THÉORIE DES NOMBRES
BESANÇON

Années 1992/93-1993/94

La formule de Minkowski-Siegel pour les formes bilinéaires symétriques non dégénérées et définies positives

M. MISCHLER

La formule de Minkowski-Siegel pour les formes bilinéaires symétriques non dégénérées et définies positives

Maurice Mischler

Ce travail a été effectué en vue de
l'obtention du Diplôme de mathématicien
de l'Université de Lausanne,
sous la direction du Professeur
Jacques Boéchat

Introduction

Une étape importante de l'histoire des formes bilinéaires symétriques entières commence lorsque, vers 1859, Hermite démontre qu'il n'y a qu'un nombre fini de classes d'équivalence pour un déterminant et une dimension n donnés. Quand un objet mathématique possède un nombre fini d'éléments, il est naturel de se demander quel est ce nombre.

Nous allons nous intéresser aux formes non dégénérées sur $\mathbb{Z}$ et définies positives. Hermite lui-même démontra que si $1 \leq n \leq 7$, il n'y avait qu'une classe d'équivalence.

Mordell montre, en 1938, que si $n = 8$, il y a exactement deux classes.

En 1957, Kneser énumère toutes les formes jusqu'à 16 variables.

Il apparaît que si $n \equiv 0 \bmod 8$, il est possible de trouver de telles formes β telles que $\beta(x,x)$ soit pair pour tout x. Ces formes sont appelée "formes de type II" ou "paires", sinon, on dit qu'elles sont de "type I", ou "impaires".

Niemeier en 1968 donna la liste de toute les formes paires à 24 variables : il y en a exactement 24.

Conway et Sloane, en 1982, ont donné toutes les formes jusqu'à $n = 24$, puis avec Borcherds jusqu'à $n = 25$. Une liste de ces résultats est donnée dans ce travail au chapitre 5.

Mais alors, que vient faire la formule de Siegel dans tout cela ?

Imaginez que vous possédez une certaine quantité de classes de formes bilinéaires symétriques, définies positives, dans un type donné, et pour une dimension n donnée . Eh bien, la formule de Siegel permet de dire si oui ou non votre liste est complète.

Plus précisément, soit $M = M_1$ un $\mathbb{Z}$-module bilinéaire symétrique, défini positif et de dimension n. Soient $M_2, \ldots, M_k$ des représentants des classes d'équivalence dans le même type que M. Pour chacun de ces modules, on pose $O(M_i)$ le groupe orthogonal de M_i. Ce groupe est fini dans notre cas. La formule de Siegel nous donne alors pour tout n et pour tout type la somme

$$\sum_{i=1}^{k} \frac{1}{|O(M_i)|}.$$

Cette formule est donnée dans les cas qui nous intéressent dans [4, ch.16, thm. 1 et 2].

Or, les auteurs de cet ouvrages nous avertissent qu'un bon nombres d'articles concernant cette formule comportent des erreurs (notament [9] et [12]).

Le but de ce travail est donc de reprendre la théorie de Siegel, exposée par Kneser dans [7]. Cela est fait dans le chapitre 2, alors que le premier chapitre est consacré au rappel de certain résultats classiques concernant les formes bilinéaires.

La théorie étant élaborée, il reste les calculs à faire pour obtenir la formule explicitement pour chacun des types. Pour cela, nous devons calculer les cardinaux des groupes orthogonaux sur les corps finis, et sur $\mathbb{Z}/8\mathbb{Z}$. Ces calculs sont donnés dans les chapitres 3 et 4.

Enfin, le chapitre 5 est consacré au calcul proprement dit de cette formule.

Je tiens à exprimer toute ma gratitude au professeur Jacques Boéchat qui, avec une patiente attention, m'a aidé à écrire ce diplôme, et sans qui ce travail n'aurait pas vu le jour.

Je remercie aussi le professeur Henri Joris qui a aimablement été d'accord d'être l'expert de ce travail.

Enfin, je remercie Monique d'avoir bien voulu lire ce travail afin d'éliminer les principales fautes de rédaction.

Table des matières

CHAPITRE 1

Définitions et propriétés classiques des formes bilinéaires et quadratiques.

Ce premier chapitre sera essentiellement consacré au rappel de certains résultats classiques relatifs aux formes bilinéaires et quadratiques ainsi qu'aux objets dont nous aurons besoin pour ce travail.

A. Formes bilinéaires et formes quadratiques.

Définitions 1.1

Soient A un anneau unitaire commutatif, et M un A-module. Une *forme bilinéaire* est une application

$$\beta : M \times M \longrightarrow A \quad \text{telle que} \quad \begin{aligned} \beta(x+y,z) &= \beta(x,z)+\beta(y,z) \\ \beta(x,y+z) &= \beta(x,y)+\beta(x,z) \\ \beta(\lambda x,y) &= \lambda\beta(x,y) = \beta(x,\lambda y) \quad \forall x,y,z \in M, \text{ et } \lambda \in A. \end{aligned}$$

On dit que β est une *forme bilinéaire symétrique* si $\beta(x,y) = \beta(y,x)\ \forall x,y \in M$.

La plupart du temps, β sera supposée *non dégénérée*, c'est-à-dire qu'elle sera symétrique, et que l'homomorphisme

$$\begin{aligned} f_\beta : M &\longrightarrow \mathrm{Hom}_A(M,A) := M^* \\ x &\longmapsto \beta(x,\cdot) \end{aligned}$$

sera un isomorphisme.

(M,β) est alors appelé *module bilinéaire*.

Deux modules bilinéaires (M,β) et (M',β') sont dits équivalents s'il existe un isomorphisme $u : M \longrightarrow M'$ tel que $\beta'(u(x),u(y)) = \beta(x,y)\ \forall x,y \in M$, et on note $(M,\beta) \overset{A}{\simeq} (M',\beta')$; nous écrirons souvent par abus que $\beta \simeq \beta'$, ou alors $M \simeq M'$, s'il n'y a pas d'ambiguïté.

Proposition 1.2

Si (M,β) est un A-module quadratique libre de rang n, et $(e_1,\ldots,e_n)$ est une base de M, on note M_β la matrice à coefficient dans A définie par $M_{\beta_{ij}} = \beta(e_i,e_j)\ \forall i,j \in \mathbb{N}_n$.

β est non dégénérée si et seulement si $\det(M_\beta)$ est une unité de A. Nous noterons $U(A)$, l'ensemble des unités de A.

De plus, il y a équivalence entre le fait que $(M,\beta) \simeq (M',\beta')$ et l'existence d'une matrice S inversible dans $M_n(A)$ telle que $SM'_\beta S^t = M_\beta$.

Démonstration :

Le premier point découle du fait que M^* peut être muni de la base $(e_1^\#,\ldots,e_n^\#)$ où $e_i^\#(e_j) = \delta_{ij}\ \forall i,j \in \mathbb{N}_n$ et que $f_\beta(e_i) = \sum_{j=1}^{n} f_{ij}e_j^\#$. La matrice $(f_{ij})_{i,j\in\mathbb{N}_n}$ de f_β n'est autre que M_β.

Puisque f_β est un isomorphisme, on conclut.

Le second point découle aussi directement de la définition: S est la transposée de la matrice de u. •

Remarque :

Dorénavant, si cela n'est pas explicitement mentionné, M sera supposé libre de rang n et β symétrique.

Définition 1.3

Soit (M, β) un module bilinéaire. *Le déterminant de* β noté $\det \beta$ est le déterminant de M_β. La proposition précédente montre que $\det \beta$ est défini modulo A^{*^2}.
Le discriminant de β noté $\operatorname{discr} \beta = (-1)^{\frac{n(n-1)}{2}} \det \beta$.

Définitions 1.4

Soit N un sous-A-module de M muni de la forme bilinéaire β.
On note $N^\perp$ pour $\{x \in M \mid \beta(x, y) = 0 \ \forall y \in N\}$.
Il est clair que (M, β) est non dégénéré si et seulement si $M^\perp = \{0\}$, car $M^\perp$ est le noyau de f_β.
Soient N et N' deux sous-A-modules de M tels que $N \cap N' = \{0\}$. $N \oplus N'$ se note $N \boxplus N'$ si $N' \subset N^\perp$.

Proposition 1.5

Soient (M, β) un A-module bilinéaire non dégénéré et N un sous-module de M, tel que $\beta|_N$ soit non dégénérée. Alors $M = N \boxplus N^\perp$.

Démonstration :

Il suffit de voir que $M = N \oplus N^\perp$.
Soit $x \in M$, posons $f = f_\beta(x)|_N$. On a $f \in N^*$; or par hypothèse, $f_{\beta|_N}$ est un isomorphisme. Il existe donc $y \in N$ tel que $f_{\beta|_N}(y) = f$. On a ainsi :

$$\beta(x, z) = f_\beta(x)(z) = f(z) = f_{\beta|_N}(y)(z) = \beta(y, z) \quad \forall z \in N.$$

Donc $\beta(x - y, z) = 0 \ \forall z \in N$ ce qui nous donne $x - y \in N^\perp$.
Finalement, on a $x = y + (x - y) \in N \boxplus N^\perp$. Le fait que $N \cap N^\perp = \{0\}$ est trivial. •

Corollaire 1.6

Si A est un corps de caractéristique différente de 2, alors $\beta \simeq \beta'$ où β' est une forme diagonale, c'est-à-dire que la matrice M_β est diagonale et on la note $<a_1, \ldots, a_2>$, les a_i étant les coefficients diagonaux de M_β.

Démonstration :

S'il existe x et y tels que $\beta(x, y) \neq 0$, alors $\beta(x, x)$, $\beta(y, y)$ ou $\beta(x + y, x + y)$ est non nul. Supposons que ce soit x ; $\beta|_{<x>}$ est donc non dégénérée, par la proposition précédente. On a que $\beta \simeq <x> \boxplus <x>^\perp$, et on termine par récurrence. •

Définitions 1.7

Soient A un anneau commutatif et M un A-module. Une *forme quadratique* est une application :

$$q : M \longrightarrow A \quad \text{telle que} \quad q(\lambda x) = \lambda^2 q(x) \quad \forall \lambda \in A \text{ et } x \in M$$

et telle que l'application β_q avec

$$\beta_q(x, y) = q(x + y) - q(x) - q(y) \quad \forall x, y \in M$$

soit bilinéaire symétrique.
On dit que q est non dégénérée si β_q est non dégénérée, de même $\det q = \det \beta_q$ et $\operatorname{discr} q = \operatorname{discr} \beta_q$.
On dit alors que (M, q) est un *module quadratique*.
Si $M = N \boxplus N'$ pour β_q, alors $q(N \boxplus N') = q(N) + q(N')$. On peut donc aussi écrire $M = N \boxplus N'$ pour q.

Remarque :

Soit (M, β) un module bilinéaire. Il est très simple de transformer M en module quadratique, il suffit de prendre $q : M \longrightarrow A$ définie par $x \longmapsto \beta(x,x)$. Il faut noter que dans ce cas $\det q = 2^n \det \beta$ où n est la dimension de M, car $\beta_q = 2\beta$.

Réciproquement, si (M, q) est un module quadratique, β_q est entièrement déterminé par q, donc (M, β_q) est clairement un module bilinéaire.

Mais attention, il serait faux de croire qu'il y a une correspondance bi-univoque entre les deux notions : si cela est vrai sur les corps de caractéristiques différentes de 2, cela n'est pas vrai sur $\mathbb{Z}$ ni sur $\mathbb{F}_2$, ni sur les anneaux p-adiques et encore moins sur $\mathbb{Z}/8\mathbb{Z}$. Par exemple sur $\mathbb{Z}$, la forme quadratique $x_1^2 + x_1x_2 + x_2^2$ ne peut jamais s'écrire $\beta(x,x)$ où β est une forme bilinéaire ; d'autre part, sur $\mathbb{F}_2$, toute forme bilinéaire β_q associée à une forme quadratique q est "alternée" (i.e. $\beta_q(x,x) = 0\ \forall x$) donc n'est pas représentative de toutes les formes bilinéaires sur $\mathbb{F}_2$.

De plus on ne peut pas affirmer que l'une est plus "pratique" que l'autre : s'il est vrai qu'on peut facilement utiliser l'interprétation matricielle pour les formes bilinéaires, le théorème de Witt (voir chapitres 3 et 4) n'est pas toujours vrai pour elles, alors qu'il l'est pour toute forme quadratique non dégénérée.

B. Anneaux et corps p-adiques

Dans ce paragraphe, nous ferons une présentation succincte des anneaux $\mathbb{Z}_p$ et des corps $\mathbb{Q}_p$. Il me semble qu'il n'y a pas de manière plus courte et élégante de définir ces ensembles que celle de J.P. Serre dans [10, pp. 23-26], c'est pourquoi je ne donnerai que les résultats sans rien démontrer.

Définition 1.8

Soient $n \in \mathbb{N}$, $n \geq 2$, p premier et φ_n l'homomorphisme naturel de $\mathbb{Z}/p^n\mathbb{Z}$ dans $\mathbb{Z}/p^{n-1}\mathbb{Z}$ qui est évidemment surjectif.

On définit alors

$$\mathbb{Z}_p = \varprojlim(\mathbb{Z}/p^n\mathbb{Z}, \varphi_n) = \{(x_n)_{n=1}^{\infty} \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} \mid \varphi_n(x_n) = x_{n-1}\ \forall n \geq 2\}.$$

L'addition, la multiplication et la topologie sur $\mathbb{Z}_p$ sont héritées de celles induites par l'anneau topologique produit $\prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$. Les anneaux $\mathbb{Z}/p^n\mathbb{Z}$ étant munis de la topologie discrète, nous avons donc que $\prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$ est compact (Tychonov), donc $\mathbb{Z}_p$ aussi puisqu'il est fermé.

Théorème 1.9

$\mathbb{Z}_p$ possède les propriétés suivantes :

(I) $\mathbb{Z}_p/p^n\mathbb{Z}_p = \mathbb{Z}/p^n\mathbb{Z}$

(II) $\mathbb{Z}_p$ est un anneau local d'idéal maximal $p\mathbb{Z}_p$, donc les seuls idéaux de $\mathbb{Z}_p$ sont les $p^n\mathbb{Z}_p$, $n \in \mathbb{N}$; il suit que tout $x \in \mathbb{Z}_p$ s'écrit de manière unique sous la forme $p^n \cdot u$ avec u inversible.

(III) L'application

$$\begin{aligned} v_p : \mathbb{Z}_p &\longrightarrow \mathbb{N} \cup \{\infty\} \\ x &\longmapsto n \text{ tel que } x = p^n \cdot u \\ 0 &\longmapsto \infty \end{aligned}$$

est appelée *valuation p-adique*. Elle induit une distance : $d(x,y) = p^{-v_p(x-y)}$ qui définit la topologie de $\mathbb{Z}_p$. On a en outre que $\mathbb{Z}$ est dense dans $\mathbb{Z}_p$ qui est complet.

(IV) $\mathbb{Z}_p \cap \mathbb{Q} = \mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b\}$ •

Définition 1.10

Notons $\mathbb{Q}_p$ le corps des fractions de $\mathbb{Z}_p$. Vu ce qui précède, on a bien sûr que $\mathbb{Q}_p = \mathbb{Z}_p[p^{-1}]$, donc tout $x \in \mathbb{Q}_p$ s'écrit aussi de manière unique sous la forme $p^n \cdot u$, où u est un inversible de $\mathbb{Z}_p$ mais maintenant, $n \in \mathbb{Z}$; n s'appellera aussi *valuation p-adique* que l'on notera aussi $v_p(x)$; elle induira de la même manière la topologie sur $\mathbb{Q}_p$, et on obtient facilement le théorème suivant.

Théorème 1.11

(*I*) Le corps $\mathbb{Q}_p$, muni de la distance $d(x, y) = p^{-v_p(x-y)}$ est localement compact et complet ; le corps $\mathbb{Q}$ est dense dans $\mathbb{Q}_p$.

(*II*) La distance d est "ultramétrique", c'est-à-dire qu'elle vérifie l'inégalité suivante :

$$d(x, y) \leq \max(d(x, z), d(z, y)).$$

Nous obtenons grâce à cela le fait agréable que toute série de $\mathbb{Q}_p$ ou de $\mathbb{Z}_p$ est convergente si et seulement si son terme général tend vers 0.

Remarque :

Nous aurions pu définir $\mathbb{Q}_p$, de manière tout à fait analytique, comme le complété de $\mathbb{Q}$ pour la distance d, en voyant $\mathbb{Z}_p$ comme la boule unité et $p\mathbb{Z}_p$ comme la boule unité privée de la sphère unité. •

C. Réseaux et bases de réseaux

Nous allons donner dans ce paragraphe un critère pour pouvoir compléter des vecteurs linéairement indépendants en une base de réseau.

Définitions 1.12

Soient A un anneau principal, (dans la pratique A sera $\mathbb{Z}$ où $\mathbb{Z}_p$), K son corps des fractions, V un K-espace vectoriel de dimension n et $(e_1, \ldots, e_n)$ une K-base de V. Alors l'ensemble des $\lambda_1 e_1 + \cdots + \lambda_n e_n$ où les λ_i parcourent A est appelé *A-réseau* et $(e_1, \ldots, e_n)$ est appelé *base du réseau.*

Soit Λ un réseau. Un vecteur de Λ est dit *primitif*, s'il est possible de trouver $n-1$ autres vecteurs formant avec lui une base de Λ.

Si $\Lambda \subset \Gamma$ sont deux A-réseaux, on dit que Λ est un *sous-A-réseau* de Γ.

Remarque :

Il existe une définition plus générale si l'anneau n'est pas principal, mais nous n'en n'aurons pas besoin.

Définition 1.13

Soient $\Gamma \subset \Lambda$ deux A-réseaux munis des bases $(b_1, \ldots, b_n)$ et $(e_1, \ldots, e_n)$ respectivement. Pour tout $i, j \in \mathbb{N}_n$, il existe $r_{ij} \in K$ tel que $b_i = \sum_{j=1}^{n} r_{ij} e_j$.

$d(\Gamma/\Lambda) \stackrel{\text{def}}{=} det(r_{ij})$ est appelé *le discriminant de Γ sur Λ.*

Si $V = K^n$, $\Lambda = A^n$; alors $d(\Gamma/A^n)$ s'écrit $d(\Gamma)$.

Remarque :

Le discriminant est unique à un facteur de $U(A)$ près.

Démonstration :

Soient $(e_1,\dots,e_n)$, $(e'_1,\dots,e'_n)$ deux bases d'un A-réseau Λ, et soient $(b_1,\dots,b_n)$, $(b'_1,\dots,b'_n)$ deux bases d'un sous-A-réseau Γ de Λ.

On a que $b_i = \sum_{j=1}^{n} r_{ij}e_j$, $b'_i = \sum_{j=1}^{n} r'_{ij}e'_j$ avec r_{ij} ,$r'_{ij} \in A$ et $b_i = \sum_{j=1}^{n} \alpha_{ij}b'_j$, $e'_i = \sum_{j=1}^{n} \beta_{ij}e_j$ avec $(\alpha_{ij})_{i,j\in\mathbb{N}_n} = C$ et $(\beta_{ij})_{i,j\in\mathbb{N}_n} = B \in Gl_n(A)$.

On trouve facilement que

$$C(r'_{ij})_{i,j\in\mathbb{N}_n}B = (r_{ij})_{i,j\in\mathbb{N}_n}$$

et on conclut en considérant le fait que toute matrice de $Gl_n(A)$ a pour déterminant un élément de $U(A)$.

Lemme 1.14

Soit Γ un sous-A-réseau de Λ. Alors

$$d(\Gamma/\Lambda)\Lambda \subset \Gamma.$$

Démonstration :

Il suffit de montrer ce fait pour les éléments d'une base $(e_1,\dots,e_n)$ de Λ. Soit $(b_1,\dots,b_n)$ une base de Γ.

Par définition de Γ, il existe $(\gamma_{ij})_{i,j\in\mathbb{N}_n} \in M_n(A)$ telle que $d(\Gamma/\Lambda) = \det(\gamma_{ij})$ et $\sum_{j=1}^{n} \gamma_{ij}e_j = b_j$.

En résolvant ce système, on trouve une matrice $(\gamma'_{ij})_{i,j\in\mathbb{N}_n} \in M_n(A)$ telle que $d(\Gamma/\Lambda)e_i = \sum_{j=1}^{n} \gamma'_{ij}b_j \in \Gamma$.

•

Lemme 1.15

Soit Γ un sous-A-réseau de Λ et $(e_1,\dots,e_n)$ une base de Λ. Alors il existe $(a_1,\dots,a_n)$ une base de Γ telle que :

$$\begin{aligned} a_1 &= s_{11}e_1 \\ a_2 &= s_{12}e_1 + s_{22}e_2 \\ &\vdots \\ a_n &= s_{n1}e_1 + \cdots + s_{nn}e_n \end{aligned}$$

avec

$$s_{ij} \in A \text{ et } s_{ii} \neq 0,\ i,j \in \mathbb{N}_n.$$

Démonstration :

Posons $\Gamma^{(j)} = \{a \in \Gamma \mid a = \sum_{i=1}^{j} \gamma_i e_i\}$ et $P_j = \{\gamma_j \mid \exists\ \gamma_1,\dots,\gamma_{j-1}$ avec $\sum_{i=1}^{j} \gamma_i e_i \in \Gamma^{(j)}\}$. P_j est un idéal non nul de A. En effet, $d(\Gamma/\Lambda)e_j \in \Gamma^{(j)}$, et si $\mu,\nu \in A$ et $\gamma_j,\gamma'_j \in P_j$ alors $\mu\gamma_j + \nu\gamma'_j \in P_j$ clairement.

Puisque A est principal, il existe $s_{jj} \neq 0$ tel que $P_j = s_{jj}A$, et par définition de P_j, on pourra trouver $s_{1j},\dots,s_{j-1j}$ tels que $a_j := \sum_{i=1}^{j} s_{ij}e_i \in \Gamma^{(j)}$ pour tout $j \in \mathbb{N}_n$.

Montrons que les a_j engendrent Γ :

Soit $a = \sum_{i=1}^{n} \mu_i e_i \in \Gamma = \Gamma^{(n)}$ avec $\mu_n \in P_n = s_{nn}A$. Donc,

$$a - \nu_n a_n = \sum_{i=1}^{n-1} \mu'_i e_i \in \Gamma^{(n-1)}$$

et, par itération du procédé on trouve que $a = \sum_{i=1}^{n} \nu_n a_n$. •

Lemme 1.16

Soient $c_1, \ldots, c_p$ des vecteurs linéairement indépendants d'un A-réseau Λ. Alors il existe une base $(b_1, \ldots, b_n)$ de Λ telle que :

$$\begin{aligned} c_1 &= s_{11} b_1 \\ c_2 &= s_{12} b_1 + s_{22} b_2 \\ &\vdots \\ c_p &= s_{n1} b_1 + \cdots + s_{pp} b_p \end{aligned}$$

avec

$$s_{ij} \in A \text{ et } s_{ii} \neq 0,\ i, j \in \mathbb{N}_p.$$

Démonstration :

On peut choisir $c_{p+1}, \ldots, c_n \in \Lambda$ tels que $c_1, \ldots, c_n$ soient linéairement indépendants. Posons Γ le sous-réseau de Λ engendré par $c_1, \ldots, c_n$. Par le lemme 1.14, on a $d\Lambda \subset \Gamma$ où $d = d(\Gamma/\Lambda)$. Grâce au lemme précédent, nous pouvons trouver $(b_1, \ldots, b_n)$ une base de Λ telle que :

$$\begin{aligned} db_1 &= t_{11} c_1 \\ db_2 &= t_{12} c_1 + t_{22} c_2 \\ &\vdots \\ db_n &= t_{n1} c_1 + \cdots + t_{nn} c_n \end{aligned}$$

avec

$$t_{ij} \in A \text{ et } t_{ii} \neq 0,\ i, j \in \mathbb{N}_n.$$

En résolvant le système par rapport aux c_i, nous obtenons un système du type cherché. A priori, les s_{ij} se trouvent dans K seulement. Cependant, les b_i forment une base de Λ (et de V), puis $c_i \in \Lambda$; donc on trouve que $s_{ij} \in A$ grâce à l'unicité de l'écriture de tout élément relativement à une base. De plus, $s_{ii} = d/t_{ii} \neq 0$. •

Théorème 1.17

Soient $j \leq n \in \mathbb{N}$, A un anneau principal et intègre, K son corps des fractions et $c_1, \ldots, c_j \in A^n$ linéairement indépendants. Les affirmations suivantes sont équivalentes :

i) Il existe $c_{j+1}, \ldots, c_n$ tels que $c_1, \ldots, c_n$ soit une base de A^n.

ii) Les sous-déterminants de rang j de la matrice $n \times j$ $(c_1 c_2 \cdots c_j)$ n'ont pas de diviseurs communs.

iii) Si $a = v_1 c_1 + \cdots + v_j c_j \in A^n$ avec $v_1, \ldots, v_j \in K$, alors $v_1, \ldots, v_j \in A$.

Démonstration :

i)⇒ ii):

Soit $(c_1, \ldots, c_n) = P \in M_n(A)$. On a $\det(P) \in U(A)$. Par le développement de Laplace à partir des j premières colonnes, on a : $\det(P) = \sum R_M \cdot R_{M'} \in U(A)$ où les R_M sont les déterminants des matrices $j \times j$ en parcourant les j premières colonnes de P et où les $R_{M'}$ sont les déterminants des matrices $(n-j) \times (n-j)$ "complémentaires". Et par le théorème de Bezout, on conclut.

ii)⇒ iii):

Soit $a = v_1 c_1 + \cdots + v_j c_j \in A^n$. Il existe $w_1, \ldots, w_n \in A$ tels que $a = w_1 e_1 + \cdots + w_n e_n$ où $(e_1, \ldots, e_n)$ est la base canonique de A^n, donc

$$w_i = \sum_{k=1}^{j} v_k c_{ik} \ \forall i \in \mathbb{N}_n \qquad \heartsuit_i$$

avec $c_i = \sum_{k=1}^{n} c_{ki} e_k$, où $c_{ik} \in A$ pour tout $i \in N_n, k \in \mathrm{I}_j$.

En prenant au hasard j équations de type $\heartsuit_i$ et en résolvant par rapport à v_k, on obtient que $v_k R_M \in A$ pour tout $k \in N_j$ et pour toute sous-matrice Mde rang j de la matrice $(c_1 \cdots c_j)$. Or, par hypothèse, et par le théorème de Bezout, il existe $\lambda_1, \ldots, \lambda_m \in A$ tels que $\sum_M \lambda_i R_M = 1$ donc $v_k = \sum_M \lambda_i (R_M v_k) \in A$ pour tout $k \in \mathrm{I}_j$.

iii)⇒ i) :

Grâce au lemme précédent, on peut trouver $(b_1, \ldots, b_n)$ une base de A^n telle que :

$$\begin{aligned} c_1 &= s_{11} b_1 \\ c_2 &= s_{12} b_1 + s_{22} b_2 \\ &\vdots \\ c_j &= s_{n1} b_1 + \cdots + s_{jj} b_p \end{aligned}$$

avec $s_{ij} \in A$ et $s_{ii} \neq 0$. En résolvant, on trouve que :

$$\begin{aligned} b_1 &= s'_{11} c_1 \\ b_2 &= s'_{12} c_1 + s'_{22} c_2 \\ &\vdots \\ b_j &= s'_{n1} c_1 + \cdots + s'_{jj} c_p \end{aligned}$$

avec $s'_{ij} \in K$ pour tout i, j . Or $b_1, \ldots, b_j \in A^n$, donc par hypothèse $s'_{ij} \in A \quad \forall i, j$. Finalement, $(c_1, \ldots, c_j, b_{j+1}, \ldots, b_n)$ est une base de A^n. •

Corollaire 1.18

$(x_1, \ldots, x_n) \in A^n$ est primitif $\iff x_1, \ldots, x_n$ ne possèdent pas de diviseurs communs.

D. Réseaux bilinéaires et quadratiques

Définitions 1.19

Soient A un anneau principal, K son corps des fractions et (V, β) un K-espace vectoriel bilinéaire.

Soit Λ un A-réseau ; on dit que Λ est un *réseau bilinéaire* si $\beta(x, y) \in A \quad \forall x, y \in \Lambda$.

Les réseaux quadratiques se définissent de la même manière.

Remarque :

Si M est un A-module bilinéaire libre de rang n, M peut être vu comme A-réseau bilinéaire sur $V = M \otimes_A K$.

Définition 1.20

Soient A et K comme dans la définition 1.19, et soit (V, q) un K-espace vectoriel quadratique. Pour tout A-réseau Λ de V, on définit $\Lambda^{\#} = \{x \in V \mid \beta_q(x, y) \in A \quad \forall y \in \Lambda\}$.

Si Λ est un réseau quadratique, il est clair que $\Lambda \subset \Lambda^{\#}$.

Proposition 1.21

Si Λ est un réseau d'un K espace vectoriel quadratique non dégénéré (V,q) de dimension n, alors $\Lambda^\#$ est aussi un réseau, et si Λ est un réseau quadratique et q est non dégénérée sur Λ, alors $\Lambda = \Lambda^\#$.

Démonstration :

On sait par hypothèse que

$$f_{\beta_q} : V \longrightarrow \mathrm{Hom}_K(V,K)$$
$$x \longmapsto \beta_q(x,\cdot)$$

est un isomorphisme. Soit $\mathfrak{B} = (e_1,\ldots,e_n)$ une A-base de Λ. On sait que $\mathrm{Hom}_K(V,K)$ est engendré par les $e_i^\#$ où $e_i^\#(e_j) = \delta_{ij}, \quad \forall i,j \in \mathbb{N}_n$. Il existe donc des c_i linéairement indépendants tels que $f_{\beta_q}(c_i) = e_i^\#, \quad \forall i$. Nous allons voir que $\Lambda^\# = \sum_{i=1}^n Ac_i$.

Le fait que $\Lambda^\# \supset \sum_{i=1}^n Ac_i$ découle directement de la définition des c_i.

Soit maintenant $x \in \Lambda^\#$. On a $\beta_q(x,e_1) = \lambda_1 \in A$. Or $\lambda_1 = \beta_q(\lambda_1 c_1, e_1)$, donc $\beta_q(x - \lambda_1 c_1, e_1) = 0$.

On a aussi $\beta_q(x - \lambda_1 c_1, e_2) = \beta_q(\lambda_2 c_2, e_2) \in A$ car $c_i \in \Lambda^\# \ \forall i$. Donc $\beta_q(x - \lambda_1 c_1 - \lambda_2 c_2, e_2) = 0$, de même $\beta_q(x - \lambda_1 c_1 - \lambda_2 c_2, e_1) = 0$ par définition des c_i. On recommence alors ce procédé, et on obtient que $\beta_q(x - \sum \lambda_i c_i, e_j) = 0 \ \forall j$ donc $x = \sum \lambda_i c_i$.

Supposons maintenant que Λ soit un réseau quadratique, donc que $\Lambda \subset \Lambda^\#$. $\mathfrak{B}$ étant une base de V, on a que $c_i = \sum_{i=1}^n \lambda_{ij} e_j \ \forall i \in \mathbb{N}_n$ avec $\lambda_{ij} \in K$. Par le choix des c_i, on a :

$$\delta_{ik} = \beta_q(c_i,e_k) = \sum_{j=1}^n \lambda_{ij}\beta_q(e_j,e_k),$$

ce qui nous donne : $L \cdot B = I_n$ où $L_{ij} = \lambda_{ij} \ \forall i,j$, donc $L = B^{-1}$. Puisque q est non dégénérée sur Λ, on a que $\det B$ est inversible dans A, donc L est à coefficient dans A. D'où $\Lambda = \Lambda^\#$. •

Définitions 1.22

Soient A un anneau commutatif et (M,β) un A-module bilinéaire.

On définit $O_\beta(M) = \{u : M \longrightarrow M \mid u$ est un isomorphisme et $\beta(u(x),u(y)) = \beta(x,y) \ \forall x,y \in M\}$.

La composition des applications munit naturellement cet ensemble d'une structure de groupe, et on l'appellera *groupe orthogonal de* M.

Si (M,q) est un A-module quadratique, on définit de même

$O_q(M) = \{u : M \longrightarrow M \mid u$ est un isomorphisme et $q(u(x)) = q(x) \ \forall x \in M\}$.

Remarque importante :

Soient A un anneau principal, K son corps des fractions, (V,β) un espace vectoriel bilinéaire et M, M' deux réseaux bilinéaires.

Supposons que $(M,\beta|_M) \overset{A}{\simeq} (M',\beta|_{M'})$ en tant que A-modules bilinéaires. Il existe donc un isomorphisme $u : M \longrightarrow M'$ tel que $\beta|_M(x,y) = \beta|_{M'}(u(x),u(y)) \ \forall x,y \in M$. Puisque M et M' contiennent des bases de V, u se prolonge en $u \in O_\beta(V)$.

Inversément, si $u \in O_\beta(V)$ et M est un A-réseau bilinéaire, $M' = u(M)$ est aussi un A-réseau bilinéaire et on a bien sûr que $(M,\beta|_M) \overset{A}{\simeq} (M',\beta|_{M'})$ en tant que A-modules bilinéaires.

Soient maintenant u_1, $u_2 \in O_\beta(V)$ et M comme avant ; supposons que $u_1(M) = u_2(M)$, c'est-à-dire $u_1^{-1}u_2 \in O_{\beta|_M}(M)$. On obtient donc la proposition suivante :

Proposition 1.23

Soient comme avant A, K, (V,β) et M un réseau bilinéaire. Alors $O_{\beta|_M}(M) \subset O_\beta(V)$ canoniquement, et il y a bijection entre l'ensemble des sous-A-réseaux bilinéaires de (V,β) qui sont isomorphes à M en tant que A-modules bilinéaires et les classes de $O_\beta(V)$ à gauche de $O_{\beta|_M}(M)$. •

E. Quelques rappels

Nous citerons dans ce paragraphe des résultats classiques sur les formes bilinéaires et quadratiques entières, entre autres le théorème de finitude et le théorème de Hasse-Minkowski.

Définition 1.24

Soit (M,β) un $\mathbb{Z}$-module bilinéaire libre de rang n. (M,β) est dit de *type* (II) si $\beta(x,x)$ est pair pour tout $x \in M$; si (M,β) n'est pas de type (II) il est de type (I).
On note $\mathscr{S}_n$ la catégorie des $\mathbb{Z}$-modules bilinéaires libres de rang n non dégénérés et définis positifs.
$\mathscr{C}_n$ est l'ensemble des classes d'isomorphismes de $\mathscr{S}_n$ qui sont de type (II).
Finalement, on note $\mathscr{H}_n$ l'ensemble des classes d'isomorphismes de $\mathscr{S}_n$ qui sont de type (I).

Théorème 1.25 (théorème de finitude)

Le cardinal des classes à isomorphismes près des éléments de $\mathscr{S}_n$ est fini, ou plus généralement, le cardinal des classes d'équivalences des formes bilinéaires entières de déterminant d donné est fini.

Démonstration :

Une démonstration de ce théorème est donnée dans [3, pp. 135-137]. •

Corollaire 1.26

$\mathscr{C}_n$ et $\mathscr{H}_n$ sont finis.

Corollaire 1.27

Le théorème 1.25 et le corollaire 1.26 sont aussi vrais si les modules considérés sont quadratiques.

Démonstration :

$(M,q) \simeq (M',q') \Longleftrightarrow (M,\beta_q) \simeq (M',\beta_{q'})$ car $\mathbb{Z}$ est intègre. •

Définition 1.28

Soit (M,β) un $\mathbb{Z}$-module bilinéaire libre de rang n. Alors $M \otimes_{\mathbb{Z}} \mathbb{Z}_p$, est un $\mathbb{Z}_p$-module bilinéaire libre de rang n que l'on note (M_p,β_p).
De même, si (V,β) est un $\mathbb{Q}$-espace bilinéaire de dimension n ; en tensorisant par $\mathbb{Q}_p$, on obtient (V_p,β_p) et en tensorisant par $\mathbb{R}$, on obtient (V_∞,β_∞).
On peut bien sûr faire de même avec des espaces quadratiques.

Définition 1.29

Soient $\mathbb{P}$ l'ensemble des nombres premiers positifs et $\mathbb{P}' = \mathbb{P} \cup \{\infty\}$; par convention, $\mathbb{Q}_\infty = \mathbb{R}$. Fixons-nous $p \in \mathbb{P}'$. Pour tout a et $b \in \mathbb{Q}_p^*$, 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.*

Proposition 1.30

Soient $p \in \mathbb{P}'$, $a,a',b,c \in \mathbb{Q}_p^*$ et $d \in \mathbb{Q}_p^* \setminus \{1\}$. Les égalités suivantes sont satisfaites :

i) $(a,b)_p = (b,a)_p$

ii) $(aa',b)_p = (a,b)_p(a',b)_p$

iii) $(c,-c)_p = (d,1-d)_p = 1$.

Théorème 1.31

On a les égalités :

$$(a,b)_p = \begin{cases} 1 & \text{si } p=\infty,\ a \text{ ou } b>0 \\ -1 & \text{si } p=\infty,\ a \text{ et } b<0 \\ (-1)^{\frac{\alpha\beta(p-1)}{2}} \cdot \left(\frac{u}{p}\right)^{\beta} \cdot \left(\frac{v}{p}\right)^{\alpha} & \text{si } p\neq 2,\ \infty \\ (-1)^{\frac{(u-1)(v-1)}{4}+\frac{\alpha(v^2-1)}{8}+\frac{\beta(u^2-1)}{8}} & \text{si } p=2, \end{cases}$$

où $\left(\frac{\cdot}{p}\right)$ est le symbole de Legendre et a respectivement b valent $p^\alpha u$ et $p^\beta v$, u et v étant des unités de $\mathbb{Z}_p$.

Théorème 1.32 (Formule du produit de Hilbert)

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

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

Démonstration :

Ces résultats sur le symbole de Hilbert sont démontrés dans [10, pp. 37-45] •

Théorème 1.33 (Hasse-Minkowski)

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

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

Démonstration :

Ce théorème hautement non trivial, utilise ce que l'on vient de voir sur le symbole de Hilbert et demande une connaissance approfondie des formes bilinéaires sur les corps p-adiques. Toute la première partie de [10] est consacrée à la démonstration de ce théorème. •

Remarque :

Ce résultat est aussi vrai pour des espaces quadratiques, puisque tous ces corps sont de caractéristique nulle (y compris les p-adiques, bien que leur nom pourrait nous faire présupposer autre chose ...)

F. La notion de genre

Dans ce paragraphe, nous introduirons une nouvelle relation d'équivalence sur les modules bilinéaires ; nous verrons que pour ceux qui sont libres de rang n et définis positifs, il n'y a que deux classes d'équivalence : $\mathscr{H}_n$ et $\mathscr{C}_n$.

Définition 1.34

Soient (M,β) et (M',β') deux $\mathbb{Z}$-modules bilinéaires libres de rang n, on dit que (M,β) est dans le même *genre* que (M',β') si

$$(M_p,\beta_p) \overset{\mathbb{Z}_p}{\simeq} (M'_p,\beta'_p) \quad \forall p \in \mathbb{P}'$$

avec la convention que $\mathbb{Z}_\infty = \mathbb{R}$. Et on écrit $(M,\beta) \sim (M',\beta')$.

On définit cette notion de manière identique pour les modules quadratiques.

Remarque :

Si $(M,\beta) \simeq (M',\beta')$ alors $(M,\beta) \sim (M',\beta')$. Mais la réciproque n'est pas vraie, par exemple en dimension 2, où les formes β et β' définies par les matrices $\begin{pmatrix} 2 & 0 \\ 0 & 17 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \\ 0 & 34 \end{pmatrix}$ sont dans le même genre mais elles ne sont pas $\mathbb{Z}$-équivalentes. Cet exemple illustre bien qu'il n'y a pas d'équivalent au théorème de Hasse-Minkowski pour les formes entières.

Tout d'abord, nous allons énoncer toute une série de résultats :

Théorème 1.35

Soient $f \in \mathbb{Z}_p[X_1,\ldots,X_m]$, $x \in (\mathbb{Z}_p)^m$, $n,k \in \mathbb{N}$ et $j \in \mathbb{N}_m$.

Supposons que

$$0 \leq 2k < n, \quad f(x) \equiv 0 \pmod{p^n} \quad \text{et} \quad v_p\left(\frac{\partial f}{\partial X_j}(x)\right) = k.$$

Alors il existe un zéro y de f dans $(\mathbb{Z}_p)^m$ qui est congru à x modulo p^{n-k}.

Démonstration :

Ce théorème ainsi que les corollaires suivants sont démontré dans [10, pp. 28-30]. •

Corollaire 1.36

Soit p impair, et u une unité de $\mathbb{Z}_p$; alors

$$u \in U^2(\mathbb{Z}_p) \text{ si et seulement si la congruence } u \equiv X^2 \pmod{p} \text{ est résoluble.}$$

De même si $p = 2$, on a l'équivalence

$$u \in U^2(\mathbb{Z}_2) \text{ si et seulement si la congruence } u \equiv X^2 \pmod{8} \text{ est résoluble.}$$

$$\text{C'est-à-dire si et seulement si } u \equiv 1 \pmod{8}.$$

Corollaire 1.37

Soit $A = (a_{ij}) \in GL_n(\mathbb{Z}_p)$ telle que $A = A^t$. Soient $f = \sum_{i,j=1}^{n} a_{ij}X_iX_j \in \mathbb{Z}_p[X_1\ldots,X_n]$ et $a \in \mathbb{Z}_p$.

Alors il existe $(\alpha_1,\ldots,\alpha_n) \in (\mathbb{Z}_p)^n$ primitif tel que $f(\alpha_1,\ldots,\alpha_n) = a$ si et seulement si

a) p impair : il existe $x_1,\ldots,x_n \in \mathbb{Z}_p$ non tous dans $p\mathbb{Z}_p$ tels que $f(x_1,\ldots,x_n) \equiv a \pmod{p}$.

b) $p = 2$: il existe $x_1,\ldots,x_n \in \mathbb{Z}_2$ non tous pairs tels que $f(x_1,\ldots,x_n) \equiv a \pmod{8}$.

Forts de ces résultats, nous allons étudier en détail les modules de $\mathscr{S}_n$ vus sur les anneaux p-adiques.

Proposition 1.38

Soit (M,β) un $\mathbb{Z}_p$-module bilinéaire non dégénéré libre de rang n. Alors

$$M \simeq <s_1> \boxplus \cdots \boxplus <s_l> \boxplus <\begin{pmatrix} a_1 & c_1 \\ c_1 & b_1 \end{pmatrix}> \boxplus \cdots \boxplus <\begin{pmatrix} a_m & c_m \\ c_m & b_m \end{pmatrix}>$$

où $l + 2m = n$, $s_i \in U(\mathbb{Z}_p)$ $\forall i \in \mathbb{N}_l$ et $a_jb_j - c_j^2 \in U(\mathbb{Z}_p)$ $\forall j \in \mathbb{N}_m$.

Démonstration :

Supposons qu'il existe $x_1 \in M$ tel que $\beta(x_1,x_1) \in U(\mathbb{Z}_p)$; x_1 est primitif, car si $x_1 = px_1'$ alors $\beta(x_1,x_1) = p^2\beta(x_1',x_1') \notin U(\mathbb{Z}_p)$. De plus, $\beta|_{<x_1>}$ est non dégénérée, donc grâce à la proposition 1.5 et au corollaire 1.18 on a $M \simeq <x_1> \boxplus <x_1>^{\perp}$.

En continuant ainsi, on a

$$M \simeq <x_1> \boxplus \cdots \boxplus <x_l> \boxplus M' \quad \text{avec } \beta(x,x) \in p\mathbb{Z}_p \ \forall x \in M'.$$

Soit $z_1 \in M'$, z_1 primitif. Puisque $\beta|_{M'}$ est non dégénérée, il existe $t_1 \in M'$ primitif tel que $\beta(z_1,t_1) \in U(\mathbb{Z}_p)$. Nous savons que $\beta(z_1,z_1)$ et $\beta(t_1,t_1) \in p\mathbb{Z}_p$. Un rapide raisonnement de déterminant nous permet de dire que $\beta|_{<z_1,t_1>}$ est non dégénérée.

De plus il est possible d'étendre z_1, t_1 en une $\mathbb{Z}_p$-base de M', car soit $c = \frac{1}{p}(z_1 + t_1)$, alors

$$|\beta(c,z_1)| = |\frac{1}{p}\beta(z_1,z_1) + \frac{1}{p}\beta(z_1,t_1)| \overset{(*)}{=} |\frac{1}{p}\beta(z_1,t_1)| = p > 1$$

donc $c \notin M$.

L'égalité $(*)$ vient du fait que la valeur absolue p-adique est ultramétrique et que dans ce cas $|x+y| = \max(|x|,|y|)$ si $|x| \neq |y|$.

Si $c = \frac{1}{p}z_1 + t_1$ on voit de même que $|\beta(c,t_1)| = p$. En utilisant le théorème 1.17 et en faisant une brève récurrence, on conclut. •

Cas p $\neq$ 2

Proposition 1.39

Sous les mêmes hypothèse que la proposition précédente, avec p impair, alors (M,β) est diagonalisable.

Démonstration :

Grâce à la proposition 1.38, il suffit de voir qu'une forme de dimension 2 et représentée par la matrice inversible $\begin{pmatrix} a & c \\ c & b \end{pmatrix}$, avec $a,b \in p\mathbb{Z}_p$ et $c \in U(\mathbb{Z}_p)$, est diagonalisable.

Le vecteur $x = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ représente $a+b+2c$ qui est inversible si $p \neq 2$.

$\beta|_{<x>}$ étant donc non dégénérée, la forme est donc diagonalisable. •

Lemme 1.40

Soient $a,b,c \in \mathbb{F}_p$. Alors il existe x et $y \in \mathbb{F}_p$ tels que $ax^2 + by^2 = c$.

Démonstration :

Soit $A = \{ax^2 \mid x \in \mathbb{F}_p\}$ et $B = \{c - by^2 \mid y \in \mathbb{F}_p\}$.

On a $\sharp A = \sharp B = \dfrac{p-1}{2} + 1 = \dfrac{p+1}{2}$. Donc $A \cap B \neq \emptyset$ •

Proposition 1.41

Soient $p \in \mathbb{P} \setminus \{2\}$, $a_1, \ldots, a_n \in U(\mathbb{Z}_p)$ et (M,β) un module bilinéaire libre de rang n sur $\mathbb{Z}_p$, avec

$$\beta = <a_1> \boxplus \cdots \boxplus <a_n>.$$

Alors β est $\mathbb{Z}_p$-équivalente à la forme

$$<1> \boxplus \cdots \boxplus <1> \boxplus <a>$$

où $a = \prod_{i=1}^{n} a_i$.

Démonstration :

Par le lemme précédent, nous savons qu'il existe s_1 et $s_2 \in \mathbb{Z}_p$ tels que

$$a_1 s_1^2 + a_2 s_2^2 \equiv 1 \pmod{p}.$$

Sans limiter la généralité, on peut supposer que s_1 est inversible, et donc que $\dfrac{1 - a_2 s_2}{a_1}$ est un carré modulo p. Vu le corollaire 1.36, il existe donc $\overline{s_1} \in U^2(\mathbb{Z}_p)$ tel que $a_1\overline{s_1}^2 + a_2 s_2^2 = 1$. Ceci démontre la proposition pour $n = 2$; le cas n quelconque se traite par une récurrence facile. •

Corollaire 1.42

Soit $p \in \mathbb{P} \setminus \{2\}$ et $(M, \beta) \in \mathscr{S}_n$. Alors

$$\beta \overset{\mathbb{Z}_p}{\simeq} <1> \boxplus \cdots \boxplus <1>.$$

Démonstration :

β est diagonalisable vu la propositon 1.39, et on conclut grâce à la proposition précédente, sachant que $\det(\beta) = 1$. •

Cas p = 2

Remarque :

Jusqu'ici, on voit qu'il n'est donc pas nécessaire de se préoccuper des types ; ce n'est que pour $p = 2$ qu'il faudra distinguer le type *II* et le type *I*.

Modules de type *II*

Soit (M, β), un $\mathbb{Z}$-module bilinéaire de type *II*. Par la proposition 1.38, et puisque $\beta(x, x) \in 2\mathbb{Z}_2 \ \forall x \in M_2$, on peut considérer que β est une somme orthogonale de formes représentées par des matrices du type $\begin{pmatrix} a & c \\ c & b \end{pmatrix}$, $a, b \in 2\mathbb{Z}_2$ et $c \in U(\mathbb{Z}_2)$.
Nous allons voir que dans ce cas

$$\begin{pmatrix} a & c \\ c & b \end{pmatrix} \overset{\mathbb{Z}_2}{\simeq} \begin{cases} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & \text{si } \begin{pmatrix} a & c \\ c & b \end{pmatrix} \text{ représente 0 non trivialement} \\ \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} & \text{sinon.} \end{cases} \qquad (*)$$

Supposons donc qu'elle représente 0 non trivialement, c'est-à-dire, vu le corollaire 1.37, que l'équation

$$ax^2 + 2cxy + by^2 \equiv 0 \pmod 8$$

possède une solution $(x, y) \notin (2\mathbb{Z}_2)^2$; ce qui est toujours le cas sauf si $a \equiv b \equiv 2 \bmod 4$. Il est clair que, dans ce cas, on a

$$\begin{pmatrix} a & c \\ c & b \end{pmatrix} \overset{\mathbb{Z}_2}{\simeq} \begin{pmatrix} 0 & c' \\ c' & b' \end{pmatrix}$$

avec $b' \in 2\mathbb{Z}_2$ et $c' \in U(\mathbb{Z}_2)$, car on peut supposer que 0 est représenté primitivement.

Finalement, la matrice $\begin{pmatrix} \frac{-b'}{2c'} & 1 \\ \frac{1}{c'} & 0 \end{pmatrix}$ est la matrice de changement de base qui transforme $\begin{pmatrix} 0 & c' \\ c' & b' \end{pmatrix}$ en la matrice $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Si la forme ne représente pas 0, c'est-à-dire si $a \equiv b \equiv 2 \bmod 4$, on a alors que l'équation

$$ax^2 + 2cxy + by^2 \equiv 2 \pmod 8$$

est résoluble avec $(x, y) = (1, 1)$ ou $(1, -1)$ par exemple. Le corollaire 1.37 implique que notre matrice est $\mathbb{Z}_p$-équivalente à $\begin{pmatrix} 2 & c' \\ c' & b' \end{pmatrix}$ avec $b' \in 2\mathbb{Z}_2$ et $c' \in U(\mathbb{Z}_2)$.
Ce qui nous fait que $2b' - c'^2 \equiv 3 \bmod 8$ car $b' \equiv 2 \bmod 4$.
Il existe donc $\alpha \in U(\mathbb{Z}_2)$ tel que $\alpha^2(2b' - c^2) = 3$.
En faisant un changement de base défini par la matrice $\begin{pmatrix} 1 & 0 \\ \frac{1-c\alpha}{2} & \alpha \end{pmatrix}$, la matrice $\begin{pmatrix} 2 & c' \\ c' & b' \end{pmatrix}$ est $\mathbb{Z}_p$-équivalente à $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$.
Nous voilà donc en mesure de démontrer le

Théorème 1.43

Si (M,β) est un $\mathbb{Z}_2$-module bilinéaire de rang $2r$ non dégénéré de type (II), alors :

$$M_\beta \overset{\mathbb{Z}_2}{\simeq} \begin{cases} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \boxplus \cdots \boxplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & \text{si } \det(\beta) = (-1)^r \\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \boxplus \cdots \boxplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \boxplus \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} & \text{si } \det(\beta) = 3(-1)^{r-1} \end{cases}.$$

Démonstration :

Vu ce qui précède, on a :

$$\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \overset{\mathbb{Z}_2}{\simeq} \begin{pmatrix} -2 & -1 \\ -1 & -2 \end{pmatrix}$$

car $-2 \equiv 2 \bmod 4$. Donc il est évident que :

$$\begin{pmatrix} 2 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 1 & 2 \end{pmatrix} \overset{\mathbb{Z}_2}{\simeq} \begin{pmatrix} 2 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & -2 & -1 \\ 0 & 0 & -1 & -2 \end{pmatrix}$$

Mais de plus, nous avons l'égalité matricielle suivante :

$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & -1 \\ 1 & 0 & 1 & -1 \\ 0 & 1 & 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & -1 & -1 & -1 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & -2 & -1 \\ 0 & 0 & -1 & -2 \end{pmatrix},$$

on obtient donc que

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \boxplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \overset{\mathbb{Z}_2}{\simeq} \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \boxplus \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

Enfin, la remarque $(*)$ nous permet de terminer la démonstration. •

Corollaire 1.44

Si (M,β) est un module de $\mathscr{S}_n$ de type (II), alors $(M',\beta') \in \mathscr{S}_n$ est de même genre que (M,β) si et seulement si (M',β') est de type (II). Autrement dit, $\mathscr{C}_n$ représente un et un seul genre.

Démonstration :

Si (M',β') est de type (II), alors on a vu au corollaire 1.42 que

$$\beta'_p \overset{\mathbb{Z}_p}{\simeq} <1> \boxplus \cdots \boxplus <1>$$

si $p \neq 2$. Et, si $p = 2$, par le théorème précédent on a :

$$\beta'_2 \overset{\mathbb{Z}_2}{\simeq} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \boxplus \cdots \boxplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

car $\det(\beta') = 1$.

La réciproque est évidente. •

Remarque :

Il faut tout de même signaler que les formes bilinéaires de $\mathscr{S}_n$ de type (II) sont plutôt rares dans les petites dimensions ; le corollaire précédent montre déjà que $n \equiv 0 \bmod 4$, mais on peut montrer qu'en fait $n \equiv 0 \bmod 8$; ceci est démontré dans [10, p. 92].

La forme représentée par la matrice

$$\Gamma_8 = \begin{pmatrix} 2 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & -1 & 0 & 0 & 0 & 0 \\ -1 & 0 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 \end{pmatrix}$$

est le plus simple exemple d'une telle forme.

Modules de type *I*

Lemme 1.45

Si $(M, \beta) \in \mathscr{S}_n$ est de type (I) alors β est $\mathbb{Z}_2$-équivalente à une forme diagonale.

Démonstration :

Par définition, il existe e_1 tel que $\beta(e_1, e_1) = u_1 \in U(\mathbb{Z}_2)$. Donc $\beta \simeq <u_1> \boxplus \beta'$ avec β' non dégénérée.
Si β' représente une unité de $\mathbb{Z}_2$, on continue ; sinon, on considère $(e_2, \ldots, e_n)$ une base de $<e_1>^{\perp}$.
Soit $e_1' = e_1 + e_2$. Clairement $\beta(e_1', e_1') = u_1'$ est impair, car $\beta(e_2, e_2)$ est pair ; donc $\beta \simeq <u_1'> \boxplus \beta''$.
Montrons que β'' est de type (I):
β' étant non dégénérée, il existe $h \in <e_1>^{-}$ tel que $\beta(h, e_2) = 1$. Soit $t = e_1 - u_1 h$; on a

$$\beta(t, t) = \beta(e_1, e_1) + u_1^2 \beta(h, h) = \text{ impair + pair } \in U(\mathbb{Z}_2)$$

puisque on a supposé $\beta(h, h)$ pair. De plus

$$\beta(t, e_1') = \beta(e_1 - u_1 h, e_1 + e_2) = u_1 - u_1 \beta(h, e_2) = 0.$$

En résumé, $t \in <e_1'>^{-}$ et t représente une unité. Donc β'' est de type (I).
On peut donc conclure par récurrence.
Remarquons que tous les éléments de cette diagonale sont impairs, et le produit de ces éléments est 1. •

Définition 1.46

Soit p un nombre premier, (M, β) une forme bilinéaire sur $\mathbb{Q}_p$. On suppose que β est $\mathbb{Z}_p$-équivalente à une forme diagonale

$$<a_1> \boxplus \cdots \boxplus <a_n>.$$

On définit alors

$$c_p(\beta) = \prod_{i<j} (a_i, a_j)$$

où (a_i, a_j) est le symbole de Hilbert. Le nombre $c_p(\beta)$ est appelé *l'invariant de Hasse-Minkowski.*

Lemme 1.47

$c_p(\beta)$ est indépendant de la diagonalisation choisie. En particulier, si deux formes diagonales sont $\mathbb{Z}_p$-équivalentes, alors elles ont le même invariant de Hasse-Minkowski.

Démonstration :

Ce résultat est démontré dans [3, p.57]. •

Théorème 1.48

Si $(M, \beta) \in \mathscr{S}_n$ est de type (I), alors β est $\mathbb{Z}_2$-équivalente à la forme $<1> \boxplus \cdots \boxplus <1>$.

Démonstration :

On peut supposer grâce au lemme 1.45 que notre forme est diagonale.
Soient $c \in \mathbb{Z}_2$ et $a_1, \ldots, a_4 \in U(Z_2)$. Alors il existe une solution à l'équation

$$a_1 x_1^2 + \cdots + a_4 x_4^2 \equiv c \pmod 8$$

En effet, considérons
$A = \{y \mid y = a_1 x_1^2 + a_2 x_2^2,\ x_1, x_2 \in \mathbb{Z}/8\mathbb{Z}\}$ et $B = \{y \mid y = c - a_3 x_3^2 - a_4 x_4^2,\ x_1, x_2 \in \mathbb{Z}/8\mathbb{Z}\}$.

Une vérification directe nous permet de voir que le cardinal de chacun de ces ensembles est au moins 5. On trouve donc que $A \cap B \neq \emptyset$.

Si on applique ce résultat pour $c = 1$ ainsi que le corollaire 1.37, il est clair que

$$\beta \simeq <1> \boxplus \cdots \boxplus <1> \boxplus <a_1> \boxplus <a_2> \boxplus <a_3>$$

avec $\prod a_i \equiv 1 \bmod 8$.

S'il y a deux "5" ou un "1" parmi les a_i, la forme $<a_1> \boxplus <a_2> \boxplus <a_3>$ représente 1, donc nous pouvons poursuivre le procédé ; par contre si les a_i ne sont pas de cette forme, il ne nous reste que le cas $a_1 = 3$, $a_2 = 5$, $a_1 = 7$, (les autres ne sont pas de déterminant 1), mais 1 est représenté par $x_1 = 2$, $x_2 = 1$ et $x_3 = 0$.

Nous avons donc avancé d'un cran, et maintenant

$$\beta \simeq <1> \boxplus \cdots \boxplus <1> \boxplus <a_1> \boxplus <a_2>$$

avec $a_1 \cdot a_2 \equiv 1 \bmod 8$.

Il s'ensuit que $a_1 = a_2 = a$. Si $a = 1$ ou 5, le problème est réglé.

Et puisque $<3> \boxplus <3> \simeq <7> \boxplus <7>$ (la matrice de changement de base est $\begin{pmatrix} 2\alpha & \alpha \\ \alpha & -2\alpha \end{pmatrix}$ avec $\alpha \in U(\mathbb{Z}_2)$ tel que $15\alpha^2 = 7$) il ne nous reste que le cas $a = 3$.

Pour le traiter, nous avons besoin de l'invariant de Hasse-Minkowski avec toute son armada.

Tout d'abord, on a que $c_p(\beta) = 1 \ \forall p \in \mathbb{P}' \setminus \{2\}$ car pour de tels p, on a $\beta \overset{\mathbb{Z}_p}{\simeq} <1> \boxplus \cdots \boxplus <1>$; cela découle du corollaire 1.42 ainsi que d'un théorème connu sur les formes définies positives sur $\mathbb{R}$.

Vu la formule du produit de Hilbert et le lemme précédent, on en déduit que $c_2(\beta) = 1$. Or calculons $c_2(\beta')$ où

$$\beta' = <1> \boxplus \cdots \boxplus <1> \boxplus <3> \boxplus <3> \ :$$

vu le théorème 1.31, on a

$$(3,3)_2 = (-1)^{\frac{(3-1)(3-1)}{4}} = -1 \, ;$$

de plus, $(1,3)_2 = (1,1)_2 = 1$. D'où on a que $c_2(\beta') = -1$; ce qui fait que $\beta \not\simeq \beta'$ en vertu du lemme précédent.

Donc $\beta \simeq <1> \boxplus \cdots \boxplus <1> \boxplus <a>$; mais là, puisque le déterminant vaut 1, on a que $a = 1$. •

Corollaire 1.49

La relation d'équivalence "être dans le même genre que" définie sur $\mathscr{S}_n$ ne comporte que deux classes d'équivalences : les formes de type (II) et les formes de types (I).

Démonstration :

C'est un corollaire immédiat du théorème précédent et du corollaire 1.44. •

G. Enoncé du problème

Nous voilà enfin en mesure de poser clairement le problème.

On se fixe (M, β) un $\mathbb{Z}$-module bilinéaire de $\mathscr{S}_n$, et on pose $V = M \otimes \mathbb{Q}$ et $\mathscr{G}_n$ l'ensemble des classes à isomorphisme près des éléments de $\mathscr{S}_n$ qui sont dans le même genre que (M, β). Le corollaire 1.49 montre que $\mathscr{G}_n = \mathscr{C}_n$ ou $\mathscr{H}_n$.

Le théorème de Hasse-Minkowski nous permet de dire que tous les représentants de ces classes d'équivalences peuvent être vus comme des réseaux bilinéaires de V.

Soient $M_1, \ldots, M_k$ des représentants de chaque classe de $\mathscr{G}_n$

et $O(M_i)$ le groupe orthogonal de M_i $\forall i \in [\![1, k]\!]$. $O(M_i)$ est un groupe fini car isomorphe à un sous-groupe discret du groupe orthogonal de $M_i \otimes \mathbb{R}$ qui est compact.

Nous nous proposons de calculer

$$\mathscr{M}_n = \sum_{i=1}^{k} \frac{1}{|O(M_i)|}.$$

Ce nombre rationnel est appelé *masse de* $\mathscr{G}_n$.

Il existe une formule pour calculer $\mathscr{M}_n$; c'est à la démontration et au calcul de cette formule que seront consacrés les chapitres suivants. Son nom est *la formule de Minkowski-Siegel.*

Remarquons que si nous prenons un module (M, q) où q est une forme quadratique de la forme $\beta(x, x)$ avec $\beta \in \mathscr{S}_n$ et que nous faisons le même travail, nous obtenons les mêmes classes d'équivalences et les mêmes genres que précédemment. De plus, la formule de masse reste la même car les anneaux p-adiques ainsi que $\mathbb{Z}$ sont des anneaux intègres.

CHAPITRE 2
Mesures, masses et formule de Minkowski-Siegel.

Nous allons établir dans ce chapitre la formule de Minkowski-Siegel. Pour cela, il faudra faire un peu de théorie de la mesure sur les groupes orthogonaux.

A. Structure congruentielle et mesure de Haar.

Définitions 2.1

Soit G un groupe et $\mathcal{G}$ une famille de sous-groupes satisfaisant les propriétés suivantes :

(C_1) Si $K_1, K_2 \in \mathcal{G}$, alors il existe $K_3 \in \mathcal{G}$ tel que $K_3 \subset K_1 \cap K_2$.

(C_2) Si K_1 et $K_2 \in \mathcal{G}$ sont tels que $K_1 \subset K_2$, alors l'indice $[K_2 : K_1]$ est fini.

(C_3) Si $K \in \mathcal{G}$ et $u \in G$, alors $u \cdot K \cdot u^{-1} \in \mathcal{G}$.

On dit alors que $\mathcal{G}$ munit G d'une *structure congruentielle*, et les éléments de $\mathcal{G}$ sont appelés *sous-groupes de congruence principaux.*

On définit aussi

$$\mathcal{E} = \{ \bigcup_{i=1}^{n} x_i K_i \mid n \in \mathbb{N},\ x_1, \ldots, x_n \in G \text{ et } K_1, \ldots, K_n \in \mathcal{G} \}.$$

Les éléments de $\mathcal{E}$ sont appelés *ensembles de congruence.*

Proposition 2.2

A) $\mathcal{E}$ est stable par intersection et réunion finies.

B) Si $E_1, \ldots, E_n \in \mathcal{E}$, alors il existe $K \in \mathcal{G}$ tel que pour tout $i \in \mathbb{N}_n$, E_i soit réunion disjointe finie de classes à gauche modulo K.

C) Soit $E \in \mathcal{E}$ et $u \in G$; alors uE, Eu et $u^{-1}Eu \in \mathcal{E}$.

Démonstration :

Soient $E = \bigcup_i x_i K_i$ et $E' = \bigcup_j y_j L_j \in \mathcal{E}$. Il est clair que $E \cup E' \in \mathcal{E}$. De plus, $E \cap E' = \bigcup_{i,j} x_i K_i \cap y_j L_j$.
Or, pour tous sous-groupes H et H' de G, si $xH \cap yH'$ est non vide, on a l'égalité suivante :

$$xH \cap yH' = z(H \cap H') \quad \text{pour tout } z \in xH \cap yH'.$$

Ce résultat s'obtient grâce à une vérification évidente. Donc, on a que $E \cap E' = \bigcup_{i,j} z_{ij}(K_i \cap L_j)$, en supposant que $K_i \cap L_j$ est non vide pour tous i, j. Mais, pour tout sous-groupe de G contenant un K dans $\mathcal{G}$ et tel que $[H : K] < \infty$, on a que $H \in \mathcal{E}$; ceci nous permet de dire que $K_i \cap L_j \in \mathcal{E}$ pour tous i, j, grâce aux axiomes (C_1) et (C_2).

Soient maintenant $E_1, \ldots, E_n \in \mathcal{E}$. Par définition, on a pour tout i :

$$E_i = \bigcup_j x_j K_{ij} \quad \text{avec } K_{ij} \in \mathcal{G}\ \forall i, j$$

L'axiome (C_1) nous permet de prendre un sous-groupe de congruence principal K contenu dans $\bigcap_{ij} K_{ij}$ et l'axiome (C_2) nous permet de dire que K_{ij} est une réunion disjointe finie de classes à gauche modulo K. Le fait que pour tout sous-groupe H de G on ait $xH \cap yH \neq \emptyset \Longrightarrow xH = yH$ nous permet de terminer la démonstration de B).

D'autre part, si E est dans $\mathcal{E}$, alors uE et $u^{-1}Eu \in \mathcal{E}$, et comme $Eu = u(u^{-1}Eu)$, on conclut. •

Définition 2.3

Soit $(G,\mathscr{G})$ un groupe muni d'une structure congruentielle. Une *mesure de Haar* est une application μ de $\mathscr{E}$ dans $\mathbb{P}_+$ telle que :

(I) $\mu \neq 0$

(II) si $E_1, E_2 \in \mathscr{E}$ sont tels que $E_1 \cap E_2 = \emptyset$, alors $\mu(E_1 \cup E_2) = \mu(E_1) + \mu(E_2)$

(III) $\mu(uE) = \mu(E)$ pour tout $u \in G$ et $E \in \mathscr{E}$.

Théorème 2.4

Si G est un groupe muni d'une structure congruentielle $\mathscr{G}$, alors il existe une mesure de Haar, et si μ_1 et μ_2 sont deux mesures de Haar, alors il existe une constante $c > 0$ telle que $\mu_2 = c\mu_1$.

Démonstration :

a) Fixons $E_0 \in \mathscr{E}$ tel que $E_0 \neq \emptyset$. Soit $E \in \mathscr{E}$ quelconque; par la proposition 2.2, on peut choisir $K \in \mathscr{G}$ tel que $E_0 = \bigsqcup_{i=1}^{r} x_i K$ et $E = \bigsqcup_{j=1}^{s} y_j K$. Posons alors $\mu(E) = \frac{s}{r}$. Supposons que $E_0 = \bigsqcup_{i=1}^{r'} x_i' K'$ et que $E = \bigsqcup_{j=1}^{s'} y_j' K'$ et voyons que $\frac{s}{r} = \frac{s'}{r'}$.

Par (C_1), nous savons qu'il existe $L \in \mathscr{G}$ tel que $L \subset K' \cap K$, puis par (C_2), il existe m et $m' \in \mathbb{N}$ tel que

$$K = \bigsqcup_{t=1}^{m} z_t L \quad \text{et} \quad K' = \bigsqcup_{k=1}^{m'} z_k' L$$

donc

$$E_0 = \bigsqcup_{i=1}^{r} \bigsqcup_{t=1}^{m} x_i z_t L = \bigsqcup_{i=1}^{r'} \bigsqcup_{k=1}^{m'} x_i' z_t' L.$$

On a alors que $rm = r'm'$. Par un même raisonnement, on obtient que $sm = s'm'$, d'où $\frac{s}{r} = \frac{s'}{r'}$. Donc μ est bien définie.

Il est clair que $\mu \neq 0$ et que $\mu(uE) = \mu(E)$ pour tout $u \in G$ et $E \in \mathscr{E}$. Soient maintenant E et E' dans $\mathscr{E}$; vu la proposition 2.2, il existe K tel que

$$E_0 = \bigsqcup_{i=1}^{r} x_i K, \quad E = \bigsqcup_{j=1}^{s} y_j K \text{ et } E' = \bigsqcup_{l=1}^{s'} y_l' K.$$

Mais, puisque E et E' sont disjoints, on a que $y_j K \neq y_l' K \ \forall j, l$. Donc

$$E \sqcup E' = \bigsqcup_{i=1}^{s+s'} z_i K$$

où $z_i = y_i \ \forall i \in \mathbb{N}_s$ et $z_{s+i} = y_i' \ \forall i \in \mathbb{N}_{s'}$. Donc finalement,

$$\mu(E \sqcup E') = \frac{s+s'}{r} = \frac{s}{r} + \frac{s'}{r} = \mu(E) + \mu(E').$$

b) Soient μ_1 et μ_2, deux mesures de Haar sur $(G,\mathscr{G})$. Fixons-nous $E_0 \in \mathscr{E}$ tel que $\mu_1(E_0) \neq 0$. Il existe $c \geq 0$ tel que $\mu_1(E_0) = c\mu_2(E_0)$. Soit $E \in \mathscr{E}$, il existe $K \in \mathscr{G}$ tel que $E_0 = \bigsqcup_{i=1}^{r} x_i K$ et $E = \bigsqcup_{j=1}^{s} y_j K$. On a :

$$\mu_1(E) = s\mu_1(K) = \frac{s}{r}\mu_1(E_0) = \frac{s}{r}c\mu_2(E_0) = cs\mu_2(K) = c\mu_2(E).$$

Et, nous voyons que $c > 0$, puisque μ_1 et μ_2 sont non nulles. •

Définition 2.5

Soient G un groupe muni d'une structure congruentielle et μ une mesure de Haar. Définissons

$$\mu_u : \mathscr{E} \longrightarrow \mathbb{R}_+$$
$$E \longmapsto \mu(Eu).$$

C'est clairement une mesure de Haar. Donc, par le lemme précédent, il existe $c(u)$ tel que $\mu_u = c(u)\mu$. On obtient alors une application c de G dans $\mathbb{R}_+$, attachée à la structure congruentielle, et telle que $c(uv) = c(u)c(v)\ \forall u, v \in G$. Cette application s'appelle la *fonction modulaire de* $(G,\mathscr{G})$, et $(G,\mathscr{G})$ est dit *unimodulaire* si c est identiquement 1.

B. Groupe orthogonal et structure congruentielle.

Dans ce paragraphe, nous allons montrer qu'il est possible de définir une structure congruentielle sur le groupe orthogonal d'un espace vectoriel bilinéaire ou quadratique donné.

Définitions 2.6

Fixons-nous, pour le reste de ce paragraphe, A un anneau principal à quotient fini et de caractéristique différente de 2, K son corps des fractions et V un espace vectoriel de dimension n sur K. Munissons V d'une forme bilinéaire non dégénérée β. On notera q, la forme quadratique définie par $q(x) = \beta(x,x)$. Au lieu de partir d'une forme bilinéaire, prenons q une forme quadratique non dégénérée sur V. Posons β définie par $\beta(x,y) = q(x+y) - q(x) - q(y)$. Dans les deux cas, puisque A est intègre et de caractéristique différente de 2, on a $O_q(V) = O_\beta(V)$. Nous noterons ce groupe $O(V)$.
Puisque par la suite, on considérera des espaces quadratiques et des espaces bilinéaires, mais que cela n'influe en rien les raisonnements qui vont suivre, on dira que V est un espace bilinéaire ou quadratique.
Soient $N \subset M$ deux A-réseaux de V; on définit

$$O(V, M/N) = \{u \in O(V) \mid u(M) = M,\ u(N) = N \text{ et } u(x) \equiv x \bmod N\ \forall x \in M\}.$$

et

$$O(V, M) = \{u \in O(V) \mid u(M) = M\}.$$

Ces ensembles sont clairement des sous-groupes de $O(V)$. Si M est un réseau quadratique ou bilinéaire, $O(V, M)$ sera noté $O(M)$.

Soit $\mathscr{G}$ l'ensemble des sous-groupes de $O(V)$ de la forme $O(V, M/aM)$, où $a \in A$ et M est un A-réseau quelconque de V. Nous allons montrer que $\mathscr{G}$ munit $O(V)$ d'une structure congruentielle.

Lemme 2.7

Soient M_1 et M_2, deux A-réseaux. Il existe a et b dans A tels que $aM_1 \subset M_2$ et $bM_2 \subset M_1$.

Démonstration :

On sait qu'il existe $(e_1, \ldots, e_n)$ et $(f_1, \ldots, f_n)$, deux K-bases de V tels que

$$M_1 = Ae_1 \oplus \cdots \oplus Ae_n$$
$$M_2 = Af_1 \oplus \cdots \oplus Af_n.$$

Soient $a_{ij} \in K$ tels que $e_i = \sum_{j=1}^{n} a_{ij} f_j$ pour tout $i \in [\![1, n]\!]$, et a un dénominateur commun des a_{ij}. Nous avons alors

$$ae_i = \sum_{j=1}^{n} a'_{ij} f_j \quad \text{avec } a'_{ij} \in A\ \forall i, j \in [\![1, n]\!],$$

c'est à dire $aM_1 \subset M_2$. •

Remarque :

Si $A = \mathbb{Z}_p$, alors on peut supposer que a et b sont des puissances de p.

Lemme 2.8

Soient M un A-réseau et N un sous-A-module de M; alors N est un A-réseau, si et seulement s'il existe a et b dans K tels que $aN \subset M \subset bN$.

Démonstration :

S'il existe $a, b \in K$ tels que $aN \subset M \subset bN$, alors N est isomorphe à un sous-module de M; il est donc un module de génération finie, car la multiplication par a ou par b est un isomorphisme A-linéaire de N dans aN ou bN. De plus, on a $KN \subset KM \subset KN$, ce qui nous donne $KN = KM = V$; donc N est un A-réseau de V.

La réciproque est évidente grâce aux lemmes précédents. •

Lemme 2.9

Soient M et N, deux A-réseaux de V, alors $M + N$ et $M \cap N$ sont aussi des A-réseaux.

Démonstration :

Le lemme 2.7 nous dit qu'il existe a et $b \in A$ tels que $aM \subset N$ et $bN \subset M$. Or, nous avons immédiatement les inclusions suivantes :

$$b(M + N) \subset bM + bN \subset M \subset M + N$$

et

$$M \cap N \subset M \subset \frac{1}{a}M \cap \frac{1}{a}N = \frac{1}{a}(M \cap N).$$

Ce qui démontre le lemme. •

Proposition 2.10

Soient $O(V, M/bM)$ et $O(V, N/aN) \in \mathscr{G}$. Les lemmes précédents nous donnent l'existence d'un c tel que $c(M + N) \subset aN \cap bM$. Alors on a:

$$O(V, M + N/c(M + N)) \subset O(V, M/bM) \cap O(V, N/aN).$$

Démonstration :

Soient $x \in M$ et $u \in O(V, M + N/c(M + N))$. En particulier, $x \in M + N$, donc $u(x) - x \in c(M + N) \subset bM \subset M$. Ce qui nous donne que $u(x) \in M$ et $u(x) - x \in bM$.

Par un même raisonnement, si $y \in N$, nous obtenons que $u(y) \in N$ et $u(y) - y \in aN$. Nous avons que $u(M) \subset M$; or, $O(V, M + N/c(M + N))$ est un groupe; alors, en faisant le même raisonnement pour u^{-1}, il vient que $u^{-1}(M) \subset M$, donc $M \subset u(M)$. •

Proposition 2.11

Soient $O(V, M/aM) \subset O(V, N/bN) \in \mathscr{G}$. Alors

$$[O(V, N/bN) : O(V, M/aM)] < \infty.$$

Démonstration :

On sait qu'il existe ℓ et $r \in A$ tels que $\ell M \subset N$ et $rN \subset \ell abM$. Une rapide vérification nous permet de montrer les inclusions suivantes :

$$O(V, N/rN) \subset O(V, N/\ell abM) \subset O(V, M/aM) \subset O(V, N/bN).$$

Il suffit donc de démontrer que $[O(V, N/rN) : O(N/bN)]$ est fini.
Nous avons déjà que $rN \subset bN \subset N$. Soit maintenant

$$\varphi : O(V, N/bN) \longrightarrow \mathscr{L}(N/rN)$$
$$u \longmapsto \varphi(u) : N/rN \longrightarrow N/rN$$
$$x + rN \longmapsto u(x) + rN,$$

où $\mathscr{L}(N/rN)$ est le groupe des automorphismes de N/rN, vu comme A/rA-module. On a supposé que A était à quotient fini; donc $\mathscr{L}(N/rN)$ est fini. Notre application φ est bien définie, car tout élément u de $O(V, N/bN)$ est tel que $u(N) = N$, donc $u(rN) = rN$. De plus, φ est clairement un homomorphisme de groupe.
Etudions maintenant le noyau de cet homomorphisme :
Dire que $\varphi(u) = \varphi(v)$ pour $u, v \in O(V, N/bN)$ est équivalent à dire que $u^{-1}v(x) \equiv x \bmod rN$ pour tout $x \in N$ et, comme $u^{-1}v(N) = N$, cela veut dire que $u^{-1}v \in O(V, N/rN)$.
En résumé, on a que $O(V, N/bN)/O(V, N/rN)$ est isomorphe à un sous-groupe de $\mathscr{L}(N/rN)$ qui est fini.
Ce qui démontre la proposition. •

Proposition 2.12

Soient $O(V, M/aM) \in \mathscr{G}$ et $u \in O(V)$. Alors

$$uO(V, M/aM)u^{-1} = O(V, u(M)/a\,u(M))$$

Démonstration :

C'est immédiat. •

Théorème 2.13

L'ensemble $\mathscr{G}$ des sous-groupes de $O(V)$ de la forme $O(V, M/aM)$, où $a \in A$ et M est un A-réseau quelconque de V, munit $O(V)$ d'une structure congruentielle. De plus, $(G, \mathscr{G})$ est unimodulaire. Finalement, si M_1 est un sous-A-réseau de M_2, alors $O(V, M_2/M_1)$ est un ensemble de congruence.

Démonstration :

La première partie de ce théorème est une conséquence directe des propositions 2.10, 2.11 et 2.12.
On a $(G, \mathscr{G})$ est unimodulaire, car $O(V)$ est engendré par les symétries orthogonales relativement aux hyperplans de V. Ce fait est démontré dans [3, lemme 4.3, p. 20]. Puisque ces applications sont d'ordre fini dans $O(V)$, on en déduit que c est identiquement 1, car dans $\mathbb{R}_+$, il n'y a pas de racine de l'unité autre que 1 lui-même.
Pour la dernière partie de ce théorème, on sait qu'il existe $a \in A$ tel que $aM_2 \subset M_1$. De plus, on a que $O(V, M_2/aM_2) \subset O(V, M_2/M_1)$. Si on définit l'application φ de $O(V, M_2/M_1)$ dans $\mathscr{L}(M_2/aM_2)$ comme dans le lemme précédent, on voit que le noyau de cette application est $O(V, M_2/aM_2)$. Puisque $\mathscr{L}(M_2/aM_2)$ est fini, on en déduit que $O(V, M_2/M_1)$ est une réunion disjointe finie de $u_i O(V, M_2/aM_2)$, où $u_i \in O(V)$. •

C. Groupe orthogonal adélique et structure congruentielle.

Fixons-nous, pour ce paragraphe, un $\mathbb{Q}$-espace vectoriel V muni d'une forme bilinéaire ou quadratique non dégénérée. Nous allons montrer qu'il est possible de munir $\widetilde{O}(V)$ d'une structure congruentielle, où $\widetilde{O}(V)$ est le groupe orthogonal adélique que nous définirons tout à l'heure.

Lemme 2.14

Soient M un $\mathbb{Z}$-réseau de V, $\mathscr{R}$ l'ensemble de tous les $\mathbb{Z}$-réseaux de V, et $\mathscr{U}_M$ l'ensemble des familles $(E_p)_{p\in\mathbb{P}}$ formées pour chaque p d'un $\mathbb{Z}_p$-réseau de V_p, telles que $E_p = M_p$ pour tous les p sauf pour un nombre fini (on dira par la suite "pour presque tout p"). Alors l'application

$$f : N \longmapsto (N_p)_{p\in\mathbb{P}}$$

forme une bijection entre $\mathscr{R}$ et $\mathscr{U}_M$, avec

$$f^{-1} : (N_p)_{p\in\mathbb{P}} \longmapsto \bigcap_{p\in\mathbb{P}} (N_p \cap V).$$

Démonstration :

Montrons déjà que notre application f a bien son image dans $\mathscr{U}_M$:
Soit $N \in \mathscr{R}$; nous savons qu'il existe a et $a' \in \mathbb{Z}$ tels que $aN \subset M \subset a'N$. Or, a et a' sont inversibles dans $\mathbb{Z}_p$ pour presque tout p. Donc

$$aN_p = a'N_p = N_p = M_p$$

pour presque tout p, et donc $(N_p)_{p\in\mathbb{P}} \in \mathscr{U}_M$.
Montrons maintenant que $f^{-1} \circ f$ est l'identité de $\mathscr{R}$:
soient $N \in \mathscr{R}$ et $N_p = N \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Il faut voir que $N = \bigcap_{p\in\mathbb{P}}(N_p \cap V)$. Le fait que $N \subset \bigcap_{p\in\mathbb{P}}(N_p \cap V)$ est évident. Soit $x \in \bigcap_{p\in\mathbb{P}}(N_p \cap V)$; puisque $x \in V$, on peut écrire $x = \frac{y}{m}$, avec $y \in N$ et $m > 0$ minimal. Mais $x \in N_p$, donc p ne divise pas m, quel que soit $p \in \mathbb{P}$, ce qui veut dire que $m = 1$ et donc $x = y$.
Il reste à voir que $f \circ f^{-1}$ est l'identité de $\mathscr{U}_M$:
soit $(E_p)_{p\in\mathbb{P}} \in \mathscr{U}_M$; posons $N = \bigcap_{p\in\mathbb{P}}(E_p \cap V)$. Nous allons montrer dans un premier temps que N est un $\mathbb{Z}$-réseau de V, ensuite nous montrerons que $N_p = E_p$ pour tout p.
On sait que pour chaque p, il existe a_p et $b_p \in \mathbb{Q}_p$ tels que $a_pE_p \subset M_p \subset b_pE_p$. On peut choisir $a_p = b_p = 1$ pour presque tout p. Dans les autres cas, on peut choisir une puissance convenable de p.
Posons $a = \prod_{p\in\mathbb{P}} a_p$ et $b = \prod_{p\in\mathbb{P}} b_p$; cela a un sens, et de plus, $aE_p \subset M_p \subset bE_p$ pour tout p. On en déduit que

$$aN \subset M \subset bN,$$

car nous savons que $M = \bigcap_{p\in\mathbb{P}}(M_p \cap V)$. Donc N est un réseau, en vertu du lemme 2.8.
N est inclus dans E_p, donc $N_p \subset E_p$ pour tout p.
Soit maintenant $x \in E_p$, et supposons que $N = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n$; x peut donc s'écrire $\sum_{i=1}^{n} a_ie_i$, avec des $a_i \in \mathbb{Q}_p$. Or, $\mathbb{Z}$ est dense dans $\mathbb{Z}_p$, donc pour chaque i, on peut écrire $a_i = a_i' + \frac{a_i''}{p^m}$, avec $a_i' \in \mathbb{Z}_p$, $a_i'' \in \mathbb{Z}$ et $m \in \mathbb{N}$.
Soit alors $x = x' + x''$, avec $x' = \sum_{i=1}^{n} a_i'e_i$ et $x'' = \sum_{i=1}^{n} \frac{a_i''}{p^m}e_i$. Par construction, on a $x' \in N_p$. De plus, $x'' \in N \subset N_p$, car :

i) $x'' \in V$ et $x'' \in N_q \subset E_q$ pour tout $q \neq p$.

ii) Puisque $N_p \subset E_p$, on a $x'' = x - x' \in E_p$.

On obtient alors que

$$x'' \in \bigcap_{q\in\mathbb{P}} (E_q \cap V) = N$$

et on a bien $x = x' + x'' \in N_p$.

•

Définition 2.15

Soit (V, β), un $\mathbb{Q}$-espace vectoriel bilinéaire ou quadratique non dégénéré. On définit :

$$\widetilde{O}(V) = \{(u_p)_{p\in\mathbb{P}} \in \prod_{p\in\mathbb{P}} O(V_p) \mid \text{ il existe } M, \text{ un } \mathbb{Z}\text{-réseau tel que } u_p \in O(V_p, M_p) \text{ pour presque tout } p\}.$$

Remarquons que si cela est vrai pour un réseau M, c'est vrai pour tout autre réseau N , car $N_p = M_p$ pour presque tout p. Ainsi ce groupe ne dépend que de V.
Soit N, un sous-réseau de M; on définit aussi :

$$\widetilde{O}(V, M/N) = \prod_{p\in\mathbb{P}} O(V_p, M_p/N_p).$$

Nous allons montrer que $\widetilde{\mathscr{G}} = \{\widetilde{O}(V, M/aM) \mid M \in \mathscr{R} \text{ et } c \in \mathbb{Z}\}$ munit $\widetilde{O}(V)$ d'une structure congruentielle.

Lemme 2.16

Soient $\widetilde{O}(V, M/aM)$ et $\widetilde{O}(V, N/bN)$; il existe $c \in \mathbb{Z}$ tel que

$$\widetilde{O}(V, N/cN) \subset \widetilde{O}(V, M/aM) \cap \widetilde{O}(V, N/bN).$$

Démonstration :

On sait qu'il existe $P \subset \mathbb{P}$, P étant de cardinal fini, tel que $M_p = N_p \quad \forall p \in \mathbb{P} \setminus P$.

Si $p \in P$: Il existe r_p et s_p des puissances positives de p, telles que $s_pN_p \subset r_pM_p \subset N_p$. On vérifie facilement que

$$O(V_p, N_p/s_pr_pabN_p) \subset O(V_p, M_p/aM_p) \cap O(V_p, N_p/bN_p).$$

Posons $c = (\prod_{q\in P} s_qr_q)ab$; on a que $cN_p \subset s_pr_pabN_p$. On obtient donc :

$$O(V_p, cN_p) \subset O(V_p, N_p/s_pr_pabN_p).$$

Si $p \notin P$: Dans ce cas, nous avons $M_p = N_p$, et clairement

$$O(V_p, cN_p) \subset O(V_p, M_p/aM_p) \cap O(V_p, N_p/bN_p),$$

c'est à dire que

$$\widetilde{O}(V, N/cN) \subset \widetilde{O}(V, M/aM) \cap \widetilde{O}(V, N/bN).$$

•

Lemme 2.17

Soient $\widetilde{O}(V, M/aM) \subset \widetilde{O}(V, N/bN)$; alors

$$[\widetilde{O}(V, M/bM) : \widetilde{O}(V, N/aN)] < \infty$$

Démonstration :

Comme lors de la proposition 2.11, on voit facilement qu'il existe $r \in \mathbb{Z}$ tel que

$$\widetilde{O}(V, N/rN) \subset \widetilde{O}(V, M/aM) \subset \widetilde{O}(V, N/bN).$$

Il existe $P \subset \mathbb{P}$ fini tel que $rN_p = bN_p = N_p$, sauf si $p \in P$. Posons

$$\varphi : \widetilde{O}(V, N/bN) \longrightarrow \prod_{p\in P} \mathscr{L}(N_p/rN_p)$$
$$(u_p)_{p\in\mathbb{P}} \longmapsto \prod_{p\in P} \overline{u} : N_p/rN_p \longrightarrow N_p/rN_p$$
$$x_p + rN_p \longmapsto u_p(x_p) + rN_p.$$

φ est clairement un homomorphisme de groupe. Regardons son noyau :
soient $(u_p)_{p\in\mathbb{P}}$ et $(v_p)_{p\in\mathbb{P}} \in \widetilde{O}(V, N/rN)$, tels que $\varphi((u_p)_{p\in\mathbb{P}}) = \varphi((v_p)_{p\in\mathbb{P}})$. Cela est équivalent à l'égalité suivante :

$$\prod_{p\in P} u_p(x_p) + rN_p = \prod_{p\in P} v_p(x_p) + rN_p \quad \forall (x_p)_{p\in\mathbb{P}} \in \prod_{p\in p} N_p.$$

C'est aussi équivalent au fait que $u_p^{-1}v_p(x_p) - x_p \in rN_p$ quels que soient $p \in P$ et $x_p \in N_p$. Autrement dit, nous avons que

$$(u_p)_{p\in P}^{-1}(v_p)_{p\in P} \in \prod_{p\in P} O(V_p, N_p/rN_p)$$

et, comme les premiers hors de P ne nous embêtent pas, on trouve

$$(u_p)_{p\in\mathbb{P}}^{-1}(v_p)_{p\in\mathbb{P}} \in \widetilde{O}(V, N/rN).$$

Puisque $\prod_{p\in P} \mathscr{L}(N_p/rN_p)$ est fini, on conclut. •

Lemme 2.18

Soient $u\ (= (u_p)_{p\in\mathbb{P}}) \in \widetilde{O}(V)$ et $\widetilde{O}(V, M/aM) \in \widetilde{\mathscr{G}}$; alors

$$u\widetilde{O}(V, M/aM)u^{-1} = \widetilde{O}(V, u(M)/c \cdot u(M))$$

où $u(M)$ est un réseau, tel que $u(M)_p = u_p(M_p)$; il existe et il est unique en vertu du lemme 2.14.

Démonstration :

Soient $\omega \in \widetilde{O}(V, M/cM)$ et $p \in \mathbb{P}$; alors

$$u_p\omega_p u_p^{-1}(u(M_p)) = u_p\omega_p(M_p) = u_p(M_p).$$

De plus, soit $m_p \in M_p$; on a :

$$u_p\omega_p u_p^{-1}(u_p(m_p)) = u_p(\omega(m_p) - m_p) \in cu_p(M_p)$$

ce qui est équivalent à $\omega_p(m_p) - m_p \in cM_p$. •

Théorème 2.19

Le groupe orthogonal adélique $\widetilde{O}(V)$ est muni par $\mathscr{G}$ d'une structure congruentielle. De plus, $(G, \mathscr{G})$ est unimodulaire.

Démonstration :

Le fait que $\mathscr{G}$ soit une stucture congruentielle découle directement des lemmes 2.16, 2.17 et 2.18.
Soit maintenant $u \in \widetilde{O}(V)$. Nous savons que $\mu(E \cdot u) = c(u)\mu(E)$ pour tout $E \in \mathscr{E}$. Soit N un réseau. Par définition, $u_p \in O(V_p, N_p)$ pour presque tout p. Donc, $u_p(N_p) = N_p$, sauf pour $p \in S$ fini. Posons

$$u_p'' = \begin{cases} id_{V_p} & \text{si } p \in P \\ u_p & \text{si } p \notin P \end{cases} \quad \text{et} \quad u_p' = \begin{cases} id_{V_p} & \text{si } p \notin P \\ u_p & \text{si } p \in P \end{cases}$$

On a donc $u' = (u'_p)_{p\in\mathbb{P}}$ et $u'' = (u''_p)_{p\in\mathbb{P}} \in \widetilde{O}(V)$. De plus, $u = u' \circ u''$, alors $c(u) = c(u')c(u'')$. Montrons que $c(u') = c(u'') = 1$.

u' est l'identité presque partout, et pour les premiers de P, nous savons que u_p est un produit de réflexions. On obtient, par un même raisonnement que pour le théorème 2.13, que $c(u') = 1$.

Par constuction, $u'' \in \widetilde{O}(V, N)$. Puisque pour tout $E \in \mathscr{E}$, $\mu(E \cdot u'') = c(u'')\mu(E)$, cette égalité est vraie en particulier si $E = \widetilde{O}(V, N)$, or on a que $E \cdot u'' = E$ dans ce cas là. Donc $c(u'') = 1$, puisque $\mu(E) \neq 0$.

•

D. Lien entre $O(V)$ et $\widetilde{O}(V)$.

Pour ce paragraphe, ainsi que pour tout le reste du chapitre, on se fixe un $\mathbb{Q}$-espace vectoriel V de dimension n et muni d'une forme bilinéaire ou d'une forme quadratique non dégénérée et définie positive.

Remarquons tout d'abord que $O(V)$ peut être vu comme un sous-groupe de $\widetilde{O}(V)$. En effet, soient $u \in O(V)$ et M un réseau de V; $u_p = u \otimes \mathrm{id}_{\mathbb{Z}_p}$ est bien un élément de $O(V_p)$ pour tout p. De plus, $u_p(M_p) = u(M)_p$ ne diffère de M_p que pour un nombre fini de p.

Lemme 2.20

Soient N un $\mathbb{Z}$-réseau de V et $A_p \in \mathscr{E}_{O(V_p)}$ pour tout $p \in \mathbb{P}$, tel que $A_p = O(V_p, N_p)$ pour presque tout p; alors

$$\prod_{p\in\mathbb{P}} A_p \in \mathscr{E}_{\widetilde{O}(V)}.$$

Démonstration :

Soit $P = \{p \mid A_p \neq O(V_p, N_p)\}$ de cardinal fini. Pour chaque $p \in P$, on a $A_p = \bigsqcup_i x_{p_i} K_p$ où $K_p = O(V_p, N'_p/c_p N'_p)$ et où N'_p est un $\mathbb{Z}_p$-réseau de V_p. Comme toujours, on peut supposer que c_p est une puissance convenable de p. Par le lemme 2.14, il existe un unique $\mathbb{Z}$-réseau M tel que $M_p = N'_p$ si $p \in P$, et $M_p = N_p$ si $p \notin P$.

Posons $K_p = A_p$ si $p \notin P$. On obtient :

$$\prod_{p\in\mathbb{P}} K_p = \widetilde{O}(V, M/cM) \in \mathscr{G}_{\widetilde{O}(V)} \quad \text{où } c = \prod_{p\in P} c_p.$$

Et donc, $\prod_{p\in\mathbb{P}} A_p$ est une réunion finie de classes à gauche modulo $\prod_{p\in\mathbb{P}} K_p$. •

Lemme 2.21

Soit N un $\mathbb{Z}$-réseau de V. Pour tout $p \in \mathbb{P}$, fixons-nous μ_p, une mesure de Haar sur $O(V_p)$, et μ sur $\widetilde{O}(V)$. Supposons que

$$\prod_{p\in\mathbb{P}} \mu_p(O(V_p, N_p))$$

converge absolument. Cette convergence est indépendante du réseau N choisi.

Alors, il existe une constante c positive, telle que pour toute famille $(A_p)_{p\in\mathbb{P}}$, avec $A_p \in \mathscr{E}_{O(V_p)}$ quel que soit p premier et $A_p = O(V_p, N_p)$ sauf pour $p \in P$ fini, on ait :

$$\prod_{p\in\mathbb{P}} \mu_p(A_p) = c\mu(\prod_{p\in\mathbb{P}} A_p).$$

Le membre de droite de cette égalité est bien défini en vertu du lemme précédent.

On en déduit que si les μ_p sont tels que $\prod_{p\in\mathbb{P}} \mu_p$ converge, alors $\prod_{p\in\mathbb{P}} \mu_p$ est une mesure sur $\widetilde{O}(V)$.

Démonstration :

Posons $c > 0$ tel que

$$c\mu(\prod_{p\in\mathbb{P}} O(V_p, N_p)) = \prod_{p\in\mathbb{P}} \mu_p(O(V_p, N_p)).$$

Fixons-nous une famille $(A_p)_{p\in\mathbb{P}}$, telle que $A_p = O(V_p, N_p)$, sauf pour $p \in P = \{p_1, \ldots, p_s\}$. Posons

$$\begin{aligned} \xi_{p_1} \ : \mathscr{B}_{O(V_{p_1})} &\longrightarrow \mathbb{R}_+ \\ B &\longmapsto \mu_{p_1}(B) \cdot \prod_{q\in\mathbb{P}\setminus\{p_1\}} \mu_q(O(V_q, N_q)) \end{aligned}$$

et

$$\begin{aligned} \overline{\xi}_{p_1} \ : \mathscr{B}_{O(V_{p_1})} &\longrightarrow \mathbb{R}_+ \\ B &\longmapsto \mu(B \times \prod_{q\in\mathbb{P}\setminus\{p_1\}} (O(V_q, N_q)). \end{aligned}$$

ξ_{p_1} et $\overline{\xi}_{p_1}$ sont clairement des mesures sur $O(V_{p_1})$. Il existe donc c_{p_1} positif tel que $\xi_{p_1} = c_{p_1}\overline{\xi}_{p_1}$. Cette égalité est vraie, en particulier si $B = O(V_{p_1}, N_{p_1})$. On en déduit alors que $c_{p_1} = c$; donc l'égalité suivante est vérifiée :

$$c\mu(A_{p_1} \times \prod_{q\in\mathbb{P}\setminus\{p_1\}} (O(V_q, N_q)) = \mu_{p_1}(A_{p_1}) \cdot \prod_{q\in\mathbb{P}\setminus\{p_1\}} \mu_q(O(V_q, N_q)).$$

Soient maintenant

$$\begin{aligned} \xi_{p_2} \ : \mathscr{B}_{O(V_{p_2})} &\longrightarrow \mathbb{R}_+ \\ B &\longmapsto \mu_{p_2}(B) \cdot \mu_{p_1}(A_{p_1}) \cdot \prod_{q\in\mathbb{P}\setminus\{p_1,p_2\}} \mu_q(O(V_q, N_q)) \end{aligned}$$

et

$$\begin{aligned} \overline{\xi}_{p_2} \ : \mathscr{B}_{O(V_{p_2})} &\longrightarrow \mathbb{R}_+ \\ B &\longmapsto \mu(B \times A_{p_1} \times \prod_{q\in\mathbb{P}\setminus\{p_1,p_2\}} (O(V_q, N_q)). \end{aligned}$$

De nouveau, il existe c_{p_2}, tel que $\xi_{p_2} = c_{p_1}\overline{\xi}_{p_2}$; on trouve alors que $c_{p_2} = c$. On refait le même procédé jusqu'à p_s, et on trouve :

$$c\mu(\prod_{p\in\mathbb{P}} A_p) = \prod_{p\in\mathbb{P}} \mu_p(A_p).$$

•

E. Domaine fondamental et masse.

Définition 2.22

Soient $(G, \mathscr{G})$ un groupe muni d'une structure congruentielle, O un sous-groupe de G, et $M \in \mathscr{E}$. Si $F \in \mathscr{E}$ est tel que

$$OM = \bigsqcup_{x\in O} xF,$$

F est appelé *domaine fondamental pour M relatif à O.*

Lemme 2.23

Soient G un groupe, H_1, H_2 deux sous-groupes de G, et $x, y \in G$. Si $H_1xH_2 \cap H_1yH_2 \neq \emptyset$, alors

$$H_1xH_2 = H_1yH_2.$$

Démonstration :

C'est une vérification évidente. •

Théorème 2.24

S'il existe $K \in \mathscr{G}$ tel que $O \cap xKx^{-1} = \{1\}$ $\forall x \in G$, alors tout $M \in \mathscr{E}$ possède un domaine fondamental relatif à O. De plus, si F_1 et F_2 sont deux domaines fondamentaux pour M, on a $\mu(F_1) = \mu(F_2)$.

Démonstration :

Soit $M \in \mathscr{E}$; M est une réunion finie de classes à gauche d'un certain $L \in \mathscr{G}$ tel que $L \subset K$. On a

$$M = \bigsqcup_{i=1}^{t} x_i L,$$

et, grâce au lemme précédent,

$$OM = \bigcup_{i=1}^{t} Ox_i L = \bigsqcup_{j=1}^{s} Oy_j L$$

où $\{y_1, \ldots, y_s\} \subset \{x_1, \ldots, x_t\}$. Posons $F = \bigsqcup_{j=1}^{s} y_j L$. On a déjà que $OM = \bigcup_{x \in O} xF$. Il nous reste à voir que la réunion est disjointe :

Soit $v, u \in O$, $v \neq u$. Supposons que $uF \cap vF \neq \emptyset$. On a alors :

$$(\bigsqcup_{j=1}^{s} vy_j L) \cap (\bigsqcup_{j=1}^{s} uy_j L) \neq \emptyset.$$

Donc, puisque les $Oy_j L$ sont disjoints, il existe y_i et $\ell_1, \ell_2 \in L$ tels que $uy_i\ell_1 = vy_i\ell_2$. Mais cela n'est pas possible, car sinon on aurait $1 \neq u^{-1}v = y_i\ell_1\ell_2^{-1}y_i \in y_i L y_i^{-1} \subset y_i K y_i^{-1}$, ce qui est contraire à l'hypothèse.

Suposons maintenant qu'il existe F_1 et $F_2 \in \mathscr{E}$ tels que

$$\bigsqcup_{x \in O} xF_1 = \bigsqcup_{x \in O} xF_2.$$

Il existe $K \in \mathscr{G}$ tel que

$$F_1 = \bigsqcup_{i=1}^{n} x_i K \text{ et } F_2 = \bigsqcup_{j=1}^{m} y_j K.$$

On trouve que

$$\bigsqcup_{i=1}^{n} Ox_i K = \bigsqcup_{j=1}^{m} Oy_j K.$$

Le lemme précédent nous dit alors que $m = n$, donc $\mu(F_1) = \mu(F_2)$. •

Définition 2.25

Soient $(G, \mathscr{G})$ un groupe muni d'une structure congruentielle, μ la mesure associée, O un sous-groupe de G, $M \in \mathscr{E}$, et F un domaine fondamental pour M relatif à O.

On pose

$$m(O\backslash^{OM}) := \mu(F),$$

où $O\backslash^{OM} = \{Ox \mid x \in OM\}$.

On en déduit tout de suite les propriétés suivantes :

Proposition 2.26

a) $m(O\backslash^{OM}) > 0$

b) Soient M_1 et $M_2 \in \mathscr{E}$ tels que $OM_1 \cap OM_2 = \emptyset$. On a :

$$m(O\backslash^{O(M_1 \cup M_2)}) = m(O\backslash^{OM_1}) + m(O\backslash^{OM_2}).$$

Démonstration :

Evident. •

Proposition 2.27

Soient N un $\mathbb{Z}$-réseau de V, et p un nombre premier différent de 2. Alors

$$O(V) \cap \widetilde{O}(V, N/pN) = \{1\}$$

Démonstration :

Soit $1 \neq u \in O(V) \cap \widetilde{O}(V, N/pN)$. En particulier, $u \in \widetilde{O}(V, N) \cap O(V, N)$ d'après le lemme 2.14. Nous savons que $O(V, N)$ est fini puisque β est définie positive; u est alors d'ordre fini. Quitte à prendre une puissance convenable, on peut supposer que u est d'ordre $q \in \mathbb{P}$.
Relativement à une $\mathbb{Z}$-base de N, u est représentée par A une matrice à coefficients entiers. Puisque $u \neq 1$, $A = I + \overline{U}$, où I est la matrice unité, et $\overline{U}$ une matrice quelconque non nulle. Or, pour tout $x \in N$, on a $u(x) - x \in pN$, donc p divise $\overline{U}$. Finalement,

$$A = I + p^m U$$

avec $p \nmid U$ et $m \geq 1$. On obtient alors :

$$I = (I + p^m U)^q = I + q\,p^m U + \cdots \quad \text{Cette somme contient au moins 3 termes.}$$

i) Si $p \neq q$, on a : $q\,p^m U \equiv 0 \bmod p^{2m}$ donc $U \equiv 0 \bmod p^m$; ce qui veut dire que p divise U, ce qui est absurde.

ii) Si $p = q$, on obtient $p^{m+1} \equiv 0 \bmod p^{2m+1}$, car

$$I = I + p^{m+1} U + \binom{p}{2} p^{2m} U^2 + \cdots$$

et p divise $\binom{p}{2}$ puisqu'il est différent de 2. Finalement, on trouve que $U \equiv 0 \bmod p^m$ qui est aussi absurde que tout à l'heure. •

Théorème 2.28

Le groupe adélique $\widetilde{O}(V)$ possède un domaine fondamental relatif à $O(V)$. Il est donc permis de parler de $m(_{O(V)}\backslash^{\widetilde{O}(V)})$.

Démonstration :

Soit $u \in \widetilde{O}(V)$; alors

$$O(V) \cap u\,\widetilde{O}(v, N/pN)u^{-1} \overset{\text{(lemme 2.18)}}{=} O(V) \cap \widetilde{O}(V, u(N)/pu(N)) \overset{\text{(prop.2.27)}}{=} \{1\}.$$

Et on conclut, grâce au théorème 2.24. •

Théorème 2.29

Soient M un réseau quadratique pour la forme $q = \beta(x, x)$, et $\mathscr{M}$ l'ensemble des $\mathbb{Z}$-réseaux de V qui sont dans le même genre que M. L'application

$$\begin{aligned} \varphi : \widetilde{O}(V)/\widetilde{O}(M) &\longrightarrow \mathscr{M} \\ u \bmod \widetilde{O}(M) &\longmapsto u(M) \end{aligned}$$

est bien définie, et de plus, elle est bijective.

Démonstration :

Soit

$$\psi : \widetilde{O}(V) \longrightarrow \mathscr{M}$$
$$u \longmapsto u(M).$$

Rappelons que $u = (u)_{p\in\mathbb{P}}$, et que $u(M)$ est l'unique réseau, tel que $u(M)_p = u_p(M_p)$. Il s'ensuit que $u(M)$ et M sont dans le même genre.

Soient maintenant u et $u' \in \widetilde{O}(V)$, tels que $u\,u^{-1} \in \widetilde{O}(M)$. On a donc que $u_p^{-1}u'_p \in O(M_p)\ \forall p$. Cela est équivalent à :

$$u_p(M_p) = u'_p(M_p)\ \forall p \in \mathbb{P}.$$

D'où, $u'(M) = u(M)$, ce qui veut dire que l'application φ est bien définie.

Soit M' un réseau dans le même genre que M, il existe $u \in \widetilde{O}(V)$ tel que $u_p(M_p) = M'_p$; grâce au lemme 2.14, cela veut dire que $u(M) = M'$. Donc φ est surjective.

Finalement, φ est injective, car si $u\,\widetilde{O}(M)$ et $u'\,\widetilde{O}(M)$ sont tels que $u'_p(M_p) = u_p(M_p)\ \forall p$, alors, cela est équivalent au fait que ${u_p}^{-1}u'_p \in \widetilde{O}(M)$, donc que $u\,\widetilde{O}(M) = u'\,\widetilde{O}(M)$. •

Corollaire 2.30

Soient $a \in \mathbb{Z}$, M un réseau quadratique pour $q = \beta(x,x)$ respectivement pour q si V est quadratique, et $K = \widetilde{O}(V, M/aM)$. On a que $\widetilde{O}(V)$ est une réunion finie de classes doubles $O(V)\,u_i\,K$.

Démonstration :

Il suffit de démontrer ce résultat pour $K = \widetilde{O}(M)$, car les autres sont d'indice fini par rapport à lui.

Posons

$$\psi : O(V)\backslash^{\widetilde{O}(V)}/_{\widetilde{O}(M)} \longrightarrow \overline{\mathscr{M}}$$
$$O(V)\,u\,\widetilde{O}(M) \longmapsto \overline{u(M)}$$

Soient u et $v \in \widetilde{O}(V)$ tels que $O(V)\,u\,\widetilde{O}(M) = O(V)\,v\,\widetilde{O}(M)$. Cette égalité est équivalente à l'existence de $\tau \in O(V)$ et de $\xi \in \widetilde{O}(M)$ tels que $v = \tau\,u\,\xi$, qui est équivalent à $v(M) = \tau(u(M))$; ce qui veut dire que $v(M)$ et $u(M)$ sont isomorphes, ou encore que $\overline{v(M)} = \overline{u(M)}$.

Donc ψ est bien définie et injective.

Soit $M' \in \overline{M'}$ qui est une classe d'ismorphismes dans le genre de M. Le théorème précédent nous donne l'existence d'un $u \in \widetilde{O}(V)$ tel que $\varphi(u\,\widetilde{O}(M)) = M'$, ce qui veut dire que $\psi(O(V)\,u\,\widetilde{O}(M)) = \overline{M'}$. •

F. Représentations.

Définition 2.31

Soient (L, β_L) et (M, β_M) deux $\mathbb{Z}$-modules bilinéaires non dégénérés, libres de rang finis. Un homomorphisme de $\mathbb{Z}$-module u de L dans M tel que $q_M(u(x)) = q_L(x)\ \forall x \in L$ où $q_M = \beta_M(x,x)$ et $q_L = \beta_L(x,x)$ est appelé *représentation de L par M*.

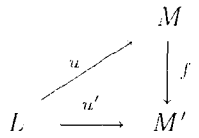
Si L et M sont des $\mathbb{Z}$-modules quadratiques non dégénérés, on défini les représentations de manière identique.

Remarquons que u est injective puisque L est non dégénéré.

Définitions 2.32

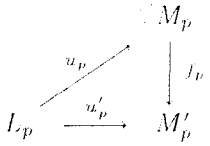
Soient L, M et M'des $\mathbb{Z}$-modules bilinéaires ou quadratiques non dégénérés; soient de plus $u : L \to M$ et $u' : L \to M'$ deux représentations. On dit que u, u' sont *équivalents*, et on écrit $u_1 \simeq u_2$, s'il existe

un isomorphisme f de M dans M' tel que le diagramme



commute. Il en découle en particulier que M_1 et M_2 sont équivalents.

On dit que u, u' sont *de même genre*, et on écrit $u_1 \sim u_2$, si pour tout p premier, il existe un isomorphisme $f_p : M_p \longrightarrow M'_p$ faisant commuter le diagramme suivant :



M et M' sont en particulier dans le même genre.

Lemme 2.33

Supposons que β_M soit définie positive.

1) Il n'existe qu'un nombre fini de représentations de L par M.
2) Il n'existe qu'un nombre fini de classes de représentations de L par des $\mathbb{Z}$-modules du genre de M.

Démonstration :

1) : Soit $a \in \mathbb{Z}$; posons $S_a = \{y \in M \mid q_M(y) = a\}$. Le cardinal de S_a est fini.

En effet, posons $V_{\mathbb{R}} = M \otimes \mathbb{R}$; q_M s'étend naturellement sur $V_{\mathbb{R}}$. Soit $v \in V_{\mathbb{R}}$; posons

$$\|v\| = \sqrt{q_M(v)}.$$

$\|\cdot\|$ est une norme sur $V_{\mathbb{R}}$. Puisque toute les normes sont équivalentes sur $V_{\mathbb{R}}$, on a que M est discret, et donc $S_a = B(0, a^2) \cap M$ est fini.

Si on veut que $q_M(u(x)) = q_L(x)$, on n'a donc qu'un nombre fini de choix pour $u(x)$; et comme u est défini en connaissant les images des vecteurs de bases de L qui sont en nombre fini, on conclut.

2) : On a vu dans le premier chapitre qu'il n'y a qu'un nombre fini de classes d'isomorphisme de $\mathbb{Z}$-module bilinéaire ou quadratique dans un genre donné. Soient donc $M = M_1, M_2, \ldots, M_k$ des représentants des classes d'équivalences dans le genre de M. Posons

$$P = \bigcup_{j=1}^{k} \{u_j \mid u_j \text{ représente } L \text{ dans } M_j\}.$$

Vu 1), nous savons que P est fini. Soit M' tel que $M' \sim M$ et tel qu'il existe u' qui représente L dans M'. On sait qu'il existe $j \in \{1\}_k$ tel que $M_j \simeq M$. Posons $u'_j : L \longrightarrow M_j$, $u_j = f \circ u'$ où f est l'isomorphisme entre M' et M_j. On a alors $u_j \in P$ et $u'_j \simeq u'$. •

Définition 2.34

Soit L un sous-$\mathbb{Z}$-module bilinéaire ou quadratique de M. L'inclusion de L dans M constitue ce que l'on appelle *une représentation spéciale de L par M*.

Remarquons que toute classe d'isomorphisme de repésentation de L par M contient une représentation spéciale; on a même mieux :

Lemme 2.35

Supposons que $V = M \otimes \mathbb{Q}$; alors toute classe de représentation de L par un $\mathbb{Z}$-module du genre de M contient une représentation spéciale de L par un $\mathbb{Z}$-réseau de V.

Démonstration :

Soit $M' \sim M$. Supposons qu'il existe $u : L \longrightarrow M'$, une représentation. Posons $V' = M' \otimes \mathbb{Q}$ et $U = L \otimes \mathbb{Q}$. U est un sous-espace vectoriel de V, et u engendre une application $\widetilde{u}$ de U dans V'. Par le théorème de Witt tel qu'il est vu dans [10, thm. 3, p. 58], $\widetilde{u}$ se prolonge en $\overline{u} : V \longrightarrow V'$, tel que

$$\overline{u} \in O(V, V') \stackrel{\text{def}}{=} \{u : V \longrightarrow V' \mid \beta_{V'}(u(x), u(y)) = \beta_V(x, y) \ \forall x, y \in V\}.$$

Posons $M'' = \overline{u}^{-1}(M')$ et $v : L \longrightarrow M''$ tel que $v = \overline{u}^{-1} \circ u$. Il est clair que $v \simeq u$. •

Définition 2.36

Soient W un sous-espace vectoriel de V, et M un réseau de V. Posons $U = W^{\perp}$.
On définit

$$O(W, M) = \{v \in O(W) \mid (v \oplus \mathrm{id}_U) \in O(V, M)\}.$$

On pose aussi

$$\widetilde{O}(W) = \{(v_p)_{p \in \mathbb{P}} \in \prod_{p \in \mathbb{P}} O(W_p) \mid \text{il existe } M \text{ un réseau de } V \text{ tel que } v_p \in O(W_p, M_p) \text{ pour presque tout } p\}.$$

Et on définit

$$\widetilde{O}(W, M) = \{(v_p)_{p \in \mathbb{P}} \in \widetilde{O}(W) \mid (v_p \oplus \mathrm{id}_{U_p})(M_p) = M_p \ \forall p \in \mathbb{P}\} = \prod_{p \in \mathbb{P}} O(W_p, M_p).$$

Ces ensembles sont clairement des groupes.

Remarque :

Si W est vu comme espace vectoriel "tout nu", lors de la définition 2.15, nous avions défini

$$\widetilde{O}(W) = \{(v_p)_{p \in \mathbb{P}} \in \prod_{p \in \mathbb{P}} O(W_p) \mid \text{il existe } M \text{ un réseau de } W \text{ tel que } v_p \in O(W_p, M_p) \text{ pour presque tout } p\}.$$

Une petite vérification nous permet de voir que ces deux groupes coïncident, donc qu'il n'y a pas d'abus de notation.

Proposition 2.37

On sait que $O(W)$ peut être muni d'une stucture congruentielle. De plus, on a que $O(W, M)$ est un ensemble de congruence de $O(W)$.

Démonstration :

Soit p la projection de V sur W le long de U. On a que $p(M)$ et $W \cap M$ sont des réseaux de W. Il existe donc $a \in \mathbb{Z}$ tel que $a \cdot p(M) \subset W \cap M$. Alors, on a :

$$O(W, p(M)/aP(M)) \subset O(W, M) \subset O(W, p(M)).$$

En prouvant ces inclusions, on prouve la proposition grâce à ce que l'on sait sur les sous-groupes de congruence.

Prouvons la première inclusion :

Soit $v \in O(W, p(M)/a \cdot p(M))$. Il suffit de voir que $(v \oplus \mathrm{id}_U)(M) = M$. Soit $m \in M$. On a que $m = m_U + m_W \in U \oplus W$. Par hypothèse, on a :

$$v(m_W) - m_W \in a\,p(M) \subset W \cap M.$$

Par définition, $(v \oplus \mathrm{id}_U)(m) = v(m_W) + m_U$. Or, comme $m \in M$, il s'ensuit que $(v(m_W) - m_W) + (m_W + m_U) \in M$. Donc, $(v \oplus \mathrm{id}_U)(M) \subset M$. En faisant le même raisonnement pour $(v^{-1} \oplus \mathrm{id}_U)$, on conclut.

Il nous reste à montrer la deuxième inclusion :

Soit $v \in O(W, M)$. Posons p' la projection sur U le long de W. On a :

$$p(M) \boxplus p'(M) = M = (v \oplus \mathrm{id}_U)(M) = v(p(M)) \boxplus p'(M).$$

Donc $v(p(M)) = p(M)$. •

Proposition 2.38

Le groupe $\widetilde{O}(W, M)$ est un ensemble de congruence pour $\widetilde{O}(W)$.

Démonstration :

La démonstration est similaire à celle de la proposition précédente. •

Proposition 2.39

Soient $L \subset M$ deux $\mathbb{Z}$-modules bilinéaires ou quadratiques libres de rang fini. Posons $V = M \otimes \mathbb{Q}$, $U = L \otimes \mathbb{Q}$, et $W = U^{\perp}$. Alors, le nombre de représentations de L par M qui sont dans la même classe d'isomorphismes que l'inclusion $j : L \hookrightarrow M$ est l'indice $[O(V, M) : O(W, M)]$.

Démonstration :

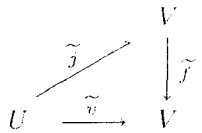
Remarquons que si v est une application linéaire de L dans M, elle se prolonge naturellement en une application linéaire $\widetilde{v}$ de U dans V.

Soient X l'ensemble des représentations de L par M qui sont isomorphes à j, et $Y = O(V, M)/\approx$ où $f \approx g$ si et seulement si $f|_L = g|_L$. Soit

$$\begin{aligned} \varphi : X &\longrightarrow Y \\ v &\longmapsto \overline{f_v}. \end{aligned}$$

L'application f_v est définie comme suit :

nous savons par hypothèse que $v \simeq j$. Il existe donc $\widetilde{f}$ faisant commuter le diagramme suivant :



Il est clair que $\widetilde{f}|_L = v$. Cela veut dire que φ est bien définie et injective.

Montrons la surjectivité :

Soit f un représentant d'une des classes de Y. Posons $v = f|_M \cdot j$; alors $\varphi(v) = \overline{f}$.

D'autre part, soit $f \approx g$; cela est équivalent à $f|_U = g|_U$ ou encore $g f^{-1}|_U = \mathrm{id}_U$. Puisque f et g sont dans $O(V, M)$, cela veut dire que $g \cdot f^{-1} \in O(W, M)$.

Donc $[O(V, M) : O(W, M)]$ compte bien le nombre de représentations de L par M dans la même classe que j. •

Remarques :

1) $\widetilde{O}(W)$ peut être vu comme un sous-groupe de $\widetilde{O}(V)$. En effet, si $v_p \in O(W_p)$, $v_p \oplus \mathrm{id}_{U_p}$ est bien défini sur V_p, et on a

$$q_p((v_p \oplus \mathrm{id}_{U_p})(x)) = q_p(x)$$

car $W = U^{\perp}$.

2) Soit γ l'ensemble des $\mathbb{Z}$-réseaux N de même genre que M et tels que les applications $u_p : M_p \longrightarrow N_p$ vérifient $\overline{u_p}|_{U_p} = \mathrm{id}_{U_p}$, où $\overline{u_p}$ est l'extension naturelle de u_p sur V_p. Alors γ est en bijection avec l'ensemble des représentations de L par M dans le même genre que j.

Ce fait est plus facile à démontrer qu'à énoncer.

Proposition 2.40

On a une bijection entre $\widetilde{O}(W)/\widetilde{O}(W, M)$ et l'ensemble des représentations de L par M dans le même genre que j.

Démonstration :

Par ce qui précède, il suffit de voir que l'application

$$\begin{aligned} \psi : \widetilde{O}(W)/\widetilde{O}(W, M) &\longrightarrow \gamma \\ u\,\widetilde{O}(W, M) &\longmapsto (u \oplus \mathrm{id}_U)(M) \end{aligned}$$

est une bijection.

Soient u et $u' \in \widetilde{O}(W)$, tels que $u\ {}^1u' \in \widetilde{O}(W, M)$. Cela veut dire que

$$(u_p\ {}^1u'_p \oplus \mathrm{id}_{U_p})(M_p) = M_p \ \forall p \in \mathbb{P};$$

ou encore

$$(u \oplus \mathrm{id}_U)(M) = (u_p \oplus \mathrm{id}_{U_p})_{p \in \mathbb{P}}(M) = (u'_p \oplus \mathrm{id}_{U_p})_{p \in \mathbb{P}}(M) = (u' \oplus \mathrm{id}_U)(M).$$

Donc ψ est bien définie et injective.

Soit $M \in \gamma$. Il existe donc $(v_p \oplus \mathrm{id}_{U_p})_{p \in \mathbb{P}} \in \widetilde{O}(V)$ tel que $(v_p \oplus \mathrm{id}_{U_p})_{p \in \mathbb{P}}(M) = M'$.

Finalement, $(v_p)_{p \in \mathbb{P}} \in \widetilde{O}(W)$, et de plus, $\psi((v_p)_{p \in \mathbb{P}}) = M'$. Donc ψ est surjective. •

Corollaire 2.41

Le groupe $\widetilde{O}(W)$ est une réunion de classes doubles $O(W)\, v_i\, \widetilde{O}(W, M)$.

Démonstration :

Posons

$$\begin{aligned} \theta : O(W) \backslash \widetilde{O}(W) / \widetilde{O}(W,M) &\longrightarrow \overline{\gamma} \\ O(W)\, v\, \widetilde{O}(W, M) &\longmapsto \overline{(v \oplus \mathrm{id}_u)(M)}. \end{aligned}$$

Par un raisonnement identique à la démonstration du corollaire 2.30, on voit que θ est injective et bien définie. La proposition précédente nous donne la surjectivité, et, puisque $\overline{\gamma}$ est fini en vertu du lemme 2.33, on conclut. •

G. Formule de Siegel.

Dans ce paragraphe, on se fixe M un $\mathbb{Z}$-réseau quadratique de V, $L \subset M$ un $\mathbb{Z}$-module quadratique libre, U le sous-espace de V engendré par L, et $W = U^{\perp}$.

Lemme 2.42

Soient $(G, \mathscr{G})$ un groupe muni d'une structure congruentielle, $K \in \mathscr{G}$, O un sous-groupe de G, et $u \in G$ tels qu'il existe $F \subset uK$ un domaine fondamental pour uK relatif à O. Ce qui veut dire que :

$$OuK = \bigsqcup_{x \in O} xF$$

alors, on a :

$$uK = \bigsqcup_{y \in O \cap uKu^{-1}} yF$$

Démonstration :

On a bien sûr :

$$uK = OuK \cap uK = \bigsqcup_{x \in O} (xF \cap uK).$$

Si $xF \cap uK \neq \emptyset$, alors $xF \subset uK$. En effet, supposons que $xf = uk$; puisque $F \subset uK$, on peut écrire $f = uk'$. On a donc que $x = uk''u^{-1} \in uKu^{-1}$. Or

$$xF \subset xuK = uk''u^{-1}uK \subset uK.$$

On obtient donc $uK = \bigsqcup_{y \in O \cap uKu^{-1}} yF$. •

Proposition 2.43

Nous savons par le corollaire 2.41 qu'il existe $u_1, \ldots, u_m \in \widetilde{O}(W)$ tels que

$$\widetilde{O}(W) = \bigsqcup_{i=1}^{m} O(W) u_i \widetilde{O}(W, M).$$

Alors, on a :

$$m(O(W)\backslash \widetilde{O}(W)) = \mu(\widetilde{O}(W, M)) \sum_{i=1}^{m} \frac{[O(u_i M) : O(W, u_i M)]}{|O(u_i M)|},$$

où μ est la mesure sur $\mathscr{E}_{\widetilde{O}(W)}$.

Démonstration :

On a :

$$m(O(W)\backslash \widetilde{O}(W)) = \sum_{i=1}^{m} m(O(W)\backslash O(W) u_i \widetilde{O}(W, M)).$$

Le théorème 2.28 nous assure l'existence pour tout $i \in \mathbb{N}_m$ d'un $F_i \in \mathscr{E}_{\widetilde{O}(W)}$ tel que

$$O(W) u_i \widetilde{O}(W, M) = \bigsqcup_{x \in O(W)} xF_i.$$

Le lemme précédent nous permet alors de dire :

$$u_i \widetilde{O}(W, M) = \bigsqcup_{x \in O(W) \cap u_i \widetilde{O}(W, M) u_i^{-1}} xF_i.$$

On vérifie facilement que

$$O(W) \cap u_i \widetilde{O}(W, M) = O(W, u_i M).$$

Or, $m(O(W)\backslash O(W) u_i \widetilde{O}(W, M)) = \mu(F_i)$. Nous savons que

$$u_i \widetilde{O}(W, M) = \bigsqcup_{x \in O(W, u_i M)} xF_i.$$

Donc

$$\mu(F_i) = \frac{\mu(u_i \widetilde{O}(W, M))}{|O(W, u_i M)|} = \frac{\mu(\widetilde{O}(W, M))}{|O(u_i M)|} [O(u_i M) : O(W, u_i M)].$$

•

Remarque :

On a que $L \subset u_i(M)\ \forall i \in \mathbb{H}_m$, car $u_i \in \widetilde{O}(W)$; et on peut voir u_i comme un élément de $\widetilde{O}(V)$ en prenant $u_{i_p} \oplus \mathrm{id}_{U_p}$. Puisque $U_p \supset L_p\ \forall p \in \mathbb{P}$, on a

$$(u_{i_p} \oplus \mathrm{id}_{U_p})(L_p) = L_p \quad \forall p \in \mathbb{P},$$

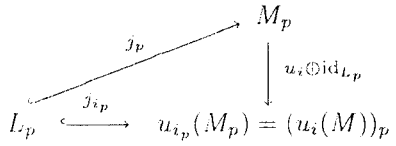
ce qui veut dire que $u_i(L_p) = L_p$.

Proposition 2.44

Les inclusions $j_i \ : \ L \longrightarrow u_i(M)$ constituent un système complet de représentants des classes de représentations qui sont dans le genre de l'inclusion $j : L \longrightarrow M$.

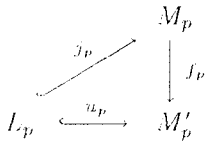
Démonstration :

On a déjà que $L \longrightarrow u_i(M)$ est dans le même genre que $j\ \forall i \in \mathbb{H}_m$; car le diagramme



commute puisque $u_i(L) = L$.

Soit maintenant $u' \ : \ L \longrightarrow M''$ du même genre que j. On sait grâce au lemme 2.35 qu'il existe $u \ : \ L \longrightarrow M'$, une représentation spéciale dans la même classe que u'. Donc quel que soit $p \in \mathbb{P}$, il existe f_p tel que le diagramme



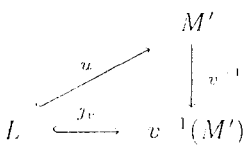
commute. Etant donné que j_p et u_p sont des inclusions, on a que $\widetilde{f}_p \ : \ V_p \longrightarrow V_p$ est telle que $\widetilde{f}_p|_{U_p} = \mathrm{id}_{U_p}$. $\widetilde{f}_p$ s'écrit alors $f'_p \oplus \mathrm{id}_{U_p}$ où $f'_p \in O(W_p)$. Or, $M_p = M'_p$ pour presque tout p, donc $(\widetilde{f}_p)_{p \in \mathbb{P}} \in \widetilde{O}(W)$; on a de plus, $(\widetilde{f}_p)_{p \in \mathbb{P}}(M) = M'$. Nous savons que

$$\widetilde{O}(W) = \bigsqcup_{i=1}^{m} O(W) u_i \widetilde{O}(W, N),$$

donc il existe un unique $i \in \mathbb{H}_m$ tel que :

$$(\widetilde{f}_p)_{p \in \mathbb{P}} = v\, u_i\, v' \quad \text{où } v \in O(W) \text{ et } v' = (v'_p)_{p \in \mathbb{P}} \in \widetilde{O}(W, M).$$

v s'étend en $v \oplus \mathrm{id}_U \in O(V)$, que nous noterons quand même par abus v. Notons j_v l'inclusion de L dans $v^{-1}(M')$. Le diagramme suivant commute :



Or, on a que $M' = (\widetilde{f}_p)_{p\in\mathbb{P}}(M) = v\,u_i\,v'(M)$. Puisque $v' \in \widetilde{O}(W, M)$, on a que $v'(M) = M$. Donc,

$$M' = v\,u_i(M) \text{ ce qui veut dire que } v^{-1}(M') = u_i(M).$$

•

Remarque :

Grâce à la proposition 2.39, nous savons que l'indice $[O(u_i(M)) : O(W, u_i(M))]$ est égal au nombre de représentations de L par $u_i(M)$ qui sont dans la même classe que l'inclusion $L \longhookrightarrow u_i(M)$.

Définition 2.45

On sait qu'il est possible de choisir $M = M_1, \ldots, M_k$ des représentants des classes d'isomorphismes dans le genre de M. Soit $s \in \mathbb{H}_k$. Posons $a(L, M_s)$, le nombre de représentations de L par M_s dans le genre de $j : L \longhookrightarrow M$.

Proposition 2.46

Soit $s \in \mathbb{H}_k$; alors on a :

$$a(L, M_s) = \sum_{i\in I}[O(u_i(M)) : O(W, u_i(M))]$$

où $I = \{i \in \mathbb{H}_m \mid u_i(M) \simeq M_s\}$. ($I$ peut être éventuellement vide.)

Démonstration :

Soient $i_1, \ldots, i_r$ tels que $u_{i_j}(M) \simeq M_s\ \forall j \in \mathbb{H}_r$. Pour tout $j \in \mathbb{H}_r$, on se fixe un isomorphisme g_j de $u_{i_j}(M)$ dans M_s préservant les formes quadratiques, ainsi que $h_j : L \longrightarrow M_s$ qui est la composition de l'incusion de L dans $u_{i_j}(M)$ avec g_j.

Nous allons tout d'abord montrer que l'ensemble des h_j constitue un système complet de représentants de représentations de L par M_s qui sont dans le même genre que l'inclusion $j : L \longhookrightarrow M$. (∗)

En effet, soit $u : L \longrightarrow M_s$ de même genre que l'inclusion de L dans M. Vu la proposition 2.44, il existe un unique $j \in \mathbb{H}_r$ et $f_j : M_s \longrightarrow u_{i_j}(M)$, tels que $f_j\,u$ soit l'inclusion de L dans $u_{i_j}(M)$. Or, par construction, $g_j^{-1}\,h_j$ est aussi égale à l'inclusion de L dans $u_{i_j}(M)$. Donc, $(g_j\,f_j)\,u = h_j$; ce qui veut dire que $u \simeq h_j$.

Soit $j \in \mathbb{H}_r$. Posons X_j, l'ensemble des représentations de L par $u_{i_j}(M)$ qui sont dans la même classe que l'inclusion $L \longhookrightarrow u_{i_j}(M)$, et Y_j, l'ensemble des représentations de L par M_s qui sont dans la classe de h_j. Alors, l'application

$$\begin{aligned} \psi : X_j &\longrightarrow Y_j \\ u &\longmapsto g_j\,u \end{aligned}$$

est une bijection. (∗∗)

Le fait que ψ soit bien définie et injective se démontre de la même manière que (∗). Soit $v \in Y_j$; il est clair que $g_j^{-1}\,v$ est dans X_j; donc ψ est bijective.

Finalement, on a :

$$a(L, M_s) \overset{(*)}{=} \sum_{j=1}^{r} |X_j| = \sum_{i\in I}[O(u_i(M) : O(W, U_i(M)].$$

La deuxième égalité est une conséquence directe de (∗∗) et de la remarque précédant la définition 2.45. •

Théorème 2.47

On a l'égalité :

$$m(O(W)\backslash\widetilde{O}(W)) = \mu(\widetilde{O}(W,M))\sum_{s=1}^{m}\frac{a(L,M_s)}{|O(M_k)|}.$$

Démonstration :

C'est un corollaire immédiat des propositions 2.43 et 2.46. •

Définition 2.48

Cette égalité est appelée *formule de Minkowski-Siegel*. Nous nous intéresserons plus particulièrement à un cas particulier de cette formule :

Corollaire 2.49

Si $L = U = \{0\}$, alors quel que soit $s \in \mathbb{N}_k$, il est clair que $a(L,M_s) = 1$ est que $V = W$. De plus, on a vu au paragraphe D que $\prod_{p\in\mathbb{P}}\mu_p$ forme une mesure $\widetilde{O}(V)$. On obtient alors :

$$\sum_{s=1}^{m}\frac{1}{|O(M_s)|} = m(O(V)\backslash\widetilde{O}(V))\prod_{p\in\mathbb{P}}\mu_p(O(M_p))^{-1}.$$

Cette égalité n'est vraie que si $\prod_{p\in\mathbb{P}}\mu_p$ converge. Le paragraphe suivant sera consacré à fixer les μ_p pour tout p de telle manière que ce produit converge.

H. Normalisation des μ_p.

Lemme 2.50

Soient $p \in \mathbb{P}$ et $V_p = V \otimes \mathbb{Q}_p$ où V est notre $\mathbb{Q}$-espace vectoriel bilinéaire ou quadratique, de dimension n et défini positif. Soient $L \subset M$ deux $\mathbb{Z}_p$-réseaux de V_p, et $u : L \longrightarrow M$ une injection linéaire telle que $L^* = \beta_q(u(\cdot), M)$. Supposons qu'il existe $k \in \mathbb{N}$ tel que $p^{k-1}q(M) \subset \mathbb{Z}_p$ et tel que $q(u(x)) \equiv q(x) \bmod p^k$. Alors, il existe $u' : L \longrightarrow V_p$ linéaire, telle que $u'(x) \equiv u(x) \bmod p^k M$ pour tout $x \in L$, et $q(u'(x)) \equiv q(x) \bmod p^{k+1}$.

Démonstration :

Soit $f : L \longrightarrow M$ à déterminer, linéaire, telle que $u'(x) = u(x) + p^k f(x)$. D'autre part, il existe $g : L \longrightarrow \mathbb{Z}_p$ telle que $q(u(x)) = q(x) + g(x)p^k$. Les égalités suivantes sont satisfaites :

$$\begin{aligned}\beta_q(x,y) + q(x) + q(y) + g(x+y)p^k &= q(x+y) + g(x+y)p^k = q(u(x+y)) = q(u(x)+u(y))\\ &= \beta_q(u(x),u(y)) + q(u(x)) + q(u(y))\\ &= \beta_q(u(x),u(y)) + q(x) + g(x)p^k + q(y) + g(y)p^k.\end{aligned}$$

Donc,

$$g(x+y) - g(x) - g(y) = p^{-k}(\beta_q(u(x),u(y)) - \beta_q(x,y)) \in \mathbb{Z}_p \quad \forall x,y \in L. \quad (*)$$

Il existe une forme bilinéaire $\gamma : L \times L \longrightarrow \mathbb{Z}_p$, non forcément symétrique, telle que $\gamma(x,x) = g(x)\ \forall x \in L$. Calculons :

$$\begin{aligned}q(u'(x)) = q(u(x) + p^k f(x)) &= \beta_q(u(x),f(x)) + q(u(x)) + p^{2k}q(f(x))\\ &= p^k\beta_q(u(x),f(x)) + q(x) + p^k\gamma(x,x) + p^{2k}q(f(x))\\ &\equiv q(x) + p^k(\beta_q(u(x),f(x)) + \gamma(x,x)) \pmod{p^{k+1}}.\end{aligned}$$

Il nous faut donc trouver f telle que

$$\beta_q(u(x), f(x)) \equiv -\gamma(x,x) \pmod{p}.$$

Fixons $y_0 \in L$. La forme $-\gamma(x, y_0)$ est un élément de L^*. Par hypothèse, il existe $f(y_0) \in M$ tel que $-\gamma(x, y_0) \equiv \beta_q(u(x), f(y_0)) \bmod p$. Soient $y_0, y_1 \in L$, on a :

$$\beta_q(u(x), f(y_0+y_1)) = -\gamma(x, y_0+y_1) = -(\gamma(x,y_0)+\gamma(x,y_1)) = -(\beta_q(u(x), f(y_0)) + \beta_q(u(x), f(y_1))).$$

Ce qui veut dire que

$$\beta_q(u(x), f(y_0+y_1) - f(y_0) - f(y_1)) = 0$$

ceci, quel que soit x. Or, u est injective, donc son image contient un base de V_p. De plus β_q est non dégénérée. Donc f est linéaire. •

Nous allons déterminer au lemme suivant le nombre d'applications f modulo pM que nous cherchions lors de la démonstation du lemme précédent, donc le nombre possible de u' modulo $p^{k+1}M$ satisfaisant la conclusion de ce lemme.

Lemme 2.51

Dans les mêmes hypothèses que pour le lemme précédent; on a exactement $p^{\frac{n(n-1)}{2}}$ possibilités pour f modulo pM.

Démonstration :

Soit $\mathbb{F}_p = \mathbb{Z}_p/p\mathbb{Z}_p$. L et M peuvent être vus comme des $\mathbb{F}_p$-espaces vectoriel. Posons $\mathscr{L}_{\mathbb{F}_p}(L, M)$ l'espace des applications linéaires de L dans M, et $\mathscr{B}_{\mathbb{F}_p}(L, \mathbb{F}_p)$ celui des formes bilinéaires symétriques de $L \times L$ dans $\mathbb{F}_p$. L'application

$$\begin{aligned} \theta : \mathscr{L}_{\mathbb{F}_p}(L, M) &\longrightarrow \mathscr{B}_{\mathbb{F}_p}(L, \mathbb{F}_p) \\ g &\longmapsto \beta_q(u(\cdot), g(\cdot)) \end{aligned}$$

est clairement linéaire et surjective, car β_q est non dégénérée et u est injective. Par le théorème du rang, on a que la dimension du noyau de θ vaut $n^2 - \frac{n(n+1)}{2} = \frac{n(n-1)}{2}$. Donc, il existe $p^{\frac{n(n-1)}{2}}$ éléments de $\mathscr{L}_{\mathbb{F}_p}(L, M)$ qui vont sur le $-\gamma(x,x)$ du lemme précédent. •

Lemme 2.52

Soient L, M dans V_p, et u comme au lemme 2.50. Alors il existe $\overline{u} : L \longrightarrow V_p$ linéaire, telle que $\overline{u}(x) \equiv u(x) \bmod p^k M$ et telle que $q(\overline{u}(x)) = q(x)$ quel que soit x dans L.

Démonstration :

Par le lemme 2.50, il existe u' tel que $u'(x) \equiv u(x) \bmod p^k M$ et $q(u'(x)) \equiv q(x) \bmod p^{k+1}$. Or, on a que $\beta_q(u'(\cdot), M) = \beta_q(u(\cdot), M) + p^k \beta_q(f(\cdot), M) = L^*$. Donc, u' satisfait les conditions du lemme 2.50 mais pour $k+1$ cette fois-ci. Il existe alors u'' tel que :

$$\begin{aligned} u''(x) &\equiv u'(x) \pmod{p^{k+1}M} \\ q(u''(x)) &\equiv q(x) \pmod{p^{k+2}}. \end{aligned}$$

Par induction, il est donc possible de se définir pour tout $n \in \mathbb{N}$, une application linéaire $u^{(n)} : L \longrightarrow V_p$ telle que :

$$\begin{aligned} u^{(n)}(x) &\equiv u^{(n-1)}(x) \pmod{p^{k+n-1}M} \\ q(u^{(n)}(x)) &\equiv q(x) \pmod{p^{k+n}}. \end{aligned}$$

Posons $\overline{u} = \lim_{n \to \infty} u^{(n)}(x)$. Cela a un sens, car V_p est homéomorphe à $\mathbb{Z}_p^n$ qui est complet, et il est simple de voir que la suite $(u^{(n)})_{n \in \mathbb{N}}$ est de Cauchy. On a donc que $\overline{u}$ est linéaire . De plus $q(\overline{u}(x)) = q(x)\ \forall x$, car la suite $q(u^{(n)}(x)) - q(x)$ converge vers 0 dans $\mathbb{Z}_p$. •

Proposition 2.53

Soient M un $\mathbb{Z}$-réseau quadratique de V, $p \in \mathbb{P}$, et $k \in \mathbb{N}^*$ tel que $p^k M_p^\# \subset M_p$ et tel que $p^{k-1} q(M_p^\#) \subset \mathbb{Z}_p$. Alors

$$\frac{\mu_p(O(V_p, M_p/p^k M_p^\#))}{\mu_p(O(V_p, M_p/p^{k+1} M_p^\#))} = p^{\frac{n(n-1)}{2}}.$$

Où μ_p est une mesure sur $O(V_p)$.

Démonstration :

Par propriété de μ_p, il suffit de montrer que l'indice $[O(V_p, M_p/p^k M_p^\#) : O(V_p, M_p/p^{k+1} M_p^\#)]$ vaut $p^{\frac{n(n-1)}{2}}$.

Posons u, l'inclusion $M_p \hookrightarrow M_p^\#$. Il est clair que M_p, $M_p^\#$ et u satisfont la donnée des lemmes précédents. L'ensemble des applications $\overline{u}$ trouvées lors du lemme 2.52 n'est autre que $O(V_p, M_p/p^k M_p^\#)$. Le lemme 2.51 nous permet de conclure sachant que les u' du lemme 2.50 sont congrus aux $\overline{u}$ modulo $p^{k+1} M$. •

Lemme 2.54

Soient L et M deux $\mathbb{Z}_p$-réseaux de V_p tels que $[M : L] = p$. Alors on peut trouver $e_1, \ldots, e_n \in V_p$ tels que $M = \sum_{i=1}^{n} \mathbb{Z}_p e_i$ et $L = \sum_{i=1}^{n-1} \mathbb{Z}_p e_i + p\mathbb{Z}_p e_n$.

Démonstration :

On a que M/L est un groupe additif à p éléments, il est donc engendré par un élément $\overline{x}$. Soit x un représentant de $\overline{x}$. Par choix de x, px est dans L, mais pas x lui-même; px est donc primitif. Il existe alors $e_1, \ldots, e_{n-1}$ tels que $(e_1, \ldots, e_{n-1}, px)$ soit une base de L. Il est clair que $(e_1, \ldots, e_{n-1}, x)$ engendre M, car $M = \bigsqcup_{i=1}^{p} ix + L$. •

Lemme 2.55

Soient L et M deux $\mathbb{Z}_p$-réseaux de V_p tels que $[M : L] = p$. Alors $[L^\# : M^\#] = p$.

Démonstration :

Prenons $e_1, \ldots, e_n$ tels que $M = \sum_{i=1}^{n} \mathbb{Z}_p e_i$ et $L = \sum_{i=1}^{n-1} \mathbb{Z}_p e_i + p\mathbb{Z}_p e_n$. Soient $c_1, \ldots, c_n$, définis lors de la proposition 1.21, tels que $M^\# = \sum_{i=1}^{n} \mathbb{Z}_p c_i$. On a :

$$L^\# = \sum_{i=1}^{n-1} \mathbb{Z}_p c_i + \mathbb{Z}_p c_n'.$$

Et, en se souvenant de la définition des c_i, on voit facilement que $c_n' = p^{-1} c_n$. •

Proposition 2.56

Soient L, M, deux $\mathbb{Z}_p$-réseaux de V_p tels que $[M : L] = p$, et $k \in \mathbb{N}^*$ tel que $p^{k-1} M^\# \subset M$, $p^{k-1} L^\# \subset L$ et $2k - 4 \geq k$, alors :

$$[O(V_p, L/p^k L^\#) : O(V_p, M/p^k M^\#)] = p^{n-1}$$

Démonstration :

Choisissons-nous $e_1, \ldots, e_n$ tels que $M = \sum_{i=1}^{n} \mathbb{Z}_p e_i$, $L = \sum_{i=1}^{n-1} \mathbb{Z}_p e_i + p\mathbb{Z}_p e_n$, $M^\# = \sum_{i=1}^{n} \mathbb{Z}_p c_i$ et $L^\# = \sum_{i=1}^{n-1} \mathbb{Z}_p c_i + p^{-1}\mathbb{Z}_p c_n$.

Soit $u \in O(V_p, L/p^k L^\#)$. Pour tout $i \in \mathbb{N}_{n-1}$, on a :

$$u(e_i) = e_i + x_i \quad \text{avec } x_i \in p^k L^\#.$$

Puisque $[p^k L^\# : p^k M^\#] = p$, le nombre des images $u(e_i)$ modulo $p^k M^\#$ possible est au plus de p pour chaque $i \in \mathbb{N}_{n-1}$; donc en tout p^{n-1}.

Lemme

Soient u et $u' \in O(V_p, L/p^k L^\#)$. Si

$$u(e_i) = e_i + x_i,\ x_i \in p^k L^\#$$
$$\text{et} \quad u'(e_i) = e_i + x_i',\ x_i' \in p^k L^\#\ \forall i \in \mathbb{N}_{n-1}$$

sont tels que $x_i \equiv x_i' \bmod p^k M^\#$. Alors, $u \equiv u' \bmod O(V_p, M/p^k M^\#)$.

Ce lemme implique que l'indice cherché est inférieur ou égal à p^{n-1}.

Démonstration du lemme :

Puisque $x_i \equiv x_i' \bmod p^k M^\#$, il est clair que $u'(e_i) \equiv u(e_i) \bmod p^k M^\#$, donc que $(u^{-1}u')(e_i) \equiv e_i \bmod u^{-1}(p^k M^\#)\ \forall i \in \mathbb{N}_{n-1}$. Or, dans notre cas, $u^{-1}(p^k M^\#)$ est égal à $p^k M^\#$. Pour voir cela, il suffit de montrer que $\beta_q(u(c_i), e_j) \in \mathbb{Z}_p \quad \forall i, j \in \mathbb{N}_n$.

1) Si $j \neq n$, $e_j \in L$, et $c_i \in L^\#$ quel que soit i; alors, $\beta_q(u(c_i), e_j) \in \mathbb{Z}_p$.
2) Si $i = j = n$, on a que $p^{-1}c_n \in L^\#$ et $pc_n \in L$. Donc, $\beta_q(u(c_n), e_n) = \beta_q(u(p^{-1}c_n), p\,e_n) \in \mathbb{Z}_p$.
3) Si $i \neq n = j$, vu la définition des c_i, il est clair que $\beta_q(u(c_i), u(e_n)) = \beta_q(c_i, e_n) = 0$. Donc, $\beta_q(u(c_i), e_n) = \beta_q(u(c_i), e_n - u(e_n))$. Or, $pe_n - u(pe_n) \in p^k L^\#$, ce qui veut dire que $e_n - u(e_n) \in p^{k-1}L^\# \subset L$. On a alors $\beta_q(u(c_i), e_n) \in \mathbb{Z}_p$ puisque $u(c_i) \in L^\#$.

Il reste à montrer que $(u^{-1}u')(e_n) := \overline{u}(e_n) \equiv e_n \bmod p^k M^\#$.

On sait que $\overline{u}(e_n) - e_n \in M^\#$, donc, $\overline{u}(e_n) - e_n = \sum_{i=1}^{n} t_i c_i$ avec $t_i \in \mathbb{Z}_p$. Il reste à voir que $t_i \in p^k\mathbb{Z}_p$. Or, $pe_n \in L$, donc $\overline{u}(pe_n) - pe_n \in p^k L^\#$. On a alors $\sum_{i=1}^{n} p t_i c_i \in p^k L^\#$. Cela veut dire que $t_n \in p^{k-2}\mathbb{Z}_p$ et que $t_i \in p^{k-1}\mathbb{Z}_p$.

D'autre part, on a que $\beta_q(\overline{u}(e_i), \overline{u}(e_n)) = \beta_q(e_i, e_n)$ pour tout $i \in \mathbb{N}_n$. Il est facile de voir que $\overline{u}(e_i) = e_i + u^{-1}(x_i' - x_i)\ \forall i \in \mathbb{N}_{n-1}$; donc, $\overline{u}(e_i) - e_i \in p^k M^\#$. De plus, $\overline{u}(e_n) - e_n \in L \subset M$; alors, $\overline{u}(e_n) \in M$. Finalement, on obtient :

$$\beta_q(e_i, e_n) = \beta_q(\overline{u}(e_i), \overline{u}(e_n)) \equiv \beta_q(e_i, \overline{u}(e_n)) = \beta_q(e_i, e_n) + t_i \pmod{p^k} \quad \forall i \in \mathbb{N}_{n-1}.$$

Donc, $t_i \in p^k\mathbb{Z}_p\ \forall i \in \mathbb{N}_{n-1}$.

Occupons-nous maintenant de t_n, on a :

$$q(u(e_n)) = q(e_n + \sum_{i=1}^{n} t_i c_i) = q(e_n) + q(\sum_{i=1}^{n} t_i c_i) + \beta_q(e_n, \sum_{i=1}^{n} t_i c_i)$$
$$= q(e_n) + q(\sum_{i=1}^{n} t_i c_i) + t_n \equiv q(e_n) + t_n \pmod{p^{k-2}\mathbb{Z}_p}.$$

La dernière équivalence vient du fait que chacun des t_i est au moins divisible par $k-2$, et parce que $2k - 4 \geq k$. Donc $t_n \in p^{k-2}\mathbb{Z}_p$. Ainsi s'achève la démonstration du lemme.

Terminons la preuve de notre proposition :

L'indice $[M : pM]$ vaut p^n. En multipliant successivement par p chaque élément de la base de M, il est possible de trouver une chaîne de réseaux $L_0 = M \supset L_1 \supset \cdots \supset L_n = pM$ tels que $[L_i : L_{i+1}] = p$. Par le lemme, on a que :

$$[O(V_p, L_i/p^k L_i^\#) : O(V_p, L_{i-1}/p^k L_{i-1}^\#)] \leq p^{n-1} \quad \forall i.$$

Grâce à la multiplicativité des indices, on trouve :

$$[O(V_p, pM/p^k(pM)^\#) : O(V_p, M/p^k M^\#)] \leq p^{n(n-1)}.$$

Or, $O(V_p, pM/p^k(pM)^\#) = O(V_p, M/p^{k-2}M^\#)$, et la proposition 2.53 nous dit que

$$[O(V_p, M/p^{k-2}M^\#) : O(V_p, M/p^k M^\#)] = p^{n(n-1)}.$$

On peut conclure, de nouveau grâce à la multiplicativité des indices. •

Définition 2.57

Soient M un réseau quadratique de V, $p \in \mathbb{P}$, k tel que $p^k M_p^\# \subset M_p$ et μ_p une mesure sur $O(V_p)$. Posons

$$c_{\mu,p} = \mu_p(O(V_p, M_p/p^k M_p^\#)) \cdot [M_p : p^k M_p^\#]^{\frac{n-1}{2}}.$$

On pourrait se demander pourquoi $c_{\mu,p}$ ne s'appelle pas plutôt $c_{\mu,p,k,M}$. Nous allons voir dans le thèorème prochain que si k est assez grand, alors $c_{\mu,p}$ est constant, et que de plus il est indépendant du réseau quadratique M choisi.

Théorème 2.58

Si k est tel que $p^{k-1}q(M_p^\#) \subset \mathbb{Z}_p$ et $p^k M_p^\# \subset M_p$, alors $c_{\mu,p}$ est constant quand k croît, il est en outre indépendant du réseau quadratique choisi.

Démonstration :

On a vu à la proposition 2.53 que

$$\frac{\mu_p(O(V_p, M_p/p^k M_p^\#))}{\mu_p(O(V_p, M_p/p^{k+1} M_p^\#))} = p^{\frac{n(n-1)}{2}}.$$

De plus, on a :

$$[M_p : p^{k+1} M_p^\#]^{\frac{n-1}{2}} = [M_p : p^k M_p^\#]^{\frac{n-1}{2}} \cdot [p^k M_p^\# : p^{k+1} M_p^\#]^{\frac{n-1}{2}} = [M_p : p^k M_p]^{\frac{n-1}{2}} \cdot p^{\frac{n(n-1)}{2}}.$$

Donc, $c_{\mu,p,k,M} = c_{\mu,p,k-1,M}$.

Soient L et M deux $\mathbb{Z}$-réseaux quadratiques de V tels que $L_p \subset M_p$. Un bref raisonnement nous permet de dire qu'il existe $s \in \mathbb{N}$ tel que $[M_p : L_p] = p^s$. Il suffit donc de montrer que $c_{\mu,p,M} = c_{\mu,p,L}$ avec $[M_p : L_p] = p$. Puisque nous venons de voir que notre $c_{\mu,p}$ était constant si k croît, on peut supposer k assez grand de telle manière que les hypothèses de la proposition 2.56 soient satisfaites. il s'ensuit alors que

$$\frac{\mu_p(O(V_p, L_k/p^k L_p^\#)}{\mu_p(O(V_p, M_p/p^k M_p^\#)} = p^{n(n-1)}.$$

Mais, on a les égalités suivantes :

$$\begin{aligned}[M_p : p^k M_p^\#]^{\frac{n-1}{2}} &= [M_p : L_p]^{\frac{n-1}{2}} \cdot [L_p : p^k L_p^\#]^{\frac{n-1}{2}} \cdot [p^k L_p^\# : p^k M_p^\#]^{\frac{n-1}{2}} \\ &\overset{\text{lemme 2.55}}{=} p^{\frac{n(n-1)}{2}} \cdot [L_p : p^k L_p^\#]^{\frac{n-1}{2}} \cdot p^{\frac{n(n-1)}{2}} \\ &= p^{n(n-1)} \cdot [L_p : p^k L_p^\#]^{\frac{n-1}{2}}.\end{aligned}$$

Donc, $c_{\mu,p,M} = c_{\mu,p,L}$. •

Nous sommes près maintenant à normaliser nos μ_p. Rappelons qu'il faut fixer les mesures μ_p de telle sorte que

$$\prod_{p \in \mathbb{P}} \mu_p(O(M_p))^{-1}$$

converge. Il est clair que $M_p = M_p^\#$ pour presque tout p, il suffit donc de voir que le produit converge pour de tels p. Pour ces p, on peut choisir $k = 1$ dans le théorème précédent. Personne ne peut m'empêcher de dire que :

$$\mu_p(O(M_p)) = [O(M_p) : O(V_p, M_p/pM_p^\#)] \cdot \mu_p(O(V_p, M_p/pM_p^\#)).$$

On trouve alors, grâce au théorème précédent que

$$\mu_p(O(V_p, M_p/pM_p^\#)) = c_{\mu,p} \cdot [M_p : pM_p]^{\frac{1-n}{2}} = c_{\mu,p} \cdot p^{\frac{n(1-n)}{2}}.$$

D'autre part, posons $\overline{M_p}$ qui est M_p/pM_p vu comme $\mathbb{F}_p$-espace vectoriel, et posons aussi $O(\overline{M_p})$ le groupe orthogonal pour la forme héritée de celle de V_p. Si $p \neq 2$, il est clair que le groupe orthogonal quadratique coïncide avec le groupe orthogonal bilinéaire. Si $p = 2$ est un "bon premier", on pose $O(\overline{M_2})$ comme étant le groupe orthogonal quadratique sur $\overline{M_2}$, car notre forme quadratique n'est pas issue d'une forme bilinéaire . En effet, puisque $M_2 = M_2^{\#}$ et que l'on a toujours que $[M_2^{\#} : M_2] = \det \beta_q$, on en déduit que β_q est non dégénérée sur M_2, ce qui n'est jamais le cas si q provient d'une forme bilinéaire. Alors, on a :

$$[O(M_p) : O(V_p, M_p/pM_p)] = |O(\overline{M_p})|.$$

En effet, l'application

$$\begin{aligned} \psi \ : \ O(M_p) &\longrightarrow O(\overline{M_p}) \\ u &\longmapsto \quad \overline{u} \ : \ \overline{M_p} \longrightarrow \overline{M_p} \\ & \qquad x_p + pM_p \longmapsto u(x_p) + pM_p. \end{aligned}$$

est clairement bien définie, son noyau est $O(V_p, M_p/pM_p)$, et elle est surjective, en vertu du lemme 2.52. En résumé, on a :

$$\mu_p(O(M_p) = c_{\mu,p} \cdot p^{\frac{n(1-n)}{2}} \cdot |O(\overline{M_p})|.$$

Pour de tels p, on verra au chapitre suivant que

$$|O(\overline{M_p})| = 2 \cdot p^{\frac{n(n-1)}{2}} \cdot \prod_{0<2i<n} (1 - p^{-2i}) \cdot \begin{cases} 1 & \text{si } n \text{ est impair} \\ (1 - \left(\frac{d}{p}\right) \cdot p^{-\frac{n}{2}}) & \text{si } n \text{ est pair.} \end{cases}$$

Où $\left(\frac{\cdot}{p}\right)$ est le symbole de Legendre, et où d est le discriminant de M.
Finalement, on a :

Théorème 2.59

Dans les mêmes hypothèses que précédemment, on a :

$$\mu_p(O(M_p)) = 2 \cdot c_{\mu,p} \cdot \prod_{0<2i<n} (1 - p^{-2i}) \cdot \begin{cases} 1 & \text{si } n \text{ est impair} \\ (1 - \left(\frac{d}{p}\right) \cdot p^{-\frac{n}{2}}) & \text{si } n \text{ est pair.} \end{cases}$$

Démonstration :

C'est immédiat. •

Ce produit converge pour tout $n \geq 2$ si on fixe pour tout p, $\mu_p(O(V_p, M_p/p^k M_p^{\#}))$ de telle manière que

$$c_{\mu,p} = \frac{1}{2}.$$

Ainsi, nous avons pu normaliser nos mesures.

CHAPITRE 3

Le groupe orthogonal sur les corps $\mathbb{F}_p$

Dans ce chapitre, nous allons calculer le cardinal du groupe orthogonal pour certaines formes quadratiques non dégénérées sur $\mathbb{F}_p$, p premier. Tout d'abord, nous allons "classifier" grossièrement les formes sur $\mathbb{F}_2$, puis sur $\mathbb{F}_p$ avec p premier impair, pour finalement calculer le cardinal de $O_q^n(\mathbb{F}_p)$ cas par cas.

A. Formes quadratiques non dégénérées sur $\mathbb{F}_2$.

Fixons-nous (V, q) un espace quadratique non dégénéré sur $\mathbb{F}_2$. On sait que $\beta_q(x, x) = 2q(x) = 0 \ \forall x \in V$. Donc β_q est une forme "alternée", de déterminant 1.

Proposition 3.1

$\beta_q \simeq <\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}> \boxplus \cdots \boxplus <\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}>$.

Démonstration :

Soient $x, y \in V$ tels que $\beta_q(x, y) = 1$. De tels vecteurs existent puisque q est non dégénérée.
On a donc $(V, \beta_q) \simeq <x, y> \boxplus <x, y>^{\perp} = <\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}> \boxplus A$, où la matrice A est du même type que M_{β_q}, car on vérifie aisément que $f_{\beta|_{<x,y>}}$ est un isomorphisme. Donc en faisant le même raisonnement sur $(<x, y>^{\perp}, \beta|_{<x,y>^{\perp}})$, on conclut. •

Remarque :

On obtient donc que la dimension de V est paire. On aurait tout de même envie de dire que certaines formes sont "moins dégénérées que d'autres" si le rang de β_q est $n-1$ par exemple. On pourrait se donner de nouvelles définitions, par exemple de semi-régularités ou de défectivités. De tels raffinements sont faits dans la littérature, par exemple dans [6, ch. *I*, § 16] et dans [7, pp 6-7]. On pourrait alors avoir une classification plus fine, mais cela alourdirait mon exposé, surtout que nous n'en n'aurons pas besoin pour la suite des événements.

Corollaire 3.2

$V \simeq H \boxplus \cdots \boxplus H$ ou $V \simeq H \boxplus \cdots \boxplus H \boxplus L$.
Où (H, μ) est la forme hyperbolique de dimension 2 : $\mu((t_1, t_2)) = t_1 \cdot t_2$
et (L, ν) est la forme "bihyperbolique" de dimension 2 : $\nu((t_1, t_2)) = t_1^2 + t_1 \cdot t_2 + t_2^2$.

Démonstration :

La proposition 3.1 nous dit que $(V, q) \simeq <x_1, y_1> \boxplus \cdots \boxplus <x_{\frac{n}{2}}, y_{\frac{n}{2}}>$ avec $q(x_i) = a_i$ et $q(y_i) = b_1$ pour tout $i \in [\![1_{\frac{n}{2}}]\!]$.
Or, si $(a_i, b_i) = (0, 0)$ alors $q|_{<x_i,y_i>} = \mu$, si $(a_i, b_i) = (1, 1)$ alors $q|_{<x_i,y_i>} = \nu$ et si $(a_i, b_i) = (0, 1)$ on remplace y_i par $y_i' = y_i + x_i$ et on obtient $q|_{<x_i,y_i'>} = \mu$.
De plus $L \boxplus L \simeq H \boxplus H$; en effet, le changement de base est :

$$\begin{array}{l} e_1 \mapsto e_1 + e_3 \\ e_2 \mapsto e_1 + e_3 + e_4 \\ e_3 \mapsto e_2 + e_4 \\ e_4 \mapsto e_2 + e_3 + e_4 \end{array} \quad \text{si } (e_1, \ldots, e_4) \text{ est un base de } L \boxplus L.$$

•

Remarque :

Ces observations étant faites, il est donc clair que si $n \equiv 0 \bmod 4$ alors $V \simeq H \boxplus \cdots \boxplus H$. Lors du calcul du groupe orthogonal au paragraphe C , nous ne nous occuperons que de ce cas-là.

B. Formes quadratiques sur $\mathbb{F}_p$, p impair

Lemme 3.3

Soit (V, q) une forme quadratique de dimension supérieure ou égale à 3. Il existe $x \neq (0, \ldots, 0)$ tel que $q(x) = 0$.

Démonstration :

On sait que q est diagonalisable puisque la caractéristique est différente de 2. Le problème se résume donc à trouver x, y, z non tous nuls tels que $ax^2 + by^2 + cz^2 = 0$. Posons alors $z = 1$, il faut donc trouver x et y tels que $ax^2 + by^2 = -c$. Le lemme 1.40 permet de conclure. •

Théorème 3.4

Soit (V, q) un espace quadratique de dimension n non dégénéré sur $\mathbb{F}_p$, p impair. Alors β_q est isomorphe à une des formes suivantes :

$$\begin{cases} <\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}> \boxplus \cdots \boxplus <\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}> \\ <\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}> \boxplus \cdots \boxplus <\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}> \boxplus <\begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{b}{2} \end{pmatrix}> & \text{avec } -b \notin \mathbb{F}_p^{*2} \\ <\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}> \boxplus \cdots \boxplus <\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}> \boxplus <\frac{a}{2}> & \text{avec } a \in \mathbb{F}_p^*. \end{cases}$$

Démonstration :

Si $n = 1$, c'est clair.

Si $n = 2$, deux cas se présentent :

a) Il existe x non nul tel que $\beta_q(x, x) = 0$. Soit y tel que (x, y) soit une base de V. Si $\beta_q(y, y) = 0$, on est content.
Si $\beta_q(y, y) \neq 0$, on pose $y' = \dfrac{\beta_q(y, y)}{2\beta_q(x, y)} \cdot x + y$. On a $\beta_q(y', y') = 0$ et $\beta_q(x, y') = \beta_q(x, y) = s \neq 0$. En posant $y'' = \dfrac{1}{s} \cdot y'$ on en déduit que $\beta_q \simeq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

b) En revanche, si $\beta_q(x, x) \neq 0$ pour tout $x \in V \setminus \{0\}$, nous savons grâce au lemme 1.40 qu'il existe y tel que $\beta_q(y, y) = \frac{1}{2}$, donc $\beta_q \simeq <\dfrac{1}{2}> \boxplus <\dfrac{b}{2}>$ avec $-b \notin \mathbb{F}_p^{*2}$, car sinon β_q représenterait 0.
Finalement, si $n \geq 3$, grâce au lemme 3.4, nous savons qu'il est possible de représenter 0 non trivialement, donc la forme s'écrit $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \boxplus F$ avec F de dimension $n - 2$. On termine par récurrence. •

Corollaire 3.5

Tout espace quadratique non dégénéré sur $\mathbb{F}_p$, p impair est isomorphe à l'un des espaces suivants :

$$\begin{cases} H \boxplus \cdots \boxplus H & \text{Type (A)} \\ H \boxplus \cdots \boxplus H \boxplus J & \text{Type (B)} \\ H \boxplus \cdots \boxplus H \boxplus I & \text{Type (C)} \end{cases}$$

où H est l'espace hyperbolique, J est l'espace de dimension 2 muni de la forme j définie par $j((t_1, t_2)) = t_1^2 + bt_2^2$, $-b \notin \mathbb{F}_p^{*2}$, et I est l'espace de dimension 1 muni de la forme i définie par $i(t) = at^2$, $a \in \mathbb{F}_p^*$.

Démonstration :

Sachant que 2 est inversible, toute forme quadratique est déterminée entièrement par sa forme bilinéaire associée β_q. •

C. Le cardinal du groupe orthogonal.

Lemme 3.6 (théorème de Witt)

Soient (V,q), (V',q') et (W,r) trois espaces quadratiques non dégénérés sur $\mathbb{F}_p$, p premier quelconque. Alors :
$V \boxplus W \simeq V' \boxplus W$ implique $V \simeq V'$.

Remarque :

Le théorème de Witt n'est pas toujours vrai si l'on considère des espaces bilinéaires, mais cette version est vraie sans conditions supplémentaires sur W, même sur des anneaux semi-locaux (donc en particulier sur $\mathbb{F}_2$). La démonstration est donnée dans [2, ch. III, §4]. •

Lemme 3.7

Soit (V,q) un espace quadratique non dégénéré sur $\mathbb{F}_p$. Posons $\alpha(V)$ le nombre de vecteurs x non nuls tels que $q(x)=0$. Alors on a :

$$\alpha(V) = \begin{cases} (p^m-1)(p^{m-1}+1) & \text{si } V \text{ est du type (A) de rang } 2m \text{ et } p \text{ premier quelconque} \\ (p^m+1)(p^{m-1}-1) & \text{si } V \text{ est du type (B) de rang } 2m \text{ et } p \text{ premier impair} \\ p^{2m}-1 & \text{si } V \text{ est du type (C) de rang } 2m+1 \text{ et } p \text{ premier impair} \end{cases}$$

Démonstration :

Par convention, nous écrirons $m \cdot H$ pour $\underbrace{H \boxplus \cdots \boxplus H}_{m \text{ fois}}$.

On va chercher un lien entre $\alpha(V)$ et $\alpha(V \boxplus H)$.

Soit $x \in V \boxplus H$, $x = v + h$ où $v \in V$ et $h = (h_1, h_2) \in H$. On a bien sûr que $q(x) = q(v) + h_1 \cdot h_2$, donc si on cherche à trouver les solutions de $q(v) + h_1 \cdot h_2 = 0$, on obtient :

$$\alpha(V \boxplus H) = 2(p-1) + \alpha(V)(2p-1) + (p^n - \alpha(V) - 1)(p-1) \quad n = \text{ dimension de } V \text{ ;}$$

le premier membre compte le nombre de solutions avec $y=0$, le second avec $q(y)=0$, $y \neq 0$, et le troisième avec $q(y) \neq 0$. Cela nous donne :

$$\alpha(V \boxplus H) = p \cdot \alpha(V) + (p^n+1)(p-1)$$

ou encore :

$$\alpha(V \boxplus H) - p^{n-1} + 1 = p \cdot (\alpha(V) - p^{n-1} + 1).$$

Donc, si V est du type (A) et p premier quelconque, c'est-à-dire si $V = m \cdot H$, on obtient par récurrence:

$$\begin{aligned} \alpha(V) - p^{2m-1} + 1 &= p \cdot (\alpha((m-2) \cdot H) - p^{2m-3} + 1) \\ &= p^2 \cdot (\alpha((m-1) \cdot H) - p^{2m-5} + 1) = \cdots \\ &= p^m \cdot (\underbrace{\alpha(0 \cdot H)}_{=0} - p^{-1} + 1). \end{aligned}$$

Ce qui nous donne :

$$\alpha(V) = p^{2m-1} - 1 - p^{m-1} + p^m = (p^m - 1)(p^{m-1} + 1).$$

Maintenant, si $V = (m-1)\cdot H \boxplus J$, J défini comme au lemme 3.5, on a :

$$\alpha(V) - p^{2m-1} + 1 = p\cdot\alpha((m-1)\cdot H \boxplus J) - p^{2m-3} + 1) = \cdots = p^{m-1}\cdot(\underbrace{\alpha(J)}_{=0} - p + 1) = p^{m-1} - p^m$$

donc :

$$\alpha(V) = p^{2m-1} - 1 + p^{m-1} - p^m = (p^m+1)(p^{m-1}-1).$$

Finalement, si V est de type (C), de rang $2m+1$ et p premier impair, on trouve :

$$\alpha(V) - p^{2m} + 1 = p\cdot(\alpha((m-1)\cdot H \boxplus I) - p^{2m-2} + 1) = \cdots = p^m\cdot(\underbrace{\alpha(I)}_{=0} - p^0 + 1) = 0$$

d'où :

$$\alpha(V) = p^{2m} - 1.$$

•

Théorème 3.8

Soient (V,q) un espace quadratique non dégénéré sur $\mathbb{F}_p$ de dimension $n = 2m$ ou $2m+1$ selon la parité de la dimension de V, et $O_q^n(V)$ le groupe orthogonal associé. On a :

$$|O_q^n(V)| = \begin{cases} 2\cdot p^{\frac{n(n-1)}{2}}(1-p^{-m})\displaystyle\prod_{0<2i<n}(1-p^{-2i}) & \text{si } V \text{ est du type (A) de rang } 2m \text{ et } p \text{ premier quelconque} \\ 2\cdot p^{\frac{n(n-1)}{2}}(1+p^{-m})\displaystyle\prod_{0<2i<n}(1-p^{-2i}) & \text{si } V \text{ est du type (B) de rang } 2m \text{ et } p \text{ premier impair} \\ 2\cdot p^{\frac{n(n-1)}{2}}\displaystyle\prod_{0<2i<n}(1-p^{-2i}) & \text{si } V \text{ est du type (C) de rang } 2m+1 \text{ et } p \text{ premier impair.} \end{cases}$$

Démonstration :

On cherche à nouveau une relation entre $|O_q(V\boxplus H)|$ et $|O_q(V)|$. Pour se fixer les idées, on pose $H = \mathbb{F}_p\cdot h_1 + \mathbb{F}_p\cdot h_2$, où $q(h_1) = q(h_2) = 0$ et $\beta_q(h_1,h_2) = 1$. Soit aussi

$$\begin{aligned} \varphi :\ O_q(V\boxplus H) &\longrightarrow \{x\in V\setminus\{0\} \mid q(x) = 0\} \\ u &\longmapsto u(h_1). \end{aligned}$$

φ est surjective en vertu du théorème de Witt. u, u' ont même image si et seulement si $u^{-1}u' \in \{u \in O_q(V\boxplus H) \mid u(h_1) = h_1\}$. Donc, les classes à gauche de ce groupe sont en bijection avec l'ensemble des vecteurs non nuls de longueur nulle. Ainsi, on a :

$$|O_q(V\boxplus H)| = \alpha(V\boxplus H)\cdot|\{u\in O_q(V\boxplus H) \mid u(h_1) = h_1\}|.$$

Nous allons maintenant nous donner une nouvelle surjection :

$$\begin{aligned} \psi :\ \{u\in O_q(V\boxplus H) \mid u(h_1) = h_1\} &\longrightarrow \mathscr{F} \\ u &\longmapsto u(h_2), \end{aligned}$$

où $\mathscr{F}$ est l'ensemble des $h_2' \in V\boxplus H$ tels que $q(h_2') = 0$ et $\beta_q(h_1,h_2') = 1$. Comme avant, u et u' ont même image si et seulement si $u^{-1}u' \in \{u\in O_q(V\boxplus H) \mid u(h_1) = h_1,\ u(h_2) = h_2\}$; mais cet ensemble est en bijection avec $O_q(V)$, sachant que le théorème de Witt est valable dans notre cas.

Intéressons-nous maintenant au cardinal de $\mathscr{F}$:

A priori, un élément h_2' de $\mathscr{F}$ s'écrit $v + ah_1 + bh_2$, $v\in V$ et $a,b\in\mathbb{F}_p$. Or $1 = \beta_q(h_1,h_2') = b$. On a aussi que $q(h_2') = q(v) + ab = q(v) + a$.

Pour chaque v choisi, il n'y a donc qu'un a possible et un seul. Puisque le nombre de v est p^n, on obtient alors la formule :

$$|O(V \boxplus H)| = \alpha(V \boxplus H) \cdot p^n \cdot |O(V)|. \tag{I}$$

Nous pouvons donc examiner chaque cas :

type (A) : vu le lemme 3.7, on a :

$$\begin{aligned}
|O_q(m \cdot H)| &= (p^m - 1)(p^{m-1} + 1)p^{2m-2}|O((m-1) \cdot H)| \\
&= p^{(2m-1)+(2m-2)}((1 - p^{-m})(1 + p^{-(m-1)})|O_q((m-1) \cdot H)| \\
&= p^{(2m-1)+(2m-2)+(2m-3)+(2m-4)}(1 - p^{-m})(1 + p^{-(m-1)})(1 - p^{-(m-1)})(1 + p^{-(m-2)}) \cdot \\
&\qquad \cdot (1 - p^{-(m-2)})|O_q((m-2) \cdot H)| \\
&\quad \vdots \\
&= p^{(2m-1)+(2m-2)+\cdots+1}(1 - p^{-m}) \prod_{0<2i<n} (1 - p^{-2i}) \cdot 2 \\
&= 2 \cdot p^{\frac{n(n-1)}{2}}(1 - p^{-m}) \prod_{0<2i<n} (1 - p^{-2i}).
\end{aligned}$$

type (B) : Si $V = (m-1) \cdot H \boxplus J$, on obtient :

$$\begin{aligned}
|O_q(V)| &= (p^m + 1)(p^{m-1} - 1)p^{2m-2}|O_q((m-2) \cdot H \boxplus J)| \\
&\quad \vdots \\
&= p^{(2m-1)+(2m-2)+\cdots+2}(1 + p^{-m})(1 - p^{-(m-1)}) \cdots (1 + p^{-2})(1 - p^{-1})|O(J)|.
\end{aligned} \tag{II}$$

Le problème maintenant est de calculer $|O(J)|$.

Rappelons que J est un espace de dimension 2 de base (e_1, e_2) tel que $\beta_q(e_1, e_2) = 0$, $q(e_1) = 1$ et $q(e_2) = a$ avec $a \notin \mathbb{F}_p^{*2}$.

Commençons par calculer le nombre de vecteurs de longueur 1, c'est-à-dire le nombre de solutions de l'équation $x^2 + ay^2 = 1$. On peut voir le membre de gauche comme la norme de $x + y\sqrt{-a}$ dans $\mathbb{F}_p(\sqrt{-a})$ qui a p^2 éléments. Donc, les vecteurs de norme 1 peuvent être vus comme le noyau de l'application $N : \mathbb{F}_p(\sqrt{-a})^* \longrightarrow \mathbb{F}_p^*$ définie par $N(x + y\sqrt{-a}) = x^2 + ay^2$. Le cardinal de ce noyau est évidemment $\dfrac{p^2 - 1}{p - 1} = p + 1$. De plus, l'application

$$\begin{aligned}
\rho : O(J) &\longrightarrow \ker(N) \\
u &\longmapsto u(e_1)
\end{aligned}$$

est surjective et $\rho(u) = \rho(u')$ si et seulement si $u^{-1}u'(e_1) = e_1$. On remarque que compter les u dans $O(J)$ tels que $u(e_1) = e_1$ revient à compter le nombre de couples (x, y) de longueur a et orthogonaux à e_1. Il faut donc que $x = 0$ et par suite $ay^2 = a$ donc $y = \pm 1$. Cela nous fait alors deux possibilités pour y (on a supposé $p \neq 2$). Il suit :

$$|O(J)| = 2(p + 1).$$

Tenant compte de la formule (II), on obtient :

$$|O(V)| = 2 \cdot p^{\frac{n(n-1)}{2}}(1 + p^{-m}) \prod_{0<2i<n} (1 - p^{-2i}).$$

Remarque : Si $p = 2$ et si J est l'epace muni de la forme $x^2 + xy + y^2$, on voit aisément que $|O(J)| = 3$, et on obtiendrait donc la meme formule, mais avec un facteur 2 en moins.

Type (C) : Si $V = m \cdot H \boxplus <a>$, puisque p est impair, on a que $|O(<a>)| = 2$. Ce qui nous donne :

$$\begin{aligned} |O(E)| &= p^{2m-1}(p^{2m}-1)|O((m-1)\cdot H \boxplus <a>)| \\ &= p^{2m\cdot(2m-1)}(1-p^{-2m})|O((m-1)\cdot H \boxplus <a>| \\ &\vdots \\ &= 2\cdot p^{\frac{n(n-1)}{2}} \prod_{0<2i<n}(1-p^{-2i}). \end{aligned}$$

•

Corollaire 3.9

Si V est de dimension $n = 2m$ et si p est impair, alors :

$$|O_q^n(V)| = 2\cdot p^{\frac{n(n-1)}{2}}\left(1-\left(\frac{d}{p}\right)p^{-m}\right)\prod_{0<2i<n}(1-p^{-2i}).$$

Où $d = (-1)^{\frac{n(n-1)}{2}}\det(V)$ est le discriminant de V, et $(\frac{\cdot}{p})$ est le symbole de Legendre.

Démonstration :

On voit que le type(A) correspond à $(-1)^m\det(V) \in \mathbb{F}_p^{*2}$

et que le type(B) correspond à $(-1)^m\det(V) \notin \mathbb{F}_p^{*2}$. De plus $\dfrac{n(n-1)}{2} = m(n-1) \equiv m \bmod 2$. •

CHAPITRE 4
Le groupe orthogonal modulo 8.

Le but de ce chapitre est de calculer le cardinal du groupe orthogonal pour la forme $\beta = x_1y_1 + \cdots + x_ny_n$, définie sur un $\mathbb{Z}/8\mathbb{Z}$-module libre de rang n.

A. Groupes orthogonaux quadratiques et bilinéaires.

Définition 4.1

Soit M un $\mathbb{Z}/8\mathbb{Z}$-module libre de rang n muni d'une forme quadratique q. Le *groupe orthogonal quadratique modulo 8* est le groupe $O_q^n(\mathbb{Z}/8\mathbb{Z})$ formé des isomorphismes $u : M \to M$ tels que $q(u(x)) = q(x)$ pour tout $x \in M$.

Définition 4.2

Soit M un $\mathbb{Z}/8\mathbb{Z}$-module libre de rang n muni d'une forme bilinéaire β. Le *groupe orthogonal bilinéaire modulo 8* est le groupe $O_\beta^n(\mathbb{Z}/8\mathbb{Z})$ formé des isomorphismes $u : M \to M$ tels que $\beta(u(x), u(y)) = \beta(x, y)$ pour tout $x, y \in M$.

Proposition 4.3

Si $\beta(x, y) = x_1y_1 + \cdots + x_ny_n$ et $q(x) = x_1^2 + \cdots + x_n^2 \quad x, y \in M$, on a
$|O_q^n(\mathbb{Z}/8\mathbb{Z})| = 2^{n(n-1)/2} \cdot |O_\beta^n(\mathbb{Z}/8\mathbb{Z})|$

Démonstration :

Notons O_q^n pour $O_q^n(\mathbb{Z}/8\mathbb{Z})$ et O_β^n pour $O_\beta^n(\mathbb{Z}/8\mathbb{Z})$.
Il est clair que $O_\beta^n = \{O \in \mathrm{M_n}(\mathbb{Z}/8\mathbb{Z}) \mid OO^t = I_n\}$ et que $O_q^n = \{O \in \mathrm{M_n}(\mathbb{Z}/8\mathbb{Z}) \mid OO^t = I_n + 4S,\ S \in \mathscr{S}\}$ où $\mathscr{S}$ est l'ensemble des matrices $(S_{ij})_{i,j \in \mathbb{N}_n}$ telles que $S_{ij} = S_{ji} \in \mathbb{Z}/2\mathbb{Z}$ et $S_{ii} = 0$ pour tout $i, j \in \mathbb{N}_n$.
On a donc que O_β^n est un sous-groupe de O_q^n. Soit $\phi : O_q^n \to \mathscr{S}$, définie par $\phi(O) = S$ où $4S = OO^t - I_n$.
Nous allons voir que ϕ est une application surjective et qu'elle induit une bijection entre
O_q^n *modulo* O_β^n et $\mathscr{S}$.
ϕ est surjective, car si $S \in \mathscr{S}$, on a $I_n + 4S = (I_n + 4S^+)(I_n + 4S^+)^t$ où S^+ est la matrice triangulaire supérieure formée des coefficients au-dessus de la diagonale de S.
Si $O_1, O_2 \in O_q^n$ sont tels que $O_2O_2^t = O_1O_1^t = I_n + 4S$, alors $O_2O_2^tO_1^{t^{-1}} = O_1$. Donc $O_1^{-1}O_2O_2^tO_1^{t^{-1}} = (O_1^{-1}O_2)(O_1^{-1}O_2)^t = I_n$ ce qui nous donne que $O_1^{-1}O_2 \in O_\beta^n$. Réciproquement, si $O_1^{-1}O_2 \in O_\beta^n$, alors $O_1O_1^t = O_2O_2^t$ et donc $\phi(O_1) = \phi(O_2)$.
O_β^n induit une relation d'équivalence : $O_1 \sim O_2$ si $O_1^{-1}O_2 \in O_\beta^n$.
On a finalement une bijection : $O_q^n/_\sim \to \mathscr{S},\ O \mapsto \phi(O),\ O \in \bar{O}$.
Puisque $|\mathscr{S}| = 2^{n(n-1)/2}$, on conclut. •

Remarque :

Nous n'utiliserons ce résultat que dans une version atténuée lors de la proposition 5.4, à savoir que O_β^n est contenu strictement dans O_q^n.

B. Les vecteurs de norme i.

Dans ce pragraphe, nous allons calculer le cardinal des vecteurs de norme i pour i fixé dans $\mathbb{Z}/8\mathbb{Z}$.
Pour des raisons techniques, il est bon de se fixer quelques notations:
$t_i(n) := |\{x \in (\mathbb{Z}/8\mathbb{Z})^n \mid x_1^2 + \cdots + x_n^2 = i\}| \quad n \in \mathbb{N}$ et $i \in \mathbb{Z}/8\mathbb{Z}$
$u_1(n) := t_1(n) - t_3(n) + t_5(n) - t_7(n)$
$u_0(n) := t_0(n) - t_2(n) + t_4(n) - t_6(n)$
$\epsilon_i(n) := t_i(n) - t_{i+4}(n) \quad i = 0, 1, 2, 3$
$s_i(n) := t_i(n) + t_{i+4}(n) \quad i = 0, 1, 2, 3$
Si on fixe une variable, on obtient aisément la relation :

$$(*) \quad t_i(n+1) = 2t_i(n) + 4t_{i-1}(n) + 2t_{i-4}(n) \quad \forall i \in \mathbb{Z}/8\mathbb{Z},$$

car $1, 3, 5$ et 7 sont de carré 1 mod 8, 0 et 4 sont de carré 0 mod 8; enfin, 2 et 6 sont de carré 4 mod 8.
Ceci nous donne l'équation matricielle :

$$T(n+1) = A \cdot T(n)$$

$$\text{où} \quad T(n) = \begin{pmatrix} t_0(n) \\ t_1(n) \\ \vdots \\ t_7(n) \end{pmatrix} \quad \text{et} \quad A = \begin{pmatrix} 2 & 0 & 0 & 0 & 2 & 0 & 0 & 4 \\ 4 & 2 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 4 & 2 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 4 & 2 & 0 & 0 & 0 & 2 \\ 2 & 0 & 0 & 4 & 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 4 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 4 & 2 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 4 & 2 \end{pmatrix}$$

$$\text{Donc} \quad T(n+1) = A^n \cdot T(1) \quad \text{et} \quad T(1) = \begin{pmatrix} 2 \\ 4 \\ 0 \\ 0 \\ 2 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad \forall n \in \mathbb{N}$$

Les équations précédentes donnent alors, grâce à un bref raisonnement par récurence, que la première colonne de A^n n'est autre que $T(n)$ et, comme A est une matrice "circulante", A^n aussi. Donc, la première ligne de A^n est $(t_0(n), t_7(n), \ldots, t_1(n))$.
Le polynôme caractéristique de A (qui est aussi le polynôme minimal) est : $X(X^4 + 256)(X^2 - 8X + 32)(X - 8)$.
Calculons le noyau de $A^2 - 8A + 32I_8$ qui sera bien sûr contenu dans celui de $A^{n+1} - 8A^n + 32A^{n-1}$ pour tout $n \in \mathbb{N}$. Il est engendré par les deux vecteurs suivants :

$$(0, -1, 0, 1, 0, -1, 0, 1) \quad \text{et} \quad (1, 0, -1, 0, 1, 0, -1, 0).$$

Ce qui nous donne les deux équations suivantes :

$$u_i(n+1) = 8\,u_i(n) - 32\,u_i(n-1) \quad i = 0, 1 \qquad (I).$$

En itérant 2 fois cette formule, on obtient : $u_i(n+4) = -2^{10}u_i(n)$. Donc :

$$u_i(j + 4k) = (-1)^k 2^{10k} u_i(j) \quad \text{pour} \quad 1 \leq j \leq 4,\ i = 0, 1, \text{ et } k \in \mathbb{N}. \qquad (I')$$

Regardons le noyau de $A^4 + 256I_8$, donc une partie de celui de $A^{n+3} + 256A^{n-1}$ pour tout $n \in \mathbb{N}$. On trouve l'espace :

$$<(0,0,0,1,0,0,-1),(0,0,1,0,0,0,-1,0),(0,1,0,0,0,-1,0,0),(1,0,0,0,-1,0,0,0)>.$$

Cela nous donne les équations suivantes : $\epsilon_i(n+4) = -256\,\epsilon_i(n)$ pour $i = 0,1,2,3$ d'où :

$$\epsilon_i(j+4k) = (-1)^k 2^{8k}\epsilon_i(j) \quad \text{pour } 0 \leq i \leq 3,\ k \in \mathbb{N} \text{ et } j \in \mathbb{N}_4. \tag{II}$$

Le noyau de A lui-même est l'espace engendré par $(-1,1,-1,1,-1,1,-1,1)$. On trouve alors : $s_0(n) + s_2(n) = s_1(n) + s_3(n)$. Il est clair que $\sum_{i=0}^{4} s_i(n) = 8^n$, donc :

$$s_i(n) + s_{i+2}(n) = \frac{8^n}{2} \quad \text{pour } i = 1,2. \tag{III}$$

Il est évident que $u_i(n) = s_i(n) - s_{i+2}(n)$ pour $i = 0,1$. Sachant cela et vu les équations (I') et (III), on obtient le système :

$$\begin{cases} s_i(j+4k) - s_{i+2}(j+4k) = (-1)^k 2^{10k} u_i(j) \\ s_i(j+4k) + s_{i+2}(j+4k) = \dfrac{8^n}{2}. \end{cases}$$

Ce qui fait :

$$s_i(j+4k) = t_i(j+4k) + t_{i+4}(j+4k) = (-1)^k 2^{10k-1} u_i(j) + \frac{8^{j+4k}}{2^2}. \tag{IV}$$

En se souvenant de la définition de $\epsilon_i(j+4k)$ et grâce aux équations (II) et (IV), on a:

$$t_i(j+4k) = (-1)^k 2^{8k-1}(2^{2k-1}u_i(j) + \epsilon_i(j)) + 8^{j+4k-1} \quad i = 0,1 \text{ et } j \in \mathbb{N}_4 \tag{A}$$

Nous sommes donc en mesure de démontrer la

Proposition 4.4

$$t_1(n) = \begin{cases} 2^{3n-3} & \text{si } n \equiv 0 \text{ ou } 4 \pmod 8,\ n \neq 0 \\ 2^{3n-3}(1 + 2^{(1-n)/2} + 2^{2-n}) & \text{si } n \equiv 1 \pmod 8 \\ 2^{3n-3}(1 + 2^{(2-n)/2}) & \text{si } n \equiv 2 \pmod 8 \\ 2^{3n-3}(1 + 2^{(1-n)/2}) & \text{si } n \equiv 3 \pmod 8 \\ 2^{3n-3}(1 + 2^{(1-n)/2})(1 - 2^{(3-n)/2}) & \text{si } n \equiv 5 \pmod 8 \\ 2^{3n-3}(1 - 2^{(2-n)/2}) & \text{si } n \equiv 6 \pmod 8 \\ 2^{3n-3}(1 - 2^{(1-n)/2}) & \text{si } n \equiv 7 \pmod 8 \end{cases}$$

Démonstration :

Si $\mathbf{n = 1 + 4k}$, on a :
$u_1(1) = t_1(1) - t_3(1) + t_5(1) - t_7(1) = 4 + 0 + 0 + 0 = 4$ et $\epsilon_1(1) = t_1(n) - t_5(1) = 4$. Donc, l'équation (A) devient :

$$\begin{aligned} t_1(1+4k) &= (-1)^k 2^{8k-1}\left(2^2(2^{2k-1}+1)\right) + 8^{j+4k-1} = 2^{8k-1}((-1)^k(2^{2k-1}+1) + 2^{4k-1}) \\ &= 2^{2n-1}((-1)^{(n-1)/4}(2^{(n-3)/2}+1) + 2^{n-2}). \end{aligned}$$

On en déduit que si $n \equiv 1 \pmod 8$, alors :

$$t_1(n) = 2^{2n-1}(2^{n-2} + 2^{(n-3)/2} + 1) = 2^{3n-3}(1 + 2^{(1-n)/2} + 2^{2-n}),$$

et que si $n \equiv 5 \pmod 8$, on obtient

$$t_1(n) = 2^{3n-3}(1 - 2^{(1-n)/2} - 2^{2-n}) = 2^{3n-3}(1 + 2^{(1-n)/2})(1 - 2^{(3-n)/2}).$$

Si $\mathbf{n = 2 + 4k}$, on a :
$u_1(2) = 2^4 + 2^4 = 2^5$ et $\epsilon_1(2) = 2^4 - 2^4 = 0$; donc

$$\begin{aligned} t_1(n) &= (-1)^k 2^{8k-1}(2^{2k-1} \cdot 2^5) + 8^{4k+1} = 2^{10k+3}((-1)^k + 2^{2k}) \\ &= 2^{(5n-4)/2}(2^{(n-2)/2} + (-1)^{(n-2)/4}). \end{aligned}$$

Si $n \equiv 2 \pmod 8$, on a :

$$t_1(n) = 2^{(5n-4)/2}(2^{(n-2)/2} + 1) = 2^{3n-3}(1 + 2^{(2-n)/2}),$$

et si $n \equiv 6 \pmod 8$, on a

$$t_1(n) = 2^{3n-3}(1 - 2^{(2-n)/2}).$$

Pour le cas où $\mathbf{n = 3 + 4k}$, on a : $u_1(3) = 3 \cdot 2^5 - 2^6 + 3 \cdot 2^5 - 0 = 2^7$ et $\epsilon_1(2) = 3 \cdot 2^5 - 3 \cdot 2^5 = 0$, donc

$$\begin{aligned} t_1(n) &= (-1)^k 2^{8k-1}(2^{2k-1} \cdot 2^7) + 8^{4k+2} = 2^{10k+5}((-1)^k + 2^{2k+1}) \\ &= 2^{(5n-5)/2}(2^{(n-1)/2} + (-1)^{(n-3)/4}). \end{aligned}$$

Donc, si $n \equiv 3 \pmod 8$, on a :

$$t_1(n) = 2^{(5n-5)/2}(2^{(n-1)/2} + 1) = 2^{3n-3}(1 + 2^{(1-n)/2}),$$

et si $n \equiv 7 \pmod 8$, on trouve :

$$t_1(n) = 2^{3n-3}(1 - 2^{(1-n)/2}).$$

Finalement, si $\mathbf{n = 4k + 4}$, on a :
$u_1(4) = 2^9 - 2^9 + 2^9 - 2^9 = 0$ et $\epsilon_1(4) = 2^9 - 2^9 = 0$, d'où :

$$t_1(n) = 8^{n-1} = 2^{3n-3}.$$

•

Remarques :

a) Les petites valeurs de $u_1(n)$ et de $\epsilon_1(n)$ ont bien sûr été calculées grâce à l'équation $T(n+1) = A^n T(1)$.

b) Par la suite, nous aurons essentiellement besoin des $t_1(n)$ sous la forme donnée à la proposition précédente, mais les équations $(I) - (IV)$ et (A) nous permettant de calculer les autres $t_i(n)$, nous obtiendrons une formule plus compacte que la précédente, à savoir :

Proposition 4.5

$$t_i(n) = \begin{cases} 2^{3n-3} + 2^{\frac{5n-4}{2}} \cdot \cos\left(\frac{\pi}{4}(2i-n)\right) & \text{si } i \not\equiv n \pmod 4 \\ 2^{3n-3} + 2^{\frac{5n-4}{2}} \cdot \cos\left(\frac{\pi}{4}(2i-n)\right) + (-1)^{(i-n)/4} \cdot 2^{2n-1} & \text{si } i \equiv n \pmod 4 \end{cases}$$

Démonstration :

Une rapide vérification nous permet de voir que la formule marche pour $t_1(n)$.
Commençons tout d'abord par calculer $t_0(n)$:
Si $\mathbf{n = 1 + 4k}$: $u_0(1) = t_0(1) - t_2(1) + t_4(1) - t_6(1) = 2 + 2 = 4$ et $\epsilon_0(1) = t_0(1) - t_4(1) = 0$.
Donc vu (A), on a :

$$\begin{aligned} t_0(n) &= \left((-1)^{(n-1)/4} \cdot 2^{(5n-5)/2} + 2^{3n-3}\right) \\ &= (2^{3n-3} + 2^{(5n-5)/2}), \end{aligned}$$

si $n \equiv 1 \pmod 8$. Et,

$$t_0(n) = (2^{3n-3} - 2^{(5n-5)/2})$$

si $n \equiv 5 \pmod 8$).

Si $\mathbf{n = 2 + 4k}$:

$u_0(2) = 2^3 - 2^4 + 2^3 = 0$ et $\epsilon_0(2) = 2^3 - 2^3 = 0$ donc $t_0(n) = 2^{3n-3}$.

Si $\mathbf{n = 3 + 4k}$:

$u_0(3) = 2^5 - 3 \cdot 2^5 + 2^5 - 3 \cdot 2^5 = -2^7$ et $\epsilon_0(3) = 0$.

Donc, on a $t_0(n) = \left((-1)^{(n-1)/4} \cdot 2^{(5n-5)/2} + 2^{3n-3}\right) = (2^{3n-3} - 2^{(5n-5)/2})$ si $n \equiv 3 \pmod 8$ (respectivement $(2^{3n-3} + 2^{(5n-5)/2})$ si $n \equiv 7 \pmod 8$).

Si $\mathbf{n = 4 + 4k}$:

$u_0(4) = 2^7 - 3 \cdot 2^8 + 3 \cdot 2^7 - 3 \cdot 2^8 = -2^{10}$ et $\epsilon_0(3) = 2^7 - 3 \cdot 2^7 = -2^8$.

Donc, on a $t_0(n) = \left((-1)^{n/4}(2^{(5n-4)/2} + 2^{2n-1}) + 2^{3n-3}\right) = (2^{3n-3} + 2^{(5n-4)/2} + 2^{2n-1})$ si $n \equiv 0 \pmod 8$ (respectivement $(2^{3n-3} - 2^{(5n-4)/2} + 2^{2n-1})$ si $n \equiv 4 \pmod 8$).

La relation $(*)$ nous donne : $t_1(n+1) = 2t_1(n) + 4t_0(n) + 2t_5(n)$. On trouve alors facilement $t_5(n)$. Puis, en faisant varier judicieusement i dans $(*)$, on trouve les autres $t_i(n)$. •

E. Preissmann et H. Joris m'ont aimablement donné d'autres démonstrations plus analytiques de ce résultat qui par ailleurs est cité dans [8, ch. *II*, §9]. Le lecteur trouvera ces démonstrations dans l'appendice de ce travail.

C. Le cardinal du groupe O^n_β.

Dans ce paragraphe, nous allons donner une formule calculatoire pour $|O^n_\beta|$; mais pour y arriver, il faudra établir une forme "canonique" à toute forme bilinéaire non dégénérée sur $\mathbb{Z}/8\mathbb{Z}$, puis chercher les vecteurs de norme 1 qui ont des supplémentaires orthogonaux pairs. Ces vecteurs seront appelés "mauvais vecteurs", car le théorème de Witt ne s'applique pas pour eux.

Lemme 4.6

Soit (V, β) une forme bilinéaire de dimension n sur $\mathbb{Z}/8\mathbb{Z}$. Si $x \in V$ est tel que $\beta(x,x) = a$ impair (donc inversible), alors $\beta \simeq <a> \boxplus U$. D'autre part, si $\beta(x,x)$ et $\beta(y,y)$ sont pairs mais que $\beta(x,y)$ est impair, alors $V \simeq <x,y> \boxplus <x,y>^\perp$.

Démonstration :

a) Si f est une application linéaire de $<x>$ dans $\mathbb{Z}/8\mathbb{Z}$, il est clair que $\beta\left(\frac{x \cdot f(x)}{\beta(x,x)}, \cdot\right) = f$, donc $\beta|_{<x>}$ est non dégénérée. La proposition 1.5 nous donne : $V \simeq <x> \boxplus <x>^\perp$.

b) Soit $f : <x,y> \to \mathbb{Z}/8\mathbb{Z}$ linéaire. Pour prouver que $\beta|_{<x,y>}$ est non dégénérée, il suffit de trouver un $z = \lambda x + \mu y$ tel que $\beta(z,x) = f(x)$ et $\beta(z,y) = f(y)$, ce qui nous donne le système suivant à résoudre :

$$\begin{cases} \lambda\beta(x,x) + \mu\beta(y,x) = f(x) \\ \lambda\beta(x,y) + \mu\beta(y,y) = f(y). \end{cases}$$

En posant $\mu = f(x)\beta(x,y)\,(1 - \beta(x,x)\beta(y,y)) - f(y)\beta(x,x)$ et $\lambda = \beta(x,y)\,(f(y) - \mu\beta(x,y))$, on conclut grâce à la proposition 1.5. •

Corollaire 4.7

Toute forme bilinéaire symétrique non dégénérée sur $\mathbb{Z}/8\mathbb{Z}$ est isomorphe à une forme du type :

$$<a_1> \boxplus \cdots \boxplus <a_j> \boxplus <\begin{pmatrix} b_1 & d_1 \\ d_1 & c_1 \end{pmatrix}> \boxplus \cdots \boxplus <\begin{pmatrix} b_i & d_i \\ d_i & c_i \end{pmatrix}>,$$

où a_k impair $\forall k$ et $\det \begin{pmatrix} b_l & d_l \\ d_l & c_l \end{pmatrix}$ impair $\forall l$.

Démonstration :

S'il existe x_1 tel que $\beta(x_1,x_1)=a_1$ impair, alors par le lemme précédent : $\beta \simeq <a_1> \boxplus V$. Et on refait le même raisonnement jusqu'à ce que $\beta \simeq <a_1> \boxplus \cdots \boxplus <a_j> \boxplus V'$ où $\beta(x,x)$ pair $\forall x \in V'$. Comme β est non dégénérée, $\exists x_1, y_1$ tels que $\beta(x_1,y_1)$ impair, donc par le lemme précédent :

$$\beta \simeq <a_1> \boxplus \cdots \boxplus <a_j> \boxplus <\begin{pmatrix} \beta(x_1,x_1) & \beta(x_1,y_1) \\ \beta(x_1,y_1) & \beta(y_1,y_2) \end{pmatrix}> \boxplus V''$$

et on termine par récurrence. •

Corollaire 4.8

Si (V,β) est non dégénérée et de dimension impaire, alors il existe $x \in V$ tel que $\beta(x,x)$ impair. On dit alors par convention que V est *impair*, sinon, V est dit *pair*. •

Lemme 4.9

Supposons que $E \boxplus V \simeq E \boxplus V'$ et que E, V et V' sont impairs, alors $V \simeq V'$.

Démonstration :

Cette version du théorème de Witt est démontrée dans [2, thm 4.5, pp. 82-83] •

Lemme 4.10

Soit (V,β) tel que $M_\beta = I_n$ et $n \not\equiv 1 \pmod 8$. Si $x \in V$ est tel que $\beta(x,x)=1$, alors il existe U et $y \in U$ tels que $V \simeq <x> \boxplus U$ et $\beta(y,y)$ impair.

Démonstration :

Par le lemme 4.6, on sait qu'il existe U avec $V \simeq <x> \boxplus U$. Par le corollaire 4.8, si n est pair, donc si $\dim(U)$ est impair, le lemme est prouvé. Si n est impair et $n \not\equiv 1 \pmod 8$, on a que $\dim(U)$ est paire et $\det(U, \beta|_U) = 1$. Supposons que U ne représente que des éléments pairs, alors :

$$U \simeq <\begin{pmatrix} a_1 & c_1 \\ c_1 & b_1 \end{pmatrix}> \boxplus \cdots \boxplus <\begin{pmatrix} a_{(n-1)/2} & c_{(n-1)/2} \\ c_{(n-1)/2} & b_{(n-1)/2} \end{pmatrix}>,$$

avec $\det \begin{pmatrix} a_i & c_i \\ c_i & b_i \end{pmatrix}$ impair. Mais puisque a_i, b_i sont pairs $\forall i$, on a que $\det \begin{pmatrix} a_i & c_i \\ c_i & b_i \end{pmatrix} = -1$ ou 3, et c_i est impair $\forall i$.

Soient λ et α impairs, grâce aux matrices de changement de base $\begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix}$, $\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix}$, on montre facilement que l'on peut supposer que $\begin{pmatrix} a_i & c_i \\ c_i & b_i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ ou $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$.

Or, sur $\mathbb{Z}_2$ on a la relation :

$$\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \boxplus \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \simeq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \boxplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{(théorème 1.41.)}$$

donc a fortiori cela est vrai sur $\mathbb{Z}_2/8\mathbb{Z}_2 = \mathbb{Z}/8\mathbb{Z}$. Finalement, pour une raison de déterminant, on peut supposer que

$$\begin{pmatrix} a_i & c_i \\ c_i & b_i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \forall i$$

Résumons-nous. On a donc montré que :

$$<1> \boxplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \boxplus \cdots \boxplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \simeq <1> \boxplus \cdots \boxplus <1>$$

Mais cela n'est pas vrai. En effet, on a $<1>\boxplus\begin{pmatrix}0&1\\1&0\end{pmatrix} \simeq <1>\boxplus<1>\boxplus<-1>$. (la matrice de changement de base est $\begin{pmatrix}1&1&1\\1&0&1\\0&-1&-1\end{pmatrix}$). Donc, on a

$$<1>\boxplus\cdots\boxplus<1> \simeq \underbrace{<1>\boxplus\cdots\boxplus<1>}_{(n+1)/2}\boxplus\underbrace{<-1>\boxplus\cdots\boxplus<-1>}_{(n-1)/2}.$$

Le lemme 4.9 nous permet donc de dire que :

$$<1>\boxplus\cdots\boxplus<1> \simeq -\Big(\underbrace{<1>\boxplus\cdots\boxplus<1>}_{(n-1)/2}\Big).$$

On en déduit donc que $t_1((n-1)/2) = t_7((n-1)/2)$, mais cela est faux si $n \not\equiv 1 \pmod 8$ vu la proposition 4.5. On a donc une contradiction. •

Lemme 4.11

Soit (V,β) tel que $M_\beta = I_n$ et $n \equiv 1 \pmod 8$. Posons $x = (a_1,\ldots,a_n)$ tel que $\beta(x,x) = 1$. Alors, x possède un supplémentaire orthogonal pair si et seulement si $a_1,\ldots,a_n$ sont tous impairs.

Démonstration :

"$\Longleftarrow$" :

$$\text{Posons}\quad M = \begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_{n-1} & a_n\\ a_1 & 0 & a_3 & \ldots & a_{n-1} & a_n\\ a_1 & a_2 & 0 & \ldots & a_{n-1} & a_n\\ \vdots & \vdots & & \ddots & \vdots & \vdots\\ a_1 & a_2 & a_3 & \ldots & 0 & a_n\\ a_1 & a_2 & a_3 & \ldots & a_{n-1} & 0 \end{pmatrix}.$$

$$\text{On a donc :}\quad M\cdot M^t = \begin{pmatrix} 1 & 0 & 0 & 0 & \ldots & 0\\ 0 & 0 & -1 & -1 & \ldots & -1\\ 0 & -1 & 0 & -1 & \ldots & -1\\ 0 & -1 & -1 & \ddots & & \vdots\\ \vdots & \vdots & \vdots & & \ddots & -1\\ 0 & -1 & -1 & \ldots & -1 & 0 \end{pmatrix} = <1>\boxplus A.$$

A est du type $I_{8k} - J_{8k}$ où $J_{8k} = \begin{pmatrix}1&\ldots&1\\ \vdots& &\vdots\\ 1&\ldots&1\end{pmatrix}$. Bien sûr, $J_{8k}^2 \equiv 0 \pmod 8$, donc $A\cdot(I_{8k}+J_{8k}) = I_{8k}$.

Ce qui veut dire que A, donc M, est inversible. Et trivialement A ne représente que des éléments pairs,

"$\Longrightarrow$" :

Montrons la contraposée : sans limiter la généralité, on peut supposer que a_n est pair. Comme $\beta(x,x) = 1$, et vu le lemme 4.6, on a $V = <x>\boxplus<x>^\perp$. De plus, $a_1^2+\cdots+a_{n-1}^2 \equiv 1$ ou $5 \pmod 8$ donc $(a_1,\ldots,a_{n-1})$ possède un supplémentaire orthogonal U de dimension impaire pour la forme β' définie par la matrice I_{n-1}. Alors, il existe $y' = (b_1,\ldots,b_{n-1}) \in U$ tel que $\beta'(y,y)$ soit impair. Finalement, $y = (b_1,\ldots,b_{n-1},0)$ appartient à $<x>^\perp$, et $\beta(y,y)$ est impair. •

Remarque :

Il y a donc 4^n "mauvais vecteurs" si $n \equiv 1 \pmod 8$.

Théorème 4.12

Si $V = (\mathbb{Z}/8\mathbb{Z})^n$ et β est la forme bilinéaire définie par la matrice I_n, alors :

$$|O^n_\beta(\mathbb{Z}/8\mathbb{Z})| = \prod_{k=1}^{n} t'_1(k)$$

$$\text{où} \quad t'_1(k) = \begin{cases} t_1(k) & \text{si } k \not\equiv 1 \pmod 8 \text{ ou } k = 1 \\ t_1(k) - 4^k = 2^{3k-3}(1 - 2^{(1-k)/2})(1 + 2^{(3-k)/2}) & \text{si } k \equiv 1 \pmod 8 \text{ et } k \neq 1 \end{cases}$$

Démonstration :

Par récurrence sur n : si $n = 1$, c'est clair.

Supposons que $n \not\equiv 1 \pmod 8$, et soit $x \in V$ tel que $\beta(x,x) = 1$. On sait que $<x> \boxplus <x>^\perp \simeq (\mathbb{Z}/8\mathbb{Z})^n$, donc vu les lemmes 4.9 et 4.10, $<x>^\perp \simeq (\mathbb{Z}/8\mathbb{Z})^{n-1}$. On conclut alors par récurrence, en raisonnant sur $<x>^\perp$.

Si $n \equiv 1 \pmod 8$, on prend x tel que $\beta(x,x) = 1$, x étant un "bon vecteur". Alors, en faisant le même raisonnement, et en utilisant le lemme 4.11, on conclut. •

Remarque :

Cette formule est en contradiction avec celle citée dans [5, ch. V, §25, pp 186-187], mais nous avons toutes les raisons de croire que la nôtre est la bonne. En particulier parce que la formule de Minkowski-Siegel que nous obtenons lors du chapitre suivant correpond à celle citée dans [4, ch. 16, §2].

CHAPITRE 5

Calcul explicite de la formule de Minkowski-Siegel pour les formes entières et définies positives.

Pour ce chapitre, on se fixe $(M,\beta) \in \mathscr{S}_n$, $V = M \otimes \mathbb{Q}$, μ_p une mesure sur $O(V_p)$ pour tout $p \in \mathbb{P}$, normée de telle manière que $c_{\mu,p} = \frac{1}{2}$, et $M_1 = M, M_2, \ldots, M_k$, des représentants de chaque classe d'équivalence dans $\mathscr{G}_n$, le genre de M.

Théorème 5.1

Rappelons que $m(_{O(V)}\backslash^{\widetilde{O}(V)})$ représente la mesure d'un domaine fondamental pour $\widetilde{O}(V)$ relatif à $O(V)$. Cette constante ne dépend que de n, nous l'appellerons $c(n)$. De plus, on a :

$$c(0) = 1,\ c(1) = \frac{1}{2},\ c(2) = \frac{1}{2\pi} \text{ et } c(n) = \frac{c(n-1)}{n \cdot \rho_n} \quad \text{où } \rho_n \text{ est le volume de la boule } B^n,\ n \geq 3.$$

Démonstration :

Ce résultat, qui demande une bonne vingtaine de pages de preuve, est démontré dans [7, ch.X, § 34.]. Il est aussi prouvé dans [5, Satz 26.1] avec les recommandations d'usage concernant cet ouvrage. Enfin, il est démontré dans l'article originel de Siegel [11, Hilfsatz 26 + §9 et §10]. •

Corollaire 5.2

$$c(n) = \begin{cases} \pi^{\frac{1-n^2}{4}} \cdot 2^{\frac{-n^2-8n-9}{8}} \cdot \prod_{i=1}^{\frac{n-1}{2}} 1 \cdot 3 \cdot \cdots \cdot (2i-1) \cdot (i-1)! & \text{si } n \text{ est impair} \\ \pi^{\frac{-n^2}{4}} \cdot 2^{\frac{-n^2-6n-8}{8}} \cdot (\frac{n-2}{2})! \cdot \prod_{i=1}^{\frac{n-2}{2}} 1 \cdot 3 \cdot \cdots \cdot (2i-1) \cdot (i-1)! & \text{si } n \text{ est pair.} \end{cases}$$

Démonstration :

On rappelle que

$$\rho_n = \frac{\pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2}+1)},$$

où Γ est définie par $\Gamma(z) = \int_0^\infty t^{z-1} e^{-t}\, dt$. Cette fonction est définie sur les nombres complexes de partie réelle strictement positive. On a :

$$c(n) = \frac{c(n-1)\Gamma(\frac{n}{2}+1)}{n \cdot \pi^{\frac{n}{2}}} = \cdots = \frac{\pi^{\frac{1}{2}} \cdot \prod_{i=3}^{n} \Gamma(\frac{i}{2}+1)}{n! \cdot \pi^{\frac{n}{2}} \cdot \cdots \cdot \pi^{\frac{1}{2}}}$$
$$= \frac{2 \cdot \prod_{i=1}^{n} \Gamma(\frac{i}{2}+1)}{n! \cdot \pi^{\frac{n(n+1)}{4}}}.$$

La dernière égalité utilise le fait que $\Gamma(\frac{3}{2}) = \frac{1}{2} \cdot \pi^{\frac{1}{2}}$ et que $\Gamma(2) = 1$. Ces propriétés de la fonction Γ ainsi que toutes celles que j'utiliserai par la suite sont citées dans [1, ch. 6].

Comme autre propriété, on a que $\Gamma(z+1) = z\Gamma(z)\ \forall z$, donc

$$c(n) = \frac{\prod_{i=1}^{n} \Gamma(\frac{i}{2})}{2^{n-1} \cdot \pi^{\frac{n(n+1)}{4}}}.$$

La fonction Γ est telle que :

$$\Gamma(m+1) = m! \quad \text{et} \quad \Gamma(m+\frac{1}{2}) = \frac{1\cdot 3\cdot\cdots\cdot(2m-1)}{2^m}\pi^{\frac{1}{2}} \quad \text{pour tout } m \in \mathbb{N}.$$

Supposons que n soit impair. On a :

$$\prod_{i=2,4,\ldots,n-1} \Gamma(\frac{i}{2}) = \prod_{i=1}^{\frac{n-1}{2}} \Gamma(i) = \prod_{i=1}^{\frac{n-1}{2}} (i-1)! \ .$$

On a aussi :

$$\begin{aligned}\prod_{i=1,3,\ldots,n} \Gamma(\frac{i}{2}) &= \prod_{i=0}^{\frac{n-1}{2}} \Gamma(i+\frac{1}{2}) = \pi^{\frac{1}{2}} \cdot \prod_{i=1}^{\frac{n-1}{2}} \frac{1\cdot 3\cdot\cdots\cdot(2i-1)\cdot\pi^{\frac{1}{2}}}{2^i} \\ &= 2^{\frac{1-n^2}{8}} \cdot \pi^{\frac{n+1}{4}} \prod_{i=1}^{\frac{n-1}{2}} 1\cdot 3\cdot\cdots\cdot(2i-1).\end{aligned}$$

D'où :

$$c(n) = \pi^{\frac{1-n^2}{4}} \cdot 2^{\frac{-n^2-8n+9}{8}} \cdot \prod_{i=1}^{\frac{n-1}{2}} 1\cdot 3\cdot\cdots\cdot(2i-1)\cdot(i-1)! \ .$$

Si n est pair, on a :

$$\prod_{i=2,4,\ldots,n} \Gamma(\frac{i}{2}) = \prod_{i=1}^{\frac{n}{2}} (i-1)! \ .$$

et

$$\begin{aligned}\prod_{i=1,3,\ldots,n-1} \Gamma(\frac{i}{2}) &= \pi^{\frac{1}{2}} \cdot \prod_{i=1}^{\frac{n-2}{2}} \frac{1\cdot 3\cdot\cdots\cdot(2i-1)\cdot\pi^{\frac{1}{2}}}{2^i} \\ &= 2^{\frac{(2-n)n}{8}} \cdot \pi^{\frac{n}{4}} \prod_{i=1}^{\frac{n-2}{2}} 1\cdot 3\cdot\cdots\cdot(2i-1).\end{aligned}$$

Donc

$$c(n) = \pi^{\frac{-n^2}{4}} \cdot 2^{\frac{-n^2-6n-8}{8}} \cdot (\frac{n-2}{2})! \cdot \prod_{i=1}^{\frac{n-2}{2}} 1\cdot 3\cdot\cdots\cdot(2i-1)\cdot(i-1)! \ .$$

•

A. La formule de Minkowski-Siegel dans le cas de $\mathscr{C}_n$.

Supposons que M soit de type (II). Alors, $n \equiv 0 \bmod 8$. Posons $q(x) = \frac{1}{2}\beta(x,x)$, M est un module quadratique non dégénéré pour cette forme. On a donc $M_p = M_p^{\#}$, pour tout $p \in \mathbb{P}$. On obtient alors grâce au corollaire 2.49, au théorème 2.59, ainsi qu'au théorème 3.8 et au corollaire 3.9 :

$$\mathscr{M}_{\mathscr{C}_n} = c(n) \cdot \prod_{p\in\mathbb{P}} (1-p^{-\frac{n}{2}})^{-1} \cdot \prod_{p\in\mathbb{P}} \prod_{0<2i<n} (1-p^{-2i})^{-1} \ .$$

Ceci, parce que le discriminant de M vaut 1.

Théorème 5.3

On a :

$$\mathscr{M}_{\mathscr{C}_n} = 2^{1-n} \cdot \frac{|B_{\frac{n}{2}}|}{(\frac{n}{2})!} \cdot \prod_{i=1}^{\frac{n}{2}-1} |B_{2i}| \ ,$$

où B_i sont les nombres de Bernoulli. Ces nombres sont définis dans [1, ch. 23] par exemple.

Démonstration :

Nous avons tout d'abord besoin d'un résultat classique sur la fonction ζ de Riemann :

$$\zeta(2i) = \prod_{p\in\mathbb{P}}(1-p^{-2i})^{-1} = \frac{(2\pi)^{2i}}{2(2i)!}|B_{2i}|.$$

Ce résultat est démontré dans [10, ch. VII, Proposition 7]. On trouve alors :

$$\mathscr{M}_{\mathscr{G}_n} = \pi^{\frac{-n^2}{4}} \cdot 2^{\frac{-n^2-6n+8}{8}} \cdot (\frac{n-2}{2})! \cdot \prod_{i=1}^{\frac{n-2}{2}} 1\cdot 3\cdot\cdots\cdot(2i-1)\cdot(i-1)! \cdot \frac{(2\pi)^{\frac{n}{2}}}{2} \cdot \prod_{0<2i<n} \frac{(2\pi)^{2i}}{2(2i)!} \cdot K,$$

où $K = \dfrac{|B_{\frac{n}{2}}|}{(\frac{n}{2})!} \cdot \displaystyle\prod_{i=1}^{\frac{n}{2}-1} |B_{2i}|$. En développant, on trouve :

$$\begin{aligned}
\mathscr{M}_{\mathscr{G}_n} &= \pi^{\frac{-n^2+2n}{4}} \cdot \pi^{\frac{n^2-2n}{4}} \cdot 2^{\frac{-n^2-6n}{8}} \cdot 2^{\frac{n}{2}} \cdot 2^{\frac{-n+2}{2}} \cdot 2^{\frac{n^2-2n}{4}} \cdot (\frac{n-2}{2})! \cdot \prod_{i=1}^{\frac{n-2}{2}} \frac{1\cdot 3\cdot\cdots\cdot(2i-1)(i-1)!}{(2i)!} \cdot K \\
&= 2^{\frac{n^2-10n+8}{8}} \cdot (\frac{n-2}{2})! \cdot \prod_{i=1}^{\frac{n-2}{2}} \frac{(i-1)!}{2^i\cdot i!} \cdot K \\
&= 2^{\frac{n^2-10n+8}{8}} \cdot \prod_{i=1}^{\frac{n-2}{2}} \frac{1}{2^i} \cdot K \\
&= 2^{1-n} \cdot K.
\end{aligned}$$

•

B. La formule de Minkowski-Siegel dans le cas de $\mathscr{H}_n$.

Supposons maintenant que M soit de type (I). Puisque la formule ne dépend que du genre, on peut supposer que β soit la forme $x_1y_1 + \cdots + x_ny_n$. Posons $q(x) = \beta(x,x)$. Cette fois-ci, (M,q) est un module quadratique dégénéré. On a néanmoins $M_p = M_p^{\#}$ pour tout p différent de 2. Pour $p=2$, on trouve $M_2 = 2M_2^{\#}$. Le but est de calculer $\mu_2(O(M_2))$. Grâce au théorème 2.57, nous savons que $c_{\mu,2}$ est constant si $k=4$ par exemple. On a :

$$\mu_2(O(M_2)) = [O(M_2) : O(V_2, M_2/2^4M_2^{\#})] \cdot \mu_2(O(V_2, M_2/2^4M_2^{\#})).$$

On trouve alors, par la définition de $c_{\mu,2}$:

$$\mu_2(O(V_2, M_2/2^4M_2^{\#})) = c_{\mu,2} \cdot [M_2 : 2^3M_2]^{\frac{1-n}{2}} = c_{\mu,2} \cdot 2^{\frac{3n(1-n)}{2}}.$$

Proposition 5.4

Posons $\overline{M_2} = M_2/2^3M_2$ vu comme $\mathbb{Z}/8\mathbb{Z}$-module. Alors :

$$[O(M_2) : O(V_2, M_2/2^3M_2)] = |O_\beta^n(\overline{M_2})| \cdot \frac{1}{2^n} = |O_\beta^n(\mathbb{Z}/8\mathbb{Z})| \cdot \frac{1}{2^n}.$$

Le groupe $O_\beta^n(\mathbb{Z}/8\mathbb{Z})$ à été défini au chapitre 4.

Démonstration :

L'application :

$$\begin{aligned}
\psi \,:\, O(M_2) &\longrightarrow O_\beta^n(\mathbb{Z}/8\mathbb{Z}) \\
u &\longmapsto \quad \overline{u} \,:\, \overline{M_2} \longrightarrow \overline{M_2} \\
&\qquad x + 2^3M_2 \longmapsto u(x) + 2^3M_2
\end{aligned}$$

est bien définie * . Son noyau est bien $O(V_2, M_2/2^3M_2)$. Mais on ne peut pas utiliser le lemme 2.52, donc ψ n'est pas forcément surjective. On va montrer que $[O^n_\beta(\mathbb{Z}/8\mathbb{Z}) : \mathrm{Im}(\psi)] = 2^n$.
Soit $\overline{u} \in O^n_\beta(\mathbb{Z}/8\mathbb{Z})$. $\overline{u}$ peut être représentée par une matrice $A \in M_n(\mathbb{Z}_2)$ telle que $A \cdot A^t = I_n + 8 \cdot B$ où B est une matrice symétrique. Soit

$$\varphi : O^n_\beta(\mathbb{Z}/8\mathbb{Z}) \longrightarrow (\mathbb{F}_2)^n$$
$$A \longmapsto \mathrm{diag}(B) \pmod 2 \quad \text{avec } B \text{ telle que } 8B = AA^t - I_n.$$

Lemme

φ est bien définie, en outre, $\varphi(A) = (0, \ldots, 0)$ si et seulement si $A \in \mathrm{Im}(\psi)$

Démonstration du lemme

Soit $A \in O^n_\beta(\mathbb{Z}/8\mathbb{Z})$. Supposons que A_1 et $A_2 \in M_n(\mathbb{Z}_2)$ sont telles que $\overline{A_1} = \overline{A_2} = A$. Il existe $C \in M_n(\mathbb{Z}_2)$ telle que $A_1 = A_2 + 8C$. On a :

$$I_n + 8B_1 = A_1A_1^t = (A_2 + 8C)(A_2^t + 8C^t) = I_n + 8(B_2 + A_2C^t + CA_2^t + 8CC^t).$$

Et on remarque que

$$\mathrm{diag}(B_1) \equiv \mathrm{diag}(B_2 + A_2C^t + CA_2^t + 8CC^t) \equiv \mathrm{diag}(B_2) \pmod 2,$$

car $\mathrm{diag}(X + X^t) \equiv 0 \bmod 2 \ \forall X \in M_n(\mathbb{Z}_2)$. Donc φ est bien définie.
Soit $\overline{A} \in \mathrm{Im}(\psi)$; il existe en particulier X et B telles que

$$(A + 8X) \cdot (A + 8X)^t = I_n + 8(B + AX^t + XA^t) \equiv I_n \pmod{16}.$$

Donc $B \equiv (AX^t + XA^t) \bmod 2$, ce qui veut dire que $\mathrm{diag}(B) \equiv (0, \ldots, 0) \bmod 2$.
Réciproquement, soit $AA^t = I_n + 8B$, avec B n'ayant que des éléments pairs dans la diagonale. Posons B^-, la matrice triangulaire inférieure telle que $B^- + B^{-t} = B$. On a :

$$(A - 8B^- A)(A - 8B^- A)^t \equiv I_n \pmod{16}$$

et $A_1 := (A - 8B^- A) \equiv A \bmod 8$. On refait le même raisonnement, on a $A_1A_1^t = I_n + 16B_1$. On vérifie que $\mathrm{diag}(B_1) \equiv (0, \ldots, 0) \bmod 2$, et on obtient $A_2 = A_1 + 16C_1 \in M_n(\mathbb{Z}_2)$ telle que $A_2A_2^t \equiv I_n \bmod 32$. Et ainsi de suite; on trouve alors une suite $(A_n)_{n\in\mathbb{N}}$ qui converge dans $M_n(\mathbb{Z}_2)$. La limite de cette suite est une matrice X de $O(M_2)$, et on a $X \equiv A \bmod 8$. Donc $\overline{A} \in \mathrm{Im}(\psi)$.
Ainsi s'achève la démonstration du lemme.

Notre application φ est surjective. En effet, soit $B \in M_n(\mathbb{Z}_2)$ symétrique. La somme

$$I_n + \frac{1}{2} \cdot (8B) - \frac{1}{2^2 \cdot 2} \cdot (8B)^2 + \frac{1 \cdot 3}{2^3 \cdot 2 \cdot 3} \cdot (8B)^3 + \cdots + (-1)^{n-1} \cdot \frac{1 \cdot 3 \cdot \cdots \cdot (2n-3)}{2^n \cdot n!} \cdot (8B)^n + \cdots$$

converge. En effet, dans $n!$ nous avons au plus $[\frac{n}{2}] + [\frac{n}{4}] + \cdots$ facteurs 2. Or,

$$[\frac{n}{2}] + [\frac{n}{4}] + \cdots \leq \frac{n}{2} + \frac{n}{4} + \cdots = n \cdot (\frac{1}{2} + \frac{1}{4} + \cdots) = n.$$

La norme p-adique du n-ième terme de notre série est donc au plus 2^{-n}, elle est alors convergente. Notons A sa limite, qui est une matrice symétrique puisque B l'est.

---

* Remarquons que ψ aurait été bien définie aussi, si nous avions pris $O^n_q(\mathbb{Z}/8\mathbb{Z})$ comme groupe d'arrivée. Nous prenons alors le plus petit des deux (voir le premier paragraphe du chapitre 4).

Tout le monde aura reconnu dans cette somme, le développement de Taylor de $\sqrt{I_n + 8B}$. Donc, on a :

$$A^2 = A \cdot A^t = I_n + 8B.$$

φ est donc surjective, il suffit de prendre B avec une diagonale convenable.
Il nous reste à voir que $A_1^{-1}A_2 \in \mathrm{Im}(\psi)$ si et seulement si $\varphi(A_1) = \varphi(A_2)$.
Supposons que $A_1^{-1}A_2 \in \mathrm{Im}(\psi)$. On a $(A_1^{-1}A_2)(A_1^{-1}A_2)^t = I_n + 8B$ avec B symétrique ne comportant que des éléments pairs dans la diagonale. Calculons :

$$(A_1^{-1}A_2)(A_1^{-1}A_2)^t = A_1^{-1}(I_n + 8B_2)A_1^{t^{-1}}.$$

On vérifie que $A_1^{-1}A_1^{t^{-1}} = I_n - 8A_1^{-1}B_1A_1^{t^{-1}}$. On trouve finalement :

$$I_n + 8B = I_n + 8A_1^{-1}(B_2 - B_1)A_1^{t^{-1}}.$$

Autrement dit, $A_1^{-1}(B_2 - B_1)A_1^{t^{-1}} \equiv B \bmod 2$; donc $\mathrm{diag}(B_2 - B_1) \equiv 0 \bmod 2$, ce qui veut dire que $\varphi(A_1) = \varphi(A_2)$.
On démontre la réciproque de manière identique. •

Lemme 5.5

Supposons que n soit impair, alors on a :

$$c(n) \cdot \prod_{0<2i<n} \prod_{p\in\mathbb{P}} (1 - p^{-2i})^{-1} = 2^{\frac{n-1}{2}} \cdot 2^{-2n+2} \cdot \frac{1}{(\frac{n-1}{2})!} \cdot |B_2 \cdot \cdots \cdot B_{n-1}|.$$

Démonstration :

Le corollaire 5.2 nous permet de dire :

$$\begin{aligned}
c(n) \cdot \prod_{0<2i<n} \prod_{p\in\mathbb{P}} (1 - p^{-2i})^{-1} &= \pi^{\frac{1-n^2}{4}} \cdot 2^{\frac{-n^2-8n+9}{8}} \cdot \prod_{i=1}^{\frac{n-1}{2}} 1 \cdot 3 \cdot \cdots \cdot (2i-1) \cdot (i-1)! \cdot \prod_{i=2,4,\ldots,n-1} \frac{|B_i| \cdot (2\pi)^i}{2 \cdot (i)!} \\
&= \pi^{\frac{1-n^2}{4}} \cdot 2^{\frac{-n^2-8n+9}{8}} \cdot (2\pi)^{\frac{2(n^2-1)}{8}} \cdot \prod_{i=1}^{\frac{n-1}{2}} \frac{1 \cdot 3 \cdot \cdots \cdot (2i-1)}{(2i)!} \cdot \frac{1}{2} \cdot (i-1)! \cdot \prod_{i=1}^{\frac{n-1}{2}} |B_{2i}| \\
&= 2^{\frac{n^2-8n+7}{8}} \cdot 2^{\frac{1-n}{2}} \cdot \prod_{i=1}^{\frac{n-1}{2}} \frac{(i-1)!}{(2 \cdot 4 \cdot \cdots \cdot 2i)} \cdot |B_2 \cdot \cdots \cdot B_{n-1}| \\
&= 2^{\frac{n^2-12n+11}{8}} \cdot 2^{\frac{1-n^2}{8}} \cdot \prod_{i=1}^{\frac{n-1}{2}} \frac{1}{i} \\
&= 2^{\frac{n-1}{2}} \cdot 2^{-2n+2} \cdot \frac{1}{(\frac{n-1}{2})!} \cdot |B_2 \cdot \cdots \cdot B_{n-1}|.
\end{aligned}$$

•

Lemme 5.6

Posons $\kappa(s) = \sum_{k=1}^{\infty} (-1)^k (2k+1)^{-s}$. Alors, pour tout $m \in \mathbb{N}$, on a

$$\kappa(2m+1) = \prod_{p\in\mathbb{P}\setminus\{2\}} (1 - (-1)^{\frac{p-1}{2}} \cdot p^{-(2m+1)}) = \frac{(\pi/2)^{2m+1}}{2(2m)!} |E_{2m}|,$$

Où E_i sont les nombres d'Euler. Ces nombres sont définis dans [1,ch. 23] par exemple.

Démonstration :

La deuxième égalité est citée dans [1, 23.2.22]. D'autre part, on a

$$\kappa(s) = \sum_{n=1}^{\infty} \frac{c_n}{n^s}.$$

On vérifie sans peine que les c_n sont multiplicatifs, donc

$$\kappa(s) = \prod_{p \in \mathbb{P}} \sum_{m=0}^{\infty} c_{p^m} p^{-ms}.$$

Or,

$$c_{p^m} = \begin{cases} 1 & \text{si } p \equiv 1 \pmod 4 \\ (-1)^m & \text{si } p \equiv 3 \pmod 4 \\ 0 & \text{si } p = 2 \end{cases}$$

On trouve alors $c_{p^m} = (-1)^{\frac{(p-1)m}{2}}$ si p est impair. Pour un tel p, on a :

$$\sum_{m=0}^{\infty} ((-1)^{\frac{p-1}{2}} \cdot p^{-s})^m = (1 - (-1)^{\frac{p-1}{2}} \cdot p^{-s}),$$

par propriété des séries géométriques. On a donc bien :

$$\kappa(s) = \prod_{p \in \mathbb{P} \setminus \{2\}} (1 - (-1)^{\frac{p-1}{2}} \cdot p^{-(2m+1)}).$$

•

Lemme 5.7

Supposons que $n \equiv \pm 2 \bmod 8$, alors on a :

$$c(n) \cdot \prod_{0<2i<n} (1 - p^{-2i})^{-1} \cdot \prod_{p \in \mathbb{P} \setminus \{2\}} (1 - (-1)^{\frac{p-1}{2}} \cdot p^{-\frac{n}{2}}) = \frac{2^{-2n+1}}{(\frac{n-2}{2})!} \cdot |E_{\frac{n-2}{2}} \cdot B_2 \cdot \cdots \cdot B_{n-2}|.$$

Démonstration :

$$\begin{aligned} c(n) \cdot \prod_{0<2i<n} (1 - p^{-2i})^{-1} \cdot \prod_{p \in \mathbb{P} \setminus \{2\}} (1 - (-1)^{\frac{p-1}{2}} \cdot p^{-\frac{n}{2}}) &= \pi^{\frac{-n^2}{4}} \cdot 2^{\frac{-n^2-6n+8}{8}} \cdot (\frac{n-2}{2})! \cdot \frac{(\frac{\pi}{2})^{\frac{n}{2}}}{2(\frac{n-2}{2})!} \cdot |E_{\frac{n-2}{2}}| \\ &= \cdot \prod_{i=1}^{\frac{n-2}{2}} 1 \cdot 3 \cdot \cdots \cdot (2i-1) \cdot (i-1)! \cdot \prod_{i=1}^{\frac{n-2}{2}} \frac{(2\pi)^{2i}}{2(2i)!} |B_{2i}| \\ &= \cdots \\ &= \frac{2^{-2n+1}}{(\frac{n-2}{2})!} \cdot |E_{\frac{n-2}{2}} \cdot B_2 \cdot \cdots \cdot B_{n-2}|. \end{aligned}$$

•

Nous voilà enfin prêt à démontrer le théorème principal de ce diplôme.

Théorème 5.8

$$\mathscr{M}_{\mathscr{H}_n} = \begin{cases} \dfrac{(1+2^{\frac{2-n}{2}})(1-2^{\frac{-n}{2}})}{2\cdot(\frac{n}{2})!}\cdot|B_{\frac{n}{2}}\cdot B_2\cdot\cdots\cdot B_{n-2}| & \text{si } n\equiv 0 \pmod 8 \\ \dfrac{(2^{\frac{n-1}{2}}+1)}{2^n\cdot(\frac{n-1}{2})!}\cdot|B_2\cdot\cdots\cdot B_{n-1}| & \text{si } n\equiv \pm 1 \pmod 8 \\ \dfrac{1}{2^{n+1}\cdot(\frac{n-2}{2})!}\cdot|E_{\frac{n-2}{2}}\cdot B_2\cdot\cdots\cdot B_{n-2}| & \text{si } n\equiv \pm 2 \pmod 8 \\ \dfrac{(2^{\frac{n-1}{2}}-1)}{2^n\cdot(\frac{n-1}{2})!}\cdot|B_2\cdot\cdots\cdot B_{n-1}| & \text{si } n\equiv \pm 3 \pmod 8 \\ \dfrac{(1-2^{\frac{2-n}{2}})(1-2^{\frac{-n}{2}})}{2\cdot(\frac{n}{2})!}\cdot|B_{\frac{n}{2}}\cdot B_2\cdot\cdots\cdot B_{n-2}| & \text{si } n\equiv 4 \pmod 8. \end{cases}$$

Démonstration :

Vu la proposition 5.4 et le théorème 4.12, on a :

$$\begin{aligned}\mu_2(O(M_2)) &= c_{\mu,2}\cdot 2^{\frac{3n(1-n)}{2}}\cdot 2^{-n}\cdot|O^n_\beta(\mathbb{Z}/8\mathbb{Z})| \\ &= 2^{-n^2-1}\cdot 2^{\frac{3n(1-n)}{2}}\prod_{k=1}^{n}\ell'_1(k).\end{aligned}$$

a) Supposons que $n=8$. On a, grâce au théorème 4.12 et à la proposition 4.4 :

$$\begin{aligned}\mu_2(O(M_2)) &= 2^{-9}\cdot 2^{-84}\cdot 2^{3\cdot 6+\cdots+21}\cdot 8\cdot\frac{1}{(1+2^{-3})(1-2^{-4})}\cdot(1-2^{-2})(1-2^{-4})(1-2^{-6})(1-2^{-4}) \\ &= 2^{-6}\cdot\frac{1}{(1+2^{-3})(1-2^{-4})}\cdot(1-2^{-2})(1-2^{-4})(1-2^{-6})(1-2^{-4}).\end{aligned}$$

Si $p\neq 2$, on trouve comme pour le type (II)

$$\mu_p(O(M_p)) = (1-p^{-4})\cdot\prod_{0<2i<8}(1-p^{-2i}).$$

On trouve alors

$$\begin{aligned}\mathscr{M}_{\mathscr{H}_8} &= c(8)\cdot\prod_{p\in\mathbb{P}}(1-p^{-4})^{-1}\cdot\prod_{0<2i<8}\prod_{p\in\mathbb{P}}(1-p^{-2i})\cdot\frac{(1+2^{-3})(1-2^{-4})}{2^{-6}} \\ &= \frac{(1+2^{-3})(1-2^{-4})}{2^{7-6}\cdot 4!}\cdot|B_4\cdot B_2\cdot B_4\cdot B_6|.\end{aligned}$$

La dernière égalité vient du calcul fait pour le type (II).

b) Supposons $n\equiv 0 \bmod 8$, $n>8$, et que

$$|O^{n-8}_\beta| = \frac{2^{\frac{3(n-8)(n-9)}{2}}\cdot 8}{(1+2^{\frac{10-n}{2}})}(1-2^{-2})(1-2^{-4})\cdot\cdots\cdot(1-2^{10-n}).$$

Calculons :

$$\begin{aligned}|O^n_\beta| &= 2^{3[(n-1)+\cdots+(n-8)]}(1-2^{\frac{2-n}{2}})(1-2^{\frac{4-n}{2}})(1+2^{\frac{4-n}{2}})(1-2^{\frac{6-n}{2}})(1+2^{\frac{6-n}{2}}) \\ &\quad\cdot(1+2^{\frac{8-n}{2}})(1-2^{\frac{8-n}{2}})(1+2^{\frac{10-n}{2}})\cdot|O^{n-8}_\beta| \\ &= 2^{\frac{3(2n-9)+3(n-8)(n-9)}{2}}\cdot 8\cdot(1-2^{\frac{2-n}{2}})(1-2^{4-n})(1-2^{6-n})(1-2^{8-n})(1+2^{\frac{10-n}{2}}) \\ &\quad\cdot\frac{1}{(1+2^{\frac{10-n}{2}})}\cdot(1-2^{-2})(1-2^{-4})\cdot\cdots\cdot(1-2^{10-n}) \\ &= \frac{2^{\frac{3n(n-1)}{2}}\cdot 8}{(1+2^{\frac{2-n}{2}})(1-2^{\frac{n}{2}})}\cdot(1-2^{-2})(1-2^{-4})\cdot\cdots\cdot(1-2^{2-n})\cdot(1-2^{-\frac{n}{2}}).\end{aligned}$$

Donc,

$$\begin{aligned}\mu_2(O(M_2)) &= c_{\mu,2}\cdot 2^{-\frac{3n(n-1)}{2}}\cdot 2^{-n}\cdot |O_p^n(\mathbb{Z}/8\mathbb{Z})| \\ &= \frac{4\cdot 2^{-n}}{(1+2^{\frac{2-n}{2}})(1-2^{-\frac{n}{2}})}\cdot (1-2^{-2})(1-2^{-4})\cdot\cdots\cdot(1-2^{2-n})\cdot(1-2^{-\frac{n}{2}}).\end{aligned}$$

On trouve alors :

$$\begin{aligned}\mathscr{M}_{\mathscr{L}_n} &= c(n)\cdot\prod_{p\in\mathbb{P}}(1-p^{-\frac{n}{2}})^{-1}\cdot\prod_{0<2i<n}\prod_{p\in\mathbb{P}}(1-p^{-2i})\cdot\frac{(1+2^{\frac{2-n}{2}})(1-2^{-\frac{n}{2}})}{4\cdot 2^{-n}} \\ &= \frac{(1+2^{\frac{2-n}{2}})(1-2^{-\frac{n}{2}})}{4\cdot(\frac{n}{2})!\cdot 2^{-n}\cdot 2^{n-1}}\cdot|B_{\frac{n}{2}}\cdot B_2\cdot\cdots\cdot B_{n-2}| \\ &= \frac{(1+2^{\frac{2-n}{2}})(1-2^{-\frac{n}{2}})}{2\cdot(\frac{n}{2})!}\cdot|B_{\frac{n}{2}}\cdot B_2\cdot\cdots\cdot B_{n-2}|.\end{aligned}$$

c) Supposons $n\equiv 1 \bmod 8$.

Si $n=1$, on a clairement que $\mathscr{M}_{\mathscr{L}_1}=\frac{1}{2}$. Supposons donc $n\neq 1$. Grâce au calcul précédent, à la proposition 4.2 et au théorème 4.10, nous pouvons dire que

$$\begin{aligned}\mu_2(O(M_2)) &= 2^{-n-1}\cdot 2^{-\frac{3n(n-1)}{2}}\cdot\frac{2^{\frac{3n(n-1)}{2}}\cdot 8}{(1+2^{\frac{3-n}{2}})}\cdot(1-2^n)\cdot\cdots\cdot(1-2^{3-n})(1-2^{\frac{1-n}{2}})(1+2^{\frac{3-n}{2}}) \\ &= \frac{2^{-n\cdot 2}}{(1+2^{\frac{1-n}{2}})}(1-2^n)\cdot\cdots\cdot(1-2^{3-n})(1-2^{1-n}).\end{aligned}$$

Le lemme 5.5 nous donne alors :

$$\begin{aligned}\mathscr{M}_{\mathscr{L}_n} &= \frac{(1+2^{\frac{1-n}{2}})\cdot 2^{\frac{n-1}{2}}}{2^{2n-2-n+2}\cdot(\frac{n-1}{2})!}\cdot|B_2\cdot\cdots\cdot B_{n-1}| \\ &= \frac{(2^{\frac{n-1}{2}}+1)}{2^n\cdot(\frac{n-1}{2})!}\cdot|B_2\cdot\cdots\cdot B_{n-1}|.\end{aligned}$$

d) Supposons $n\equiv 2 \bmod 8$.

Calculons :

$$\begin{aligned}\mu_2(O(M_2)) &= c_{\mu,2}\cdot 2^{-\frac{3n(n-1)}{2}}\cdot 2^{-n}\cdot 2^{\frac{3n(n-1)}{2}}\cdot\frac{8}{1+2^{\frac{2-n}{2}}}\cdot(1-2^{-2})(1-2^{-4})\cdot\cdots\cdot(1-2^{2-n})(1+2^{\frac{2-n}{2}}) \\ &= 2^{-n+2}\cdot(1-2^{-2})(1-2^{-4})\cdot\cdots\cdot(1-2^{2-n}).\end{aligned}$$

Or, le discriminant de M vaut -2^n; donc, si p est impair, le symbole de Legendre $(\frac{-2^n}{p})=(\frac{-1}{p})=(-1)^{\frac{p-1}{2}}$.
On trouve alors :

$$\begin{aligned}\mathscr{M}_{\mathscr{L}_n} &= 2^{n-2}\cdot c(n)\cdot\prod_{0<2i<n}(1-p^{2i})^{-1}\cdot\prod_{p\in\mathbb{P}\setminus\{2\}}(1-(-1)^{\frac{p-1}{2}}p) \\ &\overset{\text{lemme 5.7}}{=} \frac{2^{n-2}\cdot 2^{n-1}}{(\frac{n-1}{2})!}\cdot|E_{\frac{n-2}{2}}\cdot B_2\cdot\cdots\cdot B_{n-2}|. \\ &= \frac{1}{2^{n-1}\cdot(\frac{n-1}{2})!}\cdot|E_{\frac{n-2}{2}}\cdot B_2\cdot\cdots\cdot B_{n-2}|.\end{aligned}$$

e) Supposons $n\equiv 3 \bmod 8$.

On trouve :

$$\mu_2(O(M_2)) = c_{\mu,2}\cdot 2^{-n}\cdot(1-2^{-2})(1-2^{-4})\cdot\cdots\cdot(1-2^{3-n})(1-2^{1-n})\cdot\frac{8}{(1-2^{\frac{1-n}{2}})}.$$

D'où

$$\begin{aligned}\mathscr{M}_{\mathscr{L}_n} &= 2^{n-2}\cdot(1-2^{\frac{1-n}{2}})\cdot c(n)\cdot\prod_{0<2i<n}\prod_{p\in\mathbb{P}}(1-p^{-2i})^{-1}\\ &\overset{\text{lemme 5.5}}{=} 2^{\frac{2n-4-4n+4}{2}}\cdot\frac{(2^{\frac{n-1}{2}}-1)}{(\frac{n-1}{2})!}\cdot|B_2\cdot\dots\cdot B_{n-1}|.\\ &= \frac{(2^{\frac{n-1}{2}}-1)}{2^n\cdot(\frac{n-1}{2})!}\cdot|B_2\cdot\dots\cdot B_{n-1}|.\end{aligned}$$

f) Supposons $n\equiv 4 \bmod 8$.

On obtient :

$$\mu_2(O(M_2)) = \frac{2^{-n+2}}{(1-2^{\frac{2-n}{2}})(1-2^{\frac{-n}{2}})}\cdot(1-2^{-2})(1-2^{-4})\cdot\dots\cdot(1-2^{2-n})(1-2^{\frac{-n}{2}}).$$

On a alors :

$$\begin{aligned}\mathscr{M}_{\mathscr{L}_n} &= 2^{n-2}\cdot(1-2^{\frac{2-n}{2}})(1-2^{\frac{-n}{2}})\cdot c(n)\cdot\prod_{p\subset\mathbb{P}}(1-p^{\frac{-n}{2}})\cdot\prod_{0<2i<n}\prod_{p\subset\mathbb{P}}(1-p^{-2i})^{-1}\\ &\overset{\text{th.5.3}}{=} 2^{n-2-n+1}\cdot\frac{(1-2^{\frac{2-n}{2}})(1-2^{\frac{-n}{2}})}{(\frac{n}{2})!}\cdot|B_{\frac{n}{2}}\cdot B_2\cdot\dots\cdot B_{n-2}|.\end{aligned}$$

g) Supposons $n\equiv 5 \bmod 8$.

On a :

$$\begin{aligned}\mu_2(O(M_2)) &= \frac{2^{-n+2}}{(1-2^{\frac{3-n}{2}})}\cdot(1-2^{-2})(1-2^{-4})\cdot\dots\cdot(1-2^{3-n})\cdot(1-2^{\frac{3-n}{2}})\cdot(1+2^{\frac{1-n}{2}})\\ &= \frac{2^{-n-2}}{(1-2^{\frac{1-n}{2}})}\cdot(1-2^{-2})(1-2^{-4})\cdot\dots\cdot(1-2^{3-n})\cdot(1-2^{1-n}).\end{aligned}$$

Comme pour $n\equiv 3 \bmod 8$, le lemme 5.5 nous permet de dire que

$$\mathscr{M}_{\mathscr{L}_n} = \frac{(2^{\frac{n-1}{2}}-1)}{2^n\cdot(\frac{n-1}{2})!}\cdot|B_2\cdot\dots\cdot B_{n-1}|.$$

h) Supposons $n\equiv 6 \bmod 8$.

On trouve :

$$\begin{aligned}\mu_2(O(M_2)) &= \frac{2^{-n+2}}{(1-2^{\frac{2-n}{2}})}\cdot(1-2^{-2})(1-2^{-4})\cdot\dots\cdot(1-2^{4-n})\cdot(1-2^{2-n})\cdot(1+2^{\frac{2-n}{2}})\\ &= 2^{-n+2}\cdot(1-2^{-2})(1-2^{-4})\cdot\dots\cdot(1-2^{4-n})\cdot(1-2^{2-n}).\end{aligned}$$

Par le lemme 5.7, on a :

$$\mathscr{M}_{\mathscr{L}_n} = \frac{1}{2^{n-1}\cdot(\frac{n-2}{2})!}\cdot|E_{\frac{n-2}{2}}\cdot B_2\cdot\dots\cdot B_{n-2}|.$$

i) Supposons enfin que $n\equiv 7 \bmod 8$.

On finit par trouver :

$$\begin{aligned}\mu_2(O(M_2)) &= 2^{-n-2}\cdot(1-2^{-2})(1-2^{-4})\cdot\dots\cdot(1-2^{3-n})\cdot(1+2^{\frac{1-n}{2}})\\ &= \frac{2^{-n-2}}{(1+2^{\frac{1-n}{2}})}\cdot(1-2^{-2})(1-2^{-4})\cdot\dots\cdot(1-2^{3-n})\cdot(1-2^{1-n}).\end{aligned}$$

Le lemme 5.5 nous donne alors :

$$\mathscr{M}_{\mathscr{L}_n} = \frac{(2^{\frac{n-1}{2}}+1)}{2^n\cdot(\frac{n-1}{2})!}\cdot|B_2\cdot\dots\cdot B_{n-1}|.$$

Voilà ! •

C. Applications et conclusion.

La formule de Minkowski-Siegel est utile pour calculer le cardinal de $\mathscr{H}_n$ et de $\mathscr{C}_n$, autrement dit pour trouver le nombre de classes d'équivalences de $\mathscr{S}_n$.

a) Le cas de $\mathscr{C}_n$

Si $n = 8$, on sait que Γ_8 défini au chapitre 1 est un élément de $\mathscr{C}_n$. Il est possible de voir (Bourbaki, groupe et algèbre de Lie, chap. VI, §4, N°10, ou alors [4, ch 2, p. 50]) que

$$|O(\Gamma_8)| = 2^{14} \cdot 3^5 \cdot 5^2 \cdot 7.$$

Or, le théorème 5.3 nous donne

$$\mathscr{M}_{\mathscr{C}_8} = \frac{1}{2^{14} \cdot 3^5 \cdot 5^2 \cdot 7}.$$

On en déduit donc que $|\mathscr{C}_8| = 1$.

Si $n = 16$, posons

$$\Gamma_{16} = \begin{pmatrix}
2 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\
0 & 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 & 0 \\
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4
\end{pmatrix}.$$

On peut montrer que

$$|O(\Gamma_8 \boxplus \Gamma_8)| = 2^{29} \cdot 3^{10} \cdot 5^4 \cdot 7^2 \quad \text{et} \quad |O(\Gamma_{16})| = 2^{15} \cdot (16)!$$

Le théorème 5.3 nous permet d'affirmer que :

$$\mathscr{M}_{\mathscr{C}_{16}} = \frac{1}{2^{29} \cdot 3^{10} \cdot 5^4 \cdot 7^2} + \frac{1}{2^{15} \cdot (16)!}$$

donc que $|\mathscr{C}_{16}| = 2$.

Si $n = 24$, ça ce complique, on a que $|\mathscr{C}_{24}| = 24$. La détermination de ces classes d'équivalences a été faite par H. Niemeier en 1968. La liste de ces réseaux est donnée dans [4, ch. 16 et 18]. Notons que parmi ces réseaux, l'un d'eux est particulièrement remarquable. Il s'agit du réseau de Leech. On le note souvent Λ_{24}. Il ne contient aucun vecteur tel que $\beta(x, x) = 2$, en outre, l'ordre du groupe $O(\Lambda_{24})$ est

$$2^{22} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23.$$

Le quotient $O(\Lambda_{24})/\{\pm 1\}$ est le groupe Co_0 construit par Conway. Il s'agit d'un "groupe simple sporadique".

Pour plus de détail sur le réseau de Leech, voir [4, ch. 8, 12, 23, 24, 25 et 26], voir aussi [4, ch. 10, 11 et 12] à propos de Co_0.

Si $n = 32$, Le théorème 5.3 nous donne que $\mathscr{M}_{\mathscr{C}_{32}} > 4 \cdot 10^7$. Puisque $|O(M)| \geq 2$ pour tout M, on trouve que $\mathscr{C}_{32}$ a plus de 80 millions d'éléments. Un travail similaire à celui de Niemeier pour ce cas paraît humainement inabordable.

b) Le cas de $\mathscr{H}_n$

Si $n \leq 8$, le théorème 5.8 nous donne que

$$\mathscr{M}_{\mathscr{H}_n} = \frac{1}{2^n \cdot n!}$$

Munissons $\mathbb{Z}^n$ de la forme définie par la matrice identité. On a alors $O(\mathbb{Z}^n) = 2^n \cdot n!$ (voir [4, ch. 4, §5]). On obtient donc que le cardinal de $\mathscr{H}_n$ vaut 1. Posons s_n, le nombre de classes d'équivalences de $\mathscr{S}_n$. Ce qui précède ainsi que le paragraphe F du premier chapitre nous donne :

$$s_n = \begin{cases} 1 & \text{si } n \leq 7 \quad \text{(ce résultat était déjà connu par Hermite)} \\ 2 & \text{si } n = 8 \quad \text{(Mordell)} \end{cases}$$

Si $n = 9$, on utilise aussi cette méthode pour trouver que :

$$\mathscr{H}_n = \{\Gamma_8 \boxplus <1>, \mathrm{I}_9\}.$$

donc, $|\mathscr{H}_n| = s_n = 2$.

Finalement, les connaissances actuelles sur ces cardinaux se résument à ce tableau :

n	$1 \leq n \leq 7$	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
$\lvert\mathscr{C}_n\rvert$	0	1	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	24	0	0
$\lvert\mathscr{H}_n\rvert$	1	1	2	2	2	3	3	4	5	6	9	13	16	28	40	68	117	273	665	?
s_n	1	2	2	2	2	3	3	4	5	8	9	13	16	28	40	68	117	297	665	?

Pour plus de détails, voir dans [4].

APPENDICE

Deux nouvelles démonstrations de la proposition 4.5.

Rappelons que le but est de calculer le cardinal des vecteurs de $(\mathbb{Z}/8\mathbb{Z})^n$ de longueur k fixé. On a appelé ce nombre : $t_k(n)$.

Lemme 1.

Posons $\zeta = e^{\frac{2i\pi}{8}}$ et $\Omega = \{\zeta^r \mid 0 \leq r \leq 7\}$. Soit $s \in \mathbb{N}$. On a :

$$\sum_{\omega \in \Omega} \omega^s = \sum_{r=0}^{7} (\zeta^s)^r = \begin{cases} 8 & \text{si } \zeta^s = 1 \\ 0 & \text{sinon.} \end{cases}$$

Démonstration :

Une démonstration de ce fait est donnée dans [10, ch. 6, §1, proposition 4]. Mais bon, on peut aussi le vérifier directement. •

Proposition 4.5

$$t_k(n) = \begin{cases} 2^{3n-3} + 2^{\frac{5n-4}{2}} \cdot \cos\left(\frac{\pi}{4}(2k-n)\right) & \text{si } k \not\equiv n \pmod 4 \\ 2^{3n-3} + 2^{\frac{5n-4}{2}} \cdot \cos\left(\frac{\pi}{4}(2k-n)\right) + (-1)^{(k-n)/4} \cdot 2^{2n-1} & \text{si } k \equiv n \pmod 4 \end{cases}$$

Démonstation de E. Preissmann

Posons $\Psi = \{(l,m) \in \mathbb{Z}^2 \mid l, m \geq 0,\ l+m \leq n \text{ et } m+4l = k\}$. On a :

$$|\{x \in \mathbb{Z}/8\mathbb{Z} \mid x^2 = 0\}| = 2$$
$$|\{x \in \mathbb{Z}/8\mathbb{Z} \mid x^2 = 1\}| = 4$$
$$|\{x \in \mathbb{Z}/8\mathbb{Z} \mid x^2 = 4\}| = 2.$$

Un rapide raisonnement de combinatoire nous donne :

$$t_k(n) = \sum_{l,m \in \Psi} 2^{n-l-m} 4^m 2^l \cdot \binom{n}{l\,m} = 2^n \cdot \sum_{l,m \in \Psi} 2^m \binom{n}{l\,m}.$$

Rappelons que $\binom{n}{l\,m} = \dfrac{n!}{l!\,m!\,(n-l-m)!}$. Soient $a, b \in \mathbb{N}$. Calculons :

$$\begin{aligned} \sum_{\omega \in \Omega} (1 + \omega^a + 2\omega^b)^n \cdot \omega^{-k} &= \sum_{\omega \in \Omega} \sum_{l,m} 1^{n-l-m} (\omega^a)^l (2\omega^b)^m \binom{n}{l\,m} \cdot \omega^{-k} \\ &= \sum_{l,m} \sum_{\omega \in \Omega} \omega^{al+bm-k}\, 2^n \binom{n}{l\,m} \\ &\overset{\text{lemme 1}}{=} \sum_{\substack{l,m \\ 8 \mid al+bm-k}} 8 \cdot 2^m \binom{n}{l\,m} \end{aligned}$$

Posons $a = 4$ et $b = 1$. On trouve donc :

$$\sum_{\omega \in \Omega} (1 + \omega^4 + 2\omega)^n \cdot \omega^{-k} = \sum_{l,m \in \Psi} 8 \cdot 2^m \binom{n}{l\,m} = 2^{n-3} \cdot t_k(n).$$

Donc,

$$t_k(n) = 2^{n-3} \sum_{\omega \in \Omega} (1 + \omega^4 + 2\omega)^n \cdot \omega^{-k} := 2^{n-3} \cdot \Xi(n,k).$$

Posons $\Omega_1 = \{\zeta, \zeta^3, \zeta^5, \zeta^7\}$. On obtient :

$$\Xi(n,k) = \sum_{\omega\in\Omega_1} (2\omega)^n \omega^{-k} + (2+2i)^n\, i^{-k} + (2-2i)^n (-i)^{-k} + 0 + 4^n.$$

Or,

$$\begin{aligned}\sum_{\omega\in\Omega_1} (2\omega)^n \omega^{-k} &= 2^n \cdot (\zeta^{n-k} + \zeta^{3(n-k)} + \zeta^{5(n-k)} + \zeta^{7(n-k)}) \\ &= 2^n \zeta^{n-k} \cdot (1 + \zeta^{2(n-k)} + \zeta^{4(n-k)} + \zeta^{6(n-k)}) \\ &= \begin{cases} 0 & \text{si 4 ne divise pas } n-k \\ 2^{n+2}\zeta^{n-k} & \text{si 4 divise } n-k. \end{cases}\end{aligned}$$

La dernière égalité est un corollaire du lemme 1. Il suit que :

a) $\Xi(n,k) = 2^{2n} + 2^{n+1} \cdot \Re((1+i)^n\, i^{-k})$ si 4 ne divise pas $n-k$.
b) $\Xi(n,k) = 2^{2n} + 2^{n-1} \cdot \Re((1+i)^n\, i^{-k}) + (-1)^{(k-n)/4} \cdot 2^{n+2}$ si 4 divise $n-k$.

Sachant que $1+i = \sqrt{2}\cdot\zeta$, et que $\Re(\zeta^{n-2k}) = \cos\left(\frac{\pi}{4}(2k-n)\right)$, on conclut. •

Démonstation de H. Joris

Posons $\mathrm{e}_8(z) = \exp(\frac{2\pi \mathrm{i} z}{8})$. Nous avons $\mathrm{i} = \mathrm{e}_8(2)$ et $1+\mathrm{i} = \sqrt{2}\mathrm{e}_8(1)$, et

$$\sum_{s=0}^{7} \mathrm{e}_8(s(\sum_{k=1}^{n} m_k^2 - r)) = \begin{cases} 8 & \text{si } \sum_{k=1}^n m_k^2 \equiv r \pmod 8; \\ 0 & \text{sinon.} \end{cases}$$

Nous en déduisons

$$\begin{aligned} 8\,t_r(n) &= \sum_{m_1=0}^{7}\sum_{m_2=0}^{7}\cdots\sum_{m_n=0}^{7}\sum_{s=0}^{7} \mathrm{e}_8(s(\sum_{k=1}^{n} m_k^2 - r)) \\ &= \sum_{s=0}^{7} \mathrm{e}_8(-rs) \sum_{m_1=0}^{7}\sum_{m_2=0}^{7}\cdots\sum_{m_n=0}^{7} \mathrm{e}_8(sm_1^2)\mathrm{e}_8(sm_2^2)\ldots\mathrm{e}_8(sm_n^2) = \sum_{s=0}^{7} \mathrm{e}_8(-rs)\,(\Omega(s))^n\,, \end{aligned}$$

où

$$\Omega(s) = \sum_{m=0}^{7} \mathrm{e}_8(sm^2) = 2 + 2(-1)^s + 4\mathrm{e}_8(s) = \begin{cases} 4\mathrm{e}_8(s) & \text{si } s = 2t+1 \text{ est impair;} \\ 4(1+\mathrm{i}^t) & \text{si } s = 2t \text{ est pair.} \end{cases}$$

Il suit

$$\begin{aligned} 8t_r(n) &= \sum_{t=0}^{3} \mathrm{e}_8(-r(2t+1))\Omega(2t+1)^n + \sum_{t=0}^{3} \mathrm{e}_8(-r(2t))\Omega(2t)^n \\ &= \sum_{t=0}^{3} \mathrm{e}_8(-r(2t+1))4^n \mathrm{e}_8((2t+1)n) + \sum_{t=0}^{3} \mathrm{i}^{-rt} 4^n (1+\mathrm{i}^t)^n \\ &= 4^n\Big(\mathrm{e}_8(n-r)\sum_{t=0}^{3} \mathrm{i}^{t(n-r)} + \sum_{t=0}^{3} \mathrm{i}^{-rt} 4^n (1+\mathrm{i}^t)^n\Big) \\ &= 4^n\Big(\mathrm{e}_8(n-r)\sum_{t=0}^{3} \mathrm{i}^{t(n-r)} + 2^n + (1+\mathrm{i})^n \mathrm{i}^{-r} + (1-\mathrm{i})^n \mathrm{i}^r\Big) \\ &= 4^n\Big(\mathrm{e}_8(n-r)\sum_{t=0}^{3} \mathrm{i}^{t(n-r)} + 2^n + 2\Re(\sqrt{2}^n \mathrm{e}_8(n-2r))\Big) \\ &= 4^n\Big(\mathrm{e}_8(n-r)\sum_{t=0}^{3} \mathrm{i}^{t(n-r)} + 2^n + 2\sqrt{2}^n \cos(\frac{n-2r}{4}\pi)\Big) \\ &= \begin{cases} 4^n\Big(4(-1)^{(n-r)/4} + 2^n + 2^{1+n/2}\cos(\frac{n\pi}{4} - \frac{r\pi}{2})\Big) & \text{si } n \equiv r \bmod 4\,; \\ 4^n\Big(2^n + 2^{1+n/2}\cos(\frac{n\pi}{4} - \frac{r\pi}{2})\Big) & \text{sinon.} \end{cases} \end{aligned}$$

Finalement nous obtenons

$$t_r(n) = \begin{cases} 2^{3n-3} + 2^{2n-2+n/2}\cos(\frac{n\pi}{4} - \frac{r\pi}{2}) + 2^{2n-1}(-1)^{(n-r)/4} & \text{si } n \equiv r \bmod 4\,; \\ 2^{3n-3} + 2^{2n-2+n/2}\cos(\frac{n\pi}{4} - \frac{r\pi}{2}) & \text{sinon}\,. \end{cases}$$

•

Bibliographie

[1] ABRAMOWITZ, M. & STEGUN, I.A. : *Handbook of Mathematical Functions.* National Bureau of Standard Appl. Math. Series 55, U.S. Dept. of Commerce. Washington. 1970

[2] BAEZA, R. : *Quadratic Forms over semilocal rings.* Lecture Notes in Mathematics Vol **655**. Springer-Verlag. Berlin, Heidelberg, New York. 1978.

[3] CASSELS, J.W.S. : *Rational Quadratic Forms.* London Math. Society. 1978.

[4] CONWAY, J.H. & SLOANE, N.J.A. : *Sphere Packing.* Springer-Verlag. Berlin, Heidelberg, New York. 1988.

[5] EICHLER, M. : *Quadratische Formen und orthogonale Gruppen.* Grundlehren des Math. Wiss. zu Berlin. No. **63**. Springer-Verlag. Berlin, Heidelberg, New York. 1952.

[6] DIEUDONNE, J. : *La Géométrie des groupes classiques.* Springer-Verlag. Berlin, Göttingen, Heidelberg. 1955.

[7] KNESER, M. : *Quadratische Formen.* Vorlesung SS/WS 1973-74, Mathematisches Institut. Göttingen. 1974.

[8] MILNOR, J. & HUSEMOLLER, D. : *Symmetric bilinear forms.* Ergebnisse der Math. No. **73**. Springer-Verlag. Berlin, Heidelberg, New York. 1973.

[9] PALL, G. : *The Weight of a Genus of Positive n-ary Quadratic forms.* Proc. of sympos. in pure Math. No. **8** pp. 95–105. 1965

[10] SERRE, J.-P. : *Cours d'arithmétique.* Collection SUP No.2. Presses Universitaires de France. Paris. 1970.

[11] SIEGEL, C.L. : *Über die Analytische Theorie der Quadratische Formen.* Annals of Mathematics No. **36**. 1935.

[12] WATSON, G.L. : *The 2-adic density of a quadratic form.* Mathematika No. **23** pp. 94–106. 1976.