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* $i = 1,\ldots,s$, *et* $W = M\otimes\mathbb{Q}$.

Soit $i = 1,\ldots,s$. *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* $g = b_n \prod_{j1}^{n} (X - \beta_j)$ *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 :

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

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 $\overline{\check{t}_i} \circ \alpha_i = \alpha_i \circ \overline{t_i}$. En particulier, $\overline{t_i}$ est annulé par le polynôme minimal de $\check{t}_i$ 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 :

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

La partie f) du lemme 1.3.7 nous apprend que $|N_{\mathbb{Q}(\zeta_{n_i})/\mathbb{Q}}(\frac{f}{\Phi_{n_i}}(\zeta_{n_i}))| = |\operatorname{Res}(\Phi_{n_i}, \frac{f}{\Phi_{n_i}})|$, 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 :*

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

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

Par conséquent :

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

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 $\gamma_i = \dfrac{1}{n_i} \mathrm{Tr}_{\mathbb{Q}(\zeta_{n_i})/\mathbb{Q}} \circ k_i$. 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 $\not{\pi}$ dans $O_{K_\mathfrak{p}}$, et que $\not{\pi} O_{K_\mathfrak{p}} = \mathfrak{p}$. 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 $\not{\pi}^2 = \pi$ (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]. ❄