THÉORIE DES NOMBRES
BESANÇON

Années 1994/95-1995/96

Un lien entre les $\mathbb{Z}$-réseaux unimodulaires et les formes hermitiennes : les F-réseaux

M. MISCHLER

Abstract

Let $F = \Phi_{n_1}^{r_1} \cdots \Phi_{n_s}^{r_s}$ be a product of cyclotomic polynomials. A unimodular $\mathbb{Z}$-lattices is said to be an *F-lattice* if it has an isometry with characteristic polynomial F. We denote then by $\overline{\mathscr{E}}(F)$ the set of *F-lattice* up to $\mathbb{Z}-$isometry.

The first chapter gives a formula that allows to make an estimate of the mass of $\overline{\mathscr{E}}(F)$, which is by definition the sum

$$\Omega(F) = \sum_{M \in \overline{\mathscr{E}}(F)} \frac{1}{|O(M)|},$$

where $O(M)$ is the orthogonal group of the $\mathbb{Z}$-lattice M. To each F-lattice, we associate hermitians forms, and we prove that the mass of $\overline{\mathscr{E}}(F)$ is smaller than a sum including the mass of genus of these hermitian forms (cf. theorems 1.6.6, 1.6.8 and 1.6.9). In addition, the first chapter contains a deep study of hermitian genus (cf. §5).

The second chapter provides the mass formula for hermitian genus of forms over $\mathbb{Z}[\zeta_n]$ (ζ_n is a nth primitive root of unity). This chapter also contains theorems allowing to compute easily local densities, and hence the mass formula.

In the third chapter we are interested in $\mathbb{Z}$-lattices having a so called *perfect* isometry. An isometry t of a $\mathbb{Z}$-lattice (M, β) is *perfect* if $1 - t$ is invertible. In this case, (M, β) is of type II, i.e., $\beta(x, x)$ is even for all $x \in M$. We show the following result : (M, β) is a unimodular $\mathbb{Z}$-lattice of rank 32 having a perfect isometry if and only if (M, β) is an F-lattice, where F belongs to the following list :

Φ_6^{16} Φ_{10}^8 Φ_{34}^2

$\Phi_6\Phi_{18}^5$ $\Phi_6^4\Phi_{18}^4$ $\Phi_6^6\Phi_{66}$ $\Phi_6^7\Phi_{18}^3$ $\Phi_6^7\Phi_{54}$ $\Phi_6^{10}\Phi_{18}^2$ $\Phi_6^{13}\Phi_{18}$ $\Phi_{10}^3\Phi_{50}$

$\Phi_6\Phi_{18}^2\Phi_{54}$ $\Phi_6^3\Phi_{18}^2\Phi_{66}$ $\Phi_6^4\Phi_{10}^2\Phi_{30}^2$ $\Phi_6^4\Phi_{10}^4\Phi_{30}$ $\Phi_6^4\Phi_{14}^2\Phi_{42}$ $\Phi_6^4\Phi_{18}\Phi_{54}$ $\Phi_6^8\Phi_{10}^2\Phi_{30}$

$\Phi_6\Phi_{10}^2\Phi_{18}\Phi_{30}^2$ $\Phi_6\Phi_{10}^4\Phi_{18}\Phi_{30}$ $\Phi_6\Phi_{14}^2\Phi_{18}\Phi_{42}$ $\Phi_6^2\Phi_{10}^2\Phi_{18}^2\Phi_{30}$ $\Phi_6^5\Phi_{10}^2\Phi_{18}\Phi_{30}$ (cf. theorem 3.2.3).

The fourth chapter yields estimates of the mass of $\overline{\mathscr{E}}(F)$, for F in the previous list using the techniques given in chapter 1 and 2. However, for the sake of calculation, we have to restrict ourselves to polynomials with one or two irreducible factors. We obtain the following upperbounds :

$\Omega(\Phi_6^{16}) \leq 0,0029$	$\Omega(\Phi_{10}^8) \leq 0,006$	$\Omega(\Phi_{34}^2) \leq 4,3355$	
$\Omega(\Phi_6\Phi_{18}^5) \leq 0,1717$	$\Omega(\Phi_6^4\Phi_{18}^4) \leq 0,4238$	$\Omega(\Phi_6^7\Phi_{18}^3) \leq 0,151$	$\Omega(\Phi_6^{10}\Phi_{18}^2) \leq 5,39 \cdot 10^{-5}$
$\Omega(\Phi_6^{13}\Phi_{18}) \leq 2,24 \cdot 10^{-8}$	$\Omega(\Phi_6^7\Phi_{54}) \leq 2,61 \cdot 10^{-10}$	$\Omega(\Phi_6^6\Phi_{66}) \leq 2,23 \cdot 10^{-5}$	$\Omega(\Phi_{10}^3\Phi_{50}) \leq 2,73 \cdot 10^{-3}$.

To make a comparison, the mass of unimodular $\mathbb{Z}$-lattices of type II is approximately $4,031 \cdot 10^7$.

Résumé

Soit $F = \Phi_{n_1}^{r_1} \cdots \Phi_{n_s}^{r_s}$ un produit de polynômes cyclotomiques. Notons $\overline{\mathscr{E}}(F)$ l'ensemble, à $\mathbb{Z}-$isométries près, des $\mathbb{Z}$-réseaux unimodulaires possédant une isométrie de polynôme caractéristique F. Ces réseaux sont appelés *F-réseaux.*

Le premier chapitre donne une formule permettant d'estimer la masse de $\overline{\mathscr{E}}(F)$, c'est-à-dire la somme

$$\Omega(F) := \sum_{M \in \overline{\mathscr{E}}(F)} \frac{1}{|O(M)|},$$

où $O(M)$ est le groupe orthogonal du $\mathbb{Z}$-réseau M. A tout F-réseau, nous associons des formes hermitiennes, et nous montrons que la masse de $\overline{\mathscr{E}}(F)$ est inférieure à une somme faisant intervenir la masse des genres des formes hermitiennes associées. Il s'agit des théorèmes 1.6.6, 1.6.8 et 1.6.9. Le premier chapitre contient aussi une étude approfondie des genres hermitiens (le §5).

Le deuxième chapitre donne la formule de masse pour les genres de formes hermitiennes à valeur dans $\mathbb{Z}[\zeta_n]$ (ζ_n étant une racine primitive n-ième de l'unité). Ce chapitre comprend aussi des théorèmes permettant de calculer aisément diverses densités locales, et ainsi, la formule de masse elle-même.

Au troisième chapitre, nous nous intéressons aux $\mathbb{Z}$-réseaux possédant des isométries dites parfaites. Une isométries t d'un $\mathbb{Z}$-réseau (M, β) est *parfaite* si $1-t$ est inversible. Dans ce cas, (M, β) est de type II, c'est-à-dire $\beta(x,x)$ est pair pour tout $x \in M$. Nous montrons que (M, β) est un $\mathbb{Z}$-réseaux unimodulaire de rang 32 possédant une isométrie parfaite si et seulement si (M, β) est un F-réseau, où F est un des polynômes suivant :

Φ_6^{16} Φ_{10}^8 Φ_{34}^2

$\Phi_6\Phi_{18}^5$ $\Phi_6^4\Phi_{18}^4$ $\Phi_6^6\Phi_{66}$ $\Phi_6^7\Phi_{18}^3$ $\Phi_6^7\Phi_{54}$ $\Phi_6^{10}\Phi_{18}^2$ $\Phi_6^{13}\Phi_{18}$ $\Phi_{10}^3\Phi_{50}$

$\Phi_6\Phi_{18}^2\Phi_{54}$ $\Phi_6^3\Phi_{18}^2\Phi_{66}$ $\Phi_6^4\Phi_{10}^2\Phi_{30}^2$ $\Phi_6^4\Phi_{10}^4\Phi_{30}$ $\Phi_6^4\Phi_{14}^2\Phi_{42}$ $\Phi_6^4\Phi_{18}\Phi_{54}$ $\Phi_6^8\Phi_{10}^2\Phi_{30}$

$\Phi_6\Phi_{10}^2\Phi_{18}\Phi_{30}^2$ $\Phi_6\Phi_{10}^4\Phi_{18}\Phi_{30}$ $\Phi_6\Phi_{14}^2\Phi_{18}\Phi_{42}$ $\Phi_6^2\Phi_{10}^2\Phi_{18}^2\Phi_{30}$ $\Phi_6^5\Phi_{10}^2\Phi_{18}\Phi_{30}$ (cf. théorème 3.2.3).

Au quatrième chapitre, nous donnons des estimations de la masse de $\overline{\mathscr{E}}(F)$, où F fait partie de la liste ci-dessus, utilisant les techniques données aux chapitres 1 et 2. Nous devons néanmoins, pour des raisons calculatoires, nous restreindre aux polynômes possédant un ou deux facteurs irréductibles distincts. Nous obtenons les résultats suivants :

$\Omega(\Phi_6^{16}) \leq 0,0029$ $\Omega(\Phi_{10}^8) \leq 0,006$ $\Omega(\Phi_{34}^2) \leq 4,3355$

$\Omega(\Phi_6\Phi_{18}^5) \leq 0,1717$ $\Omega(\Phi_6^4\Phi_{18}^4) \leq 0,4238$ $\Omega(\Phi_6^7\Phi_{18}^3) \leq 0,151$ $\Omega(\Phi_6^{10}\Phi_{18}^2) \leq 5,39 \cdot 10^{-5}$

$\Omega(\Phi_6^{13}\Phi_{18}) \leq 2,24 \cdot 10^{-8}$ $\Omega(\Phi_6^7\Phi_{54}) \leq 2,61 \cdot 10^{-10}$ $\Omega(\Phi_6^6\Phi_{66}) \leq 2,23 \cdot 10^{-5}$ $\Omega(\Phi_{10}^3\Phi_{50}) \leq 2,73 \cdot 10^{-3}$.

Pour avoir un ordre de grandeur, il faut savoir que la masse des réseaux unimodulaires de type II vaut environ $4,031 \cdot 10^7$.

Introduction

Les formes bilinéaires entières ont une longue histoire. Cette histoire est intimement liée à celle de la théorie des nombres elle-même. Les travaux de Legendre, Hermite, Gauss, Minkowski, Hasse et Siegel, pour ne citer que les plus illustres, ont grandement contribué à notre connaissance dans ce domaine. Il existe une classification des formes bilinéaires entières, unimodulaires et indéfinies. En revanche, il n'existe rien de tel pour les formes définies. Ces formes sont néanmoins très étudiées et, par petites touches, notre savoir augmente régulièrement sur le sujet.

Dans la théorie de nombres, les énoncés des problèmes sont souvent très simples, et paraissent "naturels", mais il est étonnant de constater que la résolution de ces problèmes est en revanche très ardue, et demande la maîtrise d'objets très "exotiques" et abstraits, qui semblent se situer à des années lumières du problème initial. La question qui nous intéresse n'échappe pas à cette règle :

Soit $F \in \mathbb{Z}[X]$ un polynôme entier de degré n. Combien existe-t-il, à $\mathbb{Z}$-isométries près, de $\mathbb{Z}$-modules libres de rang n munis d'une forme bilinéaire entière, unimodulaire et définie positive (M, β) possédant une isométrie de polynôme caractéristique F ?

Un $\mathbb{Z}$-module libre de rang n muni d'une forme bilinéaire entière, définie positive se nomme *$\mathbb{Z}$-réseau de rang n*. S'il possède une isométrie de polynôme caractéristique F, on l'appelle *F-réseau*. L'ensemble, à $\mathbb{Z}$-isométries près, des F-réseaux unimodulaires se note $\overline{\mathscr{E}}(F)$. Il est à peu près évident de montrer que si $\overline{\mathscr{E}}(F) \neq \emptyset$, alors F est un produit de polynômes cyclotomiques $\Phi_{n_1}^{r_1} \cdots \Phi_{n_s}^{r_s}$. Eva Bayer-Fluckiger, dans [Bay], donne une condition nécessaire et suffisante pour que $\overline{\mathscr{E}}(F) \neq \emptyset$. Connaître le nombre de F-réseaux n'est pour l'instant pas envisageable à court terme au vu des connaissances mathématiques actuelles. Ce problème est aussi difficile que de calculer le cardinal des classes d'isométries de $\mathbb{Z}$-réseaux unimodulaires de dimension donnée.

Considérons la somme suivante :

$$\Omega(F) := \sum_{M \in \overline{\mathscr{E}}(F)} \frac{1}{|O(M)|},$$

où $O(M)$ est le groupe orthogonal du $\mathbb{Z}$-réseau M. On l'appelle la masse de $\overline{\mathscr{E}}(F)$. Nous allons poser une nouvelle question :

Soit $F \in \mathbb{Z}[X]$ un polynôme entier. Est-il possible de calculer, ou au moins d'estimer la masse de $\overline{\mathscr{E}}(F)$?

Ce problème peut paraître encore plus difficile à résoudre que le premier. Or, il n'en est rien, et nous allons dans ce travail donner une borne supérieure à la masse de $\overline{\mathscr{E}}(F)$. Une borne évidente est fournie par le raisonnement suivant : $\overline{\mathscr{E}}(F)$ est inclus dans $\mathscr{S}_n$, l'ensemble à $\mathbb{Z}$-isométrie près des $\mathbb{Z}$-réseaux unimodulaires de rang n, où n est le degré de F. Or la masse de $\mathscr{S}_n$ est connue (cf. [Mis]), et ainsi, la masse de $\overline{\mathscr{E}}(F)$ est inférieure ou égale à celle de $\mathscr{S}_n$. Dans les "petites" dimensions, c'est-à-dire jusqu'à environ $n = 30$, cette borne est concurrentielle avec celle que nous présentons ici. En revanche, nous verrons qu'elle donne des résultats intéressants en dimension 32.

Les méthodes que nous utilisons sont largement inspirées par celle de la thèse de E. Bannaï [Ban], pour l'établissement de la formule. Nous obtenons toutefois des résultats plus généraux.

Nous mentionnons dans le titre de ce travail la notion de forme hermitienne. Voici comment nous construisons, à partir d'un F-réseau, des formes hermitiennes : soient $F = \Phi_{n_1}^{r_1} \cdots \Phi_{n_s}^{r_s}$, (M, β) un F-réseau et t une isométrie de (M, β) de polynôme caractéristique F. Un raisonnement simple nous montrera que le polynôme minimal de t est $f = \Phi_{n_1} \cdots \Phi_{n_s}$. Posons $W = M \otimes \mathbb{Q}$ sur lequel β et t se prolongent naturellement. Posons encore, pour $i = 1, \ldots, s$, $W_i = \frac{f}{\Phi_{n_i}}(t)(W)$, $t_i = t|_{W_i}$, $\beta_i = \beta|_{W_i}$, et $M_i = M \cap W_i$.

Il est clair que $t_i(M_i) = M_i$, et que le polynôme minimal de t_i est Φ_{n_i}. Ainsi, M_i peut être muni d'une structure de $\mathbb{Z}[\zeta_{n_i}]$-module (ζ_{n_i} étant une racine primitive n_i-ième de l'unité) sur lequel nous définissons la forme hermitienne

$$\begin{aligned} h_i \ : \ M_i \times M_i &\longrightarrow \mathbb{Z}[\zeta_{n_i}] \\ (x \ , \ y) &\longmapsto \sum_{j=0}^{n_i-1} \beta_i(t_i^{-j}(x), y)\zeta_{n_i}^j. \end{aligned}$$

Nous montrons, à la fin du premier chapitre, que la masse de $\overline{\mathscr{E}}(F)$ est inférieure à une somme faisant intervenir la masse des genres des formes (M_i, h_i) (cf. théorèmes 1.6.6, 1.6.8 et 1.6.9). Une fois que cette borne est théoriquement établie, nous allons donner des exemples "concrets". Pour pouvoir calculer ces exemples, nous serons obligés de faire une étude approfondie des genres de formes hermitiennes. Nous donnons ainsi un théorème qui fournit un système d'invariants presque complet pour les genres de formes hermitiennes (cf. théorème 1.5.5). En plus de cela, nous avons besoin de calculer la masse de divers genres de formes hermitiennes connaissant le système d'invariants du théorème 1.5.5. Le chapitre 2, et plus particulièrement les théorèmes 2.2.5, 2.2.6 et 2.3.1 nous permettent d'atteindre cet objectif.

Le troisième chapitre est un peu à part : nous nous intéressons à des $\mathbb{Z}$-réseaux possédant des isométries particulières dites *parfaites*. Une isométrie t est dite *parfaite* si $1 - t$ est inversible. Si (M, β) possède une telle isométrie, alors il est de type II, c'est-à-dire que $\beta(x, x)$ est pair pour tout $x \in M$. Le résultat principal de ce chapitre est le suivant : (M, β) est un $\mathbb{Z}$-réseau unimodulaire de dimension 32 possédant une isométrie parfaite si et seulement si (M, β) est un F-réseau, où F est un des polynômes suivants :

Φ_6^{16} Φ_{10}^8 Φ_{34}^2

$\Phi_6\Phi_{18}^5$ $\Phi_6^4\Phi_{18}^4$ $\Phi_6^6\Phi_{66}$ $\Phi_6^7\Phi_{18}^3$ $\Phi_6^7\Phi_{54}$ $\Phi_6^{10}\Phi_{18}^2$ $\Phi_6^{13}\Phi_{18}$ $\Phi_{10}^3\Phi_{50}$

$\Phi_6\Phi_{18}^2\Phi_{54}$ $\Phi_6^3\Phi_{18}^2\Phi_{66}$ $\Phi_6^4\Phi_{10}^2\Phi_{30}^2$ $\Phi_6^4\Phi_{10}^4\Phi_{30}$ $\Phi_6^4\Phi_{14}^2\Phi_{42}$ $\Phi_6^4\Phi_{18}\Phi_{54}$ $\Phi_6^8\Phi_{10}^2\Phi_{30}$

$\Phi_6\Phi_{10}^2\Phi_{18}\Phi_{30}^2$ $\Phi_6\Phi_{10}^4\Phi_{18}\Phi_{30}$ $\Phi_6\Phi_{14}^2\Phi_{18}\Phi_{42}$ $\Phi_6^2\Phi_{10}^2\Phi_{18}^2\Phi_{30}$ $\Phi_6^5\Phi_{10}^2\Phi_{18}\Phi_{30}$ (cf. théorème 3.2.3).

Cela nous offre la possibilité d'essayer notre théorie sur des polynômes intéressants. Ainsi, au quatrième chapitre, nous donnons des estimations de la masse de $\overline{\mathscr{E}}(F)$, où F fait partie de la liste ci-dessus, utilisant les techniques données aux chapitres 1 et 2. Nous devons néanmoins, pour des raisons calculatoires, nous restreindre aux polynômes possédant un ou deux facteurs irréductibles. Nous obtenons les résultats suivants :

$\Omega(\Phi_6^{16}) \leq 0,0029$ $\Omega(\Phi_{10}^8) \leq 0,006$ $\Omega(\Phi_{34}^2) \leq 4,3355$

$\Omega(\Phi_6\Phi_{18}^5) \leq 0,1717$ $\Omega(\Phi_6^4\Phi_{18}^4) \leq 0,4238$ $\Omega(\Phi_6^7\Phi_{18}^3) \leq 0,151$ $\Omega(\Phi_6^{10}\Phi_{18}^2) \leq 5,39 \cdot 10^{-5}$

$\Omega(\Phi_6^{13}\Phi_{18}) \leq 2,24 \cdot 10^{-8}$ $\Omega(\Phi_6^7\Phi_{54}) \leq 2,61 \cdot 10^{-10}$ $\Omega(\Phi_6^6\Phi_{66}) \leq 2,23 \cdot 10^{-5}$ $\Omega(\Phi_{10}^3\Phi_{50}) \leq 2,73 \cdot 10^{-3}$.

Ces estimations sont meilleures que la borne évidente qui est la masse des $\mathbb{Z}$-réseaux de type II. Cette masse vaut environ $4,031 \cdot 10^7$.

Table des matières

CHAPITRE 1

Estimation de la masse des F-réseaux

§ 1. Quelques rappels et énoncé du problème

Soit (M,β) un $\mathbb{Z}$-module libre de rang fini, muni d'une forme bilinéaire entière et définie positive (c'est-à-dire $\beta(x,x)$ est strictement positif pour tout x non nul dans M). Nous noterons $\det(M,\beta)$ ou $\det(M)$ le déterminant de la matrice de β relativement à une base de M. Dans notre cas, $\det(M)$ est strictement positif. Nous dirons que M est *unimodulaire* si $\det(M)=1$.

L'ensemble des isomorphismes $u : M \longrightarrow M$ tels que $\beta(u(x),u(y))=\beta(x,y)$ pour tout x,y dans M, muni de la composition des applications, est appelé *groupe orthogonal de* (M,β). Nous noterons $O(M,\beta)$ ou $O(M)$ ce groupe. Chaque élément de $O(M)$ est appelé *isométrie de* (M,β). Puisque (M,β) est défini positif, $O(M)$ est fini. Une démonstration de ce résultat est donnée par exemple dans ([Mis], Lemme 2.33). Il existe donc, pour toute isométrie t, un entier m positif, tel que $t^m = Id_M$. Le polynôme minimal de t est donc un diviseur de X^m-1. Nous avons la formule suivante :

$$X^m - 1 = \prod_{d|m} \Phi_d$$

où Φ_d est le d-ième polynôme cyclotomique. Ce résultat est démontré dans ([Lang],VIII,§3). Ainsi, le polynôme minimal de t est un produit de polynômes cyclotomiques sans facteurs carrés, et son polynôme caractéristique est un produit de puissances de polynômes cyclotomiques.

Soit A un anneau commutatif. Les A-modules munis de formes bilinéaires (M',β') et (M'',β'') sont dits *A-équivalents*, et nous écrirons $(M',\beta') \overset{A}{\simeq} (M'',\beta'')$, s'il existe $u : M' \longrightarrow M''$ telle que $\beta''(u(x),u(y))=\beta'(x,y)$, pour tout x,y dans M'.

Soient $\mathbb{P}=(\mathbb{P}(\mathbb{Z}))$ l'ensemble de tous les nombres premiers positifs, et $\mathbb{P}'=\mathbb{P}\cup\{\infty\}$. Si $p\in\mathbb{P}'$, on note $\mathbb{Z}_p$ l'anneau des entiers p-adiques usuels, avec la convention que $\mathbb{Z}_\infty=\mathbb{R}$, et on note $\mathbb{Q}_p$ le corps des nombres p-adiques, aussi avec la convention que $\mathbb{Q}_\infty=\mathbb{R}$. Les $\mathbb{Z}$-modules bilinéaires (M',β') et (M'',β'') sont dits *dans le même genre*, si pour tout $p\in\mathbb{P}'$, on a $(M'\otimes\mathbb{Z}_p,\beta'\otimes\mathbb{Z}_p) \overset{\mathbb{Z}_p}{\simeq} (M''\otimes\mathbb{Z}_p,\beta''\otimes\mathbb{Z}_p)$. Si deux modules sont $\mathbb{Z}$-équivalents, ils sont dans le même genre. Il est bien connu que les $\mathbb{Z}$-modules unimodulaires et définis positifs forment exactement deux genres. Le premier genre est composé des formes *paires* ou *de type II*, c'est-à-dire possédant la propriété que $\beta(x,x)$ est pair pour tout x. Le second est formé de toutes les autres formes qu'on appelle *impaires* ou *de type I*. La dimension d'un $\mathbb{Z}$-module pair, unimodulaire et défini positif est forcément un multiple de 8 (cf. [Se], p. 92).

Définitions 1.1.1

Fixons $p\in\mathbb{P}'$.

a) Pour tout a et $b\in\mathbb{Q}_p^*:=\mathbb{Q}_p-\{0\}$, on pose :

$$(a,b)_p = \begin{cases} 1 & \text{si } ax^2+by^2=z^2 \text{ possède une solution non triviale dans } \mathbb{Q}_p \\ -1 & \text{sinon.} \end{cases}$$

Ce nombre s'appelle le *symbole de Hilbert de a et b*.

b) Soit (M,β) un $\mathbb{Z}_p$-module de rang fini muni d'une forme bilinéaire. Supposons que relativement à une base, la matrice de β soit $(b_1)\oplus\cdots\oplus(b_n)$. Le produit

$$c_p(\beta)=\prod_{i<j}(b_i,b_j)_p$$

est indépendant de la base choisie et on l'appelle *l'invariant de Hasse de β*.

Voici deux théorèmes classiques :

Théorème 1.1.2

Soient $a, b \in \mathbb{Q}^*$. Alors $(a,b)_p = 1$ sauf pour un sous-ensemble fini de $\mathbb{P}'$ et

$$\prod_{p \in \mathbb{P}'} (a,b)_p = 1.$$

Ce théorème est connu sous le nom de "formule du produit de Hilbert"

Démonstration :

Voir ([Se], Théorème 3, p. 44). ❄

Théorème 1.1.3

Soient (V,β) et (V',β') deux $\mathbb{Q}$-espaces bilinéaires de dimension finie. Alors :

$$(V,\beta) \overset{\mathbb{Q}}{\simeq} (V',\beta') \quad \text{si et seulement si} \quad (V \otimes \mathbb{Q}_p, \beta \otimes \mathbb{Q}_p) \overset{\mathbb{Q}_p}{\simeq} (V' \otimes \mathbb{Q}_p, \beta' \otimes \mathbb{Q}_p) \quad \forall p \in \mathbb{P}'.$$

On appelle ce résultat "théorème de Hasse-Minkowski"

Démonstration :

Voir ([Se], Théorème 9, p. 77). ❄

Définition 1.1.4

Soient A un anneau de Dedekind, K son corps des fractions, et V un K-espace vectoriel de dimension n. Tout sous-A-module de V contenant une K-base de V, et contenu dans un A-module libre de rang n est appelé *A-réseau de V*.

Le résultat suivant montre que tout $\mathbb{Z}$-module libre de rang n muni d'une forme bilinéaire unimodulaire peut être vu comme un $\mathbb{Z}$-réseau de $\mathbb{Q}^n$ muni du produit scalaire usuel. De tels réseaux seront appelés *$\mathbb{Z}$-réseaux unimodulaires*. En outre, nous écrirons "*$\mathbb{Z}$-réseau*", pour "$\mathbb{Z}$-réseau de $\mathbb{Q}^n$ muni du produit scalaire usuel".

Théorème 1.1.5

Soit B une matrice symétrique définie positive de $Gl_n(\mathbb{Z})$. Alors il existe une matrice $N \in Gl_n(\mathbb{Q})$ telle que

$$NN^t = B$$

Démonstration :

Le procédé d'orthogonalisation de Gram-Schmitt montre qu'on peut supposer B diagonale. Soient $b_1, \ldots, b_n$ les coefficients de cette diagonale. On montre facilement que $B \overset{\mathbb{Q}_p}{\simeq} I_n$ pour $p \neq 2$, où I_n est la matrice unité. Une démonstration se trouve dans ([Mis], Corollaire 1.42).

Soit β la forme définie par B. L'invariant de Hasse $c_p(\beta \otimes \mathbb{Z}_p)$ possède la propriété suivante en vertu de la formule du produit de Hilbert :

$$\prod_{p \in \mathbb{P}'} c_p(\beta \otimes \mathbb{Z}_p) = 1.$$

Puisque $c_p(\beta \otimes \mathbb{Z}_p) = 1$ pour tout $p \neq 2$, on en déduit que $c_2(\beta \otimes \mathbb{Z}_2) = 1$, donc $B \overset{\mathbb{Q}_2}{\simeq} I_n$. Le théorème de Hasse-Minkowski nous permet de conclure. ❄

Soit F un produit de puissances de polynômes cyclotomiques de degré n. Notons $\mathscr{E}(F)$, l'ensemble des $\mathbb{Z}$-réseaux unimodulaires indécomposables de $\mathbb{Q}^n$ possédant au moins une isométrie (que nous noterons toujours t) de polynôme caractéristique F. Ces réseaux sont appelés *F-réseaux*. L'ensemble des classes d'isométries de F-réseaux se note $\overline{\mathscr{E}}(F)$. Son cardinal est fini, car l'ensemble des classes d'isométries de $\mathbb{Z}$-réseaux unimodulaires de dimension donnée est fini.

Définition 1.1.6

Fixons $\mathscr{G}$, un genre de réseaux unimodulaires de $\mathbb{Q}^n$, à $\mathbb{Z}$-isométrie près. La somme suivante :

$$\sum_{\overline{M}\in\mathscr{G}} \frac{1}{|O(M)|}$$

où M est n'importe quel représentant de la classe $\overline{M}$ est appelée *masse* de $\mathscr{G}$.

Remarque :

Il est possible de calculer explicitement cette somme grâce à la *formule de Siegel* (cf. [Mis]).

Le but de ce premier chapitre est d'estimer la somme suivante :

$$\sum_{\overline{M}\in\overline{\mathscr{E}}(F)} \frac{1}{|O(M)|}.$$

Nous appellerons cette somme *masse de* $\overline{\mathscr{E}}(F)$.

Nous allons procéder de la manière suivante :

supposons que $F = \Phi_{n_1}^{r_1}\cdots\Phi_{n_s}^{r_s}$. A tout F-réseau, il sera possible de trouver un sous-réseau qui pourra s'écrire comme somme orthogonale de $\Phi_{n_i}^{r_i}$-réseaux M_i. Nous verrons que chaque M_i peut être muni d'une structure de $\mathbb{Z}[\zeta_{n_i}]$-module (ζ_{n_i} étant une racine n_i-ième de l'unité). Nous munirons M_i d'une forme hermitienne h_i, puis nous comparerons la masse de $\overline{\mathscr{E}}(F)$ avec les différentes masses des genres hermitiens des (M_i, h_i).

§ 2. Espaces vectoriels hermitiens associés à un espace vectoriel bilinéaire muni d'une isométrie

Avant d'entrer dans le vif du sujet, nous avons besoin de quelques résultats sur les racines de l'unité.

Définitions 1.2.1

a) L'application

$$\mu : \mathbb{N} \longrightarrow \{-1,0,1\}$$
$$n \longmapsto \begin{cases} 0 & \text{si } n \text{ possède au moins un facteur carré} \\ 1 & \text{si } n = 1 \\ (-1)^s & \text{si } n = p_1\cdots p_s \text{ avec } p_i \in \mathbb{P} \text{ pour tout } i, \text{ et } p_i \neq p_j \text{ si } i \neq j. \end{cases}$$

est appelée *fonction de Möbius.* C'est une *fonction arithmétique multiplicative*, c'est-à-dire $\mu(mn) = \mu(m)\mu(n)$ si m et n sont premiers entre eux. Donc, μ est la seule fonction arithmétique multiplicative telle que $\mu(p^k) = \begin{cases} -1 & \text{si k=1} \\ 0 & \text{si } k > 1 \end{cases}$ pour tout $p \in \mathbb{P}$.

b) La *fonction φ d'Euler* est aussi une fonction arithmétique multiplicative, avec $\varphi(p^k) = p^{k-1}(p-1)$, si k est un entier positif quelconque, et $p \in \mathbb{P}$. Il est bien connu que $\varphi(d)$ est le degré du polynôme Φ_d.

Lemme 1.2.2

a) Soient m et n des entiers positifs premiers entre eux. Le polynôme Φ_m divise $\Phi_m(X^n)$.

b) Pour tout entier m, notons Tr_m la trace de l'extension $\mathbb{Q}(\zeta_m)$ sur $\mathbb{Q}$, où ζ_m est une racine primitive m-ième de l'unité. On a :

$$\sum_{i=0}^{m-1} \mathrm{Tr}_m(\zeta_m^i)\zeta_m^i = m.$$

Démonstration :

a) Puisque m et n sont premiers entre eux, ζ_m^n est aussi une racine primitive m-ième de l'unité. Donc $\Phi(\zeta_m^n) = 0$, d'où Φ_m divise $\Phi_m(X^n)$.

b) Montrons tout d'abord le résultat suivant : soit d un entier. Alors $\mathrm{Tr}_d(\zeta_d) = \mu(d)$.
Si $p \in \mathbb{P}$, on a :

$$\Phi_{p^k} = X^{p^{k-1}(p-1)} + X^{p^{k-1}(p-2)} + \cdots + X^{p^{k-1}} + 1 \quad \text{pour tout entier positif } k.$$

Ce résultat est montré dans ([Lang],VIII,§3). D'autre part, il est facile de voir que $\mathrm{Tr}_d(\zeta_d)$ est le coefficient de $X^{\varphi(d)-1}$ dans $-\Phi_d$. On a donc $\mathrm{Tr}_{p^k}(\zeta_{p^k}) = \mu(p^k)$ pour tout p et k. De plus, l'application $d \longmapsto \mathrm{Tr}_d(\zeta_d)$ est multiplicative. En effet, si d et d' sont premiers entre eux, on a $\mathbb{Q}(\zeta_{dd'}) = \mathbb{Q}(\zeta_d) \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_{d'})$. Ce résultat est montré dans ([Fr-Ta],Chap VI, Result 1.14). Donc $\mathrm{Tr}_{dd'}(\zeta_d\zeta_{d'}) = \mathrm{Tr}_d(\zeta_d)\,\mathrm{Tr}_{d'}(\zeta_{d'})$.
Calculons :

$$\begin{aligned}
\sum_{i=0}^{m-1} \mathrm{Tr}_m(\zeta_m^i)\zeta_m^i &= \sum_{d|m} \sum_{\substack{\zeta_d \text{ racine primitive} \\ d-\text{ième de l'unité}}} \mathrm{Tr}_m(\zeta_d)\zeta_d \\
&= \sum_{d|m} \mathrm{Tr}_m(\zeta_d) \sum_{\substack{\zeta_d \text{ racine primitive} \\ d-\text{ième de l'unité}}} \zeta_d \\
&= \sum_{d|m} \mathrm{Tr}_m(\zeta_d)\,\mathrm{Tr}_d(\zeta_d) \\
&= \sum_{d|m} \frac{\varphi(m)}{\varphi(d)} \mathrm{Tr}_d(\zeta_d)^2.
\end{aligned}$$

Or, nous savons que $\mathrm{Tr}_d(\zeta_d) = \mu(d)$. Donc $\sum_{i=0}^{m-1} \mathrm{Tr}_m(\zeta_m^i)\zeta_m^i = \varphi(m)\sum_{d|m} \frac{\mu(d)^2}{\varphi(d)}$. Posons $\mathbb{N}_r = \{1,\ldots,r\}$ et supposons que $m = p_1^{k_1}\cdots p_r^{k_r}$. Poursuivons nos calculs :

$$\begin{aligned}
\varphi(m)\sum_{d|m} \frac{\mu(d)^2}{\varphi(d)} &= \varphi(m) \sum_{A \subset \mathbb{N}_r} \varphi(\prod_{i\in A} p_i)^{-1} \\
&= p_1^{k_1-1}\cdots p_r^{k_r-1} \sum_{A\subset\mathbb{N}_r} \prod_{i\in A}(p_i - 1).
\end{aligned}$$

Finalement, la formule $\prod_{i=1}^{s}(a_i+1) = \sum_{A\subset\mathbb{N}_s} \prod_{i\in A} a_i$ nous donne $\sum_{A\subset\mathbb{N}_r} \prod_{i\in A}(p_i-1) = p_1\cdots p_r$ et donc $\sum_{i=0}^{m-1} \mathrm{Tr}_m(\zeta_m^i)\zeta_m^i = m$. ❄

Supposons que (W,β) est un $\mathbb{Q}$-espace vectoriel muni d'une forme bilinéaire définie positive, possédant une isométrie t de polynôme caractéristique $F = \Phi_{n_1}^{r_1}\cdots\Phi_{n_s}^{r_s}$ et de polynôme minimal $f = \Phi_{n_1}\cdots\Phi_{n_s}$. Posons pour $i = 1,\ldots,s$, $W_i = \frac{f}{\Phi_{n_i}}(t)(W)$. Le théorème bien connu d'algèbre linéaire dit de la "décomposition primaire" affirme que $W = W_1 \oplus \cdots \oplus W_s$. Nous allons montrer qu'il s'agit d'une somme orthogonale.

Proposition 1.2.3

Soit $W = W_1 \oplus \cdots \oplus W_s$, comme précédemment. Posons $\beta_i = \beta|_{W_i}$ pour tout $i = 1, \ldots, s$. On a

$$(W, \beta) = (W_1, \beta_1) \boxplus \cdots \boxplus (W_s, \beta_s).$$

Démonstration :

Posons $t_i = t|_{W_i}$. Il est clair que t_i est de polynôme minimal Φ_{n_i}, donc $t_i^{n_i} = Id_{W_i}$. Soient $w_i \in W_i$ et $w_j \in W_j$ avec $i \neq j$. Il existe $w \in W$ tel que $w_j = \frac{f}{\Phi_{n_j}}(t)(w)$. Puisque t est une isométrie, on a $\beta(t_i^{n_i-1}(w_i), w) = \beta(w_i, t(w))$. Calculons :

$$\beta(w_i, w_j) = \beta(w_i, \frac{f}{\Phi_{n_j}}(t)(w)) = \beta(\frac{f}{\Phi_{n_i}}(t^{n_i-1})(w_i), w).$$

Nous avons vu au lemme précédent que Φ_{n_i} divise $\Phi_{n_i}(X^{n_i-1})$, donc Φ_{n_i} divise $\frac{f}{\Phi_{n_j}}(X^{n_i-1})$, c'est à dire que $\frac{f}{\Phi_{n_i}}(t^{n_i-1})(w_i) = 0$. ❄

Chaque W_i est un $\mathbb{Q}(\zeta_{n_i})$-espace vectoriel : l'action est définie par $\zeta_{n_i} \cdot x = t_i(x)$. Sur chacun de ces W_i, on définit la forme suivante :

$$\boxed{\begin{array}{rcl} h_i : W_i \times W_i & \longrightarrow & \mathbb{Q}(\zeta_{n_i}) \\ (x\ ,\ y) & \longmapsto & \displaystyle\sum_{j=0}^{n_i-1} \beta_i(t^{-j}(x), y)\zeta_{n_i}^j . \end{array}}$$

On montre facilement que c'est une forme hermitienne relativement à la conjugaison complexe. Nous allons voir qu'il est possible de retrouver β_i, connaissant h_i :

Proposition 1.2.4

Soit $W = W_1 \boxplus \cdots \boxplus W_s$, comme précédemment. Pour tout $i = 1, \ldots, s$, on a :

$$\boxed{\beta_i(x, y) = \frac{1}{n_i} \mathrm{Tr}_{n_i}(h_i(x, y))}$$

où Tr_{n_i} est la trace de l'extension $\mathbb{Q}(\zeta_{n_i})$ sur $\mathbb{Q}$.

Démonstration :

Calculons la trace de $h_i(x, y)$:

$$\begin{aligned} \mathrm{Tr}_{n_i}(h_i(x, y)) &= \mathrm{Tr}_{n_i}(\sum_{j=0}^{n_i-1} \beta_i(t^{-j}(x), y)\zeta_{n_i}^j) \\ &= \sum_{j=0}^{n_i-1} \mathrm{Tr}_{n_i}(\beta_i(t^{-j}(x), y)\zeta_{n_i}^j) \\ &= \sum_{j=0}^{n_i-1} \mathrm{Tr}_{n_i}(\zeta_{n_i}^j)\beta_i(t^{-j}(x), y) \\ &= \sum_{j=0}^{n_i-1} \mathrm{Tr}_{n_i}(\zeta_{n_i}^j)\beta_i(x, t^j(y)) \\ &= \beta_i(x, \sum_{j=0}^{n_i-1} \mathrm{Tr}_{n_i}(\zeta_{n_i}^j)t^j(y)) \\ &=: \beta_i(x, G(t)(y)). \end{aligned}$$

Le lemme 1.2.2 nous apprend que $\sum_{j=0}^{n_i-1} \mathrm{Tr}_{n_i}(\zeta_{n_i}^j)\zeta_{n_i}^j = n_i$. C'est-à-dire que Φ_{n_i} divise le polynôme $G - n_i$. D'où, puisque $y \in W_i$, on trouve :

$$\mathrm{Tr}_{n_i}(h_i(x,y)) = \beta_i(x,(G-n_i)(t)(y)) + n_i\beta_i(x,y) = n_i\beta_i(x,y).$$

❄

Grâce à cette formule et à ce qui va suivre, nous allons montrer que les formes h_i sont totalement définies positives.

Définition 1.2.5

Soient $E = \mathbb{Q}(\zeta)$ un corps cyclotomique, $K = \mathbb{Q}(\zeta + \bar{\zeta})$ le corps fixe pour la conjugaison complexe, V un E-espace vectoriel de dimension n, et $h : V \times V \longrightarrow E$, une forme hermitienne pour la conjugaison complexe.

a) Cette forme est dite *totalement définie positive* si $\sigma(h(x,x)) > 0$, pour tout plongement σ du groupe de Galois $\mathrm{Gal}(K/\mathbb{Q})$.

b) Cette forme est dite *non dégénérée* si $h(x,y) = 0$ pour tout y implique $x = 0$.

Lemme 1.2.6

Soient $E = \mathbb{Q}(\zeta)$ et $K = \mathbb{Q}(\zeta + \bar{\zeta})$, comme dans la définition précédente. Soient V, un E-espace vectoriel de dimension n, et $h : V \times V \longrightarrow E$, une forme hermitienne non dégénérée. Supposons que $\mathrm{Tr}_{E/\mathbb{Q}}(h(x,x)) > 0$ pour tout x. Alors h est totalement définie positive.

Démonstration :

Un théorème classique d'algèbre linéaire nous dit que h est diagonalisable. Supposons donc que relativement à la base $e_1, \ldots, e_n$, la matrice de h soit $(\alpha_1) \oplus \cdots \oplus (\alpha_n)$. Il est clair que $\alpha_i \in K$ pour tout i. Supposons que h ne soit pas totalement définie positive. Alors les α_i ne sont pas tous totalement positifs. Supposons que α_1 ne le soit pas. Soient $\sigma_1, \ldots, \sigma_m$, les plongements de K. On peut supposer que $\sigma_1(\alpha_1) < 0$. Par le théorème d'approximation faible (voir par exemple ([O'M], Theorem 11:8)), on peut trouver un élément $\lambda \in K$, tel que $|\sigma_1(\lambda)|^2 > |\sigma_1(\lambda)| > \max(1, \frac{2}{|\sigma_1(\alpha_1)|})$, et tel que $|\sigma_i(\lambda)|^2 < |\sigma_i(\lambda)| < \min(1, \frac{1}{m\,|\sigma_i(\alpha_1)|})$ pour $i = 2, \ldots, m$.

Posons $y = \lambda e_1$. On a $h(y,y) = \alpha_1\lambda\bar{\lambda}$. Calculons

$$\begin{aligned}\mathrm{Tr}_{E/\mathbb{Q}}(h(y,y)) &= [E:K] \cdot \mathrm{Tr}_{K/\mathbb{Q}}(h(y,y)) = 2 \cdot \sum_{i=1}^{m} \sigma_i(h(y,y)) \\ &= 2 \cdot \left[\sigma_1(\alpha_1)|\sigma_1(\lambda)|^2 + \sum_{i=2}^{m} \sigma_i(\alpha_1)\ |\sigma_i(\lambda)|^2\right] < 0.\end{aligned}$$

On trouve une contradiction. Donc h est totalement définie positive. ❄

Corollaire 1.2.7

Soient $i = 1, \ldots, s$, et (W_i, h_i) le $\mathbb{Q}(\zeta_{n_i})$-espace vectoriel hermitien défini précédemment. La forme h_i est totalement définie positive.

Démonstration :

Soit $x \in W_i$. On a vu à la proposition 1.2.4 que $\mathrm{Tr}_{n_i}(h_i(x,x)) = n_i\beta_i(x,x) > 0$, car β est supposée définie positive. On conclut en vertu du lemme précédent. ❄

§ 3. Résultats sur le dual bilinéaire et le dual hermitien

Définition 1.3.1

Soient A un anneau commutatif intègre, K son corps des fractions, et V un K-espace vectoriel muni d'une forme bilinéaire ou hermitienne k. Soit $N \subset V$ et $\tilde{N}$ l'espace vectoriel engendré par N. On définit

$$N_k^{\#} := \{x \in \tilde{N} \mid k(x,y) \in A \ \forall\, y \in N\}.$$

Cet ensemble est appelé le *dual de N relativement à k*. Lorsqu'il n'y a pas d'ambigüité, on écrira $N^{\#}$. Il est bien connu (cf. [Co-Slo], p. 48) que si (M,β) est un $\mathbb{Z}$-réseau, alors $[M_\beta^{\#} : M] = \det(M,\beta)$.

Soit (M,β) un $\mathbb{Z}$-réseau unimodulaire. Soit $t \in O(M)$ de polynôme caractéristique $F = \Phi_{n_1}^{r_1} \cdots \Phi_{n_s}^{r_s}$ et donc de polynôme minimal $f = \Phi_{n_1} \cdots \Phi_{n_s}$. Soit $i = 1, \ldots, s$. Posons $W_i = \dfrac{f}{\Phi_{n_i}}(t)(W)$, avec $W = M \otimes \mathbb{Q}$ $(= \mathbb{Q}^n)$, sur lequel β et t se prolongent naturellement. Posons encore $M_i = M \cap W_i$ et notons $p_i : W \longrightarrow W_i$ la projection orthogonale de W sur W_i. On a vu au paragraphe précédent que $W = W_1 \boxplus \cdots \boxplus W_s$. Ainsi $M_1 \boxplus \cdots \boxplus M_s$ est un sous-réseau de M.

Proposition 1.3.2

Pour tout $i = 1, \ldots s$, on a

$$(M_i)_{\beta_i}^{\#} = p_i(M),$$

où β_i est la restriction de β à W_i.

Démonstration :

Notons $M_i^{\#}$ pour $(M_i)_{\beta_i}^{\#}$. Soient x et $y \in W$. On a clairement que $\beta(p_i(x), y) = \beta(x, p_i(y))$ pour tout i. Soient $x \in M_i$ et $y \in M$. Alors, on a $\beta(x, p_i(y)) = \beta(p_i(x), y) = \beta(x,y) \in \mathbb{Z}$. Donc $p_i(M) \subset M_i^{\#}$ pour tout i, ou, ce qui est équivalent, $M_i \subset p_i(M)^{\#}$. Or, puisque $M = M^{\#}$, $M_1 \boxplus \cdots \boxplus M_s$ est le plus grand sous-réseau de M se scindant en s parties orthogonales, chacune contenue dans un W_i. On trouve donc $M_i = p_i(M)^{\#}$, ou encore, $p_i(M) = M_i^{\#}$. ❄

Corollaire 1.3.3

Soit $i = 1, \ldots, s$. Posons

$$a(F,i) = \min\{a \in \mathbb{N} - \{0\} \mid \exists\, g, h \in \mathbb{Z}[X] \text{ avec } g\Phi_{n_i} + h\frac{f}{\Phi_{n_i}} = a\}.$$

Alors on a : $a(F,i)(M_i)_{\beta_i}^{\#} \subset M_i$.

Démonstration :

Soient g et $h \in \mathbb{Z}[X]$ réalisant $a(F,i)$. On voit facilement que p_i est égale à $\dfrac{1}{a(F,i)}\dfrac{hf}{\Phi_{n_i}}(t)$. Ainsi, $a(F,i)(M_i)_{\beta_i}^{\#} = a(F,i)p_i(M) = \dfrac{hf}{\Phi_{n_i}}(t)(M) \subset M$ car $t(M) = M$. ❄

Définition 1.3.4

Si (N,γ) est un $\mathbb{Z}$-réseau, la forme

$$\overline{\gamma} : N^{\#}/N \times N^{\#}/N \longrightarrow \mathbb{Q}/\mathbb{Z}$$
$$(x\,,\,y) \qquad \longmapsto \gamma(x,y) \pmod{\mathbb{Z}}$$

est appelée *forme déterminant de* (N,γ). Les formes déterminant $(N^{\#}/N,\overline{\gamma})$ et $(N'^{\#}/N',\overline{\gamma'})$ sont dites *anti-isométriques*, s'il existe $\nu : N^{\#}/N \longrightarrow N'^{\#}/N'$, telle que $\overline{\gamma'}(\nu(x),\nu(y)) = -\overline{\gamma}(x,y)$, pour tout x,y dans $N^{\#}/N$. L'application ν est bien sûr appelée *anti-isométrie.*

Voici un résultat qui jouera un rôle important dans la suite.

Proposition 1.3.5

Supposons que $F = \Phi_{n_1}^{r_1}\cdots\Phi_{n_s}^{r_s}$, $f = \Phi_{n_1}\cdots\Phi_{n_s}$, $(M,\beta)\in\mathscr{O}(F)$, *et* $M_i = M\cap W_i$ *avec* $W_i = \dfrac{f}{\Phi_{n_i}}(t)(W)$, *pour tout* $i = 1,\dots,s$, *et* $W = M\otimes\mathbb{Q}$.

Soit $i = 1,\dots,s$. *Posons* $\breve{W}_i := W_1\boxplus\cdots\boxplus W_{i-1}\boxplus W_{i+1}\boxplus\cdots\boxplus W_s$ *et* $\breve{p}_i : W\longrightarrow\breve{W}_i$ *la projection orthogonale de* W *sur* $\breve{W}_i$, *ainsi que* $\breve{M}_i := M\cap\breve{W}_i$. *Alors, il existe un isomorphisme*

$$\boxed{\alpha_i : M_i^{\#}/M_i \xrightarrow{\simeq} \breve{M}_i^{\#}/\breve{M}_i}$$

où $M_i^{\#} = (M_i)_{\beta_i}^{\#}$, $\breve{M}_i^{\#} = (\breve{M}_i)_{\breve{\beta}_i}^{\#}$, *et où* $\breve{\beta}_i$ *est la restriction de* β *à* $\breve{M}_i$. *Cet isomorphisme possède les propriétés suivantes :*

a) c'est une anti-isométrie de $(M_i^{\#}/M_i,\overline{\beta_i})$ *sur* $(\breve{M}_i^{\#}/\breve{M}_i,\overline{\breve{\beta}_i})$,

b) le diagramme suivant est commutatif :

$$\begin{array}{ccc} M_i^{\#}/M_i & \xrightarrow{\alpha_i} & \breve{M}_i^{\#}/\breve{M}_i \\ \Big\downarrow{\scriptstyle \overline{t_i}} & & \Big\downarrow{\scriptstyle \overline{\breve{t}_i}} \\ M_i^{\#}/M_i & \xrightarrow{\alpha_i} & \breve{M}_i^{\#}/\breve{M}_i. \end{array}$$

où $t_i = t|_{W_i}$, $\breve{t}_i = t|_{\breve{W}_i}$, $\overline{t_i} : x+M_i\longmapsto t_i(x)+M_i$ *est l'isométrie de* $(M_i^{\#}/M_i,\overline{\beta_i})$ *définie par* t_i, *et* $\overline{\breve{t}_i} : x+\breve{M}_i\longmapsto\breve{t}_i(x)+\breve{M}_i$ *est l'isométrie de* $(\breve{M}_i^{\#}/\breve{M}_i,\overline{\breve{\beta}_i})$ *définie par* $\breve{t}_i$.

Démonstration :

Les applications $\overline{t_i}$ et $\overline{\breve{t}_i}$ sont bien définies, car on vérifie facilement que $t_i(M_i^{\#}) = M_i^{\#}$, et que $\breve{t}_i(\breve{M}_i^{\#}) = \breve{M}_i^{\#}$.

On a $p_i(M) = M_i^{\#}$ (cf. proposition 1.3.2). Ainsi, l'application $x\longmapsto p_i(x)+M_i$ est un homomorphisme surjectif de M sur $M_i^{\#}/M_i$, et son noyau est $M_i\boxplus\breve{M}_i$. Il induit un isomorphisme de $M/(M_i\boxplus\breve{M}_i)$ sur $M_i^{\#}/M_i$ noté $\overline{p_i}$. De manière analogue, $\breve{p}_i$ induit un isomorphisme de $M/(M_i\boxplus\breve{M}_i)$ sur $\breve{M}_i^{\#}/\breve{M}_i$ noté $\overline{\breve{p}_i}$. Ainsi, $\alpha_i := \overline{\breve{p}_i}\circ\overline{p_i}^{-1}$ est l'isomorphisme cherché. En effet :

a) De la définition de α_i, il suit que $M = \{x+y\in M_i^{\#}\boxplus\breve{M}_i^{\#} \mid \alpha_i(x+M_i) = y+\breve{M}_i\}$. Soit $x+y\in M$ avec $\alpha_i(x+M_i) = y+\breve{M}_i$. On a $\mathbb{Z}\ni\beta(x+y,x+y) = \beta_i(x,x)+\breve{\beta}_i(y,y)$. Donc

$$\overline{\beta_i}(x+M_i,x+M_i)+\overline{\breve{\beta}_i}(y+\breve{M}_i,y+\breve{M}_i) = \overline{\beta_i}(x+M_i,x+M_i)+\overline{\breve{\beta}_i}(\alpha_i(x+M_i),\alpha_i(x+M_i))$$
$$\equiv 0 \pmod{\mathbb{Z}}.$$

b) Soit $x+M_i\in M_i^{\#}/M_i$. On veut montrer que $\overline{\breve{t}_i}(\alpha_i(x+M_i)) = \alpha_i(t_i(x)+M_i)$. Supposons que $\alpha_i(x+M_i) = y+\breve{M}_i$. On a $\overline{\breve{t}_i}(y+\breve{M}_i) = \breve{t}_i(y)+\breve{M}_i$. On a aussi par définition de y que $x+y\in M$, donc $t(x+y) = t_i(x)+\breve{t}_i(y)\in M$.

D'autre part, supposons que $\alpha_i(t_i(x)+M_i) = y'+\breve{M}_i$. On a donc $t_i(x)+y'\in M$. D'où $M\ni t_i(x)+\breve{t}_i(y)-(t_i(x)+y') = \breve{t}_i(y)-y'\in\breve{W}_i$. Ainsi, $\breve{t}_i(y)-y'\in\breve{W}_i\cap M = \breve{M}_i$, donc $\breve{t}_i(y)+\breve{M}_i = y'+\breve{M}_i$. ❄

Le résultat précédent va nous permettre d'estimer le déterminant des (M_i, β_i), en fonction du polynôme $F = \Phi_{n_1}^{r_1} \cdots \Phi_{n_s}^{r_s}$. Avant cela, introduisons la notion de résultant et de facteur invariant. Ces deux notions seront souvent utilisés dans ce travail.

Définition 1.3.6

Soit A un anneau factoriel. On considère les deux polynômes $f = a_m X^m + \cdots + a_1 X + a_0$ et $g = b_n X^n + \cdots + b_1 X + b_0$ de $A[X]$. On définit *le résultant de f et g* comme étant le déterminant de la matrice

$$\left.\begin{matrix} \\ n \text{ lignes} \\ \\ \\ \\ m \text{ lignes} \\ \\ \\ \end{matrix}\right\{ \left(\begin{array}{ccccccccc} a_m & a_{m-1} & \cdots & \cdots & a_0 & 0 & \cdots & \cdots & 0 \\ 0 & a_m & a_{m-1} & \cdots & \cdots & a_0 & 0 & \cdots & 0 \\ \multicolumn{9}{c}{\dotfill} \\ 0 & \cdots & 0 & a_m & a_{m-1} & \cdots & \cdots & \cdots & a_0 \\ b_n & b_{n-1} & \cdots & \cdots & b_0 & 0 & \cdots & \cdots & 0 \\ 0 & b_n & b_{n-1} & \cdots & \cdots & b_0 & 0 & \cdots & 0 \\ \multicolumn{9}{c}{\dotfill} \\ 0 & \cdots & 0 & b_n & b_{n-1} & \cdots & \cdots & \cdots & b_0 \end{array} \right).$$

On note ce déterminant $\mathrm{Res}(f, g)$.

Lemme 1.3.7

Soient A un anneau factoriel, et $f = a_m X^m + \cdots + a_1 X + a_0$ et $g = b_n X^n + \cdots + b_1 X + b_0 \in A[X]$. On a les résultats suivants :

a) $\mathrm{Res}(f, g) = (-1)^{mn} \mathrm{Res}(g, f)$.

b) $\mathrm{Res}(f, g) = 0$ *si et seulement si* $a_m = b_n = 0$, *ou alors, f et g ont un diviseur commun de degré positif.*

c) Il existe $\tilde{f}$ *et* $\tilde{g}$ *dans* $A[X]$ *tels que* $f\tilde{f} + g\tilde{g} = \mathrm{Res}(f, g)$.

d) On a $\mathrm{Res}(f_1 f_2, g) = \mathrm{Res}(f_1, g)\,\mathrm{Res}(f_2, g)$ *pour tout* $f_1, f_2 \in A[X]$.

e) Supposons que $f = a_m \prod_{i=1}^{m}(X - \alpha_i)$ *et* $g = b_n \prod_{j_1}^{n}(X - \beta_j)$ *avec* α_i, β_j *dans une clôture algébrique du corps des fractions de A. Alors on a*

$$\begin{aligned} \mathrm{Res}(f, g) &= a_m^n b_n^m \prod_{i=1}^{m}\prod_{j=1}^{n}(\alpha_i - \beta_j) \\ &= a_m^n \prod_{i=1}^{m} g(\alpha_i) \\ &= (-1)^{mn} b_n^m \prod_{j=1}^{n} f(\beta_j). \end{aligned}$$

f) Si f et g sont irréductibles dans $\mathbb{Z}[X]$, posons $E = \mathbb{Q}[X]/(f) = \mathbb{Q}(\alpha)$ et $K = \mathbb{Q}[X]/(g) = \mathbb{Q}(\alpha')$. Alors on a :

$$|\mathrm{Res}(f, g)| = |N_{E/\mathbb{Q}}(g(\alpha))| = |N_{K/\mathbb{Q}}(f(\alpha'))|.$$

g) Supposons que $f = \Phi_d$ et que $g = \Phi_{d'}$ avec $d' \geq d$. On a

$$\mathrm{Res}(\Phi_d, \Phi_{d'}) = \begin{cases} 0 & \text{si } d = d' \\ p^{\varphi(d')/\varphi(p^i)} & \text{si } d' = p^i d \text{ avec } p \in \mathbb{P} \text{ et } \mathrm{pgcd}(p, d) = 1 \\ p^{\varphi(d')/p^i} & \text{si } d' = p^i d \text{ avec } p \in \mathbb{P} \text{ et } \mathrm{pgcd}(p, d) \neq 1 \\ \pm 1 & \text{sinon.} \end{cases}$$

Démonstration :

Les points a) à f) sont montrés dans ([Mar], §3.5). Le point g) est montré dans ([Sto], Proposition 3.4) (avec une petite erreur dans l'énoncé du résultat). ❄

Théorème 1.3.8

Soient A un anneau de Dedekind, K son corps des fraction, et V un K-espace vectoriel de dimension n. Soient N et L des A-réseaux de V. Alors il existe $x_1, \dots, x_n$ une base de V telle que

$$\begin{cases} N = \mathfrak{r}_1 x_1 \oplus \cdots \oplus \mathfrak{r}_n x_n \\ L = \mathfrak{r}_1 \mathfrak{a}_1 x_1 \oplus \cdots \oplus \mathfrak{r}_n \mathfrak{a}_n x_n \end{cases}$$

où les $\mathfrak{r}_i$, $\mathfrak{a}_i$ sont des idéaux fractionnaires tels que

$$\mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \cdots \supset \mathfrak{a}_n.$$

Les $\mathfrak{a}_i$ définis de cette manière sont uniques. On les appelle les facteurs invariants de L dans N. De plus, si $L \subset N$ alors les $\mathfrak{a}_i$ sont des idéaux entiers, et on a :

$$N/L \simeq \bigoplus_{i=1}^{n} A/\mathfrak{a}_i.$$

Ce résultat est bien entendu connu sous le nom de "théorème des facteurs invariants"

Démonstration :

Cf. ([O'M] Theorem 81:11 p. 215) ❄

Remarque :

Dans le théorème précédent, si A est un anneau principal, on peut choisir $\mathfrak{r}_i = A$ pour tout i.

Théorème 1.3.9

Supposons que $F = \Phi_{n_1}^{r_1} \cdots \Phi_{n_s}^{r_s}$, $f = \Phi_{n_1} \cdots \Phi_{n_s}$, $(M, \beta) \in \mathscr{E}(F)$, et $M_i = M \cap W_i$ avec $W_i = \frac{f}{\Phi_{n_i}}(t)(W)$ pour tout $i = 1, \dots, s$, et $W = M \otimes \mathbb{Q}$. Alors on a :

$$\boxed{|M_i^{\#}/M_i| \text{ divise } \mathrm{Res}(\Phi_{n_i}, \frac{f}{\Phi_{n_i}})^{r_i}}$$

pour tout $i = 1, \dots s$, où $M_i^{\#} = (M_i)_{\beta_i}^{\#}$.

Démonstration :

L'action de t_i sur W_i munit cet ensemble d'une structure de $\mathbb{Q}(\zeta_{n_i})$-espace vectoriel de dimension r_i, dans lequel $M_i \subset M_i^{\#}$ sont des $\mathbb{Z}[\zeta_{n_i}]$-réseaux. Ainsi, le théorème des facteurs invariants nous assure de l'existence de r_i idéaux $\mathfrak{a}_1, \dots, \mathfrak{a}_{r_i}$ de $\mathbb{Z}[\zeta_{n_i}]$ tels que

$$M_i^{\#}/M_i \simeq \bigoplus_{j=1}^{r_i} \mathbb{Z}[\zeta_{n_i}]/\mathfrak{a}_j.$$

La proposition 1.3.5 affirme qu'il existe α_i tel que $\overline{t_i} \circ \alpha_i = \alpha_i \circ \overline{t_i}$. En particulier, $\overline{t_i}$ est annulé par le polynôme minimal de $\overline{t_i}$ qui est $\frac{f}{\Phi_{n_i}}$. C'est-à-dire que l'idéal engendré par $\frac{f}{\Phi_{n_i}}(\zeta_{n_i})$ est inclus dans $\mathfrak{a}_j$ pour tout $j = 1, \dots, r_i$. On trouve alors :

$$\begin{aligned} |M_i^{\#}/M_i| &= \prod_{j=1}^{r_i} [\mathbb{Z}[\zeta_{n_1}] : (\frac{f}{\Phi_{n_i}}(\zeta_{n_i}))][\mathfrak{a}_j : (\frac{f}{\Phi_{n_i}}(\zeta_{n_i}))]^{-1} \\ &= |N_{\mathbb{Q}(\zeta_{n_i})/\mathbb{Q}}(\frac{f}{\Phi_{n_i}}(\zeta_{n_i}))|^{r_i} \cdot (\prod_{j=1}^{r_i} [\mathfrak{a}_j : (\frac{f}{\Phi_{n_i}}(\zeta_{n_i}))])^{-1}. \end{aligned}$$

La partie f) du lemme 1.3.7 nous apprend que $|N_{\mathbb{Q}(\zeta_{n_i})/\mathbb{Q}}(\frac{f}{\Phi_{n_i}}(\zeta_{n_i}))| = |\mathrm{Res}(\Phi_{n_i}, \frac{f}{\Phi_{n_i}})|$, ce qui nous permet de conclure. ❄

Rappelons que pour $i = 1, \ldots, s$, l'ensemble M_i possède deux structures. Premièrement, M_i est un $\mathbb{Z}$-réseau du $\mathbb{Q}$-espace vectoriel W_i, muni de la forme β_i, et de dimension $\varphi(n_i)r_i$. Deuxièmement, M_i est un $\mathbb{Z}[\zeta_{n_i}]$-réseau du $\mathbb{Q}(\zeta_{n_i})$-espace vectoriel W_i, de dimension r_i, et muni de la forme h_i définie par $h_i(x,y) = \sum_{j=0}^{n_i-1} \beta_i(t^{-j}(x), y)\zeta_{n_i}^j$. Il est donc possible de définir le dual $(M_i)_{\beta_i}^{\#}$ de M_i relativement à β_i, et de définir le dual $(M_i)_{h_i}^{\#}$ de M_i relativement à h_i. Nous allons voir qu'il existe un lien entre ces deux ensembles. Pour cela, nous devons introduire la notion de différente.

Définition 1.3.10

Soient E/K une extension de corps de nombres, O_E et O_K leur anneau des entiers. Notons $\mathrm{Tr}_{E/K}$ la trace de cette extension. Le dual de O_E relativement à la forme bilinéaire trace, est l'ensemble

$$\mathfrak{a} = \{x \in E \mid \mathrm{Tr}_{E/K}(xy) \in O_K \ \forall\, y \in O_E\}.$$

C'est un idéal fractionnaire de E. Nous appellerons *différente de E/K* l'idéal entier de E, $\mathscr{D}(E/K) = \mathfrak{a}^{-1}$.

Lorsque $E = \mathbb{Q}(\zeta_n)$ où ζ_n est une racine primitive n-ième de l'unité et $K = \mathbb{Q}$, on écrira $\mathscr{D}_n$ pour $\mathscr{D}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

Lemme 1.3.11

Soient E un corps de nombres et V un E-espace vectoriel de dimension finie. Supposons que E soit muni d'une involution notée $x \mapsto \overline{x}$ telle que $\overline{O_E} = O_E$ où O_E est l'anneau des entiers de E. Soit $h : V \times V \longrightarrow E$ une forme hermitienne relativement à cette involution et N un O_E-réseau de V. Posons $b = \mathrm{Tr}_{E/\mathbb{Q}} \circ h$. Nous avons les résultats suivants :

a) $N_b^{\#}$ est un O_E-module.

b) $N_b^{\#} = \mathscr{D}^{-1} \cdot N_h^{\#}$ où $\mathscr{D}$ est la différente de $E/\mathbb{Q}$.

Démonstration :

a) Soient $x \in N_b^{\#}$, $\alpha \in O_E$ et $y \in N$. Il est clair que :

$$b(\alpha x, y) = \mathrm{Tr}_{E/\mathbb{Q}}(h(\alpha x, y)) = \mathrm{Tr}_{E/\mathbb{Q}}(h(x, \overline{\alpha} y)) = b(x, \overline{\alpha} y) \in \mathbb{Z}.$$

b) Soient $\alpha \in \mathscr{D}^{-1}$, $x \in N_h^{\#}$ et $y \in N$. Nous avons : $b(\alpha x, y) = \mathrm{Tr}_{E/\mathbb{Q}}(\alpha \underbrace{h(x,y)}_{\in O_E}) \in \mathbb{Z}$. Donc $\mathscr{D}^{-1} N_h^{\#} \subset N_b^{\#}$.

Soient $x \in N_b^{\#}$, $y \in N$ et $\alpha \in \mathscr{D}$. Nous avons vu en a) que $N_b^{\#}$ est un O_E-module. Ainsi, $\mathrm{Tr}_{E/\mathbb{Q}}(\nu h(x,y)) = b(\nu x, y) \in \mathbb{Z}$ pour tout $\nu \in O_E$. Nous en déduisons que $h(x,y) \in \mathscr{D}^{-1}$. D'où $h(\alpha x, y) = \alpha h(x,y) \in \mathscr{D} \cdot \mathscr{D}^{-1} = O_E$. Et ainsi, $N_b^{\#} \subset \mathscr{D}^{-1} N_h^{\#}$. ❄

Remarque :

Sous les mêmes hypothèses que pour le lemme précédent, soient $\mathfrak{a}_1 \supset \cdots \supset \mathfrak{a}_n$ les facteurs invariants de N dans $N_h^{\#}$. Il est facile de voir que $\overline{\mathscr{D}} = \mathscr{D}$. Nous en déduisons donc que $\overline{\mathfrak{a}_i} = \mathfrak{a}_i$, pour tout $i = 1, \ldots, n$.

Théorème 1.3.12

Supposons à nouveau que $F = \Phi_{n_1}^{r_1} \cdots \Phi_{n_s}^{r_s}$, $f = \Phi_{n_1} \cdots \Phi_{n_s}$, $(M, \beta) \in \mathscr{E}(F)$ *et* $M_i = M \cap W_i$ *avec* $W_i = \dfrac{f}{\Phi_{n_i}}(t)(W)$ *et* $W = M \otimes \mathbb{Q}$. *Munissons* M_i *de la forme hermitienne* h_i *définie par* $h_i(x,y) = \sum_{j=0}^{n_i-1} \beta_i(t^{-j}(x), y)\zeta_{n_i}^j$ *avec* $\beta_i = \beta|_{W_i}$. *On a :*

$$\boxed{M_i \subset (M_i)_{\beta_i}^{\#} \subset (M_i)_{h_i}^{\#} = \frac{1}{n_i}\mathscr{D}_{n_i}(M_i)_{\beta_i}^{\#}} \quad \text{pour } i = 1, \ldots, s$$

où $\mathscr{D}_{n_i} = \mathscr{D}(\mathbb{Q}(\zeta_{n_i})/\mathbb{Q})$.

Par conséquent :

$$\boxed{\det(M_i, \beta_i) = [(M_i)_{\beta_i}^{\#} : M_i] = \frac{d(\mathbb{Q}(\zeta_{n_i}))^{r_i}}{n_i^{r_i\varphi(n_i)}} \cdot [(M_i)_{h_i}^{\#} : M_i]} \quad \text{pour } i = 1, \ldots, s$$

où $d(\mathbb{Q}(\zeta_{n_i}))$ *est le discriminant de l'extension* $\mathbb{Q}(\zeta_{n_i})$ *sur* $\mathbb{Q}$.

Démonstration :

Cela découle du lemme précédent, de la Proposition 1.2.4 qui nous apprend que $\mathrm{Tr}_{\mathbb{Q}(\zeta_{n_i})/\mathbb{Q}} \circ h_i = n_i\beta_i$, et que $[\mathbb{Z}[\zeta_{n_i}] : \mathscr{D}_{n_i}] = d(\mathbb{Q}(\zeta_{n_i}))$, cf. par exemple ([Fr-Ta], Result 2.14, p. 125).

❄

§ 4. Le cas $F = \Phi_{n_1}^{r_1}\Phi_{n_2}^{r_2}$

Supposons, comme le suggère le titre de ce paragraphe, que $F = \Phi_{n_1}^{r_1}\Phi_{n_2}^{r_2}$ et que $(M, \beta) \in \mathscr{E}(F)$. Posons $W = M \otimes \mathbb{Q}$, sur lequel β et l'isométrie t se prolongent naturellement. On sait que $W = W_1 \boxplus W_2$, avec $W_1 = \Phi_{n_2}(t)(W)$ et $W_2 = \Phi_{n_1}(t)(W)$. En appliquant la proposition 1.3.5 et le théorème 1.3.9 à ce cas, on trouve que $(M_1^{\#}/M_1, \overline{\beta_1})$ est anti-isométrique à $(M_2^{\#}/M_2, \overline{\beta_2})$, et que $|M_1^{\#}/M_1| = |M_2^{\#}/M_2|$ divise $\mathrm{Res}(\Phi_{n_1}, \Phi_{n_2})^r$, où $M_i = W_i \cap M$, $M_i^{\#} = (M_i)_{\beta_i}^{\#}$, pour $i = 1, 2$, et $r = \min(r_1, r_2)$.

Posons $t_i = t|_{W_i}$ pour $i = 1, 2$. On a vu que $t_i(M_i) = M_i$ et que $t_i(M_i^{\#}) = M_i^{\#}$. Ainsi, puisque le polynôme minimal de t_i est Φ_{n_i}, $M_i \subset M_i^{\#}$ sont des $\mathbb{Z}[\zeta_{n_i}]$-réseaux de W_i, où ζ_{n_i} est une racine primitive n_i-ième de l'unité. Nous allons démontrer qu'il existe un lien entre les facteurs invariants de M_1 dans $M_1^{\#}$ et ceux de M_2 dans $M_2^{\#}$.

Théorème 1.4.1

Soient $\mathfrak{a}_1 \supset \cdots \supset \mathfrak{a}_{r_1}$ *les facteurs invariants de* M_1 *dans* $M_1^{\#}$ *et* $\mathfrak{b}_1 \supset \cdots \supset \mathfrak{b}_{r_2}$, *ceux de* M_2 *dans* $M_2^{\#}$. *Sans limiter la généralité, supposons que* $r_1 \leq r_2$. *Posons* $\mathfrak{a}_i = \mathbb{Z}[\zeta_{n_1}]$ *si* $r_1 + 1 \leq i \leq r_2$. *On a :*

$$\mathbb{Z}[\zeta_{n_1}]/\mathfrak{a}_i \simeq \mathbb{Z}[\zeta_{n_2}]/\mathfrak{b}_i \quad \forall\, i = 1, \ldots, r_2.$$

En outre, soit $i = 1, \ldots, r_2$. *Si* $\mathfrak{a}_i = \mathfrak{p}_1^{l_1} \cdots \mathfrak{p}_s^{l_s}$ *est la décomposition de* $\mathfrak{a}_i$ *en idéaux premiers de* $\mathbb{Z}[\zeta_{n_1}]$ *et si* $\mathfrak{b}_i = \mathfrak{P}_1^{m_1} \cdots \mathfrak{P}_k^{m_k}$ *est la décomposition de* $\mathfrak{b}_i$ *en idéaux premiers de* $\mathbb{Z}[\zeta_{n_2}]$, *on a* $s = k$, *et, moyennant une renumérotation éventuelle,* $m_j = l_j$ *et* $\mathbb{Z}[\zeta_{n_1}]/\mathfrak{p}_j \simeq \mathbb{Z}[\zeta_{n_2}]/\mathfrak{P}_j$, *pour tout* $j = 1, \ldots, s$.

Démonstration :

Nous savons en vertu de la proposition 1.3.5 que le carré suivant commute :

$$\begin{array}{ccc} M_1^{\#}/M_1 & \xrightarrow{\alpha_1} & M_2^{\#}/M_2 \\ \Big\downarrow{\scriptstyle \overline{t_1}} & & \Big\downarrow{\scriptstyle \overline{t_1}=\overline{t_2}} \\ M_1^{\#}/M_1 & \xrightarrow{\alpha_1} & M_2^{\#}/M_2 \end{array}$$

De cela découle que $\overline{t_1}$ et $\overline{t_2}$ sont chacun annulés par Φ_{n_1} et par Φ_{n_2}. Ainsi, α_1 est un isomorphisme de B-modules, où $B = \mathbb{Z}[X]/(\Phi_{n_1}, \Phi_{n_2})$. Or, on a les isomorphismes d'anneaux suivants :

$$\mathbb{Z}[\zeta_{n_1}]/(\Phi_{n_2}(\zeta_{n_1})) \simeq B \simeq \mathbb{Z}[\zeta_{n_2}]/(\Phi_{n_1}(\zeta_{n_2})).$$

Le théorème des facteurs invariants affirme que $M_1^\#/M_1 \simeq \bigoplus_{j=1}^{r_1} \mathbb{Z}[\zeta_{n_1}]/\mathfrak{a}_j$. Puisque $M_1^\#/M_1$ est un B-module, on a $\mathfrak{a}_1 \supset \cdots \supset \mathfrak{a}_{r_1} \supset (\Phi_{n_2}(\zeta_{n_1}))$. Ces idéaux correspondent à d'uniques idéaux $\overline{\mathfrak{a}_1} \supset \cdots \supset \overline{\mathfrak{a}_{r_1}}$ de B. Ainsi, $M_1^\#/M_1 \simeq \bigoplus_{j=1}^{r_1} B/\overline{\mathfrak{a}_j}$. En faisant le même raisonnement sur les $\mathfrak{b}_1 \supset \cdots \supset \mathfrak{b}_{r_2}$, on voit qu'il existe des uniques idéaux $\overline{\mathfrak{b}_1} \supset \cdots \supset \overline{\mathfrak{b}_{r_2}}$ de B tels que $M_2^\#/M_2 \simeq \bigoplus_{j_i}^{r_2} B/\overline{\mathfrak{b}_j}$. On en déduit que $\overline{\mathfrak{a}_j} = \overline{\mathfrak{b}_j}$ pour tout $i = 1, \ldots, r_2$, car $M_1^\#/M_1$ et $M_2^\#/M_2$ sont B-isomorphes, et grâce à l'unicité des facteurs invariants. Cela démontre la première partie du théorème. La deuxième partie se déduit directement du théorème des restes chinois. ❄

Remarque :

Soit $f = \Phi_{n_1}\Phi_{n_2}$. Soit $\mathscr{A}_f$, la catégorie dont les objets sont des triplets (M, β, t) où (M, β) est un $\mathbb{Z}$-réseau unimodulaire et t est une isométrie de (M, β) de polynôme minimal f. Soit $\mathscr{B}_f$, la catégorie dont les objets sont des quintuplets $(N_1, N_2, k_1, k_2, \nu)$ où, pour $i = 1, 2$, (N_i, k_i) est un $\mathbb{Z}[\zeta_{n_i}]$-module projectif hermitien totalement défini positif et ν est une anti-isométrie de $(N_1)_{\gamma_1}^\#/N_1$ sur $(N_2)_{\gamma_2}^\#/N_2$ avec $\gamma_i = \frac{1}{n_i}\mathrm{Tr}_{\mathbb{Q}(\zeta_{n_i})/\mathbb{Q}} \circ k_i$. Alors, les deux catégories $\mathscr{A}_f$ et $\mathscr{B}_f$ sont équivalentes. Ce résultat n'étant pas utile pour estimer la masse des F-réseaux, le lecteur pourra trouver un énoncé moins succinct et une démonstration de ce résultat en annexe.

§ 5. Le genre d'une forme hermitienne

Soient ζ_m une racine primitive m-ième de l'unité, et M un $\mathbb{Z}[\zeta_m]$-réseau d'un $\mathbb{Q}(\zeta_m)$-espace vectoriel W, de dimension finie, muni d'une forme hermitienne h non dégénérée (i.e. $h(x, y) = 0$ pour tout $y \in W$ implique $x = 0$). Typiquement, (M, h) est un des (M_i, h_i) des paragraphes précédents. Supposons que les facteurs invariants de M dans $M_h^\#$ soient connus, et que h soit totalement définie positive. Sous ces hypothèses, le genre de (M, h) est-il déterminé ?

Nous verrons que la réponse est non en général (cf. théorème 1.5.5). Mais si ζ_m est une racine primitive m-ième de l'unité avec m différent d'une puissance de 2, et si les facteurs invariants satisfont certaines hypothèses, alors la réponse est oui. Dans les chapitres suivants, lors de calculs explicites, nous nous trouverons souvent dans le cas où les facteurs invariants déterminent le genre.

Voici tout d'abord un résultat nous permettant de contrôler la ramification de certains idéaux du corps $\mathbb{Q}(\zeta + \bar{\zeta})$ dans le corps $\mathbb{Q}(\zeta)$.

Définition 1.5.1

Soient E/K une extension galoisienne de corps de nombres, O_E et O_K l'anneau des entiers de E et de K respectivement. Soit $\mathfrak{p}$ un idéal premier de O_K. D'après la théorie classique des entiers algébriques, il existe $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ des idéaux premiers de O_E, et e un entier positif tel que $\mathfrak{p}O_E = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^e$. On dit que $\mathfrak{p}$ *se ramifie dans* O_E si $e > 1$, *se ramifie totalement dans* O_E si $e = [E : K]$ et donc $r = 1$, *se décompose dans* O_E si $r > 1$ et *est inerte dans* O_E si $r = 1$ et $e = 1$.

Dans le cas d'une extension quadratique, tout idéal premier se ramifie (totalement), se décompose, ou est inerte dans O_E.

Lemme 1.5.2

Soient $E = \mathbb{Q}(\zeta_m)$, $K = E \cap \mathbb{R} = \mathbb{Q}(\zeta_m + \overline{\zeta_m})$, O_E et O_K leur anneau des entiers respectifs.

a) Si $m = q^k$ ou $2p^k$, avec $q \in \mathbb{P}$, $p \in \mathbb{P} - \{2\}$, et k un entier positif, alors il existe un unique idéal premier de O_K qui se ramifie dans O_E.

b) Si m est d'un autre type, alors aucun premier de O_K ne se ramifie dans O_E.

Démonstration :

D'une manière générale, si L'/L est une extension de corps de nombre, $\mathfrak{p} \subset O_L$ ramifie dans $O_{L'}$ si et seulement si $\mathfrak{p}$ divise l'idéal $N_{L'/L}(\mathscr{D}(L'/L))$, où $N_{L'/L}$ est la norme relative de l'extension L'/L. Ce résultat est démontré dans ([Fr-Ta], Theorem 22 p. 126).

a) Puisque $\mathbb{Q}(\zeta_{2p^k}) = \mathbb{Q}(\zeta_{p^k})$ si p est impair, nous pouvons supposer que $m = q^k$ avec $q \in \mathbb{P}$. Il est bien connu que $qO_E = (1 - \zeta_{q^k})^{\varphi(q^k)}$ et que $d(E/\mathbb{Q}) = N_{E/\mathbb{Q}}(\mathscr{D}(E/\mathbb{Q}))$ est une puissance de q. Ainsi, l'unique idéal de K au-dessus de q est aussi l'unique idéal de K, se ramifiant dans O_E.

b) On a $\mathscr{D}(E/K) = f'(\zeta_m)O_E$ avec $f = X^2 - (\zeta_m + \overline{\zeta_m})X + 1$. Ce résultat est vrai pour tout m et est démontré dans ([Fr-Ta], Result 2.20, p. 127). Donc, $\mathscr{D}(E/K) = (1 - \zeta_m^2)O_E$. Supposons que $m \neq q^k, 2p^k$. Dans ce cas, $(1 - \zeta_m^2)$ est inversible, voir ([Fr-Ta], Theorem 45 p. 210). Ainsi, $N_{E/K}(\mathscr{D}(E/K)) = O_K$. Donc aucun idéal premier de O_K ne se ramifie dans O_E. ❄

Rappels sur les complétions

Soit L un corps de nombres. Notons $\mathbb{P}(L)$ l'ensemble des idéaux premiers de O_L. Cet ensemble est souvent appelé *l'ensemble des places finies de L*. Soit $\{u_1, \ldots, u_t\}$ l'ensemble des plongements de L dans $\mathbb{C}$. Cet ensemble est appelé *l'ensemble des places infinies de L*. Enfin, la réunion $\mathbb{P}(L) \cup \{u_1, \ldots, u_t\} = \mathbb{P}'(L)$ est appelée *l'ensemble des places de L*. Soient $\mathfrak{p} \in \mathbb{P}(L)$ et $\mathfrak{a}$ un idéal fractionnaire de O_L. Il existe un entier, noté $v_\mathfrak{p}(\mathfrak{a})$, et appelé *valuation $\mathfrak{p}$-adique de $\mathfrak{a}$*, tel que $\mathfrak{a} = \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})}\mathfrak{a}'\mathfrak{b}'^{-1}$ avec $\mathfrak{a}', \mathfrak{b}' \subset O_E$ et $\mathfrak{p} \nmid \mathfrak{a}'\mathfrak{b}'$. L'application $a \mapsto |a|_\mathfrak{p} := N_{L/\mathbb{Q}}(\mathfrak{p})^{-v_\mathfrak{p}(aO_L)}$ est une valeur absolue de L appelée *valeur absolue $\mathfrak{p}$-adique*. Si u est une place infinie de L, l'application $a \mapsto |a|_u := |u(a)|_\infty$, où $|z|_\infty$ désigne le module du nombre complexe z, est aussi une valeur absolue. Ainsi, à chaque élément $\mathfrak{p}$ de $\mathbb{P}'(L)$, il est possible d'associer une valeur absolue, munissant ainsi L d'une structure de corps topologique. Chaque $\mathfrak{p}$ engendre une topologie différente. Le complété de L relativement à une telle topologie est noté $L_\mathfrak{p}$. Si $\mathfrak{p}$ est une place finie de L, le corps $L_\mathfrak{p}$ est une extension finie de $\mathbb{Q}_p$ où $p = \mathfrak{p} \cap \mathbb{Z}$. Il est ainsi possible de définir l'anneau des éléments de $L_\mathfrak{p}$ entiers sur $\mathbb{Z}_p$. Cet anneau se note $O_{L_\mathfrak{p}}$. C'est aussi l'adhérence de O_L dans $L_\mathfrak{p}$. Si u est une place infinie, $L_u = \mathbb{R}$ ou $\mathbb{C}$, et on pose $O_{L_u} = L_u$.

Soient $E \subset \mathbb{C}$ un corps de nombres galoisien, totalement complexe, K le corps fixe pour la conjugaison complexe notée $x \mapsto \overline{x}$. Si $\mathfrak{p} \in \mathbb{P}'(K)$, on note $\boxed{\tilde{E}_\mathfrak{p} \text{ pour } E \otimes_K K_\mathfrak{p}, \text{ et } \tilde{O}_{E_\mathfrak{p}} \text{ pour } O_E \otimes_{O_K} O_{K_\mathfrak{p}}.}$ La conjugaison complexe se transporte naturellement sur $\tilde{E}_\mathfrak{p} : x \otimes y \mapsto \overline{x} \otimes y$. Cette nouvelle involution est aussi notée avec une barre. Il est facile de voir que $K_\mathfrak{p} = \{x \in \tilde{E}_\mathfrak{p} \mid \overline{x} = x\}$, que $O_{K_\mathfrak{p}} = \{x \in \tilde{O}_{E_\mathfrak{p}} \mid \overline{x} = x\}$, et que $[\tilde{E}_\mathfrak{p} : K_\mathfrak{p}] = [\tilde{O}_{E_\mathfrak{p}} : O_{K_\mathfrak{p}}] = 2$.

Voici une formule bien connue :

$$\tilde{E}_\mathfrak{p} = \prod_{\mathfrak{P}|\mathfrak{p}} E_\mathfrak{P} \text{ et } \tilde{O}_{E_\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} O_{E_\mathfrak{P}}$$

où $E_\mathfrak{P}$ est le complété de E relativement à la valeur absolue $\mathfrak{P}$-adique, et $O_{E_\mathfrak{P}}$ est le complété de O_E relativement à cette même valeur absolue. Le lecteur trouvera une démonstration de ce résultat dans ([Fr-Ta], Theorem 17, p. 107)

On en déduit donc que si $\mathfrak{p}$ ne se décompose pas, alors $\tilde{E}_\mathfrak{p} = E_\mathfrak{P}$ est un corps, et $\tilde{O}_{E_\mathfrak{p}} = O_{E_\mathfrak{P}}$ est un anneau local. L'idéal maximal se note encore $\mathfrak{P}$, et il est engendré par un élément $\not{\pi}$, appelé *uniformisante*

de $\mathfrak{P}$. Si $\mathfrak{p}$ est inerte dans O_E, on peut choisir π dans $O_{K_\mathfrak{p}}$, et que $\pi O_{K_\mathfrak{p}} = \mathfrak{p}$. Si $\mathfrak{p}$ se ramifie dans O_E et $2 \notin \mathfrak{p}$, on peut supposer que $\mathfrak{p}$ vu dans $O_{K_\mathfrak{p}}$ est engendré par une uniformisante π telle que $\pi^2 = \pi$ (cf. [Jac] p. 451).

Si $\mathfrak{p}$ se décompose, alors $\tilde{E}_\mathfrak{p} = E_{\mathfrak{P}_1} \times E_{\mathfrak{P}_2}$. Ici, l'involution permute $E_{\mathfrak{P}_1}$ et $E_{\mathfrak{P}_2}$. Les corps $E_{\mathfrak{P}_1}$ et $E_{\mathfrak{P}_2}$ sont isomorphes, et $K_\mathfrak{p}$ est la "diagonale", c'est-à-dire que $K_\mathfrak{p}$ est égal à l'ensemble $\{(x, \overline{x}) \mid x \in E_{\mathfrak{P}_1}\}$. Les mêmes phénomènes se produisent au niveau des anneaux.

Définitions 1.5.3

Soient A un anneau muni d'une involution, et (M, h) un A-module muni d'une forme hermitienne relativement à cette involution. L'ensemble des isomorphismes $u : M \longrightarrow M$, tels que $h(u(x), u(y)) = h(x, y)$ pour tout x, y dans M, muni de la composition des applications, est appelé *groupe unitaire de* (M, h). Nous noterons $U(M, h)$ ou $U(M)$ ce groupe. Chaque élément de $U(M)$ est appelé *isométrie de* (M, h). Les A-modules hermitiens (M, h) et (M', h') sont dits A-équivalents, et nous écrirons $(M, h) \overset{A}{\simeq} (M', h')$ s'il existe un isomorphisme $u : M \longrightarrow M'$, tel que $h'(u(x), u(y)) = h(x, y)$ pour tout x, y dans M.

Soient $E \subset \mathbb{C}$ un corps de nombres galoisien, totalement complexe, muni de l'involution définie par la conjugaison complexe, O_E son anneau des entiers, K le corps fixe pour cette involution, et O_K son anneau des entiers. Soient (M, h) et (M', h') deux O_E-modules projectifs hermitiens de rang n. Nous dirons que (M, h) et (M', h') sont *dans le même genre* si pour tout $\mathfrak{p} \in \mathbb{P}'(K)$ nous avons

$$(M \otimes_{O_E} \tilde{O}_{E_\mathfrak{p}}, h \otimes_{O_E} \tilde{O}_{E_\mathfrak{p}}) \overset{\tilde{O}_{E_\mathfrak{p}}}{\simeq} (M' \otimes_{O_E} \tilde{O}_{E_\mathfrak{p}}, h' \otimes_{O_E} \tilde{O}_{E_\mathfrak{p}}).$$

Par la suite, nous écrirons $\boxed{M_\mathfrak{p} \text{ pour } M \otimes_{O_E} \tilde{O}_{E_\mathfrak{p}} \text{ et } h_\mathfrak{p} \text{ pour } h \otimes_{O_E} \tilde{O}_{E_\mathfrak{p}}.}$ Le genre de (M, h) noté $\mathscr{G}_M$ est l'ensemble des classes d'isométries de tous les O_E-modules projectifs hermitiens qui sont dans le même genre que (M, h). Si (M, h) est non dégénéré, alors $\mathscr{G}_M$ est fini.

Le déterminant de h relativement à n'importe quelle base de M se note $d(M)$ ou $d(M, h)$. C'est un élément de $K^*/N_{E/K}(U(O_E))$, où $N_{E/K}$ est la norme de l'extension E/K, $E^* = E - \{0\}$, et $U(O_E)$ dénote l'ensemble des éléments inversibles de O_E.

Le E-espace vectoriel $W := M \otimes_{O_E} E$ est de dimension n dans lequel M est un O_E-réseau. la forme $h \otimes_{O_E} E$ se note encore h. Comme avant, le déterminant de h relativement à une base de W se note $d(W)$ ou $d(W, h)$. C'est un élément de $K^*/N_{E/K}(E^*)$. Si $\mathfrak{p} \in \mathbb{P}'(K)$, nous noterons évidemment $\boxed{W_\mathfrak{p} \text{ pour } W \otimes_E \tilde{E}_\mathfrak{p} \text{ et } h_\mathfrak{p} \text{ pour } h \otimes_E \tilde{E}_\mathfrak{p}}$.

Soit $\{u_1, \ldots, u_t\}$ l'ensemble des places infinies de K. Pour tout $i = 1, \ldots, t$, la forme (W_{u_i}, h_{u_i}) est équivalente à la forme définie par p_i copies de la forme $< 1 >$ et par q_i copies de la forme $< -1 >$. Le couple (p_i, q_i) est appelé *signature de* (W_{u_i}, h_{u_i}).

Théorème 1.5.4

Soient $E \subset \mathbb{C}$ un corps de nombres, galoisien, totalement complexe, muni de l'involution définie par la conjugaison complexe, O_E son anneau des entiers, K le corps fixe pour cette involution et O_K son anneau des entiers. Soit encore W un E-espace vectoriel de dimension n muni d'une forme hermitienne non dégénérée h. Si $\{u_1, \ldots, u_t\}$ est l'ensemble des places infinies de K, et que pour tout $i = 1, \ldots, t$, (p_i, q_i) est la signature de (W_{u_i}, h_{u_i}), alors l'ensemble $\boxed{\{n, d(W), (p_1, q_1), \ldots, (p_t, q_t)\}}$ forme un système complet d'invariants des classes d'isométries de formes non dégénérées sur E. C'est-à-dire, si (W', h') est une E-espace vectoriel hermitien de dimension n tel que $d(W) = d(W')$, et $(p_i, q_i) = (p'_i, q'_i)$ pour tout $i = 1, \ldots t$, alors $(W, h) \overset{E}{\simeq} (W', h')$.

Démonstration :

Ce théorème est connu sous le nom de "théorème de Landherr". Il est démontré dans [Land]. ❄

Le théorème suivant est le point central de ce paragraphe. Il donne un système d'invariants presque complet pour les genres de formes hermitiennes.

Théorème 1.5.5

Soient E un corps de nombres, galoisien, totalement complexe muni de l'involution donnée par la conjugaison complexe que nous noterons $x \mapsto \overline{x}$, O_E son anneau des entiers, K le corps fixe pour cette involution, et O_K son anneau des entiers. Supposons qu'il y ait au plus un idéal premier $\mathfrak{p}_0$ de O_K qui se ramifie dans O_E. Notons $\mathfrak{P}_0$ l'idéal de O_E au-dessus de $\mathfrak{p}_0$, et supposons que $2 \notin \mathfrak{P}_0$. Soit $\{u_1, \ldots, u_t\}$ l'ensemble des places infinies de K.

Soit n un entier positif, $(p_1, q_1), \ldots, (p_t, q_t)$ des couples d'entiers positifs tels que $p_i + q_i = n$, $i = 1, \ldots, t$. Soient $\mathfrak{a}_1 \supset \cdots \supset \mathfrak{a}_n$ des idéaux entiers non nuls de O_E, et

$$\boxed{I := \{n, (p_1, q_1), \ldots, (p_t, q_t), \mathfrak{a}_1, \ldots, \mathfrak{a}_n\}.}$$

Posons encore $N = N(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) = |\{v_{\mathfrak{P}_0}(\mathfrak{a}_i) \mid i = 1, \ldots, t \text{ et } v_{\mathfrak{P}_0}(\mathfrak{a}_i) \in 2\mathbb{Z}\}|$.

Soit $\mathrm{Gen}(I)$, l'ensemble de tous les genres de O_E-modules projectifs hermitiens (M, h), de rang n, tels que les facteurs invariants de M dans $M_h^{\#}$ soient $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$, et tels que les formes (M_{u_i}, h_{u_i}) soient de signature (p_i, q_i), $i = 1, \ldots, t$. Alors, nous avons le résultat suivant :

$$|\mathrm{Gen}(I)| \leq 2^{\max(0, N-1)}.$$

Démonstration :

Le reste de ce paragraphe sera consacré à la démonstration de ce théorème.

Voici une esquisse de la démonstration :
nous allons étudier $M_{\mathfrak{p}}$ pour tout $\mathfrak{p} \in \mathbb{P}'(K)$. Si u_i est une place infinie, il est évident que (M_{u_i}, h_{u_i}) est équivalent à la forme diagonale donnée par la signature (p_i, q_i), donc à une forme canonique ne dépendant que de I. Si $\mathfrak{p} \in \mathbb{P}(K)$ est inerte ou se décompose, nous verrons que $(M_{\mathfrak{p}}, h_{\mathfrak{p}})$ est équivalent à une forme canonique ne dépendant que des facteurs invariants. Si $\mathfrak{p}$ se ramifie dans O_E, $M_{\mathfrak{p}}$ n'est pas équivalent à une forme canonique, et c'est là que se concentreront les difficultés.

Remarque :

Nous avons vu dans le lemme 1.5.2 que $E = \mathbb{Q}(\zeta_m)$, avec m différent d'une puissance de 2 satisfait les hypothèses du théorème.

Lemme 1.5.6

Si (M, h) satisfait les hypothèses du théorème 1.5.5, on a l'égalité suivante :

$$(M_{\mathfrak{p}})_{h_{\mathfrak{p}}}^{\#} = (M_h^{\#})_{\mathfrak{p}}$$

pour tout $\mathfrak{p} \in \mathbb{P}(K)$.

Démonstration :

Soit $\mathrm{Tr} : \tilde{E}_{\mathfrak{p}} \longrightarrow K_{\mathfrak{p}}$ la trace définie par $\mathrm{Tr}(x) = x + \overline{x}$. Posons

$$\mathscr{D}^{-1}(\tilde{E}_{\mathfrak{p}}/K_{\mathfrak{p}}) := \{x \in \tilde{E}_{\mathfrak{p}} \mid \mathrm{Tr}(\tilde{O}_{E_{\mathfrak{p}}} x) \subset O_{K_{\mathfrak{p}}}\} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathscr{D}^{-1}(E_{\mathfrak{P}}/K_{\mathfrak{p}}).$$

La dernière égalité vient du fait que si $x = (x_{\mathfrak{P}})_{\mathfrak{P}|\mathfrak{p}} \in \tilde{E}_{\mathfrak{p}}$, alors $\mathrm{Tr}(x) = \sum_{\mathfrak{P}|\mathfrak{p}} \mathrm{Tr}_{E_{\mathfrak{P}}/K\mathfrak{p}}(x_{\mathfrak{P}})$.

Définissons encore

$$\begin{aligned} \beta_{\mathfrak{p}} : W_{\mathfrak{p}} \times W_{\mathfrak{p}} &\longrightarrow K_{\mathfrak{p}} \\ (x\ ,\ y) &\longmapsto \mathrm{Tr}(h_{\mathfrak{p}}(x,y)). \end{aligned}$$

La forme $\beta_{\mathfrak{p}}$ est clairement bilinéaire. L'affirmation suivante se démontre de la même manière que le Lemme 1.3.11 :

$$(M_{\mathfrak{p}})^{\#}_{\beta_{\mathfrak{p}}} = \mathscr{D}^{-1}(\tilde{E}_{\mathfrak{p}}/K_{\mathfrak{p}}) \cdot (M_{\mathfrak{p}})^{\#}_{h_{\mathfrak{p}}}.$$

Or, nous avons $\mathscr{D}^{-1}(\tilde{E}_{\mathfrak{p}}/K_{\mathfrak{p}}) = (\mathscr{D}^{-1}(E/K))_{\mathfrak{p}}$ (cf. [Fr-Ta], Result 2.17, p. 126). De même, $(M_{\mathfrak{p}})^{\#}_{\beta_{\mathfrak{p}}} = (M^{\#}_{\beta})_{\mathfrak{p}}$, où $\beta = \mathrm{Tr}_{E/K} \circ h$ (cf. ([Fr-Ta], Result 2.7, p. 122). On obtient donc :

$$(M_{\mathfrak{p}})^{\#}_{h_{\mathfrak{p}}} = \mathscr{D}^{-1}(\tilde{E}_{\mathfrak{p}}/K_{\mathfrak{p}}) \cdot (M_{\mathfrak{p}})^{\#}_{\beta_{\mathfrak{p}}} = (\mathscr{D}^{-1}(E/K) M^{\#}_{\beta})_{\mathfrak{p}} = (M^{\#}_{h})_{\mathfrak{p}}.$$

❄

Définition 1.5.7

Supposons que $\mathfrak{p} \in \mathbb{P}(K)$ ne se décompose pas dans E. Fixons $\not{\pi}$ une uniformisante du corps $\tilde{E}_{\mathfrak{p}} = E_{\mathfrak{P}}$. Soit N un $O_{E_{\mathfrak{P}}}$-réseau d'un $E_{\mathfrak{P}}$-espace vectoriel V, muni d'une forme hermitienne k. Un élément $x \in N$ est dit *primitif* si $x \notin \mathfrak{P}N$ ou, ce qui est équivalent, x se prolonge en une $O_{E_{\mathfrak{P}}}$-base de N. Le réseau (N, k) est dit $\mathfrak{P}^i$-*modulaire* si $k(x, N) = \not{\pi}^i \cdot O_{E_{\mathfrak{P}}} = \mathfrak{P}^i$ pour tout x primitif.

Lemme 1.5.8

Sous les mêmes hypothèses que pour la définition précédente, N peut se décomposer comme somme orthogonale $N_1 \boxplus \cdots \boxplus N_r$, telle que pour tout $i = 1, \ldots, r$, chacun des N_i est $\mathfrak{P}^{m_i}$-modulaire, avec n_i un entier positif. Cette somme s'appelle décomposition de Jordan. Les m_i et la dimension des N_i ne dépendent pas de la décomposition de Jordan.

Démonstration :

Cf. ([Jac], p. 449). ❄

Etude de $M_{\mathfrak{p}}$ si $\mathfrak{p}$ est inerte

Rappelons que dans ce cas $\tilde{E}_{\mathfrak{p}} = E_{\mathfrak{P}}$ d'uniformisante $\not{\pi} \in O_{K_{\mathfrak{p}}}$.

Théorème 1.5.9

Soit N un $O_{E_{\mathfrak{P}}}$-réseau d'un $E_{\mathfrak{P}}$-espace vectoriel V, muni d'une forme hermitienne non dégénérée k. Supposons que (N, k) soit $\mathfrak{P}^i$-modulaire. Alors, il existe une base de N telle que la matrice de k relativement à cette base est

$$(\not{\pi}^i) \oplus \cdots \oplus (\not{\pi}^i).$$

Démonstration :

Cf. ([Jac], p. 451). ❄

Corollaire 1.5.10

Supposons que (M,h) satisfasse les hypothèses du théorème 1.5.5. Soit $\mathfrak{p}$ un idéal de O_K, inerte dans O_E. Alors, il existe une base de $M_\mathfrak{p}$ telle que la matrice de $h_\mathfrak{p}$ relativement à cette base ne dépende que de $\{\mathfrak{a}_1,\dots,\mathfrak{a}_n\}$.

Plus précisément, supposons que $\{v_\mathfrak{P}(\mathfrak{a}_1),\dots,v_\mathfrak{P}(\mathfrak{a}_n)\} = \{m_1,\dots,m_l\}$ avec $m_1 < \cdots < m_l$. Soit $i = 1,\dots,l$. Posons $n_i = |\{\mathfrak{a}_j \mid v_\mathfrak{P}(\mathfrak{a}_j) = m_i,\ j = 1,\dots,n\}|$. Alors, il existe une base de $M_\mathfrak{p}$, telle que la matrice de $h_\mathfrak{p}$ relativement à cette base soit

$$\underbrace{(\mathfrak{p}^{m_1})\oplus\cdots\oplus(\mathfrak{p}^{m_1})}_{n_1 \text{ fois}}\oplus\cdots\oplus\underbrace{(\mathfrak{p}^{m_l})\oplus\cdots\oplus(\mathfrak{p}^{m_l})}_{n_l \text{ fois}}.$$

Démonstration :

Soit $M_1 \boxplus \cdots \boxplus M_{l'}$ une décomposition de Jordan de $M_\mathfrak{p}$. Chacun des M_i est $\mathfrak{P}^{m_i'}$-modulaire pour tout $i = 1,\dots l'$.

Le théorème précédent nous dit qu'il existe $e_1,\dots,e_n$ une base de $M_\mathfrak{p}$, telle que relativement à cette base la matrice de $h_\mathfrak{p}$ soit

$$\underbrace{(\mathfrak{p}^{m_1'})\oplus\cdots\oplus(\mathfrak{p}^{m_1'})}_{n_1' \text{ fois}}\oplus\cdots\oplus\underbrace{(\mathfrak{p}^{m_{l'}'})\oplus\cdots\oplus(\mathfrak{p}^{m_{l'}'})}_{n_{l'}' \text{ fois}}.$$

On montre facilement que dans ce cas,

$$(M_\mathfrak{p})^\#_{h_\mathfrak{p}} = \mathfrak{P}^{-m_1'}e_1\oplus\cdots\oplus\mathfrak{P}^{-m_1'}e_{n_1'}\boxplus\cdots\boxplus\mathfrak{P}^{-m_{l'}'}e_{n-n_{l'}'}\oplus\cdots\oplus\mathfrak{P}^{-m_i'}e_n.$$

Or, on a vu que $(M_\mathfrak{p})^\#_{h_\mathfrak{p}} = (M_h^\#)_\mathfrak{p}$. On trouve ainsi que $l = l'$, $n_i' = n_i$, et que $m_j' = m_j$, en vertu de l'unicité des facteurs invariants. ❄

Etude de $M_\mathfrak{p}$ si $\mathfrak{p}$ est décomposé

Dans ce cas, nous savons que $\tilde{E}_\mathfrak{p} = E_{\mathfrak{P}_1}\times E_{\mathfrak{P}_2}$ et que $\tilde{O}_{E_\mathfrak{p}} = O_{E_{\mathfrak{P}_1}}\times O_{E_{\mathfrak{P}_2}}$. L'involution permute les composantes. Posons

$$W_{\mathfrak{P}_1} := (1,0)\cdot W_\mathfrak{p} \qquad W_{\mathfrak{P}_2} := (0,1)\cdot W_\mathfrak{p}$$
$$M_{\mathfrak{P}_1} := (1,0)\cdot M_\mathfrak{p} \qquad M_{\mathfrak{P}_2} := (0,1)\cdot M_\mathfrak{p}.$$

On a $W_\mathfrak{p} = W_{\mathfrak{P}_1}\oplus W_{\mathfrak{P}_2}$ et $M_\mathfrak{p} = M_{\mathfrak{P}_1}\oplus M_{\mathfrak{P}_2}$. L'espace $W_{\mathfrak{P}_i}$ est un $E_{\mathfrak{P}_i}$-espace vectoriel dans lequel $M_{\mathfrak{P}_i}$ est un $O_{E_{\mathfrak{P}_i}}$-réseau, pour $i = 1,2$. On vérifie facilement que $h_\mathfrak{p}|_{W_{\mathfrak{P}_1}} = h_\mathfrak{p}|_{W_{\mathfrak{P}_2}} = 0$. Ainsi,

$$\begin{aligned} h_\mathfrak{p} : (W_{\mathfrak{P}_1}\oplus W_{\mathfrak{P}_2})\times(W_{\mathfrak{P}_1}\oplus W_{\mathfrak{P}_2}) &\longrightarrow E_{\mathfrak{P}_1}\times E_{\mathfrak{P}_2} \\ ((x_1+x_2)\ ,\quad (y_1+y_2)) &\longmapsto (h_\mathfrak{p}(x_1,y_2),h_\mathfrak{p}(x_2,y_1)). \end{aligned}$$

On a alors le

Théorème 1.5.11

Il existe $x_1, \dots, x_n \in M_{\mathfrak{P}_1}$, $y_1, \dots, y_n \in M_{\mathfrak{P}_2}$, *et* $\mathfrak{r}_1 \supset \cdots \supset \mathfrak{r}_n$ *des uniques idéaux de* $O_{E_{\mathfrak{P}_2}}$ *tels que*

$$M_{\mathfrak{p}} = (O_{E_{\mathfrak{P}_1}} x_1 \oplus \cdots \oplus O_{E_{\mathfrak{P}_1}} x_n) \oplus (\mathfrak{r}_1 y_1 \oplus \cdots \oplus \mathfrak{r}_n y_n)$$

avec $h_{\mathfrak{p}}(x_i + y_i, x_j + y_j) = \delta_{ij}$ *pour tout* i, j. *De plus,* $E_{\mathfrak{P}_1}$ *étant isomorphe à* $E_{\mathfrak{P}_2}$, *chaque idéal* $\mathfrak{r}_i$ *de* $O_{E_{\mathfrak{P}_2}}$ *correspond à un unique idéal* $\mathfrak{r}'_i$ *de* $O_{E_{\mathfrak{P}_1}}$. *Et on a*

$$(M_{\mathfrak{p}})^{\#}_{h_{\mathfrak{p}}} = (\mathfrak{r}'^{-1}_1 x_1 \oplus \cdots \oplus \mathfrak{r}'^{-1}_n x_n) \oplus (O_{E_{\mathfrak{P}_2}} y_1 \oplus \cdots \oplus O_{E_{\mathfrak{P}_2}} y_n).$$

Démonstration :

Le premier résultat est montré dans ([Shi], Proposition 3.2) et le second est une vérification facile. ❄

Corollaire 1.5.12

Supposons que (M, h) *satisfasse les hypothèses du théorème 1.5.5. Soit* $\mathfrak{p}$ *un idéal premier de* O_K *qui décompose dans* O_E *et* $\mathfrak{P}_1, \mathfrak{P}_2$ *les idéaux de* O_E *au-dessus de* $\mathfrak{p}$. *Nous avons vu, lors de la remarque qui suit le lemme 1.3.11, que* $\overline{\mathfrak{a}_i} = \mathfrak{a}_i$. *Donc* $v_{\mathfrak{P}_1}(\mathfrak{a}_i) = v_{\mathfrak{P}_2}(\mathfrak{a}_i)$ *pour tout* $i = 1, \dots n$, *puisque l'involution permute* $\mathfrak{P}_1$ *et* $\mathfrak{P}_2$. *Soit* $\mathfrak{P} = \mathfrak{P}_1$ *ou* $\mathfrak{P}_2$. *Supposons que* $\{v_{\mathfrak{P}}(\mathfrak{a}_1), \dots, v_{\mathfrak{P}}(\mathfrak{a}_n)\} = \{m_1, \dots, m_l\}$, *avec* $m_1 < \cdots < m_l$. *Posons* $n_i = |\{\mathfrak{a}_j \mid v_{\mathfrak{P}}(\mathfrak{a}_j) = m_i,\ j = 1, \dots, n\}|$ *pour* $i = 1, \dots, l$. *Alors le* n*-uplet* $(\mathfrak{r}_1, \dots, \mathfrak{r}_n)$ *d'idéaux du théorème précédent est égal à*

$$(\underbrace{\mathfrak{P}_2^{m_1}, \dots, \mathfrak{P}_2^{m_1}}_{n_1 \text{ fois}}, \dots, \underbrace{\mathfrak{P}_2^{m_l}, \dots, \mathfrak{P}_2^{m_l}}_{n_l \text{ fois}}).$$

Ainsi, comme dans le cas inerte, la forme $h_{\mathfrak{p}}$ *ne dépend que des idéaux* $\mathfrak{a}_1, \dots, \mathfrak{a}_n$.

Démonstration :

Le résultat se démontre aisément en utilisant à nouveau que $(M_h^{\#})_{\mathfrak{p}} = (M_{\mathfrak{p}})^{\#}_{h_{\mathfrak{p}}}$ ainsi que l'unicité des facteurs invariants, mais cette fois pour $M_{\mathfrak{P}_1}$ et $M_{\mathfrak{P}_2}$. ❄

Remarque :

A ce stade, nous avons déjà montré que si aucun premier ne ramifie, alors $|\mathrm{Gen}(I)| \leq 1$. En effet, si $\mathfrak{p}$ est infini, la forme $h_{\mathfrak{p}}$ est isomorphe à la forme diagonale, déterminée par la signature associée à $\mathfrak{p}$. Ainsi, toute la difficulté va se concentrer dans le cas où $\mathfrak{p}$ ramifie.

Etude de $M_{\mathfrak{p}}$ si $\mathfrak{p}$ se ramifie et démonstration du Théorème 1.5.5 .

Commençons par rappeler quelques résultats de la théorie du corps de classe.

Définition 1.5.13

Soit F/L une extension de corps de nombres de degré 2, $N_{F/L}$ la norme de l'extension F/L. Choisissons $\sigma \in L^*$ tel que $F = L(\sqrt{\sigma})$, et soit $\mathfrak{p} \in \mathbb{P}'(L)$ une place finie ou infinie de L.

Définissons

$$\tilde{c}_{\mathfrak{p}} : L^* \longrightarrow \{\pm 1\}$$

$$y \longmapsto (y, \sigma)_{\mathfrak{p}} = \begin{cases} 1 & \text{s'il existe } \eta \text{ et } \nu \in L^*_{\mathfrak{p}} \text{ tels que } y\eta^2 + \sigma\nu^2 = 1 \\ -1 & \text{sinon.} \end{cases}$$

Le symbole $a, b \mapsto (a,b)_{\mathfrak{p}}$ est appelé, comme dans la définition 1.1.1, *symbole de Hilbert.* Un résultat classique ([Co], p. 9) nous dit que $y \in N_{F_{\mathfrak{P}}/L_{\mathfrak{p}}}(F_{\mathfrak{p}}^*)$, avec $\mathfrak{P}|\mathfrak{p}$, si et seulement si $(y,\sigma)_{\mathfrak{p}} = 1$, et $y \in N_{F/L}(F^*)$ si et seulement si $\tilde{c}_{\mathfrak{p}}(y) = 1$, pour tout $\mathfrak{p}$. Il est donc possible de définir

$$\begin{aligned} c_{\mathfrak{p}} : L^*/N_{F/L}(F^*) &\longrightarrow \{\pm 1\} \\ cl(y) &\longmapsto (y,\sigma)_{\mathfrak{p}}. \end{aligned}$$

Le lemme suivant est une généralisation de la formule du produit de Hilbert classique.

Lemme 1.5.14

Soit $y \in L^*$. Nous avons les résultats suivants :

1) $c_{\mathfrak{p}}(cl(y)) = 1$ *pour presque tout* $\mathfrak{p}$

2) $c_{\mathfrak{p}}(cl(y)) = 1$ *si* $\mathfrak{p}$ *décompose*

3) $c_{\mathfrak{p}}(cl(y)) = (-1)^{v_{\mathfrak{p}}(y)}$ *si* $\mathfrak{p}$ *est inerte*

4) $c_{\mathfrak{p}}(cl(y)) = 1$ *pour tout* $\mathfrak{p}$ *si et seulement si* $cl(y) = 1$

5) $\prod_{\mathfrak{p} \in \mathbb{P}'} c_{\mathfrak{p}}(cl(y)) = 1$.

Démonstration :

Cf. ([Co], p. 9). ❄

Poursuivons la démonstration du théorème 1.5.5. Nous nous trouvons donc dans le cas où $\mathfrak{p} = \mathfrak{p}_0$ est l'unique idéal premier de O_K qui ramifie dans O_E. Nous savons aussi que $\tilde{E}_{\mathfrak{p}} = E_{\mathfrak{P}}$ est un corps local.

Lemme 1.5.15

Supposons que (M,h) satisfasse les hypothèses du théorème 1.5.5. Alors, pour tout $\mathfrak{p} \in \mathbb{P}'(K)$, on a :

$$c_{\mathfrak{p}}(cl(\det(W))) = (\det(M_{\mathfrak{p}}), \sigma)_{\mathfrak{p}}$$

où $W = M \otimes \mathbb{Q}$, $\sigma \in K$ est tel que $E = K(\sqrt{\sigma})$, et $\det(M_{\mathfrak{p}})$ est le déterminant de la matrice de $h_{\mathfrak{p}}$ relativement à n'importe quelle base de $M_{\mathfrak{p}}$, modulo $N_{E_{\mathfrak{P}}/K_{\mathfrak{p}}}(U(O_{E_{\mathfrak{P}}}))$, avec $U(O_{E_{\mathfrak{P}}})$ désignant les unités de $O_{E_{\mathfrak{P}}}$.

Démonstration :

Si $\mathfrak{p}$ est décomposé, le résultat est évident, car le symbole de Hilbert est trivial dans ce cas. Supposons que $\mathfrak{p}$ soit inerte, ramifié, ou infini. Soit $e_1, \ldots, e_n$ une E-base de W. Alors, $e_1 \otimes_E E_{\mathfrak{P}}, \ldots, e_n \otimes_E E_{\mathfrak{P}}$ est une $E_{\mathfrak{P}}$-base de $W_{\mathfrak{p}}$. On a donc les égalités suivantes :

$$c_{\mathfrak{p}}(cl(\det(W))) = c_{\mathfrak{p}}(cl(\det(h(e_i,e_j)))) = (\det(h_{\mathfrak{p}}(e_i,e_j)), \sigma)_{\mathfrak{p}}.$$

Soit $f_1, \ldots, f_n$ une $O_{E_{\mathfrak{P}}}$-base de $M_{\mathfrak{p}}$. C'est une $E_{\mathfrak{P}}$-base de $W_{\mathfrak{p}}$. Soient $H = (h(e_i,e_j))_{1 \le i,j \le n}$ et $H' = (h_{\mathfrak{p}}(f_i,f_j))_{1 \le i,j \le n}$. Il existe $S \in \mathrm{Gl}_n(E_{\mathfrak{P}})$ telle que $H' = SH\overline{S}^t$. D'où :

$$\det(M_{\mathfrak{p}}) = \det(H') = \det(H) \cdot N_{E_{\mathfrak{P}}/K_{\mathfrak{p}}}(\det(S)) \in cl_{K_{\mathfrak{p}}^*/N_{(E_{\mathfrak{P}}/K_{\mathfrak{p}})}(E_{\mathfrak{P}}^*)}(\det(W)).$$

❄

Corollaire 1.5.16

Soit (M,h) satisfaisant les hypothèses du théorème 1.5.5. Alors

$$\prod_{\mathfrak{p}\in\mathbb{P}'}(d(M_\mathfrak{p}),\sigma)_\mathfrak{p}=1.$$

Démonstration :

Cela suit des deux lemmes précédents. ❄

Ainsi, connaissant $(d(M_\mathfrak{p}),\sigma)_\mathfrak{p}$ pour tout $\mathfrak{p}$ non ramifié, on en déduit $(d(M_\mathfrak{p}),\sigma)_\mathfrak{p}$ pour l'unique $\mathfrak{p}$ qui ramifie. Or, on connaît $(d(M_\mathfrak{p}),\sigma)_\mathfrak{p}$ si $\mathfrak{p}$ ne se ramifie pas :

a) Si $\mathfrak{p}$ est infini, $(d(M_\mathfrak{p}),\sigma)_\mathfrak{p}=(-1)^{q_i}$ où (p_i,q_i) est la signature relativement à $\mathfrak{p}$.

b) Si $\mathfrak{p}$ se décompose, on sait que $(d(M_\mathfrak{p}),\sigma)_\mathfrak{p}=1$.

c) Si $\mathfrak{p}$ est inerte, on a, $(d(M_\mathfrak{p}),\sigma)_\mathfrak{p}=(-1)^{v_\mathfrak{p}(\det(M))}$.

Avant de terminer la démonstration du théorème 1.5.5, nous avons encore besoin d'un théorème nous permettant de mettre $M_\mathfrak{p}$ sous la forme la plus "canonique possible".

Remarque :

Supposons que $\mathfrak{p}=\mathfrak{p}_0$ est l'unique idéal premier de O_K se ramifiant dans O_E. Alors $U(O_{K_\mathfrak{p}})/N_{E_\mathfrak{P}/K_\mathfrak{p}}(U(O_{E_\mathfrak{P}}))$ est le groupe d'ordre 2 (cf. [Co], Lemma 1.3, p. 5). Ce groupe est formé de la classe de 1 et de celle d'un élément que nous noterons ϵ.

Théorème 1.5.17

Soit N un $O_{E_\mathfrak{P}}$-réseau d'un $E_\mathfrak{P}$-espace vectoriel V muni d'une forme hermitienne non dégénérée k. Supposons que $\mathfrak{p}\subset O_{K_\mathfrak{p}}$ ramifie dans $O_{E_\mathfrak{p}}$. Supposons que N soit $\mathfrak{P}^i$-modulaire.

a) Si i est impair, alors il existe une base de N, dont la matrice de k relativement à cette base est

$$H(i)\oplus\cdots\oplus H(i)$$

où $H(i)$ est la matrice $\begin{pmatrix}0 & \mathfrak{p}^i\\ \bar{\mathfrak{p}}^i & 0\end{pmatrix}$.

b) Si i est pair, alors k n'est pas isomorphe à une forme canonique. On peut trouver une base de N, dont la matrice de k relativement à cette base est

$$(\pi^{\frac{i}{2}})\oplus\cdots\oplus(\pi^{\frac{i}{2}})\oplus(\lambda\cdot\pi^{\frac{i}{2}})$$

où π est une uniformisante de $O_{K_\mathfrak{p}}$, et $\lambda=1$ ou ϵ selon le déterminant de (N,k).

Dans les deux cas les facteurs invariants de N dans $N_k^\#$ sont

$$\underbrace{\mathfrak{P}^i,\ldots,\mathfrak{P}^i}_{\dim(N)\text{ fois}}.$$

Démonstration :

Cf. ([Jac], Proposition 8.1, p. 453). ❄

Fin de la démonstration du Théorème 1.5.5 :

Si $\mathfrak{p}$ ne se ramifie pas, nous avons vu que $h_{\mathfrak{p}}$ est isomorphe à une forme canonique ne dépendant que de I. Supposons que $\mathfrak{p}$ soit l'unique idéal premier de O_K ramifiant dans O_E. Soit $M_1, \ldots, M_l$ une décomposition de Jordan de $M_{\mathfrak{p}}$. Chacun des M_i est, disons, $\mathfrak{P}^{m_i}$-modulaire. Supposons que $m_1 < \cdots < m_s$ soient impairs et que $m_{s+1} < \cdots < m_l$ soient pairs. Le théorème précédant nous assure de l'existence d'une base telle que, relativement à cette base, la matrice de $h_{\mathfrak{p}}$ est égale à $A \oplus B$, où

$$A = \underbrace{H(m_1) \oplus \cdots \oplus H(m_1)}_{\frac{1}{2}\dim(M_1) \text{ fois}} \oplus \cdots \oplus \underbrace{H(m_s) \oplus \cdots \oplus H(m_s)}_{\frac{1}{2}\dim(M_s) \text{ fois}}.$$

et où

$$B = \underbrace{(\pi^{\frac{m_{s+1}}{2}}) \oplus \cdots \oplus (\pi^{\frac{m_{s+1}}{2}}) \oplus (\lambda_1 \cdot \pi^{\frac{m_{s+1}}{2}})}_{\dim(M_{s+1}) \text{ fois}} \oplus \cdots \oplus \underbrace{(\pi^{\frac{m_l}{2}}) \oplus \cdots \oplus (\pi^{\frac{m_l}{2}}) \oplus (\lambda_{l-s} \cdot \pi^{\frac{m_l}{2}})}_{\dim(M_l) \text{ fois}}.$$

En utilisant à nouveau le fait que $(M_h^{\#})_{\mathfrak{p}} = (M_{\mathfrak{p}})_{h_{\mathfrak{p}}}^{\#}$ et l'unicité des facteurs invariants, on en déduit que $N(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) = l - s$, que $\{v_{\mathfrak{P}}(\mathfrak{a}_i) \mid i = 1, \ldots, n \text{ , et } v_{\mathfrak{P}}(\mathfrak{a}_i) \notin 2\mathbb{Z}\} = \{m_1, \ldots, m_s\}$, que $\{v_{\mathfrak{P}}(\mathfrak{a}_i) \mid i = 1, \ldots, n \text{ , et } v_{\mathfrak{P}}(\mathfrak{a}_i) \in 2\mathbb{Z}\} = \{m_{s+1}, \ldots, m_l\}$, et que $|\{\mathfrak{a}_j \mid v_{\mathfrak{P}}(\mathfrak{a}_j) = m_i\}| = \dim(M_i)$, pour tout $i = 1, \ldots, l$.

De plus, on a vu lors du corollaire 1.5.16 que $(d(M_{\mathfrak{p}}), \sigma)_{\mathfrak{p}}$ est connu. C'est-à-dire que la classe de $\prod_{i=1}^{N} \lambda_i \in U(O_{K_{\mathfrak{p}}})/N_{E_{\mathfrak{P}}/K_{\mathfrak{p}}}(U(O_{E_{\mathfrak{P}}}))$ est déterminée. Ainsi, pour tout $i = 1, \ldots, N-1$, il y a deux choix pour λ_i. Ces choix étant faits, λ_N est déterminé. Donc pour un choix de système d'invariants I, il y a $2^{\max(0,N-1)}$ possibilités pour la matrice B. Le théorème est démontré. ❄

Remarque :

Il est même possible que $|\mathrm{Gen}(I)| = 2^{\max(0,N-1)}$ comme le montre l'exemple suivant : soient $i < j$ des entiers positifs. Posons $H = \begin{pmatrix} \pi^i & 0 \\ 0 & \pi^j \end{pmatrix}$ et $H' = \begin{pmatrix} \epsilon\pi^i & 0 \\ 0 & \epsilon\pi^j \end{pmatrix}$, alors $H \overset{O_{E_{\mathfrak{P}}}}{\not\sim} H'$. En effet, supposons qu'il existe un réseau hermitien (N, k) possédant une base telle que la matrice de k relativement à cette base soit H, et une autre base dont la matrice associée soit H'. On en déduit que $N = N_1 \boxplus N_2 = N_1' \boxplus N_2'$ possède deux décompositions de Jordan. Sans limiter la généralité, on peut supposer que N_1 et N_1' sont $\mathfrak{P}^{2i}$-modulaires. Or, la démonstration du Théorème 8.2 de ([Jac], p. 454) nous dit qu'alors $d(N_1) \equiv d(N_1')$ (mod $N_{E_{\mathfrak{P}}/K_{\mathfrak{p}}}(E_{\mathfrak{P}}^*)$). Autrement dit : la forme $< \epsilon\pi^i >$ est équivalente à la forme $< \pi^i >$, ce qui est évidement faux

§ 6 Retour aux F-réseaux et estimation de leur masse

Le but de ce paragraphe, qui est aussi le but de ce chapitre, est d'estimer la masse des F-réseaux. Nous serons obligés de truffer cette partie de définitions techniques, et le théorème central peut paraître un peu rébarbatif. Mais c'est pour pouvoir obtenir des résultats calculatoirement satisfaisants, dans les cas particuliers où nous serons capables de faire des estimations explicites. Voici donc, pour le lecteur pressé, une idée du raisonnement que l'on va suivre. Si (M, β) est un F-réseau, nous avons vu au paragraphe 3 que nous pouvons lui associer un sous-réseau $M_1 \boxplus \cdots \boxplus M_s$, tel que chaque M_i possède une structure de réseau hermitien totalement défini positif, et tel que son dual relativement à cette forme se déduit du dual bilinéaire de M_i (voir le corollaire 1.2.7 et le théorème 1.3.12). Or, l'indice de M_i dans son dual bilinéaire est borné par un nombre qui ne dépend que de F (théorème 1.3.9). Ainsi, le choix des facteurs invariants de M_i dans son dual hermitien est fini. En utilisant le théorème 1.5.5, on trouve alors que l'ensemble des genres possibles pour M_i est fini. Nous allons voir dans ce paragraphe que la masse des F-réseaux est comparable avec la masse de ces différents genres hermitiens. Ce sera le théorème 1.6.6.

Définition 1.6.1

a) Soit $F = \Phi_{n_1}^{r_1} \cdots \Phi_{n_s}^{r_s}$. Posons $\mathscr{F}(F)$ l'ensemble des s-uplets de modules hermitiens, totalement définis positifs $((N_1,k_1),\ldots,(N_s,k_s))$ tels que, pour $i=1,\ldots,s$, (N_i,k_i) soit projectif de rang r_i sur $\mathbb{Z}[\zeta_{n_i}]$, et que la forme $\gamma_i := \frac{1}{n_i}\operatorname{Tr}_{n_i} \circ k_i$ soit une forme bilinéaire sur $\mathbb{Z}$, avec $N_i \subsetneq (N_i)_{\gamma_i}^{\#}$. Supposons de plus que $(N_1 \boxplus \cdots \boxplus N_s, \gamma)$ avec $\gamma(x_1+\cdots+x_s, y_1+\cdots+y_s) = \gamma_1(x_1,y_1)+\cdots+\gamma_s(x_s,y_s)$ soit un $\mathbb{Z}$-réseau de $\mathbb{Q}^n$ muni du produit scalaire usuel, avec $n = \sum_{i=1}^{s} \varphi(n_i) r_i$.

b) Soit $((N_1,k_1),\ldots,(N_s,k_s)) \in \mathscr{F}(F)$. Notons $t : x_1+\cdots+x_s \mapsto \zeta_{n_1}x_1+\cdots+\zeta_{n_s}x_s$. Cette application est clairement une isométrie de $(N_1 \boxplus \cdots \boxplus N_s, \gamma)$, de polynôme caractéristique F.

c) Soit $((N_1,k_1),\ldots,(N_s,k_s)) \in \mathscr{F}(F)$. On définit $\mathscr{L}_{(N_1,\ldots,N_s)}$ comme étant l'ensemble des $\mathbb{Z}$-réseaux unimodulaires indécomposables notés N, tels que

i) $N_1 \boxplus \cdots \boxplus N_s \subset N \subset (N_1)_{\gamma_1}^{\#} \boxplus \cdots \boxplus (N_s)_{\gamma_s}^{\#}$

ii) $N \cap (N_i \otimes_{\mathbb{Z}} \mathbb{Q}) = N_i$ pour tout $i = 1,\ldots,s$

iii) $p_i(N) = (N_i)_{\gamma_i}^{\#}$ où p_i est la projection orthogonale de $\mathbb{Q}^n$ sur $N_i \otimes_{\mathbb{Z}} \mathbb{Q}$ pour tout $i = 1,\ldots,s$

iv) $t(N) = N$.

L'ensemble $\mathscr{L}_{(N_1,\ldots,N_s)}/\overset{\mathbb{Z}}{\simeq}$ se note évidemment $\overline{\mathscr{L}}_{(N_1,\ldots,N_s)}$.

Lemme 1.6.2

Soient $F = \Phi_{n_1}^{r_1}\cdots\Phi_{n_s}^{r_s}$ et $((N_1,k_1),\ldots,(N_s,k_s)) \in \mathscr{F}(F)$. On a l'inégalité suivante :

$$\sum_{N \in \overline{\mathscr{L}}_{(N_1,\ldots,N_s)}} \frac{1}{|O(N)|} \leq \frac{|\overline{\mathscr{L}}_{(N_1,\ldots,N_s)}|}{|U(N_1,k_1)|\cdots|U(N_s,k_s)|}$$

où $O(N)$ est le groupe orthogonal de N, et $U(N_i,k_i)$ est le groupe unitaire de (N_i,k_i).

Démonstration :

Puisqu'ici il n'y a pas d'équivoque, écrivons $\mathscr{L}$ pour $\mathscr{L}_{(N_1,\ldots,N_s)}$. Posons $H = U(N_1,k_1)\times\cdots\times U(N_s,k_s)$.

Montrons d'abord que H agit sur $\mathscr{L}$: soit $\sigma = \sigma_1+\cdots+\sigma_s \in H$. L'application σ étant définie sur $N_1 \boxplus \cdots \boxplus N_s$, elle s'étend naturellement sur $\mathbb{Q}^n := V$ tout entier. Soient $x = x_1+\cdots+x_s$ et $y = y_1+\cdots+y_s \in V$. Montrons d'abord que $\sigma \in O(V)$. Il suffit de voir que $\gamma_i(\sigma_i(x_i),\sigma_i(y_i)) = \gamma_i(x_i,y_i)$ pour tout $i = 1,\ldots,s$. Cela est évident :

$$\begin{aligned}\gamma_i(x_i,y_i) &= \frac{1}{n_i}\operatorname{Tr}_{n_i}(k_i(x_i,y_i))\\ &= \frac{1}{n_i}\operatorname{Tr}_{n_i}(k_i(\sigma_i(x_i),\sigma_i(y_i)))\\ &= \gamma_i(\sigma_i(x_i),\sigma_i(y_i)).\end{aligned}$$

Soit $N \in \mathscr{L}$. Puisque N est unimodulaire et indécomposable, $\sigma(N)$ l'est aussi.

Montrons que $p_i(\sigma(N)) = (N_i)_{\gamma_i}^{\#}$, pour tout $i = 1,\ldots,s$. C'est évident, car $p_i(\sigma(N)) = \sigma_i(p_i(N)) = \sigma_i((N_i)_{\gamma_i}^{\#}) = (N_i)_{\gamma_i}^{\#}$. La dernière égalité demande néanmoins une petite vérification utilisant le fait que $\sigma_i \in O(N_i,\gamma_i)$.

Voyons que $\sigma(N)\cap V_i = N_i$, où $V_i = N_i \otimes_{\mathbb{Z}} \mathbb{Q}$, pour tout $i = 1,\ldots,s$. Soient $y \in \sigma(N)\cap N_i$ et $x = x_1+\cdots+x_s \in N$ tel que $\sigma(x) = y$. Puisque $y \in V_i$, et que $\sigma(V_j) = V_j$ pour tout j, on en déduit que $x = x_i \in V_i \cap N = N_i$, par hypothèse. Ainsi, $y \in \sigma(N_i) = N_i$. Réciproquement, soit $y \in N_i$. De $\sigma(N_i) = N_i$, il suit que $y = \sigma(x)$, avec $x \in N_i \subset N$. Donc $y \in \sigma(N)\cap V_i$.

Finalement, $t(\sigma(N)) = \sigma(t(N)) = \sigma(N)$ par définition de t.

Terminons la démonstration : notons " $\bullet$ " l'action de H sur $\mathscr{L}$. Il existe $K_1,\ldots,K_l \in \mathscr{L}$ tels que

$$\overline{\mathscr{L}} = H\bullet K_1 \sqcup \cdots \sqcup H \bullet K_l.$$

Posons $H_i = \{\sigma \in H \mid \sigma(K_i) = K_i\}$ pour tout $i = 1, \ldots, l$. C'est un sous-groupe de $O(K_i)$. On a évidemment $|H| = |H_i| \cdot |H \bullet K_i|$ pour tout $i = 1, \ldots, l$. D'où :

$$\sum_{\overline{N} \in \overline{\mathscr{L}}} \frac{1}{|O(N)|} \leq \sum_{i=1}^{l} \frac{1}{|O(K_i)|} \leq \sum_{i=1}^{l} \frac{1}{|H_i|} = \sum_{i=1}^{l} \frac{|H \bullet K_i|}{|H|} = \frac{|\overline{\mathscr{L}}|}{|H|}.$$

❄

Définition 1.6.3

Soit $F = \Phi_{n_1}^{r_1} \cdots \Phi_{n_s}^{r_s}$. Rappelons que $\mathscr{E}(F)$ est l'ensemble de F-réseaux de $\mathbb{Q}^n$, et que $\overline{\mathscr{E}}(F) = \mathscr{E}(F)/\overset{\mathbb{Z}}{\simeq}$. Soit $i = 1, \ldots, s$. On rappelle aussi que $a(i) = a(F, i)$ est le plus petit entier positif a, tel qu'il existe $g, h \in \mathbb{Z}[x]$ avec $g\Phi_{n_i} + h\frac{f}{\Phi_{n_i}} = a$, où $f = \Phi_{n_1} \cdots \Phi_{n_s}$ (voir le corollaire 1.3.3).

Pour $i = 1, \ldots, s$, posons $\mathfrak{D}_i = \mathfrak{D}_i(F) = \{d_1^{(i)}, \ldots, d_{l_i}^{(i)}\}$, l'ensemble des diviseurs de $\mathrm{Res}(\Phi_{n_i}, \frac{f}{\Phi_{n_i}})^{r_i}$ différents de 1. Si de plus, $j = 1, \ldots, l_i$, on note $A'_{i,j}$ l'ensemble des r_i-uplets d'idéaux $(\mathfrak{a}'_1, \ldots, \mathfrak{a}'_{r_i})$ de $\mathbb{Z}[\zeta_{n_i}]$ tels que

a) $\mathfrak{a}'_1 \supset \cdots \supset \mathfrak{a}'_{r_i}$

b) $\prod_{k=1}^{r_i} |\mathbb{Z}[\zeta_{n_i}]/\mathfrak{a}'_k| = d_j^{(i)}$

c) $\mathfrak{a}'_k \supset a(i)\mathbb{Z}[\zeta_{n_i}]$ pour tout $k = 1, \ldots, r_i$.

On définit encore $A_{i,j}$ l'ensemble des r_i-uplets d'idéaux $(\mathfrak{a}_i, \ldots, \mathfrak{a}_{r_i})$ de $\mathbb{Z}[\zeta_{n_i}]$ tels que

$$\frac{1}{n_i}\mathscr{D}_{n_i}(\mathfrak{a}_i, \ldots, \mathfrak{a}_{r_i}) \in A'_{i,j}.$$

Enfin, pour tout $i = 1, \ldots, s$, définissons $\mathscr{G}(F, d^{(1)}, \ldots, d^{(s)})$ comme étant les s-uplets de genres (à isométrie près) $(\mathscr{G}_{N_1}, \ldots, \mathscr{G}_{N_s})$ de formes hermitiennes $(N_1, k_1), \ldots, (N_s, k_s)$ chacune sur $\mathbb{Z}[\zeta_{n_i}]$, de dimension r_i, et telles que

a) $((N_1, k_1), \ldots, (N_s, k_s)) \in \mathscr{F}(F)$.

b) Les facteurs invariants de N_i dans $(N_i)_{k_i}^{\#}$ sont dans $A_{i,j}$, avec j tel que $d^{(i)} = d_j^{(i)}$.

Le lemme suivant est en quelque sorte la clef de voûte de ce chapitre :

Lemme 1.6.4

Soit $F = \Phi_{n_1}^{r_1} \cdots \Phi_{n_s}^{r_s}$, avec n_i distinct d'une puissance de 2, pour tout $i = 1, \ldots s$. On a les résultats suivants :

a) $\mathscr{G}(F, d^{(1)}, \ldots, d^{(s)})$ est fini pour tout $d^{(i)} \in \mathfrak{D}_i$, $i = 1, \ldots s$.

b) Quel que soit $(M, \beta) \in \overline{\mathscr{E}}(F)$, on a

$$(\mathscr{G}_{M_1}, \ldots, \mathscr{G}_{M_s}) \in \bigsqcup_{d^{(1)} \in \mathfrak{D}_1} \cdots \bigsqcup_{d^{(s)} \in \mathfrak{D}_s} \mathscr{G}(F, d^{(1)}, \ldots, d^{(s)})$$

où, $M_i = M \cap W_i$, avec $W_i = \frac{f}{\Phi_{n_i}}(t)(W)$, et $W = M \otimes \mathbb{Q}$, et que M_i est muni de la forme hermitienne h_i définie par $h_i(x, y) = \sum_{j=0}^{n_i - 1} \beta_i(t^{-j}(x), y)\zeta_{n_i}^j$, avec $\beta_i = \beta|_{W_i}$.

Démonstration :

Démontrons a) : pour tout $i = 1, \ldots, s$, on sait que $d^{(i)} = d_j^{(i)}$ pour un certain $j = 1, \ldots, l_i$. Soit $(\mathscr{G}_{N_1}, \ldots, \mathscr{G}_{N_s}) \in \mathscr{G}(F, d^{(1)}, \ldots, d^{(s)})$. Fixons $i = 1, \ldots, s$. Soient $\mathfrak{a}_i \supset \cdots \supset \mathfrak{a}_{r_i}$ les facteurs invariants de N_i dans $(N_i)_{k_i}^{\#}$. Par définition, on a que $(\mathfrak{a}_i, \ldots, \mathfrak{a}_{r_i}) \in A_{i,j}$ qui est un ensemble fini. D'autre part, (N_i, k_i) est totalement défini positif, donc la signature relativement à n'importe quelle place infinie est

$(r_i, 0)$. Le théorème 1.5.5 nous apprend que le nombre de genre associé à $(r_i, (r_i,0), \ldots, (r_i,0), \mathfrak{a}_i, \ldots, \mathfrak{a}_{r_i})$ est fini, donc $\mathscr{G}(F, d^{(1)}, \ldots, d^{(s)})$ l'est aussi.

Démontrons b) : soit $i = 1, \ldots, s$. Le $\mathbb{Z}[\zeta_{n_i}]$-module hermitien (M_i, h_i) est totalement défini positif en vertu du corollaire 1.2.7. La proposition 1.2.4 nous apprend que la forme $\frac{1}{n_i}\operatorname{Tr}_{n_i} \circ h_i$ n'est autre que β_i, et on sait que $M_i \subset (M_i)^{\#}_{\beta_i}$. D'autre part, le théorème 1.3.9 nous dit que $d^{(i)} := |M_i^{\#}/M_i|$ divise $\operatorname{Res}(\Phi_{n_i}, \frac{f}{\Phi_{n_i}})^{r_i}$, et le corollaire 1.3.3 nous assure que $a(i)(M_i)^{\#}_{\beta_i} \subset M_i$. Tous ces résultats nous montrent alors que les facteurs invariants de M_i dans $(M_i)^{\#}_{\beta_i}$, vus comme $\mathbb{Z}[\zeta_{n_i}]$-réseaux de W_i, sont dans $A'_{i,j}$, et par suite, ceux de M_i dans $(M_i)^{\#}_{h_i}$ sont dans $A_{i,j}$, en vertu du théorème 1.3.12 qui nous dit que $(M_i)^{\#}_{h_i} = \frac{1}{n_i}\mathscr{D}_{n_i}(M_i)^{\#}_{\beta_i}$. En résumé, $(\mathscr{G}_{M_1}, \ldots, \mathscr{G}_{M_s}) \in \mathscr{G}(F, d^{(1)}, \ldots, d^{(s)})$ avec $d^{(i)} \in \mathfrak{D}_i$ pour tout $i = 1, \ldots, s$. ❄

Définition 1.6.5

Soit (N, k) une forme hermitienne sur $\mathbb{Z}[\zeta_m]$ totalement définie positive. On note :

$$\omega(N) = \sum_{L \in \mathscr{G}_N} \frac{1}{|U(L)|}$$

où $\mathscr{G}_N$ est le genre de (N, k) à isométries près et $U(L)$ est le groupe unitaire de L. Cette somme est appelée *masse de* $\mathscr{G}_N$.

Voici le théorème central de ce chapitre :

Théorème 1.6.6

Soit $F = \Phi_{n_1}^{r_1} \cdots \Phi_{n_s}^{r_s}$, avec n_i distinct d'une puissance de 2, pour tout $i = 1, \ldots s$. On a :

$$\sum_{M \in \overline{\mathscr{E}}(F)} \frac{1}{|O(M)|} \leq \sum_{d^{(1)} \in \mathfrak{D}_1} \cdots \sum_{d^{(s)} \in \mathfrak{D}_s} \sum_{(\mathscr{G}_{N_1}, \ldots, \mathscr{G}_{N_s}) \in \mathscr{G}_{(F, d^{(1)}, \ldots, d^{(s)})}} |\overline{\mathscr{L}}_{(N_1, \ldots, N_s)}| \cdot \omega(N_1) \cdots \omega(N_s).$$

Démonstration :

L'ensemble $\overline{\mathscr{E}}(F)$ est fini. Mettons que $\overline{\mathscr{E}}(F) = \{\overline{M^{(1)}}, \ldots, \overline{M^{(k)}}\}$. On a :

$$\begin{aligned}
\sum_{M \in \overline{\mathscr{E}}(F)} \frac{1}{|O(M)|} &= \sum_{i=1}^{k} \frac{1}{|O(M^{(i)})|} \\
&\leq \sum_{i=1}^{k} \sum_{N \in \overline{\mathscr{L}}(M_1^{(i)}, \ldots, M_s^{(i)})} \frac{1}{|O(N)|} \\
&\overset{\text{(Lemme 1.6.2)}}{\leq} \sum_{i=1}^{k} \frac{|\overline{\mathscr{L}}_{(M_1^{(i)}, \ldots, M_s^{(i)})}|}{|U(M_1^{(i)}, h_1^{(i)})| \cdots |U(M_s^{(i)}, h_s^{(i)})|} \\
&\leq \sum_{i=1}^{k} \sum_{(L_1, \ldots, L_s) \in (\mathscr{G}_{M_1^{(i)}}, \ldots, \mathscr{G}_{M_s^{(i)}})} \frac{|\overline{\mathscr{L}}_{(M_1^{(i)}, \ldots, M_s^{(i)})}|}{|U(L_1^{(i)}, k_1^{(i)})| \cdots |U(L_s^{(i)}, k_s^{(i)})|} \\
&= \sum_{i=1}^{k} |\overline{\mathscr{L}}_{(M_1^{(i)}, \ldots, M_s^{(i)})}| \cdot \omega(M_1^{(i)}) \cdots \omega(M_s^{(i)}) \\
&\overset{\text{(Lemme 1.6.4)}}{\leq} \sum_{d^{(1)} \in \mathfrak{D}_1} \cdots \sum_{d^{(s)} \in \mathfrak{D}_s} \sum_{(\mathscr{G}_{N_1}, \ldots, \mathscr{G}_{N_1}) \in \mathscr{G}_{(F, d^{(1)}, \ldots, d^{(s)})}} |\overline{\mathscr{L}}_{(N_1, \ldots, N_s)}| \cdot \omega(N_1) \cdots \omega(N_s).
\end{aligned}$$

❄

Nous allons maintenant donner un raffinement du théorème précédent dans le cas où $F = \Phi_{n_1}^{r_1}\Phi_{n_2}^{r_2}$. Dans ce cas, nous avons obtenu des résultats supplémentaires au paragraphe 4, et nous allons les introduire dans la définition suivante pour obtenir un théorème un peu plus fort.

Définition 1.6.7

Supposons que $F = \Phi_{n_1}^{r_1}\Phi_{n_2}^{r_2}$, toujours avec des n_i qui ne sont pas des puissances de 2. Sans limiter la généralité, supposons que $r_1 \leq r_2$. Dans ce cas, selon les notations de la définition 1.6.3, on pose $\mathfrak{D}_1 = \mathfrak{D}$.

Soit $d \in \mathfrak{D}$. On définit A'_d comme étant l'ensemble des $2r_2$-uplets d'idéaux $(\mathfrak{a}_1, \ldots, \mathfrak{a}_{r_2}, \mathfrak{b}_1, \ldots, \mathfrak{b}_{r_2})$ tels que

a) $\mathfrak{a}_1 \supset \cdots \supset \mathfrak{a}_{r_2}$ et $\mathfrak{b}_1 \supset \cdots \supset \mathfrak{b}_{r_2}$

b) $\mathfrak{a}_i = \mathbb{Z}[\zeta_{n_1}]$, $\mathfrak{b}_i = \mathbb{Z}[\zeta_{n_2}]$ $\forall i > r_1$

c) $\mathbb{Z}[\zeta_{n_1}]/\mathfrak{a}_j \simeq \mathbb{Z}[\zeta_{n_2}]/\mathfrak{b}_j$

d) $\prod_{l=1}^{r_1} |\mathbb{Z}[\zeta_{n_1}]/\mathfrak{a}_l| = \prod_{l=1}^{r_2} |\mathbb{Z}[\zeta_{n_2}]/\mathfrak{b}_l| = d$

e) $\mathfrak{a}_k \supset a\mathbb{Z}[\zeta_{n_1}]$ et $\mathfrak{b}_l \supset a\mathbb{Z}[\zeta_{n_2}]$ avec $a = a(F,1) = a(F,2)$ et pour tout $k, l = 1, \ldots, r_2$.

On pose A_d l'ensemble des $2r_2$-uplets d'idéaux $(\mathfrak{a}_1, \ldots, \mathfrak{a}_{r_2}, \mathfrak{b}_1, \ldots, \mathfrak{b}_{r_2})$, tels que

$$\frac{1}{n_1}\mathscr{D}_{n_1} \cdot (\mathfrak{a}_1, \ldots, \mathfrak{a}_{r_2}) \times \frac{1}{n_2}\mathscr{D}_{n_2}(\mathfrak{b}_1, \ldots, \mathfrak{b}_{r_2}) \in A'_d.$$

Enfin, soit $\mathscr{G}(F,d)$ l'ensemble des couples de genres $(\mathscr{G}_{N_1}, \mathscr{G}_{N_2})$ de formes hermitiennes (N_i, k_i) chacune sur $\mathbb{Z}[\zeta_{n_i}]$, de dimension r_i et telles que

i) $((N_1,k_1),(N_2,k_2)) \in \mathscr{T}(F)$

ii) si les facteurs invariants de N_1 dans $(N_1)_{k_1}^{\#}$ sont $\mathfrak{a}_1, \ldots, \mathfrak{a}_{r_1}$, et si ceux de N_2 dans $(N_2)_{k_2}^{\#}$ sont $\mathfrak{b}_1, \ldots, \mathfrak{b}_{r_1}$, alors $(\mathfrak{a}_1, \ldots, \mathfrak{a}_{r_2}, \mathfrak{b}_1, \ldots, \mathfrak{b}_{r_2}) \in A_d$, en ayant pris le soin de poser $\mathfrak{a}_i = \mathbb{Z}[\zeta_{n_1}]$ si $i > r_1$.

iii) les espaces $((N_1)_{\gamma_1}^{\#}/N_1, \overline{\gamma_1})$ et $((N_2)_{\gamma_2}^{\#}/N_2, \overline{\gamma_2})$ sont anti-isomorphes, et si α est cet anti-isomorphisme, le diagramme suivant commute :

$$\begin{array}{ccc} N_1^{\#}/N_1 & \xrightarrow{\alpha} & N_2^{\#}/N_2 \\ \Big\downarrow{\scriptstyle \overline{t_1}} & & \Big\downarrow{\scriptstyle \overline{t_2}} \\ N_1^{\#}/N_1 & \xrightarrow{\alpha} & N_2^{\#}/N_2 \end{array}$$

où t_i est la multiplication par ζ_{n_i} pour $i = 1, 2$.

Théorème 1.6.8

Soit $F = \Phi_{n_1}^{r_1}\Phi_{n_2}^{r_2}$. On a :

$$\sum_{\overline{M} \in \overline{\mathscr{E}}(F)} \frac{1}{|O(M)|} \leq \sum_{d \in \mathfrak{D}} \sum_{(\mathscr{G}_{N_1}, \mathscr{G}_{N_2}) \in \mathscr{G}(F,d)} |\overline{\mathscr{L}}_{(N_1,N_2)}| \cdot \omega(N_1) \cdot \omega(N_2).$$

Démonstration :

C'est un corollaire immédiat des théorèmes 1.6.6 et 1.4.1, et de la proposition 1.3.5. ❄

Finalement, suivant notre politique qui est d'aller du cas le plus général au cas le plus particulier, nous allons donner un résultat qui se rapporte au cas où $F = \Phi_n^r$ ne possède qu'un facteur irréductible.

Théorème 1.6.9

Soit $F = \Phi_n^r$, avec n différent d'une puissance de 2. On pose $\mathscr{G}(F)$ comme étant l'ensemble des genres de $\mathbb{Z}[\zeta_n]$-modules hermitiens (M, h), projectifs de rang r, dont la forme hermitienne est totalement définie positive, et dont les facteurs invariants sont $\underbrace{n \cdot \mathscr{D}_n^{-1}, \ldots, n \cdot \mathscr{D}_n^{-1}}_{r \text{ fois}}$. Le théorème 1.5.5 nous assure que $|\mathscr{G}(F)| = 1$. Alors on a :

$$\sum_{\overline{M} \in \overline{\mathscr{E}}(F)} \frac{1}{|O(M)|} \leq \omega(N) \quad \text{où } N \text{ est un représentant d'une classe de } \mathscr{G}(F).$$

Démonstration :

C'est évident, car ici on a $M_1 = \cdots = M_s = M$, pour tout $M \in \mathscr{G}(F)$. ❄

Remarque :

Le théorème est aussi vrai dans le cas où $n = 2^r$, avec $r \geq 2$. En effet, dans ce cas on a $|\mathscr{G}(F)| = 1$ ou 2. Et procédant de la même manière que dans les théorèmes précédents, on conclut. Le fait que $|\mathscr{G}(F)| = 1$ ou 2 est démontré dans ([Ha], Proposition 3.8).

CHAPITRE 2

Autour de la formule de masse pour les formes hermitiennes

Dans ce chapitre, nous allons donner explicitement la formule de masse, et nous allons fournir une myriade de petits résultats nous permettant d'affiner les calculs du chapitre 1 et de donner des résultats numériquement satisfaisants aux membres de droite des théorèmes 1.6.6 et 1.6.8.

Pour tout ce chapitre, fixons $E = \mathbb{Q}(\zeta_d)$ un corps cyclotomique. L'involution définie par la conjugaison complexe se notera $x \mapsto \overline{x}$. Soit O_E l'anneau des entiers de E, K le corps fixe pour l'involution et O_K son anneau des entiers. Le symbole $\mathfrak{p}$ dénotera toujours un idéal premier de O_K. Nous noterons $f_\mathfrak{p}$ pour le degré résiduel $[O_K/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}]$, si $p \in \mathbb{P}(\mathbb{Z})$ est tel que $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. On a $\mathfrak{p}O_E = \mathfrak{P}$, $\mathfrak{P}^2$, ou $\mathfrak{P}_1\mathfrak{P}_2$, selon que $\mathfrak{p}$ est inerte, se ramifie, ou se décompose dans O_E. Rappelons que l'on note $\tilde{E}_\mathfrak{p}$ pour $E \otimes_K K_\mathfrak{p}$, et $\tilde{O}_{E_\mathfrak{p}}$ pour $O_E \otimes_{O_K} O_{K_\mathfrak{p}}$ avec $K_\mathfrak{p}$ le complété $\mathfrak{p}$-adique de K. Nous savons aussi que :

$$\tilde{E}_\mathfrak{p} = \prod_{\mathfrak{P}|\mathfrak{p}} E_\mathfrak{P} \text{ et } \tilde{O}_{E_\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} O_{E_\mathfrak{P}}$$

où $E_\mathfrak{P}$ est le complété $\mathfrak{P}$-adique de E.

Soit (M, h) un O_E-module hermitien, projectif de rang fini. Nous écrirons toujours $M_\mathfrak{p}$ pour $M \otimes_{O_E} \tilde{O}_{E_\mathfrak{p}}$ et $h_\mathfrak{p}$ pour $h \otimes_{O_E} \tilde{O}_{E_\mathfrak{p}}$. Si W est le E-espace vectoriel $M \otimes_{O_E} E$ sur lequel h se prolonge naturellement et se note encore h, on écrit $W_\mathfrak{p}$ pour $W \otimes_E \tilde{E}_\mathfrak{p}$ et $h_\mathfrak{p}$ pour $h \otimes_E \tilde{E}_\mathfrak{p}$.

§ 1. La formule

Voici quelques définitions préalables :

Définition 2.1.1

Soient (M, h) et (N, k) deux $\tilde{O}_{E_\mathfrak{p}}$-modules hermitiens, libres de rang respectivement r et s, avec $r \geq s$, et m un entier positif. On définit $\mathcal{A}_{\mathfrak{p}^m}(M, N)$ comme étant l'ensemble des homomorphismes $\tilde{O}_{E_\mathfrak{p}}$-linéaires $u : N \longrightarrow M$ distincts modulo $\mathfrak{p}^m \tilde{O}_{E_\mathfrak{p}} M$, satisfaisant la congruence

$$h(u(x), u(y)) \equiv k(x, y) \pmod{\mathfrak{p}^m \tilde{O}_{E_\mathfrak{p}}} \quad \text{pour tout } x, y \in N.$$

Notons $A_{\mathfrak{p}^m}(M, N)$ le cardinal de cet ensemble.

Proposition 2.1.2

Soient (M, h) et (N, k) deux $\tilde{O}_{E_\mathfrak{p}}$-modules hermitiens, libres de rang respectivement r et s, avec $r \geq s$. On a

$$A_{\mathfrak{p}^{m+1}}(M, N) = p^{f_\mathfrak{p} s(2r-s)} A_{\mathfrak{p}^m}(M, N) \quad \text{avec } \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$$

si $m \geq 2 \cdot v_\mathfrak{p}(\mathfrak{a}) + 1$, avec $\mathfrak{a} = \mathfrak{a}_1 \cdots \mathfrak{a}_s$, et où $\mathfrak{a}_1 \supset \cdots \supset \mathfrak{a}_s$ sont les facteurs invariants de N dans $N_k^\#$.

Démonstration :

Cf. ([Re], Hilfsatz 5.3). ❄

Définition 2.1.3

Soit (M,h) un $\tilde{O}_{E_\mathfrak{p}}$-module hermitien, libre de rang r. Posons

$$\mathfrak{B}_\mathfrak{p}(M) = \lim_{m\to\infty} p^{-f_\mathfrak{p} r^2 m} A_{\mathfrak{p}^m}(M,M).$$

La proposition précédente assure l'existence de cette limite. Elle nous dit même mieux : la suite $\left(p^{-f_\mathfrak{p} r^2 m} A_{\mathfrak{p}^m}(M,M)\right)_{m=1}^{\infty}$ est stationnaire. Le nombre $\mathfrak{B}_\mathfrak{p}(M)$ est appelé *densité locale de M en $\mathfrak{p}$.*

Théorème 2.1.4

Soit (M,h) un O_E-module hermitien, projectif de rang n, et totalement défini positif. Rappelons que $\omega(M) = \sum_{L\in\mathscr{G}_M} \frac{1}{|U(L)|}$ où $\mathscr{G}_M$ est le genre de M. On a

$$\omega(M) = 2\cdot|d(E)|^{\frac{n(n+1)}{4}}\cdot|d(K)|^{-\frac{n}{2}}\cdot\left(\prod_{j=1}^{n}\frac{(j-1)!}{(2\pi)^j}\right)^{\frac{\varphi(d)}{2}}\cdot[M_h^\# : M]^{\frac{n}{2}}\cdot\prod_{\mathfrak{p}\in\mathbb{P}(K)}\mathfrak{B}_\mathfrak{p}(M_\mathfrak{p})^{-1}$$

où $d(E)$ et $d(K)$ sont les discriminant des extensions $E/\mathbb{Q}$ et $K/\mathbb{Q}$ respectivement.

Ce théorème s'appelle "formule de masse pour les formes hermitiennes"

Démonstration :

La démonstration de cette formule est très longue. Cf. ([Re], formule (4.5), p. 20), ([Bo], p. 112]), et ([Br], Satz VI). ❄

Pour pouvoir calculer explicitement cette formule, nous nous verrons contraints de calculer le produit $\prod_{\mathfrak{p}\in\mathbb{P}(K)}\mathfrak{B}_\mathfrak{p}(M_\mathfrak{p})^{-1}$ dans plusieurs cas (selon la ramification de $\mathfrak{p}$ et selon les facteurs invariants de $M_\mathfrak{p}$ dans $(M_\mathfrak{p})_{h_\mathfrak{p}}^\#$). Avant cela, voici un lemme bien utile, qui nous permettra de restreindre le nombre de cas :

Lemme 2.1.5

Soient (M,h) et (N,k) deux O_E-modules hermitiens, projectifs de rang n. Supposons que (M,h) et (N,k) soient dans le même genre, et qu'il existe $\lambda\in O_K$ tel que $h=\lambda h'$ avec $M\subset M_{h'}^\#$. Alors $k=\lambda k'$ avec $N\subset N_{k'}^\#$.

Démonstration :

Soient $\mathfrak{a}_1\supset\cdots\supset\mathfrak{a}_n$ les facteurs invariants de M dans $M_h^\#$, et $\mathfrak{a}'_1\supset\cdots\supset\mathfrak{a}'_n$ ceux de M dans $M_{h'}^\#$. Puisque $\lambda M_h^\# = M_{h'}^\#$, on a $\mathfrak{a}_i=\lambda\mathfrak{a}'_i$ pour tout $i=1,\ldots,n$. D'autre part, soient $\mathfrak{b}_1\supset\cdots\supset\mathfrak{b}_n$ les facteurs invariants de N dans $N_k^\#$. Par hypothèse, pour tout $\mathfrak{p}\in\mathbb{P}(K)$, on a $(N,k_\mathfrak{p}) \overset{\tilde{O}_{E_\mathfrak{p}}}{\simeq} (M,h_\mathfrak{p})$. Fixons $i=1,\ldots,n$. En vertu des corollaires 1.5.10 et 1.5.12 ainsi que du théorème 1.5.17, on trouve que $(\mathfrak{a}_i)_\mathfrak{p}=(\mathfrak{b}_i)_\mathfrak{p}$ pour tout $\mathfrak{p}\in\mathbb{P}(K)$. Donc, $\mathfrak{a}_i=\mathfrak{b}_i$, ou encore $\mathfrak{b}_i=\lambda\mathfrak{b}'_i$ avec $\mathfrak{b}'_i\subset O_E$. Ainsi, en posant $k'=\frac{1}{\lambda}k$, on remarque que $N_{k'}^\# = \lambda N_k^\# \supset N$. ❄

§ 2. Quelques calculs de densités locales

Dans ce paragraphe, nous allons supposer que $\mathfrak{p}$ est non dyadique (i.e. $2\notin\mathfrak{p}$), et qu'il ramifie ou est inerte dans O_E. Dans ce cas, $\tilde{E}_\mathfrak{p}=E_\mathfrak{P}$ est un corps local. L'idéal maximal de $\tilde{O}_{E_\mathfrak{p}}$ se note encore $\mathfrak{P}$. Il est engendré par un élément que l'on note π. Le corps $K_\mathfrak{p}$ est un sous-corps de $\tilde{E}_\mathfrak{p}$ d'indice 2. L'idéal maximal de $O_{K_\mathfrak{p}}$, noté encore $\mathfrak{p}$ est engendré par un élément noté π. Si $\mathfrak{p}$ est inerte, on peut choisir $\pi=\pi$. Si $\mathfrak{p}$ se ramifie, on peut choisir $\pi=\pi^2$. Dans le cas ramifié, $f_\mathfrak{p}$ vaut 1. En effet, nous avons vu dans le lemme 1.5.2 que $E=\mathbb{Q}(\zeta_{p^k})$ ou $E=\mathbb{Q}(\zeta_{2p^k})$, avec $p\in\mathbb{P}(\mathbb{Z})$, et dans ce cas, p se ramifie totalement dans O_E. Evidemment, nous ne pouvons rien dire sur $f_\mathfrak{p}$ dans le cas inerte.

Proposition 2.2.1

Soit (M,h) un $\tilde{O}_{E_\mathfrak{p}}$-module hermitien, libre de dimension n. Supposons que $h = \pi^m h'$, avec $M \subset M_{h'}^{\#}$ et $m \geq 1$. Alors, si (M,h') est symbolisé par M', et que l est un entier strictement positif, on a $A_{\mathfrak{p}^{l+m}}(M,M) = p^{2f_\mathfrak{p}mn^2} A_{\mathfrak{p}^l}(M',M')$. De cette formule, on déduit que

$$\boxed{\mathfrak{B}_\mathfrak{p}(M) = p^{f_\mathfrak{p}mn^2}\mathfrak{B}_\mathfrak{p}(M')}.$$

Démonstration :

Soit

$$\psi : \mathcal{A}_{\mathfrak{p}^{l+m}}(M,M) \longrightarrow \mathcal{A}_{\mathfrak{p}^l}(M',M')$$
$$u \pmod{\mathfrak{p}^{l+m}} \longmapsto u \pmod{\mathfrak{p}^l}.$$

L'application ψ est surjective. Plus précisément, si $u \in \mathcal{A}_{\mathfrak{p}^l}(M',M')$, on vérifie facilement que l'ensemble des $u + \pi^l v$, où v est n'importe quel endomorphisme modulo $\mathfrak{p}^m\tilde{O}_{E_\mathfrak{p}}$, est l'ensemble des u' tels que $\psi(u') = u$. Puisque $|\tilde{O}_{E_\mathfrak{p}}/\mathfrak{p}^m\tilde{O}_{E_\mathfrak{p}}| = |O_{K_\mathfrak{p}}/\mathfrak{p}^m|^2 = p^{2f_\mathfrak{p}m}$, le nombre de v, qui est aussi le nombre de u' vaut $p^{2f_\mathfrak{p}mn^2}$. Ainsi, $A_{\mathfrak{p}^{l+m}}(M,M) = p^{2f_\mathfrak{p}mn^2}A_{\mathfrak{p}^l}(M',M')$.

Soit l assez grand. On a

$$\mathfrak{B}_\mathfrak{p}(M) = \frac{A_{\mathfrak{p}^{l+m}}(M,M)}{p^{f_\mathfrak{p}(l+m)n^2}} = \frac{p^{2f_\mathfrak{p}mn^2}A_{\mathfrak{p}^l}(M',M')}{p^{f_\mathfrak{p}mn^2}p^{f_\mathfrak{p}ln^2}} = p^{f_\mathfrak{p}mn^2}\mathfrak{B}_\mathfrak{p}(M').$$

❄

Lemme 2.2.2

Soit (M,h) un $\tilde{O}_{E_\mathfrak{p}}$-module hermitien, libre de rang n. Supposons que (M,h) soit $\mathfrak{P}^m$-modulaire, avec $m \geq 0$ (pour une définition de $\mathfrak{P}^m$-modulaire, voir la définition 1.5.7). Soit (N,k) un autre $\tilde{O}_{E_\mathfrak{p}}$-module hermitien, libre de rang n.

a) Supposons que $\mathfrak{p}$ soit inerte dans O_E. Nous savons, en vertu du théorème 1.5.9 qu'il existe une base $e_1,\ldots,e_n$ de M telle que, relativement à cette base, la matrice de h, notée H_M, vaut $(\not{\pi}^m) \oplus \cdots \oplus (\not{\pi}^m)$. Supposons qu'il existe $f_1,\ldots,f_n$, une base de N, telle que la congruence suivante est satisfaite :

$$H_M \equiv H_N \pmod{\mathfrak{p}^{m+1}\tilde{O}_{E_\mathfrak{p}}}.$$

Alors $(M,h) \overset{\tilde{O}_{E_\mathfrak{p}}}{\simeq} (N,k)$.

b) Supposons que $\mathfrak{p}$ ramifie dans O_E. Nous savons, en vertu du théorème 1.5.17, qu'il existe une base $e_1,\ldots,e_n$ de M telle que, relativement à cette base, la matrice de h vaut $(\pi^{\frac{m}{2}}) \oplus \cdots \oplus (\pi^{\frac{m}{2}}) \oplus (\lambda \cdot \pi^{\frac{m}{2}})$, avec $\lambda \in U(O_{K_\mathfrak{p}})$, ou alors $H(m) \oplus \cdots \oplus H(m)$, avec $H(m) = \begin{pmatrix} 0 & \not{\pi}^m \\ \not{\pi}^m & 0 \end{pmatrix}$, selon la parité de m. Supposons qu'il existe $f_1,\ldots,f_n$, une base de N, telle que la congruence suivante est satisfaite :

$$H_M \equiv H_N \pmod{\mathfrak{p}^{[\frac{m}{2}]+1}\tilde{O}_{E_\mathfrak{p}}}$$

où H_N est la matrice de k relativement à cette base, et $[x]$ dénote la partie entière du nombre réel x. Alors, à nouveau, $(M,h) \overset{\tilde{O}_{E_\mathfrak{p}}}{\simeq} (N,k)$.

Démonstration :

a) Soit $x = \sum_{i=1}^n x_i f_i$ un élément primitif de N. Il est clair que $k(x,y) \in \mathfrak{P}^m$, pour tout $y \in N$. En effet, $k(f_i,f_j) \equiv h(e_i,e_j) \pmod{\mathfrak{p}^{m+1}\tilde{O}_{E_\mathfrak{p}}}$; ainsi, $v_\mathfrak{p}(k(f_i,f_j)) \geq m$ pour tout $i,j = 1,\ldots,n$. D'autre

part, puisque x est primitif, il existe $i \in \{1,\dots,n\}$, tel que $x_i \in U(\tilde{O}_{E_\mathfrak{p}})$. Calculons $v_{\mathfrak{P}}(k(x,f_i))$. On a :

$$v_{\mathfrak{P}}(k(x_i f_i, f_i)) = v_{\mathfrak{P}}(k(f_i,f_i)) = v_{\mathfrak{P}}(k(e_i,e_i)) = m.$$

D'autre part, $v_{\mathfrak{P}}(k(\sum_{j\neq i} x_j f_j, f_i)) \geq m+1$. Donc

$$v_{\mathfrak{P}}(k(x,f_i)) = \inf(v_{\mathfrak{P}}(k(x_i f_i,f_i)), v_{\mathfrak{P}}(k(\sum_{j\neq i} x_j f_j, f_i))) = m.$$

Donc, (N,k) est $\mathfrak{P}^m$-modulaire. Nous avons vu au théorème 1.5.9 que H_N peut être mise sous une forme canonique (la même que H_M), donc $(M,h) \overset{\tilde{O}_{E_\mathfrak{p}}}{\simeq} (N,k)$.

b) Comme pour la partie a), il est facile de voir que (N,k) est $\mathfrak{P}^m$-modulaire. Donc, si m est impair, H_N peut être mise sous une forme canonique, autrement dit $(M,h) \overset{\tilde{O}_{E_\mathfrak{p}}}{\simeq} (N,k)$. Si m est pair, ça se complique. Nous n'avons, nous le savons, pas de forme canonique. Pour achever la démonstration, il reste à montrer que $\det(M,h) = \det(N,k)$. Cela se fait au moyen du lemme de Hensel. Nous savons que $\det(M,h) = \det(H_M) = \lambda\pi^{\frac{mn}{2}}$. Pour tout $i = 1,\dots,n-1$, on a $k(f_i,f_i) = \pi^{\frac{m}{2}} + \pi^{\frac{m}{2}+1}\alpha_i$, et $k(f_n,f_n) = \lambda\pi^{\frac{m}{2}} + \pi^{\frac{m}{2}+1}\alpha_n$, avec $\alpha_i, \alpha_n \in O_{K_\mathfrak{p}}$. Si $i \neq j$, alors $k(f_i,f_j)$ est un multiple de $\pi^{\frac{m}{2}+1}$. Donc $\det(H_N) = \lambda\pi^{\frac{mn}{2}} + \pi^{\frac{mn}{2}+1}\alpha = \pi^{\frac{mn}{2}}(\lambda+\pi\alpha)$ pour un α dans $O_{K_\mathfrak{p}}$. Posons $\eta = \frac{\lambda+\pi\alpha}{\lambda} = 1+\pi\frac{\alpha}{\lambda} \equiv 1 \pmod{\mathfrak{p}}$. Le lemme de Hensel nous apprend que η est un carré de $U(O_{K_\mathfrak{p}})$; en particulier, c'est la norme d'un élément de $U(\tilde{O}_{E_\mathfrak{p}})$. Donc, $\det(M,h) = \det(N,k)$. ❄

Lemme 2.2.3

Soient (M,h) et (N,k) des $\tilde{O}_{E_\mathfrak{p}}$-modules hermitiens, libres de rang n_1 et n_2 respectivement, tels que $n_1 \geq n_2 \geq 1$. Posons H_M et H_N les matrices de h et de k. Supposons que (N,k) et $m \geq 1$ possèdent la propriété suivante : si (N',k') est un $\tilde{O}_{E_\mathfrak{p}}$-module hermitien, libre de rang n_2, dont une matrice $H_{N'}$ satisfait la congruence $H_N \equiv H_{N'} \pmod{\mathfrak{p}^m \tilde{O}_{E_\mathfrak{p}}}$, alors $(N,k) \overset{\tilde{O}_{E_\mathfrak{p}}}{\simeq} (N',k')$ (typiquement, le (M,h) et le $m+1$ du lemme précédent satisfont cette propriété). Alors,

$$A_{\mathfrak{p}^{m+1}}(M,N) = p^{f_\mathfrak{p} n_2(2n_1-n_2)} A_{\mathfrak{p}^m}(M,N).$$

Démonstration :

La démonstration de ce fait se trouve dans ([Ban], Proposition 5.4, p.23) pour le cas ramifié. Le cas inerte se démontre exactement de la même manière. ❄

Lemme 2.2.4

Soit (M,h) un $\tilde{O}_{E_\mathfrak{p}}$-module hermitien, libre de rang n. Supposons que $M = M_1 \boxplus \cdots \boxplus M_l$ est une décomposition de Jordan de M. Autrement dit, pour tout $i = 1,\dots,l$, chacun des $(M_i, h|_{M_i})$ est $\mathfrak{P}^{m_i}$-modulaire, de dimension n_i, et $m_1 < \cdots < m_l$. Supposons encore que $m_1 = 0$ ou 1 si $\mathfrak{p}$ se ramifie dans O_E, et $m_1 = 0$ si $\mathfrak{p}$ est inerte dans O_E. Alors

$$A_{\mathfrak{p}^m}(M,M) = p^{f_\mathfrak{p} m_1 n_1 (n-n_1)} A_{\mathfrak{p}^m}(M,M_1) A_{\mathfrak{p}^m}(M_2 \boxplus \cdots \boxplus M_l, M_2 \boxplus \cdots \boxplus M_l) \text{ pour tout } m \geq 1.$$

Démonstration :

La démonstration se trouve dans ([Ban], Proposition 5.5, p.24) dans le cas ramifié, et le cas inerte se démontre de manière identique. ❄

Le théorème qui va suivre est bien utile. Il nous donne une formule de récurrence pour la valeur de $\mathfrak{B}_{\mathfrak{p}}(M)$. Ainsi, il suffira de connaître $\mathfrak{B}_{\mathfrak{p}}(M)$ dans certains cas particuliers. Si (M,h) est tel que $h=\pi^m h'$, avec $m\geq 1$, et $M\subset M_{h'}^{\#}$, nous avons vu dans la proposition 2.2.1 que $\mathfrak{B}_{\mathfrak{p}}(M)=p^{f_{\mathfrak{p}}mn^2}\mathfrak{B}_{\mathfrak{p}}(M')$, par conséquent, nous pouvons supposer que h ne soit pas un multiple de π.

Théorème 2.2.5

Soit (M,h) un $\tilde{O}_{E_{\mathfrak{p}}}$-module hermitien, libre de rang n. Notons $M=M_1\boxplus\cdots\boxplus M_l$ la décomposition de Jordan de (M,h), toujours avec la convention que chaque M_i est $\mathfrak{P}^{m_i}$-modulaire, que $m_1<\cdots<m_l$, et que la dimension des M_i vaut n_i. Grâce à la remarque qui précède le théorème, nous pouvons supposer que $m_1=0$ ou 1 dans le cas ramifié, et que $m_1=0$ dans le cas inerte.

a) *Supposons que $\mathfrak{p}$ ramifie dans O_E. Posons $m_2=2m_2'+\epsilon(m_2)$, avec $\epsilon(m_2)=\begin{cases}1 & \text{si } m_2 \text{ est impair}\\ 0 & \text{sinon.}\end{cases}$. Il est clair que si on définit $M_2'\boxplus\cdots\boxplus M_l':=(M_2,h_2')\boxplus\cdots\boxplus(M_l,h_l')$, avec $h_i=\pi^{m_2'}h_i'$, on a $M_i\subset(M_i)_{h_i'}^{\#}$ pour tout $i=1,\ldots,l$, et M_2' est $\mathfrak{P}^{\epsilon(m_2')}$-modulaire. Sous ces hypothèses et conventions, on a les résultats suivants :*

i) supposons que $(m_1,m_2)\neq(0,1)$, alors

$$\boxed{\mathfrak{B}_{\mathfrak{p}}(M)=p^{m_2'(n-n_1)^2+m_1n_1(n-n_1)}\,\mathfrak{B}_{\mathfrak{p}}(M_1)\,\mathfrak{B}_{\mathfrak{p}}(M_2'\boxplus\cdots\boxplus M_l').}$$

ii) Supposons que $(m_1,m_2)=(0,1)$, alors

$$\boxed{\mathfrak{B}_{\mathfrak{p}}(M)=\mathfrak{B}_{\mathfrak{p}}(M_2)^{-1}\,\mathfrak{B}_{\mathfrak{p}}(M_1\boxplus M_2)\,\mathfrak{B}_{\mathfrak{p}}(M_2\boxplus\cdots\boxplus M_l).}$$

b) *Considérons le cas inerte. Ici, on définit $M_2'\boxplus\cdots\boxplus M_l':=(M_2,h_2')\boxplus\cdots\boxplus(M_l,h_l')$, avec $h_i=\pi^{m_2}h_i'$. Dans ce cas, M_2' est unimodulaire, et $M_i\subset(M_i)_{h_i'}^{\#}$ pour tout $i=1,\ldots,l$. On a le résultat suivant :*

$$\boxed{\mathfrak{B}_{\mathfrak{p}}(M)=p^{f_{\mathfrak{p}}m_2(n-n_1)^2}\,\mathfrak{B}_{\mathfrak{p}}(M_1)\,\mathfrak{B}_{\mathfrak{p}}(M_2'\boxplus\cdots\boxplus M_l').}$$

Démonstration :

Posons $\mu=2(m_1+\cdots+m_l)$. Dans tous les cas, en vertu du théorème 2.1.4, on a $\mathfrak{B}_{\mathfrak{p}}(M)=\dfrac{A_{\mathfrak{p}^{\mu+1}}(M,M)}{p^{f_{\mathfrak{p}}(\mu+1)n^2}}$. D'autre part, le lemme 2.2.4 nous apprend que

$$A_{\mathfrak{p}^m}(M,M)=p^{f_{\mathfrak{p}}m_1n_1(n-n_1)}\,A_{\mathfrak{p}^m}(M,M_1)\,A_{\mathfrak{p}^m}(M_2\boxplus\cdots\boxplus M_l,M_2\boxplus\cdots\boxplus M_l)\text{ pour tout } m\geq 1.$$

Finalement, le lemme 2.2.2 , et le lemme 2.2.3 itéré μ fois nous montrent que

$$A_{\mathfrak{p}^{\mu+1}}(M,M_1)=p^{f_{\mathfrak{p}}\mu n_1(2n-n_1)}A_{\mathfrak{p}}(M,M_1).$$

Démontrons la partie i) de a) : dans ce cas, nous savons que $m_2\geq 2$. Nous affirmons alors que $A_{\mathfrak{p}}(M,M_1)=p^{2n_1(n-n_1)}A_{\mathfrak{p}}(M_1,M_1)$. En effet, soit $u\in A_{\mathfrak{p}}(M,M_1)$. L'application u est représentée par une matrice $U=\begin{pmatrix}\overbrace{U_1}^{n_1}\\ U_2\end{pmatrix}\begin{matrix}\}n_1\\ \}n-n_1\end{matrix}\in \mathrm{M}_{n\times n_1}(\tilde{O}_{E_{\mathfrak{p}}})$ telle que $\overline{U}^tH_MU\equiv H_{M_1}\pmod{\mathfrak{p}\tilde{O}_{E_{\mathfrak{p}}}}$. Dans notre cas, nous avons que $\mathfrak{p}\tilde{O}_{E_{\mathfrak{p}}}=\mathfrak{P}^2$. Donc, $H=H_{M_1}\oplus H_{M_2}\oplus\cdots\oplus H_{M_l}\equiv\begin{pmatrix}H_{M_1}&0\\0&0\end{pmatrix}\pmod{\mathfrak{P}^2}$, puisque $m_2\geq 2$. On en déduit que $\overline{U}^tH_MU\equiv\overline{U_1}^tH_{M_1}U_1\equiv H_{M_1}\pmod{\mathfrak{P}^2}$, et donc que $U_1\in\mathcal{A}_{\mathfrak{p}}(M_1,M_1)$. Par suite, $A_{\mathfrak{p}}(M,M_1)=p^{2n_1(n-n_1)}A_{\mathfrak{p}}(M_1,M_1)$.

On vérifie aussi, grâce à la proposition 2.2.1, que

$A_{\mathfrak{p}^{k+m_2'}}(M_2 \boxplus \cdots \boxplus M_l, M_2 \boxplus \cdots \boxplus M_l) = p^{2m_2'(n-n_1)^2} A_{\mathfrak{p}^k}(M_2' \boxplus \cdots \boxplus M_l', M_2' \boxplus \cdots \boxplus M_l')$ pour tout k positif.

Forts de tous ces résultats, nous sommes maintenant capables de calculer $\mathfrak{B}_{\mathfrak{p}}(M)$. Allons-y :

$$\begin{aligned}\mathfrak{B}_{\mathfrak{p}}(M) &= p^{-(\mu+1)n^2+m_1n_1(n-n_1)+\mu n_1(2n-n_1)+2n_1(n-n_1)+2m_2'(n-n_1)^2} \\ &\quad \cdot p^{n_1^2+(n-n_1)^2(\mu+1-m_2')} \cdot \frac{A_{\mathfrak{p}}(M_1,M_1)}{p^{n_1^2}} \cdot \frac{A_{\mathfrak{p}^{\mu+1-m_2'}}(M_2' \boxplus \cdots \boxplus M_l', M_2' \boxplus \cdots \boxplus M_l')}{p^{(n-n_1)^2(\mu+1-m_2')}} \\ &= p^{m_2'(n-n_1)^2+m_1n_1(n-n_1)} \mathfrak{B}_{\mathfrak{p}}(M_1) \mathfrak{B}_{\mathfrak{p}}(M_2' \boxplus \cdots \boxplus M_l').\end{aligned}$$

Démontrons la partie ii) de a) : le lemme 2.2.4 nous affirme que $A_{\mathfrak{p}^3}(M_1 \boxplus M_2, M_1) = \frac{A_{\mathfrak{p}^3}(M_1 \boxplus M_2, M_1 \boxplus M_2)}{A_{\mathfrak{p}^3}(M_2, M_2)}$. D'autre part, le lemme 2.2.3 nous apprend que $A_{\mathfrak{p}^3}(M_1 \boxplus M_2, M_1) = p^{2n_1(2(n_1+n_2)-n_1)} A_{\mathfrak{p}}(M_1 \boxplus M_2, M_1)$. D'où,

$$A_{\mathfrak{p}}(M_1 \boxplus M_2, M_1) = p^{-2n_1(2(n_1+n_2)-n_1)} \frac{A_{\mathfrak{p}^3}(M_1 \boxplus M_2, M_1 \boxplus M_2)}{A_{\mathfrak{p}^3}(M_2, M_2)}.$$

En reprenant le raisonnement de la partie i), on voit facilement que

$$A_{\mathfrak{p}}(M, M_1) = p^{2(n-(n_1+n_2)n_1} A_{\mathfrak{p}}(M_1 \boxplus M_2, M_1).$$

A nouveau, nous voilà en mesure de calculer :

$$\begin{aligned}\mathfrak{B}_{\mathfrak{p}}(M) &= p^{\mu n_1(2n-n_1)-\mu+1)n^2+2n_1(n-(n_1+n_2))-2n_1(2n_2+n_1)} \\ &\quad \cdot p^{3(n_1+n_2)^2-3n_2^2+(\mu+1)(n-n_1)^2} \cdot \mathfrak{B}_{\mathfrak{p}}(M_2)^{-1} \mathfrak{B}_{\mathfrak{p}}(M_1 \boxplus M_2) \mathfrak{B}_{\mathfrak{p}}(M_2 \boxplus \cdots \boxplus M_l) \\ &\overset{\text{ô miracle !}}{=} \mathfrak{B}_{\mathfrak{p}}(M_2)^{-1} \mathfrak{B}_{\mathfrak{p}}(M_1 \boxplus M_2) \mathfrak{B}_{\mathfrak{p}}(M_2 \boxplus \cdots \boxplus M_l).\end{aligned}$$

La partie b) se démontre de la même manière que la partie i) de a), sauf que dans ce cas, $m_1 = 0$ et $f_{\mathfrak{p}} \neq 1$, donc on remplace partout p par $p^{f_{\mathfrak{p}}}$. ❄

Grâce au théorème précédent, les valeurs particulières de densités locales qu'il suffit de connaître sont les suivantes :

a) si $\mathfrak{p}$ se ramifie dans O_E, il suffit de connaître $\mathfrak{B}_{\mathfrak{p}}(M)$ si M est unimodulaire, $\mathfrak{P}$-modulaire, ou encore somme orthogonale d'un espace unimodulaire et d'un espace $\mathfrak{P}$-modulaire.

b) Si $\mathfrak{p}$ est inerte dans O_E, il suffit de connaître $\mathfrak{B}_{\mathfrak{p}}(M)$ si M est unimodulaire.

Or, ces choses sont bien connues dans la littérature. Nous allons résumer la situation dans le théorème suivant, ce qui terminera le paragraphe.

Théorème 2.2.6

Soit (M,h) un $\tilde{O}_{E_{\mathfrak{p}}}$-module hermitien, libre de rang n.

a) Supposons que $\mathfrak{p}$ se ramifie dans O_E.

i) Si M est unimodulaire, de déterminant $\lambda \in \{1,\epsilon\}$ $\left(= U(O_{K_{\mathfrak{p}}})/N_{\tilde{E}_{\mathfrak{p}}/K_{\mathfrak{p}}}(U(O_{\tilde{E}_{\mathfrak{p}}}))\right)$, et que n est pair, alors

$$\mathfrak{B}_{\mathfrak{p}}(M) = 2(1 - \left(\frac{(-1)^{\frac{n}{2}}\lambda}{\mathfrak{p}}\right) p^{-\frac{n}{2}}) \prod_{i=1}^{\frac{n-2}{2}} (1-p^{-2i})$$

où $\left(\frac{x}{\mathfrak{p}}\right) = \begin{cases} 1 & \text{si } x \text{ est un carré } (\mathrm{mod}\ \mathfrak{p}) \\ -1 & \text{sinon.} \end{cases}$

ii) Si M est unimodulaire, et que n est impair, alors

$$\mathfrak{B}_{\mathfrak{p}}(M) = 2\prod_{i=1}^{\frac{n-1}{2}}(1-p^{-2i}).$$

iii) Si M est $\mathfrak{P}$-modulaire. On a vu au paragraphe 3 que dans ce cas, n est pair. Alors la densité locale en $\mathfrak{p}$ vaut :

$$\mathfrak{B}_{\mathfrak{p}}(M) = p^{\frac{n(n+1)}{2}}\prod_{i=1}^{\frac{n}{2}}(1-p^{-2i}).$$

iv) Supposons que la décomposition de Jordan de M soit $M_1 \boxplus M_2$, avec M_1 unimodulaire, de dimension n_1 paire et de déterminant $\lambda \in \{1, \epsilon\}$, et avec M_2, $\mathfrak{P}$-modulaire, de dimension $n_2 = n - n_1$, nécessairement paire. Dans ce cas, on a :

$$\mathfrak{B}_{\mathfrak{p}}(M) = \frac{2p^{\frac{n_2(n_2+1)}{2}}\prod_{i=1}^{\frac{n_1}{2}}(1-p^{-2i})\prod_{i=1}^{\frac{n_2}{2}}(1-p^{-2i})}{1+\left(\frac{(-1)^{\frac{n_1}{2}}\lambda}{p}\right)p^{-\frac{n_1}{2}}}.$$

v) Supposons que l'on se trouve dans la même situation qu'en iv), mais qu'au lieu d'être paire, la dimension de M_1 soit impaire. Alors on aura :

$$\mathfrak{B}_{\mathfrak{p}}(M) = 2p^{\frac{n_2(n_2+1)}{2}}\prod_{i=1}^{\frac{n_1-1}{2}}(1-p^{-2i})\prod_{i=1}^{\frac{n_2}{2}}(1-p^{-2i}).$$

b) Supposons que $\mathfrak{p}$ est inerte dans O_E. La situation est beaucoup plus simple. Le seul cas que nous devrons considérer est le cas où M est unimodulaire, et sa densité locale en $\mathfrak{p}$ est :

$$\mathfrak{B}_{\mathfrak{p}}(M) = \prod_{i=1}^{n}(1-(-1)^i p^{-f_{\mathfrak{p}}i}).$$

c) Si $\mathfrak{p}$ se décompose dans O_E, nous n'aurons à considérer que le cas unimodulaire. Et l'on a :

$$\mathfrak{B}_{\mathfrak{p}}(M) = \prod_{i=1}^{n}(1-p^{-f_{\mathfrak{p}}i}).$$

Démonstration :

la partie a) de ce théorème est montrée dans ([Ban], pp. 24-28) et les parties b) et c) sont montrées dans ([Re], Hilfsatz 5.3). ❄

§ 3. Estimation du produit de presque toutes les densités locales

Supposons dans cette partie que $E = \mathbb{Q}(\zeta_{2p^k})$ avec $p \in \mathbb{P}(\mathbb{Z})$, $K = \mathbb{Q}(\zeta_{2p^k} + \bar{\zeta}_{2p^k})$, et que (M, h) est un O_E-module hermitien, projectif de rang n, et totalement défini positif. Il est évident que $(M_{\mathfrak{p}}, h_{\mathfrak{p}})$ est unimodulaire pour tout $\mathfrak{p} \in \mathbb{P}(K)$ sauf pour un nombre fini. Posons S l'ensemble des "mauvais premiers", c'est-à-dire ceux pour lesquels $(M_{\mathfrak{p}}, h_{\mathfrak{p}})$ n'est pas unimodulaire. Notons $\mathfrak{p}_0$ l'unique idéal premier de O_K au-dessus de p, c'est-à-dire le seul idéal de O_K qui se ramifie dans O_E. Supposons que $\mathfrak{p}_0 \in S$. Posons encore $S' = \{q \in \mathbb{P}(\mathbb{Z}) \mid \exists\, \mathfrak{p} \in S,\ \mathfrak{p} \cap \mathbb{Z} = q\mathbb{Z}\}$, et on suppose que $\{\mathfrak{p} \in \mathbb{P}(K) \mid \mathfrak{p} \cap \mathbb{Z} = q\mathbb{Z},\ q \in S'\} = S$.

Le but de ce paragraphe est d'estimer $\prod_{\mathfrak{p} \in \mathbb{P}(K)-S} \mathfrak{B}_{\mathfrak{p}}(M_{\mathfrak{p}})$. Mais avant tout, nous devons faire quelques rappels sur la décomposition des idéaux d'extensions galoisiennes. Soit $\mathfrak{p} \in \mathbb{P}(K) - \{\mathfrak{p}_0\}$. Nous rappelons

la notation $f_{\mathfrak{p}}$ pour $[O_K/\mathfrak{p} : \mathbb{Z}/q\mathbb{Z}]$ où q est tel que $\mathfrak{p}\cap\mathbb{Z} = q\mathbb{Z}$. Soit maintenant $q \in S' - \{p\}$. On sait que $qO_K = \mathfrak{p}_1 \cdots \mathfrak{p}_{r_q^{(1)}}\mathfrak{p}_{r_q^{(1)}+1} \cdots \mathfrak{p}_{r_q^{(1)}+r_q^{(2)}}$, avec $\mathfrak{p}_i$ est inerte dans O_E pour $i = 1, \ldots, r_q^{(1)}$, et $\mathfrak{p}_{r_q^{(1)}+j}$ se décompose dans O_E pour $j = 1, \ldots, r_q^{(2)}$. L'extension $K/\mathbb{Q}$ étant galoisienne, on a que $r_q^{(1)} = 0$ si et seulement si $r_q^{(2)} \neq 0$. En outre, il est bien connu que $f_{\mathfrak{p}_i} = f_{\mathfrak{p}_j} := f_q$ pour tout $i, j = 1, \ldots, r_q^{(1)} + r_q^{(2)}$. Enfin, on a l'égalité $(r_q^{(1)}+r_q^{(2)})f_q = \dfrac{\varphi(p^k)}{2}$. On note encore F_S pour $\displaystyle\prod_{q\in S'-\{p\}} (1+q^{-f_q})^{-r_q^{(1)}}(1-q^{-f_q})^{-r_q^{(2)}}$.
Dernière convention : si $d(E)$ et $d(K)$ sont les discriminants des extensions $E/\mathbb{Q}$ et $K/\mathbb{Q}$ respectivement, il est bien connu que $|d(K)| = p^{\frac{p^{k-1}(kp-k-1)-1}{2}}$ et que $|d(E)| = p^{p^{k-1}(kp-k-1)}$. Par commodité, nous noterons $|d(K)| = p^s$ et $|d(E)| = p^{2s+1}$, où $s = \frac{p^{k-1}(kp-k-1)-1}{2}$.

Théorème 2.3.1

Sous les hypothèses, notations et conventions de l'introduction de ce paragraphe, on a

$$\prod_{\mathfrak{p}\in\mathbb{P}(K)-S} \mathfrak{B}_{\mathfrak{p}}(M_{\mathfrak{p}})^{-1} \leq 2^{\frac{\varphi(p^k)-2}{2}} p^{-(\frac{s+1}{2}+k)} \pi^{\frac{\varphi(p^k)}{2}} \cdot F_S \cdot \left(\prod_{i=2}^{n} \zeta(i) \prod_{q\in S'} (1-q^{-i})\right)^{\frac{\varphi(p^k)}{2}}$$

Démonstration :

a) Supposons que (M, h) soit unimodulaire et de rang 1. Dans ce cas, on sait calculer $\omega(M)$. En effet, $\omega(M) = |\{x \in O_E \mid x\bar{x} = 1\}| = \dfrac{1}{2p^k}$. Utilisant la formule de masse, on trouve :

$$\frac{1}{2p^k} = 2p^{\frac{2s+1}{2}} p^{-\frac{s}{2}} (2\pi)^{-\frac{\varphi(p^k)}{2}} \prod_{\mathfrak{p}\in\mathbb{P}(K)} \mathfrak{B}_{\mathfrak{p}}(M_{\mathfrak{p}})^{-1}.$$

Donc, $\prod_{\mathfrak{p}\in\mathbb{P}(K)} \mathfrak{B}_{\mathfrak{p}}(M_{\mathfrak{p}})^{-1} = 2^{\frac{\varphi(p^k)-4}{2}} \cdot p^{-(\frac{s+1}{2}+k)} \pi^{\frac{\varphi(p^k)}{2}}$. Or, nous avons vu au théorème 2.2.6 que

$$\mathfrak{B}_{\mathfrak{p}}(M_{\mathfrak{p}}) = \begin{cases} 2 & \text{si } \mathfrak{p} = \mathfrak{p}_0 \\ (1+q^{-f_q}) & \text{si } \mathfrak{p} \text{ est inerte dans } O_E, \text{ et } q\mathbb{Z} = \mathfrak{p}\cap\mathbb{Z} \\ (1-q^{-f_q}) & \text{si } \mathfrak{p} \text{ se décompose dans } O_E, \text{ et } q\mathbb{Z} = \mathfrak{p}\cap\mathbb{Z}. \end{cases}$$

Donc,

$$\begin{aligned} \prod_{\mathfrak{p}\in\mathbb{P}(K)-S} \mathfrak{B}_{\mathfrak{p}}(M_{\mathfrak{p}})^{-1} &= 2^{\frac{\varphi(p^k)-2}{2}} \cdot p^{-(\frac{s+1}{2}+k)} \cdot \pi^{\frac{\varphi(p^k)}{2}} \cdot F_S \\ &= \prod_{q\in\mathbb{P}(\mathbb{Z})-S'} (1+q^{-f_q})^{-r_q^{(1)}}(1-q^{-f_q})^{-r_q^{(2)}}. \end{aligned}$$

b) Pour (M, h) quelconque, on a :

$$\begin{aligned} \prod_{\mathfrak{p}\in\mathbb{P}(K)-S} \mathfrak{B}_{\mathfrak{p}}(M_{\mathfrak{p}})^{-1} &= \prod_{q\in\mathbb{P}(\mathbb{Z})-S'} \prod_{i=1}^{n} (1-(-1)^i q^{-f_q\cdot i})^{-r_q^{(1)}}(1-q^{-f_q\cdot i})^{-r_q^{(2)}} \\ &= 2^{\frac{\varphi(p^k)-2}{2}} \cdot p^{-(\frac{s+1}{2}+k)} \cdot \pi^{\frac{\varphi(p^k)}{2}} \cdot F_S \\ &\quad \cdot \prod_{q\in\mathbb{P}(\mathbb{Z})-S'} \prod_{i=2}^{n} (1-(-1)^i q^{-f_q\cdot i})^{-r_q^{(1)}}(1-q^{-f_q\cdot i})^{-r_q^{(2)}} \\ &\leq 2^{\frac{\varphi(p^k)-2}{2}} \cdot p^{-(\frac{s+1}{2}+k)} \cdot \pi^{\frac{\varphi(p^k)}{2}} \cdot F_S \left(\prod_{i=2}^{n} \prod_{q\in\mathbb{P}(\mathbb{Z})-S'} (1-q^{-i})^{-1}\right)^{\frac{\varphi(p^k)}{2}} \\ &= 2^{\frac{\varphi(p^k)-2}{2}} p^{-(\frac{s+1}{2}+k)} \pi^{\frac{\varphi(p^k)}{2}} \cdot F_S \cdot \left(\prod_{i=2}^{n} \zeta(i) \prod_{q\in S'} (1-q^{-i})\right)^{\frac{\varphi(p^k)}{2}}. \end{aligned}$$

❄

CHAPITRE 3

Un exemple d'application: les isométries parfaites

Voici un problème qui prend sa source dans la théorie des noeuds, cf. [Ker]. Soit (M, β) un $\mathbb{Z}$-module bilinéaire symétrique, unimodulaire, de dimension n. La question est la suivante : existe-t-il une forme γ sur M, unimodulaire mais non symétrique, telle que

$$\beta(x, y) = \gamma(x, y) + \gamma(y, x) \quad \text{pour tout } x, y \in M.$$

Le problème s'énonce matriciellement ainsi : si B est une matrice de β, existe-t-il une matrice $A \in GL_n(\mathbb{Z})$ telle que $A + A^{\mathrm{tr}} = B$?

Dans ce cas, il est clair que (M, β) est de type II. Ainsi, le rang de M est un multiple de 8. Michel Kervaire, dans [Ker1], donne des résultats jusqu'en dimension 24, et pour les (M, β) possédant un système complet de racines. En dimension 32, la formule de masse pour les formes bilinéaires nous apprend qu'il y a au moins 80 millions de classes (cf. [Mis], théorème 5.3), et un nombre très restreint d'entre elles possèdent un système complets de racines (cf. [Ker2] et Annexe 4).

Voici comment nous allons procéder pour faire avancer quelque peu notre connaissance sur le sujet : nous allons voir au lemme 3.1.1 que le problème est équivalent à la question sur l'existence d'une isométrie t dont le polynôme caractéristique F vérifie $F(1) = 1$. Nous allons, grâce à un théorème d'Eva Bayer, donner la liste complète de tous les polynômes possibles. Cette liste est longue, mais nous parviendrons à la réduire considérablement, jusqu'à n'avoir plus que 23 polynômes.

§ 1. Résultats généraux

Lemme 3.1.1

Soit (M, β) un $\mathbb{Z}$-réseau unimodulaire de dimension n. Notons B la matrice de β relativement à une certaine base. Les affirmations suivantes sont équivalentes :

a) Il existe $A \in GL_n(\mathbb{Z})$ telle que $B = A + A^{\mathrm{tr}}$.

b) (M, β) possède une isométrie t telle que $1 - t$ est inversible.

c) (M, β) possède une isométrie t dont le polynôme caractéristique F vérifie $F(1) = 1$. Autrement dit, (M, β) est un F-réseau, avec $F(1) = 1$.

Démonstration :

L'équivalence de a) et de b) est démontrée dans ([Ker], Lemme, p.177). Les parties b) et c) sont trivialement équivalentes : si T est la matrice de t, alors $F(1) = \det(Id_n - T)$. ❄

Définition 3.1.2

Les isométries de (M, β) satisfaisant les parties b) ou c) du théorème précédent sont appelées *isométries parfaites de (M, β)*.

Rappelons que si (M,β) est défini positif, alors le polynôme caractéristique de toute isométrie est un produit de puissances de polynômes cyclotomiques. Voici un lemme technique concernant certaines valeurs que peuvent prendre les polynômes cyclotomiques.

Lemme 3.1.3

Soient $d \geq 2$ un entier naturel, et Φ_d le d-ième polynôme cyclotomique. On a les résultats suivants :

a) $\Phi_d(1) > 0$ *et* $\Phi_1(1) = 0$.

b) $\Phi_d(1) = p$ *si* $d = p^m$, *avec* $p \in \mathbb{P}(\mathbb{Z})$ *et* $m > 0$.

c) $\Phi_d(1) = 1$ *si d a au moins deux facteurs premiers distincts.*

d) $\Phi_d(-1) = 1$ *si d est impair et différent de 1.*

e) $\Phi_{2d}(-1) = \Phi_d(1)$ *pour tout d.*

Démonstration :

a) On a déjà $\Phi_2(1) = 2$. Supposons $d \geq 3$, et soit ζ_d une racine primitive d-ième de l'unité, et N_d la norme de l'extension $\mathbb{Q}(\zeta_d)/\mathbb{Q}$. Puisque $d \geq 3$, $\varphi(d)$ est paire, où φ est la fonction d'Euler, et on trouve :

$$\Phi_d(1) = \prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})} \sigma(1-\zeta_d) = N_d(1-\zeta_d) > 0,$$

car $\mathbb{Q}(\zeta_d)$ n'a pas de plongement réel.

b) En effet, $\Phi_{p^m}(X) = X^{p^{m-1}(p-1)} + X^{p^{m-1}(p-2)} + \cdots + X^{p^{m-1}} + 1$.

c) De $X^{d-1} + \cdots + X + 1 = \prod_{\substack{u|d \\ u \neq 1}} \Phi_u(X)$, et de a) et b), on déduit le résultat.

d) Par un argument similaire à la démonstration de a), on montre que $\Phi_d(-1) > 0$ pour tout $d \geq 2$. D'autre part, si d est impair, l'égalité polynomiale $\dfrac{X^d-1}{X-1} = \prod_{\substack{u|d \\ u \neq 1}} \Phi_u(X)$ évaluée en -1 nous donne que $\prod_{\substack{u|d \\ u \neq 1}} \Phi_u(-1) = 1$, donc $\Phi_d(-1) = 1$.

e) Si d est impair, on sait que $\Phi_{2d}(X) = \Phi_d(-X)$ cf. ([Lang], VIII, §3).
Si d est pair on écrit $d = 2^n d'$ avec d' impair. On a aussi [Lang] : $\Phi_{2^{n+1}d'}(X) = \Phi_{2d'}(X^{2^n})$. En évaluant en -1, on trouve

$$\Phi_{2d}(-1) = \Phi_{2d'}(1) = \begin{cases} 1 = \Phi_d(1) & \text{si } d' \neq 1 \\ 2 = \Phi_d(1) & \text{si } d' = 1. \end{cases}$$

❄

Théorème 3.1.4

Soit F un produit de polynômes cyclotomiques tel que $F(1) = 1$. Il existe un F-réseau unimodulaire si et seulement si F est un produit de polynômes du type suivant :

1) Φ_m^n *de degré divisible par 8, tel que* $\Phi_m^n(-1)$ *est un carré.*

2) $\Phi_{2p^{n_1}} \cdots \Phi_{2p^{n_r}}$ *de degré divisible par 8, tel que* $\Phi_{2p^{n_1}} \cdots \Phi_{2p^{n_r}}(-1)$ *est un carré, et p est un nombre premier impair.*

3) $\Phi_{2p^n q^m} \Phi_{2p^n}^2$, *où p et q sont des nombres premiers impairs distincts congrus à* 3 (mod 4), *et p est un carré* (mod q).

4) $\Phi_{p^n q^m} \Phi_{p^n q^r}$ *ou* $\Phi_{2p^n q^m} \Phi_{2p^n q^r}$, *où p et q sont des nombres premiers impairs distincts congrus à* 3 (mod 4), *et p est un carré* (mod q).

5) $\Phi_{4p^n} \Phi_{2p^n}^2$, *où p est un nombre premier impair congru à* 3 (mod 4) *et 2 n'est pas un carré* (mod p).

6) $\Phi_{4p^n}\Phi_{4p^m}$, *où* p *est un nombre premier impair.*

7) $\Phi_{p^nq^m}\Phi_{2p^nq^m}$, p *et* q *sont des nombres premiers impairs distincts congrus à* 3 (mod 8)

Démonstration :

cf.([Bay], théorème 2.1). ❄

Le théorème précédent nous permet notamment de trouver tous les polynômes F de degré 32, tels que $F(1) = 1$, et dont l'ensemble des F-réseaux $\mathscr{E}(F)$ n'est pas vide. Le cardinal de l'ensemble de ces polynômes est 846. Nous en donnerons la liste au prochain paragraphe. Les deux résultats qui suivent nous permettront de réduire considérablement le nombre de ces polynômes.

Lemme 3.1.5

Si F *et* G *sont des produits de puissances de polynômes cyclotomiques, tels que* $\mathrm{Res}(F,G) = \pm 1$, *alors il existe un* FG*-réseau si et seulement s'il existe un* F*-réseau et un* G*-réseau.*

Démonstration :

Soit $(M,\beta) \in \mathscr{E}(FG)$. Puisque $\mathrm{Res}(F,G) = \pm 1$, il existe des polynômes h et k tels que $hF + kG = 1$. En posant $M_1 = G(t)(M)$ et $M_2 = F(t)(M)$, puis β_1 et β_2 les restrictions de β à M_1 et M_2 respectivement, on trouve que $(M,\beta) \simeq (M_1,\beta_1) \boxplus (M_2,\beta_2)$ (voir la proposition 1.2.3). Finalement, on voit que $(M_1,\beta_1) \in \mathscr{E}(F)$ et que $(M_2,\beta_2) \in \mathscr{E}(G)$.

La réciproque est évidente. ❄

Lemme 3.1.6

Soit $F = \Phi_{p^{n_1}m_1}^{r_1} \cdots \Phi_{p^{n_s}m_s}^{r_s}$, *avec* $p \in \mathbb{P}$, $p \nmid m_i$ *pour tout* $i = 1,\ldots,s$, *et* $n_1 < n_j$ *pour tout* $j = 2,\ldots,s$. *Soit* $(M,\beta) \in \mathscr{E}(F)$. *Il existe donc* $t \in O(M)$ *telle que* $car(t) = F$. *Alors on a :*

$$car(t^{p^{n_1-1}}) = \Phi_{pm_1}^{r_1p^{n_1-1}} \cdot \Phi_{p^{n_2-n_1+1}m_2}^{r_2p^{n_1-1}} \cdots \Phi_{p^{n_s-n_1+1}m_s}^{r_sp^{n_1-1}}$$
$$et \quad car(t^{p^{n_1}}) = \Phi_{m_1}^{r_1\varphi(p^{n_1})} \cdot \Phi_{p^{n_2-n_1}m_2}^{r_2p^{n_1}} \cdots \Phi_{p^{n_s-n_1}m_s}^{r_sp^{n_1}}.$$

Démonstration :

Posons $W = M \otimes \mathbb{Q}$ sur lequel β et t se prolongent naturellement. On a vu dans la proposition 1.2.3 que $W = W_1 \boxplus \cdots \boxplus W_s$, avec $W_i = \dfrac{f}{\Phi_{p^{n_i}m_i}}(t)(W)$, pour $i = 1,\ldots,s$, et $f = \Phi_{p^{n_1}m_1} \cdots \Phi_{p^{n_s}m_s}$. On note t_i pour $t|_{W_i}$. Il est évident que $car(t_i) = \Phi_{p_{n_i}m_i}^{r_i}$ pour tout $i = 1,\ldots,s$, et que $car(t^l) = car(t_1^l) \cdots car(t_s^l)$ pour tout entier l. Soit $q \in \mathbb{P}$, $l \in \mathbb{N}$, $m \in \mathbb{N} - q\mathbb{Z}$, et $j = 0,\ldots,l-1$. Selon ([Lang], VIII, §3), on a :

$$\Phi_{q^lm}(X) = \Phi_{q^{l-i}m}(X^{q^i}).$$

Soit maintenant $i = 1,\ldots,s$. On a donc l'égalité $\Phi_{p^{n_i-n_1+1}m_i}(t_i^{p^{n_1-1}}) = \Phi_{p^{n_i}m_i}(t_i) = 0$. Ainsi, le polynôme minimal de $t_i^{p^{n_i-1}}$ vaut $\Phi_{p^{n_i-n_1+1}m_1}$, et par suite, $car(t_i^{p^{n_i-1}}) = \Phi_{p^{n_i-n_1+1}m_i}^{r_ip^{n_1-1}}$, car la dimension de W_i vaut $\varphi(p^{n_i}m_i)r_i$. La première égalité du lemme est démontrée.

En suivant le même raisonnement, on voit tout de suite que $car(t_i^{p^{r_1}}) = \Phi_{p^{r_i-r_1}m_i}^{r_ip^{r_1}}$, pour $i = 2,\ldots,s$. Pour $i = 1$, on utilise un autre résultat :

$$\Phi_{qm}(X) = \frac{\Phi_m(X^q)}{\Phi_m(X)} \quad \forall q \in \mathbb{P} \text{ et } q \nmid m \quad \text{cf. ([Lang], VIII, §3).}$$

On trouve alors : $\Phi_{m_1}(t_1^{p^{n_1}}) = \Phi_{pm_1}(t_1^{p^{n_1-1}}) \cdot \Phi_{m_1}(t_1^{p^{n_1-1}}) = \Phi_{p^{n_1}m_1}(t_1) \cdot \Phi_{m_1}(t_1^{p^{n_1-1}}) = 0$. Donc Φ_{m_1} est le polynôme minimal de $t_1^{p^{n_1}}$, et $\Phi_{m_1}^{r_1\varphi(p^{n_1})}$ est son polynôme caractéristique. ❄

§ 2. Application de la théorie en dimension 32

Dans ce paragraphe, nous allons trouver tous les polynômes F de degré 32, tels que $F(1) = 1$, et $\mathscr{E}(F) \neq 0$. Puis, nous utiliserons les lemmes 3.1.5 et 3.1.6 pour éliminer les polynômes "inutiles".

Notations

Nous dirons qu'un polynôme est de *type* i s'il satisfait la partie i) du théorème 3.1.4 pour $i = 1, \ldots, 7$.

Il s'agit dans un premier temps de trouver les polynômes de type i et de degré 32, 24, 16 et 8.

Les polynômes de type 1

Ils sont du type Φ_m^n avec m possédant au moins deux facteurs premiers (car il faut que $\Phi_m(1) = 1$) et $\Phi_m^n(-1)$ doit être un carré.

de degré 32 :

Un polynôme F est de type 1 et de degré 32 si et seulement si F est l'un des polynômes suivants :

$$\Phi_6^{16} \quad \Phi_{10}^8 \quad \Phi_{12}^8 \quad \Phi_{15}^4 \quad \Phi_{20}^4 \quad \Phi_{24}^4 \quad \Phi_{30}^4 \quad \Phi_{34}^2 \quad \Phi_{40}^2 \quad \Phi_{48}^2 \quad \Phi_{51} \quad \Phi_{60}^2 \quad \Phi_{68} \quad \Phi_{80} \quad \Phi_{96} \quad \Phi_{102} \quad \Phi_{120}.$$

de degré 24 :

Un polynôme F est de type 1 et de degré 24 si et seulement si F est l'un des polynômes suivants :

$$\Phi_6^{12} \quad \Phi_{10}^6 \quad \Phi_{12}^6 \quad \Phi_{14}^4 \quad \Phi_{15}^3 \quad \Phi_{18}^4 \quad \Phi_{20}^3 \quad \Phi_{21}^2 \quad \Phi_{24}^3 \quad \Phi_{26}^2 \quad \Phi_{28}^2 \quad \Phi_{30}^3$$
$$\Phi_{35} \quad \Phi_{36}^2 \quad \Phi_{39} \quad \Phi_{42}^2 \quad \Phi_{45} \quad \Phi_{52} \quad \Phi_{56} \quad \Phi_{70} \quad \Phi_{72} \quad \Phi_{78} \quad \Phi_{84} \quad \Phi_{90}.$$

de degré 16 :

Un polynôme F est de type 1 et de degré 16 si et seulement si F est l'un des polynômes suivants :

$$\Phi_6^8 \quad \Phi_{10}^4 \quad \Phi_{12}^4 \quad \Phi_{15}^2 \quad \Phi_{20}^2 \quad \Phi_{24}^2 \quad \Phi_{30}^2 \quad \Phi_{40} \quad \Phi_{48} \quad \Phi_{60}.$$

de degré 8 :

Un polynôme F est de type 1 et de degré 8 si et seulement si F est l'un des polynômes suivants :

$$\Phi_6^4 \quad \Phi_{10}^2 \quad \Phi_{12}^2 \quad \Phi_{15} \quad \Phi_{20} \quad \Phi_{24} \quad \Phi_{30}.$$

Les polynômes de type 2

On cherche les polynômes $F = \Phi_{2p^{n_1}} \cdots \Phi_{2p^{n_r}}$, tels que r est pair et $(p-1)(p^{n_1-1} + \cdots + p^{n_r-1}) \equiv 0 \pmod 8$.

de degré 32 :

On doit résoudre l'équation $(p-1)(p^{n_1-1} + \cdots + p^{n_r-1}) = 32$ avec p premier et r pair. Les seuls candidats pour p sont : 3,5 et 17.
Si $p = 3$, on trouve 7 polynômes nouveaux (c'est-à-dire qui ne se composent pas d'un produit de plusieurs polynômes de type 1) :

$$\Phi_6\Phi_{18}^5 \quad \Phi_6^7\Phi_{18}^3 \quad \Phi_6^7\Phi_{54} \quad \Phi_6^{10}\Phi_{18}^2 \quad \Phi_6^{13}\Phi_{18} \quad \Phi_6\Phi_{18}^2\Phi_{54} \quad \Phi_6^4\Phi_{18}\Phi_{54}.$$

Si $p = 5$, on trouve 1 polynôme nouveau :

$$\Phi_{10}^3\Phi_{50}.$$

Si $p = 17$, on trouve Φ_{34}^2 qui existe déjà.

de degré 24 :

Pour résoudre l'équation $(p-1)(p^{n_1-1}+\cdots+p^{n_r-1})=24$, avec p premier et r pair, les candidats pour p sont : 3,5,7 et 13.

Si $p=3$, on trouve 5 polynômes nouveaux :

$$\Phi_6^3\Phi_{18}^3 \quad \Phi_6^3\Phi_{54} \quad \Phi_6^6\Phi_{18}^2 \quad \Phi_6^9\Phi_{18} \quad \Phi_{18}\Phi_{54}.$$

Si $p=5$, on trouve 1 polynôme nouveau :

$$\Phi_{10}\Phi_{50}.$$

Si $p=7$ ou 13, on ne trouve pas de nouveau cas.

de degré 16 :

Pour résoudre l'équation $(p-1)(p^{n_1-1}+\cdots+p^{n_r-1})=16$, avec p premier et r pair, les candidats pour p sont : 3 et 5.
Si $p=3$, on trouve 2 polynômes nouveaux :

$$\Phi_6^2\Phi_{18}^2 \quad \Phi_6^5\Phi_{18}.$$

Le cas $p=5$ ne présente pas de nouveau cas.

de degré 8 :

Pour résoudre l'équation $(p-1)(p^{n_1-1}+\cdots+p^{n_r-1})=8$, avec p premier et r pair, les candidats pour p sont : 3 et 5.
On ne trouve dans le cas $p=3$ que le polynôme

$$\Phi_6\Phi_{18}.$$

Le cas $p=5$ ne présente pas de nouveau cas.

Les polynômes de type 3

Il faut trouver les polynômes $F=\Phi_{2p^nq^m}\Phi_{2p^n}^2$ tels que $p\equiv q\equiv 3 \pmod 4$ et tels que le symbole de Legendre $(\frac{p}{q})$ soit égal à 1. Le degré de F vaut $p^{n-1}(p-1)(q^{m-1}(q-1)+2)$.

de degré 32 :

Pour résoudre $p^{n-1}(p-1)(q^{m-1}(q-1)+2)=32$, on doit avoir que $n=1$ et $p=3$. Il nous reste donc à résoudre $q^{m-1}(q-1)=14$ avec q premier. Cela est impossible. Il n'y a donc aucun nouveau cas.

de degré 24 :

Si $n\neq 1$, on a $p=3$ et que $n=2$, mais alors q ne peut valoir que 3. Or p et q doivent être distincts. Si $n=1$, on voit que $p\equiv 3 \pmod 4$ peut valoir 3 ou 7. On trouve ainsi 2 nouveaux polynômes :

$$\Phi_6^2\Phi_{66} \quad \Phi_{14}^2\Phi_{42}.$$

de degré 16 ou 8 :

Comme pour le degré 32, on voit que $n=1$ et $p=3$. Dans ce cas, q ne peut valoir que 3, ce qui est impossible. Il n'y a aucun nouveau cas non plus.

Les polynômes de type 4

On cherche des polynômes du type $F = \Phi_{p^n q^m}\Phi_{p^n q^r}$ ou $F = \Phi_{2p^n q^m}\Phi_{2p^n q^r}$, avec $p \equiv q \equiv 3 \pmod 4$ et $(\frac{p}{q}) = 1$. Dans les deux cas, le degré de F est $p^{n-1}(p-1)(q-1)(q^{m-1}+q^{r-1})$.

De $p^{n-1}(p-1)(q-1)(q^{m-1}+q^{r-1}) \leq 32$ et $(\frac{p}{q}) = 1$, on déduit $(p-1)(q-1) \leq 16$, et donc $p = 3$, $q = 7$, et finalement $m = n = r = 1$. Les seuls polynômes possibles sont Φ_{21}^2 et Φ_{42}^2, mais ils sont déjà de type 1.

Les polynômes de type 5

On cherche des polynômes du type $F = \Phi_{4p^n}\Phi_{2p^n}^2$, avec $p \equiv 3 \pmod 4$ et où 2 n'est pas un carré (mod p). Ces conditions sont équivalentes à $p \equiv 3 \pmod 8$ par le théorème de réciprocité quadratique. Le degré de F est $4p^{n-1}(p-1)$, ce qui implique $p \leq 8$, et donc $p = 3$. Pour $\deg(F) = 8, 16, 24, 32$, on a donc $3^{n-1} = 1, 2, 3, 4$. Donc on a pas de polynômes de degré 16 et 32. Et un nouveau polynôme de degré 24 et 8, à savoir :

$$\Phi_{18}^2\Phi_{36} \text{ et } \Phi_6^2\Phi_{12}.$$

Les polynômes de type 6

On cherche des polynômes du type $F = \Phi_{4p^n}\Phi_{4p^m}$, avec p un premier impair. Le degré de F est $2(p-1)(p^{n-1}+p^{m-1})$.

de degré 32 :

Il est impossible de résoudre l'équation $(p-1)(p^{n-1}+p^{m-1}) = 16$ si p est premier et n, m sont des entiers positifs. Donc aucun nouveau cas.

de degré 24 :

Résolvons $(p-1)(p^{n-1}+p^{m-1}) = 12$: les candidats pour p sont 3,5 ou 7. Avec $p = 3$, on trouve Φ_{36}^2 qui est déjà un polynôme de type 1. Le cas $p = 5$ est impossible. Avec $p = 7$, on trouve le polynôme Φ_{28}^2, mais il est aussi déjà de type 1. Aucun nouveau cas non plus.

de degré 16 :

Pour résoudre $(p-1)(p^{n-1}+p^{m-1}) = 8$, les premiers possibles sont $p = 3$ et 5. Dans le cas $p = 3$, en posant $n = 1$ et $m = 2$, on trouve un nouveau polynôme :

$$\Phi_{12}\Phi_{36}.$$

Dans le cas $p = 5$, on trouve avec $n = m = 1$ le polynôme Φ_{20}^2 qui est déjà de type 1.

de degré 8 :

Pour résoudre $(p-1)(p^{n-1}+p^{m-1}) = 4$, on doit poser $p = 3$ et $n = m = 1$, et on trouve Φ_{12}^2 qui est de type 1. Aucun nouveau cas.

Les polynômes de type 7

On cherche des polynômes de type $F = \Phi_{p^n q^m}\Phi_{2p^n q^m}$, avec p et q des nombres premiers impairs distincts congrus à 3 (mod 8). Le degré de F est $2(p-1)(q-1)p^{n-1}q^{m-1}$. De $(p-1)(q-1)p^{n-1}q^{m-1} = 16, 12, 8, 4$ et $p \equiv q \equiv 3 \pmod 8$, on voit que $p = 3$, mais il n'y a pas de possibilités pour q, donc pas de polynômes nouveaux.

On trouve donc 25 polynômes de degré 32, 33 de degré 24, 13 de degré 16 et 9 de degré 8. En multipliant entre eux tous ces polynômes de façon à trouver des polynômes de degré 32, on obtient alors, en vertu du théorème 3.1.4, la proposition suivante :

Proposition 3.2.1

Soit (M,β) un $\mathbb{Z}$-réseau unimodulaire, pair et de dimension 32. Soit t une isométrie de (M,β). Alors t est une isométrie parfaite si et seulement si son polynôme caractéristique est un des polynômes suivants :

Φ_6^{16} Φ_{10}^8 Φ_{12}^8 Φ_{15}^4 Φ_{20}^4 Φ_{24}^4 Φ_{30}^4 Φ_{34}^2 Φ_{40}^2 Φ_{48}^2 Φ_{51} Φ_{60}^2 Φ_{68} Φ_{80} Φ_{96} Φ_{102} Φ_{120}

$\Phi_6\Phi_{18}^5$ $\Phi_6^2\Phi_{12}^7$ $\Phi_6^4\Phi_{10}^6$ $\Phi_6^4\Phi_{12}^6$ $\Phi_6^4\Phi_{14}^4$ $\Phi_6^4\Phi_{15}^3$ $\Phi_6^4\Phi_{18}^4$ $\Phi_6^4\Phi_{20}^3$ $\Phi_6^4\Phi_{21}^2$ $\Phi_6^4\Phi_{24}^3$

$\Phi_6^4\Phi_{26}^2$ $\Phi_6^4\Phi_{28}^2$ $\Phi_6^4\Phi_{30}^3$ $\Phi_6^4\Phi_{35}$ $\Phi_6^4\Phi_{36}^2$ $\Phi_6^4\Phi_{39}$ $\Phi_6^4\Phi_{42}^2$ $\Phi_6^4\Phi_{45}$ $\Phi_6^4\Phi_{52}$ $\Phi_6^4\Phi_{56}$

$\Phi_6^4\Phi_{70}$ $\Phi_6^4\Phi_{72}$ $\Phi_6^4\Phi_{78}$ $\Phi_6^4\Phi_{84}$ $\Phi_6^4\Phi_{90}$ $\Phi_6^6\Phi_{12}^5$ $\Phi_6^6\Phi_{66}$ $\Phi_6^7\Phi_{18}^3$ $\Phi_6^7\Phi_{54}$ $\Phi_6^8\Phi_{10}^4$ $\Phi_6^8\Phi_{12}^4$

$\Phi_6^8\Phi_{15}^2$ $\Phi_6^8\Phi_{20}^2$ $\Phi_6^8\Phi_{24}^2$ $\Phi_6^8\Phi_{30}^2$ $\Phi_6^8\Phi_{40}$ $\Phi_6^8\Phi_{48}$ $\Phi_6^8\Phi_{60}$ $\Phi_6^{10}\Phi_{12}^3$ $\Phi_6^{10}\Phi_{18}^2$ $\Phi_6^{12}\Phi_{10}^2$

$\Phi_6^{12}\Phi_{12}^2$ $\Phi_6^{12}\Phi_{15}$ $\Phi_6^{12}\Phi_{20}$ $\Phi_6^{12}\Phi_{24}$ $\Phi_6^{12}\Phi_{30}$ $\Phi_6^{13}\Phi_{18}$ $\Phi_6^{14}\Phi_{12}$ $\Phi_{10}^2\Phi_{12}^6$ $\Phi_{10}^2\Phi_{14}^4$ $\Phi_{10}^2\Phi_{15}^3$

$\Phi_{10}^2\Phi_{18}^4$ $\Phi_{10}^2\Phi_{20}^3$ $\Phi_{10}^2\Phi_{21}^2$ $\Phi_{10}^2\Phi_{24}^3$ $\Phi_{10}^2\Phi_{26}^2$ $\Phi_{10}^2\Phi_{28}^2$ $\Phi_{10}^2\Phi_{30}^3$ $\Phi_{10}^2\Phi_{35}$ $\Phi_{10}^2\Phi_{36}^2$ $\Phi_{10}^2\Phi_{39}$

$\Phi_{10}^2\Phi_{42}^2$ $\Phi_{10}^2\Phi_{45}$ $\Phi_{10}^2\Phi_{52}$ $\Phi_{10}^2\Phi_{56}$ $\Phi_{10}^2\Phi_{70}$ $\Phi_{10}^2\Phi_{72}$ $\Phi_{10}^2\Phi_{78}$ $\Phi_{10}^2\Phi_{84}$ $\Phi_{10}^2\Phi_{90}$ $\Phi_{10}^3\Phi_{50}$

$\Phi_{10}^4\Phi_{12}^4$ $\Phi_{10}^4\Phi_{15}^2$ $\Phi_{10}^4\Phi_{20}^2$ $\Phi_{10}^4\Phi_{24}^2$ $\Phi_{10}^4\Phi_{30}^2$ $\Phi_{10}^4\Phi_{40}$ $\Phi_{10}^4\Phi_{48}$ $\Phi_{10}^4\Phi_{60}$ $\Phi_{10}^6\Phi_{12}^2$ $\Phi_{10}^6\Phi_{15}$

$\Phi_{10}^6\Phi_{20}$ $\Phi_{10}^6\Phi_{24}$ $\Phi_{10}^6\Phi_{30}$ $\Phi_{12}^2\Phi_{14}^4$ $\Phi_{12}^2\Phi_{15}^3$ $\Phi_{12}^2\Phi_{18}^4$ $\Phi_{12}^2\Phi_{20}^3$ $\Phi_{12}^2\Phi_{21}^2$ $\Phi_{12}^2\Phi_{24}^3$ $\Phi_{12}^2\Phi_{26}^2$

$\Phi_{12}^2\Phi_{28}^2$ $\Phi_{12}^2\Phi_{30}^3$ $\Phi_{12}^2\Phi_{35}$ $\Phi_{12}^2\Phi_{36}^2$ $\Phi_{12}^2\Phi_{39}$ $\Phi_{12}^2\Phi_{42}^2$ $\Phi_{12}^2\Phi_{45}$ $\Phi_{12}^2\Phi_{52}$ $\Phi_{12}^2\Phi_{56}$ $\Phi_{12}^2\Phi_{70}$

$\Phi_{12}^2\Phi_{72}$ $\Phi_{12}^2\Phi_{78}$ $\Phi_{12}^2\Phi_{84}$ $\Phi_{12}^2\Phi_{90}$ $\Phi_{12}^4\Phi_{15}^2$ $\Phi_{12}^4\Phi_{20}^2$ $\Phi_{12}^4\Phi_{24}^2$ $\Phi_{12}^4\Phi_{30}^2$ $\Phi_{12}^4\Phi_{40}$ $\Phi_{12}^4\Phi_{48}$

$\Phi_{12}^4\Phi_{60}$ $\Phi_{12}^5\Phi_{36}$ $\Phi_{12}^6\Phi_{15}$ $\Phi_{12}^6\Phi_{20}$ $\Phi_{12}^6\Phi_{24}$ $\Phi_{12}^6\Phi_{30}$ $\Phi_{14}^4\Phi_{15}$ $\Phi_{14}^4\Phi_{20}$ $\Phi_{14}^4\Phi_{24}$ $\Phi_{14}^4\Phi_{30}$

$\Phi_{15}\Phi_{18}^4$ $\Phi_{15}\Phi_{20}^3$ $\Phi_{15}\Phi_{21}^2$ $\Phi_{15}\Phi_{24}^3$ $\Phi_{15}\Phi_{26}^2$ $\Phi_{15}\Phi_{28}^2$ $\Phi_{15}\Phi_{30}^3$ $\Phi_{15}\Phi_{35}$ $\Phi_{15}\Phi_{36}^2$ $\Phi_{15}\Phi_{39}$

$\Phi_{15}\Phi_{42}^2$ $\Phi_{15}\Phi_{45}$ $\Phi_{15}\Phi_{52}$ $\Phi_{15}\Phi_{56}$ $\Phi_{15}\Phi_{70}$ $\Phi_{15}\Phi_{72}$ $\Phi_{15}\Phi_{78}$ $\Phi_{15}\Phi_{84}$ $\Phi_{15}\Phi_{90}$ $\Phi_{15}^2\Phi_{20}^2$

$\Phi_{15}^2\Phi_{24}^2$ $\Phi_{15}^2\Phi_{30}^2$ $\Phi_{15}^2\Phi_{40}$ $\Phi_{15}^2\Phi_{48}$ $\Phi_{15}^2\Phi_{60}$ $\Phi_{15}^3\Phi_{20}$ $\Phi_{15}^3\Phi_{24}$ $\Phi_{15}^3\Phi_{30}$ $\Phi_{18}^4\Phi_{20}$ $\Phi_{18}^4\Phi_{24}$

$\Phi_{18}^4\Phi_{30}$ $\Phi_{20}\Phi_{21}^2$ $\Phi_{20}\Phi_{24}^3$ $\Phi_{20}\Phi_{26}^2$ $\Phi_{20}\Phi_{28}^2$ $\Phi_{20}\Phi_{30}^3$ $\Phi_{20}\Phi_{35}$ $\Phi_{20}\Phi_{36}^2$ $\Phi_{20}\Phi_{39}$ $\Phi_{20}\Phi_{42}^2$

$\Phi_{20}\Phi_{45}$ $\Phi_{20}\Phi_{52}$ $\Phi_{20}\Phi_{56}$ $\Phi_{20}\Phi_{70}$ $\Phi_{20}\Phi_{72}$ $\Phi_{20}\Phi_{78}$ $\Phi_{20}\Phi_{84}$ $\Phi_{20}\Phi_{90}$ $\Phi_{20}^2\Phi_{24}^2$ $\Phi_{20}^2\Phi_{30}^2$

$\Phi_{20}^2\Phi_{40}$ $\Phi_{20}^2\Phi_{48}$ $\Phi_{20}^2\Phi_{60}$ $\Phi_{20}^3\Phi_{24}$ $\Phi_{20}^3\Phi_{30}$ $\Phi_{21}^2\Phi_{24}$ $\Phi_{21}^2\Phi_{30}$ $\Phi_{24}\Phi_{26}^2$ $\Phi_{24}\Phi_{28}^2$ $\Phi_{24}\Phi_{30}^3$

$\Phi_{24}\Phi_{35}$ $\Phi_{24}\Phi_{36}^2$ $\Phi_{24}\Phi_{39}$ $\Phi_{24}\Phi_{42}^2$ $\Phi_{24}\Phi_{45}$ $\Phi_{24}\Phi_{52}$ $\Phi_{24}\Phi_{56}$ $\Phi_{24}\Phi_{70}$ $\Phi_{24}\Phi_{72}$ $\Phi_{24}\Phi_{78}$

$\Phi_{24}\Phi_{84}$ $\Phi_{24}\Phi_{90}$ $\Phi_{24}^2\Phi_{30}^2$ $\Phi_{24}^2\Phi_{40}$ $\Phi_{24}^2\Phi_{48}$ $\Phi_{24}^2\Phi_{60}$ $\Phi_{24}^3\Phi_{30}$ $\Phi_{26}^2\Phi_{30}$ $\Phi_{28}^2\Phi_{30}$ $\Phi_{30}\Phi_{35}$

$\Phi_{30}\Phi_{36}^2$ $\Phi_{30}\Phi_{39}$ $\Phi_{30}\Phi_{42}^2$ $\Phi_{30}\Phi_{45}$ $\Phi_{30}\Phi_{52}$ $\Phi_{30}\Phi_{56}$ $\Phi_{30}\Phi_{70}$ $\Phi_{30}\Phi_{72}$ $\Phi_{30}\Phi_{78}$ $\Phi_{30}\Phi_{84}$

$\Phi_{30}\Phi_{90}$ $\Phi_{30}^2\Phi_{40}$ $\Phi_{30}^2\Phi_{48}$ $\Phi_{30}^2\Phi_{60}$ $\Phi_{40}\Phi_{48}$ $\Phi_{40}\Phi_{60}$ $\Phi_{48}\Phi_{60}$

$\Phi_6\Phi_{10}^6\Phi_{18}$ $\Phi_6\Phi_{12}^6\Phi_{18}$ $\Phi_6\Phi_{14}^4\Phi_{18}$ $\Phi_6\Phi_{15}^3\Phi_{18}$ $\Phi_6\Phi_{18}\Phi_{20}^3$ $\Phi_6\Phi_{18}\Phi_{21}^2$ $\Phi_6\Phi_{18}\Phi_{24}^3$

$\Phi_6\Phi_{18}\Phi_{26}^2$ $\Phi_6\Phi_{18}\Phi_{28}^2$ $\Phi_6\Phi_{18}\Phi_{30}^3$ $\Phi_6\Phi_{18}\Phi_{35}$ $\Phi_6\Phi_{18}\Phi_{36}^2$ $\Phi_6\Phi_{18}\Phi_{39}$ $\Phi_6\Phi_{18}\Phi_{42}^2$

$\Phi_6\Phi_{18}\Phi_{45}$ $\Phi_6\Phi_{18}\Phi_{52}$ $\Phi_6\Phi_{18}\Phi_{56}$ $\Phi_6\Phi_{18}\Phi_{70}$ $\Phi_6\Phi_{18}\Phi_{72}$ $\Phi_6\Phi_{18}\Phi_{78}$ $\Phi_6\Phi_{18}\Phi_{84}$

$\Phi_6\Phi_{18}\Phi_{90}$ $\Phi_6\Phi_{18}^2\Phi_{54}$ $\Phi_6\Phi_{18}^3\Phi_{36}$ $\Phi_6^2\Phi_{10}^2\Phi_{12}^5$ $\Phi_6^2\Phi_{10}^2\Phi_{12}^5$ $\Phi_6^2\Phi_{10}^4\Phi_{66}$ $\Phi_6^2\Phi_{10}^4\Phi_{18}^2$ $\Phi_6^2\Phi_{10}^6\Phi_{12}$

$\Phi_6^2\Phi_{12}\Phi_{14}^4$ $\Phi_6^2\Phi_{12}\Phi_{15}^3$ $\Phi_6^2\Phi_{12}\Phi_{18}^4$ $\Phi_6^2\Phi_{12}\Phi_{20}^3$ $\Phi_6^2\Phi_{12}\Phi_{21}^2$ $\Phi_6^2\Phi_{12}\Phi_{24}^3$ $\Phi_6^2\Phi_{12}\Phi_{26}^2$

$\Phi_6^2\Phi_{12}\Phi_{28}^2$ $\Phi_6^2\Phi_{12}\Phi_{30}^3$ $\Phi_6^2\Phi_{12}\Phi_{35}$ $\Phi_6^2\Phi_{12}\Phi_{36}^2$ $\Phi_6^2\Phi_{12}\Phi_{39}$ $\Phi_6^2\Phi_{12}\Phi_{42}^2$ $\Phi_6^2\Phi_{12}\Phi_{45}$

$\Phi_6^2\Phi_{12}\Phi_{52}$ $\Phi_6^2\Phi_{12}\Phi_{56}$ $\Phi_6^2\Phi_{12}\Phi_{70}$ $\Phi_6^2\Phi_{12}\Phi_{72}$ $\Phi_6^2\Phi_{12}\Phi_{78}$ $\Phi_6^2\Phi_{12}\Phi_{84}$ $\Phi_6^2\Phi_{12}\Phi_{90}$ $\Phi_6^2\Phi_{12}^2\Phi_{66}$

$\Phi_6^2\Phi_{12}^3\Phi_{15}^2$ $\Phi_6^2\Phi_{12}^3\Phi_{20}^2$ $\Phi_6^2\Phi_{12}^3\Phi_{24}^2$ $\Phi_6^2\Phi_{12}^3\Phi_{30}^2$ $\Phi_6^2\Phi_{12}^3\Phi_{40}$ $\Phi_6^2\Phi_{12}^3\Phi_{48}$ $\Phi_6^2\Phi_{12}^3\Phi_{60}$

$\Phi_6^2\Phi_{12}^4\Phi_{18}^2$ $\Phi_6^2\Phi_{12}^4\Phi_{36}$ $\Phi_6^2\Phi_{12}^5\Phi_{15}$ $\Phi_6^2\Phi_{12}^5\Phi_{20}$ $\Phi_6^2\Phi_{12}^5\Phi_{24}$ $\Phi_6^2\Phi_{12}^5\Phi_{30}$ $\Phi_6^2\Phi_{15}\Phi_{66}$ $\Phi_6^2\Phi_{15}^2\Phi_{18}^2$

$\Phi_6^2\Phi_{18}^2\Phi_{20}^2$ $\Phi_6^2\Phi_{18}^2\Phi_{24}^2$ $\Phi_6^2\Phi_{18}^2\Phi_{30}^2$ $\Phi_6^2\Phi_{18}^2\Phi_{40}$ $\Phi_6^2\Phi_{18}^2\Phi_{48}$ $\Phi_6^2\Phi_{18}^2\Phi_{60}$ $\Phi_6^2\Phi_{20}\Phi_{66}$ $\Phi_6^2\Phi_{24}\Phi_{66}$

$\Phi_6^2\Phi_{30}\Phi_{66}$ $\Phi_6^3\Phi_{10}^2\Phi_{18}^3$ $\Phi_6^3\Phi_{10}^2\Phi_{54}$ $\Phi_6^3\Phi_{12}^2\Phi_{18}^3$ $\Phi_6^3\Phi_{12}^2\Phi_{54}$ $\Phi_6^3\Phi_{12}^5\Phi_{18}$ $\Phi_6^3\Phi_{15}\Phi_{18}^3$ $\Phi_6^3\Phi_{15}\Phi_{54}$

$\Phi_6^3\Phi_{18}\Phi_{66}$ $\Phi_6^3\Phi_{18}^3\Phi_{20}$ $\Phi_6^3\Phi_{18}^3\Phi_{24}$ $\Phi_6^3\Phi_{18}^3\Phi_{30}$ $\Phi_6^3\Phi_{20}\Phi_{54}$ $\Phi_6^3\Phi_{24}\Phi_{54}$ $\Phi_6^3\Phi_{30}\Phi_{54}$ $\Phi_6^4\Phi_{10}\Phi_{50}$

$\Phi_6^4\Phi_{10}^2\Phi_{12}^4$ $\Phi_6^4\Phi_{10}^2\Phi_{15}^2$ $\Phi_6^4\Phi_{10}^2\Phi_{20}^2$ $\Phi_6^4\Phi_{10}^2\Phi_{24}^2$ $\Phi_6^4\Phi_{10}^2\Phi_{30}^2$ $\Phi_6^4\Phi_{10}^2\Phi_{40}$ $\Phi_6^4\Phi_{10}^2\Phi_{48}$ $\Phi_6^4\Phi_{10}^2\Phi_{60}$

$\Phi_6^4\Phi_{10}^4\Phi_{12}^2$ $\Phi_6^4\Phi_{10}^4\Phi_{15}$ $\Phi_6^4\Phi_{10}^4\Phi_{20}$ $\Phi_6^4\Phi_{10}^4\Phi_{24}$ $\Phi_6^4\Phi_{10}^4\Phi_{30}$ $\Phi_6^4\Phi_{12}\Phi_{66}$ $\Phi_6^4\Phi_{12}^2\Phi_{15}^2$ $\Phi_6^4\Phi_{12}^2\Phi_{20}^2$

$\Phi_6^4\Phi_{12}^2\Phi_{24}^2$ $\Phi_6^4\Phi_{12}^2\Phi_{30}^2$ $\Phi_6^4\Phi_{12}^2\Phi_{40}$ $\Phi_6^4\Phi_{12}^2\Phi_{48}$ $\Phi_6^4\Phi_{12}^2\Phi_{60}$ $\Phi_6^4\Phi_{12}^3\Phi_{18}^2$ $\Phi_6^4\Phi_{12}^3\Phi_{36}$

$\Phi_6^4\Phi_{12}^4\Phi_{15}$ $\Phi_6^4\Phi_{12}^4\Phi_{20}$ $\Phi_6^4\Phi_{12}^4\Phi_{24}$ $\Phi_6^4\Phi_{12}^4\Phi_{30}$ $\Phi_6^4\Phi_{14}^2\Phi_{42}$ $\Phi_6^4\Phi_{15}\Phi_{20}^2$ $\Phi_6^4\Phi_{15}\Phi_{24}^2$ $\Phi_6^4\Phi_{15}\Phi_{30}^2$

$\Phi_6^4\Phi_{15}\Phi_{40}$ $\Phi_6^4\Phi_{15}\Phi_{48}$ $\Phi_6^4\Phi_{15}\Phi_{60}$ $\Phi_6^4\Phi_{15}^2\Phi_{20}$ $\Phi_6^4\Phi_{15}^2\Phi_{24}$ $\Phi_6^4\Phi_{15}^2\Phi_{30}$ $\Phi_6^4\Phi_{18}\Phi_{54}$

$\Phi_6^4\Phi_{18}^2\Phi_{36}$ $\Phi_6^4\Phi_{20}\Phi_{24}^2$ $\Phi_6^4\Phi_{20}\Phi_{30}^2$ $\Phi_6^4\Phi_{20}\Phi_{40}$ $\Phi_6^4\Phi_{20}\Phi_{48}$ $\Phi_6^4\Phi_{20}\Phi_{60}$ $\Phi_6^4\Phi_{20}^2\Phi_{24}$

$\Phi_6^4\Phi_{20}^2\Phi_{30}$ $\Phi_6^4\Phi_{24}\Phi_{30}^2$ $\Phi_6^4\Phi_{24}\Phi_{40}$ $\Phi_6^4\Phi_{24}\Phi_{48}$ $\Phi_6^4\Phi_{24}\Phi_{60}$ $\Phi_6^4\Phi_{24}^2\Phi_{30}$ $\Phi_6^4\Phi_{30}\Phi_{40}$

$\Phi_6^4\Phi_{30}\Phi_{48}$ $\Phi_6^4\Phi_{30}\Phi_{60}$ $\Phi_6^5\Phi_{10}^4\Phi_{18}$ $\Phi_6^5\Phi_{12}\Phi_{18}^3$ $\Phi_6^5\Phi_{12}\Phi_{54}$ $\Phi_6^5\Phi_{12}^4\Phi_{18}$ $\Phi_6^5\Phi_{15}^2\Phi_{18}$

$\Phi_6^5\Phi_{18}\Phi_{20}^2$ $\Phi_6^5\Phi_{18}\Phi_{24}^2$ $\Phi_6^5\Phi_{18}\Phi_{30}^2$ $\Phi_6^5\Phi_{18}\Phi_{40}$ $\Phi_6^5\Phi_{18}\Phi_{48}$ $\Phi_6^5\Phi_{18}\Phi_{60}$ $\Phi_6^6\Phi_{10}^2\Phi_{12}^3$

$\Phi_6^6\Phi_{10}^2\Phi_{18}^2$ $\Phi_6^6\Phi_{10}^4\Phi_{12}$ $\Phi_6^6\Phi_{12}\Phi_{15}^2$ $\Phi_6^6\Phi_{12}\Phi_{20}^2$ $\Phi_6^6\Phi_{12}\Phi_{24}^2$ $\Phi_6^6\Phi_{12}\Phi_{30}^2$ $\Phi_6^6\Phi_{12}\Phi_{40}$

$\Phi_6^6\Phi_{12}\Phi_{48}$ $\Phi_6^6\Phi_{12}\Phi_{60}$ $\Phi_6^6\Phi_{12}^2\Phi_{18}^2$ $\Phi_6^6\Phi_{12}^2\Phi_{36}$ $\Phi_6^6\Phi_{12}^3\Phi_{15}$ $\Phi_6^6\Phi_{12}^3\Phi_{20}$ $\Phi_6^6\Phi_{12}^3\Phi_{24}$

$\Phi_6^6\Phi_{12}^3\Phi_{30}$ $\Phi_6^6\Phi_{15}\Phi_{18}^2$ $\Phi_6^6\Phi_{18}^2\Phi_{20}$ $\Phi_6^6\Phi_{18}^2\Phi_{24}$ $\Phi_6^6\Phi_{18}^2\Phi_{30}$ $\Phi_6^7\Phi_{12}^3\Phi_{18}$ $\Phi_6^8\Phi_{10}^2\Phi_{12}^2$

$\Phi_6^8\Phi_{10}^2\Phi_{15}$ $\Phi_6^8\Phi_{10}^2\Phi_{20}$ $\Phi_6^8\Phi_{10}^2\Phi_{24}$ $\Phi_6^8\Phi_{10}^2\Phi_{30}$ $\Phi_6^8\Phi_{12}\Phi_{18}^2$ $\Phi_6^8\Phi_{12}\Phi_{36}$ $\Phi_6^8\Phi_{12}^2\Phi_{15}$

$\Phi_6^8\Phi_{12}^2\Phi_{20}$ $\Phi_6^8\Phi_{12}^2\Phi_{24}$ $\Phi_6^8\Phi_{12}^2\Phi_{30}$ $\Phi_6^8\Phi_{15}\Phi_{20}$ $\Phi_6^8\Phi_{15}\Phi_{24}$ $\Phi_6^8\Phi_{15}\Phi_{30}$ $\Phi_6^8\Phi_{20}\Phi_{24}$

$\Phi_6^8\Phi_{20}\Phi_{30}$ $\Phi_6^8\Phi_{24}\Phi_{30}$ $\Phi_6^9\Phi_{10}^2\Phi_{18}$ $\Phi_6^9\Phi_{12}^2\Phi_{18}$ $\Phi_6^9\Phi_{15}\Phi_{18}$ $\Phi_6^9\Phi_{18}\Phi_{20}$ $\Phi_6^9\Phi_{18}\Phi_{24}$

$\Phi_6^9\Phi_{18}\Phi_{30}$ $\Phi_6^{10}\Phi_{10}^2\Phi_{12}$ $\Phi_6^{10}\Phi_{12}\Phi_{15}$ $\Phi_6^{10}\Phi_{12}\Phi_{20}$ $\Phi_6^{10}\Phi_{12}\Phi_{24}$ $\Phi_6^{10}\Phi_{12}\Phi_{30}$ $\Phi_6^{11}\Phi_{12}\Phi_{18}$

$\Phi_{10}\Phi_{12}^2\Phi_{50}$ $\Phi_{10}\Phi_{15}\Phi_{50}$ $\Phi_{10}\Phi_{20}\Phi_{50}$ $\Phi_{10}\Phi_{24}\Phi_{50}$ $\Phi_{10}\Phi_{30}\Phi_{50}$ $\Phi_{10}^2\Phi_{12}^2\Phi_{15}^2$ $\Phi_{10}^2\Phi_{12}^2\Phi_{20}^2$

$\Phi_{10}^2\Phi_{12}^2\Phi_{24}^2$ $\Phi_{10}^2\Phi_{12}^2\Phi_{30}^2$ $\Phi_{10}^2\Phi_{12}^2\Phi_{40}$ $\Phi_{10}^2\Phi_{12}^2\Phi_{48}$ $\Phi_{10}^2\Phi_{12}^2\Phi_{60}$ $\Phi_{10}^2\Phi_{12}^3\Phi_{36}$ $\Phi_{10}^2\Phi_{12}^4\Phi_{15}$

$\Phi_{10}^2\Phi_{12}^4\Phi_{20}$ $\Phi_{10}^2\Phi_{12}^4\Phi_{24}$ $\Phi_{10}^2\Phi_{12}^4\Phi_{30}$ $\Phi_{10}^2\Phi_{14}^2\Phi_{42}$ $\Phi_{10}^2\Phi_{15}\Phi_{20}^2$ $\Phi_{10}^2\Phi_{15}\Phi_{24}^2$ $\Phi_{10}^2\Phi_{15}\Phi_{30}^2$ $\Phi_{10}^2\Phi_{15}\Phi_{40}$

$\Phi_{10}^2\Phi_{15}\Phi_{48}$ $\Phi_{10}^2\Phi_{15}\Phi_{60}$ $\Phi_{10}^2\Phi_{15}^2\Phi_{20}$ $\Phi_{10}^2\Phi_{15}^2\Phi_{24}$ $\Phi_{10}^2\Phi_{15}^2\Phi_{30}$ $\Phi_{10}^2\Phi_{18}\Phi_{54}$ $\Phi_{10}^2\Phi_{18}^2\Phi_{36}$

$\Phi_{10}^2\Phi_{20}\Phi_{24}^2$ $\Phi_{10}^2\Phi_{20}\Phi_{30}^2$ $\Phi_{10}^2\Phi_{20}\Phi_{40}$ $\Phi_{10}^2\Phi_{20}\Phi_{48}$ $\Phi_{10}^2\Phi_{20}\Phi_{60}$ $\Phi_{10}^2\Phi_{20}^2\Phi_{24}$ $\Phi_{10}^2\Phi_{20}^2\Phi_{30}$

$\Phi_{10}^2\Phi_{24}\Phi_{30}^2$ $\Phi_{10}^2\Phi_{24}\Phi_{40}$ $\Phi_{10}^2\Phi_{24}\Phi_{48}$ $\Phi_{10}^2\Phi_{24}\Phi_{60}$ $\Phi_{10}^2\Phi_{24}^2\Phi_{30}$ $\Phi_{10}^2\Phi_{30}\Phi_{40}$ $\Phi_{10}^2\Phi_{30}\Phi_{48}$

$\Phi_{10}^2\Phi_{30}\Phi_{60}$ $\Phi_{10}^4\Phi_{12}\Phi_{36}$ $\Phi_{10}^4\Phi_{12}^2\Phi_{15}$ $\Phi_{10}^4\Phi_{12}^2\Phi_{20}$ $\Phi_{10}^4\Phi_{12}^2\Phi_{24}$ $\Phi_{10}^4\Phi_{12}^2\Phi_{30}$ $\Phi_{10}^4\Phi_{15}\Phi_{20}$

$\Phi_{10}^4\Phi_{15}\Phi_{24}$ $\Phi_{10}^4\Phi_{15}\Phi_{30}$ $\Phi_{10}^4\Phi_{20}\Phi_{24}$ $\Phi_{10}^4\Phi_{20}\Phi_{30}$ $\Phi_{10}^4\Phi_{24}\Phi_{30}$ $\Phi_{12}\Phi_{15}^2\Phi_{36}$ $\Phi_{12}\Phi_{20}^2\Phi_{36}$

$\Phi_{12}\Phi_{24}^2\Phi_{36}$ $\Phi_{12}\Phi_{30}^2\Phi_{36}$ $\Phi_{12}\Phi_{36}\Phi_{40}$ $\Phi_{12}\Phi_{36}\Phi_{48}$ $\Phi_{12}\Phi_{36}\Phi_{60}$ $\Phi_{12}^2\Phi_{14}^2\Phi_{42}$ $\Phi_{12}^2\Phi_{15}\Phi_{20}^2$ $\Phi_{12}^2\Phi_{15}\Phi_{24}^2$

$\Phi_{12}^2\Phi_{15}\Phi_{30}^2$ $\Phi_{12}^2\Phi_{15}\Phi_{40}$ $\Phi_{12}^2\Phi_{15}\Phi_{48}$ $\Phi_{12}^2\Phi_{15}\Phi_{60}$ $\Phi_{12}^2\Phi_{15}^2\Phi_{20}$ $\Phi_{12}^2\Phi_{15}^2\Phi_{24}$ $\Phi_{12}^2\Phi_{15}^2\Phi_{30}$

$\Phi_{12}^2\Phi_{18}\Phi_{54}$ $\Phi_{12}^2\Phi_{18}^2\Phi_{36}$ $\Phi_{12}^2\Phi_{20}\Phi_{24}^2$ $\Phi_{12}^2\Phi_{20}\Phi_{30}^2$ $\Phi_{12}^2\Phi_{20}\Phi_{40}$ $\Phi_{12}^2\Phi_{20}\Phi_{48}$ $\Phi_{12}^2\Phi_{20}\Phi_{60}$

$\Phi_{12}^2\Phi_{20}^2\Phi_{24}$ $\Phi_{12}^2\Phi_{20}^2\Phi_{30}$ $\Phi_{12}^2\Phi_{24}\Phi_{30}^2$ $\Phi_{12}^2\Phi_{24}\Phi_{40}$ $\Phi_{12}^2\Phi_{24}\Phi_{48}$ $\Phi_{12}^2\Phi_{24}\Phi_{60}$ $\Phi_{12}^2\Phi_{24}^2\Phi_{30}$

$\Phi_{12}^2\Phi_{30}\Phi_{40}$ $\Phi_{12}^2\Phi_{30}\Phi_{48}$ $\Phi_{12}^2\Phi_{30}\Phi_{60}$ $\Phi_{12}^3\Phi_{15}\Phi_{36}$ $\Phi_{12}^3\Phi_{20}\Phi_{36}$ $\Phi_{12}^3\Phi_{24}\Phi_{36}$ $\Phi_{12}^3\Phi_{30}\Phi_{36}$

$\Phi_{12}^4\Phi_{15}\Phi_{20}$ $\Phi_{12}^4\Phi_{15}\Phi_{24}$ $\Phi_{12}^4\Phi_{15}\Phi_{30}$ $\Phi_{12}^4\Phi_{20}\Phi_{24}$ $\Phi_{12}^4\Phi_{20}\Phi_{30}$ $\Phi_{12}^4\Phi_{24}\Phi_{30}$ $\Phi_{14}^2\Phi_{15}\Phi_{42}$

$\Phi_{14}^2\Phi_{20}\Phi_{42}$ $\Phi_{14}^2\Phi_{24}\Phi_{42}$ $\Phi_{14}^2\Phi_{30}\Phi_{42}$ $\Phi_{15}\Phi_{18}\Phi_{54}$ $\Phi_{15}\Phi_{18}^2\Phi_{36}$ $\Phi_{15}\Phi_{20}\Phi_{24}^2$ $\Phi_{15}\Phi_{20}\Phi_{30}^2$ $\Phi_{15}\Phi_{20}\Phi_{40}$

$\Phi_{15}\Phi_{20}\Phi_{48}$ $\Phi_{15}\Phi_{20}\Phi_{60}$ $\Phi_{15}\Phi_{20}^2\Phi_{24}$ $\Phi_{15}\Phi_{20}^2\Phi_{30}$ $\Phi_{15}\Phi_{24}\Phi_{30}^2$ $\Phi_{15}\Phi_{24}\Phi_{40}$ $\Phi_{15}\Phi_{24}\Phi_{48}$ $\Phi_{15}\Phi_{24}\Phi_{60}$

$\Phi_{15}\Phi_{24}^2\Phi_{30}$ $\Phi_{15}\Phi_{30}\Phi_{40}$ $\Phi_{15}\Phi_{30}\Phi_{48}$ $\Phi_{15}\Phi_{30}\Phi_{60}$ $\Phi_{15}^2\Phi_{20}\Phi_{24}$ $\Phi_{15}^2\Phi_{20}\Phi_{30}$ $\Phi_{15}^2\Phi_{24}\Phi_{30}$ $\Phi_{18}\Phi_{20}\Phi_{54}$

$\Phi_{18}\Phi_{24}\Phi_{54}$ $\Phi_{18}\Phi_{30}\Phi_{54}$ $\Phi_{18}^2\Phi_{20}\Phi_{36}$ $\Phi_{18}^2\Phi_{24}\Phi_{36}$ $\Phi_{18}^2\Phi_{30}\Phi_{36}$ $\Phi_{20}\Phi_{24}\Phi_{30}^2$ $\Phi_{20}\Phi_{24}\Phi_{40}$ $\Phi_{20}\Phi_{24}\Phi_{48}$

$\Phi_{20}\Phi_{24}\Phi_{60}$ $\Phi_{20}\Phi_{24}^2\Phi_{30}$ $\Phi_{20}\Phi_{30}\Phi_{40}$ $\Phi_{20}\Phi_{30}\Phi_{48}$ $\Phi_{20}\Phi_{30}\Phi_{60}$ $\Phi_{20}^2\Phi_{24}\Phi_{30}$ $\Phi_{24}\Phi_{30}\Phi_{40}$ $\Phi_{24}\Phi_{30}\Phi_{48}$

$\Phi_{24}\Phi_{30}\Phi_{60}$

$\Phi_6\Phi_{10}\Phi_{18}\Phi_{50}$ $\Phi_6\Phi_{10}^2\Phi_{12}^4\Phi_{18}$ $\Phi_6\Phi_{10}^2\Phi_{15}^2\Phi_{18}$ $\Phi_6\Phi_{10}^2\Phi_{18}\Phi_{20}^2$ $\Phi_6\Phi_{10}^2\Phi_{18}\Phi_{24}^2$

$\Phi_6\Phi_{10}^2\Phi_{18}\Phi_{30}^2$ $\Phi_6\Phi_{10}^2\Phi_{18}\Phi_{40}$ $\Phi_6\Phi_{10}^2\Phi_{18}\Phi_{48}$ $\Phi_6\Phi_{10}^2\Phi_{18}\Phi_{60}$ $\Phi_6\Phi_{10}^4\Phi_{12}^2\Phi_{18}$

$\Phi_6\Phi_{10}^4\Phi_{15}\Phi_{18}$ $\Phi_6\Phi_{10}^4\Phi_{18}\Phi_{20}$ $\Phi_6\Phi_{10}^4\Phi_{18}\Phi_{24}$ $\Phi_6\Phi_{10}^4\Phi_{18}\Phi_{30}$ $\Phi_6\Phi_{12}^2\Phi_{15}^2\Phi_{18}$

$\Phi_6\Phi_{12}^2\Phi_{18}\Phi_{20}^2$ $\Phi_6\Phi_{12}^2\Phi_{18}\Phi_{24}^2$ $\Phi_6\Phi_{12}^2\Phi_{18}\Phi_{30}^2$ $\Phi_6\Phi_{12}^2\Phi_{18}\Phi_{40}$ $\Phi_6\Phi_{12}^2\Phi_{18}\Phi_{48}$

$\Phi_6\Phi_{12}^2\Phi_{18}\Phi_{60}$ $\Phi_6\Phi_{12}^3\Phi_{18}\Phi_{36}$ $\Phi_6\Phi_{12}^4\Phi_{15}\Phi_{18}$ $\Phi_6\Phi_{12}^4\Phi_{18}\Phi_{20}$ $\Phi_6\Phi_{12}^4\Phi_{18}\Phi_{24}$

$\Phi_6\Phi_{12}^4\Phi_{18}\Phi_{30}$ $\Phi_6\Phi_{14}^2\Phi_{18}\Phi_{42}$ $\Phi_6\Phi_{15}\Phi_{18}\Phi_{20}^2$ $\Phi_6\Phi_{15}\Phi_{18}\Phi_{24}^2$ $\Phi_6\Phi_{15}\Phi_{18}\Phi_{30}^2$ $\Phi_6\Phi_{15}\Phi_{18}\Phi_{40}$

$\Phi_6\Phi_{15}\Phi_{18}\Phi_{48}$ $\Phi_6\Phi_{15}\Phi_{18}\Phi_{60}$ $\Phi_6\Phi_{15}^2\Phi_{18}\Phi_{20}$ $\Phi_6\Phi_{15}^2\Phi_{18}\Phi_{24}$ $\Phi_6\Phi_{15}^2\Phi_{18}\Phi_{30}$

$\Phi_6\Phi_{18}\Phi_{20}\Phi_{24}^2$ $\Phi_6\Phi_{18}\Phi_{20}\Phi_{30}^2$ $\Phi_6\Phi_{18}\Phi_{20}\Phi_{40}$ $\Phi_6\Phi_{18}\Phi_{20}\Phi_{48}$ $\Phi_6\Phi_{18}\Phi_{20}\Phi_{60}$

$\Phi_6\Phi_{18}\Phi_{20}^2\Phi_{24}$ $\Phi_6\Phi_{18}\Phi_{20}^2\Phi_{30}$ $\Phi_6\Phi_{18}\Phi_{24}\Phi_{30}^2$ $\Phi_6\Phi_{18}\Phi_{24}\Phi_{40}$ $\Phi_6\Phi_{18}\Phi_{24}\Phi_{48}$

$\Phi_6\Phi_{18}\Phi_{24}\Phi_{60}$ $\Phi_6\Phi_{18}\Phi_{24}^2\Phi_{30}$ $\Phi_6\Phi_{18}\Phi_{30}\Phi_{40}$ $\Phi_6\Phi_{18}\Phi_{30}\Phi_{48}$ $\Phi_6\Phi_{18}\Phi_{30}\Phi_{60}$

$\Phi_6^2\Phi_{10}\Phi_{12}\Phi_{50}$ $\Phi_6^2\Phi_{10}^2\Phi_{12}\Phi_{15}^2$ $\Phi_6^2\Phi_{10}^2\Phi_{12}\Phi_{20}^2$ $\Phi_6^2\Phi_{10}^2\Phi_{12}\Phi_{24}^2$ $\Phi_6^2\Phi_{10}^2\Phi_{12}\Phi_{30}^2$

$\Phi_6^2\Phi_{10}^2\Phi_{12}\Phi_{40}$ $\Phi_6^2\Phi_{10}^2\Phi_{12}\Phi_{48}$ $\Phi_6^2\Phi_{10}^2\Phi_{12}\Phi_{60}$ $\Phi_6^2\Phi_{10}^2\Phi_{12}^2\Phi_{18}^2$ $\Phi_6^2\Phi_{10}^2\Phi_{12}^2\Phi_{36}$

$\Phi_6^2\Phi_{10}^2\Phi_{12}^3\Phi_{15}$ $\Phi_6^2\Phi_{10}^2\Phi_{12}^3\Phi_{20}$ $\Phi_6^2\Phi_{10}^2\Phi_{12}^3\Phi_{24}$ $\Phi_6^2\Phi_{10}^2\Phi_{12}^3\Phi_{30}$ $\Phi_6^2\Phi_{10}^2\Phi_{15}\Phi_{18}^2$
$\Phi_6^2\Phi_{10}^2\Phi_{18}^2\Phi_{20}$ $\Phi_6^2\Phi_{10}^2\Phi_{18}^2\Phi_{24}$ $\Phi_6^2\Phi_{10}^2\Phi_{18}^2\Phi_{30}$ $\Phi_6^2\Phi_{10}^4\Phi_{12}\Phi_{15}$ $\Phi_6^2\Phi_{10}^4\Phi_{12}\Phi_{20}$
$\Phi_6^2\Phi_{10}^4\Phi_{12}\Phi_{24}$ $\Phi_6^2\Phi_{10}^4\Phi_{12}\Phi_{30}$ $\Phi_6^2\Phi_{12}\Phi_{14}^2\Phi_{42}$ $\Phi_6^2\Phi_{12}\Phi_{15}\Phi_{20}^2$ $\Phi_6^2\Phi_{12}\Phi_{15}\Phi_{24}^2$ $\Phi_6^2\Phi_{12}\Phi_{15}\Phi_{30}^2$
$\Phi_6^2\Phi_{12}\Phi_{15}\Phi_{40}$ $\Phi_6^2\Phi_{12}\Phi_{15}\Phi_{48}$ $\Phi_6^2\Phi_{12}\Phi_{15}\Phi_{60}$ $\Phi_6^2\Phi_{12}\Phi_{15}^2\Phi_{20}$ $\Phi_6^2\Phi_{12}\Phi_{15}^2\Phi_{24}$
$\Phi_6^2\Phi_{12}\Phi_{15}^2\Phi_{30}$ $\Phi_6^2\Phi_{12}\Phi_{18}\Phi_{54}$ $\Phi_6^2\Phi_{12}\Phi_{18}^2\Phi_{36}$ $\Phi_6^2\Phi_{12}\Phi_{20}\Phi_{24}^2$ $\Phi_6^2\Phi_{12}\Phi_{20}\Phi_{30}^2$
$\Phi_6^2\Phi_{12}\Phi_{20}\Phi_{40}$ $\Phi_6^2\Phi_{12}\Phi_{20}\Phi_{48}$ $\Phi_6^2\Phi_{12}\Phi_{20}\Phi_{60}$ $\Phi_6^2\Phi_{12}\Phi_{20}^2\Phi_{24}$ $\Phi_6^2\Phi_{12}\Phi_{20}^2\Phi_{30}$
$\Phi_6^2\Phi_{12}\Phi_{24}\Phi_{30}^2$ $\Phi_6^2\Phi_{12}\Phi_{24}\Phi_{40}$ $\Phi_6^2\Phi_{12}\Phi_{24}\Phi_{48}$ $\Phi_6^2\Phi_{12}\Phi_{24}\Phi_{60}$ $\Phi_6^2\Phi_{12}\Phi_{24}^2\Phi_{30}$
$\Phi_6^2\Phi_{12}\Phi_{30}\Phi_{40}$ $\Phi_6^2\Phi_{12}\Phi_{30}\Phi_{48}$ $\Phi_6^2\Phi_{12}\Phi_{30}\Phi_{60}$ $\Phi_6^2\Phi_{12}^2\Phi_{15}\Phi_{18}^2$ $\Phi_6^2\Phi_{12}^2\Phi_{15}\Phi_{36}$
$\Phi_6^2\Phi_{12}^2\Phi_{18}^2\Phi_{20}$ $\Phi_6^2\Phi_{12}^2\Phi_{18}^2\Phi_{24}$ $\Phi_6^2\Phi_{12}^2\Phi_{18}^2\Phi_{30}$ $\Phi_6^2\Phi_{12}^2\Phi_{20}\Phi_{36}$ $\Phi_6^2\Phi_{12}^2\Phi_{24}\Phi_{36}$
$\Phi_6^2\Phi_{12}^2\Phi_{30}\Phi_{36}$ $\Phi_6^2\Phi_{12}^3\Phi_{15}\Phi_{20}$ $\Phi_6^2\Phi_{12}^3\Phi_{15}\Phi_{24}$ $\Phi_6^2\Phi_{12}^3\Phi_{15}\Phi_{30}$ $\Phi_6^2\Phi_{12}^3\Phi_{20}\Phi_{24}$
$\Phi_6^2\Phi_{12}^3\Phi_{20}\Phi_{30}$ $\Phi_6^2\Phi_{12}^3\Phi_{24}\Phi_{30}$ $\Phi_6^2\Phi_{15}\Phi_{18}^2\Phi_{20}$ $\Phi_6^2\Phi_{15}\Phi_{18}^2\Phi_{24}$ $\Phi_6^2\Phi_{15}\Phi_{18}^2\Phi_{30}$
$\Phi_6^2\Phi_{18}^2\Phi_{20}\Phi_{24}$ $\Phi_6^2\Phi_{18}^2\Phi_{20}\Phi_{30}$ $\Phi_6^2\Phi_{18}^2\Phi_{24}\Phi_{30}$ $\Phi_6^3\Phi_{10}^2\Phi_{12}^3\Phi_{18}$ $\Phi_6^3\Phi_{10}^4\Phi_{12}\Phi_{18}$
$\Phi_6^3\Phi_{12}\Phi_{15}^2\Phi_{18}$ $\Phi_6^3\Phi_{12}\Phi_{18}\Phi_{20}^2$ $\Phi_6^3\Phi_{12}\Phi_{18}\Phi_{24}^2$ $\Phi_6^3\Phi_{12}\Phi_{18}\Phi_{30}^2$ $\Phi_6^3\Phi_{12}\Phi_{18}\Phi_{40}$
$\Phi_6^3\Phi_{12}\Phi_{18}\Phi_{48}$ $\Phi_6^3\Phi_{12}\Phi_{18}\Phi_{60}$ $\Phi_6^3\Phi_{12}^2\Phi_{18}\Phi_{36}$ $\Phi_6^3\Phi_{12}^3\Phi_{15}\Phi_{18}$ $\Phi_6^3\Phi_{12}^3\Phi_{18}\Phi_{20}$
$\Phi_6^3\Phi_{12}^3\Phi_{18}\Phi_{24}$ $\Phi_6^3\Phi_{12}^3\Phi_{18}\Phi_{30}$ $\Phi_6^4\Phi_{10}^2\Phi_{12}\Phi_{18}^2$ $\Phi_6^4\Phi_{10}^2\Phi_{12}\Phi_{36}$ $\Phi_6^4\Phi_{10}^2\Phi_{12}^2\Phi_{15}$
$\Phi_6^4\Phi_{10}^2\Phi_{12}^2\Phi_{20}$ $\Phi_6^4\Phi_{10}^2\Phi_{12}^2\Phi_{24}$ $\Phi_6^4\Phi_{10}^2\Phi_{12}^2\Phi_{30}$ $\Phi_6^4\Phi_{10}^2\Phi_{15}\Phi_{20}$ $\Phi_6^4\Phi_{10}^2\Phi_{15}\Phi_{24}$
$\Phi_6^4\Phi_{10}^2\Phi_{15}\Phi_{30}$ $\Phi_6^4\Phi_{10}^2\Phi_{20}\Phi_{24}$ $\Phi_6^4\Phi_{10}^2\Phi_{20}\Phi_{30}$ $\Phi_6^4\Phi_{10}^2\Phi_{24}\Phi_{30}$ $\Phi_6^4\Phi_{12}\Phi_{15}\Phi_{18}^2$
$\Phi_6^4\Phi_{12}\Phi_{15}\Phi_{36}$ $\Phi_6^4\Phi_{12}\Phi_{18}^2\Phi_{20}$ $\Phi_6^4\Phi_{12}\Phi_{18}^2\Phi_{24}$ $\Phi_6^4\Phi_{12}\Phi_{18}^2\Phi_{30}$ $\Phi_6^4\Phi_{12}\Phi_{20}\Phi_{36}$
$\Phi_6^4\Phi_{12}\Phi_{24}\Phi_{36}$ $\Phi_6^4\Phi_{12}\Phi_{30}\Phi_{36}$ $\Phi_6^4\Phi_{12}^2\Phi_{15}\Phi_{20}$ $\Phi_6^4\Phi_{12}^2\Phi_{15}\Phi_{24}$ $\Phi_6^4\Phi_{12}^2\Phi_{15}\Phi_{30}$
$\Phi_6^4\Phi_{12}^2\Phi_{20}\Phi_{24}$ $\Phi_6^4\Phi_{12}^2\Phi_{20}\Phi_{30}$ $\Phi_6^4\Phi_{12}^2\Phi_{24}\Phi_{30}$ $\Phi_6^4\Phi_{15}\Phi_{20}\Phi_{24}$ $\Phi_6^4\Phi_{15}\Phi_{20}\Phi_{30}$
$\Phi_6^4\Phi_{15}\Phi_{24}\Phi_{30}$ $\Phi_6^4\Phi_{20}\Phi_{24}\Phi_{30}$ $\Phi_6^5\Phi_{10}^2\Phi_{12}^2\Phi_{18}$ $\Phi_6^5\Phi_{10}^2\Phi_{15}\Phi_{18}$ $\Phi_6^5\Phi_{10}^2\Phi_{18}\Phi_{20}$
$\Phi_6^5\Phi_{10}^2\Phi_{18}\Phi_{24}$ $\Phi_6^5\Phi_{10}^2\Phi_{18}\Phi_{30}$ $\Phi_6^5\Phi_{12}\Phi_{18}\Phi_{36}$ $\Phi_6^5\Phi_{12}^2\Phi_{15}\Phi_{18}$ $\Phi_6^5\Phi_{12}^2\Phi_{18}\Phi_{20}$
$\Phi_6^5\Phi_{12}^2\Phi_{18}\Phi_{24}$ $\Phi_6^5\Phi_{12}^2\Phi_{18}\Phi_{30}$ $\Phi_6^5\Phi_{15}\Phi_{18}\Phi_{20}$ $\Phi_6^5\Phi_{15}\Phi_{18}\Phi_{24}$ $\Phi_6^5\Phi_{15}\Phi_{18}\Phi_{30}$
$\Phi_6^5\Phi_{18}\Phi_{20}\Phi_{24}$ $\Phi_6^5\Phi_{18}\Phi_{20}\Phi_{30}$ $\Phi_6^5\Phi_{18}\Phi_{24}\Phi_{30}$ $\Phi_6^6\Phi_{10}^2\Phi_{12}\Phi_{15}$ $\Phi_6^6\Phi_{10}^2\Phi_{12}\Phi_{20}$
$\Phi_6^6\Phi_{10}^2\Phi_{12}\Phi_{24}$ $\Phi_6^6\Phi_{10}^2\Phi_{12}\Phi_{30}$ $\Phi_6^6\Phi_{12}\Phi_{15}\Phi_{20}$ $\Phi_6^6\Phi_{12}\Phi_{15}\Phi_{24}$ $\Phi_6^6\Phi_{12}\Phi_{15}\Phi_{30}$
$\Phi_6^6\Phi_{12}\Phi_{20}\Phi_{24}$ $\Phi_6^6\Phi_{12}\Phi_{20}\Phi_{30}$ $\Phi_6^6\Phi_{12}\Phi_{24}\Phi_{30}$ $\Phi_6^7\Phi_{10}^2\Phi_{12}\Phi_{18}$ $\Phi_6^7\Phi_{12}\Phi_{15}\Phi_{18}$
$\Phi_6^7\Phi_{12}\Phi_{18}\Phi_{20}$ $\Phi_6^7\Phi_{12}\Phi_{18}\Phi_{24}$ $\Phi_6^7\Phi_{12}\Phi_{18}\Phi_{30}$ $\Phi_{10}^2\Phi_{12}\Phi_{15}\Phi_{36}$ $\Phi_{10}^2\Phi_{12}\Phi_{20}\Phi_{36}$
$\Phi_{10}^2\Phi_{12}\Phi_{24}\Phi_{36}$ $\Phi_{10}^2\Phi_{12}\Phi_{30}\Phi_{36}$ $\Phi_{10}^2\Phi_{12}^2\Phi_{15}\Phi_{20}$ $\Phi_{10}^2\Phi_{12}^2\Phi_{15}\Phi_{24}$ $\Phi_{10}^2\Phi_{12}^2\Phi_{15}\Phi_{30}$
$\Phi_{10}^2\Phi_{12}^2\Phi_{20}\Phi_{24}$ $\Phi_{10}^2\Phi_{12}^2\Phi_{20}\Phi_{30}$ $\Phi_{10}^2\Phi_{12}^2\Phi_{24}\Phi_{30}$ $\Phi_{10}^2\Phi_{15}\Phi_{20}\Phi_{24}$ $\Phi_{10}^2\Phi_{15}\Phi_{20}\Phi_{30}$
$\Phi_{10}^2\Phi_{15}\Phi_{24}\Phi_{30}$ $\Phi_{10}^2\Phi_{20}\Phi_{24}\Phi_{30}$ $\Phi_{12}\Phi_{15}\Phi_{20}\Phi_{36}$ $\Phi_{12}\Phi_{15}\Phi_{24}\Phi_{36}$ $\Phi_{12}\Phi_{15}\Phi_{30}\Phi_{36}$
$\Phi_{12}\Phi_{20}\Phi_{24}\Phi_{36}$ $\Phi_{12}\Phi_{20}\Phi_{30}\Phi_{36}$ $\Phi_{12}\Phi_{24}\Phi_{30}\Phi_{36}$ $\Phi_{12}^2\Phi_{15}\Phi_{20}\Phi_{24}$ $\Phi_{12}^2\Phi_{15}\Phi_{20}\Phi_{30}$
$\Phi_{12}^2\Phi_{15}\Phi_{24}\Phi_{30}$ $\Phi_{12}^2\Phi_{20}\Phi_{24}\Phi_{30}$ $\Phi_{15}\Phi_{20}\Phi_{24}\Phi_{30}$

$\Phi_6\Phi_{10}^2\Phi_{12}\Phi_{18}\Phi_{36}$ $\Phi_6\Phi_{10}^2\Phi_{12}^2\Phi_{15}\Phi_{18}$ $\Phi_6\Phi_{10}^2\Phi_{12}^2\Phi_{18}\Phi_{20}$ $\Phi_6\Phi_{10}^2\Phi_{12}^2\Phi_{18}\Phi_{24}$ $\Phi_6\Phi_{10}^2\Phi_{12}^2\Phi_{18}\Phi_{30}$
$\Phi_6\Phi_{10}^2\Phi_{15}\Phi_{18}\Phi_{20}$ $\Phi_6\Phi_{10}^2\Phi_{15}\Phi_{18}\Phi_{24}$ $\Phi_6\Phi_{10}^2\Phi_{15}\Phi_{18}\Phi_{30}$ $\Phi_6\Phi_{10}^2\Phi_{18}\Phi_{20}\Phi_{24}$ $\Phi_6\Phi_{10}^2\Phi_{18}\Phi_{20}\Phi_{30}$
$\Phi_6\Phi_{10}^2\Phi_{18}\Phi_{24}\Phi_{30}$ $\Phi_6\Phi_{12}\Phi_{15}\Phi_{18}\Phi_{36}$ $\Phi_6\Phi_{12}\Phi_{18}\Phi_{20}\Phi_{36}$ $\Phi_6\Phi_{12}\Phi_{18}\Phi_{24}\Phi_{36}$ $\Phi_6\Phi_{12}\Phi_{18}\Phi_{30}\Phi_{36}$
$\Phi_6\Phi_{12}^2\Phi_{15}\Phi_{18}\Phi_{20}$ $\Phi_6\Phi_{12}^2\Phi_{15}\Phi_{18}\Phi_{24}$ $\Phi_6\Phi_{12}^2\Phi_{15}\Phi_{18}\Phi_{30}$ $\Phi_6\Phi_{12}^2\Phi_{18}\Phi_{20}\Phi_{24}$ $\Phi_6\Phi_{12}^2\Phi_{18}\Phi_{20}\Phi_{30}$
$\Phi_6\Phi_{12}^2\Phi_{18}\Phi_{24}\Phi_{30}$ $\Phi_6\Phi_{15}\Phi_{18}\Phi_{20}\Phi_{24}$ $\Phi_6\Phi_{15}\Phi_{18}\Phi_{20}\Phi_{30}$ $\Phi_6\Phi_{15}\Phi_{18}\Phi_{24}\Phi_{30}$ $\Phi_6\Phi_{18}\Phi_{20}\Phi_{24}\Phi_{30}$
$\Phi_6^2\Phi_{10}^2\Phi_{12}\Phi_{15}\Phi_{20}$ $\Phi_6^2\Phi_{10}^2\Phi_{12}\Phi_{15}\Phi_{24}$ $\Phi_6^2\Phi_{10}^2\Phi_{12}\Phi_{15}\Phi_{30}$ $\Phi_6^2\Phi_{10}^2\Phi_{12}\Phi_{20}\Phi_{24}$ $\Phi_6^2\Phi_{10}^2\Phi_{12}\Phi_{20}\Phi_{30}$
$\Phi_6^2\Phi_{10}^2\Phi_{12}\Phi_{24}\Phi_{30}$ $\Phi_6^2\Phi_{12}\Phi_{15}\Phi_{20}\Phi_{24}$ $\Phi_6^2\Phi_{12}\Phi_{15}\Phi_{20}\Phi_{30}$ $\Phi_6^2\Phi_{12}\Phi_{15}\Phi_{24}\Phi_{30}$ $\Phi_6^2\Phi_{12}\Phi_{20}\Phi_{24}\Phi_{30}$
$\Phi_6^3\Phi_{10}^2\Phi_{12}\Phi_{15}\Phi_{18}$ $\Phi_6^3\Phi_{10}^2\Phi_{12}\Phi_{18}\Phi_{20}$ $\Phi_6^3\Phi_{10}^2\Phi_{12}\Phi_{18}\Phi_{24}$ $\Phi_6^3\Phi_{10}^2\Phi_{12}\Phi_{18}\Phi_{30}$ $\Phi_6^3\Phi_{12}\Phi_{15}\Phi_{18}\Phi_{20}$
$\Phi_6^3\Phi_{12}\Phi_{15}\Phi_{18}\Phi_{24}$ $\Phi_6^3\Phi_{12}\Phi_{15}\Phi_{18}\Phi_{30}$ $\Phi_6^3\Phi_{12}\Phi_{18}\Phi_{20}\Phi_{24}$ $\Phi_6^3\Phi_{12}\Phi_{18}\Phi_{20}\Phi_{30}$ $\Phi_6^3\Phi_{12}\Phi_{18}\Phi_{24}\Phi_{30}$

Il y a 846 polynômes.

Elimination des polynômes superflus

Nous allons, pour le reste du chapitre, diminuer le nombre de polynômes grâce à deux méthodes :

(A) Elimination des polynômes attachés à des réseaux décomposables

La proposition 3.1.5 nous apprend que si F et G sont tels que $\mathrm{Res}(F,G) = \pm 1$, alors tout FG-réseau unimodulaire se scinde en deux sous-réseaux unimodulaires de dimension inférieure.

Dans le cas qui nous intéresse, nous connaissons tous les réseaux de dimension inférieure à 32 possédant des isométries parfaites [Ker1]. Donc, tout polynôme attaché à un réseau scindé de dimension 32 peut être supprimé de la liste de la proposition 3.2.1; pour autant, bien entendu, que les deux sous-réseaux possèdent eux-mêmes des isométries parfaites.

D'autre part nous nous savons que $\mathrm{Res}(\Phi_m, \Phi_n) = \pm 1$, sauf si $m = p^r n$ avec p premier (cf. lemme 1.3.7). En outre, on a vu dans le même lemme que $\mathrm{Res}(FG,H) = \mathrm{Res}(F,H)\,\mathrm{Res}(G,H)$ pour tout $F,G,H \in \mathbb{Z}[X]$.

Ces résultats nous permettent d'énoncer la proposition suivante :

Proposition 3.2.2

Soit (M,β) un $\mathbb{Z}$-réseau unimodulaire indécomposable, pair et de dimension 32. Si (M,β) possède une isométrie parfaite, alors le polynôme caractéristique de cette isométrie est un des polynômes suivants :

Φ_6^{16} Φ_{10}^8 Φ_{12}^8 Φ_{15}^4 Φ_{20}^4 Φ_{24}^4 Φ_{30}^4 Φ_{34}^2 Φ_{40}^2 Φ_{48}^2 Φ_{51} Φ_{60}^2 Φ_{68} Φ_{80} Φ_{96} Φ_{102} Φ_{120}
$\Phi_6\Phi_{18}^5$ $\Phi_6^2\Phi_{12}^7$ $\Phi_6^4\Phi_{12}^6$ $\Phi_6^4\Phi_{18}^4$ $\Phi_6^4\Phi_{24}^3$ $\Phi_6^4\Phi_{30}^3$ $\Phi_6^4\Phi_{42}^2$ $\Phi_6^4\Phi_{78}$ $\Phi_6^6\Phi_{12}^5$ $\Phi_6^6\Phi_{66}$ $\Phi_6^7\Phi_{18}^3$
$\Phi_6^7\Phi_{54}$ $\Phi_6^8\Phi_{12}^4$ $\Phi_6^8\Phi_{24}^2$ $\Phi_6^8\Phi_{30}^2$ $\Phi_6^8\Phi_{48}$ $\Phi_6^{10}\Phi_{12}^3$ $\Phi_6^{10}\Phi_{18}^2$ $\Phi_6^{12}\Phi_{12}^2$ $\Phi_6^{12}\Phi_{24}$ $\Phi_6^{12}\Phi_{30}$
$\Phi_6^{13}\Phi_{18}$ $\Phi_6^{14}\Phi_{12}$ $\Phi_{10}^2\Phi_{20}^3$ $\Phi_{10}^2\Phi_{30}^3$ $\Phi_{10}^2\Phi_{70}$ $\Phi_{10}^2\Phi_{90}$ $\Phi_{10}^3\Phi_{50}$ $\Phi_{10}^4\Phi_{20}^2$ $\Phi_{10}^4\Phi_{30}^2$ $\Phi_{10}^4\Phi_{40}$
$\Phi_{10}^6\Phi_{20}$ $\Phi_{10}^6\Phi_{30}$ $\Phi_{12}^2\Phi_{24}^3$ $\Phi_{12}^2\Phi_{36}^2$ $\Phi_{12}^2\Phi_{84}$ $\Phi_{12}^4\Phi_{24}^2$ $\Phi_{12}^4\Phi_{48}$ $\Phi_{12}^4\Phi_{60}$ $\Phi_{12}^5\Phi_{36}$ $\Phi_{12}^6\Phi_{24}$
$\Phi_{15}\Phi_{30}^3$ $\Phi_{15}\Phi_{45}$ $\Phi_{15}^2\Phi_{30}^2$ $\Phi_{15}^2\Phi_{60}$ $\Phi_{15}^3\Phi_{30}$ $\Phi_{20}^2\Phi_{40}$ $\Phi_{20}^2\Phi_{60}$ $\Phi_{24}\Phi_{72}$ $\Phi_{24}^2\Phi_{48}$ $\Phi_{30}\Phi_{90}$
$\Phi_{30}^2\Phi_{60}$
$\Phi_6\Phi_{12}^6\Phi_{18}$ $\Phi_6\Phi_{18}\Phi_{24}^3$ $\Phi_6\Phi_{18}\Phi_{30}^3$ $\Phi_6\Phi_{18}\Phi_{36}^2$ $\Phi_6\Phi_{18}\Phi_{42}^2$ $\Phi_6\Phi_{18}\Phi_{72}$ $\Phi_6\Phi_{18}\Phi_{78}$
$\Phi_6\Phi_{18}\Phi_{90}$ $\Phi_6\Phi_{18}^2\Phi_{54}$ $\Phi_6\Phi_{18}^3\Phi_{36}$ $\Phi_6^2\Phi_{12}\Phi_{18}^4$ $\Phi_6^2\Phi_{12}\Phi_{24}^3$ $\Phi_6^2\Phi_{12}\Phi_{30}^3$ $\Phi_6^2\Phi_{12}\Phi_{36}^2$
$\Phi_6^2\Phi_{12}\Phi_{42}^2$ $\Phi_6^2\Phi_{12}\Phi_{78}$ $\Phi_6^2\Phi_{12}\Phi_{84}$ $\Phi_6^2\Phi_{12}^2\Phi_{66}$ $\Phi_6^2\Phi_{12}^3\Phi_{24}^2$ $\Phi_6^2\Phi_{12}^3\Phi_{30}^2$ $\Phi_6^2\Phi_{12}^3\Phi_{48}$ $\Phi_6^2\Phi_{12}^3\Phi_{60}$
$\Phi_6^2\Phi_{12}^4\Phi_{18}^2$ $\Phi_6^2\Phi_{12}^4\Phi_{36}$ $\Phi_6^2\Phi_{12}^5\Phi_{24}$ $\Phi_6^2\Phi_{12}^5\Phi_{30}$ $\Phi_6^2\Phi_{18}^2\Phi_{24}^2$ $\Phi_6^2\Phi_{18}^2\Phi_{30}^2$ $\Phi_6^2\Phi_{18}^2\Phi_{48}$ $\Phi_6^2\Phi_{24}\Phi_{66}$ $\Phi_6^2\Phi_{30}\Phi_{66}$
$\Phi_6^3\Phi_{12}^2\Phi_{18}^3$ $\Phi_6^3\Phi_{12}^2\Phi_{54}$ $\Phi_6^3\Phi_{12}^5\Phi_{18}$ $\Phi_6^3\Phi_{18}\Phi_{66}$ $\Phi_6^3\Phi_{18}^3\Phi_{24}$ $\Phi_6^3\Phi_{18}^3\Phi_{30}$ $\Phi_6^3\Phi_{24}\Phi_{54}$ $\Phi_6^3\Phi_{30}\Phi_{54}$
$\Phi_6^4\Phi_{10}^2\Phi_{30}^2$ $\Phi_6^4\Phi_{10}^4\Phi_{30}$ $\Phi_6^4\Phi_{12}\Phi_{66}$ $\Phi_6^4\Phi_{12}^2\Phi_{24}^2$ $\Phi_6^4\Phi_{12}^2\Phi_{30}^2$ $\Phi_6^4\Phi_{12}^2\Phi_{48}$ $\Phi_6^4\Phi_{12}^2\Phi_{60}$ $\Phi_6^4\Phi_{12}^3\Phi_{18}^2$
$\Phi_6^4\Phi_{12}^3\Phi_{36}$ $\Phi_6^4\Phi_{12}^4\Phi_{24}$ $\Phi_6^4\Phi_{12}^4\Phi_{30}$ $\Phi_6^4\Phi_{14}^2\Phi_{42}$ $\Phi_6^4\Phi_{15}\Phi_{30}^2$ $\Phi_6^4\Phi_{15}^2\Phi_{30}$ $\Phi_6^4\Phi_{18}\Phi_{54}$ $\Phi_6^4\Phi_{18}^2\Phi_{36}$
$\Phi_6^4\Phi_{24}\Phi_{30}^2$ $\Phi_6^4\Phi_{24}\Phi_{48}$ $\Phi_6^4\Phi_{24}^2\Phi_{30}$ $\Phi_6^4\Phi_{30}\Phi_{48}$ $\Phi_6^4\Phi_{30}\Phi_{60}$ $\Phi_6^5\Phi_{12}\Phi_{18}^3$ $\Phi_6^5\Phi_{12}\Phi_{54}$
$\Phi_6^5\Phi_{12}^4\Phi_{18}$ $\Phi_6^5\Phi_{18}\Phi_{24}^2$ $\Phi_6^5\Phi_{18}\Phi_{30}^2$ $\Phi_6^5\Phi_{18}\Phi_{48}$ $\Phi_6^6\Phi_{12}\Phi_{24}^2$ $\Phi_6^6\Phi_{12}\Phi_{30}^2$ $\Phi_6^6\Phi_{12}\Phi_{48}$
$\Phi_6^6\Phi_{12}\Phi_{60}$ $\Phi_6^6\Phi_{12}^2\Phi_{18}^2$ $\Phi_6^6\Phi_{12}^2\Phi_{36}$ $\Phi_6^6\Phi_{12}^3\Phi_{24}$ $\Phi_6^6\Phi_{12}^3\Phi_{30}$ $\Phi_6^6\Phi_{18}^2\Phi_{24}$ $\Phi_6^6\Phi_{18}^2\Phi_{30}$
$\Phi_6^7\Phi_{12}^3\Phi_{18}$ $\Phi_6^8\Phi_{10}^2\Phi_{30}$ $\Phi_6^8\Phi_{12}\Phi_{18}^2$ $\Phi_6^8\Phi_{12}\Phi_{36}$ $\Phi_6^8\Phi_{12}^2\Phi_{24}$ $\Phi_6^8\Phi_{12}^2\Phi_{30}$ $\Phi_6^8\Phi_{15}\Phi_{30}$
$\Phi_6^8\Phi_{24}\Phi_{30}$ $\Phi_6^9\Phi_{12}^2\Phi_{18}$ $\Phi_6^9\Phi_{18}\Phi_{24}$ $\Phi_6^9\Phi_{18}\Phi_{30}$ $\Phi_6^{10}\Phi_{12}\Phi_{24}$ $\Phi_6^{10}\Phi_{12}\Phi_{30}$ $\Phi_6^{11}\Phi_{12}\Phi_{18}$
$\Phi_{10}\Phi_{20}\Phi_{50}$ $\Phi_{10}\Phi_{30}\Phi_{50}$ $\Phi_{10}^2\Phi_{12}^3\Phi_{36}$ $\Phi_{10}^2\Phi_{15}\Phi_{30}^2$ $\Phi_{10}^2\Phi_{15}^2\Phi_{30}$ $\Phi_{10}^2\Phi_{20}\Phi_{30}^2$ $\Phi_{10}^2\Phi_{20}\Phi_{40}$
$\Phi_{10}^2\Phi_{20}\Phi_{60}$ $\Phi_{10}^2\Phi_{20}^2\Phi_{30}$ $\Phi_{10}^2\Phi_{30}\Phi_{40}$ $\Phi_{10}^2\Phi_{30}\Phi_{60}$ $\Phi_{10}^4\Phi_{15}\Phi_{30}$ $\Phi_{10}^4\Phi_{20}\Phi_{30}$ $\Phi_{12}\Phi_{24}^2\Phi_{36}$
$\Phi_{12}\Phi_{36}\Phi_{48}$ $\Phi_{12}\Phi_{36}\Phi_{60}$ $\Phi_{12}^2\Phi_{15}\Phi_{60}$ $\Phi_{12}^2\Phi_{18}^2\Phi_{36}$ $\Phi_{12}^2\Phi_{20}\Phi_{60}$ $\Phi_{12}^2\Phi_{24}\Phi_{48}$ $\Phi_{12}^2\Phi_{24}\Phi_{60}$
$\Phi_{12}^2\Phi_{30}\Phi_{60}$ $\Phi_{12}^3\Phi_{15}\Phi_{36}$ $\Phi_{12}^3\Phi_{20}\Phi_{36}$ $\Phi_{12}^3\Phi_{24}\Phi_{36}$ $\Phi_{12}^3\Phi_{30}\Phi_{36}$ $\Phi_{15}\Phi_{20}\Phi_{60}$ $\Phi_{15}\Phi_{30}\Phi_{60}$
$\Phi_{20}\Phi_{30}\Phi_{60}$

$\Phi_6\Phi_{10}^2\Phi_{18}\Phi_{30}^2$ $\Phi_6\Phi_{10}^4\Phi_{18}\Phi_{30}$ $\Phi_6\Phi_{12}^2\Phi_{18}\Phi_{24}^2$ $\Phi_6\Phi_{12}^2\Phi_{18}\Phi_{30}^2$ $\Phi_6\Phi_{12}^2\Phi_{18}\Phi_{48}$
$\Phi_6\Phi_{12}^2\Phi_{18}\Phi_{60}$ $\Phi_6\Phi_{12}^3\Phi_{18}\Phi_{36}$ $\Phi_6\Phi_{12}^4\Phi_{18}\Phi_{24}$ $\Phi_6\Phi_{12}^4\Phi_{18}\Phi_{30}$ $\Phi_6\Phi_{14}^2\Phi_{18}\Phi_{42}$ $\Phi_6\Phi_{15}\Phi_{18}\Phi_{30}^2$
$\Phi_6\Phi_{15}^2\Phi_{18}\Phi_{30}$ $\Phi_6\Phi_{18}\Phi_{24}\Phi_{30}^2$ $\Phi_6\Phi_{18}\Phi_{24}\Phi_{48}$ $\Phi_6\Phi_{18}\Phi_{24}^2\Phi_{30}$ $\Phi_6\Phi_{18}\Phi_{30}\Phi_{48}$
$\Phi_6\Phi_{18}\Phi_{30}\Phi_{60}$ $\Phi_6^2\Phi_{10}^2\Phi_{12}\Phi_{30}^2$ $\Phi_6^2\Phi_{10}^2\Phi_{12}^2\Phi_{36}$ $\Phi_6^2\Phi_{10}^2\Phi_{12}^3\Phi_{30}$ $\Phi_6^2\Phi_{10}^2\Phi_{18}^2\Phi_{30}$
$\Phi_6^2\Phi_{10}^4\Phi_{12}\Phi_{30}$ $\Phi_6^2\Phi_{12}\Phi_{14}^2\Phi_{42}$ $\Phi_6^2\Phi_{12}\Phi_{15}\Phi_{30}^2$ $\Phi_6^2\Phi_{12}\Phi_{15}\Phi_{60}$ $\Phi_6^2\Phi_{12}\Phi_{15}^2\Phi_{30}$ $\Phi_6^2\Phi_{12}\Phi_{18}\Phi_{54}$
$\Phi_6^2\Phi_{12}\Phi_{18}^2\Phi_{36}$ $\Phi_6^2\Phi_{12}\Phi_{20}\Phi_{60}$ $\Phi_6^2\Phi_{12}\Phi_{24}\Phi_{30}^2$ $\Phi_6^2\Phi_{12}\Phi_{24}\Phi_{48}$ $\Phi_6^2\Phi_{12}\Phi_{24}\Phi_{60}$
$\Phi_6^2\Phi_{12}\Phi_{24}^2\Phi_{30}$ $\Phi_6^2\Phi_{12}\Phi_{30}\Phi_{48}$ $\Phi_6^2\Phi_{12}\Phi_{30}\Phi_{60}$ $\Phi_6^2\Phi_{12}^2\Phi_{15}\Phi_{36}$ $\Phi_6^2\Phi_{12}^2\Phi_{18}^2\Phi_{24}$
$\Phi_6^2\Phi_{12}^2\Phi_{18}^2\Phi_{30}$ $\Phi_6^2\Phi_{12}^2\Phi_{20}\Phi_{36}$ $\Phi_6^2\Phi_{12}^2\Phi_{24}\Phi_{36}$ $\Phi_6^2\Phi_{12}^2\Phi_{30}\Phi_{36}$ $\Phi_6^2\Phi_{12}^3\Phi_{15}\Phi_{30}$
$\Phi_6^2\Phi_{12}^3\Phi_{24}\Phi_{30}$ $\Phi_6^2\Phi_{15}\Phi_{18}^2\Phi_{30}$ $\Phi_6^2\Phi_{18}^2\Phi_{24}\Phi_{30}$ $\Phi_6^3\Phi_{12}\Phi_{18}\Phi_{24}^2$ $\Phi_6^3\Phi_{12}\Phi_{18}\Phi_{30}^2$
$\Phi_6^3\Phi_{12}\Phi_{18}\Phi_{48}$ $\Phi_6^3\Phi_{12}\Phi_{18}\Phi_{60}$ $\Phi_6^3\Phi_{12}^2\Phi_{18}\Phi_{36}$ $\Phi_6^3\Phi_{12}^3\Phi_{18}\Phi_{24}$ $\Phi_6^3\Phi_{12}^3\Phi_{18}\Phi_{30}$
$\Phi_6^4\Phi_{10}^2\Phi_{12}\Phi_{36}$ $\Phi_6^4\Phi_{10}^2\Phi_{12}^2\Phi_{30}$ $\Phi_6^4\Phi_{10}^2\Phi_{15}\Phi_{30}$ $\Phi_6^4\Phi_{10}^2\Phi_{20}\Phi_{30}$ $\Phi_6^4\Phi_{10}^2\Phi_{24}\Phi_{30}$
$\Phi_6^4\Phi_{12}\Phi_{15}\Phi_{36}$ $\Phi_6^4\Phi_{12}\Phi_{18}^2\Phi_{24}$ $\Phi_6^4\Phi_{12}\Phi_{18}^2\Phi_{30}$ $\Phi_6^4\Phi_{12}\Phi_{20}\Phi_{36}$ $\Phi_6^4\Phi_{12}\Phi_{24}\Phi_{36}$
$\Phi_6^4\Phi_{12}\Phi_{30}\Phi_{36}$ $\Phi_6^4\Phi_{12}^2\Phi_{15}\Phi_{30}$ $\Phi_6^4\Phi_{12}^2\Phi_{24}\Phi_{30}$ $\Phi_6^4\Phi_{15}\Phi_{24}\Phi_{30}$ $\Phi_6^5\Phi_{10}^2\Phi_{18}\Phi_{30}$
$\Phi_6^5\Phi_{12}\Phi_{18}\Phi_{36}$ $\Phi_6^5\Phi_{12}^2\Phi_{18}\Phi_{24}$ $\Phi_6^5\Phi_{12}^2\Phi_{18}\Phi_{30}$ $\Phi_6^5\Phi_{15}\Phi_{18}\Phi_{30}$ $\Phi_6^5\Phi_{18}\Phi_{24}\Phi_{30}$
$\Phi_6^6\Phi_{10}^2\Phi_{12}\Phi_{30}$ $\Phi_6^6\Phi_{12}\Phi_{15}\Phi_{30}$ $\Phi_6^6\Phi_{12}\Phi_{24}\Phi_{30}$ $\Phi_6^7\Phi_{12}\Phi_{18}\Phi_{24}$ $\Phi_6^7\Phi_{12}\Phi_{18}\Phi_{30}$
$\Phi_{10}^2\Phi_{12}\Phi_{24}\Phi_{36}$ $\Phi_{10}^2\Phi_{15}\Phi_{20}\Phi_{30}$ $\Phi_{12}\Phi_{15}\Phi_{24}\Phi_{36}$ $\Phi_{12}\Phi_{20}\Phi_{24}\Phi_{36}$ $\Phi_{12}\Phi_{24}\Phi_{30}\Phi_{36}$
$\Phi_6\Phi_{10}^2\Phi_{12}\Phi_{18}\Phi_{36}$ $\Phi_6\Phi_{10}^2\Phi_{12}^2\Phi_{18}\Phi_{24}$ $\Phi_6\Phi_{10}^2\Phi_{12}^2\Phi_{18}\Phi_{30}$ $\Phi_6\Phi_{10}^2\Phi_{15}\Phi_{18}\Phi_{30}$ $\Phi_6\Phi_{10}^2\Phi_{18}\Phi_{20}\Phi_{30}$
$\Phi_6\Phi_{10}^2\Phi_{18}\Phi_{24}\Phi_{30}$ $\Phi_6\Phi_{12}\Phi_{15}\Phi_{18}\Phi_{36}$ $\Phi_6\Phi_{12}\Phi_{18}\Phi_{20}\Phi_{36}$ $\Phi_6\Phi_{12}\Phi_{18}\Phi_{24}\Phi_{36}$ $\Phi_6\Phi_{12}\Phi_{18}\Phi_{30}\Phi_{36}$
$\Phi_6\Phi_{12}^2\Phi_{15}\Phi_{18}\Phi_{24}$ $\Phi_6\Phi_{12}^2\Phi_{15}\Phi_{18}\Phi_{30}$ $\Phi_6\Phi_{12}^2\Phi_{18}\Phi_{20}\Phi_{24}$ $\Phi_6\Phi_{12}^2\Phi_{18}\Phi_{20}\Phi_{30}$ $\Phi_6\Phi_{12}^2\Phi_{18}\Phi_{24}\Phi_{30}$
$\Phi_6\Phi_{15}\Phi_{18}\Phi_{20}\Phi_{30}$ $\Phi_6\Phi_{15}\Phi_{18}\Phi_{24}\Phi_{30}$ $\Phi_6\Phi_{18}\Phi_{20}\Phi_{24}\Phi_{30}$ $\Phi_6^2\Phi_{10}^2\Phi_{12}\Phi_{15}\Phi_{30}$ $\Phi_6^2\Phi_{10}^2\Phi_{12}\Phi_{20}\Phi_{30}$
$\Phi_6^2\Phi_{10}^2\Phi_{12}\Phi_{24}\Phi_{30}$ $\Phi_6^2\Phi_{12}\Phi_{15}\Phi_{20}\Phi_{30}$ $\Phi_6^2\Phi_{12}\Phi_{15}\Phi_{24}\Phi_{30}$ $\Phi_6^2\Phi_{12}\Phi_{20}\Phi_{24}\Phi_{30}$ $\Phi_6^3\Phi_{10}^2\Phi_{12}\Phi_{18}\Phi_{24}$
$\Phi_6^3\Phi_{10}^2\Phi_{12}\Phi_{18}\Phi_{30}$ $\Phi_6^3\Phi_{12}\Phi_{15}\Phi_{18}\Phi_{24}$ $\Phi_6^3\Phi_{12}\Phi_{15}\Phi_{18}\Phi_{30}$ $\Phi_6^3\Phi_{12}\Phi_{18}\Phi_{20}\Phi_{24}$ $\Phi_6^3\Phi_{12}\Phi_{18}\Phi_{20}\Phi_{30}$
$\Phi_6^3\Phi_{12}\Phi_{18}\Phi_{24}\Phi_{30}$

Démonstration :

La liste ci-dessus est inclue dans la liste de la proposition 3.2.1. Raisonnons sur un exemple : considérons le polynôme $\Phi_6\Phi_{18}\Phi_{21}^2$. Ce polynôme est dans la liste de la proposition 3.2.1, mais pas dans celle ci-dessus. On a $\mathrm{Res}(\Phi_6\Phi_{18}, \Phi_{21}^2) = \mathrm{Res}(\Phi_6, \Phi_{21}^2)\,\mathrm{Res}(\Phi_{18}, \Phi_{21}^2) = 1$. En outre, $\Phi_6\Phi_{18}$ fait partie des polynômes de type 2 de degré 8, et Φ_{21}^2 fait partie des polynômes de type 1 de degré 24. Ainsi, les réseaux associés à $\Phi_6\Phi_{18}\Phi_{21}^2$ sont décomposables; il est donc normal que ce polynôme ne fasse pas partie de la liste ci-dessus. Chaque polynôme a été soumis à ce crible, la liste ci-dessus en est le résultat. Il reste tout de même 301 polynômes. ❄

(B) Elimination des polynômes par la méthode inspirée du lemme 3.1.6

Raisonnons sur deux exemples :

α) on sait grâce à la proposition 3.2.1 qu'il existe un réseau unimodulaire (M, β) et une isométrie t de M possédant Φ_{12}^8 comme polynôme caractéristique. La proposition 3.1.6 nous apprend que le polynôme caractéristique de t^2 est Φ_6^{16}. Cela veut dire que $\mathscr{E}(\Phi_{12}^8) \subset \mathscr{E}(\Phi_6^{16})$. Le polynôme Φ_{12}^8 est rendu ainsi inutile si on cherche à estimer le nombre de réseaux unimodulaires indécomposables associés aux polynômes de la liste de la proposition 3.2.2, c'est-à-dire possédant (au moins) une isométrie parfaite. Pour ne pas devoir nous répéter à chaque fois, nous noterons simplement $\Phi_{12}^8 \overset{t^2}{\rightsquigarrow} \Phi_6^{16}$.

β) Si t est de polynôme minimal $\Phi_{12}\Phi_{24}$, c'est-à-dire si t est de polynôme caractéristique $F = \Phi_{12}^2\Phi_{24}^3$, $\Phi_{12}^4\Phi_{24}^2$ ou $\Phi_{12}^6\Phi_{24}$, on dira alors que ce polynôme est "associé" à $\Phi_{12}\Phi_{24}$. Le polynôme minimal de t^2 vaut $\Phi_6\Phi_{12}$, car il ne doit pas posséder de facteur carré. Ce polynôme évalué en 1 vaut 1, donc le

polynôme caractéristique de t^2 est $G = \Phi_6^{n_1}\Phi_{12}^{n_2}$ doit se trouver obligatoirement dans la liste. Ainsi, $\mathscr{E}(F) \subset \mathscr{E}(G)$, et donc tous les polynômes associés à $\Phi_{12}\Phi_{24}$ sont alors éliminés. Remarquons que lorsque nous traiterons les polynômes associés à $\Phi_6\Phi_{12}$, nous ne tomberons pas sur $\Phi_{12}\Phi_{24}$, car notre procédé a pour effet de diminuer la grandeur des indices des polynômes cyclotomiques, ainsi que le nombre de facteurs irréductibles. Nous résumerons ce raisonnement par $\Phi_{12}\Phi_{24} \overset{t^2}{\rightsquigarrow} \Phi_6\Phi_{12}$.

(i) Les polynômes de la liste de la proposition 3.2.2 ne possédant qu'un facteur irréductible :

on a

$$\begin{array}{llll}
\Phi_{120} \overset{t^{12}}{\rightsquigarrow} \Phi_{10}^8, & \Phi_{102} \overset{t^2}{\rightsquigarrow} \Phi_{51} \\
\Phi_{60}^2 \overset{t^3}{\rightsquigarrow} \Phi_{20}^4, & \Phi_{30}^4 \overset{t^5}{\rightsquigarrow} \Phi_6^{16} \\
\Phi_{96} \overset{t^{16}}{\rightsquigarrow} \Phi_6^{16}, & \Phi_{80} \overset{t^8}{\rightsquigarrow} \Phi_{10}^8 \\
\Phi_{68} \overset{t^2}{\rightsquigarrow} \Phi_{34}^2, & \Phi_{48}^2 \overset{t^8}{\rightsquigarrow} \Phi_6^{16} \\
\Phi_{40}^2 \overset{t^4}{\rightsquigarrow} \Phi_{10}^8, & \Phi_{24}^4 \overset{t^4}{\rightsquigarrow} \Phi_6^{16} \\
\Phi_{20}^4 \overset{t^2}{\rightsquigarrow} \Phi_{10}^8, & \Phi_{12}^8 \overset{t^2}{\rightsquigarrow} \Phi_6^{16}.
\end{array}$$

Il reste

$$\Phi_6^{16} \quad \Phi_{10}^8 \quad \Phi_{15}^4 \quad \Phi_{34}^2 \quad \Phi_{51}.$$

Si t possède Φ_{51} comme polynôme minimal, celui de $-t$ est Φ_{102}. La relation $\Phi_{34}(X)\Phi_{102}(X) = \Phi_{34}(X^3)$ nous donne que $-t^3$ a pour polynôme minimal Φ_{34} et donc Φ_{34}^2 comme polynôme caractéristique. Le polynôme Φ_{51} est donc éliminé. On supprime encore Φ_{15}^4 par le même raisonnement.

Les seuls polynômes restants sont donc :

$$\boxed{\Phi_6^{16} \quad \Phi_{10}^8 \quad \Phi_{34}^2.}$$

(ii) Les polynômes de la liste de la proposition 3.2.2 possédant deux facteurs irréductibles :

Soient p un nombre premier différent de 2 et r_1, r_2 des entiers positifs. On a clairement

$$\Phi_{4p}^{r_1}\Phi_{4pm}^{r_2} \overset{t^2}{\rightsquigarrow} \Phi_{2p}^{2r_1}\Phi_{2pm}^{2r_2}.$$

On élimine ainsi :

$$\Phi_{12}^2\Phi_{24}^3 \quad \Phi_{12}^2\Phi_{36}^2 \quad \Phi_{12}^2\Phi_{84} \quad \Phi_{12}^4\Phi_{24}^2 \quad \Phi_{12}^4\Phi_{48} \quad \Phi_{12}^4\Phi_{60} \quad \Phi_{12}^5\Phi_{36} \quad \Phi_{12}^6\Phi_{24} \quad \Phi_{20}^2\Phi_{40} \quad \Phi_{20}^2\Phi_{60}.$$

Pour $\Phi_{8p}^{r_1}\Phi_{8pm}^{r_2}$, grâce au même raisonnement, mais en élevant t à la puissance 4, on élimine

$$\Phi_{24}\Phi_{72} \quad \Phi_{24}^2\Phi_{48}.$$

La relation $\Phi_{15}(X^4) = \Phi_{15}\Phi_{30}\Phi_{60}$ nous permet de dire que $\Phi_{15}\Phi_{30} \overset{t^4}{\rightsquigarrow} \Phi_{15}$, $\Phi_{15}\Phi_{60} \overset{t^4}{\rightsquigarrow} \Phi_{15}$ et $\Phi_{30}\Phi_{60} \overset{t^4}{\rightsquigarrow} \Phi_{15}$. On élimine ainsi

$$\Phi_{15}\Phi_{30}^3 \quad \Phi_{15}^2\Phi_{30}^2 \quad \Phi_{15}^2\Phi_{60} \quad \Phi_{15}^3\Phi_{30} \quad \Phi_{30}^2\Phi_{60}.$$

On a aussi $\Phi_{15}\Phi_{45} \overset{-t}{\rightsquigarrow} \Phi_{30}\Phi_{90} \overset{t^5}{\rightsquigarrow} \Phi_6\Phi_{18}$. On élimine donc

$$\Phi_{15}\Phi_{45} \text{ et } \Phi_{30}\Phi_{90}.$$

Enfin, soit avec p un nombre premier impair et un entier m tel que $(p, m) = 1$. On montre facilement que $\Phi_{2p}\Phi_{2pm}$ divise $\Phi_{2p}(-X^{2m})$. On a donc $\Phi_{2p}\Phi_{2pm} \overset{-t^{2m}}{\rightsquigarrow} \Phi_{2p}$. Nous pouvons alors supprimer les polynômes suivants :

$\Phi_6^2\Phi_{12}^7$ $\Phi_6^4\Phi_{12}^6$ $\Phi_6^4\Phi_{24}^3$ $\Phi_6^4\Phi_{30}^3$ $\Phi_6^4\Phi_{42}^2$ $\Phi_6^4\Phi_{78}$ $\Phi_6^6\Phi_{12}^5$ $\Phi_6^8\Phi_{12}^4$ $\Phi_6^8\Phi_{24}^2$ $\Phi_6^8\Phi_{30}^2$ $\Phi_6^8\Phi_{48}$ $\Phi_6^{10}\Phi_{12}^3$ $\Phi_6^{12}\Phi_{12}^2$ $\Phi_6^{12}\Phi_{24}$ $\Phi_6^{12}\Phi_{30}$ $\Phi_6^{14}\Phi_{12}$ $\Phi_{10}^2\Phi_{20}^3$ $\Phi_{10}^2\Phi_{30}^3$ $\Phi_{10}^2\Phi_{70}$ $\Phi_{10}^2\Phi_{90}$ $\Phi_{10}^4\Phi_{20}^2$ $\Phi_{10}^4\Phi_{30}^2$ $\Phi_{10}^4\Phi_{40}$ $\Phi_{10}^6\Phi_{20}$ $\Phi_{10}^6\Phi_{30}$.

Tout compte fait, il reste

$$\boxed{\Phi_6^{13}\Phi_{18}\quad \Phi_6^{10}\Phi_{18}^2\quad \Phi_6^7\Phi_{18}^3\quad \Phi_6^4\Phi_{18}^4\quad \Phi_6\Phi_{18}^5\quad \Phi_6^7\Phi_{54}\quad \Phi_6^6\Phi_{66}\quad \Phi_{10}^3\Phi_{50}}$$

(iii) Les polynômes de la liste de la proposition 3.2.2 possédant trois facteurs irréductibles :

Soit p nombre premier impair, m et n des entiers positifs tels que $(p,m)=(p,n)=1$. On a

$$\Phi_{2p}\Phi_{2pm}\Phi_{2pn} \overset{-t^{2mn}}{\rightsquigarrow} \Phi_{2p}.$$

De même, $\Phi_{2p}\Phi_{2pm}\Phi_{2p^2n} \overset{-t^{2mn}}{\rightsquigarrow} \Phi_{2p}\Phi_{2p^2}$ et $\Phi_{2p}\Phi_{2p^2m}\Phi_{2p^2n} \overset{-t^{2mn}}{\rightsquigarrow} \Phi_{2p}\Phi_{2p^2}$. Nous pouvons alors supprimer les polynômes suivants :

$\Phi_6\Phi_{12}^6\Phi_{18}$ $\Phi_6\Phi_{18}\Phi_{24}^3$ $\Phi_6\Phi_{18}\Phi_{30}^3$ $\Phi_6\Phi_{18}\Phi_{36}^2$ $\Phi_6\Phi_{18}\Phi_{42}^2$ $\Phi_6\Phi_{18}\Phi_{72}$ $\Phi_6\Phi_{18}\Phi_{78}$
$\Phi_6\Phi_{18}\Phi_{90}$ $\Phi_6\Phi_{18}^3\Phi_{36}$ $\Phi_6^2\Phi_{12}\Phi_{18}^4$ $\Phi_6^2\Phi_{12}\Phi_{24}^3$ $\Phi_6^2\Phi_{12}\Phi_{30}^3$ $\Phi_6^2\Phi_{12}\Phi_{36}^2$
$\Phi_6^2\Phi_{12}\Phi_{42}^2$ $\Phi_6^2\Phi_{12}\Phi_{78}$ $\Phi_6^2\Phi_{12}\Phi_{84}$ $\Phi_6^2\Phi_{12}^3\Phi_{24}^2$ $\Phi_6^2\Phi_{12}^3\Phi_{30}^2$ $\Phi_6^2\Phi_{12}^3\Phi_{48}$ $\Phi_6^2\Phi_{12}^3\Phi_{60}$
$\Phi_6^2\Phi_{12}^4\Phi_{18}^2$ $\Phi_6^2\Phi_{12}^4\Phi_{36}$ $\Phi_6^2\Phi_{12}^5\Phi_{24}$ $\Phi_6^2\Phi_{12}^5\Phi_{30}$ $\Phi_6^2\Phi_{18}^2\Phi_{24}^2$ $\Phi_6^2\Phi_{18}^2\Phi_{30}^2$ $\Phi_6^2\Phi_{18}^2\Phi_{48}$
$\Phi_6^3\Phi_{12}^2\Phi_{18}^3$ $\Phi_6^3\Phi_{12}^5\Phi_{18}$ $\Phi_6^3\Phi_{18}^3\Phi_{24}$ $\Phi_6^3\Phi_{18}^3\Phi_{30}$
$\Phi_6^4\Phi_{12}^2\Phi_{24}^2$ $\Phi_6^4\Phi_{12}^2\Phi_{30}^2$ $\Phi_6^4\Phi_{12}^2\Phi_{48}$ $\Phi_6^4\Phi_{12}^2\Phi_{60}$ $\Phi_6^4\Phi_{12}^3\Phi_{18}^2$
$\Phi_6^4\Phi_{12}^3\Phi_{36}$ $\Phi_6^4\Phi_{12}^4\Phi_{24}$ $\Phi_6^4\Phi_{12}^4\Phi_{30}$ $\Phi_6^4\Phi_{18}^2\Phi_{36}$
$\Phi_6^4\Phi_{24}\Phi_{30}^2$ $\Phi_6^4\Phi_{24}\Phi_{48}$ $\Phi_6^4\Phi_{24}^2\Phi_{30}$ $\Phi_6^4\Phi_{30}\Phi_{48}$ $\Phi_6^4\Phi_{30}\Phi_{60}$ $\Phi_6^5\Phi_{12}\Phi_{18}^3$
$\Phi_6^5\Phi_{12}^4\Phi_{18}$ $\Phi_6^5\Phi_{18}\Phi_{24}^2$ $\Phi_6^5\Phi_{18}\Phi_{30}^2$ $\Phi_6^5\Phi_{18}\Phi_{48}$ $\Phi_6^6\Phi_{12}\Phi_{24}^2$ $\Phi_6^6\Phi_{12}\Phi_{30}^2$ $\Phi_6^6\Phi_{12}\Phi_{48}$
$\Phi_6^6\Phi_{12}\Phi_{60}$ $\Phi_6^6\Phi_{12}^2\Phi_{18}^2$ $\Phi_6^6\Phi_{12}^2\Phi_{36}$ $\Phi_6^6\Phi_{12}^3\Phi_{24}$ $\Phi_6^6\Phi_{12}^3\Phi_{30}$ $\Phi_6^6\Phi_{18}^2\Phi_{24}$ $\Phi_6^6\Phi_{18}^2\Phi_{30}$
$\Phi_6^7\Phi_{12}^3\Phi_{18}$ $\Phi_6^8\Phi_{12}\Phi_{18}^2$ $\Phi_6^8\Phi_{12}\Phi_{36}$ $\Phi_6^8\Phi_{12}^2\Phi_{24}$ $\Phi_6^8\Phi_{12}^2\Phi_{30}$ $\Phi_6^8\Phi_{15}\Phi_{30}$
$\Phi_6^8\Phi_{24}\Phi_{30}$ $\Phi_6^9\Phi_{12}^2\Phi_{18}$ $\Phi_6^9\Phi_{18}\Phi_{24}$ $\Phi_6^9\Phi_{18}\Phi_{30}$ $\Phi_6^{10}\Phi_{12}\Phi_{24}$ $\Phi_6^{10}\Phi_{12}\Phi_{30}$ $\Phi_6^{11}\Phi_{12}\Phi_{18}$
$\Phi_{10}\Phi_{20}\Phi_{50}$ $\Phi_{10}\Phi_{30}\Phi_{50}$ $\Phi_{10}^2\Phi_{20}\Phi_{30}^2$ $\Phi_{10}^2\Phi_{20}\Phi_{40}$
$\Phi_{10}^2\Phi_{20}\Phi_{60}$ $\Phi_{10}^2\Phi_{20}^2\Phi_{30}$ $\Phi_{10}^2\Phi_{30}\Phi_{40}$ $\Phi_{10}^2\Phi_{30}\Phi_{60}$ $\Phi_{10}^4\Phi_{20}\Phi_{30}$.

Si t est de polynôme minimal $\Phi_{4p}\Phi_{4m}\Phi_{4n}$, t^2 est de polynôme minimal $\Phi_{2p}\Phi_{2m}\Phi_{2n}$. On élimine ainsi les polynômes suivants :

$\Phi_{12}\Phi_{24}^2\Phi_{36}$ $\Phi_{12}\Phi_{36}\Phi_{48}$ $\Phi_{12}\Phi_{36}\Phi_{60}$ $\Phi_{12}^2\Phi_{20}\Phi_{60}$ $\Phi_{12}^2\Phi_{24}\Phi_{48}$ $\Phi_{12}^2\Phi_{24}\Phi_{60}$
$\Phi_{12}^2\Phi_{30}\Phi_{60}$ $\Phi_{12}^3\Phi_{20}\Phi_{36}$ $\Phi_{12}^3\Phi_{24}\Phi_{36}$.

Pour la suite, on regarde chaque polynôme individuellement. On a :

$\Phi_6\Phi_{12}\Phi_{54} \overset{-t^4}{\rightsquigarrow} \Phi_6\Phi_{54}$, $\Phi_6\Phi_{24}\Phi_{54} \overset{-t^8}{\rightsquigarrow} \Phi_6\Phi_{54}$,
$\Phi_6\Phi_{30}\Phi_{54} \overset{-t^{10}}{\rightsquigarrow} \Phi_6\Phi_{54}$, $\Phi_6\Phi_{15}\Phi_{30} \overset{-t^{10}}{\rightsquigarrow} \Phi_6$,
$\Phi_{10}\Phi_{15}\Phi_{30} \overset{-t^6}{\rightsquigarrow} \Phi_{10}$, $\Phi_{10}\Phi_{12}\Phi_{36} \overset{-t^4}{\rightsquigarrow} \Phi_6\Phi_{10}\Phi_{18}$,
$\Phi_{12}\Phi_{18}\Phi_{36} \overset{-t^4}{\rightsquigarrow} \Phi_6\Phi_{18}$, $\Phi_{12}\Phi_{30}\Phi_{36} \overset{-t^{20}}{\rightsquigarrow} \Phi_6\Phi_{18}$,
$\Phi_{12}\Phi_{15}\Phi_{60} \overset{-t^{20}}{\rightsquigarrow} \Phi_6$, $\Phi_{12}\Phi_{20}\Phi_{36} \overset{-t^4}{\rightsquigarrow} \Phi_6\Phi_{10}\Phi_{18}$,
$\Phi_{15}\Phi_{20}\Phi_{60} \overset{-t^{12}}{\rightsquigarrow} \Phi_{10}$, $\Phi_{15}\Phi_{30}\Phi_{60} \overset{-t^{20}}{\rightsquigarrow} \Phi_6$,
$\Phi_{20}\Phi_{30}\Phi_{60} \overset{-t^{12}}{\rightsquigarrow} \Phi_{10}$, $\Phi_6\Phi_{12}\Phi_{66} \overset{-t^4}{\rightsquigarrow} \Phi_6\Phi_{66}$
$\Phi_6\Phi_{24}\Phi_{66} \overset{-t^8}{\rightsquigarrow} \Phi_6\Phi_{66}$, $\Phi_6\Phi_{30}\Phi_{66} \overset{-t^{10}}{\rightsquigarrow} \Phi_6\Phi_{66}$.

Finalement, il ne reste que

$$\boxed{\Phi_6\Phi_{18}^2\Phi_{54}\quad \Phi_6^3\Phi_{18}\Phi_{66}\quad \Phi_6^4\Phi_{10}^2\Phi_{30}^2\quad \Phi_6^4\Phi_{10}^4\Phi_{30}\quad \Phi_6^4\Phi_{14}^2\Phi_{42}\quad \Phi_6^4\Phi_{18}\Phi_{54}\quad \Phi_6^8\Phi_{10}^2\Phi_{30}.}$$

(iv) Les polynômes de la liste de la proposition 3.2.2 possédant quatre facteurs irréductibles :

Notations :

Soient $n_1, \ldots, n_r$ des entiers positifs. On écrit $F_{n_1,\ldots,n_r}$ pour $\Phi_{n_1} \cdots \Phi_{n_r}$.

Voici quelques relations qui vont nous être utiles :

$$F_{6,18}(-X^4) = \Phi_3\Phi_6\Phi_9\Phi_{12}\Phi_{18}\Phi_{36} \quad \text{(a)}$$
$$F_{6,18}(-X^8) = F_{6,18}(-X^4)\Phi_{24}\Phi_{72} \quad \text{(b)}$$
$$F_{6,18}(-X^{16}) = F_{6,18}(-X^8)\Phi_{48}\Phi_{144} \quad \text{(c)}$$
$$F_{6,18}(-X^{10}) = \Phi_3\Phi_6\Phi_9\Phi_{15}\Phi_{18}\Phi_{30}\Phi_{45}\Phi_{90} \quad \text{(d)}$$
$$F_{6,18}(-X^{20}) = F_{6,18}(-X^{10})\Phi_{12}\Phi_{36}\Phi_{60}\Phi_{180} \quad \text{(e)}$$
$$F_{6,18}(-X^{40}) = F_{6,18}(-X^{20})\Phi_{24}\Phi_{72}\Phi_{120}\Phi_{360} \quad \text{(f)}$$
$$F_{6,18}(-X^{80}) = F_{6,18}(-X^{40})\Phi_{48}\Phi_{144}\Phi_{240}\Phi_{720} \quad \text{(g)}$$
$$F_{6,10,30}(-X^4) = \Phi_3\Phi_5\Phi_6\Phi_{10}\Phi_{12}\Phi_{15}\Phi_{20}\Phi_{30}\Phi_{60} \quad \text{(h)}$$
$$F_{6,10,30}(-X^8) = F_{6,10,30}(-X^4)\Phi_{24}\Phi_{40}\Phi_{120} \quad \text{(i)}$$
$$F_{6,18,54}(-X^4) = \Phi_3\Phi_6\Phi_9\Phi_{12}\Phi_{18}\Phi_{27}\Phi_{36}\Phi_{54}\Phi_{108} \quad \text{(j)}$$
$$F_{6,18,54}(-X^8) = F_{6,18,54}(-X^4)\Phi_{24}\Phi_{72}\Phi_{108} \quad \text{(k)}$$
$$F_{6,10,18}(-X^4) = \Phi_3\Phi_5\Phi_6\Phi_9\Phi_{10}\Phi_{12}\Phi_{18}\Phi_{20}\Phi_{36} \quad \text{(l)}$$
$$F_{6,10,18}(-X^8) = F_{6,10,18}(-X^4)\Phi_{24}\Phi_{40} \quad \text{(m)}$$
$$F_{6,10,18,30}(-X^4) = \Phi_3\Phi_5\Phi_6\Phi_9\Phi_{10}\Phi_{12}\Phi_{15}\Phi_{18}\Phi_{20}\Phi_{30}\Phi_{36}\Phi_{60} \quad \text{(n)}$$
$$F_{6,10,18,30}(-X^8) = F_{6,10,18,30}(-X^4)\Phi_{24}\Phi_{40}\Phi_{72}\Phi_{120} \quad \text{(o)}$$
$$F_{6,14,42}(-X^4) = \Phi_3\Phi_6\Phi_7\Phi_{12}\Phi_{14}\Phi_{21}\Phi_{28}\Phi_{42}\Phi_{84} \quad \text{(p)}$$

Les polynômes suivants sont associés à un polynôme P tel que $P \overset{-t^4}{\rightsquigarrow} \Phi_6\Phi_{18}$, grâce à la relation (a) :

$\Phi_6^5\Phi_{12}\Phi_{18}\Phi_{36}$ $\Phi_6^3\Phi_{12}^2\Phi_{18}\Phi_{36}$ $\Phi_6^2\Phi_{12}\Phi_{18}^2\Phi_{36}$ $\Phi_6\Phi_{12}^3\Phi_{18}\Phi_{36}$.

Les polynômes suivants sont associés à un polynôme P, tel que $P \overset{-t^8}{\rightsquigarrow} \Phi_6\Phi_{18}$ grâce à la relation (b) :

$\Phi_6^3\Phi_{12}\Phi_{18}\Phi_{24}^2$ $\Phi_6^7\Phi_{12}\Phi_{18}\Phi_{24}$ $\Phi_6^5\Phi_{12}^2\Phi_{18}\Phi_{24}$ $\Phi_6^4\Phi_{12}\Phi_{24}\Phi_{36}$ $\Phi_6^4\Phi_{12}\Phi_{18}^2\Phi_{24}$
$\Phi_6^3\Phi_{12}^3\Phi_{18}\Phi_{24}$ $\Phi_6^2\Phi_{12}^2\Phi_{24}\Phi_{36}$ $\Phi_6^2\Phi_{12}^2\Phi_{18}^2\Phi_{24}$ $\Phi_6\Phi_{12}^4\Phi_{18}\Phi_{24}$ $\Phi_6\Phi_{12}^2\Phi_{18}\Phi_{24}^2$.

Les polynômes suivants sont associés à un polynôme P, tel que $P \overset{-t^{16}}{\rightsquigarrow} \Phi_6\Phi_{18}$, grâce à la relation (c) :

$\Phi_6^3\Phi_{12}\Phi_{18}\Phi_{48}$ $\Phi_6^2\Phi_{12}\Phi_{24}\Phi_{48}$ $\Phi_6\Phi_{18}\Phi_{24}\Phi_{48}$ $\Phi_6\Phi_{12}^2\Phi_{18}\Phi_{48}$.

Les polynômes suivants sont associés à un polynôme P, tel que $P \overset{-t^{10}}{\rightsquigarrow} \Phi_6\Phi_{18}$, grâce à la relation (d) :

$\Phi_6^5\Phi_{15}\Phi_{18}\Phi_{30}$ $\Phi_6^2\Phi_{15}\Phi_{18}^2\Phi_{30}$ $\Phi_6\Phi_{15}^2\Phi_{18}\Phi_{30}$ $\Phi_6\Phi_{15}\Phi_{18}\Phi_{30}^2$.

Les polynômes suivants sont associés à un polynôme P, tel que $P \overset{-t^{20}}{\rightsquigarrow} \Phi_6\Phi_{18}$, grâce à la relation (e) :

$\Phi_6^7\Phi_{12}\Phi_{18}\Phi_{30}$ $\Phi_6^6\Phi_{12}\Phi_{15}\Phi_{30}$ $\Phi_6^5\Phi_{12}^2\Phi_{18}\Phi_{30}$ $\Phi_6^4\Phi_{12}^2\Phi_{15}\Phi_{30}$ $\Phi_6^2\Phi_{12}^3\Phi_{15}\Phi_{30}$
$\Phi_6^4\Phi_{12}\Phi_{30}\Phi_{36}$ $\Phi_6^4\Phi_{12}\Phi_{18}^2\Phi_{30}$ $\Phi_6^4\Phi_{12}\Phi_{15}\Phi_{36}$ $\Phi_6^3\Phi_{12}^3\Phi_{18}\Phi_{30}$ $\Phi_6^2\Phi_{12}^2\Phi_{30}\Phi_{36}$
$\Phi_6^3\Phi_{12}\Phi_{18}\Phi_{60}$ $\Phi_6^3\Phi_{12}\Phi_{18}\Phi_{30}^2$ $\Phi_6^2\Phi_{12}^2\Phi_{18}^2\Phi_{30}$ $\Phi_6^2\Phi_{12}\Phi_{30}\Phi_{60}$ $\Phi_6^2\Phi_{12}\Phi_{15}\Phi_{60}$
$\Phi_6^2\Phi_{12}\Phi_{15}\Phi_{30}^2$ $\Phi_6\Phi_{18}\Phi_{30}\Phi_{60}$ $\Phi_6\Phi_{12}^4\Phi_{18}\Phi_{30}$ $\Phi_6\Phi_{12}^2\Phi_{18}\Phi_{60}$ $\Phi_6\Phi_{12}^2\Phi_{18}\Phi_{30}^2$.

Les polynômes suivants sont associés à un polynôme P, tel que $P \overset{-t^{40}}{\rightsquigarrow} \Phi_6\Phi_{18}$, grâce à la relation (f) :

$\Phi_{12}\Phi_{24}\Phi_{30}\Phi_{36}$ $\Phi_{12}\Phi_{15}\Phi_{24}\Phi_{36}$ $\Phi_6^6\Phi_{12}\Phi_{24}\Phi_{30}$ $\Phi_6^5\Phi_{18}\Phi_{24}\Phi_{30}$
$\Phi_6^4\Phi_{15}\Phi_{24}\Phi_{30}$ $\Phi_6^4\Phi_{12}^2\Phi_{24}\Phi_{30}$ $\Phi_6^2\Phi_{18}^2\Phi_{24}\Phi_{30}$ $\Phi_6^2\Phi_{12}^3\Phi_{24}\Phi_{30}$ $\Phi_6^2\Phi_{12}\Phi_{24}^2\Phi_{30}$
$\Phi_6^2\Phi_{12}\Phi_{24}\Phi_{60}$ $\Phi_6^2\Phi_{12}\Phi_{24}\Phi_{30}^2$ $\Phi_6\Phi_{18}\Phi_{24}^2\Phi_{30}$ $\Phi_6\Phi_{18}\Phi_{24}\Phi_{30}^2$.

Les polynômes suivants sont associés à un polynôme P, tel que $P \overset{-t^{80}}{\rightsquigarrow} \Phi_6\Phi_{18}$, grâce à la relation (g) :

$$\Phi_6^2\Phi_{12}\Phi_{30}\Phi_{48} \quad \Phi_6\Phi_{18}\Phi_{30}\Phi_{48}.$$

Les polynômes suivants sont associés à un polynôme P, tel que $P \overset{-t^{4}}{\rightsquigarrow} \Phi_6\Phi_{10}\Phi_{30}$, grâce à la relation (h) :

$\Phi_{10}^2\Phi_{15}\Phi_{20}\Phi_{30}$ $\Phi_6^4\Phi_{10}^2\Phi_{20}\Phi_{30}$ $\Phi_6^4\Phi_{10}^2\Phi_{15}\Phi_{30}$ $\Phi_6^4\Phi_{10}^2\Phi_{12}^2\Phi_{30}$ $\Phi_6^2\Phi_{12}\Phi_{20}\Phi_{60}$
$\Phi_6^2\Phi_{12}\Phi_{15}^2\Phi_{30}$ $\Phi_6^2\Phi_{10}^4\Phi_{12}\Phi_{30}$ $\Phi_6^2\Phi_{10}^2\Phi_{12}^3\Phi_{30}$ $\Phi_6^2\Phi_{10}^2\Phi_{12}\Phi_{30}^2$.

Remarquons que les polynômes associés à $F_{6,10,30}$ correspondent à des réseaux scindés. Il en est de même pour ceux associés à $F_{6,10,18}$.

Les polynômes suivants sont associés à un polynôme P, tel que $P \overset{-t^{8}}{\rightsquigarrow} \Phi_6\Phi_{10}\Phi_{30}$, grâce à la relation (i) :

$$\Phi_6^6\Phi_{10}^2\Phi_{12}\Phi_{30} \quad \Phi_6^4\Phi_{10}^2\Phi_{24}\Phi_{30}.$$

Le polynôme suivant est associé à $\Phi_6\Phi_{12}\Phi_{18}\Phi_{54}$, et $\Phi_6\Phi_{12}\Phi_{18}\Phi_{54} \overset{-t^{4}}{\rightsquigarrow} \Phi_6\Phi_{18}\Phi_{54}$, grâce à la relation (j) :

$$\Phi_6^2\Phi_{12}\Phi_{18}\Phi_{54}.$$

Les polynômes suivants sont associés à un polynôme P, tel que $P \overset{-t^{4}}{\rightsquigarrow} \Phi_6\Phi_{10}\Phi_{18}$, grâce à la relation (l) :

$$\Phi_6^4\Phi_{10}^2\Phi_{12}\Phi_{36} \quad \Phi_6^2\Phi_{12}^2\Phi_{20}\Phi_{36} \quad \Phi_6^2\Phi_{10}^2\Phi_{12}^2\Phi_{36}.$$

Les polynômes suivants sont associés à un polynôme P, tel que $P \overset{-t^{8}}{\rightsquigarrow} \Phi_6\Phi_{10}\Phi_{18}$, grâce à la relation (m) :

$$\Phi_{10}^2\Phi_{12}\Phi_{24}\Phi_{36} \quad \Phi_{12}\Phi_{20}\Phi_{24}\Phi_{36} \quad \Phi_6^4\Phi_{12}\Phi_{20}\Phi_{36}.$$

Le polynôme suivant est associé à un polynôme P, tel que $P \overset{-t^{8}}{\rightsquigarrow} \Phi_6\Phi_{10}\Phi_{18}\Phi_{30}$, grâce à la relation (n) :

$$\Phi_6^2\Phi_{12}^2\Phi_{15}\Phi_{36}.$$

Enfin, le polynôme suivant est associé à un polynôme P, tel que $P \overset{-t^{4}}{\rightsquigarrow} \Phi_6\Phi_{14}\Phi_{42}$ grâce à la relation (p) :

$$\Phi_6^2\Phi_{12}\Phi_{14}^2\Phi_{42}.$$

Il ne reste donc que les polynômes suivants

$$\boxed{\Phi_6\Phi_{14}^2\Phi_{18}\Phi_{42} \quad \Phi_6^5\Phi_{10}^2\Phi_{18}\Phi_{30} \quad \Phi_6^2\Phi_{10}^2\Phi_{18}^2\Phi_{30} \quad \Phi_6\Phi_{10}^2\Phi_{18}\Phi_{30}^2 \quad \Phi_6\Phi_{10}^4\Phi_{18}\Phi_{30}.}$$

(v) Les polynômes de la liste de la proposition 3.2.2 possédant cinq facteurs irréductibles :

Dans cette section, nous allons réutiliser les équations introduites précédemment.

Le polynôme suivant est associé à un polynôme P, tel que $P \overset{-t^8}{\rightsquigarrow} \Phi_6\Phi_{18}$, grâce à la relation (b) :

$$\Phi_6\Phi_{12}\Phi_{18}\Phi_{24}\Phi_{36}.$$

Les polynômes suivants sont associés à un polynôme P, tel que $P \overset{-t^{20}}{\rightsquigarrow} \Phi_6\Phi_{18}$, grâce à la relation (e) :

$$\Phi_6\Phi_{12}\Phi_{15}\Phi_{18}\Phi_{36} \quad \Phi_6\Phi_{12}\Phi_{18}\Phi_{30}\Phi_{36} \quad \Phi_6\Phi_{12}^2\Phi_{15}\Phi_{18}\Phi_{30} \quad \Phi_6^3\Phi_{12}\Phi_{15}\Phi_{18}\Phi_{30}.$$

Les polynômes suivants sont associés à un polynôme P, tel que $P \overset{-t^{40}}{\rightsquigarrow} \Phi_6\Phi_{18}$, grâce à la relation (f) :

$$\Phi_6^3\Phi_{12}\Phi_{18}\Phi_{24}\Phi_{30} \quad \Phi_6\Phi_{12}^2\Phi_{15}\Phi_{18}\Phi_{24} \quad \Phi_6\Phi_{12}^2\Phi_{18}\Phi_{24}\Phi_{30} \quad \Phi_6\Phi_{15}\Phi_{18}\Phi_{24}\Phi_{30} \quad \Phi_6^2\Phi_{12}\Phi_{15}\Phi_{24}\Phi_{30}.$$

$$\Phi_6^3\Phi_{12}\Phi_{15}\Phi_{18}\Phi_{24}.$$

Les polynômes suivants sont associés à un polynôme P, tel que $P \overset{-t^4}{\rightsquigarrow} \Phi_6\Phi_{10}\Phi_{30}$, grâce à la relation (h) :

$$\Phi_6^2\Phi_{10}^2\Phi_{12}\Phi_{15}\Phi_{30} \quad \Phi_6^2\Phi_{10}^2\Phi_{12}\Phi_{20}\Phi_{30} \quad \Phi_6^2\Phi_{12}\Phi_{15}\Phi_{20}\Phi_{30}.$$

Les polynômes suivants sont associés à un polynôme P, tel que $P \overset{-t^8}{\rightsquigarrow} \Phi_6\Phi_{10}\Phi_{30}$, grâce à la relation (i) :

$$\Phi_6^2\Phi_{10}^2\Phi_{12}\Phi_{24}\Phi_{30} \quad \Phi_6^2\Phi_{12}\Phi_{20}\Phi_{24}\Phi_{30}.$$

Les polynômes suivants sont associés à un polynôme P, tel que $P \overset{-t^4}{\rightsquigarrow} \Phi_6\Phi_{10}\Phi_{18}$ grâce, à la relation (l) :

$$\Phi_6\Phi_{10}^2\Phi_{12}\Phi_{18}\Phi_{36}.$$

Les polynômes suivants sont associés à un polynôme P, tel que $P \overset{-t^8}{\rightsquigarrow} \Phi_6\Phi_{10}\Phi_{18}$, grâce à la relation (l) :

$$\Phi_6\Phi_{10}^2\Phi_{12}^2\Phi_{18}\Phi_{24} \quad \Phi_6^3\Phi_{10}^2\Phi_{12}\Phi_{18}\Phi_{24} \quad \Phi_6^3\Phi_{12}\Phi_{18}\Phi_{20}\Phi_{24}.$$

Les polynômes suivants sont associés à un polynôme P, tel que $P \overset{-t^4}{\rightsquigarrow} \Phi_6\Phi_{10}\Phi_{18}\Phi_{30}$, grâce à la relation (n) :

$$\Phi_6\Phi_{10}^2\Phi_{12}^2\Phi_{18}\Phi_{30} \quad \Phi_6\Phi_{10}^2\Phi_{15}\Phi_{18}\Phi_{30} \quad \Phi_6\Phi_{10}^2\Phi_{18}\Phi_{20}\Phi_{30} \quad \Phi_6\Phi_{12}\Phi_{18}\Phi_{20}\Phi_{36} \quad \Phi_6\Phi_{12}^2\Phi_{18}\Phi_{20}\Phi_{30}$$

$$\Phi_6\Phi_{15}\Phi_{18}\Phi_{20}\Phi_{30} \quad \Phi_6^3\Phi_{10}^2\Phi_{12}\Phi_{18}\Phi_{30} \quad \Phi_6^3\Phi_{12}\Phi_{18}\Phi_{20}\Phi_{30}.$$

Les polynômes suivants sont associés à un polynôme P, tel que $P \overset{-t^8}{\rightsquigarrow} \Phi_6\Phi_{10}\Phi_{18}\Phi_{30}$, grâce à la relation (o) :

$$\Phi_6\Phi_{10}^2\Phi_{18}\Phi_{24}\Phi_{30} \quad \Phi_6\Phi_{12}^2\Phi_{18}\Phi_{20}\Phi_{24} \quad \Phi_6\Phi_{18}\Phi_{20}\Phi_{24}\Phi_{30}.$$

Tous les polynômes à 5 facteurs irréductibles ont donc été éliminés. Nous sommes alors en mesure d'énoncer le

Théorème 3.2.3

Soit (M,β) un $\mathbb{Z}$-réseau unimodulaire indécomposable, pair et de dimension 32. Alors, (M,β) possède une isométrie parfaite, si et seulement si (M,β) est un F-réseau, où F est un des polynômes suivants :

Φ_6^{16}	Φ_{10}^8	Φ_{34}^2						
$\Phi_6\Phi_{18}^5$	$\Phi_6^4\Phi_{18}^4$	$\Phi_6^6\Phi_{66}$	$\Phi_6^7\Phi_{18}^3$	$\Phi_6^7\Phi_{54}$	$\Phi_6^{10}\Phi_{18}^2$	$\Phi_6^{13}\Phi_{18}$	$\Phi_{10}^3\Phi_{50}$	
$\Phi_6\Phi_{18}^2\Phi_{54}$	$\Phi_6^3\Phi_{18}^2\Phi_{66}$	$\Phi_6^4\Phi_{10}^2\Phi_{30}^2$	$\Phi_6^4\Phi_{10}^4\Phi_{30}$	$\Phi_6^4\Phi_{14}^2\Phi_{42}$	$\Phi_6^4\Phi_{18}\Phi_{54}$	$\Phi_6^8\Phi_{10}^2\Phi_{30}$		
$\Phi_6\Phi_{10}^2\Phi_{18}\Phi_{30}^2$	$\Phi_6\Phi_{10}^4\Phi_{18}\Phi_{30}$	$\Phi_6\Phi_{14}^2\Phi_{18}\Phi_{42}$	$\Phi_6^2\Phi_{10}^2\Phi_{18}^2\Phi_{30}$	$\Phi_6^5\Phi_{10}^2\Phi_{18}\Phi_{30}$.				

Corollaire 3.2.4

Soit (M,β) un $\mathbb{Z}$-réseau unimodulaire indécomposable, pair et de dimension 32. Alors (M,β) possède une isométrie parfaite, si et seulement si (M,β) possède une isométrie de polynôme minimal appartenant à la liste suivante :

Φ_6	Φ_{10}	Φ_{34}						
$\Phi_6\Phi_{18}$	$\Phi_6\Phi_{54}$	$\Phi_6\Phi_{66}$	$\Phi_{10}\Phi_{50}$					
$\Phi_6\Phi_{10}\Phi_{30}$	$\Phi_6\Phi_{14}\Phi_{42}$	$\Phi_6\Phi_{18}\Phi_{54}$	$\Phi_6\Phi_{18}\Phi_{66}$					
$\Phi_6\Phi_{10}\Phi_{18}\Phi_{30}$	$\Phi_6\Phi_{14}\Phi_{18}\Phi_{42}$.							

CHAPITRE 4

Estimations numériques pour certains exemples

Résumons brièvement la situation. Au premier chapitre, nous avons obtenu des formules pour l'estimation de la masse de $\overline{\mathscr{E}}(F)$. C'étaient les théorèmes 1.6.6, 1.6.8 et 1.6.9. Le chapitre 2 nous permet de calculer explicitement la formule de masse pour certaines formes hermitiennes. Enfin, le troisième chapitre nous a fourni certains polynômes intéressants. Il paraît naturel d'estimer la masse de $\overline{\mathscr{E}}(F)$ pour ces polynômes. Nous ne pourrons hélas pas faire les calculs pour tous les polynômes du théorème 3.2.3. Il faudra se restreindre à ceux qui possèdent un ou deux facteurs irréductibles distincts. En effet, il y a un terme qui intervient lors des théorèmes 1.6.6 et 1.6.8 dont nous n'avons pas encore parlé : c'est le cardinal de l'ensemble $\mathscr{L}_{(N_1,\dots,N_s)}$ (voir la définition 1.6.1). Le calcul de ce cardinal est facilité, comme nous le verrons au théorème 4.2.3, lorsque $s = 2$, grâce aux théorèmes 1.3.5 et 1.4.1. Ces théorèmes ne se généralisent pas, ou mal, lorsque $s \geq 3$.

§ 1. Estimation de la masse de $\overline{\mathscr{E}}(\Phi_4^{16})$, $\overline{\mathscr{E}}(\Phi_6^{16})$, $\overline{\mathscr{E}}(\Phi_{10}^{8})$ et $\overline{\mathscr{E}}(\Phi_{34}^{2})$

Avant de faire ces estimations, nous avons besoin de quelques résultats calculatoires :

Définition 4.1.1

Supposons que $n = 4, 6, 10, 18, 34, 50$ ou 54. Posons $\mathfrak{p}_n$, l'unique idéal premier de $\mathbb{Q}(\zeta_n + \overline{\zeta_n})$ se ramifiant dans $\mathbb{Q}(\zeta_n)$. L'idéal premier de $\mathbb{Q}(\zeta_n)$ au-dessus de $\mathfrak{p}_n$ se note $\mathfrak{P}_n$. Nous savons que $\mathfrak{P}_n$ est l'idéal engendré par $1 + \zeta_n$.

Soit n un entier positif. La différente $\mathscr{D}_n$ est l'idéal engendré par $\Phi_n'(\zeta_n)$. Nous aurons fréquemment besoin de connaître l'idéal $n \cdot \mathscr{D}_n^{-1}$. Voici quelques valeurs :

Lemme 4.1.2

On a :

$$\begin{aligned}
&4 \cdot \mathscr{D}_4^{-1} = \mathfrak{P}_4^2 = 2 \cdot \mathbb{Z}[\zeta_4] && 6 \cdot \mathscr{D}_6^{-1} = 2 \cdot \mathfrak{P}_6 \\
&10 \cdot \mathscr{D}_{10}^{-1} = 2 \cdot \mathfrak{P}_{10} && 18 \cdot \mathscr{D}_{18}^{-1} = 2 \cdot \mathfrak{P}_{18}^3 \\
&34 \cdot \mathscr{D}_{34}^{-1} = 2 \cdot \mathfrak{P}_{34} && 50 \cdot \mathscr{D}_{50}^{-1} = 2 \cdot \mathfrak{P}_{50}^5 \\
&54 \cdot \mathscr{D}_{54}^{-1} = 2 \cdot \mathfrak{P}_{54}^9 && 66 \cdot \mathscr{D}_{66}^{-1} = 2 \cdot \mathfrak{P}_{(1,3),66}\mathfrak{P}_{(2,3),66}\mathfrak{P}_{11,66},
\end{aligned}$$

$$\begin{aligned}
\text{avec} \quad \mathfrak{P}_{(1,3),66} &= (1 - \zeta_{66}^2 - \zeta_{66}^3 - \zeta_{66}^4 + \zeta_{66}^5) \cdot \mathbb{Z}[\zeta_{66}] \\
\mathfrak{P}_{(2,3),66} &= (1 - \zeta_{66} - \zeta_{66}^2 - \zeta_{66}^3 + \zeta_{66}^5) \cdot \mathbb{Z}[\zeta_{66}] \\
\text{et} \quad \mathfrak{P}_{11,66} &= (\zeta_{66} + \overline{\zeta_{66}} - 1)\mathbb{Z}[\zeta_{66}].
\end{aligned}$$

En outre,

$$\begin{aligned}
11 \cdot \mathbb{Z}[\zeta_{66}] &= \mathfrak{P}_{11,66}^{10}, \\
3 \cdot \mathbb{Z}[\zeta_{66}] &= (\mathfrak{P}_{(1,3),66}\mathfrak{P}_{(2,3),66})^2.
\end{aligned}$$

De plus, $\mathfrak{P}_{(1,3),66}\mathfrak{P}_{(2,3),66} = (-1 - (\zeta_{66} + \overline{\zeta_{66}})^3 - (\zeta_{66} + \overline{\zeta_{66}})^4 + (\zeta_{66} + \overline{\zeta_{66}})^5) \cdot \mathbb{Z}[\zeta_{66}]$

est engendré par un élément de $\mathbb{Z}[\zeta_{66} + \overline{\zeta_{66}}]$.

Démonstration :

Le fait que $\mathscr{D}_n$ soit l'idéal engendré par $\Phi'_n(\zeta_n)$ est bien connu (cf. [Fr-Ta], Result 2.20). Les autres résultats sont des calculs facilement vérifiables grâce au programme PARI, au moyen de la fonction "`idealfactor`". ❄

Remarquons que le polynôme Φ_4^{16} ne fait pas partie de la liste du théorème 3.2.3, car $\Phi_4^{16}(1) = 2^{16} \neq 1$. Ainsi, un Φ_4^{16}-réseau ne possède pas forcément une isométrie parfaite. L'introduction de ce polynôme dans le titre de ce paragraphe est motivée par le résultat suivants :

Proposition 4.1.3

Soit (M, β) un $\mathbb{Z}$-réseau unimodulaire de dimension 32. Alors (M, β) possède une isométrie, différente de $\pm I_{32}$, de polynôme minimal irréductible si et seulement si (M, β) est un F-réseau, où F est l'un des polynômes suivants :

$$\Phi_4^{16} \quad \Phi_6^{16} \quad \Phi_{10}^{8} \quad \Phi_{34}^{2}.$$

Démonstration :

Les polynômes Φ_n^m de degré 32, avec $n \neq 1, 2$ sont les suivants :

$$\Phi_3^{16} \quad \Phi_4^{16} \quad \Phi_5^{8} \quad \Phi_6^{16} \quad \Phi_8^{8} \quad \Phi_{10}^{8} \quad \Phi_{12}^{8} \quad \Phi_{15}^{4} \quad \Phi_{16}^{4} \quad \Phi_{17}^{2} \quad \Phi_{20}^{4}$$
$$\Phi_{24}^{4} \quad \Phi_{30}^{4} \quad \Phi_{32}^{2} \quad \Phi_{34}^{2} \quad \Phi_{40}^{2} \quad \Phi_{48}^{2} \quad \Phi_{51} \quad \Phi_{60}^{2} \quad \Phi_{64} \quad \Phi_{68} \quad \Phi_{80} \quad \Phi_{96} \quad \Phi_{102} \quad \Phi_{120}.$$

Les méthodes du chapitre 3 nous permettent d'affirmer le résultat suivant : si (M, β) est un $\mathbb{Z}$-réseau unimodulaire de dimension 32 possédant une isométrie de polynôme minimal irréductible, différent de $X - 1$ ou $X + 1$, alors (M, β) est un F-réseau, où F est l'un des polynômes suivants :

$$\Phi_4^{16} \quad \Phi_6^{16} \quad \Phi_{10}^{8} \quad \Phi_{34}^{2}.$$

La réciproque suit du théorème 2.1 de [Bay], dont nous avons donné une version atténuée au théorème 3.1.4. ❄

Remarque :

Suite à la proposition précédente, on peut remarquer qu'un réseau unimodulaire, impair, de dimension 32, et possédant une isométrie de polynôme minimal irréductible différent de $X - 1$ ou $X + 1$ est obligatoirement un Φ_4^{16}-réseau. En effet, nous savons que les Φ_6^{16}-réseaux, les Φ_{10}^{8}-réseaux, et les Φ_{34}^{2}-réseaux sont forcément pairs (cf. théorème 3.1.1); nous allons voir au théorème suivant que ces réseaux sont probablement peu abondants. En revanche, les Φ_4^{16}-réseaux semblent plus courants.

Théorème 4.1.4

On a les résultats suivants :

$$\sum_{\overline{M}\in\overline{\mathscr{E}}(\Phi_4^{16})} \frac{1}{|O(M)|} \leq 3,27\cdot 10^9$$

$$\sum_{\overline{M}\in\overline{\mathscr{E}}(\Phi_6^{16})} \frac{1}{|O(M)|} \leq 0,0029$$

$$\sum_{\overline{M}\in\overline{\mathscr{E}}(\Phi_{10}^{8})} \frac{1}{|O(M)|} \leq 0,006$$

$$\sum_{\overline{M}\in\overline{\mathscr{E}}(\Phi_{34}^{2})} \frac{1}{|O(M)|} \leq 4,3355$$

où $\overline{\mathscr{E}}(F)$ est, rappelons-le, l'ensemble à $\mathbb{Z}$-isométries près des F-réseaux.

Démonstration :

Nous allons appliquer le théorème 1.6.9 pour chacun des cas. Il affirme que $\sum_{\overline{M}\in\overline{\mathscr{E}}(\Phi_n^r)} \frac{1}{|O(M)|} \leq \omega(N)$, où (N,h) est un $\mathbb{Z}[\zeta_n]$-module hermitien, totalement défini positif, projectif de rang r, et dont les facteurs invariants de N dans $N_h^\#$ sont $\underbrace{n\cdot\mathscr{D}_n^{-1},\ldots,n\cdot\mathscr{D}_n^{-1}}_{r \text{ fois}}$.

Démontrons le théorème pour le cas Φ_4^{16}. Nous savons (cf. lemme 4.1.2) que $4\cdot\mathscr{D}_4^{-1} = 2\cdot\mathbb{Z}[\zeta_4]$. Ainsi, les facteurs de N dans $N_h^\#$ sont $(2\cdot\mathbb{Z}[\zeta_4],\ldots,2\cdot\mathbb{Z}[\zeta_4])$. Il faut donc calculer $\omega(N)$, où (N,h) est de rang 16, totalement défini positif, et tel que $h = 2h'$, avec (N,h') unimodulaire (cf. théorème 1.3.12). Le lemme 2.1.5 nous apprend que $\omega(N) = \omega(N')$, où N' symbolise (N,h'). Or, la thèse de E. Bannaï nous permet de calculer directement la masse des $\mathbb{Z}[\zeta_4]$-modules hermitiens, unimodulaires et totalement définis positifs. On a :

$$\prod_{p\neq 2}\mathfrak{B}_p(N')^{-1} \leq \frac{1}{32}\pi^3 e^{\frac{1}{2}}\prod_{i=3}^{16}(1-2^{-i}) \quad \text{(cf. [Ban], proposition 9.2).}$$

D'autre part, $\mathfrak{B}_2(N')^{-1} \leq 0,8$, (cf. [Ban], propositions 5.12 et 5.14). Or, il y a deux genres de modules hermitiens, unimodulaires et totalement définis positifs (cf. [Ha], proposition 3.8). Donc

$$\begin{aligned}\sum_{\overline{M}\in\overline{\mathscr{E}}(\Phi_4^{16})} \frac{1}{|O(M)|} &\leq 2\cdot 2\cdot d(\mathbb{Q}(\zeta_4))^{68}\prod_{j=1}^{16}\frac{(j-1)!}{(2\pi)^j}\cdot\prod_{p\in\mathbb{P}(\mathbb{Z})}\mathfrak{B}_p(N')^{-1}\\ &\leq 4^{69}\cdot 2,54\cdot 10^{-32}\cdot\frac{1}{32}\cdot\pi^3\cdot e^{\frac{1}{2}}\prod_{i=3}^{16}(1-2^{-i})\cdot 0,8\\ &\leq 3,27\cdot 10^9 \qquad \text{(cf. théorème 2.1.4).}\end{aligned}$$

Pour le cas $F = \Phi_6^{16}$, les facteurs invariants de N dans $N_h^\#$ sont $(2\cdot\mathfrak{P}_6,\ldots,2\cdot\mathfrak{P}_6)$ (cf. théorème 1.3.12 et lemme 4.1.2). Le lemme 2.1.5 nous montre qu'on peut supposer, pour calculer la masse de N, que les facteurs invariants de N dans $N_h^\#$ sont $(\mathfrak{P}_6,\ldots,\mathfrak{P}_6)$. Par conséquent, (N_3,h_3) est $\mathfrak{P}_6$-modulaire, et (N_p,h_p) est unimodulaire pour tout premier différent de 3. On en déduit, grâce au théorème 2.3.1, que

$$\prod_{p\in\mathbb{P}(\mathbb{Q})-\{3\}}\mathfrak{B}_p(N)^{-1} \leq 3^{-\frac{3}{2}}\cdot\pi\cdot\prod_{i=2}^{16}\zeta(i)(1-3^{-i}) \leq 1,166$$

$$\text{et que} \qquad \mathfrak{B}_3(N)^{-1} = 3^{-136}\cdot\prod_{i=1}^{8}(1-3^{-2i})^{-1} \leq 1,475\cdot 10^{-65}$$

en vertu du théorème 2.2.6 iii). Le théorème 1.5.5 nous affirme que, dans notre cas, il y a exactement un seul genre de modules hermitiens. On trouve ainsi, par le théorème 2.1.4 :

$$\sum_{M\in\overline{\mathscr{E}}(\Phi_6^{16})}\frac{1}{|O(M)|}\leq\omega(N)\leq 2\cdot|d(\mathbb{Q}(\zeta_6)|^{68}\cdot\prod_{i=1}^{16}\frac{(j-1)!}{(2\pi)^j}\cdot|\mathbb{Z}[\zeta_6]/\mathfrak{P}_6|^{128}\cdot 1,166\cdot 1,475\cdot 10^{-65}\leq 0,0029.$$

Dorénavant, nous ne rédigerons plus tous les calculs, car nous avons créé une fonction informatique du programme PARI, nommé `oomega`, qui est capable de calculer la masse de la plupart des modules hermitiens totalement définis positifs, connaissant les facteurs invariants du module dans son dual. Le *listing* de ce module est donnée en annexe. Un mode d'emploi abrégé se trouve dans la remarque qui suit ce théorème.

Pour le cas $F=\Phi_{10}^8$, on peut considérer (cf. lemmes 2.1.5, 4.1.2 et 1.3.12) que les facteurs invariants de N dans $N_h^\#$ sont $(\mathfrak{P}_{10},\dots,\mathfrak{P}_{10})$. Donc, $(N_{\mathfrak{p}_{10}},h_{\mathfrak{p}_{10}})$ est $\mathfrak{P}_{10}$-modulaire, et $(N_\mathfrak{p},h_\mathfrak{p})$ est unimodulaire pour tout $\mathfrak{p}\neq\mathfrak{p}_{10}$. Ainsi, introduisant ces données dans le programme, on trouve :

$$\sum_{M\in\overline{\mathscr{E}}(\Phi_{10}^8)}\frac{1}{|O(M)|}\leq\omega(N)=\texttt{oomega([1,...,1],5,1)}\leq 0,006.$$

Calculons la masse de $\overline{\mathscr{E}}(\Phi_{34}^2)$. On peut supposer, de manière analogue aux cas précédents, que les facteurs invariants de N dans $N_h^\#$ sont $(\mathfrak{P}_{34},\mathfrak{P}_{34})$. Ainsi, $(N_{\mathfrak{p}_{34}},h_{\mathfrak{p}_{34}})$ est $\mathfrak{P}_{34}$-modulaire, et $(N_\mathfrak{p},h_\mathfrak{p})$ est unimodulaire, pour tout $\mathfrak{p}\neq\mathfrak{p}_{34}$. On trouve alors :

$$\sum_{M\in\overline{\mathscr{E}}(\Phi_{34}^2)}\frac{1}{|O(M)|}\leq\omega(N)=\texttt{oomega([1,1],17,1)}\leq 4,3355.$$

❄

Remarque :

a) Afin de donner un ordre de grandeur, rappelons que la masse des réseaux unimodulaires impairs de dimension 32 est $4,33\cdot 10^{16}$, et que celle des réseaux pairs est $4,031\cdot 10^7$, cf. ([Mis], théorèmes 5.3 et 5.8) ou ([Co-Slo], théorèmes 1 et 2, chapitre 16). Ainsi, on en déduit que l'ensemble des classes d'isométries de réseaux possédant des isométries parfaites de polynôme minimal irréductible a une masse très faible, inférieure à 4,34.

b) Voici une description de l'utilisation de la fonction informatique "`oomega`" : supposons que (M,h) soit un $\mathbb{Z}[\zeta_n]$-module hermitien totalement défini positif, que $\mathbb{Q}(\zeta_n)=\mathbb{Q}(\zeta_{p^k})$, avec $p\in\mathbb{P}-\{2\}$, et que les facteurs invariants de M dans $M_h^\#$ soient $\mathfrak{P}^{m_1}\supset\cdots\supset\mathfrak{P}^{m_r}$, avec $m_1=0$ ou 1, et où $\mathfrak{P}$ est l'unique idéal au-dessus de p. Alors, pour obtenir $\omega(M)$, il suffit d'entrer "`oomega([m1,...,mr],p,k)`".

§ 2. Autour de $\mathscr{L}_{(M_1,M_2)}$

Soient $F=\Phi_{n_1}^{r_1}\Phi_{n_2}^{r_2}$ et $\mathfrak{D}$ l'ensemble des diviseurs différents de 1 de $\mathrm{Res}(\Phi_{n_1},\Phi_{n_2})^{\min(r_1,r_2)}$. Soient (M_1,h_1) et (M_2,h_2) tels que $(\mathscr{G}_{M_1},\mathscr{G}_{M_2})\in\coprod_{d\in\mathfrak{D}}\mathscr{G}(F,d)$ (cf. définition 1.6.7). Notons $\beta_i=\frac{1}{n_1}\mathrm{Tr}_{n_i}\circ h_i$, défini sur $W_i=M_i\otimes\mathbb{Q}$. Nous noterons $M_i^\#$ pour $(M_i)_{\beta_i}^\#$, $i=1,2$. Puisque $(\mathscr{G}_{M_1},\mathscr{G}_{M_2})\in\coprod_{d\in\mathfrak{D}}\mathscr{G}(F,d)$, il existe une anti-isométrie α de $(M_1^\#/M_1,\overline{\beta_1})$ sur $(M_2^\#/M_2,\overline{\beta_2})$ telle que le diagramme suivant commute :

$$\begin{array}{ccc} M_1^\#/M_1 & \xrightarrow{\alpha} & M_2^\#/M_2 \\ \downarrow{\scriptstyle \overline{t_1}} & & \downarrow{\scriptstyle \overline{t_2}} \\ M_1^\#/M_1 & \xrightarrow{\alpha} & M_2^\#/M_2 \end{array}$$

où t_i est la multiplication par ζ_{n_i}, pour $i=1,2$.

Définition 4.2.1

Soient (N,γ) un $\mathbb{Z}$-réseau, et q un nombre premier. Nous dirons que (N,γ) est *q-élémentaire*, si $qN^{\#} \subset N$. Ainsi, $N^{\#}/N$ est un $\mathbb{F}_q$-espace vectoriel de dimension inférieure ou égale au $\mathbb{Z}$-rang de N.

Supposons que $a(F,1) = a(F,2) =: p$ est un nombre premier (voir le corollaire 1.3.3 pour la définition de $a(F,i)$). Ainsi, (M_1,β_1) et (M_2,β_2) sont p-élémentaires, de plus, $M_1^{\#}/M_1$ et $M_2^{\#}/M_2$ sont des $\mathbb{F}_p$-espaces vectoriels isomorphes. Dans ce cas, on montre aisément que pour $i = 1,2$, $\beta_i(M_i^{\#}, M_i^{\#}) \subset \frac{1}{p}\mathbb{Z}$. On voit ainsi que $\overline{\beta_i}$ est à valeurs dans $\frac{1}{p}\mathbb{Z}/\mathbb{Z}$ que nous associerons à $\mathbb{F}_p$. Pour $i = 1,2$, notons $\overline{T_i}$ la matrice de $\overline{t_i}$ relativement à une $\mathbb{F}_p$-base de $M_i^{\#}/M_i$, et $\overline{B_i}$, la matrice de $\overline{\beta_i}$ relativement à la même base. Puisque $\overline{t_i}$ est une isométrie de $(M_i^{\#}/M_i, \overline{\beta_i})$, on a ${}^{\mathrm{tr}}\overline{T_i}\,\overline{B_i}\,\overline{T_i} = \overline{B_i}$.

Lemme 4.2.2

Sous les hypothèses du début de ce paragraphe, on a :

$$\det(\overline{B_i}) \in \mathbb{F}_p^*.$$

Démonstration :

En effet, supposons que $\overline{\beta_i}(x + M_i, y + M_i) = 0$ pour tout $y + M_i$. Cela veut dire que $\beta_i(x,y) \in \mathbb{Z}$ pour tout $y \in M_i^{\#}$. Ce qui signifie que $x \in M_i^{\#\#} = M_i$, autrement dit, $x + M_i = 0 + M_i$. ❄

Nous savons, grâce au théorème 1.6.8, que pour estimer la masse de $\overline{\mathscr{E}}(F)$, il faut calculer le cardinal de $\mathscr{L}_{(M_1,M_2)}$ pour de tels $((M_1,h_1),(M_2,h_2))$. Le théorème suivant donne une bijection de $\mathscr{L}_{(M_1,M_2)}$ sur un ensemble dont le cardinal est aisément calculable.

Théorème 4.2.3

Sous les hypothèses de l'introduction de ce paragraphe, posons $\Delta(M_1,M_2)$ l'ensemble des anti-isométries ν de $(M_1^{\#}/M_1, \overline{\beta_1})$ sur $(M_2^{\#}/M_2, \overline{\beta_2})$ telles que $\overline{t_2} \circ \nu = \nu \circ \overline{t_1}$. Enfin, pour $i = 1,2$, posons $\Omega(M_i)$ l'ensemble des isométries de $(M_i^{\#}/M_i, \overline{\beta_i})$ qui commutent avec $\overline{t_i}$. Alors, on a :

$$|\mathscr{L}_{(M_1,M_2)}| = |\Delta(M_1,M_2)| = |\Omega(M_1)| = |\Omega(M_2)|.$$

Ainsi, le cardinal de $\mathscr{L}_{(M_1,M_2)}$ est égal au nombre de matrices $X \in GL_n(\mathbb{F}_p)$ telles que ${}^{\mathrm{tr}}X\overline{B_i}X = \overline{B_i}$, et telles que $\overline{T_i}X = X\overline{T_i}$, pour $i = 1$ ou 2, et si n est la dimension de $M_i^{\#}/M_i$ sur $\mathbb{F}_p$.

Démonstration :

Tout d'abord, nous allons voir que $\mathscr{L}_{(M_1,M_2)}$ est en bijection avec $\Delta(M_1,M_2)$.

Soit $M \in \mathscr{L}_{(M_1,M_2)}$. Clairement, M est un $\Phi_{n_1}^{r_1}\Phi_{n_2}^{r_2}$-réseau. Nous avons vu, lors de la démonstration de la proposition 1.3.5, qu'il existait deux isomorphismes, que nous avons nommés $\overline{p_1}$ et $\overline{p_1}^{-1}$ tels que $M_1^{\#}/M_1 \xrightarrow{\overline{p_1}^{-1}} M/M_1 \boxplus M_2 \xrightarrow{\overline{p_1}} M_2^{\#}/M_2$. Nous avons remarqué que $\alpha_M := \overline{p_1} \circ \overline{p_1}^{-1}$ était un élément de $\Delta(M_1,M_2)$. Ainsi, nous avons une application de $\mathscr{L}_{(M_1,M_2)}$ dans $\Delta(M_1,M_2)$, $M \mapsto \alpha_M$.

Soit $\nu \in \Delta(M_1,M_2)$. Posons $M_\nu := \{x + y \in M_1^{\#} \boxplus M_2^{\#} \mid \nu(x + M_1) = y + M_2\}$. Nous avons déjà vu, toujours dans la démonstration de la proposition 1.3.5, que $M_{\alpha_M} = M$. Il reste à voir que $M_\nu \in \mathscr{L}_{(M_1,M_2)}$ pour tout $\nu \in \Delta(M_1,M_2)$, et que $\nu \mapsto M_\nu$ est injective.

Soit $\nu \in \Delta(M_1,M_2)$. Puisque ν est un isomorphisme de $M_1^{\#}/M_1$ sur $M_2^{\#}/M_2$, il suit immédiatement que $p_i(M_\nu) = M_i^{\#}$ et $M_\nu \cap W_i = M_i$, pour $i = 1,2$. On voit aussi que $M_\nu \subset M_\nu^{\#}$, grâce au fait que ν est

une anti-isométrie. D'autre part, $[M_\nu : M_1 \boxplus M_2] = [M_1^\# : M_1] = [M_2^\# : M_2]$. Ainsi,

$$\begin{aligned}[M_1^\# : M_1][M_2^\# : M_2] &= [M_1^\# \boxplus M_2^\# : M_1 \boxplus M_2] \\ &= [M_1^\# \boxplus M_2^\# : M_\nu^\#][M_\nu^\# : M_\nu][M_\nu : M_1 \boxplus M_2] \\ &= [M_1^\# : M_1][M_\nu^\# : M_\nu][M_2^\# : M_2],\end{aligned}$$

donc $[M_\nu^\# : M_\nu] = 1$, ou encore $M_\nu = M_\nu^\#$, c'est-à-dire que M_ν est unimodulaire. Enfin, $t(M_\nu) = M_\nu$ se déduit directement de $\overline{t_2} \circ \nu = \nu \circ \overline{t_1}$.

Pour terminer la démonstration du théorème, il faut trouver une bijection de $\Delta(M_1, M_2)$ sur $\Omega(M_1)$, par exemple. Nous avons supposé par hypothèse que $\Delta(M_1, M_2)$ possédait un élément que nous avons baptisé α. Soit $f : \nu \mapsto \alpha^{-1} \circ \nu$. C'est une application injective de $\Delta(M_1, M_2)$ dans $\Omega(M_1)$. Posons $g : \mu \mapsto \alpha \circ \mu$. C'est une application injective de $\Omega(M_1)$ dans $\Delta(M_1, M_2)$, et on montre facilement que $f \circ g = Id_{\Omega(M_1)}$, et $g \circ f = Id_{\Delta(M_1,M_2)}$, ce qui achève la démonstration. ❄

Nous savons à présent que pour calculer le cardinal de $\mathscr{L}_{(M_1,M_2)}$, il suffit de connaître la matrice $\overline{T_1}$ et la matrice $\overline{B_1}$. Nous verrons lors du prochain paragraphe qu'il suffira, pour nos exemples, de connaître $\overline{T_1}$ et $\det(\overline{B_1})$.

Souvenons-nous que les polynômes de la liste du théorème 3.2.3 possédant exactement 2 facteurs irréductibles distincts sont tous de la forme $\Phi_6^{r_1}\Phi_{n_2}^{r_2}$, avec $n_2 = 18, 54$ ou 66, ou alors $\Phi_{10}^3\Phi_{50}$. Les trois lemmes suivants nous donnent la matrice de $\overline{t_1}$ pour ces cas.

Lemme 4.2.4

Sous les hypothèses de ce paragraphe, supposons que $F = \Phi_6^{r_1}\Phi_{n_2}^{r_2}$ *avec* $n_2 = 18$ *ou* 54. *Alors* (M_1, β_1) *et* (M_2, β_2) *sont 3-élémentaires. En outre, si* $(\mathbb{Z}[\zeta_6], \ldots, \mathbb{Z}[\zeta_6], \underbrace{\mathfrak{P}_6, \ldots, \mathfrak{P}_6}_{m_1 \text{ fois}}, \underbrace{\mathfrak{P}_6^2, \ldots, \mathfrak{P}_6^2}_{m_2 \text{ fois}})$ *sont les facteurs invariants de* M_1 *dans* $M_1^\#$ *vus comme* $\mathbb{Z}[\zeta_6]$*-réseaux de* W_1, *alors il existe une* $\mathbb{F}_3$*-base de* $M_1^\#/M_1$ *telle que, relativement à cette base, la matrice de* $\overline{t_1}$ *vaut :*

$$\underbrace{(-1) \oplus \cdots \oplus (-1)}_{m_1 \text{ fois}} \oplus \underbrace{A \oplus \cdots \oplus A}_{m_2 \text{ fois}} \quad \text{avec } A = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \text{ ou } \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}.$$

Démonstration :

Le fait que $3M_1^\# \subset M_1$ et $3M_2^\# \subset M_2$ se déduit des relations polynomiales suivantes :

$$\Phi_{18} - (X+1)(X^3-1)\Phi_6 = 3$$
$$\Phi_{54} - (X^6 - X^3 + 1)(X+1)(X^9-2)\Phi_6 = 3.$$

En effet, cela montre que pour $i = 1, 2$, $n_2 = 18, 54$, et r_1, r_2 quelconque, on a $a(\Phi_6^{r_1}\Phi_{n_2}^{r_2}, i) = 3$, et on conclut grâce au corollaire 1.3.3. Ainsi, $M_1^\#/M_1$ est un $\mathbb{F}_3$-espace vectoriel. Si $\mathfrak{a}_1 \supset \cdots \supset \mathfrak{a}_n$ sont les facteurs invariants de M_1 dans $M_1^\#$, alors $\mathfrak{a}_i = \mathfrak{P}_6^j$ avec $j = 0, 1, 2$, car $3\mathbb{Z}[\zeta_6] = \mathfrak{P}_6^2$. Supposons donc, en vertu du théorème des facteurs invariants, et grâce au fait que $\mathbb{Z}[\zeta_6]$ est principal, qu'il existe $e_1, \ldots, e_n$ une $\mathbb{Z}[\zeta_6]$-base de W_1 telle que

$$M_1^\# = \mathbb{Z}[\zeta_6]e_1 \oplus \cdots \oplus \mathbb{Z}[\zeta_6]e_n,$$
$$M_1 = \mathbb{Z}[\zeta_6]e_1 \oplus \cdots \oplus \mathbb{Z}[\zeta_6]e_l \oplus \mathfrak{P}_6 e_{l+1} \oplus \cdots \oplus \mathfrak{P}_6 e_{l+m_1} \oplus \mathfrak{P}_6^2 e_{l+m_1+1} \oplus \cdots \oplus \mathfrak{P}_6^2 e_{l+m_1+m_2},$$

avec $l = n - m_1 - m_2$. On voit que $(e_1, t(e_1), \ldots, e_n, t(e_n))$ est une $\mathbb{Z}$-base de $M_1^\#$. Relativement à cette base, la matrice de t_1 $(= t|_{W_1})$ vaut

$$\underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \oplus \cdots \oplus \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}}_{n\text{fois}},$$

car le polynôme minimal de t_1 est $\Phi_6 = X^2 - X + 1$. En tant que $\mathbb{F}_3$-espace vectoriel, $M_1^\#/M_1$ est donc engendré par

$$e_{l+1} + M_1, \ldots, e_{l+m_1} + M_1, e_{l+m_1+1} + M_1, t(e_{l+m_1+1}) + M_1, \ldots, e_{l+m_1+m_2} + M_1, t(e_{l+m_1+m_2}) + M_1.$$

Or, nous savons que $\mathfrak{P}_6$ est engendré par $1 + \zeta_6$. Ainsi, $(1 + \zeta_6)e_{l+i} = e_{l+i} + t(e_{l+i}) \in M_i$, pour tout $i = 1, \ldots, m_1$. C'est-à-dire $\overline{t_1}(e_{l+i} + M_1) = t(e_{l+i}) + M_1 = -(e_{l+i} + M_1)$, pour tout $i = 1, \ldots, m_1$.

Pour terminer la démonstration du lemme, remarquons que

$$S^{-1}\begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix} S \equiv \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \pmod 3 \quad \text{avec } S = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}.$$

❄

Lemme 4.2.5

A nouveau sous les hypothèses de ce paragraphe, supposons que M soit un $\Phi_6^6\Phi_{66}$-réseau. Alors (M_1, β_1) et (M_2, β_2) sont 11-élémentaires. De plus, si $(\mathbb{Z}[\zeta_6], \ldots, \mathbb{Z}[\zeta_6], \underbrace{11 \cdot \mathbb{Z}[\zeta_6], \ldots, 11 \cdot \mathbb{Z}[\zeta_6]}_{m_1 \text{ fois}})$ sont les facteurs invariants de M_1 dans $M_1^\#$ vus comme $\mathbb{Z}[\zeta_6]$-réseaux de W_1, alors il existe une $\mathbb{F}_{11}$-base de $M_1^\#/M_1$ telle que, relativement à cette base, la matrice de $\overline{t_1}$ soit

$$\underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \oplus \cdots \oplus \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}}_{m_1 \text{ fois}}.$$

Démonstration :

L'égalité polynomiale

$$(-X + 1)\Phi_{66} - (-X^{19} - X^{18} + X^{17} + 3X^{16} + 2X^{15} - 2X^{14} - 5X^{13} - 3X^{12} +$$
$$3X^{11} + 7X^{10} + 4X^9 - 3X^8 - 8X^7 - 6X^6 + 2X^5 + 9X^4 + 8X^3 - X^2 - 10X - 10)\Phi_6 = 11$$

prouve que $11M_1^\# \subset M_1$. Pour achever la démonstration, on remarque que 11 reste premier dans $\mathbb{Z}[\zeta_6]$. Ainsi, un facteur invariant de M_1 dans $M_1^\#$ ne peut être que $\mathbb{Z}[\zeta_6]$ ou $11 \cdot \mathbb{Z}[\zeta_6]$. ❄

Lemme 4.2.6

Toujours sous les hypothèses du début de ce paragraphe, supposons que M soit un $\Phi_{10}^3\Phi_{50}$-réseau. (M_1, β_1) et (M_2, β_2) sont 5-élémentaires. Et si

$$(\mathbb{Z}[\zeta_{10}], \ldots, \mathbb{Z}[\zeta_{10}], \underbrace{\mathfrak{P}_{10}, \ldots, \mathfrak{P}_{10}}_{m_1 \text{fois}}, \underbrace{\mathfrak{P}_{10}^2, \ldots, \mathfrak{P}_{10}^2}_{m_2 \text{fois}}, \underbrace{\mathfrak{P}_{10}^3, \ldots, \mathfrak{P}_{10}^3}_{m_3 \text{fois}}, \underbrace{\mathfrak{P}_{10}^4, \ldots, \mathfrak{P}_{10}^4}_{m_4 \text{fois}})$$

sont les facteurs invariants de M_1 dans $M_1^\#$ vus comme $\mathbb{Z}[\zeta_{10}]$-réseaux de W_1, alors il existe une $\mathbb{F}_5$-base de $M_1^\#/M_1$ telle que, relativement à cette base, la matrice de $\overline{t_1}$ soit

$$\underbrace{A_1 \oplus \cdots \oplus A_1}_{m_1 \text{fois}} \oplus \underbrace{A_2 \oplus \cdots \oplus A_2}_{m_2 \text{fois}} \oplus \underbrace{A_3 \oplus \cdots \oplus A_3}_{m_3 \text{fois}} \oplus \underbrace{A_4 \oplus \cdots \oplus A_4}_{m_4 \text{fois}}$$

$$\text{où } A_1 = (-1), \quad A_2 = \begin{pmatrix} 0 & -1 \\ 1 & -2 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & -3 \\ 0 & 1 & -3 \end{pmatrix} \quad \text{et } A_4 = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Démonstration :

La démonstration de ce lemme est identique à celle des lemmes précédents, connaissant l'identité polynomiale suivante :

$$\Phi_{50} - (X + 1)(X^{15} - 2X^{10} + 3X^5 - 4)\Phi_{10} = 5,$$

sachant que $\Phi_{10} = X^4 - X^3 + X^2 - X + 1$, que $\mathfrak{P}_{10}^2$ est engendré par $(1 + \zeta_{10})^2 = 1 + 2\zeta_{10} + \zeta_{10}^2$, que $\mathfrak{P}_{10}^3$ est engendré par $(1 + \zeta_{10})^3 = 1 + 3\zeta_{10} + 3\zeta_{10}^2 + \zeta_{10}^3$, et que $5 \cdot \mathbb{Z}[\zeta_{10}] = \mathfrak{P}_5^4$. ❄

§ 3. Estimation de la masse de $\overline{\mathscr{E}}(F)$, si $F = \Phi_{n_1}^{r_1}\Phi_{n_2}^{r_2}$ fait partie de la liste du théorème 3.2.3

Souvenons-nous que ces polynômes sont les suivants :

$$\Phi_6\Phi_{18}^5 \quad \Phi_6^4\Phi_{18}^4 \quad \Phi_6^6\Phi_{66} \quad \Phi_6^7\Phi_{18}^3 \quad \Phi_6^7\Phi_{54} \quad \Phi_6^{10}\Phi_{18}^2 \quad \Phi_6^{13}\Phi_{18} \quad \Phi_{10}^3\Phi_{50}.$$

Soit $F = \Phi_{n_1}^{r_1}\Phi_{n_2}^{r_2}$, un de ces polynômes. Convenons, comme pour le paragraphe précédent, que (M_1, h_1) et (M_2, h_2) sont tels que $(\mathscr{G}_{M_1}, \mathscr{G}_{M_2}) \in \coprod_{d\in\mathfrak{D}} \mathscr{G}(F,d)$, avec $\mathfrak{D}$ l'ensemble des diviseurs différents de 1 de $\mathrm{Res}(\Phi_{n_1}, \Phi_{n_2})^{\min(r_1,r_2)}$, et que $\mathscr{G}(F,d)$ est l'ensemble introduit à la définition 1.6.7. Notons, pour $i = 1, 2$, $\beta_i = \frac{1}{n_i}\mathrm{Tr}_{n_i} \circ h_i$, défini sur $W_i := M_i \otimes \mathbb{Q}$.

Puisque F fait partie de la liste du théorème 3.2.3, il est clair que, pour $i = 1, 2$, (M_i, β_i) est tel que $\beta_i(x,x) \in 2\mathbb{Z}$, pour tout $x \in M_i$. Nous dirons, comme pour les $\mathbb{Z}$-réseaux unimodulaires, que (M_i, β_i) est *de type II*. Nous avons montré aux lemmes 4.2.4, 4.2.5 et 4.2.6 que de tels (M_i, β_i) étaient p-élémentaires, avec p premier. Le lemme suivant va nous montrer qu'il n'existe pas forcément de tels $\mathbb{Z}$-réseaux bilinéaires de déterminant donné dans toutes les dimensions.

Lemme 4.3.1

Soient $p \in \mathbb{P} - \{2\}$, et (M, β) un $\mathbb{Z}$-réseau bilinéaire défini positif, p-élémentaire, de type II, de déterminant p^k, et de dimension n. La congruence suivante est satisfaite :

$$n \equiv \pm 2 - 2 - (p-1)k \pmod 8.$$

Démonstration :

Cf. ([Co-Slo], theorem 13, p. 386) ❄

Voici encore un lemme classique.

Lemme 4.3.2

a) Soient $p \in \mathbb{P} - \{2\}$ et (M, β), un $\mathbb{F}_p$-espace vectoriel de dimension n, muni d'une forme bilinéaire symétrique non dégénérée. Posons $d = (-1)^{\frac{n(n-1)}{2}} \det(M, \beta)$. On a :

$$|O(M,\beta)| = \begin{cases} 2 \cdot p^{\frac{n(n-1)}{2}} \cdot (1 - (\frac{d}{p})p^{-m}) \cdot \prod_{0<2i<n} (1 - p^{-2i}) & \text{si } n = 2m \\ 2 \cdot p^{\frac{n(n-1)}{2}} \cdot \prod_{0<2i<n} (1 - p^{-2i}) & \text{sinon,} \end{cases}$$

où $(\frac{d}{p})$ est le symbole de Legendre.

b) Soient $p \in \mathbb{P} - \{2\}$ et (M, γ), un $\mathbb{F}_p$-espace vectoriel de dimension n, muni d'une forme bilinéaire antisymétrique non dégénérée. Soit G une matrice de γ. On a $G^{\mathrm{tr}} = -G \in Gl_n(\mathbb{F}_p)$. Il existe $S \in Gl_n(\mathbb{F}_p)$ telle que $S^{\mathrm{tr}}GS = J := H \oplus \cdots \oplus H$, où $H = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Notons

$$Sp_n(\mathbb{F}_p) := \{X \in M_n(\mathbb{F}_p) \mid X^{\mathrm{tr}}JX = J\},$$

appelé le *groupe symplectique*. On a

$$|Sp_n(\mathbb{F}_p)| = (p^n - 1)p^{n-1}(p^{n-2} - 1)p^{n-3} \cdots (p^2 - 1)p.$$

Démonstration :

a) Cf. ([Mis], corollaire 3.9).

b) Cf. ([Jacn], theorem 6.18). ❄

Définition 4.3.3

Soient $p \in \mathbb{P}$ et (M, β), un $\mathbb{F}_p$-espace vectoriel de dimension n, muni d'une forme bilinéaire symétrique. Soit B une matrice de β relativement à une certaine base de M. On pose

$$O(B) = \{A \in Gl_n(\mathbb{F}_p) \mid A^{\mathrm{tr}} B A = B\}.$$

Alors, $O(B)$ est un groupe isomorphe à $O(M, \beta)$.

(A) Le cas $F = \Phi_6 \Phi_{18}^5$

Nous savons que dans ce cas, (M_1, β_1) et (M_2, β_2) sont 3-élémentaires, et que $\det(M_1, \beta_1) = \det(M_2, \beta_2)$ divise 3^2. Or, le $\mathbb{Z}$-rang de M_1 est 2. Le lemme 4.3.1 nous affirme donc que $\det(M_1, \beta_1) = \det(M_2, \beta_2) = 3$. Ainsi, le facteur invariant de M_1 dans $M_1^{\#}$ vus comme $\mathbb{Z}[\zeta_6]$-réseaux de W_1 ne peut être que $\mathfrak{P}_6$. Grâce au lemme 4.2.4, on trouve que la matrice $\overline{T_1}$ vaut (-1). Celle de $\overline{B_1}$ vaut donc (± 1). Ainsi,

$$|\mathscr{L}_{(M_1,M_2)}| = |\Omega(M_1)| = |\{a \in \mathbb{F}_3 \mid a^2 = 1\}| = 2.$$

Le théorème 1.3.12 et le lemme 4.1.2 nous montrent que le facteur invariant de M_1 dans $M_{1h_1}^{\#}$ est $2 \cdot \mathfrak{P}_6^2 = 6\mathbb{Z}[\zeta_n]$. Ainsi, la masse du genre de (M_1, h_1) est égale à la masse de $(M_1, \frac{1}{6}h_1)$ (cf. lemme 2.1.5). On trouve alors $\omega(M_1) = \texttt{oomega([0],3,1)} = 1/6$.

Les facteurs invariants de M_2 dans $M_2^{\#}$ vus comme $\mathbb{Z}[\zeta_{18}]$-réseaux de W_2 sont $(\underbrace{\mathbb{Z}[\zeta_{18}], \ldots, \mathbb{Z}[\zeta_{18}]}_{4 \text{ fois}}, \mathfrak{P}_{18})$ (cf. théorème 1.4.1). Ainsi, les facteurs invariants de M_2 dans $(M_2)_{h_2}^{\#}$ sont $(\underbrace{2 \cdot \mathfrak{P}_{18}^3, \ldots, 2 \cdot \mathfrak{P}_{18}^3}_{4 \text{ fois}}, 2 \cdot \mathfrak{P}_{18}^4)$, en vertu du théorème 1.3.12, et du lemme 4.1.2. Or, on vérifie facilement que $\mathfrak{P}_{18}^3 = (\zeta_{18} + \overline{\zeta_{18}} + 2) \cdot \mathfrak{P}_{18}$. On peut donc supposer, pour le calcul de la masse du genre de M_2, que les facteurs invariants de M_2 dans $(M_2)_{h_2}^{\#}$ sont $(\underbrace{\mathfrak{P}_{18}, \ldots, \mathfrak{P}_{18}}_{4 \text{ fois}}, \mathfrak{P}_{18}^2)$ (cf. lemme 2.1.5). Ainsi,

$$\omega(M_2) = \texttt{oomega([1,1,1,1,2],3,2)} = 0.5151.$$

Donc, au vu de ce qui précède, et grâce au théorème 1.6.8, on a le

Théorème 4.3.4

$$\sum_{\overline{M} \in \overline{\mathscr{E}}(\Phi_6 \Phi_{18}^5)} \frac{1}{|O(M)|} \leq |\mathscr{L}(M_1, M_2)| \omega(M_1) \omega(M_2) \leq 0,1717.$$

❄

(B) Le cas $F = \Phi_6^4 \Phi_{18}^4$

Ce sera le calcul plus long. Ici aussi, nous savons aussi que (M_1, β_1) et (M_2, β_2) sont 3-élémentaires, et que $\det(M_1, \beta_1) = \det(M_2, \beta_2)$ divise $\mathrm{Res}(\Phi_6, \Phi_{18})^4 = 3^8$. Puisque le rang de M_1 vu comme $\mathbb{Z}$-réseau est 8, on voit que $\det(M_i, \beta_i) = 3^2, 3^4, 3^6$ ou 3^8, pour i=1,2 (cf. lemme 4.3.1).

(i) Le sous-cas $\det(M_1,\beta_1)=\det(M_2,\beta_2)=3^8$

Les facteurs invariants de M_1 dans $M_1^\#$ vus comme $\mathbb{Z}[\zeta_6]$-réseaux de W_1 sont $(\mathfrak{P}_6^2,\mathfrak{P}_6^2,\mathfrak{P}_6^2,\mathfrak{P}_6^2)$. Une matrice de $\overline{t_1}$ vaut donc $\begin{pmatrix}-1&-1\\0&-1\end{pmatrix}\oplus\cdots\oplus\begin{pmatrix}-1&-1\\0&-1\end{pmatrix}$ (cf. lemme 4.2.4). On peut trouver un changement de base tel que

$$\overline{T_1}=\begin{pmatrix}-I_4&0\\-I_4&-I_4\end{pmatrix}$$

où I_4 est la matrice identité de dimension 4×4. De ${}^{\mathrm{tr}}\overline{T_1}\,\overline{B_1}\,\overline{T_1}=\overline{B_1}$, on tire $\overline{B_1}=\begin{pmatrix}b_1&b_2\\-b_2&0\end{pmatrix}$ avec $b_1^{\mathrm{tr}}=b_1$, et $b_2^{\mathrm{tr}}=-b_2\in Gl_4(\mathbb{F}_3)$ (cf. lemme 4.2.2). Le cardinal de $\mathscr{L}_{(M_1,M_2)}$ est le nombre de matrices X satisfaisant ${}^{\mathrm{tr}}X\overline{B_1}X=\overline{B_1}$ et $\overline{T_1}X=X\overline{T_1}$. De $\overline{T_1}X=X\overline{T_1}$, on tire $X=\begin{pmatrix}x_1&0\\x_2&x_1\end{pmatrix}$. De ${}^{\mathrm{tr}}X\overline{B_1}X=\overline{B_1}$, on obtient le système d'équation :

$$x_1^{\mathrm{tr}}b_2x_1=b_2 \tag{1}$$

$$x_1^{\mathrm{tr}}b_2x_2-x_2^{\mathrm{tr}}b_2x_1=b_1-x_1^{\mathrm{tr}}b_1x_1. \tag{2}$$

Puisque $b_2^{\mathrm{tr}}=-b_2\in Gl_4(\mathbb{F}_3)$, l'ensemble des x_1 satisfaisant (1) est égal au cardinal du groupe symplectique $|Sp_4(\mathbb{F}_3)|=(3^4-1)3^3(3^2-1)3=2^73^45$. Pour x_1 fixé, le nombre de matrices satisfaisant (2) est égal au nombre de matrices $m\in M_4(\mathbb{F}_3)$ telle que $m+m^{\mathrm{tr}}=b_1-x_1^{\mathrm{tr}}b_1x_1$, car b_2 et x_1 sont inversibles. Ce nombre vaut 3^6. On trouve donc

$$|\mathscr{L}_{(M_1,M_2)}|=2^73^{10}5.$$

D'autre part, en utilisant les mêmes arguments que pour le calcul de la masse de $\overline{\mathscr{E}}(\Phi_6\Phi_{18}^5)$, on trouve

$$\omega(M_1)=\texttt{oomega([1,1,1,1],3,1)}\leq 8,42\ 10^{-6}$$

$$\omega(M_2)=\texttt{oomega([1,1,1,1],3,2)}\leq 1,17\ 10^{-3}.$$

On en déduit que $|\mathscr{L}_{(M_1,M_2)}|\omega(M_1)\omega(M_2)\leq 0,37204$.

(ii) Le sous-cas $\det(M_1,\beta_1)=\det(M_2,\beta_2)=3^6$

Les facteurs invariants de M_1 dans $M_1^\#$ vus comme $\mathbb{Z}[\zeta_6]$-réseaux de W_1 pourraient être $(\mathbb{Z}[\zeta_6],\mathfrak{P}_6^2,\mathfrak{P}_6^2,\mathfrak{P}_6^2)$. Mais cela est impossible, car dans ce cas, les facteurs invariants de $(M_1)_3$ dans $((M_1)_{h_1}^\#)_3$ seraient $(\mathfrak{P}_6,\mathfrak{P}_6^3,\mathfrak{P}_6^3,\mathfrak{P}_6^3)$. La décomposition de Jordan serait $N_1\boxplus N_2$, où N_1 serait $\mathfrak{P}_6$-modulaire de rang 1, et N_2 serait $\mathfrak{P}_6^3$-modulaire de rang 3. Cela est impossible, car nous avons vu au théorème 1.5.17 que tout $\mathbb{Z}[\zeta_6]_{\mathfrak{P}_6}$-module, $\mathfrak{P}_6^m$-modulaire, avec m impair, était de rang pair.

Par la suite, et pour ne pas devoir répéter ce raisonnement, nous dirons que les facteurs invariants de M_1 dans $M_1^\#$ ne peuvent pas être $(\mathbb{Z}[\zeta_6],\mathfrak{P}_6^2,\mathfrak{P}_6^2,\mathfrak{P}_6^2)$, par *parité de rang.*

Les facteurs invariants de M_1 dans $M_1^\#$ ne peuvent donc être que $(\mathfrak{P}_6,\mathfrak{P}_6,\mathfrak{P}_6^2,\mathfrak{P}_6^2)$. Dans ce cas, nous avons vu au lemme 4.2.4 qu'une matrice de $\overline{t_1}$ pouvait être $\begin{pmatrix}-1&0\\0&-1\end{pmatrix}\oplus\begin{pmatrix}-1&-1\\0&-1\end{pmatrix}\oplus\begin{pmatrix}-1&-1\\0&-1\end{pmatrix}$. Or, cette matrice est semblable à

$$\overline{T_1}=\begin{pmatrix}-I_2&0&0\\0&-I_2&0\\-I_2&0&-I_2\end{pmatrix}$$

où I_2 est la matrice identité de dimension 2×2. Puisque ${}^{\mathrm{tr}}\overline{T_1}\,\overline{B_1}\,\overline{T_1}=\overline{B_1}$, on voit que

$$\overline{B_1}=\begin{pmatrix}b_1&b_2&b_3\\b_2^{\mathrm{tr}}&b_4&0\\-b_3&0&0\end{pmatrix}$$

avec $b_4^{\mathrm{tr}} = b_4 \in Gl_2(\mathbb{F}_3)$ et $b_3^{\mathrm{tr}} = -b_3 \in Gl_2(\mathbb{F}_3)$ (cf. lemme 4.2.2). Nous allons calculer $|\mathscr{L}_{(M_1,M_2)}|$. Soit $X \in M_6(\mathbb{F}_3)$ telle que $X\overline{T_1} = \overline{T_1}X$. On vérifie que

$$X = \begin{pmatrix} x_1 & 0 & 0 \\ x_4 & x_5 & 0 \\ x_7 & x_8 & x_1 \end{pmatrix}.$$

Supposons que X satisfasse $X^{\mathrm{tr}}\overline{B_1}X = \overline{B_1}$; on tire alors 4 équations :

$$x_1^{\mathrm{tr}} b_3 x_1 = b_3 \tag{1}$$

$$x_5^{\mathrm{tr}} b_4 x_5 = b_4 \tag{2}$$

$$x_1^{\mathrm{tr}} b_2 x_4 + (x_1^{\mathrm{tr}} b_2 x_4)^{\mathrm{tr}} + x_1^{\mathrm{tr}} b_3 x_7 + (x_1^{\mathrm{tr}} b_3 x_7)^{\mathrm{tr}} + x_4^{\mathrm{tr}} b_4 x_4 = b_1 - x_1^{\mathrm{tr}} b_1 x_1 \tag{3}$$

$$b_2 - x_1^{\mathrm{tr}} b_2 x_5 - x_4^{\mathrm{tr}} b_4 x_5 = x_1^{\mathrm{tr}} b_3 x_8. \tag{4}$$

Il y a $|Sp_2(\mathbb{F}_3)| = (3^2-1)\cdot 3 = 2^3 \cdot 3$ choix pour les matrices x_1 satisfaisant l'équation (1). Il y a $|O(b_4)|$ choix pour les matrices x_5 satisfaisant l'équation (2). Si $\det(b_4) = -1$, alors $|O(b_4)| = 2\cdot 3\cdot(1-3^{-1}) = 2^2$, et si $\det(b_4) = 1$, alors $|O(b_4)| = 2\cdot 3\cdot(1+3^{-1}) = 2^3$ (cf. lemme 4.3.2). Nous verrons en annexe que dans notre cas, $\det(\overline{B_1}) = -1$, et donc que $\det(b_4) = -1$. Fixons x_4 de manière arbitraire. Cela fait 3^4 possibilités. Le nombre de matrices x_7 satisfaisant (3) est le nombre de matrices $m \in M_2(\mathbb{F}_3)$ telles que $m+m^{\mathrm{tr}}$ est fixé, car x_1 et b_3 sont inversibles. Cela fait 3 possibilités. Les matrices x_1, x_4, x_5 étant choisies, la matrice x_8 est déterminée à nouveau car x_1 est b_3 sont inversibles. On a ainsi $|\mathscr{L}_{(M_1,M_2)}| = 2^5\cdot 3^6$. Par conséquent, on trouve :

$$\begin{aligned} |\mathscr{L}_{(M_1,M_2)}|\omega(M_1)\omega(M_2) &= 2^5\cdot 3^6 \texttt{oomega([0,0,1,1],3,1)}\cdot\texttt{oomega([0,0,1,1],3,2)} \\ &\leq 0,092. \end{aligned}$$

(iii) Le sous-cas $\det(M_1,\beta_1) = \det(M_2,\beta_2) = 3^4$

Les facteurs invariants de M_1 dans $M_1^{\#}$ ne peuvent pas être $(\mathbb{Z}[\zeta_6], \mathfrak{P}_6, \mathfrak{P}_6, \mathfrak{P}_6^2)$ par parité de rang.

a) Supposons que les facteurs invariants de M_1 dans $M_1^{\#}$ soient $(\mathfrak{P}_6, \mathfrak{P}_6, \mathfrak{P}_6, \mathfrak{P}_6)$.
Dans ce cas, $\overline{T_1} = -I_4$. Nous verrons en annexe que dans ce cas $\det(\overline{B_1}) = 1$. Ainsi,

$$|\mathscr{L}_{(M_1,M_2)}| = |O(\overline{B_1})| = 2\cdot 3^6\cdot(1-3^{-2})^2 = 2^7\cdot 3^2.$$

On trouve alors

$$\begin{aligned} |\mathscr{L}_{(M_1,M_2)}|\omega(M_1)\omega(M_2) &= 2^7\cdot 3^2 \texttt{oomega([0,0,0,0],3,1)}\cdot\texttt{oomega([0,0,0,0],3,2)} \\ &\leq 2,84\cdot 10^{-4}. \end{aligned}$$

b) Supposons que les facteurs invariants de M_1 dans $M_1^{\#}$ soient $(\mathbb{Z}[\zeta_6], \mathbb{Z}[\zeta_6], \mathfrak{P}_6^2, \mathfrak{P}_6^2)$.
Dans ce cas, et de manière semblable au cas $\det(M_i,\beta_i) = 3^8$, on a $\overline{T_1} = \begin{pmatrix} -I_2 & 0 \\ -I_2 & -I_2 \end{pmatrix}$. Et on trouve que $\overline{B_1} = \begin{pmatrix} b_1 & b_2 \\ -b_2 & 0 \end{pmatrix}$. Par suite, $|\mathscr{L}_{(M_1,M_2)}| = 3^3\cdot|Sp_2(\mathbb{F}_3)| = 3^3\cdot(3^2-1)\cdot 3 = 2^3\cdot 3^4$. Donc :

$$\begin{aligned} |\mathscr{L}_{(M_1,M_2)}|\omega(M_1)\omega(M_2) &= 2^3 3^4 \texttt{oomega([1,1,3,3],3,1)}\cdot\texttt{oomega([1,1,3,3],3,2)} \\ &\leq 5,1672\cdot 10^{-2}. \end{aligned}$$

(iv) Le sous-cas $\det(M_1,\beta_1)=\det(M_2,\beta_2)=3^2$

Les facteurs invariants de M_1 dans $M_1^{\#}$ ne peuvent pas être $(\mathbb{Z}[\zeta_6],\mathbb{Z}[\zeta_6],\mathbb{Z}[\zeta_6],\mathfrak{P}_6^2)$ par parité de rang.

Les facteurs invariants de M_1 dans $M_1^{\#}$ ne peuvent donc être que $(\mathbb{Z}[\zeta_6],\mathbb{Z}[\zeta_6],\mathfrak{P}_6,\mathfrak{P}_6)$. Dans ce cas, $\overline{T_1}=-I_2$. Ainsi, $|\mathscr{L}_{(M_1,M_2)}|=O(\overline{B_1})=3\cdot(1-3^{-1})=2^2$, car $\det(\overline{B_1})=-1$, comme nous le verrons en annexe. On trouve alors :

$$|\mathscr{L}_{(M_1,M_2)}|\omega(M_1)\omega(M_2)=2^2\cdot \texttt{oomega([1,1,2,2],3,1)}\cdot \texttt{oomega([1,1,2,2],3,2)}\leq 1{,}58\cdot 10^{-5}.$$

De ces calculs et du théorème 1.6.8, on peut énoncer le

Théorème 4.3.5

$$\sum_{M\in\overline{\mathscr{E}}(\Phi_6^4\Phi_{18}^4)}\frac{1}{|O(M)|}\leq 0{,}4237521.$$

❄

(C) Le cas $F=\Phi_6^7\Phi_{18}^3$

Les $\mathbb{Z}$-réseaux (M_1,β_1) et (M_2,β_2) sont 3-élémentaires, et la dimension de $M_1=14\equiv 6\pmod 8$. Le lemme 4.3.1 nous donne que $\det(M_1,\beta_1)=\det(M_2,\beta_2)=3^1,3^3$ ou 3^5.

(i) Le sous-cas $\det(M_1,\beta_1)=\det(M_2,\beta_2)=3^5$

Les facteurs invariants de M_1 dans $M_1^{\#}$ vus comme $\mathbb{Z}[\zeta_6]$-réseaux de W_1 ne peuvent être ni $(\mathbb{Z}[\zeta_6],\mathbb{Z}[\zeta_6],\underbrace{\mathfrak{P}_6,\ldots,\mathfrak{P}_6}_{5\text{ fois}})$, ni $(\mathbb{Z}[\zeta_6],\mathbb{Z}[\zeta_6],\mathbb{Z}[\zeta_6],\mathfrak{P}_6,\mathfrak{P}_6,\mathfrak{P}_6,\mathfrak{P}_6^2)$, car le M_2 est de rang 3 en tant que $\mathbb{Z}[\zeta_{18}]$-réseau de W_1, et en vertu du théorème 1.4.1.

Le seul cas est donc $(\mathbb{Z}[\zeta_6],\mathbb{Z}[\zeta_6],\mathbb{Z}[\zeta_6],\mathbb{Z}[\zeta_6],\mathfrak{P}_6,\mathfrak{P}_6^2,\mathfrak{P}_6^2)$. Relativement à une base convenable, on a :

$$\overline{T_1}=\begin{pmatrix}-I_2 & -I_2 & 0\\ 0 & -I_2 & 0\\ 0 & 0 & -I_1\end{pmatrix}.$$

Puisque $\overline{T_1}^{\mathrm{tr}}\overline{B_1}\,\overline{T_1}=\overline{B_1}$, on en déduit que

$$\overline{B_1}=\begin{pmatrix}0 & b_2 & 0\\ -b_2 & b_4 & b_5\\ 0 & b_5^{\mathrm{tr}} & b_6\end{pmatrix}$$

avec $b_2^{\mathrm{tr}}=-b_2\in Gl_2(\mathbb{F}_3)$, et $b_6=(\pm 1)$ (cf. lemme 4.2.2). Soit $X\in M_5(\mathbb{F}_3)$ tel que $X\overline{T_1}=\overline{T_1}X$. Alors X est de la forme

$$\begin{pmatrix}x_1 & x_2 & x_3\\ 0 & x_1 & 0\\ 0 & x_8 & x_9\end{pmatrix}.$$

Si X satisfait en plus $X^{\mathrm{tr}}\overline{B_1}X=\overline{B_1}$, on trouve comme avant 4 équations :

$$x_1^{\mathrm{tr}}b_2x_1=b_2 \tag{1}$$

$$x_9^{\mathrm{tr}}b_6x_9=b_6 \tag{2}$$

$$x_2^{\mathrm{tr}}b_2x_1+(x_2^{\mathrm{tr}}b_2x_1)^{\mathrm{tr}}+x_1^{\mathrm{tr}}b_5x_8+(x_1^{\mathrm{tr}}b_5x_8)^{\mathrm{tr}}+x_8^{\mathrm{tr}}b_6x_8=b_4-x_1^{\mathrm{tr}}b_4x_1 \tag{3}$$

$$b_5-x_1^{\mathrm{tr}}b_5x_9-x_8^{\mathrm{tr}}b_6x_9=x_1^{\mathrm{tr}}b_2^{\mathrm{tr}}x_3. \tag{4}$$

En raisonnant de la même manière que dans (B)(ii), mais en sachant que $|O(b_6)| = 2$, si $b_6 = (\pm 1)$, on trouve $|\mathscr{L}_{(M_1,M_2)}| = 2^4 \cdot 3^6$.

On peut considérer que les facteurs invariants de M_1 dans $(M_1)_{h_1}^{\#}$ sont $(\mathfrak{P}_6, \mathfrak{P}_6, \mathfrak{P}_6, \mathfrak{P}_6, \mathfrak{P}_6^2, \mathfrak{P}_6^3, \mathfrak{P}_6^3)$ (cf. théorème 1.3.12, lemmes 2.1.5 et 4.1.2). Ceux de M_2 dans $(M_2)_{h_2}^{\#}$ sont, en vertu du théorème 1.4.1, et du lemme 1.3.12, $(2 \cdot \mathfrak{P}_{18}^4, 2 \cdot \mathfrak{P}_{18}^5, 2 \cdot \mathfrak{P}_{18}^5)$, et on peut considérer pour le calcul de la masse de M_2 que ces facteurs sont $(\mathbb{Z}[\zeta_{18}], \mathfrak{P}_{18}, \mathfrak{P}_{18})$, car $\mathfrak{P}_{18}^4 = (\zeta_{18} + \overline{\zeta_{18}} + 2)^2 \cdot \mathbb{Z}[\zeta_{18}]$, et en vertu du lemme 2.1.5. Donc :

$$|\mathscr{L}_{(M_1,M_2)}\omega(M_1)\omega(M_2) = 2^4 3^6 \cdot \texttt{oomega([1,1,1,1,2,3,3],3,1)} \cdot \texttt{oomega([0,1,1],3,2)} \leq 0,15075.$$

(ii) Le sous-cas $\det(M_1, \beta_1) = \det(M_2, \beta_2) = 3^3$

Les facteurs invariants de M_1 dans $M_1^{\#}$ ne peuvent pas être $(\underbrace{\mathbb{Z}[\zeta_6], \ldots, \mathbb{Z}[\zeta_6]}_{5 \text{ fois}}, \mathfrak{P}_6, \mathfrak{P}_6^2)$ par parité de rang. Ainsi, le seul cas possible est $(\underbrace{\mathbb{Z}[\zeta_6], \ldots, \mathbb{Z}[\zeta_6]}_{4 \text{ fois}}, \mathfrak{P}_6, \mathfrak{P}_6, \mathfrak{P}_6)$. Donc, $\overline{T_1} = -I_3$, et $|\mathscr{L}_{(M_1,M_2)}| = |O(\overline{B_1})| = 2 \cdot 3^3 \cdot (1 - 3^3) = 48$. Par suite, on trouve

$$|\mathscr{L}_{(M_1,M_2)}|\omega(M_1)\omega(M_2) = 48 \cdot \texttt{oomega([1,1,1,1,2,2,2],3,1)} \cdot \texttt{oomega([0,0,0],3,2)} \leq 5,32 \cdot 10^{-8}.$$

(iii) Le sous-cas $\det(M_1, \beta_1) = \det(M_2, \beta_2) = 3$

Ici, les facteurs invariants de M_1 dans $M_1^{\#}$ sont $(\underbrace{\mathbb{Z}[\zeta_6], \ldots, \mathbb{Z}[\zeta_6]}_{6 \text{ fois}}, \mathfrak{P}_6)$, donc $|\mathscr{L}_{(M_1,M_2)}| = 2$, et

$$|\mathscr{L}_{(M_1,M_2)}|\omega(M_1)\omega(M_2) = 2 \cdot \texttt{oomega([1,1,1,1,1,1,2],3,1)} \cdot \texttt{oomega([1,1,2],3,2)} \leq 2,5 \cdot 10^{-11}.$$

De ces trois sous-cas, et du théorème 1.6.8, on a le

Théorème 4.3.6

$$\sum_{\overline{M} \in \overline{\mathscr{E}}(\Phi_6^7 \Phi_{18}^3)} \frac{1}{|O(M)|} \leq 0,151.$$

❄

(D) Le cas $F = \Phi_6^{10}\Phi_{18}^2$

Le théorème 1.3.9 et le lemme 4.3.1 nous apprennent que $\det(M_1, \beta_1) = \det(M_2, \beta_2) = 3^4$ ou 3^2.

(i) Le sous-cas $\det(M_1, \beta_1) = \det(M_2, \beta_2) = 3^4$

Les facteurs invariants de M_1 dans $M_1^{\#}$ ne peuvent être que $(\underbrace{\mathbb{Z}[\zeta_6], \ldots, \mathbb{Z}[\zeta_6]}_{8 \text{ fois}}, \mathfrak{P}_6^2, \mathfrak{P}_6^2)$. Ainsi,

$$\overline{T_1} = \begin{pmatrix} -I_2 & 0 \\ -I_2 & -I_2 \end{pmatrix} \quad \text{et} \quad \overline{B_1} = \begin{pmatrix} b_1 & b_2 \\ -b_2 & 0 \end{pmatrix},$$

avec $b_2^{\mathrm{tr}} = -b_2 \in Gl_2(\mathbb{F}_3)$. Soit $X \in M_4(\mathbb{F}_3)$ tel que $X\overline{T_1} = \overline{T_1}X$ et $X^{\mathrm{tr}}\overline{B_1}X = \overline{B_1}$. Alors

$$X = \begin{pmatrix} x_1 & 0 \\ x_2 & x_1 \end{pmatrix},$$

et x_1, x_2 doivent satisfaire les équations :

$$x_1^{\mathrm{tr}} b_2 x_1 = b_2$$
$$x_1^{\mathrm{tr}} b_2 x_2 + (x_1^{\mathrm{tr}} b_2 x_2)^{\mathrm{tr}} = b_1 - x_1^{\mathrm{tr}} b_1 x_1.$$

On obtient $|\mathscr{L}_{(M_1,M_2)}| = (3^2-1)\cdot 3 \cdot 3 = 72$. Ainsi,

$$|\mathscr{L}_{(M_1,M_2)}| \cdot \omega(M_1)\cdot\omega(M_2) = 72 \cdot \texttt{oomega([1,1,1,1,1,1,1,1,3,3],3,1)} \cdot \texttt{oomega([1,1],3,2)}$$
$$\leq 5,387 \cdot 10^{-5}.$$

(ii) Le sous-cas $\det(M_1,\beta_1) = \det(M_2,\beta_2) = 3^2$

Les facteurs invariants de M_1 dans $(M_1)^{\#}$ ne peuvent pas être $(\underbrace{\mathbb{Z}[\zeta_6],\ldots,\mathbb{Z}[\zeta_6]}_{9 \text{ fois}},\mathfrak{P}_6^2)$ par parité de rang. Ces facteurs sont donc$(\underbrace{\mathbb{Z}[\zeta_6],\ldots,\mathbb{Z}[\zeta_6]}_{8 \text{ fois}},\mathfrak{P}_6,\mathfrak{P}_6)$. Ainsi, $|\mathscr{L}_{(M_1,M_2)}| \leq 2\cdot 3\cdot(1+3^{-1}) = 8$, car $\overline{T_1} = -I_2$. On en déduit :

$$|\mathscr{L}_{(M_1,M_2)}| \cdot \omega(M_1)\omega(M_2) \leq 8 \cdot \texttt{oomega([1,1,1,1,1,1,1,1,2,2],3,1)} \cdot \texttt{oomega([0,0],3,2)}$$
$$\leq 3,65 \cdot 10^{-9}.$$

De ces deux sous-cas, et du théorème 1.6.8, on a le

Théorème 4.3.7

$$\sum_{\overline{M}\in\overline{\mathscr{E}}(\Phi_6^{10}\Phi_{18}^2)} \frac{1}{|O(M)|} \leq 5,39\cdot 10^{-5}.$$

❄

(E) Le cas $F = \Phi_6^{13}\Phi_{18}$

Le théorème 1.3.9 et le lemme 4.3.1 nous apprennent que $\det(M_1,\beta_1) = \det(M_2,\beta_2) = 3$.

Les facteurs invariants de M_1 dans $M_1^{\#}$ sont donc $(\underbrace{\mathbb{Z}[\zeta_6],\ldots,\mathbb{Z}[\zeta_6]}_{12 \text{ fois}},\mathfrak{P}_6)$. Ainsi, $\overline{T_1} = (-1)$. Donc $|\mathscr{L}_{(M_1,M_2)}| = 2$. Par suite :

$$|\mathscr{L}_{(M_1,M_2)}| \cdot \omega(M_1)\cdot\omega(M_2) = 2 \cdot \texttt{oomega([1,...,1,2],3,1)} \cdot \texttt{oomega([0],3,2)} \leq 2,24\cdot 10^{-8}.$$

D'où,

Théorème 4.3.8

$$\sum_{\overline{M}\in\overline{\mathscr{E}}(\Phi_6^{13}\Phi_{18})} \frac{1}{|O(M)|} \leq 2,24\cdot 10^{-8}.$$

❄

(F) Le cas $F = \Phi_6^7\Phi_{54}$

Le théorème 1.3.9 et le lemme 4.3.1 nous apprennent que $\det(M_1,\beta_1) = \det(M_2,\beta_2) = 3$, car $|\operatorname{Res}(\Phi_6,\Phi_{54})| = 3^2$.

Les facteurs invariants de M_1 dans $M_1^\#$ sont $(\underbrace{\mathbb{Z}[\zeta_6],\dots,\mathbb{Z}[\zeta_6]}_{6\text{ fois}},\mathfrak{P}_6)$. Ainsi, on voit que $\overline{T_1} = (-1)$ et $|\mathscr{L}_{(M_1,M_2)}| = 2$ (cf. lemme 4.2.4). Le facteur invariant de M_2 dans $M_2^\#$ est donc $\mathfrak{P}_{54}$ (cf. théorème 1.4.1). Nous savons que $54\cdot\mathscr{D}_{54} = 2\cdot\mathfrak{P}_{54}^9$ (cf. lemme 4.1.2). Ainsi, le facteur invariant de M_2 dans $(M_2)_{h_2}^\#$ est $2\cdot\mathfrak{P}_{54}^{10}$. Puisque $\mathfrak{P}_{54}^{10} = (\zeta_{54}+\overline{\zeta_{54}})^5\cdot\mathbb{Z}[\zeta_{54}]$, on peut supposer, pour le calcul de la masse de M_2, que $M_2 = (M_2)_{h_2}^\#$. En résumé,

$$|\mathscr{L}_{(M_1,M_2)}|\cdot\omega(M_1)\omega(M_2) = 2\cdot\texttt{oomega([1,1,1,1,1,1,2],3,1)}\cdot\texttt{oomega([0],3,3)} \le 2{,}61\cdot10^{-10}.$$

D'où,

Théorème 4.3.9

$$\sum_{\overline{M}\in\overline{\mathscr{E}}(\Phi_6^7\Phi_{54})}\frac{1}{|O(M)|} \le 2{,}61\cdot10^{-10}.$$

❄

(G) Le cas $F = \Phi_6^6\Phi_{66}$

Puisque $\operatorname{Res}(\Phi_6,\Phi_{66}) = 11^2$, le théorème 1.3.9 et le lemme 4.3.1 nous apprennent que $\det(M_1,\beta_1) = \det(M_2,\beta_2) = 11^2$. Les facteurs invariants de M_1 dans $M_1^\#$ sont alors $(\underbrace{\mathbb{Z}[\zeta_6],\dots,\mathbb{Z}[\zeta_6]}_{5\text{ fois}},11\cdot\mathbb{Z}[\zeta_6])$. le lemme 4.2.5 nous donne que $\overline{T_1} = \begin{pmatrix}0 & -1\\ 1 & 1\end{pmatrix}$. De ${}^{\mathrm{tr}}\overline{T_1}\,\overline{B_1}\,\overline{T_1} = \overline{B_1}$, on tire que $\overline{B_1} = \begin{pmatrix}2a & a\\ a & 2a\end{pmatrix}$ avec $a\in\mathbb{F}_{11}^*$. On en déduit, après calculs, que

$$|\mathscr{L}_{(M_1,M_2)}| = |\{X\in M_2(\mathbb{F}_{11}) \mid X\overline{T_1} = \overline{T_1}X \text{ et } X^{\mathrm{tr}}\overline{B_1}X = \overline{B_1}\}| = |\{\pm I_2\}| = 2.$$

On peut considérer que les facteurs invariants de M_1 dans $(M_1)_{h_1}^\#$ sont $(\underbrace{\mathfrak{P}_6,\dots,\mathfrak{P}_6}_{5\text{ fois}},11\mathfrak{P}_6)$ (cf. théorème 1.3.12 et lemme 2.1.5). Nous allons calculer la masse de (M_1,h_1) "à la main", car $(M_1)_p$ est non unimodulaire si $p = 3$ et 11. La fonction "oomega" n'est donc pas utilisable dans ce cas. Ainsi,

$$\mathfrak{B}_3(M_1) = 3^{21}\cdot\prod_{i=1}^{3}(1-3^{-2i}) = 2^{10}\cdot3^9\cdot5\cdot7\cdot13 \quad \text{(cf. théorème 2.2.6)}.$$

D'autre part, $\mathfrak{B}_{11}(M_1) = \mathfrak{B}_{11}(N_1\boxplus N_2)$, où N_1 est unimodulaire de rang 5, et N_2 est $11\mathbb{Z}[\zeta_6]_{11}$-modulaire. On en déduit (cf. théorèmes 2.2.5 et 2.2.6) que

$$\begin{aligned}\mathfrak{B}_{11}(M_1) &= 11\cdot\mathfrak{B}_{11}(N_1)\cdot\mathfrak{B}_{11}(N_2')\\ &= 11\cdot\prod_{i=1}^{5}(1-(-1)^i\cdot11^{-i})\cdot(1+11^{-1}) \ge 12{,}99.\end{aligned}$$

De plus,

$$\prod_{p\neq3,11}\mathfrak{B}_p(M_1)^{-1} \le 3^{-\frac{3}{2}}\cdot\pi\cdot(1+11^{-1})^{-1}\cdot\prod_{i=2}^{6}\zeta(i)(1-3^{-i})(1-11^{-i}) \le 1{,}043 \quad \text{(cf. théorème 2.3.1)}.$$

Finalement,

$$\begin{aligned}\omega(M_1) &= 2\cdot 3^{\frac{21}{2}}\cdot\prod_{j=1}^{6}\frac{(j-1)}{(2\pi)^j}\cdot[(M_1)_{h_1}^{\#}:M_1]^3\cdot\prod_{p\in\mathbb{P}(\mathbb{Z})}\mathfrak{B}_p(M_1)^{-1}\\ &\leq 7,347\cdot 10^{-4},\end{aligned}$$

car

$$[(M_1)_{h_1}^{\#}:M_1]=\underbrace{|\mathbb{Z}[\zeta_6]/\mathfrak{P}_6|\cdots|\mathbb{Z}[\zeta_6]/\mathfrak{P}_6|}_{6\text{ fois}}\cdot|\mathbb{Z}[\zeta_6]/11\mathbb{Z}[\zeta_6]|=3^6\cdot 11^2.$$

Nous allons maintenant calculer $\omega(M_2)$. Le théorème 1.4.1 nous apprend que le facteur invariant de M_2 dans $M_2^{\#}$ est $\mathfrak{P}_{11,66}$. Ainsi, le facteur invariant de M_2 dans $(M_2)_{h_2}^{\#}$ est $\mathfrak{P}_{11,66}^2\cdot\mathfrak{P}_{(1,3),66}\cdot\mathfrak{P}_{(2,3),66}$ (cf. théorème 1.3.12 et lemme 4.1.2). Or, cet idéal est engendré par un élément de $\mathbb{Z}[\zeta_{66}+\overline{\zeta_{66}}]$ (cf. lemme 4.1.2). Ainsi, on peut supposer que $M_2=(M_2)_{h_2}^{\#}$ pour le calculs de $\omega(M_2)$. D'où,

$$\omega(M_2)=|\{x\in\mathbb{Z}[\zeta_{66}]\mid x\overline{x}=1\}|=\frac{1}{66}.$$

De cela et du théorème 1.6.8, on a le

Théorème 4.3.10

$$\sum_{\overline{M}\in\overline{\mathscr{E}}(\Phi_6^6\Phi_{66})}\frac{1}{|O(M)|}\leq 2,23\cdot 10^{-5}.$$

❄

(H) Le cas $F=\Phi_{10}^3\Phi_{50}$

Puisque $\mathrm{Res}(\Phi_{10},\Phi_{50})=5^4$, le théorème 1.3.9 et le lemme 4.3.1 nous apprennent que $\det(M_1,\beta_1)=\det(M_2,\beta_2)=5$ ou 5^3.

(i) Le sous-cas $\det(M_1,\beta_1)=\det(M_2,\beta_2)=5$

Les facteurs invariants de M_1 dans $M_1^{\#}$ sont alors $(\mathbb{Z}[\zeta_{10}],\mathbb{Z}[\zeta_{10}],\mathfrak{P}_{10})$. Dans ce cas, la matrice $\overline{T_1}=(-1)$, et ainsi $|\mathscr{L}_{(M_1,M_1)}|=2$ (cf. lemme 4.2.6). Puisque $10\cdot\mathscr{D}_{10}^{-1}=2\cdot\mathfrak{P}_{10}$, on peut considérer que les facteurs invariants de M_1 dans $(M_1)_{h_1}^{\#}$ sont $(\mathfrak{P}_{10},\mathfrak{P}_{10},\mathfrak{P}_{10}^2)$ (cf. lemme 4.1.2 et lemme 2.1.5).

D'autre part, le facteur invariant de M_2 dans $M_2^{\#}$ est $\mathfrak{P}_{50}$ (cf. théorème 1.4.1). Puisque $50\cdot\mathscr{D}_{50}^{-1}=2\cdot\mathfrak{P}_{50}^5$ et que $2\cdot\mathfrak{P}_{50}^6$ est engendré par un élément de $\mathbb{Z}[\zeta_{50}+\overline{\zeta_{50}}]$, on peut considérer que $M_2=(M_2)_{h_2}^{\#}$. Ainsi, dans ce cas,

$$\begin{aligned}\mathscr{L}_{(M_1,M_2)}\cdot\omega(M_1)\cdot\omega(M_2) &= 2\cdot\texttt{oomega([1,1,2],5,1)}\cdot\texttt{oomega([0],5,2)}\\ &\leq 2,2\cdot 10^{-5}\end{aligned}$$

(ii) Le sous-cas $\det(M_1,\beta_1)=\det(M_2,\beta_2)=5^3$

Les facteurs invariants de M_1 dans $M_1^{\#}$ sont $(\mathbb{Z}[\zeta_{10}],\mathbb{Z}[\zeta_{10}],\mathfrak{P}_{10}^3)$. Dans ce cas, la matrice

$$\overline{T_1}=\begin{pmatrix}0&0&-1\\1&0&-3\\0&1&-3\end{pmatrix}\quad\text{(cf. lemme 4.2.6).}$$

Puisque ${}^{\mathrm{tr}}\overline{T_1}\,\overline{B_1}\,\overline{T_1}=\overline{B_1}$, on trouve que

$$\overline{B_1}=\begin{pmatrix}x&y&y-3x\\y&x&y\\y-3x&y&x\end{pmatrix},\ \text{avec } x,y\in\mathbb{F}_5.$$

Après calculs on trouve $|\mathscr{L}_{(M_1,M_2)}| = |\{X \in M_3(\mathbb{F}_5) \mid X\overline{T_1} = \overline{T_1}X \text{ et } X^{\mathrm{tr}}\overline{B_1}X = \overline{B_1}\}| = 10$.

On peut supposer que les facteurs invariants de M_1 dans $(M_1)^{\#}_{h_1}$ sont $(\mathfrak{P}_{10}, \mathfrak{P}_{10}, \mathfrak{P}_{10}^4)$, et que $M_2 = (M_2)^{\#}_{h_2}$. D'où,

$$\begin{aligned}|\mathscr{L}_{(M_1,M_2)}| \cdot \omega(M_1) \cdot \omega(M_2) &= 10 \cdot \texttt{oomega([1,1,4],5,1)} \cdot \texttt{oomega([0],5,2)} \\ &\leq 2,7 \cdot 10^{-3}.\end{aligned}$$

De ces deux sous-cas et du théorème 1.6.8, on a le

Théorème 4.3.11

$$\sum_{\overline{M} \in \overline{\mathscr{E}}(\Phi_{10}^3 \Phi_{50})} \frac{1}{|O(M)|} \leq 2,73 \cdot 10^{-3}.$$

❄

ANNEXE 1

Une équivalence de catégorie

Définition A1.1

Soit $f = \Phi_{n_1}\Phi_{n_2}$.

On considère la catégorie $\mathscr{A}_f$ *dont les objets sont des triplets* (M, β, t) *où* t *est une isométrie de polynôme minimal* f *du réseau unimodulaire* (M, β). *Soient* (M, β, t) *et* (M', β', t') *des objets de* $\mathscr{A}_f$. *Les morphismes de* $\mathscr{A}_f$ *sont les isométries* $\varphi : M \longrightarrow M'$ *telles que le carré suivant commute :*

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & M' \\ {\scriptstyle t}\downarrow & & \downarrow{\scriptstyle t'} \\ M & \xrightarrow{\varphi} & M' \end{array}$$

On considère la catégorie $\mathscr{B}_f$ *dont les objets sont des 5-uplets* $(M_1, M_2, h_1, h_2, \alpha)$ *satisfaisant les propriétés suivantes :*

a) Pour $i = 1, 2$, (M_i, h_i) *est un* $\mathbb{Z}[\zeta_{n_i}]$*-module projectif, hermitien, totalement défini positif.*

b) Pour $i = 1, 2$, *la forme* $\beta_i(x, y) := \frac{1}{n_i} \mathrm{Tr}_{\mathbb{Q}(\zeta_{n_i})/\mathbb{Q}} \circ h_i$ *est à valeur dans* $\mathbb{Z}$.

c) Pour $i = 1, 2$, *la multiplication par* ζ_{n_i} *se note* t_i. *Il est clair que* t_i *est une* $\mathbb{Z}$*-isométrie de* (M_i, β_i). *Elle se prolonge naturellement sur* $W_i := M_i \otimes \mathbb{Q}$. *Dans* W_i, *on définit* $M_i^{\#} = (M_i)_{\beta_i}^{\#}$. *On suppose que* α *est une anti-isométrie de* $M_1^{\#}/M_1$ *sur* $M_2^{\#}/M_2$ *telle que* $\overline{t_2} \circ \alpha = \alpha \circ \overline{t_1}$, *où, pour* $i = 1, 2$, $\overline{t_i}$ *est l'automorphisme de* $M_i^{\#}/M_i$ *induit par* t_i.

Soient $(M_1, M_2, h_1, h_2, \alpha)$ *et* $(M_1', M_2', h_1', h_2', \alpha')$ *des objets de* $\mathscr{B}_f$. *Les morphismes de* $\mathscr{B}_f$ *sont les couples* (φ_1, φ_2) *tels que, pour* $i = 1, 2$, φ_i *est une isométrie de* (M_i, h_i) *sur* (M_i', h_i'). *On remarque que, pour* $i = 1, 2$, φ_i *est aussi une isométrie de* (M_i, β_i) *sur* (M_i', β_i'). *On suppose que le carré suivant commute :*

$$\begin{array}{ccc} M_1^{\#}/M_1 & \xrightarrow{\alpha} & M_2^{\#}/M_2 \\ {\scriptstyle \overline{\varphi_1}}\downarrow & & \downarrow{\scriptstyle \overline{\varphi_2}} \\ M_1'^{\#}/M_1' & \xrightarrow{\alpha'} & M_2'^{\#}/M_2'. \end{array}$$

Proposition A1.2

Les catégories $\mathscr{A}_f$ et $\mathscr{B}_f$ sont équivalentes.

Démonstration :

Nous allons définir un foncteur de $\mathscr{A}_f$ sur $\mathscr{B}_f$. Soit (M, β, t) un objet de $\mathscr{A}_f$. Posons $W = M \otimes \mathbb{Q}$, $W_i = \frac{f}{\Phi_{n_i}}(t)(W)$, $h_i = \sum_{j=0}^{n_i-1} \beta_i(t_i^{-j}(x), y)\, \zeta_{n_i}^j$, $M_i = M \cap W_i$, p_i la projection de W sur W_i, pour $i = 1, 2$. Enfin, on pose $\alpha = \overline{p_1} \circ \overline{p_2}^{-1}$, l'application définie à la proposition 1.3.5. Soit

$$\begin{aligned} F : \mathscr{A}_f &\longrightarrow \mathscr{B}_f \\ (M, \beta, t) &\longmapsto (M_1, M_2, h_1, h_2, \alpha) \end{aligned}$$

La proposition 1.3.5 et le corollaire 1.2.7 montrent que $(M_1, M_2, h_1, h_2, \alpha)$ est un objet de $\mathscr{B}_f$.

Soient (M, β, t), (M', β', t') des objets de $\mathscr{A}_f$ et $\varphi \in \mathrm{Mor}_{\mathscr{A}_f}((M, \beta, t), (M', \beta', t'))$. Les applications t, t' et φ s'étendent naturellement sur W et W'. On a pour $i = 1, 2$:

$$\varphi(W_i) = \varphi(\Phi_{n_i}(t)(W)) = \Phi_{n_i}(t')(\varphi(W)) = \Phi_{n_i}(t')(W') = W_i'.$$

Ainsi, $\varphi(M_i) = \varphi(M \cap W_i) = \varphi(M) \cap \varphi(W_i) = M' \cap W_i' = M_i'$. On pose alors :

$$F(\varphi) = (\varphi|_{M_1}, \varphi|_{M_2}) := (\varphi_1, \varphi_2).$$

On vérifie aisément que $(\varphi_1, \varphi_2) \in \mathrm{Mor}_{\mathscr{B}_f}(F(M,\beta,t), F(M',\beta',t'))$, et que $F(\varphi \circ \varphi') = F(\varphi) \circ F(\varphi')$. Il s'agit de montrer que F est dense et pleinement fidèle pour achever la démonstration de la proposition.

Montrons que F est dense, c'est-à-dire que c'est une sujection au niveau des objets :

Soit $B = (M_1, M_2, h_1, h_2, \alpha)$ un objet de $\mathscr{B}_f$. Posons $W_1 = M_1 \otimes \mathbb{Q}$, $W_2 = M_2 \otimes \mathbb{Q}$, $W = W_1 \boxplus W_2$, et $\beta := \beta_1 + \beta_2$. Définissons

$$M = \{x_1 + x_2 \in M_1^{\#} \boxplus M_2^{\#} \mid x_2 + M_2 = \alpha(x_1 + M_1)\} \quad \text{et } t = t_1 \oplus t_2.$$

Le fait que (M,β,t) est un objet de $\mathscr{A}_f$ a été démontré au théorème 4.2.3. Il reste à voir que $F(M,\beta,t) = (M_1, M_2, h_1, h_2, \alpha)$. Pour $i = 1,2$, on a $M_i = M \cap W_i$ par définition de M et de W_i. D'autre part,

$$\sum_{l=0}^{n_i-1} \beta_i(t^{-l}(x), y)\zeta_{n_i}^l = h_i(x,y) \text{ pour tout } x, y \in W_i.$$

En effet, soient $\sigma_0, \ldots, \sigma_{\varphi(n_i)-1}$ les plongements de $\mathbb{Q}(\zeta_{n_i})$ dans $\mathbb{C}$. On a :

$$\begin{aligned}
\sum_{l=0}^{n_i-1} \beta_i(t^{-l}(x), y)\zeta_{n_i}^l &= \frac{1}{n_i} \sum_{l=0}^{n_i-1} \mathrm{Tr}(h_i(t^{-l}(x), y))\zeta_{n_i}^l \\
&= \frac{1}{n_i} \sum_{l=0}^{n_i-1} \mathrm{Tr}(\zeta_{n_i}^{-l} h_i(x,y))\zeta_{n_i}^l \\
&= \frac{1}{n_i} \sum_{l=0}^{n_i-1} \sum_{j=0}^{\varphi(n_i)-1} \sigma_j(\zeta_{n_i}^{-l} h_i(x,y))\zeta_{n_i}^l \\
&= \frac{1}{n_i} \sum_{j=0}^{\varphi(n_i)-1} \sigma_j(h_i(x,y)) \cdot \sum_{l=0}^{n_i-1} \sigma_j(\zeta_{n_i}^{-l})\zeta_{n_i}^l \\
&= h_i(x,y).
\end{aligned}$$

La dernière égalité vient du fait que $\sum_{l=0}^{n_i-1} \sigma_j(\zeta_{n_i}^{-l})\zeta_{n_i}^l = 0$ sauf quand σ_j est l'identité, et dans ce cas là, cette somme vaut n_i. Posons p_i la projection orthogonale de W sur W_i, $i = 1,2$. On voit facilement que $p_i(M) = M_i^{\#}$, ainsi, on trouve deux isomorphismes :

$$M_1^{\#}/M_1 \xrightarrow{\overline{p_1}} M/M_1 \boxplus M_2 \xrightarrow{\overline{p_2}^{-1}} M_1^{\#}/M_1,$$

donc,

$$M = \{x_1 + x_2 \in M_1^{\#} \boxplus M_2^{\#} \mid (\overline{p_2}^{-1} \circ \overline{p_1})(x_1 + M_1) = x_2 + M_2\}.$$

On en déduit que $\overline{p_2}^{-1} \circ \overline{p_1} = \alpha$, et donc que F est dense.

Montrons que F est pleinement fidèle, c'est-à-dire pour tout objets $(M,\beta,t), (M',\beta',t')$ de $\mathscr{A}_f$, l'application

$$\begin{aligned}
\mathrm{Mor}_{\mathscr{A}_f}((M,\beta,t),(M',\beta',t')) &\longrightarrow \mathrm{Mor}_{\mathscr{B}_f}(F(M,\beta,t), F(M',\beta',t')) \\
\varphi &\longmapsto F(\varphi) = (\varphi_1, \varphi_2)
\end{aligned}$$

est un isomorphisme. Soient donc, φ et $\varphi' \in \mathrm{Mor}_{\mathscr{A}_f}((M,\beta,t),(M',\beta',t'))$ tels que $F(\varphi) = F(\varphi')$. On a donc $\varphi|_{M_1 \boxplus M_2} = \varphi'|_{M_1 \boxplus M_2}$, ainsi, $\varphi = \varphi'$, car $M_1 \boxplus M_2$ contient une base de W. Finalement, soit

$(\varphi_1, \varphi_2) \in \mathrm{Mor}_{\mathscr{B}_f}(F(M,\beta,t), F(M',\beta',t'))$. Posons $\varphi := \varphi_1 + \varphi_2$. Il suffit de montrer que $\varphi(M) = M'$. On voit facilement que $\varphi(M_1 \boxplus M_2) = M_1' \boxplus M_2'$ et que $\varphi(M_1^{\#} \boxplus M_2^{\#}) = M_1'^{\#} \boxplus M_2'^{\#}$. Il faut voir que l'image de

$$\overline{\varphi} : M/(M_1 \boxplus M_2) \longrightarrow (M_1'^{\#} \boxplus M_2'^{\#})/(M_1 \boxplus M_2)$$
$$(x_1 + M_1) + (x_2 + M_2) \longmapsto (\varphi_1(x_1) + M_1) + (\varphi_2(x_2) + M_2)$$

est $M'/(M_1' \boxplus M_2')$. Cela vient de

$$\begin{aligned}(\varphi_1(x_1) + M_1) + (\varphi_2(x_2) + M_2) &= (\varphi_1(x_1) + M_1) + (\overline{\varphi_2}(x_2 + M_2)) \\ &= (\varphi_1(x_1) + M_1) + \overline{\varphi_2}(\alpha(x_1 + M_1)) \\ &= (\varphi_1(x_1) + M_1) + \alpha'(\overline{\varphi_1}(x_1 + M_1)) \in M'/(M_1' \boxplus M_2').\end{aligned}$$

Ainsi, F est pleinement fidèle et $\mathscr{A}_f$ est équivalente à $\mathscr{B}_f$. ❋

ANNEXE 2

Voici le *listing* de la fonction oomega :

```
{ppsi(n)=
v1=sort(vector(n,j,if(gcd(j,n)==1,j,0)));
v2=vector(phi(n),j,v1[n-phi(n)+j]);
prod(1,j=1,phi(n)/2,mod(y-(x^(v2[j])+x^(-(v2[j])))),cyclo(n)));}
{beeta(p,k,r)=2^((phi(p^k)-2)/2)*pi^(phi(p^k)/2)*p^(-(k+(1/2)))*
disc(subst(compo(ppsi(p^k),2),y,x))^(-1/2)*
prod(1,j=2,r,(1-p^(-j))*zeta(j))^(phi(p^k)/2);}
{valdif(fil)=matrix(length(set(fil)),2,j,s,if(s==1,set(fil)[j],sum(0,l=1,length(fil),
if(fil[l]==set(fil)[j],1,0)))))}
{densinv01mod(k,p,r)=if(k==0,if(mod(r,2)==mod(0,2),
(2*(1-p^(-r/2))*prod(1,s=1,(r-2)/2,(1-p^(-2*s))))^(-1),
(2*prod(1,s=1,(r-1)/2,(1-p^(-2*s))))^(-1)),
(p^(r*(r+1)/2)*prod(1,s=1,r/2,(1-p^(-2*s))))^(-1))}
{densinv12mod(p,r,ro)=if(mod(ro,2)==mod(0,2),
((2*p^((r-ro)*(r-ro+1)/2)*prod(1,s=1,ro/2,(1-p^(-2*s)))*
prod(1,s=1,(r-ro)/2,(1-p^(-2*s))))/(1+p^(-ro/2)))^(-1),
(2*p^((r-ro)*(r-ro+1)/2)*prod(1,s=1,(ro-1)/2,(1-p^(-2*s)))*
prod(1,s=1,(r-ro)/2,(1-p^(-2*s))))^(-1))}
{mdensinvloc(fi,p)=
if(length(valdif(fi)~)==1,
   densinv01mod(valdif(fi)[1,1],p,valdif(fi)[1,2])
   ,
   if(length(valdif(fi)~)==2,
      if(valdif(fi)[1,1]==0&valdif(fi)[2,1]==1,
       densinv12mod(p,valdif(fi)[1,2]+valdif(fi)[2,2],valdif(fi)[2,2])
        ,
        p^(-valdif(fi)[1,1]*valdif(fi)[1,2]*valdif(fi)[2,2]-
        divres(valdif(fi)[2,1],2)[1]*valdif(fi)[2,2]^2)*
        densinv01mod(divres(valdif(fi)[2,1],2)[2],p,valdif(fi)[2,2])*
        densinv01mod(valdif(fi)[1,1],p,valdif(fi)[1,2])
       )
      ,
      if(valdif(fi)[1,1]==0&valdif(fi)[2,1]==1,
      mdensinvloc(vector(valdif(fi)[2,2],j,valdif(fi)[2,1]),p)^(-1)*
      mdensinvloc(vector(valdif(fi)[1,2]+valdif(fi)[2,2],j,fi[j]),p)*
      mdensinvloc(vector(sum(0,j=1,length(valdif(fi)~)-1,
               valdif(fi)[j+1,2]),l,fi[l+valdif(fi)[1,2]]),p)
        ,
        p^(-divres(valdif(fi)[2,1],2)[1]*(length(fi)-valdif(fi)[1,2])^2-
        valdif(fi)[1,1]*valdif(fi)[1,2]*(length(fi)-valdif(fi)[1,2]))*
        mdensinvloc(vector(valdif(fi)[1,2],j,valdif(fi)[1,1]),p)*
        mdensinvloc(vector(sum(0,j=1,length(valdif(fi)~)-1,
        valdif(fi)[j+1,2]),l,fi[l+valdif(fi)[1,2]]-2*divres(valdif(fi)[2,1],2)[1]),p)
      )
   )
))}
{oomega(fii,p,k)=
abs(2*(disc(cyclo(p^k))/disc(subst(compo(ppsi(p^k),2),y,x))^2)^(length(fii)*(length(fii)+1)/4)*
(prod(1,j=1,length(fii),(j-1)!/((2*pi)^j)))^(phi(p^k)/2)*
disc(subst(compo(ppsi(p^k),2),y,x))^((length(fii)^2)/2)*
p^(sum(0,j=1,length(fii),fii[j])*length(fii)/2)*
mdensinvloc(fii,p)*beeta(p,k,length(fii)))}
```

Description de ce programme :

a) La sous-fonction "`ppsi`" donne le polynôme minimal de $\zeta_n + \overline{\zeta_n}$. Il suffit d'entrer "`ppsi(n)`" pour obtenir ce polynôme.

b) La sous-fonction "`beeta`" donne une estimation du produit de presque toutes les densités locale, c'est-à-dire celles pour lesquelles la forme est unimodulaire (cf. théorème 2.3.1). Ici, il faut que la seule place pour laquelle cette forme n'est pas unimodulaire soit l'unique idéal $\mathfrak{p}_0$ qui se ramifie entre $\mathbb{Q}(\zeta_{p^k} + \overline{\zeta_{p^k}})$ et $\mathbb{Q}(\zeta_{p^k})$. Il suffit d'entrer "`beeta(p,k,r)`" si r est le rang du module hermitien pour obtenir cette estimation.

c) La sous-fonction "mdensinvloc" donne l'inverse de la densité locale en $\mathfrak{p}_0$. Il suffit d'entrer "`mdensinvloc([m1,...,mr],p)`" si les facteurs invariants du module dans son dual sont $\mathfrak{P}_0^{m_1} \supset \cdots \supset \mathfrak{P}_0^{m_r}$, avec $m_1 = 0$ ou 1, et $\mathfrak{P}_0$ est l'unique idéal de $\mathbb{Z}[\zeta_{p^k}]$ au-dessus de p.

d) Supposons que (M, h) soit un $\mathbb{Z}[\zeta_n]$-module hermitien totalement défini positif, que $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{p^k})$, avec $p \in \mathbb{P} - \{2\}$, et que les facteurs invariants de M dans $M_h^\#$ soient $\mathfrak{P}_0^{m_1} \supset \cdots \supset \mathfrak{P}_0^{m_r}$, avec $m_1 = 0$ ou 1, et où $\mathfrak{P}_0$ est l'unique idéal au-dessus de p. Alors, pour obtenir $\omega(M)$, il suffit d'entrer "`oomega([m1,...,mr],p,k)`".

ANNEXE 3

Liste complète des $\mathbb{Z}$-réseaux 3-élémentaires, de type II, et de dimension 8

Nous savons que si (M, β) est 3-élémentaire, de type II, et de dimension 8, alors $M^{\#}/M \simeq \mathbb{F}_p^k$, avec $k = 0, 2, 4, 6$ ou 8 (cf. lemme 4.3.1). Le lemme suivant nous montre qu'il suffira de considérer les cas où $k = 0, 2$ ou 4. Tout d'abord une définition.

Définition A3.1

Soit (M, β) un $\mathbb{Z}$-réseau de rang n tel que $M^{\#}/M = \mathbb{F}_3^k$, avec $0 \leq k \leq n$, et $p \in \mathbb{P}$. On définit ${}^pM$ comme étant le réseau $\sqrt{p} \cdot M^{\#}$.

Lemme A3.2

Soit $p \in \mathbb{P}$. L'application $M \longmapsto {}^pM$ est un bijection de l'ensemble des $\mathbb{Z}$-réseaux, p-élémentaires, de déterminant p^k et de rang n sur l'ensemble des $\mathbb{Z}$-réseaux, p-élémentaires, de déterminant p^{n-k} et de rang n.

Démonstration :

Montrons d'abord que $\beta({}^pM, {}^pM) \subset \mathbb{Z}$:

$$\begin{aligned} \beta({}^pM, {}^pM) &= \beta(\sqrt{p} \cdot M^{\#}, \sqrt{p} \cdot M^{\#}) \\ &= \beta(p \cdot M^{\#}, M^{\#}) \\ &\subset \beta(M, M^{\#}) \subset \mathbb{Z} \end{aligned}$$

D'autre part, $\det(\sqrt{p} \cdot M^{\#}) = p^n \det(M^{\#}) = p^{n-k}$.

On a aussi, $p \cdot {}^pM^{\#} \subset {}^pM$:

$$\begin{aligned} \text{on a} \quad & {}^pM^{\#} = (\sqrt{p} \cdot M^{\#})^{\#} = \frac{1}{\sqrt{p}} \cdot M^{\#\#} = \frac{1}{\sqrt{p}} \cdot M, \\ \text{donc} \quad & p \cdot {}^pM^{\#} = \frac{p}{\sqrt{p}} \cdot M = \sqrt{p} \cdot M \subset \sqrt{p} \cdot M^{\#} = {}^pM \end{aligned}$$

Finalement, ${}^p({}^pM) = M$:

$${}^p({}^pM) = {}^p(\sqrt{p} \cdot M^{\#}) = \sqrt{p} \cdot (\sqrt{p} \cdot M^{\#})^{\#} = \frac{\sqrt{p}}{\sqrt{p}} \cdot M^{\#\#} = M$$

Lemme A3.3

Soit $p \in \mathbb{P} - \{2\}$. L'ensemble des $\mathbb{Z}$-réseaux , p-élémentaires, de type II, de rang n, et de déterminant p^k, avec k satisfaisant la congruence

$$n \equiv \pm 2 - 2 - (p-1)k \pmod 8$$

forme un unique genre que l'on notera $\mathscr{G}_{II,3^k}$.

Démonstration :

Cf. ([Co-Slo], theorem 13, p. 386) ❄

Voici une méthode générale pour calculer la matrice de $\overline{\beta}$ connaissant celle de β.

Lemme A3.4

Soit (M,β) un $\mathbb{Z}$-réseau p-élémentaire. Soit B une matrice de β. Il est bien connu qu'il existe $A, B \in Gl_n(\mathbb{Z})$ telles que

$$A^{\mathrm{tr}}BC = \underbrace{(p)\oplus\cdots\oplus(p)}_{\text{k fois}}\oplus\underbrace{(1)\oplus\cdots\oplus(1)}_{\text{n-k fois}} \qquad \text{(cf. [Jacn], theorem 3.8, p. 176)}$$

La fonction "smith2" du programme PARI fait ce travail. Alors, si

$$A^{\mathrm{tr}}BA = \begin{pmatrix} \overbrace{X_1}^{k} & X_2 \\ X_3 & X_4 \end{pmatrix}\begin{matrix}\}k\\ \}n-k\end{matrix},$$

on a $X_1 \in M_k(p\mathbb{Z})$, et $\frac{1}{p}\cdot X_1$ fournit une matrice de $\overline{\beta}$.

Démonstration :

Si $e_1,\ldots,e_n$ sont les vecteurs colonnes de A, alors on voit facilement que $M = \mathbb{Z}e_1\oplus\cdots\oplus\mathbb{Z}e_n$ et que $M^{\#} = \mathbb{Z}\frac{1}{p}e_1\oplus\cdots\oplus\mathbb{Z}\frac{1}{p}e_k\oplus\mathbb{Z}e_{k+1}\oplus\cdots\oplus\mathbb{Z}e_n$. Ainsi, la matrice de $\overline{\beta}$ relativement à la base $(\overline{\frac{1}{p}e_1},\ldots,\overline{\frac{1}{p}e_k})$ de $M^{\#}/M$ vaut $\frac{1}{p}\cdot X_1$ via la bijection canonique entre $\frac{1}{p}\mathbb{Z}/\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z}$. ❄

(A) Le cas $\det(M,\beta) = 1$

Dans ce cas, il est bien connu que $|\mathscr{G}_{II,3^0}| = 1$. Cette unique classe se note usuellement E_8, et la masse de ce genre vaut

$$\frac{1}{|O(E_8)|} = \frac{1}{2^{14}\cdot 3^5\cdot 5^2\cdot 7} \qquad \text{(cf. [Co-Slo], p. 121).}$$

(B) Le cas $\det(M,\beta) = 3^8$

Le lemme A3.2 nous montre que $\mathscr{G}_{II,3^8} = \{{}^3E_8\}$. Dans ce cas, la matrice de $\overline{\beta}$ est simplement n'importe quelle matrice de E_8 modulo 3, car si $(e_1,\ldots,e_8)$ est une base quelconque de ${}^3E_8$, alors $(\frac{1}{3}e_1,\ldots,\frac{1}{3}e_8)$ est une base de ${}^3E_8^{\#}$.

(C) Le cas $\det(M,\beta) = 3^2$

Ici, nous avons besoin d'un autre programme informatique. Il se nomme "tn". L'utilisation de ce programme est très simple : il suffit d'entrer une matrice symétrique et définie positive, puis une routine va chercher toutes les matrices du même genre que la matrice de départ au moyen de la méthode des "voisins de Kneser". Enfin, le programme vérifie que la liste est complète au moyen de la "formule de Siegel". Ce programme m'a été donné par R. Scharlau et B. Hemkemeier.

On trouve alors que $\mathscr{G}_{II,3^2} = \{A_2 \boxplus E_6\}$, où A_2 peut être représenté par la matrice $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ ou $\begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$, et E_6 peut être représenté par la matrice $\begin{pmatrix} 2 & 0 & -1 & 0 & 0 & 0 \\ 0 & 2 & 0 & -1 & 0 & 0 \\ -1 & 0 & 2 & -1 & 0 & 0 \\ 0 & -1 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & -1 & 2 \end{pmatrix}$.

En utilisant les méthodes données au lemme A3.4, on trouve $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ comme matrice pour $\overline{\beta}$.

(D) Le cas $\det(M, \beta) = 3^6$

Le lemme A3.2 nous donne que $\mathscr{G}_{II,3^6} = \{{}^3A_2 \boxplus {}^3E_6\}$. Or, il est évident que ${}^3A_2 = A_2$. On calcule ${}^3E_6$, et on trouve $\begin{pmatrix} 4 & 3 & 0 & 0 & 0 & 0 \\ 3 & 6 & 6 & 0 & 0 & 0 \\ 0 & 6 & 12 & -3 & 0 & 0 \\ 0 & 0 & -3 & 6 & -3 & 0 \\ 0 & 0 & 0 & -3 & 6 & -3 \\ 0 & 0 & 0 & 0 & -3 & 6 \end{pmatrix}$.

Ainsi, dans ce cas, la matrice $\overline{\beta}$ vaut $\begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & -1 & -1 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 1 & 0 & -1 \\ 0 & -1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & -1 & -1 & 0 \end{pmatrix}$. Son déterminant vaut -1.

(E) Le cas $\det(M, \beta) = 3^4$

Au moyen du programme "tn", nous trouvons que $\mathscr{G}_{II,3^4} = \{A_2 \boxplus A_2 \boxplus A_2 \boxplus A_2, \Lambda\}$ où Λ peut être représenté par la matrice $\begin{pmatrix} 2 & 1 & 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & 2 & 0 & 0 & 1 & -1 & 0 & -1 \\ 1 & 0 & 2 & 0 & 1 & 0 & -1 & 0 \\ 1 & 0 & 0 & 2 & 0 & 0 & 0 & -1 \\ 1 & 1 & 1 & 0 & 4 & -2 & -2 & 1 \\ -1 & -1 & 0 & 0 & -2 & 4 & 2 & -1 \\ -1 & 0 & -1 & 0 & -2 & 2 & 4 & 0 \\ -1 & -1 & 0 & -1 & 1 & -1 & 0 & 4 \end{pmatrix}$

Dans le cas $A_2 \boxplus A_2 \boxplus A_2 \boxplus A_2$, la matrice de $\overline{\beta}$ vaut $-I_4$, et dans le cas Λ, la matrice de $\overline{\beta}$ vaut $\begin{pmatrix} -1 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 \\ -1 & 1 & 0 & -1 \\ 0 & 0 & -1 & 1 \end{pmatrix}$. Dans les deux cas, le déterminant de $(M^{\#}/M, \overline{\beta})$ est 1.

ANNEXE 4

Réalisation explicites pour certains polynômes

Nous utilisons dans cette annexe les résultats obtenus dans [Ker1] et [Ker2].

Etudions le problème dans les dimensions inférieure à 32 pour les $\mathbb{Z}$-réseaux unimodulaires de type II :

Si $n = 8$, nous savons qu'il n'y a que E_8. Ainsi, E_8 est un F-réseau où est F est dans la liste suivante :

$$\Phi_6^4 \quad \Phi_{10}^2 \quad \Phi_{12}^2 \quad \Phi_{15} \quad \Phi_{20} \quad \Phi_{24} \quad \Phi_{30} \quad \Phi_6\Phi_{18} \quad \Phi_6^2\Phi_{12} \quad \text{(cf. théorème 3.1.4)}.$$

Si $n = 16$, il existe 2 classes : $E_8 \boxplus E_8$ et le réseau associé au système de racines D_{16}. Or, ce dernier réseau ne possède pas d'isométrie parfaite (cf. [Ker1], corollaire p.180). Notons tout de même que $E_8 \boxplus E_8$ est un F-réseau pour les polynômes suivants :

$$\Phi_{40} \quad \Phi_{48} \quad \Phi_{60} \quad \Phi_{12}\Phi_{36},$$

et que ces derniers ne proviennent pas de la somme directe de deux isométries de E_8.

Si $n = 24$, il est bien connu que, excepté Λ le réseau de Leech, tous les $\mathbb{Z}$-réseaux possèdent un système complet de racines. On les nomme donc souvent par la donnée de ce système. Les réseaux suivants sont les seuls à posséder une isométrie parfaite :

$$A_{24} \quad 2A_{12} \quad 3A_8 \quad 4A_6 \quad 12A_2 \quad 6D_4 \quad 4E_6 \quad 3E_8 \quad \text{et } \Lambda \qquad \text{(cf. [Ker1], p. 181)}.$$

L'article [Ker1] nous donne des moyens explicite pour calculer des isométries parfaites. Nous trouvons alors que

A_{24} est un $\Phi_{10}\Phi_{50}$-réseau,	$2A_{12}$ est un Φ_{26}^2-réseau,	$3A_8$ est un $\Phi_6^3\Phi_{18}^3$-réseau,
$4A_6$ est un Φ_{14}^4-réseau,	$12A_2$ est un Φ_6^{12}-réseau,	$6D_4$ est un Φ_6^{12}-réseau,
$4E_6$ est un Φ_6^{12}-réseau,	$3E_8$ est un Φ_6^{12}-réseau,	Λ est un Φ_6^{12}-réseau.

Si $n = 32$, il y a 132 réseaux indécomposables possédant un système complet de racines (cf. [Ker2]). Voici un lemme permettant de trouver, parmi ces 132 réseaux, ceux qui possèdent une isométrie parfaite :

Lemme A4.1

Soient (M, β) un $\mathbb{Z}$-réseau unimodulaire de rang n, et $R = \{x \in M \mid \beta(x,x) = 2\}$ l'ensemble des vecteurs de longueur 2.

a) Si R se décompose en $A_{2k-1} \boxplus R'$, $D_{4+k} \boxplus R'$ ou $E_7 \boxplus R'$, avec $k \leq 1$, alors (M, β) ne possède pas d'isométrie parfaite.

b) Si R se décompose en $\boxplus_{i=1}^{p} A_{2k_i} \boxplus qE_6 \boxplus rE_8$, avec $p, q, r \geq 0$ et $n = \sum_{i=1}^{p} 2k_i + 6q + 8r$, alors (M, β) possède une isométrie parfaite

Démonstration :

Cf. ([Ker1], propositions 3 et 4). ❄

Grâce à ce lemme, et aux données explicites de [Ker2], nous obtenons les résultats suivants :

$4A_2 \boxplus 4E_6$ est un Φ_6^{16}-réseau,	$10A_2 \boxplus 2E_6$ est un Φ_6^{16}-réseau,	$13A_2 \boxplus E_6$ est un Φ_6^{16}-réseau,
$A_2 \boxplus 3A_8 \boxplus E_6$ est un $\Phi_6^7\Phi_{18}^3$-réseau,	$A_6 \boxplus A_{20} \boxplus E_6$ est un $\Phi_6^4\Phi_{14}^2\Phi_{42}$-réseau,	$A_{26} \boxplus E_6$ est un $\Phi_6^4\Phi_{18}\Phi_{54}$-réseau,
$16A_2$ est un Φ_6^{16}-réseau,	$2A_2 \boxplus 2A_{14}$ est un $\Phi_6^4\Phi_{10}^2\Phi_{30}^2$-réseau,	$8A_4$ est un Φ_{10}^8-réseau,
$4A_8$ est un $\Phi_6^4\Phi_{18}^4$-réseau,	$2A_{16}$ est un Φ_{34}^2-réseau.	

Voici quelques exemples de résultats matriciels : Il existe une base du réseau $2A_{16}$ dont la matrice de β est

$$\overbrace{\begin{pmatrix} 2 & 1 & \cdots & 1 & 0 & 0 & \cdots & 0 & 13 \\ 1 & \ddots & \ddots & \vdots & 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 1 & \vdots & \ddots & \ddots & 0 & \vdots \\ 1 & \cdots & 1 & 2 & 0 & \cdots & 0 & 0 & 13 \\ \hline 0 & 0 & \cdots & 0 & 2 & 1 & \cdots & 1 & 1 \\ 0 & \ddots & \ddots & \vdots & 1 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & \ddots & \ddots & 1 & \vdots \\ 0 & \cdots & 0 & 0 & 1 & \cdots & 1 & 2 & 1 \\ \hline 13 & \cdots & \cdots & 13 & 1 & \cdots & \cdots & 1 & 160 \end{pmatrix}}^{16}$$

Relativement à la même base, la matrice de l'isométrie parfaite trouvée est

$$\overbrace{\begin{pmatrix} 1 & \cdots & \cdots & 1 & 1 & 0 & \cdots & \cdots & 0 & 13 & 13 \\ \hline -1 & 0 & \cdots & 0 & 0 & 0 & \cdots & \cdots & 0 & 13 & 0 \\ 0 & \ddots & \ddots & \vdots & \vdots & 0 & \cdots & \cdots & 0 & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & -1 & 0 & 0 & \cdots & \cdots & 0 & 13 & 0 \\ \hline 0 & \cdots & \cdots & 0 & 0 & 1 & \cdots & \cdots & 1 & 2 & 1 \\ \hline 0 & \cdots & \cdots & 0 & 0 & -1 & 0 & \cdots & 0 & 1 & 0 \\ 0 & \cdots & \cdots & 0 & \vdots & 0 & \ddots & \ddots & \vdots & \vdots & \vdots \\ \vdots & \ddots & \ddots & \vdots & \vdots & \vdots & \ddots & \ddots & 0 & \vdots & \vdots \\ 0 & \cdots & \cdots & 0 & 0 & 0 & \cdots & 0 & -1 & 1 & 0 \\ \hline 0 & \cdots & \cdots & 0 & 0 & \underbrace{0 \quad \cdots \quad \cdots \quad 0}_{14} & & & & -17 & -1 \end{pmatrix}}^{15}$$

Comparons cet exemple avec le réseau $2A_{12}$: une matrice de β est

$$\overbrace{\begin{pmatrix} 2 & 1 & \cdots & 1 & 0 & 0 & \cdots & 0 & 8 \\ 1 & \ddots & \ddots & \vdots & 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 1 & \vdots & \ddots & \ddots & 0 & \vdots \\ 1 & \cdots & 1 & 2 & 0 & \cdots & 0 & 0 & 8 \\ \hline 0 & 0 & \cdots & 0 & 2 & 1 & \cdots & 1 & 1 \\ 0 & \ddots & \ddots & \vdots & 1 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & \ddots & \ddots & 1 & \vdots \\ 0 & \cdots & 0 & 0 & 1 & \cdots & 1 & 2 & 1 \\ \hline 8 & \cdots & \cdots & 8 & 1 & \cdots & \cdots & 1 & 60 \end{pmatrix}}^{12}$$

Relativement à la même base, la matrice de l'isométrie parfaite trouvée est

$$\overbrace{\begin{pmatrix} 1 & \cdots & \cdots & 1 & 1 & 0 & \cdots & \cdots & 0 & 8 & 8 \\ \hline -1 & 0 & \cdots & 0 & 0 & 0 & \cdots & \cdots & 0 & 8 & 0 \\ 0 & \ddots & \ddots & \vdots & \vdots & 0 & \cdots & \cdots & 0 & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & -1 & 0 & 0 & \cdots & \cdots & 0 & 8 & 0 \\ \hline 0 & \cdots & \cdots & 0 & 0 & 1 & \cdots & \cdots & 1 & 2 & 1 \\ \hline 0 & \cdots & \cdots & 0 & 0 & -1 & 0 & \cdots & 0 & 1 & 0 \\ 0 & \cdots & \cdots & 0 & \vdots & 0 & \ddots & \ddots & \vdots & \vdots & \vdots \\ \vdots & \ddots & \ddots & \vdots & \vdots & \vdots & \ddots & \ddots & 0 & \vdots & \vdots \\ 0 & \cdots & \cdots & 0 & 0 & 0 & \cdots & 0 & -1 & 1 & 0 \\ \hline 0 & \cdots & \cdots & 0 & 0 & \underbrace{0 \quad \cdots \quad \cdots \quad 0}_{10} & & & & -13 & -1 \end{pmatrix}}^{11}$$

Bibliographie

[Ban] : E. BANNAI, *Positive definite unimodular lattices with trivial automorphism groups*, Memoirs of the AMS, Number 429, (1990).

[Bay] : E. BAYER-FLUCKIGER, *Lattices with automorphisms of given characteristic polynomial*, à paraître.

[Bo] : S. BOGE, *Schiefhermitesche Formen über Zahlkörpern und Quaternionenschiefkörpern*, J. Reine Angew. Math 221 (1966), pp. 85–112.

[Br] : H. BRAUN, *Zur Theorie des hermiteschen Formen*, Abh. Math. Sem. Hamburg 14 (1941), pp. 61–150.

[Co] : P.E. CONNER *Note on the Witt Classification of Hermitian Innerproduct Spaces over a Ring of Algebraic Integers*, University of Texas Press, Austin and London (1979).

[Co-Slo] : J.H. CONWAY & N.J.A. SLOANE, *Sphere Packings, Lattices and Groups*, Springer-Verlag, Berlin, Heidelberg, New York (1988).

[Fr-Ta] : A. FROHLICH & M.J. TAYLOR, *Algebraic number theory*, Cambridge University Press, (1991).

[Ha] : K. HASHIMOTO, *Elliptic conjugacy classes of the Siegel modular group and unimodular hermitian forms over the ring of cyclotomic integers*, J. Fac, Sci. Univ. Tokyo Sect. IA, Math. 33 (1986), 57–82.

[Jac] : R. JACOBOWITZ, *Hermitian forms over local fields*, Am. J. Math. 84 (1962), pp. 441–465.

[Jacn] : N. JACOBSON, *Basic Algebra I*, W.H. Freeman and Comp., San Fransisco (1974).

[Ker1] : M. KERVAIRE, *Formes de Seifert et formes quadratiques entières*, l'Enseign. Math 31 (1985), pp. 173–186.

[Ker2] : M. KERVAIRE, *Unimodular lattices with a complete root system*, l'Enseign. Math 40 (1994), pp. 59–104.

[Land] : W. LANDHERR, *Äquivalenz Hermitescher Formen über einem beliebigen algebraischen Zahlkörper*, Abh. Math. Sem. Univ. Hamburg 11 (1935), pp. 245-248.

[Lang] : S. LANG, *Algebra*, Addison-Wesley Publishing Company (1969).

[Mar] : M. MARCUS, *Introduction to modern Algerbra*, M. Dekker INC, New-york, Basel (1978).

[Mis] : M. MISCHLER, *La formule de Minkowski-Siegel pour les formes symétriques, non dégénérées et définies positives*, Publ. Fac. Sci. Besançon, Univ. Franche-Comté, Besançon (1995).

[O'M] : O.T. O'MEARA, *Introduction to quadratic forms*, Springer-Verlag, Berlin, New-york (1963).

[Re] : U. REHMANN, *Klassenzahlen einiger totaldefiniter klassischer Gruppen über Zahlkörpern*, (Diss.), Göttingen (1971).

[Se] : J.-P. SERRE, *Cours d'arithmétique*, Collection SUP No.2, Presses Universitaires de France, Paris (1970).

[Shi] : G. SHIMURA, *Arithmetic of unitary groups*, Annals of Math. 79 (1964), pp. 369–409.

[Sto] : N. STOLZFUS, *Unraveling the integral knot concordance group*, Memoirs of the AMS 12, Number 192 (1977).