontré la relation pour tous les monômes Q de degré inférieur à n, soit Q un monôme de degré $n+1$ s'écrivant $Q = z_{i',j'}Q_1$,

$$\begin{aligned}(\omega\cdot P(\underline{\partial}))(\omega\cdot Q) &= ((\omega\cdot P(\underline{\partial}))(\omega\cdot z_{i',j'}))(\omega\cdot Q_1) + z_{i',j'}(\omega\cdot P(\underline{\partial})).Q_1 \\ &= \omega\cdot(P(\underline{\partial})z_{i,j}) + (\omega\cdot z_{i',j'})\,\omega P(\underline{\partial}).(\omega\cdot Q_1).\end{aligned}$$

Grâce à l'hypothèse de récurrence, $(\omega\cdot P(\underline{\partial}))(\omega\cdot Q) = \omega\cdot(P(\underline{\partial})Q)$.

– Finalement, supposons la relation démontrée pour tout polynôme Q et tout polynôme P de degré inférieur à n, soit P un monôme de degré $n+1$, disons $P = z_{i,j}P_1$, alors,

$$\begin{aligned}(\omega \cdot P(\underline{\partial}))(\omega \cdot Q) &= (\omega \cdot P_1(\underline{\partial}))[(\omega \cdot \partial_{z_{i,j}})(\omega \cdot Q)] \\ &= (\omega \cdot P_1(\underline{\partial}))[\omega \cdot (\partial_{z_{i,j}} Q)] \\ &= \omega \cdot (P_1(\underline{\partial})\partial_{z_{i,j}} Q) \\ &= \omega \cdot (P(\underline{\partial})Q).\end{aligned}$$

Ce qui achève de prouver la relation (2.22).

Lorsqu'on évalue cette relation en zéro sur chacune des composantes homogènes, on obtient comme attendu

$$[\omega \cdot P, \omega \cdot Q] = [P, Q]\,.$$

□

Définition 2.68. — La notation $\Delta_q(\cdot)$ désigne le mineur principal d'ordre q d'une matrice quelconque (de taille supérieure à q).

Proposition 2.69. — *Soient $v \in \mathfrak{V}_\infty$ une place archimédienne, $(x_i)_{1 \leqslant i \leqslant \check{s}}$ une famille libre de vecteurs de ${k_v}^n$, V le vecteur drapeau de $\mathbb{S}_\sharp^\lambda({k_v}^n)$*

$$V = \begin{array}{|c|c|c|c|c|c|}
\hline x_{\check{s}} & & & & & \\
\hline & & & & & \\
\hline & & & & & \\
\hline x_2 & x_2 & \cdot & \cdot & x_2 & \\
\hline x_1 & x_1 & \cdot & \cdot & \cdot & x_1 \\
\hline
\end{array}$$

et X la matrice des vecteurs colonnes $(x_i)_{1 \leqslant i \leqslant \check{s}}$, la hauteur locale de V peut se calculer par la formule

$$H_v(V) = \left(\Delta_{\check{\lambda}_1}(X'X) \cdots \Delta_{\check{\lambda}_s}(X'X)\right)^{d_v/2} H_v\left(e_{U(\lambda)}\right).$$

Démonstration. — Soit g un élément de $\mathbf{GL}_n(k_v)$ qui envoie le drapeau canonique sur le drapeau engendré par X, de sorte que $H(V) = H\left(\pi_\lambda(g) \cdot e_{U(\lambda)}\right)$. D'après la décomposition d'Iwasawa, l'élément g peut s'écrire comme un produit $g = u\,d\,b$ où u est une matrice unitaire, d une matrice diagonale — disons $d = \mathrm{Diag}(\alpha_1, \ldots, \alpha_n)$ — et b une matrice unipotente triangulaire supérieure.

Nous avons déjà vu que l'action de $\mathbf{U}_n(\mathbb{C})$ ne modifiait pas la norme (lemme 2.67). Donc $H_v(\pi_\lambda(g).e_{U(\lambda)}) = H_v(\pi_\lambda(db).e_{U(\lambda)})$. D'autre part, pour tout q, $\Delta_q(g'g) = \Delta_q(b'd'db)$. Nous pouvons supposer que $u = \mathrm{I}_n$.

Par ailleurs, comme $e_{U(\lambda)}$ est le vecteur de plus haut poids, $\pi_\lambda(d\,b) \cdot e_{U(\lambda)} = \chi_\lambda(d)e_{U(\lambda)} = \left(\prod_{i=1}^n \alpha_i^{\lambda_i}\right) e_{U(\lambda)}$, donc

$$H_v\left(\pi_\lambda(d\,b).e_{U(\lambda)}\right) = \left|\prod_{i=1}^n \alpha_i^{\lambda_i}\right| H_v\left(e_{U(\lambda)}\right).$$

Mais $d\,b$ est une matrice triangulaire supérieure. En particulier $d\,b$ peut s'écrire par bloc $\begin{pmatrix} m_1 & * \\ 0 & m_2 \end{pmatrix}$ de tailles q et $n-q$ et par conséquent le produit $(db)'db$ prend la forme $\begin{pmatrix} {m_1}'m_1 & * \\ * & * \end{pmatrix}$, ce qui justifie l'égalité $\Delta_q\left((db)'db\right) = \|\Delta_q\,(db)\|^2$. Il s'en suit que

$$\Delta_q\,(b'd'db) = |\Delta_q\,(d)|^{2/d_v} = \prod_{i=1}^{\ell} |\alpha_i|^{2/d_v}\,.$$

Mais alors, $\prod_{q=1}^{s} \Delta_{\lambda_q^*}(g'g) = \prod_{i=1}^{n} |\alpha_i^{\lambda_i}|^{2/d_v}$ car le terme α_i apparait exactement λ_i fois parmi les déterminants $\left(\Delta_{\check{\lambda}_\ell}\,(g'g)\right)_{1\leqslant \ell \leqslant s}$. Cette dernière égalité conclut la preuve de la proposition. □

Hauteurs locales de $\mathbb{S}^\lambda\,({k_v}^n)$ lorsque $v \in \mathfrak{V}_f$. Nous connaissons déjà une base de $\mathbb{S}^\lambda\,({k_v}^n)$, donnée par les f_λ^n vecteurs e_T, où T est un *tableau standard*. Nous définissons la norme locale $H_v\,(x)$ (v place finie) comme le maximum de la valeur absolue $|\cdot|_v$ des coordonnées de x dans cette base.

De la sorte, nous avons en outre l'égalité suivante

$$\mathbb{S}^\lambda\,({\mathfrak{o}_v}^n) = \{V \in \mathbb{S}^\lambda\,({k_v}^n)\,;\, H_v(V) \leqslant 1\} \tag{2.23}$$

ce qui motive le choix de notre norme locale.

Normalisation La constante h_0 est choisie pour que $H(e_{U(\lambda)}) = 1$.

Remarque 2.70. — Dans le cas où π_λ est la représentation sur l'espace des puissances extérieures de k^n, la hauteur que nous obtenons est la même que celle étudiée en exemple dans [Wat00], car la base retenue pour les places finies est également orthonormale pour les produits scalaires des places infinies. Par conséquent la constante étudiée ici correspond dans ce cas à la constante définie par J. Thunder dans [Thu98].

2.3.2 La hauteur d'Arakelov

Afin de donner une version plus géométrique des hauteurs que nous considérons, nous exposons la construction suivante, qui conduit à la même hauteur que celle définie dans le paragraphe précédent.

2.3.2.1 Stratégie générale

Définition 2.71. — Soit $\mathcal{L}$ un fibré en droites sur la variété algébrique $\mathcal{V}$ définie sur k. Une métrique sur $\mathcal{L}$ est une norme $\|\cdot\|$ définie sur chacune des fibres. On dit du couple $\overline{\mathcal{L}} = (\mathcal{L}, \|\cdot\|)$ qu'il s'agit d'un *fibré en droite métrisé*.
Une métrique est dite localement bornée si $\log \|\mathfrak{s}\|$ est localement bornée sur $\mathcal{U}$ pour pour tout ouvert $\mathcal{U}$ de $\mathcal{V}$ et toute section $\mathfrak{s}$ de $\mathcal{L}(\mathcal{U})$.

On peut former le produit tensoriel $(\mathcal{L} \otimes \mathcal{M}, \|\cdot\|)$ de deux fibrés en droites métrisés $\overline{\mathcal{L}}$ et $\overline{\mathcal{M}}$: la norme de la fibre en x du nouveau fibré en droites métrisé étant simplement le produit des normes définies sur les fibres en x des fibrés $\mathcal{L}$ et $\mathcal{M}$.

Exemple 2.72. — Dans le cas où $\mathcal{V} = \mathbb{P}(k^n)$, on dispose du fibré en droite tautologique $\mathcal{O}_{\mathbb{P}(k^n)}(-1)$, dont la fibre en x est la droite dirigée par x, et plus généralement des fibrés $\mathcal{O}_{\mathbb{P}(k^n)}(m) = \mathcal{O}_{\mathbb{P}(k^n)}(-1)^{\otimes -m}$. Les sections globales de $\mathcal{O}_{\mathbb{P}(k^n)}(m)$ s'identifient aux polynômes homogènes de degré m. On définit sur $\mathcal{O}_{\mathbb{P}(k^n)}(1)$ la *métrique standard* par

$$\|\mathfrak{s}(x)\|_v = \frac{|\mathfrak{s}(x)|_v}{\max_{j=1}^n |x_j|_v} \tag{2.24}$$

pour toute forme linéaire $\mathfrak{s}$ et toute place ultramétrique $v \in \mathfrak{V}_f$. Pour le reste, si $v \in \mathfrak{V}_\infty$ est une place archimédienne, on définit la *métrique de Fubini–Study* par

$$\|\mathfrak{s}(x)\|_v = \frac{|\mathfrak{s}(x)|_v}{\left(\sum_{j=1}^n |x_j|_v^{2/d_v}\right)^{d_v/2}} \tag{2.25}$$

Définition 2.73. — Étant donnés un fibré en droites métrisé localement borné, un point P de $\mathcal{V}$, et $\mathfrak{s}$ une section méromorphe non-nulle dont P évite le support, on définit

$$h(P) = -\sum_{v \in \mathfrak{V}} \log \|\mathfrak{s}(P)\|_v \tag{2.26}$$

On appelle $H(P) = \exp(h(P))$ la *hauteur* de P.

Encore une fois, la formule du produit justifie que la hauteur ne dépend pas de la section choisie.

2.3.2.2 Fibrés en droites de la variété drapeau

Soient a_i le nombre d'occurrences de la part d_i dans la partition $\breve{\lambda}$. L'espace des grassmanniennes de dimension q peut être envoyé par le plongement de Plücker dans l'espace projectif $\mathbb{P}\left(\bigwedge^q k^n\right)$. En utilisant le plongement de Veronese, qui permet d'envoyer un sous-espace vectoriel E dans $\mathrm{Sym}^a E$ et le plongement de Segre, qui permet d'envoyer un produit dans le produit tensoriel, on dispose de la chaîne d'inclusions suivante.

$$\mathscr{D}_{\mathrm{d}} \subset \prod_{i=1}^{\ell} \mathscr{G}_{d_i}(k^n) \subset \prod_{i=1}^{\ell} \mathbb{P}\left(\bigwedge^{d_i} k^n\right) \subset \cdots$$

$$\cdots \subset \prod_{i=1}^{\ell} \mathbb{P}\left(\mathrm{Sym}^{a_i} \bigwedge^{d_i} k^n\right) \subset \mathbb{P}\left(\bigotimes_{i=1}^{\ell} \mathrm{Sym}^{a_i} \bigwedge^{d_i} k^n\right)$$

Il est possible d'associer à l'espace des grasmanniennes $\mathscr{G}_q(k^n)$ de dimension q le fibré en droites suivant $V \mapsto (V, \bigwedge^q V)$, muni de la métrique standard pour les places ultramétriques et de la métrique de Fubini-Study pour les places archimédiennes issue de la métrique de $\mathbb{P}\left(\bigwedge^q k^n\right)$. Par produit tensoriel, on définit alors un fibré en droites métrisé $\mathcal{O}(a_1, \ldots, a_\ell)$ de la variété $\mathscr{D}_{\mathrm{d}}$ donné explicitement par

$$\Delta = (V_1, \ldots, V_\ell) \mapsto \bigwedge^{d_1} V_1^{\otimes a_1} \otimes \ldots \bigwedge^{d_\ell} V_\ell^{\otimes a_\ell}. \tag{2.27}$$

Ce fibré peut aussi s'obtenir par la construction suivante : soit χ un caractère du sous-groupe parabolique P_{d}. On construit le fibré en droites $L(\chi)$ défini par

$$L(\chi) = G \times^{P_{\mathrm{d}}} k = G \times k/(g \cdot p \times z \sim g \times \chi(p)z)$$

pour $g \in G$, $p \in P_{\mathrm{d}}$ et $z \in k$. Le fibré $\mathcal{O}(a_1, \ldots, a_\ell)$ coïncide avec $L(\chi_\lambda)$ où χ_λ est donné par

$$\forall p \in P_{\mathrm{d}}, \quad \chi_\lambda(p) = \Delta_{d_1}(p)^{a_1} \cdots \Delta_{d_\ell}(p)^{a_\ell}. \tag{2.28}$$

Le fibré en droites métrisé $\mathcal{O}(a_1, \ldots, a_\ell)$ coïncide exactement avec le fibré en droites $\mathcal{O}(1)$ obtenu par tiré en arrière du plongement de la variété drapeau dans $\mathbb{P}\left(\mathbb{S}^\lambda(k^n)\right)$. Ainsi, à une éventuelle constante près, la hauteur construite de cette seconde manière coïncide avec la hauteur de Weil définie au premier paragraphe.

Et voilà. Maintenant le ressort est bandé. Cela n'a plus qu'à se dérouler tout seul. — J. Anouilh « Antigone »

Théorie de Voronoï dans le cas général 3

3.1 La constante d'Hermite généralisée

La famille des constantes dont cette présente thèse fait l'objet a été introduite par T. Watanabe dans l'article [Wat00] sous le terme de « constantes d'Hermite généralisées ». Nous rappelons ici les principales caractéristiques de cette famille.

Nous notons $\mathbf{GL}_n(k_{\mathbb{A}})^1$ la partie unimodulaire du groupe, c'est-à-dire, dans notre cas, les élements g du groupe adélique satisfaisant $|\text{dét}\, g|_{k_{\mathbb{A}}} = 1$.

Définition 3.1 (Watanabe). — On appelle *invariant d'Hermite* d'un élément g du groupe linéaire adélique la quantité

$$\gamma_{n,\lambda}(g) = \min_{\gamma \in \mathbf{GL}_n(k)} H\left(\pi_\lambda(g\gamma) \cdot e_{U(\lambda)}\right)^2. \tag{3.1}$$

On appelle *constante d'Hermite* du groupe linéaire adélique la quantité

$$\gamma_{n,\lambda} = \max_{g \in \mathbf{GL}_n(k_{\mathbb{A}})^1} \gamma_{n,\lambda}(g). \tag{3.2}$$

Cette définition est inspirée du fait que la constante d'Hermite classique peut se reformuler sous la forme $\gamma_n = \max_{g \in \mathbf{GL}_n(\mathbb{R})} \min_{\gamma \in \mathbf{GL}_n(\mathbb{Z})} \|g\gamma \cdot e_1\|^2$.

Démonstration. — De même que dans le cas de la constante classique, l'existence de la borne supérieure et le fait que l'on puisse parler de minimum ou maximum au lieu de simples bornes inférieures ou supérieures relève de la théorie de la réduction [God63]. □

En vertu de la formule du produit, l'invariant d'Hermite ainsi défini ne dépend pas en réalité du vecteur de plus haut poids choisi.

Corollaire 3.2. — *La* constante d'Hermite *est aussi définie comme la plus petite constante C telle que pour tout automorphisme $A \in \mathbf{GL}_n(k_{\mathbb{A}})$, il existe un drapeau Δ de $\mathscr{D}_{\mathrm{d}}$ défini sur k vérifiant*

$$H_A(\Delta) \leqslant C^{1/2} |\text{dét}\, A|_{k_{\mathbb{A}}}. \tag{3.3}$$

Preuve. — En effet, lorsque γ parcourt $\mathbf{GL}_n(k)$, $\pi(\gamma) \cdot e_{U(\lambda)}$ parcourt l'ensemble des vecteurs drapeaux, qui correspondent exactement à l'image d'un drapeau rationnel dans l'espace projectif $\mathbb{P}\left(\mathbb{S}^\lambda(k^n)\right)$ par le plongement décrit au paragraphe 2.2.3. □

On peut encore remarquer que si l'on remplace une partition λ par une partition dont on a répété q fois chacune des parts $(\breve{\lambda}_i)_{1\leqslant i\leqslant s}$, la hauteur obtenue est la puissance $q^{\text{ième}}$ de la hauteur initiale.

Exemple 3.3 (Correspondance avec les constantes existantes). —

1. La constante d'Hermite classique correspond au cas $\lambda = \square$ et $k = \mathbb{Q}$.
2. Lorsque la partition $\breve{\lambda}$ ne comporte qu'une part et que $k = \mathbb{Q}$, la constante $\gamma_{n,\lambda}$ correspond à la constante de Rankin.
3. Si $\lambda = \square$, la constante $\gamma_{n,\lambda}$ correspond à la constante de Hermite–Humbert.
4. Lorsque la partition $\breve{\lambda}$ ne comporte qu'une part, la constante obtenue coïncide avec la constante définie par Thunder [Thu98].

Remarque 3.4 (Constantes fondamentales). — Dans une démarche propre à rendre la définition des constantes ainsi déclarées plus intrinsèque, une seconde définition des constantes d'Hermite, dites « fondamentales » a été proposée par T. Watanabe dans l'article [Wat03]. Cette définition offre l'avantage de se débarrasser d'une dépendance en la représentation et, par la même, de la façon dont la variété drapeau est plongée un un espace projectif, la hauteur étant définie directement sur les éléments du groupe $\mathbf{GL}_n(k_{\mathbb{A}})$ par une décomposition de Levi. La hauteur obtenue est alors unique à un exposant près, qui peut être fixé par un choix de normalisation. Toutefois cette définition ne s'applique qu'au cas où le sous-groupe parabolique en jeu est maximal, ce qui, pour le cas du groupe linéaire, revient à supposer que les parts de la partition λ sont toutes égales. Elle ne peut pas être étendue au cas des groupes non-maximaux.

3.2 La constante d'Hermite des formes de Hermite–Humbert

La clef de ce chapitre consiste à concentrer les informations portées par les contributions de chacune des places en un assemblage fini d'objets. À cette fin, nous présentons dans cette section les formes d'Humbert, formes dont l'éponyme a initié la théorie de la réduction [Hum49] et qui ont été employée dans [Ica97] pour définir les premières constantes d'Hermite relatives à un corps de nombres par analogie avec le cas classique. D'autre part, nous montrons encore comment l'apport des places ultramétriques peut être maîtrisé.

3.2.1 Formes de Hermite–Humbert

3.2.1.1 Les formes d'Hermite–Humbert

Nous identifierons sans plus de précision une forme quadratique sur k^n, $\mathbb{R}^n$ ou $\mathbb{C}^n$ avec la matrice qui la représente dans la base canonique de l'espace ambiant.

Définition 3.5. — On appelle *forme de Hermite–Humbert* tout r-upplet de formes $\mathcal{A} = (A_v)_{v\in\mathfrak{V}_\infty}$ issues de $(\mathcal{S}_n^{>0})^{r_1} \times (\mathcal{H}_n^{>0})^{r_2}$ et qui vérifient[1] de plus dét $A_v = 1$ pour $v \in \mathfrak{V}_\infty$.

On note $\mathcal{P}_n(k)$ l'ensemble des formes de Hermite–Humbert.

[1] Selon les auteurs, la condition de normalisation par les déterminants n'est pas toujours retenue. Dans le cadre de notre travail, la plus grande lisibilité des énoncés rend justice à ce choix.

Ces formes ont été étudiées pour la première fois par P. Humbert [Hum49] qui recherchait une théorie de la réduction sur les corps de nombre. Un élément se distingue : le r-upplet formé de r exemplaires de la matrice identité, noté $\mathcal{I} = (\mathrm{I}_n)_{v\in\mathfrak{V}}$.

Définition 3.6. — Soit $\mathcal{A}$ une forme d'Hermite–Humbert, soient $(x_i)_{1\leqslant i\leqslant \check{s}} \subset k^n$ une famille libre de vecteurs, soit $V \in \mathbb{S}^{\lambda}_{\sharp}(L_\iota)$ le vecteur drapeau donné par

$$V = \begin{array}{|c|c|c|c|c|c|}
\hline x_{\check{s}} & & & & & \\
\hline & & & & & \\
\hline & & & & & \\
\hline x_2 & x_2 & \cdot & \cdot & x_2 & \\
\hline x_1 & x_1 & \cdot & \cdot & \cdot & x_1 \\
\hline
\end{array}$$

et X la matrice $n \times \check{s}$ des vecteurs $(x_i)_{1\leqslant i\leqslant \check{s}}$. Alors la notation $\mathcal{A}[V]$ désigne l'évaluation de $\mathcal{A}$ en V, c'est-à-dire :

$$\mathcal{A}[X] = \prod_{v\in\mathfrak{V}_\infty} \prod_{q\in\check{\lambda}} \left(\Delta_q\left(X^{\sigma_v *} A_v X^{\sigma_v}\right)\right)^{d_v}. \tag{3.4}$$

Rappelons que $\Delta_q(\cdot)$ désigne le mineur principal d'ordre q.

3.2.1.2 Leurs éléments caractéristiques

Nous fixons dans ce paragraphe un réseau de corps de nombre L qui s'écrit sous la forme

$$L = \mathfrak{c}_1 u_1 \oplus \cdots \oplus \mathfrak{c}_{n-1} u_{n-1} \oplus \mathfrak{c}_n u_n$$

ainsi que décrit en 2.1.3.3.

Définition 3.7. — On appelle *déterminant* par rapport au réseau L d'une forme de Hermite–Humbert $\mathcal{A} = (A_v)_{v\in\mathfrak{V}_\infty}$ le produit des déterminants suivants, calculés par rapport au système de vecteur $(u_i)_{1\leqslant i\leqslant n}$.

$$\text{dét}_L(\mathcal{A}) = \mathcal{N}(\mathfrak{c}_1\mathfrak{c}_2\cdots\mathfrak{c}_n) \prod_{v\in\mathfrak{V}_\infty} \text{dét}_{(u_1,\ldots,u_n)}(A_v)^{d_v}. \tag{3.5}$$

On définit, également par rapport au réseau de corps de nombre L et à un vecteur V du module de Schur $\mathbb{S}^{\lambda}(k^n)$, l'idéal fractionnaire $\mathfrak{A}^L_V$ selon la formule

$$(\mathfrak{A}^L_V)^{-1} = \left\{\alpha \in k,\ \alpha V \in \mathbb{S}^{\lambda}(L)\right\}. \tag{3.6}$$

Dans le cas où $\lambda = \square$, V appartient à k^n directement et cet idéal n'est rien d'autre que le plus grand commun diviseur des coordonnées de V.

Définition 3.8. — On appelle *minimum de la forme de Hermite–Humbert* $\mathcal{A}$ relativement au réseau L la quantité

$$m_L(\mathcal{A}) = \min_{V\in\mathbb{S}^{\lambda}_{\sharp}(L)} \frac{\mathcal{A}[V]}{\mathcal{N}\left(\mathfrak{A}^L_V\right)^2}. \tag{3.7}$$

Remarque 3.9. — Par le même procédé que celui décrit pour une forme au paragraphe 2.1.2.4, on peut décomposer chaque terme d'une forme d'Hermite $\mathcal{A} = (A_v)_{v\in\mathfrak{V}_\infty}$ sous la forme $A_v = {g_v}^* g_v$ ce que nous noterons $\mathcal{A} = g^* g$.

3.2.1.3 Une nouvelle constante d'Hermite

Définition 3.10. — On appelle *invariant d'Hermite* de la forme d'Hermite–Humbert $\mathcal{A} = (A_v)_{v\in\mathfrak{V}_\infty}$ par rapport au réseau L de k^n le nombre

$$\gamma_L(\mathcal{A}) = \frac{m_L(\mathcal{A})}{(\text{dét}_L \mathcal{A})^{\frac{|\lambda|}{n}}}. \tag{3.8}$$

On appelle *constante d'Hermite* par rapport au réseau L des formes d'Hermite–Humbert le nombre

$$\gamma_L = \sup_{\mathcal{A}\in\mathcal{P}_n(k)} \gamma_L(\mathcal{A}). \tag{3.9}$$

On peut observer que deux réseaux L et L' affichant la même classe de Steinitz procurent des constantes d'Hermite γ_L et $\gamma_{L'}$ égales.

Définition 3.11. — On appelle encore *constante d'Hermite* des formes d'Hermite–Humbert la valeur

$$\gamma^\circ_{n,\lambda} = \sup_{L \text{ réseau de } k^n} \gamma_L = \max_{1\leqslant\iota\leqslant h} \gamma_{L_\iota}. \tag{3.10}$$

Dans le cas où la partition ne comporte qu'une part, $\lambda = \square$, cette constante — ou parfois la constante γ_{L_1} seulement — a été étudiée sous le nom de « constante d'Hermite–Humbert » dans divers articles (voir notamment [Ica97, BI97, BCIO01, PW05, CIO07]).

3.2.2 Équivalence des constantes généralisées et de Humbert

Proposition 3.12. — *La constante d'Hermite des formes d'Hermite–Humbert $\gamma^\circ_{n,\lambda}$ et la constante d'Hermite du groupe linéaire adélique $\gamma_{n,\lambda}$ coïncident.*

Démonstration. — Soit v une place ultramétrique. Pour tout indice ι compris entre 1 et h, l'idéal $\mathfrak{a}_\iota$ devient principal par localisation dans k_v et peut s'écrire sous la forme $\mathfrak{a}_\iota \otimes \mathfrak{o}_v = a_{\iota,v}\mathfrak{o}_v$. En complétant nos notations par $a_{\iota,v} = 1$ lorsque v est une place archimédienne, on achève de construire un adèle, encore noté a_ι. Soit δ_ι la matrice diagonale $\mathrm{Diag}(1,\dots,1,a_\iota^{-1})$ de $\mathbf{GL}_n(k_\mathbb{A})$. Remarquons déjà que

$$\delta_\iota L_\iota = L_1 \qquad \text{et} \qquad |\text{dét}\,\delta_\iota|_{k_\mathbb{A}} = \mathcal{N}(\mathfrak{a}_\iota)$$

Il en résulte pour le groupe $\mathbf{GL}_n(k_\mathbb{A})$ la décomposition en double classes suivantes (*cf.* [PR94]),

$$\mathbf{GL}_n(k_\mathbb{A}) = \bigsqcup_{\iota=1}^{h} \mathbf{GL}_n(k_\mathbb{A}(\mathfrak{V}_\infty)) \cdot \delta_\iota \cdot \mathbf{GL}_n(k) \tag{3.11}$$

obtenue par l'action de multiplication par $\mathbf{GL}_n(k)$ à droite et l'action de multiplication par $\mathbf{GL}_n(k_\mathbb{A}(\mathfrak{V}_\infty))$ à gauche.

La valeur du minimum $\min_{\gamma\in\mathbf{GL}_n(k)} H\left(\pi_\lambda(g\gamma)\cdot e_{U(\lambda)}\right)^2$ ne dépend pas en réalité de la classe de l'élément $g \in \mathbf{GL}_n(k_\mathbb{A})$ modulo le groupe des points rationnels $\mathbf{GL}_n(k)$. En outre, quand γ parcourt ce groupe, l'expression $\pi_\lambda(\gamma)e_{U(\lambda)}$

décrit l'ensemble des vecteurs drapeaux de $\mathbb{S}_\sharp^\lambda(k^n)$. Aussi, la constante peut être réécrite

$$\begin{aligned}\gamma_{n,\lambda} &= \max_{g\in\mathbf{GL}_n(k_\mathbb{A})/\mathbf{GL}_n(k)} \min_{V\in\mathbb{S}_\sharp^\lambda(k^n)} \frac{H\left(\pi_\lambda(g)\cdot V\right)^2}{|\text{dét}\, g|_{k_\mathbb{A}}^{\frac{2|\lambda|}{n}}} \\ &= \max_{\substack{g\in\mathbf{GL}_n(k_\mathbb{A}(\mathfrak{V}_\infty))\\ 1\leqslant\iota\leqslant h}} \min_{V\in\mathbb{S}_\sharp^\lambda(k^n)} \frac{H\left(\pi_\lambda(g\delta_\iota)\cdot V\right)^2}{|\text{dét}\, g\lambda_\iota|_{k_\mathbb{A}}^{\frac{2|\lambda|}{n}}}.\end{aligned}$$

Grâce à la formule du produit et quitte à multiplier V par une constante suffisamment grande, on peut faire l'hypothèse que V ne parcourt que l'ensemble $\mathbb{S}_\sharp^\lambda(L_\iota)$. À cause de l'invariance des hauteurs locales sous l'action de $\mathbf{GL}_n(\mathfrak{o}_v)$, on peut restreindre le domaine d'appartenance de g à $\mathbf{GL}_n(k_\infty) = \prod_{v\in\mathfrak{V}_\infty}\mathbf{GL}_n(k_v)$. Pour résumer

$$\gamma_{n,\lambda} = \max_{\substack{g\in\mathbf{GL}_n(k_\infty)\\ 1\leqslant\iota\leqslant h}} \min_{V\in\mathbb{S}_\sharp^\lambda(L_\iota)} \frac{H\left(\pi_\lambda(g\delta_i)\cdot V\right)^2}{|\text{dét}\, g|_{k_\mathbb{A}}^{\frac{2|\lambda|}{n}}\,\mathcal{N}\left(\mathfrak{a}_\iota\right)^{\frac{2|\lambda|}{n}}}.$$

Associons à tout élément $g\in\mathbf{GL}_n(k_\infty)$ la forme de Hermite-Humbert $\mathcal{A} = g'g$. Alors, comme $\delta_{\iota,v} = \mathrm{I}_n$ quand v est une place archimédienne, on peut vérifier que

$$\prod_{v\in\mathfrak{V}_\infty} H_v\left(\pi_\lambda(g_v\delta_{\iota,v})\cdot V\right)^2 = \mathcal{A}[V] \quad \text{et} \quad \prod_{v\in\mathfrak{V}_f} H_v\left(\pi_\lambda(g_v\delta_{\iota,v})\cdot V\right) = \frac{1}{\mathcal{N}\left(\mathfrak{A}_X^\iota\right)}.$$

En effet décomposons $V = \sum_T V_T e_T$, où T parcourt l'ensemble des tableaux standards, dans la base canonique de $\mathbb{S}^\lambda(k^n)$. L'action de δ_ι se réduit à multiplier e_T par ${a_\iota}^{-C_T(n)}$, d'où la formule

$$H_v\left(\delta_\iota\cdot V\right) = \max_T \left|{a_\iota}^{-C_T(n)}\right|_v H_v\left(X_T\right).$$

Mais αV appartient à $\mathbb{S}^\lambda(L_\iota) = \bigoplus_T \mathfrak{a}_\iota{}^{C_T(n)} e_T$ si et seulement si $|\alpha V_T|_v \geqslant \left|\mathfrak{a}_\iota{}^{C_T(n)}\right|$ pour toute place finie v. Par conséquent, $|\mathfrak{A}_V^\iota| = \max_T \frac{\left|\mathfrak{a}_\iota{}^{C_T(n)}\right|}{|V_T|_v}$. En rassemblant toutes les égalités, obtient la formule attendue et par conséquent,

$$\gamma_{n,\lambda} = \sup_{\substack{\mathcal{A}\in\mathcal{P}_n(k)\\ 1\leqslant\iota\leqslant h}} \min_{V\in\mathbb{S}_\sharp^\lambda(L_\iota)} \frac{\mathcal{A}[V]}{\mathcal{N}\left(\mathfrak{A}_V^\iota\right)^2\left(\text{dét}_{L_\iota}\mathcal{A}\right)^{\frac{|\lambda|}{n}}} = \gamma_{n,\lambda}^\circ,$$

ce qu'on désirait. □

3.3 Eutaxie et perfection

La théorie de Voronoï classique [Vor08] s'appuye sur deux propriétés des formes quadratiques, la perfection et l'eutaxie, qui caractérisent exactement les formes extrêmes, c'est-à-dire les formes qui accomplissent un maximum local de l'invariant d'Hermite γ.

Dans son article [Bav97], Christophe Bavard a exhibé un cadre général dont nous nous approprions ici pour proposer des définitions d'eutaxie et de perfection idoines. Ce cadre est le suivant : l'invariant d'Hermite d'un objet p est défini comme le minimum de l'évaluation en p d'une famille de « fonctions longueurs » $(f_c)_{c\in C}$, qui sont des fonctions à valeurs strictement positives, définie sur l'espace $\mathcal{V}$ qui paramétrise l'ensemble des objets p en vue. Pour obtenir le cadre classique de la théorie de Voronoï, $\mathcal{V}$ doit être choisi comme l'espace des matrices symétriques définies positives de déterminant 1, les fonctions longueur sont les fonctions $A \mapsto u'Au \in \mathbb{R}_+$ et sont indexées par l'ensemble des vecteurs u non-nuls de $\mathbb{Z}^n$.

Dans ce cadre géométrique, l'eutaxie et la perfection d'un objet p peuvent se formuler en terme de propriétés sur les gradients des fonctions longueur qui atteignent le minimum (*cf. infra.*). De plus, lorsque la condition $(\mathscr{C})$ suivante est satisfaite, le théorème de Voronoï est vérifié, c'est-à-dire que pour que l'invariant d'Hermite de p soit un maximum local il faut et il suffit que p soit eutactique et parfait.

Soit $S(p)$ l'ensemble des indices $\varsigma \in C$ des fonctions longueurs f_ς qui commettent leur minimum en p. La condition $(\mathscr{C})$ peut être rapportée comme suit :

> « Pour tout point p de $\mathcal{V}$, pour tout sous-ensemble $T \subset S$, pour tout vecteur non nul x orthogonal aux gradients $(\nabla f_\vartheta)_{\vartheta\in T}$, il existe un germe de courbes de classe $\mathcal{C}^1$, disons $c : [0,\varepsilon[\to \mathcal{V}$, tel que $c(0) = p$, $c'(0) = x$ et pour tout ϑ appartenant à T, $f_\vartheta(c(t))$ est strictement supérieur à $f_\vartheta(p)$ dès lors que t appartient au voisinage $]0,\varepsilon[$. »

3.3.1 Reformulation géométrique

L'espace dans lequel nous nous apprêtons à travailler est l'espace des formes de Hermite–Humbert $\mathcal{P}_n(k)$ muni d'une *structure riemannienne*. L'espace tangent au point $\mathcal{A}$ consiste en les r-upplets suivants :

$$\mathrm{T}_{\mathcal{A}}\mathcal{P}_n(k) = \left\{\mathcal{X} = (X_v)_{v\in\mathfrak{V}_\infty}\ ;\ \mathrm{Tr}(A_v^{-1}X) = 0\right\}. \tag{3.12}$$

Le produit scalaire est défini par la formule

$$\forall \mathcal{X},\, \mathcal{Y} \in \mathrm{T}_{\mathcal{A}}\mathcal{P}_n(k), \qquad \langle \mathcal{X}, \mathcal{Y}\rangle_{\mathcal{A}} = \sum_{v\in\mathfrak{V}_\infty} \mathrm{Tr}(A_v^{-1}X_v\, A_v^{-1}Y_v). \tag{3.13}$$

Définition 3.13. — Soit $\varsigma = (\iota, V)$ un couple formé d'un entier ι compris entre 1 et le nombre de classes h d'une part et d'un vecteur drapeau $V \in \mathbb{S}_\sharp^\lambda(L_\iota)$ d'autre part, on appelle *fonction longueur* l'application définie pour toute forme de Humbert $\mathcal{A} = (A_v)_{v\in\mathfrak{V}_\infty}$ appartenant à $\mathcal{P}_n(k)$ par

$$\ell_V^\iota(\mathcal{A}) = \ln\left(\frac{\mathcal{A}[V]}{\mathcal{N}\left(\mathfrak{A}_V^\iota\right)^2 \mathcal{N}\left(\mathfrak{a}_\iota\right)^{\frac{|\lambda|}{n}}}\right). \tag{3.14}$$

Remarque 3.14. — En réalité, plusieurs indices distincts peuvent paramétrer la même fonction longueur. En effet, si α appartient au corps global k, les fonctions ℓ_V^ι et $\ell_{\alpha V}^\iota$ coïncident.

Soit V un vecteur drapeau de $\mathbb{S}_\sharp^\lambda(L_\iota)$, donné sous la forme,

$$V = \begin{array}{|c|c|c|c|c|c|}
\hline x_{\breve{s}} & & & & & \\
\hline & & & & & \\
\hline & & & & & \\
\hline x_2 & x_2 & \cdot & \cdot & x_2 & \\
\hline x_1 & x_1 & \cdot & \cdot & \cdot & x_1 \\
\hline
\end{array} .$$

Pour tout entier $p \leqslant \breve{s}$, convenons d'appeler X_p la matrice $n \times p$ dont les colonnes sont les vecteurs $(x_i)_{1 \leqslant i \leqslant p} \subset k^n$. Le *gradient* au point $\mathcal{A} = (A_v)_{v \in \mathfrak{V}_\infty}$ de la fonction longueur ℓ_V^ι est le résultat du calcul suivant :

$$\begin{aligned}
\nabla\Big(\ell_V^\iota(\mathcal{A})\Big) &= \Big[d_v \nabla\big(\ln A_v[V]\big)\Big]_{v \in \mathfrak{V}_\infty} \\
&= \left[d_v \sum_{q \in \breve{\lambda}} \nabla \ln\big(\text{dét}\,(X_q^{\sigma_v\prime} A_v X_q^{\sigma_v})\big)\right]_{v \in \mathfrak{V}_\infty} \\
&= \left[d_v \sum_{q \in \breve{\lambda}} \Big(A_v X_q^{\sigma_v} \left(X_q^{\sigma_v\prime} A_v X_q^{\sigma_v}\right)^{-1} X_q^{\sigma_j\prime} A_v - \frac{q}{n} A_v\Big)\right]_{v \in \mathfrak{V}_\infty} .
\end{aligned}$$

Appelons $p_{A,X}$, ou simplement p_X si $A = \mathrm{I}_n$, l'endomorphisme $p_{A,X} = X(X'AX)^{-1}X'A$. Il s'agit en vérité de la projection A-orthogonale sur l'espace engendré par les vecteurs colonnes de X.

Lemme 3.15. — *Le gradient des fonctions longueur s'exprime encore par la formule suivant :*

$$\nabla\Big(\ell_V^\iota(\mathcal{A})\Big) = \left[d_v A_v \left(\sum_{q \in \breve{\lambda}} p_{A_v, X_q^{\sigma_v}} - \frac{|\lambda|}{n}\mathrm{I}_n\right)\right]_{v \in \mathfrak{V}_\infty} . \tag{3.15}$$

En particulier, la norme des gradients peut être calculée aisément :

$$\begin{aligned}
\left\|\nabla\Big(\ell_V^\iota(\mathcal{A})\Big)\right\| &= \sum_{v \in \mathfrak{V}_\infty} d_v^2 \,\mathrm{Tr}\left(\sum_{q \in \breve{\lambda}} p_{A_v, X_q^{\sigma_v}} - \frac{|\lambda|}{n}\mathrm{I}_n\right)^2 \\
&= (r_1 + 4r_2)\left(\sum_{l=1}^{s}\left(1 + 2(l-1) - \frac{|\lambda|}{n}\right)\breve{\lambda}_l + \left(\frac{|\lambda|}{n}\right)^2\right).
\end{aligned}$$

La norme du gradient est constante, indépendante de la fonction longueur considérée.

Définition 3.16. — Soit $\mathcal{A} = (A_v)_{v \in \mathfrak{V}_\infty} \in \mathcal{P}_n(k)$ une forme d'Humbert, on note $\mathscr{S}(\mathcal{A})$ l'ensemble des paramètres $\varsigma = (\iota, V)$ qui accomplissent le minimum de $\ell_V^\iota(\mathcal{A})$.

Lemme 3.17. — *Une forme d'Hermite–Humbert $\mathcal{A} = (A_v)_{v \in \mathfrak{V}_\infty}$ étant donnée, il n'existe qu'un nombre fini de fonctions longueur distinctes qui réalisent le minimum de $\mathcal{A}$.*

Preuve. — En effet, on a vu à la section 3.2.2, qu'en décomposant $\mathcal{A}$ en $\mathcal{A} = (g'g)$, il est possible de représenter $\frac{\mathcal{A}[V]}{\mathcal{N}(\mathfrak{A}_V^\iota)^2 \mathcal{N}(\mathfrak{a}_\iota)^{\frac{m}{n}}}$ par $H(g\lambda_\iota V)$. L'application $X \mapsto H(g\lambda_\iota X)$ définit encore une hauteur. La propriété de Northcott (*cf.* théorème 2.65), affirme qu'il n'existe qu'un nombre fini de points de hauteur bornée. □

Ce résultat de finitude, associé au calcul de la norme du gradient précédent, garantit la finitude locale de l'ensemble des fonctions longueur servant à définir l'invariant d'Hermite (cf remarque 1.1 de [Bav05]). Cette observation est indispensable pour utiliser la théorie de Ch. Bavard.

En suivant [Bav97], nous posons les définitions suivantes.

Définition 3.18. — On dit qu'une forme d'Hermite-Humbert $\mathcal{A} \in \mathcal{P}_n(k)$ est *parfaite* relativement à λ si la famille des gradients $\left(\nabla \ell_V^\iota\right)_{\varsigma=(\iota,V)\in\mathscr{S}(\mathcal{A})}$ engendre affinement l'espace tangent $\mathrm{T}_{\mathcal{A}}\mathcal{P}_n(k)$.
On dit qu'une forme d'Hermite-Humbert $\mathcal{A} \in \mathcal{P}_n(k)$ est *eutactique* relativement à λ si le vecteur nul appartient à l'intérieur affine de l'enveloppe convexe de la famille des gradients $\left(\nabla \ell_V^\iota\right)_{\varsigma=(\iota,V)\in\mathscr{S}(\mathcal{A})}$.
On dit qu'une forme d'Hermite-Humbert $\mathcal{A} \in \mathcal{P}_n(k)$ est *extrême* relativement à λ si elle réalise un maximum local de l'invariant d'Hermite des formes d'Hermite-Humbert.

Remarque 3.19. — Si l'on note $\Pi_{\mathcal{A},X} = \left[\sum_{q\in\check{\lambda}} p_{A_v, X_q^{\sigma_v}}\right]_{v\in\mathfrak{V}_\infty}$ la somme des projections, la perfection et l'eutaxie peuvent se reformuler comme suit :

- Une forme d'Hermite-Humbert est parfaite si et seulement si le rang au sens d'espaces vectoriels réels de la famille $(\Pi_{\mathcal{A},U})_{U\in\mathscr{S}(\mathcal{A})}$ est égal à la dimension de l'espace tangent $\mathrm{T}_{\mathcal{A}}\mathcal{P}_n(k)$ augmentée d'une unité :

$$\dim_{\mathbb{R}} \mathrm{T}_{\mathcal{A}}\mathcal{P}_n(k) + 1 = \frac{r_1 n(n+1)}{2} + r_2 n^2 - r + 1.$$

- Une forme d'Hermite-Humbert $\mathcal{A} = g'g$ est eutactique si et seulement si l'application identité $\mathcal{I} = (\mathrm{I}_n)_{v\in\mathfrak{V}}$ est une combinaison linéaire à coefficients tous strictement positifs des applications somme de projection $(\Pi_{\mathcal{I},gU})_{U\in\mathscr{S}(\mathcal{A})}$.

Preuve. — La reformulation de la perfection provient du fait d'algèbre linéaire suivant. Soit E un $\mathbb{R}$-espace vectoriel, $H \subset E$ un hyperplan et u un vecteur supplémentaire à H, alors la famille h_i engendre affinement H si et seulement si la famille $h_i + u$ engendre vectoriellement E.
Pour l'eutaxie, par définition la forme $\mathcal{A}$ est eutactique s'il existe des coefficients $(\rho_\varsigma)_{\varsigma\in S(\mathcal{A})}$ strictement positifs et de somme égale à 1 tels que

$$0 = \sum_{\varsigma=(V,\iota)\in\mathscr{S}(\mathcal{A})} \rho_\varsigma \nabla \ell_V^\iota,$$

ce qui équivaut à

$$\left[\sum_{\varsigma\in\mathscr{S}(\mathcal{A})} \rho_\varsigma\, d_v \left(\sum_{q\in\check{\lambda}} A_v X_q \left(X_q{}' A_v X_q\right)^{-1} X_q{}' A_v\right)\right]_{v\in\mathfrak{V}_\infty} = \left[\frac{|\lambda|}{n} A_v\right]_{v\in\mathfrak{V}_\infty}.$$

En utilisant la décomposition $A_v = g_v{}' g_v$, on obtient,

$$\left[\sum_{\varsigma\in\mathscr{S}(\mathcal{A})} \rho_\varsigma\, d_v\, g_v{}' \Pi_{\mathrm{I}_n, g_v X} g_v\right]_{v\in\mathfrak{V}_\infty} = \left[\frac{|\lambda|}{n} g_v{}' g_v\right]_{v\in\mathfrak{V}_\infty}.$$

D'où,

$$\left[\sum_{\varsigma\in S(\mathcal{A})} \rho_\varsigma\, \frac{n}{|\lambda|}\, d_v\, \Pi_{\mathrm{I}_n, g_v X}\right]_{v\in\mathfrak{V}_\infty} = \left[\mathrm{I}_n\right]_{v\in\mathfrak{V}_\infty}.$$

□

Remarque 3.20. — Les notions de perfection et d'eutaxie introduites correspondent avec les notions déjà définies par ailleurs, notamment dans [Cou96] ou [Cou01].

3.3.2 Un théorème à la Voronoï

Théorème 3.21. — *Pour qu'une forme d'Hermite–Humbert soit extrême par rapport à λ, il faut et il suffit qu'elle soit parfaite et eutactique.*

Démonstration. — Il suffit de montrer que la condition $(\mathscr{C})$ est remplie.

Le preuve proposée ici doit beaucoup à celle que l'on trouve au paragraphe 2.11 de [Bav05]. Soit $\mathcal{R} = (R_v)_{v\in\mathfrak{V}_\infty}$ un élément de $\big(\mathbf{SL}_n(\mathbb{R})\big)^{r_1} \times \big(\mathbf{SL}_n(\mathbb{C})\big)^{r_2}$. L'action de l'application $\Phi_{\mathcal{R}}$ sur l'espace des formes de Humbert $\mathcal{P}_n(k)$ définie pour une forme $\mathcal{A} = (A_v)_{v\in\mathfrak{V}_\infty}$ par

$$\Phi_{\mathcal{R}}\Big(\mathcal{A}\Big) = \Big(R_v{}' A_v R_v\Big)_{v\in\mathfrak{V}_\infty}$$

est isométrique et transitive. Elle permet de se relocaliser dans un voisinage de l'identité $\mathcal{I} = (\mathrm{I}_n)_{v\in\mathfrak{V}}$.

Soit $\mathscr{T}$ un sous-ensemble fini de $\mathscr{S}(\mathcal{I})$, dont nous choisissons des représentants sous forme de matrices $n \times \check{s}$ de rang $\check{s}$ et dont les colonnes successives décrivent les drapeaux. Soient $\mathcal{X}$ et $\mathcal{Y}$ deux vecteurs de l'espace tangent $\mathrm{T}_{\mathcal{I}}\mathcal{P}_n(k)$, tels que $\mathcal{X}$ satisfait aux conditions d'orthogonalités avec les éléments de $\mathscr{T}$.

On considère la courbe

$$c(t) = \exp(t\mathcal{X} + t^2\mathcal{Y}^2/2)$$

et on pose $f_V^\iota = \ell_V^\iota \circ c$ ($V \in \mathscr{T}$ et $1 \leqslant \iota \leqslant h$). Pour prouver la conditon $\mathscr{C}$, nous avons besoin de développer $f_V^\iota(t)$ jusqu'à l'ordre 4. La relation $f_V^\iota{}'(0) = 0$, exprime la condition d'orthogonalité sur $\mathcal{X}$, et on calcule que

$$f_V^\iota{}''(0) = \sum_{v\in\mathfrak{V}_\infty} d_v \left(\sum_{q\in\check{\lambda}} \mathrm{Tr}\big(p_{V[q]^{\sigma_v}} Y_v\big) + \mathrm{Tr}\big(p_{V[q]^{\sigma_v}} X_v^2\big) - \mathrm{Tr}\big(\,(p_{V[q]^{\sigma_v}} X_v)^2\,\big)\right).$$

Rappelons que la notation p_V renvoie à la matrice de projection $V(V'V)^{-1}V'$ et que $V[q]$ est la matrice $n \times q$ obtenue en extrayant les q premières colonnes de V. On peut vérifier que pour toute matrice symétrique Z,

$$\mathrm{Tr}\big((p_V Z)^2\big) \leqslant \mathrm{Tr}\big(p_V Z^2\big)$$

avec égalité si et seulement si Z commute avec P_V. On définit donc le sous-ensemble $\mathscr{T}_0 \subset \mathscr{T}$ des paramètres $U \in \mathscr{T}$ tels que pour toute place $v \in \mathfrak{V}_\infty$ et tout indice compris entre 1 et s, la commutation

$$p_{U[\lambda_l^*]^{\sigma_v}} X_v = X_v p_{U[\check{\lambda}_l]^{\sigma_v}}$$

ait lieu ainsi que $\mathscr{T}_1 = \mathscr{T} \smallsetminus \mathscr{T}_0$ son complémentaire. Pour U dans $\mathscr{T}_0$, la dérivée tierce ${f_U^\iota}^{(3)}(0)$ s'évanouit et l'expression de la dérivée quatrième est

$${f_U^\iota}^{(4)}(0) = \sum_{v \in \mathfrak{V}_\infty} d_v \left(\sum_{q \in \check{\lambda}} \mathrm{Tr}\big(p_{U[q]^{\sigma_v}} Y_v^2\big) - \mathrm{Tr}\big(\,(p_{U[q]^{\sigma_v}} Y_v)^2\,\big) \right).$$

Ces calculs découlent facilement du calcul du développement de dét $(U'AU)$ par Christophe Bavard [Bav97] p 111 et de l'identité suivante

$$\ln\left(1 + \beta\frac{t^2}{2} + \delta\frac{t^4}{24}\right) = \beta\frac{t^2}{2} + (\delta - 3\beta^2)\frac{t^4}{24} + o(t^4).$$

Nous cherchons un r-upplet de matrices $\mathcal{Y} = (Y_v)_{v \in \mathfrak{V}_\infty}$ telles que pour $U \in \mathscr{T}_1$, ${f_U^\iota}''(0) > 0$ et pour $U \in \mathscr{T}_0$, ${f_U^\iota}''(0) = 0$ et ${f_U^\iota}^{(4)}(0) > 0$. Les premières conditions portant sur $U \in \mathscr{T}_1$ pourront toujours être satisfaites pour peu que l'on remplace $\mathcal{Y}$ par $\varepsilon\mathcal{Y}$ où ε est un coefficient strictement positif assez petit. Les secondes conditions portant sur $U \in \mathscr{T}_0$ sont équivalentes à $\sum_{v \in \mathfrak{V}_\infty} \mathrm{Tr}\big(p_{V[q]^{\sigma_v}} Y_v\big) = 0$ et il existe (v_0, ℓ_0) tels que $p_{U[\check{\lambda}_l]^{\sigma_v}}$ et Y_v ne commutent pas. Le même argument utilisé pour construire Y dans la preuve de la proposition 2.8 de [Bav97] s'applique ici, pour n'importe quel couple d'indices (v_0, ℓ_0), ce qui fournit une matrice Y_{v_0}. Pour les autres indices $v \neq v_0$, on peut choisir $Y_v = 0$ par exemple. □

3.3.3 Algébricité de la constante

Proposition 3.22. — *1. Étant donné un entier n, une partition λ et un corps de nombre k, les formes parfaites relativement à ces paramètres n'existent qu'en nombre fini à transformation unimodulaire près.*

2. La constante d'Hermite est toujours algébrique.

Démonstration. — 2. La propriété d'algébricité est un fait général qui a été mentionné dans [Bav05]. La justification est la suivante. La perfection d'une forme d'Hermite–Humbert $\mathcal{A}$ signifie que la sous-variété algébrique $\mathcal{C}_{\mathscr{S}(\mathcal{A})}$ définie par les équations polynomiales $\ell_V^\iota(\mathcal{X}) = 0$ pour $(\iota, V) \in \mathscr{S}(\mathcal{A})$ est de dimension zéro. Ainsi, les équations définissant $\mathcal{C}_{\mathscr{S}(\mathcal{A})}$ étant toutes polynomiales à coefficients rationnels, les points de $\mathcal{C}_{\mathscr{S}(\mathcal{A})}$ sont tous algébriques et en particulier $\mathcal{A}$ est algébrique.

1. À présent, pour démontrer qu'il n'y a qu'un nombre fini de formes parfaites à transformation unimodulaire près, nous démontrons qu'il existe un ensemble fini S_0 au sein duquel demeurent toujours les drapeaux minimaux d'un certain représentant de chaque classe de formes parfaites. Par suite, les systèmes d'équations $\ell_V^\iota(\mathcal{X})$, où (V, ι) appartient à S_0, qui définissent une forme parfaite ne peuvent se rencontrer qu'en nombre fini.

D'après la théorie de réduction d'Humbert [Hum49], une forme d'Humbert $\mathcal{A}$ peut toujours se réécrire, à une équivalence unimodulaire près, sous la forme $\mathcal{A} = (D_v[U_v])_{v\in\mathfrak{V}}$ où les matrices $(D_v)_{v\in\mathfrak{V}_\infty}$ sont des matrices diagonales dont les coefficients consécutifs $d_v(i)$ et $d_v(i+1)$ en $i^{\text{ème}}$ et $i+1^{\text{ème}}$ position respectent l'inégalité $\frac{d_v(i)}{d_v(i+1)} \leqslant B$ pour une certaine borne B strictement positive et telle que les matrices $(U_v)_{v\in\mathfrak{V}_\infty}$ sont des matrices unipotentes triangulaires supérieures à coefficients bornés également.

Rappelons que la hauteur locale d'un vecteur drapeau $V \in \mathbb{S}^\lambda_\sharp(k_v^n)$ est simplement le carré de la norme $A_v[V] = \|\pi_\lambda(D_vU_v)V\|^2$ où $\|\cdot\|$ est la norme définie sur $\mathbb{S}^\lambda(k_v^n)$. Comme $\pi(D_vU_v)$ est inversible, on obtient, en utilisant la norme d'opérateur,

$$\forall V \in \mathbb{S}^\lambda(k_v^n), \quad A_v[V] \geqslant \left\|\pi_\lambda(D_vU_v)^{-1}\right\|^{-1} \|V\|^2 .$$

Comme U_v est triangulaire et unipotente, les coefficients de $\pi_\lambda(U_v^{-1})$ sont polynomiaux en les coefficients de U_v et $\left\|\pi_\lambda(U_v^{-1})\right\|$ peut être uniformément borné sur l'ensemble des formes de Humbert réduites que nous examinons. D'autre part, $\pi_\lambda(D_v^{-1})$ est un endomorphisme diagonal dont les valeurs propres associées au vecteur e_T sont simplement $\prod_{i=1}^n d_v(i)^{-\sharp\{i\,;\,i\in T\}}$. En utilisant les bornes sur les quotients de coefficients $d_v(i)$ consécutifs, on peut s'assurer que les valeurs propres de $\pi_\lambda(D_v^{-1})$ sont majorées par un certain $B^\mu \prod_{i=1}^n d_v(i)^{-\lambda_i} = B^\mu \chi_\lambda(d_v^{-1})$ pour une certaine puissance μ de B suffisamment grande. Ainsi il existe une constante θ telle que pour toute forme de Humbert $\mathcal{A}$ réduite :

$$\forall V \in \mathbb{S}^\lambda(k_v^n), \quad A_v[V] \geqslant \theta \ \|V\|^2 .$$

On en déduit que les vecteurs drapeaux minimaux V d'une forme de Humbert réduite ont une hauteur bornée : les hauteurs locales archimédiennes sont majorées par exemple par θ^{-r} tandis que les hauteurs locales ultramétriques sont toujours inférieures à 1. Selon la propriété de Northcott, ils ne peuvent former qu'un ensemble fini, ce qui achève la preuve. $\square$

Des machines à calculer, les hommes ne sont rien d'autre. — T. Bernhard « Perturbation »

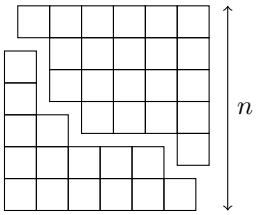
Inégalités et calculs exacts | 4

4.1 Relations entre les constantes

Cette partie explore les liens qui peuvent être assez immédiatement établis entre les constantes correspondant à différents paramètres. Ils généralisent des résultats connus et que l'on obtient facilement dans le cadre classique.

4.1.1 Une égalité de dualité

Si λ est une partition à moins de n parts, on appelle partition complémentaire par rapport à n la partition $\overline{\lambda}$ (notée aussi éventuellement $\overline{\lambda}^n$) telle que pour tout ℓ entre 1 et s, $\breve{\lambda}_\ell + \breve{\overline{\lambda}}_{s+1-\ell} = n$. Visuellement, elle s'obtient en complétant la partition en un rectangle de hauteur n :



Proposition 4.1. — *Soit λ une partition et $\overline{\lambda}^n$ sa partition complémentaire par rapport à n, alors l'égalité suivante est vérifiée*

$$\gamma_{n,\lambda} = \gamma_{n,\overline{\lambda}^n}. \tag{4.1}$$

Démonstration. — Une partition λ étant fixée, nous considérons la représentation suivante $(\mathbb{S}^\lambda(k^n), \rho)$ où $\rho = \pi_\lambda(w_0 g'^{-1} w_0^{-1})$ et w_0 est l'automorphisme miroir de $\mathbf{GL}_n(k)$ qui échange les vecteurs e_i et e_{n+1-i}. Nous pouvons observer que ρ est une représentation irréductible, que $e_{U(\lambda)}$ dirige la droite des vecteurs de plus haut poids, que $e_{U(\lambda)}$ admet pour stabilisateur le sous-groupe parabolique $P_{\overline{\lambda}}$. Le caractère de ρ est en réalité dét $^{-n} \cdot \chi_{\overline{\lambda}}$.

Compte tenu de nos normalisations $H\left(e_{U(\lambda)}\right) = H\left(e_{U(\overline{\lambda})}\right) = 1$, lorsque $g \in \mathbf{GL}_n^1(k_\mathbb{A})$. En décomposant g sous la forme $g = kdu$ avec k appartenant au groupe compact maximal $K(k_\mathbb{A})$, d matrice diagonale et u unipotente, nous

obtenons encore

$$H\left(\rho(g)e_{U(\lambda)}\right) = |\chi_{\overline{\lambda}}(d)|_{k_{\mathbb{A}}} = H\left(\pi_{\overline{\lambda}}(g)e_{U(\overline{\lambda})}\right).$$

De cette égalité provient l'égalité des constantes $\gamma_{n,\lambda} = \gamma_{n,\overline{\lambda}^n}$. □

4.1.2 L'inégalité de Mordell

Avec le point de vue des hauteurs tordues en tête, nous pouvons prouver l'inégalité suivante, qui généralise l'inégalité de Mordell.

Proposition 4.2. — *Soient λ une partition, m et n deux entiers tels que $\check{s} \leqslant m \leqslant n$, alors,*

$$\gamma_{n,\lambda} \leqslant \gamma_{m,\lambda}\left(\gamma_{n,m}\right)^{|\lambda|/m}. \tag{4.2}$$

Démonstration. — Donnons-nous un automorphisme A vérifiant $\|\text{dét}\,(A)\|_{k_{\mathbb{A}}} = 1$. Soit Δ un drapeau de k^n qui minimise la hauteur tordue $H_A(\Delta)$ et soit W un sous-espace de dimension m tel que $H_A(W) \leqslant \gamma_{m,n}^{1/2}$. Il existe une application injective ϕ qui envoie k^m sur $W \subset k^n$ surjectivement. Admettons un temps la validité du lemme suivant, qui sera démontré plus loin. (Ce lemme et sa preuve se déduisent aisément du corollaire 4.3 de [RT96] où ce résultat est établi dans le cas des puissances symétriques et extérieures uniquement).

Lemme 4.3. — *Soient $\phi : k^m \hookrightarrow k^n$ une application injective et A un automorphisme de $\mathbf{GL}_n(k_{\mathbb{A}})$. On désignera encore par ϕ le $k_{\mathbb{A}}$-homomorphisme qui étend ϕ entre ${k_{\mathbb{A}}}^m$ et ${k_{\mathbb{A}}}^n$. Il existe alors un automorphisme $B \in \mathbf{GL}_m(k_{\mathbb{A}})$ tel que la hauteur tordue $H_B(\cdot)$ coïncide avec la hauteur tordue $H_A(\cdot)$ dans le sens suivant : pour toute partition λ et tout drapeau Δ de forme λ de sous-espaces emboîtés dans k^m, on a*

$$H_A(\phi(\Delta)) = H_B(\Delta). \tag{4.3}$$

En particulier, lorsque λ est la partition de m verticale $\lambda = \begin{smallmatrix}\square\\ \square\\ \square\end{smallmatrix}$ et si W désigne l'image de ϕ, on obtient

$$H_A(W) = |\text{dét}\,(B)|_{k_{\mathbb{A}}}. \tag{4.4}$$

Fixons désormais un automorphisme $B \in \mathbf{GL}_m(k)$ jouissant des propriétés du lemme.

Il existe par ailleurs un drapeau Δ' de k^m tel que

$$H_B(\Delta') \leqslant \gamma_{m,\lambda}^{1/2}\,|\text{dét}\,(B)|_{k_{\mathbb{A}}}^{|\lambda|/m} = \gamma_{m,\lambda}^{1/2} H_A(W)^{|\lambda|/m} \leqslant \gamma_{m,\lambda}^{1/2}\gamma_{n,m}^{|\lambda|/2m}.$$

Alors,

$$H_A(\Delta) \leqslant H_A(\phi(\Delta')) = H_B(\Delta') \leqslant \gamma_{m,\lambda}^{1/2}\gamma_{n,m}^{|\lambda|/2m}$$

ce qui achève la preuve de la proposition. □

Preuve. — Commençons par construire des autormophismes $B_v \in \mathbf{GL}_n(k_v)$ pour toute place v tel que $A_v \circ \phi \circ B_v^{-1}$ préserve la norme. À cette fin, si v est une place archimédienne, nous considérons les antécédents d'une famille de m vecteurs A_v-orthonormaux de k_v^n et prenons pour B_v, l'automorphisme qui envoie la base canonique de k_v^m sur ces vecteurs. Lorsque v est une place ultramétrique, il

faut et il suffit pour que la norme soit préservée que $A_v \circ \phi \circ B_v^{-1}$ envoie $\mathfrak{o}_v^m$ sur un $\mathfrak{o}_v$-module de rang m primitif dans $\mathfrak{o}_v^n$. Nous choisissons B_v tel que $B_v(\mathfrak{o}_v^n) = (A_v \circ \phi)^{-1}(\mathfrak{o}_v^n)$.

Remarquons que pour presque toute place finie, $A_v \circ \phi$ est déjà une isométrie, et que l'on peut se contenter de choisir $B_v = \mathrm{I}_n$. Ceci nous assure que $B = (B_v)_{v \in \mathfrak{V}}$ est bien un élément de $\mathbf{GL}_m(k_{\mathbb{A}})$ et ainsi

$$\forall x \in k^m, \quad H_A(\phi(x)) = H_B(x).$$

Montrons que cette égalité s'étend aux drapeaux de toute forme. Nous pouvons décomposer chaque application $A_v \circ \phi \circ B_v^{-1}$ en une composition $\psi_v \circ \mathscr{I}$, où $\mathscr{I}$ est l'injection $k^m \hookrightarrow k^n$ donnée par ajout de zéros par $(x_1, \ldots, x_m) \mapsto (x_1, \ldots, x_m, 0, \ldots, 0)$ et ψ_v est une isométrie. Alors, l'application

$$\mathbb{S}^\lambda\left(A_v \circ \phi \circ B_v^{-1}\right) = \pi_\lambda(\psi_v) \circ \mathbb{S}^\lambda(\mathscr{I})$$

est une injection isométrique de k_v^m dans k_v^n car, d'une part, ψ_v est une isométrie et par construction nos hauteurs locales sont invariantes sous l'action d'une isométrie et, d'autre part, l'injection $\mathbb{S}^\lambda(\mathscr{I})$ est une isométrie. Ainsi pour toute partition λ et tout drapeau Δ de forme λ,

$$H_A(\phi(\Delta)) = H_B(\Delta).$$

□

4.1.3 Des inégalités avec la constante de Bergé–Martinet

4.1.3.1 Définition de la constante de Bergé–Martinet

Rappelons que la constante de Bergé–Martinet désigne pour un réseau le maximum du produit du minimum d'un réseau par le minimum du réseau dual. En termes adèliques, ceci s'écrit comme suit.

Définition 4.4. — Étant donné un entier n, une partition λ de profondeur inférieure à n et un corps de nombre k, on appelle *constante de Bergé–Martinet* la constante

$$\gamma'_{n,\lambda} = \max_{g \in \mathbf{GL}_n(k_{\mathbb{A}})} \left(\min_{\gamma \in \mathbf{GL}_n(k)} H\left(\pi_\lambda(g\gamma) e_{U(\lambda)}\right) \min_{\gamma \in \mathbf{GL}_n(k)} H\left(\pi_\lambda(g'^{-1}\gamma) e_{U(\lambda)}\right) \right). \tag{4.5}$$

Bien entendu, il est avéré pour toute partition λ que $\gamma'_{n,\lambda} \leqslant \gamma_{n,\lambda}$.

4.1.3.2 Constante de Bergé–Martinet et partition autocomplémentaire

Par ailleurs, on peut démontrer le proposition suivante.

Proposition 4.5. — *Soit κ la partition* $\begin{smallmatrix}\square\\ \square\square\end{smallmatrix}$ *de degré n , alors $\gamma'^2_{n,\square} \leqslant \gamma_{n,\kappa}$.*

Démonstration. — Notons $g^c = w_0 g' w_0^{-1}$ où w_0 est l'automorphisme miroir qui échange les vecteurs e_i et e_{n+1-i}. On peut remarquer que lorsque g est un automorphisme diagonal $g = (d_1, \ldots, g_n) \in \mathbf{GL}_n(k_{\mathbb{A}})$, on a l'égalité

$$H(g \cdot e_1) H(g^c \cdot e_1) = H(d_1 e_1) H\left(d_1^{-1} e_1\right) = |d_1 \cdot d_1 \cdots d_{n-1}|_{k_{\mathbb{A}}}$$

puisque $|\text{dét}\, g|_{k_{\mathbb{A}}} = 1$. Il s'en suit par conséquent que $H(g \cdot e_1) H(g^c \cdot e_1) = H\left(\pi_\kappa(g) e_{U(\kappa)}\right)$ pour toute matrice diagonale.

L'égalité est évidemment satisfaite pour toute matrice triangulaire supérieure unipotente, puisque tous les termes valent un, et s'étend sans peine à tout élément $g \in \mathbf{GL}_n(k_{\mathbb{A}})$.

Dès lors, pour tout élément g de $\mathbf{GL}_n(k_{\mathbb{A}})$,

$$\min_{\gamma \in \mathbf{GL}_n(k)} H(g\gamma \cdot e_1) \min_{\gamma \in \mathbf{GL}_n(k)} H\left(g'^{-1}\gamma \cdot e_1\right) \leqslant \min_{\gamma \in \mathbf{GL}_n(k)} H(g\gamma \cdot e_1) H(g^c\gamma \cdot e_1).$$

Aussi

$$\min_{\gamma \in \mathbf{GL}_n(k)} H(g\gamma \cdot e_1) \min_{\gamma \in \mathbf{GL}_n(k)} H\left(g'^{-1}\gamma \cdot e_1\right) = \min_{\gamma \in \mathbf{GL}_n(k)} H\left(\pi_\kappa(g\gamma) e_{U(\kappa)}\right)$$

ce qui conduit aussitôt à l'inégalité que l'on convoitait. □

4.1.3.3 Généralisation d'inégalités classiques

Cette partie généralise au cas d'un corps de nombre quelconque les inégalités de Bergé-Martinet que l'on peut trouver par exemple au chapitre 2.8 de [Mar03] et qui ont été initialement démontrées dans [BM89].

Nous noterons dans ce qui suit $\check{A}$ l'objet A'^{-1} pour tout objet A inversible et transposable. Par ailleurs, nous noterons simplement $\gamma'_{n,p}(k)$ ou même $\gamma'_{n,p}$ la constante de Bergé-Martinet sur le corps de nombre p associée à la partition $\lambda = \ydiagram{1,1,1}$ comportant p boîtes.

Lemme 4.6. — *Soit $A \in \mathbf{GL}_n(k_{\mathbb{A}})$ un automorphisme, Δ un drapeau sur k^n de forme λ et $\Delta^\perp$ le drapeau complémentaire formé des sous-espaces orthogonaux aux espaces de Δ (au sens de la forme bilinéaire canonique sur k^n), alors*

$$H_A(\Delta) = |\text{dét}\, A|_{k_{\mathbb{A}}}^s H_{\check{A}}\left(\Delta^\perp\right), \tag{4.6}$$

où rappelons que $s = \lfloor \check{\lambda} \rfloor$.

Preuve. — Il s'agit d'une version revisitée du théorème de dualité de [Thu93]. □

Lemme 4.7. — *Soient des entiers n, q et p tels que $n = q + p$. Soit $A \in \mathbf{GL}_n(k_{\mathbb{A}})$ un automorphisme et soit V un sous-espace de k^n de dimension p. Notons $V^\perp$ l'orthogonal de V pour la forme bilinéaire canonique de k^n. Alors il existe un automorphisme $\tilde{A}$ tel que pour tout sous-espace W de l'orthogonal $V^\perp$*

$$H_A(V \oplus W) = H_A(V) \cdot H_{\tilde{A}}(W). \tag{4.7}$$

De plus, il existe un plongement ϕ de k^q dans $V^\perp$ et un automorphisme B de $\mathbf{GL}_q(k_{\mathbb{A}})$ tel que $H_{\check{A}}(\phi(W_0)) = H_B(W_0)$ pour tout sous-espace W_0 de k^q et tel que $H_{\tilde{A}}(\phi(W_0)) = H_{\check{B}}(W_0)$.

Remarque 4.8. — La première partie de ce lemme connaît plusieurs avatars dans la littérature et est utilisée fréquemment (voir [Thu93] ou [BV93]). Ce résultat exprime en version adélique la proposition 1.3.4 de [Mar03] portant sur la projection de réseaux euclidiens sur un sous-espace.

Preuve. — Quitte à opérer un changement de base et à tordre A et B *in fine*, on peut supposer que V est l'espace engendré par les p premiers vecteurs $(e_i)_{1\leqslant i\leqslant p}$ de la base canonique et $V^\perp$ est engendré par les q derniers. De plus, l'isomorphisme ϕ peut tout simplement associer e_i à e_{i+p}.

En décomposant A sous la forme kdu où d est une matrice diagonale et u une matrice unipotente supérieure, on considère alors par exemple $\tilde{A} = d\tilde{u}$ où $\tilde{u}$ est la matrice u dont on a extirpé le bloc supérieur droit de taille $p\times q$, autrement dit la matrice dont les q derniers vecteurs colonnes ont été projetés sur $V^\perp$. Puisque u comme $\tilde{u}$ sont unipotentes triangulaires supérieures, les hauteurs $H_A(V\oplus W)$ et $H_{\tilde{A}}(V\oplus W)$ sont égales. De plus comme $\tilde{u}$ conserve V et $V^\perp$, et notamment leur orthogonalité pour toute place locale[1], on a l'égalité $H_{\tilde{A}}(V\oplus W) = H_{\tilde{A}}(V)\cdot H_{\tilde{A}}(W)$ qui devient encore

$$H_A(V\oplus W) = H_A(V)\cdot H_{\tilde{A}}(W)$$

Pour le choix de B, il suffit de considérer la matrice $q\times q$ extraite en bas à droite de $\check{d}\check{u}$ et de remarquer que comme du est triangulaire par bloc, B coïncide aussi avec le bloc en position basse à droite de $\tilde{A}$. □

Notons dans ce qui suit $d_\lambda(A) = \min_{\gamma\in\mathbf{GL}_n(k)} H_A\left(\gamma\cdot e_{U(\lambda)}\right)$ pour toute partition λ. Le lemme qui précède implique en particulier que $d_\lambda(A) = d_{\overline{\lambda}^n}(\check{A})\,|\text{dét}\,A|^s_{k_\mathbb{A}}$.

Lemme 4.9. — *Soit $A\in\mathbf{GL}_n(k_\mathbb{A})$ un automorphisme et soient des entiers h et p tels que $0<h<p\leqslant n$, alors*

$$d_p(A) \leqslant \left(\gamma'_{n-h,p-h}(k)\right)^2 d_h(A)\left(d_{p-h}\left(\check{A}\right)\right)^{-1}. \tag{4.8}$$

Preuve. — On commence par sélectionner un sous-espace W de k^n de dimension h tel que $H_A(H) = d_h(A)$. On construit conformément au lemme 4.7 un automorphisme $\tilde{A}\in\mathbf{GL}_n(k_\mathbb{A})$, une injection $\phi : k^{n-h}\to W^\perp$ et un automorphisme $B\in\mathbf{GL}_{n-h}(k_\mathbb{A})$. Il existe un sous-espace U_0 de k^{n-h} de dimension $p-h$ particulier tel que $H_{\check{B}}(U_0) = d_{p-h}(\check{B})$. Alors

$$\begin{aligned} H_{\check{B}}(U_0) &= d_{p-h}(\check{B})d_{p-h}(B)\left(d_{p-h}(B)\right)^{-1} \\ &\leqslant (\gamma'_{n-h,p-h})^2\left(d_{p-h}(B)\right)^{-1}. \end{aligned}$$

Mais comme $H_{\check{A}}(\phi(W_0)) = H_B(W_0)$, on a encore $d_{p-h}(B)\geqslant d_{p-h}(\check{A})$, donc

$$H_{\check{B}}(U_0)\leqslant(\gamma'_{n-h,p-h})^2\left(d_{p-h}(\check{A})\right)^{-1}.$$

Notons $U=\phi(U_0)$, on a alors

$$\begin{aligned} d_p(A) &\leqslant H_A(W\oplus U) = H_A(W)\,H_{\tilde{A}}(U) = H_A(W)\,H_{\check{B}}(U_0) \\ &\leqslant d_h(A)(\gamma'_{n-h,p-h})^2\left(d_{p-h}(\check{A})\right)^{-1}. \end{aligned}$$

Ceci conclut la preuve. □

Théorème 4.10. — *Soient des entiers n, p et q tels que $n=p+q$ et $0<p\leqslant\frac{n}{2}$, alors les inégalités suivantes sont vérifiées*

[1] Insistons : orthogonal signifie ici que deux vecteurs a et b sont orthogonaux si $|a+b|_v^2 = |a|_v^2+|b|_v^2$ lorsque v est une place archimédienne et $|a+b|_v = \max(|a|_v, |b|_v)$ lorsque v est une place ultramétrique (*c.f.* [Wei95]).

1. $\left(\gamma_{n,p}(k)\right)^n \leqslant \left(\gamma_{q,p}(k)\right)^q \left(\gamma'_{n,p}(k)\right)^{2p}$,
2. $\gamma'_{n,2p}(k) \leqslant \left(\gamma'_{q,p}(k)\right)^2$.

Démonstration. — Nous démontrons les deux inégalités par des considérations sur les hauteurs tordues.

1. Soit $A \in \mathbf{GL}_n(k_{\mathbb{A}})$ un automorphisme. Il existe alors un sous-espace W de dimension q tel que $H_A(W) = d_q(A)$. D'après le lemme 4.3, une injection ϕ de k^q dans W ainsi qu'un automorphisme B dans $\mathbf{GL}_q(k_{\mathbb{A}})$ tel que pour tout drapeau Δ de k^m, $H_A(\phi(\Delta)) = H_B(\Delta)$ et en particulier $H_A(W) = |\text{dét}\, B|_{k_{\mathbb{A}}}$. On a encore

$$\begin{aligned} |\text{dét}\, B|_{k_{\mathbb{A}}} &= \left(d_q(A)d_q(\check{A})\right)\left(d_q(\check{A})\right)^{-1} \\ &= \left(d_q(A)d_q(\check{A})\right)|\text{dét}\, A|_{k_{\mathbb{A}}}\left(d_p(A)\right)^{-1} \end{aligned}$$

   Soit W' un sous-espace de dimension p de k^m tel que $H_B(W') = d_p(B)$. En notant $W'' = \phi(W')$, il est clair que

$$d_p(A) \leqslant H_A(W'') = H_B(W') = d_p(B). \tag{4.9}$$

   Cependant, par définition de $\gamma_{q,p}$,

$$d_p(B) \leqslant \gamma_{q,p}\,|\text{dét}\, B|_{k_{\mathbb{A}}}^{p/q}.$$

   En réunissant l'ensemble, on obtient

$$d_p(A) \leqslant \gamma_{q,p}\left(\left(d_q(A)d_q(\check{A})\right)|\text{dét}\, A|_{k_{\mathbb{A}}}\left(d_p(A)\right)^{-1}\right)^{p/q}.$$

   L'inégalité attendue en découle en passant à la borne supérieure de part et d'autre.

2. On multiplie l'inégalité du lemme 4.9 appliquée à A et à $\check{A}$ ce qui fournit la nouvelle inégalité suivante

$$\gamma'_{n,p}(A) = d_p(A)d_p(\check{A}) \leqslant {\gamma'_{n-h,p-h}}^2\gamma'_{n,h}(A)\gamma'_{n,p-h}(A)^{-1}.$$

   Les deux derniers termes s'éliminent lorsque l'on choisit $p = 2h = p$.

□

Corollaire 4.11. — *Lorsque n est pair, on a*

$$\gamma_{n,\frac{n}{2}}(k) = \gamma'_{n,\frac{n}{2}}(k). \tag{4.10}$$

Preuve. — En général, on a seulement l'inégalité $\gamma'_{n,\frac{n}{2}} \leqslant \gamma_{n,\frac{n}{2}}$. Cependant, en choisissant $p = q = \frac{n}{2}$, la première inégalité du théorème 4.10 fournit l'inégalité réciproque. □

Corollaire 4.12. — *Pour tout $n' \leqslant \frac{n}{2}$, on a l'inégalité*

$$\gamma_{n,n'}^{n-2n'}(k) \leqslant \gamma_{n-n',n'}^{n-n'}(k). \tag{4.11}$$

Cette inégalité généralise l'inégalité de Mordell que l'on retrouve en choisissant $n' = 1$.

Preuve. — Cette inégalité provient toujours du premier point du théorème 4.10, que l'on combine à l'inégalité $\gamma'_{n,\lambda} \leqslant \gamma_{n,\lambda}$ déjà mentionnée. □

Corollaire 4.13. — *Pour tout entier n, on a l'inégalité*

$$\gamma'_{2n+1,\square}(k) \leqslant \gamma'_{n+1,\square}(k). \tag{4.12}$$

Preuve. — Il suffit d'appliquer le second point du théorème avec $p = 1$. □

Dans le théorème et dans chacun des trois corollaires précédents, remplacer le corps de nombre k par le corps des rationnels $\mathbb{Q}$ permet de retrouver les inégalités classiques (*c.f.* [Mar03]). Rappelons en particulier que $\gamma'_{n,\square}(\mathbb{Q})$ ne désigne rien d'autre que la constante de Bergé-Martinet habituellement notée γ'_n.

4.2 Calculs exacts et approximations

4.2.1 Détermination de quelques constantes sur $\mathbb{Q}$

4.2.1.1 Réinterprétation de la réduction de Korkine et Zolotareff

Nous calculons dans cette partie quelques constantes de la forme $\gamma_{n,(2,1,\check{\ldots},1)}(\mathbb{Q})$ par le biais de la réduction de Korkine et Zolotareff.

Proposition 4.14. — *La constante $\gamma_{3,\boxplus}(\mathbb{Q})$ est égale à $\frac{3}{2}$ et n'est atteinte que pour le réseau de racine $\mathbb{A}_3$ et son dual $\mathbb{A}_3^*$.*

La constante $\gamma_{4,\boxplus}(\mathbb{Q})$ est égale à 2 et n'est atteinte que pour le réseau de racine $\mathbb{D}_4$ (qui est isomorphe à son dual).

n	$\gamma_{n,(2,1,\ldots,1)}(\mathbb{Q})$	Réseau
3	$\frac{3}{2}$	$\mathbb{A}_3$
4	2	$\mathbb{D}_4$
5	$\frac{32}{15} \leqslant \gamma''_5 < \frac{9}{4}$	

Tab. 4.1 – Constantes $\gamma_{n,(2,1,\ldots,1)}(\mathbb{Q})$

Pour les références à la réduction au sens de Korkine-Zolotareff, nous renvoyons à [Mar03] section 2.9 ou à l'article originel [KZ73]. Soit L un réseau de $\mathbb{R}^3$ et Λ_1 un sous-réseau de L dont une section de dimension 2 est minimale. Deux cas peuvent se produire selon qu'il est possible de trouver un sous-réseau Λ_1 contenant ou non un vecteur minimal de L.

1. Dans le premier cas, soit u_1 vecteur minimal jouissant de telles propriétés et soit u_2 un second vecteur de Λ_1 de sorte que (u_1, u_2) en forme une base. Mais alors, u_1, u_2 est le début d'une base de L réduite au sens d'Hermite–Korkine–Zolotareff, disons (u_1, u_2, u_3). Si ce n'était pas le cas, le début d'une autre base HKZ réduite fournirait un meilleur sous-réseau Λ_1. Dans ce cas, en notant A_1 la norme de u_1, A_2 la norme de la projection de u_2 sur l'orthogonal de u_1 et A_3 la norme de la projection de u_3 sur l'orthogonal

de u_1 et u_2, la constante vaut

$$\gamma_{3,\boxplus}(L) = \frac{A_1^2 A_2}{A_1 A_2 A_3} = \frac{A_1}{A_3}.$$

Il a été établi par Korkine et Zolotareff que ce rapport n'excédait jamais $\frac{3}{2}$ et était atteint uniquement lorsque $L = \mathbb{A}_3$ ou $L = \mathbb{A}_3^*$.

2. Le second cas à étudier correspond à la situation où aucun des sous-reséaux Λ_1 de dimension 2 et de déterminant minimal ne contient de vecteur minimal. On peut commencer par considérer une base (u_1, u_2) réduite du réseau Λ_1 et e_m un vecteur minimal de L. Le triplet (u_1, u_2, e_m) forme alors une base de L. En effet, supposons par l'absurde qu'il existe un autre vecteur x de L non contenu dans le réseau engendré par ce triplet. Quitte à opérer quelques réductions, nous pouvons supposer que $\langle x, e_m\rangle \leqslant \frac{1}{2}\|e_m\|$, $\langle x, u_1\rangle \leqslant \frac{1}{2}\|u_1\|$ et $\langle x, u_2\rangle \leqslant \frac{1}{2}\|u_2\|$. Alors le déterminant du réseau $\Lambda_1' = \mathbb{Z}x + \mathbb{Z}u_1$ est majoré par

$$\begin{aligned} \text{dét}\,\Lambda &\leqslant \|x\|^2 \|u_1\|^2 \leqslant (\frac{1}{2}\|e_m\|^2 + \frac{1}{2}\|u_1\|^2 + \frac{1}{2}\|u_2\|^2)\|u_1\|^2 \\ &< \frac{3}{4}\|u_2\|^2 \|u_1\|^2 . \end{aligned}$$

Or les propriétés de réduction de la base u_1, u_2 impliquent que $\text{dét}\,\Lambda_1 \geqslant \frac{3}{4}\|u_2\|^2 \|u_1\|^2$.
Notons A_3 la norme de la projection de e_m sur l'orthogonal de Λ_1. En exprimant que e_m est un vecteur minimal et (u_1, u_2) est une base réduite, il vient la chaîne d'inégalités $\|e_m\|^2 \leqslant \|u_1\|^2 = A_1 \leqslant \frac{4}{3}A_2$. Par ailleurs, en comparant les déterminants des réseaux Λ_1 et $\mathbb{Z}e_m + \mathbb{Z}u_1$, il vient $A_1 A_3 \geqslant A_1 A_2$. Aussi $\|e_m\|^2 \leqslant \frac{4}{3}A_3$. Par conséquent, dans ce second cas

$$\gamma_{3,\boxplus}(L) = \frac{A_1 A_2 \|e_m\|}{A_1 A_2 A_3} \leqslant \frac{4}{3}$$

ce qui est une majoration plus basse que le cas 1.

Mutatis mutandis, si L est un réseau de dimension 4, deux cas se distinguent, selon qu'il existe ou non un sous-réseau Λ_1 de dimension 3 de déterminant minimal contenant un vecteur minimal de L. Dans le premier cas, on peut exhiber une base réduite au sens de Korkine Zolotareff dans laquelle la constante s'exprime

$$\gamma_{4,\boxplus}(L) = \frac{A_1^2 A_2 A_3}{A_1 A_2 A_3 A_4} = \frac{A_1}{A_4}$$

et est majorée par 2 selon les travaux de Korkine et Zolotareff. Cette majoration est atteinte uniquement lorsque $\Lambda = \mathbb{D}_4$.
Dans le second cas, une base de L peut être exhibée en adjoignant un vecteur minimal à une base réduite de Λ_1. Il peut être montré que $\gamma_{4,\boxplus}(L) = \frac{3}{2}$.

Remarque 4.15. — Il appert de ces déterminations que $\gamma_{3,\boxplus}(\mathbb{Q})$ et $\gamma_{4,\boxplus}(\mathbb{Q})$ sont exactement égaux à γ_3' et γ_4' respectivement (cas d'égalité dans la proposition 4.5).
En dimension cinq, l'inégalité devient stricte. Suivons [BM89] et appelons γ_5''

la borne supérieure de la quantité $\frac{A_1}{A_5}$ qui apparaît dans le cas de la réduction de Korkine et Zolotareff d'une forme à plus de cinq variables. La valeur de γ_5'' n'est pas connue mais l'on dispose de l'encadrement $\frac{32}{15} \leqslant \gamma_5'' < \frac{9}{4}$. Il permet de prouver avec le même raisonnement que ci-dessus que $\gamma_{5,\begin{smallmatrix}\square\\\square\square\end{smallmatrix}}(\mathbb{Q}) = \gamma_5''$ alors que la valeur de γ_5' est 2, d'après les calculs de [PY06].

4.2.1.2 Extension des résultats

Rappelons que d'après la proposition 4.2, pour tous entiers $n' \leqslant n$ et toute partition λ de profondeur $\lfloor \lambda \rfloor$ inférieure à n', on a la comparaison suivante

$$\gamma_{n,\lambda} \leqslant \gamma_{n',\lambda} \left(\gamma_{n,n'}\right)^{|\lambda|/n'} . \tag{4.13}$$

Exploitons cette inégalité en utilisant diverses valeurs connues de $\gamma_{n',\lambda}$ et de la constante de Rankin[2] $\gamma_{n,n'}$ [Ran53, SWO08]. Dans bien des cas, l'inégalité obtenue est atteinte ce qui permet de conclure sur la valeur de la constante $\gamma_{n,\lambda}$. Dans d'autres cas, on obtient qu'une borne supérieure.

Proposition 4.16. — *Nous résumons les résultats dans le tableau 4.2 suivant. Les*

$n = 4$	$n = 6$	$n = 8$
$\gamma_{4,\begin{smallmatrix}\square\square\\\square\end{smallmatrix}} = \dfrac{3\sqrt{2}}{2}$	$\gamma_{6,\begin{smallmatrix}\square\square\\\square\square\end{smallmatrix}} = 2\sqrt{3}$	$\gamma_{8,\begin{smallmatrix}\square\square\\\square\square\end{smallmatrix}} = 6$
$\gamma_{4,\begin{smallmatrix}\square\\\square\\\square\end{smallmatrix}} = 2$	$\dfrac{8}{2^{2/3}} \leqslant \gamma_{6,\begin{smallmatrix}\square\\\square\\\square\end{smallmatrix}} \leqslant 2 \cdot 3^{2/3}$	$\gamma_{8,\begin{smallmatrix}\square\\\square\\\square\end{smallmatrix}} = 8$
$\gamma_{4,\begin{smallmatrix}\square\square\square\\\square\end{smallmatrix}} = 3$	$8 \leqslant \gamma_{6,\begin{smallmatrix}\square\square\square\\\square\end{smallmatrix}} \leqslant 9$	$\gamma_{8,\begin{smallmatrix}\square\square\square\\\square\end{smallmatrix}} = 24$

Tab. 4.2 – Quelques constantes généralisées sur $\mathbb{Q}$ de forme quelconque

constantes ainsi calculées sont atteintes sur $\mathbb{D}_4$, $\mathbb{E}_6$ et $\mathbb{E}_8$.

Démonstration. — Voici le détail des calculs justificatifs :

1. On a l'inégalité

$$\gamma_{4,\begin{smallmatrix}\square\square\\\square\end{smallmatrix}} \leqslant \gamma_{3,\begin{smallmatrix}\square\square\\\square\end{smallmatrix}} \left(\gamma_{4,3}\right)^{3/3} = \gamma_{3,\begin{smallmatrix}\square\square\\\square\end{smallmatrix}}\gamma_{4,1} = \frac{3}{2}\sqrt{2}.$$

Or $\gamma_{4,\begin{smallmatrix}\square\square\\\square\end{smallmatrix}}(\mathbb{D}_4) = \frac{3}{2}\sqrt{2}$. Ainsi

$$\gamma_{4,\begin{smallmatrix}\square\square\\\square\end{smallmatrix}} = \frac{3}{2}\sqrt{2}. \tag{4.14}$$

2. On a l'inégalité

$$\gamma_{4,\begin{smallmatrix}\square\square\square\\\square\end{smallmatrix}} \leqslant \gamma_{3,\begin{smallmatrix}\square\square\square\\\square\end{smallmatrix}} \left(\gamma_{4,3}\right)^{6/3} = \gamma_{3,\begin{smallmatrix}\square\square\\\square\end{smallmatrix}}\gamma_{4,1}^2 = \frac{3}{2}\sqrt{2}^2 = 3$$

Mais, comme les sections minimales de rang 1, 2 et 3 de $\mathbb{D}_4$ sont $\mathbb{A}_1$, $\mathbb{A}_2$ et $\mathbb{A}_3$ respectivement et sont emboîtées les unes dans les autres, on en tire $\gamma_{4,\begin{smallmatrix}\square\square\square\\\square\end{smallmatrix}}(\mathbb{D}_4) = \frac{2\cdot 3\cdot 4}{4^{6/4}} = 3$. En conclusion,

$$\gamma_{4,\begin{smallmatrix}\square\square\square\\\square\end{smallmatrix}} = 3. \tag{4.15}$$

[2] Vis-à-vis de nos conventions, la notation par $\gamma_{n,n'}$ de la constante de Rankin est impropre et il faut comprendre en réalité $\gamma_{n,\begin{smallmatrix}\square\\\square\\\square\end{smallmatrix}}$ où la partition $\begin{smallmatrix}\square\\\square\\\square\end{smallmatrix}$ compte n' boîtes.

3. On peut produire de deux manière une même borne supérieure de la façon suivante :
$$\gamma_{8,\substack{\square\square\\\square\square}} \leqslant \gamma_{3,\substack{\square\square\\\square\square}} (\gamma_{8,3})^{3/3} = \frac{3}{2} \cdot 4 = 6$$
$$\gamma_{8,\substack{\square\square\\\square\square}} \leqslant \gamma_{2,\substack{\square\square\\\square\square}} (\gamma_{8,2})^{3/2} = \gamma_{2,\square} (\gamma_{8,2})^{3/2} = \frac{2}{\sqrt{3}} \cdot 3^{3/2} = 6$$
Or on peut vérifier que $\gamma_{8,\substack{\square\square\\\square\square}}(\mathbb{E}_8) = \gamma_{8,\substack{\square\\\square}}(\mathbb{E}_8) \cdot \gamma_{8,\square}(\mathbb{E}_8) = 3 \cdot 2 = 6$, puisque une section minimale de dimension 2 du réseau $\mathbb{E}_8$ comprend toujours un vecteur minimum. Ainsi
$$\gamma_{8,\substack{\square\square\\\square\square}} = 6 \tag{4.16}$$
et la constante est atteinte sur $\mathbb{E}_8$.
4. On a également la majoration
$$\gamma_{6,\substack{\square\square\\\square\square}} \leqslant \gamma 2, \substack{\square\square\\\square\square} \cdot (\gamma_{6,2})^{3/2} = \gamma_{2,\square} (\gamma_{6,2})^{3/2} = \frac{2}{\sqrt{3}} \left(3^{2/3}\right)^{3/2} = 2\sqrt{3}.$$
Par ailleurs, $\gamma_{6,\substack{\square\square\\\square\square}}(\mathbb{E}_6) = \gamma_{6,\substack{\square\\\square}}(\mathbb{E}_6) \cdot \gamma_{6,\square}(\mathbb{E}_6) = 3^{2/3} \frac{2}{3^{1/6}} = 2\sqrt{3}$. En conclusion
$$\gamma_{6,\substack{\square\square\\\square\square}} = 2\sqrt{3} \tag{4.17}$$
et la constante est atteinte sur $\mathbb{E}_6$.
5. On peut écrire
$$\gamma_{8,\substack{\square\square\\\square\square\\\square\square}} \leqslant \gamma_{4,\substack{\square\square\\\square\square\\\square\square}} (\gamma_{8,4})^{4/4} = 2 \cdot 4 = 8$$
ou bien
$$\gamma_{8,\substack{\square\square\\\square\square\\\square\square}} \leqslant \gamma_{3,\substack{\square\square\\\square\square\\\square\square}} (\gamma_{8,3})^{4/3} = \gamma_{3,\square} (\gamma_{8,3})^{4/3} = 2^{1/3} \cdot 4^{4/3} = 8.$$
Par un calcul direct, on vérifie que $\gamma_{8,\substack{\square\square\\\square\square\\\square\square}}(\mathbb{E}_8) = \gamma_{8,\substack{\square\square\\\square\square}}(\mathbb{E}_8) \cdot \gamma_{8,\square}(\mathbb{E}_8) = 4 \cdot 2 = 8$. On en déduit que
$$\gamma_{8,\substack{\square\square\\\square\square\\\square\square}} = 8. \tag{4.18}$$
6. On a
$$\gamma_{6,\substack{\square\square\\\square\square\\\square\square}} \leqslant \gamma_{4,\substack{\square\square\\\square\square\\\square\square}} (\gamma_{6,4})^{4/4} = \gamma_{4,\substack{\square\square\\\square\square\\\square\square}} \gamma_{6,2} = 2 \cdot 3^{2/3} \simeq 4.160.$$
Mais d'un autre côté, $\gamma_{6,\substack{\square\square\\\square\square\\\square\square}}(\mathbb{E}_6) = \gamma_{6,\substack{\square\square\\\square\square}}(\mathbb{E}_6) \cdot \gamma_{6,\square}(\mathbb{E}_6) = \frac{4}{\sqrt{3}} \frac{2}{3^{1/6}} = \frac{8}{2^{2/3}} \simeq 3.846$. Il s'agit du meilleur invariant connu.
7. On a
$$\gamma_{8,\substack{\square\square\\\square\square\\\square\square\\\square\square}} \leqslant \gamma_{4,\substack{\square\square\\\square\square\\\square\square\\\square\square}} (\gamma_{8,4})^{6/4} = 3 \cdot 4^{3/2} = 24$$
ou de façon équivalente
$$\gamma_{8,\substack{\square\square\\\square\square\\\square\square\\\square\square}} \leqslant \gamma 3, \substack{\square\square\\\square\square\\\square\square\\\square\square} (\gamma_{8,3})^{6/3} = \gamma_{3,\substack{\square\square\\\square\square}} \gamma_{8,3}^2 = \frac{3}{2} \cdot 16 = 24.$$
A présent, comme $\mathbb{A}_1 \subset \mathbb{A}_2 \subset \mathbb{A}_3$ forment des sections minimales de $\mathbb{E}_8$ et sont incluses l'une dans l'autre, $\gamma_{8,\substack{\square\square\\\square\square\\\square\square\\\square\square}}(\mathbb{E}_8) = \frac{2 \cdot 3 \cdot 4}{1^{6/8}} = 24$. Donc
$$\gamma_{8,\substack{\square\square\\\square\square\\\square\square\\\square\square}} = 24. \tag{4.19}$$

8. On a enfin
$$\gamma_{6,\begin{smallmatrix}\square\\\square\square\square\end{smallmatrix}} \leqslant \gamma_{4,\begin{smallmatrix}\square\\\square\square\square\end{smallmatrix}} (\gamma_{6,4})^{6/4} = 3 \cdot (3^{2/3})^{3/2} = 9.$$
Par ailleurs, $\gamma_{6,\begin{smallmatrix}\square\\\square\square\square\end{smallmatrix}}(\mathbb{E}_6) = \frac{2\cdot 3\cdot 4}{3^{6/6}} = 8$. La borne est insuffisante pour conclure et ne fournit qu'une majoration.

□

4.2.2 Majoration par les minima successifs

4.2.2.1 Principe général

Proposition 4.17. — *Soient A un automorphisme de $\mathbf{GL}_n(k_{\mathbb{A}})$ et Δ un drapeau de forme λ et $(x_i)_{1\leqslant i\leqslant \check{s}}$ une suite de vecteurs qui engendre Δ, alors l'inégalité suivante est satisfaite :*
$$H_A(\Delta) \leqslant \prod_{\ell=1}^{\check{s}} H_A(x_\ell)^{\lambda_\ell}. \tag{4.20}$$

Démonstration. — Quitte à transformer A, il suffit de s'assurer que cette inégalité soit satisfaite lorsque le drapeau Δ est le drapeau construit à partir de la base canonique, c'est-à-dire quand $x_\ell = e_\ell$ pour tout ℓ. L'automorphisme A peut se décomposer sous la forme $g = kdu$ où k appartient à $K_n(k_{\mathbb{A}})$, d est une matrice diagonale dont les coefficients sont disons $d_i \in {k_{\mathbb{A}}}^\times$ et u est une matrice unipotente triangulaire supérieure. L'action de k ne modifie pas les valeurs des termes qui apparaissent dans les deux membres de l'inégalité (4.20). L'action du produit du sur le vecteur $e_{U(\lambda)}$ revient à multiplier la hauteur par la quantité $|\chi_\lambda(d)|_{k_{\mathbb{A}}}$ dans le terme de gauche. Pour le terme de droite, $H(u\cdot e_i) \geqslant H(e_i)$ et $H(du\cdot e_i) = |d_i|_{k_{\mathbb{A}}} H(u\cdot e_i) \geqslant d_i H(e_i)$, ce qui achève de prouver l'égalité (4.20). □

4.2.2.2 Majoration par le second théorème de Minkowski

D'après la version adèlique du second théorème de Minkowski pour les domaines convexes (cf. [McF71] ou [Thu96]), pour un automorphisme A fixé, il existe une base de k^n telle que
$$\prod_{\ell=1}^{n} H_A(x_\ell) \leqslant \frac{2^{nr} D_k^{n/2}}{{\omega_n}^{r_1}{\omega_{2n}}^{r_2}} |\text{dét}\, A|_{k_{\mathbb{A}}}$$
où D_k est le discriminant du corps de nombre k et ω_n le volume de la boule unité de dimension n.

Nous pouvons supposer, quitte à opérer une permutation, que $H_A(x_1) \leqslant H_A(x_2) \leqslant \cdots \leqslant H_A(x_n)$, ce qui permet alors d'écrire
$$\left(\prod_{\ell=1}^{\check{s}} H(x_\ell)^{\lambda_\ell}\right)^n \leqslant \left(\prod_{\ell=1}^{n} H_A(x_\ell)\right)^{|\lambda|}$$
d'où il découle le corollaire suivant.

Corollaire 4.18. — *L'inégalité suivante est vérifiée :*
$$\gamma_{n,\lambda}(k)^{1/2|\lambda|} \leqslant \frac{2^r D_k^{1/2}}{{\omega_n}^{r_1/n}{\omega_{2n}}^{r_2/n}}. \tag{4.21}$$

4.2.3 Majoration par changement de corps de base

4.2.3.1 Préliminaires

Lemme 4.19. — *Soit A une matrice hermitienne définie positive, alors*

$$\text{dét}\ (A) \leqslant \text{dét}\ (\Re A)\,. \tag{4.22}$$

Preuve. — Nous donnons deux preuves de ce résultat. La seconde est tirée d'une source en ligne et a été recopiée pour cette raison.

1. On peut commencer par supposer que A se décompose sous la forme $D + \mathrm{i}H$ où D est une matrice diagonale à coefficients positifs et H est une matrice réelle antisymétrique. En effet, comme $\Re A$ est encore une matrice symétrique, il est possible de trouver une transformation P telle que $P'AP$ est diagonal. Par suite, en posant $D = P'(\Re A)P$ et $H = P'(\Im A)P$, on obtient la forme voulue. A présent, l'inégalité d'Hadamard indique que
$$\text{dét}\, A \leqslant A[1,1] \cdot A[2,2] \cdots A[n,n] = \text{dét}\, D = \text{dét}\ (\Re A)$$
2. Seconde preuve d'après [Aut96][3] qui attribue de résultat à M. Grainger. Décomposons A et $A = X + \mathrm{i}Y$, où X est une matrice symétrique réelle et Y une matrice antisymétrique réelle et posons $B = \begin{pmatrix} X & -Y \\ Y & X \end{pmatrix}$ qui est encore une matrice symétrique définie positive. Par des opérations sur les lignes et les colonnes, $\text{dét}\, B = (\text{dét}\, A)^2$. D'autre part, d'après l'inégalité de Fischer (voir par exemple théorème 13.5.5 dans [Mir90]), on a $\text{dét}\, B \leqslant (\text{dét}\, X)^2$.

□

Remarque 4.20. — Heuristiquement, cette inégalité revient à comparer le volume d'un parallélotope formé par certains vecteurs avec celui d'un parallélotope formé avec des vecteurs de même norme, mais en position un peu plus « orthogonale ». En dimension 2 ou 3, il est possible de la justifier par des méthodes analytiques comme suit.

1. Si la dimension vaut 2, posons pour fixer les notations
$$A = \begin{pmatrix} a & c + \mathrm{i}\gamma \\ c - \mathrm{i}\gamma & b \end{pmatrix}.$$
Alors
$$\text{dét}\, A = ab - c^2 - \gamma^2 \leqslant ab - c^2 = \text{dét}\, \Re A$$
2. Si la dimension vaut 3, posons
$$A = \begin{pmatrix} a & d + \mathrm{i}\delta & e + \mathrm{i}\varepsilon \\ d - \mathrm{i}\delta & b & f + \mathrm{i}\phi \\ e - \mathrm{i}\varepsilon & f - \mathrm{i}\phi & c \end{pmatrix}.$$
Alors, d'une part $\Re A$ est encore une matrice euclidienne définie positive et et d'autre part, on a la relation
$$\text{dét}\ (\Re A) = \text{dét}\, A + (\Re A)\,[\phi, -\varepsilon, \delta],$$
ce qui garantit l'inégalité souhaitée.

[3] Je remercie Pierre Bel de m'avoir signalé cette référence

Rappelons d'autre part le résultat classique suivant.

Lemme 4.21 (Réduction simultanée). — *Soient A et B deux matrices symétriques définies positives, euclidiennes ou hermitiennes, alors il existe une matrice inversible P telle que P^*AP et P^*BP sont toutes deux des matrices diagonales.*

Ce lemme permet de montrer les deux résultats suivants.

Lemme 4.22. — *L'application $\psi : \mathcal{H}_n^{>0} \to \mathbb{R}$ définie par $\psi = \ln \circ \text{dét}$ est concave. En particulier, si $(A_j)_{1\leqslant j\leqslant p} \in (\mathscr{H}_n^{++})^p$, alors, d'après l'inégalité de Jensen,*

$$\left(\text{dét}\left(\prod_{j=1}^{p} A_j\right)\right)^{\frac{1}{p}} \leqslant \frac{\text{dét}\left(\sum_{j=1}^{p} A_j\right)}{p}. \tag{4.23}$$

Lemme 4.23. — *Soient $(A_{v,q})_{\substack{v\in\mathfrak{V}_\infty\\ q\in\check{\lambda}}}$ une famille de matrices définies positives, alors,*

$$\sum_{v\in\mathfrak{V}_\infty} d_v \prod_{q\in\check{\lambda}} \text{dét}\,(A_{v,q}) \leqslant \prod_{q\in\check{\lambda}} \left(\sum_{v\in\mathfrak{V}_\infty} \text{dét}\,(d_v A_{v,q})\right).$$

Preuve. — Pour plus de clarté, nous limitons la preuve au cas où les indices v et q ne prennent que deux valeurs chacun, autrement dit nous nous contentons de montrer que

$$\text{dét}\,(A_1 + A_1')\text{dét}\,(A_2 + A_2') \leqslant \text{dét}\,A_1\text{dét}\,A_2 + \text{dét}\,A_1'\text{dét}\,A_2'$$

pour quatre matrices A_1, A_1', A_2, A_2'. Le cas général va à l'avenant en doublant si nécessaire, quand d_v vaut 2 plutôt que 1, $A_{v,q}$ dans la liste des matrices à considérer.

Soient A et A' deux matrices symétriques définies positives de taille n, que l'on peut supposer diagonales. Notons $(a_i)_{1\leqslant i\leqslant n}$ les coefficients diagonaux de A et $(a_i')_{1\leqslant i\leqslant n}$ ceux de A', alors comme tous les termes sont positifs,

$$\begin{aligned} &\text{dét}\,A + \text{dét}\,A' = a_1a_2\cdots a_n + a_1'a_2'\cdots a_n' \\ \leqslant\ & (a_1+a_1')(a_2+a_2')\cdots(a_n+a_n') = \text{dét}\,(A+A'). \end{aligned}$$

On voit que l'inégalité s'étend pareillement à toute somme finie de plusieurs déterminants. Par ailleurs, si l'on développe l'expression, on obtient

$$\begin{aligned} &\text{dét}\,(A_1 + A_1')\text{dét}\,(A_2 + A_2') \\ \geqslant\ & (\text{dét}\,A_1 + \text{dét}\,A_1')\,(\text{dét}\,A_2 + \text{dét}\,A_2') \\ \geqslant\ & \text{dét}\,A_1\text{dét}\,A_2 + \text{dét}\,A_1'\text{dét}\,A_2' \end{aligned}$$

en utilisant que tous les termes oubliés sont positifs. □

4.2.3.2 La majoration

Nous exhibons à présent l'inégalité suivante, démontrée dans l'article [OW01] pour le cas $\lambda = \square$.

Théorème 4.24. — *Soit λ une partition, si D_k désigne le discriminant du corps k, l'inégalité suivante est vérifiée*

$$\gamma_{n,\lambda}(k) \leqslant \frac{|D_k|^{|\lambda|}(\gamma_{nd,\lambda}(\mathbb{Q}))^d}{d^d}. \tag{4.24}$$

Démonstration. — L'idée de la démonstration est de transformer tous les $\mathfrak{o}$-modules en $\mathbb{Z}$-modules. À cette fin, on introduit comme dans [OW01] des scalaires de k notés $(u_1^{(\iota)} \dots, u_d^{(\iota)})$ qui forment une base sur $\mathbb{Z}$ de l'idéal $\mathfrak{a}_\iota$. Nous pouvons alors considérer la base produit $\mathcal{B}^{(\iota)}$ de L_ι vu en tant que $\mathbb{Z}$-module, qui est constituée des vecteurs $\varepsilon_{j,l}^{(\iota)} = u_j^{(1)} e_l$ pour $1 \leqslant j \leqslant d$ et $1 \leqslant l \leqslant n-1$ et des vecteurs $\varepsilon_{j,n} = u_j^{(\iota)} e_n$ pour $1 \leqslant j \leqslant d$. Ceci fait, à toute forme quadratique d'Hermite-Humbert $\mathcal{A} \in \mathcal{P}_n(k)$, on associe la forme quadratique $\Phi^{(\iota)}$ définie sur $\mathbb{Q}^{nd}$ et donnée par la formule ci-dessous où y appartient à $\mathbb{Q}^{nd}$ et Y est le vecteur de k^n de coordonnées y dans la base $\mathcal{B}^{(\iota)}$

$$\Phi^{(\iota)}(y) = \sum_{v \in \mathfrak{V}_\infty} d_v Y' A_v Y. \tag{4.25}$$

Pour tout $\check{s}$-upplet de vecteurs libres $(Y_1, \dots, Y_{\check{s}}) \subset L_\iota$, dont les coordonnées dans $\mathbb{Q}^{nd}$ sont $(y_1, \dots, y_{\check{s}}) \subset \mathbb{Q}^{nd}$, notons X_q la matrices dans $\mathcal{M}_{n,q}(k)$ des q vecteurs $[Y_1, \dots, Y_q]$ et x_q la matrice $[y_1, \dots, y_q]$ dans $\mathcal{M}_{nd,q}(\mathbb{Q})$ et posons

$$V = \begin{array}{|c|c|c|c|c|}\hline Y_{\check{s}} & & & & \\ \hline & & & & \\ \hline & & & & \\ \hline Y_2 & Y_2 & \cdot & Y_2 & \\ \hline Y_1 & Y_1 & \cdot & \cdot & Y_1 \\ \hline \end{array} \in \mathbb{S}_\sharp^\lambda(L_\iota) \qquad v = \begin{array}{|c|c|c|c|c|}\hline y_{\check{s}} & & & & \\ \hline & & & & \\ \hline & & & & \\ \hline y_2 & y_2 & \cdot & y_2 & \\ \hline y_1 & y_1 & \cdot & \cdot & y_1 \\ \hline \end{array} \in \mathbb{S}_\sharp^\lambda\left(\mathbb{Q}^{nd}\right).$$

Remarquons d'ores et déjà que par construction $\Re\left(\sum_{v \in \mathfrak{V}_\infty} d_v A_v [X_q]\right)$ coïncide avec $\Phi^{(\iota)}[x_q]$.

La combinaison du premier et des deux derniers lemmes préliminaires permet d'écrire la comparaison

$$(\mathcal{A}[V])^{\frac{1}{d}} \leqslant \frac{\Phi^{(\iota)}[v]}{d} \tag{4.26}$$

qui est en quelque sorte une inégalité arithmético-géométrique. Détaillons plus

ce passage, qui utilise successivement les lemmes 4.22, 4.23 puis 4.19 :

$$\begin{aligned}
(\mathcal{A}[V])^{\frac{1}{d}} &= \left(\prod_{v\in\mathfrak{V}_\infty}\left(\prod_{q\in\check{\lambda}}\text{dét}\,\left(X_q^{\sigma_v\prime}A_vX_q^{\sigma_v}\right)\right)^{d_v}\right)^{1/d}\\
&\leqslant \frac{1}{d}\sum_{v\in\mathfrak{V}_\infty}\left(d_v\prod_{q\in\check{\lambda}}\text{dét}\,\left(X_q^{\sigma_v\prime}A_vX_q^{\sigma_v}\right)\right)\\
&\leqslant \frac{1}{d}\prod_{q\in\check{\lambda}}\text{dét}\,\left(\sum_{v\in\mathfrak{V}_\infty}d_vX_q^{\sigma_v\prime}A_vX_q^{\sigma_v}\right)^{d_v}\\
&\leqslant \frac{1}{d}\prod_{q\in\check{\lambda}}\text{dét}\,\left(\Phi^{(\iota)}[x_q]\right)^{d_v}\\
&= \frac{1}{d}\Phi^{(\iota)}[v].
\end{aligned}$$

En particulier en passant au minimum sur les t-upplets, la définition de $\gamma_\lambda^{nd}(\mathbb{Q})$ permet d'écrire

$$\min_V\,(\mathcal{A}[v])^{\frac{1}{d}} \leqslant \frac{\gamma_{nd,\lambda}(\mathbb{Q})\ \text{dét}\,(\Phi^{(\iota)})^{\frac{|\lambda|}{nd}}}{d}. \tag{4.27}$$

Le déterminant de $\Phi^{(\iota)}$ est détaillé dans [OW01], sa valeur est

$$\text{dét}\,(\Phi^{(\iota)}) = \mathcal{N}\,(\mathfrak{a}_\iota)\,|D_k|^n\text{dét}\,\mathcal{A} = |D_k|^n\text{dét}_{\,L_\iota}\mathcal{A}.$$

Comme l'idéal $\mathfrak{A}_Z$ est toujours entier, on a même

$$\frac{m_{L_\iota}(\mathcal{A})}{(\text{dét}_{\,L_\iota}\mathcal{A})^{\frac{|\lambda|}{n}}} \leqslant \frac{(\gamma_{nd,\lambda}(\mathbb{Q}))^d\ |D_k|^{|\lambda|}}{d^d}. \tag{4.28}$$

D'où l'on tire facilement l'inégalité attendue. □

Remarque 4.25. — Trois inégalités sont employées et altèrent potentiellement les majorations : il s'agit des lemmes 4.19, 4.22 et 4.23. Le lemme 4.19 redevient une égalité lorsque la forme d'Humbert optimale est à coefficient réels. Lorsque $\mathfrak{V}_\infty$ ne contient qu'une place, l'inégalité du lemme 4.22 redevient une égalité quelque soit la partition λ. Par contre l'inégalité du lemme 4.23 introduit une erreur dès que λ compte strictement plus d'une boîte.

4.2.3.3 Application aux réseaux de corps quadratiques imaginaires.

Cette inégalité permet dans certains cas de calculer les constantes d'Hermite-Humbert de corps de nombres quadratiques imaginaires k. En effet, dans ce cas, l'inégalité entre les moyennes géométriques et arithmétiques est systématiquement une égalité. Si par surcroît la constante $\gamma_{2n,\square}(\mathbb{Q})$ est atteinte pour un réseau ayant une structure de $\mathfrak{o}_k$-module, chacun des deux termes de part et d'autre sont atteints par le même réseau, vu à gauche comme réseau complexe et à droite comme réseau réel. Les inégalités des lemmes 4.19 et 4.23 sont aussi des égalités.

À cause de la formule (2.11), valable pour tout réseau ayant une structure de module sur l'anneau des entiers d'un corps quadratique imaginaire, et du fait de l'égalité $d^d = 2^2 = 4$, l'inégalité est en fait une égalité dans ce cas.

De l'extrémalité des réseaux de racine $\mathbb{D}_4$, $\mathbb{E}_6$, $\mathbb{E}_8$ et du réseau de Leech Λ_{24}, on déduit les valeurs du tableau suivant.

n	k	$\gamma_{n,\square}(k)$	Réseau réel
2	$\mathbb{Q}[\mathrm{i}]$	2	$\mathbb{D}_4$
3	$\mathbb{Q}[\mathrm{j}]$	$\sqrt[3]{9}$	$\mathbb{E}_6$
4	$\mathbb{Q}[\mathrm{i}]$	4	$\mathbb{E}_8$
4	$\mathbb{Q}[\mathrm{j}]$	3	$\mathbb{E}_8$
4	$\mathbb{Q}[\sqrt{-7}]$	7	$\mathbb{E}_8$
12	$\mathbb{Q}[\mathrm{i}]$	16	Λ_{24}
12	$\mathbb{Q}[\mathrm{j}]$	12	Λ_{24}

Tab. 4.3 – Constantes d'Humbert pour certains corps imaginaires

4.2.3.4 Raffinement de l'inégalité dans le cas des corps quadratiques imaginaires

Nous proposons dans le cas des corps quadratiques imaginaires une inégalité un peu plus fine, qui coïncide avec la précédente lorsque λ n'a qu'une part. Toutefois, cette nouvelle majoration ne permet malheureusement pas de calculer de nouvelles constantes comme le montrent les exemples ci-dessous.

Théorème 4.26. — *Soit k un corps quadratique imaginaire, alors*

$$\gamma_{n,\lambda}(k) \leqslant \left(\frac{|D_k|}{4}\right)^{|\lambda|} (\gamma_{2n,\lambda}(\mathbb{Q}))^2 \tag{4.29}$$

Démonstration. — En gardant les mêmes notations que pour la démonstration du théorème 4.24 précédent et en remarquant qu'il n'y a qu'une place infinie, on peut écrire pour une forme de Humbert $\mathcal{A} = (A)$ et en utilisant le lemme

$$\begin{aligned}
\mathcal{A}[V] &= \prod_{q\in\check{\lambda}} \text{dét}\ (X_q{}^* A X_q)^2 \\
&\leqslant \left(\prod_{q\in\check{\lambda}} \text{dét}\ \left(x_q{}' \frac{\Phi^{(\iota)}}{2} x_q\right)\right)^2 = \left(\frac{\Phi^{(\iota)}}{2}[v]\right)^2 \\
&\leqslant \left(\gamma_{2n,\lambda}(\mathbb{Q})\text{dét}\ \frac{\Phi^{(\iota)}}{2}\right)^2
\end{aligned}$$

puisque $(2A)[V] = \Phi^{(\iota)}[v]$. Par ailleurs, puisque $\Phi^{(\iota)}$ est de dimension $2n$, on peut réutiliser le calcul de son déterminant pour obtenir, $\text{dét}\ \frac{\Phi^{(\iota)}}{2} = \frac{|D_k|^n}{2^{2n}} \text{dét}_{L_\iota} \mathcal{A}$. On conclut comme pour le théorème 4.24 précédent. □

Remarque 4.27. — Cette inégalité coïncide bien avec le théorème 4.24 puisque $d^d = 2^2 = 4$. Elle permet de gagner ce qui avait été perdu bêtement dans par les inégalités du lemme 4.22 qui devient inutile et surtout du lemme 4.23 qui majore très grossièrement les produits.

Exemple 4.28. — Dans les cas suivants, l'inégalité n'est pas une égalité. On sait que $\gamma_{3,\boxminus}(\mathbb{Q}[\mathrm{j}]) = \gamma_{3,\square}(\mathbb{Q}[\mathrm{j}])$ est atteint sur la forme de matrice

$$\begin{pmatrix} 3 & 0 & -\mathrm{i}\sqrt{3} \\ 0 & 3 & -\mathrm{i}\sqrt{3} \\ \mathrm{i}\sqrt{3} & \mathrm{i}\sqrt{3} & 3 \end{pmatrix}^{-1} = \frac{1}{3}\begin{pmatrix} 2 & 1 & \mathrm{i}\sqrt{3} \\ 1 & 2 & \mathrm{i}\sqrt{3} \\ -\mathrm{i}\sqrt{3} & -\mathrm{i}\sqrt{3} & 3 \end{pmatrix}$$

et vaut $3^{2/3}$. En revanche, $\left(\frac{|D_{\mathbb{Q}[\mathrm{j}]}|}{4}\right)^2 (\gamma_{6,\boxminus}(\mathbb{Q}))^2 = \frac{27}{16}\sqrt[3]{3}$ qui est bien plus grand.

De même, $\gamma_{4,\boxminus}(\mathbb{Q}[\mathrm{i}]) = \gamma_{4,\square}(\mathbb{Q}[\mathrm{i}]) = 4$ alors que le membre de droite vaut 16. On a encore $\gamma_{4,\boxminus}(\mathbb{Q}[\mathrm{j}]) = \gamma_{4,\square}(\mathbb{Q}[\mathrm{j}]) = 3$, tandis que le membre de droite correspondant vaut $\frac{27}{4}$.

Exemple 4.29. — On a aussi les majorations $\gamma_{4,\boxminus}(\mathbb{Q}[\mathrm{i}]) \leqslant 9$ et $\gamma_{4,\boxminus}(\mathbb{Q}[\mathrm{j}]) \leqslant \frac{81}{16}$, tandis que $\gamma_{4,\boxminus}(\mathbb{Q}[\mathrm{i}])(\mathbb{E}_8) = 4$ et $\gamma_{4,\boxminus}(\mathbb{Q}[\mathrm{j}])(\mathbb{E}_8) = 4$ où, par abus de notation, nous désignons par $\mathbb{E}_8$ la forme de Humbert gaussienne ou eisensteinienne tirée de l'exemple 2.35 dont la forme réelle coïncide avec celle du réseau $\mathbb{E}_8$.

4.2.4 Trace dyadique et exploitation des inégalités de Bergé–Martinet

La ligne de mire de cette partie est l'espoir de calculer explicitement des constantes d'Hermite que le paragraphe précédant échoue à calculer. Cette partie reproduit dans le cadre des formes de Humbert une méthode initiée par C. Poor et D. Yuen [PY06] en la généralisant. Son intérêt a été motivé par les résultats récents de [SWO08] et en particulier le calcul très aisé de constantes de Rankin.

4.2.4.1 Trace dyadique

Commençons par présenter un lemme facile dont le secours sera fréquent dans ce qui suit.

Lemme 4.30. — *Soient $(a_i)_{i\in I}$ et $(b_i)_{i\in I}$ deux familles finies de réels strictement positifs, alors*

$$\left(\prod_{i\in I}(a_i+b_i)\right)^{1/|I|} \geqslant \left(\prod_{i\in I} a_i\right)^{1/|I|} + \left(\prod_{i\in I} b_i\right)^{1/|I|} \tag{4.30}$$

Preuve. — Introduisons les réels $(\alpha_i)_{i\in I}$ et $(\beta_i)_{i\in I}$ tels que pour tout indice $i \in I$, $a_i = \exp(\alpha_i)$ et $b_i = \exp(\beta_i)$. Alors, l'inégalité à démontrer devient, en passant aux logarithmes,

$$\frac{1}{|I|}\sum_{i\in I}\ln(e^{\alpha_i}+e^{\beta_i}) \geqslant \ln\left(e^{\sum_{i\in I}\frac{\alpha_i}{|I|}} + e^{\sum_{i\in I}\frac{\beta_i}{|I|}}\right)$$

qui est encore équivalente à

$$\frac{1}{|I|}\sum_{i\in I}\ln(e^{\frac{\alpha_i-\beta_i}{2}}+e^{\frac{\beta_i-\alpha_i}{2}}) \geqslant \ln\left(e^{\sum_{i\in I}\frac{\alpha_i-\beta_i}{2|I|}} + e^{\sum_{i\in I}\frac{\beta_i-\alpha_i}{2|I|}}\right).$$

Or la véracité de cette dernière inégalité relève d'une inégalité de Jensen appliquée à la fonction convexe $t \mapsto \ln(\operatorname{ch} t)$. □

Nous pouvons à présent définir des analogues aux traces dyadiques utilisées par C. Poor et D. Yuen [PY06] puis généralisés au cas rationnel grassmanien dans [SWO08].

Définition 4.31. — Etant données deux formes de Hermite–Humbert $\mathcal{A}$ et $\mathcal{B}$ appartenant à $\mathcal{P}_n(k)$, on définit la quantité suivante

$$\prec \mathcal{A}, \mathcal{B} \succ = \left(\prod_{v \in \mathfrak{V}_\infty} Tr({A_v}^* B_v)^{d_v} \right)^{\frac{1}{d}}. \tag{4.31}$$

Définition 4.32. — On dit qu'une fonction ϕ définie sur l'ensemble des formes de Hermite–Humbert à valeur dans $\mathbb{R}_+^*$ est *de type un* si elle satisfait

1. $\phi(t\mathcal{A}) = \left(\prod_{v \in \mathfrak{V}_\infty} t_v^{d_v}\right)^{\frac{1}{d}} \phi(\mathcal{A})$ pour $t = (t_v)_{v \in \mathfrak{V}_\infty} \in (\mathbb{R}_+^*)^r$,
2. $\phi(\mathcal{A} + \mathcal{B}) \leqslant \phi(\mathcal{A}) + \phi(\mathcal{B})$ pour tout $\mathcal{A}$, $\mathcal{B}$ dans $\mathcal{P}_n(k)$.

Lorsque ϕ est invariante par changement de classe sous l'action de $\Phi_{\mathcal{R}}$ pour $\mathcal{R} = (R_v)_{v \in \mathfrak{V}_\infty} \in \mathbf{SL}_n(\mathbb{R})^{r_1} \times \mathbf{SL}_n(\mathbb{C})^{r_2}$, on dit que ϕ est une fonction de classe de type un. Etant donnée une fonction de type un, on peut parler de la *fonction duale*, définie par l'expression suivante :

$$\hat{\phi}(\mathcal{A}) = \inf_{\mathcal{B} \in \mathcal{P}_n(k)} \frac{\prec \mathcal{A}, \mathcal{B} \succ}{\phi(\mathcal{B})}. \tag{4.32}$$

En appliquant le lemme 4.30, on peut observer que cette fonction est encore une fonction de type un. Cette fonction duale demeure invariante par classe si ϕ l'est initialement. On vérifie immédiatement le lemme suivant.

Lemme 4.33. — *Si deux fonctions ϕ_1 et ϕ_2 de type un vérifient pour toute forme de Humbert $\mathcal{A}$ l'inégalité $\phi_1(\mathcal{A}) \leqslant \phi_2(\mathcal{A})$, alors leur duales vérifient encore $\hat{\phi}_1(\mathcal{A}) \geqslant \hat{\phi}_2(\mathcal{A})$ pour toute forme $\mathcal{A}$.*

Exemple 4.34. — Etant donné un réseau L de k^n, la fonction $\mathcal{A} \mapsto \sqrt{n^d}\,(\text{dét}\,_L\mathcal{A})^{\frac{1}{dn}}$ admet la fonction $\mathcal{A} \mapsto \sqrt{n^d}\,(\text{dét}\,_{L^*}\mathcal{A})^{\frac{1}{dn}}$ pour duale.

Proposition 4.35. — *Soit λ une partition et L un réseau de k^n. La fonction $m_L^\circ = \mathcal{A} \mapsto (m_L(\mathcal{A}))^{\frac{1}{d|\lambda|}}$, où m_L est le minimum défini en fonction de λ dans la partie 3.2, est une fonction de type un.*

Démonstration. — Cette preuve suit celle employée dans [SWO08]. Soient $\mathcal{A}$ et $\mathcal{B}$ deux formes de Hermite–Humbert. En utilisant le lemme 4.30 que l'on applique aux valeurs propres des différentes matrices qui apparaissent dans l'expression

$$\mathcal{A}[V] = \prod_{v \in \mathfrak{V}_\infty} \prod_{q \in \check{\lambda}} \left(\Delta_q \left({X^{\sigma_v}}^* A_v X^{\sigma_v} \right) \right)^{d_v}$$

et dans les expressions correspondantes pour $\mathcal{B}[V]$ et $(\mathcal{A}+\mathcal{B})[V]$, on peut écrire

$$\begin{aligned}(m_L(\mathcal{A}+\mathcal{B}))^{\frac{1}{d|\lambda|}} &= \min_{V\in\mathbb{S}_\sharp^\lambda(L)} (\mathcal{A}+\mathcal{B})[V]^{\frac{1}{d|\lambda|}} \\ &\geqslant \min_{V\in\mathbb{S}_\sharp^\lambda(L)} \mathcal{A}[V]^{\frac{1}{d|\lambda|}} + \mathcal{B}[V]^{\frac{1}{d|\lambda|}} \\ &\geqslant \min_{V\in\mathbb{S}_\sharp^\lambda(L)} \mathcal{A}[V]^{\frac{1}{d|\lambda|}} + \min_{V\in\mathbb{S}_\sharp^\lambda(L)} \mathcal{B}[V]^{\frac{1}{d|\lambda|}}.\end{aligned}$$

Autrement dit,

$$(m_L(\mathcal{A}+\mathcal{B}))^{\frac{1}{d|\lambda|}} \geqslant (m_L\mathcal{A})^{\frac{1}{d|\lambda|}} + (m_L\mathcal{B})^{\frac{1}{d|\lambda|}}.$$

□

Ce type d'inégalité est très classique et est parfois attribué à Minkowski (cf. par exemple théorème 5.8.6 dans [Web94]).

Définition 4.36. — A l'image de [PY06] et de [SWO08], nous définissons

$$c_{n,\lambda,L}(\mathcal{A}) = \inf_{\mathcal{B}\in\mathcal{P}_n(k)} \frac{\prec\mathcal{A},\mathcal{B}\succ^{d|\lambda|}}{m_L(\mathcal{A})m_{L^*}(\mathcal{B})},$$

ainsi que

$$c_{n,\lambda}(\mathcal{A}) = \min_{1\leqslant\iota\leqslant h} \inf_{\mathcal{B}\in\mathcal{P}_n(k)} \frac{\prec\mathcal{A},\mathcal{B}\succ^{d|\lambda|}}{m_{L_\iota}(\mathcal{A})m_{L_\iota^*}(\mathcal{B})}.$$

Par ailleurs nous définissons

$$c_{n,\lambda,L} = \inf_{\mathcal{A}\in\mathcal{P}_n(k)} c_{n,\lambda,L}(\mathcal{A}) \quad \text{et} \quad c_{n,\lambda} = \inf_{\mathcal{A}\in\mathcal{P}_n(k)} c_{n,\lambda}(\mathcal{A}). \tag{4.33}$$

Théorème 4.37. — *Etant donné un corps de nombre k et une partition λ de profondeur inférieure à n, on a les inégalités suivantes*

$$\frac{1}{\big(\gamma_{n,\lambda}(k)\big)^2} \leqslant \frac{c_{n,\lambda}(k)}{n^{|\lambda|}} \leqslant \frac{1}{\big(\gamma'_{n,\lambda}(k)\big)^2}.$$

Remarque 4.38. — Ce théorème a été d'abord montré dans l'article [PY06] pour la constante d'Hermite usuelle puis dans [SWO08] pour les constantes de Rankin.

Démonstration. — Soit L un réseau, par définition de $\gamma_{n,\lambda}$, on a l'inégalité

$$m_L^\circ(\mathcal{A}) \leqslant (\gamma_{n,\lambda})^{\frac{1}{d|\lambda|}} \left(\text{dét}_L\mathcal{A}\right)^{\frac{1}{nd}}. \tag{4.34}$$

En appliquant le lemme 4.33, on obtient encore

$$\inf_{\mathcal{B}\in\mathcal{P}_n(k)} \frac{\prec\mathcal{A},\mathcal{B}\succ}{m_L^\circ(\mathcal{B})} \geqslant (\gamma_{n,\lambda})^{\frac{1}{d|\lambda|}}\, n^d \left(\text{dét}_{L^*}\mathcal{A}\right)^{\frac{1}{nd}}. \tag{4.35}$$

En rassemblant les deux dernières inégalités, il suit que

$$\inf_{\mathcal{B}\in\mathcal{P}_n(k)} \frac{\prec\mathcal{A},\mathcal{B}\succ}{m_{L^*}^\circ(\mathcal{B})} \geqslant \frac{n^d}{\gamma_{n,\lambda}{}^{\frac{2}{d|\lambda|}}} m_L^\circ(\mathcal{A}).$$

En identifiant les termes, il vient $c_{n,\lambda,L} \geqslant \dfrac{n^{|\lambda|}}{\gamma_{n,\lambda}^2}$ et même $c_{n,\lambda} \geqslant \dfrac{n^{|\lambda|}}{\gamma_{n,\lambda}^2}$.

Par ailleurs, par définition de de $c_{n,\lambda}$, en choisissant $\mathcal{B} = \mathcal{A}^{-1} = (A_v^{-1})_{v\in\mathfrak{V}_\infty}$, on obtient,

$$c_{n,\lambda} \leqslant c_{n,\lambda,L} \leqslant \frac{n^{|\lambda|}}{m_L(\mathcal{A})m_{L^*}(\mathcal{A}^{-1})}.$$

On en déduit sans peine

$$(\gamma'_{n,\lambda})^2 \leqslant \frac{n^{|\lambda|}}{c_{n,\lambda}}$$

qui est la seconde inégalité attendue. □

4.2.4.2 Quelques calculs de constantes de Bergé–Martinet

Nous nous concentrons dans cette partie dans le cas où k est le corps quadratique imaginaire $\mathbb{Q}[\mathrm{i}]$ ou $\mathbb{Q}[\mathrm{j}]$. Dans ce cas, il n'y a qu'une place et le nombre de classe de k vaut 1. Pour deux formes de Humbert $\mathcal{A} = (A)$ et $\mathcal{B} = (B)$, on a tout simplement $\prec A, B \succ = \mathrm{Tr}(A^*B)$, si bien que les quantités introduites précédemment deviennent

$$w(A) = \inf_{B\in\mathcal{P}_n(k)} \frac{\mathrm{Tr}A^*B}{m_{\mathfrak{o}^n}B}$$

$$c_{n,\square}(A) = \frac{w(A)}{m(A)}.$$

Lemme 4.39. — *Si A^{-1} est semi-eutactique, autrement dit, si A peut s'écrire $A = \sum_{x\in\mathscr{S}(A^{-1})} \rho_x xx^*$ avec des coefficients ρ_x tous positifs, $w(A)$ se calcule comme suit*

$$w(A) = \frac{n}{\min A^{-1}}. \tag{4.36}$$

Preuve. — Calculer $w(A)$ revient dans ce cas à estimer la borne inférieure de la somme $\sum_{x\in\mathscr{S}(A^{-1})} \rho_x \frac{B[x]}{\min B}$, qui est minimale lorsque les vecteurs minimaux de B contiennent $\mathscr{S}\left(A^{-1}\right)$. L'infimum est donc atteint par exemple lorsque $B = A^{-1}$ ce qui conduit au résultat attendu. □

Remarque 4.40. — En réalité, on peut démontrer avec le même type de preuve que $w(A)$ est une fonction linéaire par morceau. Précisément, en notant $\varpi(P)$, le cône de Voronoï[4], on a pour tout $A \in \varpi(P)$, $w(A) = \frac{Tr(A^*P)}{\min P}$.

Exemple 4.41. — Les réseaux gaussiens dont la forme réelle correspond à $\mathbb{D}_6$, $\mathbb{D}_8$ et $\mathbb{E}_8$ ainsi que leur duaux sont fortement eutactiques. Leurs invariants w et de Bergé-Martinet sont consignés dans le tableau 4.4.

Exemple 4.42. — Parmi les réseaux eisensteiniens, les deux formes parfaites pour $\lambda = \square$ en dimension $n = 3$ ($\mathbb{E}_6$ et $\mathbb{E}_6^*$) et les cinq formes parfaites en dimension $n = 4$ ($\mathbb{E}_8$, P_{13}, P_{43}, le réseau de Barnes $\mathrm{L}_8 = \mathrm{P}_{62}$ et Si) sont fortement eutactiques ainsi que $\mathbb{E}_8^*$, P_{62}^* et Si^*. Les valeurs des invariants sont présentés dans le tableau 4.5.

[4] On entend le cône convexe engendré par les matrices de projection sur les vecteurs minimaux de P

Dimension	Réseau réel	Invariant de Bergé–Martinet	Invariant w
3	$\mathbb{D}_6$	2	3
4	$\mathbb{E}_8$	4	8
4	$\mathbb{D}_8$	2	4

TAB. 4.4 – Invariant de Bergé–Martinet des réseaux gaussiens parfaits en dimension 3 et 4

Dimension	Réseau réel	Invariant de Bergé–Martinet	Invariant w
3	$\mathbb{E}_6$	2	3
4	$\mathbb{E}_8$	3	$\frac{8}{3}$
4	P_{13}	2	
4	P_{43}	2	
4	P_{62}	2	8
4	Si	$\frac{9}{4}$	$\frac{32}{3}$

TAB. 4.5 – Invariants de Bergé–Martinet des réseaux eisensteiniens parfaits en dimension 3 et 4

Exemple 4.43. — Le tableau 4.6 présente les invariants de quelques réseaux sur $\mathbb{Q}[\sqrt{-7}]$. (Pour les définitions des formes, consultez l'annexe B).

Dimension	Réseau réel	Invariant de Bergé–Martinet
3	$\mathbb{A}_6$	3
3	$\mathbb{A}_6^{(2)}$	4
4	$\mathbb{E}_8$	7

TAB. 4.6 – Invariants de Bergé–Martinet de réseaux de $\mathbb{Q}[\sqrt{-7}]$

Proposition 4.44. — *La constante $c_{n,\square}$ est atteinte sur une forme parfaite de minimum 1.*

Ce résultat est déjà présent pour $k = \mathbb{Q}$ dans [PY06]. Nous l'étendons au cas d'un corps quadratique imaginaire uniquement.

Démonstration. — Comme $\frac{w(A)}{m(A)}$ est invariant par multiplication scalaire, on peut supposer que A est de minimum supérieur à 1, c'est-à-dire que A appartient au domaine de Ryshkov. Comme w est une fonction de type un, son minimum est atteint sur les sommets du domaine de Ryshkov, c'est-à-dire sur une forme parfaite de minimum 1. □

Proposition 4.45. — *Les invariants de Bergé–Martinet prennent les valeurs décrites dans le tableau 4.7. Elles sont atteintes sur les formes $\mathbb{D}_6$ et $\mathbb{E}_8$ dans le cas gaussien, $\mathbb{E}_6$ et $\mathbb{E}_8$ dans le cas eisensteinien et $\mathbb{A}_6^{(2)}$ et $\mathbb{E}_8$ sur $\mathbb{Q}[\sqrt{-7}]$.*

Démonstration. — Dans le cas où la constante d'Hermite est atteinte sur un réseau

Dimension	Cas gaussien	Cas eisensteinien	Cas $\mathbb{Q}[\sqrt{-7}]$
3	$\gamma'_{3,\square}(\mathbb{Q}[\mathrm{i}]) = 2$	$\gamma'_{3,\square}(\mathbb{Q}[\mathrm{j}]) = 2$	$\gamma'_{3,\square}(\mathbb{Q}[\sqrt{-7}]) = 4$
4	$\gamma'_{4,\square}(\mathbb{Q}[\mathrm{i}]) = 4$	$\gamma'_{4,\square}(\mathbb{Q}[\mathrm{j}]) = 3$	$\gamma'_{4,\square}(\mathbb{Q}[\sqrt{-7}]) = 7$

Tab. 4.7 – Constantes de Bergé–Martinet gaussiennes et eisensteiniennes

et son dual, les inégalités du théorème 4.37 deviennent des égalités. Ce fait a été mentionné dans [PY06] (proposition 1.4) et sa démonstration s'applique encore ici. Il permet de conclure lorsque $n = 4$. Quand $n = 3$, on peut calculer $c_{n,\square}$ avec la proposition précédente et vérifier que la majoration du théorème 4.37 est atteinte. □

4.2.4.3 Application aux constantes de Rankin généralisées

Proposition 4.46. — *Les constantes d'Hermite gaussiennes et eisensteiniennes suivantes, analogues aux constantes de Rankin sur $\mathbb{Q}$, prennent les valeurs décrites ci-dessous*

$$\gamma_{4,\boxminus}(\mathbb{Q}[\mathrm{i}]) = 4 \qquad \textit{et} \qquad \gamma_{4,\boxminus}(\mathbb{Q}[\mathrm{j}]) = 4$$

et sont atteintes sur les formes d'Humbert correspondant au réseau réel $\mathbb{E}_8$.

Démonstration. — La démonstration est identique dans les deux cas et imite celle de [SWO08]. Pour $k = \mathbb{Q}[\mathrm{i}]$ ou $k = \mathbb{Q}[\mathrm{j}]$, on commence par observer que $\gamma_{4,\boxminus}(k) = \gamma'_{4,\boxminus}(k)$ en vertu du corollaire 4.11 puis on applique la seconde inégalité du théorème 4.10, c'est-à-dire $\gamma'_{4,\square}(k) \leqslant \left(\gamma'_{3,\square}(k)\right)^2$. Dans les deux cas, on obtient 4 comme majoration. Celle-ci est atteinte pour les réseaux complexes ayant pour forme réelle le réseau $\mathbb{E}_8$. □

La religion drapeautique remplaça promptement la céleste. — L.–F. Céline. « Voyage au bout de la nuit ».

Designs vexillaires et réseaux fortement parfaits 5

Dans toute cette partie, nous mettons de côté les aspects de théorie des nombres employés jusqu'ici. Le corps global considéré sera $k = \mathbb{Q}$. Une partition λ à moins de n parts est toujours fixée. Nous supposons toujours que les parts $(\breve{\lambda}_i)_{1\leqslant i\leqslant \breve{s}}$ de $\breve{\lambda}$ prennent exactement les valeurs $(d_i)_{1\leqslant i\leqslant \ell}$ mais peuvent éventuellement se répéter. Nous rappelons qu'à tout réseau L contenu dans $\mathbb{R}^n$ est associé l'*invariant d'Hermite* $\gamma(L)$ défini par

$$\gamma(L) = \inf_{\Lambda\subset L} \frac{\text{dét}\,(\Lambda_1)\cdots\text{dét}\,(\Lambda_{\breve{s}})}{(\text{dét}\,(L))^{\frac{|\lambda|}{n}}} \tag{5.1}$$

où $\Lambda = (\Lambda_1, \ldots, \Lambda_{\breve{\lambda}})$ est une chaîne de sous-réseaux de L emboîtés vérifiant la condition $\text{rg}(\Lambda_i) = \breve{\lambda}_i$ pour tout $1 \leqslant i \leqslant \breve{s}$ et que la *constante d'Hermite* associée est la borne supérieure de $\gamma(L)$ quand L décrit l'ensemble des réseaux d'une dimension donnée. Pour plus de simplicité, nous omettons dans cette partie l'indice λ.

5.1 Fonctions de la variété drapeau et designs

5.1.1 Fonctions de carré intégrable sur la variété drapeau

5.1.1.1 Décomposition de $\mathscr{L}^2(\mathscr{D}_\mathrm{d})$

Soit $\mathscr{L}^2(\mathscr{D}_\mathrm{d})$ l'espace des fonctions de carré intégrable de la variété drapeau $\mathscr{D}_\mathrm{d}$ munie de la mesure de Haar de poids total 1. Toute fonction régulière définie sur $\mathcal{M}_{n,m}(\mathbb{R})$ et stable sous l'action à droite de multiplication de la variable par un élément de $\mathbf{O_m}$ fournit par restriction une fonction de $\mathscr{L}^2(\mathscr{D}_\mathrm{d})$ et *vice–versa*. Nous pouvons par conséquent écrire que

$$\mathscr{L}^2(\mathscr{D}_\mathrm{d}) \subset \bigoplus_{\substack{\mu \\ \lfloor\mu\rfloor\leqslant \min n,m}} (M^\mu)^{\mathrm{I}_n\times O(\mathbf{m})} = \bigoplus_{\substack{\mu \\ \lfloor\mu\rfloor\leqslant \min n,m}} \mathbb{S}^\mu(\mathbb{R}^n)\otimes(\mathbb{S}^\mu(\mathbb{R}^m))^{O(\mathbf{m})}.$$

Soient Θ_0 un tableau standard et e_{Θ_0} le vecteur de $\mathbb{S}^\mu(\mathbb{R}^m)$ associé. Soient C_1 et C_2 le choix de d boîtes dans deux colonnes d'un vecteur tableau V_0 opéré selon les règles de description du module complémentaire J^λ (*cf.* 2.2.6). La somme

des monômes déterminantaux $\mathscr{M}_{\{V_0,\Theta_0\}}$ obtenus après substitutions prescrites comporte le facteur

$$\sum_{I=i_1<\cdots<i_d} \text{dét}\left(\left(z_{i,j}\right)_{\substack{i\in I\\ j\in C_1}}\right) \text{dét}\left(\left(z_{i,j}\right)_{\substack{i\in I\\ j\in C_2^d}}\right) \mod I_>^{(\mu)} \tag{5.2}$$

qui n'est rien d'autre que l'expression du produit scalaire des vecteurs $\bigwedge_{j\in C_1} u_j$ et $\bigwedge_{j\in C_2} u_j$ dans $\bigwedge^d \mathbb{R}^n$ où u_j désigne le $j^{\text{ième}}$ vecteur colonne de la matrice des indéterminées Z. Cette expression est invariante sous l'action de $\mathbf{O}_n(\mathbb{R})$ (voir aussi section 5 de [dCP76]). Évaluée en la matrice X_Δ qui représente le drapeau Δ, cette expression vaut systématiquement 1 ou 0 selon que les indices de C_1 et C_2 sont égaux ou non puisque les colonnes de X_Δ sont orthonormales. Ainsi, tout polynôme de $J^\mu \otimes \mathbb{S}^\mu\left(\mathbb{R}^m\right)^{\mathbf{O_m}} \subset M^\lambda$ se comporte comme un polynôme de plus bas degré sur la variété drapeau. Finalement, on a démontré la proposition suivante.

Proposition 5.1. — *La décomposition de $\mathscr{L}^2\left(\mathscr{D}_\mathrm{d}\right)$ sous l'action de $\mathbf{O}_n(\mathbb{R})$ est*

$$\mathscr{L}^2\left(\mathscr{D}_\mathrm{d}\right) \cong \bigoplus_\mu \mathbb{S}^{[\mu]}\left(\mathbb{R}^n\right) \otimes N^\mu \cong \bigoplus_\mu \mathbb{S}^{[\mu]}\left(\mathbb{R}^n\right)^{\oplus n_\mu} \tag{5.3}$$

où μ parcourt l'ensemble des partitions à moins de m et $n/2$ parts et n_μ désigne la multiplicité de la composante isotypique de poids μ, autrement dit la dimension, éventuellement nulle, du sous-espace invariant $N^\mu = \mathbb{S}^\mu\left(\mathbb{R}^m\right)^{\mathbf{O_m}}$.

Nous munissons cet espace du produit scalaire $\langle f, g\rangle = \int_{\mathscr{D}_\mathrm{d}} f\cdot g$, qui est proportionnel au produit scalaire déjà défini $[\cdot,\cdot]$ sur chaque composante irréductible sous $\mathbf{O}_n \times \mathbf{O_m}$ de $\mathscr{L}^2\left(\mathscr{D}_\mathrm{d}\right)$.

5.1.1.2 Description des espaces de multiplicité

Décrivons enfin quelques-uns des sous-espaces stables N^μ qui contrôlent la multiplicité de chaque composante isotypique. À cette fin, nous calculons par exemple l'image de l'endomorphisme de $\mathbb{S}^\mu\left(\mathbb{R}^m\right)$ défini par un procédé de moyenne sur l'ensemble du groupe $\varphi : V \mapsto \int_{\mathbf{O_m}} \tau\cdot V\,\mathrm{d}\tau$. Si Θ est un tableau standard, dont le contenu n'est pas pair pour l'un des entiers disons v, alors, en échangeant dans e_Θ le vecteur e_v par son opposé, on peut écrire que $\varphi(e_T) = \varphi(-e_T) = 0$. Ainsi on justifie que

Lemme 5.2. — *Les dimensions $n_{\ydiagram{1}}$, $n_{\ydiagram{3}}$, $n_{\ydiagram{2,1}}$, $n_{\ydiagram{1,1,1}}$, $n_{\ydiagram{2,1,1}}$, $n_{\ydiagram{1,1,1,1}}$ s'évanouissent*[1] *toutes.*

Par ailleurs, les autres espaces de multiplicité de degré inférieur à 4 se comportent comme suit.

Lemme 5.3. — 1. *L'espace $N^{\ydiagram{2}}$ est de dimension $n_{\ydiagram{2}} = \ell$; il est engendré par les vecteurs $\displaystyle\sum_{d_i\leqslant v<d_{i-1}} \boxed{\varepsilon_v}\boxed{\varepsilon_v}$ pour i entre 1 et ℓ.*

2. *L'espace $N^{\ydiagram{3}}$ est de dimension $n_{\ydiagram{3}} = \frac{\ell(\ell+1)}{2}$; il est engendré par les vecteurs $\displaystyle\sum_{\substack{d_i\leqslant v<d_{i-1}\\ d_i\leqslant w<d_{i-1}}} \boxed{\varepsilon_v}\boxed{\varepsilon_v}\boxed{\varepsilon_w}\boxed{\varepsilon_w}$ pour $i\leqslant j$ compris entre 1 et ℓ.*

[1] comme eût dit Hermite

3. *L'espace* $N^{\boxplus}$ *est de dimension* $n_{\boxplus} = \ell$ *; il est engendré par les vecteurs* $\displaystyle\sum_{d_i \leqslant v < w < d_{i-1}} \begin{array}{|c|c|}\hline \varepsilon_w & \varepsilon_w \\ \hline \varepsilon_v & \varepsilon_v \\ \hline \end{array}$ *pour* $i \leqslant j$ *entre* 1 *et* ℓ.

Preuve. — En effet, les vecteurs $\boxed{\varepsilon_v}\boxed{\varepsilon_v}$ et $\boxed{\varepsilon_{v'}}\boxed{\varepsilon_{v'}}$ appartiennent à la même orbite sous l'action de $\mathbf{O_m}$ du moment que $d_i \leqslant v, v' < d_{i-1}$. Par suite $\varphi(\boxed{\varepsilon_v}\boxed{\varepsilon_v})$ et $\varphi(\boxed{\varepsilon_{v'}}\boxed{\varepsilon_{v'}})$ sont égaux. Aussi, $\varphi(\boxed{\varepsilon_v}\boxed{\varepsilon_v}) = \dfrac{1}{d_{i-1} - d_i} \displaystyle\sum_{d_i \leqslant v < d_{i-1}} \boxed{\varepsilon_v}\boxed{\varepsilon_v}$. Mais $\displaystyle\sum_{d_i \leqslant v < d_{i-1}} \boxed{\varepsilon_v}\boxed{\varepsilon_v}$ est invariant sous $\mathbf{O_m}$, ce qui achève la justification. Les autres cas se traitent de la même manière. □

Cette étude peut se résumer par la proposition suivante.

Proposition 5.4. — *L'espace des fonctions polynomiales de degré inférieur à 4 est réduit à*

$$\mathbb{R} \oplus \mathbb{S}^{[\square]}(\mathbb{R}^n) \otimes N^{\square} \oplus \mathbb{S}^{[\boxplus]}(\mathbb{R}^n) \otimes N^{\boxplus} \oplus \mathbb{S}^{[\square\square]}(\mathbb{R}^n) \otimes N^{\square\square}. \tag{5.4}$$

Définition 5.5. — On définit le vecteur $\Upsilon_{d_\iota} = \displaystyle\sum_{v \leqslant d_\iota} \boxed{\varepsilon_v}\boxed{\varepsilon_v} \in N^{\square}$ for $1 \leqslant \iota \leqslant s$; ces vecteurs forment une base de $N^{\square}$.

5.1.2 Fonctions zonales

Définition 5.6. — Pour tout sous-$\mathbf{O}_n(\mathbb{R})$-module $\mathscr{V}$ de $\mathscr{L}^2(\mathscr{D}_{\mathrm{d}})$, on appelle *fonction zonale* toute fonction $Z : \mathscr{D}_{\mathrm{d}} \times \mathscr{D}_{\mathrm{d}} \to \mathbb{R}$ qui jouit des propriétés suivantes

1. pour tout drapeau $\Delta_0 \in \mathscr{D}_{\mathrm{d}}$ de forme d, les applications $Z(\Delta_0, \cdot)$ et $Z(\cdot, \Delta_0)$ appartiennent à l'espace $\mathscr{V}$,
2. pour toute transformation orthogonale $\tau \in \mathbf{O}_n(\mathbb{R})$, on a

$$Z(\tau \cdot \Delta, \tau \cdot \Delta') = Z(\Delta, \Delta'). \tag{5.5}$$

On note $\mathcal{Z}(\mathscr{V})$ leur ensemble.

La construction ci-dessous justifie la non-vacuité de cet espace.

Soit $(h_i)_{1 \leqslant i \leqslant f^n_{[\mu]}}$ une base orthonormée de $\mathbb{S}^{[\mu]}(\mathbb{R}^n)$, au sens du produit scalaire $[\cdot, \cdot]$. Étant donné Ξ et Ξ' dans N^μ, on définit l'application $Z_{\Xi,\Xi'}(\Delta, \Delta')$ par

$$Z_{\Xi,\Xi'}(\Delta, \Delta') = \frac{1}{f^n_{[\mu]}} \sum_{i=1}^{f^n_{[\mu]}} (h_i \otimes \Xi)(\Delta) \cdot (h_i \otimes \Xi')(\Delta'), \tag{5.6}$$

où le produit $(h_i \otimes \Xi)$ est plongé dans $\mathbb{R}[Z]$ au sens de l'isomorphisme noté ψ au paragraphe 2.2.5. L'expression $Z_{\Xi,\Xi'}$ est bilinéaire en Ξ et Ξ'.

Proposition 5.7. — *Soient* Ξ *et* Ξ' *deux éléments de* N^μ,

1. $Z_{\Xi,\Xi'}(\Delta, \Delta')$ *ne dépend pas du choix de la base orthonormale* $(h_i)_{1 \leqslant i \leqslant f^n_{[[\mu]]}}$.
2. *L'application* $Z_{\Xi,\Xi'}$ *appartient à* $\mathcal{Z}\left(\mathscr{L}^2(\mathscr{D}_{\mathrm{d}})\right)$ *et envoie* $(\mathbb{S}^{[\mu]}(\mathbb{R}^n) \otimes \Xi)$ *sur* $(\mathbb{S}^{[\mu]}(\mathbb{R}^n) \otimes \Xi')$ *par convolution.*

Démonstration. — Soit $(h'_i)_{1\leqslant i\leqslant f^n_{[\mu]}}$ une autre base orthonormée de $\mathbb{S}^{[\mu]}(\mathbb{R}^n)$, que l'on exprime en fonction de la première base par $h'_i = \sum_{j=1}^{f^n_{[\mu]}} \alpha_{j,i} h_i$ pour tout i. Alors, par linéarité du projecteur ψ et par orthogonalité des coefficients $((\alpha_{j,i}))_{1\leqslant j,i\leqslant f^n_{[\mu]}}$,

$$\begin{aligned}
&\sum_{i=1}^{f^n_{[\mu]}} (h'_i \otimes \Xi)(\Delta)\cdot(h'_i\otimes\Xi')(\Delta') \\
=\ & \sum_{1\leqslant i,j,j'\leqslant f^n_{[\mu]}} \alpha_{j,i}\alpha_{j',i}(h_j\otimes\Xi)(\Delta)\cdot(h_{j'}\otimes\Xi')(\Delta') \\
=\ & \sum_{1\leqslant j,j'\leqslant f^n_{[\mu]}} \left(\sum_{i=1}^{f^n_{[\mu]}} \alpha_{j,i}\alpha_{j',i}\right)(h_j\otimes\Xi)(\Delta)\cdot(h_{j'}\otimes\Xi')(\Delta') \\
=\ & Z_{\Xi,\Xi'}(\Delta,\Delta').
\end{aligned}$$

Le second point n'est qu'une reformulation du premier, en tenant compte du fait que le produit scalaire est $\mathbf{O}_n(\mathbb{R})$ invariant. □

Lemme 5.8. — *Soit $\mathscr{V}$ un sous-$\mathbf{O}_n(\mathbb{R})$-module de $\mathscr{L}^2(\mathscr{D}_{\mathrm{d}})$. Si la dimension de $\mathcal{Z}(\mathscr{V})$ est inférieure à 1, alors, $\mathscr{V}$ est irréductible.*

Ce lemme est assez classique (voir par exemple [Ven01]). Il en résulte que $\mathcal{Z}\left(\mathscr{L}^2(\mathscr{D}_{\mathrm{d}})\right)$ est totalement décrit par les fonctions $(Z_{\Xi,\Xi'})_{(\Xi,\Xi')\in N^\mu}$ lorsque μ varie.

Calculs Dans le cas des grassmanniennes, c'est-à-dire lorsque $\ell = 1$, la multiplicité des espaces isotypiques n'excède jamais 1 ; les fonctions zonales ont été calculées dans [JC74]. Nous calculons quelques fonctions zonales pour $\mu = \square\square$, $\Xi = \Upsilon_{d_\iota}$ et $\Xi' = \Upsilon_{d_{\iota'}}$.

L'espace $J^{\square\square}$ est engendré par $\sum_{i=1}^n \boxed{e_i}\boxed{e_i}$ d'une part. D'autre part, les vecteurs sans violations (*cf.* définition de ces vecteurs au paragraphe 2.2.6) sont les $\left(\boxed{e_i}\boxed{e_j}\right)_{1\leqslant i<j\leqslant n}$, qui sont déjà orthogonaux à $J^{\square\square}$, et les $\left(\boxed{e_i}\boxed{e_i}\right)_{2\leqslant i\leqslant n}$. Les projetés de ces derniers sont les vecteurs suivants $\left(\boxed{e_i}\boxed{e_i} - \boxed{e_1}\boxed{e_1}\right)_{2\leqslant i\leqslant n}$, dont la matrice de Gram (de dimension $(n-1)\times(n-1)$) a pour inverse

$$\begin{pmatrix} 2 & 1 & \cdots & 1 \\ 1 & 2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \cdots & 1 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} \frac{n-1}{n} & -\frac{1}{n} & \cdots & -\frac{1}{n} \\ -\frac{1}{n} & \frac{n-1}{n} & \ddots & \vdots \\ \vdots & \ddots & \ddots & -\frac{1}{n} \\ -\frac{1}{n} & \cdots & -\frac{1}{n} & \frac{n-1}{n} \end{pmatrix}.$$

En toute généralité, $Z_{\boxed{\varepsilon_j}\boxed{\varepsilon_j},\boxed{\varepsilon_{j'}}\boxed{\varepsilon_{j'}}}(X_\Delta, X_{\Delta'})$ est égal à :

$$\sum_{2\leqslant i\leqslant n}(x^2_{i,j}-x^2_{1,j})(x'^2_{i,j'}-x'^2_{1,j'}) - \frac{1}{n}\sum_{2\leqslant i,i'\leqslant n}(x^2_{i,j}-x^2_{1,j})(x'^2_{i',j'}-x'^2_{1,j'}) + \sum_{1\leqslant i\neq i'\leqslant n} x_{i,j}x_{i',j}\,x'_{i,j'}x'_{i',j'}.$$

Comme le groupe $\mathbf{O}_n(\mathbb{R})$ agit transitivement sur l'ensemble des drapeaux, nous pouvons nous contenter de calculer $Z_{\Upsilon_{d_\iota},\Upsilon_{d_{\iota'}}}(\Delta_0,\Delta)$ où Δ_0 est le drapeau de forme λ engendré par les vecteurs $(e_i)_{1\leqslant i\leqslant s}$, ce qui revient à remplacer $x_{i,j}$ par le symbole de Kronecker $\delta_{i,j}$. Tous calculs faits, on obtient

$$Z_{\Upsilon_{d_\iota},\Upsilon_{d_{\iota'}}}(\Delta_0,\Delta) = \sum_{\substack{1\leqslant i\leqslant d_\iota\\ 1\leqslant j\leqslant d_{\iota'}}} x_{i,j}^2 - \frac{d_\iota}{n}\sum_{\substack{d_\iota<i\leqslant n\\ 1\leqslant j\leqslant d_{\iota'}}} x_{i,j}^2.$$

La première somme s'identifie à la somme des normes carrées des projetés des $d_{\iota'}$ premiers vecteurs de X_Δ sur l'espace $(\Delta_0)_\iota$, autrement dit à la trace $\mathrm{Tr}(\mathrm{pr}_{(\Delta_0)_\iota}\circ \mathrm{pr}_{(\Delta)_{\iota'}})$ ou encore à la somme des cosinus carrés des angles principaux définis entre $(\Delta_0)_\iota$ et $\Delta_{\iota'}$. La seconde somme vaut $d_{\iota'}$ car X_Δ est une matrice aux colonnes orthonormées.

En général, on a donc

$$Z_{\Upsilon_{d_\iota},\Upsilon_{d_{\iota'}}} = \mathrm{Tr}(\mathrm{pr}_{\Delta_\iota}\circ \mathrm{pr}_{\Delta_{\iota'}}) - \frac{d_\iota d_{\iota'}}{n}. \tag{5.7}$$

5.1.3 Définition des designs vexillaires

Définition 5.9. — On appelle *t-design vexillaire*[2] tout sous-ensemble $\mathcal{D}$ fini de la variété drapeau $\mathscr{D}_\mathrm{d}$ tel que pour toute fonction f polynomiale de degré inférieur à t, c'est-à-dire une fonction appartenant à $\bigoplus_{\substack{|\mu|\leqslant t\\ \lfloor\mu\rfloor\leqslant m}} \mathbb{S}^{[\mu]}(\mathbb{R}^n)^{\oplus n_\mu}$, la formule de quadrature

$$\int_{\mathscr{D}_\mathrm{d}} f(\Delta)\,\mathrm{d}\Delta = \frac{1}{|\mathcal{D}|}\sum_{\Delta\in\mathcal{D}} f(\Delta) \tag{5.8}$$

est en réalité une égalité.

Remarque 5.10. — Lorsque la partition $\check{\lambda}$ n'a qu'une part, on retombe sur la notion de *design grasmannien* introduits dans l'article [BCN02]. En particulier, si $\lambda=\square$, il s'agit même de *designs sphériques*.

Exemple 5.11. — Les vecteurs minimaux de $\mathbb{A}_2$ forment un 5-design. (Voir illustration 5.1).

Théorème 5.12. — *Les conditions suivantes sont équivalentes :*

1. *L'ensemble $\mathcal{D}$ est un t-design vexillaire.*
2. *Pour tout polynôme homogène de degré inférieur à t, pour toute transformation orthogonale $\tau\in\mathbf{O}_n(\mathbb{R})$, on a*

$$\sum_{\Delta\in\mathcal{D}} f(\Delta) = \sum_{\Delta\in\mathcal{D}} f(\tau\cdot\Delta). \tag{5.9}$$

3. *Pour toute partition μ de degré $0<|\mu|\leqslant t$, pour tout Ξ appartenant à $N^\mu=\mathbb{S}^\mu(\mathbb{R}^m)^{\mathbf{O}_\mathbf{m}(\mathbb{R})}$ et pour toute fonction f de $(\mathbb{S}^{[\mu]}(\mathbb{R}^n)\otimes\Xi)$, la somme $\sum_{\Delta\in\mathcal{D}} f(\Delta)$ est nulle.*

[2] relatif aux drapeaux ; du latin *vexillarius*, porte–étendard des légions romaines.

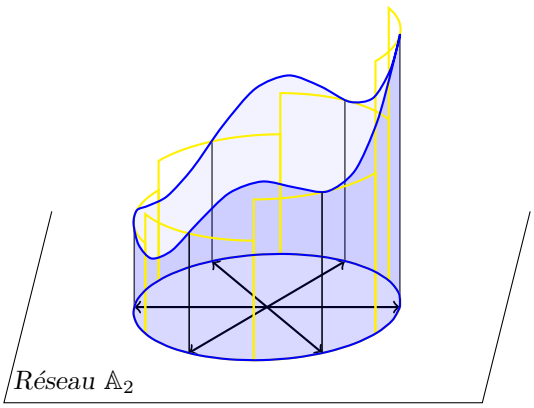
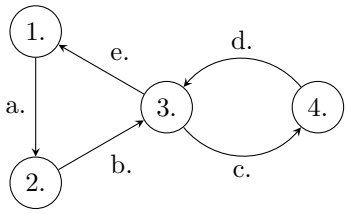


FIG. 5.1 – Représentation du 4-design sphérique associé à $\mathbb{A}_2$

4. *Pour toute partition μ de degré $0 < |\mu| \leqslant t$, pour tous Ξ et Ξ' appartenant à N^μ et pour tout $\Delta' \in \mathscr{D}_{\mathrm{d}}$,*

$$\sum_{\Delta \in \mathcal{D}} Z_{\Xi,\Xi'}(\Delta, \Delta') = 0. \tag{5.10}$$

Démonstration. — Nous démontrons les différentes implications selon le schéma suivant.



- a. Comme la mesure $\mathrm{d}\Delta$ est invariante par le changement de variable $\Delta \mapsto \tau \cdot \Delta$, on a en utilisant deux fois l'équation (5.8)

$$\sum_{\Delta \in \mathcal{D}} f(\Delta) = |\mathcal{D}| \int_{\mathscr{D}_{\mathrm{d}}} f(\Delta)\,\mathrm{d}\Delta = |\mathcal{D}| \int_{\mathscr{D}_{\mathrm{d}}} f(\tau \cdot \Delta)\,\mathrm{d}\Delta = \sum_{\Delta \in \mathcal{D}} f(\tau \cdot \Delta).$$

- b. L'application $(\mathbb{S}^{[\mu]}(\mathbb{R}^n) \otimes \Xi) \to \mathbb{R}$ définie par $f \mapsto \sum_{\Delta \in \mathcal{D}} f(\Delta)$ est une application linéaire. Son noyau est un sous-espace $\mathbf{O}_n(\mathbb{R})$-irréductible et non-trivial à cause du théorème du rang. Il ne peut s'agir que de $(\mathbb{S}^{[\mu]}(\mathbb{R}^n) \otimes \Xi)$ tout entier, ce qui justifie la nullité de la somme.
- c. Cette implication provient de l'appartenance de $Z_{\Xi,\Xi'}(\cdot, \Delta')$ à l'espace $(\mathbb{S}^{[\mu]}(\mathbb{R}^n) \otimes \Xi)$.
- d. L'ensemble des fonctions $Z_{\Xi,\Xi'}(\cdot, \Delta')$ engendre sous l'action de $\mathbf{O}_n(\mathbb{R})$ un espace irréductible non-nul, qui par suite ne peut être que $(\mathbb{S}^{[\mu]}(\mathbb{R}^n) \otimes \Xi)$. La nullité de la somme s'étend par conséquent à l'espace tout entier.
- e. Soit f une fonction de degré inférieur à t, que l'on peut décomposer par projection sur les composantes isotypiques en $f = \sum_{|\mu| \leqslant t} f_\mu$. L'intégrale

peut se calculer comme suit

$$\int_{\mathscr{D}_{\mathrm{d}}} f(\Delta)\,\mathrm{d}\Delta = \langle f, \mathbf{1}\rangle = \langle f_0, \mathbf{1}\rangle = \frac{1}{|\mathcal{D}|}\sum_{\Delta\in\mathcal{D}} f_0(\Delta) = \frac{1}{|\mathcal{D}|}\sum_{\Delta\in\mathcal{D}} f(\Delta)$$

en tenant compte de l'orthogonalité entre eux des espaces $\mathbb{S}^{[\mu]}\left(\mathbb{R}^n\right)^{\oplus n_\mu}$ et de l'hypothèse.

□

À l'image des articles [LST01] et [BCN02], nous disposons du théorème suivant, qui relie les t-designs avec la théorie des groupes.

Théorème 5.13. — *Soit G un sous-groupe fini du groupe orthogonal $\mathbf{O}_n(\mathbb{R})$, alors sont équivalentes les propriétés suivantes :*

1. *La décomposition de l'espace vectoriel $\bigoplus_{\substack{|\mu|\leqslant t\\ \lfloor\mu\rfloor\leqslant m}} \mathbb{S}^{[\mu]}\left(\mathbb{R}^n\right)^{\oplus n_\mu}$ en G-modules invariants ne fait apparaître la représentation triviale $\mathbf{1_G}$ qu'une seule fois.*
2. *Pour tout drapeau Δ_0, l'orbite $G\cdot\Delta_0$ de Δ_0 sous l'action de G forme un t-design vexillaire.*

Démonstration. — Pour une partition μ de degré $0<|\mu|\leqslant t$ et des éléments Ξ et Ξ' de N^μ, on considère l'application $\Delta\mapsto\sum_{g\in G} Z_{\Xi,\Xi'}(g\cdot\Delta,\Delta')$, où $\Delta'\in\mathscr{D}_{\mathrm{d}}$ est fixé. Il s'agit d'une application G-invariante de $(\mathbb{S}^{[\mu]}\left(\mathbb{R}^n\right)\otimes\Xi)$. Mais compte tenu du point 1, seules les fonctions constantes peuvent être G-invariantes et non-nulles simultanément. Donc $\sum_{\Delta\in G\cdot\Delta_0} Z_{\Xi,\Xi'}(\Delta,\Delta')=0$, ce qui est une condition nécessaire et suffisante (cf 4. du théorème 5.12) pour que $G\cdot\Delta_0$ soit un t-design.

Réciproquement, si la représentation triviale $\mathbf{1_G}$ apparaît plus d'une fois parmi $\bigoplus_{\substack{|\mu|\leqslant t\\ \lfloor\mu\rfloor\leqslant m}} \mathbb{S}^{[\mu]}\left(\mathbb{R}^n\right)^{\oplus n_\mu}$, c'est qu'il existe une fonction G-invariante et non identiquement nulle f qui appartient à l'un des espaces $(\mathbb{S}^{[\mu]}\left(\mathbb{R}^n\right)\otimes\Xi)$ avec $0<|\mu|\leqslant t$. Pour un certain drapeau Δ_0, $f(\Delta_0)$ est non-nul, et $\sum_{\Delta\in G\cdot\Delta_0} f(\Delta) = |G|\cdot f(\Delta_0)$ est non-nul aussi. Donc $G\cdot\Delta_0$ n'est pas un t-design. □

Corollaire 5.14. — *Pour que l'orbite $G\cdot\Delta_0$ d'un drapeau Δ_0 sous l'action d'un sous-groupe G fini du groupe orthogonal $\mathbf{O}_n(\mathbb{R})$ forme un t-design, il faut et il suffit que l'orbite du sous-espace de dimension maximale $(\Delta_0)_1$ forme un t-design.*

Preuve. — Aux multiplicités près, les composantes isotypiques non-vides qui apparaissent dans la décomposition de $\bigoplus_{\substack{|\mu|\leqslant t\\ \lfloor\mu\rfloor\leqslant m}} \mathbb{S}^{[\mu]}\left(\mathbb{R}^n\right)^{\oplus n_\mu}$ demeurent les mêmes lorsqu'on se restreint aux grassmanniennes de dimension m. □

Exemple 5.15. — La recherche de designs grassmanniens apparaissant comme orbite d'un seul sous-espace sous l'action d'un groupe a été entreprise dans différents articles, notamment [BCN02] et surtout [Bac05] qui fait le bilan dans le cas de réseau de petite dimension.

5.2 Réseaux fortement parfaits

Commençons par rappeler quelques résultats et notations issus des chapitres précédents.

À un drapeau de réseaux $\Lambda = (\Lambda_1, \ldots, \Lambda_{\check{\lambda}})$, nous associons la *somme des projections* orthogonales pr_{Λ_i} sur l'espace vectoriel engendré par Λ_i,

$$\Pi_\Lambda = \sum_{i=1}^{\check{\lambda}} \mathrm{pr}_{\Lambda_i}, \tag{5.11}$$

qui est un endomorphisme symétrique.

Les définitions 3.18 reformulées en termes de réseaux adoptent la tournure suivante.

Définition 5.16. —
1. Un réseau est dit *parfait* relativement à la partition λ si les endomorphismes de la famille $(\Pi_\Lambda)_{\Lambda \in \mathscr{S}(L)}$ engendrent l'espace des endomorphismes symétriques.
2. Un réseau est dit *eutactique* relativement à la partition λ si l'identité est une combinaison linéaire à coefficients strictement positifs de toutes les sommes de projections $(\Pi_\Lambda)_{\Lambda \in \mathscr{S}(L)}$.
3. Un réseau est dit *extrême* relativement à la partition λ s'il réalise un maximum local de $\gamma(L)$.

Nous ajoutons deux définitions supplémentaires :

Définition 5.17. —
1. On dit qu'un réseau est *fortement parfait* relativement à la partition λ si l'ensemble de ses drapeaux minimaux constitue un 4-design.
2. On dit qu'un réseau est *fortement eutactique* relativement à la partition λ s'il est eutactique et que ses coefficients d'eutaxie sont identiques.

Proposition 5.18. — *Un réseau dont l'ensemble des drapeaux minimaux est habité d'une structure de 2-design est fortement eutactique.*

Démonstration. — Nous allons montrer que la somme $S = \sum_{\Lambda \in \mathscr{S}(L)} \Pi_\Lambda$ est proportionnelle à l'identité. Précisément, un calcul de trace indique que la seule constante c possible est $\frac{|\lambda| \cdot s_\lambda}{n}$. Comme l'ensemble des sommes de projecteurs Π_{Δ_0} engendre l'espace des endomorphismes symétriques lorsque Δ_0 décrit l'ensemble des drapeaux, il suffit de vérifier que $\langle S, \Pi_{\Delta_0} \rangle = \frac{s_\lambda \cdot |\lambda|^2}{n}$. Comme d'une part

$$\langle \Pi_\Lambda, \Pi_{\Delta_0} \rangle = \sum_{q, q' \in \check{\lambda}} \left(Z_{\Upsilon_q, \Upsilon_{q'}}(\Lambda, \Delta_0) + \frac{qq'}{n} \right)$$

d'après le calcul 5.7 et d'autre part la somme $\sum_{\Lambda \in \mathscr{S}(L)} Z_{\Upsilon_{\check{\lambda}_i}, \Upsilon_{\check{\lambda}_i}}(\Lambda, \Delta_0)$ est nulle d'après le théorème 5.12 de caractérisation des designs, cette égalité est satisfaite. □

Théorème 5.19. — *Relativement à une partition λ, un réseau fortement parfait est extrême.*

Démonstration. — Compte tenu du théorème à la Voronoï 3.21 et de la proposition 5.18, il reste encore à démontrer que la forte perfection implique la perfection, autrement dit que le fait que les drapeaux minimaux forment 4-design implique que le rang des applications $(\Pi_\Lambda)_{\Lambda\in\mathscr{S}(L)}$ est maximal.

À cette fin, nous montrons que la matrice $C = \big(\langle \Pi_\Delta, \Pi_{\Delta'}\rangle\big)_{\Delta,\Delta'\in\mathscr{S}(L)}$ admet pour rang $n\,(n+1)/2$. Notons dans un premier temps P la matrice $P_{\Upsilon_{\check\lambda_{\iota_1}},\Upsilon_{\check\lambda_{\iota_2}}} = \big(Z_{\Upsilon_{\check\lambda_{\iota_1}},\Upsilon_{\check\lambda_{\iota_2}}}(\Delta,\Delta')\big)_{\Delta,\Delta'\in\mathscr{S}(L)}$ et calculons le produit de matrices $P_{\Upsilon_{\check\lambda_{\iota_1}},\Upsilon_{\check\lambda_{\iota_2}}} \cdot P_{\Upsilon_{\check\lambda_{\iota_3}},\Upsilon_{\check\lambda_{\iota_4}}}$

$$\begin{aligned}
&\sum_{\Delta''\in\mathscr{S}(L)} Z_{\Upsilon_{\check\lambda_{\iota_1}},\Upsilon_{\check\lambda_{\iota_2}}}(\Delta,\Delta'')Z_{\Upsilon_{\check\lambda_{\iota_3}},\Upsilon_{\check\lambda_{\iota_4}}}(\Delta'',\Delta')\\
=\ &\frac{1}{N^2}\sum_{\Delta''\in\mathscr{S}(L)}\sum_{1\leqslant i,j\leqslant N}(h_i\otimes\Upsilon_{\check\lambda_{\iota_1}})(\Delta)(h_i\otimes\Upsilon_{\check\lambda_{\iota_2}})(\Delta'')(h_j\otimes\Upsilon_{\check\lambda_{\iota_3}})(\Delta'')(h_j\otimes\Upsilon_{\check\lambda_{\iota_4}})(\Delta')\\
=\ &\frac{1}{N^2}\sum_{1\leqslant i,j\leqslant N}(h_i\otimes\Upsilon_{\check\lambda_{\iota_1}})(\Delta)(h_j\otimes\Upsilon_{\check\lambda_{\iota_4}})(\Delta')\sum_{\Delta''\in\mathscr{S}(L)}(h_i\otimes\Upsilon_{\check\lambda_{\iota_2}})(\Delta'')(h_j\otimes\Upsilon_{\check\lambda_{\iota_3}})(\Delta'').
\end{aligned}$$

Cependant, l'application $f : \Delta'' \mapsto (h_i\otimes\Upsilon_{\check\lambda_{\iota_2}})(\Delta'')(h_j\otimes\Upsilon_{\check\lambda_{\iota_3}})(\Delta'')$, qui est de degré 4, peut se décomposer en somme sur les composantes isotypiques

$$f = f_0 + f_{\square} + f_{\boxplus} + f_{\square\square\square}.$$

Comme $\mathcal{S}(\Delta)$ est un 4-design, la somme des termes de degré supérieur à deux $\sum_{\Delta''\in\mathscr{S}(L)} f_{\square}(\Delta'')+f_{\boxplus}(\Delta'')+f_{\square\square\square}(\Delta'')$ s'évanouit. Le terme constant se calcule d'autre part comme suit : $f_0 = \langle f, \mathbf{1}\rangle\,\mathbf{1} = \left\langle h_i\otimes\Upsilon_{\check\lambda_{\iota_2}}, h_j\otimes\Upsilon_{\check\lambda_{\iota_3}}\right\rangle\mathbf{1} = \frac{\kappa_{i,j}}{n}\delta_{i,j}\mathbf{1}$, où $\delta_{i,j}$ est le symbole de Kronecker et $\kappa_{i,j} = n\cdot\min(\check\lambda_i,\check\lambda_j)) - \check\lambda_i\check\lambda_j$. Alors la somme totale ci-dessus devient :

$$\begin{aligned}
\sum_{\Delta''\in\mathscr{S}(L)}(h_i\otimes\Upsilon_{\check\lambda_{\iota_2}})(\Delta'')(h_j\otimes\Upsilon_{\check\lambda_{\iota_3}})(\Delta'') &= \sum_{\Delta''\in\mathscr{S}(L)} f_0(\Delta'')\\
&= \frac{s_\lambda\cdot\kappa_{\iota_2,\iota_3}}{n}\delta_{i,j}.
\end{aligned}$$

Finalement, on a démontré que le produit est :

$$P_{\Upsilon_{\check\lambda_{\iota_1}},\Upsilon_{\check\lambda_{\iota_2}}}\cdot P_{\Upsilon_{\check\lambda_{\iota_3}},\Upsilon_{\check\lambda_{\iota_4}}} = \frac{s_\lambda\cdot\kappa_{\iota_2,\iota_3}}{Nn}P_{\Upsilon_{\check\lambda_{\iota_1}},\Upsilon_{\check\lambda_{\iota_4}}}.$$

Alors, en notant J la matrice ne comptant que des 1, on a

$$C = \sum_{q,q'\in\check\lambda} P_{\Upsilon_q,\Upsilon_{q'}} + \frac{|\lambda|^2}{n}J. \tag{5.12}$$

On appele κ la constante $\kappa = \sum_{1\leqslant i,j\leqslant s}\kappa_{\lambda_i,\lambda_j}$, de sorte que

$$\left(\sum_{q,q'\in\check\lambda} P_{\Upsilon_q,\Upsilon_{q'}}\right)^2 = \frac{s_\lambda\cdot\kappa}{Nn}\sum_{q,q'\in\check\lambda} P_{\Upsilon_q,\Upsilon_{q'}}. \tag{5.13}$$

Compte tenu des relations de commutations $JP_{\Upsilon_{\breve{\lambda}_{\iota_1}},\Upsilon_{\breve{\lambda}_{\iota_2}}} = 0 = P_{\Upsilon_{\breve{\lambda}_{\iota_1}},\Upsilon_{\breve{\lambda}_{\iota_2}}} J$, qui proviennent du fait que $\mathscr{S}(L)$ est un 2-design, et on peut dégager par élévation au carré

$$C^2 = \frac{s_\lambda \kappa}{Nn} \sum_{q,q' \in \breve{\lambda}} P_{\Upsilon_q,\Upsilon_{q'}} + \frac{|\lambda|^4}{n^2} s_\lambda J = \frac{s_\lambda \kappa}{Nn} C + \frac{s_\lambda}{n^2} \left(|\lambda|^4 - \frac{\kappa |\lambda|^2}{N} \right) J.$$

Finalement,

$$C^2 = \frac{s_\lambda \kappa}{nN} C + \frac{s_\lambda |\lambda|^2}{n^2} \left(|\lambda|^2 - \frac{\kappa}{N} \right) J. \tag{5.14}$$

Comme les matrices C^2, C et J commutent et sont symétriques, elles sont simultanément diagonalisables. La matrice J possède deux valeurs propres qui sont s_λ avec multiplicité 1 et 0 avec multiplicité $s_\lambda - 1$. Appelons $(\omega_i)_{1 \leqslant i \leqslant s}$ les valeurs propres de C, en prenant soin d'associer ω_1 au vecteur propre $(1, \ldots, 1)$. Comme $nCJ = |\lambda|^2 s_\lambda J$, ce qui peut s'obtenir par multiplication de (5.12) par J, nous avons $\omega_1 = \frac{|\lambda|^2 s_\lambda}{n}$. Ensuite, en utilisant (5.14), on obtient que pour tout $i \geqslant 2$, $n^2 \omega_i^2 = \frac{\kappa s_\lambda n}{N} \omega_i$, d'où l'on tire les valeurs admissibles pour pour les valeurs propres : $\omega_i = 0$ ou bien $\omega_i = \frac{s_\lambda \kappa}{nN}$. En notant α la multiplicité de cette dernière valeur propre, on extrait par un calcul de trace

$$\mathrm{Tr}(C) = s_\lambda \sum_{i=1}^{s} (2i-1) \breve{\lambda}_i = \frac{|\lambda|^2 s_\lambda}{n} + \alpha \frac{s_\lambda \kappa}{nN}.$$

On en acquiert la valeur de α

$$\alpha = \frac{nN}{\kappa} \left(\sum_{i=1}^{s} (2i-1) \breve{\lambda}_i - \frac{|\lambda|^2}{n} \right) = N = \frac{n(n+1)}{2} - 1.$$

Comme les $(\kappa_{i,j})$ et κ lui-même sont tous strictement positifs, le rang de C est exactement égal à $\frac{n(n+1)}{2}$ et le réseau L est parfait. □

5.3 Calculs

Dans chacun des cas suivants, on applique le critère du théorème 5.13 au groupe d'automorphisme du réseau pour montrer que toute orbite de drapeau est au moins un 4-design vexillaire. En conséquence, les réseaux sont fortement parfaits et par conséquent extrêmes.

Proposition 5.20. — *1. Les orbites d'un drapeau sous l'action du groupe d'automorphisme des réseaux K'_{10}, ${K'_{10}}^*$ et du réseau de Coxeter–Todd K_{12} sont des 4-designs sphériques mais seulement des 2-designs vexillaires lorsque $\lfloor \lambda \rfloor \geqslant 2$.*

2. Les orbites d'un drapeau sous l'action du groupe d'automorphisme des réseaux $\mathbb{D}_4$, $\mathbb{E}_6$, $\mathbb{E}_7$ sont des 4-designs vexillaires.

3. L'orbite d'un drapeau sous l'action du groupe d'automorphisme de $\mathbb{E}_8$ est un 6-design vexillaire.

4. L'orbite d'un drapeau sous l'action du groupe d'automorphisme de Λ_{24} est un 10-design vexillaire.

Preuve. — La justification procède de la même manière que [BCN02]. Pour vérifier que la représentation triviale d'un groupe dans $\bigoplus_{\substack{|\mu|\leqslant 2t \\ \lfloor\mu\rfloor\leqslant m}} \mathbb{S}^{[\mu]}(\mathbb{R}^n)^{\oplus n_\mu}$ est de multiplicité un, on compare son nombre d'occurence dans $\mathrm{Sym}^t(\mathrm{Sym}^2(\mathbb{R}^n))$ en tant que G-module avec le nombre d'occurrence de la représentation triviale en tant que $\mathbf{O}(n)$-module. La théorie des caractères fournit un outil approprié pour effectuer cette comparaison.

Pour les réseaux $\mathbb{D}_4$, $\mathbb{E}_6$, $\mathbb{E}_7$, $\mathbb{E}_8$ et Λ_{24}, le premier polynôme invariant apparaît pour une partition en ligne, ce qui justifie que les drapeaux minimaux sont des t-designs indépendamment de la forme λ. Le degré coïncide avec le degré du design annoncé dans l'énoncé de la proposition. Par contre pour les réseaux K'_{10}, ${K'_{10}}^*$, K_{12}, le polynôme invariant de plus bas degré apparaît pour la partition $\lambda = \boxplus$, ce qui explique pourquoi le degré du design dépend de la forme. □

Théorème 5.21. — *Les réseaux de racine $\mathbb{D}_4$, $\mathbb{E}_6$, $\mathbb{E}_7$, $\mathbb{E}_8$ et le réseau de Leech Λ_{24} sont fortement parfaits et extrêmes.*

Les réseaux K'_{10}, ${K'_{10}}^*$ et le réseau de Coxeter-Todd K_{12} sont fortement parfaits dès lors que λ ne possède qu'une seule part.

Proposition 5.22. — *Les orbites d'un drapeau sous l'action du groupe d'automorphisme des réseaux de Barnes-Wall d'indice $k \geqslant 3$ forment des 6-designs vexillaires.*

Preuve. — Notons $\mathcal{G}_k$ le groupe d'automorphisme du réseau de Barnes-Wall de dimension $n = 2^k$. D'après le théorème 5.1 de [Bac05], on sait que pour tout $k \geqslant 3$ et $d \leqslant 3$, les éléments invariants suivants sont égaux :

$$\left((\mathbb{R}^n)^{\otimes d}\right)^{\mathcal{G}_k} = \left((\mathbb{R}^n)^{\otimes d}\right)^{\mathbf{O}(n)}.$$

Comme toutes les représentations qu'il nous faut prendre en compte sont incluses dans le produit tensoriel, on peut en déduire que les drapeaux minimaux des réseaux de Barnes–Wall forment des 6-designs. □

Théorème 5.23. — *Les réseaux de Barnes–Wall sont fortement parfaits et, par suite, extrêmes.*

Ce que j'étais capable de dire a été dit ; ce que je pouvais apprendre a été appris. Occupons-nous pour un temps d'autres travaux. — M. Yourcenar « Les mémoires d'Hadrien »

Table des valeurs connues | A

Nous présentons un survol de la littérature concernant les valeurs de la constante d'Hermite généralisée, complété de calculs effectués par nos soins.

A.1 Sur le corps des rationnels

A.1.1 Constante d'Hermite traditionnelle

On pourra consulter §40 de [GL87] pour un survol des différentes manières d'obtenir la constante d'Hermite. Nous reprenons dans le tableau A.1 les valeurs de la constante d'Hermite.

Dimension n	γ_n	Réseau maximal	Référence
1	1	$\mathbb{Z}$	
2	$2/\sqrt{3}$	$\mathbb{A}_2$	[Lag73]
3	$\sqrt[3]{2}$	$\mathbb{A}_3 \simeq \mathbb{D}_3$	[Gau40]
4	$\sqrt{2}$	$\mathbb{D}_4$	[KZ72]
5	$2^{3/5}$	$\mathbb{D}_5$	[KZ77]
6	$2/\sqrt[6]{3}$	$\mathbb{E}_6$	[Bli25]
7	$2^{6/7}$	$\mathbb{E}_7$	[Bli35]
8	2	$\mathbb{E}_8$	[Bli35]
24	4	Λ_{24}	[CK04]

Tab. A.1 – Valeurs de la constante d'Hermite traditionnelle

A.1.2 Meilleurs invariants connus

Le tableau A.2 présente les meilleurs invariants d'Hermite généralisés connus. Rappelons que pour $\lambda = \boxminus$ ou $\lambda = \boxminus\!\!\boxminus$, il s'agit de l'invariant Rankin. Les valeurs du tableau ont été calculées à l'aide de Magma.

La première constante de Rankin calculée correspond à $\gamma_{4,2}$ et a été obtenue par Rankin lui-même [Ran53]. A partir de calculs de la constante de Bergé–Martinet par Poor et Yuen [PY06], Sawatani, Watanabe et Okuda ont obtenu

Réseau L	$\gamma_{\square}(L)$	$\gamma_{\begin{smallmatrix}\square\\\square\end{smallmatrix}}(L)$	$\gamma_{\square\square}(L)$	$\gamma_{\begin{smallmatrix}\square\\\square\\\square\end{smallmatrix}}(L)$
$\mathbb{D}_3$			$3/2^{\dagger}$	
$\mathbb{D}_4$	$3/2^{\dagger}$		$3/\sqrt{2}^{\dagger}$	
$\mathbb{D}_5$	$3 \cdot 2^{-4/5}$		$3 \cdot 2^{-1/5}$	
$\mathbb{E}_6$	$3^{2/3\dagger}$	$4/\sqrt{3}$	$6/\sqrt{3}^{\dagger}$	
$\mathbb{E}_7$	$3/2^{2/7}$	$4/2^{3/7}$	$6/2^{3/7}$	
$\mathbb{E}_8$	$3^{\dagger}$	$4^{\dagger}$	$6^{\dagger}$	$4^{\dagger}$

† : Atteint la constante d'Hermite généralisée

Tab. A.2 – Meilleurs invariants connus sur $\mathbb{Q}$.

les valeurs des constantes $\gamma_{6,2}$, $\gamma_{8,2}$, $\gamma_{8,3}$ et $\gamma_{8,4}$ [SWO08]. Les autres valeurs sont reprises du paragraphe 4.2.1.1.

A.2 Formes binaires sur les corps de nombres

A.2.1 Quelques corps quadratiques imaginaires principaux

Les constantes d'Hermite généralisées relatives à un corps de nombre quadratique imaginaire et principal ont été calculées par M. Newman (voir chapitre XI de [New72]). Soit κ le *minimum euclidien* du corps k, c'est-à-dire

$$\kappa = \max_{z \in k} \min_{a \in \mathfrak{o}} |z - a|^2 . \tag{A.1}$$

Il s'agit aussi peu ou prou du *rayon de recouvrement* associé au réseau des entiers $\mathfrak{o}_k$ dans l'espace $k \otimes_{\mathbb{Q}} \mathbb{R}$. Le coefficient κ est le coefficient qui apparait naturellement lorsqu'on effectue une division euclidienne : soient a et b deux éléments de k, alors il existe $c \in \mathfrak{o}_k$ tel que

$$\mathcal{N}(a - c\,b) \leqslant \kappa\, \mathcal{N}(b) . \tag{A.2}$$

Proposition A.1. — *Le minimum euclidien κ du corps de nombre $\mathbb{Q}[\sqrt{-d}]$ vérifie*

$$\kappa = \begin{cases} \dfrac{d+1}{4} & si \quad d \equiv 1, 2 \mod 4 \\ \dfrac{(d+1)^2}{16} & si \quad d \equiv 3 \mod 4. \end{cases} \tag{A.3}$$

Théorème A.2 (Newman). — *Soit $d \in \{1, 2, 3, 7, 11\}$, alors la constante d'Hermite généralisée sur $\mathbb{Q}[\sqrt{-d}]$ est donnée par la valeur*

$$\gamma_{2,\square}(\mathbb{Q}[\sqrt{-d}]) = (1 - \kappa)^{-1}. \tag{A.4}$$

Démonstration. — Rappelons qu'ici $\mathcal{N}(a) = a\overline{a}$. Nous exhibons d'abord un domaine de réduction sous l'action de $\mathbf{GL}_2(\mathfrak{o})$. Soit A une forme binaire hermitienne définie positive :

$$A = \begin{pmatrix} a & b \\ \overline{b} & c \end{pmatrix} .$$

On peut supposer sans perte de généralité que le minimum de A est a. Alors par une transformation dans $\mathbf{GL}_2(\mathfrak{o})$ bien choisie, on :

$$\begin{pmatrix} 1 & 0 \\ \overline{x} & 1 \end{pmatrix} \begin{pmatrix} a & b \\ \overline{b} & c \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & ax+b \\ \overline{ax+b\overline{x}} & * \end{pmatrix}.$$

Ainsi, à transformation unimodulaire près, on peut toujours supposer que

$$\frac{1}{\kappa}\mathcal{N}(b) \leqslant \mathcal{N}(a) \leqslant \mathcal{N}(c).$$

Mais alors $\sqrt{\mathcal{N}(a^2)} \leqslant \sqrt{\mathcal{N}(ac)} = \sqrt{\mathcal{N}(b^2 + \text{dét}\, A)} \leqslant \kappa^2\sqrt{\mathcal{N}(a^2)} + \sqrt{\mathcal{N}(\text{dét}\, A)}$. Il vient par suite :

$$\mathcal{N}(a) \leqslant (1-\kappa)^{-1}\sqrt{\mathcal{N}(\text{dét}\, A)},$$

ce qu'il fallait démontrer. □

Le tableau A.3 ci-dessous reprend l'ensemble des valeurs. Avec les mêmes notations, on observera que la valeur de la constante d'Hermite n'est atteinte sur une forme A que si $a = c$ et que $\|b\| = \kappa$. On peut supposer égaux à 1 sans perte de généralité. Dans ce cas, comme 1 est le minimum de la forme A, il faut encore que $\Re(\sqrt{\kappa}e^{i\alpha}) = \frac{1}{2}$, faute de quoi $e_1 - e_2$ ou $e_1 + e_2$ serait de norme plus petite que 1. La forme parfaite correspondante s'écrit :

$$\begin{pmatrix} 1 & \sqrt{\kappa}\, e^{i\alpha} \\ \sqrt{\kappa}\, e^{-i\alpha} & 1 \end{pmatrix}. \tag{A.5}$$

d	κ	$\gamma_{2,\square}(\mathbb{Q}[\sqrt{-d}])$	α	$\sqrt{\kappa}\, e^{-i\alpha}$
1	$\frac{1}{2}$	2	$\frac{\pi}{4}$	$\frac{1}{2} + i\frac{1}{2}$
2	$\frac{3}{4}$	4	$\arccos(\frac{1}{\sqrt{3}})$	$\frac{1}{2} + i\frac{\sqrt{2}}{2}$
3	$\frac{1}{3}$	3/2	$\frac{\pi}{6}$	$\frac{1}{2} + i\frac{\sqrt{3}}{6}$
7	$\frac{4}{7}$	7/3	$\arccos\frac{\sqrt{7}}{4}$	$\frac{1}{2} + i\frac{3\sqrt{7}}{14}$
11	$\frac{9}{11}$	11/2	$\arccos\frac{\sqrt{11}}{6}$	$\frac{1}{2} + i\frac{5\sqrt{11}}{22}$

Tab. A.3 – Formes binaires des corps quadratiques imaginaires

Remarque A.3. — Nous rappelons que dans toute cette thèse, les normes n'ont pas été normalisées par le degré du corps, ce qui explique que les valeurs citées ici soit les carrés des valeurs citées par exemple dans [Wat04].

A.2.2 Quelques corps quadratiques réels

On peut obtenir, avec beaucoup plus de travail, la constante d'Hermite sur des corps quadratiques réels. Le tableau A.4 en fait la synthèse.

d	$\gamma_2(\mathbb{Q}[\sqrt{d}])$	Référence
2	$\dfrac{4}{2\sqrt{6}-3}$	[BCIO01]
3	4	[BCIO01]
5	$\dfrac{4}{\sqrt{5}}$	[BCIO01]
13	$\sqrt{\dfrac{1476+144\sqrt{91}}{175}}$	[PW05]

Tab. A.4 – Corps quadratiques réels

A.2.3 Un corps cubique

Dans le cas de corps cubique, les calculs deviennent encore plus difficile ; seul un exemple a été traité entièrement à ce jour [CIO07]. Soit ρ une racine du polynôme $x^3 - x^2 + 1 \in \mathbb{Z}[x]$ et k le corps de nombre $\mathbb{Q}[\rho]$. Les paramètres sont alors les suivants : $r_1 = r_2 = 1$, $D_k = -23$ et $h_k = 1$ et la constante d'Hermite est rappelée dans le tableau A.5.

$\gamma_2(\mathbb{Q}[\rho])$	Référence
$\frac{4\sqrt{3}}{9} + \frac{2}{9}(3\rho^2 - 4\rho + 2)\sqrt{1-\rho^2}$	[CIO07]

Tab. A.5 – Un exemple de corps cubique, formes binaires

Si [l'homme] dédaigne le pain sec que la raison humaine lui tend croyant bien faire, c'est uniquement parce qu'en secret il fait bombance à la table des dieux. — F. Hölderlin, « Hypérion »

B Algorithme de Voronoï pour les corps quadratiques imaginaires

Il n'existe malheureusement pas d'algorithme connu qui fasse l'inventaire des formes parfaites dans le cas général et qui calcule la constante d'Hermite ; il faut se consoler de la seule extension découverte à ce jour, qui concerne le cas des corps quadratiques imaginaires [Kœc60].

Désormais, k est un corps de nombre quadratique imaginaire de nombre de classes $h = 1$. On regarde k comme un sous-corps de $\mathbb{C}$. On suppose fixé un élément τ de $\mathbb{C}$ tel que $\mathfrak{o}_k = \mathbb{Z} + \mathbb{Z}\tau$, soit

$$\tau = \mathrm{i},\ \mathrm{i}\sqrt{2},\ \frac{1+\mathrm{i}\sqrt{3}}{2},\ \frac{1+\mathrm{i}\sqrt{7}}{2},\ \frac{1+\mathrm{i}\sqrt{11}}{2}$$

selon le corps de nombre envisagé. On note encore $d = 1, 2, 3, 7$ ou 11.

B.1 L'algorithme de Voronoï d'après Kœcher

B.1.1 Présentation

Indépendamment de la question du calcul de la constante d'Hermite, on peut comprendre les travaux de Voronoï comme une tentative d'obtenir une théorie de la réduction pour les formes quadratiques. En effet, la réunion des domaines de Voronoï d'une famille – finie – des représentants des classes de formes parfaites orchestre la composition d'un domaine fondamental, c'est-à-dire d'un ensemble contenant un représentant de chaque forme quadratique à équivalence arithmétique près.

Dans cette optique, les résultats de Voronoï ont été étendus par M. Kœcher [Kœc60] ; ils ont été discutés ensuite par Opgenorth [Opg01] sous une forme plus générale qui dissocie cône initial et son dual et sont au cœur de l'ouvrage [Sch08a]. Toutefois, notons dès à présent que l'invariant d'Hermite sous-jacent dans ces deux premiers articles est un invariant additif : une forme de Humbert $\mathcal{A} = (A_v)_{v\in\mathfrak{V}_\infty}$ étant donnée, on y étudie le minimum de $\sum_{v\in\mathfrak{V}} d_v\, A_v[x]$ quand x varie plutôt que le minimum de $\prod_{v\in\mathfrak{V}} A_v[x]^{d_v}$; ces deux invariants coïncident néanmoins lorsque $\{r_1, r_2\} = \{0, 1\}$. Dans le cas où k est le corps des rationnels ou un corps quadratique imaginaire de nombre de classe égal à un, la théorie de la réduction obtenue par M. Kœcher pour les formes de Humbert concourt

à l'établissement d'un algorithme d'énumération des classes de formes parfaites relativement à la partition $\lambda = \square$ dont nous reprenons rapidement le signalement. Il a été utilisé, à la main, par Staffeldt [Sta79] pour l'énumération des formes parfaites binaires et ternaires sur l'anneau des entiers de Gauß. L'algorithme relatif aux formes réelles est présenté avec plus de détail dans [Mar03].

Lemme B.1 ([Kœc60], lemma 3). — *Pour toute forme hermitienne définie positive $A \in \mathcal{H}_n^{>0}$, il existe un voisinage $U \subset \mathcal{H}_n^{>0}$ tel que $\mathscr{S}(B) \subset \mathscr{S}(A)$ et $|\min B - \min A| < \varepsilon$ si $B \in U$. Autrement dit, le minimum est une fonction continue.*

Définition B.2. — Soient A une forme hermitienne définie positive et $\mathscr{S}(A)$ ses vecteurs minimaux définis sur $\mathfrak{o}_k$. On appelle *rang de perfection* et on note $\eta(A)$ le rang de la famille des projecteurs $(uu^*)_{u\in\mathscr{S}(A)}$.

Une forme parfaite est une forme dont le rang vaut n^2.

Lemme B.3. — *Soient A une forme hermitienne définie positive et $\vec{F}$ un élément de l'orthogonal de $\mathscr{S}(A)$, alors il existe un réel c tel que $A+c\vec{F}$ est encore définie positive,* $\min A = \min A + c\vec{F}$, $\mathscr{S}(A) \subset \mathscr{S}\left(A + c\vec{F}\right)$ *et* $\eta(A) \leqslant \eta(A + c\vec{F})$.

Preuve. — Il s'agit d'une reformulation du lemme 4 de [Kœc60] duquel nous éliminons un cas qui ne peut survenir ici. □

Définition B.4. — On appelle *domaine de Voronoï D_P* d'une forme parfaite P le cône engendré par l'enveloppe convexe des matrices de projection $(p_u)_{u\in\mathscr{S}(P)}$, où $p_u = uu^*$, dans $\mathbb{R}^{n^2}$:

$$D_P = \{ \sum_{u\in\mathscr{S}(A)} c_u p_u;\ c_u \geqslant 0\}. \tag{B.1}$$

Lemme B.5. — *Toute face F (i.e. un bord de codimension 1) du domaine de Voronoï est définie par les conditions $\langle F, p_u\rangle = 0$ si $p_u \in F$ et $\langle F, p_u\rangle > 0$ sinon. On note $\vec{F}$ le vecteur de face F, c'est-à-dire le vecteur unité orthogonal à F orienté vers l'intérieur du domaine.*

En utilisant les deux lemmes précédents, on peut démontrer la proposition suivante.

Proposition B.6. — *Étant donné une forme parfaite et un vecteur de face $\vec{F}$ de son domaine de Voronoï, il existe une unique forme parfaite Q sur la demi-droite $P + \mathbb{R}_+^\times \vec{F}$ de minimum 1.*
Les formes comprises entre P et Q sont de minimum 1, de rang de perfection $n^2 - 1$; leurs vecteurs minimaux u correspondent aux projections p_u qui appartiennent à F.
Les formes au-delà de Q ont un minimum inférieur à 1 ou bien ne sont pas définies positives.
On dit que P et Q sont deux formes contiguës.

Définition B.7. — On dit que deux formes hermitiennes définies positives A et B sont *arithmétiquement équivalentes* s'il existe une matrice $U \in \mathbf{GL}_n(\mathfrak{o})$ telle que $A = U^*BU$.

Théorème B.8 ([Kœc60] Satz 8). — *L'ensemble des domaines de Voronoï des formes parfaites de minimum 1 forme une tessalation de $\mathcal{H}_n^{>0}$. Chaque domaine ne possède qu'un nombre fini de voisins : les domaines des formes contiguës. De plus, il existe un domaine fondamental de $\mathcal{H}_n^{>0}$ relativement à l'action du groupe $\mathbf{GL}_n(\mathfrak{o})$ par similitude défini par les domaines de Voronoï d'un ensemble fini de formes parfaites.*

Définition B.9. — On appelle *graphe de Voronoï* le graphe qui relie les formes parfaites de minimum 1 dont les cônes de Voronoï partagent une face commune, c'est-à-dire les formes contiguës.

Ce graphe est encore défini modulo l'action du groupe $\mathbf{GL}_n(\mathfrak{o})$. Le théorème peut se reformuler comme suit.

Théorème B.10. — *Modulo équivalence arithmétique, le graphe de Voronoï est fini et connexe.*

B.1.2 L'équivalence arithmétique dans les corps imaginaires

Pour des besoins pratiques, nous montrons ici comment rapporter la question de l'équivalence arithmétique complexe à des questions réelles, pour lesquelles des algorithmes existent et sont implémentés sous magma notamment [PS97].

Notons Ω_1 la matrice $n \times 2n$ suivante $\Omega_1 = \begin{pmatrix} \mathrm{I}_n & \mathrm{i}\,\mathrm{I}_n \end{pmatrix}$. et Ω_2 la matrice $2n \times 2n$ suivante $\Omega_2 = \begin{pmatrix} \mathrm{I}_n & \Re\tau\,\mathrm{I}_n \\ 0 & \Im\tau\,\mathrm{I}_n \end{pmatrix}$. Lorsque $A \in \mathcal{M}_n(\mathbb{C})$, on a en particulier

$$\Re\left({\Omega_1}^* A \Omega_1\right) = \begin{pmatrix} \Re A & -\Im A \\ \Im A & \Re A \end{pmatrix} \quad \text{et} \quad \Im\left({\Omega_1}^* A \Omega_1\right) = \begin{pmatrix} \Im A & \Re A \\ -\Re A & \Im A \end{pmatrix}.$$

Lemme B.11. — *Soient U une matrice de $\mathcal{M}_n(\mathbb{C})$ et $\widehat{U}$ la matrice de $\mathcal{M}_{2n}(\mathbb{R})$*

$$\widehat{U} = \begin{pmatrix} \Re U & -\Im U \\ \Im U & \Re U \end{pmatrix},$$

alors $\operatorname{dét} \widehat{U} = |\operatorname{dét} U|^2$.

Preuve. — Par des opérations élémentaires sur les lignes et les colonnes, on se ramène successivement à

$$\begin{pmatrix} \Re U + \mathrm{i}\Im U & -\Im U + \mathrm{i}\Re U \\ \Im U & \Re U \end{pmatrix} \quad \text{puis} \quad \begin{pmatrix} \Re U + \mathrm{i}\Im U & 0 \\ \Im U & \Re U - i\Im U \end{pmatrix},$$

matrice à laquelle on applique la formule de déterminants par blocs. □

Notons encore Ω la matrice $n \times 2n$ suivante :

$$\Omega = \Omega_1\Omega_2 = \begin{pmatrix} 1 & 0 & \cdots & 0 & \tau & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots & 0 & \tau & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 & \tau \end{pmatrix}. \tag{B.2}$$

Définition B.12. — Si A est une forme hermitienne, on peut construire la matrice $\widetilde{A} = \Omega^* A \Omega$ et noter $\widetilde{A}_\Re = \Re\widetilde{A}$ et $\widetilde{A}_\Im = \Im\widetilde{A}$ ses parties réelle et imaginaire. $\widetilde{A}_\Re$ est encore une forme quadratique définie positive de dimension $2n$, tandis que $\widetilde{A}_\Im$ est une forme symplectique.

Proposition B.13. — *1. Les valeurs prises par A sur $\mathfrak{o}^n$ coïncident avec les valeurs prises par $\widetilde{A}_{\Re}$ sur $\mathbb{Z}^{2n}$. En particulier les minima sont égaux.*

2. Deux formes hermitiennes A et B sont arithmétiquement équivalentes (i.e. il existe une transformation $U \in \mathbf{GL}_n(\mathfrak{o}_k)$ telle que $B = U^*AU$) si et seulement si les couples $(\widetilde{A}_{\Re}, \widetilde{A}_{\Im})$ et $(\widetilde{B}_{\Re}, \widetilde{B}_{\Im})$ sont arithmétiquement équivalents (i.e. il existe une transformation $\overline{U} \in \mathbf{GL}_{2n}(\mathbb{Z})$ telle que $\widetilde{B}_{\Re} = \overline{U}'\widetilde{A}_{\Re}\overline{U}$ et $\widetilde{B}_{\Im} = \overline{U}'\widetilde{A}_{\Im}\overline{U}$).

Preuve. — Si $x = (a_i + \tau b_i)_{1\leqslant i\leqslant n}$ et $y = (c_i + \tau d_i)_{1\leqslant i\leqslant n}$ sont des vecteurs de k^n, notons $\widetilde{x}$ et $\widetilde{y}$ les vecteurs colonnes $(a_1, \ldots, a_n, b_1, \ldots, b_n)$ et $(c_1, \ldots, c_n, d_1, \ldots, d_n)$, de sorte que

$$\forall x, y \in k^n, \quad x^*Ay = \widetilde{x}'\widetilde{A}_{\Re}\widetilde{y} \ + \ \mathrm{i}\,\widetilde{x}'\widetilde{A}_{\Im}\widetilde{y}. \tag{B.3}$$

1. La première assertion provient de l'égalité (B.3) combinée au fait que $(1, \tau)$ forme une base sur $\mathbb{Z}$ de $\mathfrak{o}_k$.
2. Les matrices A et B désignent dans ce qui suit deux formes hermitiennes. Condition nécessaire. Supposons que A et B soient reliées par une relation telle que $A = U^*BU$. Alors, on peut vérifier par le calcul qu'en posant

$$\widehat{U} = \begin{pmatrix} \Re U & -\Im U \\ \Im U & \Re U \end{pmatrix},$$

qui est une matrice de déterminant 1 d'après le lemme B.11, on obtient la relation

$$\Re({\Omega_1}^*A\Omega) = \widehat{U}'\Re({\Omega_1}^*B\Omega)\widehat{U} \quad \text{et} \quad \Im({\Omega_1}^*A\Omega) = \widehat{U}'\Im({\Omega_1}^*B\Omega)\widehat{U}. \tag{B.4}$$

et par suite, comme Ω_2 est une matrice réelle, on peut écrire en introduisant convenablement Ω_2

$$\widetilde{A}_{\Re} = \widetilde{B}_{\Re}[\Omega_2^{-1}\widehat{U}\Omega_2] \quad \text{et} \quad \widetilde{A}_{\Im} = \widetilde{B}_{\Im}[\Omega_2^{-1}\widehat{U}\Omega_2].$$

Supposons que U appartienne à $\mathbf{GL}_n(\mathfrak{o})$ et décomposons les éléments de U selon la base $(1, \tau)$, $U = U_{[1]} + \tau U_{[\tau]}$, on obtient alors par le calcul que

$$\Omega_2^{-1}\widehat{U}\Omega_2 = \begin{pmatrix} U_{[1]} & -\left|\tau\right|^2 U_{[\tau]} \\ U_{[\tau]} & 2\Re(\tau)U_{[\tau]} + U_{[1]} \end{pmatrix}$$

qui est une matrice à coefficients entiers et de déterminant 1.

Condition suffisante. On suppose que A et B sont reliées par les deux relations $\widetilde{A}_{\Re} = \overline{U}'\widetilde{B}_{\Re}\overline{U}$ et $\widetilde{A}_{\Im} = \overline{U}'\widetilde{B}_{\Im}\overline{U}$ pour une certaine matrice $U \in \mathbf{GL}_{2n}(\mathbb{Z})$. Posons $\widehat{U} = \Omega_2\overline{U}\Omega_2^{-1}$, ce qui conduit à la relation B.4, ou encore en additionnant les deux égalités

$$\begin{pmatrix} A & \mathrm{i}A \\ -\mathrm{i}A & A \end{pmatrix} = \widehat{U}' \begin{pmatrix} B & \mathrm{i}B \\ -\mathrm{i}B & B \end{pmatrix} \widehat{U}.$$

En notant $U = \begin{pmatrix} U_{1,1} & U_{1,2} \\ U_{2,1} & U_{2,2} \end{pmatrix}$ et en posant $C_1 = U_{1,1} + \mathrm{i}U_{2,1}$, $C_2 = U_{2,2} + \mathrm{i}U_{1,2}$, il vient des quatre blocs $C_1BC_1 = C_1BC_2 = C_2BC_1 = C_2BC_2 = A$, Par exemple, en considérant le bloc supérieur gauche, il vient

$$\begin{aligned} A &= {U_{1,1}}'BU_{1,1} + {U_{2,1}}'(-\mathrm{i}B)U_{1,1} + {U_{1,1}}'(\mathrm{i}B)U_{2,1} + U_{2,1}BU_{2,1} \\ &= (U_{1,1} + \mathrm{i}U_{2,1})^*\, B\, (U_{1,1} + \mathrm{i}U_{2,1}). \end{aligned}$$

Alors $(C_1 - C_2)B(C_1 - C_2) = A + A - A - A = 0$ et par suite vu que B est non dégénéré, $C_1 = C_2$. Les coefficients de la matrice C_1 appartiennent par construction à $\mathbb{Z} + \tau\mathbb{Z}$; d'après le lemme B.11, C_1 possède un déterminant de module 1.

□

B.1.3 Implémentation

Les programmes utilisés pour l'exécution de l'algorithme combinent le logiciel de calcul symbolique Magma [BCP97] avec le programme Qhull [BDH96] pour le traitement de l'enveloppe convexe (passage d'une description par les points extrêmes à une description par les faces).

Le programme ne manipule que des formes hermitiennes définies positives dont le minimum est 1.

Pour toute forme hermitienne P, on tient à jour une variable correspondant aux formes $\widetilde{A}_{\Re}$ et $\frac{1}{\sqrt{d}}\widetilde{A}_{\Im}$ (la division factice par $\sqrt{d}$ garantit que les coefficients manipulés restent dans $\mathbb{Q}$).

Algorithme B.14 (Minimum). — Recherche les vecteur minimaux d'une forme hermitienne A à partir de l'algorithme classique de recherche des plus courts vecteurs appliqué à $\widetilde{A}_{\Re}$.

Algorithme B.15 (Groupe d'automorphisme). — Recherche le groupe d'automorphisme d'une forme A par la recherche du groupe stabilisant $\widetilde{A}_{\Re}$ et $\frac{1}{\sqrt{d}}\widetilde{A}_{\Im}$.

Algorithme B.16 (Isométrie). — Teste l'isométrie de deux formes A et B par la recherche d'une isométrie entre $\widetilde{A}_{\Re}$ et $\widetilde{B}_{\Re}$ d'une part et $\frac{1}{\sqrt{d}}\widetilde{A}_{\Im}$ et $\frac{1}{\sqrt{d}}\widetilde{B}_{\Im}$ d'autre part.

Algorithme B.17 (Phase d'initialisation). — À partir de la forme identité I_n, qui est une forme de minimum 1 mais n'est pas parfaite, l'algorithme recherche par itération successive une direction dans laquelle il peut accroître le rang de perfection de la forme courante et s'arrête lorsqu'il a trouvé une forme parfaite.

Algorithme B.18 (Étude d'une forme). — Entrée : forme hermitienne A

- Recherche les vecteurs minimaux (algorithme B.14) et calcul du groupe d'automorphisme (algorithme B.15).
- Calcule les n^2 coefficients réels de la matrice de projection.
- Construit par Qhull les équations des faces du cône de Voronoï (calcul effectué en flottants).
- Pour toute face F
  - Recherche une approximation rationnelle d'un vecteur $\vec{F}$ normal à une face.
  - Explore la demi-droite $A + \mathbb{R}_+^\times \vec{F}$ pour trouver son unique forme parfaite.
  - Teste l'isométrie avec les formes parfaites déjà connues. Ajoute à la liste des formes connues si nouvelle classe de forme.
  - Élimine des faces obtenues sous l'action du groupe d'automorphisme dans la liste des faces à traiter.

Algorithme B.19 (Algorithme complet). — Entrée : n, d.

- Recherche une première forme parfaite (algorithme B.17). Initialise une liste de formes parfaites
- Tant que toutes les formes de la liste des formes parfaites n'est pas traitée, applique l'algorithme B.18 et met à jour cette liste.
- Compare les déterminants de toutes les formes parfaites et renvoie le plus petit.

Remarque B.20. — La partie la plus longue du calcul réside dans le traitement du cône de Voronoï (dont l'espace ambiant est de dimension n^2) et le calcul des équations (ou vecteurs normaux) de ses faces à partir des points qui le définissent.

À partir de la dimension 4, il peut arriver que la structure du réseau $\mathbb{E}_8$ survienne au sein de l'une des formes parfaites. Dans le cas classique, il possède le cône de Voronoï le plus difficile à traiter et a nécessité l'écriture d'algorithmes particuliers qui tiennent compte des symétries nombreuses de ce réseau [DSSV07]. À cet égard, il est vain de penser que l'algorithme présenté ici suffise à traiter ces cas.

B.2 Résultats en dimension 3

Nous présentons les résultats sous la forme suivante. Nous dressons la liste des formes parfaites construites par l'algorithme. Nous présentons dans un tableau quelques éléments significatifs pour chaque forme. Nous montrons le graphe de Voronoï à équivalence arithmétique près, en explicitant sur chaque arrête le nombre de faces sortantes dans le graphe initial.

B.2.1 Énumération des formes parfaites ternaires de $\mathbb{Q}[\sqrt{-1}]$

L'exécution de l'algorithme de Voronoï conduit à une seule forme parfaite.

$$P_1 := \begin{pmatrix} 1 & \frac{1}{2}+\frac{1}{2}\mathrm{i} & \frac{1}{2} \\ \frac{1}{2}-\frac{1}{2}\mathrm{i} & 1 & 0 \\ \frac{1}{2} & 0 & 1 \end{pmatrix}$$

Forme	Vecteurs minimaux	Déterminant	Faces	Ordre du groupe
P_1	15	$\frac{1}{4}$	48	384

Tab. B.1 – Récapitulatif des formes parfaites ternaires sur $\mathbb{Q}[\sqrt{-1}]$

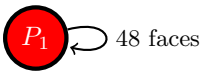


Fig. B.1 – Graphe de Voronoï des formes ternaires sur $\mathbb{Q}[\sqrt{-1}]$

Ainsi, la constante d'Hermite $\gamma_{3,\square}(\mathbb{Q}[\sqrt{-1}])$ vaut $2\sqrt[3]{2}$.

Remarque B.21. — Ce calcul a déjà été effectué à la main dans [Sta79]. Il est confirmé par A. Schürmann [Sch08b] dans le cadre de sa recherche des réseaux gaussiens parfaits[1]. Nous trouvons une forme équivalente à la forme parfaite suivante trouvée par Staffeldt

$$\begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{2}+\frac{\mathrm{i}}{2} \\ \frac{1}{2}-\frac{\mathrm{i}}{2} & 1 & \frac{1}{2}+\frac{\mathrm{i}}{2} \\ \frac{1}{2}-\frac{\mathrm{i}}{2} & \frac{1}{2}-\frac{\mathrm{i}}{2} & 1 \end{pmatrix}.$$

Remarque B.22. — La structure réelle de P_1 est (à facteur multiplicatif près) celle de $\mathbb{D}_6$.

Remarque B.23. — Cette forme et son dual sont eutactiques.

[1] au sens de la $\mathcal{T}$-perfection, ce qui signifie que n'est pas testée l'équivalence des parties imaginaires.

B.2.2 Énumération des formes parfaites ternaires de $\mathbb{Q}[\sqrt{-2}]$

L'exécution de l'algorithme de Voronoï conduit aux deux formes parfaites suivantes.

$$P_1 := \begin{pmatrix} 1 & \frac{1}{2} + \mathrm{i}\frac{\sqrt{2}}{2} & \frac{1}{2} \\ \frac{1}{2} - \mathrm{i}\frac{\sqrt{2}}{2} & 1 & -\mathrm{i}\frac{\sqrt{2}}{4} \\ \frac{1}{2} & \mathrm{i}\frac{\sqrt{2}}{4} & 1 \end{pmatrix}$$

$$P_2 := \begin{pmatrix} 1 & \frac{1}{4} - \mathrm{i}\frac{\sqrt{2}}{4} & \frac{1}{4} - \mathrm{i}\frac{\sqrt{2}}{2} \\ \frac{1}{4} + \mathrm{i}\frac{\sqrt{2}}{4} & 1 & \frac{1}{4} - \mathrm{i}\frac{3\sqrt{2}}{8} \\ \frac{1}{4} + \mathrm{i}\frac{\sqrt{2}}{2} & \frac{1}{4} + \mathrm{i}\frac{3\sqrt{2}}{8} & 1 \end{pmatrix}$$

Forme	Vecteurs minimaux	Déterminant	Faces	Ordre du groupe
P_1	21	$\frac{1}{8}$	128	32
P_2	12	$\frac{5}{32}$	15	6

Tab. B.2 – Récapitulatif des formes parfaites ternaires sur $\mathbb{Q}[\sqrt{-2}]$

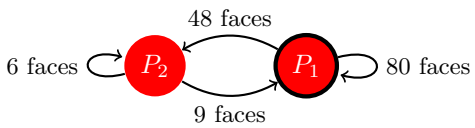


Fig. B.2 – Graphe de Voronoï des formes ternaires sur $\mathbb{Q}[\sqrt{-2}]$

Ainsi, la constante d'Hermite $\gamma_{3,\square}(\mathbb{Q}[\sqrt{-2}])$ vaut 4.

Remarque B.24. — Les réseaux réels correspondant à P_1 et P_2 ne sont pas connus du catalogue de G. Nebe et N. Sloane.

Remarque B.25. — Ces deux formes sont également eutactiques. Ce n'est pas le cas de leur dual.

B.2.3 Énumération des formes parfaites ternaires de $\mathbb{Q}[\sqrt{-3}]$

L'exécution de l'algorithme de Voronoï conduit aux deux formes parfaites suivantes.

$$P_1 := \begin{pmatrix} 1 & \frac{1}{2}+\mathrm{i}\frac{\sqrt{3}}{6} & \frac{1}{2}+\mathrm{i}\frac{\sqrt{3}}{6} \\ \frac{1}{2}-\mathrm{i}\frac{\sqrt{3}}{6} & 1 & 0 \\ \frac{1}{2}-\mathrm{i}\frac{\sqrt{3}}{6} & 0 & 1 \end{pmatrix}$$

$$P_2 = \begin{pmatrix} 1 & \frac{1}{4}-\mathrm{i}\frac{\sqrt{3}}{4} & \frac{1}{4}-\mathrm{i}\frac{\sqrt{3}}{4} \\ \frac{1}{4}+\mathrm{i}\frac{\sqrt{3}}{4} & 1 & \frac{1}{4}+\mathrm{i}\frac{\sqrt{3}}{4} \\ \frac{1}{4}+\mathrm{i}\frac{\sqrt{3}}{4} & \frac{1}{4}-\mathrm{i}\frac{\sqrt{3}}{4} & 1 \end{pmatrix}$$

Forme	Vecteurs minimaux	Déterminant	Faces	Ordre du groupe
P_1	12	$\frac{1}{3}$	81	1296
P_2	9	$\frac{3}{8}$	9	1296

TAB. B.3 – Récapitulatif des formes parfaites ternaires sur $\mathbb{Q}[\sqrt{-3}]$

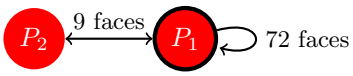


FIG. B.3 – Graphe de Voronoï des formes ternaires sur $\mathbb{Q}[\sqrt{-3}]$

La constante d'Hermite est atteinte pour P_1 et vaut $\sqrt[3]{9}$.

Remarque B.26. — L'énumération des formes parfaites coïncide avec celle de A. Schürmann des réseaux eisensteiniens parfaits. Ce résultat avait déjà été prouvé (*cf.* table 4.3). La structure réelle de la forme ici nommée P_1 est isomètre à celle du réseau $\mathbb{E}_6$ à un facteur près puisque son minimum est 1 plutôt que 2 (*cf.* exemple 2.33).

Remarque B.27. — La structure réelle de P_1 est celle de $\mathbb{E}_6$; la structure réelle de P_2 est celle de $\mathbb{E}_6^*$

Remarque B.28. — Les formes P_1 comme P_2 sont eutactiques.

B.2.4 Énumération des formes parfaites ternaires de $\mathbb{Q}[\sqrt{-7}]$

L'exécution de l'algorithme de Voronoï conduit aux deux formes parfaites suivantes.

$$P_1 := \begin{pmatrix} 1 & \frac{1}{2} + \mathrm{i}\frac{3\sqrt{7}}{14} & \frac{1}{2} + \mathrm{i}\frac{\sqrt{7}}{14} \\ \frac{1}{2} - \mathrm{i}\frac{3\sqrt{7}}{14} & 1 & 0 \\ \frac{1}{2} + \mathrm{i}\frac{\sqrt{7}}{14} & 0 & 1 \end{pmatrix}$$

$$P_2 = \begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{4} - \frac{-\mathrm{i}\sqrt{7}}{4} \\ \frac{1}{2} & 1 & -\frac{1}{4} - \frac{-\mathrm{i}\sqrt{7}}{4} \\ \frac{1}{4} + \frac{-\mathrm{i}\sqrt{7}}{4} & -\frac{1}{4} + \frac{-\mathrm{i}\sqrt{7}}{4} & 1 \end{pmatrix}$$

Forme	Vecteurs minimaux	Déterminant	Faces	Ordre du groupe
P_1	21	$\frac{1}{7}$	24	42
P_2	21	$\frac{1}{8}$	24	336

Tab. B.4 – Récapitulatif des formes parfaites ternaires sur $\mathbb{Q}[\sqrt{-7}]$

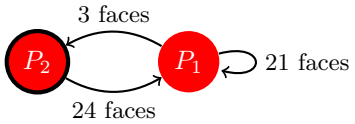


Fig. B.4 – Graphe de Voronoï des formes ternaires sur $\mathbb{Q}[\sqrt{-7}]$

La constante d'Hermite est atteinte pour P_2 et vaut 4.

Remarque B.29. — Le réseau réel correspondant à P_1 possède la structure de $\mathbb{A}_6$, tandis que le réseau réel correspondant à P_2 possède la structure de $\mathbb{A}_6^{(2)}$.

Remarque B.30. — Les formes qui apparaissent sont eutactiques, leur dual aussi.

B.2.5 Énumération des formes parfaites ternaires de $\mathbb{Q}[\sqrt{-11}]$

L'exécution de l'algorithme de Voronoï conduit aux douze formes parfaites suivantes.

$$P_1 := \begin{pmatrix} 1 & \frac{1}{2}+\mathrm{i}\frac{5\sqrt{11}}{22} & \mathrm{i}\frac{\sqrt{11}}{11} \\ \frac{1}{2}-\mathrm{i}\frac{5\sqrt{11}}{22} & 1 & 0 \\ -\mathrm{i}\frac{\sqrt{11}}{11} & 0 & 1 \end{pmatrix}$$

$$P_2 = \begin{pmatrix} 1 & -\frac{1}{4}+\frac{5\mathrm{i}\sqrt{11}}{44} & \frac{1}{44}-\frac{7\sqrt{11}}{44} \\ -\frac{1}{4}-\frac{5\mathrm{i}\sqrt{11}}{44} & 1 & \frac{1}{4}-\frac{5\mathrm{i}\sqrt{11}}{44} \\ \frac{1}{44}-\frac{7\sqrt{11}}{44} & \frac{1}{4}+\frac{5\mathrm{i}\sqrt{11}}{44} & 1 \end{pmatrix}$$

$$P_3 = \begin{pmatrix} 1 & \frac{1}{4}-\frac{3\mathrm{i}\sqrt{11}}{44} & \frac{1}{4}+\frac{3\mathrm{i}\sqrt{11}}{44} \\ \frac{1}{4}+\frac{3\mathrm{i}\sqrt{11}}{44} & 1 & \frac{1}{4}-\frac{9\mathrm{i}\sqrt{11}}{44} \\ \frac{1}{4}-\frac{3\mathrm{i}\sqrt{11}}{44} & \frac{1}{4}+\frac{9\mathrm{i}\sqrt{11}}{44} & 1 \end{pmatrix}$$

$$P_4 = \begin{pmatrix} 1 & \frac{1}{2}-\frac{\mathrm{i}\sqrt{11}}{11} & \frac{1}{2}-\frac{3\mathrm{i}\sqrt{11}}{22} \\ \frac{1}{2}+\frac{\mathrm{i}\sqrt{11}}{11} & 1 & \frac{1}{4}+\frac{3\sqrt{11}}{44} \\ \frac{1}{2}+\frac{3\mathrm{i}\sqrt{11}}{22} & \frac{1}{4}-\frac{3\sqrt{11}}{44} & 1 \end{pmatrix}$$

$$P_5 = \begin{pmatrix} 1 & -\frac{1}{10}-\frac{3\mathrm{i}\sqrt{11}}{22} & \frac{1}{10}-\frac{3\mathrm{i}\sqrt{11}}{22} \\ -\frac{1}{10}+\frac{3\mathrm{i}\sqrt{11}}{22} & 1 & -\frac{1}{10}+\frac{5\mathrm{i}\sqrt{11}}{22} \\ \frac{1}{10}+\frac{3\mathrm{i}\sqrt{11}}{22} & -\frac{1}{10}-\frac{5\mathrm{i}\sqrt{11}}{22} & 1 \end{pmatrix}$$

$$P_6 = \begin{pmatrix} 1 & \frac{1}{4}-\frac{5\mathrm{i}\sqrt{11}}{44} & -\frac{3\mathrm{i}\sqrt{11}}{22} \\ \frac{1}{4}+\frac{5\mathrm{i}\sqrt{11}}{44} & 1 & \frac{1}{4}-\frac{\mathrm{i}\sqrt{11}}{4} \\ \frac{3\mathrm{i}\sqrt{11}}{22} & \frac{1}{4}+\frac{\mathrm{i}\sqrt{11}}{4} & 1 \end{pmatrix}$$

$$P_7 = \begin{pmatrix} 1 & \frac{1}{3}-\frac{2\mathrm{i}\sqrt{11}}{11} & \frac{1}{3} \\ \frac{1}{3}-\frac{2\mathrm{i}\sqrt{11}}{11} & 1 & -\frac{1}{3}-\frac{2\mathrm{i}\sqrt{11}}{33} \\ \frac{1}{3} & -\frac{1}{3}+\frac{2\mathrm{i}\sqrt{11}}{33} & 1 \end{pmatrix}$$

$$P_8 = \begin{pmatrix} 1 & \frac{1}{2}+\frac{\mathrm{i}\sqrt{1}}{22} & \frac{1}{8}+\frac{5\mathrm{i}\sqrt{11}}{88} \\ \frac{1}{2}-\frac{\mathrm{i}\sqrt{1}}{22} & 1 & -\frac{1}{4}+\frac{10\mathrm{i}\sqrt{11}}{44} \\ \frac{1}{8}-\frac{5\mathrm{i}\sqrt{11}}{88} & -\frac{1}{4}+\frac{10\mathrm{i}\sqrt{11}}{44} & 1 \end{pmatrix}$$

$$P_9 = \begin{pmatrix} 1 & \frac{1}{2}+\frac{\mathrm{i}\sqrt{11}}{22} & \frac{3}{8}+\frac{7\mathrm{i}\sqrt{11}}{88} \\ \frac{1}{2}-\frac{\mathrm{i}\sqrt{11}}{22} & 1 & \frac{1}{4}+\frac{10\mathrm{i}\sqrt{11}}{44} \\ \frac{3}{8}-\frac{7\mathrm{i}\sqrt{11}}{88} & \frac{1}{4}-\frac{10\mathrm{i}\sqrt{11}}{44} & 1 \end{pmatrix}$$

$$P_{10} = \begin{pmatrix} 1 & \frac{1}{6}+\frac{5\mathrm{i}\sqrt{11}}{66} & \frac{1}{6}-\frac{5\mathrm{i}\sqrt{11}}{66} \\ \frac{1}{6}-\frac{5\mathrm{i}\sqrt{11}}{66} & 1 & -\frac{1}{6}+\frac{15\mathrm{i}\sqrt{11}}{66} \\ \frac{1}{6}+\frac{5\mathrm{i}\sqrt{11}}{66} & -\frac{1}{6}-\frac{15\mathrm{i}\sqrt{11}}{66} & 1 \end{pmatrix}$$

$$P_{11} = \begin{pmatrix} 1 & -\frac{2\mathrm{i}\sqrt{11}}{33} & -\frac{7\mathrm{i}\sqrt{11}}{33} \\ \frac{2\mathrm{i}\sqrt{11}}{33} & 1 & -\frac{1}{3}+\frac{4\mathrm{i}\sqrt{11}}{33} \\ \frac{7\mathrm{i}\sqrt{11}}{33} & -\frac{1}{3}-\frac{4\mathrm{i}\sqrt{11}}{33} & 1 \end{pmatrix}$$

$$P_{12} = \begin{pmatrix} 1 & -\frac{1}{3} + \frac{2\mathrm{i}\sqrt{11}}{33} & -\frac{1}{2} + \frac{\mathrm{i}\sqrt{11}}{6} \\ -\frac{1}{3} - \frac{2\mathrm{i}\sqrt{11}}{33} & 1 & \frac{1}{2} - \frac{\mathrm{i}\sqrt{11}}{6} \\ -\frac{1}{2} - \frac{\mathrm{i}\sqrt{11}}{6} & \frac{1}{2} + \frac{\mathrm{i}\sqrt{11}}{6} & 1 \end{pmatrix}$$

Forme	Vecteurs minimaux	Déterminant	Faces	Ordre du groupe
P_1	20	$\frac{1}{11}$	97	16
P_2	12	$\frac{1}{11}$	29	6
P_3	9	$\frac{9}{88}$	9	16
P_4	10	$\frac{5}{44}$	13	2
P_5	12	$\frac{124}{1375}$	29	6
P_6	12	$\frac{5}{44}$	12	2
P_7	12	$\frac{32}{297}$	12	6
P_8	9	$\frac{5}{44}$	9	2
P_9	9	$\frac{5}{44}$	9	2
P_{10}	10	$\frac{32}{297}$	13	6
P_{11}	10	$\frac{29}{297}$	13	6
P_{12}	10	$\frac{32}{297}$	13	6

Tab. B.5 – Récapitulatif des formes parfaites ternaires sur $\mathbb{Q}[\sqrt{-11}]$

La constante d'Hermite est atteinte pour P_5 et vaut $\sqrt{\frac{1890625}{15376}}$. Le graphe de Voronoï[2] est un peu plus touffu dans ce cas.

Remarque B.31. — Nous n'avons reconnu aucun réseau connu parmi les structures réelles de ces douze formes parfaites.

Remarque B.32. — Toutes ses formes sont eutactiques sauf P_4 et P_{12}.

[2] Avec mes remerciements à Frédéric Mazoit qui m'a permis de le dessiner de manière présentable.

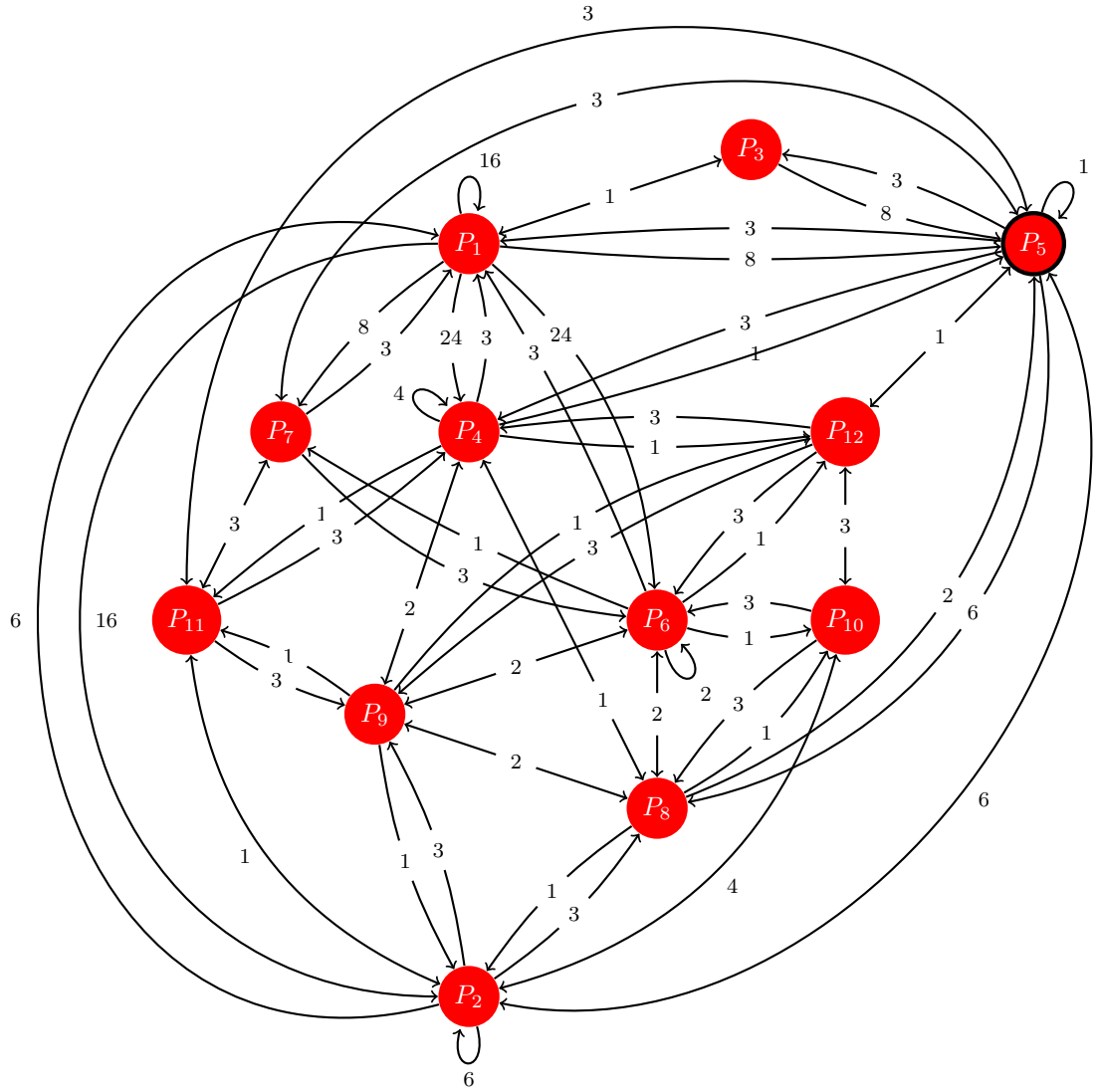


FIG. B.5 – Graphe de Voronoï des formes ternaires sur $\mathbb{Q}[\sqrt{-11}]$

Table des figures

1.1 Empilement régulier de sphères quelconque en dimension 2 . . . 2
1.2 Illustration du lemme de Siegel 4
1.3 Vue des formes parfaites et eutactiques 7

2.1 Déterminant et pairs de vecteurs minimaux d'un réseau L 17
2.2 Drapeau minimal dans le réseau cubique face centrée ($\mathbb{D}_3$) 18

5.1 Représentation du 4-design sphérique associé à $\mathbb{A}_2$ 76

B.1 Graphe de Voronoï des formes ternaires sur $\mathbb{Q}[\sqrt{-1}]$ 93
B.2 Graphe de Voronoï des formes ternaires sur $\mathbb{Q}[\sqrt{-2}]$ 94
B.3 Graphe de Voronoï des formes ternaires sur $\mathbb{Q}[\sqrt{-3}]$ 95
B.4 Graphe de Voronoï des formes ternaires sur $\mathbb{Q}[\sqrt{-7}]$ 96
B.5 Graphe de Voronoï des formes ternaires sur $\mathbb{Q}[\sqrt{-11}]$ 99

Liste des tableaux

2.1 Correspondance entre réseaux euclidiens et formes quadratiques . 19

4.1 Constantes $\gamma_{n,(2,1,\ldots,1)}(\mathbb{Q})$ 55
4.2 Quelques constantes généralisées sur $\mathbb{Q}$ de forme quelconque . . . 57
4.3 Constantes d'Humbert pour certains corps imaginaires 64
4.4 Invariant de Bergé–Martinet des réseaux gaussiens parfaits en dimension 3 et 4 69
4.5 Invariants de Bergé–Martinet des réseaux eisensteiniens parfaits en dimension 3 et 4 69
4.6 Invariants de Bergé–Martinet de réseaux de $\mathbb{Q}[\sqrt{-7}]$ 69
4.7 Constantes de Bergé–Martinet gaussiennes et eisensteiniennes . . 70

A.1 Valeurs de la constante d'Hermite traditionnelle 83
A.2 Meilleurs invariants connus sur $\mathbb{Q}$. 84
A.3 Formes binaires des corps quadratiques imaginaires 85
A.4 Corps quadratiques réels 86
A.5 Un exemple de corps cubique, formes binaires 86

B.1 Récapitulatif des formes parfaites ternaires sur $\mathbb{Q}[\sqrt{-1}]$ 93
B.2 Récapitulatif des formes parfaites ternaires sur $\mathbb{Q}[\sqrt{-2}]$ 94
B.3 Récapitulatif des formes parfaites ternaires sur $\mathbb{Q}[\sqrt{-3}]$ 95
B.4 Récapitulatif des formes parfaites ternaires sur $\mathbb{Q}[\sqrt{-7}]$ 96
B.5 Récapitulatif des formes parfaites ternaires sur $\mathbb{Q}[\sqrt{-11}]$ 98

Index

$|\cdot|_v$, 20
$\check{\cdot}$, transposé de l'inverse, 52
$\leqslant$, ordre des partitions, 12
$\langle\cdot,\cdot\rangle$, produit scalaire de $\mathscr{L}^2(\mathscr{D}_{\mathrm{d}})$, 72
$[\cdot,\cdot]$, produit scalaire, 13
$\cdot^*$, matrice transconjuguée, 15
$\cdot'$, 15
équivalence arithmétique, 88

$k_{\mathbb{A}}$, adèles, 22
$\mathcal{A} = (A_v)_{v\in\mathfrak{V}_\infty}$, 38
$\mathfrak{a}_\iota$, classe d'idéal, 19
$\mathfrak{A}_V^L$, idéal, 39

Bergé–Martinet, constante de, 51
bitableau, 13
    standard, 13

χ_λ, caractère, 24, 35
$c_{n,\lambda}$, constante, 67
constante d'Hermite
    des formes d'Humbert, 40
    groupe linéaire adélique, 37
    réseau, 71
    réseau euclidien, 17
C_T, contenu, 12

d, degré d'extension, 19
$\mathrm{d} = (d_1,\ldots,d_\ell)$, forme du drapeau, 15
$\mathscr{D}_{\mathrm{d}}$, variété drapeau, 15, 27
degré
    partition, 11
Δ, drapeau, 15
$\Delta_q(\cdot)$, mineur d'ordre q, 32
δ_n, densité optimale, 1
design
    grassmannien, 8
    sphérique, 8
    vexillaire, 75
déterminant
    forme d'Humbert, 39
    réseau, 16
D_k, discriminant, 19
drapeau, 15
    vecteur, 27, 39
dualité, 2
dualité, théorème de, 52
d_v, degré local, 20

$(e_i)_{1\leqslant i\leqslant n}$, base canonique, 15
Eisenstein, entiers de, 20
$e_{U(\lambda)}$, vecteur de plus haut poids, 27
eutaxie, 5, 44, 78
eutaxie forte, 78
extrême, 5, 44

Ferrer, diagramme de, 11
fibré en droite métrisé, 33
f_λ^n, 24
$f_{[\lambda]}^n$, dimension de la représentation $\mathbb{S}^{[\lambda]}(\mathbb{R}^n)$, 29

Gauß, entiers de, 19
$\mathbf{GL}_n(\mathbb{K})$, groupe linéaire, 15
Gram, matrice de, 16
grassmanienne, variété, 3
groupe des automorphismes, 16

h, nombre de classes, 19
hauteur, 34
$H(\cdot)$, hauteur, 30
$H_A(\cdot)$, hauteur tordue, 31, 37
$\mathcal{H}_n^{>0}$, 15
Hermite–Humbert, constante, 3
Hermite–Humbert, forme de, 38

$\mathfrak{i}$, 19
$\mathcal{I} = (\mathrm{I}_n)_{v\in\mathfrak{V}}$, 39
$\Im$, partie imaginaire, 11
I_n, identité, 15
invariant d'Hermite
    groupe linéaire adélique, 37
    réseau, 71
    réseau euclidien, 17
$I^{(\mu)}(Z)$, idéal déterminantal, 14
$I_t(Z)$, idéal déterminantal, 14

$\mathfrak{j}$, 20
J^λ, 30, 72

k, corps de nombre, 19
$\varkappa_t$, 12
$\mathbb{K}[Z]$, polynômes, 13

$\mathcal{L}$, fibré en droite, 33
ℓ, profondeur du drapeau, 15
$\mathscr{L}^2(\cdot)$, fonctions de carré intégrable, 71
λ, partition, 11
L_ι, réseau, 20
ℓ_V^ι, fonction longueur, 42

métrique, 33
    de Fubini–Study, 34
    standard, 34
minimal
    drapeau, 18
    vecteur, 16
minimum
    forme d'Humbert, 39
    réseau, 16
minimum euclidien, 84
$\mathcal{M}_n(\mathbb{K})$, 15
Mordel, inégalité de, 2
$\mathscr{M}_{\{T,\Theta\}}$, monôme déterminantal, 14
μ, partition, 14

$\mathcal{N}(\cdot)$, 19
n, dimension, 15
N^μ, espace de multiplicité, 72
n_μ, multiplicité, 72

$\mathcal{O}$, fibré en droite, 34
$\mathfrak{o}$, 19
ω_n, volume de la boule unité, 1, 59

partition, 11

P_{d}, sous-groupe parabolique, 15
perfection, 5, 44, 78
    rang de, 88
perfection forte, 8, 78
$\Pi_{\mathcal{A},X}$, somme des projections, 44
π_λ, représentation de poids λ, 24
Plücker, plongement de, 27
plongement projectif, 27
$\mathcal{P}_n(k)$, 38
profondeur, 11

r, nombre de plongements, 19
r_1, nombre de plongements réels, 19
r_2, nombre de plongements complexes, 19
Rankin, constante de, 2, 57, 70, 83
rayon de recouvrement, 84
$\Re$, partie réelle, 11
réseau
    $\mathbb{A}_2$, 4
    $\mathbb{A}_2$, 17, 19
    Barnes–Wall BW_n, 17
    $\mathbb{D}_4$, 17, 21, 64, 81
    $\mathbb{D}_6$, 69
    $\mathbb{D}_8$, 21
    d'un corps de nombre, 20
    de Leech, 17, 22, 64
    de racine, 17
    $\mathbb{E}_6$, 17, 21, 64, 69, 81
    $\mathbb{E}_7$, 17, 81
    $\mathbb{E}_8$, 17, 21, 64, 69, 70, 81
    eisensteinien, 21, 64, 68
    euclidien, 16
    gaussien, 21, 64, 68
Ryshkov, domaine de, 5, 69

$\mathfrak{s}$, section, 34
s, profondeur de λ, 11
$\mathscr{S}(\mathcal{A})$, minimum, 43
$\check{s}$, profondeur de $\check{\lambda}$, 11
Siegel, lemme de, 4
$\mathbb{S}^\lambda(\cdot)$, foncteur de Schur, 25, 27
$\mathbb{S}^{[\lambda]}(\cdot)$, foncteur de ?, 29, 72
$\mathbb{S}^\lambda_\sharp(\cdot)$, vecteurs drapeau, 27
$\mathbf{SL}_n(\mathbb{K})$, groupe spécial linéaire, 15
$\mathscr{S}^{n-1}$, sphère unité de $\mathbb{R}^n$, 8
standard
    monôme, 14
    tableau, 27
Steinitz, classe de, 20

$\mathcal{S}_n^{>0}$, 15

T, tableau, 13
tableau, 12
    standard, 12
Θ, tableau, 13
$\{T, \Theta\}$, bitableau, 13, 14
type un, fonction de, 66

u, profondeur de $\breve{\mu}$, 14
$U(\lambda)$, tableau initial, 12, 13, 27

$\mathcal{V}$, variété algébrique, 33
$\mathfrak{V}$, places, 20
valeur absolue, 20
variété drapeau, 15
Veronese, plongement de, 28
violation, 30, 74
Voronoï
    domaine de, 88
Voronoï, graphe de, 5

X_Δ, matrice du drapeau Δ, 16

Z, matrice d'indéterminées, 13
zonale, fonction, 73

Bibliographie

[AMRT75] A. Ash, D. Mumford, M. Rapoport & Y. Tai – *Smooth compactification of locally symmetric varieties*, Math. Sci. Press, Brookline, Mass., 1975, Lie Groups : History, Frontiers and Applications, Vol. IV.

[ASS05] I. Aliev, A. Schinzel & W. M. Schmidt – « On vectors whose span contains a given linear subspace », *Monatsh. Math.* **144** (2005), no. 3, p. 177–191.

[Aut96] Auteur Anonyme – « An inequality for the determinant of a positive definite hermitian matrix », 1996, p. 1, `www.numbertheory.org/pdfs/grm.pdf`.

[Bac05] C. Bachoc – « Designs, groups and lattices », *J. Théor. Nombres Bordeaux* **17** (2005), no. 1, p. 25–44.

[Bav97] C. Bavard – « Systole et invariant d'Hermite », *J. Reine Angew. Math.* **482** (1997), p. 93–120.

[Bav05] — , « Théorie de Voronoï géométrique. Propriétés de finitude pour les familles de réseaux et analogues », *Bull. Soc. Math. France* **133** (2005), no. 2, p. 205–257.

[BBC04] C. Bachoc, E. Bannai & R. Coulangeon – « Codes and designs in Grassmannian spaces », *Discrete Math.* **277** (2004), no. 1-3, p. 15–28.

[BCIO01] R. Baeza, R. Coulangeon, M. I. Icaza & M. O'Ryan – « Hermite's constant for quadratic number fields », *Experiment. Math.* **10** (2001), no. 4, p. 543–551.

[BCN02] C. Bachoc, R. Coulangeon & G. Nebe – « Designs in Grassmannian spaces and lattices », *J. Algebraic Combin.* **16** (2002), no. 1, p. 5–19.

[BCP97] W. Bosma, J. Cannon & C. Playoust – « The Magma algebra system. I. The user language », *J. Symbolic Comput.* **24** (1997), no. 3-4, p. 235–265, Computational algebra and number theory (London, 1993).

[BDH96] C. B. Barber, D. P. Dobkin & H. Huhdanpaa – « The quickhull algorithm for convex hulls », *ACM Trans. Math. Software* **22** (1996), no. 4, p. 469–483.

[BG06] E. Bombieri & W. Gubler – *Heights in diophantine geometry*, New mathematical monographs, vol. 4, Cambridge University Press, 2006.

[BI97] R. Baeza & M. I. Icaza – « On Humbert-Minkowski's constant for a number field », *Proc. Amer. Math. Soc.* **125** (1997), no. 11, p. 3195–3202.

[Bli25] H. F. Blichfeldt – « On the minimum value of positive real quadratic forms in six variables », *BAMS* **31** (1925), no. 1, p. 386.

[Bli35] — , « The minimum values of positive quadratic forms in six, seven and eight variables », *Math. Z.* **39** (1935), no. 1, p. 1–15.

[BM89] A.-M. Bergé & J. Martinet – « Sur un problème de dualité lié aux sphères en géométrie des nombres », *J. Number Theory* **32** (1989), no. 1, p. 14–42.

[BM91] A.-M. Bergé & J. Martinet – « Réseaux extrêmes pour un groupe d'automorphismes », *Astérisque* (1991), no. 198-200, p. 41–66 (1992), Journées Arithmétiques, 1989 (Luminy, 1989).

[BMS92] A.-M. Bergé, J. Martinet & F. Sigrist – « Une généralisation de l'algorithme de Voronoĭ pour les formes quadratiques », *Astérisque* (1992), no. 209, p. 12, 137–158, Journées Arithmétiques, 1991 (Geneva).

[BV83] E. Bombieri & J. Vaaler – « On Siegel's lemma », *Invent. Math.* **73** (1983), no. 1, p. 11–32.

[BV84] — , « Addendum to : "On Siegel's lemma" », *Invent. Math.* **75** (1984), no. 2, p. 377.

[BV88] W. Bruns & U. Vetter – *Determinantal rings*, Lecture Notes in Mathematics, vol. 1327, Springer-Verlag, Berlin, 1988.

[BV93] E. B. Burger & J. D. Vaaler – « On the decomposition of vectors over number fields », *J. Reine Angew. Math.* **435** (1993), p. 197–219.

[BV01] C. Bachoc & B. Venkov – « Modular forms, lattices and spherical designs », in *Réseaux euclidiens, designs sphériques et formes modulaires*, Monogr. Enseign. Math., vol. 37, Enseignement Math., Geneva, 2001, p. 87–111.

[CIO07] R. Coulangeon, M. I. Icaza & M. O'Ryan – « Lenstra's constant and extreme forms in number fields », *Experiment. Math.* **16** (2007), no. 4, p. 455–462.

[CK04] H. Cohn & A. Kumar – « The densest lattice in twenty-four dimensions », *Electron. Res. Announc. Amer. Math. Soc.* **10** (2004), p. 58–67 (electronic).

[Cou96] R. Coulangeon – « Réseaux k-extrêmes », *Proc. London Math. Soc. (3)* **73** (1996), no. 3, p. 555–574.

[Cou01] — , « Voronoï theory over algebraic number fields », in *Réseaux euclidiens, designs sphériques et formes modulaires*, Monogr. Enseign. Math., vol. 37, Enseignement Math., Geneva, 2001, p. 147–162.

[Cou04] — , *Document de synthèse en vue de l'habilitation à diriger des recherches*, Non paru, Université Bordeaux 1, 2004.

[CS99] J. H. Conway & N. J. A. Sloane – *Sphere packings, lattices and groups*, third éd., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 290, Springer-Verlag, New York, 1999, 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.

[CSM95] R. Carter, G. Segal & I. Macdonald – *Lectures on Lie groups and Lie algebras*, London Mathematical Society Student Texts, vol. 32, Cambridge University Press, Cambridge, 1995, With a foreword by Martin Taylor.

[dCEP80] C. de Concini, D. Eisenbud & C. Procesi – « Young diagrams and determinantal varieties », *Invent. Math.* **56** (1980), no. 2, p. 129–165.

[dCP76] C. de Concini & C. Procesi – « A characteristic free approach to invariant theory », *Advances in Math.* **21** (1976), no. 3, p. 330–354.

[DGS77] P. Delsarte, J.-M. Goethals & J. J. Seidel – « Spherical codes and designs », *Geometriae Dedicata* **6** (1977), no. 3, p. 363–388.

[DRS74] P. Doubilet, G.-C. Rota & J. Stein – « On the foundations of combinatorial theory. IX. Combinatorial methods in invariant theory », *Studies in Appl. Math.* **53** (1974), p. 185–216.

[DSSV07] M. Dutour-Sikirić, A. Schürmann & F. Vallentin – « Classification of eight-dimensional perfect forms », *Electron. Res. Announc. Amer. Math. Soc.* **13** (2007), p. 21–32 (electronic).

[Ebe02] W. Ebeling – *Lattices and codes*, revised éd., Advanced Lectures in Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 2002, A course partially based on lectures by F. Hirzebruch.

[EVGS02] 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, p. 321–324.

[FH91] W. Fulton & J. Harris – *Representation theory*, Graduate Texts in Mathematics, vol. 129, Springer-Verlag, New York, 1991, A first course, Readings in Mathematics.

[Ful97] W. Fulton – *Young tableaux*, London Mathematical Society Student Texts, vol. 35, Cambridge University Press, Cambridge, 1997, With applications to representation theory and geometry.

[Gau40] C.-F. Gauss – « Untersuchung über die Eigenschaften der positiven ternären quadratischen formen von ludwig august seeber », *J. Reine Angew. Math.* **20** (1840), p. 312–320.

[GL87] P. M. Gruber & C. G. Lekkerkerker – *Geometry of numbers*, second éd., North-Holland Mathematical Library, vol. 37, North-Holland Publishing Co., Amsterdam, 1987.

[God63] R. Godement – « Domaines fondamentaux des groupes arithmétiques », in *Séminaire Bourbaki, Vol. 8*, Soc. Math. France, Paris, 1963, p. Exp. No. 257, 201–225.

[GW98] R. Goodman & N. R. Wallach – *Representations and invariants of the classical groups*, Encyclopedia of Mathematics and its Applications, vol. 68, Cambridge University Press, Cambridge, 1998.

[Hla43] E. Hlawka – « Zur Geometrie der Zahlen », *Math. Zeit.* **49** (1943), p. 285–312.

[HST91] E. Hlawka, J. Schoissengeier & R. Taschner – *Geometric and analytic number theory*, Universitext, Springer-Verlag, Berlin, 1991, Translated from the 1986 German edition by Charles Thomas.

[Hum49] P. Humbert – « Réduction de formes quadratiques dans un corps algébrique fini », *Comment. Math. Helv.* **23** (1949), p. 50–63.

[Ica97] M. I. Icaza – « Hermite constant and extreme forms for algebraic number fields », *J. London Math. Soc. (2)* **55** (1997), no. 1, p. 11–22.

[JC74] A. T. James & A. G. Constantine – « Generalized Jacobi polynomials as spherical functions of the Grassmann manifold », *Proc. London Math. Soc. (3)* **29** (1974), p. 174–192.

[Kœc60] M. Kœcher – « Beiträge zu einer Reduktionstheorie in Positivitätsbereichen. I », *Math. Ann.* **141** (1960), p. 384–432.

[KZ72] A. Korkine & G. Zolotareff – « Sur les formes quadratiques positives quaternaires », *Math. Ann.* **5** (1872), no. 4, p. 581–583.

[KZ73] — , « Sur les formes quadratiques », *Math. Ann.* **6** (1873), no. 3, p. 366–389.

[KZ77] — , « Sur les formes quadratiques positives », *Math. Ann.* **11** (1877), no. 4, p. 242–292.

[Lag73] J.-L. Lagrange – « Recherches d'arithmétique », in *Œuvres de Lagrange*, Nouv. Mém. Acad. Berlin, vol. III, 1773, p. 265–312.

[LS78] R. Lee & R. H. Szczarba – « On the torsion in $K_4(\mathbf{Z})$ and $K_5(\mathbf{Z})$ », *Duke Math. J.* **45** (1978), no. 1, p. 101–129.

[LST01] W. Lempken, B. Schröder & P. H. Tiep – « Symmetric squares, spherical designs, and lattice minima », *J. Algebra* **240** (2001), no. 1, p. 185–208, With an appendix by Christine Bachoc and Tiep.

[LT85] G. Lancaster & J. Towber – « Representation-functors and flag-algebras for the classical groups. II », *J. Algebra* **94** (1985), no. 2, p. 265–316.

[Mal85] M.-P. Malliavin – *Algèbre commutative*, Collection Maîtrise de Mathématiques Pures., Masson, Paris, 1985, Applications en géométrie et théorie des nombres.

[Mar03] J. Martinet – *Perfect lattices in Euclidean spaces*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 327, Springer-Verlag, Berlin, 2003.

[McF71] R. B. McFeat – « Geometry of numbers in adele spaces », *Dissertationes Math. Rozprawy Mat.* **88** (1971), p. 49.

[Mey09] B. Meyer – « Generalised Hermite constants, Voronoi theory and heights on flag varieties », *A paraître Bull. Soc. Math. Fr.* (2009).

[MH67] H. Minkowski & D. Hilbert – *Gesammelte Abhandlungen von Hermann Minkowski*, 2nd éd., Chelsea publishing company, New York, 1967.

[Min10] H. Minkowski – *Geometrie der Zahlen*, Bibliotheca Mathematica Teubneriana, Band 40, Johnson Reprint Corp., New York, 1910.

[Mir90] L. Mirsky – *An introduction to linear algebra*, Dover Publications Inc., New York, 1990, Reprint of the 1972 edition.

[MW01] M. Morishita & T. Watanabe – « Adèle geometry of numbers », in *Class field theory—its centenary and prospect (Tokyo, 1998)*, Adv. Stud. Pure Math., vol. 30, Math. Soc. Japan, Tokyo, 2001, p. 509–536.

[New72] M. Newman – *Integral matrices*, Academic Press, New York, 1972, Pure and Applied Mathematics, Vol. 45.

[O'M00] O. T. O'Meara – *Introduction to quadratic forms*, Classics in Mathematics, Springer-Verlag, Berlin, 2000, Reprint of the 1973 edition.

[Opg01] J. Opgenorth – « Dual cones and the Voronoi algorithm », *Experiment. Math.* **10** (2001), no. 4, p. 599–608.

[OW01] S. Ohno & T. Watanabe – « Estimates of Hermite constants for algebraic number fields », *Comment. Math. Univ. St. Paul.* **50** (2001), no. 1, p. 53–63.

[Pac08] C. Pache – « Extremality and designs in spaces of quadratic forms », *arXiv :0804.0173v2* (2008), p. 1–38.

[PR94] V. Platonov & A. Rapinchuk – *Algebraic groups and number theory*, Pure and Applied Mathematics, vol. 139, Academic Press Inc., Boston, MA, 1994.

[PS97] W. Plesken & B. Souvignier – « Computing isometries of lattices », *J. Symbolic Comput.* **24** (1997), no. 3-4, p. 327–334, Computational algebra and number theory (London, 1993).

[PW05] M. E. Pohst & M. Wagner – « On the computation of Hermite-Humbert constants for real quadratic number fields », *J. Théor. Nombres Bordeaux* **17** (2005), no. 3, p. 905–920.

[PY06] C. Poor & D. S. Yuen – « The Bergé–Martinet constant and slopes of Siegel cusp forms », *Bull. London Math. Soc.* **38** (2006), p. 913–924.

[Ran53] R. A. Rankin – « On positive definite quadratic forms », *J. London Math. Soc.* **28** (1953), p. 309–314.

[RB79] S. S. Ryškov & E. P. Baranovskiĭ – « Classical methods of the theory of lattice packings », *Russian Math. Surveys* **34** (1979), no. 4(208), p. 1–68.

[RT96] D. Roy & J. L. Thunder – « An absolute Siegel's lemma », *J. Reine Angew. Math.* **476** (1996), p. 1–26.

[RT99] — , « Addendum and erratum to : "An absolute Siegel's lemma" », *J. Reine Angew. Math.* **508** (1999), p. 47–51.

[Sam67] P. Samuel – *Théorie algébrique des nombres*, Hermann, Paris, 1967.

[SB06] N. I. Shepherd-Barron – « Perfect forms and the moduli space of abelian varieties », *Invent. Math.* **163** (2006), no. 1, p. 25–45.

[Sch08a] A. Schürmann – *Computational geometry of positive definite quadratic forms*, University Lecture Series, American Mathematical Society, Providence, RI, 2008.

[Sch08b] — , « Enumerating perfect forms », Préprint, 2008.

[Sie89] C. L. Siegel – *Lectures on the geometry of numbers*, Springer-Verlag, Berlin, 1989, Notes by B. Friedman, Rewritten by Komaravolu Chandrasekharan with the assistance of Rudolf Suter.

[ST02] I. Stewart & D. Tall – *Algebraic number theory and Fermat's last theorem*, third éd., A K Peters Ltd., Natick, MA, 2002.

[Sta79] R. E. Staffeldt – « Reduction theory and K_3 of the Gaussian integers », *Duke Math. J.* **46** (1979), no. 4, p. 773–798.

[SWO08] K. Sawatani, T. Watanabe & K. Okuda – « A note on the Hermite–Rankin constant », communication privée, 2008.

[Thu93] J. L. Thunder – « Asymptotic estimates for rational points of bounded height on flag varieties », *Compositio Math.* **88** (1993), no. 2, p. 155–186.

[Thu96] — , « An adelic Minkowski-Hlawka theorem and an application to Siegel's lemma », *J. Reine Angew. Math.* **475** (1996), p. 167–185.

[Thu98] — , « Higher-dimensional analogs of Hermite's constant », *Michigan Math. J.* **45** (1998), no. 2, p. 301–314.

[Tie06] P. H. Tiep – « Finite groups admitting Grassmannian 4-designs », *J. Algebra* **306** (2006), no. 1, p. 227–243.

[Tit71] J. Tits – « Représentations linéaires irréductibles d'un groupe réductif sur un corps quelconque », *J. Reine Angew. Math.* **247** (1971), p. 196–220.

[Vaa03] J. D. Vaaler – « The best constant in Siegel's lemma », *Monatsh. Math.* **140** (2003), no. 1, p. 71–89.

[Van08] S. Vance – « Mordell's inequality for Eisenstein and Hurwitz lattices », *arXiv :0810.2336v1* (2008), p. 1–15.

[Ven01] B. Venkov – « Réseaux et designs sphériques », in *Réseaux euclidiens, designs sphériques et formes modulaires*, Monogr. Enseign. Math., vol. 37, Enseignement Math., Geneva, 2001, p. 10–86.

[Vor08] G. Voronoï – « Nouvelles applications des paramètres continus à la théorie des formes quadratiques », *J. Reine Angew. Math.* **133** (1908), p. 97–178.

[Wat00] T. Watanabe – « On an analog of Hermite's constant », *J. Lie Theory* **10** (2000), no. 1, p. 33–52.

[Wat03] — , « Fundamental Hermite constants of linear algebraic groups », *J. Math. Soc. Japan* **55** (2003), no. 4, p. 1061–1080.

[Wat04] — , « A survey and a complement of fundamental Hermite constants », in *Algebraic and arithmetic theory of quadratic forms*, Contemp. Math., vol. 344, Amer. Math. Soc., Providence, RI, 2004, p. 339–350.

[Wat06] — , « On the best bound of the minimal twisted height of linear subspaces », *Arch. Math. (Basel)* **87** (2006), no. 4, p. 320–329.

[Web94] R. Webster – *Convexity*, Oxford Science Publications, The Clarendon Press Oxford University Press, New York, 1994.

[Wei82] A. Weil – *Adeles and algebraic groups*, Progress in Mathematics, vol. 23, Birkhäuser Boston, Mass., 1982, With appendices by M. Demazure and Takashi Ono.

[Wei95] — , *Basic number theory*, Classics in Mathematics, Springer-Verlag, Berlin, 1995, Reprint of the second (1973) edition.

[Wey97] H. Weyl – *The classical groups*, Princeton Landmarks in Mathematics, Princeton University Press, Princeton, NJ, 1997, Their invariants and representations, Fifteenth printing, Princeton Paperbacks.

Résumé

Cette thèse étend la théorie de Voronoï aux invariants d'Hermite généralisés définis par T. Watanabe pour le groupe linéaire adèlique : elle caractérise via des propriétés de perfection et d'eutaxie les maxima locaux de cet invariant en terme de formes de Humbert. Par l'extension d'inégalités et de méthodes développées dans le cas classique, elle présente les valeurs de ces constantes dans certains cas particuliers. Enfin, elle introduit pour la variété drapeau des notions de design vexillaire et de réseau fortement parfait qui fournissent via la théorie des groupes une large classe d'exemple de réseaux extrême.

Mots-clefs

Constante d'Hermite, théorie de Voronoï, forme de Humbert, géométrie des nombres, hauteur, adèles, représentation du groupe linéaire, réduction de Korkine et Zolotareff, design, réseau fortement parfait, inégalité de Mordell, constante de Rankin, constante de Bergé–Martinet.

Abstract

This thesis extends Voronoy theory to the generalised Hermite invariants defined by T. Watanabe for the adelic linear group : it characterises via perfection and eutaxy properties the local maxima of this invariant in terms of Humbert forms. By extension of the inequalities and the methods known in the classical case, some values of the constants are presented in particular cases. Finally, notions of vexillar design and strongly perfect lattice are introduced for the flag variety and provide via group theory a large class of examples of extreme lattices.

Keywords

Hermite constant, Voronoy theory, Humbert form, geometry of numbers, height, adèles, representation of the general linear group, Korkine and Zolotarev reduction, design, strongly perfect lattice, Mordell inequality, Rankin constant, Bergé–Martinet constant.