

N°ORDRE : 4368



Université Lille 1 Sciences et Technologies
Ecole Doctorale régionale Sciences Pour l'Ingénieur
Lille Nord-de-France

Thèse pour obtenir le grade de Docteur en Sciences de
l'Université Lille 1

présentée par **Benoît GRANDPIERRE**
le 04 juin 2009

Discipline : **MATHÉMATIQUES PURES**

**PRODUITS AUTOMORPHES, CLASSIFICATION DES RÉSEAUX
ET THÉORIE DU CODAGE**

Directeur de Thèse : Valery GRITSENKO

Jury :

Présidente	Christine BACHOC	Professeur	Université de Bordeaux 1
Examineur	Valery GRITSENKO	Professeur	Université de Lille 1
Examineur	Dimitri MARKUSCHEVICH	Professeur	Université de Lille 1
Examineur	Viacheslav NIKULIN	Professeur	Université de Liverpool
Rapporteur	Nils SCHEITHAUER	Professeur	Université de Darmstadt
Rapporteur	Patrick SOLÉ	Dir. Recherche	CNRS Sophia-Antipolis
Examineur	Mikhail VERBITSKY	Dir. Recherche	Russian Academy of Science

Résumé

La fonction Φ_{12} de Borchers, forme modulaire en 26 variables pour le groupe orthogonal $O^+(II_{2,26})$ et le caractère déterminant, de poids singulier 12, a été construite par R.E. Borcherds en 1994 avec la théorie des produits automorphes. Elle détermine la “Fake Monster Lie Algebra”, qui joue le rôle fondamental dans la preuve de la “Moonshine Conjecture”.

Φ_{12} est aussi une forme modulaire réflexive (ses zéros sont des hyperplans définissant une réflexion orthogonale de $O^+(II_{2,26})$). Beaucoup d'exemples ont été construits par Borcherds, et Nikulin a montré qu'il n'y a, en principe, qu'un nombre fini de formes modulaires réflexives. Gritsenko et Nikulin ont classifié les formes modulaires réflexives dans le cas des réseaux maximaux de signature $(1, 2)$ (1998 – 2002). Enfin, d'autres exemples importants de formes réflexives de poids singuliers ont été construits par N. Scheithauer (2000 – 2005).

La classification des formes modulaires réflexives est un problème très important, de telles formes ont beaucoup d'applications dans différents domaines mathématiques et physiques : en théorie des algèbres de Kac-Moody, en géométrie algébrique, en théorie des cordes...

Dans cette thèse, nous décrivons une nouvelle classe de formes modulaires réflexives associée à la fonction Φ_{12} de Borcherds. La signature des groupes orthogonaux considérés varie entre $(2, 3)$ et $(2, 25)$. Toutes les formes obtenues sont des quasi-restrictions de Φ_{12} . Cette méthode, très arithmétique, nous donne plus de 60 formes modulaires réflexives, dont la première est la forme modulaire de Siegel de poids 35 construite par Igusa en 1964.

Mots clés : formes modulaires pour les groupes orthogonaux, produits de Borcherds, classification des formes réflexives, codes de Golay, réseaux de Niemeier, formes modulaires de Siegel.

Abstract

Automorphic products, classification of lattices and coding theory

Borcherds' Φ_{12} function is a modular form in 26 variables for the orthogonal group $O^+(II_{2,26})$ and the character determinant, of singular weight 12, it was constructed by Borcherds in 1994 together with the automorphic products theory. It determines the Fake Monster Lie Algebra, which plays the fundamental role in the proof of the Moonshine Conjecture.

Φ_{12} is also a reflective form (its zeros are hyperplans of orthogonal reflections in $O^+(II_{2,26})$). Many examples were constructed by Borcherds, and Nikulin has proved there is, in principle, only a finite number of reflective modular forms. Gritsenko and Nikulin classified reflective modular forms in the case of maximal lattices of signature $(1, 2)$ (1998 – 2002). Other important examples of reflective forms of singular weight were constructed by N. Scheithauer (2000 – 2005).

The classification of reflective modular forms is a very important question, such forms have many applications in different fields of mathematics and physics : in the theory of Kac-Moody algebras, in algebraic geometry, in string theory...

In this thesis, we describe a new class of reflective forms related to the Borcherds' function Φ_{12} . The signature of the orthogonal groups we consider goes between $(2, 3)$ and $(2, 25)$. All the forms we obtain are quasi pull-back of Φ_{12} . This arithmetic method gives more than 60 reflective modular forms, the first of them being the Siegel modular form of weight 35 constructed by Igusa in 1964.

Keywords : modular forms for orthogonal groups, Borcherds' products, classification of reflective forms, Golay codes, Niemeier lattices, Siegel modular forms.

Remerciements

Mes premiers remerciements vont à Valery Gritsenko, pour son encadrement durant ces trois années de thèse, sa disponibilité et la confiance qu'il m'a accordée. J'ai beaucoup enrichi ma culture mathématique lors des séances de notre groupe de travail, et j'ai particulièrement apprécié les divers séjours en Allemagne et les exposés qu'il m'a permis de faire lors de séminaires internationaux.

Je remercie Nils Scheithauer et Patrick Solé d'avoir accepté d'être les rapporteurs de cette thèse, ainsi que Christine Bachoc, Dimitri Markushevich, Viacheslav Nikulin et Mikhail Verbitsky d'avoir bien voulu faire partie du jury.

Un grand merci également à Pierre Dèbes qui m'a invité le premier à Lille et m'a fait rencontrer mon directeur de thèse, puis m'a aidé dans la constitution de mon dossier de demande de bourse de thèse à l'ENS Cachan. Merci aussi à Michel Matignon mon directeur de Mémoire de M2 et à Marc Hindry qui ont permis ce contact initial.

Je remercie Jean d'Almeida pour l'entretien du séminaire des doctorants dont j'ai été co-responsable durant la dernière année de ma thèse.

Merci à Sandra Delaunay, ma tutrice pédagogique, et à Barbara Tumpach, avec qui j'ai eu plaisir à travailler dans le cadre des enseignements que j'ai fait pour le monitorat.

J'ai aussi une pensée particulière pour le laboratoire Paul Painlevé, l'UFR de mathématiques, et l'Ecole doctorale, pour les excellentes conditions de travail, tant matérielles qu'humaines, de l'université de Lille 1.

Je remercie chaleureusement Alain Juhel, Patrick Caron, et Pascal Saumon pour l'aide qu'ils m'ont, chacun à leur manière, apportée.

Enfin, je remercie les thésards du laboratoire Paul Painlevé pour leur soutien, Anne et ses gâteaux, Bénédicte toujours de bonne humeur, Shuyan, Amandine la marcheuse, Eric et Raphaël les coureurs, Patrick et ses histoires de clic-clac, Vincent malgré ses nombreux forfaits, Martin qui malgré ses "absences" est celui qui nous a permis de rejouer au foot, Léon "Patrick Veira", Fabien dont la culture mathématique (et footballistique) n'a pas de borne, Alexis bien évidemment, et mes "co-bureau" Nour, Orlando, Fethi et Mozher, ainsi que Youcef pour ses conseils et son investissement. Je remercie mon entourage non-mathématique pour qui cela n'a pas toujours été facile, Carole tout d'abord, nos familles, et nos amis.

Table des matières

Introduction	11
1 Réseaux, codes, groupes orthogonaux et formes modulaires	17
1.1 Réseaux	17
1.1.1 Réseaux quadratiques	17
1.1.2 Séries Thêta	20
1.1.3 Réseaux de racines	21
1.1.4 Formes quadratiques discriminantes	26
1.1.5 Sur-réseaux	30
1.2 Codes	31
1.2.1 Généralités sur les codes	31
1.2.2 Liens entres codes et réseaux	33
1.2.3 Exemples de codes linéaires	33
1.2.4 Codes de Golay	35
1.3 Groupes orthogonaux et formes modulaires	41
1.3.1 Domaines homogènes	41
1.3.2 Groupes orthogonaux	42
1.3.3 Formes modulaires	45
1.3.4 Diviseurs quadratiques rationnels	45
1.3.5 Groupe stable orthogonal	46
1.3.6 Automorphismes du groupe discriminant	50
1.4 Réseaux de Niemeier	52
1.4.1 Configurations possibles pour les racines	52
1.4.2 Construction des réseaux de Niemeier	53
2 Produits automorphes	63
2.1 La fonction Φ_{12} de Borcherds	63
2.1.1 Généralités	63
2.1.2 Construction de Φ_{12}	64
2.2 La méthode de quasi-restriction	65
2.2.1 Théorème de quasi-restriction	66
2.2.2 Caractérisation des formes réflexives	67
2.2.3 Algorithme de détermination des formes modulaires réflexives	71

3	Classification des formes modulaires réflexives obtenues par quasi-restriction, première approche	73
3.1	Formes modulaires strictement -2 -réflexives	73
3.1.1	Condition suffisante	73
3.1.2	Classification des formes modulaires strictement -2 -réflexives . . .	74
3.2	Autres formes réflexives	78
3.2.1	Algorithme de recherche	78
3.2.2	Liste des formes réflexives obtenues à partir des “21 premiers” réseaux de Niemeier	80
3.2.3	Liste des formes réflexives obtenues à partir des réseaux de Niemeier $N(12A_2)$ et $N(24A_1)$	99
4	A propos du groupe modulaire maximal pour la quasi-restriction	109
4.1	Prolongement des automorphismes	109
4.2	Transformation de F_L	110
4.3	Retour sur les formes obtenues	111
5	Classification des formes modulaires réflexives obtenues par quasi-restriction, autres exemples	123
5.1	Choix du réseau L	123
5.2	Calcul de $L_{L'}^\perp$	124
5.3	Calcul des formes	125
5.4	Détermination du groupe modulaire maximal des nouvelles formes obtenues	128
5.5	Bilan sur les formes obtenues	129
	Annexe 1 : Liste des formes modulaires réflexives	131
	Annexe 2 : Calculs de diviseurs	135
	Index	148
	Bibliographie	149

Introduction

La fonction Φ_{12} de Borcherds est une forme modulaire en 26 variables, pour le groupe orthogonal associé au réseau unimodulaire pair de signature $(2, 26)$, $II_{2,26}$, et le caractère déterminant. Cette fonction a été construite par R.E. Borcherds avec la théorie des produits automorphes (voir l'article [Bo95]).

Cette forme modulaire est de poids 12, c'est le poids singulier (le plus petit poids possible) pour les formes modulaires pour le groupe orthogonal associé au réseau unimodulaire pair de signature $(2, 26)$. C'est le deuxième exemple de forme modulaire en 26 variables de poids singulier, le premier exemple étant dû à V. Gritsenko dans [Gr88] et [Gr94], et faisant appel au "lifting additif" d'une forme de Jacobi. C'était alors le premier cas de forme modulaire pour un groupe orthogonal non-triviale et de poids singulier.

Si la forme construite par Gritsenko était de caractère trivial (on dira que la forme est *invariante*), la forme Φ_{12} construite par Borcherds est de caractère déterminant (on dira que la forme est *anti-invariante*), et est d'ailleurs, à scalaire multiplicatif près, l'unique forme modulaire anti-invariante de poids 12 pour le groupe orthogonal associé au réseau unimodulaire pair de signature $(2, 26)$: son diviseur est "le plus petit possible".

Φ_{12} est aussi un exemple remarquable de forme modulaire définie par un produit infini, cette théorie inventée par Borcherds est développée dans ses deux articles fondamentaux [Bo95] et [Bo98]. On trouve beaucoup d'applications dans les articles [GN98-1], [GN98-2] et [GN02] de V. Gritsenko et V. Nikulin, dans [Br04] de J.H. Bruinier, dans [S06] de N. Scheithauer...

Une application remarquable de ces produits automorphes, due à Borcherds, est l'obtention de la formule dénominateur de la "Fake Monster Lie Algebra",

$$e^{-2\pi i(\rho|v)} \prod_{r>0} (1 - e^{2\pi i(r|v)})^{p_{24}(1-r^2/2)} = \sum_{w \in W} \sum_{n>0} \det(w) \tau(n) e^{-2\pi i n(w(\rho)|v)},$$

qui joue le rôle fondamental dans la preuve de la "Moonshine Conjecture" ([Bo92]). Or cette égalité peut s'obtenir à partir de la fonction Φ_{12} .

Enfin, les zéros de Φ_{12} sont des hyperplans qui définissent une réflexion orthogonale laissant le réseau $II_{2,26}$ invariant. Plus précisément, le diviseur de Φ_{12} (l'ensemble de ses zéros) est l'union des hyperplans qui sont l'orthogonal de vecteurs de $II_{2,26}$ de norme -2 .

Nous connaissons une autre forme anti-invariante célèbre dont le diviseur est lui aussi l'union des hyperplans qui sont l'orthogonal de vecteurs de $II_{2,26}$ de norme -2 . Il s'agit de la forme Δ_{35} , forme modulaire anti-invariante de poids 35 pour le groupe orthogonal associé au réseau $2U \oplus \langle -2 \rangle$ de signature $(2, 3)$. Cette forme a été construite pour la première fois par Igusa dans son article [I64] (pour Igusa, il s'agit d'une forme modulaire

de Siegel, qui peut être considérée suivant notre approche comme une forme modulaire pour le groupe orthogonal $SO^+(2U \oplus \langle -2 \rangle)$, voir [Gr94]). Deux autres constructions plus simples de cette forme sont dues à V. Gritsenko et V. Nikulin, dans leurs articles [GN96] et [GN98-2], à l'aide de formes de Jacobi et d'opérateurs de Hecke. Enfin, H. Aoki et T. Ibukiyama dans [AI05] retrouvent une autre construction de Δ_{35} à partir de calculs de déterminants et de dérivées partielles. Nous trouvons dans cette thèse une construction naturelle de cette forme modulaire (notée ici F_{A_1}) à partir de Φ_{12} et en utilisant le code de Golay, en partie 3.1.2.

On dira d'une forme modulaire pour le groupe orthogonal associé à un réseau L , dont les zéros sont des hyperplans définissant une réflexion orthogonale laissant le réseau L invariant, qu'elle est réflexive. Φ_{12} et Δ_{35} sont donc deux exemples particuliers de formes réflexives.

Le problème de la classification des formes modulaires réflexives est très important, de telles formes ont des propriétés remarquables et beaucoup d'applications dans différents domaines mathématiques et physique : en théorie des algèbres de Lie de Kac-Moody, en géométrie algébrique, en théorie des cordes...

Suivant les résultats de classification des réseaux hyperboliques dus à Nikulin, il n'y a, en principe, qu'un nombre fini de formes modulaires réflexives (voir [GN02] pour les résultats et les autres références), on peut donc essayer de les classifier. Dans son article [Bo00], R.E. Borcherds donne de nombreux exemples de formes modulaires réflexives associées à des réseaux unimodulaires pairs. V. Gritsenko et V. Nikulin, dans l'article [GN02] ont classifié les formes modulaires réflexives associées aux réseaux de signature $(2, 3)$ de la forme $2U + \langle -2t \rangle$, $t \in \mathbb{N}^*$. Ils ont ainsi construit 29 formes réflexives, donné leurs expressions en produit automorphe ainsi qu'en "lifting additif", et décrit leurs diviseurs. N. Scheithauer a lui classifié les formes modulaires réflexives de poids singuliers dont les composantes du diviseur sont de multiplicité 0 ou 1, dans le cas où le réseau associé est de niveau sans facteur carré, dans son article [S06].

Dans cette thèse, nous obtenons une nouvelle classe de formes réflexives associée à Φ_{12} (les "baby functions" de Φ_{12}). Nous nous intéressons à la remarque faite par Borcherds dans [Bo95], exemples 3 et 4 de la partie 16 (il y construit en particulier la forme réflexive associée à $2U \oplus \mathbb{E}_8(-1)$, où $L(-1)$ désigne le réseau L muni d'une forme quadratique définie négative). La forme Φ_{12} est une forme modulaire définie sur le domaine homogène associé au réseau $II_{2,26}$ (voir la partie 1.3.1 et la définition 1.34). Si L est un sous-réseau de $II_{2,26}$ contenant deux plans hyperboliques, alors le domaine associé à L est un sous-domaine de celui associé à $II_{2,26}$. On souhaiterait considérer la restriction de Φ_{12} à ce domaine, cependant, étant données les propriétés des zéros de Φ_{12} , cette restriction est identiquement nulle dès lors qu'il existe une racine dans l'orthogonal de L dans $II_{2,26}$. C'est pourquoi il faut considérer la restriction au sous-domaine associé à L du quotient de Φ_{12} par le produit des fonctions linéaires correspondants aux facteurs qui s'annulent sur L . La fonction alors obtenue, qu'on nommera par la suite quasi-restriction de Φ_{12} , est une forme modulaire pour le groupe orthogonal associé à L (de signature $(2, n')$) et le caractère déterminant. Son poids est $12 + \frac{1}{2} \# \{r \in L_{II_{2,26}}^+ \mid r^2 = -2\}$, et son diviseur peut être déduit de celui de Φ_{12} par l'étude des projections des vecteurs de norme -2 de $II_{2,26}$.

L'idée de Borchers a été largement utilisée, dans l'article [BKPS98] pour démontrer un résultat relatif aux familles de surfaces de Kähler. Dans [GHS07] et [GHS08-1], Gritsenko, Hulek et Sankaran utilisent la quasi-restriction de Φ_{12} dans leurs études des espaces de modules des surfaces $K3$ et des variétés symplectiques irréductibles, comme l'avait aussi fait S. Kondo dans [Ko99].

L'objet de cette thèse est donc d'étudier cette classe de fonctions réflexives obtenues par quasi-restriction de la fonction Φ_{12} . A l'aide de méthodes arithmétiques, pour un sous-réseau donné L de $II_{2,26}$ contenant deux plans hyperboliques, nous calculons le diviseur de la fonction obtenue par quasi-restriction, et déterminons si la forme est réflexive ou non.

Le premier chapitre permet de fixer les notations, et de rappeler des résultats sur les réseaux et les codes ([Eb02], [CS98]), sur le groupe orthogonal associé à un réseau ([Gr94]), et sur les formes modulaires pour les groupes orthogonaux ([Bo95]). En particulier, une forme modulaire f de poids $k \in \mathbb{Z}$ et caractère $\chi \in \widehat{O^+(L)}$ pour un groupe orthogonal $O^+(L)$ est une fonction holomorphe sur le domaine $\mathcal{D}^0(L)$ vérifiant les relations

- (i) $\forall \lambda \in \mathbb{C}^*, f(\lambda Z) = \lambda^{-k} f(Z)$.
- (ii) $\forall g \in O^+(L), f(gZ) = \chi(g) f(Z)$.
- (iii) "une condition d'holomorphicité à l'infini".

Nous citons aussi des résultats sur les formes quadratiques discriminantes ([N79]), quelques lemmes utiles lors de la classification en partie 3.2.2, et des tables explicites pour manipuler les réseaux de Niemeier (voir la partie 1.4.2, basée sur [CS98]).

Le second chapitre, partie fondamentale de la thèse, explicite, après avoir rappelé des résultats sur Φ_{12} et sa construction, la méthode de quasi-restriction. En particulier, les composantes du diviseur de la fonction F_L obtenue par la quasi-restriction de Φ_{12} relative au réseau L , sont les hyperplans dirigés par les projections l^* dans le réseau dual de L , L^* , dont la norme vérifie $-2 \leq l^{*2} < 0$, des racines de $II_{2,26}$. Nous donnons une méthode systématique pour calculer ces composantes, et déterminer si une telle forme est réflexive. Cette méthode s'appuie essentiellement sur les techniques des formes quadratiques discriminantes introduites par Nikulin ([N79]), mais nécessite aussi une description explicite des réseaux manipulés, d'où le recours aux tables de la partie 1.4.2 et aux codes de Golay (partie 1.2.4).

Le troisième chapitre quant à lui est dédié à la classification proprement dite. Après avoir défini une classe particulière de formes réflexives, appelées formes strictement -2 -réflexives et correspondant aux formes réflexives (associées à un réseau L) dont le diviseur coïncide exactement avec l'union de tous les hyperplans dirigés par des vecteurs de norme -2 du réseau L , avec multiplicité 1 (Φ_{12} et Δ_{35} sont de telles formes), nous donnons une classification complète de ces formes, obtenues par quasi-restriction de Φ_{12} , dans le cas de la décomposition du réseau unimodulaire pair de signature $(2, 26)$ sous la forme $2U \oplus N(-1)$ où N est l'un des 23 réseaux de Niemeier différent du réseau de Leech. Nous trouvons 25 formes, toutes sauf une correspondant à des réseaux de racines. En particulier, nous retrouvons ici la forme Δ_{35} de Igusa (partie 3.1.2), ainsi que d'autres formes qui apparaissent dans [Kl05], [DK03] et [Kr05].

Dans un second temps, nous donnons la liste exhaustive des formes modulaires réflexives obtenues par quasi-restriction de Φ_{12} , à partir d'un sous-réseau $2U \oplus L(-1)$ de $2U \oplus N(-1) \cong II_{2,26}$ contenant deux plans hyperboliques et où L est une composante orthogonale du sous-réseau de racines de N , l'un des 23 réseaux de Niemeier différent du réseau de Leech. Nous trouvons alors 23 formes réflexives supplémentaires. Le calcul des formes relatives au réseau de Niemeier $N(24A_1)$ fait largement appel aux propriétés du code de Golay binaire étendu, et certains calculs ont nécessité l'utilisation (très simple) de l'ordinateur (voir Annexe 2).

Chacune de ces 48 formes est donnée avec la description précise de son diviseur.

Le quatrième chapitre est une révision des résultats précédents. En effet, la méthode de quasi-restriction permet d'obtenir, à partir de Φ_{12} et d'un réseau pair L contenant deux plans hyperboliques, une forme modulaire pour le groupe stable orthogonal associé à L , $\tilde{O}^+(L)$. Ce dernier groupe n'est qu'un sous-groupe (d'indice fini) du groupe orthogonal associé à L , $O^+(L)$. Il est donc raisonnable de se demander si le groupe modulaire maximal de la forme obtenue n'est pas plus important que $\tilde{O}^+(L)$. A partir de résultats dus à Nikulin ([N79]) et des tables de la partie 1.4.2, nous étudions, pour chacune des 48 formes précédemment construites, leur groupe modulaire maximal, et donnons le cas échéant la nouvelle description de leur diviseur sous l'action de ce groupe.

Enfin, dans le cinquième et dernier chapitre, nous présentons quelques exemples particuliers de formes modulaires réflexives obtenues par quasi-restriction, dans un cas plus général que pour la classification faite en chapitre 3. Cependant, les choix des réseaux L n'ont pas été faits au hasard, l'objectif étant d'une part d'obtenir des formes relatives à des réseaux de racines pour lesquels nous avons trouvé en chapitre 3 une forme strictement -2 -réflexive, et d'autre part que ces formes aient un poids le plus petit possible. Nous trouvons ainsi 13 formes modulaires réflexives, dont nous déterminons le groupe modulaire maximal et le diviseur. Ensuite, en considérant le quotient de ces formes par la forme strictement -2 -réflexive construite dans le chapitre 3 leur correspondant, nous obtenons 13 formes réflexives (mais qui ne sont plus des quasi-restrictions). L'une d'entre elles est une forme de poids singulier, elle est associée au réseau de signature $(2, 8)$, $2U \oplus 3A_2(-1)$. Trois autres sont le carré de formes de poids singuliers, associées aux réseaux $2U \oplus 4A_1(-1)$ (signature $(2, 6)$), $2U \oplus 2D_4(-1)$ (signature $(2, 10)$) et $2U \oplus D_8(-1)$ (signature $(2, 10)$).

Nous pouvons aussi faire de nombreux liens avec des formes déjà connues. En particulier, nos formes F_{A_1} et G_{A_1} correspondent aux formes Δ_{35} et Δ_5^2 construites par Igusa dans [I64], et on a la relation $F_{A_1}^{(2)} = \Delta_{30}\Delta_5^3$. Dans la thèse de Klöcker ([Kl05]), chapitre 5, on trouve les formes modulaires ψ_3 (p.100), ψ_{30} (p.100) et ψ_{54} (p.92), que l'on peut relier à nos résultats avec les relations suivantes : $G_{3A_1} = \psi_3^2$, $F_{3A_1} = \psi_{30}\psi_3$ et $F_{A_3} = \psi_{54}$. Dans l'article de T. Dern et A. Krieg, [DK03], nous trouvons les formes notées ϕ_9 (p.261) et ϕ_{45} (p.261) qui correspondent respectivement à G_{A_2} et F_{A_2} , ainsi que les formes ϕ_4 (p.261) et ϕ_{30} (p.261), vérifiant $\phi_4^2 = G_{2A_1}$ et $F_{2A_1} = \phi_{30}\phi_4$. On trouvera aussi la forme G_{A_2} dans [D03] p.227 et [D06] p.109 où elle est notée $F_{\Delta(\tau)_{a-3,1}}$. Il faut aussi noter que les formes F_{2A_1} et G_{2A_1} sont des généralisations des formes Δ_{35} et Δ_5 (Δ_5^2 pour être plus précis). Enfin, nous retrouvons dans l'article de Krieg [Kr05], p.932, les formes qu'il note Δ et G_8 , qui satisfont les relations $\Delta = F_{D_4}$ et $G_8^2 = G_{D_4}$.

En annexe 1, nous donnons la liste des 73 formes construites dans cette thèse, leur poids, le réseau associé, et leur diviseur. En annexe 2, nous détaillons les procédures Maple (très basiques) utilisées pour calculer les diviseurs des formes F_{8A_1} , F_{9A_1} , F_{10A_1} et F_{4A_2} .

Nous avons obtenu dans cette thèse 73 formes modulaires réflexives associées à des réseaux de signature $(2, n)$ pour $3 \leq n \leq 25$. 60 sont obtenues par quasi-restriction, 24 parmi celles-ci sont strictement -2 -réflexives (leur diviseur est le plus “petit” possible). Les 13 autres sont réflexives et obtenues par quotient de deux quasi-restrictions. Nous pouvons affirmer que la fonction Φ_{12} de Borchers est une fonction très importante dans la théorie des formes automorphes où elle joue le rôle d’une fonction universelle. En effet, nous avons montré que celle-ci contient “toute l’information” de nombreuses formes automorphes.

Chapitre 1

Réseaux, codes, groupes orthogonaux et formes modulaires

1.1 Réseaux

1.1.1 Réseaux quadratiques

Dans cette partie, nous introduisons la notion de réseau quadratique, sans détailler les preuves des propriétés annoncées. L'objectif étant de fixer les notations. Nous suivons essentiellement le livre d'Ebeling [Eb02].

Définition 1.1. On appelle réseau quadratique un \mathbb{Z} -module libre de rang $n \in \mathbb{N}^*$ noté L , muni d'une forme bilinéaire symétrique non dégénérée sur $L \otimes \mathbb{Q}$. Soit (e_1, \dots, e_n) une \mathbb{Z} -base de L , on dira que (e_1, \dots, e_n) est une base du réseau L . n est le rang du réseau L ou encore la dimension du réseau L .

On notera $L(-1)$ le \mathbb{Z} -module L muni de la forme bilinéaire symétrique $-(\cdot|\cdot)$.

Par la suite, on dira souvent "réseau" pour "réseau quadratique". On dira qu'un réseau quadratique est *entier* s'il vérifie

$$\forall x, y \in L, (x|y) \in \mathbb{Z},$$

où $(\cdot|\cdot)$ est la forme bilinéaire symétrique attachée au réseau L . On dira qu'un réseau quadratique est *pair* s'il vérifie

$$\forall x \in L, x^2 = (x|x) \in 2\mathbb{Z}.$$

En particulier, un réseau pair est entier (formule de polarisation).

Exemple. Un exemple de réseau quadratique entier, mais non pair, est \mathbb{Z}^n , $n \in \mathbb{N}^*$, dans l'espace \mathbb{R}^n muni du produit scalaire euclidien usuel. Un autre exemple fondamental est le *plan hyperbolique*, noté U , qui consiste en l'ensemble \mathbb{Z}^2 muni de la forme bilinéaire symétrique donnée par la matrice $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. C'est un réseau entier pair. Une base (e, f)

de U telle que $e^2 = f^2 = 0$ et $(e|f) = 1$ est appelée *couple hyperbolique*.

Citons maintenant un théorème utile auquel nous nous réfèrerons par la suite sous le nom de théorème de la base adaptée (voir [Go05] pour une preuve).

Théorème 1.1. [Théorème de la base adaptée]

Soit A un anneau principal, M un A -module libre de rang r , et N un sous-module de M , alors

(i) le module N est libre de rang $s \leq r$,

(ii) il existe (e_1, \dots, e_r) une base de M sur A et $a_1, \dots, a_s \in A$ tels que a_i divise a_{i+1} et

$$N = Aa_1e_1 \oplus \dots \oplus Aa_s e_s.$$

Les a_i sont appelés facteurs invariants de N .

Matriciellement, cela signifie que pour toute matrice $M \in \mathcal{M}_r(A)$, il existe deux matrices $A, B \in SL_r(A)$ telle que AMB^{-1} soit une matrice diagonale dont les coefficients diagonaux non nuls $a_1, \dots, a_s \in A$ sont tels que a_i divise a_{i+1} .

Définition 1.2. On dit que deux réseaux quadratiques L et M sont isomorphes s'il existe ϕ un isomorphisme de \mathbb{Z} -modules de L vers M , tel que

$$\forall x, y \in L, (\phi(x)|\phi(y))_M = (x|y)_L.$$

où $(\cdot|\cdot)_L$ désigne la forme bilinéaire symétrique attachée à L et $(\cdot|\cdot)_M$ celle attachée à M .

En particulier, la matrice de ϕ dans un couple de bases pour L et M est à coefficients entiers, et est inversible, elle est donc de déterminant ± 1 .

Soit maintenant L un réseau entier, (e_1, \dots, e_n) une base de L . On forme la matrice $G = ((e_i|e_j))_{1 \leq i, j \leq n}$. G est une matrice à coefficients entiers, symétrique, de déterminant non nul, appelée *matrice de Gram* de L . Ce déterminant est indépendant du choix de la base choisie pour L (en effet, d'après ce qui précède un changement de base définit un automorphisme de L , et sa matrice est de déterminant ± 1), ainsi on appelle *déterminant* de L le déterminant de G . On le notera $\det(L)$.

Définition 1.3. On appelle sous-réseau de L tout sous-module M de L (non nécessairement de rang n), muni de la forme bilinéaire symétrique $(\cdot|\cdot)_M$ obtenue par la restriction de $(\cdot|\cdot)$ à $M \otimes \mathbb{Q}$.

Le théorème de la base adaptée (théorème 1.1) nous permet d'assurer que M est bien un réseau.

Définition 1.4. On appelle réseau dual de L le réseau

$$L^* = \{x \in L \otimes \mathbb{Q} \mid \forall y \in L, (x|y) \in \mathbb{Z}\}.$$

L^* est bien un réseau, car si (e_1, \dots, e_n) est une base de L , on vérifie que la base duale associée à (e_1, \dots, e_n) est une base de L^* . En particulier, L et L^* ont le même rang. La matrice de Gram de L^* est G^{-1} . Si L est un réseau entier, alors $L \subset L^*$ en tant que sous-réseau, et $|L^*/L| = \det(L)$.

Définition 1.5. *Un réseau L est dit unimodulaire lorsque l'on a $L = L^*$.*

Lemme 1.1. *Soient L_1 et L_2 deux réseaux entiers de rang $n \in \mathbb{N}^*$, tels que $L_1 \subset L_2$. Alors on a la suite d'inclusions*

$$L_1 \subset L_2 \subset L_2^* \subset L_1^*.$$

PREUVE : La première inclusion vient de l'hypothèse $L_1 \subset L_2$, la seconde vient du fait que L_2 soit entier, reste à traiter la troisième. Soit $y \in L_2^*$, alors par définition de L_2^* , $\forall x \in L_2, (x|y) \in \mathbb{Z}$. En particulier, puisque $L_1 \subset L_2, \forall x \in L_1, (x|y) \in \mathbb{Z}$, ce qui signifie que $y \in L_1^*$. Finalement on a bien montré que $L_2^* \subset L_1^*$. \square

Définition 1.6. *Soit M un réseau, et L un sous-réseau de M . Alors L est dit primitif si M/L est un \mathbb{Z} -module libre.*

Définition 1.7. *Soit M un réseau, et L un sous-réseau (quelconque) de M . On pose*

$$L' = \{x \in M \mid \forall y \in L, (x|y) = 0\}.$$

Alors L' est un réseau, on l'appelle le réseau orthogonal à L dans M , noté $L' = L_M^\perp$.

Lemme 1.2. *Soit M un réseau, L_1 un sous-réseau (quelconque) de M , et $L_2 = L_1_M^\perp$ le réseau orthogonal à L_1 dans M . Alors $\text{rg}(L_1) + \text{rg}(L_2) = \text{rg}(M)$.*

PREUVE : $\text{rg}(L_1) = \dim(L_1 \otimes \mathbb{Q}), \text{rg}(L_2) = \dim(L_2 \otimes \mathbb{Q})$ et $\text{rg}(M) = \dim(M \otimes \mathbb{Q})$. Comme $L_2 \otimes \mathbb{Q}$ est l'orthogonal dans $M \otimes \mathbb{Q}$ de $L_1 \otimes \mathbb{Q}$ en tant que \mathbb{Q} -espaces vectoriels, l'égalité annoncée sur les rangs vient de l'égalité des dimensions connues pour les espaces vectoriels. \square

Lemme 1.3. *Soient M un réseau et L un sous-réseau de M . Alors L est primitif si et seulement si il existe un sous-réseau L' de M tel que $L = L_M'^\perp$.*

PREUVE : • S'il existe L' sous-réseau de M tel que $L = L_M'^\perp$. On suppose par l'absurde que L n'est pas un sous-réseau primitif, c'est-à-dire que le \mathbb{Z} -module M/L n'est pas libre. Il existe donc $v \in M$ tel que $v \notin L$, et $k \in \mathbb{N}^*$ tel que $kv \in L$. Pourtant, $\forall u \in L', k(u|v) = (u|kv) = 0$, avec $k \neq 0$, c'est-à-dire que $\forall u \in L', (u|v) = 0$ et donc

$v \in L'_M^\perp = L$, ce qui est absurde. Donc L est bien primitif.

• Si L est primitif, considérons $L' = L_M^\perp$ le réseau orthogonal à L dans M . Soit $l \in L$, alors $\forall l' \in L'$, $(l|l') = 0$ par définition de L' . Donc en particulier, $l \in L'_M^\perp$, ce qui signifie que $L \subset L'_M^\perp$. Supposons par l'absurde qu'il existe $l \in L'_M^\perp$ mais $l \notin L$. D'après le lemme 1.2, $\text{rg}(L) = \text{rg}(L'_M^\perp)$, puis le théorème de la base adaptée (théorème 1.1) nous permet d'affirmer qu'il existe $k \in \mathbb{N}^*$ tel que $kl \in L$ (par exemple prendre pour k le plus grand des facteurs invariants convient). Ceci est en contradiction avec le fait que L est primitif, donc $L = L'_M^\perp$ et l'affirmation du lemme est bien prouvée. \square

Pour terminer cette partie, nous introduisons une notion importante en théorie des réseaux, en ce qui concerne les empilements de sphères.

Définition 1.8. Soit L un réseau quadratique défini positif. Le kissing number τ_L de L est la norme minimale d'un vecteur non-nul de L :

$$\tau_L = \min\{\alpha \in \mathbb{R} \mid (x|x) = \alpha, x \in L, x \neq 0\}.$$

1.1.2 Séries Thêta

Soit L un réseau défini positif. On peut associer à L une fonction définie sur le demi-plan supérieur (dit demi-plan de Poincaré), $\mathbb{H}_1 = \{\tau \in \mathbb{C} \mid \text{Im}\tau > 0\}$.

Définition 1.9. La série thêta du réseau L est la série définie, pour $\tau \in \mathbb{H}_1$, posant $q = e^{2\pi i\tau}$, par :

$$\vartheta_L(\tau) = \sum_{x \in L} q^{\frac{1}{2}(x|x)}.$$

Cette série converge normalement sur \mathbb{H}_1 .

On suppose (pour simplifier) que L est un réseau entier pair. La série converge normalement sur \mathbb{H}_1 , et définit donc une fonction holomorphe sur \mathbb{H}_1 . On peut aussi réécrire la série précédente sous la forme

$$\vartheta_L(\tau) = \sum_{r=0}^{\infty} a_r q^r,$$

où $a_r = \#\{x \in L \mid (x|x) = 2r\}$, c'est à dire que les nombres a_r comptent le nombre de vecteurs de L de norme $2r$. En particulier, le kissing number de L est $2r_0$, où r_0 est le premier indice non nul r tel que a_r est non nul.

On dispose de nombreux résultats sur les séries thêta, et nous n'avons pas pour but de tous les citer. Nous donnons à la suite les quelques résultats qui nous concernent.

Définition 1.10. Soit $\mu \in \mathbb{N}^*$. On appelle sous-groupe principal de congruence de niveau μ le sous-groupe de $SL_2(\mathbb{Z})$ défini par

$$\Gamma(\mu) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid a \equiv d \equiv 1 \pmod{\mu}, b \equiv c \equiv 0 \pmod{\mu} \right\}$$

On appelle sous-groupe de congruence de niveau μ tout sous-groupe de $\Gamma(\mu)$.

Définition 1.11. Soit $\mu \in \mathbb{N}^*$. Soit f une fonction holomorphe sur \mathbb{H}_1 , et soit $\Gamma' \subset \Gamma(\mu)$ un sous-groupe de congruence de niveau μ . Soient $k \in \mathbb{Z}$ et χ un caractère de Γ' . On dira que f est une forme modulaire de poids k et de caractère χ si f vérifie :

$$(i) \forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma', (cz + d)^{-k} f\left(\frac{az+b}{cz+d}\right) = \chi(\gamma)f(z),$$

$$(ii) \forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}), (cz + d)^{-k} f\left(\frac{az+b}{cz+d}\right) \text{ peut s'écrire sous la forme } \sum_{n=0}^{\infty} a_n q_N^n$$

où $q_N = e^{\frac{i2\pi z}{N}}$.

Lorsque $\mu = 1$ et $\Gamma' = SL_2(\mathbb{Z})$, on retrouve la définition usuelle d'une forme modulaire.

Proposition 1.1. ([Eb02], p.40)

Soit L un réseau unimodulaire pair de rang n . Alors

$$(i) n \equiv 0 \pmod{8},$$

$$(ii) \vartheta_L \text{ est une forme modulaire de poids } \frac{n}{2}.$$

Définition 1.12. Soit L un réseau entier pair de rang $n \in \mathbb{N}^*$. On appelle niveau de L l'entier $\lambda \in \mathbb{N}^*$ défini par

$$\lambda = \min\{k \in \mathbb{N}^* \mid \forall l^* \in L^*, kl^{*2} \in 2\mathbb{Z}\}.$$

En particulier, $\lambda \mid \det(L)$ et $\det(L) \mid \lambda^n$.

Proposition 1.2. ([Eb02], p.99)

Soit L un réseau entier pair de rang $n \in \mathbb{N}^*$, avec n pair, $n \geq 2$, et de niveau $\lambda \in \mathbb{N}^*$. Alors ϑ_L est une forme modulaire de poids $\frac{n}{2}$ et caractère χ pour le groupe $\Gamma_0(\lambda)$, où on

$$\Gamma_0(\lambda) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid \lambda \mid c \right\} \text{ et } \chi : \Gamma_0(\lambda) \rightarrow \mathbb{C}^* ; A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \left(\frac{\Delta}{d}\right) \text{ où } \Delta = (-1)^{\frac{n}{2}} \det(L) \text{ et } (\cdot) \text{ est le symbole de Legendre.}$$

Enfin, il existe de nombreuses tables (bien utiles) pour les coefficients des séries thêta de réseaux (non nécessairement entiers, et non nécessairement de dimension paire). On pourra consulter par exemple [CS98], p.101 à p.135.

1.1.3 Réseaux de racines

Les réseaux dit "de racines" joueront par la suite un rôle très important. Leurs définition et propriétés principales font l'objet de ce paragraphe.

Définition 1.13. Soit L un réseau défini positif. On appelle racine de L un vecteur de carré 2, on note $R_L = \{x \in L \mid x^2 = 2\}$ les racines de L . L est alors appelé réseau de racines s'il est engendré par R_L .

Définition 1.14. Soit L un réseau entier pair défini positif. On appelle sous-réseau de racines de L le sous-réseau L_R de L engendré par les racines de L . En particulier, c'est un réseau de racines.

On peut classifier les réseaux de racines. Donnons d'abord une description de leurs ensembles générateurs.

Définition 1.15. On appelle système fondamental de racines d'un réseau de racines L , un ensemble $S \subset R_L$ tel que

(i) S est une base de L ,

(ii) Chaque $\beta \in R_L$ peut s'écrire comme combinaison linéaire $\beta = \sum_{\alpha \in S} k_\alpha \alpha$, avec les $k_\alpha \in \mathbb{Z}$ tous positifs ou nuls, ou tous négatifs ou nuls.

Théorème 1.2. ([Eb02], p.16)

Soit L un réseau de racines. Alors il existe un système fondamental de racines pour L , que l'on note (e_1, \dots, e_n) . Cette base vérifie

$$\forall 1 \leq i \leq n, e_i^2 = 2, \quad \forall 1 \leq i, j \leq n, i \neq j, (e_i | e_j) \in \{0, -1\}.$$

Diagrammes de Coxeter-Dynkin. A tout système fondamental de racines (e_1, \dots, e_n) d'un réseau de racines L , on peut associer le diagramme de Coxeter-Dynkin défini comme suit :

si $(e_i | e_j) = -1$, pour $i \neq j$, alors on relie les sommets i et j par une arête,

si $(e_i | e_j) = 0$, pour $i \neq j$, alors on ne relie pas les sommets i et j .

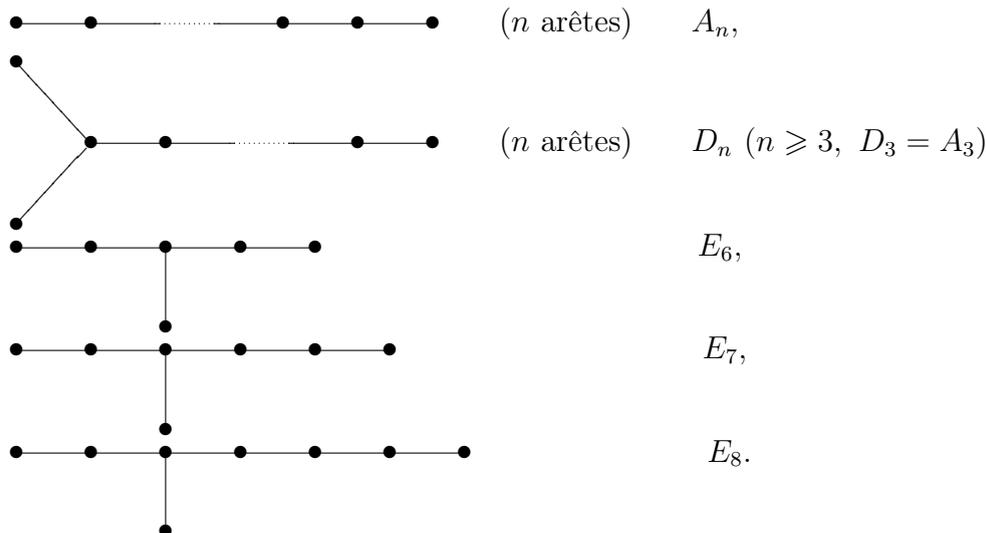
$$\begin{aligned} (e_i | e_j) = -1 &\longleftrightarrow \begin{array}{c} \bullet \text{---} \bullet \\ e_i \quad e_j \end{array} \\ (e_i | e_j) = 0 &\longleftrightarrow \begin{array}{cc} \bullet & \bullet \\ e_i & e_j \end{array} \end{aligned}$$

Définition 1.16. Un réseau L est dit réductible si $L = L_1 \oplus L_2$ est somme directe orthogonale de deux réseaux L_1, L_2 de rangs ≥ 1 . Sinon, L est dit irréductible.

Soit L un réseau de racines. Alors L est irréductible si et seulement si son diagramme de Coxeter-Dynkin est connexe. De façon générale, un réseau de racines est somme directe de réseaux de racines irréductibles.

Théorème 1.3. ([Eb02], p.22)

Tout réseau de racines L est somme directe orthogonale de réseaux de racines irréductibles, chacun ayant un diagramme de Coxeter-Dynkin de la forme de l'un des graphes suivants :



Nombre de Coxeter. On définit le *nombre de Coxeter* d'un réseau de racines L comme étant

$$h = \frac{\#R_L}{n}.$$

Proposition 1.3. ([Eb02], prop. 1.6 p.30)

Soit L un réseau de racines irréductible. Alors pour $y \in L \otimes \mathbb{R}$, on a

$$\sum_{x \in R_L} (x|y)^2 = 2h(y|y),$$

où h est le nombre de Coxeter de L .

Groupe de Weyl d'un réseau de racines. Soit L un réseau de racines. Soit r une racine de L , alors la réflexion $\sigma_r : v \mapsto v - (v|r)r$ est un élément du groupe des automorphismes du réseau $O(L)$.

Définition 1.17. Soit L un réseau de racines. On appelle *groupe de Weyl* de L , noté $W(L)$, le sous-groupe de $O(L)$ engendré par les réflexions $\sigma_r, r \in R_L$.

Lemme 1.4. ([Eb02], p.25)

Soit L un réseau de racines irréductible. Alors le groupe de Weyl, $W(L)$, agit :

- irréductiblement sur $L \otimes \mathbb{R}$ (i.e. si U est un espace $W(L)$ -invariant, alors $U = \{0\}$ ou $U = L \otimes \mathbb{R}$),
- transitivement sur les racines de L .

Corollaire 1.1. *Soit L un réseau de racines irréductible, alors $W(L)$ agit transitivement sur les couples de racines (r_1, r_2) tels que $(r_1|r_2) = 0$ et sur ceux tels que $(r_1|r_2) = -1$.*

PREUVE : Soient (r_1, r_2) et (r'_1, r'_2) deux couples de racines de L tels que $(r_1|r_2) = 0$ et $(r'_1|r'_2) = 0$. Il existe $g \in W(L)$, $g(r_1) = r'_1$. D'autre part, comme $g \in O(L)$, $(g(r_2)|g(r_1)) = (g(r_2)|r'_1) = 0$. Ainsi, on vérifie que $\sigma_{g(r_2)-r'_2} \circ g$ envoie r_1 sur r'_1 (car $r'_1 \perp g(r_2), r'_2$) et r_2 sur r'_2 (par construction de $\sigma_{g(r_2)-r'_2}$). $W(L)$ est bien transitif sur un tel couple. Si (r_1, r_2) et (r'_1, r'_2) sont deux couples de racines de L tels que $(r_1|r_2) = -1$ et $(r'_1|r'_2) = -1$, alors la même démonstration s'applique. \square

Construction des réseaux de racines irréductibles. Passons maintenant à l'existence des réseaux de racines irréductibles. Nous donnons pour cela une réalisation de ces réseaux, sur laquelle nous nous appuyerons par la suite. Cette partie suit [CS98]. Dans la suite, on se placera dans l'espace \mathbb{R}^n (ou \mathbb{R}^{n+1} si on en fait mention), muni du produit scalaire euclidien usuel.

Réseaux \mathbb{A}_n : On note (e_0, e_1, \dots, e_n) la base canonique de \mathbb{R}^{n+1} . On pose

$$\mathbb{A}_n = \{(x_0, x_1, \dots, x_n) \in \mathbb{Z}^{n+1} \mid x_0 + \dots + x_n = 0\}.$$

\mathbb{A}_n est un réseau pair de dimension n . $(e_1 - e_0, e_2 - e_1, \dots, e_n - e_{n-1})$ en est une base dont le diagramme de Dynkin est de type A_n :



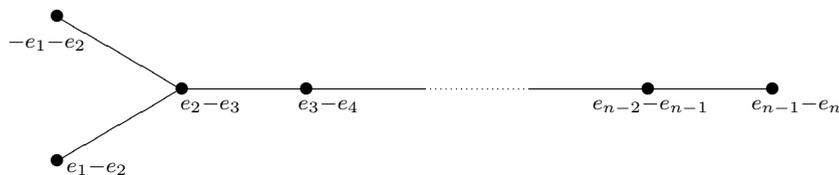
C'est donc un réseau de racines irréductible. On a $\det(\mathbb{A}_n) = n + 1$, le nombre de racines (kissing number) est $\tau_{\mathbb{A}_n} = n(n + 1)$, et le nombre de Coxeter est $h = n + 1$.

Pour $n = 1$, on notera aussi assez souvent $\mathbb{A}_1 = \langle 2 \rangle$, et $\mathbb{A}_1(-1) = \langle -2 \rangle$ le \mathbb{Z} -module \mathbb{A}_1 muni d'une forme bilinéaire symétrique définie négative.

Réseaux \mathbb{D}_n : On note (e_1, \dots, e_n) la base canonique de \mathbb{R}^n , $n \geq 3$. On pose

$$\mathbb{D}_n = \{(x_1, \dots, x_n) \in \mathbb{Z}^n \mid x_1 + \dots + x_n \equiv 0 \pmod{2}\}.$$

\mathbb{D}_n est un réseau pair de dimension n . $(-e_1 - e_2, e_1 - e_2, e_2 - e_3, \dots, e_{n-1} - e_n)$ en est une base dont le diagramme de Dynkin est de type D_n :

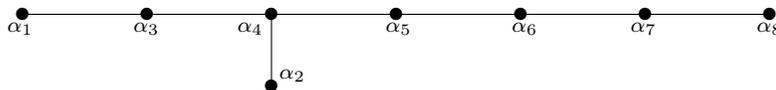


C'est donc un réseau de racines irréductible. On a $\det(\mathbb{D}_n) = 4$, le nombre de racines (kissing number) est $\tau_{\mathbb{D}_n} = 2n(n - 1)$, et le nombre de Coxeter est $h = 2(n - 1)$.

Réseau \mathbb{E}_8 : On note (e_1, \dots, e_8) la base canonique de \mathbb{R}^8 . On pose

$$\mathbb{E}_8 = \left\{ (x_1, \dots, x_8) \in \mathbb{Z}^8 \cup \left(\mathbb{Z} + \frac{1}{2} \right)^8 \mid x_1 + \dots + x_8 \equiv 0 \pmod{2} \right\}.$$

\mathbb{E}_8 est un réseau pair de dimension 8. $(\alpha_1 = \frac{1}{2}(e_1 + e_8) - \frac{1}{2}(e_2 + \dots + e_7), \alpha_2 = e_1 + e_2, \alpha_3 = e_2 - e_1, \alpha_4 = e_3 - e_2, \alpha_5 = e_4 - e_3, \alpha_6 = e_5 - e_4, \alpha_7 = e_6 - e_5, \alpha_8 = e_7 - e_6)$ en est une base dont le diagramme de Dynkin est de type E_8 :

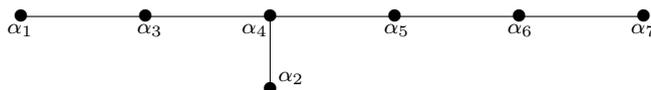


C'est donc un réseau de racines irréductible. On a $\det(\mathbb{E}_8) = 1$ (\mathbb{E}_8 est unimodulaire), le nombre de racines (kissing number) est $\tau_{\mathbb{E}_8} = 240$, et le nombre de Coxeter est $h = 30$. \mathbb{E}_8 est le seul réseau unimodulaire pair de dimension 8.

Réseau \mathbb{E}_7 : On définit \mathbb{E}_7 comme étant le réseau orthogonal dans \mathbb{E}_8 à une racine de \mathbb{E}_8 . Comme le groupe de Weyl agit transitivement sur les racines, le réseau ne dépend pas du choix de la racine. On pose $r = (e_7 + e_8)$, et on a

$$\mathbb{E}_7 = r_{\mathbb{E}_8}^\perp = \left\{ (x_1, \dots, x_8) \in \mathbb{Z}^8 \cup \left(\mathbb{Z} + \frac{1}{2} \right)^8 \mid x_1 + \dots + x_8 \equiv 0 \pmod{2}, x_7 + x_8 = 0 \right\}.$$

\mathbb{E}_7 est un réseau pair de dimension 7. $(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7)$ en est une base dont le diagramme de Dynkin est de type E_7 :

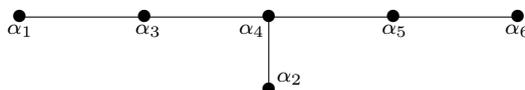


C'est donc un réseau de racines irréductible. On a $\det(\mathbb{E}_7) = 2$, le nombre de racines (kissing number) est $\tau_{\mathbb{E}_7} = 126$, et le nombre de Coxeter est $h = 18$.

Réseau \mathbb{E}_6 : On définit \mathbb{E}_6 comme étant le réseau orthogonal dans \mathbb{E}_8 à une copie de \mathbb{A}_2 . Comme le groupe de Weyl agit transitivement sur les copies de \mathbb{A}_2 dans \mathbb{E}_8 , le réseau ne dépend pas du choix de la copie de \mathbb{A}_2 . On pose $r_1 = (e_7 + e_8)$, $r_2 = (e_6 - e_7)$, si bien que (r_1, r_2) est une base d'un réseau de type \mathbb{A}_2 , et on a

$$\begin{aligned} \mathbb{E}_6 &= \langle r_1, r_2 \rangle_{\mathbb{E}_8}^\perp \\ &= \left\{ (x_1, \dots, x_8) \in \mathbb{Z}^8 \cup \left(\mathbb{Z} + \frac{1}{2} \right)^8 \mid x_1 + \dots + x_8 \equiv 0 \pmod{2}, x_7 + x_8 = 0, x_6 - x_7 = 0 \right\}. \end{aligned}$$

\mathbb{E}_6 est un réseau pair de dimension 6. $(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6)$ en est une base dont le diagramme de Dynkin est de type E_6 :



C'est donc un réseau de racines irréductible. On a $\det(\mathbb{E}_6) = 3$, le nombre de racines (kissing number) est $\tau_{\mathbb{E}_6} = 72$, et le nombre de Coxeter est $h = 12$.

Soit L un réseau de racines. On peut donc décomposer le réseau L en somme directe orthogonale $L = L_1 \oplus \dots \oplus L_r$, où les L_i sont des réseaux de racines irréductibles (donc de type $\mathbb{A}_n, \mathbb{D}_n, \mathbb{E}_6, \mathbb{E}_7$ ou \mathbb{E}_8), et $r \in \mathbb{N}$.

Définition 1.18. On dira que le sous-réseau L' de L est une composante orthogonale du réseau L si on peut écrire $L' = L_{i_1} \oplus \dots \oplus L_{i_s}$ où $s \leq r$ et les $i_j \in \llbracket 1, r \rrbracket$.

1.1.4 Formes quadratiques discriminantes

Les techniques relatives aux formes quadratiques discriminantes ont été développées par Nikulin en 1979, dans son article *integral Symmetric bilinear forms and some of their applications* ([N79]). C'est un outil fondamental dont nous ferons grand usage par la suite.

Soit L un réseau quadratique pair, et $(\cdot|\cdot)$ la forme bilinéaire symétrique associée.

Définition 1.19. On appelle groupe discriminant du réseau L le groupe $D(L) = L^*/L$. Son cardinal est $\#D(L) = \det(L)$. Soit $l^* \in L^*$, on notera \bar{l}^* la classe de l^* dans $D(L)$.

$(\cdot|\cdot)$ induit sur le groupe discriminant $D(L)$, une forme bilinéaire symétrique

$$b_L : L^*/L \times L^*/L \rightarrow \mathbb{Q}/\mathbb{Z} ; (x + L, y + L) \mapsto (x|y) \pmod{\mathbb{Z}}.$$

De plus, comme L est pair, $\forall x \in L^*/L$, $(x + L|x + L)$ est bien défini modulo $2\mathbb{Z}$. On dispose donc de l'application

$$q_L : L^*/L \rightarrow \mathbb{Q}/2\mathbb{Z} ; (x + L) \mapsto x^2 \pmod{2\mathbb{Z}}.$$

q_L est une forme quadratique finie, c'est à dire qu'elle est définie sur le groupe abélien fini L^*/L et satisfait les relations :

$$\begin{aligned} (i) \quad & q_L(rx) = r^2 q_L(x), \quad \forall r \in \mathbb{Z}, \forall x \in L^*/L, \\ (ii) \quad & q_L(x + y) - q_L(x) - q_L(y) \equiv 2b_L(x, y) \pmod{2\mathbb{Z}}, \end{aligned}$$

avec b_L forme bilinéaire symétrique. b_L est d'ailleurs appelée *forme bilinéaire associée* à q_L .

Définition 1.20. Soit L un réseau pair. On appelle forme quadratique discriminante de L la forme quadratique finie q_L .

Lemme 1.5. Soit L un réseau entier pair. On note λ son niveau. Alors tout élément $\bar{l}^* \in D(L)$ vérifie $\bar{l}^{*2} \equiv \frac{2a}{\lambda} \pmod{2\mathbb{Z}}$ avec $0 \leq a < \lambda$.

PREUVE : Soit l^* un représentant dans L^* de \bar{l}^* . Par définition de λ , on a $\lambda l^{*2} \in 2\mathbb{Z}$, donc il existe $b \in \mathbb{Z}$ tel que $l^{*2} = \frac{2b}{\lambda}$. On peut ensuite écrire $b = a + k\lambda$, avec $0 \leq a < \lambda$ et $k \in \mathbb{Z}$, ce qui donne $l^{*2} = \frac{2b}{\lambda} = \frac{2a}{\lambda} + 2k$, d'où le résultat annoncé. \square

Quelques propriétés arithmétiques des réseaux. Dans le paragraphe suivant, nous donnons quelques définitions importantes, puis citons quelques résultats techniques dont nous aurons besoin par la suite.

Définition 1.21. Soit L un réseau entier. On appelle diviseur de $l \in L$ l'entier positif $\text{div}(l)$ qui engendre l'idéal $(l|L) \subset \mathbb{Z}$.

Définition 1.22. Soit L un réseau. Soit $l \in L$, on dit que l est primitif s'il n'existe pas d'entier $k \in \mathbb{N}$, $k \geq 2$, et de vecteur $l' \in L$, tels que $l = kl'$.

Proposition 1.4. Soit L un réseau entier. Soit $l \in L$ un vecteur primitif. On a les propriétés suivantes :

- (i) $(l|L) = d\mathbb{Z} \Leftrightarrow \frac{1}{d}l$ est primitif dans L^* ,
- (ii) $\text{ord}_{L^*/L} \left(\frac{l}{\text{div}(l)} \right) = \text{div}(l)$,
- (iii) $\text{div}(l) | \det(L)$,
- (iv) si L est unimodulaire, $\text{div}(l) = 1$,
- (v) $\exists l_* \in L^*$, $(l|l_*) = 1$,
- (vi) si $l^2 = 0$, alors $l^\perp / \mathbb{Z}l = L \cap l^\perp \cap l_*^\perp$.

PREUVE : Les points (i) à (v) sont de simples vérifications. Pour (vi), on a $\mathbb{Z}l \subset l^\perp$, et on considère la projection

$$l^\perp \rightarrow L \cap l^\perp \cap l_*^\perp ; v \mapsto v - (v|l_*)l.$$

L'image d'un vecteur $v \in l^\perp$ est bien dans $L \cap l^\perp \cap l_*^\perp$ (vérification immédiate), elle est surjective par construction, et son noyau est $\mathbb{Z}l$. \square

Lemme 1.6. Soit L un réseau entier, et L^* son réseau dual. Soit $l^* \in L^*$ un vecteur primitif (dans L^*). Alors il existe un élément $l_1 \in L$ tel que $(l^*|l_1) = 1$.

PREUVE : L'idéal de \mathbb{Z} $(l^*|L)$ est engendré par un élément $a \in \mathbb{N}^*$, donc $(l^*|L) = a\mathbb{Z}$. Ainsi $(\frac{l^*}{a}|L) = \mathbb{Z}$, et donc $\frac{l^*}{a}$ est un élément de L^* . Si $a \neq 1$, ceci contredit la primitivité de l^* dans L^* . Donc, $(l^*|L) = \mathbb{Z}$, et il existe $l_1 \in L$, $(l^*|l_1) = 1$. \square

Lemme 1.7. Soit L un réseau entier, et L^* son réseau dual. Soit $l^* \in L^*$ un vecteur primitif. Soit $k \in \mathbb{N}^*$ l'ordre de $\overline{l^*}$ la classe de l^* dans $D(L) = L^*/L$. Alors $l = kl^*$ est primitif (dans L), et $\text{div}(l) = k$.

PREUVE : Soient l^* un élément primitif de L^* , tel que $\overline{l^*}$ est d'ordre k dans $D(L)$, et le vecteur $l = kl^* \in L$. Si l n'est pas primitif dans L , alors il existe $k' \in \mathbb{Z}$, et $l' \in L$, tels que $kl^* = k'l'$ et $k' > 1$. En particulier, $\frac{k}{k'}l^* = l' \in L$. Montrons que nécessairement $\frac{k}{k'} \in \mathbb{Z}$. D'après le lemme 1.6, il existe $l_1 \in L$, tel que $(l^*|l_1) = 1$, donc $\frac{k}{k'} = (l'|l_1) \in \mathbb{Z}$, puisque

le réseau L est entier. On pose $b = \frac{k}{k'}$. On a donc la relation $bl^* = l' \in L$. Comme l'ordre de \bar{l}^* dans $D(L)$ est k , $k|b$, et il existe $a \in \mathbb{Z}$ tel que $ak = b$, puis comme $b = \frac{k}{k'}$, on a $akk' = k$, ce qui impose $a = k' = 1$. C'est absurde car $k' > 1$. On a donc prouvé que kl^* est bien primitif.

L'affirmation $\text{div}(l) = k$ est alors une conséquence immédiate de la deuxième assertion de la proposition 1.4. \square

Lemme 1.8. *Soit L un réseau pair défini négatif. Alors chaque classe \bar{l}^* dans $D(U \oplus L) = (U \oplus L^*)/(U \oplus L)$ admet un représentant l^* qui est un vecteur primitif, et tel que $-2 \leq l^{*2} < 0$.*

PREUVE : Soit $\bar{l}^* \in D(U \oplus L)$, et $l^* \in U \oplus L^*$ un représentant de cette classe. On peut écrire $l^* = u + l_1$, avec $u \in U$, $l_1 \in L^*$. Alors, $\bar{l}_1 = \bar{l}^*$. Notons $l_1^2 = a + 2c$, avec $a \in \mathbb{Q}$, $-2 \leq a < 0$ et $c \in \mathbb{Z}$. On pose $u_1 = e - cf$, où (e, f) est un couple hyperbolique. Alors $u_1 \in U$ et u_1 est primitif, parce que e l'est, et $u_1^2 = -2c$. Donc, $(u_1 + l_1)^2 = a$. On a prouvé que $u_1 + l_1$ est un représentant primitif de \bar{l}^* tel que $-2 \leq (u_1 + l_1)^2 < 0$. \square

Lemme 1.9. *Soit L un réseau pair défini négatif, de niveau λ . Soit $l^* \in U \oplus L^*$ tel que $-2 \leq l^{*2} < 0$. On peut écrire $l^{*2} = -\frac{2a}{\lambda}$ (voir le lemme 1.5).*

- Si l^* n'est pas primitif, alors il existe $l' \in U \oplus L^*$ (primitif) et $k \in \mathbb{N}^*$, $k > 1$ tels que $l^* = kl'$. Si on pose $l'^2 = -\frac{2b}{\lambda} \pmod{2}$, $-\lambda \leq b < 0$, alors on a $k^2|a$ et $\lambda|(b - \frac{a}{k^2})$.
- Inversement, s'il existe $k \in \mathbb{N}^*$, $k > 1$, tel que $k^2|a$, et une classe \bar{l}' , avec $\bar{l}'^2 = -\frac{2b}{\lambda} \pmod{2}$, $-\lambda \leq b < 0$, telle que $\overline{kl}' = \bar{l}^*$ et $\lambda|(b - \frac{a}{k^2})$, la classe \bar{l}^* admet un représentant non-primitif dans $U \oplus L^*$.

PREUVE : • Soient $l' \in U \oplus L^*$, primitif, et $k \in \mathbb{N}^*$, $k > 1$ tels que $l^* = kl'$, et $l'^2 = -\frac{2b}{\lambda} \pmod{2}$, $-\lambda \leq b < 0$. Il existe $c \in \mathbb{Z}$ tel que

$$l^{*2} = -\frac{2a}{\lambda} = -\frac{2k^2b}{\lambda} + 2k^2c,$$

c'est à dire

$$-a = -k^2b + k^2c\lambda.$$

Ainsi, $k^2|a$ et on a, posant $a = k^2d$ avec $d \in \mathbb{Z}$,

$$k^2b - a = k^2c\lambda \Leftrightarrow b - d = c\lambda.$$

Donc $\lambda|(b - \frac{a}{k^2})$.

- On suppose qu'il existe $k \in \mathbb{N}^*$, $k > 1$, tel que $k^2|a$, et une classe \bar{l}' , avec $\bar{l}'^2 = -\frac{2b}{\lambda} \pmod{2}$, $-\lambda \leq b < 0$, tels que $\overline{kl}' = \bar{l}^*$ et $\lambda|(b - \frac{a}{k^2})$. Soit $d \in \mathbb{Z}$ tel que $a = k^2d$, soit $c \in \mathbb{Z}$ tel que $\lambda c = (b - d)$, soit l' un représentant de la classe \bar{l}' dans L^* (toujours possible car $D(L) = D(U \oplus L)$), et soit $\alpha \in \mathbb{Z}$ tel que $l'^2 = -\frac{2b}{\lambda} + 2\alpha$. On pose $u = e + (c - \alpha)f \in U$, où (e, f) est un couple hyperbolique de U . Alors le vecteur $l'' = u + l' \in U \oplus L^*$ est primitif (car $u \perp l'$ et u est primitif), est un représentant de la classe \bar{l}' dans $U \oplus L^*$, on a $\overline{kl}'' = \bar{l}^*$ et

$$(kl'')^2 = 2k^2(c - \alpha) - \frac{2k^2b}{\lambda} + 2k^2\alpha = -\frac{2k^2(\lambda c - b)}{\lambda} = -\frac{2k^2d}{\lambda} = -\frac{2a}{\lambda}.$$

Ainsi, on a montré que le vecteur non-primitif kl'' est un représentant de la classe \bar{l}^* dans $U \oplus L^*$. \square

Tables pour les réseaux de racines. Dans cette partie nous donnons, pour chaque famille de réseaux de racines irréductibles, un système de représentants du groupe discriminant. Adaptant légèrement les notations de [CS98], nous noterons ε_i un représentant primitif dans L^* de la classe $\bar{\varepsilon}_i = [i]$, et de norme minimale. Nous garderons donc toujours en tête, lorsque l'on parlera de forme quadratique discriminante, les valeurs prises par ε_i (on notera la forme quadratique Q_L), et les valeurs prises par $[i]$ (on notera la forme quadratique q_L). Par abus de langage (mais pas de notations), il nous arrivera d'appeller forme quadratique discriminante la forme Q_L .

Réseaux \mathbb{A}_n : On a $\mathbb{A}_n^*/\mathbb{A}_n = \{\bar{\varepsilon}_i = [i] \mid 0 \leq i \leq n\}$ où $\varepsilon_i = (\frac{i}{n+1}, \dots, \frac{i}{n+1}, \frac{-j}{n+1}, \dots, \frac{-j}{n+1})$ avec j composantes égales à $\frac{i}{n+1}$ et $i + j = n + 1$. Ce groupe est isomorphe à $\mathbb{Z}/(n+1)\mathbb{Z}$, un générateur est $[1]$. On dispose alors de la forme quadratique discriminante suivante :

$$Q_{\mathbb{A}_n} : \varepsilon_i \mapsto \frac{ij}{n+1}. \quad q_{\mathbb{A}_n} : [i] \mapsto \frac{ij}{n+1} \pmod{2\mathbb{Z}}.$$

En particulier, le niveau de \mathbb{A}_n est $n + 1$ si n est pair, $2(n + 1)$ si n est impair.

Réseaux \mathbb{D}_n : On a $\mathbb{D}_n^*/\mathbb{D}_n = \{\bar{0} = [0], \bar{\varepsilon}_1 = [1], \bar{\varepsilon}_2 = [2], \bar{\varepsilon}_3 = [3]\}$, où $\varepsilon_1 = \frac{e_1 + \dots + e_n}{2}$, $\varepsilon_2 = e_2$, $\varepsilon_3 = \frac{e_1 + \dots + e_{n-1} - e_n}{2}$. Ce groupe est isomorphe au groupe de Klein $V_4 = (\mathbb{Z}/2\mathbb{Z})^2$ si n est pair, et à $\mathbb{Z}/4\mathbb{Z}$ si n est impair. Si n est pair, un ensemble générateur est $[1], [3]$ et si n est impair, $[1]$ est générateur de $\mathbb{D}_n^*/\mathbb{D}_n$. On dispose alors de la forme quadratique discriminante suivante :

$$\begin{array}{ll} Q_{\mathbb{D}_n} : 0 \mapsto 0, & q_{\mathbb{D}_n} : [0] \mapsto 0 \pmod{2\mathbb{Z}}, \\ \varepsilon_1 \mapsto \frac{n}{4}, & [1] \mapsto \frac{n}{4} \pmod{2\mathbb{Z}}, \\ \varepsilon_2 \mapsto 1, & [2] \mapsto 1 \pmod{2\mathbb{Z}}, \\ \varepsilon_3 \mapsto \frac{n}{4}. & [3] \mapsto \frac{n}{4} \pmod{2\mathbb{Z}}. \end{array}$$

En particulier, le niveau de \mathbb{D}_n est 2 si $n \equiv 0 \pmod{4}$, 4 si $n \equiv 2 \pmod{4}$, et 8 si n est impair.

Réseau \mathbb{E}_8 : \mathbb{E}_8 étant unimodulaire, le groupe discriminant est trivial, ainsi que sa forme quadratique associée. Le niveau est 1.

Réseau \mathbb{E}_7 : On a $\mathbb{E}_7^*/\mathbb{E}_7 = \{\bar{0} = [0], \bar{\varepsilon}_1 = [1]\}$, où $\varepsilon_1 = (\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, 0, 0)$. Ce groupe est isomorphe à $\mathbb{Z}/2\mathbb{Z}$, un générateur est $[1]$. On dispose alors de la forme quadratique discriminante suivante :

$$Q_{\mathbb{E}_7} : \varepsilon_1 \mapsto \frac{3}{2}. \quad q_{\mathbb{E}_7} : [1] \mapsto \frac{3}{2} \pmod{2\mathbb{Z}}.$$

Le niveau de \mathbb{E}_7 est 4.

Réseau \mathbb{E}_6 : On a $\mathbb{E}_6^*/\mathbb{E}_6 = \{\bar{0} = [0], \bar{\varepsilon}_1 = [1], \bar{\varepsilon}_2 = [2]\}$, où $\varepsilon_1 = (0, 0, 0, 0, 0, \frac{2}{3}, \frac{2}{3}, -\frac{2}{3}) = -\varepsilon_2$. Ce groupe est isomorphe à $\mathbb{Z}/3\mathbb{Z}$, un générateur est $[1]$. On dispose alors de la forme quadratique discriminante suivante :

$$Q_{\mathbb{E}_6} : \varepsilon_i \mapsto \frac{4}{3}. \quad q_{\mathbb{E}_6} : [i] \mapsto \frac{4}{3} \pmod{2\mathbb{Z}}.$$

Le niveau de \mathbb{E}_6 est 3.

1.1.5 Sur-réseaux

Définition 1.23. Soit L un réseau quadratique pair, et $(\cdot|\cdot)$ sa forme bilinéaire symétrique associée. On appelle sur-réseau pair de L tout réseau quadratique $M \subset L \otimes \mathbb{Q}$, pair (pour $(\cdot|\cdot)$), tel que $L \subset M$.

Soit L un réseau quadratique pair. On dira que L est *maximal* s'il n'existe pas de sur-réseau pair M de L . Si M est un sur-réseau pair de L , on a la suite d'inclusions

$$L \subset M \subset M^* \subset L^*,$$

ce qui donne en particulier que $|\det(L)| = |M/L|^2 |\det(M)|$. Donc, si $\det(L)$ est sans facteur carré, alors L est maximal.

Si l'on note $H_M = M/L$ le quotient de M par L , où M est un sur-réseau pair de L , alors H_M est un sous-groupe de L^*/L le groupe discriminant de L . De plus, les éléments de H_M sont isotropes pour la forme quadratique discriminante de L^*/L (puisque M est un réseau pair), le groupe H_M est donc un sous-groupe totalement isotrope de L^*/L . On dira que H_M est le *code associé au sur-réseau M de L* .

Les propositions suivantes sont dues à Nikulin ([N79] prop. 1.4.1 et 1.4.2 p.110, ou encore [Eb02] prop. 3.5 et 3.6 p.103) :

Proposition 1.5. La correspondance $M \mapsto H_M$ est une correspondance bijective entre les sur-réseaux pairs de L et les sous-groupes totalement isotropes de L^*/L . Les réseaux unimodulaires correspondant aux sous-groupes H totalement isotropes avec $|H|^2 = |\det(L)|$.

Proposition 1.6. Deux sur-réseaux pairs M et M' de L sont isomorphes si et seulement si les sous-groupes totalement isotropes H_M et $H_{M'}$ sont conjugués sous l'action d'un automorphisme de L .

Corollaire 1.2. ([Eb02] cor. 3.6 p.104)

Soit L un réseau de racines. Il y a une correspondance bijective naturelle entre les classes d'isomorphismes des sur-réseaux pairs M de L tel que $R_M = \{x \in M \mid x^2 = 2\} = R_L$ et les orbites (pour le groupe induit par les automorphismes de L) des sous-groupes totalement isotropes $H \subset L^*/L$ tels que $\forall \xi \in H, l_L(\xi) \neq 2$, où $l_L(\xi) = \min\{x^2 \mid x \in L, \bar{x} = \xi\}$. Les réseaux unimodulaires correspondant aux sous-groupes H avec $|H|^2 = |\det(L)|$.

1.2 Codes

1.2.1 Généralités sur les codes

Qu'est-ce qu'un code ? Lorsqu'une personne A veut envoyer un message m à une autre personne B via un certain moyen de transmission (téléphone, satellite ou autre), le message doit d'une part être codé (choix d'un "alphabet") pour être transportable, et d'autre part, il peut être altéré (il y a des erreurs dues au "bruit" de la transmission). Se posent donc les questions du choix de l'alphabet, de la taille des données à transmettre, et enfin, des moyens dont on peut disposer pour corriger un message (éventuellement détérioré).

Définition 1.24. Soient $n \in \mathbb{N}^*$ et A un ensemble fini. C est un code de longueur n et d'alphabet A si C est un sous-ensemble non vide de A^n . Les éléments $c \in C$ sont appelés mots de C , et les composantes de c dans A^n sont appelées les lettres de c .

Lorsque $A = \mathbb{F}_2$, on dira que C est un code *binnaire*, si $A = \mathbb{F}_3$, on parlera de code *ternaire*. Si $|C| = 1$, le code sera dit *trivial*.

Le schéma général de transmission de l'information est le suivant : soit m un message, on l'encode en un élément $f(m) \in C$. Ensuite, on transmet $f(m)$ via un canal de communication, et on retrouve un élément $b \in A^n$ (qui a pu subir des perturbations) à la sortie du canal. Il faut donc "décoder" b pour obtenir un élément $g(b)$ qui doit être égal au message initial m . Le choix de f (et donc de g) est un choix important, il doit satisfaire (au moins) deux contraintes, à savoir minimiser la taille de l'information à transmettre (contraintes techniques de réalisation de la communication), et corriger le plus d'erreurs possible (permettre de restituer efficacement le message initial malgré les altérations du message lors de la transmission).

Afin de détecter le plus d'erreurs possible, l'idée naturelle consiste à choisir un code C (c'est-à-dire choisir f) de sorte que chaque mot soit le "plus différent possible" des autres. Ainsi, on peut assimiler un élément de A^n au mot qui en est "le plus proche" (ce sera la fonction g qui fera ce travail).

Voici un exemple très simple. On considère le code binnaire (alphabet $\mathbb{F}_2 = \{0, 1\}$) à répétition de longueur 3, $C = \{(0, 0, 0), (1, 1, 1)\} \subset \mathbb{F}_2^3$ (par exemple $(0, 0, 0)$ correspond à $m =$ "non" et $(1, 1, 1)$ correspond à $m =$ "oui"). Si le récepteur du message reçoit $b = (0, 1, 0)$, il est raisonnable de supposer que le message initial était $(0, 0, 0)$, c'est-à-dire $m =$ "non". On voit tout de suite que ce code peut corriger une erreur (au plus une seule coordonnée peut avoir été modifiée afin de restituer le message). Sur cet exemple nous voyons que la bonne considération est la notion de distance entre deux mots. D'où la

Définition 1.25. Soit $x \in A^n$, le poids de x est défini comme étant le nombre de lettres non-nulles de x . Soient $x, y \in A^n$, la distance de Hamming entre x et y , $d(x, y)$ est le nombre de lettres qui diffèrent entre x et y , en respectant l'ordre d'apparition (c'est-à-dire que si $x = (x_1, \dots, x_n)$ et $y = (y_1, \dots, y_n)$, $d(x, y) = \#\{i \in \llbracket 1, n \rrbracket \mid x_i \neq y_i\}$). La distance minimale d'un code C (non trivial) est $d_C = \min\{d(x, y) \mid x, y \in C, x \neq y\}$. Ainsi, un

$[n, M, d]$ -code sera un code de longueur n , avec M mots, et de distance minimale d .

Il est alors facile de voir qu'un code de distance minimale d corrige $t = \frac{d-1}{2}$ erreurs si d est impair, et $t = \frac{d-2}{2}$ erreurs si d est pair. Comme on l'a vu précédemment, on recherche des codes dont la distance minimale est la plus grande possible. Revenons à notre exemple simple du code à répétition. Sa distance minimale est 3, il corrige 1 erreur. Mais, il coûte trop d'information, il nécessite le codage sur 3 bits d'une information qui ne représente qu'un seul bit (0 ou 1). La problématique principale est donc de construire des codes avec d le plus grand possible, et n le plus petit possible (choses à priori antagonistes).

Enfin, un code ne dépend pas du choix des coordonnées, le groupe symétrique \mathcal{S}_n agit sur A^n en permutant les coordonnées. D'où la

Définition 1.26. Deux codes C et C' sont dits équivalents s'il existe $\sigma \in \mathcal{S}_n$, $\sigma(C) = C'$.

Codes linéaires. Parmi les différents choix de code, il existe un choix particulièrement intéressant, celui des codes linéaires. En effet, si l'on impose à A d'être un corps (fini!), et à C d'être un sous-espace vectoriel de A^n , alors la théorie de l'algèbre linéaire va nous donner un nombre important d'outils pour manipuler notre code, et contrôler ses propriétés.

Définition 1.27. Soient $n \in \mathbb{N}^*$, $1 \leq k \leq n$, et A un corps fini ($A = \mathbb{F}_q$), on appelle code linéaire de dimension k et de longueur n un sous-espace vectoriel C de A^n de dimension k .

La distance minimale d'un code linéaire est le poids minimum d'un mot non nul de C (vérification aisée). Si d est la distance minimale de C , on dira qu'il s'agit d'un $[n, k, d]$ -code. Si l'on écrit les vecteurs de \mathbb{F}_q^n en colonne, alors un code linéaire est entièrement déterminé par la suite exacte

$$0 \rightarrow \mathbb{F}_q^k \xrightarrow{A} \mathbb{F}_q^n \xrightarrow{B} \mathbb{F}_q^{n-k} \rightarrow 0,$$

où A et B sont des matrices. L'exactitude de la suite est équivalente aux trois conditions : $\text{rg}(A) = k$, $BA = 0$, $\text{rg}(B) = n - k$. Ainsi, on peut définir un code linéaire de deux façons. Soit en indiquant la matrice $A \in \mathcal{M}_{n,k}(\mathbb{F}_q)$, ses colonnes forment alors une base de C (usuellement on donne plutôt tA , dont les lignes forment une base de C , tA est alors appelée *matrice génératrice de C*). Soit en indiquant la matrice $B \in \mathcal{M}_{n-k,n}(\mathbb{F}_q)$ (appelée *matrice de contrôle de C*), dans ce cas $C = \ker B$, ce qui donne une description moins "visible" de C , mais en même temps un critère efficace de test d'appartenance à C . Dans ce dernier cas, les lignes de B sont les relations qui définissent C , et Bx est appelé *syndrome* de x (les mots de C sont les mots de syndrome nul).

Définition 1.28. Soit C un code linéaire sur \mathbb{F}_q , de longueur n . On appelle code dual de C l'ensemble

$$C^\perp = \{y \in \mathbb{F}_q^n \mid x \cdot y = 0, \forall x \in C\},$$

où $x \cdot y = \sum_{i=1}^n x_i y_i$, pour $x = (x_i)_{1 \leq i \leq n}$, $y = (y_i)_{1 \leq i \leq n}$.

On vérifie aisément que C^\perp est un code linéaire de dimension $n - k$ et longueur n , où k est la dimension de C et n la longueur de C . De plus, C^\perp est défini par la suite exacte

$$0 \rightarrow \mathbb{F}_q^{n-k} \xrightarrow{tB} \mathbb{F}_q^n \xrightarrow{tA} \mathbb{F}_q^k \rightarrow 0.$$

Définition 1.29. *On dit qu'un code linéaire C est auto-dual si $C = C^\perp$. Un code binaire est dit doublement pair si les poids $w(x)$ de tous les mots (non nuls) $x \in C$ sont divisibles par 4.*

1.2.2 Liens entres codes et réseaux

On peut construire des réseaux à partir de codes binaires. Par exemple, considérons le réseau "standard" $\mathbb{Z}^n \subset \mathbb{R}^n$ (on munit \mathbb{R}^n du produit scalaire euclidien usuel), et la réduction modulo 2 :

$$\rho_2 : \mathbb{Z}^n \rightarrow (\mathbb{Z}/2\mathbb{Z})^n = \mathbb{F}_2^n.$$

C'est un homomorphisme de groupes. Soit maintenant C un $[n, k, d]$ -code. C est un sous-groupe d'indice 2^{n-k} de \mathbb{F}_2^n . Alors, $\rho_2^{-1}(C)$, la préimage de C dans \mathbb{Z}^n , est un sous-groupe d'indice 2^{n-k} dans \mathbb{Z}^n , en particulier, c'est un sous-groupe libre de rang n , c'est bien un réseau de \mathbb{R}^n . On a de plus $\text{Vol}(\mathbb{R}^n/\rho_2^{-1}(C)) = 2^{n-k}$.

Définition 1.30. *On pose $L_C = \frac{1}{\sqrt{2}}\rho_2^{-1}(C)$. C'est le réseau associé au code C .*

On a les résultats suivants.

Lemme 1.10. *([Eb02], prop. 1.3 p.13)*

Soit C un code binaire. Alors

- (i) $C \subset C^\perp$ si et seulement si L_C est un réseau entier,*
- (ii) C est doublement pair si et seulement si L_C est un réseau pair,*
- (iii) C est auto-dual si et seulement si L_C est unimodulaire.*

Lemme 1.11. *([Eb02], lem. 1.11 p.28)*

Soit C un code binaire. Alors

$$L_C^* = L_{C^\perp}.$$

1.2.3 Exemples de codes linéaires

Les codes suivants sont présentés dans [Eb02] et [CS98].

Codes de Hamming. Il existe de nombreuses façons de présenter le *code de Hamming* H_7 . Nous allons ici nous contenter de donner une matrice génératrice et une matrice de contrôle.

On a

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

est une matrice génératrice de H_7 . Une matrice de contrôle est

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Il s'agit d'un $[7, 4, 3]$ -code linéaire. Le groupe des automorphismes de H_7 est $PSL_2(\mathbb{F}_7) \cong GL_3(\mathbb{F}_2)$ (groupe simple d'ordre 168).

Le code de Hamming n'est pas auto-dual, nous allons donc considérer le code dit *code étendu*. Ce procédé consiste, pour un code binaire donné, à ajouter à chaque mot une dernière lettre, appelée *bit de parité*, qui vaut 0 si le poids du mot est pair, et 1 sinon. Ceci permet de transformer un code quelconque en un code pair.

Considérons donc le *code de Hamming étendu* $H_8 = \tilde{H}_7$, il est donné par la matrice génératrice

$$\tilde{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

et la matrice de contrôle est

$$\tilde{H} = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Il s'agit d'un $[8, 4, 4]$ -code linéaire auto-dual, doublement pair. Il a 1 mot de poids 0, 1 mot de poids 8, et 14 mots de poids 4. Le groupe des automorphismes de \tilde{H}_7 est le groupe affine d'ordre 1344, $8 \cdot GL_3(\mathbb{F}_2)$ agissant sur \mathbb{F}_2^3 (c'est à dire qu'il s'agit du groupe des applications affines de l'espace affine \mathbb{F}_2^3 , une application affine f étant définie par sa partie linéaire $\tilde{f} \in GL_3(\mathbb{F}_2)$ et une translation \vec{t} qui est l'un des 8 vecteurs de \mathbb{F}_2^3 . De façon générale, soit G un groupe linéaire agissant sur un espace vectoriel E et T un ensemble de k vecteurs de E formant un sous-groupe additif de E , on notera $k \cdot G$ le groupe affine composé des applications dont la partie linéaire est un élément de G et la translation l'un des vecteurs de T).

Le réseau $L_{\tilde{H}_7}$ associé est un réseau unimodulaire pair de dimension 8, c'est donc nécessairement \mathbb{E}_8 .

Codes d_n . Soit $n \in \mathbb{N}^*$. On considère l'ensemble

$$d_n = \{(u_1, \dots, u_n) \in \mathbb{F}_2^n \mid u_1 + \dots + u_n = 0\}.$$

C'est un sous-espace vectoriel de dimension $n - 1$ de \mathbb{F}_2^n . Il s'agit d'un $[n, n - 1, 2]$ -code linéaire.

On peut construire \mathbb{D}_n , $n \geq 3$, à partir de ce code. En effet, considérons la projection

$$\rho_2 : \mathbb{Z}^n \rightarrow (\mathbb{Z}/2\mathbb{Z})^n = \mathbb{F}_2^n.$$

C'est un homomorphisme de groupes. d_n est un sous-groupe d'indice 2 de \mathbb{F}_2^n . Alors, $\rho_2^{-1}(d_n)$ est un réseau de \mathbb{R}^n (d'indice 2), qui est \mathbb{D}_n si $n \geq 3$ (vérification aisée).

Lorsque n est pair, on peut aussi retrouver le réseau \mathbb{D}_n , mais cette fois en tant que réseau associé à un code (ce n'était pas le cas juste avant). On considère le code double de $d_{\frac{n}{2}}$, que l'on notera $d_{\frac{n}{2}}^2$, défini par

$$d_{\frac{n}{2}}^2 = \{(v_1, \dots, v_n) \in \mathbb{F}_2^n \mid v_1 = v_2 = u_1, \dots, v_{n-1} = v_n = u_{\frac{n}{2}}, (u_1, \dots, u_{\frac{n}{2}}) \in d_{\frac{n}{2}}\}.$$

Alors $D_n = L_{d_{\frac{n}{2}}^2}$ (voir partie 1.2.2), le code étant doublement pair on retrouve le fait que \mathbb{D}_n est pair.

Hexacode. On va construire un $[6, 3, 4]$ -code linéaire sur \mathbb{F}_4 , noté \mathcal{C}_6 , et appelé *hexacode*. On écrit $\mathbb{F}_4 = \{0, 1, \omega, \bar{\omega}\}$, où $\omega^2 = 1 + \omega = \bar{\omega}$. Les mots de ce code sont de la forme $(a, b, c, f(1), f(\omega), f(\bar{\omega}))$, où $f(x) = ax^2 + bx + c$. Une matrice génératrice de \mathcal{C}_6 est

$$\begin{pmatrix} 1 & 0 & 0 & 1 & \bar{\omega} & \omega \\ 0 & 1 & 0 & 1 & \omega & \bar{\omega} \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

On peut vérifier qu'alors la distance minimale de \mathcal{C}_6 est 4. Si l'on munit maintenant \mathbb{F}_4^6 du produit scalaire $x \cdot y = \sum_{i=1}^6 x_i \bar{y}_i$ où $x \mapsto \bar{x}$ est l'application \mathbb{F}_2 -linéaire définie par $1 \mapsto 1$ et $\omega \mapsto \bar{\omega}$, alors \mathcal{C}_6 est un code auto-dual.

Il a 1 mot de poids 0, 45 mots de poids 4, et 18 mots de poids 6. Le groupe des automorphismes de \mathcal{C}_6 est le groupe affine $3 \cdot \mathcal{A}_6$ (ici \mathcal{A}_6 agit de façon linéaire sur les composante de \mathbb{F}_4^6 et T est le groupes d'ordre 3 composé des translations $(1, 1, 1, 1, 1, 1)$, $(\omega, \omega, \omega, \omega, \omega, \omega)$ et $(\bar{\omega}, \bar{\omega}, \bar{\omega}, \bar{\omega}, \bar{\omega}, \bar{\omega})$).

On pourra se référer à [CS98], p.300, pour se familiariser avec la manipulation de ce code.

1.2.4 Codes de Golay

Les codes de Golay sont des objets remarquables. Nous allons ici nous contenter de présenter les codes de Golay binaire étendu, et ternaire étendu, les seuls dont nous aurons besoin. Nous énoncerons en particulier quelques-unes de leurs propriétés.

Code de Golay binaire étendu Nous suivons dans un premier temps la construction de [Eb02], p.68, parce qu'elle s'appuie sur l'hexacode. On trouvera d'autres constructions dans [CS98]. On pourra aussi étudier le chapitre 11 de [CS98], qui donne à partir de la p.303 des méthodes efficaces pour manipuler des mots de \mathcal{C}_{24} .

Pour construire le code binaire de dimension 24, \mathcal{C}_{24} , représentons les mots de \mathbb{F}_2^{24} par des matrices de taille 4×6 , à coefficients dans \mathbb{F}_2 . Ces matrices doivent satisfaire les 2 règles suivantes :

(A) Les 6 sommes des éléments des colonnes et la somme des éléments de la première ligne doivent avoir la même parité.

(B) Si r_i désigne la $i^{\text{ième}}$ ligne ($1 \leq i \leq 4$), alors $r_2 + \omega r_3 + \bar{\omega} r_4 \in \mathbb{F}_4^6$ est un mot de l'hexacode (voir la partie 1.2.3).

Dans la pratique, pour construire un mot de \mathcal{C}_{24} , on suit les instructions suivantes :

(i) Choisir un mot de l'hexacode.

(ii) Choisir la parité de la première ligne.

(iii) Choisir les 5 premières colonnes de façon à ce que la somme (B) donne les coordonnées correspondantes de l'hexacode choisi en (i). On donne les tables des correspondances entre des colonnes de \mathbb{F}_2^4 et les éléments de \mathbb{F}_4 obtenus en sommant comme en (B) en figure 1.1.

(iv) Il ne reste alors plus qu'une seule possibilité pour le choix de la colonne 6.

$$\begin{array}{cccccccc}
 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
 \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} & \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} & \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} & \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} & \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} & \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} & \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} & \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} \\
 \omega & \omega & \omega & \omega & \bar{\omega} & \bar{\omega} & \bar{\omega} & \bar{\omega} \\
 \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} & \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} & \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} & \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} & \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} & \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} & \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} & \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}
 \end{array}$$

FIG. 1.1 – Correspondance entre les colonnes de \mathbb{F}_2^4 et les éléments de \mathbb{F}_4 obtenus par sommation (B).

On peut montrer que \mathcal{C}_{24} est un $[24, 12, 8]$ -code binaire, qui est auto-dual et doublement pair. C'est le code étendu d'un autre code (dit *code de Golay binaire*). Il y a 1 mot de poids 0, 759 mots de poids 8, 2576 mots de poids 12, 759 mots de poids 16 et 1 mot de poids 24.

Suivant la partie 1.2.2 et le corollaire 1.2, le réseau associé à \mathcal{C}_{24} est un réseau unimodulaire pair de dimension 24 dont le sous-réseau de racines est $24A_1$.

Donnons aussi une matrice génératrice de \mathcal{C}_{24} :

$$G = \left(\begin{array}{cccccccccccc|cccccccc|c} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{array} \right).$$

Cette matrice sera utilisée pour les calculs faits en annexe 2.

Le groupe des automorphismes de \mathcal{C}_{24} est le groupe de Mathieu M_{24} (voir [CS98] chapitre 10 pour plus de précisions). Ce groupe est 5-transitif sur les coordonnées des éléments de \mathbb{F}_2^{24} .

Nous allons maintenant donner quelques définitions et propriétés du code de Golay binaire étendu \mathcal{C}_{24} (nous suivons les appellations de [CS98]).

Définition 1.31. *On appelle :*

- octades spéciales les ensembles de 8 entiers $\{i_1, \dots, i_8\} \subset \llbracket 1, 24 \rrbracket$ tels qu'il existe un mot $x = (x_1, \dots, x_{24})$ de \mathcal{C}_{24} dont les lettres non-nulles sont exactement x_{i_1}, \dots, x_{i_8} . Par abus de langage on désignera parfois par octade spéciale un mot de \mathcal{C}_{24} de poids 8.
- dodécades ombrales les ensembles de 12 entiers $\{i_1, \dots, i_{12}\} \subset \llbracket 1, 24 \rrbracket$ tels qu'il existe un mot $x = (x_1, \dots, x_{24})$ de \mathcal{C}_{24} dont les lettres non-nulles sont exactement $x_{i_1}, \dots, x_{i_{12}}$. Par abus de langage on désignera parfois par dodécade ombrale un mot de \mathcal{C}_{24} de poids 12.

Définition 1.32. *On appelle :*

- tétrades les ensembles de 4 entiers $\{i_1, \dots, i_4\} \subset \llbracket 1, 24 \rrbracket$.
- octades les ensembles de 8 entiers $\{i_1, \dots, i_8\} \subset \llbracket 1, 24 \rrbracket$.
- dodécades les ensembles de 12 entiers $\{i_1, \dots, i_{12}\} \subset \llbracket 1, 24 \rrbracket$.
- n -ades les sous-ensembles de n entiers de $\llbracket 1, 24 \rrbracket$.

Une paire complémentaire de dodécades ombrales est appelée un *duo*. Un triplet d'octades spéciales disjointes est appelé un *trio*. Un système de 6 tétrades disjointes telles que l'union de tout couple de telles tétrades est une octade spéciale est appelé un *sextet*.

Définition 1.33. *Soit S un ensemble à v éléments, et \mathcal{B} un ensemble de sous-ensembles à k éléments de S (appelés blocs), avec la propriété que tout sous-ensemble à t éléments de S ($t \leq k$) est contenu dans exactement un bloc. Le couple (S, \mathcal{B}) est appelé système de*

Steiner $S(t, k, v)$.

Proposition 1.7. *Les octades spéciales de \mathcal{C}_{24} forment un système de Steiner $S(5, 8, 24)$.*

PREUVE : Il y a exactement 759 octades spéciales dans \mathcal{C}_{24} , donc, suivant les notations de la définition précédente, on pose $S = \llbracket 1, 24 \rrbracket$, et \mathcal{B} est l'ensemble des 759 octades spéciales (qui sont des sous-ensembles de cardinal 8 de S). Comme \mathcal{C} est doublement pair, chaque 5-ades est contenue dans au plus l'une de ces octades spéciales (en effet, sinon on additionne ces deux octades spéciales, on trouve un mot de poids au plus 6 - puisque 5 composantes au moins sont communes, comme la distance minimale est 8, c'est impossible).

D'autre part, il y a

$$\binom{24}{5} = 759 \cdot \binom{8}{5}$$

5-ades. Ainsi, chaque 5-ades est contenu dans exactement une des octades spéciales, ce qui signifie que les octades spéciales de \mathcal{C}_{24} forment un système de Steiner $S(5, 8, 24)$. \square

Les deux théorèmes suivants, issus de [CS98], seront largement utilisés en partie 3.2.3 pour étudier les quasi-restrictions relatives au réseau $N(24A_1)$ (voir partie 1.4.2).

Théorème 1.4. ([CS98], théorème 11 p.277)

Soit $\{a_1, \dots, a_8\}$ une octade spéciale. Alors le nombre d'octades spéciales intersectant $\{a_1, \dots, a_i\}$ en $\{a_1, \dots, a_j\}$ exactement est donné par la $(j+1)$ -ième entrée dans la $(i+1)$ -ième ligne du tableau de la figure 1.2 :

759							
506	253						
330	176	77					
210	120	56	21				
130	80	40	16	5			
78	52	28	12	4	1		
46	32	20	8	4	0	1	
30	16	16	4	4	0	0	1
30	0	16	0	4	0	0	1

FIG. 1.2 – Intersections d'octades.

En particulier, pour une octade spéciale donnée, il y a 30 octades spéciales qui lui sont disjointes, aucune qui l'intersecte en 1, 3, 5, 6 ou 7 point, 1 (elle-même) qui l'intersecte en 8 points, 16 qui l'intersectent en 2 points donnés, et donc $16 \cdot \binom{8}{2} = 448$ qui l'intersectent en 2 points quelconques, et 4 qui l'intersectent en 4 points donnés, donc $4 \cdot \binom{8}{4} = 280$ qui l'intersectent en 4 points quelconques.

De même, le nombre de dodécades ombrales intersectant $\{a_1, \dots, a_i\}$ en $\{a_1, \dots, a_j\}$ exactement est donné par la $(j+1)$ -ième entrée dans la $(i+1)$ -ième ligne du tableau de la figure 1.3.

Pour terminer cette partie, nous allons décrire les orbites des différentes n -ades sous l'action du groupe de Mathieu M_{24} . Fixons d'abord quelques définitions. Un ensemble de

2576									
1288	1288								
616	6726	616							
280	336	336	280						
120	160	176	160	120					
48	72	88	88	72	48				
16	32	40	48	40	32	16			
0	16	16	24	24	16	16	0		
0	0	16	0	24	0	16	0	0	

FIG. 1.3 – Intersections dodécades/octades.

cardinal $n < 12$ est dit *spécial*, noté S_n , s'il contient, ou est contenu dans une octade spéciale (donc une octade spéciale est bien spéciale); ou est dit *ombral*, noté U_n , s'il est contenu dans une dodécade ombrale; ou est dit *transverse*, noté T_n , sinon. Une dodécade qui n'est pas ombrale est *extraspéciale*, notée S_{12}^+ , si elle contient trois octades spéciales; ou *spéciale*, notée S_{12} , si elle contient une seule dodécade spéciale; *pénombrale*, notée U_{12}^- , si elle contient tous les points, sauf un, d'une dodécade ombrale; et enfin *transverse*, notée T_{12} , dans tous les autres cas. Les ensembles de plus de 12 éléments sont décrits par les mêmes adjectifs et notations que leur complémentaire.

Théorème 1.5. ([CS98], théorème 22 p.283)

Les sous-ensembles de $\llbracket 1, 24 \rrbracket$ se distribuent en 49 orbites sous l'action du groupe de Mathieu M_{24} . On décrit ces orbites dans le graphe de la figure 1.4. Chaque noeud du graphe correspondant à une orbite, et chaque arrête indiquant le nombre de façons de passer d'une orbite à l'autre en enlevant ou ajoutant un seul point.

Code de Golay ternaire étendu On considère le code ternaire de dimension 12 donné par la matrice génératrice

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 2 & 1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 1 & 0 \end{pmatrix}.$$

C'est un $[12, 6, 6]$ -code, autodual, que l'on appelle *code de Golay ternaire étendu*, noté \mathcal{C}_{12} .

Il y a 132 paires de mots de poids 6 équivalents par multiplication par -1 , ce qui définit donc 132 sous-ensembles de $\llbracket 1, 12 \rrbracket$ à 6 éléments. Ils forment un système de Steiner $S(5, 6, 12)$ (unique à permutation près).

Le groupe des isomorphismes de \mathcal{C}_{12} est un produit semi-direct du groupe de Mathieu M_{12} et de $\mathbb{Z}/2\mathbb{Z}$ (agissant par multiplication par -1).

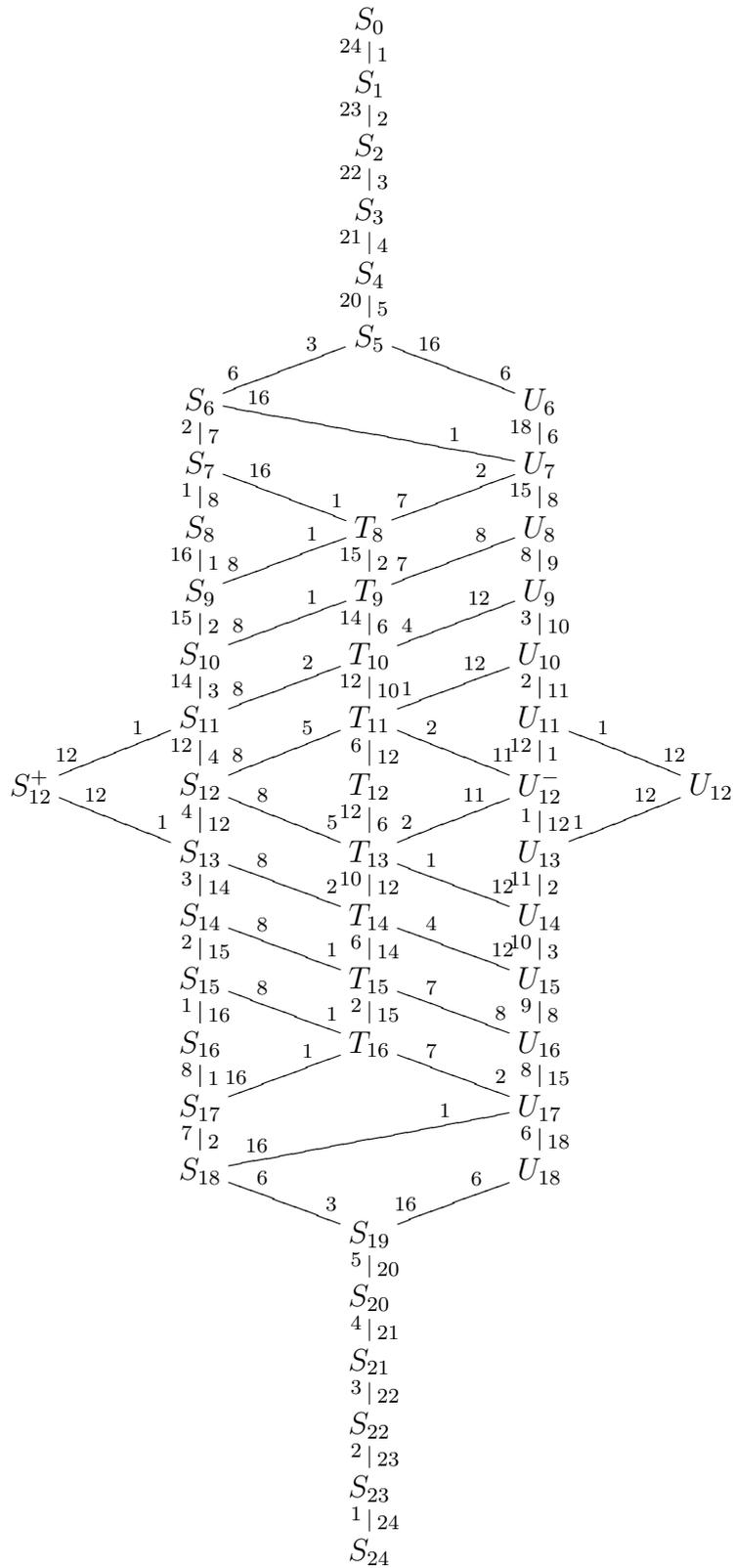


FIG. 1.4 – Action de M_{24} sur $[1, 24]$.

Pour plus de détails sur ce code, nous renvoyons à [Eb02] et à [CS98].

1.3 Groupes orthogonaux et formes modulaires

1.3.1 Domaines homogènes

Domaine projectif. Soit $n \in \mathbb{N}$, on considère l'espace \mathbb{R}^{n+4} muni d'une forme bilinéaire symétrique non dégénérée de signature $(2, n+2)$, notée $(\cdot|\cdot)$. Soit L un réseau entier de cet espace. On considère l'ensemble

$$\Omega(L) = \{[Z] \in \mathbb{P}(L \otimes \mathbb{C}) \mid (Z|Z) = 0, (Z|\bar{Z}) > 0\}.$$

Cet ensemble projectif a deux composantes connexes. En effet, écrivons $Z = X + iY$, avec $X, Y \in L \otimes \mathbb{R}$, nous avons les relations

$$0 = (Z|Z) = (X|X) - (Y|Y) + 2i(X|Y), \quad 0 < (Z|\bar{Z}) = (X|X) + (Y|Y),$$

ce qui implique que

$$X^2 = Y^2 > 0, \quad X \perp Y.$$

Soit l'application continue qui à $Z \in \Omega(L)$ associe l'orientation de la base (X, Y) du plan (réel) qu'ils engendrent, alors son image est $\{+, -\}$, selon que l'orientation de cette base est positive ou négative. Ainsi, $\Omega(L)$ a deux composantes connexes, l'une correspondant à l'orientation positive (notée $\Omega^+(L)$), l'autre à l'orientation négative (notée $\Omega^-(L)$).

On choisit alors arbitrairement l'orientation positive, et on note

$$\mathcal{D}(L) = \{[Z] \in \mathbb{P}(L \otimes \mathbb{C}) \mid (Z|Z) = 0, (Z|\bar{Z}) > 0\}^+ = \Omega^+(L)$$

la composante connexe de $\Omega(L)$ correspondant aux plans d'orientation positive. On l'appellera *domaine homogène projectif*.

Autrement dit, on a montré que $\Omega(L) \cong \text{Gr}_{2,+}(L)$, et que $\mathcal{D}(L) \cong \text{Gr}_{2,+}^+(L)$, où $\text{Gr}_{m,+}(L)$ désigne les Grassmanniennes de dimension m définies positives de $L \otimes \mathbb{R}$, et $\text{Gr}_{m,+}^+(L)$ désigne les Grassmanniennes de dimension m définies positives de $L \otimes \mathbb{R}$ orientées positivement.

Dans la suite, on considérera le \mathbb{C}^* -fibré de $\mathcal{D}(L)$

$$\mathcal{D}^0(L) = \{Z \in L \otimes \mathbb{C} \mid [Z] \in \mathcal{D}(L)\}.$$

Modèle affine. Nous allons maintenant chercher à donner un modèle affine de $\mathcal{D}(L)$. Supposons que $L = U \oplus L_1$, où U est un plan hyperbolique et L_1 est un réseau de signature $(1, n+1)$.

Soit la base de L $(e_1, e_2, \dots, e_{n+3}, e_{n+4})$, où (e_1, e_{n+4}) est un couple hyperbolique de U , et (e_2, \dots, e_{n+3}) est une base de L_1 . Soit $[Z] \in \mathcal{D}(L)$, on écrit $[Z] = [(z_1, z, z_{n+4})]$, avec z_1, z_{n+4} les coordonnées relatives respectivement à e_1 et e_{n+4} , et $z \in L_1 \otimes \mathbb{C}$. Si $z_{n+4} = 0$, alors les relations

$$0 = (Z|Z) = 2z_1 z_4 + (z|z)_{L_1}, \quad 0 < (Z|\bar{Z}) = 2 \text{Re}(z_1 \bar{z}_{n+4}) + (z|\bar{z})_{L_1},$$

où $(\cdot|\cdot)_{L_1}$ désigne la restriction de $(\cdot|\cdot)$ à $L_1 \otimes \mathbb{C}$, impliquent que

$$x^2 = y^2, \quad x \perp y, \quad x^2 > 0,$$

où on a noté $z = x + iy$, $x, y \in L_1 \otimes \mathbb{R}$. On disposerait alors dans $L_1 \otimes \mathbb{R}$, de signature $(1, n + 1)$, de deux vecteurs x et y non nuls, orthogonaux, et de normes strictement positives, c'est absurde par définition de la signature.

Ainsi, $z_{n+4} \neq 0$, et on peut choisir un représentant de $[Z]$ dont la dernière coordonnée vaut 1. Plus précisément, à l'aide des relations précédentes, on voit qu'un tel représentant a pour coordonnée $z_1 = -\frac{1}{2}(z|z)_{L_1}$.

Considérons donc maintenant l'application

$$\Psi : \begin{array}{ccc} \mathcal{D}(L) & \rightarrow & L \otimes \mathbb{C} \\ [Z] = \left[\begin{array}{c} z_1 \\ z \\ z_{n+4} \end{array} \right] & \mapsto & \begin{pmatrix} z_1/z_{n+4} \\ z/z_{n+4} \\ 1 \end{pmatrix} = \begin{pmatrix} -\frac{1}{2}(z'|z')_{L_1} \\ z' \\ 1 \end{pmatrix}. \end{array}$$

Cette application est biholomorphe, et définit un isomorphisme entre $\mathcal{D}(L)$ et

$$\mathcal{D}^{\text{aff}}(L) = \{z \in L_1 \otimes \mathbb{C} \mid z = x + iy, \quad x, y \in L_1 \otimes \mathbb{R}, \quad y^2 > 0\}^+,$$

où encore une fois $+$ désigne le choix d'une composante connexe de $\{z \in L_1 \otimes \mathbb{C} \mid z = x + iy, \quad x, y \in L_1 \otimes \mathbb{R}, \quad y^2 > 0\}$, correspondant au choix de l'orientation. On notera par l'application qui à $z \in \mathcal{D}^{\text{aff}}(L)$ associe le représentant $Z = \begin{pmatrix} -\frac{1}{2}(z|z)_{L_1} \\ z \\ 1 \end{pmatrix} \in \mathcal{D}^0(L)$ de $[Z] \in \mathcal{D}(L)$.

Exemples. On suppose exceptionnellement que $n = -1$, et $L = U + \langle 2 \rangle$. On considère l'ensemble $\mathcal{D}^{\text{aff}}(L) = \{z \in \mathbb{C} \mid z = x + iy, \quad x, y \in \mathbb{R}, \quad y^2 > 0\}^+$. Cet ensemble est le demi-plan de Poincaré \mathbb{H}_1 . En effet, la condition $y^2 > 0$ correspond aux demi-plans supérieur et inférieur de \mathbb{C} , le $+$ signifiant le choix (arbitraire) de la composante supérieure.

On suppose que $n = 0$, et $L = 2U$. Alors $\mathcal{D}^{\text{aff}}(L) = \{(z_1, z_2) \in \mathbb{C} \times \mathbb{C} \mid z_j = x_j + iy_j, \quad x_j, y_j \in \mathbb{R}, \quad j = 1, 2, \quad 2y_1y_2 > 0\}^+$. Cet ensemble est le produit direct de deux demi-plans supérieurs (choix $+$) de \mathbb{C} , $\mathbb{H}_1 \times \mathbb{H}_1$.

On suppose que $n = 1$, et $L = 2U + \langle -2 \rangle$. Alors $\mathcal{D}^{\text{aff}}(L) = \{(\omega, z, \tau) \in L_1 \otimes \mathbb{C} \mid \omega\tau - z^2 > 0\}^+$. La condition $+$ étant le choix de $\omega, \tau \in \mathbb{C}$. Il s'agit du domaine de Siegel de genre 1, $\mathbb{H}_2 = \left\{ Z = \begin{pmatrix} \omega & z \\ z & \tau \end{pmatrix} \in \mathcal{M}_2(\mathbb{C}) \mid \omega, \tau \in \mathbb{H}_1, \quad \text{Im } Z > 0 \right\}$, où $\text{Im } Z > 0$ signifie que la forme bilinéaire symétrique représenté par la partie imaginaire de Z est définie positive.

1.3.2 Groupes orthogonaux

Action sur $\mathcal{D}(L)$. Suivant les notations du paragraphe précédent, on se place dans \mathbb{R}^{n+4} muni d'une forme bilinéaire symétrique non dégénérée $(\cdot|\cdot)$, et on considère un réseau entier L . On suppose que l'on a la décomposition $L = U \oplus L_1$, avec U plan hyperbolique et L_1

de signature $(1, n+1)$, et que $L_1 = U + L_0(-1)$, avec L_0 un réseau entier défini positif. On note $O_{\mathbb{R}}(L)$ le groupe orthogonal (réel) associé à $(\cdot|\cdot)$. Ce groupe agit (par l'action linéaire) sur $\Omega(L)$ (et sur $\Omega^0(L)$ son \mathbb{C}^* -fibré), car $\forall [Z] \in \Omega(L), \forall g \in O_{\mathbb{R}}(L), [g(Z)] \in \Omega(L)$.

Cette action induit une permutation des deux composantes connexes de $\Omega(L)$. Montrons que cette action induite est non triviale, son noyau sera alors un sous-groupe d'indice 2, dont nous allons montrer qu'il est différent du groupe spécial orthogonal (réel) $SO_{\mathbb{R}}(L)$. On fixe une base $(e_1, e_2, \dots, e_{n+3}, e_{n+4})$ de L , telle que (e_1, e_{n+4}) soit un couple hyperbolique de la première copie de U , (e_2, e_{n+3}) un couple hyperbolique de la deuxième copie de U , et (e_3, \dots, e_{n+2}) une base de $L_0(-1)$. On considère dans cette base l'élément

$$g = \begin{pmatrix} 1 & & & & & \\ & -1 & & & & \\ & & I_n & & & \\ & & & -1 & & \\ & & & & & 1 \end{pmatrix}.$$

Il appartient à $O_{\mathbb{R}}(L)$, et est de déterminant 1. Soit l'élément $[Z] = \left[\begin{pmatrix} 1 \\ i \\ 0_{n,1} \\ i \\ 1 \end{pmatrix} \right]$ de $\mathcal{D}(L)$

(ou de $\Omega^-(L)$ respectivement), on peut le décomposer en $Z = X + iY = \begin{pmatrix} 1 \\ 0 \\ 0_{n,1} \\ 0 \\ 1 \end{pmatrix} +$

$i \begin{pmatrix} 0 \\ 1 \\ 0_{n,1} \\ 1 \\ 0 \end{pmatrix}$. Alors $[g(Z)] = \left[\begin{pmatrix} 1 \\ -i \\ 0_{n,1} \\ -i \\ 1 \end{pmatrix} \right] = [X - iY]$ appartient à $\Omega^-(L)$ (ou appartient

à $\mathcal{D}(L)$ respectivement), puisque l'orientation du couple (X, Y) a été changée. Ainsi, le noyau de l'action induite est un sous-groupe d'indice 2 de $O_{\mathbb{R}}(L)$, différent de $SO_{\mathbb{R}}(L)$, que l'on notera $O_{\mathbb{R}}^+(L)$. Ce groupe agit sur $\mathcal{D}(L)$ et le laisse invariant.

On notera aussi $SO_{\mathbb{R}}^+(L)$ le sous-groupe d'indice 4 de $O_{\mathbb{R}}(L)$ correspondant à l'intersection $SO_{\mathbb{R}}(L) \cap O_{\mathbb{R}}^+(L)$, c'est la composante connexe de l'identité dans $O_{\mathbb{R}}(L)$.

On définit aussi les groupes

$$\begin{aligned} O(L) &= \{g \in O_{\mathbb{R}}(L) \mid \forall l \in L, g(l) \in L\}, \\ O^+(L) &= O(L) \cap O_{\mathbb{R}}^+(L), \\ SO^+(L) &= O(L) \cap SO_{\mathbb{R}}^+(L). \end{aligned}$$

Ces deux derniers groupes conservent à la fois $\mathcal{D}(L)$, $\mathcal{D}^0(L)$ et le réseau L .

Lien avec la norme spinorielle. Dans l'espace $L \otimes \mathbb{R} \cong \mathbb{R}^{n+4}$ muni d'une forme bilinéaire symétrique non dégénérée $(\cdot|\cdot)$, on dispose de deux morphismes de groupe, appelés

“normes spinorielles”, θ^+ et θ^- , définis de la façon suivante : soit $\rho \in O_{\mathbb{R}}(L)$, alors il existe des vecteurs a_i , $1 \leq i \leq r$, non isotropes, tels que $\rho = \sigma_{a_1} \circ \dots \circ \sigma_{a_r}$, où $\sigma_{a_i} \in O_{\mathbb{R}}(L)$ est la symétrie orthogonale de direction a_i , c’est à dire $\forall v \in \mathbb{R}^{n+4}$, $\sigma_{a_i}(v) = v - 2\frac{(a_i|v)}{a_i^2}a_i$. On pose $\theta^+(\rho) = 1$ si $\prod_{i=1}^r (a_i|a_i) > 0$, $\theta^+(\rho) = -1$ si $\prod_{i=1}^r (a_i|a_i) < 0$, et $\theta^-(\rho) = 1$ si $\prod_{i=1}^r (-(a_i|a_i)) > 0$, $\theta^-(\rho) = -1$ si $\prod_{i=1}^r (-(a_i|a_i)) < 0$. On peut montrer que ces applications sont bien définies (indépendance vis à vis du choix des a_i), sont bien des morphismes de groupes, et que leur noyau est un sous-groupe d’indice 2 de $O_{\mathbb{R}}(L)$ différent de $SO_{\mathbb{R}}(L)$ (voir par exemple le livre d’Artin *Algèbre géométrique* [Ar62], ou [Kn02], ou encore [GHS08-2]). D’autre part, ces deux applications coïncident sur $SO_{\mathbb{R}}(L)$.

Montrons maintenant que le groupe $O_{\mathbb{R}}^+(L)$ est le noyau de la norme spinorielle θ^- . Comme θ^- est un morphisme, et que tout élément de $O_{\mathbb{R}}(L)$ est produit de réflexions orthogonales de direction un vecteur non isotrope, il suffit de montrer qu’une réflexion dirigée par un vecteur de carré positif (donc de norme spinorielle -1) échange les composantes connexes de $\Omega(L)$, tandis qu’une réflexion dirigée par un vecteur de carré négatif (donc de norme spinorielle 1) conserve $\mathcal{D}(L)$.

Soit $a \in L \otimes \mathbb{R}$, non isotrope. Quitte à renormaliser a , on peut supposer que $a^2 = \pm \frac{1}{2}$, et donc $\sigma_a(v) = v \mp (a|v)a$. Supposons dans un premier temps que $a^2 = -\frac{1}{2}$. Il existe $b \in L \otimes \mathbb{C}$, $b^2 = \frac{1}{2}$ et $(a|b) = 0$. On peut alors former le couple hyperbolique $(e_1 = b + a, e_{n+4} = b - a)$, et le compléter en une base $(e_1, e_2, \dots, e_{n+3}, e_{n+4})$ telle que e_1, e_2 soient orthogonaux aux autres vecteurs e_i , $2 \leq i \leq n+3$, que (e_2, e_{n+3}) soit un autre couple hyperbolique, et que e_3, \dots, e_{n+2} soient orthogonaux à e_2, e_{n+3} . Dans cette base, on considère l’élément

$$[Z] = \left[\begin{pmatrix} 1 \\ i \\ 0_{n,1} \\ i \\ 1 \end{pmatrix} \right] \text{ de } \mathcal{D}(L) \text{ (ou de } \Omega^-(L)), \text{ on peut le décomposer en } Z = X + iY =$$

$$\begin{pmatrix} 1 \\ 0 \\ 0_{n,1} \\ 0 \\ 1 \end{pmatrix} + i \begin{pmatrix} 0 \\ 1 \\ 0_{n,1} \\ 1 \\ 0 \end{pmatrix}. \text{ D’autre part, } \sigma_a \text{ a pour matrice } \begin{pmatrix} & & & & 1 \\ & & & & \\ & & I_{n+2} & & \\ & & & & \\ 1 & & & & \end{pmatrix}. \text{ Ainsi } [\sigma_a(Z)] =$$

$$\left[\begin{pmatrix} 1 \\ i \\ 0_{n,1} \\ i \\ 1 \end{pmatrix} \right] \text{ appartient à } \mathcal{D}(L) \text{ (ou à } \Omega^-(L) \text{ respectivement), et donc } \sigma_a \text{ conserve } \mathcal{D}(L).$$

Inversement, si $a^2 = \frac{1}{2}$, la démonstration précédente reste valable en échangeant les rôles de a et de b , mais alors cette fois la matrice de σ_a est $\begin{pmatrix} & & & & -1 \\ & & & & \\ & & I_{n+2} & & \\ & & & & \\ -1 & & & & \end{pmatrix}$, si bien que

$$\left[\sigma_a \left(\begin{pmatrix} 1 \\ i \\ 0_{n,1} \\ i \\ 1 \end{pmatrix} \right) \right] = \left[\begin{pmatrix} 1 \\ -i \\ 0_{n,1} \\ -i \\ 1 \end{pmatrix} \right] = [X - iY] \text{ appartient à } \Omega^-(L) \text{ (ou appartient à } \mathcal{D}(L)$$

respectivement), et donc σ_a ne préserve pas $\mathcal{D}(L)$.

On a donc établi que $O_{\mathbb{R}}^+(L) = \ker \theta^-$.

1.3.3 Formes modulaires

Définition 1.34. Soit L un réseau quadratique entier de signature $(2, n + 2)$, $n \in \mathbb{N}^*$. Soient $\Gamma \subset O^+(L)$ un sous-groupe d'indice fini, et $\chi : \Gamma \rightarrow \mathbb{C}^*$ un caractère. On appelle forme modulaire de poids k et caractère χ pour Γ , une fonction holomorphe $F : \mathcal{D}^0(L) \rightarrow \mathbb{C}$ telle que :

- (i) $\forall t \in \mathbb{C}^*, \forall Z \in \mathcal{D}^0(L), F(tZ) = t^{-k}F(Z)$,
- (ii) $\forall \gamma \in \Gamma, \forall Z \in \mathcal{D}^0(L), F(\gamma(Z)) = \chi(\gamma)F(Z)$.

Si on autorise pour n les valeurs -1 et 0 , alors il faut rajouter une condition d'holomorphicité aux points paraboliques et demander au caractère d'être d'ordre fini.

1.3.4 Diviseurs quadratiques rationnels

On considère un réseau L de signature $(2, n + 2)$.

Définition 1.35. Soit $r \in L^*$ tel que $r^2 < 0$. On appelle diviseur quadratique rationnel dirigé par r l'ensemble

$$\mathcal{D}_r(L) = \{[Z] \in \mathcal{D}(L) \mid (Z, r) = 0\}.$$

Le terme “quadratique” se justifie de la façon suivante : un élément $[Z] \in \mathcal{D}(L)$ admet un représentant $(\text{pr}(\Psi([Z])))$ dont les coordonnées sont $\begin{pmatrix} -\frac{1}{2}(z|z)_{L_1} \\ z \\ 1 \end{pmatrix}$, si bien que la condition $(Z|r) = 0$ se traduit par l'équation quadratique $-\frac{1}{2}(z|z)_{L_1}r_{n+4} + r_1 + (r|z) = 0$.

Domaines homogènes. Voyons maintenant quel domaine est défini par $\mathcal{D}_r(L)$. Si $r^2 < 0$, alors $\mathcal{D}_r(L) \cap \mathcal{D}(L)$ est un domaine homogène défini par un réseau de signature $(2, n + 1)$, r_L^\perp .

Si $r^2 > 0$, alors $r_L^\perp \otimes \mathbb{R}$ est de signature $(1, n + 2)$. Ecrivons alors, pour $[Z] \in \mathcal{D}(L)$, $Z = X + iY$, avec $X, Y \in \otimes \mathbb{R}$. On a alors les conditions $(Z|Z) = 0$, donc $X^2 = Y^2$ et $X \perp Y$, et $(Z|\bar{Z}) > 0$, donc $X^2 + Y^2 > 0$. Ainsi, si $[Z]$ est dans $\mathcal{D}_r(L)$, on dispose alors de deux vecteurs orthogonaux de carré strictement positif dans $r_L^\perp \otimes \mathbb{R}$, ce qui est contradictoire avec la signature de cet espace. Ainsi, $\mathcal{D}_r(L) \cap \mathcal{D}(L) = \emptyset$.

Si $r^2 = 0$, alors l'espace $(r_L^\perp \otimes \mathbb{R})/\mathbb{R}r$ est de signature $(1, n + 1)$, et on peut réitérer le raisonnement précédent pour aboutir à $\mathcal{D}_r(L) \cap \mathcal{D}(L) = \emptyset$.

Ainsi, lorsque l'on dispose d'un vecteur $r \in L$ tel que $r^2 < 0$, et d'une forme modulaire F , on peut considérer la restriction de F au sous-domaine $\mathcal{D}_r^0(L) = \{Z \in \mathcal{D}^0(L) \mid (Z|r) = 0\}$ de $\mathcal{D}^0(L)$.

Réflexions. Soit $r \in L^*$ un vecteur non isotrope, on définit la *réflexion orthogonale de direction r* de la façon suivante :

$$\sigma_r(l) = l - 2 \frac{(l|r)}{r^2} r.$$

A quelle condition un élément σ_r appartient-il au groupe $O^+(L)$? σ_r appartient à $O(L)$ si et seulement si pour tout $l \in L$, $\sigma_r(l) = l - 2 \frac{(l|r)}{r^2} r \in L$. D'autre part, comme on l'a déjà vu, $\sigma_r \in O_{\mathbb{R}}^+(L)$ si et seulement si $r^2 < 0$. On appellera *vecteur réflexif* un vecteur non isotrope $r \in L^*$ tel que $\sigma_r \in O^+(L)$. En particulier, les vecteurs de carré -2 sont réflexifs.

Soit F une forme modulaire définie sur $\mathcal{D}^0(L)$, pour le groupe $O^+(L)$ et de caractère déterminant, et $r \in L$ un vecteur réflexif. On a alors la relation $F(\sigma_r(Z)) = -F(Z)$, donc pour $Z \in \mathcal{D}_r^0(L)$, $F(Z) = -F(Z)$, et donc $F|_{\mathcal{D}_r^0(L)} \equiv 0$.

Enfin, on a la définition suivante :

Définition 1.36. Soit F une forme modulaire pour un sous-groupe $\Gamma \subset O^+(L)$ d'indice fini. On dit que F est une forme modulaire réflexive si F ne s'annule que le long de diviseurs quadratiques rationnels dirigés par des vecteurs réflexifs.

1.3.5 Groupe stable orthogonal

Définition 1.37. Soit L un réseau entier pair. On définit le groupe stable orthogonal de L comme étant le sous-groupe distingué de $O(L)$ suivant :

$$\tilde{O}(L) = \{g \in O(L) \mid \forall l^* \in L^*, g(l^*) - l^* \in L\}.$$

Il s'agit bien d'un sous-groupe distingué de $O(L)$. En effet, $g \in O(L)$ induit un élément de $O(L^*)$, que l'on notera encore g . On peut donc considérer l'application

$$\Psi : \begin{array}{ccc} O(L) & \rightarrow & O(D(L)) \\ g & \mapsto & \bar{g} \end{array},$$

où \bar{g} est l'application induite par g sur $O(D(L))$. Il est alors clair que le noyau de cet homomorphisme de groupe est $\tilde{O}(L)$.

Lemme 1.12. Soit N un réseau pair, et L un sous-réseau de N . On note $M = L_N^\perp$ son orthogonal. Soit $\tilde{g} \in \tilde{O}(L)$, alors il existe $g \in \tilde{O}(N)$ tel que la restriction de g à L vérifie $g|_L = \tilde{g}$. De plus, $g|_M = id_M$.

PREUVE : On dispose de la double inclusion

$$L \oplus M \subset N \subset N^* \subset L^* \oplus M^*.$$

On considère l'élément $g \in O(L \oplus M)$ tel que $g|_L = \tilde{g}$ et $g|_M = id_M$, ce qui est possible puisque $L \perp M$. Regardons g comme un élément de $O((L \oplus M) \otimes \mathbb{Q})$, on a $g \in O(L^* \oplus M^*)$ (car $\forall x \in L, y \in L^*, (x|g(y)) = (g^{-1}(x)|y) \in \mathbb{Z}$). Regardons $g|_{N^*}$. Tout vecteur $v^* \in N^*$ s'écrit $v^* = l^* + m^*$ avec $l^* \in L^*$ et $m^* \in M^*$. Alors, $g(v^*) - v^* = (\tilde{g}(l^*) + m^*) - (l^* + m^*) = \tilde{g}(l^*) - l^* \in L \subset N$, et donc $g \in \tilde{O}(N)$. On a bien démontré le lemme. \square

Lemme 1.13. *Soit L un réseau pair et $a \in L$ un vecteur isotrope ($a^2 = 0$) non nul. Pour tout vecteur $b \in \mathbb{Z}a_L^\perp$, on définit l'application de $O(\mathbb{Z}a_L^\perp)$*

$$t_{a,b} : \mathbb{Z}a_L^\perp \rightarrow \mathbb{Z}a_L^\perp \\ l \mapsto l - (l|b)a.$$

Alors il existe une unique transformation orthogonale du réseau L , $T_{a,b} \in O(L)$, telle que

$$T_{a,b}|_{\mathbb{Z}a_L^\perp} = t_{a,b}.$$

De plus, $\forall l \in L, T_{a,b}(l) = l - (l|b)a + (l|a)b - \frac{1}{2}(b|b)(l|a)a$.

PREUVE : Le fait que $t_{a,b} \in O(\mathbb{Z}a_L^\perp)$ est évident. Définissons l'application $T_{a,b}$ qui à $l \in L$ associe le vecteur $l - (l|b)a + (l|a)b - \frac{1}{2}(b|b)(l|a)a$. Cette application est bien linéaire, $T_{a,b}(l) \in L$, et on peut vérifier que $\forall l \in L, T_{a,b}(l)^2 = l^2$. D'autre part, $\forall l \in \mathbb{Z}a_L^\perp, T_{a,b}(l) = l - (l|b)a = t_{a,b}$, d'où l'existence d'une application $T_{a,b} \in O(L)$ telle que $T_{a,b}|_{\mathbb{Z}a_L^\perp} = t_{a,b}$.

Montrons l'unicité. Considérons les vecteurs dans $L \otimes \mathbb{Q}$. Comme $a^2 = 0$ et $a \neq 0$, il existe un plan hyperbolique $U \otimes \mathbb{Q}$ et un vecteur $v \in U \otimes \mathbb{Q}$, isotrope, non nul, et tel que $(a|v) = 1$ et $U \otimes \mathbb{Q} = \langle a, v \rangle$. De plus, on a $L \otimes \mathbb{Q} = (U \otimes \mathbb{Q}) \oplus (U \otimes \mathbb{Q})_{L \otimes \mathbb{Q}}^\perp$. Supposons avoir l'existence de T_1 et T_2 dans $O(L)$ tels que $T_1|_{\mathbb{Z}a_L^\perp} = T_2|_{\mathbb{Z}a_L^\perp} = t_{a,b}$. En particulier, $T_1 \circ T_2^{-1}$ préserve $(U \otimes \mathbb{Q})_{L \otimes \mathbb{Q}}^\perp$, et on a $T_1 \circ T_2^{-1}|_{(U \otimes \mathbb{Q})_{L \otimes \mathbb{Q}}^\perp} = id_{(U \otimes \mathbb{Q})_{L \otimes \mathbb{Q}}^\perp}$. Ainsi, $U \otimes \mathbb{Q}$ est aussi stable par $T_1 \circ T_2^{-1}$. On calcule $T_1 \circ T_2^{-1}(a) = a$. Enfin, reste à calculer la valeur de $T_1 \circ T_2^{-1}(v)$. Comme $U \otimes \mathbb{Q}$ est stable par $T_1 \circ T_2^{-1}$, $T_1 \circ T_2^{-1}(v) = xa + yv$, avec $x, y \in \mathbb{Q}$. On a alors

$$1 = (v|a) = (v|(T_1 \circ T_2^{-1})^{-1}(a)) = (T_1 \circ T_2^{-1}(v)|a) = (xa + yv|a) = y,$$

donc $y = 1$, puis $T_1 \circ T_2^{-1}(v)$ est isotrope, donc on a $0 = (xa + v)^2 = 2x$, donc $x = 0$ et enfin $T_1 \circ T_2^{-1}(v) = v$. On a donc établi que $T_1 \circ T_2^{-1} = id_{L \otimes \mathbb{Q}}$, en particulier, $T_1 = T_2$ en tant que transformations orthogonales de L , d'où l'unicité annoncée. \square

Définition 1.38. *La transformation $T_{a,b}$ définie dans le lemme précédent est appelée transvection orthogonale.*

Lemme 1.14. *Soient $a \in L$ un vecteur isotrope non-nul, et $b \in \mathbb{Z}a_L^\perp$. Si b est un vecteur non-isotrope, alors*

$$T_{a,b} = \sigma_b \circ \sigma_{b + \frac{1}{2}(b|b)a} \in SO(L \otimes \mathbb{Q}), \quad \text{où pour } v \in L, v^2 \neq 0, \forall l \in L, \sigma_v(l) = l - 2 \frac{(l|v)}{v^2} v.$$

PREUVE : On remarque que $b^2 = (b + \frac{1}{2}(b|b)a)^2$, donc si b est non-isotrope les deux réflexions sont bien définies. On calcule, pour $l \in \mathbb{Z}a^\perp$,

$$\begin{aligned} \sigma_b \circ \sigma_{b+\frac{1}{2}(b|b)a}(l) &= \sigma_{b+\frac{1}{2}(b|b)a}(l) - 2 \frac{\left(\sigma_{b+\frac{1}{2}(b|b)a}(l) \middle| b \right)}{b^2} b \\ &= \left(l - 2 \frac{(b + \frac{1}{2}b^2a|l)}{b^2} (b + \frac{1}{2}b^2a) \right) - 2 \frac{\left(l - 2 \frac{(b|l)}{b^2} (b + \frac{1}{2}b^2a) \middle| b \right)}{b^2} b \\ &= l - 2 \frac{(b|l)}{b^2} (b + \frac{1}{2}b^2a) - 2 \frac{(l|b)}{b^2} b + 4 \frac{(b|l)b^2}{(b^2)^2} b \\ &= l - (b|l)a = t_{a,b}(l). \end{aligned}$$

Donc on a bien établi que $T_{a,b} = \sigma_b \circ \sigma_{b+\frac{1}{2}(b|b)a} \in SO(L \otimes \mathbb{Q})$. \square

Corollaire 1.3. Soient $a \in L$ un vecteur isotrope non-nul, et $b \in \mathbb{Z}a^\perp$. Alors $T_{a,b} \in S\tilde{O}^+(L)$.

PREUVE : Commençons par traiter le cas où b est non-isotrope. D'après le lemme 1.14, $T_{a,b} = \sigma_b \circ \sigma_{b+\frac{1}{2}(b|b)a}$. Donc en particulier, $T_{a,b} \in SO(L)$. On a remarqué aussi que $b^2 = (b + \frac{1}{2}(b|b)a)^2$, donc d'après le théorème de Witt, il existe $\rho \in O(L \otimes \mathbb{R})$ tel que $\rho(b) = b + \frac{1}{2}(b|b)a$. On a alors

$$T_{a,b} = \sigma_b \circ \sigma_{b+\frac{1}{2}(b|b)a} = \sigma_b \circ \rho \circ \sigma_{b+\frac{1}{2}(b|b)a} \circ \rho^{-1},$$

puis la norme spinorielle de $T_{a,b}$ est égale au produit des normes spinorielles de σ_b , $\sigma_{b+\frac{1}{2}(b|b)a}$, ρ et ρ^{-1} , et du fait que la norme spinorielle est un morphisme de groupe, il vient que $T_{a,b} \in SO^+(L)$.

Si b est un vecteur isotrope, comme de plus $a \perp b$, il existe $b' \in L \otimes \mathbb{Q}$ un vecteur isotrope non nul, tel que $b' \perp a$ et $(b|b') = 1$. On vérifie alors que les vecteurs $b_+ = \frac{1}{2}(b + b')$ et $b_- = \frac{1}{2}(b - b')$ ne sont pas isotropes, et que $T_{a,b} = T_{a,b_+} \circ T_{a,b_-}$, ce qui permet de conclure puisque d'après ce qui précède T_{a,b_+} et T_{a,b_-} sont dans $SO^+(L)$.

Enfin, pour montrer que $T_{a,b} \in \tilde{O}(L)$, il suffit de calculer : soit $l^* \in L^*$, alors $T_{a,b}(l^*) - l^* = -(l^*|b)a + (l^*|a)b - \frac{1}{2}b^2(l^*|a)a \in L$. \square

Lemme 1.15. Soit $L = 2U$, où U est un plan hyperbolique. Alors pour tout $l \in L$, il existe $g \in S\tilde{O}^+(L)$ tel que $g(l) \in U^{(2)}$, où $U^{(2)}$ désigne la deuxième copie de U de L .

PREUVE : On considère l'ensemble

$$L' = \left\{ \left(\begin{array}{cc} a & -b \\ c & d \end{array} \right) \in \mathcal{M}_2(\mathbb{Z}) \middle| a, b, c, d \in \mathbb{Z} \right\}$$

munit de la forme bilinéaire symétrique $Q(X) = 2 \det(X) = 2(ad+bc)$ où $X = \begin{pmatrix} a & -b \\ c & d \end{pmatrix} \in$

L' . Ainsi construit, L' est un réseau isomorphe à $2U$.

Considérons l'application

$$\begin{aligned} F &: SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z}) \rightarrow S\tilde{O}^+(L') \\ (A, B) &\mapsto (F_{A,B} : X \mapsto AXB^{-1}) . \end{aligned}$$

F est bien définie car pour tous $(A, B) \in SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z})$, pour tout $X \in L'$, $F_{A,B}(X) \in L'$, $F_{A,B}$ est linéaire, et pour tous $(A, B) \in SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z})$, pour tout $X \in L'$, $\det AXB^{-1} = \det X$. Notons maintenant $e_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $f_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, $e_2 = \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix}$

et $f_2 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, alors (e_1, f_1) est un couple hyperbolique de la première copie de U et

(e_2, f_2) un couple hyperbolique de la seconde copie de U . On note $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbb{Z})$

et $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in SL_2(\mathbb{Z})$, on sait que ces deux matrices engendrent $SL_2(\mathbb{Z})$. Remar-

quons (calcul) que $T_{e_1, e_2} = F_{T, I_2}$ et $T_{f_1, f_2} = F_{T', I_2}$, où $T' = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. Comme on calcule

$TT'^{-1}T = S$, on déduit que T et T' engendrent $SL_2(\mathbb{Z})$, puis que les F_{A, I_2} pour $A \in SL_2(\mathbb{Z})$ sont des produits de tranvections. Ensuite, on remarque (calcul) que $T_{e_2, f_1} = F_{I_2, T^{-1}}$ et $T_{f_2, e_1} = F_{I_2, T'}$, d'où l'on déduit que les $F_{I_2, B}$ pour $B \in SL_2(\mathbb{Z})$ sont des produits de tranvections. Ainsi, les $F_{A, B}$ pour $(A, B) \in SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z})$ sont des produits de tranvections.

Soit $X \in \mathcal{M}_2(\mathbb{Z})$, d'après le théorème de la base adaptée (théorème 1.1), il existe $(A, B) \in SL_2(\mathbb{Z})$ tel que $AXB^{-1} = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$ avec $\alpha, \beta \in \mathbb{Z}$, $\alpha|\beta$ et $\alpha\beta = \det(X)$. En d'autre termes, pour $X \in L'$, on a trouvé $(A, B) \in SL_2(\mathbb{Z})$ tel que $F_{A, B}(X)$ soit dans la deuxième copie de U de L' , comme on a vu que $F_{A, B}$ était un produit de tranvections, on a bien établi le résultat annoncé. \square

Théorème 1.6. Critère d'Eichler ([Ei74] §10 ou [GHS08-1] lemme 3.5)

Soit L un réseau pair de signature $(2, n+2)$, $n \in \mathbb{N}$. On suppose que $L = 2U \oplus L_0(-1)$ où U est le plan hyperbolique et L_0 un réseau pair défini positif. Soient $l_1, l_2 \in L$ des vecteurs primitifs, tels que $l_1^2 = l_2^2$ et $\frac{l_1}{\text{div}(l_1)} \equiv \frac{l_2}{\text{div}(l_2)} \pmod{L}$. Alors, il existe $g \in \tilde{O}(L)$ tel que $g(l_1) = l_2$.

Remarque. Notons $l_1^* = \frac{l_1}{\text{div}(l_1)}$, alors pour tout $g \in \tilde{O}(L)$, $g(l_1^*) \equiv l_1^* \pmod{L}$, ainsi l'énoncé du critère d'Eichler est optimal.

PREUVE : Dans un premier temps, nous allons nous ramener au cas où l_1 et l_2 sont des vecteurs primitifs de $U^{(2)} \oplus L_0(-1)$, où $U^{(2)}$ désigne la seconde copie de $2U$. On écrit, pour $i = 1, 2$, $l_i = u_i + l'_i$ avec $u_i \in 2U$ et $l'_i \in L_0(-1)$. D'après le lemme 1.15, il existe $g_1, g_2 \in S\tilde{O}^+(2U)$ tels que $g_i(u_i) \in U^{(2)}$, pour $i = 1, 2$. D'après le lemme 1.12, ces éléments g_i se prolongent en transformations orthogonales de $S\tilde{O}^+(2U \oplus L_0(-1))$, que nous noterons

encore g_i , et qui vérifient $g_i|_{L_0(-1)} = id_{L_0(-1)}$. On a alors $g_i(l_i) = g_i(u_i) + l'_i \in U^{(2)} \oplus L_0(-1)$, pour $i = 1, 2$.

On suppose maintenant que $l_1, l_2 \in U^{(2)} \oplus L_0(-1)$. Notons (e, f) un couple hyperbolique de $U^{(1)}$. On considère les éléments $\tilde{l}_i \in U^{(2)} \oplus L_0(-1)$ tels que $(l_i|\tilde{l}_i) = d_i$ où $\text{div}(l_i) = d_i$, pour $i = 1, 2$. Ces éléments \tilde{l}_i existent par définition du diviseur d'un vecteur, et peuvent être choisis dans $U^{(2)} \oplus L_0(-1)$ plutôt que dans $2U \oplus L_0(-1)$ du fait que $U^{(1)} \perp U^{(2)} \oplus L_0(-1)$. D'autre part, la proposition 1.4 permet de justifier que $d_1 = d_2 = d = \text{ordre}_{L^*/L}(\frac{l_i}{\text{div}(l_i)})$, $i = 1, 2$. On pose alors $w = \frac{l_1 - l_2}{d} \in L$ (car $\frac{l_1}{d} \equiv \frac{l_2}{d} \pmod{L}$), et on calcule successivement

$$T_{e, \tilde{l}_1}(l_1) = l_1 - de,$$

$$\begin{aligned} T_{f, w}(l_1 - de) &= (l_1 - de) - (l_1 - de|\frac{l_1 - l_2}{d})f + (l_1 - de|f)\frac{l_1 - l_2}{d} - \frac{1}{2}(\frac{l_1 - l_2}{d})^2(l_1 - de|f)f \\ &= l_1 - de + \left(-\frac{l_1^2 - (l_1|l_2)}{d}\right)f - l_1 + l_2 + \frac{1}{2}\frac{l_1^2 + l_2^2 - 2(l_1|l_2)}{d}f \\ &= l_2 - de, \end{aligned}$$

$$T_{e, -\tilde{l}_2}(l_2 - de) = l_2,$$

ce qui achève la démonstration du théorème. \square

On adoptera alors les notations suivantes, pour la suite. La $\tilde{O}^+(L)$ -orbite d'un vecteur primitif $v \in L$, de norme $v^2 = a$ et tel que $\frac{v}{\text{div}(v)} \equiv \bar{b} \pmod{L}$ sera notée $H_a(\bar{b})$.

1.3.6 Automorphismes du groupe discriminant

Soit L un réseau entier pair. Considérons l'application

$$\Psi^+ : \begin{array}{ccc} O^+(L) & \rightarrow & O(D(L)) \\ g & \mapsto & \bar{g} \end{array},$$

où \bar{g} est l'application induite par g sur $O(D(L))$.

Nous avons vu que le noyau de cet homomorphisme de groupe est, par définition, $\tilde{O}^+(L)$. La question qu'il est alors naturel de se poser, est qu'en est-il de la surjectivité de Ψ^+ .

Nous allons traiter cette question sur des exemples particuliers dont nous aurons besoin par la suite, explicitant ainsi (lorsque cela existe) des antécédents aux éléments de $O(D(L))$. Pour cela, nous allons considérer dans un premier temps des réseaux L pairs qui sont somme de deux plans hyperboliques U et d'un réseaux de racines irréductibles (défini négatif). Dans un second temps, L sera juste un réseau de racines irréductibles (défini négatif), et pour terminer, nous traiterons le cas de la somme directe de plusieurs réseaux irréductibles.

Réseaux de la famille \mathbb{A}_n : Dans un premier temps, considérons, pour $n \geq 2$, le réseau $L = 2U \oplus \mathbb{A}_n(-1)$. D'après les tables données en partie 1.1.4, le groupe des automorphismes $O(D(2U \oplus \mathbb{A}_n(-1)))$ est $\mathbb{Z}/2\mathbb{Z}$. Il consiste en l'élément identité et l'application $[i] \mapsto [n + 1 - i]$. Cette dernière peut se réaliser comme étant induite par l'élément

$g \in O^+(L)$ qui réalise l'identité sur $2U$ et $-id$ sur $\mathbb{A}_n(-1)$. En effet, $\mathbb{A}_n(-1)$ étant défini négatif, $-id$ est produit de réflexions de direction un vecteur de carré négatif, donc $-id \in O_{\mathbb{R}}^+(\mathbb{A}_n(-1))$, et comme $-id$ préserve $\mathbb{A}_n(-1)$, $-id \in O((\mathbb{A}_n(-1)))$, puis il vient que $g \in O^+(L)$. On a donc montré la surjectivité de Ψ^+ dans ce cas. Dans le cas de $\mathbb{A}_1(-1)$, les automorphismes de $D(L)$ sont réduits à l'élément trivial.

Considérons maintenant le réseau $L = \mathbb{A}_n(-1)$. On dispose du même groupe $O(D(L))$ que précédemment, et l'élément $-id \in O^+(L)$ donne un relèvement de l'élément non trivial de $O(D(L))$, on a à nouveau montré la surjectivité de Ψ^+ .

Si l'on suppose maintenant que L est somme directe de $k \in \mathbb{N}^*$ copies de $\mathbb{A}_n(-1)$. Alors $D(k\mathbb{A}_n(-1)) = \bigoplus_{i=1}^k D(\mathbb{A}_n(-1))$, et le groupe des automorphismes de L est alors engendré par les éléments des groupes d'automorphismes $O(D(\mathbb{A}_n(-1)))$ de chaque copie, et par les éléments qui permutent les copies de $\mathbb{A}_n(-1)$. Pour montrer la surjectivité de Ψ^+ dans ce cas, il reste à relever chaque permutation de deux copies de $\mathbb{A}_n(-1)$ dans $O^+(L)$. Considérons (e_1^1, \dots, e_n^1) une base orthogonale de vecteurs de norme -1 d'une copie de $\mathbb{A}_n(-1) \otimes \mathbb{Q}$, et (e_1^2, \dots, e_n^2) une base orthogonale de vecteurs de norme -1 d'une autre copie de $\mathbb{A}_n(-1) \otimes \mathbb{Q}$. Alors l'application linéaire qui échange chaque élément e_i^1 avec e_i^2 , $1 \leq i \leq n$, est un élément de $O^+(L)$ qui convient. On a donc établi la surjectivité de Ψ^+ dans le cas où L est somme directe de copies de $\mathbb{A}_n(-1)$. Il est clair que Ψ^+ est encore surjective si l'on ajoute deux plans hyperboliques.

Réseaux de la famille \mathbb{D}_n : Dans un premier temps, considérons, pour $n \geq 3$, le réseau $L = 2U \oplus \mathbb{D}_n(-1)$. D'après les tables données en partie 1.1.4, le groupe des automorphismes $O(D(2U \oplus \mathbb{D}_n(-1)))$ est $\mathbb{Z}/2\mathbb{Z}$ si $n \not\equiv 4 \pmod{8}$. Il consiste en l'élément identité, et l'application $[1] \mapsto [3]$. $O(D(2U \oplus \mathbb{D}_n(-1)))$ est \mathcal{S}_3 si $n \equiv 4 \pmod{8}$. Il consiste en les permutations de $[1]$, $[2]$ et $[3]$. Dans tous les cas, la transposition $\tau_{[1],[3]} : [1] \mapsto [3]$ se relève dans $O^+(L)$ par l'élément $\sigma_{\varepsilon_2} \in O^+(L)$ (voir le lemme 2.1 pour la réflexivité de ε_2), où ε_2 est un représentant dans \mathbb{D}_n^* de la classe $[2]$ de norme -1 (voir partie 1.1.4). La vérification est facile et laissée au lecteur. Dans le cas $n \equiv 4 \pmod{8}$ et $n \neq 4$, soit (e, f) un couple hyperbolique de U , on considère l'élément $l_1 = \frac{1}{2} \left(\frac{n}{4} - 1 \right) e + f + \varepsilon_1 \in L^*$. On a $l_1^2 = -1$, et donc d'après le lemme 2.1, $\sigma_l \in O^+(L)$. On vérifie facilement que cette réflexion permute $[2]$ et $[3]$. De même on construit une réflexion qui induit la permutation de $[1]$ et $[2]$. Lorsque $n = 4$, on peut prendre $l_1 = \varepsilon_2$ et $l_3 = \varepsilon_3$. On a donc montré la surjectivité de Ψ^+ dans le cas $L = 2U \oplus \mathbb{D}_n(-1)$.

Considérons maintenant le réseau $L = \mathbb{D}_n(-1)$. On dispose du même groupe $O(D(L))$ que précédemment, et le relèvement de la transposition $\tau_{[1],[3]}$ est encore possible. Cependant, lorsque $n \equiv 4 \pmod{8}$ et $n \neq 4$, les transpositions $\tau_{[1],[2]}$ et $\tau_{[2],[3]}$ n'admettent pas d'antécédent par Ψ^+ . En effet, s'il existe $g \in O^+(L)$ tel que g induit la transposition $\tau_{[1],[2]}$, soit $\underline{\varepsilon_2}$ un représentant de la classe $[2]$ dans $D_n(-1)^*$, de norme -1 . Alors $g(\varepsilon_2)^2 = -1$, et $g(\varepsilon_2) = [1]$. Pourtant, la classe $[1]$ n'admet pas de représentant de norme $\geq -\frac{n}{4}$, avec $-\frac{n}{4} < -1$. C'est donc absurde. On applique le même raisonnement à la transposition $\tau_{[1],[3]}$. De même, il n'y a pas de 3-cycle dans l'image de Ψ^+ . En revanche, pour $n = 4$, on peut réaliser les permutations comme précédemment (avec σ_{ε_i} , $1 \leq i \leq 3$). On a donc

établi la surjectivité de Ψ^+ lorsque $L = 2U \oplus \mathbb{D}_n(-1)$ avec $n \not\equiv 4 \pmod{8}$ ou $n = 4$. Lorsque $n \equiv 4 \pmod{8}$ et $n \neq 4$, Ψ^+ n'est pas surjective, son image est $\{id, \sigma_{\varepsilon_2}\}$.

Si l'on suppose maintenant que L est somme directe de $k \in \mathbb{N}^*$ copies de $\mathbb{D}_n(-1)$. Alors $D(k\mathbb{D}_n(-1)) = \bigoplus_{i=1}^k D(\mathbb{D}_n(-1))$, et le groupe des automorphismes de L est alors engendré par les éléments des groupes d'automorphismes $O(D(\mathbb{D}_n(-1)))$ de chaque copie, et par les éléments qui permutent les copies de $\mathbb{D}_n(-1)$. Relevons chaque permutation de deux copies de $\mathbb{D}_n(-1)$ dans $O^+(L)$ de la même façon que dans le cas des réseaux de type \mathbb{A}_n .

Réseaux \mathbb{E}_8 , \mathbb{E}_7 et \mathbb{E}_6 : Il n'y a rien à faire dans les deux premiers cas, les groupes d'automorphismes étant triviaux. Dans le cas de \mathbb{E}_6 , le groupe discriminant est $\mathbb{Z}/2\mathbb{Z}$, et l'élément à considérer pour obtenir un relèvement en $-id$ sur \mathbb{E}_6 . La démonstration est la même que pour la famille \mathbb{A}_n . Ainsi, Ψ^+ est encore surjective, pour $L = \mathbb{E}_6$, $L = 2U \oplus \mathbb{E}_6$, $L = k\mathbb{E}_6$ et $L = 2U \oplus k\mathbb{E}_6$.

Somme directe (finie) de réseaux de racines irréductibles : Dans ce cas, on regroupe les copies de réseaux irréductibles par familles, et le groupe des automorphismes de $D(L)$ est le produit direct des groupes des automorphismes des $D(L_i)$ où les L_i sont des $k_i\mathbb{A}_{n_i}$, $k_j\mathbb{D}_{n_j}$ ou $k_l\mathbb{E}_{n_l}$, pour des n_i, n_j, n_l distincts. L'étude de la surjectivité de Ψ^+ est alors ramenée à l'étude précédente.

1.4 Réseaux de Niemeier

1.4.1 Configurations possibles pour les racines

On considère L un réseau unimodulaire pair de dimension n . D'après ce que l'on a déjà vu (proposition 1.9), nécessairement, $n \equiv 0 \pmod{8}$. Intéressons-nous au cas où $0 < n \leq 24$.

Proposition 1.8. ([Eb02] prop. 3.3 p.100)

Soit L un réseau unimodulaire pair de dimension $n = 8, 16$ ou 24 . Soit $y \in L \otimes \mathbb{R}$, on a

$$\sum_{x \in R_L} (x|y)^2 = \frac{2(y|y)}{n} |R_L|.$$

Corollaire 1.4. ([Eb02] cor. 3.4 p.100)

Sous les hypothèses de la proposition précédente, on a $R_L = \emptyset$ ou R_L engendre $L \otimes \mathbb{R}$.

Corollaire 1.5. ([Eb02] cor. 3.5 p.100)

Sous les hypothèses de la proposition précédente, les composantes irréductibles du sous-réseau de racines L_R de L ont le même nombre de Coxeter h , et $h = \frac{1}{n}|R_L|$.

Par conséquent, on montre facilement que pour $n = 8$, le seul sous-réseau de racines possible pour L est \mathbb{E}_8 , et pour $n = 16$ il y a deux possibilités qui sont $L_R = \mathbb{D}_{16}$, et alors $L = \mathbb{D}_{16}^+$ qui est obtenu à partir de \mathbb{D}_{16} et le code associé au sur-réseau $H = \{[0], [1]\}$ (notations de la partie 1.1.4) ou $L = L_R = 2\mathbb{E}_8$. Enfin, lorsque $n = 24$, on a la proposition suivante, qui se vérifie de façon combinatoire (on teste tous les cas possibles satisfaisant les corollaires précédents).

Proposition 1.9. (*[Eb02], prop. 3.4 p.101*)

Soit L un réseau unimodulaire pair de dimension $n = 24$. Alors L_R est l'un des 24 réseaux suivant :

$$\begin{aligned} & \{0\}, \\ & 24\mathbb{A}_1, 12\mathbb{A}_2, 8\mathbb{A}_3, 6\mathbb{A}_4, 4\mathbb{A}_6, 3\mathbb{A}_8, 2\mathbb{A}_{12}, \mathbb{A}_{24}, \\ & 6\mathbb{D}_4, 4\mathbb{D}_6, 3\mathbb{D}_8, 2\mathbb{D}_{12}, \mathbb{D}_{24}, \\ & 4\mathbb{E}_6, 3\mathbb{E}_8, \\ & 4\mathbb{A}_5 \oplus \mathbb{D}_4, 2\mathbb{A}_7 \oplus 2\mathbb{D}_5, 2\mathbb{A}_9 \oplus \mathbb{D}_6, \mathbb{A}_{15} \oplus \mathbb{D}_9, \\ & \mathbb{E}_8 \oplus \mathbb{D}_{16}, 2\mathbb{E}_7 \oplus \mathbb{D}_{10}, \mathbb{E}_7 \oplus \mathbb{A}_{17}, \mathbb{E}_6 \oplus \mathbb{D}_7 \oplus \mathbb{A}_{11}. \end{aligned}$$

1.4.2 Construction des réseaux de Niemeier

Théorème 1.7. (*Niemeier 1973, voir par exemple [Eb02], thm 3.4 p.106*)

A isomorphisme près, il existe exactement 24 réseaux unimodulaires pairs de dimension 24. Chaque réseau est déterminé de façon unique par son sous-réseau de racines. Les sous-réseaux de racines possibles sont les 24 réseaux de la proposition 1.9.

Définition 1.39. On appelle réseaux de Niemeier les 24 réseaux unimodulaires pairs du théorème 1.7. Celui dont le sous-réseau de racines est trivial est appelé réseau de Leech.

Pour prouver ce théorème, on peut utiliser le corollaire 1.2 pour construire les différents sur-réseaux unimodulaires pairs possibles pour chacune des 24 configurations données des racines (plus précisément 23, le cas $L_R = \{0\}$ se traite à part, voir par exemple [CS98] p.131). On peut montrer dans chaque cas que le sous-groupe totalement isotrope de L_R^*/L_R caractérisant L est unique (à isomorphisme près), ce qui achève l'existence et l'unicité des 24 réseaux unimodulaires pairs de dimension 24. Nous ne le ferons pas, mais renvoyons par exemple à [CS98] chapitre 18, p.429.

Néanmoins, nous allons donner une description des 23 réseaux de Niemeier dont le sous-réseau de racines est non trivial, description tirée de [CS98] chapitre 16, p.406 (mais aussi du chapitre 18, p.429). Pour chacun de ces 23 réseaux, nous allons donner une réalisation concrète de $H = N/N_R$ (suivant les notations "canoniques" données en partie 1.1.4), en écrivant tous les éléments de H , mais aussi en décrivant les groupes d'invariants de N .

Soit N l'un des 23 réseaux de Niemeier dont le sous-réseau de racines n'est pas trivial, et N_R son sous-réseau de racines, et $N_R = N_1 \oplus \dots \oplus N_r$ la décomposition de son sous-réseau de racines en composantes irréductibles. Soit $g \in O(N)$ un automorphisme de N . g induit une permutation des composantes irréductibles N_i (permutation éventuellement triviale, c'est le cas en particulier si les N_i sont tous distincts en tant que réseaux de racines irréductibles), on notera ce groupe $G_2(N)$.

On a $G_2(N) \cong O(N)/G_{01}$ où G_{01} est le sous-groupe distingué de $O(N)$ constitué des automorphismes de N qui induisent la permutation triviale sur les N_i .

Soit $G_0(N)$ le sous-groupe distingué de G_{01} qui consiste en les automorphismes de G_{01} qui laissent invariante chaque classe $\bar{y}_i \in L_i^*/L_i$. Alors le quotient $G_{01}/G_0(N)$ est isomorphe au groupe $G_1(N)$, dont les éléments sont des permutations des différentes classes des L_i^*/L_i .

En particulier, on a $\#O(N) = \#G_2(N)\#G_1(N)\#G_0(N)$.

Passons maintenant à l'étude systématique, réseau par réseau. Les notations sont les suivantes, pour un réseau de Niemeier N dont le sous-réseau N_R de racines s'écrit en composantes irréductibles $N_R = N_1 \oplus \dots \oplus N_r$ (dans cet ordre), on notera $[a_1, \dots, a_r]$ l'élément de $D(N_R)$ tel que $[a_i]$ soit une classe de $D(N_i)$, les $[a_i]$ étant notés suivant les conventions adoptées dans la partie 1.1.4.

Le réseau $N(D_{24})$: On a $\#D(\mathbb{D}_{24}) = 4$, donc on cherche un sous-groupe totalement isotrope de cardinal 2 de $D(\mathbb{D}_{24})$, satisfaisant le corollaire 1.2. Poser

$$H = \{[0], [1]\} \cong \mathbb{Z}/2\mathbb{Z}$$

convient. Le réseau $N(\mathbb{D}_{24})$ est alors celui qui est régulièrement noté \mathbb{D}_{24}^+ (dans [CS98] par exemple), c'est l'unique (à isomorphisme près) sur-réseau pair de \mathbb{D}_{24} .

Les invariants de ce réseau sont $G_2(N) = \{1\}$, $G_1(N) = \{1\}$, $G_0(N) = O(N)$.

Le réseau $N(D_{16} + E_8)$: On a $\#D(\mathbb{D}_{16} \oplus \mathbb{E}_8) = 4$, donc on cherche un sous-groupe totalement isotrope de cardinal 2 de $D(\mathbb{D}_{16} \oplus \mathbb{E}_8)$, satisfaisant le corollaire 1.2. Poser

$$H = \{[0, 0], [1, 0]\} \cong \mathbb{Z}/2\mathbb{Z}$$

convient. Le réseau $N(D_{16} + E_8)$ est alors $\mathbb{D}_{16}^+ \oplus \mathbb{E}_8$, c'est l'unique (à isomorphisme près) sur-réseau pair de $\mathbb{D}_{16} + \mathbb{E}_8$.

Les invariants de ce réseau sont $G_2(N) = \{1\}$, $G_1(N) = \{1\}$, $G_0(N) = O(N)$.

Le réseau $N(3E_8)$: Il est unimodulaire, et donc

$$H = \{[0]\}.$$

Les invariants de ce réseau sont $G_2(N) = \mathcal{S}_3$, $G_1(N) = \{1\}$.

Le réseau $N(A_{24})$: On a $\#D(\mathbb{A}_{24}) = 25$, donc on cherche un sous-groupe totalement isotrope de cardinal 5 de $D(\mathbb{A}_{24})$, satisfaisant le corollaire 1.2. Poser

$$H = \langle [5] \rangle = \{[0], [5], [10], [15], [20]\} \cong \mathbb{Z}/5\mathbb{Z}$$

convient.

Les invariants de ce réseau sont $G_2(N) = \{1\}$, $G_1(N) = \mathbb{Z}/2\mathbb{Z}$ (l'élément trivial et $x \mapsto -x$).

Le réseau $N(2D_{12})$: On a $\#D(2\mathbb{D}_{12}) = 16$, donc on cherche un sous-groupe totalement isotrope de cardinal 4 de $D(2\mathbb{D}_{12})$, satisfaisant le corollaire 1.2. Poser

$$H = \langle [12], [21] \rangle = \{[0, 0], [1, 2], [2, 1], [3, 3]\} \cong (\mathbb{Z}/2\mathbb{Z})^2$$

convient.

Les invariants de ce réseau sont $G_2(N) = \mathbb{Z}/2\mathbb{Z}$ (l'élément trivial et l'échange des deux copies de \mathbb{D}_{12}), $G_1(N) = \{1\}$.

Le réseau $N(A_{17} + E_7)$: On a $\#D(\mathbb{A}_{17} \oplus \mathbb{E}_7) = 36$, donc on cherche un sous-groupe totalement isotrope de cardinal 6 de $D(\mathbb{A}_{17} \oplus \mathbb{E}_7)$, satisfaisant le corollaire 1.2. Poser

$$H = \langle [3, 1] \rangle = \{[0, 0], [3, 1], [6, 0], [9, 1], [12, 0], [15, 1]\} \cong \mathbb{Z}/6\mathbb{Z}$$

convient.

Les invariants de ce réseau sont $G_2(N) = \{1\}$, $G_1(N) = \mathbb{Z}/2\mathbb{Z}$ (l'élément trivial et $x \mapsto -x$).

Le réseau $N(D_{10} + 2E_7)$: On a $\#D(\mathbb{D}_{10} \oplus 2\mathbb{E}_7) = 16$, donc on cherche un sous-groupe totalement isotrope de cardinal 4 de $D(\mathbb{D}_{10} \oplus 2\mathbb{E}_7)$, satisfaisant le corollaire 1.2. Poser

$$H = \langle [1, 1, 0], [3, 0, 1] \rangle = \{[0, 0, 0], [3, 0, 1], [1, 1, 0], [2, 1, 1]\} \cong (\mathbb{Z}/2\mathbb{Z})^2$$

convient.

Les invariants de ce réseau sont $G_2(N) = \mathbb{Z}/2\mathbb{Z}$ (échange des copies de \mathbb{E}_7), $G_1(N) = \{1\}$.

Le réseau $N(A_{15} + D_9)$: On a $\#D(\mathbb{A}_{15} \oplus \mathbb{D}_9) = 64$, donc on cherche un sous-groupe totalement isotrope de cardinal 8 de $D(\mathbb{A}_{15} \oplus \mathbb{D}_9)$, satisfaisant le corollaire 1.2. Poser

$$H = \langle [2, 1] \rangle = \{[0, 0], [2, 1], [4, 2], [6, 3], [8, 0], [10, 1], [12, 2], [14, 3]\} \cong \mathbb{Z}/8\mathbb{Z}$$

convient.

Les invariants de ce réseau sont $G_2(N) = \{1\}$, $G_1(N) = \mathbb{Z}/2\mathbb{Z}$ ($x \mapsto -x$).

Le réseau $N(3D_8)$: On a $\#D(3\mathbb{D}_8) = 64$, donc on cherche un sous-groupe totalement isotrope de cardinal 8 de $D(3\mathbb{D}_8)$, satisfaisant le corollaire 1.2. Poser

$$\begin{aligned} H &= \langle [1, 2, 2], [2, 1, 2], [2, 2, 1] \rangle \\ &= \{[0, 0, 0], [1, 2, 2], [2, 1, 2], [2, 2, 1], [3, 3, 0], [3, 0, 3], [0, 3, 3], [1, 1, 1]\} \cong (\mathbb{Z}/2\mathbb{Z})^3 \end{aligned}$$

convient.

Les invariants de ce réseau sont $G_2(N) = \mathcal{S}_3$ (permutations des copies de \mathbb{D}_8), $G_1(N) = \{1\}$.

Le réseau $N(2A_{12})$: On a $\#D(2\mathbb{A}_{12}) = 169$, donc on cherche un sous-groupe totalement isotrope de cardinal 13 de $D(2\mathbb{A}_{12})$, satisfaisant le corollaire 1.2. Poser

$$\begin{aligned} H &= \langle [1, 5] \rangle \\ &= \{[0, 0], [1, 5], [2, 10], [3, 2], [4, 7], [5, 12], [6, 4], [7, 9], [8, 1], [9, 6], [10, 11], [11, 3], [12, 8]\} \\ &\cong \mathbb{Z}/13\mathbb{Z} \end{aligned}$$

convient.

Les invariants de ce réseau sont $G_2(N) = \mathbb{Z}/2\mathbb{Z}$ (échange des copies de \mathbb{A}_{12}), $G_1(N) = \mathbb{Z}/2\mathbb{Z}$ ($x \mapsto -x$).

Le réseau $N(A_{11} + D_7 + E_6)$: On a $\#D(\mathbb{A}_{11} \oplus \mathbb{D}_7 \oplus \mathbb{E}_6) = 144$, donc on cherche un sous-groupe totalement isotrope de cardinal 12 de $D(\mathbb{A}_{11} \oplus \mathbb{D}_7 \oplus \mathbb{E}_6)$, satisfaisant le corollaire 1.2. Poser

$$\begin{aligned} H &= \langle [1, 1, 1] \rangle \\ &= \left\{ \begin{array}{l} [0, 0, 0], [1, 1, 1], [2, 2, 2], [3, 3, 0], [4, 0, 1], [5, 1, 2], \\ [6, 2, 0], [7, 3, 1], [8, 0, 2], [9, 1, 0], [10, 2, 1], [11, 3, 2] \end{array} \right\} \\ &\cong \mathbb{Z}/12\mathbb{Z} \end{aligned}$$

convient.

Les invariants de ce réseau sont $G_2(N) = \{1\}$, $G_1(N) = \mathbb{Z}/2\mathbb{Z}$ ($x \mapsto -x$).

Le réseau $N(4E_6)$: On a $\#D(4\mathbb{E}_6) = 81$, donc on cherche un sous-groupe totalement isotrope de cardinal 9 de $D(4\mathbb{E}_6)$, satisfaisant le corollaire 1.2. Poser

$$\begin{aligned} H &= \langle [1, 0, 1, 2], [1, 2, 0, 1], [1, 1, 2, 0] \rangle \\ &= \{[0, 0, 0, 0], [1, 0, 1, 2], [1, 2, 0, 1], [1, 1, 2, 0], [2, 0, 2, 1], [2, 1, 0, 2], [2, 2, 1, 0], \\ &\quad [0, 1, 1, 1], [0, 2, 2, 2]\} \\ &\cong (\mathbb{Z}/3\mathbb{Z})^2 \end{aligned}$$

convient.

Les invariants de ce réseau sont $G_2(N) = \mathcal{S}_4$ (permutations des copies de \mathbb{E}_6), $G_1(N) = \mathbb{Z}/2\mathbb{Z}$ ($x \mapsto -x$).

Le réseau $N(2A_9 + D_6)$: On a $\#D(2A_9 \oplus D_6) = 400$, donc on cherche un sous-groupe totalement isotrope de cardinal 20 de $D(2A_9 \oplus D_6)$, satisfaisant le corollaire 1.2. Poser

$$\begin{aligned} H &= \langle [2, 4, 0], [5, 0, 1], [0, 5, 3] \rangle \\ &= \left\{ \begin{array}{ccccc} [0, 0, 0], & [2, 4, 0], & [4, 8, 0], & [6, 2, 0], & [8, 6, 0], \\ [5, 0, 1], & [7, 4, 1], & [9, 8, 1], & [1, 2, 1], & [3, 6, 1], \\ [0, 5, 3], & [2, 9, 3], & [4, 3, 3], & [6, 7, 3], & [8, 1, 3], \\ [5, 5, 2], & [7, 9, 2], & [9, 3, 2], & [1, 7, 2], & [3, 1, 2] \end{array} \right\} \\ &\cong (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/5\mathbb{Z} \end{aligned}$$

convient.

Les invariants de ce réseaux sont $G_2(N) = \mathbb{Z}/2\mathbb{Z}$ (permutations des copies de A_9), $G_1(N) = \mathbb{Z}/2\mathbb{Z}$ ($x \mapsto -x$).

Le réseau $N(4D_6)$: On a $\#D(4D_6) = 16^2$, donc on cherche un sous-groupe totalement isotrope de cardinal 16 de $D(4D_6)$, satisfaisant le corollaire 1.2. Poser

$$\begin{aligned} H &= \langle [0, 1, 2, 3], [1, 3, 2, 0], [1, 2, 0, 3], [1, 0, 3, 2] \rangle \\ &= \left\{ \begin{array}{cccccc} [0, 0, 0, 0], & [0, 2, 3, 1], & [2, 2, 2, 2], & [2, 3, 0, 1], & [1, 2, 0, 3], & [2, 0, 1, 3], \\ [1, 1, 1, 1], & [1, 0, 3, 2], & [3, 0, 2, 1], & [1, 3, 2, 0], & [0, 1, 2, 3], & \\ [3, 1, 0, 2], & [3, 2, 1, 0], & [0, 3, 1, 2], & [3, 3, 3, 3], & [2, 1, 3, 0] & \end{array} \right\} \\ &\cong (\mathbb{Z}/2\mathbb{Z})^4 \end{aligned}$$

convient.

Les invariants de ce réseau sont $G_2(N) = \mathcal{S}_4$ (permutations des copies de D_6), $G_1(N) = \{1\}$.

Le réseau $N(3A_8)$: On a $\#D(3A_8) = 3^6$, donc on cherche un sous-groupe totalement isotrope de cardinal 27 de $D(3A_8)$, satisfaisant le corollaire 1.2. Poser

$$\begin{aligned} H &= \langle [1, 1, 4], [4, 1, 1], [1, 4, 1] \rangle \\ &= \left\{ \begin{array}{ccccccccc} [0, 0, 0], & [1, 1, 4], & [2, 2, 8], & [3, 3, 3], & [4, 4, 7], & [5, 5, 2], & [6, 6, 6], & [7, 7, 1], & [8, 8, 5], \\ [3, 0, 6], & [4, 1, 1], & [5, 2, 5], & [6, 3, 0], & [7, 4, 4], & [8, 5, 8], & [0, 6, 3], & [1, 7, 7], & [2, 8, 2], \\ [6, 0, 3], & [7, 1, 7], & [8, 2, 2], & [0, 3, 6], & [1, 4, 1], & [2, 5, 5], & [3, 6, 0], & [4, 7, 4], & [5, 8, 8] \end{array} \right\} \\ &\cong (\mathbb{Z}/3\mathbb{Z})^3 \end{aligned}$$

convient.

Les invariants de ce réseau sont $G_2(N) = \mathcal{S}_3$ (permutations des copies de A_8), $G_1(N) = \mathbb{Z}/2\mathbb{Z}$ ($x \mapsto -x$).

Le réseau $N(2A_7 + 2D_5)$: On a $\#D(2A_7 \oplus 2D_5) = 32^2$, donc on cherche un sous-groupe totalement isotrope de cardinal 32 de $D(2A_7 \oplus 2D_5)$, satisfaisant le corollaire 1.2. Poser

$$\begin{aligned}
H &= \langle [1, 1, 1, 2], [1, 7, 2, 1] \rangle \\
&= \left\{ \begin{array}{cccc} [0, 0, 0, 0], & [1, 1, 1, 2], & [2, 2, 2, 0], & [3, 3, 3, 2], \\ [4, 4, 0, 0], & [5, 5, 1, 2], & [6, 6, 2, 0], & [7, 7, 3, 2], \\ [2, 0, 3, 3], & [3, 1, 0, 1], & [4, 2, 1, 3], & [5, 3, 2, 1], \\ [6, 4, 3, 3], & [7, 5, 0, 1], & [0, 6, 1, 3], & [1, 7, 2, 1], \\ [4, 0, 2, 2], & [5, 1, 3, 0], & [6, 2, 0, 2], & [7, 3, 1, 0], \\ [0, 4, 2, 2], & [1, 5, 3, 0], & [2, 6, 0, 2], & [3, 7, 1, 0], \\ [6, 0, 1, 1], & [7, 1, 2, 3], & [0, 2, 3, 1], & [1, 3, 0, 3], \\ [2, 4, 1, 1], & [3, 5, 2, 3], & [4, 6, 3, 1], & [5, 7, 0, 3] \end{array} \right\} \\
&\cong (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z})
\end{aligned}$$

convient.

Les invariants de ce réseau sont $G_2(N) = (\mathbb{Z}/2\mathbb{Z})^2$ (permutations indépendantes des copies de A_7 et D_5), $G_1(N) = \mathbb{Z}/2\mathbb{Z}$ ($x \mapsto -x$).

Le réseau $N(4A_6)$: On a $\#D(4A_6) = 49^2$, donc on cherche un sous-groupe totalement isotrope de cardinal 49 de $D(4A_6)$, satisfaisant le corollaire 1.2. Poser

$$\begin{aligned}
H &= \langle [1, 2, 1, 6], [1, 6, 2, 1] \rangle \\
&= \left\{ \begin{array}{cccccc} [0, 0, 0, 0], & [1, 2, 1, 6], & [2, 4, 2, 5], & [3, 6, 3, 4], & [4, 1, 4, 3], & [5, 3, 5, 2], & [6, 5, 6, 1], \\ [1, 6, 2, 1], & [2, 1, 3, 0], & [3, 3, 4, 6], & [4, 5, 5, 5], & [5, 0, 6, 4], & [6, 2, 0, 3], & [0, 4, 1, 2], \\ [2, 5, 4, 2], & [3, 0, 5, 1], & [4, 2, 6, 0], & [5, 4, 0, 6], & [6, 6, 1, 5], & [0, 1, 2, 4], & [1, 3, 3, 3], \\ [3, 4, 6, 3], & [4, 6, 0, 2], & [5, 1, 1, 1], & [6, 3, 2, 0], & [0, 5, 3, 6], & [1, 0, 4, 5], & [2, 2, 5, 4], \\ [4, 3, 1, 4], & [5, 5, 2, 3], & [6, 0, 3, 2], & [0, 2, 4, 1], & [1, 4, 5, 0], & [2, 6, 6, 6], & [3, 1, 0, 5], \\ [5, 2, 3, 5], & [6, 4, 4, 4], & [0, 6, 5, 3], & [1, 1, 6, 2], & [2, 3, 0, 1], & [3, 5, 1, 0], & [4, 0, 2, 6], \\ [6, 1, 5, 6], & [0, 3, 6, 5], & [1, 5, 0, 4], & [2, 0, 1, 3], & [3, 2, 2, 2], & [4, 4, 3, 1], & [5, 6, 4, 0] \end{array} \right\} \\
&\cong (\mathbb{Z}/7\mathbb{Z})^2
\end{aligned}$$

convient.

Les invariants de ce réseau sont $G_2(N) = \mathcal{A}_4$ (permutations paires des copies de A_6 , ce groupe est 2-transitif sur les copies de A_6), $G_1(N) = \mathbb{Z}/2\mathbb{Z}$ ($x \mapsto -x$).

Le réseau $N(4A_5 + D_4)$: On a $\#D(4A_5 \oplus D_4) = 72^2$, donc on cherche un sous-groupe totalement isotrope de cardinal 72 de $D(4A_5 \oplus D_4)$, satisfaisant le corollaire 1.2. Poser

$$\begin{aligned}
H &= \langle [5, 2, 1, 0, 2], [5, 3, 2, 4, 1], [3, 0, 0, 3, 3] \rangle \\
&\cong (\mathbb{Z}/6\mathbb{Z})^2 \times (\mathbb{Z}/2\mathbb{Z})
\end{aligned}$$

convient. La description des éléments de H est donnée en figure 1.5.

Les invariants de ce réseau sont $G_2(N) = \mathcal{S}_4$ (permutations des copies de A_5), $G_1(N) = \mathbb{Z}/2\mathbb{Z}$ ($x \mapsto -x$).

$$\left(\begin{array}{cccccc} [0, 0, 0, 0, 0], & [5, 2, 1, 0, 2], & [4, 4, 2, 0, 0], & [3, 0, 3, 0, 2], & [2, 2, 4, 0, 0], & [1, 4, 5, 0, 2], \\ [5, 3, 2, 4, 1], & [4, 5, 3, 4, 3], & [3, 1, 4, 4, 1], & [2, 3, 5, 4, 3], & [1, 5, 0, 4, 1], & [0, 1, 1, 4, 3], \\ [4, 0, 4, 2, 0], & [3, 2, 5, 2, 2], & [2, 4, 0, 2, 0], & [1, 0, 1, 2, 2], & [0, 2, 2, 2, 0], & [5, 4, 3, 2, 2], \\ [3, 3, 0, 0, 1], & [2, 5, 1, 0, 3], & [1, 1, 2, 0, 1], & [0, 3, 3, 0, 3], & [5, 5, 4, 0, 1], & [4, 1, 5, 0, 3], \\ [2, 0, 2, 4, 0], & [1, 2, 3, 4, 2], & [0, 4, 4, 4, 0], & [5, 0, 5, 4, 2], & [4, 2, 0, 4, 0], & [3, 4, 1, 4, 2], \\ [1, 3, 4, 2, 1], & [0, 5, 5, 2, 3], & [5, 1, 0, 2, 1], & [4, 3, 1, 2, 3], & [3, 5, 2, 2, 1], & [2, 1, 3, 2, 3], \\ [3, 0, 0, 3, 3], & [2, 2, 1, 3, 1], & [1, 4, 2, 3, 3], & [0, 0, 3, 3, 1], & [5, 2, 4, 3, 3], & [4, 4, 5, 3, 1], \\ [2, 3, 2, 1, 2], & [1, 5, 3, 1, 0], & [0, 1, 4, 1, 2], & [5, 3, 5, 1, 0], & [4, 5, 0, 1, 2], & [3, 1, 1, 1, 0], \\ [1, 0, 4, 5, 3], & [0, 2, 5, 5, 1], & [5, 4, 0, 5, 3], & [4, 0, 1, 5, 1], & [3, 2, 2, 5, 3], & [2, 4, 3, 5, 1], \\ [0, 3, 0, 3, 2], & [5, 5, 1, 3, 0], & [4, 1, 2, 3, 2], & [3, 3, 3, 3, 0], & [2, 5, 4, 3, 2], & [1, 1, 5, 3, 0], \\ [5, 0, 2, 1, 3], & [4, 2, 3, 1, 1], & [3, 4, 4, 1, 3], & [2, 0, 5, 1, 1], & [1, 2, 0, 1, 3], & [0, 4, 1, 1, 1], \\ [4, 3, 4, 5, 2], & [3, 5, 5, 5, 0], & [2, 1, 0, 5, 2], & [1, 3, 1, 5, 0], & [0, 5, 2, 5, 2], & [5, 1, 3, 5, 0] \end{array} \right)$$

FIG. 1.5 – Eléments du code H associé au sur-réseau $N(4A_5 + D_4)$ de $4A_5 \oplus \mathbb{D}_4$.

Le réseau $N(6D_4)$: On a $\#D(6\mathbb{D}_4) = 64^2$, donc on cherche un sous-groupe totalement isotrope de cardinal 64 de $D(6\mathbb{D}_4)$, satisfaisant le corollaire 1.2. L'hexacode (partie 1.2.3) convient. On a (avec les notations du chapitre 11 de [CS98]) que

$$\begin{aligned} H &= \langle [2, 2, 2, 2, 0, 0], [0, 0, 2, 2, 2, 2], [1, 1, 1, 1, 0, 0], [0, 0, 1, 1, 1, 1], [2, 1, 2, 1, 2, 1], \\ &\quad [3, 2, 3, 2, 3, 2] \rangle \\ &\cong (\mathbb{Z}/2\mathbb{Z})^6 \end{aligned}$$

convient. La description des éléments de H est donnée en figure 1.6.

$$\left(\begin{array}{cccccc} [2, 2, 2, 2, 0, 0], & [0, 0, 2, 2, 2, 2], & [1, 1, 1, 1, 0, 0], & [0, 0, 1, 1, 1, 1], & [2, 1, 2, 1, 2, 1], \\ [3, 2, 3, 2, 3, 2], & [2, 2, 0, 0, 2, 2], & [3, 3, 3, 3, 0, 0], & [2, 2, 3, 3, 1, 1], & [0, 3, 0, 3, 2, 1], \\ [1, 0, 1, 0, 3, 2], & [1, 1, 3, 3, 2, 2], & [0, 0, 3, 3, 3, 3], & [2, 1, 0, 3, 0, 3], & [3, 2, 1, 0, 1, 0], \\ [1, 1, 0, 0, 1, 1], & [3, 0, 3, 0, 2, 1], & [2, 3, 2, 3, 3, 2], & [2, 1, 3, 0, 3, 0], & [3, 2, 2, 3, 2, 3], \\ [1, 3, 1, 3, 1, 3], & [3, 3, 1, 1, 2, 2], & [2, 2, 1, 1, 3, 3], & [0, 3, 2, 1, 0, 3], & [1, 0, 3, 2, 1, 0], \\ [3, 3, 2, 2, 1, 1], & [1, 2, 1, 2, 2, 1], & [0, 1, 0, 1, 3, 2], & [0, 3, 1, 2, 3, 0], & [1, 0, 0, 1, 2, 3], \\ [3, 1, 3, 1, 1, 3], & [1, 1, 2, 2, 3, 3], & [3, 0, 1, 2, 0, 3], & [2, 3, 0, 1, 1, 0], & [2, 1, 1, 2, 1, 2], \\ [3, 2, 0, 1, 0, 1], & [1, 3, 3, 1, 3, 1], & [3, 0, 2, 1, 3, 0], & [2, 3, 3, 2, 2, 3], & [0, 2, 0, 2, 1, 3], \\ [1, 3, 0, 2, 0, 2], & [3, 3, 0, 0, 3, 3], & [1, 2, 3, 0, 0, 3], & [0, 1, 2, 3, 1, 0], & [0, 3, 3, 0, 1, 2], \\ [1, 0, 2, 3, 0, 1], & [3, 1, 1, 3, 3, 1], & [1, 2, 0, 3, 3, 0], & [0, 1, 1, 0, 2, 3], & [2, 0, 2, 0, 1, 3], \\ [3, 1, 2, 0, 0, 2], & [3, 0, 0, 3, 1, 2], & [2, 3, 1, 0, 0, 1], & [0, 2, 2, 0, 3, 1], & [1, 3, 2, 0, 2, 0], \\ [0, 2, 1, 3, 0, 2], & [1, 2, 2, 1, 1, 2], & [0, 1, 3, 2, 0, 1], & [2, 0, 0, 2, 3, 1], & [3, 1, 0, 2, 2, 0], \\ [2, 0, 3, 1, 0, 2], & [0, 2, 3, 1, 2, 0], & [2, 0, 1, 3, 2, 0], & [0, 0, 0, 0, 0, 0] \end{array} \right)$$

FIG. 1.6 – Eléments du code H associé au sur-réseau $N(6D_4)$ de $6\mathbb{D}_4$.

Les invariants de ce réseau sont $G_2(N) = \mathcal{S}_6$ (permutations des copies de \mathbb{D}_4), $G_1(N) = \mathbb{Z}/3\mathbb{Z}$.

Le réseau $N(6A_4)$: On a $\#D(6A_4) = 125^2$, donc on cherche un sous-groupe totalement isotrope de cardinal 125 de $D(6A_4)$, satisfaisant le corollaire 1.2. Poser

$$H = \langle [1, 4, 1, 0, 1, 4], [1, 1, 0, 1, 4, 4], [1, 0, 1, 4, 4, 1] \rangle \\ \cong (\mathbb{Z}/5\mathbb{Z})^3$$

convient. La description des éléments de H est donnée en figure 1.7.

$$\left\{ \begin{array}{l} [0, 0, 0, 0, 0, 0], [1, 4, 1, 0, 1, 4], [2, 3, 2, 0, 2, 3], [3, 2, 3, 0, 3, 2], [4, 1, 4, 0, 4, 1], \\ [1, 1, 0, 1, 4, 4], [2, 0, 1, 1, 0, 3], [3, 4, 2, 1, 1, 2], [4, 3, 3, 1, 2, 1], [0, 2, 4, 1, 3, 0], \\ [2, 2, 0, 2, 3, 3], [3, 1, 1, 2, 4, 2], [4, 0, 2, 2, 0, 1], [0, 4, 3, 2, 1, 0], [1, 3, 4, 2, 2, 4], \\ [3, 3, 0, 3, 2, 2], [4, 2, 1, 3, 3, 1], [0, 1, 2, 3, 4, 0], [1, 0, 3, 3, 0, 4], [2, 4, 4, 3, 1, 3], \\ [4, 4, 0, 4, 1, 1], [0, 3, 1, 4, 2, 0], [1, 2, 2, 4, 3, 4], [2, 1, 3, 4, 4, 3], [3, 0, 4, 4, 0, 2], \\ [1, 0, 1, 4, 4, 1], [2, 4, 2, 4, 0, 0], [3, 3, 3, 4, 1, 4], [4, 2, 4, 4, 2, 3], [0, 1, 0, 4, 3, 2], \\ [2, 1, 1, 0, 3, 0], [3, 0, 2, 0, 4, 4], [4, 4, 3, 0, 0, 3], [0, 3, 4, 0, 1, 2], [1, 2, 0, 0, 2, 1], \\ [3, 2, 1, 1, 2, 4], [4, 1, 2, 1, 3, 3], [0, 0, 3, 1, 4, 2], [1, 4, 4, 1, 0, 1], [2, 3, 0, 1, 1, 0], \\ [4, 3, 1, 2, 1, 3], [0, 2, 2, 2, 2, 2], [1, 1, 3, 2, 3, 1], [2, 0, 4, 2, 4, 0], [3, 4, 0, 2, 0, 4], \\ [0, 4, 1, 3, 0, 2], [1, 3, 2, 3, 1, 1], [2, 2, 3, 3, 2, 0], [3, 1, 4, 3, 3, 4], [4, 0, 0, 3, 4, 3], \\ [2, 0, 2, 3, 3, 2], [3, 4, 3, 3, 4, 1], [4, 3, 4, 3, 0, 0], [0, 2, 0, 3, 1, 4], [1, 1, 1, 3, 2, 3], \\ [3, 1, 2, 4, 2, 1], [4, 0, 3, 4, 3, 0], [0, 4, 4, 4, 4, 4], [1, 3, 0, 4, 0, 3], [2, 2, 1, 4, 1, 2], \\ [4, 2, 2, 0, 1, 0], [0, 1, 3, 0, 2, 4], [1, 0, 4, 0, 3, 3], [2, 4, 0, 0, 4, 2], [3, 3, 1, 0, 0, 1], \\ [0, 3, 2, 1, 0, 4], [1, 2, 3, 1, 1, 3], [2, 1, 4, 1, 2, 2], [3, 0, 0, 1, 3, 1], [4, 4, 1, 1, 4, 0], \\ [1, 4, 2, 2, 4, 3], [2, 3, 3, 2, 0, 2], [3, 2, 4, 2, 1, 1], [4, 1, 0, 2, 2, 0], [0, 0, 1, 2, 3, 4], \\ [3, 0, 3, 2, 2, 3], [4, 4, 4, 2, 3, 2], [0, 3, 0, 2, 4, 1], [1, 2, 1, 2, 0, 0], [2, 1, 2, 2, 1, 4], \\ [4, 1, 3, 3, 1, 2], [0, 0, 4, 3, 2, 1], [1, 4, 0, 3, 3, 0], [2, 3, 1, 3, 4, 4], [3, 2, 2, 3, 0, 3], \\ [0, 2, 3, 4, 0, 1], [1, 1, 4, 4, 1, 0], [2, 0, 0, 4, 2, 4], [3, 4, 1, 4, 3, 3], [4, 3, 2, 4, 4, 2], \\ [1, 3, 3, 0, 4, 0], [2, 2, 4, 0, 0, 4], [3, 1, 0, 0, 1, 3], [4, 0, 1, 0, 2, 2], [0, 4, 2, 0, 3, 1], \\ [2, 4, 3, 1, 3, 4], [3, 3, 4, 1, 4, 3], [4, 2, 0, 1, 0, 2], [0, 1, 1, 1, 1, 1], [1, 0, 2, 1, 2, 0], \\ [4, 0, 4, 1, 1, 4], [0, 4, 0, 1, 2, 3], [1, 3, 1, 1, 3, 2], [2, 2, 2, 1, 4, 1], [3, 1, 3, 1, 0, 0], \\ [0, 1, 4, 2, 0, 3], [1, 0, 0, 2, 1, 2], [2, 4, 1, 2, 2, 1], [3, 3, 2, 2, 3, 0], [4, 2, 3, 2, 4, 4], \\ [1, 2, 4, 3, 4, 2], [2, 1, 0, 3, 0, 1], [3, 0, 1, 3, 1, 0], [4, 4, 2, 3, 2, 4], [0, 3, 3, 3, 3, 3], \\ [2, 3, 4, 4, 3, 1], [3, 2, 0, 4, 4, 0], [4, 1, 1, 4, 0, 4], [0, 0, 2, 4, 1, 3], [1, 4, 3, 4, 2, 2], \\ [3, 4, 4, 0, 2, 0], [4, 3, 0, 0, 3, 4], [0, 2, 1, 0, 4, 3], [1, 1, 2, 0, 0, 2], [2, 0, 3, 0, 1, 1] \end{array} \right\}$$

FIG. 1.7 – Éléments du code H associé au sur-réseau $N(6A_4)$ de $6A_4$.

Les invariants de ce réseau sont $G_2(N) = PGL_2(\mathbb{F}_5)$ (3-transitif sur les copies de \mathbb{A}_4), $G_1(N) = \mathbb{Z}/2\mathbb{Z}$ ($x \mapsto -x$).

Le réseau $N(8A_3)$: On a $\#D(8A_3) = 256^2$, donc on cherche un sous-groupe totalement isotrope de cardinal 256 de $D(8A_3)$, satisfaisant le corollaire 1.2. L'octacode (voir [FST92] et [HKCSS94] pour une description de ce code) convient. C'est par exemple le code défini comme suit :

$$H = \langle [3, 2, 0, 0, 1, 0, 1, 1], [3, 1, 2, 0, 0, 1, 0, 1], [3, 1, 1, 2, 0, 0, 1, 0], [3, 0, 1, 1, 2, 0, 0, 1] \rangle \\ \cong (\mathbb{Z}/4\mathbb{Z})^4$$

La description des éléments de H est donnée en figure 1.8.

[0, 0, 0, 0, 0, 0, 0, 0],	[3, 0, 1, 1, 2, 0, 0, 1],	[2, 0, 2, 2, 0, 0, 0, 2],	[1, 0, 3, 3, 2, 0, 0, 3],	[3, 1, 1, 2, 0, 0, 1, 0],
[2, 1, 2, 3, 2, 0, 1, 1],	[1, 1, 3, 0, 0, 0, 1, 2],	[0, 1, 0, 1, 2, 0, 1, 3],	[2, 2, 2, 0, 0, 0, 2, 0],	[1, 2, 3, 1, 2, 0, 2, 1],
[0, 2, 0, 2, 0, 0, 2, 2],	[3, 2, 1, 3, 2, 0, 2, 3],	[1, 3, 3, 2, 0, 0, 3, 0],	[0, 3, 0, 3, 2, 0, 3, 1],	[3, 3, 1, 0, 0, 0, 3, 2],
[2, 3, 2, 1, 2, 0, 3, 3],	[3, 1, 2, 0, 0, 1, 0, 1],	[2, 1, 3, 1, 2, 1, 0, 2],	[1, 1, 0, 2, 0, 1, 0, 3],	[0, 1, 1, 3, 2, 1, 0, 0],
[2, 2, 3, 2, 0, 1, 1, 1],	[1, 2, 0, 3, 2, 1, 1, 2],	[0, 2, 1, 0, 0, 1, 1, 3],	[3, 2, 2, 1, 2, 1, 1, 0],	[1, 3, 0, 0, 0, 1, 2, 1],
[0, 3, 1, 1, 2, 1, 2, 2],	[3, 3, 2, 2, 0, 1, 2, 3],	[2, 3, 3, 3, 2, 1, 2, 0],	[0, 0, 1, 2, 0, 1, 3, 1],	[3, 0, 2, 3, 2, 1, 3, 2],
[2, 0, 3, 0, 0, 1, 3, 3],	[1, 0, 0, 1, 2, 1, 3, 0],	[2, 2, 0, 0, 0, 2, 0, 2],	[1, 2, 1, 1, 2, 2, 0, 3],	[0, 2, 2, 2, 0, 2, 0, 0],
[3, 2, 3, 3, 2, 2, 0, 1],	[1, 3, 1, 2, 0, 2, 1, 2],	[0, 3, 2, 3, 2, 2, 1, 3],	[3, 3, 3, 0, 0, 2, 1, 0],	[2, 3, 0, 1, 2, 2, 1, 1],
[0, 0, 2, 0, 0, 2, 2, 2],	[3, 0, 3, 1, 2, 2, 2, 3],	[2, 0, 0, 2, 0, 2, 2, 0],	[1, 0, 1, 3, 2, 2, 2, 1],	[3, 1, 3, 2, 0, 2, 3, 2],
[2, 1, 0, 3, 2, 2, 3, 3],	[1, 1, 1, 0, 0, 2, 3, 0],	[0, 1, 2, 1, 2, 2, 3, 1],	[1, 3, 2, 0, 0, 3, 0, 3],	[0, 3, 3, 1, 2, 3, 0, 0],
[3, 3, 0, 2, 0, 3, 0, 1],	[2, 3, 1, 3, 2, 3, 0, 2],	[0, 0, 3, 2, 0, 3, 1, 3],	[3, 0, 0, 3, 2, 3, 1, 0],	[2, 0, 1, 0, 0, 3, 1, 1],
[1, 0, 2, 1, 2, 3, 1, 2],	[3, 1, 0, 0, 0, 3, 2, 3],	[2, 1, 1, 1, 2, 3, 2, 0],	[1, 1, 2, 2, 0, 3, 2, 1],	[0, 1, 3, 3, 2, 3, 2, 2],
[2, 2, 1, 2, 0, 3, 3, 3],	[1, 2, 2, 3, 2, 3, 3, 0],	[0, 2, 3, 0, 0, 3, 3, 1],	[3, 2, 0, 1, 2, 3, 3, 2],	[3, 2, 0, 0, 1, 0, 1, 1],
[2, 2, 1, 1, 3, 0, 1, 2],	[1, 2, 2, 2, 1, 0, 1, 3],	[0, 2, 3, 3, 3, 0, 1, 0],	[2, 3, 1, 2, 1, 0, 2, 1],	[1, 3, 2, 3, 3, 0, 2, 2],
[0, 3, 3, 0, 1, 0, 2, 3],	[3, 3, 0, 1, 3, 0, 2, 0],	[1, 0, 2, 0, 1, 0, 3, 1],	[0, 0, 3, 1, 3, 0, 3, 2],	[3, 0, 0, 2, 1, 0, 3, 3],
[2, 0, 1, 3, 3, 0, 3, 0],	[0, 1, 3, 2, 1, 0, 0, 1],	[3, 1, 0, 3, 3, 0, 0, 2],	[2, 1, 1, 0, 1, 0, 0, 3],	[1, 1, 2, 1, 3, 0, 0, 0],
[2, 3, 2, 0, 1, 1, 1, 2],	[1, 3, 3, 1, 3, 1, 1, 3],	[0, 3, 0, 2, 1, 1, 1, 0],	[3, 3, 1, 3, 3, 1, 1, 1],	[1, 0, 3, 2, 1, 1, 2, 2],
[0, 0, 0, 3, 3, 1, 2, 3],	[3, 0, 1, 0, 1, 1, 2, 0],	[2, 0, 2, 1, 3, 1, 2, 1],	[0, 1, 0, 0, 1, 1, 3, 2],	[3, 1, 1, 1, 3, 1, 3, 3],
[2, 1, 2, 2, 1, 1, 3, 0],	[1, 1, 3, 3, 3, 1, 3, 1],	[3, 2, 1, 2, 1, 1, 0, 2],	[2, 2, 2, 3, 3, 1, 0, 3],	[2, 2, 3, 0, 1, 1, 0, 0],
[0, 2, 0, 1, 3, 1, 0, 1],	[1, 0, 0, 0, 1, 2, 1, 3],	[0, 0, 1, 1, 3, 2, 1, 0],	[3, 0, 2, 2, 1, 2, 1, 1],	[2, 0, 3, 3, 3, 2, 1, 2],
[0, 1, 1, 2, 1, 2, 2, 3],	[3, 1, 2, 3, 3, 2, 2, 0],	[2, 1, 3, 0, 1, 2, 2, 1],	[1, 1, 0, 1, 3, 2, 2, 2],	[3, 2, 2, 0, 1, 2, 3, 3],
[2, 2, 3, 1, 3, 2, 3, 0],	[1, 2, 0, 2, 1, 2, 3, 1],	[0, 2, 1, 3, 3, 2, 3, 2],	[2, 3, 3, 2, 1, 2, 0, 3],	[1, 3, 0, 3, 3, 2, 0, 0],
[0, 3, 1, 0, 1, 2, 0, 1],	[3, 3, 2, 1, 3, 2, 0, 2],	[0, 1, 2, 0, 1, 3, 1, 0],	[3, 1, 3, 1, 3, 3, 1, 1],	[2, 1, 0, 2, 1, 3, 1, 2],
[1, 1, 1, 3, 3, 3, 1, 3],	[3, 2, 3, 2, 1, 3, 2, 0],	[2, 2, 0, 3, 3, 3, 2, 1],	[1, 2, 1, 0, 1, 3, 2, 2],	[0, 2, 2, 1, 3, 3, 2, 3],
[1, 3, 1, 1, 3, 3, 3, 1],	[0, 3, 2, 2, 1, 3, 3, 2],	[3, 3, 3, 3, 3, 3, 3, 3],	[2, 3, 0, 0, 1, 3, 3, 0],	[1, 0, 1, 2, 1, 3, 0, 0],
[0, 0, 2, 3, 3, 3, 0, 1],	[3, 0, 3, 0, 1, 3, 0, 2],	[2, 0, 0, 1, 3, 3, 0, 3],	[2, 0, 0, 0, 2, 0, 2, 2],	[1, 0, 1, 1, 0, 0, 2, 3],
[0, 0, 2, 2, 2, 0, 2, 0],	[3, 0, 3, 3, 0, 0, 2, 1],	[1, 1, 1, 2, 2, 0, 3, 2],	[0, 1, 2, 3, 0, 0, 3, 3],	[3, 1, 3, 0, 2, 0, 3, 0],
[2, 1, 0, 1, 0, 0, 3, 1],	[0, 2, 2, 0, 2, 0, 0, 2],	[3, 2, 3, 1, 0, 0, 0, 3],	[2, 2, 0, 2, 2, 0, 0, 0],	[1, 2, 1, 3, 0, 0, 0, 1],
[3, 3, 3, 2, 2, 0, 1, 2],	[2, 3, 0, 3, 0, 0, 1, 3],	[1, 3, 1, 0, 2, 0, 1, 0],	[0, 3, 2, 1, 0, 0, 1, 1],	[1, 1, 2, 0, 2, 1, 2, 3],
[0, 1, 3, 1, 0, 1, 2, 0],	[3, 1, 0, 2, 2, 1, 2, 1],	[2, 1, 1, 3, 0, 1, 2, 2],	[0, 2, 3, 2, 2, 1, 3, 3],	[3, 2, 0, 3, 0, 1, 3, 0],
[2, 2, 1, 0, 2, 1, 3, 1],	[1, 2, 2, 1, 0, 1, 3, 2],	[3, 3, 0, 0, 2, 1, 0, 3],	[2, 3, 1, 1, 0, 1, 0, 0],	[1, 3, 2, 2, 2, 1, 0, 1],
[0, 3, 3, 3, 0, 1, 0, 2],	[2, 0, 1, 2, 2, 1, 1, 3],	[1, 0, 2, 3, 0, 1, 1, 0],	[0, 0, 3, 0, 2, 1, 1, 1],	[3, 0, 0, 1, 0, 1, 1, 2],
[0, 2, 0, 0, 2, 2, 2, 0],	[3, 2, 1, 1, 0, 2, 2, 1],	[2, 2, 2, 2, 2, 2, 2, 2],	[1, 2, 3, 3, 0, 2, 2, 3],	[3, 3, 1, 2, 2, 2, 3, 0],
[2, 3, 2, 3, 0, 2, 3, 1],	[1, 3, 3, 0, 2, 2, 3, 2],	[0, 3, 0, 1, 0, 2, 3, 3],	[2, 0, 2, 0, 2, 2, 0, 0],	[1, 0, 3, 1, 0, 2, 0, 1],
[0, 0, 0, 2, 2, 2, 0, 2],	[3, 0, 1, 3, 0, 2, 0, 3],	[1, 1, 3, 2, 2, 2, 1, 0],	[0, 1, 0, 3, 0, 2, 1, 1],	[3, 1, 1, 0, 2, 2, 1, 2],
[2, 1, 2, 1, 0, 2, 1, 3],	[3, 3, 2, 0, 2, 3, 2, 1],	[2, 3, 3, 1, 0, 3, 2, 2],	[1, 3, 0, 2, 2, 3, 2, 3],	[0, 3, 1, 3, 0, 3, 2, 0],
[2, 0, 3, 2, 2, 3, 3, 1],	[1, 0, 0, 3, 0, 3, 3, 2],	[0, 0, 1, 0, 2, 3, 3, 3],	[3, 0, 2, 1, 0, 3, 3, 0],	[1, 1, 0, 0, 2, 3, 0, 1],
[0, 1, 1, 1, 0, 3, 0, 2],	[3, 1, 2, 2, 2, 3, 0, 3],	[2, 1, 3, 3, 0, 3, 0, 0],	[0, 2, 1, 2, 2, 3, 1, 1],	[3, 2, 2, 3, 0, 3, 1, 2],
[2, 2, 3, 0, 2, 3, 1, 3],	[1, 2, 0, 1, 0, 3, 1, 0],	[1, 2, 0, 0, 3, 0, 3, 3],	[0, 2, 1, 1, 1, 0, 3, 0],	[3, 2, 2, 2, 3, 0, 3, 1],
[2, 2, 3, 3, 1, 0, 3, 2],	[0, 3, 1, 2, 3, 0, 0, 3],	[3, 3, 2, 3, 1, 0, 0, 0],	[2, 3, 3, 0, 3, 0, 0, 1],	[1, 3, 0, 1, 1, 0, 0, 2],
[3, 0, 2, 0, 3, 0, 1, 3],	[2, 0, 3, 1, 1, 0, 1, 0],	[1, 0, 0, 2, 3, 0, 1, 1],	[0, 0, 1, 3, 1, 0, 1, 2],	[2, 1, 3, 2, 3, 0, 2, 3],
[1, 1, 0, 3, 1, 0, 2, 0],	[0, 1, 1, 0, 3, 0, 2, 1],	[3, 1, 2, 1, 1, 0, 2, 2],	[0, 3, 2, 0, 3, 1, 3, 0],	[3, 3, 3, 1, 1, 1, 3, 1],
[2, 3, 0, 2, 3, 1, 3, 2],	[1, 3, 1, 3, 1, 1, 3, 3],	[3, 0, 3, 2, 3, 1, 0, 0],	[2, 0, 0, 3, 1, 1, 0, 1],	[1, 0, 1, 0, 3, 1, 0, 2],
[0, 0, 2, 1, 1, 1, 0, 3],	[2, 1, 0, 0, 3, 1, 1, 0],	[1, 1, 1, 1, 1, 1, 1, 1],	[0, 1, 2, 2, 3, 1, 1, 2],	[3, 1, 3, 3, 1, 1, 1, 3],
[1, 2, 1, 2, 3, 1, 2, 0],	[0, 2, 2, 3, 1, 1, 2, 1],	[3, 2, 3, 0, 3, 1, 2, 2],	[2, 2, 0, 1, 1, 1, 2, 3],	[3, 0, 0, 0, 3, 2, 3, 1],
[2, 0, 1, 1, 1, 2, 3, 2],	[1, 0, 2, 2, 3, 2, 3, 3],	[0, 0, 3, 3, 1, 2, 3, 0],	[2, 1, 1, 2, 3, 2, 0, 1],	[1, 1, 2, 3, 1, 2, 0, 2],
[0, 1, 3, 0, 3, 2, 0, 3],	[3, 1, 0, 1, 1, 2, 0, 0],	[1, 2, 2, 0, 3, 2, 1, 1],	[0, 2, 3, 1, 1, 2, 1, 2],	[3, 2, 0, 2, 3, 2, 1, 3],
[2, 2, 1, 3, 1, 2, 1, 0],	[0, 3, 3, 2, 3, 2, 2, 1],	[3, 3, 0, 3, 1, 2, 2, 2],	[2, 3, 1, 0, 3, 2, 2, 3],	[1, 3, 2, 1, 1, 2, 2, 0],
[2, 1, 2, 0, 3, 3, 3, 2],	[1, 1, 3, 1, 1, 3, 3, 3],	[0, 1, 0, 2, 3, 3, 3, 0],	[3, 1, 1, 3, 1, 3, 3, 1],	[1, 2, 3, 2, 3, 3, 0, 2],
[0, 2, 0, 3, 1, 3, 0, 3],	[3, 2, 1, 0, 3, 3, 0, 0],	[2, 2, 2, 1, 1, 3, 0, 1],	[0, 3, 0, 0, 3, 3, 1, 2],	[3, 3, 1, 1, 1, 3, 1, 3],
[2, 3, 2, 2, 3, 3, 1, 0],	[1, 3, 3, 3, 1, 3, 1, 1],	[3, 0, 1, 2, 3, 3, 2, 2],	[2, 0, 2, 3, 1, 3, 2, 3],	[1, 0, 3, 0, 3, 3, 2, 0],
[0, 0, 0, 1, 1, 3, 2, 1]				

FIG. 1.8 – Eléments du code H associé au sur-réseau $N(8A_3)$ de $8A_3$.

Les invariants de ce réseau sont $G_2(N) = 2^3 \cdot PGL_2(\mathbb{F}_7)$ (3-transitif sur les copies de \mathbb{A}_3), $G_1(N) = \mathbb{Z}/2\mathbb{Z}$ ($x \mapsto -x$).

Le réseau $N(12A_2)$: On a $\#D(12A_2) = 3^{12}$, donc on cherche un sous-groupe totalement isotrope de cardinal $3^6 = 729$ de $D(12A_2)$, satisfaisant le corollaire 1.2. Le code de Golay ternaire (voir partie 1.2.4) convient.

On peut donner les invariants de ce réseau, $G_2(N)$ est le groupe de Mathieu M_{12} (5-

transitif sur les copies de \mathbb{A}_2), et $G_1(N) = \mathbb{Z}/2\mathbb{Z}$ ($x \mapsto -x$).

Le réseau $N(24A_1)$: On a $\#D(24\mathbb{A}_1) = 2^{24}$, donc on cherche un sous-groupe totalement isotrope de cardinal $2^{12} = 4096$ de $D(24\mathbb{A}_1)$, satisfaisant le corollaire 1.2. Le code de Golay binaire (voir partie 1.2.4) convient.

On peut donner les invariants de ce réseau, $G_2(N)$ est le groupe de Mathieu M_{24} (5-transitif sur les copies de \mathbb{A}_1), et $G_1(N) = \{1\}$.

Chapitre 2

Produits automorphes

2.1 La fonction Φ_{12} de Borchers

2.1.1 Généralités

L'objet central de cette thèse est une forme modulaire de poids 12, en 26 variables, de caractère déterminant, pour un groupe orthogonal associé à un réseau unimodulaire pair de signature $(2, 26)$. Cette fonction a été construite par R.E. Borchers, dans son article [Bo95], en partie 10, qui est selon ses propres termes le coeur de l'article. Nous noterons cette fonction Φ_{12} .

A isomorphisme près, il existe un unique réseau unimodulaire pair de signature $(2, 26)$, en particulier les 24 réseaux $2U \oplus N(-1)$, où N est l'un des 24 réseaux de Niemeier (et où $N(-1)$ désigne le \mathbb{Z} -module N muni de la forme bilinéaire symétrique $-Q$ pour Q la forme bilinéaire symétrique définie positive associée à N , voir le premier chapitre), sont isomorphes. On notera $II_{2,26}$ l'un de ces réseaux. De même, les 24 groupes orthogonaux $O^+(2U \oplus N(-1))$, où N est l'un des 24 réseaux de Niemeier, sont égaux. On notera ce groupe $O^+(II_{2,26})$. Ainsi Φ_{12} est une forme modulaire de poids 12 pour le groupe $O^+(II_{2,26})$ et le caractère déterminant. Dans la pratique, nous choisirons un réseau de Niemeier N et considérerons Φ_{12} comme une forme modulaire pour le groupe $O^+(2U \oplus N(-1))$.

Dans ce contexte, si l'on fixe un modèle affine associé à un réseau $2U \oplus N(-1)$, où N est l'un des réseaux de Niemeier (voir partie 1.3.1), alors les éléments de $\mathcal{D}^{\text{aff}}(2U \oplus N(-1))$ sont déterminés par 26 coordonnées, c'est dans ce sens que l'on parlera de Φ_{12} comme une forme modulaire en 26 variables (complexes). On remarque aussi que les coordonnées dépendent du choix de N , les 24 réalisations $2U \oplus N(-1)$ de $II_{2,26}$ donnent lieu à 24 systèmes de coordonnées différents pour Φ_{12} .

La fonction Φ_{12} a de nombreuses propriétés. Premièrement, pour une forme en 26 variables, le poids singulier est 12, ainsi Φ_{12} est une forme de poids singulier, ce qui rend le calcul de ses coefficients de Fourier raisonnable. D'autre part, Borchers a montré que Φ_{12} s'annule le long des diviseurs quadratiques rationnels dirigés par des vecteurs de norme -2 , avec multiplicité 1 exactement. Or, comme on l'a vu dans le paragraphe 1.3.4, une forme modulaire pour le groupe $O^+(II_{2,26})$ et le caractère déterminant s'annule nécessairement le long des diviseurs quadratiques rationnels dirigés par des vecteurs de norme -2 . Par

conséquent, Φ_{12} est l'unique forme modulaire anti-invariante de poids 12 pour le groupe $O^+(II_{2,26})$, à un scalaire multiplicatif près : en considérant le quotient d'une autre telle forme par Φ_{12} , on obtient une forme modulaire de poids 0, donc constante. La description exacte des zéros de Φ_{12} est la propriété la plus importante pour les applications que nous ferons dans ce qui suit.

Sous réserve d'existence, nous avons donc caractérisé Φ_{12} comme étant (à scalaire multiplicatif près) l'unique forme modulaire anti-invariante, de poids 12, pour le groupe orthogonal $O^+(II_{2,26})$. Cette forme est de poids singulier et son diviseur est l'union des diviseurs quadratiques rationnels dirigés par des vecteurs de $II_{2,26}$ de norme -2 .

2.1.2 Construction de Φ_{12}

Nous donnerons ici une rapide description de la construction faite par Borcherds dans [Bo95]. Cependant, on trouvera dans l'introduction et le premier paragraphe de [GN02] des informations éclairantes sur les liens qui unissent Φ_{12} et les algèbres de Kac-Moody et leurs généralisations.

Dans son article, Borcherds adopte des conventions différentes des nôtres, à commencer par le choix de la signature. Il considère en fait le réseau $II_{26,2}$ et ses réalisations $2U \oplus N$ avec N un réseau de Niemeier (d'ailleurs il note aussi $U = II_{1,1}$). Ceci a peu d'importance, puisque les groupes $O^+(II_{2,26})$ et $O^+(II_{26,2})$ sont égaux et les domaines associés sont isomorphes. La seule "difficulté" tient donc aux notations.

La manipulation des formes modulaires pour les groupes orthogonaux de Borcherds est aussi légèrement différente. Il définit souvent les formes modulaires comme ayant leurs variables dans le domaine affine associé au réseau (autrement dit il fixe d'abord un réseau L de signature $(n+1, 1)$ et regarde f comme une fonction d'une variable dans $L \otimes \mathbb{C}$, puis considère implicitement le réseau $M = U \oplus L$ lorsqu'il veut parler de forme modulaire).

Considérons maintenant, comme Borcherds, L un réseau unimodulaire pair de signature $(s+1, 1)$ et le réseau $M = L \oplus II_{1,1}$. On choisit un vecteur r_0 de norme strictement négative dans $L \otimes \mathbb{R}$ et on écrit $r > 0$ pour signifier que $(r|r_0) > 0$. Alors on dispose du

Théorème 2.1. ([Bo95], théorème 10.1)

Supposons que $f(\tau) = \sum_n c(n)q^n$ est une forme modulaire presque holomorphe (i.e. méromorphe avec éventuels pôles aux points paraboliques) de poids $-s/2$ pour $SL_2(\mathbb{Z})$ (donc au sens classique), telle que les $c(n)$ soient entiers et que $24|c(0)$ si $s = 0$. Alors il existe un unique vecteur $\rho \in L$ tel que

$$\Phi(v) = e^{-2\pi i(\rho|v)} \prod_{r>0} (1 - e^{-2\pi i(r|v)})^{c(-r|r)/2}$$

soit une forme automorphe méromorphe (en $s+2$ variables) de poids $c(0)/2$ pour $O^+(M)$. Tous les zéros et pôles de Φ se situent le long des diviseurs quadratiques rationnels, et la multiplicité du zéro (ou du pôle lorsque cette multiplicité est strictement négative) de Φ le long du diviseur quadratique rationnel dirigé par le vecteur primitif de norme positive

$r \in M$ est donnée par

$$\sum_{n>0} c(-n^2(r|r)/2).$$

En particulier, lorsque ce nombre est toujours positif ou nul, Φ est holomorphe.

On renvoie à l'article de Borcherds [Bo95] pour la preuve.

L'application fondamentale de ce théorème, toujours suivant Borcherds, est faite en considérant le réseau $II_{25,1}$ (unique réseau unimodulaire pair de signature $(25, 1)$) et la forme $f(\tau) = \frac{1}{\Delta(\tau)}$, où $\Delta(\tau) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{m \geq 0} \tau(m) q^m \in S_{12}(SL_2(\mathbb{Z}))$ avec $q = e^{2\pi i \tau}$ et $\tau(m)$ est la fonction de Ramanujan. En effet, on peut calculer

$$\frac{1}{\Delta(\tau)} = \sum_{n=-1}^{\infty} p_{24}(n+1) q^n,$$

où $p_{24}(n)$ désigne le nombre de partitions de n en parties de 24 couleurs, en particulier, $p_{24}(n)$ est entier, et $p_{24}(0) = 24$. Ainsi, $f(\tau)$ est une forme modulaire presque holomorphe (avec un pôle d'ordre 1 au seul point parabolique de $SL_2(\mathbb{Z})$) à coefficients entiers, de poids -12 . D'après le théorème 2.1, on peut construire une forme Φ_{12} de poids 12, modulaire pour le groupe $O^+(II_{26,2})$, dont on peut montrer (dans la preuve du théorème, voir [Bo95]) qu'elle est anti-invariante. Enfin, d'après la formule du théorème 2.1, la multiplicité du zéro (ou pôle) de Φ_{12} le long du diviseur quadratique rationnel dirigé par le vecteur primitif de norme positive r est donnée par

$$\sum_{n=1}^{\infty} p_{24}(1 - n^2(r|r)/2) = \begin{cases} 1 & \text{si } (r|r) = 2, \\ 0 & \text{sinon.} \end{cases}$$

En particulier, ceci montre bien que Φ_{12} est holomorphe et que Φ_{12} s'annule exactement le long des diviseurs quadratiques rationnels dirigés par des vecteurs de M de norme 2.

Enfin, pour terminer, mentionons que la forme Φ_{12} permet d'obtenir la formule dénominateur de la Fake Monster Lie Algebra, en égalant la formule de type produit du théorème 2.1 et son développement de Fourier (que l'on sait calculer) :

$$\Phi_{12}(v) = e^{-2\pi i(\rho|v)} \prod_{r>0} (1 - e^{2\pi i(r|v)})^{p_{24}(1-r^2/2)} = \sum_{w \in W} \sum_{n>0} \det(w) \tau(n) e^{-2\pi i n(w(\rho)|v)},$$

où W désigne le groupe de Weyl du réseau $II_{25,1}$.

2.2 La méthode de quasi-restriction

Notre but est de trouver des formes modulaires réflexives à partir de restrictions de la fonction Φ_{12} (qui est réflexive), plus précisément, il s'agit de quasi-restrictions de Φ_{12} . L'idée originale de cette méthode est due à Borcherds, dès son article [Bo95], partie 16, exemples 3 et 4. Elle a ensuite été reprise par Borcherds, Katzarkov, Pantev et Shepherd-Barron dans l'article [BKPS98], puis par Kondo dans [Ko99], et enfin par Gritsenko, Hulek et Sankaran dans [GHS07].

La parties suivantes présentent le théorème fondamental de la thèse et décrivent les méthodes que nous utiliserons pour construire des formes réflexives.

2.2.1 Théorème de quasi-restriction

Théorème 2.2. Quasi-restriction ([Bo95], exemples 3 et 4 de la partie 16; [BKPS98], p.185)

Soit N l'un des 24 réseaux de Niemeier. Soit L un sous réseau (quelconque) non nul de N , $M = L^\perp_N$ l'orthogonal de L dans N , et $R_M = \{x \in M \mid x^2 = 2\}$. Soit Φ_{12} la forme modulaire de poids 12 pour le groupe orthogonal $O^+(2U \oplus N(-1))$, et le caractère déterminant (construite par Borcherds et introduite au paragraphe précédent).

Soit la fonction

$$F_L(Z) = \frac{\Phi_{12}(Z)}{\prod_{\{\pm r\} \in R_M} (Z|r)} \Big|_{\mathcal{D}_{2U \oplus L(-1)}^0}.$$

Alors :

(i) F_L est bien définie, et F_L est non identiquement nulle ;

(ii) $F_L \in M_{12 + \frac{1}{2}\#R_M}(\tilde{O}^+(2U \oplus L(-1)), \det)$;

(iii) F_L s'annule le long des diviseurs quadratiques rationnels définis par les projections sur $2U \oplus L(-1)$ des vecteurs $r \in 2U \oplus L(-1)$ tels que $r^2 = -2$, notées l^* , telles que $-2 \leq l^{*2} < 0$.

PREUVE : (i) On a $\Phi_{12}(Z) = 0$ si et seulement si $Z \perp r$, où $r \in 2U \oplus N(-1)$, $r^2 = -2$,

et la multiplicité d'un tel zéro est 1. On peut donc écrire $\Phi_{12}(Z) = \left(\prod_{\{\pm r\} \in R_M} (Z|r) \right) \Phi(Z)$,

où $\Phi(Z)$ est une fonction holomorphe sur $\mathcal{D}^0(2U \oplus N(-1))$ non identiquement nulle. Cette dernière écriture donne immédiatement la bonne définition de F_L .

(ii) L'holomorphie vient de (i). Le poids est bien $12 + \frac{1}{2}\#R_M$, le 12 venant de Φ_{12} , et le $\frac{1}{2}\#R_M$ venant de la linéarité de $(\cdot|\cdot)$ par rapport à la première variable et du nombre de facteurs du produit. Enfin, l'anti-invariance du produit par $\tilde{O}^+(2U \oplus L(-1))$ est donnée par le fait que, pour $L \subset N$, $\tilde{O}(L) \subset \tilde{O}(N)$ (lemme 1.12), ce qui donne ici $\tilde{O}^+(2U \oplus L(-1)) \subset \tilde{O}^+(2U \oplus N(-1)) = O^+(2U \oplus N(-1))$. L'inclusion du premier groupe dans le second s'obtient en prolongeant un élément $\tilde{g} \in \tilde{O}^+(2U \oplus L(-1))$ en $g \in O^+(2U \oplus N(-1))$ en posant $g|_M = id_M$. Ainsi, le numérateur est bien anti-invariant par $\tilde{g} \in \tilde{O}^+(2U \oplus L(-1))$, et le dénominateur est invariant puisqu'un élément du groupe orthogonal laissant $2U \oplus L$ invariant laisse invariant son orthogonal M .

(iii) $F_L(Z)$ s'annule si et seulement si $\Phi_{12}(Z) = 0$, c'est à dire si et seulement si $Z \in \mathcal{D}^0(2U \oplus L(-1)) \cap \mathcal{D}_r^0(2U \oplus N(-1))$, pour $r \in 2U \oplus N(-1)$, $r^2 = -2$. Notons alors $r = l^* + m^*$, avec $l^* \in 2U \oplus L^*(-1)$ et $m^* \in M^*(-1)$ (la décomposition vient de la double inclusion $2U \oplus L(-1) \oplus M(-1) \subset 2U \oplus N(-1) \subset 2U \oplus L^*(-1) \oplus M^*(-1)$). l^* est la projection orthogonale de r sur le réseau $2U \oplus L(-1)$, et ainsi $\mathcal{D}^0(2U \oplus L(-1)) \cap \mathcal{D}_r^0(2U \oplus N(-1)) = \mathcal{D}_{l^*}^0(2U \oplus L(-1))$. Or, $\mathcal{D}_{l^*}^0(2U \oplus L(-1))$ est non vide si et seulement si $-2 \leq l^{*2} < 0$ (partie 1.3.4), ce qui achève la démonstration. \square

2.2.2 Caractérisation des formes réflexives

Fixons les notations de cette partie, soit N un des réseaux de Niemeier, soit $L \neq \{0\}$ un sous-réseau (quelconque) de N , et M un sous-réseau de N tel que $L \perp M$ et $\text{rg}(L \oplus M) = \text{rg}(N)$ (en particulier, M n'est pas nécessairement primitif, et on dispose de la double inclusion $L \oplus M \subset N \subset L^* \oplus M^*$). Afin de simplifier les notations, on considérera que N, L, M sont définis négatifs, c'est à dire que l'on omettra le “(-1)” dans les notations $N(-1), L(-1), M(-1)$, le contexte donnant un sens évident aux nouvelles notations.

Soit F_L la quasi-restriction de la fonction Φ_{12} de Borchers obtenue dans le théorème 2.2.

Nous recherchons à caractériser, parmi les formes modulaires obtenues par la méthode de quasi-restriction, celles qui sont réflexives, afin d'obtenir une méthode systématique pour les classifier.

Dans un premier temps, remarquons que les vecteurs r de norme -2 de $2U \oplus L$ définissent un diviseur quadratique rationnel le long duquel F_L s'annule. En effet, ces vecteurs déterminent un diviseur quadratique rationnel le long duquel Φ_{12} s'annule avec multiplicité 1, ici, la projection de r sur M^* est nulle. Ces diviseurs quadratiques rationnels définis par des -2 -vecteurs de $2U \oplus L$ seront appelés *-2 -diviseurs quadratiques rationnels*. Lorsque F_L s'annule le long d'un diviseur quadratique rationnel dirigé par un vecteur $l^* \notin 2U \oplus L$ obtenu par la projection sur $2U \oplus L^*$ d'une racine de $2U \oplus N$, nous dirons que le diviseur de F_L admet une *composante additionnelle*. Enfin, nous dirons d'un diviseur quadratique rationnel (ou d'une composante additionnelle) qu'il est *réflexif* s'il est dirigé par un vecteur réflexif.

Recherchons des conditions nécessaires pour qu'une forme obtenue par quasi-restriction soit réflexive.

Lemme 2.1. *Soit L un réseau pair. Soit $l^* \in 2U \oplus L^*$, primitif. Alors l^* dirige un diviseur quadratique rationnel réflexif si et seulement si on a $l^{*2} = -\frac{1}{k}$ ou $l^{*2} = -\frac{2}{k}$, où k est l'ordre de \bar{l}^* dans $(2U \oplus L^*)/(2U \oplus L)$. Si l^* n'est pas primitif mais vérifie $l^{*2} = -\frac{1}{k}$ ou $l^{*2} = -\frac{2}{k}$, où k est l'ordre de \bar{l}^* dans $(2U \oplus L^*)/(2U \oplus L)$, alors l^* dirige un diviseur quadratique rationnel réflexif.*

PREUVE : Si $l^{*2} = -\frac{1}{k}$ ou $l^{*2} = -\frac{2}{k}$, alors

$$\forall v \in 2U \oplus L, \sigma_{l^*}(v) = v + 2(l^*|v)kl^* \in 2U \oplus L,$$

ou

$$\forall v \in 2U \oplus L, \sigma_{l^*}(v) = v + (l^*|v)kl^* \in 2U \oplus L,$$

ce qui montre que l^* est réflexif.

Inversement, on suppose l^* primitif. Soit λ le niveau de $2U \oplus L$, alors il existe $a \in \mathbb{N}$, tel que $l^{*2} = -\frac{2a}{\lambda}$ (voir lemme 1.5). Soit k l'ordre de \bar{l}^* dans $(2U \oplus L^*)/(2U \oplus L)$. Alors $l = kl^* \in 2U \oplus L$. Pour avoir $\sigma_{l^*} \in O(2U \oplus L)$, il faut donc

$$\forall v \in 2U \oplus L, \sigma_{l^*}(v) = v + \frac{\lambda(l^*|v)}{a}l^* \in 2U \oplus L,$$

ce qui équivaut à

$$\forall v \in 2U \oplus L, \frac{\lambda(l^*|v)}{a} l^* \in 2U \oplus L.$$

D'après le lemme 1.6, il existe $l_1 \in 2U \oplus L$ tel que $(l^*|l_1) = 1$. Donc pour $v = l_1$, on a $\frac{\lambda}{a} l^* \in L$. Appliquant à nouveau le lemme 1.6, il vient $\frac{\lambda}{a} \in \mathbb{Z}$ puisque $2U \oplus L$ est un réseau entier. On pose $b = \frac{\lambda}{a}$, et on a la relation $bl^* \in 2U \oplus L$, puis $k|b$ puisque k est l'ordre de \bar{l}^* dans $D(2U \oplus L)$, donc il existe $c \in \mathbb{Z}$ tel que $b = kc$. D'où $\lambda = kac$, et donc $l^{*2} = \frac{-2}{kc}$. Enfin, comme $l = kl^* \in 2U \oplus L$, $-\frac{2}{c} = (l|l^*) \in \mathbb{Z}$, et $c = 1$ ou $c = 2$, ce qui correspond à $l^{*2} = -\frac{1}{k}$ ou $l^{*2} = -\frac{2}{k}$. \square

Proposition 2.1. *Si F_L est une forme réflexive, alors L est un sous-réseau primitif de N .*

PREUVE : On utilise la caractérisation du lemme 1.3, L est un sous-réseau primitif de N si et seulement si L est l'orthogonal dans N d'un sous-réseau de N . Supposons par l'absurde que $\forall M \subset N$ sous-réseau, $L \neq M_N^\perp$. Soit $M = L_N^\perp$, c'est un sous-réseau primitif de N . On a

$$L \subsetneq M_N^\perp \subset N.$$

Soit $l \in M_N^\perp \setminus L$, alors $l^2 = -2k$, $k \in \mathbb{N}^*$. Il existe $u \in 2U$, u primitif (prendre $u = e + (k-1)f$ où (e, f) couple hyperbolique de U), tel que $(u+l)^2 = -2$. Des inclusions $2U \oplus L \oplus M \subset 2U \oplus N \subset 2U \oplus L^* \oplus M^*$, on déduit que $u+l = l^* + m^*$ avec $l^* \in 2U \oplus L^*$, $m^* \in M^*$. On a $m^* = 0$, et donc $l^{*2} = -2$. Par construction $l^* = (u+l)$ est primitif (puisque u l'est), d'après le lemme 2.1, l^* définit un diviseur quadratique rationnel si et seulement si $l^{*2} = -\frac{1}{k}$ ou $l^{*2} = -\frac{2}{k}$ avec k l'ordre de \bar{l}^* dans $D(2U \oplus L)$. On doit donc avoir $k = 1$, mais cela signifierait $l^* \in 2U \oplus L$, ce qui est absurde. Donc L est bien primitif. \square

Dans la démonstration de cette proposition, nous avons mis en évidence l'existence, lorsque le sous-réseau L n'est pas primitif, d'un (au moins) diviseur quadratique rationnel dirigé par un vecteur $l^* \in 2U \oplus L^* \setminus 2U \oplus L$ primitif provenant d'une racine r de $2U \oplus N$ dont la projection $m^* = \pi_M(r)$ de r sur M^* est nulle. F_L s'annule le long de ce diviseur, il définit donc une composante additionnelle du diviseur de F_L . On dira que l^* dirige une *composante additionnelle de type 0 du diviseur de F_L* . Ces composantes sont dirigées par des vecteurs non-réflexifs.

On supposera donc désormais, sauf mention explicite du contraire, que L est un sous-réseau primitif de N . Ceci équivaut à dire que $L = (L_N^\perp)_N^\perp$.

On a la suite d'inclusions

$$2U \oplus L \oplus M \subset 2U \oplus N \subset 2U \oplus L^* \oplus M^*,$$

d'où l'on déduit en particulier que

$$(2U \oplus N)/((2U \oplus L) \oplus M) = H \cong N/(L \oplus M) \subset (L^*/L) \oplus (M^*/M).$$

Autrement dit, le sur-réseau N de $L \oplus M$ (ou de façon équivalente le sur-réseau $2U \oplus N$ de $2U \oplus L \oplus M$) est caractérisé par le groupe H , qui est un sous-groupe totalement isotrope de $(L^*/L) \oplus (M^*/M)$. H est le code associé au sur-réseau N de $L \oplus M$, ou de façon équivalente au sur-réseau $2U \oplus N$ de $2U \oplus L \oplus M$ (voir la partie 1.1.5).

On dispose ainsi des projections naturelles suivantes :

$$\begin{aligned} p &: 2U \oplus N \rightarrow H, & p' &: N \rightarrow H, \\ p_L &: H \rightarrow L^*/L = D(L), & p_M &: H \rightarrow M^*/M = D(M), \\ \pi_L &: 2U \oplus N \rightarrow 2U \oplus L^*, & \pi_M &: 2U \oplus N \rightarrow M^*. \end{aligned}$$

On dispose alors du

Lemme 2.2. (*[N79], p.111 et [GHS08-1] partie 3*)

On suppose que L est primitif. Soit $M = L_N^\perp$. Les projections p_L et p_M sont injectives. De plus, si $h_M \in p_M(H)$, alors il existe un unique $h_L \in p_L(H)$ tel que $h_L + h_M \in H$. En d'autres termes, h_L et h_M sont les coordonnées de $h \in H$ dans $D(L) \oplus D(M)$.

Remarque importante 1. Dans le cas plus général où L est un sous-réseau quelconque de N , M un autre sous-réseau quelconque de N , $L \perp M$ et $\text{rg}(L \oplus M) = \text{rg}(N)$, nous pouvons toujours définir les applications p_L et p_M . En effet, soit H le code associé au sur-réseau N de $L \oplus M$, pour tout $h \in H$, les éléments $h_L = p_L(h)$ et $h_M = p_M(h)$ désignent bien les coordonnées de $h = h_L + h_M$ dans $D(L)$ et $D(M)$ respectivement. Mais, sans hypothèses supplémentaires sur L et M , le lemme 2.2 n'est pas valable.

Mais, si l'on suppose que L est primitif, nous disposons alors d'une version affaiblie du lemme 2.2. Soit donc L un sous-réseau primitif de N , et M un sous-réseau quelconque de N tel que $L \perp M$ et $\text{rg}(L \oplus M) = \text{rg}(N)$. La projection p_L n'est plus nécessairement injective, mais p_M est injective. En effet, soient $h, h' \in H$ avec $h \neq h'$, on suppose que $p_M(h) = p_M(h') = h_M$, et on dispose alors des égalités

$$h = h_L + h_M, \quad h' = h'_L + h_M.$$

On en déduit que $h - h' = h_L - h'_L \in H \setminus \{0\}$, ce qui signifie qu'il existe $l' \in (N \setminus L) \cap (L \otimes \mathbb{Q})$ et $k \in \mathbb{N}$, $k \geq 2$, tels que $\bar{l}' = h_L - h'_L$ et $kl' \in L$ mais $l' \notin L$, ce qui contredit la primitivité de L . Ainsi, p_M est injective, et pour tout $d_M \in p_M(H)$, il existe un unique $h_L \in p_L(H)$ tel que $h_L + h_M \in H$.

Les propositions suivantes lient les composantes du diviseur de F_L aux images de H par les projections p_L et p_M .

Lemme 2.3. *Sous les hypothèses précédentes (L primitif et $M = L_N^\perp$), toute composante additionnelle du diviseur de F_L est déterminée par $l^* \in 2U \oplus L^*$ avec $-2 < l^{*2} < 0$. On pose $h_L = \bar{l}^*$ où \bar{l}^* est la classe de l^* dans $D(2U \oplus L)$, et soit h_M associé à h_L suivant la correspondance du lemme 2.2. Alors h_M a un représentant m^* dans M^* de norme vérifiant $-2 < m^{*2} < 0$.*

PREUVE : Si l^* dirige une composante additionnelle du diviseur de F_L , alors il existe $r \in 2U \oplus N$ et $m^* \in M^*$, tels que $r = l^* + m^*$, et $l^* \notin 2U \oplus L$. De plus, d'après le théorème 2.2, on a $-2 \leq l^{*2} < 0$. Plus précisément, $l^{*2} \neq -2$, sinon on aurait $m^* = 0$ puis $l^* \perp M$ mais $l^* \notin 2U \oplus L$, ce qui est absurde puisque $L = M_N^\perp$. Ainsi, $-2 < m^{*2} < 0$. On a ensuite $\bar{l}^* \in p_L(H)$, $\bar{m}^* \in p_M(H)$, et $\bar{l}^* + \bar{m}^* \in H$, ce qui justifie l'écriture $h_L = \bar{l}^*$ et le fait que m^* est un représentant de h_M (associé à h_L via la correspondance du lemme 2.2). Comme $-2 < m^{*2} < 0$, on a le résultat annoncé. \square

Proposition 2.2. *Sous les hypothèses précédentes (L primitif et $M = L_N^\perp$), pour tout $h_M \in p_M(H)$ admettant (dans M^*) un représentant m^* dont la norme vérifie $-2 < m^{*2} < 0$, il existe $l^* \in 2U \oplus L^*$ avec $-2 < l^{*2} < 0$ tel que $\bar{l}^* = h_L$, où \bar{l}^* est la classe de l^* dans $D(2U \oplus L)$ et h_L est associé à h_M suivant la correspondance du lemme 2.2. Ce l^* dirige un diviseur quadratique rationnel qui est une composante additionnelle du diviseur de F_L .*

PREUVE : Soit $h_M \in p_M(H)$ admettant dans $D(M)$ un représentant m^* de norme $-2 < m^{*2} < 0$. D'après le lemme 2.2, il existe un unique $h_L \in p_L(H)$ tel que $h_L + h_M \in H$, et donc, par surjectivité de p' , il existe $r_1 \in N$ tel que $p'(r_1) = h_L + h_M$. Soit alors $m_1^* = \pi_M(r_1)$, par hypothèse, il existe $m_1 \in M \subset N$ tel que $m_1^* + m_1 = m^*$, avec $-2 < m^{*2} < 0$. Alors, $r_2 = r_1 + m$ vérifie $r_2 \in N$, $p'(r_2) = h_L + h_M$, $r_2^2 \in 2\mathbb{Z}$. Ainsi, il existe $u \in 2U$ tel que $r = u + r_2 \in 2U \oplus N$ et $r^2 = -2$ et $p(r) = h_L + h_M$. Enfin, $l^* = \pi_L(r)$ vérifie $-2 < l^{*2} < 0$ (car $-2 < m^{*2} < 0$ et $r = l^* + m^*$) et dirige donc un diviseur quadratique rationnel, ce qui prouve la proposition. \square

Cette dernière proposition et le lemme précédent permettent donc de caractériser les composantes additionnelles du diviseur de F_L . F_L s'annule le long des diviseurs quadratiques rationnels dirigés par des vecteurs primitifs $l^* \in 2U \oplus L^*$ de norme $-2 < l^{*2} < 0$ provenant de racines $r \in 2U \oplus N$ dont la projection m^* sur M^* est non nulle et vérifie $-2 < m^{*2} < 0$. On dira alors que l^* dirige une *composante additionnelle de type 1 du diviseur de F_L* . Ces composantes additionnelles peuvent éventuellement coïncider avec des -2 -diviseurs quadratiques rationnels.

Ainsi, dans le cas général, les zéros de F_L sont les -2 -diviseurs quadratiques rationnels d'une part, avec multiplicité 1, les composantes additionnelles de type 0 (si et seulement si L n'est pas primitif, et alors la forme n'est pas réflexive), avec multiplicité 1, et les composantes additionnelles de type 1 (ces composantes peuvent ne pas être réflexives, il faut vérifier. Elles peuvent aussi coïncider avec des -2 -diviseurs quadratiques rationnels, dans ce cas elles en augmentent la multiplicité), avec une multiplicité à déterminer.

Théorème 2.3. *Soient N un réseau de Niemeier, L un sous-réseau non nul quelconque de N , et $M = L_N^\perp$ son orthogonal dans N . Alors la quasi-restriction associée au réseau L , F_L , est réflexive si et seulement si L est un sous-réseau primitif de N et si pour tout $h_M \in p_M(H)$ admettant un représentant m^* de norme $-2 < m^{*2} < 0$, on a $m^{*2} = \frac{1}{k} - 2$ ou $m^{*2} = \frac{2}{k} - 2$, où k est l'ordre dans $D(2U \oplus L)$ de h_L associé à h_M suivant la correspondance du lemme 2.2.*

PREUVE : On suppose que L est primitif (i.e. $L = M_N^\perp$) et que pour tout $h_M \in p_M(H)$ admettant un représentant m^* de norme $-2 < m^{*2} < 0$, $m^{*2} = \frac{1}{k} - 2$ ou $m^{*2} = \frac{2}{k} - 2$, où k est l'ordre dans $D(2U \oplus L)$ de h_L associé à h_M suivant la correspondance du lemme 2.2. Il s'agit de contrôler les diviseurs additionnels, puisque les -2 -diviseurs quadratiques rationnels sont réflexifs. D'après le lemme 2.3 une composante additionnelle dirigée par $l^* \in 2U \oplus L$, $-2 \leq l^{*2} < 0$, du diviseur de F_L est déterminée par h_M admettant un représentant m^* de norme $-2 < m^{*2} < 0$. D'après les hypothèses, on a plus précisément $m^{*2} = \frac{1}{k} - 2$ ou $m^{*2} = \frac{2}{k} - 2$, ce qui implique que l^* est de norme $l^{*2} = -\frac{1}{k}$ ou $-\frac{2}{k}$, et en vertu du lemme 2.1, la composante additionnelle est réflexive, et donc F_L est bien une

forme réflexive.

Si L n'est pas primitif (i.e. $L \neq M_N^\perp$), alors la forme ne peut pas être réflexive d'après la proposition 2.1. On supposera donc que $L = M_N^\perp$. S'il existe $h_M \in p_M(H)$ admettant un représentant m^* de norme $-2 < m^{*2} < 0$ mais ne vérifiant ni $m^{*2} = \frac{1}{k} - 2$ ni $m^{*2} = \frac{2}{k} - 2$, où k est l'ordre dans $D(2U \oplus L)$ de h_L associé à h_M suivant la correspondance du lemme 2.2, alors il existe $l^* \in 2U \oplus L^*$ qui dirige un diviseur quadratique rationnel (proposition 2.2), avec $l^{*2} \neq -\frac{1}{k}$ et $-\frac{2}{k}$, où k est l'ordre de \bar{l}^* dans $D(2U \oplus L)$, donc d'après le lemme 2.1, la forme F_L n'est pas réflexive. \square

Remarque importante 2. Replaçons nous dans le cas plus général où L est un sous-réseau primitif de N , et M un sous-réseau quelconque de N tel que $L \perp M$ et $\text{rg}(L \oplus M) = \text{rg}(N)$. Nous avons vu que la conclusion du lemme 2.2 restait valable à l'exception de l'injectivité de p_L .

Avec ces hypothèses, le lemme 2.3 est légèrement modifié, il n'y a plus unicité de l'élément h_M associé à h_L . Mais nous pouvons alors affirmer qu'il existe un élément $h_M \in p_M(H)$ associé à h_L , admettant un représentant m^* de norme vérifiant $-2 < m^{*2} < 0$.

Les proposition 2.2 et théorème 2.3 restent valables sans aucune modification d'énoncé (mais la preuve se trouve modifiée légèrement suite aux modifications des lemmes 2.2 et 2.3).

2.2.3 Algorithme de détermination des formes modulaires réflexives

Nous sommes maintenant en mesure de décrire un "algorithme" pour déterminer, pour un sous-réseau donné L d'un réseau de Niemeier N , le poids et les diviseurs (comptés avec multiplicité et classés suivant leur $\tilde{O}^+(2U \oplus L)$ -orbite) de la forme F_L obtenue par quasi-restriction.

1. **Choix du plongement.** Soit N l'un des 24 réseaux de Niemeier. On choisit L un réseau, et j un plongement de L dans N . La forme F_L ne dépend pas que de L , mais aussi du choix de j , tous les plongements ne sont pas équivalents.

2. **Calcul de H , F_L et autres caractéristiques.** On calcule L_N^\perp , le code H associé au sur-réseau N de $L \oplus L_N^\perp$, et les projections p_L et $p_{L_N^\perp}$. On peut déjà vérifier que L est primitif (sinon la forme n'est pas réflexive, mais on peut continuer le calcul des caractéristiques de F_L). Lorsque le réseau L est une composante orthogonale du sous-réseau de racines d'un réseau de Niemeier et que M est le complément orthogonal de ce sous-réseau de racines (en particulier $L \perp M$, $\text{rg}(L \oplus M) = \text{rg}(N)$ et M est un réseau de racines), le calcul de H et des projections p_L et p_M est fait dans la partie 1.4.2.

On peut appliquer le théorème 2.2 pour obtenir F_L de poids k .

3. **Recherche des composantes du diviseur de F_L .** Les -2 -vecteurs de $2U \oplus L$ dirigent des -2 -diviseurs quadratiques le long desquels la forme F_L s'annule, avec multiplicité un. On recherche les diviseurs additionnels. Si L n'est pas primitif, alors il faut rechercher les composantes additionnelles de type 0 (données par les éléments de $H \cap L^*$). Dans tous les cas, il faut rechercher les composantes additionnelles de type 1, mais les

propositions et lemmes de la partie précédente n'étant valables que pour des sous-réseaux primitifs L et des sous-réseaux $M \subset N$ tels que $L \perp M$ et $\text{rg}(L \oplus M) = \text{rg}(N)$, nous ne donnerons une méthode systématique que pour ces réseaux (les seuls intéressants pour la recherche de formes réflexives, dans les autres cas, il faut faire la recherche "à la main", c'est à dire en utilisant pour tous les éléments $h \in H$, la décomposition en coordonnées h_L et h_M , et vérifier les différentes propriétés des éléments h_L et h_M). Il s'agit donc de calculer $p_M(H)$, et d'en rechercher des représentants (dans M^*) de norme maximale (n'oublions pas que M^* est défini négatif). On utilise alors les remarques importantes 1 et 2 de la partie 2.2.2 et le théorème 2.3 pour savoir si la forme est réflexive ou non (le théorème 2.3 permet de calculer tous les diviseurs de F_L , réflexifs ou non).

4. Calcul de la multiplicité de chaque composante du diviseur de F_L . Il s'agit maintenant, pour chaque composante additionnelle dirigée par $l^* \in 2U \oplus L^*$ (réflexive ou non), d'en calculer la multiplicité. Chaque $r \in 2U \oplus N$ de norme $r^2 = -2$ dirigeant une composante de multiplicité 1 du diviseur de Φ_{12} , la multiplicité de la composante dirigée par l^* dans le diviseur de F_L est donc égale au nombre de racines $r \in 2U \oplus N$ dont la projection sur $2U \oplus L^*$ est exactement l^* . Il s'agit donc du nombre de vecteurs $m^* \in M^*$ tels que la classe $\overline{m^*}$ de m^* dans $D(M)$ soit h_M (où h_M est associé à h_L la classe de l^* dans $D(2U \oplus L)$ via la correspondance du lemme 2.2 et la remarque importante 1), et dont la norme est $-2 - l^{*2}$.

5. Classification des orbites de chaque composante à l'aide du critère d'Eichler. Nous connaissons maintenant les vecteurs l^* qui dirigent les différentes composantes du diviseur de F_L . Plus précisément, nous connaissons la classe $\overline{l^*}$ dans $D(2U \oplus L)$ et la norme de l^* . Il est donc naturel de classifier les orbites des composantes additionnelles suivant le critère d'Eichler (Théorème 1.6). La classe $\overline{l^*}$ admet au moins un représentant primitif dans $2U \oplus L^*$ (lemme 1.8). Si on note k son ordre dans $D(2U \oplus L)$, le lemme 1.7 assure que le vecteur $l = kl^* \in 2U \oplus L$ est primitif et d'après le critère d'Eichler (théorème 1.6) nous disposons de l'orbite caractérisée par $l^2 = k^2 l^{*2}$ et $l/\text{div}(l) \equiv l^* \pmod{2U \oplus L}$, notée $H_{k^2 l^{*2}}(\overline{l^*})$. Ensuite il faut vérifier s'il existe ou non des représentants non-primitifs de la classe $\overline{l^*}$ dans $2U \oplus L^*$, ce qui peut être déterminé par le lemme 1.9. Soit donc l'^* un vecteur primitif de $2U \oplus L^*$ et $d \in \mathbb{N}^*$, $d > 1$ tel que la classe $\overline{dl'^*}$ soit égale à $\overline{l^*}$ (voir la démonstration du lemme 1.9). On peut appliquer au vecteur l'^* les lemme 1.7 et théorème 1.6 pour classifier la nouvelle orbite ainsi obtenue (il existe alors autant d'orbites que d'entiers $d \in \mathbb{N}^*$ tels que d^2 divise a où $l^{*2} = -\frac{2a}{\lambda}$, λ étant le niveau de L (notations du lemme 1.9)).

Chapitre 3

Classification des formes modulaires réflexives obtenues par quasi-restriction, première approche

3.1 Formes modulaires strictement -2 -réflexives

3.1.1 Condition suffisante

Reprenons les notations de la partie précédente, soit N un des réseaux de Niemeier, soit $L \neq \{0\}$ un sous-réseau (quelconque) de N , et M un sous-réseau de N tel que $L \perp M$ et $\text{rg}(L \oplus M) = \text{rg}(N)$. Afin de simplifier les notations, on considérera que N, L, M sont définis négatifs, c'est à dire qu'on omettra le " (-1) " dans les notations $N(-1), L(-1), M(-1)$.

Soit F_L la quasi-restriction de la fonction Φ_{12} de Borchers obtenue dans le théorème 2.2.

Intéressons-nous maintenant aux formes modulaires F_L qui n'ont pas de diviseur additionnel. Ce sont les formes "les plus simples" que l'on peut obtenir par quasi-restriction, et elles sont, dans un certain sens, proche de Φ_{12} , puisque comme elle leur diviseur est la réunion des diviseurs quadratiques rationnels dirigés par des -2 vecteurs, avec multiplicité 1. Par contre, elles ne peuvent pas être de poids singulier (puisque la quasi-restriction augmente le poids mais diminue la dimension).

Définition 3.1. Soit F une forme modulaire pour Γ un sous-groupe de $O^+(2U \oplus L)$ contenant $\tilde{O}^+(2U \oplus L)$, où L est un réseau défini négatif.

On appelle F une forme modulaire strictement -2 -réflexive si son diviseur coïncide avec l'union de tous les -2 -diviseurs quadratiques rationnels, et si la multiplicité de chaque composante est 1.

On appelle F une forme modulaire -2 -réflexive si son diviseur est une union de -2 -diviseurs quadratiques rationnels, la multiplicité de chaque composante étant quelconque (en particulier elle peut être nulle).

Proposition 3.1. *Soit L un sous-réseau primitif de N et F_L la forme obtenue par quasi-restriction. Soit \bar{x} une classe non nulle de $D(L)$ admettant un représentant $l^* \in L^*$ de norme vérifiant $-2 \leq l^{*2} < 0$. Soit $l_1^* \in 2U \oplus L^*$ un représentant de la classe \bar{x} . Alors l_1^* dirige une composante additionnelle du diviseur de F_L si et seulement s'il existe un vecteur $m^* \in M^*$ tel que $l^* + m^*$ est une racine de N .*

En particulier, lorsque L est une composante orthogonale du sous-réseau de racines de N (voir la définition 1.18), il n'existe pas de composante additionnelle du diviseur de F_L dirigée par l^ .*

PREUVE : D'après le lemme 2.3, la proposition 2.2 et la remarque importante 1, F_L admet un diviseur additionnel dirigé par l_1^* si et seulement s'il existe un élément $h_M \in p_M(H)$ admettant un représentant de norme comprise entre -2 et 0 strictement tel que $\bar{l}_1^* + h_M \in H$. On suppose que F_L admet un diviseur additionnel dirigé par l_1^* . Soit donc $h_M \in p_M(H)$ associé à $h_L = \bar{l}^*$ par la correspondance du lemme 2.2 (il peut y avoir plusieurs possibilités pour h_M d'après la remarque importante 1), et m^* un représentant de h_M dans M^* tel que $-2 < m^{*2} < 0$. h_M étant non nul, h_L est aussi non nul (p_M étant injective). On peut aussi écrire $l^* = l_1^* + l_1$, avec $l_1 \in 2U \oplus L$ puisque $\bar{l}^* = \bar{l}_1^* = \bar{x}$. Ainsi l'élément $r = l^* + m^* = l_1 + l_1^* + m^* \in 2U \oplus N$ du fait que $\bar{l}_1^* + \bar{m}^* \in H$ et que $l_1 \in 2U \oplus L \subset 2U \oplus N$, et $r \in L^* \oplus M^*$. Donc $r \in N$ et vérifie $-4 < l^{*2} + m^{*2} = r^2 < 0$, donc nécessairement, $r^2 = -2$, ce qui montre que $l^* + m^*$ est une racine de N .

Inversement, on suppose que $l^* + m^*$ est une racine de N . On déduit que $l_1^* + m^*$ est une racine de $2U \oplus N$, puisque $l_1^* + m^* = -l_1 + l^* + m^* \in 2U \oplus N$ (où on a posé $l^* = l_1 + l_1^*$ avec $l_1 \in 2U \oplus L \subset 2U \oplus N$) et que $(l_1^* + m^*)^2 = -2$. Alors d'après le théorème 2.2 l_1^* dirige une composante additionnelle (de type 1).

Enfin, si L est une composante orthogonale du sous-réseau de racines de N , les conditions $l^* + m^*$ est une racine de N et $\bar{l}^* \neq 0$ sont impossibles à réaliser simultanément, puisque toute racine de N est racine du sous-réseau de racines de N , et donc se trouve soit dans L soit dans M . Il n'y a donc pas de composante additionnelle dirigée par l_1^* au diviseur de F_L . □

Proposition 3.2. *Soit L un sous-réseau de N qui est une composante orthogonale du sous-réseau de racines de N . On suppose de plus que L est primitif. On suppose enfin que pour toute classe non nulle $\bar{x} \in D(L) = L^*/L$, il existe $v \in L^*$, v primitif, tel que $-2 \leq v^2 < 0$ et $\bar{v} = \bar{x}$. Alors la forme F_L obtenue par quasi-restriction est une forme strictement -2 -réflexive.*

PREUVE : C'est une application immédiate de la proposition précédente dans le cas où L est une composante orthogonale du sous-réseau de racines de N . Il n'y a pas de composante additionnelle au diviseur de F_L , la forme est bien strictement -2 -réflexive. □

3.1.2 Classification des formes modulaires strictement -2 -réflexives

Dans ce paragraphe, nous nous intéressons à la recherche des formes modulaires strictement -2 -réflexives obtenues par quasi-restriction. A partir de quels types de réseaux L peut-on les obtenir, et peut-on les trouver toutes?

Dans un premier temps, nous allons supposer que N est un réseau de Niemeier différent du réseau de Leech. Nous allons, sous ces hypothèses, chercher des conditions nécessaires sur L pour que F_L puisse être une forme modulaire strictement -2 -réflexive, puis nous donnerons une liste de telles formes.

Proposition 3.3. *Soit N un réseau de Niemeier qui n'est pas le réseau de Leech. Soit F_L une forme modulaire strictement -2 -réflexive. Soit L_R le sous-réseau de racines de L . Alors $\text{rg}(L_R) = \text{rg}(L)$ et L_R est une composante orthogonale du sous-réseau de racines d'un réseau de Niemeier.*

PREUVE : • Soit N_R le sous-réseau de racines du réseau de Niemeier N , $N_R = N_1 \oplus \dots \oplus N_r$, où N_i , $1 \leq i \leq r$, sont des sous-réseaux de racines irréductibles. Comme L_R est le sous-réseau de racines de L , et comme N est un réseau de Niemeier, on a $L_R \subset N_R$. Si $L_R = \{0\}$, alors L_R est une composante orthogonale (nulle) du sous-réseau de racines de N . Sinon, on peut écrire $L_R = L_{i_1} \oplus \dots \oplus L_{i_s}$ avec $1 \leq s \leq r$, $\forall j \in \llbracket 1, s \rrbracket, i_j \in \llbracket 1, r \rrbracket$, et $\forall j \in \llbracket 1, s \rrbracket, L_{i_j} \subset N_{i_j}, L_{i_j} \neq \{0\}$. Soit $\tilde{L} = N_{i_1} \oplus \dots \oplus N_{i_s}$, \tilde{L} est une composante orthogonale (non nulle) du réseau N_R . $\forall j \in \llbracket 1, s \rrbracket$, soit $M_{i_j} = L_{i_j}^\perp$. Alors on a la situation suivante :

$$L = L_{i_1} \oplus \dots \oplus L_{i_s} \subset \tilde{L} = N_{i_1} \oplus \dots \oplus N_{i_s},$$

$$\forall j \in \llbracket 1, s \rrbracket, L_{i_j} \oplus M_{i_j} \subset N_{i_j}, \quad L_{i_j} \perp M_{i_j}.$$

S'il existe $j \in \llbracket 1, s \rrbracket$ tel que $M_{i_j} \neq \{0\}$, alors, soit $r \in N_{i_j}$ tel que $r^2 = -2$. Il est possible de choisir $r \in N_{i_j}$ de sorte que l'on puisse écrire $r = l^* + m^*$, avec $l^* \in L_{i_j}^* \subset 2U \oplus L^*$, et $m^* \in M_{i_j}^*$ tel que $m^* \neq 0$. Sinon, on aurait une partition non-triviale de l'ensemble des racines de N_{i_j} , $R_{N_{i_j}} = R_{L_{i_j}} \sqcup R_{M_{i_j}}$, ce qui contredirait le caractère irréductible du réseau de racines N_{i_j} . Ainsi $l^{*2} \neq -2$ (et donc $l^* \notin 2U \oplus L$), l^* dirige une composante additionnelle (de type 1) du diviseur de F_L . Donc nécessairement, $L_R = \tilde{L}$, L_R est bien une composante orthogonale de N_R .

• Si $\text{rg}(L_R) \neq \text{rg}(L)$, alors $L_{R\tilde{L}}^\perp \neq \{0\}$, et on a, en posant $M = L_N^\perp$,

$$L_R \oplus L_{R\tilde{L}}^\perp \oplus M \subset N \subset L_R^* \oplus (L_{R\tilde{L}}^\perp)^* \oplus M^*.$$

D'après ce qui précède, $L_R = \bigoplus_{j=1}^s N_{i_j}$. Soit $k \notin \{i_1, \dots, i_s\}$, et $v \in N_k$, $v^2 = -2$. Alors on peut écrire

$$v = l_1^* + l^* + m^*, \quad l_1^* \in L_R^*, \quad l^* \in (L_{R\tilde{L}}^\perp)^*, \quad m^* \in M^*, \quad (l_1^* | l_1) = (l_1^* | m^*) = (l^* | m^*) = 0.$$

De plus, $l_1^* = 0$, car on a choisi v dans N_k et $N_k \perp L_R$. On peut choisir k et v tel que $v^2 = -2$ pour avoir l^* non nul. Sinon, pour tout $v \in \bigoplus_{k \in \llbracket 1, r \rrbracket \setminus \{i_1, \dots, i_s\}} N_k$ tel que $v^2 = -2$, on aurait $v \perp (L_{R\tilde{L}}^\perp)^*$, donc $(L_{R\tilde{L}}^\perp)^* \perp \bigoplus_{k \in \llbracket 1, r \rrbracket \setminus \{i_1, \dots, i_s\}} N_k \oplus L_R = N_R$, donc $(L_{R\tilde{L}}^\perp)^* = \{0\}$, et donc $L_{R\tilde{L}}^\perp = \{0\}$, ce qui est absurde. Ainsi, $-2 \leq l^{*2} < 0$. Si $l^{*2} \neq -2$ il dirige une composante additionnelle de type 1 du diviseur de F_L , et si $l^{*2} = -2$, il dirige une composante additionnelle de type 0 du diviseur de F_L (et on déduit que L n'est pas l'orthogonal de M). \square

Proposition 3.4. *Soit N l'un des réseaux de Niemeier (différent du réseau de Leech), et L un sous-réseau de N , de sous-réseau de racines L_R . On suppose que $\text{rg}(L_R) = \text{rg}(L)$. Si F_{L_R} est une forme modulaire s'annulant le long d'un diviseur quadratique rationnel de type 1, alors F_L s'annule aussi le long d'un diviseur quadratique rationnel de type 1.*

PREUVE : Soit $l^* \in 2U \oplus L_R^*$ primitif dirigeant un diviseur quadratique rationnel de type 1 le long duquel F_{L_R} s'annule. Alors il existe $r \in 2U \oplus N$ et $m^* \in (L_{R_N}^\perp)^*$ tels que $r = l^* + m^*$. On a de plus $-2 < l^{*2} < 0$ et $-2 < m^{*2} < 0$. Montrons que $l^* \in 2U \oplus L^*$ et $m^* \in M^*$ (où $M = L_N^\perp$). En effet, soit $l \in 2U \oplus L$, l s'écrit $l = l_1 + h$ avec $l_1 \in 2U \oplus L_R$ et $h \in (N \setminus L) \cap L \otimes \mathbb{Q}$. On a alors $(l^*|l) = (l^*|l_1) + (l^*|h)$. Or, $(l^*|l_1) \in \mathbb{Z}$ puisque $l_1 \in 2U \oplus L_R$ et $l^* \in 2U \oplus L_R^*$, et $(l^*|h) = (r - m^*|h) = (r|h) \in \mathbb{Z}$, puisque d'une part $h \perp m^*$ et d'autre part $r \in N, h \in N$. On a donc montré que $l^* \in 2U \oplus L^*$. Ensuite, pour tout $m \in M$, $(r - l^*|m) = (r|m) \in \mathbb{Z}$ puisque $l^* \perp m$ et $r, m \in N$. Ainsi, la racine $r \in 2U \oplus N$ s'écrit aussi $r = l^* + m^*$, avec $l^* \in 2U \oplus L^*$ et $m^* \in M^*$ et $-2 < l^{*2} < 0$. Ainsi, F_L s'annule bien le long d'un diviseur quadratique rationnel de type 1. \square

Ainsi, pour trouver une forme modulaire strictement -2 -réflexive, nous pouvons procéder de la façon suivante. Soit N un réseau de Niemeier différent du réseau de Leech, et L un sous-réseau non nul de N . Si F_L est réflexive, d'après la proposition 2.1, L est primitif. La proposition 3.3 affirme que le sous-réseau de racines de L doit être une composante orthogonale du sous-réseau de racines N_R de N , et son rang doit être égal au rang de L . Soit donc L_R une composante orthogonale de N_R . Alors, $L = (L_{R_N}^\perp)_N^\perp$ est primitif et a pour sous-réseau de racines L_R . F_L est alors une forme strictement -2 -réflexive si et seulement si son diviseur n'admet pas de composante additionnelle de type 1, ce qui peut être vérifié à partir du calcul du diviseur de F_{L_R} et de la proposition 3.4.

Nous allons donc maintenant étudier les formes modulaires associées à des réseaux L qui sont des composantes orthogonales du sous-réseau de racines d'un réseau de Niemeier. Il n'y a qu'un nombre fini (raisonnable!) de possibilités pour L . Une condition suffisante portant sur L pour que F_L soit strictement -2 -réflexive est de satisfaire la proposition 3.2, ce qui donne la liste suivante :

Proposition 3.5. *Les réseaux satisfaisant la proposition 3.2 sont les 24 réseaux suivants :*

$$\begin{aligned} & \mathbb{E}_8, 2\mathbb{E}_8, 3\mathbb{E}_8, \mathbb{E}_7, \mathbb{E}_6, \\ & \mathbb{D}_8, \mathbb{D}_7, \mathbb{D}_6, \mathbb{D}_5, \mathbb{D}_4, 2\mathbb{D}_4, \\ & \mathbb{A}_7, \mathbb{A}_6, \mathbb{A}_5, \mathbb{A}_4, \mathbb{A}_3, 2\mathbb{A}_3, \mathbb{A}_2, 2\mathbb{A}_2, 3\mathbb{A}_2, \mathbb{A}_1, 2\mathbb{A}_1, 3\mathbb{A}_1, 4\mathbb{A}_1. \end{aligned}$$

PREUVE : C'est juste un simple vérification à partir des tables données dans la partie 1.1.4. \square

Nous avons une liste de formes modulaires strictement -2 -réflexives, mais qui n'est pas à priori complète. Il peut y avoir d'autres formes, qui ne satisfont pas la proposition 3.2,

ou encore, qui sont obtenues à partir du réseau de Leech. Par la suite, nous étudierons toutes les formes réflexives que l'on peut obtenir par quasi-restriction, en prenant pour N un réseau de Niemeier différent du réseau de Leech, et L un réseau de racines qui est une composante orthogonale du sous-réseau de racines de N (ne satisfaisant pas nécessairement la proposition 3.2), et, en utilisant les propositions 3.3 et 3.4, nous verrons qu'il existe une seule autre forme strictement -2 -réflexive obtenue ainsi, ce qui portera notre liste à 25 formes modulaires strictement -2 -réflexives.

Une première liste des formes modulaires strictement -2 -réflexives (on en trouve 24) est donc donnée par le tableau de la figure 3.1, où L désigne le réseau associé à la forme, N est le (ou les) réseau(x) de Niemeier dans le(s)quel(s) on a plongé L et où on a classifié les orbites des composantes du diviseur de chaque forme, en suivant le critère d'Eichler (théorème 1.6). En particulier, pour les réseaux de types $k\mathbb{A}_1$, v_i désigne une racine de la i -ième copie de \mathbb{A}_1 .

F_L	N	pois de F_L	diviseur
$F_{\mathbb{E}_8}$	$N(3E_8), N(E_8 + D_{16})$	252	$H_{-2}(\bar{0})$
$F_{2\mathbb{E}_8}$	$N(3E_8)$	132	$H_{-2}(\bar{0})$
$F_{3\mathbb{E}_8} = \Phi_{12}$	$N(3E_8)$	12	$H_{-2}(\bar{0})$
$F_{\mathbb{E}_7}$	$N(A_{17} + E_7), N(D_{10} + 2E_7)$	165	$H_{-2}(\bar{0})$
$F_{\mathbb{E}_6}$	$N(A_{11} + D_7 + E_6), N(4E_6)$	120	$H_{-2}(\bar{0})$
$F_{\mathbb{D}_8}$	$N(3D_8)$	124	$H_{-2}(\bar{0})$
$F_{\mathbb{D}_7}$	$N(A_{11} + D_7 + E_6)$	114	$H_{-2}(\bar{0})$
$F_{\mathbb{D}_6}$	$N(2A_9 + D_6), N(4D_6)$	102	$H_{-2}(\bar{0})$
$F_{\mathbb{D}_5}$	$N(2A_7 + 2D_5)$	88	$H_{-2}(\bar{0})$
$F_{\mathbb{D}_4}$	$N(4A_5 + D_4), N(6D_4)$	72	$H_{-2}(\bar{0})$
$F_{2\mathbb{D}_4}$	$N(6D_4)$	60	$H_{-2}(\bar{0})$
$F_{\mathbb{A}_7}$	$N(2A_7 + 2D_5)$	80	$H_{-2}(\bar{0})$
$F_{\mathbb{A}_6}$	$N(4A_6)$	75	$H_{-2}(\bar{0})$
$F_{\mathbb{A}_5}$	$N(4A_5 + D_4)$	69	$H_{-2}(\bar{0})$
$F_{\mathbb{A}_4}$	$N(6A_4)$	62	$H_{-2}(\bar{0})$
$F_{\mathbb{A}_3}$	$N(8A_3)$	54	$H_{-2}(\bar{0})$
$F_{2\mathbb{A}_3}$	$N(8A_3)$	48	$H_{-2}(\bar{0})$
$F_{\mathbb{A}_2}$	$N(12A_2)$	45	$H_{-2}(\bar{0})$
$F_{2\mathbb{A}_2}$	$N(12A_2)$	42	$H_{-2}(\bar{0})$
$F_{3\mathbb{A}_2}$	$N(12A_2)$	39	$H_{-2}(\bar{0})$
$F_{\mathbb{A}_1}$	$N(24A_1)$	35	$H_{-2}(\bar{0}) \cup H_{-2}(\frac{v}{2})$
$F_{2\mathbb{A}_1}$	$N(24A_1)$	34	$H_{-2}(\bar{0}) \cup H_{-2}(\frac{v_1}{2}) \cup H_{-2}(\frac{v_2}{2})$
$F_{3\mathbb{A}_1}$	$N(24A_1)$	33	$H_{-2}(\bar{0}) \cup H_{-2}(\frac{v}{2}) \cup H_{-2}(\frac{v_2}{2})$ $\cup H_{-2}(\frac{v_3}{2})$
$F_{4\mathbb{A}_1}$	$N(24A_1)$	32	$H_{-2}(\bar{0}) \cup H_{-2}(\frac{v_1}{2}) \cup H_{-2}(\frac{v_2}{2})$ $\cup H_{-2}(\frac{v_3}{2}) \cup H_{-2}(\frac{v_4}{2})$

FIG. 3.1 – Liste de formes modulaires strictement -2 -réflexives

Nous retrouvons dans cette liste la forme Φ_{12} , mais aussi, et c'est remarquable, la forme Δ_{35} d'Igusa sous le nom de $F_{\mathbb{A}_1}$. On pourra consulter [GN98-2] p.213 à 218 pour l'identification des formes modulaires pour le groupe $O^+(2U \oplus \langle -2 \rangle)$ avec les formes modulaires de Siegel, et p.250-251 pour une construction de Δ_{35} .

On renvoie aussi à [DK03] pour les formes $F_{\mathbb{A}_2}$ (notée ϕ_{45} p.261) et $F_{2\mathbb{A}_1}$ (correspondant au produit $\phi_{30}\phi_4$ p.261), à [Kl05] pour $F_{\mathbb{A}_3}$ (notée ψ_{54} p.92) et $F_{3\mathbb{A}_1}$ (correspondant au produit $\psi_{30}\psi_3$, p.100), et enfin à [Kr05] pour $F_{\mathbb{D}_4}$ (notée Δ , p.932).

3.2 Autres formes réflexives

On reprend les notations des parties précédentes, soit N un des réseaux de Niemeier différent du réseau de Leech, soit $L \neq \{0\}$ un sous-réseau (quelconque) de N , et M un sous-réseau de N tel que $L \perp M$ et $\text{rg}(L \oplus M) = \text{rg}(N)$. Afin de simplifier les notations, on considérera que N, L, M sont définis négatifs, c'est à dire qu'on omettra le " (-1) " dans les notations $N(-1), L(-1), M(-1)$.

Soit F_L la quasi-restriction de la fonction Φ_{12} de Borcherds obtenue dans le théorème 2.2.

On va se limiter aux cas où L est une composante orthogonale du sous-réseau de racines N_R d'un réseau de Niemeier (mais L non nécessairement primitif), et alors on prendra pour M le complément orthogonal de L dans N_R , ce sera aussi un réseau de racines, et $L \oplus M = N_R$. On a déjà trouvé une famille de formes strictement -2 -réflexives, il s'agit maintenant de compléter cette liste (en utilisant les propositions 3.3 et 3.4) comme annoncé, mais aussi au passage de déterminer quelles formes obtenues par quasi-restriction pour un réseau qui est une composante orthogonale du sous-réseau de racines d'un réseau de Niemeier, sont réflexives.

3.2.1 Algorithme de recherche

Nous reprenons l'algorithme proposé en partie 2.2.3, mais nous allons l'adapter :

1. **Choix du plongement.** Soit N l'un des 24 réseaux de Niemeier. On choisit L une composante orthogonale du sous-réseau de racines N_R de N . Nous noterons j le plongement de L dans N ainsi choisi. Nous utiliserons la partie 1.4.2 afin de déterminer quels sont les plongements équivalents, afin de minimiser les calculs. Précisément, nous rappellerons dans chaque cas le groupe $G_2(N)$, et étudierons sa k -transitivité sur les composantes N_i de N_R . Par défaut, lorsque plusieurs plongements sont équivalents, on choisira d'étudier celui défini par l'ordre d'apparition des composantes irréductibles de L (par exemple si $N_R = 4N_1 + N_2$ avec N_i réseau de racines irréductible, et $L = 2N_1$, on choisira le plongement de L dans N correspondant aux deux premières copies de N_1).

2. **Calcul de H, F_L et autres caractéristiques.** On calcule $M = L_N^\perp$, le code H associé au sur-réseau N de $L \oplus M$, et les projections p_L et p_M . Nous sommes dans le cas particulier où le calcul de H et des projections p_L et p_M est fait dans la partie 1.4.2. On

rappelle aussi les formes quadratiques discriminantes à considérer et le niveau de L .

On peut appliquer le théorème 2.2 pour obtenir F_L de poids k .

3. Recherche des composantes du diviseur de F_L . Les -2 -vecteurs de $2U \oplus L$ dirigent des -2 -diviseurs quadratiques le long desquels la forme F_L s'annule, avec multiplicité un. Recherchons les composantes additionnelles de type 1. Lorsque L est primitif, il s'agit donc de calculer $p_M(H)$, et d'en rechercher des représentants (dans M^*) de norme maximale (n'oublions pas que M^* est défini négatif). On utilise alors les remarques importantes 1 et 2 de la partie 2.2.2 et le théorème 2.3 pour savoir si la forme est réflexive ou non. L'inconvénient de cette méthode est que, lorsque L est primitif, le groupe $D(M)$ contient plus de coordonnées que le groupe $D(L)$. D'autre part, lorsque L n'est pas primitif, cette méthode ne s'applique pas, et pourtant nous avons besoin pour compléter notre liste de forme strictement -2 -réflexive, de tester des réseaux L non-primitifs. Nous allons donc procéder "naïvement", en recherchant pour chaque élément $h_L \in p_L(H)$, l'élément (ou les éléments) de $p_M(H)$ correspondant(s), puis nous en rechercherons un représentant de norme maximale. On peut se restreindre aux éléments h_L dont tout représentant dans L^* est de norme < -2 , sinon, comme on l'a vu dans la partie précédente (argument de la démonstration de la proposition 3.2), soit cela ne donne pas lieu à une composante additionnelle, soit c'est une composante additionnelle de type 0 (et donc non intéressante pour notre recherche de formes modulaires strictement -2 -réflexives). Nous ne détaillerons pas toujours les calculs, puisqu'ils sont une simple lecture des tables des parties 1.1.4 et 1.4.2, et nous nous contenterons d'annoncer les classes h_L donnant des composantes additionnelles. Enfin, utilisant le lemme 2.1, nous verrons si la forme ainsi obtenue est réflexive. Pour tester si l'on peut obtenir une forme strictement -2 -réflexive (de sous-réseau de racines L), nous nous contenterons de vérifier l'existence de diviseurs additionnels de type 1 (proposition 3.4). La recherche est exhaustive (proposition 3.3), soit on trouve une forme réflexive dont on peut dire qu'elle est ou pas strictement -2 -réflexive, soit on trouve une forme non réflexive, mais alors on a vérifié l'existence de composantes additionnelles de type 1 (s'il y a une telle composante, il n'y a pas de forme strictement -2 -réflexive de sous-réseau de racines L , sinon, la forme $F_{M_N^\perp}$ est strictement -2 -réflexive).

4. Calcul de la multiplicité de chaque composante du diviseur de F_L . Il s'agit maintenant, pour chaque composante additionnelle dirigée par $l^* \in 2U \oplus L^*$ (réflexive ou non), d'en calculer la multiplicité. Nous ne conduirons ce calcul que pour des réseaux L primitif, puisque l'étape précédente répond complètement à la question de la recherche des formes strictement -2 -réflexives. Chaque $r \in 2U \oplus N$ de norme $r^2 = -2$ dirigeant une composante de multiplicité 1 du diviseur de Φ_{12} , la multiplicité de la composante dirigée par l^* dans le diviseur de F_L est donc égale au nombre de racines $r \in 2U \oplus N$ dont la projection sur $2U \oplus L^*$ est exactement l^* . Il s'agit donc du nombre de vecteurs $m^* \in M^*$ tels que la classe $\overline{m^*}$ de m^* dans $D(M)$ soit h_M (où h_M est associé à h_L la classe de l^* dans $D(2U \oplus L)$ via la correspondance du lemme 2.2), et dont la norme est $-2 - l^{*2}$. De même qu'à l'étape précédente, nous ne détaillerons en général pas ce calcul, la démarche à suivre étant parfaitement claire.

5. Classification des orbites de chaque composante à l'aide du critère d'Eichler. Nous connaissons maintenant les vecteurs l^* qui dirigent les différentes composantes

du diviseur de F_L . Plus précisément, nous connaissons la classe \bar{l}^* dans $D(2U \oplus L)$ et la norme de l^* . Il est donc naturel de classifier les orbites des composantes additionnelles suivant le critère d'Eichler (Théorème 1.6). La classe \bar{l}^* admet au moins un représentant primitif dans $2U \oplus L^*$ (lemme 1.8). Si on note k son ordre dans $D(2U \oplus L)$, le lemme 1.7 assure que le vecteur $l = kl^* \in 2U \oplus L$ est primitif et d'après le critère d'Eichler (théorème 1.6) nous disposons de l'orbite caractérisée par $l^2 = k^2 l^{*2}$ et $l/\text{div}(l) \equiv l^* \pmod{2U \oplus L}$, notée $H_{k^2 l^{*2}}(\bar{l}^*)$. Ensuite il faut vérifier s'il existe ou non des représentants non-primitifs de la classe \bar{l}^* dans $2U \oplus L^*$, ce qui peut être déterminé par le lemme 1.9. Soit donc l'^* un vecteur primitif de $2U \oplus L^*$ et $d \in \mathbb{N}^*$, $d > 1$ tel que la classe $\overline{dl'^*}$ soit égale à \bar{l}^* (voir la démonstration du lemme 1.9). On peut appliquer au vecteur l'^* les lemme 1.7 et théorème 1.6 pour classifier la nouvelle orbite ainsi obtenue (il existe alors autant d'orbites que d'entiers $d \in \mathbb{N}^*$ tels que d^2 divise a où $l^{*2} = -\frac{2a}{\lambda}$, λ étant le niveau de L (notations du lemme 1.9)).

Pour la rédaction de cette étape, nous reprendrons directement les notations des paramètres du lemme 1.9.

3.2.2 Liste des formes réflexives obtenues à partir des “21 premiers” réseaux de Niemeier

Nous testons les cas des réseaux de Niemeier, sauf les cas des réseaux $N(12A_2)$, $N(24A_1)$, et du réseau de Leech, en classant par réseaux de Niemeier N , puis par composantes orthogonales du sous-réseau de racines de N .

Notations. Fixons les notations de cette partie, afin de systématiser l'étude qui est faite. On donnera en titre le nom du réseau $N = N(N_1 + \dots + N_r)$, puis nous donnerons le groupe G_2 des permutations des N_i induit par le groupe $O(N)$ (voir partie 1.4.2), en précisant si ce groupe agit transitivement sur tous les plongements possibles des réseaux $\{0\} \neq L \subset N$. Ensuite, nous rappelons les tables des formes quadratiques discriminantes Q_{N_i} .

Dans un second temps, nous distinguons l'étude par sous-réseau $\{0\} \neq L \subset N$ qui est une composante orthogonale du sous-réseau de racines de N , il n'y a qu'un nombre fini de cas. Nous précisons à chaque fois si L est primitif, le niveau λ de L , et le poids w de la forme F_L . Tout cela correspond aux étapes 1 et 2 de l'algorithme de la partie 3.2.1. Ensuite, nous suivons les autres étapes de l'algorithme, calcul des composantes additionnelles (étape 3), test de la réflexivité (étape 4), et finalement classification des orbites (étape 5). En conclusion, nous donnons les propriétés de la forme modulaire obtenue.

Exemple détaillé. Traitons maintenant un exemple assez compliqué avec tous les détails, afin de bien fixer la méthode. On choisit le réseau $N = N(2A_9 + D_6)$, et le sous-réseau $L = \mathbb{A}_9$, qui est une composante orthogonale du sous-réseau de racines $2\mathbb{A}_9 \oplus \mathbb{D}_6$ de N .

Première chose à vérifier, il y a deux façons de choisir une copie de \mathbb{A}_9 dans $2\mathbb{A}_9 \oplus \mathbb{D}_6$ (choix de la première ou de la seconde copie). Or, le groupe $G_2(N)$ des permutations des copies de \mathbb{A}_9 induit par le groupe des automorphismes de N , est $\mathbb{Z}/2\mathbb{Z}$, c'est à dire que les choix de la première ou de la seconde copie sont équivalents (modulo la conjugaison par un élément de $O(N)$).

Deuxième point. Rappelons d'abord le code associé à N (voir la partie 1.4.2, par la suite on ne recopiera plus les tables) :

$$\begin{aligned}
H &= \langle [2, 4, 0], [5, 0, 1], [0, 5, 3] \rangle \\
&= \left\{ \begin{array}{ccccc} [0, 0, 0], & [2, 4, 0], & [4, 8, 0], & [6, 2, 0], & [8, 6, 0], \\ [5, 0, 1], & [7, 4, 1], & [9, 8, 1], & [1, 2, 1], & [3, 6, 1], \\ [0, 5, 3], & [2, 9, 3], & [4, 3, 3], & [6, 7, 3], & [8, 1, 3], \\ [5, 5, 2], & [7, 9, 2], & [9, 3, 2], & [1, 7, 2], & [3, 1, 2] \end{array} \right\} \\
&\cong (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/5\mathbb{Z}
\end{aligned}$$

Ensuite, on calcule \mathbb{A}_9^\perp . On a $\mathbb{A}_9 \oplus \mathbb{D}_6 \subset \mathbb{A}_9^\perp$, et d'après la table des éléments de H , $\mathbb{A}_9^\perp = \langle \mathbb{A}_9 \oplus \mathbb{D}_6, [0, 5, 3] \rangle$. Mais ce qui est important, c'est que le sous-réseau de racines de \mathbb{A}_9^\perp est $M = \mathbb{A}_9 \oplus \mathbb{D}_6$ qui contient donc $9 * 10 + 2 * 6 * 5 = 150$ racines, et donc la forme $F_{\mathbb{A}_9}$ est de poids 87. Le réseau \mathbb{A}_9 est bien primitif, car c'est l'orthogonal dans N du sous-réseau $\mathbb{A}_9 \oplus \mathbb{D}_6$ (on le vérifie à partir de la table des éléments de H). Le calcul des projections p_L et p_M est transparent, la première coordonnée d'un élément h de H étant h_L , les deux autres étant h_M . Enfin, on donne le niveau de \mathbb{A}_9 , qui est 20, et les tables des deux formes quadratiques discriminantes à considérer :

$$\begin{aligned}
Q_{\mathbb{A}_9} : \quad & \begin{array}{l} 0 \quad \mapsto \quad 0, \\ \varepsilon_1, \varepsilon_9 \quad \mapsto \quad -\frac{9}{10}, \\ \varepsilon_2, \varepsilon_8 \quad \mapsto \quad -\frac{8}{5}, \end{array} \quad \left| \quad \begin{array}{l} \varepsilon_3, \varepsilon_7 \quad \mapsto \quad -2 - \frac{1}{10}, \\ \varepsilon_4, \varepsilon_6 \quad \mapsto \quad -2 - \frac{2}{5}, \\ \varepsilon_5 \quad \mapsto \quad -2 - \frac{1}{2}, \end{array} \right. \\
Q_{\mathbb{D}_6} : \quad & \begin{array}{l} 0 \quad \mapsto \quad 0, \\ \varepsilon_1 \quad \mapsto \quad -\frac{3}{2}, \\ \varepsilon_2 \quad \mapsto \quad -1, \\ \varepsilon_3 \quad \mapsto \quad -\frac{3}{2}. \end{array}
\end{aligned}$$

Troisième point. Tous les -2 -diviseurs quadratiques rationnels de $\mathcal{D}(2U \oplus L)$ sont des composantes du diviseur de F_L . Il faut chercher les composantes additionnelles. \mathbb{A}_9 étant primitif, il suffit de chercher les composantes additionnelles de type 1. D'après les remarques que l'on a déjà faites (en particulier dans la description de l'algorithme), nous allons chercher les élément h_L dont tous les représentant dans \mathbb{A}_9^* sont de norme strictement inférieure à -2 . La lecture de la table des valeurs de $Q_{\mathbb{A}_9}$ montre que l'on dispose de 5 possibilités pour h_L , ces possibilités sont [3] et [7] de représentants respectifs ε_3 et ε_7 de norme maximale $-2 - \frac{1}{10}$, [4] et [6] de représentants respectifs ε_4 et ε_6 de norme maximale $-2 - \frac{2}{5}$, et [5] de représentant ε_5 de norme maximale $-2 - \frac{1}{2}$. Si $d_L = [3]$, alors les possibilités pour h sont $h = [3, 6, 1]$ et $h = [3, 1, 2]$. Le premier cas correspond à $d_M = [6, 1]$ de norme $-3 - \frac{9}{10} < -2$, et donc il ne donne pas lieu à une composante additionnelle, le second cas correspond à $d_M = [1, 2]$, de norme $-1 - \frac{9}{10}$, et donc il donne lieu à une composante additionnelle. Le même raisonnement montre que [7] correspondant à $h = [7, 9, 2]$, [4] correspondant à $[4, 8, 0]$, [6] correspondant à $[6, 2, 0]$ et [5] correspondant à $[5, 0, 1]$ donnent lieu à des composantes additionnelles, et ce sont les seuls cas. Enfin, il faut tester pour chacun des 5 cas, la réflexivité du diviseur à partir du lemme 2.1. [3] et [7] sont d'ordre 10 dans $D(\mathbb{A}_9)$, et $q_{\mathbb{A}_9}([3]) = q_{\mathbb{A}_9}([7]) \equiv -\frac{1}{10} \pmod{2}$, et donc les diviseurs qu'ils définissent sont réflexifs. [4] et [6] sont d'ordre 5 dans $D(\mathbb{A}_9)$, et $q_{\mathbb{A}_9}([4]) = q_{\mathbb{A}_9}([6]) \equiv -\frac{2}{5} \pmod{2}$, et donc les diviseurs qu'ils définissent sont réflexifs. Enfin, [5] est d'ordre 2 dans $D(\mathbb{A}_9)$, et $q_{\mathbb{A}_9}([5]) \equiv -\frac{1}{2} \pmod{2}$, et donc les diviseurs qu'il définit sont réflexifs. Nous savons maintenant que $F_{\mathbb{A}_9}$ est une forme réflexive.

Quatrième point, le calcul de la multiplicité. On suit la remarque faite dans le point 4. de l’algorithme. Pour [3] par exemple, il s’agit du nombre de vecteurs m^* de $\mathbb{A}_9^* \oplus \mathbb{D}_6^*$ dont la classe est [1, 2] et la norme $-1 - \frac{9}{10}$. Un représentant de norme $-1 - \frac{9}{10}$ de la classe [1, 2] est

$$(\varepsilon_1, \varepsilon_2) = \left(\underbrace{\left(\frac{1}{10}, \dots, \frac{1}{10}, \frac{-9}{10} \right)}_{9 \text{ coordonnées}}, (1, 0, 0, 0, 0, 0) \right).$$

Les éléments de $\mathbb{A}_9^* \oplus \mathbb{D}_6^*$ dont la classe est [1, 2] s’obtiennent à partir de $(\varepsilon_1, \varepsilon_2)$ en ajoutant des vecteurs de $\mathbb{A}_9 \oplus \mathbb{D}_6$, et pour conserver la norme égale à $-1 - \frac{9}{10}$, on constate que nécessairement on ne peut modifier la composante correspondant à ε_1 qu’en choisissant la place de la coordonnée valant $\frac{-9}{10}$, cela fait donc 10 choix, et on ne peut modifier la composante correspondant à ε_2 qu’en choisissant la place de la coordonnée 1, ce qui fait 6 choix, et comme $-\overline{\varepsilon_2} = \overline{\varepsilon_2}$, les vecteurs opposés conviennent aussi, ce qui fait 6 possibilités supplémentaires. On a donc établi qu’il y a $10 * 12 = 120$ possibilités pour m^* . La multiplicité de la composante additionnelle donnée par [3] est donc 120. De même, on vérifie que la multiplicité de la composante additionnelle donnée par [7] est 120, celle de [4] et [6] est 45, et enfin celle de [5] est 32.

Cinquième point, la détermination des orbites des composantes du diviseur de $F_{\mathbb{A}_9}$. Occupons-nous d’abord des orbites dirigées par des -2 -vecteurs. De tels vecteurs sont primitifs dans $2U \oplus \mathbb{A}_9$. Le diviseur d’un -2 -vecteur est 1 ou 2. Dans le premier cas, on obtient l’orbite caractérisée, suivant le critère d’Eichler (théorème 1.6), par $l^2 = -2$ et $\frac{l}{\text{div}(l)} \in 2U \oplus \mathbb{A}_9$, notée $H_{-2}(\overline{0})$. Dans le second cas, on obtiendrait un -2 -vecteur $l \in 2U \oplus \mathbb{A}_9$ tel que $l^* = \frac{l}{\text{div}(l)} \in 2U \oplus \mathbb{A}_9^*$ vérifie $l^{*2} = -\frac{2}{2^2} = -\frac{1}{2}$. C’est possible en choisissant pour $l^* \in 2U \oplus \mathbb{A}_9^*$ le vecteur primitif $u + \varepsilon_5$, où $u = e + f \in U$, avec (e, f) couple hyperbolique de U et $u^2 = 2$. C’est la seule possibilité pour l^* (mod $2U \oplus \mathbb{A}_9$). Le vecteur $l = 2(u + \varepsilon_5)$ vérifie bien $l^2 = -2$ et $\frac{l}{\text{div}(l)} \equiv [5] \pmod{2U \oplus \mathbb{A}_9}$, on dispose donc de l’orbite $H_{-2}([5])$.

Les classes [3] et [7] correspondent à des vecteurs $l^* \in 2U \oplus \mathbb{A}_9$ de norme $-\frac{1}{10}$ et l’ordre de $\overline{l^*}$ dans $D(2U \oplus L)$ est 10. D’après le lemme 1.8, il existe des représentants primitifs des classes [3] et [7], puis d’après le lemme 1.7 et le critère d’Eichler (théorème 1.6) les orbites correspondantes sont caractérisées par les vecteurs $l \in 2U \oplus L$ tels que $l^2 = 10^2 * \frac{-1}{10} = -10$ et $\frac{l}{\text{div}(l)} \equiv [3]$ ou $[7] \pmod{2U \oplus L}$ respectivement, orbites que l’on a notées $H_{-10}([3])$ et $H_{-10}([7])$. De même, on obtient les orbites $H_{-10}([4])$, $H_{-10}([6])$ et $H_{-2}([5])$.

Reste un dernier point à vérifier. Comme on l’a vu dans le lemme 1.9, un vecteur $l^* \in 2U \oplus L^*$ n’est pas forcément primitif, et alors l’orbite du diviseur qu’il dirige n’est pas la même que celle dirigée par un vecteur l^* de même classe et norme mais primitif. Le lemme 1.9 permet de trouver toutes les orbites possibles. Pour la classe [3], on a $l^{*2} = -\frac{1}{10} = -\frac{2}{20}$. Reprenons les notations du lemme 1.9, on a écrit l^{*2} sous la forme $l^{*2} = -\frac{2a}{\lambda}$, avec ici $\lambda = 20$, et donc $a = 1$. Donc l^* est primitif, le seul diviseur positif de 1 étant 1 (voir le lemme 1.9). De même, on montre que les projections $l^* \in 2U \oplus \mathbb{A}_9^*$ correspondant à [7] sont des vecteurs primitifs. Pour la classe [5], on a $l^{*2} = -\frac{1}{2} = -\frac{2*5}{20}$, donc $a = 5$ qui est sans facteurs carrés, donc d’après le lemme 1.9, l^* est primitif. Enfin, restent les cas des classes [4] et [6]. Soit $l^* \in 2U \oplus \mathbb{A}_9^*$ de classe [4] et tel que $l^{*2} = -\frac{2}{5} = -\frac{2*2^2}{20}$, alors $a = 2^2$, et $k = 2$ est le seul entier positif différent de 1 tel que $k^2|a$. Suivant le lemme 1.9, cherchons une classe $\overline{l'}$ de $D(2U \oplus \mathbb{A}_9)$ telle que $2\overline{l'} = \overline{l^*}$. Les possibilités sont $\overline{l'} = [2]$

ou $\bar{l}' = [7]$. Dans le premier cas, $\bar{l}' \equiv -\frac{8}{5} \pmod{2} \equiv -\frac{2*16}{20} \pmod{2}$, donc, suivant les notations du lemme 1.9, $b = 16$, puis $(b - \frac{a}{k^2}) = 15$ qui n'est pas divisible par 20, donc il n'existe pas de vecteur primitif $l' \in 2U \oplus \mathbb{A}_9^*$ dont la classe dans $D(2U \oplus \mathbb{A}_9)$ est $[2]$ et tel que $2l' = l^*$. Dans le second cas, $\bar{l}' \equiv -\frac{1}{10} \pmod{2} \equiv -\frac{2}{20} \pmod{2}$, donc, suivant les notations du lemme 1.9, $b = 1$, puis $(b - \frac{a}{k^2}) = 0$ qui est divisible par 20, donc il existe un vecteur primitif $l' \in 2U \oplus \mathbb{A}_9^*$ dont la classe dans $D(2U \oplus \mathbb{A}_9)$ est $[7]$ et tel que $2l' = l^*$. De même, pour la classe $[6]$, on montre qu'il existe un vecteur primitif $l' \in 2U \oplus \mathbb{A}_9^*$ dont la classe dans $D(2U \oplus \mathbb{A}_9)$ est $[3]$ et tel que $2l' = l^*$.

Conclusion. On a trouvé les orbites suivantes : $H_{-2}(\bar{0})$ et $H_{-2}([5])$ avec multiplicité 1, provenant des -2 -vecteurs de $2U \oplus \mathbb{A}_9$, $H_{-10}([3])$ et $H_{-10}([7])$ avec multiplicité 120, provenant des projections des racines de $2U \oplus N$ correspondant aux éléments $h = [3, 1, 2]$ et $h = [7, 9, 2]$, $H_{-10}([6])$ et $H_{-2}([5])$ puis $H_{-10}([3])$ et $H_{-10}([7])$ avec multiplicité 45, provenant des projections des racines de $2U \oplus N$ correspondant aux éléments $h = [4, 8, 0]$ et $[6, 2, 0]$ (il y a deux types d'orbites d'après le lemme 1.9), et enfin $H_{-2}([5])$ avec multiplicité 32, provenant des projections des racines de $2U \oplus N$ correspondant à l'élément $h = [5, 0, 1]$. On a donc obtenu la forme modulaire $F_{\mathbb{A}_9}$ pour le groupe $\tilde{O}^+(2U \oplus \mathbb{A}_9)$, de poids 87 et de caractère déterminant. Le diviseur de cette forme est

$$H_{-2}(\bar{0}) \cup 33H_{-2}([5]) \cup 165H_{-10}([3]) \cup 165H_{-10}([7]) \cup 45H_{-10}([4]) \cup 45H_{-10}([6]).$$

Cette forme est réflexive.

Passons maintenant au traitement systématique de la classification des formes réflexives.

Le réseau $N(D_{24})$

$$G_2 = \{1\}.$$

Il n'y a pas d'autre composante orthogonale de \mathbb{D}_{24} autre que \mathbb{D}_{24} elle-même. La forme $F_{\mathbb{D}_{24}}$ obtenue par quasi-restriction n'est pas réflexive puisque \mathbb{D}_{24} n'est pas primitif. Elle n'a pas de composante additionnelle de type 1 à son diviseur, donc \mathbb{D}_{24} est le sous-réseau de racines d'un réseau primitif L pour lequel la forme obtenue par quasi-restriction est une forme strictement -2 -réflexive, mais alors il ne peut s'agir que de Φ_{12} (à cause du rang de L), ce n'est donc pas une nouvelle forme strictement -2 -réflexive.

De façon générale, par la suite, on ne considérera plus les réseaux L de rang 24, ils donnent tous lieux, suivant le raisonnement précédent, à une forme modulaire strictement -2 -réflexive de poids 12, c'est Φ_{12} .

Le réseau $N(D_{16} + E_8)$

$$G_2 = \{1\}.$$

Les formes quadratiques discriminantes à considérer sont :

$$\begin{aligned}
 Q_{\mathbb{D}_{16}} : \quad 0 &\mapsto 0, \\
 \varepsilon_1 &\mapsto -4, \\
 \varepsilon_2 &\mapsto -1, \\
 \varepsilon_3 &\mapsto -4.
 \end{aligned}$$

Si $L = \mathbb{E}_8$; on retrouve la forme $F_{\mathbb{E}_8}$ que l'on a trouvé en partie 3.1.2.

Si $L = \mathbb{D}_{16}$; on a $L_N^\perp = \mathbb{E}_8 = M$, et L n'est pas primitif, la forme n'est pas réflexive. D'autre part, l'étude des éventuelles composantes additionnelles de type 1 pour $F_{\mathbb{D}_{16}}$ montre justement qu'il n'y a pas de telles composantes additionnelles ($p_M(H) = \{0\}$). Autrement dit, $F_{M_N^\perp}$ est une forme strictement -2 -réflexive. Précisément, $M_N^\perp = \mathbb{D}_{16}^+$, c'est un réseau unimodulaire pair de dimension 16 différent de $2\mathbb{E}_8$ (ces deux réseaux sont les seuls unimodulaires pairs de dimension 16). Il semblerait donc que l'on ait trouvé une nouvelle forme modulaire strictement -2 -réflexive, mais $2U \oplus 2\mathbb{E}_8 \cong 2U \oplus \mathbb{D}_{16}^+$, et donc on a retrouvé la forme $F_{2\mathbb{E}_8}$ de la partie 3.1.2.

Le réseau $N(3E_8)$

$G_2 = \mathcal{S}_3$, tous les plongements sont équivalents (choix des copies de E_8). Il n'y a pas besoin de forme discriminante ici, puisque $N(3E_8) = 3\mathbb{E}_8$. On retrouve les formes $F_{\mathbb{E}_8}$, $F_{2\mathbb{E}_8}$ (et $F_{3\mathbb{E}_8} = \Phi_{12}$).

Le réseau $N(A_{24})$

Il n'y a pas de nouvelle forme, pour les mêmes raisons que pour $N(D_{24})$.

Le réseau $N(2D_{12})$

$G_2 = \mathbb{Z}/2\mathbb{Z}$, tous les plongements sont équivalents (choix des copies de \mathbb{D}_{12}). Les formes quadratiques discriminantes à considérer sont :

$$\begin{aligned}
 Q_{\mathbb{D}_{12}} : \quad 0 &\mapsto 0, \\
 \varepsilon_1 &\mapsto -3 = -2 - 1, \\
 \varepsilon_2 &\mapsto -1, \\
 \varepsilon_3 &\mapsto -3 = -2 - 1.
 \end{aligned}$$

Si $L = \mathbb{D}_{12}$; $\mathbb{D}_{12}^{(1)} = \mathbb{D}_{12}^{(2)\perp}$, $\lambda = 2$, $w = 12 + \frac{1}{2}(2 * 12 * 11) = 144$.

Composantes additionnelles : [1] et [3] sont de bons candidats. Dans le groupe quotient $H = N/N_R$, on voit que [1], correspondant à [1, 3] et [3], correspondant à [3, 3], semblent possibles, mais en regardant les normes possibles pour m^* , on voit que la seule possibilité est [1].

Réflexivité : [1] est d'ordre 2 et $l^{*2} = -1 = \frac{2}{2}$, donc d'après le lemme 2.1 cette composante

est réflexive.

Multiplicité : c'est le nombre de vecteurs $m^* \in \mathbb{D}_{12}^{(2)*}$ dont la classe est [2] et le carré est -1 , d'après les tables des parties 1.1.3 et 1.1.4, la multiplicité est 24.

Orbites : [1] a pour paramètres $\lambda = 2, a = 1$ dans le lemme 1.9, donc $k = 1$ et les seules orbites possibles correspondent à [1]. On a donc la composante additionnelle (de type 1) donnée par $H_{-4}([1])$.

Conclusion. Nous avons trouvé une forme réflexive $F_{\mathbb{D}_{12}}$ de poids 144 et diviseur

$$H_{-2}(\bar{0}) \cup 24H_{-4}([1]).$$

Le réseau $N(A_{17} + E_7)$

$$G_2 = \{1\}.$$

Les formes quadratiques discriminantes à considérer sont :

$$\begin{array}{l} Q_{\mathbb{A}_{17}} : 0 \quad \mapsto 0, \\ \varepsilon_1, \varepsilon_{17} \mapsto -\frac{17}{18}, \\ \varepsilon_2, \varepsilon_{16} \mapsto -\frac{16}{9}, \\ \varepsilon_3, \varepsilon_{15} \mapsto -2 - \frac{1}{2}, \\ \varepsilon_4, \varepsilon_{14} \mapsto -2 - \frac{10}{9}, \end{array} \left| \begin{array}{l} \varepsilon_5, \varepsilon_{13} \mapsto -2 - \frac{29}{18}, \\ \varepsilon_6, \varepsilon_{12} \mapsto -4, \\ \varepsilon_7, \varepsilon_{11} \mapsto -4 - \frac{5}{18}, \\ \varepsilon_8, \varepsilon_{10} \mapsto -4 - \frac{4}{9}, \\ \varepsilon_9 \quad \mapsto -4 - \frac{1}{2}, \end{array} \right.$$

$$\begin{array}{l} Q_{\mathbb{E}_7} : 0 \quad \mapsto 0, \\ \varepsilon_1 \quad \mapsto -\frac{3}{2}. \end{array}$$

Si $L = \mathbb{E}_7$; on retrouve $F_{\mathbb{E}_7}$.

Si $L = \mathbb{A}_{17}$; $\mathbb{A}_{17} = \mathbb{E}_7^\perp$, $\lambda = 36$, $w = 12 + \frac{1}{2}(126) = 75$.

Composantes additionnelles : [3] (au moins). [3] correspond à [3, 1] dans H , donc $h_M = [1]$ qui admet un représentant dans M^* de norme $-\frac{3}{2}$. On dispose d'une composante additionnelle de type 1.

Réflexivité : [3] est d'ordre 6 et $l^{*2} = -\frac{1}{2} = -\frac{3}{6}$, donc d'après le lemme 2.1 ce vecteur n'est pas réflexif.

La forme obtenue n'est pas réflexive, et son diviseur admet une composante additionnelle de type 1.

Le réseau $N(D_{10} + 2E_7)$

$G_2 = \mathbb{Z}/2\mathbb{Z}$, tous les plongements sont équivalents (choix des copies de \mathbb{E}_7).

Les formes quadratiques discriminantes à considérer sont :

$$\begin{array}{l} Q_{\mathbb{D}_{10}} : 0 \quad \mapsto 0, \\ \varepsilon_1 \mapsto -\frac{5}{2} = -2 - \frac{1}{2}, \\ \varepsilon_2 \mapsto -1 \equiv -1 \\ \varepsilon_3 \mapsto -\frac{5}{2} = -2 - \frac{1}{2}, \end{array}$$

$$\begin{array}{l} Q_{\mathbb{E}_7} : 0 \quad \mapsto 0, \\ \varepsilon_1 \mapsto -\frac{3}{2}. \end{array}$$

Si $L = \mathbb{E}_7$; on retrouve $F_{\mathbb{E}_7}$.

Si $L = 2\mathbb{E}_7$; $2\mathbb{E}_7 = \mathbb{D}_{10}^\perp$, $\lambda = 4$, $w = 12 + \frac{1}{2}(2 * 10 * 9) = 102$.

Composantes additionnelles : $[1, 1]$ correspondant à $[2, 1, 1]$ dans H définit une composante additionnelle (de type 1).

Réflexivité : $[1, 1]$ d'ordre 2 et $l^{*2} = -1 = \frac{2}{2}$, donc d'après le lemme 2.1 la composante est réflexive.

Multiplicité : 20 (voir tables des parties 1.1.3 et 1.1.4).

Orbites : $[1, 1]$ a pour paramètres $\lambda = 4, a = 2$ dans le lemme 1.9, donc $k = 1$ et on dispose de l'orbite $H_{-4}([1, 1])$.

Conclusion. On a trouvé une forme réflexive $F_{2\mathbb{E}_7}$ de poids 102 et diviseur

$$H_{-2}(\bar{0}) \cup 20H_{-4}([1, 1]).$$

Si $L = \mathbb{D}_{10}$; $\mathbb{D}_{10} = (2\mathbb{E}_7)^\perp$, $\lambda = 4$, $w = 12 + \frac{1}{2}(2 * 126) = 138$.

Composantes additionnelles : $[1], [3]$, correspondant à $[1, 0, 1]$ et $[3, 1, 0]$ dans H définissent des composantes additionnelles.

Réflexivité : $[1]$ et $[3]$ d'ordre 2 et $l^{*2} = -\frac{1}{2}$, donc d'après le lemme 2.1 ces vecteurs sont réflexifs.

Multiplicité : 56 (table de valeurs de la série thêta de $[1] + \mathbb{E}_7$, donnée dans [CS98], p.125).

Orbites : $[1]$ et $[3]$ ont pour paramètres $\lambda = 4, a = 1$, donc $k = 1$ et les orbites sont $H_{-2}([1])$ et $H_{-2}([3])$.

Conclusion. On a trouvé une forme réflexive $F_{\mathbb{D}_{10}}$ de poids 138 et diviseur

$$H_{-2}(\bar{0}) \cup 57H_{-2}([1]) \cup 57H_{-2}([3]).$$

Si $L = \mathbb{D}_{10} + \mathbb{E}_7$; $L \neq M_N^\perp$. De plus, l'élément $[3, 0, 1]$ donne une composante additionnelle de type 1 au diviseur de $F_L, F_{M_N^\perp}$ n'est donc pas une forme strictement -2 -réflexive.

Le réseau $N(A_{15} + D_9)$

$G_2 = \{1\}$. Les formes quadratiques discriminantes à considérer sont :

$$Q_{\mathbb{A}_{15}} : \begin{array}{l} 0 \quad \mapsto \quad 0, \\ \varepsilon_1, \varepsilon_{15} \mapsto -\frac{15}{16}, \\ \varepsilon_2, \varepsilon_{14} \mapsto -\frac{7}{4}, \\ \varepsilon_3, \varepsilon_{13} \mapsto -2 - \frac{7}{16}, \\ \varepsilon_4, \varepsilon_{12} \mapsto -2 - 1, \end{array} \left| \begin{array}{l} \varepsilon_5, \varepsilon_{11} \mapsto -2 - \frac{23}{16}, \\ \varepsilon_6, \varepsilon_{10} \mapsto -2 - \frac{7}{4}, \\ \varepsilon_7, \varepsilon_9 \mapsto -2 - \frac{31}{16}, \\ \varepsilon_8 \quad \mapsto -4, \end{array} \right.$$

$$Q_{\mathbb{D}_9} : \begin{array}{l} 0 \quad \mapsto \quad 0, \\ \varepsilon_1 \mapsto -\frac{9}{4} = -2 - \frac{1}{4}, \\ \varepsilon_2 \mapsto -1, \\ \varepsilon_3 \mapsto -\frac{9}{4} = -2 - \frac{1}{4}. \end{array}$$

Si $L = \mathbb{A}_{15}$; $\mathbb{A}_{15} = \mathbb{D}_9^\perp$, $\lambda = 32$, $w = 12 + \frac{1}{2}(2 * 9 * 8) = 84$.

Composantes additionnelles : [4] (au moins), correspondant à [4, 2].

Réflexivité : [4] d'ordre 4 et $l^{*2} = -1 = \frac{4}{4}$, d'après le lemme 2.1 ce vecteur n'est pas réflexif.

La forme n'est pas réflexive, et son diviseur admet une composante additionnelle de type 1.

Si $L = \mathbb{D}_9$; $\mathbb{D}_9 = \mathbb{A}_{15}^\perp$, $\lambda = 8$, $w = 12 + \frac{1}{2}(15 * 16) = 132$.

Composantes additionnelles : [1], [3], correspondant à [2, 1] et [14, 3].

Réflexivité : [1] et [3] sont d'ordre 4 et $l^{*2} = -\frac{1}{4}$, d'après le lemme 2.1 ces vecteurs sont réflexifs.

Multiplicité : 120.

Orbites : [1] et [3] ont pour paramètres $\lambda = 8$, $a = 1$, donc $k = 1$ et on dispose des orbites $H_{-4}([1])$ et $H_{-4}([3])$.

Conclusion. on a trouvé une forme réflexive $F_{\mathbb{D}_9}$ de poids 132 et diviseur

$$H_{-2}(\bar{0}) \cup 120H_{-4}([1]) \cup 120H_{-4}([3]).$$

Le réseau $N(3D_8)$

$G_2 = \mathcal{S}_3$, tous les plongements sont équivalents (choix des copies de \mathbb{D}_8).

Les formes quadratiques discriminantes à considérer sont :

$$\begin{aligned} Q_{\mathbb{D}_8} : \quad 0 &\mapsto 0, \\ \varepsilon_1 &\mapsto -2, \\ \varepsilon_2 &\mapsto -1, \\ \varepsilon_3 &\mapsto -2. \end{aligned}$$

Si $L = \mathbb{D}_8$; on retrouve $F_{\mathbb{D}_8}$.

Si $L = 2\mathbb{D}_8$; $L \neq M_N^\perp$, et l'élément [2, 1, 2] va donner une composante additionnelle de type 1 à F_L .

Le réseau $N(2A_{12})$

$G_2 = \mathbb{Z}/2\mathbb{Z}$, tous les plongements sont équivalents (choix des copies de \mathbb{A}_{12}).

Les formes quadratiques discriminantes à considérer sont :

$$Q_{\mathbb{A}_{12}} : \quad \begin{array}{l} 0 \mapsto 0, \\ \varepsilon_1, \varepsilon_{12} \mapsto -\frac{12}{13}, \\ \varepsilon_2, \varepsilon_{11} \mapsto -\frac{22}{13}, \\ \varepsilon_3, \varepsilon_{10} \mapsto -2 - \frac{4}{13}. \end{array} \quad \left| \begin{array}{l} \varepsilon_4, \varepsilon_9 \mapsto -2 - \frac{10}{13}, \\ \varepsilon_5, \varepsilon_8 \mapsto -2 - \frac{14}{13}, \\ \varepsilon_6, \varepsilon_7 \mapsto -2 - \frac{16}{13}, \end{array} \right.$$

Si $L = \mathbb{A}_{12}$; $\mathbb{A}_{12}^{(1)} = \mathbb{A}_{12}^{(2)\perp}$, $\lambda = 13$, $w = 12 + \frac{1}{2}(12 * 13) = 90$.

Composantes additionnelles : [3] (au moins), correspondant à [3, 2].

Réflexivité : [3] d'ordre 13 et $l^{*2} = -\frac{4}{13}$, d'après le lemme 2.1 ces vecteurs ne sont pas réflexifs.

La forme n'est pas réflexive, et son diviseur admet une composante additionnelle de type 1.

Le réseau $N(A_{11} + D_7 + E_6)$

$G_2 = \{1\}$.

Les formes quadratiques discriminantes à considérer sont :

$$Q_{\mathbb{A}_{11}} : \begin{array}{l} 0 \\ \varepsilon_1, \varepsilon_{11} \\ \varepsilon_2, \varepsilon_{10} \\ \varepsilon_3, \varepsilon_9 \end{array} \mapsto \begin{array}{l} 0, \\ -\frac{11}{12}, \\ -\frac{5}{3}, \\ -2 - \frac{1}{4}, \end{array} \left| \begin{array}{l} \varepsilon_4, \varepsilon_8 \\ \varepsilon_5, \varepsilon_7 \\ \varepsilon_6 \end{array} \mapsto \begin{array}{l} -2 - \frac{2}{3}, \\ -2 - \frac{11}{12}, \\ -2 - 1, \end{array} \right.$$

$$Q_{\mathbb{D}_7} : \begin{array}{l} 0 \\ \varepsilon_1 \\ \varepsilon_2 \\ \varepsilon_3 \end{array} \mapsto \begin{array}{l} 0, \\ -\frac{7}{4}, \\ -1, \\ -\frac{7}{4}, \end{array}$$

$$Q_{\mathbb{E}_6} : \begin{array}{l} 0 \\ \varepsilon_1, \varepsilon_2 \end{array} \mapsto \begin{array}{l} 0, \\ -\frac{4}{3}. \end{array}$$

Si $L = \mathbb{A}_{11}$; $\mathbb{A}_{11} = (\mathbb{D}_7 \oplus \mathbb{E}_6)^\perp$, $\lambda = 24$, $w = 12 + \frac{1}{2}(2 * 7 * 6 + 72) = 90$.

Composantes additionnelles : [3], [9], correspondant à [3, 3, 0] et [9, 1, 0].

Réflexivité : [3] et [9] sont d'ordre 4 et $l^{*2} = -\frac{1}{4}$, d'après le lemme 2.1 ces vecteurs sont réflexifs.

Multiplicité : 64.

Orbites : [3] et [9] ont pour paramètres $\lambda = 24, a = 3$, donc $k = 1$ et on a les orbites $H_{-4}([3])$ and $H_{-4}([9])$.

Composantes additionnelles : [4], [8], correspondant à [4, 0, 1] et [8, 0, 2].

Réflexivité : [4] et [8] sont d'ordre 3 et $l^{*2} = -\frac{2}{3}$, d'après le lemme 2.1 ces vecteurs sont réflexifs.

Multiplicité : 56.

Orbites : [4] et [8] ont pour paramètres $\lambda = 24, a = 8$, donc $k = 2$ et $k = 1$ sont possibles. Mais, pour $k = 2$, on a aussi les paramètres $b = 8$ (car $[4] = 2[8]$ et $[8] = 2[4]$), et $(b - \frac{a}{k^2}) = 6$ qui n'est pas divisible par 24, ou $b = 20$ (pour $[4] = 2[2]$ et $[8] = 2[10]$), et $(b - \frac{a}{k^2}) = 18$ qui n'est pas divisible par 24, donc $k = 2$ n'est finalement pas possible, et on dispose seulement des orbites $H_{-6}([4])$ et $H_{-6}([8])$.

Composantes additionnelles : [5], [7], mais il n'y a pas de m^* de norme > -2 correspondant.

Composantes additionnelles : [6] correspondant à [6, 2, 0].

Réflexivité : [6] est d'ordre 2 et $l^{*2} = -\frac{2}{2}$, donc d'après le lemme 2.1 ces vecteurs sont réflexifs.

Multiplicité : 14.

Orbites : [6] a pour paramètres $\lambda = 24, a = 12 = 2 * 2 * 3$, donc $k = 2$ est possible, mais alors on a $b = 3$ (pour $[6] = 2[3]$ et $[6] = 2[9]$), et $(b - \frac{a}{k^2}) = 0$ qui est divisible par 24. Nous avons donc les orbites $H_{-4}([6]), H_{-4}([3])$ et $H_{-4}([9])$.

Conclusion. Nous avons trouvé une forme réflexive $F_{\mathbb{A}_{11}}$ de poids 90 et diviseur

$$H_{-2}(\bar{0}) \cup 78H_{-4}([3]) \cup 78H_{-4}([9]) \cup 56H_{-6}([4]) \cup 56H_{-6}([8]) \cup 14H_{-4}([6]).$$

Si $L = \mathbb{D}_7$; on retrouve $F_{\mathbb{D}_7}$.

Si $L = \mathbb{E}_6$; on retrouve $F_{\mathbb{E}_6}$.

Si $L = \mathbb{A}_{11} + \mathbb{D}_7$; $L \neq M_N^\perp$, et l'élément $[1, 1, 1]$ va donner une composante additionnelle de type 1 à F_L .

Si $L = \mathbb{A}_{11} + \mathbb{E}_6$; $L \neq M_N^\perp$, et l'élément $[2, 2, 2]$ va donner une composante additionnelle de type 1 à F_L .

Si $L = \mathbb{D}_7 + \mathbb{E}_6$; $\mathbb{D}_7 + \mathbb{E}_6 = \mathbb{A}_{11}^\perp$, $\lambda = 24, w = 12 + \frac{1}{2}(11 * 12) = 78$.

Composantes additionnelles : $[1, 1]$ (au moins), correspondant à $[1, 1, 1]$.

Réflexivité : $[1, 1]$ est d'ordre 12 et $l^{*2} = -\frac{13}{12}$, d'après le lemme 2.1 ce vecteur n'est pas réflexif.

La forme n'est pas réflexive, et son diviseur admet une composante additionnelle de type 1.

Le réseau $N(4E_6)$

$G_2 = \mathcal{S}_4$, tous les plongements sont équivalents.

Les formes quadratiques discriminantes à considérer sont :

$$\begin{aligned} Q_{\mathbb{E}_6} : 0 &\mapsto 0, \\ \varepsilon_1, \varepsilon_2 &\mapsto -\frac{4}{3}, \end{aligned}$$

Si $L = \mathbb{E}_6$; on retrouve $F_{\mathbb{E}_6}$.

Si $L = 2\mathbb{E}_6$; $2\mathbb{E}_6 = (2\mathbb{E}_6)^\perp$, $\lambda = 3, w = 12 + \frac{1}{2}(2 * 72) = 84$.

Composantes additionnelles : $[1, 1], [1, 2], [2, 1], [2, 2]$, correspondant à $[1, 1, 2, 0], [1, 2, 0, 1], [2, 1, 0, 2]$ et $[2, 2, 1, 0]$.

Réflexivité : Ils sont d'ordre 3 et $l^{*2} = -\frac{2}{3}$, d'après le lemme 2.1 ces vecteurs sont réflexifs.

Multiplicité : 27 (d'après la série thêta de $[1] + \mathbb{E}_6$, donné dans [CS98], p. 127).

Orbites : Ces vecteurs ont pour paramètres $\lambda = 3, a = 1$, donc $k = 1$. Nous avons les

orbites $H_{-6}([1, 1])$, $H_{-6}([1, 2])$, $H_{-6}([2, 1])$ et $H_{-6}([2, 2])$.

Conclusion. Nous avons trouvé une forme réflexive $F_{2\mathbb{E}_6}$ de poids 84 et diviseur

$$H_{-2}(\bar{0}) \cup 27H_{-6}([1, 1]) \cup 27H_{-6}([1, 2]) \cup 27H_{-6}([2, 1]) \cup 27H_{-6}([2, 2]).$$

Si $L = 3\mathbb{E}_6$; $L \neq M_N^\perp$, et l'élément $[1, 0, 1, 2]$ va donner une composante additionnelle de type 1 à F_L .

Le réseau $N(2A_9 + D_6)$

$G_2 = \mathbb{Z}/2\mathbb{Z}$, tous les plongements sont équivalents.

Les formes quadratiques discriminantes à considérer sont :

$$Q_{A_9} : \begin{array}{l} 0 \quad \mapsto \quad 0, \\ \varepsilon_1, \varepsilon_9 \mapsto -\frac{9}{10}, \\ \varepsilon_2, \varepsilon_8 \mapsto -\frac{8}{5}, \end{array} \left| \begin{array}{l} \varepsilon_3, \varepsilon_7 \mapsto -2 - \frac{1}{10}, \\ \varepsilon_4, \varepsilon_6 \mapsto -2 - \frac{2}{5}, \\ \varepsilon_5 \quad \mapsto -2 - \frac{1}{2}, \end{array} \right.$$

$$Q_{D_6} : \begin{array}{l} 0 \quad \mapsto \quad 0, \\ \varepsilon_1 \mapsto -\frac{3}{2}, \\ \varepsilon_2 \mapsto -1, \\ \varepsilon_3 \mapsto -\frac{3}{2}. \end{array}$$

Si $L = \mathbb{D}_6$; on retrouve $F_{\mathbb{D}_6}$.

Si $L = A_9$; $A_9 = (A_9 \oplus D_6)^\perp$, $\lambda = 20$, $w = 12 + \frac{1}{2}(9 * 10 + 2 * 6 * 5) = 87$.

Composantes additionnelles : [3], [7], correspondant à [3, 1, 2] et [7, 9, 2].

Réflexivité : ordre 10 et $l^{*2} = -\frac{1}{10}$, d'après le lemme 2.1 ces vecteurs sont réflexifs.

Multiplicité : 120.

Orbites : paramètres $\lambda = 20, a = 1$, donc $k = 1$ et on les orbites $H_{-10}([3])$ et $H_{-10}([7])$.

Composantes additionnelles : [4], [6], correspondant à [4, 8, 0] et [6, 2, 0].

Réflexivité : ordre 5 et $l^{*2} = -\frac{2}{5}$, d'après le lemme 2.1 ces vecteurs sont réflexifs.

Multiplicité : 45.

Orbites : paramètres $\lambda = 20, a = 4 = 2^2$, donc $k = 2$ est possible, on a alors $b = 16$ (pour [4] = 2[2] et [6] = 2[8]), et $(b - \frac{a}{k^2}) = 15$ qui n'est pas divisible par 20, ou $b = 1$ (pour [4] = 2[7] et [6] = 2[3]), et $(b - \frac{a}{k^2}) = 0$ qui est divisible par 20, on a donc les orbites $H_{-10}([4])$, $H_{-10}([6])$, $H_{-10}([3])$ et $H_{-10}([7])$.

Composantes additionnelles : [5], correspondant à [5, 0, 1].

Réflexivité : ordre 2 et $l^{*2} = -\frac{1}{2}$, d'après le lemme 2.1 ces vecteurs sont réflexifs

Multiplicité : 32.

Orbites : paramètres $\lambda = 20, a = 5$, donc $k = 1$ et on a l'orbite $H_{-2}([5])$.

Conclusion. On a trouvé une forme réflexive F_{A_9} de poids 87 et diviseur

$$H_{-2}(\bar{0}) \cup 33H_{-2}([5]) \cup 165H_{-10}([3]) \cup 165H_{-10}([7]) \cup 45H_{-10}([4]) \cup 45H_{-10}([6]).$$

Si $L = 2\mathbb{A}_9$; $L \neq M_N^\perp$, et l'élément $[5, 0, 1]$ va donner une composante additionnelle de type 1 à F_L .

Si $L = \mathbb{A}_9 + \mathbb{D}_6$; $L \neq M_N^\perp$, et l'élément $[5, 5, 2]$ va donner une composante additionnelle de type 1 à F_L .

Le réseau $N(4D_6)$

$G_2 = \mathcal{S}_4$, tous les plongements sont équivalents.

Les formes quadratiques discriminantes à considérer sont :

$$\begin{aligned} Q_{\mathbb{D}_6} : 0 &\mapsto 0, \\ \varepsilon_1 &\mapsto -\frac{3}{2}, \\ \varepsilon_2 &\mapsto -1, \\ \varepsilon_3 &\mapsto -\frac{3}{2}. \end{aligned}$$

$L = \mathbb{D}_6$; on retrouve $F_{\mathbb{D}_6}$.

$L = 2\mathbb{D}_6$; $2\mathbb{D}_6 = (2\mathbb{D}_6)^\perp$, $\lambda = 4$, $w = 12 + \frac{1}{2}(2 * 2 * 6 * 5) = 72$.

Composantes additionnelles : $[1, 2], [2, 1], [2, 3], [3, 2]$, correspondant à $[1, 2, 0, 3], [2, 1, 3, 0], [2, 3, 0, 1]$ et $[3, 2, 1, 0]$.

Réflexivité : ordre 2 et $l^{*2} = -\frac{1}{2}$, d'après le lemme 2.1 ces vecteurs sont réflexifs.

Multiplicité : 32.

Orbites : paramètres $\lambda = 4, a = 1$, donc $k = 1$ et on a les orbites $H_{-2}([1, 2]), H_{-2}([2, 1]), H_{-2}([2, 3])$ and $H_{-2}([3, 2])$.

Composantes additionnelles : $[1, 3], [3, 1]$, correspondant à $[1, 3, 2, 0], [3, 1, 0, 2]$.

Réflexivité : ordre 2 and $l^{*2} = -1$, d'après le lemme 2.1 ces vecteurs sont réflexifs.

Multiplicité : 12.

Orbites : paramètres $\lambda = 4, a = 2$, donc $k = 1$ et on a les orbites $H_{-4}([1, 3]), H_{-4}([3, 1])$.

Conclusion. On a trouvé une forme réflexive $F_{2\mathbb{D}_6}$ de poids 72 et de diviseur

$$\begin{aligned} &H_{-2}(\bar{0}) \cup 33H_{-2}([1, 2]) \cup 33H_{-2}([2, 1]) \cup 33H_{-2}([2, 3]) \cup 33H_{-2}([3, 2]) \\ &\cup 12H_{-4}([1, 3]) \cup 12H_{-4}([3, 1]). \end{aligned}$$

Si $L = 3\mathbb{D}_6$; $L \neq M_N^\perp$, et l'élément $[2, 2, 2, 2]$ va donner une composante additionnelle de type 1 à F_L .

Le réseau $N(3A_8)$

$G_2 = \mathcal{S}_3$, tous les plongements sont équivalents.

Les formes quadratiques discriminantes à considérer sont :

$$Q_{\mathbb{A}_8} : \begin{array}{l} 0 \quad \mapsto \quad 0, \\ \varepsilon_1, \varepsilon_8 \mapsto -\frac{8}{9}, \\ \varepsilon_2, \varepsilon_7 \mapsto -\frac{14}{9}. \end{array} \left| \begin{array}{l} \varepsilon_3, \varepsilon_6 \mapsto -2, \\ \varepsilon_4, \varepsilon_5 \mapsto -2 - \frac{2}{9}, \end{array} \right|$$

Si $L = \mathbb{A}_8$; $\mathbb{A}_8 = (2\mathbb{A}_8)^\perp$, $\lambda = 9$, $w = 12 + \frac{1}{2}(2 * 8 * 9) = 84$.

Composantes additionnelles : [4] et [5], correspondant à [4, 1, 1] et [5, 8, 8].

Réflexivité : ordre 9 et $l^{*2} = -\frac{2}{9}$, d'après le lemme 2.1 ces vecteurs sont réflexifs.

Multiplicité : 81.

Orbites : paramètres $\lambda = 9, a = 1$, donc $k = 1$ et on a les orbites $H_{-18}([4])$ et $H_{-18}([5])$.

Conclusion. On a trouvé une forme réflexive $F_{\mathbb{A}_8}$ de poids 84 et diviseur

$$H_{-2}(\bar{0}) \cup 81H_{-18}([4]) \cup 81H_{-18}([5]).$$

Si $L = 2\mathbb{A}_8$; $L \neq M_N^\perp$, et l'élément [5, 5, 2] va donner une composante additionnelle de type 1 à F_L .

Le réseau $N(2A_7 + 2D_5)$

$G_2 = (\mathbb{Z}/2\mathbb{Z})^2$, tous les plongements sont équivalents.

Les formes quadratiques discriminantes à considérer sont :

$$Q_{\mathbb{A}_7} : \begin{array}{l} 0 \quad \mapsto \quad 0, \\ \varepsilon_1, \varepsilon_7 \mapsto -\frac{7}{8}, \\ \varepsilon_2, \varepsilon_6 \mapsto -\frac{3}{2}, \end{array} \left| \begin{array}{l} \varepsilon_3, \varepsilon_5 \mapsto -\frac{15}{8}, \\ \varepsilon_4 \quad \mapsto -2, \end{array} \right|$$

$$Q_{\mathbb{D}_5} : \begin{array}{l} 0 \quad \mapsto \quad 0, \\ \varepsilon_1 \mapsto -\frac{5}{4}, \\ \varepsilon_2 \mapsto -1, \\ \varepsilon_3 \mapsto -\frac{5}{4}. \end{array}$$

Si $L = \mathbb{A}_7$; on retrouve $F_{\mathbb{A}_7}$.

Si $L = \mathbb{D}_5$; on retrouve $F_{\mathbb{D}_5}$.

Si $L = 2\mathbb{A}_7$; $L \neq M_N^\perp$, et l'élément [5, 1, 3, 0] va donner une composante additionnelle de type 1 à F_L .

Si $L = 2\mathbb{D}_5$; $2\mathbb{D}_5 = (2\mathbb{A}_7)^\perp$, $\lambda = 8$, $w = 12 + \frac{1}{2}(2 * 7 * 8) = 68$.

Composantes additionnelles : $[1, 2], [2, 1], [2, 3], [3, 2]$, correspondant à $[1, 1, 1, 2], [1, 7, 2, 1], [7, 1, 2, 3]$ et $[7, 7, 3, 2]$.

Réflexivité : ordre 4 et $l^{*2} = -\frac{1}{4}$, d'après le lemme 2.1 ces vecteurs sont réflexifs.

Multiplicité : 64.

Orbites : paramètres $\lambda = 8, a = 1$, donc $k = 1$ et on a les orbites $H_{-4}([1, 2]), H_{-4}([2, 1]), H_{-4}([2, 3])$ et $H_{-4}([3, 2])$.

Composantes additionnelles : $[1, 1], [1, 3], [3, 1], [3, 3]$, correspondant à $[6, 0, 1, 1], [0, 6, 1, 3], [0, 2, 3, 1]$ et $[2, 0, 3, 3]$.

Réflexivité : ordre 4 et $l^{*2} = -\frac{2}{4}$, d'après le lemme 2.1 ces vecteurs sont réflexifs.

Multiplicité : 28.

Orbites : paramètres $\lambda = 8, a = 2$, donc $k = 1$ et on a les orbites $H_{-8}([1, 1]), H_{-8}([1, 3]), H_{-8}([3, 1]), H_{-8}([3, 3])$.

Conclusion. On a trouvé la forme $F_{2\mathbb{D}_5}$ de poids 68 et diviseur

$$\begin{aligned} & H_{-2}(\bar{0}) \cup 64H_{-4}([2, 1]) \cup 64H_{-4}([1, 2]) \cup 64H_{-4}([2, 3]) \cup 64H_{-4}([3, 2]) \\ & \cup 28H_{-8}([1, 1]) \cup 28H_{-8}([1, 3]) \cup 28H_{-8}([3, 1]) \cup 28H_{-8}([3, 3]). \end{aligned}$$

Le réseau $N(4A_6)$

$G_2 = \mathcal{A}_4$. Ce groupe est 2-transitif, donc tous les choix de deux copies de \mathbb{A}_6 sont équivalents. Mais, choisir une copie de \mathbb{A}_6 détermine les trois autres (en tant qu'ensemble), donc tous les choix de trois copies de \mathbb{A}_6 sont équivalents aussi.

Les formes quadratiques discriminantes à considérer sont :

$$\begin{aligned} Q_{\mathbb{A}_6} : \quad 0 & \mapsto 0, \\ \varepsilon_1, \varepsilon_6 & \mapsto -\frac{6}{7}, \\ \varepsilon_2, \varepsilon_5 & \mapsto -\frac{10}{7}, \\ \varepsilon_3, \varepsilon_4 & \mapsto -\frac{12}{7}. \end{aligned}$$

Si $L = \mathbb{A}_6$; on retrouve $F_{\mathbb{A}_6}$.

Si $L = 2\mathbb{A}_6$; $2\mathbb{A}_6 = 2\mathbb{A}_6^\perp$, $\lambda = 7$, $w = 12 + \frac{1}{2}(2 * 6 * 7) = 54$.

Composantes additionnelles : $[1, 4]$ (au moins), correspondant à $[1, 4, 5, 0]$.

Réflexivité : $[1, 4]$ est d'ordre 7 et $l^{*2} = -\frac{4}{7}$, d'après le lemme 2.1 ce vecteur n'est pas réflexif.

La forme n'est pas réflexive, et son diviseur admet une composante additionnelle de type 1.

Si $L = 3\mathbb{A}_6$; $L \neq M_N^\perp$, et l'élément $[1, 6, 2, 1]$ va donner une composante additionnelle de type 1 à F_L .

Le réseau $N(4A_5 + D_4)$

$G_2 = \mathcal{S}_4$, tous les plongements sont équivalents.

Les formes quadratiques discriminantes à considérer sont :

$$\begin{aligned} Q_{\mathbb{A}_5} : 0 &\mapsto 0, \\ \varepsilon_1, \varepsilon_5 &\mapsto -\frac{5}{6}, \\ \varepsilon_2, \varepsilon_4 &\mapsto -\frac{4}{3}, \\ \varepsilon_3 &\mapsto -\frac{3}{2}, \end{aligned}$$

$$\begin{aligned} Q_{\mathbb{D}_4} : 0 &\mapsto 0, \\ \varepsilon_1 &\mapsto -1, \\ \varepsilon_2 &\mapsto -1, \\ \varepsilon_3 &\mapsto -1. \end{aligned}$$

Si $L = \mathbb{A}_5$; on retrouve $F_{\mathbb{A}_5}$.

Si $L = \mathbb{D}_4$; on retrouve $F_{\mathbb{D}_4}$.

Si $L = 2\mathbb{A}_5$; $2\mathbb{A}_5 = (2\mathbb{A}_5 \oplus \mathbb{D}_4)^\perp$, $\lambda = 12$, $w = 12 + \frac{1}{2}(2 * 5 * 6 + 2 * 4 * 3) = 54$.

Composantes additionnelles : $[1, 2], [2, 1], [1, 4], [4, 1], [5, 2], [2, 5], [5, 4], [4, 5]$, correspondant à $[1, 2, 0, 1, 3], [2, 1, 0, 5, 2], [1, 4, 5, 0, 2], [4, 1, 5, 0, 3], [5, 2, 1, 0, 2], [2, 5, 1, 0, 3], [5, 4, 0, 5, 3]$ et $[4, 5, 0, 1, 2]$.

Réflexivité : ordre 6 et $l^{*2} = -\frac{1}{6}$, d'après le lemme 2.1 ces vecteurs sont réflexifs.

Multiplicité : 48.

Orbites : paramètres $\lambda = 12, a = 1$, donc $k = 1$ et on a les orbites $H_{-6}([1, 2]), H_{-6}([2, 1]), H_{-6}([1, 4]), H_{-6}([4, 1]), H_{-6}([5, 2]), H_{-6}([2, 5]), H_{-6}([5, 4]), H_{-6}([4, 5])$.

Composantes additionnelles : $[1, 3], [3, 1], [5, 3], [3, 5]$, correspondant à $[1, 3, 1, 5, 0], [3, 1, 1, 1, 0], [5, 3, 5, 1, 0]$ et $[3, 5, 5, 5, 0]$.

Réflexivité : ordre 6 et $l^{*2} = -\frac{2}{6}$, d'après le lemme 2.1 ces vecteurs sont réflexifs.

Multiplicité : 36.

Orbites : paramètres $\lambda = 12, a = 2$, donc $k = 1$ et on a les orbites $H_{-12}([1, 3]), H_{-12}([3, 1]), H_{-12}([5, 3]), H_{-12}([3, 5])$.

Composantes additionnelles : $[2, 2], [2, 4], [4, 2], [4, 4]$, correspondant à $[2, 2, 4, 0, 0], [2, 4, 0, 2, 0], [4, 2, 0, 4, 0]$ et $[4, 4, 2, 0, 0]$.

Réflexivité : ordre 3 et $l^{*2} = -\frac{2}{3}$, d'après le lemme 2.1 ces vecteurs sont réflexifs.

Multiplicité : 15.

Orbites : paramètres $\lambda = 12, a = 4$, donc $k = 2$ est possible, et alors on a $b = 10$ (pour $[2, 2] = 2[1, 1], [4, 4] = 2[5, 5], [2, 4] = 2[1, 5]$ et $[4, 2] = 2[5, 1]$), et $(b - \frac{a}{k^2}) = 9$ qui n'est pas divisible par 12, ou $b = 16$ (pour $[2, 2] = 2[4, 4], [4, 4] = 2[2, 2], [2, 4] = 2[4, 2]$ et $[4, 2] = 2[2, 4]$), et $(b - \frac{a}{k^2}) = 9$ qui n'est pas divisible par 12, ou $b = 13$ (pour $[2, 2] = 2[1, 4] = 2[4, 1], [4, 4] = 2[2, 5] = 2[5, 2], [2, 4] = 2[1, 2] = 2[4, 5]$ et $[4, 2] = 2[2, 1] = 2[5, 4]$), et $(b - \frac{a}{k^2}) = 12$ qui est divisible par 12, donc on a les orbites $H_{-6}([2, 2]), H_{-6}([2, 4]), H_{-6}([4, 2]), H_{-6}([4, 4])$ et $H_{-6}([1, 2]), H_{-6}([2, 1]), H_{-6}([1, 4]),$

$H_{-6}([4, 1]), H_{-6}([5, 2]), H_{-6}([2, 5]), H_{-6}([5, 4]), H_{-6}([4, 5]).$

Composantes additionnelles : $[3, 3]$, correspondant à $[3, 3, 0, 0, 1]$.

Réflexivité : ordre 2 et $l^{*2} = -\frac{2}{2}$, d'après le lemme 2.1 ces vecteurs sont réflexifs.

Multiplicité : 8.

Orbites : paramètres $\lambda = 12, a = 6$, donc $k = 1$ et on a les orbites $H_{-4}([3, 3])$.

Conclusion. On a trouvé une forme réflexive $F_{2\mathbb{A}_5}$ de poids 54 et diviseur

$$\begin{aligned} & H_{-2}(\bar{0}) \cup 63H_{-6}([1, 2]) \cup 63H_{-6}([2, 1]) \cup 63H_{-6}([1, 4]) \cup 63H_{-6}([4, 1]) \\ & \cup 63H_{-6}([5, 2]) \cup 63H_{-6}([2, 5]) \cup 63H_{-6}([5, 4]) \cup 63H_{-6}([4, 5]) \\ & \cup 36H_{-12}([1, 3]) \cup 36H_{-12}([3, 1]) \cup 36H_{-12}([5, 3]) \cup 36H_{-12}([3, 5]) \\ & \cup 15H_{-6}([2, 2]) \cup 15H_{-6}([2, 4]) \cup 15H_{-6}([4, 2]) \cup 15H_{-6}([4, 4]) \\ & \cup 8H_{-4}([3, 3]). \end{aligned}$$

Si $L = 3\mathbb{A}_5$; $L \neq M_N^\perp$, et l'élément $[3, 3, 0, 0, 1]$ va donner une composante additionnelle de type 1 à F_L .

Si $L = 4\mathbb{A}_5$; $L \neq M_N^\perp$, et l'élément $[3, 3, 0, 0, 1]$ va donner une composante additionnelle de type 1 à F_L .

Si $L = \mathbb{A}_5 \oplus \mathbb{D}_4$; $\mathbb{A}_5 \oplus \mathbb{D}_4 = (3\mathbb{A}_5)^\perp$, $\lambda = 12$, $w = 12 + \frac{1}{2}(3 * 5 * 6) = 57$.

Composantes additionnelles : $[2, 1], [2, 2], [2, 3], [4, 1], [4, 2], [4, 3]$, correspondant à $[2, 0, 5, 1, 1], [2, 1, 0, 5, 2], [2, 5, 1, 0, 3], [4, 0, 1, 5, 1], [4, 5, 0, 1, 2]$, et $[4, 1, 5, 0, 3]$.

Réflexivité : ordre 6 et $l^{*2} = -\frac{2}{6}$, d'après le lemme 2.1 ces vecteurs sont réflexifs.

Multiplicité : 36.

Orbites : paramètres $\lambda = 12, a = 2$, donc $k = 1$ et on a les orbites $H_{-12}([2, 1]), H_{-12}([2, 2]), H_{-12}([2, 3]), H_{-12}([4, 1]), H_{-12}([4, 2]), H_{-12}([4, 3])$.

Composantes additionnelles : $[3, 1], [3, 2], [3, 3]$, correspondant à $[3, 3, 0, 0, 1], [3, 0, 3, 0, 2]$ et $[3, 0, 0, 3, 3]$.

Réflexivité : ordre 2 et $l^{*2} = -\frac{1}{2}$, d'après le lemme 2.1 ces vecteurs sont réflexifs.

Multiplicité : 20.

Orbites : paramètres $\lambda = 12, a = 3$, donc $k = 1$ et on a les orbites $H_{-2}([3, 1]), H_{-2}([3, 2]), H_{-2}([3, 3])$.

Conclusion. On a trouvé une forme réflexive $F_{\mathbb{A}_5 \oplus \mathbb{D}_4}$ de poids 57 et diviseur

$$\begin{aligned} & H_{-2}(\bar{0}) \cup 21H_{-2}([3, 1]) \cup 21H_{-2}([3, 2]) \cup 21H_{-2}([3, 3]) \cup 36H_{-12}([2, 1]) \\ & \cup 36H_{-12}([2, 2]) \cup 36H_{-12}([2, 3]) \cup 36H_{-12}([4, 1]) \cup 36H_{-12}([4, 2]) \cup 36H_{-12}([4, 3]). \end{aligned}$$

Si $L = 2\mathbb{A}_5 \oplus \mathbb{D}_4$; $L \neq M_N^\perp$, et l'élément $[3, 0, 0, 3, 3]$ va donner une composante additionnelle de type 1 à F_L .

Si $L = 3\mathbb{A}_5 \oplus \mathbb{D}_4$; $L \neq M_N^\perp$, et l'élément $[3, 0, 0, 3, 3]$ va donner une composante additionnelle de type 1 à F_L .

Le réseau $N(6D_4)$

$G_2 = \mathcal{S}_6$, tous les plongements sont équivalents.

Les formes quadratiques discriminantes à considérer sont :

$$\begin{aligned} Q_{\mathbb{D}_4} : 0 &\mapsto 0, \\ \varepsilon_1 &\mapsto -1, \\ \varepsilon_2 &\mapsto -1, \\ \varepsilon_3 &\mapsto -1. \end{aligned}$$

Si $L = \mathbb{D}_4$; on retrouve $F_{\mathbb{D}_4}$.

Si $L = 2\mathbb{D}_4$; on retrouve $F_{2\mathbb{D}_4}$.

Si $L = 3\mathbb{D}_4$; $3\mathbb{D}_4 = 3\mathbb{D}_4^\perp$, $\lambda = 2$, $w = 12 + \frac{1}{2}(3 * 2 * 4 * 3) = 48$.

Composantes additionnelles : de la forme $[1 \text{ ou } 2 \text{ ou } 3, 1 \text{ ou } 2 \text{ ou } 3, 1 \text{ ou } 2 \text{ ou } 3]$ (27 possibilités), correspondant à 9 vecteurs qui sont $[1, 1, 1, 1, 0, 0]$, $[2, 2, 2, 2, 0, 0]$, $[3, 3, 3, 3, 0, 0]$, $[3, 2, 1, 0, 1, 0]$, $[2, 1, 3, 0, 3, 0]$, $[1, 2, 3, 0, 0, 3]$, $[3, 1, 2, 0, 0, 2]$, $[2, 3, 1, 0, 0, 1]$ et $[1, 3, 2, 0, 2, 0]$.

Réflexivité : ordre 2 et $l^{*2} = -\frac{2}{2}$, d'après le lemme 2.1 ces vecteurs sont réflexifs.

Multiplicité : 8.

Orbites : paramètres $\lambda = 2$, $a = 1$, donc $k = 1$ et on a les orbites $H_{-4}([1, 1, 1])$, $H_{-4}([2, 2, 2])$, $H_{-4}([3, 3, 3])$, $H_{-4}([3, 2, 1])$, $H_{-4}([2, 1, 3])$, $H_{-4}([1, 2, 3])$, $H_{-4}([3, 1, 2])$, $H_{-4}([2, 3, 1])$, $H_{-4}([1, 3, 2])$.

Conclusion. On a trouvé une forme réflexive $F_{3\mathbb{D}_4}$ de poids 48 et diviseur

$$\begin{aligned} H_{-2}(\bar{0}) \cup 8H_{-4}([1, 1, 1]) \cup 8H_{-4}([2, 2, 2]) \cup 8H_{-4}([3, 3, 3]) \cup 8H_{-4}([2, 1, 3]) \cup 8H_{-4}([1, 2, 3]) \\ \cup 8H_{-4}([3, 1, 2]) \cup 8H_{-4}([2, 3, 1]) \cup 8H_{-4}([3, 2, 1]) \cup 8H_{-4}([1, 3, 2]). \end{aligned}$$

Si $L = 4\mathbb{D}_4$; $L \neq M_N^\perp$, et l'élément $[3, 2, 0, 1, 0, 1]$ va donner une composante additionnelle de type 1 à F_L .

Si $L = 5\mathbb{D}_4$; $L \neq M_N^\perp$, et l'élément $[3, 2, 0, 1, 0, 1]$ va donner une composante additionnelle de type 1 à F_L .

Le réseau $N(6A_4)$

$G_2 \cong PGL_2(\mathbb{F}_5)$, ce groupe est 3-transitif sur les copies de \mathbb{A}_4 , donc tous les choix d'au plus 3 copies de \mathbb{A}_4 sont équivalents. Mais, choisir 1, 2 ou 3 copies de \mathbb{A}_4 détermine les autres (en tant qu'ensemble), donc tous les choix de 4, 5 ou 6 copies de \mathbb{A}_4 sont équivalents aussi.

Les formes quadratiques discriminantes à considérer sont :

$$\begin{aligned} Q_{\mathbb{A}_4} : 0 &\mapsto 0, \\ \varepsilon_1, \varepsilon_4 &\mapsto -\frac{4}{5}, \\ \varepsilon_2, \varepsilon_3 &\mapsto -\frac{6}{5}. \end{aligned}$$

Si $L = \mathbb{A}_4$; on retrouve $F_{\mathbb{A}_4}$.

Si $L = 2\mathbb{A}_4$; $2\mathbb{A}_4 = 4\mathbb{A}_4^\perp$, $\lambda = 5$, $w = 12 + \frac{1}{2}(4 * 4 * 5) = 52$.

Composantes additionnelles : $[2, 2]$, $[2, 3]$, $[3, 2]$, $[3, 3]$, correspondant à $[2, 2, 4, 0, 4]$, $[2, 3, 0, 1, 1, 0]$, $[3, 2, 0, 4, 4, 0]$ et $[3, 3, 1, 0, 0, 1]$.

Réflexivité : ordre 5 et $l^{*2} = -\frac{2}{5}$, d'après le lemme 2.1 ces vecteurs sont réflexifs.

Multiplicité : 25.

Orbites : paramètres $\lambda = 5$, $a = 1$, donc $k = 1$ et on a les orbites $H_{-10}([2, 2])$, $H_{-10}([2, 3])$, $H_{-10}([3, 2])$, $H_{-10}([3, 3])$.

Conclusion. On a une forme réflexive $F_{2\mathbb{A}_4}$ de poids 52 et diviseur

$$H_{-2}(\bar{0}) \cup 25H_{-10}([2, 2]) \cup 25H_{-10}([2, 3]) \cup 25H_{-10}([3, 2]) \cup 25H_{-10}([3, 3]).$$

Si $L = 3\mathbb{A}_4$; $3\mathbb{A}_4 = 3\mathbb{A}_4^\perp$, $\lambda = 5$, $w = 12 + \frac{1}{2}(3 * 4 * 5) = 42$.

Composantes additionnelles : $[2, 4, 2]$ (au moins), correspondant à $[2, 4, 2, 4, 0, 0]$.

Réflexivité : ordre 5 et $l^{*2} = -\frac{6}{5}$, d'après le lemme 2.1 ce vecteur n'est pas réflexif.

La forme n'est pas réflexive, et son diviseur admet une composante additionnelle de type 1.

Si $L = 4\mathbb{A}_4$; $L \neq M_N^\perp$, et l'élément $[0, 2, 3, 4, 0, 1]$ va donner une composante additionnelle de type 1 à F_L .

Si $L = 5\mathbb{A}_4$; $L \neq M_N^\perp$, et l'élément $[0, 2, 3, 4, 0, 1]$ va donner une composante additionnelle de type 1 à F_L .

Le réseau $N(8A_3)$

$G_2 \cong 2^3 \cdot PGL_2(\mathbb{F}_7)$, ce groupe est 3-transitif sur les copies de \mathbb{A}_4 , donc tous les choix d'au plus 3 copies de \mathbb{A}_3 sont équivalents. Mais, choisir 1, 2 ou 3 copies de \mathbb{A}_3 détermine les 5, 6 ou 7 autres (en tant qu'ensemble), donc tous les choix de 5, 6 ou 7 copies de \mathbb{A}_3

sont équivalents aussi. Le cas de 4 copies est à traiter à part.
Les formes quadratiques discriminantes à considérer sont :

$$\begin{aligned} Q_{\mathbb{A}_3} : 0 &\mapsto 0, \\ \varepsilon_1, \varepsilon_3 &\mapsto -\frac{3}{4}, \\ \varepsilon_2 &\mapsto -1. \end{aligned}$$

Si $L = \mathbb{A}_3$; on retrouve $F_{\mathbb{A}_3}$.

Si $L = 2\mathbb{A}_3$; on retrouve $F_{2\mathbb{A}_3}$.

Si $L = 3\mathbb{A}_3$; $3\mathbb{A}_3 = 5\mathbb{A}_3^\perp$, $\lambda = 8$, $w = 12 + \frac{1}{2}(5 * 3 * 4) = 42$.

Composantes additionnelles : $[1, 1, 1]$, $[1, 1, 3]$, $[1, 3, 1]$, $[1, 3, 3]$, $[3, 1, 1]$, $[3, 1, 3]$, $[3, 3, 1]$, $[3, 3, 3]$, correspondant à $[1, 1, 1, 0, 0, 2, 3, 0]$, $[1, 1, 3, 0, 0, 0, 1, 2]$, $[1, 3, 1, 0, 2, 0, 1, 0]$, $[1, 3, 3, 2, 0, 0, 3, 0]$, $[3, 1, 1, 2, 0, 0, 1, 0]$, $[3, 1, 3, 0, 2, 0, 1, 0]$, $[3, 3, 1, 0, 0, 0, 3, 2]$ et $[3, 3, 3, 0, 0, 2, 1, 0]$.

Réflexivité : ordre 4 et $l^{*2} = -\frac{1}{4}$, d'après le lemme 2.1 ces vecteurs sont réflexifs.

Multiplicité : 24.

Orbites : paramètres $\lambda = 8$, $a = 1$, donc $k = 1$ et on a les orbites $H_{-4}([1, 1, 1])$, $H_{-4}([1, 1, 3])$, $H_{-4}([1, 3, 1])$, $H_{-4}([1, 3, 3])$, $H_{-4}([3, 1, 1])$, $H_{-4}([3, 1, 3])$, $H_{-4}([3, 3, 1])$, $H_{-4}([3, 3, 3])$.

Composantes additionnelles : $[2, 1, 1]$, $[2, 1, 3]$, $[2, 3, 1]$, $[2, 3, 3]$, $[1, 2, 1]$, $[1, 2, 3]$, $[3, 2, 1]$, $[3, 2, 3]$, $[1, 1, 2]$, $[1, 3, 2]$, $[3, 1, 2]$, $[3, 3, 2]$, correspondant à $[2, 1, 1, 0, 1, 0, 0, 0]$, $[2, 1, 3, 3, 0, 3, 0, 0]$, $[2, 3, 1, 1, 0, 1, 0, 0]$, $[2, 3, 3, 0, 3, 0, 0, 1]$, $[1, 2, 1, 3, 0, 0, 0, 1]$, $[1, 2, 3, 0, 1, 1, 0, 0]$, $[3, 2, 1, 0, 3, 3, 0, 0]$, $[3, 2, 3, 1, 0, 0, 0, 3]$, $[1, 1, 2, 1, 3, 0, 0, 0]$, $[1, 3, 2, 0, 0, 3, 0, 3]$, $[3, 1, 2, 0, 0, 1, 0, 1]$ et $[3, 3, 2, 3, 1, 0, 0, 0]$.

Réflexivité : ordre 4 et $l^{*2} = -\frac{2}{4}$, d'après le lemme 2.1 ces vecteurs sont réflexifs.

Multiplicité : 16 .

Orbites : paramètres $\lambda = 8$, $a = 2$, donc $k = 1$ et on a les orbites $H_{-8}([2, 1, 1])$, $H_{-8}([2, 1, 3])$, $H_{-8}([2, 3, 1])$, $H_{-8}([2, 3, 3])$, $H_{-8}([1, 2, 1])$, $H_{-8}([1, 2, 3])$, $H_{-8}([3, 2, 1])$, $H_{-8}([3, 2, 3])$, $H_{-8}([1, 1, 2])$, $H_{-8}([1, 3, 2])$, $H_{-8}([3, 1, 2])$, $H_{-8}([3, 3, 2])$.

Composantes additionnelles : des vecteurs tels que $l^{*2} = -\frac{3}{4}$, mais il n'y a pas de m^* correspondants.

Composantes additionnelles : $[2, 2, 2]$ correspondant à $[2, 2, 2, 0, 0, 0, 2, 0]$.

Réflexivité : ordre 2 et $l^{*2} = -\frac{2}{2}$, d'après le lemme 2.1 ces vecteurs sont réflexifs.

Multiplicité : 6.

Orbites : paramètres $\lambda = 8$, $a = 4$, donc $k = 2$ est possible, avec $b = 1$ et $(b - \frac{a}{k^2} = 0$, et $8|0$, donc on a les orbites $H_{-4}([2, 2, 2])$, et $H_{-4}([1, 1, 1])$, $H_{-4}([1, 1, 3])$, $H_{-4}([1, 3, 1])$, $H_{-4}([1, 3, 3])$, $H_{-4}([3, 1, 1])$, $H_{-4}([3, 1, 3])$, $H_{-4}([3, 3, 1])$, $H_{-4}([3, 3, 3])$.

Conclusion. On a trouvé une forme réflexive $F_{3\mathbb{A}_3}$ de poids 42 et diviseur

$$\begin{aligned} &H_{-2}(\bar{0}) \cup 30H_{-4}([1, 1, 1]) \cup 30H_{-4}([1, 1, 3]) \cup 30H_{-4}([1, 3, 1]) \cup 30H_{-4}([1, 3, 3]) \\ &\cup 30H_{-4}([3, 1, 1]) \cup 30H_{-4}([3, 1, 3]) \cup 30H_{-4}([3, 3, 1]) \cup 30H_{-4}([3, 3, 3]) \\ &\cup 16H_{-8}([2, 1, 1]) \cup 16H_{-8}([2, 1, 3]) \cup 16H_{-8}([2, 3, 1]) \cup 16H_{-8}([2, 3, 3]) \end{aligned}$$

$$\begin{aligned} & \cup 16H_{-8}([1, 2, 1]) \cup 16H_{-8}([1, 2, 3]) \cup 16H_{-8}([3, 2, 1]) \cup 16H_{-8}([3, 2, 3]) \\ & \cup 16H_{-8}([1, 1, 2]) \cup 16H_{-8}([1, 3, 2]) \cup 16H_{-8}([3, 1, 2]) \cup 16H_{-8}([3, 3, 2]) \\ & \cup 6H_{-4}([2, 2, 2]). \end{aligned}$$

Si $L = 4\mathbb{A}_3$; $4\mathbb{A}_3 = 4\mathbb{A}_3^\perp$, $\lambda = 8$, $w = 12 + \frac{1}{2}(4 * 3 * 4) = 36$.

Composantes additionnelles : $[[3, 1, 1, 2]$ (au moins), correspondant à $[3, 1, 1, 2, 0, 0, 1, 0]$.

Réflexivité : ordre 4 et $l^{*2} = -\frac{5}{4}$, d'après le lemme 2.1 ces vecteurs ne sont pas réflexifs

La forme n'est pas réflexive, et son diviseur admet une composante additionnelle de type 1.

Un examen attentif du code H montre que pour tout plongement de 4 copies de \mathbb{A}_3 , on retrouve une composante additionnelle de type 1 non réflexive à F_L .

Si $L = 5\mathbb{A}_3$; $L \neq M_N^\perp$, et l'élément $[3, 1, 2, 0, 0, 1, 0, 1]$ va donner une composante additionnelle de type 1 à F_L .

Si $L = 6\mathbb{A}_3$; $L \neq M_N^\perp$, et l'élément $[3, 1, 2, 0, 0, 1, 0, 1]$ va donner une composante additionnelle de type 1 à F_L .

Si $L = 7\mathbb{A}_3$; $L \neq M_N^\perp$, et l'élément $[3, 1, 2, 0, 0, 1, 0, 1]$ va donner une composante additionnelle de type 1 à F_L .

3.2.3 Liste des formes réflexives obtenues à partir des réseaux de Niemeier $N(12A_2)$ et $N(24A_1)$

Traisons maintenant les cas des réseaux $N(12A_2)$ et $N(24A_1)$, en reprenant les notations de la partie précédente. Les calculs sont beaucoup plus subtils qu'une simple vérification. Nous utiliserons largement les diverses propriétés citées dans la partie 1.2.4.

Le réseau $N(12A_2)$

$G_2 = M_{12}$, ce groupe est 5-transitif sur les copies de \mathbb{A}_2 , donc tous les choix d'au plus 5 copies de \mathbb{A}_2 sont équivalents.

Les formes quadratiques discriminantes à considérer sont :

$$\begin{aligned} Q_{\mathbb{A}_2} : 0 & \mapsto 0, \\ \varepsilon_1, \varepsilon_2 & \mapsto -\frac{2}{3}. \end{aligned}$$

Si $L = \mathbb{A}_2$; on retrouve $F_{\mathbb{A}_2}$.

Si $L = 2\mathbb{A}_2$; on retrouve $F_{2\mathbb{A}_2}$.

Si $L = 3\mathbb{A}_2$; on retrouve $F_{3\mathbb{A}_2}$.

Si $L = 4\mathbb{A}_2$; $4\mathbb{A}_2 = 8\mathbb{A}_2^\perp$, $\lambda = 3$, $w = 12 + \frac{1}{2}(8 * 2 * 3) = 36$.

Composantes additionnelles : nécessairement, elles correspondent à des mots de poids 6 du code dont 4 lettres non nulles correspondent aux 4 copies de \mathbb{A}_2 que l'on considère. Le calcul explicite précis du diviseur est fait en annexe 2.

Réflexivité : ordre 3 et $l^{*2} = -\frac{2}{3}$, d'après le lemme 2.1 ces vecteurs sont réflexifs.

Multiplicité : 9.

Orbites : paramètres $\lambda = 3$, $a = 1$, donc $k = 1$ et on a les orbites correspondant exactement aux classes trouvées en annexe 2.

Conclusion. On a trouvé une forme réflexive $F_{4\mathbb{A}_2}$ de poids 36 et dont le diviseur est constitué de la composante correspondant à $H_{-2}(\bar{0})$ avec multiplicité 1, de la composante de type $H_{-6}(1, 1, 1, 1)$ avec multiplicité 9, de la composante $H_{-6}(2, 2, 2, 2)$ avec multiplicité 9 et des 6 composantes de type $H_{-2}(1^2 2^2)$ (où $[1^2 2^2]$ désigne un élément de $D(4\mathbb{A}_2)$ dont 2 coordonnées parmi les 4 sont égales à 1 et les 2 autres à 2) avec multiplicité 9.

Si $L = 5\mathbb{A}_2$; il existe un mot de poids 6 de H dont 5 lettres non nulles correspondent aux 5 copies de \mathbb{A}_2 que l'on considère. Ce mot correspond à un diviseur additionnel de type 1 vérifiant $l^{*2} = -\frac{4}{3}$, et \bar{l}^* d'ordre 3, donc d'après le lemme 2.1, la forme obtenue n'est pas réflexive et son diviseur admet une composante additionnelle de type 1.

Si $L = k\mathbb{A}_2$, $6 \leq k \leq 11$; la forme n'est jamais réflexive, et a toujours une composante additionnelle de type 1. En effet, choisissons 5 coordonnées parmi les k correspondantes au plongement de L choisi. Soit il existe un mot de poids 6 dont exactement 5 coordonnées non nulles correspondent à 5 des k copies de \mathbb{A}_2 que l'on considère, et alors comme précédemment cela prouve que la forme n'est pas réflexive et que son diviseur admet une composante additionnelle de type 1, soit les 6 lettres non nulles sont parmi les k copies de \mathbb{A}_2 . Dans ce cas, on a une composante additionnelle de type 0 et F_L n'est pas réflexive. De plus, considérant un mot de poids 6 dont 4 lettres non nulles sont choisies parmi les k copies de \mathbb{A}_2 et une en dehors des k copies, ce mot a 4 ou 5 lettres non nulles correspondant à des copies de \mathbb{A}_2 de L . Dans chaque cas cela donne un diviseur additionnel de type 1 au diviseur de F_L , comme annoncé.

Le réseau $N(24A_1)$

$G_2 = M_{24}$, ce groupe est 5-transitif sur les copies de \mathbb{A}_1 , donc tous les choix d'au plus 5 copies de \mathbb{A}_1 sont équivalents. Pour les autres choix, nous utiliserons le théorème 1.5 pour séparer les différentes formes obtenues, en fonctions des M_{24} -orbites des ensembles à k éléments de $\{1, \dots, 24\}$. Nous renvoyons à la partie correspondante pour les notations S_n , U_n , T_n ...

Les formes quadratiques discriminantes à considérer sont :

$$\begin{aligned} Q_{\mathbb{A}_1} : 0 &\mapsto 0, \\ \varepsilon_1 &\mapsto -\frac{1}{2}. \end{aligned}$$

On en déduit le fait général suivant, une composante additionnelle d'une $F_{k\mathbb{A}_1}$, $1 \leq k \leq 23$ est donnée par un mot de poids ≥ 5 . D'autre part, un mot dont exactement 5, 6, 7 ou 8 lettres non nulles correspondent aux copies de \mathbb{A}_1 de L ne peut se relever qu'en un mot de poids 8 de \mathcal{C}_{24} pour donner une composante additionnelle (ce qui correspond ici à des m^* de poids respectifs $-\frac{3}{2}$, -1 , $-\frac{1}{2}$, et 0). Seuls les deux premiers cas donnent des composantes réflexives. De même, un mot dont exactement 9, 10, 11 ou 12 lettres non nulles correspondent aux copies de \mathbb{A}_1 de L ne peut se relever qu'un un mot de poids 12 de \mathcal{C}_{24} pour donner une composante additionnelle (ce qui correspond ici à des m^* de poids respectifs $-\frac{3}{2}$, -1 , $-\frac{1}{2}$, et 0). On réalise le même raisonnement pour les mots de poids 16...

Si $L = \mathbb{A}_1$; on retrouve $F_{\mathbb{A}_1}$.

Si $L = 2\mathbb{A}_1$; on retrouve $F_{2\mathbb{A}_1}$.

Si $L = 3\mathbb{A}_1$; on retrouve $F_{3\mathbb{A}_1}$.

Si $L = 4\mathbb{A}_1$; on retrouve $F_{4\mathbb{A}_1}$.

Si $L = 5\mathbb{A}_1$; $5\mathbb{A}_1 = 19\mathbb{A}_1^\perp$, $\lambda = 4$, $w = 12 + \frac{1}{2}(19 * 2) = 31$.

Composantes additionnelles : nécessairement, elles correspondent à des mots de poids 8 du code dont 5 lettres non nulles correspondent aux 5 copies de \mathbb{A}_1 que l'on considère. Il y en a exactement un, car les octades spéciales de \mathcal{C}_{24} forment un système de Steiner $S(5, 8, 24)$.

Réflexivité : ordre 2 et $l^{*2} = -\frac{2}{4}$, d'après le lemme 2.1 ces vecteurs sont réflexifs.

Multiplicité : $2^3 = 8$

Orbites : paramètres $\lambda = 4$, $a = 1$, donc $k = 1$ et on a l'orbite $H_{-2}([1, 1, 1, 1, 1])$.

Conclusion. On a trouvé une forme réflexive $F_{5\mathbb{A}_1}$ de poids 31 et diviseur

$$\begin{aligned} &H_{-2}(\bar{0}) \cup H_{-2}([1, 0, 0, 0, 0]) \cup H_{-2}([0, 1, 0, 0, 0]) \cup H_{-2}([0, 0, 1, 0, 0]) \\ &\cup H_{-2}([0, 0, 0, 1, 0]) \cup H_{-2}([0, 0, 0, 0, 1]) \cup 9H_{-2}([1, 1, 1, 1, 1]). \end{aligned}$$

Si $L = 6\mathbb{A}_1$; $6\mathbb{A}_1 = 18\mathbb{A}_1^\perp$, $\lambda = 4$, $w = 12 + \frac{1}{2}(18 * 2) = 30$.

Il y a 2 orbites sous M_{24} . Soit les 6 coordonnées choisies forment un S_6 (6-ade spéciale), soit elles forment un U_6 (6-ade ombrable).

Cas 1 : S_6

Composantes additionnelles : soit ω le mot de poids 8 dont 6 lettres non nulles correspondent à nos 6 copies de \mathbb{A}_1 (existe par le fait qu'on soit dans un S_6 , et est unique puisque les octades spéciales forment un système de Steiner $S(5, 8, 24)$). ω donne une composante additionnelle. Les autres possibilités de composantes additionnelles sont données par des mots dont exactement 5 lettres correspondant à 5 des 6 copies de \mathbb{A}_1 sont non nulles. Mais alors, de tels mots auraient 5 composantes (au moins) communes avec ω , donc seraient égaux à ω , ce qui est absurde. il n'y a donc aucun autre diviseur.

Réflexivité : h_L est d'ordre 2, et $l^{*2} = -1 = -\frac{4}{4}$, donc d'après le lemme 2.1, ces vecteurs

sont réflexifs.

Multiplicité : 4, c'est le nombre de vecteurs de $2\mathbb{A}_1^*$ de carré -1 .

Orbites : paramètres $\lambda = 4, a = 2$, donc $k = 1$ et on a l'orbite $H_{-2}([1, 1, 1, 1, 1, 1])$.

Conclusion. On a trouvé une forme réflexive $F_{6\mathbb{A}_1}^{(1)}$ de poids 30 et diviseur

$$H_{-2}(\bar{0}) \cup \left(\bigcup_{i=1}^6 H_{-2} \left(\frac{\overline{v_i}}{2} \right) \right) \cup \left(\bigcup_{i_1, \dots, i_5 \in \llbracket 1, 6 \rrbracket} H_{-2} \left(\frac{\overline{v_{i_1} + \dots + v_{i_5}}}{2} \right) \right) \cup 4H_{-4} \left(\frac{\overline{v_1 + \dots + v_6}}{2} \right),$$

où $v_i, v_i^2 = -2$ engendre la i -ème copie de \mathbb{A}_1 .

Cas 2 : U_6

Composantes additionnelles : il n'existe donc pas de mot ω de poids 8 dont 6 lettres non nulles correspondent à nos 6 copies de \mathbb{A}_1 (car on est dans un U_6). Mais il existe $\binom{6}{5} = 6$ mots de poids 8 dont 5 lettres non nulles correspondent à exactement 5 de nos 6 copies de \mathbb{A}_1 (existe puisque les octades spéciales forment un système de Steiner $S(5, 8, 24)$).

Réflexivité : h_L est d'ordre 2, et $l^{*2} = -\frac{1}{2} = -\frac{2}{4}$, d'après le lemme 2.1, ces vecteurs sont réflexifs.

Multiplicité : 8, c'est le nombre de vecteurs de carré $-\frac{3}{2}$ de $3\mathbb{A}_1^*$.

Orbites : paramètres $\lambda = 4, a = 1$, donc $k = 1$ et on a les orbites $H_{-2} \left(\frac{\overline{v_{i_1} + \dots + v_{i_5}}}{2} \right), i_1, \dots, i_5 \in \llbracket 1, 6 \rrbracket$.

Conclusion. On a trouvé une forme réflexive $F_{6\mathbb{A}_1}^{(2)}$ de poids 30 et diviseur

$$H_{-2}(\bar{0}) \cup \left(\bigcup_{i=1}^6 H_{-2} \left(\frac{\overline{v_i}}{2} \right) \right) \cup \left(\bigcup_{i_1, \dots, i_5 \in \llbracket 1, 6 \rrbracket} 9H_{-2} \left(\frac{\overline{v_{i_1} + \dots + v_{i_5}}}{2} \right) \right),$$

où $v_i, v_i^2 = -2$ engendre la i -ème copie de \mathbb{A}_1 .

Si $L = 7\mathbb{A}_1$; $7\mathbb{A}_1 = 17\mathbb{A}_1^\perp, \lambda = 4, w = 12 + \frac{1}{2}(17 * 2) = 29$. Il y a 2 orbites sous M_{24} . Soit les 7 coordonnées choisies forment un S_7 , soit elles forment un U_7 .

Cas 1 : S_7

Composantes additionnelles : soit ω le mot de poids 8 dont 7 lettres non nulles correspondent à nos 7 copies de \mathbb{A}_1 (existe par le fait qu'on soit dans un S_7 , et est unique puisque les octades spéciales forment un système de Steiner $S(5, 8, 24)$). ω donne une composante additionnelle.

Réflexivité : h_L est d'ordre 2, et $l^{*2} = -\frac{3}{2} = -\frac{6}{4}$, d'après le lemme 2.1 ces vecteurs ne sont pas réflexifs.

On a trouvé une forme non réflexive, dont le diviseur admet une composante additionnelle de type 1.

Cas 2 : U_7

Composantes additionnelles : d'après le théorème 1.5, 6 des 7 coordonnées correspondant à L forment un S_6 , et c'est l'unique S_6 contenu dans ce U_7 . Soit ω le mot de poids 8

correspondant dans \mathcal{C}_{24} , il définit une composante additionnelle. Les autres composantes additionnelles possibles correspondent à des mots de poids 8 dont exactement 5 lettres non nulles correspondent à L . Ces 5 lettres ne peuvent coïncider avec 5 lettres non nulles de ω (il y a au plus 4 lettres non nulles communes), donc nécessairement, l'une est la coordonnée qu'il faut enlever à U_7 pour obtenir le S_6 , et les 4 autres sont à choisir dans 4 coordonnées parmi les 6 du S_6 , ce qui donne 15 possibilités. Et ces 15 mots existent, puisque les octades spéciales de \mathcal{C}_{24} forment un système de Steiner $S(5, 8, 24)$ (on fixe 5 coordonnées, il existe un unique mot de poids 8 correspondant, et on a prouvé qu'il ne pouvait être égal à ω , donc 3 lettres non nulles sont "en dehors" de L).

Réflexivité : cas de ω : h_L d'ordre 2, et $l^{*2} = -1 = -\frac{4}{4}$, d'après le lemme 2.1, ces vecteurs sont réflexifs ;

autres cas : h_L d'ordre 2, et $l^{*2} = -\frac{1}{2} = -\frac{2}{4}$, d'après le lemme 2.1, ces vecteurs sont réflexifs.

Orbites : cas de ω : paramètres $\lambda = 4, a = 2$, donc $k = 1$ et on a l'orbite $H_{-4} \left(\frac{v_1 + \dots + v_5}{2} \right)$, où l'on a supposé pour simplifier que les 6 coordonnées correspondant à S_6 sont les 6 premières ;

autres cas : paramètres $\lambda = 4, a = 1$, donc $k = 1$ et on a les orbites $H_{-2} \left(\frac{v_{i_1} + \dots + v_{i_4} + v_7}{2} \right)$, $i_1, \dots, i_4 \in \llbracket 1, 6 \rrbracket$.

Conclusion. On a trouvé une forme réflexive F_{7A_1} de poids 29 et diviseur

$$H_{-2}(\bar{0}) \cup \left(\bigcup_{i=1}^7 H_{-2} \left(\frac{v_i}{2} \right) \right) \cup \left(\bigcup_{i_1, \dots, i_5 \in \llbracket 1, 6 \rrbracket} H_{-2} \left(\frac{v_{i_1} + \dots + v_{i_5}}{2} \right) \right) \\ \cup \left(\bigcup_{i_1, \dots, i_4 \in \llbracket 1, 6 \rrbracket} 9H_{-2} \left(\frac{v_{i_1} + \dots + v_{i_4} + v_7}{2} \right) \right) \cup H_{-4} \left(\frac{v_1 + \dots + v_6}{2} \right).$$

Si $L = 8A_1$; $8A_1 = 16A_1^\perp$, $\lambda = 4$, $w = 12 + \frac{1}{2}(16 * 2) = 28$.

Il y a 3 orbites sous M_{24} . Soit les 8 coordonnées choisies forment un S_8 , soit elles forment un U_8 , soit elles forment un T_8 .

Cas 1 : S_8

Composantes additionnelles : ces coordonnées correspondent à un (et un seul) mot ω de poids 8 de \mathcal{C}_{24} . Il définit alors une composante additionnelle de type 0, la forme F_L n'est pas réflexive. Mais, toute autre composante additionnelle serait déterminée par un mot de poids 8 de \mathcal{C}_{24} dont 5, 6 ou 7 lettres non nulles serait dans ce S_8 . Ceci est impossible, deux octades spéciales n'ayant que 0, 2, 4 ou 8 coordonnées en commun. Il n'y a donc pas de composantes additionnelles de type 1. Ainsi, la forme $F_{M_N^\perp}$ est une forme strictement -2 -réflexive de poids 28.

Conclusion. on a trouvé une nouvelle forme strictement -2 -réflexive $F_{(16A_1)_N^\perp}$ de poids 28.

Cas 2 : U_8

Composantes additionnelles : il n'y a ni S_7 , ni S_8 dans un U_8 , mais des S_6 ou des S_5 , la forme obtenue est donc réflexive. Le calcul explicite précis du diviseur est fait en annexe

2. Nous pouvons préciser ici les multiplicités, les composantes correspondant à des S_5 sont de multiplicité $2^3 = 8$, et celles correspondant à des S_6 sont de multiplicité $2^2 = 4$.

Conclusion. On a trouvé une forme réflexive $F_{8\mathbb{A}_1}$ de poids 28, dont le diviseur est constitué de la composante $H_{-2}(\bar{0})$ avec multiplicité 1, des 8 composantes caractérisées par des -2 -vecteurs de $2U \oplus 8\mathbb{A}_1$ de type $H_{-2}(1^1 0^7)$ (où $[0^1 1^7]$ désigne une classe de $D(8\mathbb{A}_1)$ dont une coordonnée parmi les 8 est 1 et les 7 autres valent 0) avec multiplicité 1, de 24 composantes de type $H_{-2}(1^5 0^3)$ avec multiplicité 1, des 32 autres de type $H_{-2}(1^5 0^3)$ avec multiplicité 9 et de 4 composantes de type $H_{-4}(1^6 0^2)$ avec multiplicité 4.

Cas 3 : T_8

Composantes additionnelles : d'après le théorème 1.5, il existe un S_7 dans T_8 . D'après le raisonnement fait dans le cas S_7 du réseau $L = 7\mathbb{A}_1$, cela conduit à l'existence d'une composante additionnelle de type 1 du diviseur de F_L , qui n'est donc pas réflexive, et $8\mathbb{A}_1$ dans ce cas là n'est pas le sous-réseau de racines d'un réseau donnant une forme strictement -2 -réflexive.

Si $L = 9\mathbb{A}_1$; $9\mathbb{A}_1 = 15\mathbb{A}_1^\perp$, $\lambda = 4$, $w = 12 + \frac{1}{2}(15 * 2) = 27$.

Il y a 3 orbites sous M_{24} . Soit les 9 coordonnées choisies forment un S_9 , soit elles forment un U_9 , soit elles forment un T_9 .

Cas 1 : S_9

Composantes additionnelles : la forme n'est pas réflexive puisqu'il existe un S_8 dans ce S_9 (par définition). Il reste à montrer qu'il existe une composante additionnelle. Soit ω le mots de poids 8 correspondant au S_8 , on considère l'octade obtenue en complétant les 5 coordonnées qui sont, d'une part la coordonnées de S_9 correspondant à une lettre nulle de ω , et 4 lettres non nulles ω . Le mot de poids 8 ω' ainsi obtenu a nécessairement exactement 4 lettres communes avec ω (voir par exemple le théorème 1.4), et donc 3 de ses lettres non nulles sont dans le complémentaire de U_9 , et donc ω' induit une composante additionnelle de type 1 au diviseur de $F_{9\mathbb{A}_1}$.

Cas 2 : U_9

Composantes additionnelles : il n'y a ni S_7 , ni S_8 dans un U_9 , mais des S_6 ou des S_5 . De même, $U_9 \subset U_{12}$, mais les composantes additionnelles obtenues à partir de dodécades ombrales sont réflexives, car le h_L correspondant serait de norme $-\frac{1}{2} \pmod{2}$. La forme obtenue est donc réflexive. Le calcul explicite précis du diviseur est fait en annexe 2. Nous pouvons préciser ici les multiplicités, les composantes correspondant à des S_5 sont de multiplicité $2^3 = 8$, celles correspondant à des S_6 sont de multiplicité $2^2 = 4$, et celle correspondant à U_{12} est de multiplicité $2^3 = 8$.

Conclusion. On a trouvé une forme réflexive $F_{9\mathbb{A}_1}$ de poids 27, dont le diviseur est constitué de la composante $H_{-2}(\bar{0})$ avec multiplicité 1, des 9 composantes de type $H_{-2}(1^1 0^8)$ avec multiplicité 1, de 72 composantes de type $H_{-2}(1^5 0^4)$ avec multiplicité 1, des 54 autres de type $H_{-2}(1^5 0^4)$ avec multiplicité 9, de 12 composantes de type $H_{-4}(1^6 0^3)$ avec multiplicité 4 et de la composante $H_{-2}(1, 1, 1, 1, 1, 1, 1, 1)$ avec multiplicité 9.

Cas 3 : T_9

Composantes additionnelles : il existe un S_7 dans T_9 (mais pas de S_8), donc il y a une composante additionnelle de type 1 non réflexive.

Si $L = 10\mathbb{A}_1$; $10\mathbb{A}_1 = 14\mathbb{A}_1^\perp$, $\lambda = 4$, $w = 12 + \frac{1}{2}(14 * 2) = 26$.

Il y a 3 orbites sous M_{24} . Soit les 10 coordonnées choisies forment un S_{10} , soit elles forment un U_{10} , soit elles forment un T_{10} .

Cas 1 : S_{10}

Composantes additionnelles : la forme n'est pas réflexive puisqu'il existe un S_8 dans ce S_{10} (par définition). Il reste à montrer qu'il existe une composante additionnelle. Soit ω le mots de poids 8 correspondant au S_8 , on considère l'octade obtenue en complétant les 5 coordonnées qui sont, d'une part une coordonnée de S_{10} correspondant à une lettre nulle de ω , et 4 lettres non nulles ω . Le mot de poids 8 ω' ainsi obtenu a nécessairement exactement 4 lettres communes avec ω (voir par exemple le théorème 1.4), et donc 2 ou 3 de ses lettres non nulles sont dans le complémentaire de U_{10} , et donc ω' induit une composante additionnelle de type 1 au diviseur de $F_{10\mathbb{A}_1}$.

Cas 2 : U_{10}

Composantes additionnelles : il n'y a ni S_7 , ni S_8 dans un U_{10} , mais des S_6 ou des S_5 . De même, $U_{10} \subset U_{12}$, mais les composantes additionnelles obtenue à partir de dodécades ombrales sont réflexives, car le h_L correspondant serait de norme $-\frac{1}{2} \pmod{2}$ ou -1 . La forme obtenue est donc réflexive. Le calcul explicite précis du diviseur est fait en annexe 2. Nous pouvons préciser ici les multiplicités, les composantes correspondant à des S_5 sont de multiplicité $2^3 = 8$, celles correspondant à des S_6 sont de multiplicité $2^2 = 4$, et celle correspondant à U_{12} est de multiplicité $2^2 = 4$.

Conclusion. On a trouvé une forme réflexive $F_{10\mathbb{A}_1}$ de poids 26, dont le diviseur est constitué de la composante $H_{-2}(\bar{0})$ avec multiplicité 1, des 10 composantes de type $H_{-2}(1^1 0^9)$ avec multiplicité 1, de 180 composantes de type $H_{-2}(1^5 0^5)$ avec multiplicité 1, des 72 autres de type $H_{-2}(1^5 0^5)$ avec multiplicité 9, de 30 composantes de type $H_{-4}(1^6 0^3)$ avec multiplicité 4, de 10 composantes de type $H_{-2}(1^9 0^1)$ avec multiplicité 1 et de la composante $H_{-2}(1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$ avec multiplicité 4.

Cas 3 : T_{10}

Composantes additionnelles : il existe un S_7 dans T_{10} (mais pas de S_8), donc il y a une composante additionnelle de type 1 non réflexive.

Si $L = 11\mathbb{A}_1$; $11\mathbb{A}_1 = 13\mathbb{A}_1^\perp$, $\lambda = 4$, $w = 12 + \frac{1}{2}(13 * 2) = 25$.

Il y a 3 orbites sous M_{24} . Soit les 11 coordonnées choisies forment un S_{11} , soit elles forment un U_{11} , soit elles forment un T_{11} .

Cas 1 : S_{11}

Composantes additionnelles : la forme n'est pas réflexive puisqu'il existe un S_8 dans ce S_{11} (par définition). Il reste à montrer qu'il existe une composante additionnelle. Soit ω le mots de poids 8 correspondant au S_8 , on considère l'octade obtenue en complétant

les 5 coordonnées qui sont, d'une part une coordonnée de S_{11} correspondant à une lettre nulle de ω , et 4 lettres non nulles ω . Le mot de poids 8 ω' ainsi obtenu a nécessairement exactement 4 lettres communes avec ω (voir par exemple le théorème 1.4), et donc 1, 2 ou 3 de ses lettres non nulles sont dans le complémentaire de U_{11} , et donc ω' induit une composante additionnelle de type 1 au diviseur de F_{11A_1} .

Cas 2 : U_{11}

Composantes additionnelles : il n'y a ni S_7 , ni S_8 dans un U_{10} , mais des S_6 ou des S_5 . Cependant, $U_{10} \subset U_{12}$, il y a donc une composante additionnelle de type 1 induite par la dodécade ombrale U_{12} , et cette composante est non réflexive (h_L de carré $-\frac{3}{2}$, voir lemme 2.1).

Cas 3 : T_{11}

Composantes additionnelles : il existe un S_7 dans T_{11} (mais pas de S_8), donc il y a une composante additionnelle de type 1 non réflexive.

Si $L = 12A_1$; $12A_1 = 12A_1^\perp$, $\lambda = 4$, $w = 12 + \frac{1}{2}(12 * 2) = 24$.

Il y a 5 orbites sous M_{24} . Les 12 coordonnées choisies forment soit un S_{12}^+ , soit un S_{12} , soit un T_{11} , soit un U_{12}^- , soit un U_{12} .

Cas 1 : S_{12}^+

Composantes additionnelles : la forme n'est pas réflexive puisqu'il existe un S_8 dans ce S_{12}^+ (par définition). Plus précisément, soient $\omega_1, \omega_2, \omega_3$ les trois mots de poids 8 contenus dans S_{12}^+ (voir la définition d'un S_{12}^+ , donnée avant le théorème 1.5). Ces 3 mots divisent S_{12}^+ en 3 tétrades (que l'on dira associées à S_{12}^+). On considère le mot de poids 8 ω' obtenu en fixant les 5 coordonnées suivantes : 2 parmi une tétrade associée à S_{12}^+ , 2 autres parmi une deuxième tétrade associée à S_{12}^+ , et une dernière dans une tétrade associée à S_{12}^+ . ω' intersecte alors l'un des 3 mots de poids 8 en au moins 4 coordonnées (disons que c'est ω_1 , quitte à réindexer), et les deux autres en 3 coordonnées au moins. D'après le théorème 1.4, on déduit que ω' intersecte chaque mot ω_i en 4 coordonnées exactement. Ce qui définit exactement 6 lettres non-nulles parmi S_{12}^+ , et donc ω' induit une composante additionnelle de type 1 au diviseur de F_L .

Cas 2 : S_{12}

Composantes additionnelles : la forme n'est pas réflexive puisqu'il existe un S_8 dans ce S_{12} (par définition). Soit ω le mot de poids 8 correspondant. On considère le mot de poids 8 ω' obtenu en fixant les 5 coordonnées suivantes : 2 parmi S_8 , et 3 parmi les 4 coordonnées restantes dans S_{12} . Supposons par l'absurde que les 3 coordonnées complémentaires soient toutes dans S_{12} . Alors nous obtiendrions dans S_{12} deux octades disjointes, dont la somme serait une autre octade (nécessairement), et ainsi cet ensemble de 3 octades formerait un S_{12}^+ , ce qui est absurde car nous avons supposé avoir ("seulement") un S_{12} . Donc 1, 2 ou 3 coordonnées complémentaires sont dans le complémentaire du S_{12} , nous avons donc établi l'existence d'une composante additionnelle de type 1 au diviseur de F_L .

Cas 3 : T_{12}

Composantes additionnelles : il existe un S_7 dans T_{12} (mais pas de S_8), donc il y a une composante additionnelle de type 1 non réflexive.

Cas 4 : U_{12}^-

Composantes additionnelles : un U_{12}^- contient tous les points, sauf un, d'une dodécade spéciale. Soit τ le mot de poids 12 correspondant à cette dodécade spéciale, il induit donc sur U_{12}^- une composante additionnelle de type 1, dont le h_L est de norme $-\frac{3}{2}$, et donc d'après le lemme 2.1, cette composante n'est pas réflexive.

Cas 5 : U_{12}

Composantes additionnelles : la forme n'est pas réflexive puisqu'il existe un U_{12} dans ce U_{12} (!). Montrons l'existence d'une composante additionnelle. En effet, il existe un S_6 dans U_{12} , mais ni S_7 ni S_8 , donc le mot de poids 8 ω obtenu en "relevant" ce S_6 , a 6 lettres non nulles exactement parmi U_{12} , et 2 dans le complémentaire de U_{12} , il définit donc une composante additionnelle de type 1 au diviseur de F_L .

Si $L = k\mathbb{A}_1$, $13 \leq k \leq 23$; nous allons montrer que toutes les formes obtenues ainsi ont (au moins) une composante additionnelle de type 1, et ne sont pas réflexives.

Le dernier point est clair, toutes les n -ades considérées contiennent soit un S_8 , soit un U_{12} (donc des mots de poids 8 ou 12 qui induisent des composantes additionnelles de type 0). Traitons ces cas par orbites.

Orbites S_{13}, S_{14}, S_{15} : le complémentaire d'un tel ensemble contient un S_8 (par définition), le mot de poids 8 lui correspondant sera noté ω . Ainsi, il existe un mot de poids 16 (obtenu en considérant la somme du mot de poids 24 et de ω), tel que toutes les coordonnées correspondant à S_{13}, S_{14} ou S_{15} soient non nulles, et donc, 3, 2 ou 1 (respectivement) lettres non nulles se trouvent dans le complémentaires de S_{13}, S_{14} ou S_{15} . On a donc montré l'existence de composantes additionnelles de type 1.

Orbites S_k , $16 \leq k \leq 20$: le complémentaire d'un tel ensemble contient un S_8 , ou contient une n -ade qui se complète en un S_8 (par définition). Le mot de poids 8 lui correspondant sera noté ω . D'après le théorème 1.4, il existe (au moins) un mot de poids 8, noté ω' , qui a exactement 2 lettres non nulles en commun avec ω , que l'on choisit comme étant 2 lettres qui ne sont pas dans le S_k considéré (possible puisque $k \leq 20$). Ce mot ω' a donc exactement deux lettres non nulles dans le complémentaire de notre S_k , et induit donc une composante additionnelle de type 1.

Orbites S_k , $21 \leq k \leq 23$: le complémentaire d'un tel ensemble contient un S_8 , ou contient une n -ade qui se complète en un S_8 (par définition). Le mot de poids 8 lui correspondant sera noté ω . Ce mot a 1, 2 ou 3 lettres non nulles dans le complémentaire de S_k , et induit donc une composante additionnelle de type 1.

Orbites T_k , $13 \leq k \leq 16$: d'après le théorème 1.5, T_k contient un U_{12}^- mais pas de U_{12} . Reprenant le raisonnement fait pour U_{12}^- (cas $L = 11\mathbb{A}_1$), on montre que F_L admet une

composante additionnelle de type 1.

Orbite U_{14} : le complémentaire de U_{14} est un U_{10} , il y a dans ce U_{10} un S_6 , qui se relève donc en un S_8 correspondant à un mot de poids 8 ω . 2 lettres non nulles de ω sont parmi U_{14} , les 6 autres sont dans le complémentaire. D'après le théorème 1.4, il existe 30 octades spéciales qui n'intersectent pas ω . Ainsi, chacun des mots de poids 8 correspondant à ces octades a 0, 1, 2, 3 ou 4 lettres non nulles dans le complémentaire de U_{14} . Combien peuvent en avoir 4 ? Au plus 5. Les 4 coordonnées en question étant fixées (il reste 4 places libres), d'après le théorème 1.4, s'il en existe un, il y en a exactement 4 autres qui coïncident avec lui en ces 4 coordonnées. Il reste donc au moins 25 mots de poids 8 dont 0, 1, 2 ou 3 lettres non nulles sont dans le complémentaire de U_{14} . Montrons qu'il ne peut y avoir plus d'un mot dont toutes les lettres non nulles sont dans U_{14} . En effet, s'il en existe 2, il en existe 3 (considérer la somme de ces deux mots), et alors ces trois mots forment un S_{12}^+ , or d'après le théorème 1.5, c'est impossible, $S_{12}^+ \not\subset U_{14}$. Donc il reste au moins 24 octades dont 1, 2 ou 3 lettres non nulles sont dans le complémentaire de U_{14} , et définissent donc des composantes additionnelles de type 1.

Orbites U_k , $15 \leq k \leq 17$: le complémentaire d'un tel ensemble contient un S_6 mais pas de S_7 ni de S_8 (théorème 1.5), le mot de poids 8 lui correspondant sera noté ω . Il a 2 lettres non nulles dans U_k et 6 dans le complémentaire de U_k . Ainsi, il existe un mot de poids 16 (obtenu en considérant la somme du mot de poids 24 et de ω), tel que $k - 2$ coordonnées exactement correspondant à U_k soient non nulles, et donc, $18 - k \in \llbracket 1, 3 \rrbracket$ lettres non nulles se trouvent dans le complémentaire de U_k . On a donc montré l'existence de composantes additionnelles de type 1.

Orbite U_{18} : le complémentaire d'un tel ensemble contient un S_5 mais pas de S_6 , S_7 ni de S_8 (théorème 1.5), le mot de poids 8 lui correspondant sera noté ω . Il a 3 lettres non nulles dans U_{18} et 5 dans le complémentaire de U_{18} . Ainsi, il existe un mot de poids 16 (obtenu en considérant la somme du mot de poids 24 et de ω), tel que 15 coordonnées exactement correspondant à U_{18} soient non nulles, et donc, 1 lettre non nulle se trouve dans le complémentaire de U_{18} . On a donc montré l'existence de composantes additionnelles de type 1.

Chapitre 4

A propos du groupe modulaire maximal pour la quasi-restriction

On reprend les notations des parties précédentes, N est un réseau de Niemeier différent du réseau de Leech (défini négatif par convention), L un sous-réseau non-nul de N , et M un sous-réseau de N tel que $L \perp M$ et $\text{rg}(L \oplus M) = \text{rg}(N)$.

4.1 Prolongement des automorphismes

La forme modulaire que l'on obtient par la méthode de quasi-restriction est, d'après le théorème 2.2, modulaire pour le groupe stable orthogonal associé au réseau $2U \oplus L$.

Mais ce groupe est-il le plus grand groupe (pour l'inclusion) pour lequel la forme F_L est modulaire (quitte à rajouter un caractère) ?

Un élément $Z \in \mathcal{D}^0(2U \oplus N)$ peut s'écrire $Z = Z_1 + Z_2$, où $Z_1 \in \mathcal{D}^0(2U \oplus L)$ et $Z_2 \in M \otimes \mathbb{C}$ (donc en particulier $Z_1 \perp Z_2$). On rappelle la définition de la forme modulaire F_L :

$$F_L(Z_1) = \frac{\Phi_{12}(Z_1 + Z_2)}{\prod_{\{\pm r\} \in R_M} (Z_1 + Z_2 | r)} \Big|_{\mathcal{D}^0(2U \oplus L)},$$

et l'égalité vaut pour tous $Z_1 \in \mathcal{D}^0(2U \oplus L)$ et $Z_2 \in M \otimes \mathbb{C}$ tels que $Z_1 + Z_2 \in \mathcal{D}^0(2U \oplus N)$.

Pour donner un sens à l'action de $g_1 \in O^+(2U \oplus L)$ sur F_L , il faut en particulier définir l'action de g_1 sur Φ_{12} . Il est donc nécessaire de pouvoir prolonger l'application g_1 en un élément de $O^+(2U \oplus N)$ (si g_1 ne se prolonge pas, alors l'action de g_1 sur F_L n'est pas bien définie).

Nous allons donner une condition nécessaire et suffisante pour prolonger un élément de $O^+(2U \oplus L)$. On rappelle que l'on dispose de l'application

$$\Psi^+ : \begin{array}{ccc} O^+(L) & \rightarrow & O(D(L)) \\ g & \mapsto & \bar{g} \end{array},$$

où \bar{g} est l'application induite par g sur $O(D(L))$.

Le noyau de cet homomorphisme de groupe est $\tilde{O}^+(L)$ et nous avons étudié, dans certains cas particuliers, la surjectivité de Ψ^+ (voir partie 1.3.6).

On suppose maintenant que L est primitif (i.e. $L = M_N^\perp$), c'est une condition nécessaire de réflexivité pour la forme F_L (proposition 2.1), donc, compte-tenu de ce qui nous intéresse, ce n'est pas restrictif.

On rappelle aussi que des inclusions

$$(2U \oplus L) \oplus M \subset 2U \oplus N \subset (2U \oplus L)^* \oplus M^*,$$

on tire que

$$H = (2U \oplus N)/((2U \oplus L) \oplus M) \cong N/(L \oplus M) \subset D(L) \oplus D(M),$$

et on dispose des projections

$$p_L : H \rightarrow L^*/L = D(L), \quad p_M : H \rightarrow M^*/M = D(M).$$

L'étude de ces objets a été faite en partie 2.2.2.

La proposition qui suit est une généralisation du lemme 1.12 :

Proposition 4.1. (*[N79], p.111 et [GHS08-1] partie 3*)

On suppose L primitif et $M = L_N^\perp$. Un élément $g_1 \in O^+(2U \oplus L)$ se prolonge en un élément $g \in O^+(2U \oplus N)$ si et seulement si

- (i) $\bar{g}_1(p_L(H)) = p_L(H)$ (stabilité d'une partie du code),
- (ii) Il existe $h \in O(M)$ tel que $p_M^{-1} \circ \bar{h} \circ p_M = p_L^{-1} \circ \bar{g}_1 \circ p_L$.

On retrouve le lemme 1.12, en effet, si $g_1 \in \tilde{O}^+(2U \oplus L)$, alors \bar{g}_1 est l'identité, donc (i) est vérifié, et posant $h = id$, (ii) est aussi vérifié, on peut prolonger g_1 . C'est l'argument utilisé dans la preuve du théorème 2.2 pour dire que F_L est modulaire pour $\tilde{O}^+(2U \oplus L)$.

Remarque importante 3. Comme lors des remarques importantes précédentes, si on suppose seulement L primitif, mais pas forcément $M = L_N^\perp$, on obtient une version faible de la proposition 4.1, qui donne l'existence d'un prolongement $g \in O^+(2U \oplus N)$ mais pas l'unicité. C'est ce que nous utiliserons en pratique dans la suite.

4.2 Transformation de F_L

Supposons maintenant avoir prolongé $g_1 \in O^+(2U \oplus L)$ en un élément $g \in O^+(2U \oplus N)$. Quelle est alors la loi de transformation de F_L sous l'action de g_1 ?

Par construction, g laisse stable $(2U \oplus L) \otimes \mathbb{Q}$ et $M \otimes \mathbb{Q}$, la matrice de g dans une base de $(2U \oplus N) \otimes \mathbb{Q}$ respectant cette décomposition est donc de la forme

$$\left(\begin{array}{c|c} G_1 & 0 \\ \hline 0 & H \end{array} \right),$$

où G_1 et H sont les matrices de g_1 et h respectivement dans les bases correspondantes de la décomposition. On a alors

a. $g(2U \oplus L) = 2U \oplus L$, $g(M) = M$ et $g(R_M) = R_M$ (on rappelle que R_M est l'ensemble des racines de M).

b. M étant défini négatif, les éléments de la forme

$$\left(\begin{array}{c|c} I & 0 \\ \hline 0 & H \end{array} \right) \in O_{\mathbb{R}}(2U \oplus N)$$

sont de norme spinorielle 1, et ceux de la forme

$$\left(\begin{array}{c|c} G_1 & 0 \\ \hline 0 & I \end{array} \right) \in O_{\mathbb{R}}(2U \oplus N)$$

sont de même norme spinorielle que G_1 , donc $g_1 \in O^+(2U \oplus L) \Leftrightarrow g \in O^+(2U \oplus N)$.

Enfin, calculons la transformation induite par g_1 : pour tous $Z_1 \in \mathcal{D}^0(2U \oplus L)$ et $Z_2 \in M \otimes \mathbb{C}$ tels que $Z_1 + Z_2 \in \mathcal{D}^0(2U \oplus N)$, pour tout $g_1 \in O^+(2U \oplus L)$ se prolongeant en $g \in O^+(2U \oplus N)$,

$$\begin{aligned} F_L(g(Z_1)) &= \frac{\Phi_{12}(g(Z_1 + Z_2))}{\prod_{\{\pm r\} \in R_M} (g(Z_1 + Z_2)|r)} \Big|_{\mathcal{D}^0(2U \oplus L)} \\ &= \det(g) \frac{\Phi_{12}(Z_1 + Z_2)}{\prod_{\{\pm r\} \in R_M} (Z_1 + Z_2|g^{-1}(r))} \Big|_{\mathcal{D}^0(2U \oplus L)} \\ &= \det(g) \frac{\Phi_{12}(Z_1 + Z_2)}{\prod_{\{\pm r\} \in R_M} (Z_1 + Z_2|r)} \Big|_{\mathcal{D}^0(2U \oplus L)} \\ &= \det(g) F_L(Z_1), \end{aligned}$$

où on a utilisé le fait que $g(R_M) = R_M$.

On remarque que la transformation est bien modulaire, seul le caractère a changé, c'est maintenant $\det(g) = \det(g_1) \det(h)$ au lieu de $\det(g_1)$. De plus, la description du diviseur peut se trouver simplifiée, des éléments qui n'étaient pas dans la même $\tilde{O}^+(2U \oplus L)$ -orbite peuvent maintenant se trouver dans la même orbite pour le groupe modulaire maximal de F_L .

4.3 Retour sur les formes obtenues

Nous allons donc maintenant essayer de calculer, pour chacune des formes réflexives que nous avons obtenues dans les parties précédentes, le groupe modulaire maximal. On reprend la même méthodologie que dans la partie 3.2.2, pour chaque réseau de Niemeier différent du réseau de leech, nous considérons les formes réflexives F_L que l'on a trouvées dans les parties 3.1.2 et 3.2.2, nous rappelons l'image de l'application Ψ^+ étudiée en

partie 1.3.6, et en étudions les relèvements. A l'aide de la proposition 4.1 et des tables de la partie 1.4.2, nous pouvons déterminer le groupe modulaire maximal de chacune des formes trouvées.

Le réseau $N(D_{16} + E_8)$

Forme $F_{\mathbb{E}_8}$. La forme $F_{\mathbb{E}_8}$ que nous avons obtenue est modulaire pour $\tilde{O}(2U \oplus L) = O(2U \oplus L)$.

Conclusion. On dispose de la forme $F_{\mathbb{E}_8}$ de poids 252 pour le groupe $O^+(2U \oplus \mathbb{E}_8)$ et le caractère déterminant. Son diviseur est $H_{-2}([0])$.

Le réseau $N(3E_8)$

Formes $F_{2\mathbb{E}_8}$ et $F_{3\mathbb{E}_8}$. Les formes $F_{2\mathbb{E}_8}$ et $F_{3\mathbb{E}_8}$ que nous avons obtenues sont modulaires pour $\tilde{O}^+(2U \oplus L) = O^+(2U \oplus L)$.

Conclusion. On dispose de la forme $F_{2\mathbb{E}_8}$ de poids 132 pour le groupe $O^+(2U \oplus 2\mathbb{E}_8)$ et le caractère déterminant. Son diviseur est $H_{-2}([0])$.

Conclusion. On dispose de la forme $F_{3\mathbb{E}_8} = \Phi_{12}$ de poids 12 pour le groupe $O^+(2U \oplus 3\mathbb{E}_8)$ et le caractère déterminant. Son diviseur est $H_{-2}([0])$.

Le réseau $N(2D_{12})$

Forme $F_{\mathbb{D}_{12}}$. Nous avons obtenu la forme $F_{\mathbb{D}_{12}}$, de poids 144. Ici, $O(D(2U \oplus L))$ n'est pas trivial, d'après la partie 1.3.6, $O(D(2U \oplus \mathbb{D}_{12})) \cong \mathcal{S}_3$, et Ψ^+ est surjective. Reprenant les notations de la partie 1.3.6, il s'agit ici de prolonger les réflexions de $O^+(2U \oplus \mathbb{D}_{12})$, σ_{l_1} , σ_{ε_2} et σ_{l_3} . Or, la lecture des tables de H (partie 1.4.2), montre que pour prolonger σ_{l_1} , il faut réaliser $\tau_{[1],[3]}$ la transposition des classes [1] et [3] dans $D(M)$, ce qui peut se faire (toujours d'après la partie 1.3.6) par la réflexion $\sigma_{\varepsilon_2} \in O(\mathbb{D}_{12})$ (cette fois-ci on réalise les automorphismes dans la deuxième copie de \mathbb{D}_{12} , bien que nous utilisions les mêmes notations, le contexte étant assez clair pour ne pas surcharger les notations). En revanche, pour prolonger $\sigma_{\varepsilon_2} \in O^+(2U \oplus \mathbb{D}_{12})$ et $\sigma_{l_3} \in O^+(2U \oplus \mathbb{D}_{12})$, il faudrait relever $\tau_{[2],[3]}$ et $\tau_{[1],[2]}$ respectivement, dans $O^+(M)$, ce qui d'après la partie 1.3.6 n'est pas possible. Ainsi, nous avons montré que le groupe modulaire maximal de $F_{\mathbb{D}_{12}}$ est le groupe $\Gamma = \langle \tilde{O}^+(2U \oplus \mathbb{D}_{12}), \sigma_{l_1} \rangle$, qui est un sous-groupe d'indice 2 de $O^+(2U \oplus L)$ plus grand que $\tilde{O}^+(2U \oplus L)$. Le caractère est $\chi : g \in \tilde{O}^+(2U \oplus L) \mapsto \det(g)$, $\sigma_{l_1} \mapsto 1$. Enfin, le diviseur de $F_{\mathbb{D}_{12}}$ est inchangé.

Conclusion. On dispose de la forme $F_{\mathbb{D}_{12}}$ de poids 144 pour le groupe $\Gamma \subset O^+(2U \oplus \mathbb{D}_{12})$ d'indice 2 et le caractère $\chi : g \in \tilde{O}^+(2U \oplus L) \mapsto \det(g)$, $\sigma_{l_1} \mapsto 1$. Son diviseur est $H_{-2}([0]) \cup 24H_{-4}([1])$.

Le réseau $N(A_{17} + E_7)$

Forme $F_{\mathbb{E}_7}$. La forme $F_{\mathbb{E}_7}$ est modulaire pour $\tilde{O}(2U \oplus L) = O(2U \oplus L)$.

Conclusion. On dispose de la forme $F_{\mathbb{E}_7}$ de poids 165 pour le groupe $O^+(2U \oplus \mathbb{E}_7)$ et le caractère déterminant. Son diviseur est $H_{-2}([0])$.

Le réseau $N(D_{10} + 2E_7)$

Forme $F_{\mathbb{E}_7}$. Déjà traitée.

Forme $F_{2\mathbb{E}_7}$. Nous avons obtenu la forme $F_{2\mathbb{E}_7}$ de poids 102. D'après la partie 1.3.6, $O(D(2U \oplus 2\mathbb{E}_7)) \cong \mathbb{Z}/2\mathbb{Z}$, et Ψ^+ est surjective. L'élément non trivial consiste en l'échange des copies de \mathbb{E}_7 , on le notera $g_1 \in O^+(2U \oplus 2\mathbb{E}_7)$. On a $\det g_1 = (-1)^7 = -1$. La lecture des tables de H (partie 1.4.2), montre que pour prolonger g_1 , il faut réaliser $\tau_{[1],[3]}$ la permutation des classes [1] et [3] dans $D(M)$, ce qui peut se faire (d'après la partie 1.3.6) par la réflexion $\sigma_{\varepsilon_2} \in O(\mathbb{D}_{10})$.

Nous avons montré que le groupe modulaire maximal de $F_{2\mathbb{E}_7}$ est le groupe $O^+(2U \oplus 2\mathbb{E}_7)$. Le caractère est $\chi : g \in \tilde{O}^+(2U \oplus L) \mapsto \det(g)$, $g_1 \mapsto 1$. Enfin, le diviseur de $F_{2\mathbb{E}_7}$ est inchangé.

Conclusion. On dispose de la forme $F_{2\mathbb{E}_7}$ de poids 102 pour le groupe $O^+(2U \oplus 2\mathbb{E}_7)$ et le caractère $\chi : g \in \tilde{O}^+(2U \oplus L) \mapsto \det(g)$, $g_1 \mapsto 1$. Son diviseur est $H_{-2}([0]) \cup 20H_{-4}([1, 1])$.

Forme $F_{\mathbb{D}_{10}}$. Nous avons obtenu la forme $F_{\mathbb{D}_{10}}$ de poids 138. D'après la partie 1.3.6, $O(D(2U \oplus \mathbb{D}_{10})) \cong \mathbb{Z}/2\mathbb{Z}$, et Ψ^+ est surjective. On remarque que le calcul réalisé pour $F_{2\mathbb{E}_7}$ s'applique à $F_{\mathbb{D}_{10}}$, et on obtient la modularité de $F_{\mathbb{D}_{10}}$ par rapport à σ_{ε_2} .

Nous avons montré que le groupe modulaire maximal de $F_{\mathbb{D}_{10}}$ est le groupe $O^+(2U \oplus \mathbb{D}_{10})$. Le caractère est $\chi : g \in \tilde{O}^+(2U \oplus L) \mapsto \det(g)$, $\sigma_{\varepsilon_2} \mapsto 1$. Enfin, le diviseur de $F_{\mathbb{D}_{10}}$ est simplifié.

Conclusion. On dispose de la forme $F_{\mathbb{D}_{10}}$ de poids 138 pour le groupe $O^+(2U \oplus \mathbb{D}_{10})$ et le caractère $\chi : g \in \tilde{O}^+(2U \oplus L) \mapsto \det(g)$, $g_1 \mapsto 1$. Son diviseur est $H_{-2}(\bar{0}) \cup 57H_{-2}([1])$.

Le réseau $N(A_{15} + D_9)$

Forme $F_{\mathbb{D}_9}$. Nous avons obtenu la forme $F_{\mathbb{D}_9}$ de poids 132. D'après la partie 1.3.6, $O(D(2U \oplus \mathbb{D}_9)) \cong \mathbb{Z}/2\mathbb{Z}$, et Ψ^+ est surjective. L'élément non-trivial de $O(D(2U \oplus L))$ est réalisé dans $O^+(2U \oplus L)$ par σ_{ε_2} , et d'après les tables de la partie 1.4.2, pour prolonger $\sigma_{\varepsilon_2} \in O^+(2U \oplus \mathbb{D}_9)$, il suffit de réaliser $h = -id$ (de déterminant $(-1)^{15} = -1$) sur \mathbb{A}_{15} (ce qui est possible).

Nous avons montré que le groupe modulaire maximal de $F_{\mathbb{D}_9}$ est le groupe $O^+(2U \oplus \mathbb{D}_9)$. Le caractère est $\chi : g \in \tilde{O}^+(2U \oplus L) \mapsto \det(g)$, $\sigma_{\varepsilon_2} \mapsto 1$. Enfin, le diviseur de $F_{\mathbb{D}_9}$ est simplifié.

Conclusion. On dispose de la forme $F_{\mathbb{D}_9}$ de poids 132 pour le groupe $O^+(2U \oplus \mathbb{D}_9)$ et le caractère $\chi : g \in \tilde{O}^+(2U \oplus L) \mapsto \det(g)$, $\sigma_{\varepsilon_2} \mapsto 1$. Son diviseur est $H_{-2}(\bar{0}) \cup 120H_{-4}([1])$.

Le réseau $N(3D_8)$

Forme $F_{\mathbb{D}_8}$. Nous avons obtenu la forme $F_{\mathbb{D}_8}$ de poids 124. D'après la partie 1.3.6, $O(D(2U \oplus \mathbb{D}_8)) \cong \mathbb{Z}/2\mathbb{Z}$, et Ψ^+ est surjective. L'élément non-trivial de $O(D(2U \oplus L))$ est réalisé dans $O^+(2U \oplus L)$ par σ_{ε_2} . Mais, d'après les tables de la partie 1.4.2, pour prolonger $\sigma_{\varepsilon_2} \in O^+(2U \oplus \mathbb{D}_8)$, il faudrait réaliser des permutations d'éléments qui n'ont pas la même norme ($[1, 2, 2]$ donnerait $[3, 3, 0]$ ou $[3, 0, 3]$), c'est impossible.

Conclusion. On dispose de la forme $F_{\mathbb{D}_8}$ de poids 124 pour le groupe $\tilde{O}^+(2U \oplus \mathbb{D}_8)$ et le caractère déterminant. Son diviseur est $H_{-2}(\bar{0})$.

Le réseau $N(A_{11} + D_7 + E_6)$

Formes $F_{\mathbb{E}_6}$, $F_{\mathbb{D}_7}$ et $F_{\mathbb{A}_{11}}$. Nous avons obtenu les formes $F_{\mathbb{E}_6}$ de poids 120, $F_{\mathbb{D}_7}$ de poids 114 et $F_{\mathbb{A}_{11}}$ de poids 90. D'après la partie 1.3.6, $O(D(2U \oplus \mathbb{E}_6)) \cong \mathbb{Z}/2\mathbb{Z}$, $O(D(2U \oplus \mathbb{D}_7)) \cong \mathbb{Z}/2\mathbb{Z}$, $O(D(2U \oplus \mathbb{A}_{11})) \cong \mathbb{Z}/2\mathbb{Z}$ et Ψ^+ est surjective dans chacun des trois cas. On considère l'élément $g \in O^+(2U \oplus N)$ de déterminant 1 composé par le "produit" de $-id_{\mathbb{A}_{11}}$ sur \mathbb{A}_{11} (déterminant -1), σ_{ε_2} sur \mathbb{D}_7 (déterminant -1) et $-id_{\mathbb{E}_6}$ sur \mathbb{E}_6 (déterminant 1). Cet élément induit, dans chacun des trois groupes $O(D(2U \oplus L))$, l'élément non-trivial.

Conclusion. On dispose de la forme $F_{\mathbb{E}_6}$ de poids 120 pour le groupe $O^+(2U \oplus \mathbb{E}_6)$ et le caractère déterminant. Son diviseur est $H_{-2}(\bar{0})$.

Conclusion. On dispose de la forme $F_{\mathbb{D}_7}$ de poids 114 pour le groupe $O^+(2U \oplus \mathbb{D}_7)$ et le caractère $\chi : g \in \tilde{O}^+(2U \oplus L) \mapsto \det(g)$, $\sigma_{\varepsilon_2} \mapsto 1$. Son diviseur est $H_{-2}(\bar{0})$.

Conclusion. On dispose de la forme $F_{\mathbb{A}_{11}}$ de poids 90 pour le groupe $O^+(2U \oplus \mathbb{A}_{11})$ et le caractère $\chi : g \in \tilde{O}^+(2U \oplus L) \mapsto \det(g)$, $-id_{\mathbb{A}_{11}} \mapsto 1$. Son diviseur est

$$H_{-2}(\bar{0}) \cup 78H_{-4}([3]) \cup 56H_{-6}([4]) \cup 14H_{-4}([6]).$$

Le réseau $N(4E_6)$

Forme $F_{2\mathbb{E}_6}$. Nous avons obtenu la forme $F_{2\mathbb{E}_6}$ de poids 84. D'après la partie 1.3.6, $O(D(2U \oplus 2\mathbb{E}_6)) \cong (\mathbb{Z}/2\mathbb{Z})^3$, et Ψ^+ est surjective. Pour obtenir ce groupe, il suffit de relever l'élément de $O(2U \oplus 2\mathbb{E}_6)$ qui induit la permutation des copies de \mathbb{E}_6 (déterminant 1), et ceux de $O(2U \oplus 2\mathbb{E}_6)$ qui induisent $-id$ sur chaque copie de \mathbb{E}_6 (déterminant 1). D'après les tables de la partie 1.4.2, on obtient le premier en considérant pour h l'élément $-id$ sur la dernière copie de \mathbb{E}_6 (déterminant 1). On obtient celui qui correspond à $-id_{\mathbb{E}_6^{(1)}}$ en considérant pour h l'élément qui permute les deux dernières copies de \mathbb{E}_6 (déterminant 1), et celui qui correspond à $-id_{\mathbb{E}_6^{(2)}}$ en considérant pour h l'élément $-id_{\mathbb{E}_6^{(3)} \oplus \mathbb{E}_6^{(4)}}$ (déterminant 1).

Nous avons montré que le groupe modulaire maximal de $F_{2\mathbb{E}_6}$ est le groupe $O^+(2U \oplus 2\mathbb{E}_6)$. Le caractère est déterminant. Enfin, le diviseur de $F_{2\mathbb{E}_6}$ est simplifié.

Conclusion. On dispose de la forme $F_{2\mathbb{E}_6}$ de poids 84 pour le groupe $O^+(2U \oplus 2\mathbb{E}_6)$ et le caractère déterminant. Son diviseur est $H_{-2}(\bar{0}) \cup 27H_{-6}([1, 1])$.

Le réseau $N(2A_9 + D_6)$

Formes $F_{\mathbb{A}_9}$ et $F_{\mathbb{D}_6}$ Nous avons obtenu les formes $F_{\mathbb{A}_9}$ de poids 87 et $F_{\mathbb{D}_6}$ de poids 102. D'après la partie 1.3.6, $O(D(2U \oplus \mathbb{A}_9)) \cong \mathbb{Z}/2\mathbb{Z}$, $O(D(2U \oplus \mathbb{D}_6)) \cong \mathbb{Z}/2\mathbb{Z}$ et Ψ^+ est surjective dans chacun des deux cas. On considère les éléments $g_1, g_2 \in O^+(2U \oplus N)$ de déterminants respectifs -1 et 1 , tels que g_1 soit composé par le "produit" de l'élément qui échange les deux copies de \mathbb{A}_9 et de $-id_{\mathbb{A}_9}$ sur la deuxième copie de \mathbb{A}_9 (déterminant 1) et par σ_{ε_2} sur \mathbb{D}_6 (déterminant -1); et tels que g_2 soit composé par $-id_{2\mathbb{A}_9}$ et par $id_{\mathbb{D}_6}$ sur \mathbb{D}_6 (déterminant 1). Le premier élément permet d'obtenir le groupe $O^+(2U \oplus \mathbb{D}_6)$, le second $O^+(2U \oplus \mathbb{A}_9)$.

Nous avons montré que le groupe modulaire maximal de $F_{\mathbb{A}_9}$ est le groupe $O^+(2U \oplus \mathbb{A}_9)$. Le caractère est $\chi : g \in \tilde{O}^+(2U \oplus L) \mapsto \det(g)$, $-id_{\mathbb{A}_9} \mapsto 1$. Enfin, le diviseur de $F_{\mathbb{A}_9}$ est simplifié.

Nous avons montré que le groupe modulaire maximal de $F_{\mathbb{D}_6}$ est le groupe $O^+(2U \oplus \mathbb{D}_6)$. Le caractère est déterminant. Enfin, le diviseur de $F_{\mathbb{D}_6}$ est inchangé.

Conclusion. On dispose de la forme $F_{\mathbb{A}_9}$ de poids 87 pour le groupe $O^+(2U \oplus \mathbb{A}_9)$ et le caractère $\chi : g \in \tilde{O}^+(2U \oplus L) \mapsto \det(g)$, $-id_{\mathbb{A}_9} \mapsto 1$. Son diviseur est

$$H_{-2}(\bar{0}) \cup 165H_{-10}([3]) \cup 45H_{-10}([4]) \cup 33H_{-2}([5]).$$

Conclusion. On dispose de la forme $F_{\mathbb{D}_6}$ de poids 102 pour le groupe $O^+(2U \oplus \mathbb{D}_6)$ et le caractère déterminant. Son diviseur est $H_{-2}(\bar{0})$.

Le réseau $N(4D_6)$

Forme $F_{2\mathbb{D}_6}$. Nous avons obtenu la forme $F_{2\mathbb{D}_6}$ de poids 72. D'après la partie 1.3.6, $O(D(2U \oplus 2\mathbb{D}_6)) \cong (\mathbb{Z}/2\mathbb{Z})^3$, et Ψ^+ est surjective. Pour obtenir ce groupe, il suffit de relever l'élément $g_1 \in O^+(2U \oplus 2\mathbb{D}_6)$ qui induit la permutation des copies de \mathbb{D}_6 (déterminant 1), et les éléments $\sigma_{\varepsilon_2}^{(i)}$ sur chaque copie de \mathbb{D}_6 (déterminant -1). D'après les tables de la parties 1.4.2, on obtient le premier en considérant pour h l'élément qui permute les deux dernières copies de \mathbb{D}_6 (déterminant 1). On ne peut pas obtenir les deux autres (on aurait $[1, 3, 2, 0] \mapsto [3, 3, 3, 3]$ ou $[1, 1, 1, 1]$ respectivement, ce qui est impossible). En revanche, l'élément $g_2 \in O^+(2U \oplus 2\mathbb{D}_6)$ (de déterminant 1) qui réalise $-id_{2\mathbb{D}_6}$ sur les deux premières copies de \mathbb{D}_6 , se prolonge en posant pour h l'élément consistant en une permutation des deux dernières copies de \mathbb{D}_6 ainsi que $-id_{2\mathbb{D}_6}$ sur ces deux copies (déterminant 1). Le groupe Γ engendré par $\tilde{O}^+(2U \oplus 2\mathbb{D}_6)$, g_1 et g_2 est d'indice 2 dans $O^+(2U \oplus 2\mathbb{D}_6)$, et on a vu que le groupe modulaire maximal pour $F_{2\mathbb{D}_6}$ ne pouvait pas être $O^+(2U \oplus 2\mathbb{D}_6)$, c'est donc Γ .

Nous avons montré que le groupe modulaire maximal de $F_{2\mathbb{D}_6}$ est le groupe $\Gamma = \langle \tilde{O}^+(2U \oplus$

$2\mathbb{D}_6), g_1, g_2\rangle$. Le caractère est déterminant. Enfin, le diviseur de $F_{2\mathbb{D}_6}$ est simplifié.

Conclusion. On dispose de la forme $F_{2\mathbb{D}_6}$ de poids 72 pour le groupe $\Gamma \subset O^+(2U \oplus 2\mathbb{D}_6)$ d'indice 2 et le caractère déterminant. Son diviseur est

$$H_{-2}(\bar{0}) \cup 33H_{-2}([1, 2]) \cup 12H_{-4}([1, 3]).$$

Le réseau $N(3A_8)$

Forme $F_{\mathbb{A}_8}$. Nous avons obtenu la forme $F_{\mathbb{A}_8}$ de poids 84. D'après la partie 1.3.6, $O(D(2U \oplus \mathbb{A}_8)) \cong (\mathbb{Z}/2\mathbb{Z})$, et Ψ^+ est surjective. Pour obtenir ce groupe, il suffit de relever $-id_{\mathbb{A}_8} \in O^+(2U \oplus \mathbb{A}_8)$ (déterminant 1). D'après les tables de la partie 1.4.2, c'est possible en considérant l'élément $-id_{3\mathbb{A}_8} \in O^+(2U \oplus 3\mathbb{A}_8)$ (déterminant 1).

Nous avons montré que le groupe modulaire maximal de $F_{\mathbb{A}_8}$ est le groupe $O^+(2U \oplus \mathbb{A}_8)$. Le caractère est déterminant. Enfin, le diviseur de $F_{\mathbb{A}_8}$ est simplifié.

Conclusion. On dispose de la forme $F_{\mathbb{A}_8}$ de poids 84 pour le groupe $O^+(2U \oplus \mathbb{A}_8)$ et le caractère déterminant. Son diviseur est $H_{-2}(\bar{0}) \cup 81H_{-18}([4])$.

Le réseau $N(2A_7 + 2D_5)$

Formes $F_{\mathbb{A}_7}$, $F_{\mathbb{D}_5}$ et $F_{2\mathbb{D}_5}$. Nous avons obtenu les formes $F_{\mathbb{A}_7}$ de poids 80, $F_{\mathbb{D}_5}$ de poids 88 et $F_{2\mathbb{D}_5}$ de poids 68. D'après la partie 1.3.6, $O(D(2U \oplus \mathbb{A}_7)) \cong \mathbb{Z}/2\mathbb{Z}$, $O(D(2U \oplus \mathbb{D}_5)) \cong \mathbb{Z}/2\mathbb{Z}$, $O(D(2U \oplus 2\mathbb{D}_5)) \cong (\mathbb{Z}/2\mathbb{Z})^3$ et Ψ^+ est surjective dans chacun des trois cas. On considère l'élément $g \in O^+(2U \oplus N)$ de déterminant 1 composé par le "produit" de $-id_{\mathbb{A}_7}$ sur la première copie de \mathbb{A}_7 (déterminant -1), $-id_{\mathbb{A}_7}$ sur la deuxième copie de \mathbb{A}_7 (déterminant -1), σ_{ε_2} sur la première copie de \mathbb{D}_5 (déterminant -1) et σ_{ε_2} sur la deuxième copie de \mathbb{D}_5 (déterminant -1). Cet élément induit, dans chacun des deux premiers groupes $O(D(2U \oplus L))$, l'élément non-trivial. Dans le troisième groupe ($O(D(2\mathbb{D}_5))$), il faut de plus relever σ_{ε_2} (déterminant -1) dans la deuxième copie de \mathbb{D}_5 et g_1 l'élément qui échange les deux copies de \mathbb{D}_5 (déterminant -1), pour obtenir le groupe $O^+(2U \oplus L)$ en entier. C'est chose faite en considérant l'élément $g' \in O^+(2U \oplus N)$ de déterminant 1 obtenu par produit de l'élément de $O(2\mathbb{A}_7)$ qui échange les deux copies de \mathbb{A}_7 (déterminant -1) et de σ_{ε_2} sur la deuxième copie de \mathbb{D}_5 (déterminant -1), et $g'' \in O^+(2U \oplus N)$ de déterminant 1 qui échange les deux copies de \mathbb{D}_5 et induit $-id_{\mathbb{A}_7^{(2)}}$ sur la deuxième copie de \mathbb{A}_7 .

Nous avons montré que le groupe modulaire maximal de $F_{\mathbb{A}_7}$ est le groupe $O^+(2U \oplus \mathbb{A}_7)$. Le caractère est $\chi : g \in \tilde{O}^+(2U \oplus L) \mapsto \det(g)$, $-id_{\mathbb{A}_7} \mapsto 1$. Enfin, le diviseur de $F_{\mathbb{A}_7}$ est inchangé.

Nous avons montré que le groupe modulaire maximal de $F_{\mathbb{D}_5}$ est le groupe $O^+(2U \oplus \mathbb{D}_5)$. Le caractère est $\chi : g \in \tilde{O}^+(2U \oplus L) \mapsto \det(g)$, $\sigma_{\varepsilon_2} \mapsto 1$. Enfin, le diviseur de $F_{\mathbb{D}_5}$ est inchangé.

Nous avons montré que le groupe modulaire maximal de $F_{2\mathbb{D}_5}$ est le groupe $O^+(2U \oplus 2\mathbb{D}_5)$. Le caractère est $\chi : g \in \tilde{O}^+(2U \oplus L) \mapsto \det(g)$, $g \notin \tilde{O}^+(2U \oplus L) \mapsto -\det(g)$. Enfin, le diviseur de $F_{2\mathbb{D}_5}$ est simplifié.

Conclusion. On dispose de la forme $F_{\mathbb{A}_7}$ de poids 80 pour le groupe $O^+(2U \oplus \mathbb{A}_7)$ et le caractère $\chi : g \in \tilde{O}^+(2U \oplus L) \mapsto \det(g)$, $-id_{\mathbb{A}_7} \mapsto 1$. Son diviseur est $H_{-2}(\bar{0})$.

Conclusion. On dispose de la forme $F_{\mathbb{D}_5}$ de poids 88 pour le groupe $O^+(2U \oplus \mathbb{D}_5)$ et le caractère $\chi : g \in \tilde{O}^+(2U \oplus L) \mapsto \det(g)$, $g \notin \tilde{O}^+(2U \oplus L) \mapsto -\det(g)$. Son diviseur est $H_{-2}(\bar{0})$.

Conclusion. On dispose de la forme $F_{2\mathbb{D}_5}$ de poids 68 pour le groupe $O^+(2U \oplus 2\mathbb{D}_5)$ et le caractère $\chi : g \in \tilde{O}^+(2U \oplus L) \mapsto \det(g)$, $\sigma_{\varepsilon_2} \mapsto 1$. Son diviseur est

$$H_{-2}(\bar{0}) \cup 64H_{-4}([1, 2]) \cup 28H_{-8}([1, 1]).$$

Le réseau $N(4A_6)$

Forme $F_{\mathbb{A}_6}$. Nous avons obtenu la forme $F_{\mathbb{A}_6}$ de poids 75. D'après la partie 1.3.6, $O(D(2U \oplus \mathbb{A}_6)) \cong (\mathbb{Z}/2\mathbb{Z})$, et Ψ^+ est surjective. Pour obtenir ce groupe, il suffit de relever $-id_{\mathbb{A}_6} \in O^+(2U \oplus \mathbb{A}_6)$ (déterminant 1). D'après les tables de la partie 1.4.2, c'est possible en considérant l'élément $-id_{4\mathbb{A}_6} \in O^+(2U \oplus 4\mathbb{A}_6)$ (déterminant 1).

Conclusion. On dispose de la forme $F_{\mathbb{A}_6}$ de poids 75 pour le groupe $O^+(2U \oplus \mathbb{A}_6)$ et le caractère déterminant. Son diviseur est $H_{-2}(\bar{0})$.

Le réseau $N(4A_5 + D_4)$

Forme $F_{\mathbb{D}_4}$. Nous avons obtenu la forme $F_{\mathbb{D}_4}$ de poids 72. D'après la partie 1.3.6, $O(D(2U \oplus \mathbb{D}_4)) \cong \mathcal{S}_3$, et Ψ^+ est surjective. Pour obtenir $O^+(2U \oplus L)$, il suffit de réaliser $\tau_{[1],[2]}$ et $\tau_{[1],[3]}$. D'après la partie 1.4.2, c'est possible pour $\tau_{[1],[2]}$ car on peut réaliser dans $O(4\mathbb{A}_5)$ l'élément qui permute les 2-ème et 3-ième copies de \mathbb{A}_5 et induit $-id_{\mathbb{A}_5}$ sur la première copie de \mathbb{A}_5 (déterminant 1). Pour $\tau_{[1],[3]}$, on peut réaliser dans $O(4\mathbb{A}_5)$ l'élément qui permute les 1-ère et 3-ième copies de \mathbb{A}_5 et induit $-id_{\mathbb{A}_5}$ sur la deuxième copie de \mathbb{A}_5 (déterminant 1).

Conclusion. On dispose de la forme $F_{\mathbb{D}_4}$ de poids 72 pour le groupe $O^+(2U \oplus \mathbb{D}_4)$ et le caractère déterminant. Son diviseur est $H_{-2}(\bar{0})$.

Forme $F_{\mathbb{A}_5}$. Nous avons obtenu la forme $F_{\mathbb{A}_5}$ de poids 69. D'après la partie 1.3.6, $O(D(2U \oplus \mathbb{A}_5)) \cong \mathbb{Z}/2\mathbb{Z}$, et Ψ^+ est surjective. Pour obtenir ce groupe, il suffit de relever $-id_{\mathbb{A}_5} \in O^+(2U \oplus \mathbb{A}_5)$ (déterminant -1). D'après les tables de la partie 1.4.2, c'est possible en considérant l'élément qui induit $-id_{4\mathbb{A}_5}$ sur $4\mathbb{A}_5$ et $id_{\mathbb{D}_4}$ sur \mathbb{D}_4 (déterminant 1).

Conclusion. On dispose de la forme $F_{\mathbb{A}_5}$ de poids 69 pour le groupe $O^+(2U \oplus \mathbb{A}_5)$ et le caractère $\chi : g \in \tilde{O}^+(2U \oplus L) \mapsto \det(g)$, $-id_{\mathbb{A}_5} \mapsto 1$. Son diviseur est $H_{-2}(\bar{0})$.

Forme $F_{2\mathbb{A}_5}$. Nous avons obtenu la forme $F_{2\mathbb{A}_5}$ de poids 54. D'après la partie 1.3.6, $O(D(2U \oplus 2\mathbb{A}_5)) \cong (\mathbb{Z}/2\mathbb{Z})^3$, et Ψ^+ est surjective. Pour obtenir le groupe tout entier, étant donné qu'on a déjà construit juste avant l'élément qui induit $-id_{2\mathbb{A}_5}$, il faudrait avoir un

élément qui induit $-id_{\mathbb{A}_5}$ sur la première copie de \mathbb{A}_5 et $id_{\mathbb{A}_5}$ sur la seconde (déterminant -1), puis un élément qui échange les deux premières copies de \mathbb{A}_5 (déterminant -1). On peut obtenir le premier en considérant l'élément de $O^+(2U \oplus 4\mathbb{A}_5 \oplus \mathbb{D}_4)$ de déterminant -1 qui consiste en $-id_{\mathbb{A}_5}$ sur la première copie, $id_{\mathbb{A}_5}$ sur la seconde, l'échange des 3-ième et 4-ième copies de \mathbb{A}_5 , et σ_{ε_1} sur \mathbb{D}_4 . on peut obtenir le second en considérant l'élément de $O^+(2U \oplus 4\mathbb{A}_5 \oplus \mathbb{D}_4)$ de déterminant -1 qui consiste en l'échange des deux premières copies de \mathbb{A}_5 , $id_{\mathbb{A}_5}$ sur la 3-ième copie de \mathbb{A}_5 , $-id_{\mathbb{A}_5}$ sur la 4-ième copie de \mathbb{A}_5 et σ_{ε_1} sur \mathbb{D}_4 .

Conclusion. On dispose de la forme $F_{2\mathbb{A}_5}$ de poids 54 pour le groupe $O^+(2U \oplus 2\mathbb{A}_5)$ et le caractère déterminant. Son diviseur est

$$H_{-2}(\bar{0}) \cup 63H_{-6}([1, 2]) \cup 36H_{-12}([1, 3]) \cup 15H_{-6}([2, 2]) \cup 8H_{-4}([3, 3]).$$

Forme $F_{\mathbb{A}_5 \oplus \mathbb{D}_4}$. Nous avons obtenu la forme $F_{\mathbb{A}_5 \oplus \mathbb{D}_4}$ de poids 57. D'après la partie 1.3.6, $O(D(2U \oplus \mathbb{A}_5 \oplus \mathbb{D}_4)) \cong (\mathbb{Z}/2\mathbb{Z}) \times \mathcal{S}_3$, et Ψ^+ est surjective. Les éléments considérés pour les formes associées aux réseaux \mathbb{D}_4 et \mathbb{A}_5 permettent d'obtenir de façon indépendante $-id_{\mathbb{A}_5}$ sur la quatrième copie de \mathbb{A}_5 en même temps que $id_{\mathbb{D}_4}$ et $id_{\mathbb{A}_5}$ sur la quatrième copie de \mathbb{A}_5 en même temps que \mathcal{S}_3 sur \mathbb{D}_4 .

Conclusion. On dispose de la forme $F_{\mathbb{A}_5 \oplus \mathbb{D}_4}$ de poids 57 pour le groupe $O^+(2U \oplus \mathbb{A}_5 \oplus \mathbb{D}_4)$ et le caractère $\chi : g \in \tilde{O}^+(2U \oplus L) \mapsto \det(g)$, $\tau_{[i],[j]} \in O(D(\mathbb{D}_4)) \mapsto -1$, $-id_{\mathbb{A}_5} \mapsto 1$. Son diviseur est

$$H_{-2}(\bar{0}) \cup 21H_{-2}([3, 1]) \cup 36H_{-12}([2, 1]).$$

Le réseau $N(6D_4)$

Forme $F_{\mathbb{D}_4}$. Déjà fait.

Forme $F_{2\mathbb{D}_4}$. Nous avons obtenu la forme $F_{2\mathbb{D}_4}$ de poids 60. D'après la partie 1.3.6, $O(D(2U \oplus 2\mathbb{D}_4))$ est engendré par les permutations des éléments du groupe discriminant de chaque copie de \mathbb{D}_4 et par les permutations de ces copies. Ψ^+ est surjective. Voyons si nous pouvons relever $\tau_{[1],[2]}$ sur la première copie de \mathbb{D}_4 . L'image de l'élément $[2, 2, 2, 2, 0, 0]$ serait $[1, 2, 3, 0, 0, 3]$ ou $[1, 2, 0, 3, 3, 0]$, et l'image de l'élément $[1, 1, 1, 1, 0, 0]$ serait $[2, 1, 3, 0, 3, 0]$ ou $[2, 1, 0, 3, 0, 3]$, or les 4 possibilités sont toutes impossibles à cause de la distribution des 0 (aucune permutation des 4 dernières copies de \mathbb{D}_4 ne permet ces distributions). De même, on pourra vérifier qu'aucune autre transposition ne se relève. En revanche, on peut relever le 3-cycle (123) dans la première copie de \mathbb{D}_4 en considérant l'élément qui consiste en $\sigma_{\varepsilon_3} \circ \sigma_{\varepsilon_1} \in O^+(\mathbb{D}_4)$ dans la première copie de \mathbb{D}_4 , id dans la deuxième, $\sigma_{\varepsilon_1} \circ \sigma_{\varepsilon_3} \in O^+(\mathbb{D}_4)$ dans la troisième, le 3-cycle (456) pour permuter les 3 dernières copies de \mathbb{D}_4 suivi de $\sigma_{\varepsilon_1} \circ \sigma_{\varepsilon_3} \in O^+(\mathbb{D}_4)$ dans chacune de ces trois copies (déterminant 1). De plus, l'échange des deux copies de \mathbb{D}_4 (déterminant 1) est possible, il est induit par l'élément $g \in O^+(2U \oplus \mathbb{D}_4)$ qui échange les deux premières et les deux dernières copies de \mathbb{D}_4 (déterminant 1). On en déduit aussi que l'on peut réaliser le 3-cycle (123) dans la

deuxième copie de \mathbb{D}_4 , mais aucune transposition dans cette deuxième copie de \mathbb{D}_4 . Enfin, on peut réaliser la transposition $\tau_{[1],[2]}$ sur les deux premières copies de \mathbb{D}_4 simultanément, en considérant l'élément $\sigma_{\varepsilon_3} \in O^+(\mathbb{D}_4)$ sur toutes les copies de \mathbb{D}_4 , puis l'échange des deux dernières copies de \mathbb{D}_4 (déterminant 1). Reste à montrer, pour avoir vérifié tous les éléments possibles, que l'on ne peut avoir un élément du type $\sigma_1 \times \sigma_2 \in O^+(2\mathbb{D}_4)$ où σ_i agit sur la i -ème copie de \mathbb{D}_4 et σ_1, σ_2 de signature contraire. En effet, sinon, on aurait l'élément $\sigma_1 \circ \sigma_2^{-1} \times id$, et $\sigma_1 \circ \sigma_2^{-1}$ de signature -1 , ce qui est impossible d'après notre raisonnement précédent. Le groupe que nous avons obtenu est d'indice 2 dans $O^+(2U \oplus 2\mathbb{D}_4)$, et est engendré par $\tilde{O}^+(2U \oplus L)$, $(123)^{(1)}$, $(123)^{(2)}$, g , $\tau_{[1],[2]} \times \tau_{[1],[2]}$, où g est l'élément qui échange les deux copies de \mathbb{D}_4 , $(123)^{(i)}$ est l'élément qui réalise le 3-cycle (123) dans la i -ème copie de \mathbb{D}_4 et $\tau_{[1],[2]} \times \tau_{[1],[2]}$ l'élément qui réalise $\tau_{[1],[2]}$ dans les deux premières copies de \mathbb{D}_4 simultanément.

Conclusion. On dispose de la forme $F_{2\mathbb{D}_4}$ de poids 60 pour le groupe $\Gamma = \langle \tilde{O}^+(2U \oplus 2\mathbb{D}_4), g, (123)^{(1)}, (123)^{(2)}, \tau_{[1],[2]} \times \tau_{[1],[2]} \rangle$ d'indice 2 dans $O^+(2U \oplus 2\mathbb{D}_4)$ et le caractère déterminant. Son diviseur est $H_{-2}(\bar{0})$.

Forme $F_{3\mathbb{D}_4}$. Nous avons obtenu la forme $F_{3\mathbb{D}_4}$ de poids 48. D'après la partie 1.3.6, $O(D(2U \oplus 3\mathbb{D}_4))$ est engendré par les permutations des éléments du groupe discriminant de chaque copie de \mathbb{D}_4 et par les permutations de ces copies. Ψ^+ est surjective. Reprenons les éléments construits précédemment, on dispose de la permutation de deux premières copies, et le relèvement que nous avons choisi fixe la troisième copie. On peut aussi relever l'élément qui réalise l'échange des deuxième et troisième copies tout en fixant la première copie, en considérant l'élément qui, sur les 3 dernières copies de \mathbb{D}_4 , fixe la quatrième, échange les deux dernières puis réalise le 3-cycle (123) (par $\sigma_{\varepsilon_3} \circ \sigma_{\varepsilon_1} \in O^+(\mathbb{D}_4)$) sur la cinquième copie, et (132) sur la sixième (par $\sigma_{\varepsilon_1} \circ \sigma_{\varepsilon_3} \in O^+(\mathbb{D}_4)$). Ainsi, on peut relever toutes les permutations des 3 copies de \mathbb{D}_4 . Ensuite, nous avons vu que l'on peut relever l'élément $\tau_{[1],[2]} \times \tau_{[1],[2]} \times \tau_{[1],[2]}$ dans les 3 premières copies de \mathbb{D}_4 . On peut aussi réaliser l'élément $(123) \times id \times (132)$. Tous ces éléments, avec le groupe $\tilde{O}^+(2U \oplus 3\mathbb{D}_4)$, engendrent un sous-groupe d'indice 4 de $O^+(2U \oplus 3\mathbb{D}_4)$. Pour montrer que ce groupe est le plus grand que l'on puisse obtenir, on constate d'abord qu'il ne peut exister d'élément de la forme $\tau \times id \times id$ où τ est une transposition, d'après le raisonnement fait pour la forme précédente. Il ne peut pas non plus y avoir d'élément de la forme $\tau \times \tau' \times id$ où τ et τ' sont deux transpositions différentes, sinon dans le calcul de la forme précédente, on aurait réussi à exhiber un élément de la forme $\tau \times id$, et on a prouvé que c'était exclu. En conclusion le groupe que nous recherchons est d'indice au moins 4 dans $O^+(2U \oplus L)$, nous l'avons donc trouvé, nous l'appellerons Γ .

Conclusion. On dispose de la forme $F_{3\mathbb{D}_4}$ de poids 48 pour le groupe $\Gamma \subset O^+(2U \oplus 3\mathbb{D}_4)$ d'indice 4 et le caractère déterminant. Son diviseur est

$$H_{-2}(\bar{0}) \cup 8H_{-4}([1, 1, 1]).$$

Le réseau $N(6A_4)$

Forme $F_{\mathbb{A}_4}$. Nous avons obtenu la forme $F_{\mathbb{A}_4}$ de poids 62. D'après la partie 1.3.6, $O(D(2U \oplus \mathbb{A}_4)) \cong \mathbb{Z}/2\mathbb{Z}$, et Ψ^+ est surjective. Pour obtenir ce groupe, il suffit de relever $-id_{\mathbb{A}_4} \in O^+(2U \oplus \mathbb{A}_4)$ (déterminant 1). D'après les tables de la partie 1.4.2, c'est possible en considérant l'élément $-id_{6\mathbb{A}_4} \in O^+(2U \oplus 6\mathbb{A}_4)$ (déterminant 1).

Conclusion. On dispose de la forme $F_{\mathbb{A}_4}$ de poids 62 pour le groupe $O^+(2U \oplus \mathbb{A}_4)$ et le caractère déterminant. Son diviseur est $H_{-2}(\bar{0})$.

Forme $F_{2\mathbb{A}_4}$. Nous avons obtenu la forme $F_{2\mathbb{A}_4}$ de poids 52. D'après la partie 1.3.6, $O(D(2U \oplus 2\mathbb{A}_4)) \cong (\mathbb{Z}/2\mathbb{Z})^3$, et Ψ^+ est surjective. Pour obtenir le groupe tout entier, étant donné qu'on a déjà construit juste avant l'élément qui induit $-id_{2\mathbb{A}_4}$, il faudrait avoir un élément qui induit $-id_{\mathbb{A}_4}$ sur la première copie de \mathbb{A}_4 , et $id_{\mathbb{A}_4}$ sur la seconde (déterminant 1). C'est chose faite en considérant l'élément de $O(4\mathbb{A}_4)$ qui réalise le 4-cycle (1342) du groupe des permutations des 4 dernières copies de \mathbb{A}_4 (déterminant 1). Ensuite, on obtient la permutation des deux premières copies de \mathbb{A}_4 (déterminant 1) avec l'élément qui induit, dans les 4 dernières copies de \mathbb{A}_4 , l'échange des copies 3 et 6 et $-id_{2\mathbb{A}_4}$ sur les copies 4 et 5 (déterminant 1).

Conclusion. On dispose de la forme $F_{2\mathbb{A}_4}$ de poids 52 pour le groupe $O^+(2U \oplus 2\mathbb{A}_4)$ et le caractère déterminant. Son diviseur est $H_{-2}(\bar{0}) \cup 25H_{-10}([2, 2])$.

Le réseau $N(8A_3)$

Forme $F_{\mathbb{A}_3}$. Nous avons obtenu la forme $F_{\mathbb{A}_3}$ de poids 54. D'après la partie 1.3.6, $O(D(2U \oplus \mathbb{A}_3)) \cong \mathbb{Z}/2\mathbb{Z}$, et Ψ^+ est surjective. Pour obtenir ce groupe, il suffit de relever $-id_{\mathbb{A}_3}$ (déterminant -1). D'après les tables de la partie 1.4.2, c'est possible en considérant l'élément $-id_{8\mathbb{A}_3}$ (déterminant 1).

Conclusion. On dispose de la forme $F_{\mathbb{A}_3}$ de poids 54 pour le groupe $O^+(2U \oplus \mathbb{A}_3)$ et le caractère $\chi : g \in \tilde{O}^+(2U \oplus L) \mapsto \det(g)$, $-id_{\mathbb{A}_3} \mapsto 1$. Son diviseur est $H_{-2}(\bar{0})$.

Forme $F_{2\mathbb{A}_3}$. Nous avons obtenu la forme $F_{2\mathbb{A}_3}$ de poids 48. D'après la partie 1.3.6, $O(D(2U \oplus 2\mathbb{A}_3)) \cong (\mathbb{Z}/2\mathbb{Z})^3$, et Ψ^+ est surjective. Pour obtenir le groupe tout entier, étant donné qu'on a déjà construit juste avant l'élément qui induit $-id_{2\mathbb{A}_3}$, il faudrait avoir un élément qui induit $-id_{\mathbb{A}_3}$ sur la première copie de \mathbb{A}_3 , et $id_{\mathbb{A}_3}$ sur la seconde (déterminant -1). C'est chose faite en considérant l'élément de $O(6\mathbb{A}_3)$ réalisé par le produit de la permutation (3475)(68) du groupe des permutations des 6 dernières copies de \mathbb{A}_3 et ensuite (dans cet ordre) de $-id_{\mathbb{A}_3}$ sur les copies 3, 4 et 8 de \mathbb{A}_3 (déterminant -1) (tester sur les générateurs pour voir l'invariance). Ensuite, on obtient la permutation des deux premières copies de \mathbb{A}_3 (déterminant -1) avec l'élément qui induit, dans les 5 dernières copies de \mathbb{A}_3 , l'échange des copies 4 et 5 et $-id_{\mathbb{A}_3}$ sur les copies 4, 5, 6 et 8 de \mathbb{A}_3 (déterminant -1).

Conclusion. On dispose de la forme $F_{2\mathbb{A}_3}$ de poids 48 pour le groupe $O^+(2U \oplus 2\mathbb{A}_3)$ et le caractère $\chi : g \in \tilde{O}^+(2U \oplus L) \mapsto \det(g)$, $g \notin \tilde{O}^+(2U \oplus L) \mapsto -\det(g)$. Son diviseur est $H_{-2}(\bar{0})$.

Forme $F_{3\mathbb{A}_3}$. Nous avons obtenu la forme $F_{3\mathbb{A}_3}$ de poids 42. D'après la partie 1.3.6, $O(D(2U \oplus 2\mathbb{A}_3))$ est engendré par les éléments des groupes d'automorphismes $O(D(\mathbb{A}_3))$ de chaque copie de \mathbb{A}_3 et par les éléments qui permutent les copies de \mathbb{A}_3 , et Ψ^+ est surjective. On obtient la permutation des deux premières copies de \mathbb{A}_3 qui laisse invariante la troisième copie de \mathbb{A}_3 (déterminant -1) avec l'élément qui induit, dans les 5 dernières copies de \mathbb{A}_3 , l'échange des copies 4 et 5 et $-id_{\mathbb{A}_3}$ sur les copies 4, 5, 6 et 8 de \mathbb{A}_3 (déterminant -1). La triple transitivité du groupe des automorphismes du réseau $N(8A_3)$ sur les copies de \mathbb{A}_3 assure l'existence des deux autres permutations (il suffit de conjuguer), ainsi on obtient toutes les permutations des copies de \mathbb{A}_3 . Peut-on avoir un élément qui induit $-id_{\mathbb{A}_3}$ sur la première copie de \mathbb{A}_3 , et $id_{\mathbb{A}_3}$ sur la seconde et la troisième (déterminant -1) ? Oui, en considérant sur les 5 dernières copies de \mathbb{A}_3 le produit de l'élément qui induit les permutations des copies 4 et 6 ainsi que 5 et 8 et de l'élément qui induit $-id$ sur les copies 5, 7 et 8 (déterminant -1). La triple transitivité du groupe des automorphismes du réseau $N(8A_3)$ sur les copies de \mathbb{A}_3 assure l'existence de $-id_{\mathbb{A}_3}$ en même temps que $id_{\mathbb{A}_3}$ sur les deux autres copies de \mathbb{A}_3 , sur chacune des deux autres copies de \mathbb{A}_3 (il suffit de conjuguer). On obtient ainsi le groupe $O^+(2U \oplus L)$ en entier.

Conclusion. On dispose de la forme $F_{3\mathbb{A}_3}$ de poids 42 pour le groupe $O^+(2U \oplus 3\mathbb{A}_3)$ et le caractère $\chi : g \in \tilde{O}^+(2U \oplus L) \mapsto \det(g)$, $g \notin \tilde{O}^+(2U \oplus L) \mapsto -\det(g)$. Son diviseur est

$$H_{-2}(\bar{0}) \cup 30H_{-4}([1, 1, 1]) \cup 16H_{-8}([1, 1, 2] \cup 6H_{-4}([2, 2, 2])).$$

Le réseau $N(12A_2)$

Formes $F_{\mathbb{A}_2}$, $F_{2\mathbb{A}_2}$, $F_{3\mathbb{A}_2}$ et $F_{4\mathbb{A}_2}$. Nous avons obtenu les formes $F_{\mathbb{A}_2}$ de poids 45, $F_{2\mathbb{A}_2}$ de poids 42, $F_{3\mathbb{A}_2}$ de poids 39 et $F_{4\mathbb{A}_2}$ de poids 36. D'après la partie 1.3.6, $O(D(2U \oplus k\mathbb{A}_2))$ est engendré par les éléments des groupes d'automorphismes $O(D(\mathbb{A}_2))$ de chaque copie de \mathbb{A}_2 et par les éléments qui permutent les copies de \mathbb{A}_2 , et Ψ^+ est surjective. On peut réaliser, modulo d'éventuelles transformations de type $\tau_{[1],[2]}$ sur quelques composantes, les permutations des copies de \mathbb{A}_2 car le groupe des automorphismes de $N(12A_2)$ est 5-transitif sur les copies de \mathbb{A}_2 . En revanche, le groupe des automorphismes du code de Golay ternaire \mathcal{C}_{12} étant le produit semi-direct de M_{12} et de $\mathbb{Z}/2\mathbb{Z}$ (action par conjugaison), on ne peut réaliser en plus que l'élément $\underbrace{\tau_{[1],[2]} \times \dots \times \tau_{[1],[2]}}_{k \text{ fois}} \underbrace{(-id_{\mathbb{A}_2} \times \dots \times -id_{\mathbb{A}_2})}_{k \text{ fois}}$.

Conclusion. On dispose de la forme $F_{\mathbb{A}_2}$ de poids 45 pour le groupe $O^+(2U \oplus \mathbb{A}_2)$ et le caractère $\chi : g \in \tilde{O}^+(2U \oplus L) \mapsto \det(g)$, $g \notin \tilde{O}^+(2U \oplus L) \mapsto -\det(g)$. Son diviseur est $H_{-2}(\bar{0})$.

Conclusion. On dispose de la forme $F_{2\mathbb{A}_2}$ de poids 42 pour le groupe d'indice 2 dans $O^+(2U \oplus 2\mathbb{A}_2)$, $\Gamma = \langle \tilde{O}^+(2U \oplus 2\mathbb{A}_2), g_1, \tau_{\mathbb{A}_2^{(1)}, \mathbb{A}_2^{(2)}} \rangle$, où $\tau_{\mathbb{A}_2^{(1)}, \mathbb{A}_2^{(2)}}$ est l'élément de $O^+(2U \oplus 2\mathbb{A}_2)$ induit par $O^+(2U \oplus 12A_2)$ qui échange les deux premières copies de \mathbb{A}_2 ; et le caractère $\chi : g \in \tilde{O}^+(2U \oplus L) \mapsto \det(g)$, $g \notin \tilde{O}^+(2U \oplus L) \mapsto -\det(g)$. Son diviseur est $H_{-2}(\bar{0})$.

Conclusion. On dispose de la forme $F_{3\mathbb{A}_2}$ de poids 39 pour le groupe d'indice 4 dans $O^+(2U \oplus 2\mathbb{A}_2)$, $\Gamma = \langle \tilde{O}^+(2U \oplus 3\mathbb{A}_2), g_1, \mathcal{S}_{3\mathbb{A}_2} \rangle$, où $\mathcal{S}_{3\mathbb{A}_2}$ désigne le groupe des automorphismes de $O^+(2U \oplus 3\mathbb{A}_2)$ qui permutent les trois premières copies de \mathbb{A}_2 . Le caractère reste à déterminer. Son diviseur est $H_{-2}(\bar{0})$.

Conclusion. On dispose de la forme $F_{4\mathbb{A}_2}$ de poids 36 pour le groupe d'indice 8 dans $O^+(2U \oplus 2\mathbb{A}_2)$, $\Gamma = \langle \tilde{O}^+(2U \oplus 4\mathbb{A}_2), g_1, \mathcal{S}_{4\mathbb{A}_2} \rangle$, où $\mathcal{S}_{4\mathbb{A}_2}$ désigne le groupe des automorphismes de $O^+(2U \oplus 4\mathbb{A}_2)$ qui permutent les quatre premières copies de \mathbb{A}_2 . Le caractère reste à déterminer. Son diviseur est $H_{-2}(\bar{0}) \cup 9H_{-6}([1, 1, 1, 1])$.

Le réseau $N(24A_1)$

Formes $F_{k\mathbb{A}_1}$, $1 \leq k \leq 5$. Nous avons obtenu les formes $F_{\mathbb{A}_1}$ de poids 35, $F_{2\mathbb{A}_1}$ de poids 34, $F_{3\mathbb{A}_1}$ de poids 33, $F_{4\mathbb{A}_1}$ de poids 32 et $F_{5\mathbb{A}_1}$ de poids 31. D'après la partie 1.3.6, $O(D(2U \oplus k\mathbb{A}_1))$ est engendré par les éléments des groupes d'automorphismes $O(D(\mathbb{A}_1))$ de chaque copie de \mathbb{A}_1 et par les éléments qui permutent les copies de \mathbb{A}_2 , donc dans ce cas présent il s'agit juste des permutations des copies de \mathbb{A}_1 . D'autre part, Ψ^+ est surjective. On peut réaliser les permutations des copies de \mathbb{A}_1 car le groupe des automorphismes de $N(24A_1)$ est 5-transitif sur les copies de \mathbb{A}_1 . Pour réaliser la permutation des copies i et j , il existe un élément de M_{24} qui les échange tout en fixant les autres coordonnées correspondant au plongement.

Conclusion. On dispose des formes $F_{k\mathbb{A}_1}$, $1 \leq k \leq 5$ de poids respectifs 35, 34, 33, 32, 31 pour le groupe $O^+(2U \oplus k\mathbb{A}_1)$. Nous ne savons pas préciser le caractère. Leur diviseur est $H_{-2}(\bar{0}) \cup H_{-2}([1^1 0^{k-1}])$.

Chapitre 5

Classification des formes modulaires réflexives obtenues par quasi-restriction, autres exemples

On reprend les notations des parties précédentes, N est un réseau de Niemeier différent du réseau de Leech (défini négatif par convention), L un sous-réseau non-nul de N , et M un sous-réseau de N tel que $L \perp M$ et $\text{rg}(L \oplus M) = \text{rg}(N)$.

5.1 Choix du réseau L

Nous voulons maintenant utiliser le théorème 2.2 pour calculer des formes modulaires réflexives à partir d'un sous-réseau L qui n'est pas une composante orthogonale du sous-réseau de racines de N (car ce cas a déjà été traité de façon exhaustive). Les diverses possibilités sont très grandes, nous allons donc faire des choix.

Afin d'obtenir des formes particulières, nous allons nous contenter de choisir pour L l'un des réseaux de la liste de la proposition 3.5. Nous connaissons déjà des formes modulaires obtenues par quasi-restriction à partir de ces réseaux. D'autre part, ces formes ont la particularité d'avoir un diviseur le plus simple possible, c'est l'union de tous les -2 -diviseurs quadratiques rationnels, avec multiplicité un, ce qui est le plus petit diviseur possible pour une forme modulaire anti-invariante pour le groupe $\tilde{O}^+(2U \oplus L)$.

Ainsi, si l'on dispose d'une nouvelle forme modulaire (obtenue par quasi-restriction) associée au réseau L , nous pourrions considérer la forme obtenue en faisant le quotient de la nouvelle forme par la forme strictement -2 -réflexive déjà connue, et nous obtiendrions une forme modulaire pour le groupe $\tilde{O}^+(2U \oplus L)$ (ou plus, suivant la méthode du chapitre précédent) et le caractère trivial. D'autre part, si la seconde forme est "bien choisie", nous avons espoir d'obtenir une nouvelle forme de poids "proche" du poids de la forme strictement -2 -réflexive déjà connue, et donc un quotient de "petit" poids, et parfois même un quotient de poids critique ou singulier.

Nous allons donc considérer des réseaux L (de la liste de la proposition 3.5), que l'on plongera dans des réseaux L' de rangs égaux à $\text{rg}(L) + 1$ et qui sont une composante orthogonale du sous-réseau de racines d'un réseau de Niemeier N .

5.2 Calcul de $L_{L'}^\perp$

Dans la liste de la proposition 3.5 se trouvent les réseaux de racines de type \mathbb{A}_n , \mathbb{D}_n , \mathbb{E}_6 , \mathbb{E}_7 et \mathbb{E}_8 . La méthode que l'on utilise qui consiste à plonger L dans L' un réseau de racines de rang $\text{rg}(L) + 1$ nous empêche de considérer $L = \mathbb{E}_8$. Calculons le complément orthogonal des autres réseaux L dans L' .

Lemme 5.1. *Les espaces considérés sont munis de l'opposé du produit scalaire euclidien usuel, ils sont définis négatifs.*

(i) Soit $n \in \mathbb{N}^*$. On considère le plongement de \mathbb{A}_n dans \mathbb{A}_{n+1} défini par

$$\mathbb{A}_n = \left\{ (x_0, \dots, x_n, x_{n+1}) \in \mathbb{Z}^{n+2} \mid \sum_{i=0}^n x_i = 0, x_{n+1} = 0 \right\}.$$

Alors $\mathbb{A}_{n\mathbb{A}_{n+1}}^\perp = \mathbb{Z} \left(\underbrace{1, \dots, 1}_{n+1}, -(n+1) \right)$. En particulier, $\mathbb{A}_{n\mathbb{A}_{n+1}}^\perp$ n'a pas de racines.

(ii) Soit $n \in \mathbb{N}^*$, $n \geq 4$. On considère le plongement de \mathbb{D}_n dans \mathbb{D}_{n+1} défini par

$$\mathbb{D}_n = \left\{ (x_1, \dots, x_n, x_{n+1}) \in \mathbb{Z}^{n+1} \mid \sum_{i=1}^n x_i \equiv 0 \pmod{2}, x_{n+1} = 0 \right\}.$$

Alors $\mathbb{D}_{n\mathbb{D}_{n+1}}^\perp = \mathbb{Z} \left(\underbrace{0, \dots, 0}_n, 2 \right)$. En particulier, $\mathbb{D}_{n\mathbb{D}_{n+1}}^\perp$ n'a pas de racines.

(iii) On considère le réseau \mathbb{E}_7 construit en partie 1.1.3, il est plongé dans le réseau \mathbb{E}_8 défini dans la même partie. Alors $\mathbb{E}_{7\mathbb{E}_8}^\perp = \mathbb{Z}(0, 0, 0, 0, 0, 0, 1, 1) \cong \mathbb{A}_1$. En particulier, $\mathbb{E}_{7\mathbb{E}_8}^\perp$ a deux racines.

(iv) On considère le réseau \mathbb{E}_6 construit en partie 1.1.3, il est plongé dans le réseau \mathbb{E}_7 défini dans la même partie. Alors $\mathbb{E}_{6\mathbb{E}_7}^\perp = \mathbb{Z}(0, 0, 0, 0, 0, 2, -1, 1)$. En particulier, $\mathbb{E}_{6\mathbb{E}_7}^\perp$ n'a pas de racines.

PREUVE : (i) Soit $y = (y_0, \dots, y_{n+1}) \in \mathbb{A}_{n+1}$, alors pour tout $x = (x_0, \dots, x_n, 0) \in \mathbb{A}_n$, $\sum_{i=0}^n x_i y_i = 0$, ce qui donne, en prenant pour x des vecteurs dont une coordonnée exactement vaut 1 une autre -1 et les autres 0, que $\forall i \in \llbracket 1, n \rrbracket$, $y_i = y_0$. Ceci impose alors $y_{n+1} = -(n+1)y_0$. Inversement, de tels vecteurs sont bien orthogonaux à \mathbb{A}_n . On a donc établi que

$$\mathbb{A}_{n\mathbb{A}_{n+1}}^\perp = \mathbb{Z} \left(\underbrace{1, \dots, 1}_{n+1}, -(n+1) \right),$$

et comme $\left(\underbrace{1, \dots, 1}_{n+1}, -(n+1) \right)^2 = -(n+1)(n+2) < -2$ il n'y a pas de racines dans

$\mathbb{A}_{n\mathbb{A}_{n+1}}^\perp$.

(ii) Soit $y = (y_1, \dots, y_{n+1}) \in \mathbb{D}_{n+1}$, alors pour tout $x = (x_1, \dots, x_n, 0) \in \mathbb{D}_n$, $\sum_{i=1}^n x_i y_i = 0$, ce qui donne, en prenant pour x des vecteurs dont une coordonnée exactement vaut 2 et les autres 0, que $\forall i \in \llbracket 1, n \rrbracket$, $y_i = 0$. Ceci impose alors $y_{n+1} \in 2\mathbb{Z}$. Inversement, de tels vecteurs sont bien orthogonaux à \mathbb{D}_n . On a donc établi que

$$\mathbb{D}_{n\mathbb{D}_{n+1}}^\perp = \mathbb{Z} \left(\underbrace{0, \dots, 0}_n, 2 \right),$$

et comme $\left(\underbrace{0, \dots, 0}_n, 2 \right)^2 = -4 < -2$ il n'y a pas de racines dans $\mathbb{D}_{n\mathbb{D}_{n+1}}^\perp$.

(iii) C'est la définition de \mathbb{E}_7 , il n'y a rien à démontrer.

(iv) Soit $y = (y_1, \dots, y_8) \in \mathbb{E}_7$. En particulier, $y_7 = -y_8$. La condition pour tout $x = (x_1, \dots, x_7, x_8) \in \mathbb{E}_7$, $\sum_{i=1}^8 x_i y_i = 0$ donne, pour $x = \alpha_2, \alpha_3, \dots, \alpha_6 \in \mathbb{E}_6$ (voir la partie 1.1.4 pour les notations), $y_1 = \dots = y_5 = 0$ et pour $x = \alpha_1$, $y_6 = -2y_7$, sachant de plus que les coordonnées y_i sont toutes entières ou demi-entières. Nécessairement, $y_7 \in \mathbb{Z}$, et $y \in \mathbb{Z}(0, 0, 0, 0, 0, 2, -1, 1)$. Inversement, un tel vecteur est dans \mathbb{E}_7 et est orthogonal à \mathbb{E}_6 . Enfin, un vecteur de ce réseau est de carré ≤ -6 . On a donc établi le résultat annoncé. \square

La première conséquence de ce lemme est le calcul du poids de F_L , celui-ci correspond aux poids des formes $F_{L'}$ calculées en parties 3.1.2 et 3.2.2.

Une deuxième conséquence, c'est qu'à partir du calcul de $L_{L'}^\perp$ fait dans le lemme 5.1 et de la proposition 3.1, il est facile et peu coûteux de calculer le diviseur de la forme F_L . En effet, les (éventuelles) composantes additionnelles sont dirigées par des vecteurs l_1^* dont la classe $h_L = \bar{l}_1^*$ dans $D(2U \oplus L)$ est non-nulle, admet un représentant l^* dans L^* dont la norme vérifie $-2 < l^{*2} < 0$, et à laquelle on peut associer, via le lemme 2.2 et la remarque importante 1, une classe $h_M \in p_M(H)$ admettant un représentant m^* dans M^* dont la norme vérifie $-2 < m^{*2} < 0$, et tel que $l^* + m^*$ soit une racine de N . Dans notre cas, $l^* + m^*$ sera nécessairement une racine de L' (cette fois-ci, contrairement aux parties 3.1.2 et 3.2.2, c'est possible), les tables de la partie 1.1.4 et le lemme 5.1 permettent donc de faire les calculs explicites.

Nous traiterons donc les cas de la liste du tableau de la figure 5.1, N est le (ou les) réseau de Niemeier dans lequel on plonge L' (et L), w est le poids de la forme obtenue, w' le poids de la forme strictement -2 -réflexive déjà obtenue, n est la dimension du réseau L , si bien que $\frac{n}{2}$ et $\frac{n+1}{2}$ sont respectivement les poids singulier et critique correspondants.

5.3 Calcul des formes

Plutôt que de se lancer dans le traitement des cas un par un, on va d'abord établir quelques résultats généraux.

L	L'	N	w	w'	$w - w'$	$\frac{n}{2}$	$\frac{n+1}{2}$
\mathbb{A}_1	\mathbb{A}_2	$N(12A_2)$	45	35	10	$\frac{1}{2}$	1
$2\mathbb{A}_1$	$2\mathbb{A}_2$	$N(12A_2)$	42	34	8	1	$\frac{3}{2}$
$3\mathbb{A}_1$	$3\mathbb{A}_2$	$N(12A_2)$	39	33	6	$\frac{3}{2}$	2
$4\mathbb{A}_1$	$4\mathbb{A}_2$	$N(12A_2)$	36	32	4	2	$\frac{5}{2}$
\mathbb{A}_2	\mathbb{A}_3	$N(8A_3)$	54	45	9	1	$\frac{3}{2}$
$2\mathbb{A}_2$	$2\mathbb{A}_3$	$N(8A_3)$	48	42	6	2	$\frac{5}{2}$
$3\mathbb{A}_2$	$3\mathbb{A}_3$	$N(8A_3)$	42	39	3	3	$\frac{7}{2}$
\mathbb{A}_3	\mathbb{A}_4	$N(6A_4)$	62	54	8	$\frac{3}{2}$	2
$2\mathbb{A}_3$	$2\mathbb{A}_4$	$N(6A_4)$	52	48	4	3	$\frac{7}{2}$
\mathbb{A}_4	\mathbb{A}_5	$N(4A_5 + D_4)$	69	62	7	2	$\frac{5}{2}$
\mathbb{A}_5	\mathbb{A}_6	$N(4A_6)$	75	69	6	$\frac{5}{2}$	3
\mathbb{A}_6	\mathbb{A}_7	$N(2A_7 + 2D_5)$	80	75	5	3	$\frac{7}{2}$
\mathbb{A}_7	\mathbb{A}_8	$N(3A_8)$	84	80	4	$\frac{7}{2}$	4
\mathbb{D}_4	\mathbb{D}_5	$N(2A_7 + 2D_5)$	88	72	16	2	$\frac{5}{2}$
$2\mathbb{D}_4$	$2\mathbb{D}_5$	$N(2A_7 + 2D_5)$	68	60	8	4	$\frac{9}{2}$
\mathbb{D}_5	\mathbb{D}_6	$N(4D_6), N(2A_9 + D_6)$	102	88	14	$\frac{5}{2}$	3
\mathbb{D}_6	\mathbb{D}_7	$N(E_6 + D_7 + A_{11})$	114	102	12	3	$\frac{7}{2}$
\mathbb{D}_7	\mathbb{D}_8	$N(3D_8)$	124	114	10	$\frac{7}{2}$	4
\mathbb{D}_8	\mathbb{D}_9	$N(A_{15} + D_9)$	132	124	8	4	$\frac{9}{2}$
\mathbb{E}_6	\mathbb{E}_7	$N(2E_7 + D_{10}), N(E_7 + A_{17})$	165	120	45	3	$\frac{7}{2}$
\mathbb{E}_7	\mathbb{E}_8	$N(3E_8), N(E_8 + D_{16})$	253	165	88	$\frac{7}{2}$	4

FIG. 5.1 – Autres formes modulaires obtenues par quasi-restriction

Cas des réseaux de type \mathbb{A}_n

Nous savons déjà que les -2 -vecteurs de L définissent des composantes (avec multiplicité 1) du diviseur de F_L . Nous avons aussi rappelé juste avant que d'après la proposition 3.1, les éventuelles composantes additionnelles de F_L sont "issues" des racines de N . Mais ces composantes, d'une part existent-elles, et d'autre part sont-elles réflexives ? On dispose de la proposition suivante pour répondre à cette question.

Proposition 5.1. *Soit $n \in \llbracket 1, 7 \rrbracket$, soit $L = k\mathbb{A}_n$ et $L' = k\mathbb{A}_{n+1}$, où L est plongé dans L' comme dans le lemme 5.1, et $k \in \mathbb{N}^*$ tel que $k\mathbb{A}_{n+1}$ est une composante orthogonale du sous-réseau de racines d'un réseau de Niemeier N . Alors F_L est réflexive si et seulement si $n = 1$ ou $n = 2$.*

PREUVE : On considère dans $\mathbb{A}_n^* \subset \mathbb{A}_{n+1}^*$ (par le plongement défini dans le lemme

5.1) le vecteur $\varepsilon_1 = \left(\underbrace{\frac{1}{n+1}, \dots, \frac{1}{n+1}}_n, -\frac{n}{n+1}, 0 \right)$, on a $\overline{\varepsilon_1} = [1]$ et $\varepsilon_1^2 = -\frac{n}{n+1}$. Soit

$m^* = -\frac{1}{n+1} \left(\underbrace{1, \dots, 1}_{n+1}, -(n+1) \right)$, alors $r = \varepsilon_1 + m^* = \left(\underbrace{0, \dots, 0}_n, -1, 1 \right)$ est une racine

de N , et d'après la proposition 3.1, ε_1 dirige une composante additionnelle du diviseur de F_L . Mais, $\bar{\varepsilon}_1$ est d'ordre $n+1$ dans $D(2U \oplus L)$, et comme $\varepsilon_1^2 = -\frac{n}{n+1}$, le lemme 2.1 montre que cette composante n'est pas réflexive pour $n \geq 3$.

Traisons le cas de $k\mathbb{A}_1$. Les seules classes non-nulles de vecteurs $l^* \in 2U \oplus L^*$ correspondant à des racines sont les classes des vecteurs $\varepsilon_1^{(i)}$, où $\varepsilon_1^{(i)}$ désigne le vecteur de $k\mathbb{A}_1^* \subset k\mathbb{A}_2$ tel que les coordonnées correspondant à la i -ième copie de \mathbb{A}_1 soient celles du vecteur ε_1 , et les autres sont nulles. Ces formes sont réflexives. Il n'y a pas d'autres orbites d'après le lemme 1.9. La multiplicité de ces composantes additionnelles est 2 car $m^* = \pm \left(\frac{1}{2}, \frac{1}{2}, -1 \right)$ convient. Ainsi les formes $F_{k\mathbb{A}_1}^{(2)}$, $1 \leq k \leq 4$, sont réflexives.

Traisons le cas de $k\mathbb{A}_2$. Les seules classes non-nulles de vecteurs $l^* \in 2U \oplus L^*$ correspondant à des racines sont les classes des vecteurs $\varepsilon_1^{(i)}$ et $\varepsilon_2^{(i)}$ (de même norme), où $\varepsilon_j^{(i)}$ désigne le vecteur de $k\mathbb{A}_2^* \subset k\mathbb{A}_3$ tel que les coordonnées correspondant à la i -ième copie de \mathbb{A}_2 soient celles du vecteur ε_j , et les autres sont nulles. Ces formes sont réflexives. Il n'y a pas d'autres orbites d'après le lemme 1.9. La multiplicité de ces composantes additionnelles est 1 car seul $m^* = -\left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}, -1 \right)$ convient pour ε_1 , et seul $m^* = \left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}, -1 \right)$ convient pour ε_2 . Ainsi les formes $F_{k\mathbb{A}_2}^{(2)}$, $1 \leq k \leq 3$, sont réflexives. \square

Proposition 5.2. *Soit $n \in \llbracket 4, 8 \rrbracket$, soit $L = \mathbb{D}_n$ ou $L = 2\mathbb{D}_4$, et $L' = \mathbb{D}_{n+1}$ ou $2\mathbb{D}_5$, où L est plongé dans L' comme dans le lemme 5.1. Alors F_L est réflexive.*

PREUVE : On considère dans $\mathbb{D}_n^* \subset \mathbb{D}_{n+1}^*$ (par le plongement défini dans le lemme 5.1) les vecteurs $\varepsilon_1 = \left(\frac{1}{2}, \dots, \frac{1}{2}, 0 \right)$, $\varepsilon_2 = (1, 0, \dots, 0)$ et $\varepsilon_3 = \left(\frac{1}{2}, \dots, \frac{1}{2}, -\frac{1}{2}, 0 \right)$, ils forment un système de représentants de $D(\mathbb{D}_n)$. D'après le lemme 5.1, seul ε_2 se relève en une racine de \mathbb{D}_{n+1} , avec comme vecteur correspondant $m^* = \pm(0, \dots, 0, 1)$, la multiplicité de ces composantes additionnelles est 2. ε_2 est réflexif d'après le lemme 2.1 (ou plus simplement par vérification immédiate). D'après le lemme 1.9, il n'y a pas d'autres orbites. \square

Proposition 5.3. *Soit $L = \mathbb{E}_6$ ou $L = \mathbb{E}_7$, et $L' = \mathbb{E}_7$ ou $L' = \mathbb{E}_8$, où L est plongé dans L' comme dans le lemme 5.1. Alors F_L n'est pas réflexive.*

PREUVE : Dans $L = \mathbb{E}_6 \subset \mathbb{E}_7$, on a la racine $r = \left(0, \dots, 0, \frac{2}{3}, \frac{2}{3}, -\frac{2}{3} \right) + \left(0, \dots, 0, -\frac{2}{3}, \frac{1}{3}, -\frac{1}{3} \right)$, qui donne d'après la proposition 3.1 une composante additionnelle au diviseur de F_L dirigée par $\varepsilon_1 = \left(0, \dots, 0, \frac{2}{3}, \frac{2}{3}, -\frac{2}{3} \right) \in \mathbb{E}_6^*$. Cette dernière n'est pas réflexive d'après le lemme 2.1 car $\varepsilon_1^2 = -\frac{4}{3}$ et $[1]$ est d'ordre 3.

Dans $L = \mathbb{E}_7 \subset \mathbb{E}_8$, on a la racine $r = \left(\frac{1}{2}, \dots, \frac{1}{2}, 0, 0 \right) + \left(0, \dots, 0, \frac{1}{2}, \frac{1}{2} \right)$, qui donne d'après la proposition 3.1 une composante additionnelle au diviseur de F_L dirigée par $\varepsilon_1 = \left(\frac{1}{2}, \dots, \frac{1}{2}, 0, 0 \right) \in \mathbb{E}_7^*$. Cette dernière n'est pas réflexive d'après le lemme 2.1 car $\varepsilon_1^2 = -\frac{3}{2}$ et $[1]$ est d'ordre 2. \square

Conclusion. Ainsi, d'après les propositions précédentes, on obtient 13 nouvelles formes réflexives par quasi-restriction, elles sont associées aux réseaux $k\mathbb{A}_1$, $1 \leq k \leq 4$, $k\mathbb{A}_2$, $1 \leq k \leq 3$, \mathbb{D}_4 , $2\mathbb{D}_4$, \mathbb{D}_5 , \mathbb{D}_6 , \mathbb{D}_7 et \mathbb{D}_8 . Elle donnent lieu (en considérant le quotient de ces

formes par les formes strictement -2 -réflexives associées) à 13 autres formes modulaires réflexives (qui ne sont pas des quasi-restrictions), notées G_L . Parmi elles, $G_{3\mathbb{A}_2}$ est une forme de poids singulier (égal à 3), $G_{2\mathbb{D}_4}$ et $G_{\mathbb{D}_8}$ sont le carré d'une forme de poids singulier (égal à 4 dans les deux cas), et $G_{4\mathbb{A}_1}$ est aussi le carré d'une forme de poids singulier (égal à 2).

Il faut aussi noter que la forme $F_{\mathbb{A}_7}^{(2)}$ que l'on obtient, bien que non-réflexive, donne par quotient une forme $G_{\mathbb{A}_7}$ (non-réflexive!) de poids 4, qui est le poids critique associé.

5.4 Détermination du groupe modulaire maximal des nouvelles formes obtenues

Comme dans le chapitre 4.1, nous allons chercher le groupe modulaire maximal des formes que nous venons de construire.

Les formes associées aux réseaux $k\mathbb{A}_1$, $1 \leq k \leq 4$, sont obtenues en plongeant le réseau $k\mathbb{A}_1$ dans $k\mathbb{A}_2$, et les éléments de $O(D(k\mathbb{A}_1))$ que nous avons besoin de relever dans $O^+(2U \oplus k\mathbb{A}_1)$ sont les permutations des copies de \mathbb{A}_1 . Or, le groupe de Mathieu $M_{12} \cong G_2(N(12A_2))$ agit de façon 5-transitive sur les copies de \mathbb{A}_2 , et donc suivant notre plongement ce groupe agit de façon 5-transitive sur nos k copies de \mathbb{A}_1 , ce qui signifie que le groupe maximal de ces 4 formes modulaires est $O^+(2U \oplus k\mathbb{A}_1)$, $1 \leq k \leq 4$ (en revanche, nous ne sommes pas en mesure de préciser le caractère).

Les formes associées aux réseaux $k\mathbb{A}_2$, $1 \leq k \leq 3$, sont obtenues en plongeant le réseau $k\mathbb{A}_2$ dans $k\mathbb{A}_3$, et les éléments de $O(D(k\mathbb{A}_2))$ que nous avons besoin de relever dans $O^+(2U \oplus k\mathbb{A}_2)$ sont les permutations des copies de \mathbb{A}_2 , et les éléments qui réalisent $-id$ sur une copie de \mathbb{A}_2 et id sur les autres. Or, ces différentes transformations ont été relevées dans $O^+(2U \oplus k\mathbb{A}_3)$ dans la partie 4.3, elle se relèvent de la même façon exactement dans $O^+(2U \oplus k\mathbb{A}_2)$, ce qui signifie que le groupe maximal de ces 3 formes modulaires est $O^+(2U \oplus k\mathbb{A}_2)$, $1 \leq k \leq 3$. Suivant la partie 4.3, on peut aussi préciser le caractère comme étant encore déterminant.

Pour les formes associées aux réseaux du type $2U \oplus \mathbb{D}_n$, $5 \leq n \leq 8$, les éléments de $O(D(k\mathbb{A}_2))$ que nous avons besoin de relever dans $O^+(2U \oplus \mathbb{D}_n)$ sont juste les transpositions $\tau_{[1],[3]}$. Or, ceci a déjà été fait dans la partie 4.3 relative au réseau $2U \oplus \mathbb{D}_{n+1}$, elle se relèvent de la même façon exactement dans $O^+(2U \oplus \mathbb{D}_n)$, ce qui signifie que le groupe maximal de ces 4 formes modulaires est $O^+(2U \oplus \mathbb{D}_n)$, $5 \leq n \leq 8$. Suivant la partie 4.3, on peut aussi préciser le caractère comme étant $\chi : g \in \tilde{O}^+(2U \oplus \mathbb{D}_n) \mapsto \det(g)$; $g \notin \tilde{O}^+(2U \oplus \mathbb{D}_n) \mapsto -\det(g)$.

Enfin, pour les formes associées aux réseaux du type $2U \oplus k\mathbb{D}_4$, $k = 1, 2$, comme précédemment on peut réaliser les éléments qui permutent les k copies de \mathbb{D}_4 et l'élément σ_{ε_2} sur chaque copie de \mathbb{D}_4 . On peut voir que c'est le plus que l'on peut réaliser, car une composante du diviseur de $F_{k\mathbb{D}_4}^{(2)}$ est de la forme $H_{-4}([2])$ ou $H_{-4}([2, 0])$, mais aucune de la forme $H_{-4}([1 \text{ ou } 3])$ ou $H_{-4}([1 \text{ ou } 3, 0])$, et donc on ne peut réaliser aucun élément qui échange $[2]$ et $[1]$ ou $[2]$ et $[3]$. On peut le vérifier directement à partir du code associé à

$N(2A_7 + 2D_5)$. Le groupe maximal de $F_{\mathbb{D}_4}^{(2)}$ (respectivement $F_{2\mathbb{D}_4}^{(2)}$) est donc un sous-groupe d'indice 3 de $O^+(2U \oplus \mathbb{D}_4)$ (respectivement d'indice 9 de $O^+(2U \oplus \mathbb{D}_4)$).

5.5 Bilan sur les formes obtenues

Parmi les formes que nous avons obtenues dans les parties précédentes, et celles obtenues dans la partie 3.1.2, nous retrouvons plusieurs formes déjà construites par d'autres méthodes dans divers articles.

Formes associées au réseau $2U \oplus \mathbb{A}_1$. Nous avons trouvé en partie 3.1.2 une forme $F_{\mathbb{A}_1}$ anti-invariante et de poids 35 pour le groupe $O^+(2U \oplus \mathbb{A}_1)$. Nous venons d'obtenir deux autres formes pour le groupe $O^+(2U \oplus \mathbb{A}_1)$, $F_{\mathbb{A}_1}^{(2)}$, anti-invariante de poids 45 et $G_{\mathbb{A}_1}$ invariante de poids 10. Ces formes ont été obtenues précédemment par Igusa, dans [I64]. Il s'agit de comparer les poids et les diviseurs pour voir que nos formes et les siennes sont les mêmes, à constante multiplicative près. $F_{\mathbb{A}_1}$ correspond à Δ_{35} , $G_{\mathbb{A}_1}$ correspond à Δ_5^2 , et enfin $F_{\mathbb{A}_1}^{(2)}$ correspond à $\Delta_{35}\Delta_5^2$.

Formes associées au réseau $2U \oplus 2\mathbb{A}_1$. Nous avons trouvé en partie 3.1.2 une forme $F_{2\mathbb{A}_1}$ de poids 34 pour le groupe $O^+(2U \oplus 2\mathbb{A}_1)$. Nous venons d'obtenir deux autres formes pour le groupe $O^+(2U \oplus 2\mathbb{A}_1)$, $F_{2\mathbb{A}_1}^{(2)}$, de poids 42 et $G_{2\mathbb{A}_1}$ de poids 8. On retrouve ces formes dans [DK03] p.261, à constante multiplicative près. $F_{2\mathbb{A}_1}$ correspond à $\phi_{30}\phi_4$, $G_{2\mathbb{A}_1}$ correspond à ϕ_2^2 , et enfin $F_{2\mathbb{A}_1}^{(2)}$ correspond à $\phi_{30}\phi_4^3$. Signalons une analogie forte entre les formes précédentes et celles-ci.

Formes associées au réseau $2U \oplus \mathbb{A}_2$. Nous avons trouvé en partie 3.1.2 une forme $F_{\mathbb{A}_2}$ anti-invariante et de poids 45 pour le groupe $O^+(2U \oplus \mathbb{A}_2)$. Nous venons d'obtenir deux autres formes pour le groupe $O^+(2U \oplus \mathbb{A}_2)$, $F_{\mathbb{A}_2}^{(2)}$, anti-invariante de poids 54 et $G_{\mathbb{A}_2}$ invariante de poids 9. On retrouve ces formes dans [DK03] p.261, à constante multiplicative près (ainsi que dans [D03] p.227 et [D06] p.109). $F_{\mathbb{A}_2}$ correspond à ϕ_{45} , $G_{\mathbb{A}_2}$ correspond à ϕ_9 , et enfin $F_{\mathbb{A}_2}^{(2)}$ correspond à $\phi_{45}\phi_9$.

Formes associées au réseau $2U \oplus 3\mathbb{A}_1$. Nous avons trouvé en partie 3.1.2 une forme $F_{3\mathbb{A}_1}$ de poids 33 pour le groupe $O^+(2U \oplus 3\mathbb{A}_1)$. Nous venons d'obtenir deux autres formes pour le groupe $O^+(2U \oplus 3\mathbb{A}_1)$, $F_{3\mathbb{A}_1}^{(2)}$, de poids 39 et $G_{3\mathbb{A}_1}$ de poids 6. On retrouve ces formes dans [Kl05] p.100, à constante multiplicative près. $F_{3\mathbb{A}_1}$ correspond à $\psi_{30}\psi_3$, $G_{3\mathbb{A}_1}$ correspond à ψ_3^2 , et enfin $F_{3\mathbb{A}_1}^{(2)}$ correspond à $\psi_{30}\psi_3^3$.

Formes associées au réseau $2U \oplus \mathbb{A}_3$. Nous avons trouvé en partie 3.1.2 une forme $F_{\mathbb{A}_3}$ anti-invariante de poids 54 pour le groupe $O^+(2U \oplus \mathbb{A}_3)$. On retrouve cette forme dans [Kl05] p.92, à constante multiplicative près. Elle correspond à ψ_{54} .

Formes associées au réseau $2U \oplus \mathbb{D}_4$. Nous avons trouvé en partie 3.1.2 une forme $F_{\mathbb{D}_4}$ anti-invariante de poids 72 pour le groupe $O^+(2U \oplus \mathbb{D}_4)$. Nous venons d'obtenir deux autres formes pour un sous-groupe d'indice 3, $\Gamma \subset O^+(2U \oplus \mathbb{D}_4)$, $F_{\mathbb{D}_4}^{(2)}$, de poids 88 et $G_{\mathbb{D}_4}$ de poids 16. On retrouve ces formes dans [Kr05] p.932, à constante multiplicative près, et effectivement les formes étaient déjà relatives à un sous-groupe d'indice 3 (nos résultats sont cohérents). $F_{\mathbb{D}_4}$ correspond à Δ , $G_{\mathbb{D}_4}$ correspond à G_8^2 , et enfin $F_{\mathbb{D}_4}^{(2)}$ correspond à ΔG_8^2 .

Annexe 1 : Liste des formes modulaires réflexives

Nous récapitulons dans cette partie toutes les formes réflexives que l'on a obtenues.

	F_L	groupe modulaire maximal	poids	diviseur
0	$F_{3\mathbb{E}_8} = \Phi_{12}$	$O^+(2U \oplus 3\mathbb{E}_8)$	12	$H_{-2}(\bar{0})$
1	$F_{2\mathbb{E}_8}$	$O^+(2U \oplus 2\mathbb{E}_8)$	132	$H_{-2}(\bar{0})$
2	$F_{\mathbb{E}_8}$	$O^+(2U \oplus \mathbb{E}_8)$	252	$H_{-2}(\bar{0})$
3	$F_{2\mathbb{E}_7}$	$O^+(2U \oplus 2\mathbb{E}_7)$	102	$H_{-2}(\bar{0}) \cup 20H_{-4}([1, 1])$
4	$F_{\mathbb{E}_7}$	$O^+(2U \oplus \mathbb{E}_7)$	165	$H_{-2}(\bar{0})$
5	$F_{2\mathbb{E}_6}$	$O^+(2U \oplus 2\mathbb{E}_6)$	84	$H_{-2}(\bar{0}) \cup 27H_{-6}([1, 1])$
6	$F_{\mathbb{E}_6}$	$O^+(2U \oplus \mathbb{E}_6)$	120	$H_{-2}(\bar{0})$
7	$F_{\mathbb{D}_{12}}$	$\tilde{O}^+(2U \oplus \mathbb{D}_{12})$	144	$H_{-2}(\bar{0}) \cup 24H_{-4}([1])$
8	$F_{\mathbb{D}_{10}}$	$O^+(2U \oplus \mathbb{D}_{10})$	138	$H_{-2}(\bar{0}) \cup 57H_{-2}([1])$
9	$F_{\mathbb{D}_9}$	$O^+(2U \oplus \mathbb{D}_9)$	132	$H_{-2}(\bar{0}) \cup 120H_{-4}([1])$
10	$F_{\mathbb{D}_8}$	$\tilde{O}^+(2U \oplus \mathbb{D}_8)$	124	$H_{-2}(\bar{0})$
11	$F_{\mathbb{D}_8}^{(2)}$	$O^+(2U \oplus \mathbb{D}_8)$	132	$H_{-2}(\bar{0}) \cup 2H_{-4}([2, 0, 0, 0])$
12	$G_{\mathbb{D}_8}$	$O^+(2U \oplus \mathbb{D}_8)$	8	$2H_{-4}([2, 0, 0, 0])$
13	$F_{\mathbb{D}_7}$	$O^+(2U \oplus \mathbb{D}_7)$	114	$H_{-2}(\bar{0})$
14	$F_{\mathbb{D}_7}^{(2)}$	$O^+(2U \oplus \mathbb{D}_7)$	124	$H_{-2}(\bar{0}) \cup 2H_{-4}([2, 0, 0])$
15	$G_{\mathbb{D}_7}$	$O^+(2U \oplus \mathbb{D}_7)$	10	$2H_{-4}([2, 0, 0])$
16	$F_{2\mathbb{D}_6}$	$\Gamma \subset O^+(2U \oplus 2\mathbb{D}_6)$ d'indice 2	72	$H_{-2}(\bar{0}) \cup 33H_{-2}([1, 2]) \cup 12H_{-4}([1, 3])$
17	$F_{\mathbb{D}_6}$	$O^+(2U \oplus \mathbb{D}_6)$	102	$H_{-2}(\bar{0})$
18	$F_{\mathbb{D}_6}^{(2)}$	$O^+(2U \oplus \mathbb{D}_6)$	114	$H_{-2}(\bar{0}) \cup 2H_{-4}([2, 0])$
19	$G_{\mathbb{D}_6}$	$O^+(2U \oplus \mathbb{D}_6)$	12	$2H_{-4}([2, 0])$
20	$F_{2\mathbb{D}_5}$	$O^+(2U \oplus 2\mathbb{D}_5)$	68	$H_{-2}(\bar{0}) \cup 64H_{-4}([1, 2]) \cup 28H_{-8}([1, 1])$
21	$F_{\mathbb{D}_5}$	$O^+(2U \oplus \mathbb{D}_5)$	88	$H_{-2}(\bar{0})$
22	$F_{\mathbb{D}_5}^{(2)}$	$O^+(2U \oplus \mathbb{D}_5)$	102	$H_{-2}(\bar{0}) \cup 2H_{-4}([2])$
23	$G_{\mathbb{D}_5}$	$O^+(2U \oplus \mathbb{D}_5)$	14	$2H_{-4}([2])$
24	$F_{3\mathbb{D}_4}$	$\Gamma \subset O^+(2U \oplus 3\mathbb{D}_4)$ d'indice 4	48	$H_{-2}(\bar{0}) \cup 8H_{-4}([1, 1, 1])$
25	$F_{2\mathbb{D}_4}$	$\Gamma \subset O^+(2U \oplus 2\mathbb{D}_4)$ d'indice 2	60	$H_{-2}(\bar{0})$
26	$F_{2\mathbb{D}_4}^{(2)}$	$\Gamma \subset O^+(2U \oplus 2\mathbb{D}_4)$ d'indice 9	68	$H_{-2}(\bar{0}) \cup 2H_{-4}([2, 0])$
27	$G_{2\mathbb{D}_4}$?	8	$2H_{-4}([2, 0])$
28	$F_{\mathbb{D}_4}$	$O^+(2U \oplus \mathbb{D}_4)$	72	$H_{-2}(\bar{0})$
29	$F_{\mathbb{D}_4}^{(2)}$	$\Gamma \subset O^+(2U \oplus \mathbb{D}_4)$ d'indice 3	88	$H_{-2}(\bar{0}) \cup 2H_{-4}([2])$

	F_L	groupe modulaire maximal	poids	diviseur
30	$G_{\mathbb{D}_4}$	$\Gamma \subset O^+(2U \oplus \mathbb{D}_4)$ d'indice 3	16	$2H_{-4}([2])$
31	$F_{\mathbb{A}_5 \oplus \mathbb{D}_4}$	$O^+(2U \oplus \mathbb{A}_5 \oplus \mathbb{D}_4)$	57	$H_{-2}(\bar{0}) \cup 21H_{-2}([3, 1]) \cup 36H_{-12}([2, 1])$
32	$F_{\mathbb{A}_{11}}$	$O^+(2U \oplus \mathbb{A}_{11})$	90	$H_{-2}(\bar{0}) \cup 78H_{-4}([3]) \cup 56H_{-6}([4])$ $\cup 14H_{-4}([6])$
33	$F_{\mathbb{A}_9}$	$O^+(2U \oplus \mathbb{A}_9)$	87	$H_{-2}(\bar{0}) \cup 165H_{-10}([3]) \cup 45H_{-10}([4])$ $\cup 33H_{-2}([5])$
34	$F_{\mathbb{A}_8}$	$O^+(2U \oplus \mathbb{A}_8)$	84	$H_{-2}(\bar{0}) \cup 81H_{-18}([4])$
35	$F_{\mathbb{A}_7}$	$O^+(2U \oplus \mathbb{A}_7)$	80	$H_{-2}(\bar{0})$
36	$F_{\mathbb{A}_6}$	$O^+(2U \oplus \mathbb{A}_6)$	75	$H_{-2}(\bar{0})$
37	$F_{2\mathbb{A}_5}$	$O^+(2U \oplus 2\mathbb{A}_5)$	54	$H_{-2}(\bar{0}) \cup 63H_{-6}([1, 2]) \cup 36H_{-12}([1, 3])$ $\cup 15H_{-6}([2, 2]) \cup 8H_{-4}([3, 3])$
38	$F_{\mathbb{A}_5}$	$O^+(2U \oplus \mathbb{A}_5)$	69	$H_{-2}(\bar{0})$
39	$F_{2\mathbb{A}_4}$	$O^+(2U \oplus 2\mathbb{A}_4)$	52	$H_{-2}(\bar{0}) \cup 25H_{-10}([2, 2])$
40	$F_{\mathbb{A}_4}$	$O^+(2U \oplus \mathbb{A}_4)$	62	$H_{-2}(\bar{0})$
41	$F_{3\mathbb{A}_3}$	$O^+(2U \oplus 3\mathbb{A}_3)$	42	$H_{-2}(\bar{0}) \cup 30H_{-4}([1, 1, 1])$ $\cup 16H_{-8}([1, 1, 2]) \cup 6H_{-4}([2, 2, 2])$
42	$F_{2\mathbb{A}_3}$	$O^+(2U \oplus 2\mathbb{A}_3)$	48	$H_{-2}(\bar{0})$
43	$F_{\mathbb{A}_3}$	$O^+(2U \oplus \mathbb{A}_3)$	54	$H_{-2}(\bar{0})$
44	$F_{4\mathbb{A}_2}$	$\Gamma \subset O^+(2U \oplus 4\mathbb{A}_2)$ d'indice 8	36	$H_{-2}(\bar{0}) \cup 9H_{-6}([1, 1, 1, 1])$
45	$F_{3\mathbb{A}_2}$	$\Gamma \subset O^+(2U \oplus 3\mathbb{A}_2)$ d'indice 4	39	$H_{-2}(\bar{0})$
46	$F_{3\mathbb{A}_2}^{(2)}$	$O^+(2U \oplus 3\mathbb{A}_2)$	48	$H_{-2}(\bar{0}) \cup H_{-6}([1, 0, 0])$
47	$G_{3\mathbb{A}_2}$	$\Gamma \subset O^+(2U \oplus 3\mathbb{A}_2)$ d'indice 4	3	$H_{-6}([1, 0, 0])$
48	$F_{2\mathbb{A}_2}$	$\Gamma \subset O^+(2U \oplus 2\mathbb{A}_2)$ d'indice 2	42	$H_{-2}(\bar{0})$
49	$F_{2\mathbb{A}_2}^{(2)}$	$O^+(2U \oplus 2\mathbb{A}_2)$	48	$H_{-2}(\bar{0}) \cup H_{-6}([1, 0])$
50	$G_{2\mathbb{A}_2}$	$\Gamma \subset O^+(2U \oplus 2\mathbb{A}_2)$ d'indice 2	6	$H_{-6}([1, 0])$
51	$F_{\mathbb{A}_2}$	$O^+(2U \oplus \mathbb{A}_2)$	45	$H_{-2}(\bar{0})$
52	$F_{\mathbb{A}_2}^{(2)}$	$O^+(2U \oplus \mathbb{A}_2)$	54	$H_{-2}(\bar{0}) \cup H_{-6}([1])$
53	$G_{\mathbb{A}_2}$	$O^+(2U \oplus \mathbb{A}_2)$	9	$H_{-6}([1])$
54	$F_{10\mathbb{A}_1}$?	26	voir la partie 3.2.3
55	$F_{9\mathbb{A}_1}$?	27	voir la partie 3.2.3
56	$F_{16\mathbb{A}_1 \perp N(24\mathbb{A}_1)}$?	28	$H_{-2}(\bar{0})$
57	$F_{8\mathbb{A}_1}$?	28	voir la partie 3.2.3
58	$F_{7\mathbb{A}_1}$?	29	voir la partie 3.2.3
59	$F_{6\mathbb{A}_1}^{(1)}$?	30	voir la partie 3.2.3
60	$F_{6\mathbb{A}_1}^{(2)}$?	30	voir la partie 3.2.3
61	$F_{5\mathbb{A}_1}$	$O^+(2U \oplus 5\mathbb{A}_1)$	31	$H_{-2}(\bar{0}) \cup H_{-2}([1, 0, 0, 0, 0])$ $\cup 9H_{-2}([1, 1, 1, 1, 1])$
62	$F_{4\mathbb{A}_1}$	$O^+(2U \oplus 4\mathbb{A}_1)$	32	$H_{-2}(\bar{0}) \cup H_{-2}([1, 0, 0, 0])$
63	$F_{4\mathbb{A}_1}^{(2)}$	$O^+(2U \oplus 4\mathbb{A}_1)$	36	$H_{-2}(\bar{0}) \cup 3H_{-2}([1, 0, 0, 0])$
64	$G_{4\mathbb{A}_1}$	$O^+(2U \oplus 4\mathbb{A}_1)$	4	$2H_{-2}([1, 0, 0, 0])$
65	$F_{3\mathbb{A}_1}$	$O^+(2U \oplus 3\mathbb{A}_1)$	33	$H_{-2}(\bar{0}) \cup H_{-2}([1, 0, 0])$
66	$F_{3\mathbb{A}_1}^{(2)}$	$O^+(2U \oplus 3\mathbb{A}_1)$	39	$H_{-2}(\bar{0}) \cup 3H_{-2}([1, 0, 0])$

	F_L	groupe modulaire maximal	poids	diviseur
67	$G_{3\mathbb{A}_1}$	$O^+(2U \oplus 3\mathbb{A}_1)$	6	$2H_{-2}([1, 0, 0])$
68	$F_{2\mathbb{A}_1}$	$O^+(2U \oplus 2\mathbb{A}_1)$	34	$H_{-2}(\bar{0}) \cup H_{-2}([1, 0])$
69	$F_{2\mathbb{A}_1}^{(2)}$	$O^+(2U \oplus 2\mathbb{A}_1)$	42	$H_{-2}(\bar{0}) \cup 3H_{-2}([1, 0])$
70	$G_{2\mathbb{A}_1}$	$O^+(2U \oplus 2\mathbb{A}_1)$	8	$2H_{-2}([1, 0])$
71	$F_{\mathbb{A}_1}$	$O^+(2U \oplus \mathbb{A}_1)$	35	$H_{-2}(\bar{0}) \cup H_{-2}([1])$
72	$F_{\mathbb{A}_1}^{(2)}$	$O^+(2U \oplus \mathbb{A}_1)$	45	$H_{-2}(\bar{0}) \cup 3H_{-2}([1])$
73	$G_{\mathbb{A}_1}$	$O^+(2U \oplus \mathbb{A}_1)$	10	$2H_{-2}([1])$

Annexe 2 : Calculs de diviseurs

Calcul des diviseurs des formes associées aux réseaux $8\mathbb{A}_1$, $9\mathbb{A}_1$ et $10\mathbb{A}_1$

On calcule ici, à l'aide du logiciel *Maple*, les diviseurs de ces formes.

Dans un premier temps, on charge les outils de “linalg”, et on réalise une matrice génératrice du code de Golay binaire étendu \mathcal{C}_{24} (on choisit celle donnée en partie 1.2.4.

```
> with(linalg):
Warning, the protected names norm and trace have been redefined and unprotected

> M:=matrix([
  [1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1],
  [0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1],
  [0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1],
  [0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1],
  [0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1],
  [0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1],
  [0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1],
  [0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1],
  [0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1],
  [0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1],
  [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1],
  [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0]]):
```

On va ensuite écrire une procédure qui permet d'associer de façon bijective, à un entier compris entre 0 et 4095, un mot de \mathcal{C}_{24} . Pour cela, on remarque qu'un mot de \mathcal{C}_{24} est une combinaison linéaire à coefficients dans \mathbb{F}_2 des 12 vecteurs lignes de M . D'autre part, l'ensemble des coefficients possibles décrit exactement les nombres 0 à 4095 écrits en base 2. On va donc procéder en deux temps, d'abord on saisit la procédure *base2* qui permet de transformer un nombre entier entre 0 et 4095 en une liste de 12 éléments de $\{0,1\}$ correspondant à son écriture binaire à l'envers, puis la procédure *golay* qui à un nombre compris entre 0 et 4095 associe un mot de \mathcal{C}_{24} sous la forme d'une liste à 24 éléments de \mathbb{F}_2 .

```
> base2:=proc(n) local l,m,i;
> l:=[];m:=n;
> for i from 1 to 12 do
```

```

> l:= [op(1),m mod 2];m:=iquo(m,2);
> od;
> l;
> end proc;
base2 := proc(n)
local l, m, i;
  l := [];
  m := n;
  for i to 12 do l := [op(1), 'mod'(m, 2)]; m := iquo(m, 2) end do
  l
end proc

> golay:=proc(n) local l,v,j;
> l:=base2(n);v:=[];
> for j from 1 to 24 do
>   v:=[op(v),sum('eval(M[k,j])*l[k] ', 'k'=1..12) mod 2];
> od;
> v;
> end proc;
golay := proc(n)
local l, v, j;
  l := base2(n);
  v := [];
  for j to 24 do
    v := [op(v), 'mod'(('sum'(('eval'(M[k, j]))*l[k] ', 'k' = (1 .. 12))), 2)]
  end do
  v
end proc

```

Ensuite, nous écrivons une procédure *scalaire* qui permet de calculer le nombre de lettres communes à deux mots u, v de \mathbb{F}_2^{24} . En particulier $scalaire(u, u)$ renvoie le poids de u . Nous utiliserons la procédure *scalaire* de deux façons. Soit pour calculer le poids d'un mot, soit pour calculer le nombre de lettres non nulles d'un mot $u \in \mathcal{C}_{24}$ parmi des coordonnées de \mathbb{F}_2^{24} choisies à l'avance, en prenant pour v un 24-uplet dont les coordonnées que l'on a choisies valent 1 et les autres 0. Par exemple, lorsque l'on considère un plongement de $8A_1$ dans $N(24A_1)$, cela revient à choisir 8 coordonnées parmi les 24 de \mathbb{F}_2^{24} . On posera v le vecteur de F_2^{24} dont les coordonnées non nulles correspondent exactement aux coordonnées du plongement. Pour $u \in \mathcal{C}_{24}$, $scalaire(u, v)$ donnera le nombre de lettres non nulles de u parmi les coordonnées du plongement. La procédure *simplifie* prend en argument deux 24-uplet de $F_2^{(24)}$, u et v , et renvoie une liste dont la longueur est égale au poids de v , et dont les éléments sont les lettres de u correspondant aux coordonnées des lettres non nulles de v . En particulier $scalaire(u, v)$ donne le nombre de lettres non nulle du mot *simplifie*(u, v).

```

> scalaire:=proc(u,v) local n;
> n:=sum('u[k]*v[k] ', 'k'=1..24);
> n;

```

```

> end proc;
    scalaire := proc(u, v)
    local n;
      n := 'sum'('u[k]*v[k]', 'k' = (1 .. 24));
      n
    end proc

> simplifie:=proc(u,v) local l,i;
> l:=[];
> for i from 1 to 24 do
>   if v[i]=1 then l:=[op(l),u[i]] fi
> od;
> l;
> end proc;
simplifie := proc(u, v)
local l, i;
  l := [];
  for i to 24 do if v[i] = 1 then l := [op(l), u[i]] end if end do
  l
end proc

```

Enfin, nous pouvons écrire la procédure *diviseur* qui prend en argument un 24-uplet v correspondant à un plongement de $L = 8A_1, 9A_1$ ou $10A_1$ (suivant l'explication précédente), et renvoie 4 listes, correspondant aux éléments qui donnent lieu à une composante additionnelle du diviseur de F_L , classifiées par type (celles qui proviennent d'un S_5 , puis celles d'un S_6 , puis celles d'un U_{12} dirigées par un mot de poids 9, puis celle d'un U_{12} dirigées par un mot de poids 10), et simplifiées (coordonnées qui correspondent au plongement seulement), en se basant sur les remarques faites dans la partie 3.2.3.

```

> diviseur:=proc(u) local l,m,i,v,p,q;
> l:=[];m:=[];p:=[];q:=[]:
> for i from 1 to 4096 do
>   v:=golay(i);
>   if scalaire(v,v)=8 then
>     if scalaire(u,v)=5 then l:=[op(l),simplifie(v,u)] else
>       if scalaire(u,v)=6 then m:=[op(m),simplifie(v,u)] fi;
>     fi;
>   else if scalaire(v,v)=12 then
>     if scalaire(u,v)=9 then p:=[op(p),simplifie(v,u)] else
>       if scalaire(u,v)=10 then q:=[op(q),simplifie(v,u)] fi;
>     fi;
>   fi;
> fi;od;
> [l,m,p,q];
> end proc;
diviseur := proc(u)
local l, m, i, v, p, q;

```

```

l := [];
m := [];
p := [];
q := [];
for i to 4096 do
  v := golay(i);
  if scalaire(v, v) = 8 then
    if scalaire(u, v) = 5 then
      l := [op(l), simplifie(v, u)]
    else
      if scalaire(u, v) = 6 then m := [op(m), simplifie(v, u)] end if
    end if
  else
    if scalaire(v, v) = 12 then
      if scalaire(u, v) = 9 then
        p := [op(p), simplifie(v, u)]
      else
        if scalaire(u, v) = 10 then q := [op(q), simplifie(v, u)] end if
      end if
    end if
  end if
end do
[l, m, p, q]
end proc

```

Passons à l'application. On remarque par exemple que le mot de \mathcal{C}_{24} correspondant à la dernière ligne de la matrice M est de poids 12. On recherche un plongement de $8\mathbb{A}_1$ qui est un U_8 , c'est-à-dire contenu dans un U_{12} . On fixe par exemple le plongement donné par le vecteur $w8$ (tous les plongements de $8\mathbb{A}_1$ qui sont des U_8 sont équivalents).

```
> w8:= [0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1,0,0,0,0,0]:
```

On lance la procédure *diviseur* appliquée à $w8$ pour obtenir la liste des composantes additionnelles.

```

> diviseur(w8);
[ [[0, 1, 1, 0, 1, 1, 1, 0], [0, 0, 0, 1, 1, 1, 1, 1],
  [0, 0, 1, 1, 1, 1, 1, 0], [0, 1, 0, 1, 0, 1, 1, 1],
  [0, 1, 1, 1, 1, 0, 1, 0], [0, 1, 1, 0, 0, 1, 1, 1],
  [0, 1, 0, 0, 1, 1, 1, 1], [0, 0, 1, 1, 1, 0, 1, 1],
  [0, 1, 0, 1, 1, 0, 1, 1], [0, 1, 1, 1, 0, 1, 1, 0],
  [0, 0, 1, 1, 0, 1, 1, 1], [0, 1, 1, 0, 1, 0, 1, 1],
  [1, 1, 0, 0, 1, 1, 0, 1], [1, 1, 0, 0, 0, 1, 1, 1],
  [1, 0, 0, 1, 1, 0, 1, 1], [1, 0, 1, 1, 0, 1, 1, 0],
  [1, 0, 0, 1, 1, 1, 0, 1], [1, 1, 1, 0, 1, 1, 0, 0],
  [1, 0, 1, 1, 1, 0, 1, 0], [1, 1, 1, 0, 0, 1, 1, 0],
  [1, 1, 0, 0, 1, 0, 1, 1], [1, 1, 1, 1, 0, 1, 0, 0],

```

```
[1, 1, 1, 0, 1, 0, 0, 1], [1, 0, 1, 1, 0, 1, 0, 1],
[1, 0, 1, 1, 1, 1, 0, 0], [1, 1, 1, 0, 1, 0, 1, 0],
[1, 0, 0, 1, 0, 1, 1, 1], [1, 1, 0, 1, 1, 0, 0, 1],
[1, 1, 1, 1, 1, 0, 0, 0], [1, 1, 0, 1, 0, 1, 0, 1],
[1, 0, 1, 1, 1, 0, 0, 1], [1, 1, 1, 0, 0, 1, 0, 1]],
```

```
[[0, 1, 1, 1, 1, 1, 0, 1], [1, 1, 1, 1, 0, 0, 1, 1],
[1, 0, 1, 0, 1, 1, 1, 1], [1, 1, 0, 1, 1, 1, 1, 0]],
```

```
[],
```

```
[]]
```

On procède de même avec w_9 et w_{10} .

```
> w9:=[0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1,0,0,0,0]:
```

```
> diviseur(w9);
```

```
[[[0, 1, 1, 0, 1, 1, 1, 0, 0], [0, 1, 0, 1, 0, 1, 1, 0, 1],
[0, 0, 0, 1, 1, 1, 1, 1, 0], [0, 0, 1, 0, 1, 0, 1, 1, 1],
[0, 1, 0, 1, 0, 1, 1, 1, 0], [0, 0, 1, 1, 0, 0, 1, 1, 1],
[0, 1, 1, 1, 1, 0, 1, 0, 0], [0, 1, 1, 0, 1, 0, 0, 1, 1],
[0, 1, 0, 0, 1, 1, 1, 0, 1], [0, 1, 1, 1, 1, 0, 0, 0, 1],
[0, 0, 0, 1, 1, 1, 0, 1, 1], [0, 0, 1, 0, 1, 1, 0, 1, 1],
[0, 1, 1, 1, 0, 0, 0, 1, 1], [0, 1, 0, 1, 1, 1, 0, 0, 1],
[0, 1, 0, 0, 1, 1, 1, 1, 0], [0, 0, 1, 1, 1, 0, 1, 1, 0],
[0, 0, 1, 1, 0, 1, 0, 1, 1], [0, 1, 1, 1, 0, 1, 1, 0, 0],
[0, 0, 1, 1, 0, 1, 1, 1, 0], [0, 1, 1, 0, 1, 0, 1, 1, 0],
[0, 0, 0, 0, 1, 1, 1, 1, 1], [0, 1, 0, 1, 0, 1, 0, 1, 1],
[0, 1, 1, 1, 0, 0, 1, 0, 1], [0, 1, 1, 0, 1, 1, 0, 0, 1],
[1, 0, 1, 0, 0, 0, 1, 1, 1], [1, 1, 0, 0, 0, 1, 1, 1, 0],
[1, 0, 0, 1, 1, 0, 1, 1, 0], [1, 0, 0, 0, 1, 1, 1, 0, 1],
[1, 1, 0, 1, 0, 0, 1, 0, 1], [1, 0, 1, 1, 0, 1, 1, 0, 0],
[1, 0, 0, 1, 1, 1, 0, 1, 0], [1, 0, 1, 0, 0, 1, 0, 1, 1],
[1, 1, 1, 0, 1, 1, 0, 0, 0], [1, 0, 1, 1, 1, 0, 1, 0, 0],
[1, 1, 1, 0, 0, 1, 1, 0, 0], [1, 1, 0, 0, 1, 0, 1, 1, 0],
[1, 1, 0, 1, 1, 0, 0, 0, 1], [1, 0, 0, 1, 1, 0, 1, 0, 1],
[1, 1, 1, 0, 1, 0, 0, 1, 0], [1, 0, 1, 1, 0, 1, 0, 1, 0],
[1, 1, 0, 1, 0, 0, 0, 1, 1], [1, 0, 0, 0, 1, 0, 1, 1, 1],
[1, 0, 1, 0, 1, 1, 0, 0, 1], [1, 0, 1, 1, 1, 1, 0, 0, 0],
[1, 1, 0, 1, 1, 0, 0, 1, 0], [1, 1, 1, 1, 1, 0, 0, 0, 0],
[1, 0, 0, 1, 1, 1, 0, 0, 1], [1, 1, 0, 1, 0, 1, 0, 1, 0],
[1, 1, 0, 0, 0, 1, 1, 0, 1], [1, 1, 1, 0, 0, 0, 0, 1, 1],
[1, 0, 1, 1, 0, 0, 1, 0, 1], [1, 0, 1, 0, 0, 1, 1, 0, 1],
[1, 1, 0, 0, 0, 0, 1, 1, 1], [1, 1, 1, 0, 0, 1, 0, 1, 0]],
```

```
[[0, 0, 1, 1, 1, 1, 1, 0, 1], [0, 1, 1, 1, 1, 1, 0, 1, 0],
```

```
[0, 1, 1, 0, 0, 1, 1, 1, 1], [0, 1, 0, 1, 1, 0, 1, 1, 1],
[1, 1, 0, 0, 1, 1, 0, 1, 1], [1, 1, 1, 1, 0, 0, 1, 1, 0],
[1, 1, 1, 1, 0, 1, 0, 0, 1], [1, 1, 1, 0, 1, 0, 1, 0, 1],
[1, 0, 0, 1, 0, 1, 1, 1, 1], [1, 0, 1, 0, 1, 1, 1, 1, 0],
[1, 0, 1, 1, 1, 0, 0, 1, 1], [1, 1, 0, 1, 1, 1, 1, 0, 0]],
```

```
[[1, 1, 1, 1, 1, 1, 1, 1, 1]],
```

```
[]]
```

```
> w10:=[0,0,0,0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1,1,0,0,0]:
```

```
> diviseur(w10);
```

```
[[[0, 1, 1, 0, 1, 1, 1, 0, 0, 0], [0, 1, 0, 1, 1, 1, 0, 0, 0, 1],
[0, 1, 0, 1, 0, 1, 1, 0, 1, 0], [0, 1, 1, 0, 0, 1, 0, 0, 1, 1],
[0, 1, 1, 1, 0, 0, 0, 1, 0, 1], [0, 1, 0, 0, 1, 0, 0, 1, 1, 1],
[0, 1, 1, 0, 0, 0, 1, 0, 1, 1], [0, 1, 0, 1, 1, 0, 1, 0, 0, 1],
[0, 0, 1, 0, 1, 0, 1, 1, 1, 0], [0, 0, 0, 1, 1, 0, 0, 1, 1, 1],
[0, 0, 1, 1, 0, 1, 0, 0, 1, 1], [0, 0, 1, 0, 0, 1, 1, 1, 0, 1],
[0, 1, 1, 0, 0, 1, 0, 1, 0, 1], [0, 1, 0, 1, 0, 1, 1, 1, 0, 0],
[0, 1, 1, 1, 1, 0, 1, 0, 0, 0], [0, 1, 1, 0, 1, 0, 0, 1, 1, 0],
[0, 0, 0, 1, 0, 1, 1, 0, 1, 1], [0, 0, 1, 0, 1, 1, 1, 0, 0, 1],
[0, 1, 0, 1, 0, 0, 1, 1, 0, 1], [0, 0, 0, 1, 1, 1, 0, 1, 1, 0],
[0, 1, 0, 0, 0, 0, 1, 1, 1, 1], [0, 1, 1, 1, 0, 0, 0, 1, 1, 0],
[0, 1, 0, 1, 1, 1, 0, 0, 1, 0], [0, 1, 0, 0, 1, 1, 1, 1, 0, 0],
[0, 0, 1, 1, 1, 0, 1, 1, 0, 0], [0, 0, 1, 1, 0, 1, 0, 1, 1, 0],
[0, 0, 0, 0, 0, 1, 1, 1, 1, 1], [0, 0, 1, 0, 1, 0, 1, 0, 1, 1],
[0, 0, 1, 1, 1, 0, 0, 1, 0, 1], [0, 1, 0, 0, 1, 1, 0, 1, 0, 1],
[0, 0, 1, 1, 0, 1, 1, 1, 0, 0], [0, 0, 0, 0, 1, 1, 1, 1, 1, 0],
[0, 1, 1, 1, 0, 0, 1, 0, 1, 0], [0, 0, 1, 1, 1, 1, 0, 0, 0, 1],
[0, 0, 0, 1, 1, 0, 1, 0, 1, 1], [0, 1, 1, 0, 1, 1, 0, 0, 1, 0],
[1, 0, 0, 1, 0, 0, 0, 1, 1, 1], [1, 0, 1, 0, 0, 0, 1, 1, 1, 0],
[1, 0, 1, 0, 1, 0, 0, 1, 0, 1], [1, 0, 0, 1, 1, 0, 1, 1, 0, 0],
[1, 0, 0, 0, 1, 1, 1, 0, 1, 0], [1, 0, 1, 1, 0, 1, 1, 0, 0, 0],
[1, 0, 0, 1, 1, 1, 0, 1, 0, 0], [1, 0, 1, 0, 0, 1, 0, 1, 1, 0],
[1, 1, 0, 1, 0, 1, 0, 0, 0, 1], [1, 1, 1, 0, 0, 1, 1, 0, 0, 0],
[1, 1, 0, 0, 1, 0, 1, 1, 0, 0], [1, 1, 0, 1, 1, 0, 0, 0, 1, 0],
[1, 0, 0, 1, 1, 0, 1, 0, 1, 0], [1, 0, 1, 0, 1, 0, 0, 0, 1, 1],
[1, 0, 0, 0, 0, 1, 0, 1, 1, 1], [1, 0, 0, 1, 0, 1, 1, 0, 0, 1],
[1, 1, 1, 0, 1, 0, 0, 1, 0, 0], [1, 1, 0, 1, 0, 0, 0, 1, 1, 0],
[1, 0, 1, 0, 1, 1, 0, 0, 1, 0], [1, 1, 1, 0, 0, 0, 1, 0, 0, 1],
[1, 0, 1, 1, 1, 1, 0, 0, 0, 0], [1, 0, 0, 0, 1, 1, 1, 0, 0, 1],
[1, 0, 1, 0, 0, 0, 1, 1, 0, 1], [1, 0, 1, 1, 0, 0, 0, 0, 1, 1],
[1, 1, 0, 0, 0, 1, 0, 0, 1, 1], [1, 1, 0, 0, 1, 0, 1, 0, 0, 1],
[1, 1, 1, 1, 1, 0, 0, 0, 0, 0], [1, 1, 0, 1, 0, 1, 0, 1, 0, 0],
[1, 1, 0, 0, 0, 1, 1, 0, 1, 0], [1, 0, 1, 1, 0, 0, 1, 0, 1, 0],
```

[1, 1, 0, 0, 1, 0, 0, 0, 1, 1], [1, 1, 1, 1, 0, 0, 0, 0, 0, 1],
 [1, 0, 0, 0, 1, 1, 0, 1, 0, 1], [1, 1, 0, 0, 0, 0, 1, 1, 1, 0],
 [1, 1, 1, 0, 0, 1, 0, 1, 0, 0], [1, 0, 0, 1, 0, 0, 1, 1, 0, 1]],

[[0, 0, 0, 1, 1, 1, 1, 1, 0, 1], [0, 0, 1, 1, 1, 1, 1, 0, 1, 0],
 [0, 1, 1, 1, 1, 1, 0, 1, 0, 0], [0, 0, 1, 1, 0, 0, 1, 1, 1, 1],
 [0, 1, 0, 0, 1, 1, 1, 0, 1, 1], [0, 1, 1, 1, 1, 0, 0, 0, 1, 1],
 [0, 1, 1, 0, 0, 1, 1, 1, 1, 0], [0, 0, 1, 0, 1, 1, 0, 1, 1, 1],
 [0, 1, 0, 1, 1, 0, 1, 1, 1, 0], [0, 1, 1, 1, 0, 1, 1, 0, 0, 1],
 [0, 1, 1, 0, 1, 0, 1, 1, 0, 1], [0, 1, 0, 1, 0, 1, 0, 1, 1, 1],
 [1, 1, 0, 0, 1, 1, 0, 1, 1, 0], [1, 1, 0, 0, 0, 1, 1, 1, 0, 1],
 [1, 1, 0, 1, 0, 0, 1, 0, 1, 1], [1, 1, 1, 1, 0, 0, 1, 1, 0, 0],
 [1, 1, 1, 0, 1, 1, 0, 0, 0, 1], [1, 0, 1, 1, 1, 0, 1, 0, 0, 1],
 [1, 1, 1, 1, 0, 1, 0, 0, 1, 0], [1, 0, 1, 1, 0, 1, 0, 1, 0, 1],
 [1, 0, 0, 0, 1, 0, 1, 1, 1, 1], [1, 1, 1, 0, 1, 0, 1, 0, 1, 0],
 [1, 0, 0, 1, 0, 1, 1, 1, 1, 0], [1, 1, 0, 1, 1, 0, 0, 1, 0, 1],
 [1, 0, 0, 1, 1, 1, 0, 0, 1, 1], [1, 1, 1, 0, 0, 0, 0, 1, 1, 1],
 [1, 0, 1, 0, 1, 1, 1, 1, 0, 0], [1, 0, 1, 0, 0, 1, 1, 0, 1, 1],
 [1, 0, 1, 1, 1, 0, 0, 1, 1, 0], [1, 1, 0, 1, 1, 1, 1, 0, 0, 0]],

[],

[[1, 1, 1, 1, 1, 1, 1, 1, 1, 1]]]

Calcul du diviseur de la forme associée au réseau $4\mathbb{A}_2$

Pour la forme $F_{4\mathbb{A}_2}$, nous suivons la même procédure. Tout d'abord on donne une matrice génératrice du code de Golay ternaire \mathcal{C}_{12} étendu, puis on écrit une procédure *base3* qui convertit un entier entre 0 et 728 en base 3, puis une procédure *golay3* qui à un entier entre 1 et 728 associe de façon bijective un élément du code de Golay ternaire étendu.

```
> N:=matrix([[1,0,0,0,0,0,0,1,1,1,1,1],[0,1,0,0,0,0,1,0,1,2,2,1],
[0,0,1,0,0,0,1,1,0,1,2,2],[0,0,0,1,0,0,1,2,1,0,1,2],[0,0,0,0,1,0,1,2,2,1,0,1],
[0,0,0,0,0,1,1,1,2,2,1,0]]);
      [1  0  0  0  0  0  0  1  1  1  1  1]
      [
      [0  1  0  0  0  0  1  0  1  2  2  1]
      [
      [0  0  1  0  0  0  1  1  0  1  2  2]
      [
      [0  0  0  1  0  0  1  2  1  0  1  2]
      [
      [0  0  0  0  1  0  1  2  2  1  0  1]
      [
      [0  0  0  0  0  1  1  1  2  2  1  0]
```

```

> base3:=proc(n) local l,m,i;
> l:=[];m:=n;
> for i from 1 to 6 do
>   l:=[op(l),m mod 3];m:=iquo(m,3);
> od;
> l;
> end proc;
base3 := proc(n)
local l, m, i;
  l := [];
  m := n;
  for i to 6 do l := [op(l), 'mod'(m, 3)]; m := iquo(m, 3) end do
  l
end proc

> golay3:=proc(n) local l,v,j;
> l:=base3(n);v:=[];
> for j from 1 to 12 do
>   v:=[op(v),sum('eval(N[k,j])*l[k] ', 'k'=1..6) mod 3];
> od;
> v;
> end proc;
golay3 := proc(n)
local l, v, j;
  l := base3(n);
  v := [];
  for j to 12 do
    v := [op(v), 'mod'(('sum'(('eval'(N[k, j]))*l[k] ', 'k' = (1 .. 6)), 3))]
  end do
  v
end proc

```

Enfin, les procédures *scalaire3*, *simplifie3* et *diviseur3* jouent le même rôle que *scalaire*, *simplifie* et *diviseur*.

```

> scalaire3:=proc(u,v) local i,n;
> n:=0;
> for i from 1 to 12 do
>   if u[i]*v[i]<>0 then n:=n+1 fi;
> od;
> n;
> end proc;
scalaire3 := proc(u, v)
local i, n;
  n := 0;
  for i to 12 do if u[i]*v[i] <> 0 then n := n + 1 end if end do

```

```

n
end proc

> simplifie3:=proc(u,v) local l,i;
> l:=[];
> for i from 1 to 12 do
>   if v[i]=1 then l:=[op(l),u[i]] fi
> od;
> l;
> end proc;
simplifie3 := proc(u, v)
local l, i;
  l := [];
  for i to 12 do if v[i] = 1 then l := [op(l), u[i]] end if end do
  l
end proc

> diviseur3:=proc(u) local l,i,v;
> l:=[];
> for i from 1 to 729 do
>   v:=golay3(i);
>   if scalaire3(v,v)=6 then
>     if scalaire3(u,v)=4 then l:=[op(l),simplifie3(v,u)] fi
>   fi;
> od;
> l;
> end proc;
diviseur3 := proc(u)
local l, i, v;
  l := [];
  for i to 729 do
    v := golay3(i);
    if scalaire3(v, v) = 6 then
      if scalaire3(u, v) = 4 then l := [op(l), simplifie3(v, u)] end if
    end if
  end do
  l
end proc

```

On applique la procédure à

```
> w:=[1,1,1,1,0,0,0,0,0,0,0,0]:
```

qui correspond au choix du plongement de $4A_2$ correspondant aux 4 premières coordonnées (mais tous les choix de 4 coordonnées sont équivalents). Ce qui donne

```
> diviseur3(w);
```

$[[1, 1, 1, 1], [2, 1, 2, 1], [1, 2, 1, 2], [2, 2, 2, 2],$
 $[1, 1, 2, 2], [2, 2, 1, 1], [1, 2, 2, 1], [2, 1, 1, 2]].$

Index

- $D(L)$, 26
- $G_0(N)$, 54
- $G_1(N)$, 54
- $G_2(N)$, 54
- G_{01} , 54
- $H_a(\bar{b})$, 50
- L (un réseau), 17
- $L(-1)$ (un réseau), 17
- L_C , 33
- L_R , 22
- M_{24} , 37
- $O(D(L))$, 50
- $O(L)$, 43
- $O^+(L)$, 43
- $O_{\mathbb{R}}^+(L)$, 43
- R_L , 22
- $S(t, k, v)$, 38
- $SO^+(L)$, 43
- $SO_{\mathbb{R}}^+(L)$, 43
- S_n , 39
- S_{12}^+ , 39
- T_n , 39
- U , 17
- U_n , 39
- U_{12}^- , 39
- $[n, M, d]$ -code, 32
- $[n, k, d]$ -code, 32
- \mathbb{A}_n , 24
- \mathbb{D}_n , 24
- $\mathcal{D}(L)$, 41
- $\mathcal{D}^0(L)$, 41
- $\mathcal{D}^{\text{aff}}(L)$, 42
- \mathbb{E}_6 , 25
- \mathbb{E}_7 , 25
- \mathbb{E}_8 , 25
- \mathbb{H}_1 , 20
- $\Omega(L)$, 41
- $\Omega^+(L)$, 41
- $\Omega^-(L)$, 41
- Φ_{12} , 63
- λ , 21
- \mathcal{C}_6 , 35
- \mathcal{C}_{12} , 39
- \mathcal{C}_{24} , 36
- σ_r , 46
- $\tilde{O}(L)$, 46
- n -ade, 37
- Alphabet, 31
- Automorphismes du groupe discriminant, 50
- Base d'un réseau, 17
- Binaire (code), 31
- Bit de parité, 34
- Bloc, 37
- Code, 31
 - $[n, M, d]$ -code, 32
 - $[n, k, d]$ -code, 32
 - équivalents, 32
 - étendu, 34
 - alphabet, 31
 - associé à un sur-réseau, 30
 - auto-dual, 33
 - binaire, 31
 - bit de parité, 34
 - code de Golay binaire étendu, 36
 - code de Golay ternaire étendu, 39
 - code de Hamming étendu, 34
 - de Hamming, 34
 - distance de Hamming, 31
 - distance minimale, 31
 - doublement pair, 33
 - dual, 32
 - hexacode, 35
 - lettre, 31
 - linéaire, 32
 - matrice de contrôle, 32
 - matrice génératrice, 32

- mot, 31
 - réseau associé au, 33
 - ternaire, 31
- Code étendu, 34
- Code associé à un sur-réseau, 30
- Code auto-dual, 33
- Code de Golay binaire, 36
- Code de Golay binaire étendu, 36
- Code de Golay ternaire étendu, 39
- Code de Hamming, 34
- Code de Hamming étendu, 34
- Code doublement pair, 33
- Code dual, 32
- Composante additionnelle, 67
- Composante additionnelle de type 0 du diviseur de F_L , 68
- Composante additionnelle de type 1 du diviseur de F_L , 70
- Composante additionnelle réflexive, 67
- Composante orthogonale d'un réseau de racines, 26
- Couple hyperbolique, 18
- Critère d'Eichler, 49

- Déterminant d'un réseau, 18
- Diagramme de Coxeter-Dynkin, 22
- Dimension d'un réseau, 17
- Distance de Hamming, 31
- Distance minimale (d'un code), 31
- Diviseur d'un vecteur, 27
- Diviseur quadratique rationnel, 45
 - 2-diviseur quadratique rationnel, 67
 - réflexif, 67
- Dodécade, 37
- Dodécade ombrale, 37
- Domaine affine $\mathcal{D}^{\text{aff}}(L)$, 42
- Domaine homogène
 - $\mathcal{D}(L)$, 41
 - $\mathcal{D}^0(L)$, 41
 - $\Omega(L)$, 41
 - $\Omega^+(L)$, 41
 - $\Omega^-(L)$, 41
 - projectif, 41
- Dual (réseau), 18
- Duo, 37

- Equivalents (codes), 32

- Extraspéciale (dodécade), 39

- Facteurs invariants, 18
- Forme modulaire
 - ("au sens classique"), 21
 - anti-invariante, 11
 - invariante, 11
- Forme modulaire -2-réflexive, 73
- Forme modulaire pour un groupe orthogonal, 45
- Forme modulaire réflexive, 46
- Forme modulaire strictement -2-réflexive, 73
- Forme quadratique discriminante d'un réseau, 26

- Groupe affine, 34
- Groupe de Mathieu M_{24} , 37
- Groupe de Weyl d'un réseau de racines, 23
- Groupe discriminant d'un réseau, 26
- Groupe orthogonal
 - $O_{\mathbb{R}}^+(L)$, 43
 - $SO_{\mathbb{R}}^+(L)$, 43
- Groupe orthogonal d'un réseau
 - $O(L)$, 43
 - $O^+(L)$, 43
 - $SO^+(L)$, 43
 - $\tilde{O}(L)$, 46
 - groupe stable orthogonal, 46
- Groupe stable orthogonal, 46

- Hexacode, 35
- Hyperbolique
 - couple, 18
 - plan, 17

- Irréductible (réseau), 22

- Kissing number, 20

- Leech (réseau), 53
- Lettre, 31
- Linéaire (code), 32

- Matrice de contrôle d'un code, 32
- Matrice de Gram, 18
- Matrice génératrice d'un code, 32
- Mot, 31
 - poids, 31

- syndrome d'un, 32
- Niemeier (réseau), 53
- Niveau d'un réseau, 21
- Nombre de Coxeter, 23
- Norme spinorielle, 43
- Octade, 37
- Octade spéciale, 37
- Ombraal (n -ade), 39
- Orthogonal d'un réseau, 19
- Pénombrale (dodécade), 39
- Plan hyperbolique, 17
- Poids (d'un mot), 31
- Primitif (réseau), 19
- Primitif (vecteur), 27
- Quasi-restriction, 66
- Réductible (réseau), 22
- Réflexif (vecteur), 46
- Réflexion orthogonale, 46
- Réseau entier, 17
- Réseau maximal, 30
- Réseau pair, 17
- Racine, 22
- Racines
 - réseau de, 22
 - sous-réseau de, 22
 - système fondamental, 22
- Rang d'un réseau, 17
- Réseau, 17
 - U , 17
 - A_n , 24
 - D_n , 24
 - E_6 , 25
 - E_7 , 25
 - E_8 , 25
 - associé au code, 33
 - base, 17
 - code associé à un sur-réseau, 30
 - composante orthogonale d'un réseau de racines, 26
 - déterminant, 18
 - de Leech, 53
 - de Niemeier, 53
 - de racines, 22
- dimension, 17
 - dual, 18
 - entier, 17
 - forme quadratique discriminante, 26
 - irréductible, 22
 - maximal, 30
 - niveau, 21
 - orthogonal, 19
 - pair, 17
 - primitif, 19
 - quadratique, 17
 - réductible, 22
 - rang, 17
 - série thêta, 20
 - sous-réseau, 18
 - sous-réseau de racines, 22
 - sur-réseau, 30
 - unimodulaire, 19
- Série thêta d'un réseau, 20
- Sextet, 37
- Sous-groupe de congruence, 21
- Sous-groupe principal de congruence, 21
- Sous-réseau de racines, 22
- Sous-réseaux, 18
- Spécial (n -ade), 39
- Sur-réseau, 30
- Syndrome (d'un mot), 32
- Système de Steiner $S(t, k, v)$, 38
- Système fondamental de racines, 22
- Tétrades, 37
- Ternaire (code), 31
- Théorème de la base adaptée, 18
- Transvection orthogonale, 47
- Transverse (n -ade), 39
- Trio, 37
- Unimodulaire (réseau), 19
- Vecteur
 - diviseur d'un, 27
 - primitif, 27
 - réflexif, 46
 - racine, 22

Bibliographie

- [AI05] H. Aoki, T. Ibukiyama : *Simple graded rings of Siegel modular forms, differential operators and Borcherds products*. International J. Math. **16**, **3**, 249–279 (2005).
- [Ar62] E. Artin : *Algèbre Géométrique*. Editions Jacques Gabay (1962)
- [BKPS98] R.E. Borcherds, L. Katzarkov, T. Pantev, N.I. Shepherd-Barron : *Families of K3 surfaces*. J. Algebraic Geometry **7**, 183–193 (1998)
- [Bo92] R.E. Borcherds : *Monstrous moonshine and monstrous Lie algebras*. Invent. Math. **109**, 405–444 (1992)
- [Bo95] R.E. Borcherds : *Automorphic forms on $O_{s+2,2}(R)$ and infinite products*. Invent. Math. **120**, 161–213 (1995)
- [Bo98] R.E. Borcherds : *Automorphic forms with singularities on Grassmannians*. Invent. Math. **132**, 491–562 (1998)
- [Bo00] R.E. Borcherds : *Reflexion groups of Lorentzian lattices*. Duke Math. J. **104**, 319–366 (2000)
- [Br04] J.H. Bruinier : *Infinite products in number theory and geometry*. Jahresber. Dtsch. Math. Ver. **106**, 151–184 (2004)
- [CS98] J.H. Conway, N.J.A. Sloane : *Sphere Packings, Lattices and Groups (3rd ed.)*. Grundlehren der mathematischen Wissenschaften **290**, Springer-Verlag, New-York (1998)
- [D03] C. Desreumaux : *Formes de Jacobi relatives au réseau de racines A_2 et applications*. Thèse de l’Université de Lille 1, numéro d’ordre 3295 (2003)
- [D06] C. Desreumaux : *Construction de formes automorphes réflexives sur un espace de dimension 4*. Journal de théorie des Nombres de Bordeaux, **18**, 89–111 (2006)
- [DK03] T. Dern, A. Krieg : *Graded rings of Hermitian modular forms of degree 2*. Manuscripta math. **110**, 251–272 (2003)
- [Eb02] W. Ebeling : *Lattices and Codes*. Advanced Lectures in Mathematics, Vieweg, Braunschweig (2002)
- [Ei74] M. Eichler : *Quadratische Formen und orthogonale Gruppen*. Grundlehren der mathematischen Wissenschaften **63**. Springer-Verlag, BerlinNew York (1974)
- [FST92] G.D. Forney Jr., N.J.A. Sloane, M.D. Trott : *The Nordstrom-Robinson Code is the binary image of the Octacode*. Coding and Quantization, DIMACS/IEEE Workshop October 1992, AMS, 19–21 (1993)
- [GHS07] V. Gritsenko, K. Hulek, G. Sankaran : *The Kodaira dimension of the moduli of K3 surfaces*. Invent. Math. **169**, 519–567 (2007)

- [GHS08-1] V. Gritsenko, K. Hulek, G. Sankaran : *Moduli spaces of irreducible symplectic manifolds*. arXiv :0802.2078 (2008)
- [GHS08-2] V. Gritsenko, K. Hulek, G. Sankaran : *Abelianisation of orthogonal groups and the fundamental group of modular varieties*. arXiv :0810.1614 (2008)
- [GN96] V. Gritsenko, V.V. Nikulin : *The Igusa modular forms and “the simplest” Lorentzian Kac-Moody algebras*. *Matem. Sbornik*. **187**, 1601–1643 (1996)
- [GN98-1] V. Gritsenko, V.V. Nikulin : *Automorphic Forms and Lorentzian Kac-Moody Algebras. Part I*. *Int.J.of Math.*, Vol **9**, No 2, 153–199 (1998)
- [GN98-2] V. Gritsenko, V.V. Nikulin : *Automorphic Forms and Lorentzian Kac-Moody Algebras. Part II*. *Int.J.of Math.*, Vol **9**, No 2, 201–275 (1998)
- [GN00] V. Gritsenko, V.V. Nikulin : *Arithmetic Mirror Symmetry and Calabi-Yau manifolds*. *Commun. Math. Phys.* **210**, 1–11 (2000)
- [GN02] V. Gritsenko, V.V. Nikulin : *On classification of Lorentzian Kac-Moody algebras*. *Russ. Math. Surv.* **57**, 921–979 (2002)
- [Go05] R. Goblot : *Algèbre linéaire*. Ellipses (2005)
- [Gr88] V. Gritsenko : *Fonctions de Jacobi de n variables (en russe)*. *Zap. Nauchn. Sem. LOMI* **168** 32-45 (1988). Traduction angl. : *J. Soviet Math.* **53**, 243–252 (1991)
- [Gr94] V. Gritsenko : *Modular forms and moduli spaces of abelian and K3 surfaces*. *Algebra i Analiz* **6 :6**, 65–102 (1994); English transl. in *St. Petersburg Math. J.* **6 :6**, 1179–1208 (1995)
- [HKCSS94] A.R. Hammons Jr., P.V. Kumar, A.R. Calderbank, N.J.A Sloane, P. Solé : *The \mathbb{Z}_4 -linearity of Kerdock, Preparata, Goethals and Related Codes*. *IEEE Trans. Information Theory*, **40**, 301–319 (1994)
- [I64] J. Igusa : *On Siegel modular forms of genus two (II)*. *Amer. J. Math.* **84** 392–412 (1964)
- [Kl05] I.H. Klöcker : *Modular forms for the orthogonal group $O(2, 5)$* . Thèse de l’Université d’Aachen (2005)
- [Kn02] M. Kneser : *Quadratische Formen*. Neu bearbeitet und herausgegeben in Zusammenarbeit mit Rudolf Schalau. Springer (2002). [Zbl 1001.11014]
- [Ko99] S. Kondo : *On the Kodaira Dimension of the Moduli Space of K3 Surfaces II*. *Composito Mathematica* **116**, 111–117 (1999)
- [Kr05] A. Krieg : *The graded ring of quaternionic modular forms of degree 2*. *Math. Z.* **251**, 929–942 (2005)
- [N79] V.V. Nikulin : *Integral symmetric bilinear forms and some of their applications*. *Math. USSR Izv.* **14**, 103–167 (1979)
- [S06] N.R. Scheithauer : *On the classification of automorphic products and generalized Kac-Moody algebras*. *Invent. Math.* **164**, 641–678 (2006)