Tesis de Maestría

Módulo de Brandt Generalizado

Gustavo Rama

Orientador: Gonzalo Tornaría

Facultad de Ciencias
Universidad de la República
Uruguay

10 de abril de 2014

Resumen

El objetivo de este trabajo es presentar una generalización del módulo de Brandt para formas cuadráticas ternarias definidas positivas descrito por Birch. Para ello introducimos la norma spin para espacios cuadráticos. Con esto podemos definir el módulo de Brandt generalizado para retículos cuadráticos en espacios cuadráticos ternarios definidos positivos.

También se exhiben ejemplos de la descomposición de dichos módulos en espacios propios comunes a todos los operadores de Hecke del modulo.

Los algoritmos para calcular los módulos de Brandt generalizados y sus operadores de Hecke son descritos e implementados.

Abstract

The aim of this work is to present a generalization of the Brandt module for positive definite ternary quadratic forms described by Birch. To do this we introduce the spin norm for quadratic spaces. With this we can define the generalized Brandt module for quadratic lattices in positive definite ternary quadratic spaces.

Examples of the decomposition of these modules in eigenspaces for all operators of Hecke module are also shown.

The algorithms to compute generalized Brandt modules and their Hecke operators are described and implemented.

Índice general

Introducción

Es sabido que dada una forma cuadrática ternaria, se puede construir un módulo libre asociado a ella, llamado módulo de Brandt, resultando de su descomposición en espacios propios, en ciertas formas modulares. Cuando los espacios propios son racionales, estas formas están asociadas a curvas elípticas.

Es esta una construcción clásica que tiene ciertas restricciones a la que no es posible asociarle todas las curvas elípticas. Por ejemplo, las curvas con signo negativo en su ecuación funcional no aparecen en dicha construcción. Todo esto se puede encontrar en el trabajo de Birch [1].

La construcción consiste en generar un grafo a partir de un número primo p y un nivel. Los vértices de este grafo serán las clases de equivalencia de formas cuadráticas ternarias integrales, y sus aristas estarán definidas por la relación de p-vecindad, donde dos formas cuadráticas Q y Q' son p-vecinas si $Q(x, y, pz) = Q'(px, y, z)$. Una vez construido el grafo, los vectores propios racionales de la matriz asociada a él se usarán para construir las formas modulares utilizando series theta.

En su tesis doctoral [9], Tornaría presenta un refinamiento, utilizando la norma spin, en la construcción del módulo asociado a las formas cuadráticas ternarias, eliminando algunas de las restricciones referidas anteriormente, lo que permite calcular formas modulares asociadas a otras curvas elípticas.

Este refinamiento presenta un método potencial para verificar la tabla de curvas elípticas de la lista de Cremona, presentada en [5]. Cremona utiliza símbolos modulares, y las matrices asociadas a los módulos de Brandt son más esparsas que las subyacentes al método de Cremona, por lo que es esperable que sea más rápido hallar los espacios propios de ellas, constituyendo un método así también más rápido. Otra característica importante es que este método nos da información adicional al de las curvas elípticas: el calculo de coeficientes de Fourier de formas modulares de peso 3/2.

Los métodos presentados fueron implementados en el sistema software matemático Sage [8], y se pueden encontrar en las últimas versiones del mismo.

Capítulo 1

Módulo de Brandt Clásico

En este capítulo presentamos las definiciones y resultados clásicos sobre formas cuadráticas y espacios cuadráticos. En la tercer sección definimos el modulo de Brandt clásico usando clases de equivalencia propia de retículos cuadráticos así como sus operadores de Hecke. Presentamos ejemplos de módulos de Brandt y su descomposición espectral. En estos ejemplos encontramos series de Eisenstein y curvas elípticas con signo positivo en su ecuación funcional.

Este capítulo esta basado en el libro de Cassels [2] y el paper de Birch [1].

1.1. Formas cuadráticas

1.1.1. Introducción

Sea I un anillo con unidad en un cuerpo k, $\mathrm{car}(k) \neq 2$. Una forma cuadrática $f = f(\mathbf{x})$ en las n variables $\mathbf{x} = (x_1, \ldots, x_n)$ es una función

$$f(\mathbf{x}) = \sum_{i,j} f_{ij} x_i x_j \ ,$$

donde $f_{ij} = f_{ji} \in k$.

La forma f representa a $c \in k$ si existe $\mathbf{b} \in I^n$ tal que

$$f(\mathbf{b}) = c \ .$$

Más generalmente, una forma $f(\mathbf{x})$ en n variables representa a una forma $g(\mathbf{y})$ en m variables sobre I si existen $\mathbf{b}_1, \ldots, \mathbf{b}_m \in I^n$ tal que

$$f(y_1\mathbf{b_1} + \cdots + y_m\mathbf{b_m}) = g(\mathbf{y}) \ , \tag{1.1}$$

donde $\mathbf{y} = (y_1, \ldots, y_m)$.

Decimos que dos formas f y g con el mismo número de variables son equivalentes sobre I o I-equivalentes, si cada una representa a la otra. Se

puede ver que la I-equivalencia es una relación de equivalencia. Por lo que podemos hablar de una clase de I-equivalencia de formas cuadráticas.

Por la definición dada, se puede escribir la forma cuadrática de la siguiente manera:

$$f(\mathbf{x}) = \mathbf{x}\mathbf{F}\mathbf{x}^t \ ,$$

donde $\mathbf{F}$ es la matriz simétrica dada por $\mathbf{F} = (f_{ij})$.

El determinante $d(f)$ de la forma f es $\det(\mathbf{F})$, y decimos que f es singular cuando $d(f) = 0$. En otro caso decimos que es regular o no singular.

En notación matricial la Ecuación (1.1) queda

$$\mathbf{G} = \mathbf{B}^t\mathbf{F}\mathbf{B} \ ,$$

donde $\mathbf{F}$ y $\mathbf{G}$ son las matrices correspondientes a f y g, con

$$\mathbf{B} = (b_{ij})_{1\leq i\leq n,\ 1\leq j\leq m},\ \mathbf{b}_i = (b_{i1}, \ldots, b_{in})$$

Si ahora f y g son equivalentes, se cumple que $n = m$ y

$$\mathbf{F} = \mathbf{C}^t\mathbf{G}\mathbf{C}$$

para alguna matriz $\mathbf{C}$ con entradas en I. Usando la definición de determinante, obtenemos

$$d(g) = (\det \mathbf{B})^2 d(f) \ ,$$
$$d(f) = (\det \mathbf{C})^2 d(g) \ .$$

Se ve entonces que si una forma es singular, la otra también lo será y podemos hablar de una clase de equivalencia regular. Además si las formas f y g son regulares:

$$(\det \mathbf{B})^2(\det \mathbf{C})^2 = 1$$

y $\det \mathbf{B}$ es una unidad de I. Vemos el recíproco del resultado en el siguiente lema, con demostración obvia.

Lema 1.1.1. *Una condición necesaria y suficiente para que dos formas regulares f y g en n variables sean I-equivalentes es que*

$$\mathbf{G} = \mathbf{B}^t\mathbf{F}\mathbf{B}$$

para alguna matriz $\mathbf{B}$ con entradas en I y $\det \mathbf{B}$ una unidad de I.

Decimos que una forma cuadrática real, $f_{ij} \in \mathbb{R}$, es definida positiva si

$$f(\mathbf{x}) > 0$$

para todo $\mathbf{x} \in \mathbb{R}^n$.

Demostramos un caso particular de la ley de inercia de Sylvester, que nos sera útil luego.

Proposición 1.1.2. *Si f es una forma cuadrática real definida positiva en n variables, luego f es $\mathbb{R}$-equivalente a*

$$x_1^2 + \cdots + x_n^2 \ .$$

Demostración. Lo demostramos por inducción. Completando el cuadrado obtenemos:

$$f(\mathbf{x}) = f_{11}(x_1 + \cdots + x_n)^2 + \sum_{i,j \geq 2} f'_{ij} x_i x_j$$

que es equivalente a

$$(x'_1)^2 + \sum_{i,j \geq 2} f'_{ij} x_i x_j \ .$$

□

1.1.2. Reducción

Consideramos formas cuadráticas reales definidas positivas

$$f(\mathbf{x}) = \sum_{i,j} f_{ij} x_i x_j, \ (f_{ij} \in \mathbb{R}) \ .$$

El objetivo de la teoría de reducción consiste en encontrar, entre infinitas formas $\mathbb{Z}$-equivalentes a f, una forma caracterizada de alguna manera intrínseca.

Definición 1.1.1. Una forma cuadrática real f definida positiva es reducida Minkowski si para todo j

$$f(\mathbf{e}_j^*) \geq f(\mathbf{e}_j) \ , \tag{1.2}$$

donde $\mathbf{e}_j = (0, \ldots, 0, 1, 0, \ldots, 0)$, y para todo $\mathbf{e}_j^*$ entero tal que $\mathbf{e}_1, \ldots, \mathbf{e}_{j-1}, \mathbf{e}_j^*$ se puede extender a una $\mathbb{Z}$-base de $\mathbb{Z}^n$.

Vemos dos casos importantes de (1.2).

Lema 1.1.3. *Si f es reducida, se cumple:*

$$0 < f_{11} \leq f_{22} \leq \cdots \leq f_{nn} \ ,$$

y

$$|2f_{ij}| \leq f_{ii}, \ (1 \leq i < j \leq n) \ .$$

Demostración. Si $i < j$ podemos tomar $\mathbf{e}_i^* = \mathbf{e}_j$ y $\mathbf{e}_j^* = \mathbf{e}_j \pm \mathbf{e}_i$. □

Teorema 1.1.4. *Toda forma cuadrática real definida positiva es equivalente a al menos una forma reducida Minkowski y como mucho a una cantidad finita.*

Demostración. Primero vemos que si $M > 0$, el conjunto $\{\mathbf{x} \in \mathbb{R}^n : f(\mathbf{x}) \leq M\}$ está acotado. Esto se deduce de la Proposición 1.1.2 ya que el conjunto sera difeomorfo a una bola en $\mathbb{R}^n$. Vemos entonces que hay una cantidad finita de $\mathbf{m} \in \mathbb{Z}^n$ tales que $f(\mathbf{m}) \leq M$.

Es claro ahora que podemos elegir de manera inductiva una $\mathbb{Z}$-base $\mathbf{b}_1, \ldots, \mathbf{b}_n$ de $\mathbb{Z}^n$ que cumple

$$f(\mathbf{b}_j) = \inf_{\mathbf{b}_j^*} f(\mathbf{b}_j^*) \ ,$$

donde el ínfimo es sobre todos los $\mathbf{b}_j^*$ tales que $\mathbf{b}_1, \ldots, \mathbf{b}_{j-1}, \mathbf{b}_j^*$ se puede extender a una $\mathbb{Z}$-base de $\mathbb{Z}^n$.

Entonces la forma

$$g(y_1, \ldots, y_n) = f(y_1\mathbf{b}_1 + \cdots + y_n\mathbf{y}_n)$$

es reducida y equivalente a f.

Los valores $f(\mathbf{b}_j)$ estan determinados de manera única por f, aunque los vectores $\mathbf{b}_j$ no. Pero sí hay un cantidad finita de vectores con esa propiedad, y por lo tanto una cantidad finita de formas cuadráticas reducidas equivalentes a f. □

Existe una caracterización muy útil para formas cuadráticas de baja dimensión que vemos en el siguiente lema.

Lema 1.1.5. *Sea $n \leq 4$. Una condición necesaria y suficiente para que la forma cuadrática real f definida positiva sea reducida es*

1. $0 < f_{11} \leq f_{22} \leq \cdots \leq f_{nn}$.
2. $f(\mathbf{s}) \geq f_{JJ}$ *para* $1 \leq J \leq n$ *y para todo* $\mathbf{s}$ *con*

$$\begin{aligned} s_j &= 0 \text{ o } \pm 1 \ (j < J) \ , \\ s_J &= 1 \ , \\ s_j &= 0 \ (j > J) \ . \end{aligned}$$

Demostración. Las dos condiciones son claramente necesarias. Para probar que son suficientes, usando la primera condición alcanzaría con probar que

$$f(\mathbf{a}) \geq f_{JJ}$$

para todo $\mathbf{a}$ integral con $a_J \neq 0$ y $a_j = 0$ $(j > J)$.

Si una forma f satisface las condiciones (1) y (2) también las satisface la forma en $n-m$ variables obtenida de igualar m de las variables a 0. Podemos suponer entonces que

$$a_j \neq 0 \ (1 \leq j \leq n)$$

y tendríamos que probar que

$$f(\mathbf{a}) \geq f_{nn} \ .$$

Luego de realizar las substituciones $x_j \to \pm x_j$ podemos suponer que $a_j > 0$ $(1 \leq j \leq n)$.

Sea $A = \max a_j$. Si $A = 1$ la desigualdad que buscamos es una de las desigualdades de la condición (2). Suponemos que $A > 1$ y usaremos inducción en $\sum_j a_j$ y n. Sea $B = \min_j a_j > 0$. Si $a_n = B$ tomo $k = n$, si no tomo k como algún índice tal que $a_k = B$. Sea

$$\begin{aligned} b_j &= a_j - B \quad (j \neq k) \\ b_k &= a_k = B \end{aligned}$$

por lo que

$$0 \leq b_j \leq a_j, \quad b_n \neq 0 \ .$$

Calculando, vemos que

$$\begin{aligned} f(\mathbf{a}) - f(\mathbf{b}) = B^2(f(1,\ldots,1) - f_{nn}) \\ + 2\sum_{i\neq k} Bb_i \sum_{j\neq k} f_{ij} \end{aligned}$$

y si podemos probar que $f(\mathbf{a}) \geq f(\mathbf{b})$ terminamos ya que $f(\mathbf{b}) \geq f_{nn}$ por hipótesis inductiva. Pero

$$f(1,\ldots,1) - f_{nn} \geq 0$$

por la condición (2), y

$$\begin{aligned} \sum_{j\neq k} f_{ij} &= \left(2 - \frac{1}{2}n\right) + \frac{1}{2}\sum_{j\neq k, j\neq i} (f_{ii} + 2f_{ij}) \\ &\geq 0 \end{aligned}$$

□

1.1.3. Formas ternarias

Si $f(x,y,z) = ax^2 + by^2 + cz^2 + ryz + sxz + txy$ es una forma cuadrática ternaria, la denotamos por

$$f = \begin{pmatrix} a & b & c \\ r & s & t \end{pmatrix} \ .$$

En la notación introducida en la introducción, los coeficientes son

$$\begin{pmatrix} a & b & c \\ r & s & t \end{pmatrix} = \begin{pmatrix} f_{11} & f_{22} & f_{33} \\ \frac{1}{2}f_{23} & \frac{1}{2}f_{13} & \frac{1}{2}f_{12} \end{pmatrix} \ .$$

Decimos que f es integral si los coeficientes a, b, c, r, s, t pertenecen al anillo I.

Observación 1.1.6. En el caso de formas cuadráticas ternarias, las condiciones de reducción Minkowski son:

1. $a \leq b \leq c$.
2. $a \geq |t|$, $a \geq |s|$, $b \geq |r|$.
3. $a + b + \delta r + \varepsilon s + \delta\varepsilon t \geq 0$. Donde $\delta^2 = \varepsilon^2 = 1$.

Demostración. Ver Lema 1.1.5. □

Ejemplo 1.1.1. Sean

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & -1 \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 1 \end{pmatrix}.$$

Se ve que f y g son $\mathbb{Z}$-equivalentes y Minkowski reducidas.

Como en el caso de formas cuadráticas binarias, querríamos una reducción que sea única por $\mathbb{Z}$-equivalencia. La siguiente es una reducción que cumple eso.

Definición 1.1.2. Una forma cuadrática ternaria se dice que es Eisentein reducida o E-reducida si cumple las siguientes condiciones:

1. $a \leq b \leq c$.
2. $r, s, t > 0$ o $r, s, t \leq 0$. En el primer caso definimos $\sigma = 1$ y en el segundo $\sigma = -1$.
3. $a \geq |t|$, $a \geq |s|$, $b \geq |r|$.
4. $a + b + r + s + t \geq 0$.
5. $2a + 2s + t \leq 0$ si $a + b + r + s + t = 0$.
6. $s \leq 2r$ si $a = t$, $t \leq 2r$ si $a = s$, $t \leq 2s$ si $b = r$.
7. $s = 0$ si $a = -t$, $t = 0$ si $a = -s$, $t = 0$ si $b = -r$.
8. $|r| \leq |s|$ si $a = b$, $|s| \leq |t|$ si $b = c$.

Ejemplo 1.1.2. En el Ejemplo 1.1.1 f no es Eisenstein reducida, pero g si.

Teorema 1.1.7. *Dada una forma cuadrática ternaria definida positiva existe una única forma E-reducida integralmente equivalente a ella.*

Demostración. Esto se puede encontrar en el libro de Dickson [6]. □

1.2. Espacios Cuadráticos

1.2.1. Introducción

Sea k un cuerpo con $\text{car}(k) \neq 2$. Un espacio cuadrático sobre k es un espacio vectorial de dimensión finita V junto a una función $\phi : V \to k$ que cumple

- $\phi(x\mathbf{v}) = x^2\phi(\mathbf{v})$, $\mathbf{v} \in V$ $x \in k$.
- $\phi(\mathbf{v}, \mathbf{v}') = \frac{1}{2}\left(\phi(\mathbf{v} + \mathbf{v}') - \phi(\mathbf{v}) - \phi(\mathbf{v}')\right)$ es una forma bilineal simétrica.

Observar que usamos la misma notación para la función ϕ definida en una variable y en dos variables

Vemos que

$$\phi(\mathbf{v}) = \phi(\mathbf{v}, \mathbf{v}) \ ,$$

por lo que podemos recuperar ϕ de la forma bilineal.

Enunciamos el siguiente lema, de facil demostracíon, para uso posterior.

Lema 1.2.1. *Supongamos que la forma bilineal $\phi(\mathbf{v}_1, \mathbf{v}_2)$ no es idénticamente 0. Luego existe un $\mathbf{v} \in V$ tal que $\phi(\mathbf{v}) \neq 0$.*

Si $\mathbf{v}_1, \ldots, \mathbf{v}_n$ es una base de V, entonces

$$f(x_1, \ldots, x_n) = \phi\left(\sum_j x_j \mathbf{v}_j\right) \tag{1.3}$$

$$= \sum_{i,j} x_i x_j \phi(\mathbf{v}_i, \mathbf{v}_j) \tag{1.4}$$

es una forma cuadrática sobre k. Si $\mathbf{v}'_1, \ldots, \mathbf{v}'_n$ es otra base de V, claramente

$$f'(x_1, \ldots, x_n) = \phi\left(\sum_j x_j \mathbf{v}'_j\right)$$

es equivalente a f sobre k, y toda forma equivalente a f surge de esta manera. Es más, toda forma cuadrática sobre k proviene de un espacio cuadrático $(V,\ \phi)$, tomando un V de dimensión adecuada y definiendo ϕ para alguna base $\mathbf{v}_1, \ldots, \mathbf{v}_n$ en función de f como en (1.4).

Denotamos el conjunto de los mapas k-lineales $V \to k$ como $\text{Hom}(V, k)$. La forma bilineal ϕ determina un mapa k-lineal

$$V \to \text{Hom}(V, k), \tag{1.5}$$

donde $\mathbf{w} \in V$ corresponde a $\phi_{\mathbf{w}} \in \text{Hom}(V, k)$ definido por

$$\phi_{\mathbf{w}}(\mathbf{v}) = \phi(\mathbf{v}, \mathbf{w}) \ .$$

Decimos que el espacio cuadrático $(V,\ \phi)$ es regular si el mapa (1.5) es un isomorfismo. Si no, decimos que es singular. Enunciamos el siguiente lema con prueba trivial.

Lema 1.2.2. *Son equivalentes:*

1. $(V,\ \phi)$ *es regular.*
2. *Si* $\mathbf{w} \in V$ *y* $\phi(\mathbf{v}, \mathbf{w}) = 0\ \forall \mathbf{v} \in V$*, entonces* $\mathbf{w} = 0$*.*
3. $\det_{1\leq i\leq n,\ 1\leq j\leq n} \phi(\mathbf{v}_i, \mathbf{v}_j) \neq 0$*, donde* $\mathbf{v}_1, \ldots, \mathbf{v}_n$ *es una base cualquiera de* V*.*
4. *La forma cuadrática dada por (1.4) es regular.*

Ahora podemos introducir un invariante importante de un espacio cuadrático regular. Sean $\mathbf{v}_1, \ldots, \mathbf{v}_n$ y $\mathbf{w}_1, \ldots, \mathbf{w}_n$ bases de V, y

$$\mathbf{v}_i = \sum_j s_{ij}\mathbf{w}_j\ (1 \leq i \leq n),$$

con $s_{ij} \in k$ y $\det(s_{ij}) \neq 0$. Es fácil de verificar que

$$\det_{i,j} \phi(\mathbf{v}_i, \mathbf{v}_j) = \left(\det_{i,j}(s_{ij})\right)^2 \det_{i,j} \phi(\mathbf{w}_i, \mathbf{w}_j)\ .$$

Por lo que $\det_{i,j} \phi(\mathbf{v}_i, \mathbf{v}_j) \in k^\times$ está definido módulo $(k^\times)^2$, y es independiente de la elección de la base $\mathbf{v}_1, \ldots, \mathbf{v}_n$. Llamamos al elemento de $k^\times/(k^\times)^2$ como el determinante $d(\phi)$ de $(V,\ \phi)$. Si $(V,\ \phi)$ es singular definimos $d(\phi) = 0$.

Decimos que $\mathbf{v}_1$ y $\mathbf{v}_2$ son ortogonales si $\phi(\mathbf{v}_1, \mathbf{v}_2) = 0$. Puede pasar que $\mathbf{v}$ sea ortogonal a sí mismo, o sea $\phi(\mathbf{v}, \mathbf{v}) = 0$.

Si $(V,\ \phi)$ es un espacio cuadrático y W un subespacio lineal de V, la forma ϕ le da una estructura de espacio cuadrático a W. Denotamos $W^\perp$ como el conjunto de vectores de V que son ortogonales a todos los vectores de W y es llamado el complemento ortogonal de W,

$$W^\perp = \{\mathbf{v} \in V : \phi(\mathbf{v}, \mathbf{w}) = 0\ \ \forall \mathbf{w} \in W\}\ .$$

Es claro que $W^\perp$ también es subespacio de V.

Lema 1.2.3. *Sea* $(V,\ \phi)$ *un espacio cuadrático, no necesariamente regular. Si* W *es un subespacio regular de* V*, entonces* V *es suma directa de* W *y* $W^\perp$*.*

Demostración. Sea $\mathbf{v} \in V$, $\mathbf{v}$ determina un elemento de $\mathrm{Hom}(W, k)$ dado por

$$\mathbf{w} \to \phi(\mathbf{v}, \mathbf{w})\ .$$

Por la definición de regularidad de W, existe un único $\mathbf{u} = \mathbf{u}(\mathbf{w}) \in W$ tal que

$$\phi(\mathbf{u}, \mathbf{w}) = \phi(\mathbf{v}, \mathbf{w}) \ \forall \mathbf{w} \in W \ .$$

Por lo que

$$\mathbf{v} = \mathbf{u} + (\mathbf{v} - \mathbf{u}) \ ,$$

donde

$$\mathbf{u} \in W, \ \ \mathbf{v} - \mathbf{u} \in W^{\perp} \ .$$

Por otro lado, si

$$\mathbf{v} = \mathbf{s} + \mathbf{t}, \ \ \mathbf{s} \in W, \ \mathbf{t} \in W^{\perp}$$

tenemos

$$\phi(\mathbf{s}, \mathbf{w}) = \phi(\mathbf{v}, \mathbf{w}) = \phi(\mathbf{u}, \mathbf{w}) \ \ \forall \mathbf{w} \in W$$

y por regularidad $\mathbf{s} = \mathbf{u}$. □

Una base $\mathbf{v}_1, \ldots, \mathbf{v}_n$ de un espacio cuadrático es normal si

$$\phi(\mathbf{v}_i, \mathbf{v}_j) = 0 \ (i \neq j) \ .$$

Lema 1.2.4. *Todo espacio cuadrático tiene una base normal.*

Demostración. Si ϕ es idénticamente 0, toda base es normal. De otra manera, por el Lema 1.2.1 existe un $\mathbf{v}_1 \in V$ tal que $\phi(\mathbf{v}_1) \neq 0$. El espacio de dimensión 1 W generado por $\mathbf{v}_1$ es regular. Por lo que V es suma directa de W y $W^{\perp}$. Por inducción en la dimensión existe una base normal $\mathbf{v}_2, \ldots, \mathbf{v}_n$ de $W^{\perp}$ y $\mathbf{v}_1, \ldots, \mathbf{v}_n$ es una base normal de V. □

Un espacio cuadrático $(V, \ \phi)$ representa $b \in k$ si existe un $\mathbf{b} \in V$ tal que $\phi(\mathbf{b}) = b$. Decimos que 0 es representado de manera no trivial si existe $\mathbf{b} \neq 0$ con $\phi(\mathbf{b}) = 0$. Un espacio regular es isotópico si representa a 0 de manera no trivial, de otra manera es anisotrópico.

Un vector $\mathbf{v} \in V$ es anisotrópico si $\phi(\mathbf{v}) \neq 0$, lo que es lo mismo que el espacio generado por $\mathbf{v}$ sea anisotrópico.

1.2.2. Isometrías y autometrías

Sean $(V_1, \ \phi_1)$ y $(V_2, \ \phi_2)$ dos espacios cuadráticos sobre un cuerpo k. Un isomorfismo

$$\sigma : V_1 \to V_2$$

entre k-espacios lineales es una isometría si preserva la estructura de espacio cuadrático, en el sentido de

$$\phi_2(\sigma \mathbf{v}) = \phi_1(\mathbf{v}) \ \forall \mathbf{v} \in V_1 \ .$$

Dos espacios cuadráticos son isométricos si hay una isometría entre ellos. Claramente, dos espacios cuadráticos son isométricos si y solo si corresponden a la misma clase de equivalencia de formas cuadráticas en el sentido de la Sección 1.2.1.

Decimos que una isometría de $(V,\ \phi)$ en $(V,\ \phi)$ es una autometría. Las autometrías de $(V,\ \phi)$ forman un grupo con la composición como producto, este grupo es llamado el grupo ortogonal $O(V)$.

Lema 1.2.5. *Sea* σ *una autometría de un espacio cuadrático regular* $(V,\ \phi)$. *Se cumple que* $\det\sigma = \pm 1$.

Demostración. Sea $\mathbf{v}_1, \ldots, \mathbf{v}_n$ una base cualquiera de V. Luego

$$\phi(\sigma\mathbf{v}_i, \sigma\mathbf{v}_j) = \phi(\mathbf{v}_i, \mathbf{v}_j)\ \forall i, j\ .$$

Por lo que

$$\det(\phi(\mathbf{v}_i, \mathbf{v}_j)) = \det(\phi(\sigma\mathbf{v}_i, \sigma\mathbf{v}_j)) = (\det\sigma)^2 \det(\phi(\mathbf{v}_i, \mathbf{v}_j))\ ,$$

y como $(V,\ \phi)$ es regular, $\det\sigma = \pm 1$. □

Si $\det\sigma = +1$ decimos que la autometría σ es propia, de otra manera decimos que es impropia. Las autometrías propias forman un subgrupo de $O(V)$ y las denotamos $O^+(V)$.

Sea W un subespacio regular de $(V,\ \phi)$, por lo que $V = W \oplus W^\perp$. Hay un mapa lineal $\sigma : V \to V$ definido por

$$\sigma\mathbf{w} = -\mathbf{w},\quad \forall\mathbf{w} \in W$$
$$\sigma\mathbf{w} = \mathbf{w},\quad \forall\mathbf{w} \in W^\perp.$$

Claramente σ es una autometría. En particular si $\mathbf{w} \in V$ es anisotrópico, podemos tomar W como el espacio generado por $\mathbf{w}$. Denotamos por $\tau_\mathbf{w}$ la autometría tal que

$$\tau_\mathbf{w}\mathbf{w} = -\mathbf{w}$$
$$\tau_\mathbf{w}\mathbf{v} = \mathbf{v} \text{ si } \phi(\mathbf{v}, \mathbf{w}) = 0,$$

y claramente $\det\tau_\mathbf{w} = -1$. Con esto vemos que el grupo ortogonal de un espacio cuadrático con ϕ no idénticamente nula tiene siempre una simetría impropia, por lo que $O^+(V)$ tiene índice 2 en $O(V)$. Además el conjunto $O^-(V)$ de las autometrías impropias es una coclase de $O(V)$.

Las $\tau_\mathbf{w}$ son llamadas simetrías. Es fácil de ver que se cumple

$$\tau_\mathbf{w}\mathbf{v} = \mathbf{v} - \frac{2\phi(\mathbf{v}, \mathbf{w})}{\phi(\mathbf{w})}\mathbf{w}\ . \tag{1.6}$$

Lema 1.2.6. *Sean* $\mathbf{v},\ \mathbf{w} \in V$ *con* $\phi(\mathbf{v}) = \phi(\mathbf{w})$ *y* $\phi(\mathbf{v}-\mathbf{w}) \neq 0$. *Luego*

$$\tau_{\mathbf{v}-\mathbf{w}}\mathbf{v} = \mathbf{w}\ .$$

Demostración.

$$\begin{aligned}
\tau_{\mathbf{v}-\mathbf{w}}\mathbf{v} &= \mathbf{v} - \frac{2\phi(\mathbf{v},\mathbf{v}-\mathbf{w})}{\phi(\mathbf{v}-\mathbf{w})}(\mathbf{v}-\mathbf{w}) \\
&= \mathbf{v} - \frac{2(\phi(\mathbf{v})-\phi(\mathbf{v},\mathbf{w}))}{\phi(\mathbf{v})-2\phi(\mathbf{v},\mathbf{w})+\phi(\mathbf{w})}(\mathbf{v}-\mathbf{w}) \\
&= \mathbf{v} - \frac{2(\phi(\mathbf{v})-\phi(\mathbf{v},\mathbf{w}))}{2(\phi(\mathbf{v})-\phi(\mathbf{v},\mathbf{w}))}(\mathbf{v}-\mathbf{w}) \\
&= \mathbf{v} - (\mathbf{v}-\mathbf{w}) \\
&= \mathbf{w}\ .
\end{aligned}$$

□

Corolario 1.2.7. *Si* $\mathbf{v},\ \mathbf{w} \in V$ *con* $\phi(\mathbf{v}) = \phi(\mathbf{w}) \neq 0$ *entonces existe una autometría* σ *tal que* $\sigma\mathbf{v} = \mathbf{w}$, *y* σ *es una simetría o el producto de dos simetrías.*

Demostración. Si $\phi(\mathbf{v}-\mathbf{w}) \neq 0$ podemos tomar $\sigma = \tau_{\mathbf{v}-\mathbf{w}}$. Si $\phi(\mathbf{v}+\mathbf{w}) \neq 0$, luego

$$\tau_{\mathbf{v}+\mathbf{w}}\mathbf{v} = -\mathbf{w}$$

y podemos tomar $\sigma = \tau_{\mathbf{w}}\tau_{\mathbf{v}+\mathbf{w}}$. Al menos uno de estos casos se tiene que cumplir, ya que

$$\begin{aligned}
\phi(\mathbf{v}+\mathbf{w}) + \phi(\mathbf{v}-\mathbf{w}) &= 2\phi(\mathbf{v}) + 2\phi(\mathbf{w}) \\
&= 4\phi(\mathbf{v}) \\
&\neq 0\ .
\end{aligned}$$

□

Corolario 1.2.8. *Si* $(V,\ \phi)$ *es un espacio cuadrático regular y* $n = \dim V > 1$, *podemos suponer que la autometría* σ *del Corolario 1.2.7 es producto de exactamente dos simetrías.*

Demostración. Existe un vector $\mathbf{u} \in V$ perpendicular a $\mathbf{v}$ con $\phi(\mathbf{u}) \neq 0$. Si $\phi(\mathbf{v}-\mathbf{w}) \neq 0$ podemos tomar $\sigma = \tau_{\mathbf{v}-\mathbf{w}}\tau_{\mathbf{u}}$. □

Lema 1.2.9. *Sea* $(V,\ \phi)$ *un espacio cuadrático regular. Toda autometría de* $(V,\ \phi)$ *es un producto de simetrías.*

Demostración. Sea ρ una autometría de V y $\mathbf{w}$ un vector de V con $\phi(\mathbf{w}) \neq 0$. Luego

$$\phi(\rho\mathbf{w}) = \phi(\mathbf{w}) \neq 0,$$

y por el Corolario 1.2.7 existe un producto de simetrías σ tal que

$$(\sigma\rho)\mathbf{w} = \mathbf{w} \ .$$

Ahora, como $\sigma\rho$ es una autometría de V que deja fijo $\mathbf{w}$, también deja fijo $W^{\perp}$ el espacio de vectores normales a $\mathbf{w}$. Por inducción en la dimensión de V podemos asumir que existe una secuencia de vectores $\mathbf{u}(1), \ldots, \mathbf{u}(T) \in W^{\perp}$ que cumple que σ^* y $\sigma\rho$ coinciden en $W^{\perp}$, donde

$$\sigma^* = \tau_{\mathbf{u}(1)}\tau_{\mathbf{u}(2)} \cdots \tau_{\mathbf{u}(T)} \ .$$

Pero $\sigma_{\mathbf{u}(t)}$ dejan fijo $\mathbf{w}$, por lo que σ^* y $\sigma\rho$ dejan fijo a $\mathbf{w}$. Entonces $\sigma\rho = \sigma^*$ y $\rho = \sigma^{-1}\sigma^*$ es un producto de simetrías. □

Observación 1.2.10. El lema anterior prueba que toda autometría es el producto de a lo sumo $2n$ simetrias, pero se puede probar que es el producto de a lo sumo n. Ver [2], capítulo 2 ejercicio 8.

1.2.3. Retículos cuadráticos

Sea I un dominio en k y $(V,\ \phi)$ un espacio cuadrático. Si $\mathbf{v}_1, \ldots, \mathbf{v}_n$ es una base de V, definimos el I-retículo con base $\mathbf{v}_1, \ldots, \mathbf{v}_n$, Λ, como

$$\Lambda = I\mathbf{v}_1 \oplus \cdots \oplus I\mathbf{v}_n \ .$$

Decimos que dos retículos Λ y Γ son equivalentes si

$$\sigma\Lambda = \Gamma, \text{ para algun } \sigma \in O(V) \ .$$

Dos retículos Λ y Γ son propiamente equivalentes, y lo denotamos como $\Lambda \sim \Gamma$, si son equivalentes con $\sigma \in O^+(V)$. Denotamos la clase de equivalencia propia de un retículo Λ como $\overline{\Lambda} = \{\sigma\Lambda : \sigma \in O^+(V)\}$.

Una autometría de Λ es $\sigma \in O(V)$ tal que $\sigma\Lambda = \Lambda$. El conjunto de autometrías de Λ es un subgrupo de $O(V)$ que denotamos por $O(\Lambda)$,

$$O(\Lambda) = \{\sigma \in O(V) : \sigma\Lambda = \Lambda\} \ .$$

Las autometrías propias de Λ forman un subgrupo

$$O^+(\Lambda) = O(\Lambda) \cap O^+(V)$$

de índice 1 o 2 en $O(\Lambda)$ dependiendo de si $O(\Lambda) \subset O^+(V)$.

Si $\mathbf{v}_1, \ldots, \mathbf{v}_n$ es una I-base de Λ, entonces

$$f(x_1, \ldots, x_n) = \phi(x_1\mathbf{v}_1 + \cdots + x_n\mathbf{v}_n)$$

es una forma cuadrática que toma valores en k. Diferentes elecciones de I-bases de Λ generan todas las formas que son I-equivalentes a f.

Lema 1.2.11. *El proceso recién descripto da una correspondencia uno a uno entre las clases de equivalencia de I-retículos y las clases de I-equivalencia de formas cuadráticas que son k-equivalentes a f.*

Demostración. Supongamos que Λ y Γ son retículos equivalentes, $\Gamma = \sigma\Lambda$ y que $\mathbf{v}_1, \ldots, \mathbf{v}_n$ es una base de Λ. Luego, $\sigma\mathbf{v}_1, \ldots, \sigma\mathbf{v}_n$ es una base de Γ. Como σ es una autometría, tenemos

$$\begin{aligned}\phi(x_1\mathbf{v}_1 + \cdots + x_n\mathbf{v}_n) &= \phi(\sigma(x_1\mathbf{v}_1 + \cdots + x_n\mathbf{v}_n)) \\ &= \phi(x_1\sigma\mathbf{v}_1 + \cdots + x_n\sigma\mathbf{v}_n)\end{aligned}$$

y Λ, Γ corresponden a la misma clase de equivalencia de formas cuadráticas. Por otro lado, si Λ y Γ corresponden a la misma clase de equivalencia de formas cuadráticas, podemos elegir bases $\mathbf{v}_1, \ldots, \mathbf{v}_n$ de Λ, y $\mathbf{u}_1, \ldots, \mathbf{u}_n$ de Γ, tales que

$$\phi(x_1\mathbf{v}_1 + \cdots + x_n\mathbf{v}_n) = \phi(x_1\mathbf{u}_1 + \cdots + x_n\mathbf{u}_n) \ .$$

Existe una única transformación lineal σ de V en V que cumple

$$\mathbf{v}_j = \sigma\mathbf{u}_j \ .$$

Claramente σ es una autometría de V y $\sigma\Lambda = \Gamma$. □

Tenemos el siguiente resultado para $k = \mathbb{Q}$ y $I = \mathbb{Z}$, con demostración similar a la anterior.

Corolario 1.2.12. *Existe una correspondencia uno a uno entre las clases de equivalencia propia de $\mathbb{Z}$-retículos en un $\mathbb{Q}$-espacio cuadrático $(V,\ \phi)$ y las clases de $\mathbb{Z}$-equivalencia propia de formas cuadráticas en una clase fija de $\mathbb{Q}$-equivalencia propia de formas cuadráticas.*

Definición 1.2.1. Sea Λ un retículo con base $\mathbf{v}_1, \ldots, \mathbf{v}_n$, definimos el discriminante de Λ como

$$\operatorname{disc}\Lambda = \begin{cases} (-1)^{n/2}\det(\mathbf{v}_1, \ldots, \mathbf{v}_n) & \text{si } n \text{ es par} \\ \frac{1}{2}\det(\mathbf{v}_1, \ldots, \mathbf{v}_n) & \text{si } n \text{ es impar} \end{cases}$$

Es claro que es un elemento bien definido de $k^\times/I^\times$, ya que la matriz de cambio de variable de la base dada a otra es invertible con elementos en I, por lo que su determinante pertenece a $I^\times$.

Definición 1.2.2. Un I-retículo Λ es integral si $\phi(\Lambda) \subset I$. Si además de integral, $\operatorname{disc}\Lambda \in I^\times$, decimos que Λ es unimodular.

De ahora en más trabajaremos con $(V,\ \phi)$ un espacio cuadrático sobre $\mathbb{Q}$ y $\mathbb{Z}$-retículos así como sus localizaciones.

Sea p un primo, denotamos las localizaciones con respecto a p de la siguiente manera:

$$V_p = V \otimes \mathbb{Q}_p$$

es un espacio cuadrático sobre $\mathbb{Q}_p$. Si Λ es un $\mathbb{Z}$-retículo en V, la localización es

$$\Lambda_p = \Lambda \otimes \mathbb{Z}_p \ ,$$

que es un $\mathbb{Z}_p$ retículo en V_p. Se observa que para casi todo primo p, o sea salvo una cantidad finita, la localización Λ_p es unimodular.

Decimos que dos retículos Λ y Γ están en el mismo género si

$$\Lambda_p \sim \Gamma_p \quad \forall p \ .$$

Teorema 1.2.13. *En un género dado hay una cantidad finita de clases de equivalencia de retículos cuadráticos.*

La prueba del teorema anterior se puede encontrar en el capítulo 9 de [2].

1.3. Módulo de Brandt

1.3.1. Retículos vecinos

Sean Λ y Γ dos $\mathbb{Z}$-retículos en un espacio cuadrático $(V,\ \phi)$ sobre $\mathbb{Q}$, y un primo p. Decimos que Λ y Γ son p-vecinos si, son integrales y cumplen:

1. $[\Lambda : \Lambda \cap \Gamma] = [\Gamma : \Lambda \cap \Gamma] = p$.
2. $\phi(\Lambda, \Gamma) \not\subset \mathbb{Z}$.

Observamos que $\Lambda_q = \Gamma_q$ para todo primo $q \neq p$ y son $\mathbb{Q}_p$-equivalentes con el mismo discriminante.

Sea Λ un $\mathbb{Z}$-retículo integral. Describimos un método para hallar todos los p-vecinos de Λ. Para cada $\mathbf{v} \in \Lambda$, sean

$$\Lambda^0_{\mathbf{v}} = \{\mathbf{u} \in \Lambda : \phi(\mathbf{v}, \mathbf{u}) \equiv 0 \pmod{p}\} \ ,$$
$$\Lambda_{\mathbf{v}} = \mathbb{Z}\frac{\mathbf{v}}{p} + \Lambda^0_{\mathbf{v}} \ .$$

Estos retículos cumplen las siguientes inclusiones

$$\Lambda^0_{\mathbf{v}} \subset \Lambda_{\mathbf{v}},\ \Lambda^0_{\mathbf{v}} \subset \Lambda \ .$$

El retículo dual de Λ es

$$\Lambda^{\#} = \{\mathbf{v} \in V : \phi(\mathbf{v}, \Lambda) \subset \mathbb{Z}\}$$

que es otro $\mathbb{Z}$-retículo. Como Λ es integral, vemos que $\Lambda \subset \Lambda^{\#}$.

Lema 1.3.1. *Los índices de las inclusiones anteriores son*

- *Si* $\mathbf{v} \in p\Lambda$
  - $\left[\Lambda : \Lambda_{\mathbf{v}}^0\right] = 1.$
  - $\left[\Lambda_{\mathbf{v}} : \Lambda_{\mathbf{v}}^0\right] = 1.$
- *Si* $\mathbf{v} \in p\Lambda^{\#}, \mathbf{v} \notin p\Lambda$
  - $\left[\Lambda : \Lambda_{\mathbf{v}}^0\right] = 1.$
  - $\left[\Lambda_{\mathbf{v}} : \Lambda_{\mathbf{v}}^0\right] = p.$
- *Si* $\mathbf{v} \notin p\Lambda^{\#}$, $p \nmid \phi(\mathbf{v}, \mathbf{v})$
  - $\left[\Lambda : \Lambda_{\mathbf{v}}^0\right] = p.$
  - $\left[\Lambda_{\mathbf{v}} : \Lambda_{\mathbf{v}}^0\right] = p^2.$
- *Si* $\mathbf{v} \notin p\Lambda^{\#}$, $p|\phi(\mathbf{v}, \mathbf{v})$
  - $\left[\Lambda : \Lambda_{\mathbf{v}}^0\right] = p.$
  - $\left[\Lambda_{\mathbf{v}} : \Lambda_{\mathbf{v}}^0\right] = p.$

Demostración. $\mathbf{v} \in p\Lambda^{\#}$ implica $\phi(\mathbf{v}, \Lambda) \subset p\mathbb{Z}$, por lo que $\Lambda_{\mathbf{v}}^0 = \Lambda$. Además $\Lambda_{\mathbf{v}}^0 = \Lambda_{\mathbf{v}}$ si y solo si $\mathbf{v} \in p\Lambda$, y $\left[\Lambda_{\mathbf{v}} : \Lambda_{\mathbf{v}}^0\right] = p$ en otro caso.

Supongamos ahora que $\mathbf{v} \notin p\Lambda^{\#}$. Existe una base de Λ $\{\mathbf{v}_1, \mathbf{v}_2, \dots\}$ que cumple $\phi(\mathbf{v}, \mathbf{v}_1) \notin p\mathbb{Z}$. Cambiando $\mathbf{v}_i$ por $\mathbf{v}_i + \alpha_i \mathbf{v}_1$, con $\mathbb{Z} \ni \alpha_i \equiv -\phi(\mathbf{v}, \mathbf{v}_i)\phi(\mathbf{v}, \mathbf{v}_1)^{-1}$ (mód p), podemos asumir que $\phi(\mathbf{v}, \mathbf{v}_i) \in p\mathbb{Z}$ para $i > 1$. Por lo que $\{p\mathbf{v}_1, \mathbf{v}_2, \dots\}$ es base de $\Lambda_{\mathbf{v}}^0$, y $\left[\Lambda : \Lambda_{\mathbf{v}}^0\right] = p$.

Finalmente, $\frac{\mathbf{v}}{p} \notin \Lambda_{\mathbf{v}}^0$, y $\mathbf{v} \in \Lambda_{\mathbf{v}}^0$ si y solo si $p|\phi(\mathbf{v}, \mathbf{v})$, en cuyo caso $\left[\Lambda_{\mathbf{v}} : \Lambda_{\mathbf{v}}^0\right] = p$. En caso contrario $\left[\Lambda_{\mathbf{v}} : \Lambda_{\mathbf{v}}^0\right] = p^2$. □

Lema 1.3.2. $\Lambda_{\mathbf{v}}$ *es integral si y solo si* $p^2|\phi(\mathbf{v})$.

Demostración. Si $\Lambda_{\mathbf{v}}$ es integral, $\phi\left(\frac{\mathbf{v}}{p}\right) \in \mathbb{Z}$ y $p^2|\phi(\mathbf{v})$.

Recíprocamente, tenemos que por definición $\frac{\phi(\mathbf{u},\mathbf{v})}{p} \in \mathbb{Z}$ para todo $\mathbf{u} \in \Lambda_{\mathbf{v}}^0$, y

$$\phi\left(x\frac{\mathbf{v}}{p} + \mathbf{u}\right) = x^2\frac{\phi(\mathbf{v})}{p^2} + x\frac{\phi(\mathbf{u}, \mathbf{v})}{p} + \phi(\mathbf{u}),$$

que es entero si $p^2|\phi(\mathbf{v})$. □

Proposición 1.3.3. *Si* $\mathbf{v} \in \Lambda$, *una condición necesaria y suficiente para que* Λ *y* $\Lambda_{\mathbf{v}}$ *sean p-vecinos es que* $\mathbf{v} \notin p\Lambda^{\#}$ *y* $p^2|\phi(\mathbf{v})$.

Demostración. Si son p-vecinos, por el Lema 1.3.2, $p^2|\phi(\mathbf{v})$. Además, si $\mathbf{v} \in p\Lambda^{\#}$ claramente $\phi(\Lambda, \Lambda_{\mathbf{v}}) \subset \mathbb{Z}$, contradiciendo la definición de p-vecindad.

Si se cumplen las condiciones de la proposición por el Lema 1.3.2 $\Lambda_{\mathbf{v}}$ es integral. En este caso el Lema 1.3.1 nos dice que $\Lambda_{\mathbf{v}}^0 = \Lambda \cap \Lambda_{\mathbf{v}}$ tiene índice p en Λ y $\Lambda_{\mathbf{v}}$. Finalmente, tomemos $\frac{\mathbf{v}}{p} \in \Lambda_{\mathbf{v}}$ y $\mathbf{w} \in \Lambda - \Lambda_{\mathbf{v}}^0$. Luego $\phi\left(\mathbf{w}, \frac{\mathbf{v}}{p}\right) \notin \mathbb{Z}$, por lo que $\phi(\Lambda, \Lambda_{\mathbf{v}}) \not\subset \mathbb{Z}$. □

Proposición 1.3.4. *Si Γ es un retículo p-vecino de Λ, existe $\mathbf{v} \in \Lambda$ tal que $\Gamma = \Lambda_{\mathbf{v}}$.*

Demostración. Por definición de p-vecindad existe un vector $\mathbf{w} \in \Gamma$ tal que $\phi(\Lambda, \mathbf{w}) \notin \mathbb{Z}$, o sea $\mathbf{w} \notin \Lambda^{\#}$ y $\mathbf{v} = p\mathbf{w} \notin p\Lambda^{\#}$. Por otro lado, como $[\Gamma : \Lambda \cap \Gamma] = p$, $\mathbf{v} \in \Lambda$, además $p^2|\phi(\mathbf{v})$. Con esto probamos que $\Lambda_{\mathbf{v}}$ es un p-vecino de Λ.

Falta probar que $\Gamma = \Lambda_{\mathbf{v}}$. Por hipótesis existe $\mathbf{u} \in \Lambda$ tal que $\phi(\mathbf{u}, \mathbf{w}) \notin \mathbb{Z}$, por lo que $\Lambda = \Lambda_{\mathbf{v}}^0 + \mathbb{Z}\mathbf{u}$, ya que $\mathbf{u} \notin \Lambda_{\mathbf{v}}^0$. Si $\mathbf{x} \in \Lambda \cap \Gamma$, $\mathbf{x} = \mathbf{y} + \lambda\mathbf{u}$ con $\mathbf{y} \in \Lambda_{\mathbf{v}}^0$ y $\lambda \in \mathbb{Z}$. Vemos entonces que

$$0 \equiv \phi(\mathbf{x}, \mathbf{v}) \equiv \phi(\mathbf{y}, \mathbf{v}) + \lambda\phi(\mathbf{u}, \mathbf{v}) \pmod{p}$$

por lo que $\lambda \in p\mathbb{Z}$ y $\Lambda \cap \Gamma \subset \Lambda_{\mathbf{v}}^0$. Ahora

$$p = [\Lambda : \Lambda \cap \Gamma] = \left[\Lambda : \Lambda_{\mathbf{v}}^0\right] \left[\Lambda_{\mathbf{v}}^0 : \Lambda \cap \Gamma\right] = p \left[\Lambda_{\mathbf{v}}^0 : \Lambda \cap \Gamma\right]$$

y $\left[\Lambda_{\mathbf{v}}^0 : \Lambda \cap \Gamma\right] = 1$, por lo que $\Lambda \cap \Gamma = \Lambda_{\mathbf{v}}^0$. Finalmente, como $\mathbf{w} \notin \Lambda \cap \Gamma$,

$$\Lambda_{\mathbf{v}} = \Lambda_{\mathbf{v}}^0 + \mathbb{Z}\mathbf{w} = \Lambda \cap \Gamma + \mathbb{Z}\mathbf{w} = \Gamma \ .$$

□

Teorema 1.3.5. *El mapa $\mathbf{v} \mapsto \Lambda_{\mathbf{v}}$, para $\mathbf{v} \in \Lambda$ en las condiciones de la Proposición 1.3.3, induce una biyeccion entre el conjunto de soluciones proyectivas no singulares de*

$$\phi(\mathbf{v}) \equiv 0 \pmod{p}, \quad \mathbf{v} \in \Lambda \tag{1.7}$$

y los retículos p-vecinos de Λ. Además, si $\Lambda_1 \neq \Lambda_2$ son dos retículos p-vecinos, entonces $\Lambda_1 \cap \Lambda_2 \subset \Lambda$.

Demostración. Sea $\mathbf{v}$ una solución no singular de (1.7). Como $\mathbf{v} \notin p\Lambda^{\#}$ por ser solución no singular, existe $\mathbf{u} \in \Lambda$ tal que $p \nmid \phi(\mathbf{v}, \mathbf{u})$. Podemos elegir entonces $\alpha \in \mathbb{Z}$ que cumple

$$\phi(\mathbf{v} + p\alpha\mathbf{u}) \equiv \phi(\mathbf{v}) + p\alpha\phi(\mathbf{v}, \mathbf{u}) \equiv 0 \pmod{p^2}$$

y $\mathbf{v} + p\alpha\mathbf{u}$ corresponde a la misma solución proyectiva. Asumimos luego que $p^2|\phi(\mathbf{v})$.

Sean $\mathbf{v}_1$ y $\mathbf{v}_2$ son vectores en Λ, con $p^2|\phi(\mathbf{v}_1)$ y $p^2|\phi(\mathbf{v}_2)$. Si $\mathbf{v}_1$, $\mathbf{v}_2$ corresponden a la misma solución de (1.7), tenemos que $\mathbf{v}_1 = x\mathbf{v}_2 + p\mathbf{u}$ para algún $x \not\equiv 0 \pmod{p}$ y $\mathbf{u} \in \Lambda$. Aplicando ϕ, vemos que $0 \equiv xp\phi(\mathbf{v}_1, \mathbf{u}) \pmod{p^2}$, y $\mathbf{u} \in \Lambda^0_{\mathbf{v}_1}$. Entonces $\frac{\mathbf{v}_2}{p} = x\frac{\mathbf{v}_1}{p} + \mathbf{u} \in \Lambda_{\mathbf{v}_1}$, por lo que $\Lambda_{\mathbf{v}_2} = \Lambda_{\mathbf{v}_1}$.

Por otro lado, si $\mathbf{v}_1$ y $\mathbf{v}_2$ corresponden a soluciones diferentes tenemos que $\frac{\mathbf{v}_1}{p} \notin \frac{\mathbf{v}_2}{p} + \Lambda$. Como $\Lambda_{\mathbf{v}_2} \subset \frac{\mathbf{v}_2}{p} + \Lambda$, vemos que $\frac{\mathbf{v}_1}{p} \notin \Lambda_{\mathbf{v}_2}$, por lo que $\Lambda_{\mathbf{v}_1} \neq \Lambda_{\mathbf{v}_2}$. También probamos que $\frac{\mathbf{v}_1}{p} \notin \Lambda_{\mathbf{v}_1} \cap \Lambda_{\mathbf{v}_2} \subset \frac{\mathbf{v}_1}{p} + \Lambda$, por lo que $\Lambda_{\mathbf{v}_1} \cap \Lambda_{\mathbf{v}_2} \subset \Lambda$.

La sobreyectividad se deduce directamente de las proposiciones (1.3.3) y (1.3.4). □

1.3.2. Módulo de Brandt

Estamos en posición de definir el módulo de Brandt asociado a un retículo cuadrático.

Definición 1.3.1. Sea Λ un $\mathbb{Z}$-retículo definido positivo en un $\mathbb{Q}$-espacio cuadrático de dimensión 3, $(V,\ \phi)$. Definimos el módulo clásico de Brandt ternario asociado a Λ como el $\mathbb{Z}$-módulo libre con base las clases de equivalencia propias en el género de Λ, y lo denotamos como $\widetilde{\mathcal{M}}(\Lambda)$.

Los operadores de Hecke $\tilde{t}_p : \widetilde{\mathcal{M}}(\Lambda) \to \widetilde{\mathcal{M}}(\Lambda)$ son operadores lineales definidos en la base de la siguiente manera

$$\tilde{t}_p \overline{\Gamma} = \sum_i \overline{\Gamma_i} \ ,$$

donde la suma es sobre todos los p-vecinos de Γ. Se verá en el próximo capítulo, Subsección 2.3.1, que dos retículos p-vecinos están en el mismo género, por lo cual la definición tiene sentido.

Podemos definir también un producto interno en $\widetilde{\mathcal{M}}_{\mathbb{R}}(\Lambda) = \widetilde{\mathcal{M}}(\Lambda) \otimes \mathbb{R}$ de la siguiente manera,

$$\left\langle \overline{\Gamma}, \overline{\Gamma'} \right\rangle = \#\left\{ \sigma \in O^+(V) : \sigma\Gamma = \Gamma' \right\} = \begin{cases} \#O^+(\Gamma) & \text{si } \overline{\Gamma} = \overline{\Gamma'} \\ 0 & \text{en otro caso .} \end{cases}$$

Proposición 1.3.6. *Los operadores de Hecke $\tilde{t}_p$ generan un álgebra conmutativa de operadores autoadjuntos. Por lo tanto $\widetilde{\mathcal{M}}_{\mathbb{R}}(\Lambda)$ tiene una base ortogonal simultánea para todos los operadores $\tilde{t}_p$.*

Demostración. Es claro que $\tilde{t}_p$ y $\tilde{t}_q$ conmutan para $p \neq q$. Para probar que $\tilde{t}_p$ es autoadjunta, vemos que

$$\begin{aligned} \left\langle \tilde{t}_p\overline{\Gamma}, \overline{\Gamma'} \right\rangle &= \#\left\{ \sigma \in O^+(V) : \sigma\Gamma' \text{ } p\text{-vecino de } \Gamma \right\} \\ &= \#\left\{ \sigma \in O^+(V) : \Gamma' \text{ } p\text{-vecino de } \sigma^{-1}\Gamma \right\} \\ &= \left\langle \overline{\Gamma}, \tilde{t}_p\overline{\Gamma'} \right\rangle \ . \end{aligned}$$

Lo último se deduce del teorema espectral. □

1.3.3. Ejemplos

Ejemplo 1.3.1. Sean $V = \mathbb{Q}^3$, $\phi(x,y,z) = x^2 + y^2 + 3z^2 - xz$ espacio cuadrático y $\Lambda_1 = \mathbb{Z}^3$. El retículo Λ_1 tiene discriminante 11. El otro retículo en el género de Λ_1 es $\Lambda_2 = \mathbf{v}_1\mathbb{Z} + \mathbf{v}_2\mathbb{Z} + \mathbf{v}_3\mathbb{Z}$, donde

$$\mathbf{v}_1 = (0,0,-2),\ \mathbf{v}_2 = (-1/2,1/2,0),\ \mathbf{v}_3 = (-1/2,-1/2,0)$$

con $\phi'(x,y,z) = \phi(x\mathbf{v}_1 + y\mathbf{v}_2 + z\mathbf{v}_3) = x^2 + y^2 + 4z^2 + yz + xz + xy$.

Calculemos $\tilde{t}_2$, las soluciones proyectivas de $\phi(x,y,z) \equiv 0 \pmod 2$ son $\mathbf{w}_1 = (1,1,0),\ \mathbf{w}_2 = (0,1,1),\ \mathbf{w}_3 = (1,1,1)$. Se puede ver que $\overline{(\Lambda_1)_{\mathbf{w}_1}} = \overline{\Lambda_1}$ y $\overline{(\Lambda_1)_{\mathbf{w}_2}} = \overline{(\Lambda_1)_{\mathbf{w}_3}} = \overline{\Lambda_2}$.

De la misma manera se puede ver que los vectores $\mathbf{u}_1 = (0,0,1)$, $\mathbf{u}_2 = (0,1,1)$, $\mathbf{u}_3 = (1,0,1)$ son soluciones proyectivas de $\phi'(x,y,z) \equiv 0 \pmod 2$ y $\overline{(\Lambda_2)_{\mathbf{u}_1}} = \overline{(\Lambda_2)_{\mathbf{u}_2}} = \overline{(\Lambda_2)_{\mathbf{u}_3}} = \overline{\Lambda_1}$.

El operador $\tilde{t}_2$, en la base $\{\overline{\Lambda_1}, \overline{\Lambda_2}\}$, es

$$\tilde{t}_2 = \begin{pmatrix} 1 & 3 \\ 2 & 0 \end{pmatrix}$$

con vectores propios $\mathbf{E}_1 = (3,2)$, $\mathbf{E}_2 = (1,-1)$ asociados a 3 y -2 respectivamente. Podemos calcular otros operadores,

$$\tilde{t}_3 = \begin{pmatrix} 2 & 3 \\ 2 & 1 \end{pmatrix},\ \tilde{t}_5 = \begin{pmatrix} 4 & 3 \\ 2 & 3 \end{pmatrix},\ \tilde{t}_7 = \begin{pmatrix} 4 & 6 \\ 4 & 2 \end{pmatrix},\ \tilde{t}_{13} = \begin{pmatrix} 10 & 6 \\ 4 & 8 \end{pmatrix}, \cdots,$$

con los mismos vectores propios y con valores propios 4, 6, 8, 14 y -1, 1, -2, 4 respectivamente. El vector $\mathbf{E}_1$ está asociado a una serie de Eisenstein de peso 2 y nivel 11. El vector $\mathbf{E}_2$ corresponde a la curva elíptica `11a`.

Ejemplo 1.3.2. Sean $V = \mathbb{Q}^3$, $\phi(x,y,z) = x^2 + 7y^2 + 14z^2 - 7yz$. Consideramos $\Lambda_1 = \mathbb{Z}^3$ de discriminante 7^3, y su género. El género está dado por otras dos clases de equivalencia, que son $\Lambda_2 = \mathbf{v}_1\mathbb{Z} + \mathbf{v}_2\mathbb{Z} + \mathbf{v}_3\mathbb{Z}$ y $\Lambda_3 = \mathbf{u}_1\mathbb{Z} + \mathbf{u}_2\mathbb{Z} + \mathbf{u}_3\mathbb{Z}$, con

$$\mathbf{v}_1 = (1,-1/2,0),\ \mathbf{v}_2 = (0,-1/2,-1),\ \mathbf{v}_3 = (0,0,-2),$$

$$\mathbf{u}_1 = (-2/3,-7/3,4/3),\ \mathbf{u}_2 = (-1/3,1/3,2/3),\ \mathbf{u}_3 = (-1/3,1/3,-1/3),$$

y respectivas formas cuadráticas ternarias

$$\phi'(x,y,z) = \phi(x\mathbf{v}_1 + y\mathbf{v}_2 + z\mathbf{v}_3) = x^2 + 2y^2 + 49z^2 - xy,$$

$$\phi''(x,y,z) = \phi(x\mathbf{u}_1 + y\mathbf{u}_2 + z\mathbf{u}_3) = 2x^2 + 7y^2 + 8z^2 - 7yz - xz\ .$$

Calculamos los operadores de Hecke

$$\tilde{t}_2 = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix},\ \tilde{t}_3 = \begin{pmatrix} 0 & 0 & 2 \\ 0 & 0 & 2 \\ 4 & 4 & 0 \end{pmatrix},\ \tilde{t}_5 = \begin{pmatrix} 0 & 0 & 3 \\ 0 & 0 & 3 \\ 6 & 6 & 0 \end{pmatrix}$$

$$\tilde{t}_{11} = \begin{pmatrix} 8 & 4 & 0 \\ 4 & 8 & 0 \\ 0 & 0 & 12 \end{pmatrix},\ \tilde{t}_{13} = \begin{pmatrix} 0 & 0 & 7 \\ 0 & 0 & 7 \\ 14 & 14 & 0 \end{pmatrix},\ \tilde{t}_{17} = \begin{pmatrix} 0 & 0 & 9 \\ 0 & 0 & 9 \\ 18 & 18 & 0 \end{pmatrix}, \cdots,$$

con vectores propios $\mathbf{E}_1 = (1, -1, 0)$, con valores propios 1, 0, 0, 4, 0, 0, $\mathbf{E}_2 = (1, 1, 2)$ con valores propios 3, 4, 6, 12, 14, 18, $\mathbf{E}_3 = (1, 1, -2)$ con valores propios 3, -4, -6, 12, -14, -18. En este caso, el vector $\mathbf{E}_1$ está asociado a la curva elíptica `49a`, curva con multiplicación compleja. Los vectores $\mathbf{E}_2$ y $\mathbf{E}_3$ están asociados a series de Eisenstein de peso 2 y nivel 7^2.

Capítulo 2

Módulo de Brandt Generalizado

En el presente capítulo introducimos la noción de norma spin para autometrías de un espacio cuadrático, esto es una definición clásica que se puede encontrar en [2]. Refinamos la noción de equivalencia propia usando la norma spin en el concepto de Θ-clase y Θ-género. Definimos $\mathscr{U}$-género y mostramos que hay una cantidad finita de Θ-clases. Por último, definimos el módulo de Brandt ternario como el $\mathbb{Z}$-módulo libre con base las Θ-clases de ciertos $\mathscr{U}$-géneros. Esto último es introducido por Tornaría en su tesis doctoral. Mostramos ejemplos y vemos como en este caso la descomposición espectral de los operadores de Hecke encuentran curvas elípticas con signo negativo en su ecuación funcional.

2.1. La norma spin

2.1.1. El álgebra de Clifford

Consideramos un álgebra A sobre un cuerpo k, de característica diferente de 2, de dimensión finita y con unidad. Necesitaremos el siguiente lema sobre existencia de inversos en álgebras.

Lema 2.1.1. *Sea* $\mathbf{u}$ *un elemento de la* k*-álgebra* A*. Supongamos que existe una solución* $\mathbf{v}$ *de*

$$\mathbf{uv} = 1,$$

o una solución $\mathbf{w}$ *de*

$$\mathbf{wu} = 1 \ .$$

Entonces existe una solución de cada ecuación y

$$\mathbf{v} = \mathbf{w} \ .$$

Además, las soluciones $\mathbf{v}$*,* $\mathbf{w}$ *son únicas.*

Demostración. Supongamos que existe $\mathbf{v}$. El mapa

$$\mathbf{x} \to \mathbf{xu} \ \forall \mathbf{x} \in A$$

es un mapa lineal de A en A, considerado como espacio vectorial. Si $\mathbf{y}$ está en el núcleo, se ve que

$$0 = (\mathbf{yu})\mathbf{v} = \mathbf{y}(\mathbf{uv}) = \mathbf{y}$$

y como A tiene dimensión finita, el mapa es invertible. En conclusión, existe un $\mathbf{w}$ que cumple $\mathbf{wu} = 1$. De igual manera se prueba que si $\mathbf{w}$ existe, $\mathbf{v}$ también.

Por otro lado

$$\mathbf{w} = \mathbf{w}(\mathbf{uv}) = (\mathbf{wu})\mathbf{v} = \mathbf{v} \ .$$

□

Teorema 2.1.2. *Sea $(V,\ \phi)$ un espacio cuadrático regular de dimensión n sobre un cuerpo k con característica diferente de 2. Existe un álgebra $C(V)$, llamada el álgebra de Clifford de $(V,\ \phi)$, sobre k que contiene a V como subespacio y cumple las siguientes propiedades:*

1. *$C(V)$ tiene dimensión 2^n.*
2. *$C(V)$ está generada por V. Más precisamente, está generada por 1 y por los productos*

$$\mathbf{x}_1\mathbf{x}_2\cdots\mathbf{x}_r,\ \forall r > 0, \mathbf{x}_j \in V \ .$$

3. *$\mathbf{xx} = \phi(\mathbf{x})\ \forall \mathbf{x} \in V$.*

Además, estas propiedades determinan $C(V)$ de manera única. Eso quiere decir que si $C'(V)$ es otra álgebra que cumple las condiciones (1), (2), y (3) entonces existe un isomorfismo de k-álgebras entre $C(V)$ y $C'(V)$ que deja fijo V.

Demostración. Si existe $C(V)$ y $\mathbf{x}$, $\mathbf{y} \in V$, la propiedad (3) implica que

$$\begin{aligned}\mathbf{xy} + \mathbf{yx} &= (\mathbf{x}+\mathbf{y})(\mathbf{x}+\mathbf{y}) - \mathbf{xx} - \mathbf{yy} \\ &= \phi(\mathbf{x}+\mathbf{y}) - \phi(\mathbf{x}) - \phi(\mathbf{y}) \\ &= 2\phi(\mathbf{x},\mathbf{y}) \ .\end{aligned}$$

Sea ahora $\mathbf{e}_1, \ldots, \mathbf{e}_n$ una base normal de V, como $\phi(\mathbf{e}_i, \mathbf{e}_j) = 0$ si $i \neq j$, vemos que

$$\mathbf{e}_i\mathbf{e}_j + \mathbf{e}_j\mathbf{e}_i = 0 \text{ si } i \neq j \ . \tag{2.1}$$

También, por la propiedad (2)

$$\mathbf{e}_i\mathbf{e}_i = \phi(\mathbf{e}_i) \in k \ . \tag{2.2}$$

Sea $J \subset \{1, 2, \ldots, n\}$ ordenado de manera creciente,

$$j_1 < j_2 < \ldots < j_r,$$

donde $r \leq n$. Definimos

$$\mathbf{e}(J) = \mathbf{e}(j_1)\mathbf{e}(j_2)\cdots\mathbf{e}(j_n) \text{ y } \mathbf{e}(j) = \mathbf{e}_j \ .$$

Denotamos $E = \varnothing$ y $\mathbf{e}(E) = 1$. Por la propiedad (2) el conjunto $\mathbf{e}(J)$, $J \subset \{1, \ldots, n\}$, genera $C(V)$. Y como $\dim(C(V)) = 2^n$, es base.

Si $I, J \subset \{1, \ldots, n\}$, por (2.1), (2.2)

$$\mathbf{e}(I)\mathbf{e}(J) = l(I, J)\mathbf{e}(I\Delta J), \tag{2.3}$$

donde

$$l(I, J) = \prod_{i\in I,\ j\in J,\ i>j} (-1) \cdot \prod_{i\in I\cap J} \phi(\mathbf{e}_i) \ . \tag{2.4}$$

Esto nos sirve para ver que

$$(\mathbf{e}(J_1)\mathbf{e}(J_2))\ \ \mathbf{e}(J_3) = \mathbf{e}(J_1)\ (\mathbf{e}(J_2)\mathbf{e}(J_3)) \ .$$

Podemos construir ahora $C(V)$. Para ello tomamos un espacio vectorial con dimensión 2^n, con base que denotamos por $\mathbf{e}(J)\ \forall J \in \{1, \ldots, n\}$. Definimos el producto en $C(V)$ dado por (2.3) y (2.4), que se extiende por linealidad a todo $C(V)$, que además es asociativo. Identificamos V como subespacio de $C(V)$ denotando

$$\mathbf{e}_i = \mathbf{e}(\{i\}),\ \forall 1 \leq i \leq n \ .$$

Por (2.1) y (2.2)

$$\mathbf{e}_i\mathbf{e}_i = \phi(\mathbf{e}_i) \quad \mathbf{e}_i\mathbf{e}_j + \mathbf{e}_j\mathbf{e}_i = 0\ i \neq j \ .$$

Finalmente, si $\mathbf{x} = \sum x_i\mathbf{e}_i \in V$, como $\mathbf{e}(E) = 1$

$$\mathbf{x}\mathbf{x} = \sum_{i,j} x_i x_j \mathbf{e}_i\mathbf{e}_j = \sum_i x_i^2 \phi(\mathbf{e}_i) = \phi(\mathbf{x}) \ .$$

El álgebra $C(V)$ construida cumple las tres propiedades del teorema, y la última afirmación del teorema es clara. □

La autometría de V

$$\mathbf{x} \mapsto -\mathbf{x},$$

induce un isomorfismo de $C(V)$ con $C(V)$ de orden 2. Definimos como $C_0(V)$ a los elementos de $C(V)$ que quedan fijos por el isomorfismo y $C_1(V)$ como los elementos que son enviados a su opuesto. Es fácil de ver que $C_0(V)$ está generado por los $\mathbf{e}(J)$ con $|J|$ par, y $C_1(V)$ está generado por los $\mathbf{e}(J)$ con $|J|$ impar. Además se verifica que $\dim(C_0(V)) = \dim(C_1(V)) = 2^{n-1}$, así como $C(V) = C_0(V) \oplus C_1(V)$ como espacios vectoriales.

Tenemos el siguiente lema sobre la estructura de $C_i(V)$.

Lema 2.1.3.

$$C_i(V)C_j(V) \subset C_m(V)$$

donde $i, j, m = 0$ *o* 1 *y* $m \equiv i + j \pmod 2$. *Además, si* $\mathbf{u} \in C_i(V)$ *y* $\mathbf{u}^{-1}$ *existe entonces* $\mathbf{u}^{-1} \in C_i(V)$.

Corolario 2.1.4. $C_0(V)$ *es una subálgebra de* $C(V)$

Lema 2.1.5. *Sea* $(V,\ \phi)$ *un espacio cuadrático regular. Un elemento de* $C_0(V)$ *que conmuta con todo elemento de* V, *pertenece a* k.

Demostración. Si el número de elementos de J es par, es fácil de verificar que

$$\mathbf{e}_i\mathbf{e}(J) = \begin{cases} +\mathbf{e}(J)\mathbf{e}_i & \text{si } i \notin J \\ -\mathbf{e}(J)\mathbf{e}_i & \text{si } i \in J\ . \end{cases}$$

□

Lema 2.1.6. *Existe un mapa* k*-lineal* $C(V) \to C(V)$, *que denotamos por* $\mathbf{u} \mapsto \mathbf{u}'$ *que cumple lo siguiente:*

1. $\mathbf{u}' = \mathbf{u}$ *si* $\mathbf{u} \in k$ *o* $\mathbf{u} \in V$.
2. $(\mathbf{uv})' = \mathbf{v}'\mathbf{u}'\ \forall \mathbf{u}, \mathbf{v} \in C(V)$.
3. $(\mathbf{u}')' = \mathbf{u}\ \forall \mathbf{u} \in C(V)$.

Demostración. Basta definir el mapa en la base $\mathbf{e}(J)$ de $C(V)$. Si $\mathbf{e}(J) = \mathbf{e}(j_1)\cdots\mathbf{e}(j_r)$, definimos

$$\mathbf{e}(J)' = \mathbf{e}(j_r)\cdots\mathbf{e}(j_1),$$

y es claro que si extendemos linealmente $'$, cumple lo requerido. □

Lema 2.1.7. *Sea* $\mathbf{u} \in C(V)$ *tal que*

$$\mathbf{uu}' \in k^\times\ .$$

Luego

$$\mathbf{u}'\mathbf{u} = \mathbf{uu}',$$

y

$$\mathbf{u}^{-1} = (\mathbf{uu}')^{-1}\mathbf{u}'\ .$$

Demostración.

$$\begin{aligned} \mathbf{u}((\mathbf{uu}')^{-1}\mathbf{u}') &= \mathbf{u}(\mathbf{u}')^{-1}\mathbf{u}^{-1}\mathbf{u}' \\ &= (\mathbf{u}^{-1}\mathbf{u}')^{-1}(\mathbf{u}^{-1}\mathbf{u}') \\ &= 1, \end{aligned}$$

con lo que probamos la segunda ecuación. La primera se deduce de la unicidad del inverso. □

2.1.2. La norma spin

Suponemos ahora que $(V,\ \phi)$ es regular.

Lema 2.1.8. *Sea* $\mathbf{u} \in C(V)$*, invertible, que cumple*

$$\mathbf{uxu}^{-1} \in V\ \forall \mathbf{x} \in V\ .$$

El mapa lineal

$$\mathbf{T_u} : \mathbf{x} \to \mathbf{uxu}^{-1}, \tag{2.5}$$

es una autometría de V*.*

Demostración.

$$\begin{aligned}\phi(\mathbf{uxu}^{-1}) &= (\mathbf{uxu}^{-1})(\mathbf{uxu}^{-1}) \\ &= \mathbf{u}(\mathbf{xx})\mathbf{u}^{-1} \\ &= (\mathbf{xx})(\mathbf{uu}^{-1}) \\ &= \mathbf{xx} \\ &= \phi(\mathbf{x})\ .\end{aligned}$$

□

Cuando $\mathbf{u} = \mathbf{y} \in V$ con $\phi(\mathbf{y}) \neq 0$ se ve que

$$\mathbf{y}^{-1} = (\phi(\mathbf{y}))^{-1}\mathbf{y}\ .$$

Usando la definición de la forma bilineal ϕ y (1.6) vemos que

$$\begin{aligned}\mathbf{yxy} &= (\mathbf{yx} + \mathbf{xy})\mathbf{y} - \mathbf{xyy} \\ &= 2\phi(\mathbf{x}, \mathbf{y})\mathbf{y} - \phi(\mathbf{y})\mathbf{x},\end{aligned}$$

y

$$\mathbf{yxy}^{-1} = -\tau_{\mathbf{y}}\mathbf{x}\ . \tag{2.6}$$

Definición 2.1.1. Denotamos por $M_0(V)$ como el conjunto de los elementos $\mathbf{u} \in C_0(V)$ que cumplen:

1. $\mathbf{u}$ es invertible.
2. $\mathbf{uxu}^{-1} \in V\ \forall \mathbf{x} \in V$.

$M_0(V)$ claramente es un grupo con el producto.

Teorema 2.1.9. *El mapa* $\mathbf{u} \mapsto \mathbf{T_u}$ *dado por (2.5) establece un isomorfismo entre* $M_0(V)/k^\times$ *y* O^+*.*

Demostración. Claramente $\mathbf{u} \mapsto \mathbf{T_u}$ es un homomorfismo de grupos. Por el Lema 2.1.5 el núcleo es $k^\times$. Tenemos que mostrar que la imagen es O^+.

Supongamos que $\sigma \in O^+$. Sabemos que

$$\sigma = \tau_{\mathbf{a}_1}\tau_{\mathbf{a}_2}\cdots\tau_{\mathbf{a}_r}$$

para algún r par y $\mathbf{a}_j \in V$ con $\phi(\mathbf{a}_j) \neq 0$. Sea

$$\mathbf{u} = \mathbf{a}_1\mathbf{a}_2\cdots\mathbf{a}_r \ .$$

Entonces

$$\mathbf{u}' = \mathbf{a}_r\mathbf{a}_{r-1}\cdots\mathbf{a}_1$$

y

$$\mathbf{u}\mathbf{u}' = \prod_{1\leq j\leq r} \phi(\mathbf{a}_j) \in k^\times$$

con lo que se ve que $\mathbf{u} \in M_0(V)$. Además, con múltiples aplicaciones de (2.6), $\mathbf{T_u x} = \sigma\mathbf{x}$ para todo $\mathbf{x} \in V$. Probando que la imagen de $\mathbf{u} \mapsto \mathbf{T_u}$ contiene a O^+.

Supongamos ahora que $\mathbf{u} \in M_0(V)$ con $\mathbf{T_u} \notin O^+$. Luego $\mathbf{T_u} \in O^-$, y de vuelta

$$\mathbf{T_u} = \tau_{\mathbf{a}_1}\tau_{\mathbf{a}_2}\cdots\tau_{\mathbf{a}_r}$$

con $\mathbf{a}_j \in V$, $\phi(\mathbf{a}_j) \in k^\times$, donde r es impar. Sea

$$\mathbf{v} = \mathbf{a}_1\mathbf{a}_2\cdots\mathbf{a}_r \ .$$

Por (2.6) tenemos

$$\mathbf{v}\mathbf{x}\mathbf{v}^{-1} = -\mathbf{T_u x} = -\mathbf{u}\mathbf{x}\mathbf{u}^{-1} \ \forall \mathbf{x} \in V,$$

y tomando $\mathbf{w} = \mathbf{u}^{-1}\mathbf{v}$ vemos que

$$\mathbf{w} \in C_1(V), \quad \mathbf{w}\mathbf{x} = -\mathbf{x}\mathbf{w} \ \forall \mathbf{x} \in V,$$

ya que $\mathbf{u}^{-1} \in C_0(V)$ y $\mathbf{v} \in C_1(V)$ y con un análogo al Lema 2.1.5 vemos que $\mathbf{w} = 0$, que contradice que sea invertible. □

Corolario 2.1.10. *Si* $\mathbf{u} \in M_0(V)$ *entonces*

$$\mathbf{u} = \mathbf{a}_1\cdots\mathbf{a}_r$$

con $\mathbf{a}_j \in V$ *y un* r *par. Además,*

$$\mathbf{u}\mathbf{u}' \in k^\times \ .$$

Demostración. Probamos que $\sigma = \mathbf{T_u}$ es de la forma

$$\tau_{\mathbf{a}_1}\tau_{\mathbf{a}_2}\cdots\tau_{\mathbf{a}_r}$$

y $\mathbf{u}^{-1}\mathbf{a}_1\mathbf{a}_2\cdots\mathbf{a}_r$ conmuta con todo elemento de V, por lo que pertenece a $k^\times$. Probamos entonces que $\mathbf{u} = l\mathbf{a}_1\mathbf{a}_2\cdots\mathbf{a}_r$ para algún $l \in k^\times$. El corolario queda probado sustituyendo $\mathbf{a}_1$ por $l\mathbf{a}_1$ □

Del teorema obtenemos inmediatamente:

Corolario 2.1.11. *Existe un homomorfismo* $\theta : O^+ \to k^\times/(k^\times)^2$*, definido de la siguiente manera. Si* $\sigma = \mathbf{T_u}$*, entonces*

$$\theta(\sigma) = (\mathbf{u}\mathbf{u}')(k^\times)^2 \ .$$

Llamamos a $\theta(\sigma)$ la norma spin de σ. Observamos que si $\sigma = \tau_{\mathbf{a}_1}\cdots\tau_{\mathbf{a}_r}$ entonces

$$\theta(\sigma) = \phi(\mathbf{a}_1)\cdots\phi(\mathbf{a}_r)(k^\times)^2 \ .$$

El núcleo de θ lo denotamos por Θ, o sea

$$\Theta = \Theta(V) = \left\{\sigma \in O^+ : \theta(\sigma) = 1\right\} \ .$$

Proposición 2.1.12. *Si* $n = 3$*, entonces* $\Theta(V)$ *es el subgrupo conmutador de* $O(V)$*.*

Demostración. Claramente Θ contiene el conmutador ya que θ tiene codominio abeliano. Hay que probar que todo $\sigma \in \Theta$ es un conmutador. Por la Observación 1.2.10, podemos escribir $\sigma = \tau_{\mathbf{u}}\tau_{\mathbf{v}}$ con $\mathbf{u}$, $\mathbf{v} \in V$ anisotrópicos, ya que $\sigma \in O^+(V)$. Como $\theta(\sigma) = 1$, se ve que $\phi(\mathbf{u})\phi(\mathbf{v}) \in (k^\times)^2$, y podemos asumir que $\phi(\mathbf{u}) = \phi(\mathbf{v})$ luego de reescalar $\mathbf{v}$. Por el Corolario 1.2.7 existe una autometría $\rho \in O(V)$ tal que $\rho\mathbf{u} = \mathbf{v}$, entonces

$$\sigma = \tau_{\mathbf{u}}\rho\tau_{\mathbf{u}}\rho^{-1} = \tau_{\mathbf{u}}\rho\tau_{\mathbf{u}}^{-1}\rho^{-1}$$

que es un conmutador. □

Denotamos la imagen de θ como $\theta(V)$, o sea

$$\theta(V) = \left\{\theta(\sigma) : \sigma \in O^+(V)\right\} \subset k^\times/(k^\times)^2 \ .$$

Si $k = \mathbb{Q}$ decimos que V es definido cuando $\theta(V) > 0$. Esta definición está relacionada con la usual por el siguiente lema.

Lema 2.1.13. *Son equivalentes:*

1. V *es definido.*
2. $\phi(V) \geq 0$ *o* $\phi(V) \leq 0$*.*

Demostración. Si $\theta(V) > 0$, y $\mathbf{v}_1$, $\mathbf{v}_2$ son vectores anisotrópicos de V, $\sigma = \tau_{\mathbf{v}_1}\tau_{\mathbf{v}_2} \in O^+(V)$ y $\theta(\sigma) = \phi(\mathbf{v}_1)\phi(\mathbf{v}_2) > 0$. Como lo anterior se cumple para todo par de vectores anisotrópicos tenemos que $\phi(V) \geq 0$ o $\phi(V) \leq 0$.

Recíprocamente, si la imagen de todo vector anisotrópico por ϕ tiene el mismo signo y $\sigma \in O^+(V)$, entonces $\sigma = \tau_{\mathbf{v}_1} \cdots \tau_{\mathbf{v}_{2s}}$. Además $\theta(\sigma) = \phi(\mathbf{v}_1) \cdots \phi(\mathbf{v}_{2s}) > 0$ y $\theta(V) > 0$. □

También para $k = \mathbb{Q}$ tenemos el siguiente resultado.

Proposición 2.1.14. *Sea $(V,\ \phi)$ un espacio cuadrático sobre $\mathbb{Q}$ de dimensión al menos 3. Entonces*

$$\theta(V) = \begin{cases} \mathbb{Q}^\times & \text{si } V \text{ es indefinido} \\ \mathbb{Q}_{>0} & \text{si } V \text{ es definido.} \end{cases}$$

Demostración. Ver lema 3.2 en [2]. □

Si Λ es un retículo, definimos la imagen de la norma spin restricta al grupo de autometrías de Λ como

$$\theta(\Lambda) = \{\theta(\sigma) : \sigma \in O^+(\Lambda)\}$$

y tenemos el siguiente lema para retículos en la misma clase de equivalencia.

Lema 2.1.15. *Si Λ y Γ son equivalentes, entonces*

$$\theta(\Lambda) = \theta(\Gamma)\ .$$

Demostración. Si $\sigma\Lambda = \Gamma$, entonces

$$O^+(\Lambda) = \{\sigma^{-1}\rho\sigma : \rho \in O^+(\Gamma)\}$$

y $\theta(\sigma^{-1}\rho\sigma) = \theta(\rho)$. □

Lema 2.1.16. *Sea Λ_p un $\mathbb{Z}_p$-retículo unimodular de dimensión al menos 2, se cumple que*

$$\theta(\Lambda_p) = \mathbb{Z}_p^\times(\mathbb{Q}_p^\times)^2\ .$$

Demostración. Puede ser probado usando los teoremas 55 y 56 de [10]. □

2.2. Θ-equivalencia y $\mathscr{U}$-géneros

2.2.1. Θ-equivalencia

Refinamos la noción de equivalencia de retículos de la siguiente manera: decimos que Λ y Γ son Θ-equivalentes, y lo denotamos por $\Lambda \simeq \Gamma$, si

$$\sigma\Lambda = \Gamma,\ \text{para algún } \sigma \in \Theta(V)$$

que es claramente una relación de equivalencia. La Θ-clase de Λ es

$$[\Lambda] = \{\Gamma : \Gamma \simeq \Lambda\} = \{\sigma\Lambda : \sigma \in \Theta(V)\} \ .$$

Para entender el refinamiento introducido consideramos el conjunto

$$\mathscr{C}(\Lambda) = \{[\Gamma] : \Gamma \sim \Lambda\} \, ,$$

o sea, el conjunto de Θ-clases de retículos propiamente equivalentes a Λ. Tenemos una acción transitiva de $\theta(\Lambda)$ en $\mathscr{C}(\Lambda)$ dada por

$$[\Gamma]^{\theta(\sigma)} = [\sigma\Gamma] \ .$$

Está bien definido porque si $\theta(\rho) = \theta(\sigma)$ para otro $\rho \in O^+(V)$, entonces

$$\rho\Gamma = (\rho\sigma^{-1})\sigma\Gamma \simeq \sigma\Gamma \ .$$

De igual manera se ve que si $\Gamma' \simeq \Gamma$, entonces $\sigma\Gamma' \simeq \sigma\Gamma$.

Proposición 2.2.1. *El conjunto $\mathscr{C}(\Lambda)$ es un espacio homogéneo principal para $\theta(V)/\theta(\Lambda)$.*

Demostración. Hay que probar que la acción de $\theta(V)/\theta(\Lambda)$ en $\mathscr{C}(\Lambda)$ es libre y transitiva. Ya probamos que es transitiva por lo que nos falta ver que es libre. Sea entonces $\Gamma \sim \Lambda$, queremos ver que $[\Gamma]^s = [\Gamma]$ si y solo si $s \in \theta(\Lambda)$. Por el Lema 2.1.15, $\theta(\Gamma) = \theta(\Lambda)$. Si $s = \theta(\sigma)$, con $\sigma \in O^+(\Gamma)$, entonces

$$[\Gamma]^s = [\sigma\Gamma] = [\Gamma] \ .$$

Por otro lado, si $[\Gamma]^s = [\Gamma]$, con $s = \theta(\sigma) \in \theta(V)$, se deduce que $\rho\sigma\Gamma = \Gamma$ para algún $\rho \in \Theta(V)$. Pero $\rho\sigma \in O^+(\Gamma)$, y

$$s = \theta(\sigma) = \theta(\rho\sigma) \in \theta(\Gamma) = \theta(\Lambda) \ .$$

□

La proposición nos permite definir lo siguiente. Si Λ y Γ son dos retículos en V, la θ-distancia entre ellos es

$$\theta(\Lambda, \Gamma) = \begin{cases} \infty & \text{si } \Lambda \not\sim \Gamma \\ \theta(\sigma) \in \theta(V)/\theta(\Lambda) & \text{si } \sigma\Lambda = \Gamma \ . \end{cases}$$

O sea, $\Lambda \sim \Gamma$ si y solo si $\theta(\Lambda, \Gamma) = s \neq \infty$, en cuyo caso $[\Lambda]^s = [\Gamma]$, y $\Lambda \simeq \Gamma$ si y solo si $\theta(\Lambda, \Gamma) = 1$. En otras palabras, $\theta(\Lambda, \Gamma) =$ "$[\Gamma]/[\Lambda]$" en el sentido de la Proposición 2.2.1.

2.2.2. $\mathscr{U}$-género

Análogamente a la definición de género decimos que Λ y Γ están en el mismo Θ-género si

$$\Lambda_p \simeq \Gamma_p \quad \forall p \ .$$

Observamos que el Θ-género no es cerrado por la acción de $O^+(V)$. La clausura de un Θ-género por la acción de $O^+(V)$ es por definición un género spin.

Consideramos

$$\mathscr{U}(V_p) = \left\{ \sigma \in O^+(V_p) : \theta(\sigma) \in \mathbb{Z}_p^\times \right\}.$$

Decimos que los retículos Λ y Γ están en el mismo $\mathscr{U}$-género si

$$\sigma_p \Lambda_p = \Gamma_p, \ \forall p, \quad \text{para algún } \sigma_p \in \mathscr{U}(V_p).$$

Lo que es lo mismo que $\theta(\Lambda_p, \Gamma_p) \in \mathbb{Z}_p^\times \theta(\Lambda_p)$. Asumamos que la dimensión de V es mayor o igual a 2, por el Lema 2.1.16 sabemos que $\mathbb{Z}_p^\times = \theta(V_p)$ para casi todo p, por lo que la definición de Θ-género y $\mathscr{U}$-género difieren solo en una cantidad finita de primos.

Para que sea útil la definición de $\mathscr{U}$-género junto con la de Θ-clase, necesitamos:

Proposición 2.2.2. *Hay una cantidad finita de Θ-clases en un $\mathscr{U}$-género dado.*

Demostración. Sabemos que cada género contiene una cantidad finita de clases. Por lo tanto alcanza con probar que cada clase contiene una cantidad finita de Θ-clases en un $\mathscr{U}$-género dado.

Sea Λ un $\mathbb{Z}$-retículo de dimensión al menos 2, ya que el caso de dimensión 1 es trivial. Consideramos S un conjunto finito de primos que cumple

$$\theta(\Lambda_p) \subset \mathbb{Z}_p^\times (\mathbb{Q}_p^\times)^2 \quad p \notin S,$$

que sabemos que existe en virtud del Lema 2.1.16, tomando S el conjunto de primos donde Λ_p no es unimodular, que es finito. Sea $\Gamma \sim \Lambda$, o sea Γ está en la misma clase que Λ. Sea $\theta(\Lambda, \Gamma) = s\theta(\Lambda)$, con $s \in \mathbb{Z}$ libre de cuadrados. Para que Λ y Γ estén en el mismo $\mathscr{U}$-género se tiene que cumplir

$$\theta(\Lambda_p, \Gamma_p) = s\theta(\Lambda_p) \in \mathbb{Z}_p^\times \theta(\Lambda_p) \ .$$

Pero si $p \notin S$ sabemos que $\theta(\Lambda_p) \subset \mathbb{Z}_p^\times (\mathbb{Q}_p^\times)^2$ y $s \in \mathbb{Z}_p^\times$ para $p \notin S$ y $[\Gamma] = [\Lambda]^s$ para una cantidad finita de elecciones de s. □

Observación 2.2.3. Cuando Λ es integral, el conjunto S consiste de los primos que dividen a $\operatorname{disc}\Lambda$, y las Θ-clases propiamente equivalentes a Λ en el $\mathscr{U}$-género de Λ están dadas por

$$[\Lambda]^s, \quad s | \operatorname{disc}\Lambda,$$

con $[\Lambda]^s = [\Lambda]^{s'}$ si y solo si $ss' \in \theta(\Lambda)$.

Proposición 2.2.4. *Sea Λ un $\mathbb{Z}$-retículo en V de dimensión al menos 3. La clausura del $\mathscr{U}$-género de Λ por la acción de $O^+(V)$ es el género de Λ.*

Demostración. Sea Γ retículo en el género de Λ. Vamos a encontrar un retículo en el $\mathscr{U}$-género de Λ que es propiamente equivalente a Γ. Si consideramos la matriz que cambia una base de Λ en una base de Γ, es una matriz con coeficientes en $\mathbb{Q}$ e invertible. Por lo que es una matriz invertible sobre $\mathbb{Z}_p$ para casi todo p. Se deduce entonces que

$$\Lambda_p = \Gamma_p \quad \text{para casi todo } p \ .$$

En particular $\theta(\Lambda_p, \Gamma_p) = 1$ para casi todo p, y existe $x \in \mathbb{Q}_{>0}$ tal que

$$x \in \mathbb{Z}_p^\times \theta(\Lambda_p, \Gamma_p) \quad \forall p \ .$$

Por la Proposición 2.1.14, existe $\sigma \in O^+(V)$ tal que $\theta(\sigma) = x$. Vemos entonces que $\sigma\Gamma$ está en el $\mathscr{U}$-género de Λ. □

2.2.3. Ejemplos

Ejemplo 2.2.1. Retomando el Ejemplo 1.3.1, calculamos las Θ-clases en el $\mathscr{U}$-género de Λ_1. Como en la Proposición 2.2.4, vemos que $[\Lambda_1]$ y $[\Lambda_2]^2$. Sabemos entonces que el $\mathscr{U}$-género estará formado por las

$$[\Lambda_1],\ [\Lambda_1]^{11},\ [\Lambda_2]^2,\ [\Lambda_2]^{2\cdot 11}$$

pero ambos retículos tienen automorfismos no triviales con norma spin 11. El de Λ_1 es $\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ y el de Λ_2 es $\begin{pmatrix} -1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & -1 \end{pmatrix}$.

Concluimos que el $\mathscr{U}$-género de Λ_1 está formado solo por dos Θ-clases, como el género de Λ_1.

Ejemplo 2.2.2. Veamos en el Ejemplo 1.3.2 las Θ-clases del $\mathscr{U}$-género de Λ_1. Como antes, estarán entre

$$[\Lambda_1], [\Lambda_1]^7, [\Lambda_2]^2, [\Lambda_2]^{2\cdot 7}, [\Lambda_3]^3, [\Lambda_3]^{3\cdot 7} \ .$$

Los retículos Λ_1 y Λ_2 tienen automorfismos no triviales de norma spin 11, pero Λ_3 no. Concluimos que hay 4 Θ-clases en el $\mathscr{U}$-género de Λ_1, cuando su género tiene 3 clases de equivalencia propia.

Ejemplo 2.2.3. Sea $V = \mathbb{Q}^3$, $\phi(x, y, z) = x^2 + 14y^2 + 3025z^2 - xy$ y $\Lambda = \mathbb{Z}^3$ con discriminante $4125 = 5^3 11^3$. El género de Λ tiene 32 clases de retículos. De éstos, 8 tienen todos sus automorfismos con norma spin 1, 16 con automorfismos con normas spin 5 o 11 y 8 con normas spin 1, 5, 11 y 55. Concluimos que hay 72 Θ-clases en el $\mathscr{U}$-género de Λ.

Ejemplo 2.2.4. Por último, si $V = \mathbb{Q}^3$,

$$\phi(x, y, z) = x^2 + 330y^2 + 28181299z^2 - 165yz - xz$$

y $\Lambda = \mathbb{Z}^3$ con discriminante

$$37199287125 = 3^3 5^3 7^2 11^3 13^2 \ .$$

El género de Λ tiene 49191 clases de retículos y su $\mathscr{U}$-género 1572480 Θ-clases.

Esto fue calculado usando el paquete de formas cuadráticas ternarias de Sage.

2.3. Módulo de Brandt

2.3.1. Operadores de Hecke

Sabemos que si Λ y Γ son dos retículos p-vecinos, entonces $\Lambda_q = \Gamma_q$ para todo primo $q \neq p$. Para la localización en p tenemos

Proposición 2.3.1. *Si Λ y Γ son retículos p-vecinos entonces $\Lambda_p \sim \Gamma_p$ y $\theta(\Lambda_p, \Gamma_p) = p$, con $\theta(\Lambda_p) \supset \mathbb{Z}_p^\times$.*

Demostración. Como Λ y Γ son p-vecinos, existen vectores $\mathbf{v} \in \Lambda$ y $\mathbf{w} \in \Gamma$ tales que $\phi(\mathbf{v}, \mathbf{w}) \notin \mathbb{Z}$. Sea $\Lambda^0 = \Lambda \cap \Gamma$, por lo que $\Lambda = \Lambda^0 + \mathbb{Z}\mathbf{v}$ y $\Gamma = \Lambda^0 + \mathbb{Z}\mathbf{w}$. Localizando,

$$\Lambda_p = \Lambda_p^0 + \mathbb{Z}_p\mathbf{v}, \qquad \Gamma_p = \Lambda_p^0 + \mathbb{Z}_p\mathbf{w}, \qquad p\phi(\mathbf{v}, \mathbf{w}) \in \mathbb{Z}_p^\times \ .$$

Como $p\mathbf{w} \in \Lambda_p^0$, estas relaciones no cambian si reemplazamos $\mathbf{v}$ por $\mathbf{v} + xp\mathbf{w}$ para $x \in \mathbb{Z}_p$, y de la misma manera si $\mathbf{w}$ es cambiado por $\mathbf{w} + yp\mathbf{v}$ con $y \in \mathbb{Z}_p$. Vemos ahora que

$$\phi(\mathbf{v} + xp\mathbf{w}) = \phi(\mathbf{v}) + xp\phi(\mathbf{v}, \mathbf{w}) + x^2p^2\phi(\mathbf{w})$$

puede tomar cualquier valor módulo p^2, ya que $p\phi(\mathbf{v}, \mathbf{w}) \in \mathbb{Z}_p^\times$. Por lo que puede tomar cualquier valor en $\mathbb{Z}_p$ por el lema de Hensel, y lo mismo para $\phi(\mathbf{w} + yp\mathbf{v})$. Podemos asumir entonces que $\phi(\mathbf{v}) = \phi(\mathbf{w}) \in \mathbb{Z}_p^\times$.

Afirmamos que

$$\tau_{\mathbf{v}-\mathbf{w}}\Lambda_p = \Gamma_p \ .$$

Si $\mathbf{u} \in \Lambda_p^0$, entonces $\phi(\mathbf{u}, \mathbf{v} - \mathbf{w}) \in \mathbb{Z}_p$ y

$$\frac{\phi(\mathbf{u}, \mathbf{v} - \mathbf{w})}{\phi(\mathbf{v} - \mathbf{w})} \in p\mathbb{Z}_p,$$

ya que $\phi(\mathbf{v} - \mathbf{w}) = \phi(\mathbf{v}) + \phi(\mathbf{w}) - \phi(\mathbf{v}, \mathbf{w}) \notin \mathbb{Z}_p$. Concluimos que

$$\tau_{\mathbf{v}-\mathbf{w}}\mathbf{u} = \mathbf{u} - \frac{\phi(\mathbf{u}, \mathbf{v} - \mathbf{w})}{\phi(\mathbf{v} - \mathbf{w})}(\mathbf{v} - \mathbf{w}) \in \Lambda_p^0,$$

ya que $p(\mathbf{v}-\mathbf{w}) \in \Lambda_p^0$. Probamos $\tau_{\mathbf{v}-\mathbf{w}}\Lambda_p^0 = \Lambda_p^0$, y como $\tau_{\mathbf{v}-\mathbf{w}}\mathbf{v} = \mathbf{w}$ se ve que $\tau_{\mathbf{v}-\mathbf{w}}\Lambda_p = \Gamma_p$.

Para terminar la prueba de la primera parte, notamos que $\phi(\mathbf{v}) \in \mathbb{Z}_p^\times$ y $\tau_{\mathbf{v}} \in O(\Lambda_p)$, y además

$$\sigma_p = \tau_{\mathbf{v}-\mathbf{w}}\tau_{\mathbf{v}} \in O^+(V_p)$$

es una equivalencia propia entre Λ_p y Γ_p, con

$$\theta(\sigma_p) = \phi(\mathbf{v}-\mathbf{w})\phi(\mathbf{v}) \in p\mathbb{Z}_p^\times(\mathbb{Q}_p^\times)^2 \ .$$

Finalmente, como vimos $\mathbf{u} = \mathbf{v} + zp\mathbf{w} \in \Lambda$, para $z \in \mathbb{Z}_p$, $\phi(\mathbf{u})$ alcanza cualquier valor de $\mathbb{Z}_p$, entonces si $\tau_{\mathbf{v}}\tau_{\mathbf{u}} \in O^+(\Lambda_p)$ $\theta(\tau_{\mathbf{v}}\tau_{\mathbf{u}})$ alcanza cualquier valor de $\mathbb{Z}_p^\times$. □

Denotamos $\Gamma^{(p)}$ un retículo tal que $\left[\Gamma^{(p)}\right] = [\Gamma]^p$, o sea $\Gamma^{(p)} = \sigma\Gamma$ para algún $\sigma \in O^+(V)$ con $\theta(\sigma) = p$. Cuando la dimensión de V es al menos 3, existe un retículo como antes por la Proposición 2.1.14, pero está definido salvo Θ-equivalencia.

Proposición 2.3.2. *Si Λ y Γ son p-vecinos, entonces están en el mismo género. Además, Λ y $\Gamma^{(p)}$ están en el mismo $\mathscr{U}$-género.*

Demostración. La primera parte de la proposición es consecuencia directa de la Proposición 2.3.1. Para la segunda parte vemos que

$$\theta\left(\Lambda_q, \Gamma_q^{(p)}\right) = p\theta(\Lambda_q, \Gamma_q) \in \mathbb{Z}_q^\times\theta(\Lambda_q)$$

trivialmente para $q \neq p$ y por la Proposición 2.3.1 para $q = p$. □

Definición 2.3.1. Sea $\mathcal{M}(\Lambda)$ el $\mathbb{Z}$-módulo libre con base las Θ-clases en el $\mathscr{U}$-género de Λ. Cuando Λ es un retículo definido de dimensión 3, llamamos a $\mathcal{M}(\Lambda)$ el módulo de Brandt del retículo cuadrático ternario Λ.

Los operadores de Hecke

$$t_p : \mathcal{M}(\Lambda) \to \mathcal{M}(\Lambda),$$

son operadores lineales definidos en la base de la siguiente manera

$$t_p[\Gamma] = \sum_i [\Gamma_i]^p,$$

donde la suma es sobre todos los p-vecinos de Γ.

Claramente $\mathcal{M}(\Lambda)$ depende solo del $\mathscr{U}$-género de Λ, y por otro lado si $\sigma \in O^+(V)$, tenemos un isomorfismo

$$\mathcal{M}(\Lambda) \to \mathcal{M}(\sigma\Lambda)$$

dado por $[\Gamma] \mapsto [\Gamma]^{\theta(\sigma)}$, que preserva la acción de los operadores de Hecke. Se ve entonces, gracias a la Proposición 2.2.4, que $\mathcal{M}(\Lambda)$ depende solo, salvo isomorfismos Hecke-lineales, del género de Λ.

Asumimos que $(V,\ \phi)$ es un espacio cuadrático definido. Esto implica que $O(\Gamma)$ es finito para cualquier retículo de V. Definimos un producto interno en $\mathcal{M}_{\mathbb{R}}(\Lambda) = \mathcal{M}(\Lambda) \otimes \mathbb{R}$ por

$$\left\langle [\Gamma], [\Gamma'] \right\rangle = \#\left\{\sigma \in \Theta(V) : \sigma\Gamma = \Gamma'\right\} = \begin{cases} \#\Theta(\Gamma) & \text{si } [\Gamma] = [\Gamma'] \\ 0 & \text{en otro caso.} \end{cases}$$

Proposición 2.3.3. *Los operadores de Hecke t_p generan un álgebra conmutativa de operadores autoadjuntos. Por lo tanto $\mathcal{M}_{\mathbb{R}}(\Lambda)$ tiene una base ortogonal simultánea para todos los operadores t_p.*

Demostración. Es claro que t_p y t_q conmutan para $p \neq q$. Para probar que t_p es autoadjunta, vemos que

$$\begin{aligned} \left\langle t_p[\Gamma], [\Gamma'] \right\rangle = & \\ &= \#\left\{\sigma \in O^+(V) : \theta(\sigma) = p,\ \sigma\Gamma' \text{ } p\text{-vecino de } \Gamma\right\} \\ &= \#\left\{\sigma \in O^+(V) : \theta(\sigma) = p,\ \Gamma' \text{ } p\text{-vecino de } \sigma^{-1}\Gamma\right\} \\ &= \left\langle [\Gamma], t_p[\Gamma'] \right\rangle. \end{aligned}$$

ya que $\theta(\sigma^{-1}) = \theta(\sigma)$. Lo último se deduce del teorema espectral. □

2.3.2. Proyecciones

Definición 2.3.2. Sea Γ un $\mathbb{Z}$-retículo, y l un primo impar que no divide a $\operatorname{disc}(\Lambda)$ o $l = 1$. Decimos que Γ es l-ambiguo si existe $t \in \theta(\Gamma)$ tal que $\left(\frac{t}{l}\right) = -1$.

Definimos $\widetilde{\mathcal{M}}_l(\Lambda)$ como el $\mathbb{Z}$-módulo libre con base las clases de equivalencia propia de $\mathbb{Z}$-retículos en el género de Λ que no son l-ambiguos. Observamos que $\widetilde{\mathcal{M}}_1(\Lambda) = \widetilde{\mathcal{M}}(\Lambda)$.

Definición 2.3.3. Si Λ $\mathbb{Z}$-retículo unimodular, definimos el grupo de divisores de Λ como

$$D(\Lambda) = \left\{s(\mathbb{Q}^\times)^2 : s | \operatorname{disc}(\Lambda),\ s \geq 0\right\}.$$

Por lo visto en la Observación 2.2.3, $D(\Lambda)$ actúa en $\mathcal{M}(\Lambda)$ y además conmuta con los operadores de Hecke.

Consideramos el grupo $\widehat{D(\Lambda)}$ de caracteres de $D(\Lambda)$. Como los elementos de $D(\Lambda)$ tienen orden 1 o 2, la imagen de cualquier carácter está en $\{-1, 1\}$. Si l primo impar, $\chi_l = \left(\frac{\cdot}{l}\right)$ define un carácter en $D(\Lambda)$. Siendo $\left(\frac{\cdot}{l}\right)$ el carácter de Legendre. Definimos $\chi_1(s) = 1$, para $s \in D(\Lambda)$. Por el teorema de progresiones aritméticas de Dirichlet y el teorema chino de los restos, vemos que, variando l, obtenemos todos los caracteres de $D(\Lambda)$.

Sean $\Gamma_1, \Gamma_2, \ldots, \Gamma_h$ representantes de las clases de equivalencia propia en el $\mathscr{U}$-género de Λ. Tenemos la siguiente proyección lineal $\pi_l : \mathcal{M}(\Lambda) \to \widetilde{\mathcal{M}}_l(\Lambda)$

$$\pi_l\left([\Gamma_i]^s\right) = \begin{cases} 0 & \text{si } \Gamma_i \text{ es } l\text{-ambiguo} \\ \chi_l(s)\overline{\Gamma_i} & \text{en otro caso,} \end{cases}$$

donde $s \in D(\Lambda)$.

Como antes, definimos operadores de Hecke en estos espacios, los definimos de la siguiente manera

$$\tilde{t}_{p,l}\left(\overline{\Gamma_i}\right) = \pi_l(t_p[\Gamma_i]) \ .$$

Es fácil de ver que $\widetilde{\mathcal{M}}_{l\mathbb{R}}(\Lambda) = \widetilde{\mathcal{M}}_l(\Lambda) \otimes \mathbb{R}$ junto con los operadores de Hecke generan un álgebra conmutativa de operadores autoadjuntos y por lo tanto $\widetilde{\mathcal{M}}_{l\mathbb{R}}(\Lambda)$ tiene una base ortogonal simultánea a todos los $\tilde{t}_{p,l}$. Además los mapas π_l respetan la estructura de Hecke-módulos de $\mathcal{M}(\Lambda)$ y $\widetilde{\mathcal{M}}_l(\Lambda)$ por definición.

Observación 2.3.4. Si Γ retículo en el $\mathscr{U}$-género de Λ. Las Θ-clases propiamente equivalentes a Γ en el $\mathscr{U}$-género de Λ son

$$[\Gamma]^s, \ s \in D(\Lambda)/\theta(\Gamma)$$

que son exáctamente $|D(\Lambda)|/|\theta(\Gamma)|$.

Concluimos que

$$\begin{aligned} \dim \mathcal{M}(\Lambda) &= \sum_i |D(\Lambda)|/|\theta(\Gamma_i)| \\ &= |D(\Lambda)| \sum_i 1/|\theta(\Gamma_i)|. \end{aligned}$$

Por otro lado, $\chi_l \in \widehat{D(\Lambda)/\theta}(\Gamma) < \widehat{D(\Lambda)}$ si y solo si Γ no es l-ambiguo, por lo que hay $|D(\Lambda)|/|\theta(\Gamma)|$ elementos de $D(\Lambda)$ que corresponden a primos l para los cuales Γ no es l-ambiguo.

Proposición 2.3.5. *Si χ_{l_i}, con $i = 1, 2, \ldots, r$, forman una base de $\widehat{D}(\Lambda)$, se cumple*

$$\mathcal{M}(\Lambda) \cong \widetilde{\mathcal{M}}_{l_1}(\Lambda) \oplus \widetilde{\mathcal{M}}_{l_2}(\Lambda) \oplus \cdots \oplus \widetilde{\mathcal{M}}_{l_r}(\Lambda)$$

mediante el mapa $\pi = \pi_{l_1} \oplus \pi_{l_2} \oplus \cdots \oplus \pi_{l_r}$

Demostración. Primero probaremos que el mapa π es inyectivo. Si

$$\pi\left(\sum_j \sum_{s \in D(\Lambda)/\theta(\Gamma_j)} \alpha_s [\Gamma_j]^s\right) = 0$$

se cumple

$$\sum_{s\in D(\Lambda)/\theta(\Gamma_j)} \alpha_s \chi_{l_i}(s) = 0$$

cuando Γ_j no es l_i ambiguo. Como son exactamente $|D(\Lambda)|/|\theta(\Gamma)|$ caracteres y la misma cantidad de s, tiene que ser $\alpha_s = 0$ para $s \in D(\Lambda)/\theta(\Gamma_j)$.

Calculemos la dimension del codominio de π.

$$\begin{aligned}
\dim \bigoplus_i \widetilde{\mathcal{M}}_{l_i}(\Lambda) &= \sum_i \dim \widetilde{\mathcal{M}}_{l_i}(\Lambda) \\
&= \sum_j \#\{\chi_l \in D(\Lambda) : \Gamma_j \text{ no es } l\text{-ambiguo}\} \\
&= \sum_j |D(\Lambda)|/|\theta(\Gamma_j)| \\
&= \dim \mathcal{M}(\Lambda) \ .
\end{aligned}$$

La segunda igualdad es clara y la tercera es lo discutido en la Observación 2.3.4.

Concluimos que el mapa es inyectivo entre espacios de igual dimensión por lo que tiene que ser biyectivo. □

2.3.3. Ejemplos

Ejemplo 2.3.1. Por lo visto en los ejemplos 1.3.1 y 2.2.1 concluimos que $\mathcal{M}(\Lambda_1) \cong \widetilde{\mathcal{M}}(\Lambda_1)$ como Hecke módulos, por lo que no hay información nueva en el enfoque del $\mathscr{U}$-género.

Ejemplo 2.3.2. Sea $V = \mathbb{Q}^3$, $\phi(x, y, z) = x^2 + 2y^2 + 5z^2 - yz - xz$. En el género de $\Lambda_1 = \mathbb{Z}^3$, hay solo uno mas, Λ_2. El $\mathscr{U}$-género de Λ_1 contiene 3 Θ-clases

$$[\Lambda_1],\ [\Lambda_2],\ [\Lambda_2]^{37}$$

Calculamos $\tilde{t}_p$ para algunos primos:

$$\tilde{t}_2 = \begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix},\ \tilde{t}_3 = \begin{pmatrix} 2 & 1 \\ 2 & 3 \end{pmatrix},\ \tilde{t}_5 = \begin{pmatrix} 2 & 2 \\ 4 & 4 \end{pmatrix}$$

$$\tilde{t}_7 = \begin{pmatrix} 2 & 3 \\ 6 & 5 \end{pmatrix},\ \tilde{t}_{11} = \begin{pmatrix} 6 & 3 \\ 6 & 9 \end{pmatrix},\ \tilde{t}_{13} = \begin{pmatrix} 2 & 6 \\ 12 & 8 \end{pmatrix},\ \tilde{t}_{17} = \begin{pmatrix} 10 & 4 \\ 8 & 14 \end{pmatrix}, \cdots$$

Tiene vectores propios $\tilde{\mathbf{E}}_1 = (1, 2)$ con valores propios

$$3, 4, 6, 8, 12, 14, 18, \ldots,$$

y $\tilde{\mathbf{E}}_2 = (1, -1)$ con valores propios

$$0, 1, 0, -1, 3, -4, 6, \ldots$$

El vector $\tilde{\mathbf{E}}_1$ está asociado a una forma de Eisenstein de peso 2 y nivel 37. El vector $\tilde{\mathbf{E}}_2$ está asociado a la curva elíptica `37b`.

Calculemos ahora t_p:

$$t_2 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 2 \\ 1 & 2 & 0 \end{pmatrix},\ t_3 = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 0 & 3 \\ 1 & 3 & 0 \end{pmatrix},\ t_5 = \begin{pmatrix} 2 & 2 & 2 \\ 2 & 1 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$t_7 = \begin{pmatrix} 2 & 3 & 3 \\ 3 & 2 & 3 \\ 3 & 3 & 2 \end{pmatrix},\ t_{11} = \begin{pmatrix} 6 & 3 & 3 \\ 3 & 2 & 7 \\ 3 & 7 & 2 \end{pmatrix},\ t_{13} = \begin{pmatrix} 2 & 6 & 6 \\ 6 & 3 & 5 \\ 6 & 5 & 3 \end{pmatrix}$$

$$t_{17} = \begin{pmatrix} 10 & 4 & 4 \\ 4 & 7 & 7 \\ 4 & 7 & 7 \end{pmatrix}, \cdots$$

En este caso tenemos 3 vectores propios racionales, que son $\mathbf{E}_1 = (1,1,1)$, $\mathbf{E}_2 = (2,-1,-1)$ y $\mathbf{E}_3 = (0,1,-1)$. Los vectores $\mathbf{E}_1$ y $\mathbf{E}_2$ tienen los mismos valores propios que $\tilde{\mathbf{E}}_1$ y $\tilde{\mathbf{E}}_2$.

El vector $\mathbf{E}_3$ tiene valores propios

$$-2, -3, -2, -1, -5, -2, 0, \ldots,$$

y está asociado a la curva elíptica `37a`, que tiene signo $-$ en su ecuación funcional.

Ejemplo 2.3.3. Revisitemos el Ejemplo 1.3.2, sabemos que tenemos 4 Θ-clases en el $\mathscr{U}$-género de Λ_1 por 2.2.2. Calculando, obtenemos

$$t_2 = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 1 & 2 \end{pmatrix},\ t_3 = \begin{pmatrix} 0 & 0 & 2 & 2 \\ 0 & 0 & 2 & 2 \\ 2 & 2 & 0 & 0 \\ 2 & 2 & 0 & 0 \end{pmatrix},\ t_5 = \begin{pmatrix} 0 & 0 & 3 & 3 \\ 0 & 0 & 3 & 3 \\ 3 & 3 & 0 & 0 \\ 3 & 3 & 0 & 0 \end{pmatrix}$$

$$t_{11} = \begin{pmatrix} 8 & 4 & 0 & 0 \\ 4 & 8 & 0 & 0 \\ 0 & 0 & 8 & 4 \\ 0 & 0 & 4 & 8 \end{pmatrix},\ t_{13} = \begin{pmatrix} 0 & 0 & 7 & 7 \\ 0 & 0 & 7 & 7 \\ 7 & 7 & 0 & 0 \\ 7 & 7 & 0 & 0 \end{pmatrix},\ t_{17} = \begin{pmatrix} 0 & 0 & 9 & 9 \\ 0 & 0 & 9 & 9 \\ 9 & 9 & 0 & 0 \\ 9 & 9 & 0 & 0 \end{pmatrix}, \cdots$$

Con vectores propios racionales y valores propios

$$\begin{aligned} &\mathbf{E}_1 = (1,-1,0,0),\ 1,0,0,4,0,0,\ldots, \\ &\mathbf{E}_2 = (0,0,1,-1),\ 1,0,0,4,0,0,\ldots, \\ &\mathbf{E}_3 = (1,1,1,1),\ 3,4,6,12,14,18,\ldots, \\ &\mathbf{E}_4 = (1,1,-1,-1),\ 3,-4,-6,12,-14,-18,\ldots \end{aligned}$$

Como en el Ejemplo 1.3.2, los vectores $\mathbf{E}_1$ y $\mathbf{E}_2$ están asociados a la curva elíptica `49a` y los vectores $\mathbf{E}_3$ y $\mathbf{E}_4$ están asociados a series de Eisenstein de peso 2 y nivel 49 y carácter cuadrático $\left(\frac{\cdot}{7}\right)$. En este caso tampoco obtuvimos información nueva, aunque el espacio tenga mayor dimensión.

Ejemplo 2.3.4. Veamos el caso $V = \mathbb{Q}^3$, $\phi(x, y, z) = x^2 + y^2 + 11z^2 - xz$. El género de $\Lambda = \mathbb{Z}^3$, de discriminante 43, esta formado por 3 clases de las cuales 2 tienen automorfismos de norma spin 43. El $\mathscr{U}$-género de Λ estará formado entonces por 4 Θ-clases.

El grupo $D(\Lambda) = \{1, 43\}$ tiene grupo de caracteres $\widehat{D(\Lambda)} = \{\chi_1, \chi_5\}$ por lo que

$$\mathcal{M}(\Lambda) \cong \widetilde{\mathcal{M}}_1(\Lambda) \oplus \widetilde{\mathcal{M}}_5(\Lambda),$$

donde la dimensión de $\widetilde{\mathcal{M}}_1(\Lambda)$ es 3 y la dimensión de $\widetilde{\mathcal{M}}_5(\Lambda)$ es 1.

A continuación presentamos los operadores de Hecke en la descomposición

$$t_2 = \begin{pmatrix} 1 & 1 & 0 \\ 2 & 0 & 1 \\ 0 & 2 & 2 \end{pmatrix} \oplus \begin{pmatrix} -2 \end{pmatrix}, \; t_3 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 2 & 1 \\ 4 & 2 & 2 \end{pmatrix} \oplus \begin{pmatrix} -2 \end{pmatrix},$$

$$t_5 = \begin{pmatrix} 2 & 0 & 1 \\ 0 & 4 & 1 \\ 4 & 2 & 4 \end{pmatrix} \oplus \begin{pmatrix} -4 \end{pmatrix}, \; t_7 = \begin{pmatrix} 0 & 2 & 1 \\ 4 & 0 & 3 \\ 4 & 6 & 4 \end{pmatrix} \oplus \begin{pmatrix} 0 \end{pmatrix},$$

$$t_{11} = \begin{pmatrix} 2 & 3 & 1 \\ 6 & 1 & 4 \\ 4 & 8 & 7 \end{pmatrix} \oplus \begin{pmatrix} 3 \end{pmatrix}, \; t_{13} = \begin{pmatrix} 4 & 3 & 1 \\ 6 & 3 & 4 \\ 4 & 8 & 9 \end{pmatrix} \oplus \begin{pmatrix} -5 \end{pmatrix} \cdots$$

Si miramos la primera coordenada vemos que hay un solo vector propio racional, el mismo está asociado a una serie de Eisenstein de peso 2 y nivel 43. Por otro lado, la segunda coordenada tiene dimensión 1 y vector y valores propios obvios. El mismo está asociado a la curva elíptica `43a`, la cual tiene signo $-$ en su ecuación funcional.

Ejemplo 2.3.5. Sea $\phi(x, y, z) = x^2 + 3y^2 + 27z^2 - xy$ y $\Lambda = \mathbb{Z}^3$, con discriminante $3^3 11$. La dimensión de $\mathcal{M}(\Lambda)$ es 30. Los operadores de Hecke tienen 20 vectores propios racionales. Todas las curvas elípticas de conductor 99 estan asociados a alguno de estos vectores, una de las cuales tiene signo $-$ en su ecuacion funcional y las otras con signo $+$.

Ejemplo 2.3.6. Consideramos ahora $\phi(x, y, z) = x^2 + 2y^2 + 635z^2 - yz - xz$, donde el género de $\Lambda = \mathbb{Z}^3$ contiene 217 clases de equivalencia propias, mientras que su $\mathscr{U}$-género contiene 423 Θ-clases. Se descompone de la siguiente manera

$$\mathcal{M}(\Lambda) \cong \widetilde{\mathcal{M}}_1(\Lambda) \oplus \widetilde{\mathcal{M}}_5(\Lambda),$$

donde la dimensión de $\widetilde{\mathcal{M}}_5(\Lambda)$ es 206. Los operadores de Hecke tienen solo 2 vectores propios racionales $\mathbf{E}_1$ y $\mathbf{E}_2$. El primero está asociado a una seria de Eisenstein de peso 2 y nivel 5077. El segundo es vector propio de $\widetilde{\mathcal{M}}_5(\Lambda)$, con valores propios

$$-2, -3, -4, -4, -6, -4, -4, -7, \ldots,$$

y está asociado a la curva elíptica `5077a`, curva de rango 3 y signo $-$ en su ecuación funcional.

Capítulo 3

Algoritmos

En este capítulo presentamos algunos resultados y algoritmos usados para la construcción de los ejemplos de los capítulos anteriores.

Lo introducido aquí esta basado en el trabajo de Birch [1] y los trabajos de Conway y Sloane [3], [4].

3.1. La fórmula de la masa

3.1.1. Introducción

Dado un género de formas cuadráticas ternarias, existe un invariante del mismo llamado la masa. Dada cualquier forma cuadrática f del género, tenemos una constante asociada a ella $m(f)$, que definimos en la Subsección 3.1.3, llamada masa de la forma cuadrática. El interés de este invariante es el siguiente:

Teorema 3.1.1. *Dado un género $\mathcal{G}$ de formas cuadráticas definidas positivas se cumple:*

$$m(f) = \sum_i \frac{1}{|Aut(f_i)|},$$

donde $f \in \mathcal{G}$ es una forma cuadrática cualquiera en el género y f_i representantes de las clases integrales de $\mathcal{G}$.

3.1.2. Descomposición de Jordan

Para poder calcular la p-masa de una forma cuadrática necesitaremos su descomposición de Jordan, que detallamos en el siguiente teorema.

Teorema 3.1.2. *Si $p \neq 2$, una forma cuadrática integral puede ser diagonalizada por una transformación integral p-ádica. Para $p = 2$ hay una transformación p-ádica integral expresando la forma como una suma directa*

de formas con matrices

$$(qx),\ \begin{pmatrix} qa & qb \\ qb & qc \end{pmatrix},$$

donde q es una potencia de 2, a y c son divisibles por 2, pero x, b y $d = ac-b^2$ no.

Demostración. Si $p \neq 2$, buscamos la entrada en la matriz asociada a la forma que sea divisible por la menor potencia de p. Si la entrada es diagonal, digamos f_{11}, podemos entonces empezar la diagonalización substrayendo múltiplos de la primera fila al resto de las filas para obtener cero en el resto de la primer fila, seguido por las correspondientes operaciones de columnas para obtener ceros en la primera fila.

Por otro lado, si una entrada no diagonal es divisible por la menor potencia de p, digamos f_{12}, y todas las entradas diagonales son divisibles por una potencia mayor de p, podemos reducir al primer caso sumando la segunda fila a la primera y la segunda columna a la primer columna. Esto reemplaza f_{11} por $f_{11}+2f_{21}+f_{22}$, y dado que $p \neq 2$, es divisible por la potencia menor de p que ocurre en todas las entradas.

El mismo método funciona si $p = 2$ salvo si llegamos a un punto donde una entrada no diagonal, digamos f_{12} es divisible por la menor potencia posible $q = 2^k$, mientras que todas las entradas diagonales son divisibles por 2^{k+1}. En este caso la submatriz principal de tamaño 2, tiene la forma

$$\begin{pmatrix} qa & qb \\ qb & qc \end{pmatrix},$$

donde a y c son divisibles por 2 pero b no, por lo que $d = ac-b^2$ no es divisible por 2. Esto implica que todo par de enteros (x, y) es una combinación lineal 2-ádica integral de (a, b) y (b, c). Por lo que, como todas las entradas son divisibles por q, podemos restar múltiplos de las dos primeras filas, seguidos por las correspondientes operaciones de columnas, para tener ceros en el resto de las dos primeras filas y las dos primeras columnas. □

3.1.3. La fórmula

La masa de una forma f la calculamos en términos de la p-masa de f, $m_p(f)$, por la siguiente fórmula,

$$m(f) = 2\pi^{-\frac{1}{4}n(n+1)} \prod_{j=1}^{n} \Gamma\left(\frac{1}{2}j\right) \prod_{p} (2m_p(f)), \quad n \geq 2\ .$$

La p-masa es el recíproco del número de automorfismos de f módulo una potencia suficientemente grande de p, multiplicada por una potencia normalizadora de p.

3.1.4. Evaluación de la masa

La fórmula da la masa de una forma f como el producto sobre todos los primos, pero se puede ver como el producto de una cantidad finita de primos, en particular los primos que dividen a dos veces el discriminante de la forma. Para casi todos los primos la p-masa es igual a la p-masa estándar $\mathrm{std}_p(f)$, dada por

$$\mathrm{std}_p(f) = \frac{1}{2(1-p^{-2})(1-p^{-4})\cdots(1-p^{1-n})}$$

si n es impar. Si todas las p-masa tuviesen la masa estándar, entonces la masa total sería la masa estándar de f, $\mathrm{std}(f)$

$$\mathrm{std}(f) = 2\pi^{-n(n+1)/4}\left(\prod_{j=1}^{n}\Gamma(j/2)\right)\zeta(2)\cdots\zeta(n-1)$$

cuando n es impar. La masa de f esta dada por un producto finito de números racionales como

$$m(f) = \mathrm{std}(f)\prod_{p|2\,\mathrm{disc}(f)}\frac{m_p(f)}{\mathrm{std}_p(f)}\ .$$

3.1.5. Evaluación de la p-masa

Si f tiene descomposición de Jordan p-ádica

$$f = \sum qf_q,$$

donde q recorre todas las potencias de p y f_q tiene discriminante invertible en $\mathbb{Z}_p$ y dimensión $n(q)$, la p-masa está dada por

$$m_p(f) = \prod_q M_p(f_q)\times\prod_{q<q'}(q'/q)^{n(q)n(q')/2}\times 2^{n(I,I)-n(II)}.$$

El último factor es solo para $p = 2$. $n(II)$ es la suma de las dimensiones de las componentes de Jordan de tipo 2, y $n(I,I)$ es el numero de pares de componentes adyacentes f_q, f_{2q} de tipo 1.

El factor $M_p(f_q)$ es llamado el factor diagonal y es la potencia de p del orden de cierto grupo ortogonal sobre $\mathbb{F}_p$. Cuando $n(q) = 0$, su valor es 1.

Para p impar su valor es

$$\frac{1}{2(1-p^{-2})(1-p^{-4})\cdots(1-p^{1-n})}$$

cuando $n(q)$ es impar, o

$$\frac{1}{2(1-p^{-2})(1-p^{-4})\cdots(1-p^{2-n})(1-p^{-n/2})}$$

cuando $n(q)$ es par y $(-1)^{n(q)/2}\operatorname{disc}(f_q)$ es un residuo cuadrático, o

$$\frac{1}{2(1-p^{-2})(1-p^{-4})\cdots(1-p^{2-n})(1+p^{-n/2})}$$

cuando $n(q)$ es par y $(-1)^{n(q)/2}\operatorname{disc}(f_q)$ es un no residuo cuadrático.

Para $p=2$, el factor diagonal $M_p(f_q)$ es mas difícil de calcular, ya que no tenemos unicidad en la descomposición de Jordan como si tenemos en el caso impar, por lo que su cálculo depende de f_{2q} y $f_{q/2}$.

- Decimos que f_q es impar o de tipo 1 si representa un entero 2-ádico impar, y par en caso contrario, o de tipo 2.
- El valor octano de f_q es un entero módulo 8; si f_q es par su valor octano es 0 si su determinante es $+1$ o -1 módulo 8, y es 4 si su determinante es $+3$ o -3 módulo 8. Mientras que si f_q es impar puede ser diagonalizado y su valor octano es el número de entradas diagonales que son 1 módulo 4 menos el numero que son 4 módulo 4.
- Decimos que f_q es ligada si al menos una de f_{2q} y $f_{q/2}$ es impar, y decimos que es libre en otro caso.
- El entero t es definido para que la dimensión de f_q sea $2t$ si f_q es par, y $2t+1$ o $2t+2$ si f_q es impar.

Luego, el factor diagonal $M_p(f_q)$ es

$$\frac{1}{2(1-p^{-2})(1-p^{-4})\cdots(1-p^{-2t})}$$

cuando la forma es ligada o tiene valor octano $+2$ o -2 módulo 8, o

$$\frac{1}{2(1-p^{-2})(1-p^{-4})\cdots(1-p^{2-2t})(1-p^{-t})}$$

cuando la forma es libre y tiene valor octano -1, 0 o $+1$ módulo 8, o

$$\frac{1}{2(1-p^{-2})(1-p^{-4})\cdots(1-p^{2-2t})(1+p^{-t})}$$

cuando la forma es libre y tiene valor octano -3, $+3$ o 4 módulo 8.

3.1.6. Ejemplos

Ejemplo 3.1.1. Sea $f=\begin{pmatrix} 1 & 1 & 2 \\ -1 & -1 & 0 \end{pmatrix}$, con determinante 12, por lo que tenemos que hallar la p-masa para $p=2$ y 3.

Usando el algoritmo dado por el Teorema 3.1.2, vemos que f es equivalente sobre $\mathbb{Z}_2$ a una forma con matriz

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 84 \end{pmatrix}.$$

La descomposición de Jordan de f en $p = 2$ está dada por una forma de dimensión 2 par en $q = 2^0$, una de dimensión 1 en $q = 2^2$ impar y el resto de dimensión 0. Las formas en $q = 2^1, 2^3$ son ligadas y el resto libres, $n(II) = 2$, $n(I, I) = 0$, y

$$m_2(f) = 1 \cdot \frac{1}{2} \cdot \frac{1}{2} \times 2^2 \times 2^{-2} = \frac{1}{4}.$$

Sobre $\mathbb{Z}_3$, $f_{3^0}(x, y) = x^2 + 4y^2$, $f_{3^1}(x) = 384x^2$, y

$$m_3(f) = \frac{3}{16} \times 3 = \frac{9}{16}.$$

La masa estándar para $n = 3$ es $1/6$, con lo que podemos calcular la masa de f,

$$m(f) = \frac{1}{6} \times \frac{1/4}{2/3} \times \frac{9/16}{9/16} = \frac{1}{16}.$$

Para comparar, el género de f tiene solo una clase, dada por f con 16 automorfismos.

Ejemplo 3.1.2. Sea ahora $f = \begin{pmatrix} 53 & 59 & 61 \\ 0 & 0 & 0 \end{pmatrix}$. La descomposición de f en $p = 2$ nos da solo una forma de dimensión positiva que es además impar. En este caso $n(I, I) = n(II) = 0$. La forma en $q = 2^0$ tiene valor octano -1 y $M_2(f_{2^0}) = 1$,

$$m_2(f) = \frac{1}{2} \cdot 1\frac{1}{2} = \frac{1}{4}.$$

Es fácil de calcular el resto de las p-masas que nos dan $m_{53}(f) = 2809/216$, $m_{59}(f) = 3481/232$, $m_{61}(f) = 3721/240$ y $m(f) = 6045/4$.

Por otro lado, se puede calcular el género de f, que tiene 3076 clases. El género contiene 2971 clases con 2 automorfismos, 101 con 4 automorfismos y 4 con 4 automorfismos, obtenemos luego

$$\sum_i \frac{1}{|Aut(f_i)|} = \frac{2971}{2} + \frac{101}{4} + \frac{4}{8} = \frac{6045}{4}$$

que coincide con lo obtenido antes.

3.2. Formas cuadráticas vecinas

Si f y g son dos formas cuadráticas ternarias integrales definidas positivas, y p es un primo que no divide a $d(f)$ ni a $d(g)$, decimos que son p-vecinas si

$$f(px, y, z) = g(x, y, pz) \quad \forall x, y, z \in \mathbb{Q}.$$

También decimos que las clases de equivalencia de f y g son p-vecinas.

Esta definición está en concordancia con la definición de retículos p-vecinos. Definimos el espacio cuadrático $V = \mathbb{Q}^3$ y $\phi(x, y, z) = f(x, y, z)$, así como los retículos

$$\Lambda = \mathbb{Z}^3, \quad \Gamma = \{(px, y, z/p) \in V : x, y, z \in \mathbb{Z}\}$$

luego la clase de f corresponde al $\mathbb{Z}$-retículo Λ y la clase de g corresponde al $\mathbb{Z}$-retículo Γ. Vemos entonces que Λ y Γ son retículos p-vecinos. De la misma manera, todo par de clases de formas cuadráticas p-vecinas se pueden obtener de esta manera.

Para construir los módulos de los capítulos anteriores, usamos los algoritmos para formas cuadráticas al ser más sencillos de programar.

Veamos cómo construir todas las formas p-vecinas de una forma

$$f = \begin{pmatrix} a & b & c \\ r & s & t \end{pmatrix}$$

a partir de las soluciones proyectivas de f módulo p.

Si $\mathbf{P}$ es una solución proyectiva de $f(x, y, z) \equiv 0 \pmod{p}$. Consideramos un levantado de $\mathbf{P}$ con entradas enteras y primitivo. Podemos construir una transformación unimodular, que lleva $\mathbf{P}$ a $(1, 0, 0)$ y f a f'. Entonces el coeficiente a de f' es divisible por p, pero como p no divide a $d(f)$, no puede dividir al mismo tiempo a t y a s, por lo que cambiando de ser necesario las coordenadas y y z podemos asumir que p no divide a s. Mediante otra transformación unimodular, podemos forzar $p^2|a$ y $p|t$. La forma obtenida de esta manera f_1 tiene como p-vecino a $g(x, y, z) = f_1(x/p, y, pz)$.

Por lo discutido anteriormente y lo demostrado en el Capítulo 1, esto nos da todas las formas p-vecinas de f.

3.2.1. Soluciones proyectivas

Por lo visto en el Teorema 1.3.5, necesitamos calcular las soluciones proyectivas no singulares de

$$f(\mathbf{x}) \equiv 0 \pmod{p}, \tag{3.1}$$

donde f es una forma cuadrática ternaria integral, y p no divide a su discriminante. Lo anterior es lo mismo que decir que f sobre el cuerpo $\mathbb{F}_p$ es no singular.

Primero vemos el siguiente resultado.

Lema 3.2.1. *Todo espacio cuadrático* $(V,\ \phi)$ *no singular de dimensión 2 sobre* $\mathbb{F}_p$ *representa todo* $\mathbb{F}_p$*, si* $p \neq 2$*.*

Demostración. Por lo visto en el Lema 1.2.4, tenemos una base normal $\mathbf{u}_1$, $\mathbf{u}_2$,

$$\phi(\mathbf{u}_1) = a_1, \quad \phi(\mathbf{u}_2) = a_2, \quad \phi(\mathbf{u}_1, \mathbf{u}_2) = 0$$

con $a_i \neq 0$ por regularidad. Para $b \neq 0$ tenemos que ver que existen c_1, $c_2 \in \mathbb{F}_p$ tales que

$$a_1 c_1^2 + a_2 c_2^2 = b \ .$$

Que lo podemos escribir de la forma

$$a_1 c_1^2 = b - a_2 c_2^2 \ .$$

Si S y T son los conjuntos de valores tomados por los dos lados de la ecuación anterior, tenemos que cada uno tiene $(p+1)/2$ elementos y por lo tanto tienen intersección no vacía, y encontramos una representación para b. □

Esto en particular nos dice, cuando $p \neq 2$, que la Ecuación (3.1) tiene alguna solucion, digamos $\mathbf{P}_0$. El plano proyectivo $\mathbb{P}^2(\mathbb{F}_p)$ tiene $p+1$ rectas que pasan por $\mathbf{P}_0$ con $p+1$ puntos cada una. Como f es regular, cada una de las rectas cortan en un punto a f. Lo que nos da un algoritmo para calcular todas las soluciones de (3.1).

Algoritmo 3.2.1. Dada la Ecuación (3.1), procedemos de la siguiente manera:

1. Buscamos una solución particular $\mathbf{P}_0$ de manera probabilística, sorteando elementos en $\mathbb{F}_p$ y verificando (3.1).

2. Dado el punto $\mathbf{P}_0$ y otro particular $\mathbf{P}$, la recta que pasa por ellos dos es $\{\mathbf{P}_0 + \lambda\mathbf{P} : \lambda \in \mathbb{F}_p\} \cup \{\mathbf{P}\}$. La solución se calcula despejando λ, si $f(P) \not\equiv 0 \pmod{p}$. Haciendo esto para los puntos $\mathbf{P}$ que se obtienen todas las rectas que pasan por $\mathbf{P}_0$.

En la parte 1 del algoritmo anterior, se encuentra una solución con probabilidad aproximadamente igual a $1/p$. Vemos que la complejidad de la parte 2 del algoritmo es lineal en p.

Ejemplo 3.2.1. Sea $f(x, y, z) = x^2 + 3y^2 + 5z^2 - xz$ y $p = 7$. Una solución particular es $\mathbf{P}_0 = (3 : 1 : 1)$. Si $P = (2 : 1 : 0)$, $f(\mathbf{P}_0 + \lambda\mathbf{P}) = 6\lambda + 3\lambda^2$, por lo que $\lambda = 5$ y encontramos el punto $(3 : 6 : 1)$. De igual manera, encontramos que las soluciones proyectivas son

$$(3,1,1)\,, (3,6,1)\,, (5,6,1)\,, (6,0,1)\,, (2,0,1)\,, (5,1,0)\,, (2,1,0)\,, (5,1,1)\,.$$

3.2.2. Extensión de bases unimodulares

Para poder construir las formas p-vecinas de una forma dada, necesitamos extender un vector integral primitivo a una matriz unimodular. En general tenemos.

Teorema 3.2.2. *Sean $\mathbf{v}_1, \ldots, \mathbf{v}_J \in \mathbb{Z}^n$. Son equivalentes*

1. *Existen $\mathbf{v}_{J+1}, \ldots, \mathbf{v}_n \in \mathbb{Z}^n$ tal que $\mathbf{v}_1, \ldots, \mathbf{v}_n$ es una base de $\mathbb{Z}^n$ como $\mathbb{Z}$-módulo.*

2. *Los determinantes de las submatrices $J \times J$ de la matriz $n \times J$ $\mathbf{v}_1 \mathbf{v}_2 \ldots \mathbf{v}_J$ no tienen divisores en común mayor que 1.*

En particular, si tenemos un vector $\mathbf{v} = (a, b, c) \in \mathbb{Z}^3$ tal que $\mathrm{mcd}(a, b, c) = 1$, existe una matriz

$$M = \begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix}, \quad \det(M) = 1.$$

Veamos como la construimos. Tenemos

$$ax + by = g = \mathrm{mcd}(a, b)$$

usando el algoritmo extendido de Euclides. También

$$x\alpha + y\beta = 1$$

y

$$g\gamma + c\delta = 1$$

ya que x, y y g, c son coprimos. Entonces

$$M = \begin{pmatrix} a & b & c \\ -x & y & 0 \\ -\beta\delta & -\alpha\delta & \gamma \end{pmatrix}.$$

3.3. Operadores de Hecke

Sea f una forma cuadrática ternaria $\mathbb{Z}$-integral definida positiva. Como antes, podemos definir el retículo $\Lambda = \mathbb{Z}^3$ en el espacio cuadrático $(\mathbb{Q}^3,\ f)$. Definimos entonces el módulo de Brandt ternario asociado a f como $\mathcal{M}(f) = \mathcal{M}(\Lambda)$. Los operadores de Hecke se definen de igual manera en $\mathcal{M}(f)$.

Sean $\Lambda = \Gamma_1, \Gamma_2, \ldots, \Gamma_h$, $\mathbb{Z}$-retículos representantes del género de Λ en el $\mathscr{U}$-género de Λ, con matrices M_i de cambio de base de Λ en Γ_i y formas reducidas f_i asociadas a las retículos Γ_i. El $\mathscr{U}$-género de Λ esta formado por las siguientes Θ-clases

$$[\Gamma_i]^s,\ i = 1, 2, \ldots, h,\ s \in D(\Lambda)/\theta(\Gamma_i).$$

Si $g_i = \#D(\Lambda)/\theta(\Gamma_i)$ y $g = g_1 + g_2 + \cdots + g_h$. La matriz H_p asociada a t_p será $g \times g$.

A continuación describimos un algoritmo para calcular el módulo de Brandt de f.

Algoritmo 3.3.1. Dada una forma cuadrática ternaria integral definida positiva E-reducida f y un primo p tal que $p \nmid \text{disc}(f)$ calculamos H_p.

1. Inicializamos H_p, matriz $g \times g$ de ceros.

2. Para $i = 1, 2, \ldots, h$, calculamos $f_{i0}, f_{i2}, \ldots, f_{ip}$ formas reducidas representantes de las clases p-vecinas de f_i junto a las matrices M_{ij} que llevan f_i en f_{ij}. Si $f_{ij} = f_k$, calculamos la norma spin s del automorfismo de f_k, $M_k^{-1} M_i M_{ij}$. Luego se aumenta en 1 la entrada correspondiente a $[\Gamma_i]$, $[\Gamma_k]^s$ en H_p.

3. Para cada $s \in D(\Lambda)$, $s \neq 1$, $i = 1, 2, \ldots, h$, $j = 1, 2, \ldots, h$ y t en $D(\Lambda)/\theta(\Gamma_j)$ se aumenta en 1 la entrada correspondiente a $[\Gamma_i]^{s \pmod{\theta(\Gamma_i)}}$, $[\Gamma_j]^{st \pmod{\theta(\Gamma_j)}}$

En el algoritmo anterior, necesitamos tener calculadas todas las clases del género de f. Esto no es realmente necesario ya que el género es transitivo bajo la acción de todos los t_p, esto se puede ver en [2], capítulo 11, sección 4. Podriamos aplicar t_p hasta encontrar un subgrafo conexo maximal de t_p, calculamos la masa parcial de estas formas y las comparamos con la masa del género. Si no obtenemos todo el género, aplicamos vecinos con otros primos hasta encontrar otra forma y poder continuar. Aplicamos esto hasta encontrar todo el género de f.

Observamos que en el algoritmo anterior el tercer paso se puede omitir. Es mas, podemos modificarlo para obtener la descomposición dada por la Proposición 2.3.5. Presentamos la modificación en el siguiente algoritmo.

Algoritmo 3.3.2. Dada una forma cuadrática ternaria integral definida positiva E-reducida f y un primo p tal que $p \nmid \text{disc}(f)$ calculamos H_p como descomposición dada por la Proposición 2.3.5, conociendo los primos $l_1, l_2, \ldots, l_r$ de la misma. O sea

$$H_p = H_{p,l_1} \oplus H_{p,l_2} \oplus \cdots \oplus H_{p,l_r}$$

1. Aplicamos los dos primeros dos pasos del Algoritmo 3.3.1 y obtenemos una matriz $\tilde{H}_p$ de tamaño $h \times g$.

2. Para cada l_i, con $i = 1, 2, \ldots, r$, obtenemos H_{p,l_i} matriz asociada a $\widetilde{\mathcal{M}}_{l_i}(\Lambda)$ aplicando el mapa π_{l_i} a $\tilde{H}_p$.

Bibliografía

[1] Birch, B. J. *Hecke actions on classes of ternary quadratic forms.* Computational number theory (Debrecen, 1989), 191–212, de Gruyter, Berlin, 1991.

[2] Cassels, J. W. S. *Rational quadratic forms.* London Mathematical Society Monographs, 13. Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London-New York, 1978. xvi+413 pp.

[3] Conway, J. H.; Sloane, N. J. A. *Low-dimensiónal lattices. IV. The mass formula.* Proc. Roy. Soc. London Ser. A 419 (1988), no. 1857, 259–286.

[4] Conway, J. H.; Sloane, N. J. A. *Sphere packings, lattices and groups.* Springer-Verlag, New York, 1999. lxxiv+703 pp.

[5] Cremona, J. E. *Algorithms for modular elliptic curves.* Cambridge University Press, Cambridge, 1992. vi+343 pp.

[6] Dickson, L. E. *Studies in the Theory of Numbers* Chelsea Publishing Company 1957

[7] Lehman, Larry *Rational eigenvectors in spaces of ternary forms.* Math. Comp. 66 (1997), no. 218, 833–839.

[8] Sage: Open Source Mathematics Software `http://www.sagemath.org/`

[9] Tornaría, Gonzalo *The Brandt module of ternary quadratic lattices* Tesis de doctorado, University of Texas at Austin, 2005 `www.cmat.edu.uy/~tornaria/pub/`

[10] Watson, G. L. *Integral quadratic forms.* Cambridge Tracts in Mathematics and Mathematical Physics, No. 51 Cambridge University Press, New York 1960 xii+143 pp.