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) $\mathbb{Z}_p \cap \mathbb{Q} = \mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} \mid p \not| b\}$ •

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 $i \in N_n, k \in \mathbb{N}_j$.

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 $k \in \mathbb{N}_j$.

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 $\Longleftrightarrow$ $x_1, \ldots, x_n$ 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 $\mathfrak{B} = (e_1,\dots,e_n)$ 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 :

$$\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \overset{\mathbb{Z}_2^3}{\simeq} \begin{pmatrix} -2 & -1 \\ -1 & -2 \end{pmatrix}$$

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

$$\begin{pmatrix} 2 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 1 & 2 \end{pmatrix} \overset{\mathbb{Z}_2^4}{\simeq} \begin{pmatrix} 2 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & -2 & -1 \\ 0 & 0 & -1 & -2 \end{pmatrix}$$

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

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \boxplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \overset{\mathbb{Z}_2^4}{\simeq} \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \boxplus \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

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 $h \in <e_1>^{\perp}$ 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, $t \in <e_1'>^{\perp}$ 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

$$a_1x_1^2 + \cdots + a_4x_4^2 \equiv c \pmod 8$$

En effet, considérons
$A = \{y \mid y = a_1x_1^2 + a_2x_2^2,\ x_1,\ x_2 \in \mathbb{Z}/8\mathbb{Z}\}$ et $B = \{y \mid y = c - a_3x_3^2 - a_4x_4^2,\ x_1,\ x_2 \in \mathbb{Z}/8\mathbb{Z}\}$.

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 $\forall i \in \llbracket 1, k \rrbracket$. $O(M_i)$ 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 $\mathscr{G}$ une famille de sous-groupes satisfaisant les propriétés suivantes :

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

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

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

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

On définit aussi

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

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

Proposition 2.2

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

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

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

Démonstration :

Soient $E = \bigcup_i x_i K_i$ et $E' = \bigcup_j y_j L_j \in \mathscr{E}$. Il est clair que $E \cup E' \in \mathscr{E}$. 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 $\mathscr{G}$ et tel que $[H : K] < \infty$, on a que $H \in \mathscr{E}$; ceci nous permet de dire que $K_i \cap L_j \in \mathscr{E}$ pour tous i, j, grâce aux axiomes (C_1) et (C_2).

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

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

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 $\mathscr{E}$, alors uE et $u^{-1}Eu \in \mathscr{E}$, 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 $i \in \mathbb{N}_n$, et a un dénominateur commun des a_{ij}. Nous avons alors

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

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

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

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 $u_iO(V, M_2/aM_2)$, 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 $\mathscr{Y}_M$ 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 $\mathscr{Y}_M$, 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 $\mathscr{Y}_M$:
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 $(N_p)_{p\in\mathbb{P}} \in \mathscr{Y}_M$.
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 $x = \dfrac{y}{m}$, 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 $\mathscr{Y}_M$:
soit $(E_p)_{p\in\mathbb{P}} \in \mathscr{Y}_M$; 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 $a_i = a_i' + \dfrac{a_i''}{p^m}$, 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 $x'' = \sum_{i=1}^{n} \dfrac{a_i''}{p^m}e_i$. 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

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