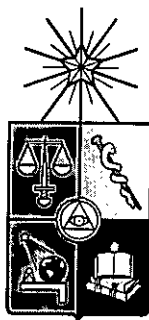


UCH-FC
DOC-M
Q 86
C. 1



**Cálculo de la norma espinorial para
formas anti-hermitianas sobre un álgebra
de cuaterniones de división sobre un
cuerpo local diádico.**

Tesis
entregada a la
Universidad de Chile
en cumplimiento parcial de los requisitos
para optar al grado de
Doctor en Ciencias con mención en Matemáticas
Facultad de Ciencias

por

Patricio Quiroz Herrera

Enero, 2013

Directores de Tesis: **Dr. Luis Arenas-Carmona**
Dr. Eduardo Friedman

FACULTAD DE CIENCIAS
UNIVERSIDAD DE CHILE

INFORME DE APROBACIÓN
TESIS DE DOCTORADO

Se informa a la Escuela de Postgrado de la Facultad de Ciencias que la Tesis de Doctorado presentada por el candidato


Patricio Quiroz Herrera


ha sido aprobada por la Comisión de Evaluación de la Tesis como requisito para optar al grado de Doctor en Ciencias con mención en Matemáticas, en el examen de Defensa de Tesis rendido el día 26 de Diciembre de 2012.

Directores de Tesis

Dr. Luis Arenas-Carmona

Dr. Eduardo Friedman



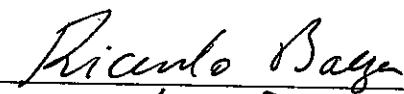


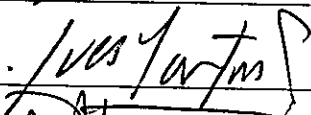
Comisión de Evaluación de la Tesis

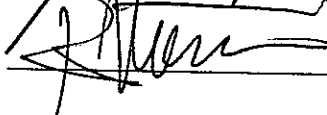
Dr. Ricardo Baeza

Dr. Yves Martin

Dr. Ricardo Menares







A Mabrs, Itor, Zorrow, Pablosky y a mi amorso.

BIOGRAFÍA



Nací el 7 de Julio de 1984 en Santiago de Chile. Crecí en el seno de una familia marcada por dos tendencias bastante distintas. Por una parte mi mamá con un espíritu humanista y por otra mi papá con un espíritu científico. Me impregné de ambos espíritus sin darme cuenta, yo sólo jugaba y jugaba a la pelota, mi gran pasión. En eso agotaba la mayor parte de mis energías, además

de no quedarme tranquilo en clases, haciendo llenar a mis profesores hojas y hojas de anotaciones negativas, sumado con numerosas citaciones al apoderado. Esa fue la tónica de mi niñez, jugar y hacerle la vida imposible a mis profesores. Ya en 7° básico, entré al Liceo de Aplicación, advertido de que tenía que cambiar mi comportamiento en la sala de clases. En el Liceo lo pasé muy bien y me comporté bastante mejor que en el Colegio Chile, mi anterior colegio. Seguí jugando a la pelota y a cada juego o deporte que estuviera de moda. Me gustaban las matemáticas, sin embargo en 4° medio tenía decidido estudiar arquitectura, ya que me gustaba también el dibujo técnico y las maquetas. En la segunda mitad de 4° medio, me di cuenta de que arquitectura no tenía mucha matemática y que en realidad me gustaban más las matemáticas que cualquier otra disciplina. Entonces decidí entrar a Ingeniería Matemática en la Usach por consejo de mi papá, con el argumento de que INGEMAT me abriría el camino para elegir entre muchas ingenierías y también para dedicarme a las matemáticas puras, si es que así lo quisiera. En el camino me convencí de que la ingeniería no era lo mío y decidí realizar los electivos que me conducirían a

obtener la Licenciatura en Matemáticas, para luego continuar con un postgrado. En ese entonces, me enteré que uno podía ir a la Facultad de Ciencias de la Chile a hacer algún electivo de álgebra, área que me atraía por sobre las otras.

Cuando llegué a Ciencias y asistí al curso de álgebra dictado por la profe Alicia Labra, me llevé una gran sorpresa. Aparte de gustarme el curso, me sentí como en casa (en ese tiempo, como en la Usach), un ambiente humano muy cómodo para mí, algo vital. Luego vi la malla de la Licenciatura y me terminé de encantar. Mientras yo hacía entre 6 y 7 cursos por semestre en Ingeniería, la mitad de los cuales no eran de matemáticas y no me gustaban, en Ciencias eran 3 por semestre y pura matemática, fantástico! pensé de inmediato: "me cambio!!". La historia continúa con el término de la Licenciatura en la Facultad de Ciencias y mi ingreso al Doctorado, conociendo en el camino a los que son hoy por hoy, junto con amigos de la Usach, mis mejores amigos y a mi polola con la cual quiero estar el resto de mis días. En el cuarto año del Doctorado aproximadamente, comenzó un gusto por las matemáticas distinto del anterior, en particular por la Teoría de Números, llegué a encontrar bonitos (de verdad!) ciertos resultados y ahora disfruto más que nunca de las matemáticas. Sigo jugando a la pelota y creo que ya me porto bien...

AGRADECIMIENTOS

Deseo agradecer a todos quienes tuvieron algo que ver con que esta tesis llegara a buen término.

A mi Familia

Claramente esta tesis no es un resultado de unos pocos años, sino que es un resultado de mas de veinte. He sentido el cariño y apoyo de mi familia a través de la historia. Me siento muy afortunado de la familia que me tocó. Espero que disfruten de este logro y lo sientan propio también. Gracias familia!!

A mi polola

Que me ha acompañado en este camino desde el segundo año del Doctorado, me ha dado contención en momentos difíciles, hemos compartido en los buenos momentos y me ha escuchado todo el "jugo" que le doy con temas de matemáticas que me gustan, en particular con lo relativo a esta tesis.

A mis amigos

Mis compadres Gonzalo y Juanito, con quienes he compartido en lo extra académico, me han acompañado en momentos difíciles y han sabido comprender los múltiples "pucha no puedo" que he pronunciado debido a las matemáticas. Al Eugenio, con quien comenzamos el proceso juntos, en general compartimos poco en tiempo pero de mucha calidad, yo sé que la amistad y el cariño no se van a acabar. A Luchin, con quien estrechamos nuestros lazos, compartimos bastante sobre todo en el último período, le tengo gran cariño y espero nunca nos dejemos de juntar.

A la Natu, con quién comenzamos el Doctorado y hemos pasado todo el proceso juntos, bueno casi todo el proceso ya que tuvimos una división entre medio, la cual ella tuvo la grandeza de ir a solucionar cuando yo debo haber pesado como una tonelada de todas las armaduras que llevaba encima, me supo comprender más de lo

que yo lo hubiera hecho. Además, me hablaba muy bien de mi polola e influyó notablemente en mi relación con ella. Muy muy importante para mi en este proceso. Muchas gracias por todo Natu!!

A la Usach

Por el cariño y formación que me ha entregado en el pregrado. Conocí a personas muy especiales allí con las cuales me desarrollé como matemático y como persona.

Al Departamento de Matemáticas

A todos los integrantes del departamento, los cuales hacen que uno sienta ganas de entregar mucho de vuelta, en particular a Santiago, el "Superman" del departamento, hace de todo, y no me extrañaría verlo un día reemplazando a un profe que no pudo llegar. A los profesores, quienes en su mayoría transmiten cercanía con los estudiantes, el hecho de poder conversar en cualquier momento con ellos, plantear ideas y discutir, es invaluable. A mis compañeros, Andrea, Leslie, Nacho, Alan, Henry, Ferr entre otros, por la buena onda y por hacer de mi estadía muy agradable.

Al profe Lucho, mi tutor, de quien he aprendido mucha matemática, formas de pensar las cosas, de investigar, de redactar, etc. Siempre dispuesto a atender mis inquietudes, casi siempre las respuestas a velocidades impresionantes. Buena persona y sencillo, a pesar de poseer un gran intelecto. Además, después de terminada la beca Conicyt, el profe me ha auspiciado con fondos de su proyecto Fondecyt. Gracias por todo profe!!

Índice

1. Introducción	1
2. Preliminares	6
2.1. Álgebras de cuaterniones	6
2.2. Cuerpos locales	9
2.3. Símbolo de Hilbert	11
2.4. Formas anti-hermitianas	12
2.5. Reticulados y órdenes	13
2.6. Aritmética en $D = \left(\frac{\pi, \Delta}{k}\right)$	16
2.7. Cohomología	19
2.8. Norma espinorial	21
2.9. Clasificación de formas anti-hermitianas cuaterniónicas enteras	22
3. Sobre $H(\Lambda)$	24
3.1. Generadores de $\mathcal{U}_k^+(\Lambda)$ y su norma espinorial	24
3.2. Hechos generales para el cálculo de $H(\Lambda)$	26
3.3. Resultados	27
4. Algoritmo para calcular imágenes espinoriales	33
4.1. El Teorema de Tsukamoto	33

	VIII
4.2. El algoritmo	34
4.3. Implementación del algoritmo	37
5. Cálculo de imágenes espinoriales sobre \mathbb{Q}_2	42
5.1. Caso I	43
5.2. Caso II	52
5.3. Aplicaciones	53
A. Apéndice	55

RESUMEN

En esta tesis, se desarrolla un algoritmo para calcular la imagen de la norma espinorial para formas anti-hermitianas sobre un álgebra de cuaterniones de división sobre un cuerpo local diádico k de característica 0. Luego se implementa el algoritmo para el cuerpo $k = \mathbb{Q}_2$ completando así, todos los cálculos locales para formas anti-hermitianas cuaterniónicas enteras sobre \mathbb{Q} . También se realizan avances en el caso general. Los cálculos para cuerpos no-diádicos fueron realizados por Böge [6].

ABSTRACT

In this thesis, we develop an algorithm to compute the image of the spinor norm for quaternionic skew-hermitian forms at dyadic local places. Then, we use it to complete all local computations for quaternionic skew-hermitian forms over \mathbb{Q} . Some advances are made in the general case. Non-dyadic places have already been completely determined by Böge [6].

Capítulo 1

Introducción

Un problema central en la teoría de formas cuadráticas es el de clasificación (módulo isometría). Sabemos que este problema para formas bilineales sobre un cuerpo de números k puede ser reducido, por el Teorema de Hasse-Minkowski, al problema de clasificarlas sobre todas las localizaciones de k (ver, por ejemplo, [10, §66]). Sin embargo, para formas sobre el anillo de enteros \mathcal{O}_k de k , no existe un principio local-global como en el caso anterior, pero la información local aún nos dice bastante de lo que ocurre globalmente. Por otro lado, existe una correspondencia entre clases de reticulados libres y clases de formas cuadráticas enteras. Así, el problema en cuestión nos lleva a la teoría de géneros y géneros espinoriales [10, §102] desarrollada por Eichler y Kneser en los años 50. Esta teoría depende en gran medida del cálculo de la imagen de la norma espinorial $(\theta, \Theta_A$ ver §2.8) ya que, bajo ciertas condiciones sobre un grupo lineal algebraico G , se tiene que el número de clases de un reticulado Λ , el cual se puede decir que mide la diferencia entre la información local y la global, es igual a la cardinalidad del grupo $\Theta_A(G_\Lambda)/(\theta(G_k)\Theta_A(G_\Lambda^A))$ (ver §2.9). Cálculos de la norma espinorial para formas bilineales enteras existen en la literatura: El caso no diádico lo podemos encontrar en [8] (M. Kneser, 1956), el caso 2-ádico en [7] (A. Earnest y J. Hsia, 1975), el caso en que el índice de ramificación es $e = 2$ en [17] (Fei Xu, 1993) y finalmente, para cuerpos diádicos en general, el cálculo lo realizó C.N. Beli [5] (2003).

Estas preguntas también tienen sentido para formas anti-hermitianas sobre un álgebra de cuaterniones de división. Dichas formas comparten muchas propiedades aritméticas con las formas bilineales [6]. Para espacios anti-hermitianos, el problema

de determinar si dos reticulados son isométricos también puede ser atacado usando la teoría de géneros y géneros espinoriales, ya que el grupo unitario de una forma anti-hermitiana cuaterniónica es isomorfo al grupo ortogonal de una forma cuadrática cuando se consideran los grupos sobre la clausura algebraica del cuerpo base [3, §3].

Generalmente el cálculo local se divide en 2: cálculo local diádico y cálculo local no-diádico. La principal diferencia entre el caso diádico y no-diádico es la cantidad de clases de cuadrados, esto se puede observar en la siguiente fórmula:

$$[k^* : k^{*2}] = 4N\mathfrak{p}^{v_{\mathfrak{p}}(2)},$$

donde $N\mathfrak{p}$ es el número de elementos del cuerpo residual y $v_{\mathfrak{p}}$ es la valuación del cuerpo k . Ver también el Teorema 2.2.1 y el Lema 2.6.4.

En el caso cuadrático, la clasificación de reticulados se hace principalmente a través de los invariantes *escala*, *norma* y *peso*. Para reticulados anti-hermitianos tenemos a disposición la escala al igual que en el caso cuadrático. No ocurre lo mismo con la norma y peso ya que un reticulado anti-hermitiano unimodular es diagonalizable.

El cálculo no-diádico lo podemos encontrar en [6]. En [2] se estudian los lugares diádicos no cubriendo todos los casos. En [4] se estudian cuerpos de representación para formas anti-hermitianas cuaterniónicas y se completan algunos casos no incluidos en [2]. Recordamos aquí, los cálculos en el caso diádico:

Sea k un cuerpo local diádico de característica 0 (§2.2) con único orden maximal \mathcal{O}_k . Sea D un álgebra de cuaterniones de división sobre k (§2.1) con único orden maximal \mathcal{O}_D . La valuación en D es denotada por ν (§2.6). Denotamos por V un D -módulo (por la izquierda) libre de rango n con una forma anti-hermitiana h (§2.4).

Un reticulado anti-hermitiano Λ tiene una descomposición del tipo

$$\Lambda = \Lambda_1 \perp \cdots \perp \Lambda_t,$$

donde cada reticulado Λ_r es de rango 1 o 2, y las escalas satisfacen $\mathfrak{s}(\Lambda_{r+1}) \subset \mathfrak{s}(\Lambda_r)$ (§2.5). Este resultado es el análogo anti-hermitiano a la descomposición de Jordan para reticulados bilineales en [10, §91]. Siguiendo [6], definimos $H(\Lambda)$ por la relación $H(\Lambda)/k^{*2} = \theta(\mathcal{U}_k^+(\Lambda))$, donde $\mathcal{U}_k^+(\Lambda)$ es el estabilizador del reticulado Λ bajo la acción del grupo especial unitario \mathcal{U}_k^+ de la forma h , y $\theta : \mathcal{U}_k^+(\Lambda) \rightarrow k^*/k^{*2}$ denota

la norma espinorial (§2.8). Notemos que $k^{*2} \subset H(\Lambda) \subset k^*$. Por abuso de lenguaje decimos que $H(\Lambda)$ es la imagen de la norma espinorial.

Las tablas 1.1 y 1.2 resumen los resultados obtenidos en [2] y [4] para un cuerpo local diádico arbitrario k :

s	$ A $	α	n	$H(\Lambda)$
-	-	-	1	$N(k(a_1)^*)$
-	> 1	-	-	k^*
0	1	$-\tilde{\Delta}$	-	$\mathcal{O}_k^* k^{*2}$
0	1	$-\tilde{u}, \tilde{\pi}$	≥ 2	k^*
$\neq 0$	-	-	-	k^*

Tabla 1.1: Reticulados modulares

s	$ A $	α	μ	$H(\Lambda)$
-	> 1	-	-	k^*
0	1	$-\tilde{\Delta}$	-	$\mathcal{O}_k^* k^{*2}$
0	1	$-\tilde{u}, \tilde{\pi}$	$\mu > \nu(16)$	$N(k(a_m)^*)$
0	1	$-\tilde{u}$	$0 < \mu \leq \nu(16)$?
0	1	$\tilde{\pi}$	$\mu < \nu(4)$	k^*
0	1	$\tilde{\pi}$	$\nu(4) \leq \mu \leq \nu(16)$?
$\neq 0$	-	-	-	k^*

Tabla 1.2: Reticulados arbitrarios

La notación para las tablas es como sigue:

1. s es el número de reticulados binarios indescomponibles en la descomposición de Λ antes mencionada.
2. Si algún Λ_m tiene rango 1, entonces $\Lambda_m = \mathcal{O}_D s_m$ y $h(s_m, s_m) = a_m$. De aquí se define $A = \{N(a_m)k^{*2} \mid \text{rango}(\Lambda_m) = 1\}$, donde N es la norma reducida (§2.1).
3. Si $|A| = 1$, entonces $A = \{\alpha\}$.
4. $\tilde{\lambda}$ es la clase λk^{*2} .
5. $\Delta \in \mathcal{O}_k^*$ es una unidad de defecto cuadrático minimal (§2.2).
6. $u \in \mathcal{O}_k^*$ es una unidad de defecto cuadrático no minimal cualquiera.
7. π es un primo arbitrario en \mathcal{O}_k .
8. $\mu \geq 0$ es la diferencia minimal entre la valuación de las escalas (§2.5) de dos componentes consecutivos de rango 1, es decir, si en la descomposición $\Lambda = \Lambda_1 \perp \cdots \perp \Lambda_t$ aparecen sumandos de la forma $\mathcal{O}_D s_i \perp \mathcal{O}_D s_{i+1} = \langle a_i \rangle \perp \langle a_{i+1} \rangle$, entonces μ es el mínimo de todas las diferencias $\nu(a_{i+1}) - \nu(a_i)$.
9. Un segmento – significa información irrelevante.

En esta tesis, completamos los cálculos en el caso $k = \mathbb{Q}_2$, culminando de esta manera todos los cálculos locales para formas anti-hermitianas cuaterniónicas enteras sobre \mathbb{Q} . También se mejora la tabla 1.2 para un cuerpo local diádico k cualquiera.

Lo descrito en el párrafo anterior se realiza considerando primero reticulados Λ de rango 2 y caracterizando, para estos reticulados, el hecho de que $H(\Lambda) = k^*$ de manera que se pueda determinar $H(\Lambda)$ mediante un cálculo finito, el cual se hace por computador. Luego, para reticulados de cualquier rango, reducimos el cálculo a los casos de rango 2 o 3 los cuales se manejan con las técnicas anteriores.

La piedra de tope para el cálculo general es el hecho de que la función $k \mapsto |k^*/k^{*2}|$ es no acotada (k diádico). Los cálculos para k diádico cualquiera realizados en [2] dependen fuertemente del Lema 2.6.4. Mencionamos también por qué dichas técnicas no se extienden para los casos restantes.

En virtud de la tabla 1.2, consideraremos reticulados diagonalizables con $|A| = 1$. Es decir, reticulados del tipo $\Lambda = \langle a_1 \rangle \perp \cdots \perp \langle a_n \rangle$, donde $N(a_i) \in N(a_1)$, $\forall i = 2, \dots, n$.

Los casos a tratar en este trabajo se encuentran en la siguiente tabla, la cual sigue las notaciones de las tablas 1.1 y 1.2:

Casos	A	μ	$H(\Lambda)$
I	$\{-\tilde{u}\}$	$0 < \mu \leq \nu(16)$?
II	$\{\tilde{\pi}\}$	$\nu(4) \leq \mu \leq \nu(16)$?

Tabla 1.3: Casos restantes

El capítulo 2 contiene material preliminar que culmina con la descripción del problema de clasificación de formas anti-hermitianas cuaterniónicas enteras. En el capítulo 3 se sientan las bases para nuestro estudio de $H(\Lambda)$ y se realizan algunos cálculos para \mathcal{O}_D -reticulados anti-hermitianos sobre un cuerpo local diádico de característica 0 cualquiera k , mejorando los resultados precedentes. En particular, se da la solución del caso II cuando $\mu = \nu(4)$. En el capítulo 4 desarrollamos un algoritmo para calcular imágenes espinoriales, cuya implementación se realiza para $k = \mathbb{Q}_2$. Finalmente, en el capítulo 5 se realizan los cálculos para los casos I y II descritos en la tabla 1.3 para \mathbb{Q}_2 usando el algoritmo descrito en el capítulo 4, y se aplican para calcular el número de clases de formas anti-hermitianas específicas.

Capítulo 2

Preliminares

En cada sección de este capítulo incluimos importantes ejemplos y observaciones sobre los objetos particulares que nos interesan en este trabajo, para su uso en capítulos posteriores. En las secciones 2.1, 2.2 y 2.3 vemos lo necesario para nuestro trabajo con álgebras de cuaterniones sobre cuerpos locales. La referencia principal para estas secciones es el texto de O'Meara [10]. En las secciones 2.4, 2.5 y 2.6 nos concentramos en la parte entera de la teoría de formas anti-hermitianas cuaterniónicas, siendo las referencias principales el artículo [2] y el texto [15]. Finalmente, las secciones 2.7, 2.8 y 2.9 están dedicadas al problema de clasificación de formas anti-hermitianas cuaterniónicas enteras usando cohomología galoisiana. Las principales referencias para estas secciones son [2], [1] y [9].

2.1. Álgebras de cuaterniones

Sea F un cuerpo y sean $\alpha, \beta \in F^*$. Consideremos un F -espacio vectorial V de dimensión 4 sobre F y una base $\{1, x_1, x_2, x_3\}$ de V . Entonces $V = F \cdot 1 + F \cdot x_1 + F \cdot x_2 + F \cdot x_3$. Definimos una multiplicación sobre los elementos de la base mediante la siguiente tabla:

\cdot	1	x_1	x_2	x_3
1	1	x_1	x_2	x_3
x_1	x_1	$\alpha 1$	x_3	αx_2
x_2	x_2	$-x_3$	$\beta 1$	$-\beta x_1$
x_3	x_3	$-\alpha x_2$	βx_1	$-\alpha \beta 1$

Extendemos esta multiplicación por linealidad a una multiplicación sobre V . Se comprueba que V es un álgebra asociativa con identidad. Así, dados un cuerpo F y elementos $\alpha, \beta \in F^*$, podemos construir una F -álgebra de dimensión 4 sobre F por el procedimiento descrito anteriormente. Diremos que un álgebra construida de esa manera es un **álgebra de cuaterniones** y la denotaremos por el símbolo

$$\left(\frac{\alpha, \beta}{F}\right).$$

Llamaremos a sus elementos *cuaterniones*. Los elementos de $F \cdot 1$ son llamados *cuaterniones escalares* y los elementos de $F \cdot x_1 + F \cdot x_2 + F \cdot x_3$ son llamados *cuaterniones puros*. El conjunto de cuaterniones puros es denotado

$$\left(\frac{\alpha, \beta}{F}\right)^0 = F \cdot x_1 + F \cdot x_2 + F \cdot x_3.$$

Cuando no haya peligro de confusión, escribiremos (α, β) en vez de $\left(\frac{\alpha, \beta}{F}\right)$. De la tabla de multiplicación, es claro que $x_r^2 \in F^* \cdot 1$ para todo $r = 1, 2, 3$ y que $x_r x_s = -x_s x_r \in F^* \cdot x_t$, para cualquier permutación r, s, t de los dígitos 1, 2, 3.

De aquí en adelante adoptaremos la notación de las referencias [2], [15]. Es decir, $1, i = x_1, j = x_2, k = x_3 = ij$, es una base del álgebra de cuaterniones (α, β) . Aquí, $i^2 = \alpha, j^2 = \beta, ij = -ji$.

Si $x = a + bi + cj + dk$, donde $a, b, c, d \in F$, es un cuaternión, definimos el conjugado de x como $\bar{x} = a - bi - cj - dk$. También diremos que $x \mapsto \bar{x}$ es la involución canónica del álgebra de cuaterniones. Es claro que $\overline{xy} = \bar{y}\bar{x}$.

Definición 2.1.1. Sea $x \in \left(\frac{\alpha, \beta}{F}\right)$. Definimos la norma N y la traza T de x mediante:

$$Nx = x\bar{x}, \quad Tx = x + \bar{x}.$$

Si $x = a + bi + cj + dk \in \left(\frac{\alpha, \beta}{F}\right)$, entonces $Nx = a^2 - b^2\alpha - c^2\beta + d^2\alpha\beta \in F$, y $Tx = 2a \in F$. Un cálculo directo prueba que $N(xy) = NxNy$, y que $T(x + y) = Tx + Ty$. Además, notemos que

$$Nx = \begin{cases} x^2 & , \text{ si } x \text{ es cuaternión escalar.} \\ -x^2 & , \text{ si } x \text{ es cuaternión puro.} \end{cases}$$

Observación 2.1.1. Un cuaternión x es invertible si y sólo si $Nx \neq 0$. En tal caso $x^{-1} = \bar{x} \cdot (Nx)^{-1}$.

Observación 2.1.2. Un cuaternión no escalar q en un álgebra de cuaterniones, genera un álgebra conmutativa semisimple de dimensión 2 sobre F , ya que es raíz del polinomio $x^2 - T(q)x + N(q) \in F[x]$. En particular, si el álgebra de cuaterniones es de división, q genera una extensión cuadrática de F .

Ejemplo 2.1.1. Considerando la matrices $Y = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, es fácil ver que

$$Y^2 = 1, Z^2 = -1, YZ = -ZY.$$

Así, usando el hecho de que un álgebra de cuaterniones es simple [10, §63], se tiene que la función $\phi : \left(\frac{1,-1}{F}\right) \rightarrow M_2(F)$ definida por $\phi(1) = I$, $\phi(x_1) = Y$, $\phi(x_2) = Z$ y $\phi(x_3) = YZ$, es un isomorfismo de álgebras.

Enunciaremos los resultados principales sobre álgebras de cuaterniones, estos hechos fueron extraídos de [10, §63]:

Proposición 2.1.1. Sean $\alpha, \beta \in F^*$. Las siguientes afirmaciones son equivalentes:

1. (α, β) es un álgebra isomorfa a $(1, -1)$.
2. (α, β) no es un álgebra de división.
3. El espacio cuadrático $\langle \alpha \rangle \perp \langle \beta \rangle$ sobre F representa a 1.
4. $\alpha \in N_{E/F}E$, donde $E = F(\sqrt{\beta})$.

Proposición 2.1.2. Sean $\alpha, \beta, \gamma, \lambda, \mu \in F^*$. Se tienen los siguientes isomorfismos de álgebras:

1. $(1, \alpha) \cong (1, -1) \cong (\alpha, -\alpha) \cong (\alpha, 1 - \alpha)$.
2. $(\alpha, \beta) \cong (\beta, \alpha) \cong (\alpha\lambda^2, \beta\mu^2)$.
3. $(\alpha, \alpha\beta) \cong (\alpha, -\beta)$.
4. $(\alpha, \beta) \otimes_F (\alpha, \gamma) \cong (\alpha, \beta\gamma) \otimes_F (1, -1)$.

2.2. Cuerpos locales

Un *cuerpo local no-arquimediano* k es un cuerpo completo respecto de un valor absoluto discreto $|\cdot|_k$ tal que el cuerpo residual $\mathcal{O}_k/\mathfrak{m}_k$ es finito; donde $\mathcal{O}_k = \{\alpha \in k \mid |\alpha|_k \leq 1\}$ es el anillo de enteros del cuerpo k , y $\mathfrak{m}_k = \{\alpha \in k \mid |\alpha|_k < 1\}$ es el único ideal maximal de \mathcal{O}_k .

Los *cuerpos locales arquimedianos* son \mathbb{R} y \mathbb{C} .

Un *cuerpo local*, es uno de los cuerpos descritos anteriormente.

Ejemplo 2.2.1. El cuerpo \mathbb{Q}_p de los números p -ádicos es un cuerpo local. Aquí $\mathcal{O}_{\mathbb{Q}_p}$ es denotado por \mathbb{Z}_p , su ideal maximal es $p\mathbb{Z}_p$, y el cuerpo residual es $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$.

En esta tesis, sólo nos interesamos en el caso no-arquimediano de característica 0. Específicamente, consideraremos sólo cuerpos locales diádicos de característica 0, es decir, extensiones finitas de \mathbb{Q}_2 . En un cuerpo local k , el anillo de enteros \mathcal{O}_k es dominio de ideales principales. Si $\mathfrak{m}_k = (\pi)$, decimos que π es un *parámetro uniformizante* en k . Todo $\alpha \in k$ se escribe de la forma $\alpha = u\pi^t$, donde $u \in \mathcal{O}_k^*$ y $t \in \mathbb{Z}$. Se define un valor absoluto en k mediante $|\alpha|_k = (1/N\pi)^t$, donde $N\pi$ es el número de elementos del cuerpo residual $\mathcal{O}_k/\mathfrak{m}_k$.

Es clara la importancia de conocer los cuadrados en el anillo de enteros de un cuerpo de números para el estudio de formas cuadráticas enteras. El siguiente teorema nos dice que si un entero en un cuerpo local está suficientemente cerca de 1 con respecto al valor absoluto $|\cdot|_k$, entonces es un cuadrado. En la sección 2.6 veremos un análogo de este resultado en el caso cuaterniónico, el cual utilizaremos con frecuencia para nuestro estudio sobre formas anti-hermitianas cuaterniónicas enteras.

Teorema 2.2.1 (Teorema de Cuadrados Locales). [10, 63:1] *Sea α un entero en un cuerpo local k . Entonces existe un entero β tal que*

$$1 + 4\pi\alpha = (1 + 2\pi\beta)^2.$$

Usando el *Teorema de Cuadrados Locales* podemos estudiar que tan lejos esta un elemento en un cuerpo local de ser un cuadrado. En efecto, consideremos un elemento ξ en un cuerpo local k . Entonces ξ tiene al menos una expresión de la

forma $\xi = \eta^2 + \alpha$, con $\eta, \alpha \in k$. Tomando la intersección sobre todas esas posibles escrituras de ξ definimos

$$\mathfrak{d}(\xi) = \bigcap_{\alpha} \alpha \mathcal{O}_k.$$

Con esta definición, $\mathfrak{d}(\xi)$ es un ideal fraccional o 0. Diremos que $\mathfrak{d}(\xi)$ es el **defecto cuadrático** de ξ . Se tienen los siguientes hechos acerca del defecto cuadrático $\mathfrak{d}(\xi)$:

1. $\mathfrak{d}(a^2\xi) = a^2\mathfrak{d}(\xi) \quad \forall a, \xi \in k$.
2. $\mathfrak{d}(\xi) = \xi \mathcal{O}_k$ si $v(\xi)$ es impar, donde $\xi \in \pi^{v(\xi)} \mathcal{O}_k^*$.

Por otra parte, si $v(\xi)$ es par, podemos escribir $\xi = \pi^{2t}\epsilon$ con ϵ una unidad y por lo tanto $\mathfrak{d}(\xi) = \pi^{2t}\mathfrak{d}(\epsilon)$. Así, basta estudiar el defecto cuadrático para el grupo de unidades \mathcal{O}_k^* módulo cuadrados, es decir, para representantes del grupo $\mathcal{O}_k^*/\mathcal{O}_k^{*2}$.

Usando el Teorema de Cuadrados Locales se pueden probar los siguientes resultados:

1. $\xi \in k^2 \Leftrightarrow \mathfrak{d}(\xi) = 0$.
2. Sea ϵ una unidad en un cuerpo local k . Si k es no diádico, entonces $\mathfrak{d}(\epsilon)$ es 0 u \mathcal{O}_k ; si k es diádico, entonces $\mathfrak{d}(\epsilon)$ es uno de los ideales¹

$$0 \subset 4\mathcal{O}_k \subset 4\mathfrak{p}^{-1} \subset 4\mathfrak{p}^{-3} \subset \dots \subset \mathfrak{p}^3 \subset \mathfrak{p}.$$

Considerando el resultado anterior, si $\mathfrak{d}(\xi) = 4\mathcal{O}_k$ diremos que ξ es un elemento de *defecto cuadrático minimal* en k .

Ejemplo 2.2.2. $5 = 1 + 4$ es una unidad de defecto cuadrático minimal en \mathbb{Q}_2 .

Se puede probar que una unidad ϵ tiene defecto cuadrático minimal, si y sólo si, la extensión $k(\sqrt{\epsilon})/k$ es cuadrática no ramificada. De este hecho se deduce que siempre existen unidades de defecto cuadrático minimal, y que dos de ellas cualquiera siempre están en la misma clase de cuadrados.

¹Notar que si el índice de ramificación e es mayor o igual a 3, efectivamente se tiene $4\mathfrak{p}^{-3} \subset \mathfrak{p}^3$. De otro modo, la cadena de ideales es más corta. En efecto, si $e = 2$ se tiene que $4\mathfrak{p}^{-3} = \mathfrak{p}$. Por otra parte, si $e = 1$, entonces la cadena se reduce a $0 \subset 4\mathcal{O}_k = \mathfrak{p}^2 \subset \mathfrak{p}$.

2.3. Símbolo de Hilbert

En esta sección, F será un cuerpo local de característica 0 en el lugar \mathfrak{p} , es decir, $F = K_{\mathfrak{p}}$ donde K es un cuerpo de números y el lugar \mathfrak{p} es la clase de equivalencia del valor absoluto respecto del cual F es completo. Aquí, dos valores absolutos sobre un cuerpo F son equivalentes, si definen sobre él la misma topología.

Para $\alpha, \beta \in F^*$, se define el **símbolo de Hilbert** mediante:

$$\left(\frac{\alpha, \beta}{\mathfrak{p}}\right) = \begin{cases} 1 & , \text{ si el espacio cuadrático } \langle \alpha \rangle \perp \langle \beta \rangle \text{ representa a } 1. \\ -1 & , \text{ si no.} \end{cases}$$

Observación 2.3.1. Usando los resultados de la sección 2.1 obtenemos la siguiente definición alternativa del símbolo de Hilbert:

$$\left(\frac{\alpha, \beta}{\mathfrak{p}}\right) = \begin{cases} 1 & , \text{ si } \left(\frac{\alpha, \beta}{F}\right) \cong \mathbb{M}_2(F). \\ -1 & , \text{ si no.} \end{cases}$$

Observación 2.3.2. De la Proposición 2.1.1 obtenemos que, si $E = F(\sqrt{\beta})$, entonces

$$\alpha \in N_{E/F}E^* \text{ si y sólo si } \left(\frac{\alpha, \beta}{\mathfrak{p}}\right) = 1.$$

Recordemos que, si a es un cuaternión puro, entonces $a^2 = -Na$. Para este caso particular, reescribiremos la observación anterior como un lema, dada su importancia posterior.

Lema 2.3.1. *Sea a un cuaternión puro en un álgebra de cuaterniones sobre un cuerpo local F . Entonces*

$$l \in N(F(a)^*) \text{ si y sólo si } \left(\frac{l, -Na}{\mathfrak{p}}\right) = 1.$$

Sabemos que las álgebras de cuaterniones que no son de división son isomorfas a $\mathbb{M}_2(F)$ (§2.1). Por otra parte, se tiene que $\left(\frac{\pi, \Delta}{\mathfrak{p}}\right) = -1$, donde π es parámetro

uniformizante de F y Δ es unidad de defecto cuadrático minimal de F . Mas aún, todas las álgebras de cuaterniones de división sobre F son isomorfas a $(\frac{\pi, \Delta}{F})$ [10, §63].

Por lo tanto, hay esencialmente dos álgebras de cuaterniones sobre F . Usando este hecho, se puede probar que los puntos 3 y 4 en la Proposición 2.1.2 se traducen en

$$\left(\frac{\alpha, \alpha\beta}{\mathfrak{p}}\right) = \left(\frac{\alpha, -\beta}{\mathfrak{p}}\right),$$

$$\left(\frac{\alpha, \beta}{\mathfrak{p}}\right) \left(\frac{\gamma, \beta}{\mathfrak{p}}\right) = \left(\frac{\alpha\gamma, \beta}{\mathfrak{p}}\right).$$

La última igualdad nos dice que, para $\beta \in F^*$ el símbolo de Hilbert define un homomorfismo de grupos $\left(\frac{\cdot, \beta}{\mathfrak{p}}\right) : F^* \rightarrow \{\pm 1\}$. Además, la Observación 2.3.2 nos dice que, si $E = F(\sqrt{\beta})$ es una extensión cuadrática, el núcleo de este homomorfismo es $N_{E/F}(E^*)$. Por otra parte, se puede probar [10, §63] que, si la extensión E/F es cuadrática, este homomorfismo es epiyectivo. Por lo tanto,

$$[F^* : N_{E/F}E^*] = 2.$$

Este hecho será de gran utilidad cuando consideremos reticulados anti-hermitianos sobre álgebras de cuaterniones de división, pues, como se observó en la sección 2.1, los cuaterniones no escalares generan extensiones cuadráticas.

2.4. Formas anti-hermitianas

Una forma anti-hermitiana es una forma (-1) -hermitiana en el sentido de [12, §7.1]. Detallamos aquí la definición para el caso que nos interesa.

Definición 2.4.1. Sea D un álgebra de cuaterniones sobre un cuerpo de números o sobre un cuerpo local k y sea V un D -módulo libre por la izquierda. Diremos que una función $h : V \times V \rightarrow D$ es una *forma anti-hermitiana* si satisface:

1. h es D -lineal en la primera variable.
2. $h(x, y) = -\overline{h(y, x)}$, $\forall x, y \in V$.

Aquí, $q \mapsto \bar{q}$ denota la involución canónica del álgebra de cuaterniones (ver §2.1).

A un par (V, h) como en la definición se le llama espacio anti-hermitiano. Si $V = D^n$, entonces cualquier forma anti-hermitiana sobre V es una función del tipo

$$h((x_1, \dots, x_n), (y_1, \dots, y_n)) = \sum_{i,j=1}^n x_i a_{ij} \overline{y_j},$$

donde $a_{ij} = -\overline{a_{ji}}$. La matriz $(a_{ij})_{i,j} \in \mathbb{M}_n(D)$ es llamada matriz de Gram de h . Notar que como $a_{ii} = -\overline{a_{ii}}$, se tiene que a_{ii} es un cuaternión puro para todo i .

Definición 2.4.2. Sea (V, h) un espacio anti-hermitiano. Diremos que una función $\phi : V \rightarrow V$ es una *isometría* de (V, h) si satisface:

1. ϕ es D -lineal invertible.
2. $h(x, y) = h(\phi(x), \phi(y)), \forall x, y \in V$.

El grupo $\{\text{isometrías } \phi : V \rightarrow V\}$ es llamado *grupo unitario* de (V, h) (o de h) y es denotado por \mathcal{U}_k . El grupo de isometrías cuya matriz correspondiente tiene norma reducida 1 es llamado *grupo especial unitario* de (V, h) y es denotado por \mathcal{U}_k^+ .

Observación 2.4.1. Si $D \cong \mathbb{M}_2(k)$, las formas anti-hermitianas sobre un D -módulo libre V de rango n están en correspondencia con formas cuadráticas sobre el k -espacio vectorial PV de dimensión $2n$, para cualquier matriz idempotente $P \in D$ de rango 1 [3, §3]. El grupo unitario de una forma anti-hermitiana h es isomorfo al grupo ortogonal de la correspondiente forma cuadrática.

Observación 2.4.2. $\mathcal{U}_k = \mathcal{U}_k^+$ cuando el álgebra de cuaterniones es de división [9, §2.6].

En esta tesis, consideramos formas anti-hermitianas sobre un álgebra de cuaterniones de división sobre un cuerpo local diádico k de característica 0. Específicamente, estudiaremos formas anti-hermitianas cuaterniónicas enteras (módulo isometría), lo cual es equivalente, como veremos en la próxima sección, a estudiar \mathcal{O}_D -reticulados libres.

2.5. Reticulados y órdenes

Sea k un cuerpo de números o un cuerpo local ($k = L_p$, con L cuerpo de números) con anillo de enteros \mathcal{O}_k .

Definición 2.5.1. Sea V un k -espacio vectorial de dimensión n sobre k . Diremos que $\Lambda \subset V$ es un *reticulado* en V , si Λ es un \mathcal{O}_k -módulo tal que existe una base $\{x_1, \dots, x_n\}$ de V con

$$\Lambda \subset \mathcal{O}_k x_1 + \dots + \mathcal{O}_k x_n.$$

Si un reticulado Λ satisface $k\Lambda = V$ diremos que Λ es un *reticulado sobre V* . Un reticulado es *libre* si lo es como \mathcal{O}_k -módulo.

Ejemplo 2.5.1. $\mathcal{O}_k x_1 + \dots + \mathcal{O}_k x_n$ es un reticulado libre sobre V .

Definición 2.5.2. Sea A una k -álgebra. Diremos que $\mathfrak{D} \subset A$ es un *orden* si \mathfrak{D} es un reticulado en A tal que $1 \in \mathfrak{D}$ y $\mathfrak{D}\mathfrak{D} = \mathfrak{D}$. Es decir, un orden es un reticulado que a su vez es un subanillo. Un orden es maximal si lo es respecto a la contención de conjuntos.

Ejemplo 2.5.2. $M_2(\mathcal{O}_k)$ es un orden maximal en la k -álgebra $M_2(k)$.

Definición 2.5.3. Sea D un álgebra de cuaterniones sobre k . Sea V un D -módulo libre y \mathcal{O}_D un orden maximal² en D . Diremos que $\Lambda \subset V$ es un \mathcal{O}_D -reticulado si es un reticulado en V tal que $\mathcal{O}_D \Lambda = \Lambda$.

Al igual que en el caso de formas cuadráticas enteras, la clasificación de formas anti-hermitianas enteras (módulo isometría) es equivalente a la clasificación de reticulados libres. En efecto, sea D un álgebra de cuaterniones sobre k y \mathcal{O}_D un orden maximal en D . Una *forma anti-hermitiana entera* es una forma anti-hermitiana $h : \mathcal{O}_D^n \times \mathcal{O}_D^n \rightarrow \mathcal{O}_D$. Tales formas se pueden extender de manera única a $V = D^n$. Sea h' otra forma anti-hermitiana entera tal que existe una isometría f entre los espacios anti-hermitianos (D^n, h) y (D^n, h') . Así, $h'(x, y) = h(f^{-1}(x), f^{-1}(y))$, para todo par de elementos $x, y \in D^n$. Decimos que h, h' están en la misma *clase*, y anotamos $h \sim_1 h'$, si existe una función D -lineal invertible $\phi : \mathcal{O}_D^n \rightarrow \mathcal{O}_D^n$ tal que

$$h(x, y) = h'(\phi(x), \phi(y)), \text{ para todo par de elementos } x, y \in \mathcal{O}_D^n. \quad (*)$$

Si definimos $\Lambda = f^{-1}(\mathcal{O}_D^n)$ se tiene que

$$h \sim_1 h' \Leftrightarrow \Lambda \sim_2 \mathcal{O}_D^n,$$

²Este es el análogo del anillo de enteros \mathcal{O}_k de un cuerpo de números k en el caso no conmutativo.

donde para \mathcal{O}_D -reticulados M, L , se escribe $M \sim_2 L$ si existe una isometría ϕ de (V, h) tal que $\phi(M) = L$.

También tenemos una versión local de lo anterior. En efecto, decimos que h y h' están en el mismo género si:

1. (*) es satisfecha para una función D_p -lineal invertible $\phi = \phi_p : \mathcal{O}_{D_p}^n \rightarrow \mathcal{O}_{D_p}^n$ con coeficientes en la completación³ \mathcal{O}_{D_p} para cada lugar finito p de k .
2. (*) es satisfecha para una función D -lineal invertible ϕ con coeficientes en la k -álgebra D .

Notar que la condición (2) es redundante (si en (1) agregamos los lugares infinitos) para formas cuadráticas debido al principio de Hasse sobre cuerpos, el cual no se tiene en el caso anti-hermitiano cuaterniónico.

Como antes, se tiene que h, h' están en el mismo género si y sólo si los reticulados Λ y \mathcal{O}_D^n son localmente equivalentes (i.e. existe una isometría local $\phi_p : D_p^n \rightarrow D_p^n$ tal que $\phi_p(\Lambda_p) = \mathcal{O}_{D_p}^n$ para cada lugar p). Recíprocamente, cualquier \mathcal{O}_D -reticulado libre Λ define, una vez que una \mathcal{O}_D -base es elegida, una forma h' que está en la misma clase o género que h si y sólo si Λ está en la misma clase o género que \mathcal{O}_D^n . Por lo tanto, la clasificación de formas anti-hermitianas enteras corresponde, al igual que en el caso cuadrático, a la clasificación de reticulados libres. Adoptaremos el lenguaje de reticulados de aquí en adelante.

En lo que resta de la sección, asumimos que k es un cuerpo local y D es un álgebra de cuaterniones de división sobre k . En este caso, podemos definir un valor absoluto discreto $|\bullet|$ en D mediante $q \mapsto |N(q)|_k$. Denotamos por \mathcal{O}_D al único orden maximal en D (ver §2.6).

Definición 2.5.4. Para un \mathcal{O}_D -reticulado Λ en un espacio anti-hermitiano (V, h) y un vector $s \in \Lambda$, se define la *altura de s* en Λ como

$$S(s) = \max_{b \in \Lambda} |h(s, b)|.$$

³Recordemos que $D_p := D \otimes_k k_p$ y $\mathcal{O}_{D_p} := \mathcal{O}_D \otimes_{\mathcal{O}_k} \mathcal{O}_{k_p}$.

También definimos la *altura* de Λ por

$$S(\Lambda) = \max_{s \in \Lambda} S(s).$$

Definición 2.5.5. Para un \mathcal{O}_D -reticulado Λ tal que $S(\Lambda) = |q|$, definimos la *escala* de Λ como el ideal⁴ $s(\Lambda) = (q)$.

Utilizando el concepto de altura de un vector se puede probar [2, §5] que un \mathcal{O}_D -reticulado Λ en un espacio anti-hermitiano (V, h) tiene una descomposición del tipo

$$\Lambda = \Lambda_1 \perp \cdots \perp \Lambda_t,$$

donde cada reticulado Λ_r tiene rango 1 o 2, y las escalas satisfacen $s(\Lambda_{r+1}) \subset s(\Lambda_r)$.

Definición 2.5.6. Un reticulado es *modular* si es suma ortogonal de reticulados indescomponibles de igual escala. Un reticulado modular es *unimodular* si su escala es (1) y *primo-modular* si su escala es (i).

Para $c \in k^*$ y una forma anti-hermitiana h , diremos que la forma ch es un reescalamiento de h . Así, cualquier reticulado modular es un reescalamiento de un reticulado unimodular o primo-modular.

2.6. Aritmética en $D = \left(\frac{\pi, \Delta}{k}\right)$.

De aquí en adelante, trabajaremos con $D = \left(\frac{\pi, \Delta}{k}\right)$, donde k es un cuerpo local diádico de característica 0, y cuya base es $\{1, i, j, ij\}$, donde

$$i^2 = \pi, \quad j^2 = \Delta, \quad ij = -ji.$$

Se define un valor absoluto discreto $|\bullet| : D \rightarrow \mathbb{R}^+$ en D mediante $|q| := |N(q)|_k$ [15, §2]. Denotamos por ν la valuación discreta en D , definida por $\nu(q) := \log_{|i|} |q|$. Sea \mathcal{O}_D el único orden maximal en D .

⁴Recordemos que todo ideal fraccional de D es de la forma

$$(q) = q\mathcal{O}_D = \mathcal{O}_D q = \{q' \in D \mid |q'| \leq |q|\},$$

para algún $q \in D$ [15].

Es claro que $D = K \oplus iK$, como K -espacios vectoriales, donde $K = k(j)$. Además, la norma reducida satisface $N(\lambda_1 + i\lambda_2) = N(\lambda_1) - \pi N(\lambda_2)$ para todo $\lambda_1, \lambda_2 \in K$, pues $i\lambda i^{-1} = \bar{\lambda}$ para todo $\lambda \in K$.

Lema 2.6.1. $\nu(\lambda)$ es par, para todo $\lambda \in K$.

Demostración: Sea $\lambda \in K$, es decir, $\lambda = a + bj$, con $a, b \in k$. En este caso, $N(\lambda) = a^2 - \Delta b^2$. Supongamos que $\nu(\lambda)$ es impar. Entonces $a^2 - \Delta b^2 = u\pi^{2t+1}$, donde $u \in \mathcal{O}_k^*$ y $t \in \mathbb{Z}$. Luego $(a/\pi^t)^2 - \Delta(b/\pi^t)^2 = u\pi$. Como las unidades de k son normas de K y la norma es multiplicativa obtenemos que $\pi \in N(k(j))$, lo cual no puede suceder ya que $\left(\frac{\pi, \Delta}{p}\right) = -1$ (§2.3). Por lo tanto, $\nu(\lambda)$ es par, para todo $\lambda \in K$. \square

El anillo \mathcal{O}_D es el conjunto de elementos de norma entera en D [15, §2], es decir, $\mathcal{O}_D = \{q \in D \mid |q| \leq 1\}$.

Lema 2.6.2. $\mathcal{O}_D = \mathcal{O}_K \oplus i\mathcal{O}_K$.

Demostración: Es claro que $\mathcal{O}_K \oplus i\mathcal{O}_K \subset \mathcal{O}_D$. Para probar la otra contención, consideramos $\lambda = \lambda_1 + i\lambda_2 \in \mathcal{O}_D$, donde $\lambda_1, \lambda_2 \in K$. Tenemos que $|\lambda_1 + i\lambda_2| = |N(\lambda_1 + i\lambda_2)|_k = |N(\lambda_1) - \pi N(\lambda_2)|_k = \max\{|N(\lambda_1)|_k, |\pi N(\lambda_2)|_k\}$, siendo la última igualdad debido a que $\nu(\lambda)$ es par para todo $\lambda \in K$. De lo anterior $|\lambda_1|, |i\lambda_2| \leq 1$. Luego, usando nuevamente la paridad de $\nu(\lambda_2)$, se tiene que $|\lambda_2| \leq 1$. Así, $\lambda_1, \lambda_2 \in \mathcal{O}_K$ lo que demuestra la otra inclusión. \square

Observación 2.6.1. \mathcal{O}_D es un anillo local principal⁵ con parámetro uniformizante i e ideal maximal $\mathcal{M}_D = \mathcal{M}_K \oplus i\mathcal{O}_K$, donde \mathcal{M}_K es el ideal maximal de \mathcal{O}_K .

Lema 2.6.3. $\mathcal{O}_K = \mathcal{O}_k[\omega]$, donde $\omega = \frac{i+1}{2}$.

Demostración: $\mathcal{O}_k[\omega] \subset \mathcal{O}_K$ pues ω es raíz del polinomio $x^2 - x - \delta$, donde $\delta \in \mathcal{O}_k^*$ satisface $\Delta = 1 + 4\delta$. Por otra parte, para $a, b \in k$, se tiene que $a + bj \in \mathcal{O}_K$ si y sólo si $N(a + bj) = a^2 - \Delta b^2 \in \mathcal{O}_k$ y $T(a + bj) = 2a \in \mathcal{O}_k$, pues el polinomio

⁵Un anillo local cuyo ideal maximal es principal.

irreducible de $a + bj$ en $k[x]$ es $x^2 - 2ax + (a^2 - \Delta b^2)$. Ahora, si $a^2 - \Delta b^2 \in \mathcal{O}_k$ y $2a \in \mathcal{O}_k$, es fácil ver que $2b \in \mathcal{O}_k$. De aquí y del hecho de que $\Delta = 1 + 4\delta$, $\delta \in \mathcal{O}_k^*$, se tiene que $a^2 - b^2 = (a - b)(a + b) \in \mathcal{O}_k$. Luego $a - b$ o $a + b$ pertenece a \mathcal{O}_k . Como $2b \in \mathcal{O}_k$, en cualquier caso se obtiene que $a - b \in \mathcal{O}_k$. Esto concluye la demostración ya que $a + bj = (a - b) + 2b\omega \in \mathcal{O}_k[\omega]$. \square

Debido a los lemas anteriores, podemos escribir $\mathcal{O}_D = \mathcal{O}_k \oplus \mathcal{O}_k \cdot \omega \oplus \mathcal{O}_k \cdot i \oplus \mathcal{O}_k \cdot i\omega$, es decir, $\{1, \omega, i, i\omega\}$ es una base de \mathcal{O}_D . Por otra parte, como

$$i\mathcal{O}_D = \pi\mathcal{O}_k \oplus \pi\mathcal{O}_k\omega \oplus \mathcal{O}_k i \oplus \mathcal{O}_k i\omega,$$

se tiene que

$$\mathcal{O}_D/i\mathcal{O}_D \cong \mathbb{F}_k \oplus \mathbb{F}_k\tilde{\omega},$$

donde $\mathbb{F}_k = \mathcal{O}_k/\pi\mathcal{O}_k$ es el cuerpo residual de k y $\tilde{\omega}$ es la clase de ω módulo i . En general se tiene:

$$\mathcal{O}_D/i^t\mathcal{O}_D \cong \begin{cases} (\mathcal{O}_k/\pi^s\mathcal{O}_k) \oplus (\mathcal{O}_k/\pi^s\mathcal{O}_k)\tilde{\omega} \oplus (\mathcal{O}_k/\pi^s\mathcal{O}_k)\tilde{i} \oplus (\mathcal{O}_k/\pi^s\mathcal{O}_k)\tilde{i}\tilde{\omega} & , t = 2s \text{ par.} \\ (\mathcal{O}_k/\pi^{s+1}\mathcal{O}_k) \oplus (\mathcal{O}_k/\pi^{s+1}\mathcal{O}_k)\tilde{\omega} \oplus (\mathcal{O}_k/\pi^s\mathcal{O}_k)\tilde{i} \oplus (\mathcal{O}_k/\pi^s\mathcal{O}_k)\tilde{i}\tilde{\omega} & , t = 2s + 1 \text{ impar.} \end{cases}$$

Aquí, $\tilde{\omega}$ e \tilde{i} son las clases módulo i^t , de ω e i respectivamente.

Ejemplo 2.6.1. Si $k = \mathbb{Q}_2$, entonces:

$$\mathcal{O}_k = \mathbb{Z}_2,$$

$$\mathcal{O}_D = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \cdot \omega \oplus \mathbb{Z}_2 \cdot i \oplus \mathbb{Z}_2 \cdot i\omega, \text{ e}$$

$$i\mathcal{O}_D = \pi\mathbb{Z}_2 \oplus \pi\mathbb{Z}_2 \cdot \omega \oplus \mathbb{Z}_2 \cdot i \oplus \mathbb{Z}_2 i\omega = 2\mathbb{Z}_2 \oplus 2\mathbb{Z}_2 \cdot \omega \oplus \mathbb{Z}_2 \cdot i \oplus \mathbb{Z}_2 i\omega \text{ ya que } \pi = 2 \cdot u, \text{ con } u \in \mathbb{Z}_2^*.$$

Así, como $\mathbb{Z}_2/2^t\mathbb{Z}_2 \cong \mathbb{Z}/2^t\mathbb{Z}$ para $t \geq 0$, se tiene:

$$\mathcal{O}_D/i^t\mathcal{O}_D \cong \begin{cases} (\mathbb{Z}/2^s\mathbb{Z}) \oplus (\mathbb{Z}/2^s\mathbb{Z})\tilde{\omega} \oplus (\mathbb{Z}/2^s\mathbb{Z})\tilde{i} \oplus (\mathbb{Z}/2^s\mathbb{Z})\tilde{i}\tilde{\omega} & , t = 2s \text{ par.} \\ (\mathbb{Z}/2^{s+1}\mathbb{Z}) \oplus (\mathbb{Z}/2^{s+1}\mathbb{Z})\tilde{\omega} \oplus (\mathbb{Z}/2^s\mathbb{Z})\tilde{i} \oplus (\mathbb{Z}/2^s\mathbb{Z})\tilde{i}\tilde{\omega} & , t = 2s + 1 \text{ impar.} \end{cases}$$

Observación 2.6.2. Si $\alpha = a + b\omega + ci + di\omega \in \mathcal{O}_D$, entonces $T(\alpha) = 2a + b$ y $N(\alpha) = a^2 + ab - \delta b^2 - \pi(c^2 + cd - \delta d^2)$, donde $\delta \in \mathcal{O}_k^*$ es tal que $\Delta = 1 + 4\delta$.

Finalizamos la sección con un resultado que usaremos con frecuencia en nues-

tros cálculos posteriores y que es consecuencia del Teorema de Cuadrados Locales (Teorema 2.2.1).

Lema 2.6.4. *Si $\alpha \in \mathcal{O}_D$ satisface $|\alpha| < 1$, entonces $N(1 + 4\alpha)$ es un cuadrado.*

Demostración: $N(1 + 4\alpha) = 1 + 4T(\alpha) + 16N(\alpha) = 1 + 4(T(\alpha) + 4N(\alpha))$. La condición $|\alpha| < 1$ implica que $\pi|T(\alpha)$. Por lo tanto, el resultado se sigue del Teorema de Cuadrados Locales 2.2.1. \square

2.7. Cohomología

Cohomología no-conmutativa

Sea G un grupo que actúa sobre un conjunto A por la izquierda. La acción de un elemento $s \in G$ sobre un elemento $a \in A$ será denotada por $a \mapsto {}^s a$. Diremos que un conjunto es un G -conjunto si G actúa sobre él. Si el G -conjunto A posee estructura de grupo y ésta es respetada por G , diremos que A es un G -grupo.

Definición 2.7.1. Sea A un G -conjunto. Definimos $H^0(G, A)$ como el subconjunto A^G de elementos de A que permanecen fijos bajo la acción de G , es decir,

$$H^0(G, A) = A^G = \{a \in A \mid {}^s a = a \forall s \in G\}.$$

La definición de $H^1(G, A)$ será dada sólo para un G -grupo A .

Definición 2.7.2. Sea A un G -grupo. Diremos que una función $f : G \rightarrow A$ es un 1-cociclo de G en A si $f(st) = f(s) {}^s f(t)$ para todo $s, t \in G$. Denotaremos la imagen por la función f de un elemento $s \in G$ por f_s y hablaremos del 1-cociclo (f_s) . Así, la ecuación que define a un 1-cociclo (f_s) se escribe como $f_{st} = f_s {}^s f_t$. Diremos que dos cociclos (a_s) y (b_s) son equivalentes si existe un elemento $c \in A$ tal que $b_s = c^{-1} a_s {}^s c$ para todo $s \in G$. Esto define una relación de equivalencia en el conjunto de 1-cociclos de G en A . Definimos $H^1(G, A)$ como el conjunto de clases de equivalencia de 1-cociclos, es decir,

$$H^1(G, A) = \{f : G \rightarrow A \mid f_{st} = f_s {}^s f_t \forall s, t \in G\} / \sim.$$

Notemos que en general, $H^1(G, A)$ no posee una estructura natural de grupo y es solamente un conjunto punteado cuyo elemento distinguido es la clase de equivalencia del cociclo neutro $s \mapsto e_A$, donde e_A es el neutro del grupo A . Si A es un subgrupo del G -grupo B , invariante bajo la acción de G , entonces hay una acción natural de G en el conjunto de clases laterales izquierdas B/A , con lo que B/A es un G -conjunto y podemos definir $H^0(G, B/A)$. Se tiene la siguiente sucesión exacta⁶ larga:

$$1 \rightarrow A^G \rightarrow B^G \rightarrow (B/A)^G \rightarrow H^1(G, A) \rightarrow H^1(G, B),$$

donde la función coborde $\delta : (B/A)^G \rightarrow H^1(G, A)$ esta dada por $\delta(bA)_s = b^{-1} \cdot {}^s b$.

Observación 2.7.1. Si A es normal en B , se puede extender la sucesión exacta larga precedente a:

$$1 \rightarrow A^G \rightarrow B^G \rightarrow (B/A)^G \rightarrow H^1(G, A) \rightarrow H^1(G, B) \rightarrow H^1(G, B/A).$$

Cohomología galoisiana

Aplicamos la teoría de cohomología no-conmutativa al caso que nos interesa. En efecto, sea A una variedad algebraica definida sobre un cuerpo k . Sea K/k una extensión galoisiana (finita o infinita). Si A_K denota el conjunto de K -puntos de A , el grupo de Galois $\mathcal{G} = Gal(K/k)$ actúa sobre A_K . Nos concentramos aquí, en el caso en que A_K es un grupo lineal algebraico y $K = \bar{k}$.

Ejemplo 2.7.1. Sea μ_n el grupo de raíces n -ésimas de la unidad y supongamos que⁷ $\mu_n \subset k$. La sucesión exacta corta

$$1 \rightarrow \mu_n \rightarrow \bar{k}^* \xrightarrow{(\cdot)^n} \bar{k}^* \rightarrow 1,$$

da origen a la sucesión exacta larga

$$1 \rightarrow \mu_n \rightarrow k^* \rightarrow k^* \rightarrow H^1(\mathcal{G}, \mu_n) \rightarrow H^1(\mathcal{G}, \bar{k}^*).$$

⁶Una sucesión de conjuntos punteados es exacta si la preimagen del elemento distinguido es igual a la imagen de la función anterior. Aquí, el elemento distinguido del conjunto $H^0(G, B/A)$ es la clase A .

⁷Si esto no se cumple hay que reemplazar μ_n por $\mu_n \cap k^*$ en la sucesión exacta larga.

Por el Teorema 90 de Hilbert $H^1(\mathcal{G}, \bar{k}^*) = \{1\}$, por lo tanto,

$$H^1(\mathcal{G}, \mu_n) \cong k^*/k^{*n}.$$

2.8. Norma espinorial

Utilizaremos cohomología galoisiana, en el caso en que la variedad algebraica en cuestión es el grupo unitario de una forma anti-hermitiana cuaterniónica, para definir una función coborde (norma espinorial) mediante la cual se pueden clasificar formas anti-hermitianas enteras (\mathcal{O}_D -reticulados) como veremos en la próxima sección.

Sea D un álgebra de cuaterniones de división sobre un cuerpo de números k y sea \mathcal{O}_D un orden maximal. Sea (V, h) un espacio anti-hermitiano y sea Λ un \mathcal{O}_D -reticulado en V . Para cualquier extensión de cuerpos E de k y cualquier grupo algebraico G , denotamos por G_E el conjunto de E -puntos de G . El estabilizador de Λ en \mathcal{U}_k^+ es denotado $\mathcal{U}_k^+(\Lambda)$. Sea μ_2 el grupo $\{1, -1\}$ de raíces cuadradas de la unidad. Sea $\widetilde{\mathcal{U}}_k^+$ el cubrimiento universal de \mathcal{U}_k^+ . La sucesión exacta⁸

$$\{1\} \longrightarrow \mu_2 \longrightarrow \widetilde{\mathcal{U}}_k^+ \longrightarrow \mathcal{U}_k^+ \longrightarrow \{1\},$$

sobre la clausura algebraica \bar{k} de k , da origen a la función coborde $\theta : \mathcal{U}_k^+ \rightarrow H^1(\mathcal{G}, \mu_2) \cong k^*/k^{*2}$, donde $\mathcal{G} = \text{Gal}(\bar{k}/k)$ (§2.7). La función θ es llamada *norma espinorial*⁹. Como en [6], definimos $H(\Lambda) \subset k^*$ por la relación

$$H(\Lambda)/k^{*2} = \theta(\mathcal{U}_k^+(\Lambda)).$$

⁸Un 2-recubrimiento universal en particular es dado por el grupo de spin para formas anti-hermitianas definido en [13].

⁹En [16] se define la norma espinorial sobre el grupo unitario U de una forma sesquilineal sobre un D -módulo derecho, donde D es un anillo de división. Esto se lleva a cabo en términos de la factorización completa de un elemento $P \in U$ como producto de elementos de dimensión 1, de manera análoga a la definición para el grupo ortogonal O de una forma cuadrática, donde se puede definir la norma espinorial para $\sigma \in O$ en términos de la factorización de σ como producto de simetrías (ver, por ejemplo [10, §55]). Se puede probar que la definición cohomológica (para k p-ádico) nos entrega la misma información en el caso anti-hermitiano cuaterniónico, a pesar de que en nuestro caso la norma espinorial tiene como codominio k^*/k^{*2} , mientras que en [16] la norma espinorial tiene como codominio D^*/Γ , para cierto subgrupo Γ de D^* .

Por abuso de lenguaje diremos que $H(\Lambda)$ es la imagen de la norma espinorial. También tenemos una norma espinorial local $\theta_p : \mathcal{U}_{k_p}^+(\Lambda) \rightarrow k_p^*/k_p^{*2}$ para cualquier lugar p . Es sabido [11, Lema 13] que la sucesión

$$\prod_{p \in \Pi(k)} \widetilde{\mathcal{U}}_{k_p}^+ \rightarrow \prod_{p \in \Pi(k)} \mathcal{U}_{k_p}^+ \xrightarrow{\prod_p \theta_p} \prod_{p \in \Pi(k)} k_p^*/k_p^{*2},$$

donde $\Pi(k)$ es el conjunto de lugares (arquimedianos y no-arquimedianos) de k , puede ser restringida al conjunto de puntos adélicos para obtener una sucesión

$$\widetilde{\mathcal{U}}_{\mathbb{A}}^+ \rightarrow \mathcal{U}_{\mathbb{A}}^+ \xrightarrow{\Theta_{\mathbb{A}}} J_k/J_k^2,$$

donde $J_k = (GL_1)_{\mathbb{A}}$ es el grupo de ideles de k .

2.9. Clasificación de formas anti-hermitianas cuaterniónicas enteras

Consideremos una forma anti-hermitiana h sobre un álgebra de cuaterniones de división sobre un cuerpo de números k . Para estudiar el problema de clasificación entera adoptaremos el lenguaje de reticulados (ver §2.5). Como en la sección anterior denotamos por $\mathcal{U}_k^+(\Lambda)$ al estabilizador del reticulado Λ . Denotamos por $\mathcal{U}_{\mathbb{A}}^+$ al grupo unitario adélico. Se define la acción de $\phi \in \mathcal{U}_{\mathbb{A}}^+$ mediante $\Lambda \mapsto \phi\Lambda$, donde $\phi\Lambda$ está definido por las relaciones locales $(\phi\Lambda)_p = \phi_p\Lambda_p$. Nótese que la clase de Λ es la órbita $\mathcal{U}_k^+.\Lambda$, donde $\mathcal{U}_k^+ \subset \mathcal{U}_{\mathbb{A}}^+$ por la incrustación diagonal. Definimos el género de Λ como la órbita $\mathcal{U}_{\mathbb{A}}^+.\Lambda$ y el género espinorial como la órbita $\mathcal{U}_k^+\mathcal{U}_{\mathbb{A}}^+.\Lambda$, donde $\mathcal{U}_{\mathbb{A}}^+$ es el núcleo de la función $\Theta_{\mathbb{A}}$ definida en la sección precedente. El conjunto de clases contenidas en un género, está en correspondencia 1 a 1 con el conjunto de clases laterales dobles

$$\mathcal{U}_k^+ \backslash \mathcal{U}_{\mathbb{A}}^+ / \mathcal{U}_{\mathbb{A}}^+(\Lambda).$$

El número de elementos del conjunto $\mathcal{U}_k^+ \backslash \mathcal{U}_{\mathbb{A}}^+ / \mathcal{U}_{\mathbb{A}}^+(\Lambda)$ es llamado el *número de clases* del reticulado Λ . Dicha cantidad es difícil de conocer en general, aunque se sabe que es finita. Un problema más fácil que el anterior es conocer el número de géneros espinoriales en un género. De hecho, éste número es igual al orden del grupo abeliano

finito

$$\Theta_{\mathbb{A}}(\mathcal{U}_{\mathbb{A}}^+)/(\theta(\mathcal{U}_k^+)\Theta_{\mathbb{A}}(\mathcal{U}_{\mathbb{A}}^+(\Lambda))).$$

Más aún, si denotamos por $P : J_k \rightarrow J_k/J_k^2$ a la proyección canónica y por $H_{\mathbb{A}}(\Lambda)$ al conjunto

$$H_{\mathbb{A}}(\Lambda) = P^{-1}(\Theta_{\mathbb{A}}(\mathcal{U}_{\mathbb{A}}^+(\Lambda))),$$

se tiene el siguiente isomorfismo de grupos

$$\Theta_{\mathbb{A}}(\mathcal{U}_{\mathbb{A}}^+)/(\theta(\mathcal{U}_k^+)\Theta_{\mathbb{A}}(\mathcal{U}_{\mathbb{A}}^+(\Lambda))) \cong J_k/k^*H_{\mathbb{A}}(\Lambda),$$

donde es claro que el grupo de la derecha depende de las imágenes de la norma espinorial local $\theta_{\mathfrak{p}} : \mathcal{U}_{k_{\mathfrak{p}}}^+(\Lambda) \rightarrow k_{\mathfrak{p}}^*/k_{\mathfrak{p}}^{*2}$ en cada lugar \mathfrak{p} del cuerpo de números k . En algunos casos (ver diagrama abajo) el número de clases de un reticulado Λ es igual al número de géneros espinoriales en el género de Λ . Por lo dicho anteriormente es que nos interesa calcular la imagen de la norma espinorial. En esta tesis completamos los cálculos de la norma espinorial local para el cuerpo \mathbb{Q}_2 y avanzamos los cálculos para un cuerpo local diádico cualquiera k .

$$\begin{array}{l} \text{gen}(\Lambda) = \mathcal{U}_{\mathbb{A}}^+.\Lambda \\ | \\ \text{spn}(\Lambda) = \mathcal{U}_k^+\mathcal{U}_{\mathbb{A}}^+.\Lambda \\ || \quad \text{Si } \mathcal{U}_k^+ \text{ es no compacto en algún lugar arquimediano.} \\ \text{cls}(\Lambda) = \mathcal{U}_k^+.\Lambda \end{array}$$

Capítulo 3

Sobre $H(\Lambda)$

Los cálculos mostrados en las tablas 1.1 y 1.2 del capítulo 1 fueron extraídos de [2] y [4]. Gracias a la Proposición 3.3.1 de este capítulo la tabla 1.2 del capítulo 1 quedará:

s	$ A $	α	μ	$H(\Lambda)$
$-$	> 1	$-$	$-$	k^*
0	1	$-\tilde{\Delta}$	$-$	$\mathcal{O}_k^* k^{*2}$
0	1	$-\tilde{u}, \tilde{\pi}$	$\mu > \nu(16)$	$N(k(a_m)^*)$
0	1	$-\tilde{u}$	$0 < \mu \leq \nu(16)$	$?$
0	1	$\tilde{\pi}$	$\mu \leq \nu(4)$	k^*
0	1	$\tilde{\pi}$	$\nu(4) < \mu \leq \nu(16)$	$?$
$\neq 0$	$-$	$-$	$-$	k^*

Los casos restantes se calcularán sólo en el caso $k = \mathbb{Q}_2$. En este capítulo describimos de manera precisa un conjunto de generadores para $\mathcal{U}_k^+(\Lambda)$, proveemos los elementos básicos para el estudio de $H(\Lambda)$ y obtenemos algunos resultados que nos simplificarán dicho estudio en los capítulos siguientes.

3.1. Generadores de $\mathcal{U}_k^+(\Lambda)$ y su norma espinorial

La norma espinorial $\theta : \mathcal{U}_k^+(\Lambda) \rightarrow k^*/k^{*2}$ es un homomorfismo. Así, basta conocer θ en los generadores de $\mathcal{U}_k^+(\Lambda)$. En esta sección mostramos un conjunto de generadores

y cómo se calcula la norma espinorial para dichos generadores. Recordemos que $H(\Lambda)$ está definido mediante la ecuación $H(\Lambda)/k^{*2} = \theta(\mathcal{U}_k^+(\Lambda))$ y decimos, por abuso de lenguaje, que $H(\Lambda)$ es la imagen de la norma espinorial.

Sea (V, h) un espacio anti-hermitiano y sean $s \in V$, $\sigma \in D^*$, tales que $\sigma - \bar{\sigma} = h(s, s)$. Se define la función $(s; \sigma) : V \rightarrow V$ mediante

$$(s; \sigma)(x) = x - h(x, s)\sigma^{-1}s.$$

Llamaremos a tales funciones *rotaciones simples* con eje de rotación s . Las rotaciones simples generan \mathcal{U}_k^+ y satisfacen

$$\theta[(s; \sigma)] = N(\sigma)k^{*2} \quad [13],$$

donde $N : D^* \rightarrow k^*$ es la norma reducida (§2.1). Notar que $\sigma \in k(a)$, donde $a = h(s, s)$.

En [2, §6] se prueban los dos lemas siguientes. El primero nos dice como construir rotaciones simples y es usado en el segundo para obtener un conjunto de generadores de $\mathcal{U}_k^+(\Lambda)$.

Lema 3.1.1. [2, §6, Lema 6.3] *Sea (V, h) un espacio anti-hermitiano, y sean $t, u \in V$ tales que $h(u, u) = h(t, t) = a$. Definimos r y t_0 por $u = rt + t_0$, donde $t_0 \in t^\perp$. Sean $s = t - u$ y $\sigma = h(t, s)$. Entonces se tienen las siguientes identidades:*

$$\sigma = a(1 - \bar{r}), \quad h(t_0, t_0) = a - ra\bar{r}, \quad \sigma - \bar{\sigma} = h(s, s).$$

En particular $(s; \sigma)$ define una rotación simple tal que $(s; \sigma)(t) = u$.

Observación 3.1.1. Si $\phi \in \mathcal{U}_k^+$, se tiene que $h(\phi(t), \phi(t)) = h(t, t)$, y el Lema anterior nos dice que existe una rotación simple $(s; \sigma)$ tal que $(s; \sigma)(t) = \phi(t)$. Este hecho permite realizar un proceso inductivo para probar el Lema siguiente.

Lema 3.1.2. [2, §6, Lema 6.7] *Sea $\Lambda = \langle a_1 \rangle \perp \cdots \perp \langle a_n \rangle = \mathcal{O}_D s_1 \perp \cdots \perp \mathcal{O}_D s_n$, un \mathcal{O}_D -reticulado anti-hermitiano, donde $a_m = h(s_m, s_m)$, para $m = 1, \dots, n$ y $|2a_m| \geq |a_l|$ para $m < l$. Entonces el grupo unitario $\mathcal{U}_k^+(\Lambda)$ del reticulado es generado por elementos de los siguientes tipos :*

A) Rotaciones simples con eje s_m , $m = 1, \dots, n$.

B) Rotaciones simples de la forma $(s; \sigma)$, donde $\sigma = a_m(1 - \bar{r})$, $s = (1 - r)s_m - s_0$, para algún $s_0 \in \mathcal{O}_D s_{m+1} \perp \dots \perp \mathcal{O}_D s_n$ y algún $r \in \mathcal{O}_D$. De hecho, basta considerar las rotaciones que satisfacen $1 - r \notin (2i)$.

Definición 3.1.1. Sea Λ como en el Lema. Denotaremos por $\mathcal{A}(\Lambda)$ al conjunto de rotaciones simples de tipo (A) y por $\mathcal{B}(\Lambda)$ al conjunto de rotaciones simples de tipo (B) tales que $|1 - r| \geq |2|$, es decir, tales que $1 - r \notin (2i)$. Así, $\mathcal{U}_k^+(\Lambda)$ está generado por el conjunto $\mathcal{A}(\Lambda) \cup \mathcal{B}(\Lambda)$.

Observación 3.1.2. Las rotaciones simples $(s_m; \sigma) \in \mathcal{A}(\Lambda)$ tienen norma espinorial $\theta[(s; \sigma)] = N(\sigma)k^{*2} \subset N(k(a_m)^*)$, pues $\sigma \in k(a_m)$.

3.2. Hechos generales para el cálculo de $H(\Lambda)$

Recordemos que un reticulado anti-hermitiano Λ sobre un álgebra de cuaterniones de división sobre un cuerpo local, tiene una descomposición ortogonal del tipo

$$\Lambda = \Lambda_1 \perp \dots \perp \Lambda_n,$$

donde Λ_i es un reticulado irreducible de rango 1 o 2 y las escalas satisfacen $\mathfrak{s}(\Lambda_{i+1}) \subset \mathfrak{s}(\Lambda_i)$. En [4] se probó que $H(\Lambda) = k^*$ para cualquier reticulado Λ irreducible de rango 2. Por lo tanto, como $H(\Lambda_i) \subset H(\Lambda)$ para cualquier Λ_i que descompone Λ , los únicos reticulados a considerar serán reticulados diagonalizables, es decir, reticulados cuyas componentes irreducibles en la descomposición ortogonal de arriba tienen rango 1. Sabemos que, si $\Lambda = \langle a_1 \rangle \perp \dots \perp \langle a_n \rangle$ es un \mathcal{O}_D -reticulado anti-hermitiano, entonces $[k^* : N(k(a_1)^*)] = 2$ (ver §2.3) y $N(k(a_1)^*) \subset H(\Lambda)$ [2, Proposición 6.1]. Una consecuencia directa de lo anterior es el siguiente resultado.

Proposición 3.2.1. Sea $\Lambda = \langle a_1 \rangle \perp \dots \perp \langle a_n \rangle$ un \mathcal{O}_D -reticulado anti-hermitiano. Entonces $H(\Lambda) = N(k(a_1)^*)$ ó $H(\Lambda) = k^*$.

Corolario 3.2.1.1. Sea $\Lambda = \langle a_1 \rangle \perp \dots \perp \langle a_n \rangle$ un \mathcal{O}_D -reticulado anti-hermitiano. Si existe $b \in \mathcal{O}_D$ con $N(b) \notin N(k(a_1)^*)$ tal que $\Lambda = \langle b \rangle \perp \Lambda'$, entonces $H(\Lambda) = k^*$.

Observación 3.2.1. Es inmediato del Corolario que si las normas $N(a_i), i = 1, \dots, n$ no están en la misma clase módulo cuadrados, entonces $H(\Lambda) = k^*$. Así, consideraremos sólo reticulados diagonalizables tales que las normas de los representantes a_i de cada componente estén en la misma clase módulo cuadrados.

Corolario 3.2.1.2. Sea $\Lambda = \langle a_1 \rangle \perp \dots \perp \langle a_n \rangle$ un \mathcal{O}_D -reticulado anti-hermitiano. Entonces $H(\Lambda) = k^*$ si y sólo si, existe $\phi \in \mathcal{U}_k^+(\Lambda)$ tal que $\theta(\phi) \notin N(k(a_1)^*)$.

Observación 3.2.2. Supongamos que $\phi \in \mathcal{U}_k^+(\Lambda)$ satisface $\theta(\phi) \notin N(k(a_1)^*)$. Sabemos que $\phi = \tau_1 \tau_2 \cdots \tau_r$, donde los τ_i , con $i = 1, \dots, r$, son rotaciones generadoras en $\mathcal{A}(\Lambda) \cup \mathcal{B}(\Lambda)$. Luego, como la norma espinorial es un homomorfismo, podemos asumir que existe una rotación simple $\tau_k = (s; \sigma) \in \mathcal{B}(\Lambda)$ tal que $\theta[(s; \sigma)] \notin N(k(a_1)^*)$ pues, por la observación 3.1.2, las rotaciones en $\mathcal{A}(\Lambda)$ tienen norma espinorial en $N(k(a_1)^*)$. Por lo tanto $H(\Lambda) = k^*$ si y sólo si, existe una rotación simple $(s; \sigma) \in \mathcal{B}(\Lambda)$ tal que $\theta[(s; \sigma)] \notin N(k(a_1)^*)$. Es claro que la afirmación anterior sigue siendo válida si cambiamos $\mathcal{B}(\Lambda)$ por un conjunto $\mathcal{B}'(\Lambda)$ tal que $\mathcal{A}(\Lambda) \cup \mathcal{B}'(\Lambda)$ genera $\mathcal{U}_k^+(\Lambda)$.

Con los resultados previos en mente, el plan es el siguiente:

1. Crear un algoritmo para buscar rotaciones en $\mathcal{B}(\Lambda)$ de norma espinorial apropiada de modo que $H(\Lambda) = k^*$ para un reticulado Λ de rango pequeño t . Esto implicaría que $H(\Lambda) = k^*$ para cualquier reticulado Λ de rango mayor o igual que t , pues si $\Lambda = \Lambda_1 \perp \Lambda_2$, entonces $H(\Lambda_i) \subset H(\Lambda)$, para $i = 1, 2$.
2. En caso de no encontrar las rotaciones buscadas en el punto 1, probar que el algoritmo efectivamente demuestra que $H(\Lambda) = N(k(a_1)^*)$ para un reticulado Λ de rango t .
3. Probar que para cualquier reticulado Λ (de rango arbitrario ≥ 2) y cualquier rotación generadora $\phi \in \mathcal{B}(\Lambda)$, existe un subreticulado Λ' de rango t que queda fijo por ϕ tal que $H(\Lambda') = N(k(a_1)^*)$. Con este resultado, bastaría calcular $H(\Lambda)$ para reticulados de rango t (pequeño).

3.3. Resultados

El siguiente resultado nos permitirá reducir, en algunos casos, el cálculo de $H(\Lambda)$ al caso en que Λ es de rango pequeño, hecho que es de gran ayuda si se quiere hacer

un cálculo algorítmico. Recordemos que para un reticulado Λ , se define $\mu = \mu(\Lambda)$ como la diferencia minimal entre la valuación de las escalas de dos componentes consecutivos de rango 1.

Lema 3.3.1. *Sea $\Lambda = \langle a_1 \rangle \perp \cdots \perp \langle a_n \rangle = \mathcal{O}_D s_1 \perp \cdots \perp \mathcal{O}_D s_n$ un \mathcal{O}_D -reticulado anti-hermitiano tal que $a_m = h(s_m, s_m)$, para $m = 1, \dots, n$, $\mu > \nu(4)$ y $N(a_2), \dots, N(a_n) \in N(a_1)k^{*2}$. Sea $(s; \sigma) \in \mathcal{B}(\Lambda)$, es decir, $s = (1 - r)s_m - s_0$, donde $s_0 = \lambda_{m+1}s_{m+1} + \cdots + \lambda_n s_n \in \mathcal{O}_D s_{m+1} \perp \cdots \perp \mathcal{O}_D s_n$, $\sigma = a_m(1 - \bar{r})$ y $|1 - \bar{r}| \geq |2|$. Si $|\lambda_{m+t}| \geq |\lambda_{m+t+i}|$, para algún $t \in \{1, \dots, n - m\}$ y para todo $l \in \{1, \dots, n - m - t\}$, existe $\Lambda' = \langle b_1 \rangle \perp \cdots \perp \langle b_{t+1} \rangle \subset \Lambda$ tal que:*

1. $(s; \sigma) \in \mathcal{U}_k^+(\Lambda')$.
2. $\mu(\Lambda') \geq \mu(\Lambda)$.
3. $N(b_i) \in N(a_1)k^{*2}$, para todo $i = 1, \dots, t + 1$.

Demostración: Sea $\Lambda' = \mathcal{O}_D s_m \perp \cdots \perp \mathcal{O}_D s_{m+t-1} \perp \mathcal{O}_D s'_0 = \langle b_1 \rangle \perp \cdots \perp \langle b_{t+1} \rangle$, donde $s'_0 = \lambda_{m+t}s_{m+t} + \cdots + \lambda_n s_n$, $b_i = h(s_{m+i-1}, s_{m+i-1}) = a_{m+i-1}$, para $i = 1, \dots, t$ y $b_{t+1} = h(s'_0, s'_0)$. Es claro que $\Lambda' \subset \Lambda$. Ahora, para probar 1 notamos que $s_0 = s'_0 - (\lambda_{m+1}s_{m+1} + \cdots + \lambda_{m+t-1}s_{m+t-1}) \in \Lambda'$ y calculamos,

$$(s; \sigma)(s_m) = r s_m + s_0 \in \Lambda',$$

$$(s; \sigma)(s_i) = s_i + h(s_i, s)\sigma^{-1}s = s_i + h(s_i, s_0)\sigma^{-1}s, \text{ para } i = m + 1, \dots, m + t - 1$$

y

$$(s; \sigma)(s'_0) = s'_0 - h(s'_0, s)\sigma^{-1}s = s'_0 + h(s'_0, s_0)\sigma^{-1}s.$$

Así, $(s; \sigma)(s_i), (s; \sigma)(s'_0) \in \Lambda'$ si $h(s_i, s_0)\sigma^{-1}, h(s'_0, s_0)\sigma^{-1} \in \mathcal{O}_D$, para $i = m + 1, \dots, m + t - 1$. Esto es cierto ya que $|\sigma| = |a_m(1 - \bar{r})| \geq |2a_m| \geq \mathbb{S}(s_0), \mathbb{S}(s'_0)$. Luego, $(s; \sigma) \in \mathcal{U}_k^+(\Lambda')$. Por otra parte,

$$b_{t+1} = h(s'_0, s'_0) = \sum_{u=m+t}^n \lambda_u a_u \bar{\lambda}_u,$$

de donde se tiene que $|b_{t+1}| = |a_{m+t}||\lambda_{m+t}|^2$ ya que $|\lambda_{m+t}| \geq |\lambda_{m+t+l}|$ para todo $l \in \{1, \dots, n - m - t\}$ y $\mu(\Lambda) > \nu(4)$. De aquí, es claro que $\mu(\Lambda') \geq \mu(\Lambda)$, lo que prueba 2. Finalmente, para probar 3 consideramos

$$N(b_{t+1}) = N(\lambda_{m+t})^2 N(a_{m+t}) N \left(1 + (\lambda_{m+t} a_{m+t} \overline{\lambda_{m+t}})^{-1} \sum_{u=m+t+1}^n \lambda_u a_u \overline{\lambda_u} \right),$$

donde $|(\lambda_{m+t} a_{m+t} \overline{\lambda_{m+t}})^{-1}| = |a_{m+t}|^{-1} |\lambda_{m+t}|^{-2}$. Luego, como $|a_{m+t+l}| < |4a_{m+t}|$ y $|\lambda_{m+t}| \geq |\lambda_{m+t+l}|$ para todo $l \in \{1, \dots, n - m - t\}$, obtenemos que

$$N \left(1 + (\lambda_{m+t} a_{m+t} \overline{\lambda_{m+t}})^{-1} \sum_{u=m+t+1}^n \lambda_u a_u \overline{\lambda_u} \right)$$

es un cuadrado por el Lema 2.6.4. Por lo tanto $N(b_{t+1}) \in N(a_{m+t})k^{*2}$ lo que prueba 3. \square

El siguiente resultado nos permitirá (en el siguiente capítulo) decir que para encontrar $H(\Lambda)$, para Λ binario, basta calcular $\theta[(s; \sigma)]$ para finitos $(s; \sigma)$.

Lema 3.3.2. *Sea $\Lambda = \mathcal{O}_D s_1 \perp \mathcal{O}_D s_2 = \langle a_1 \rangle \perp \langle a_2 \rangle$ un \mathcal{O}_D -reticulado anti-hermitiano tal que $N(a_2) \in N(a_1)k^{*2}$ y $|2a_1| \geq |a_2|$. Sea $(s; \sigma) \in \mathcal{B}(\Lambda)$, de modo que, $s = (1-r)s_1 - s_0$, donde $s_0 = \lambda s_2 \in \mathcal{O}_D s_2$ y $\sigma = a_1(1-\bar{r})$. Si $(s; \sigma)$ satisface $|\lambda| \leq |4|$, entonces $\theta[(s; \sigma)] \subset N(k(a_1)^*)$.*

Demostración: En efecto, basta ver que para $a = h(s, s)$ se cumple que $N(a) \in N(a_1)k^{*2}$ pues $\sigma \in k(a)$. Tenemos que $a = (1-r)a_1(1-\bar{r}) + a_0$, donde $a_0 = h(s_0, s_0) = \lambda a_2 \bar{\lambda}$. Se sigue que

$$N(a) = N(a_1) N(1-r)^2 N(1 + (1-r)^{-1} a_0 (1-\bar{r})^{-1} a_1^{-1}). \quad (3.1)$$

Como $|a_2||a_1^{-1}| \leq |2|$, $|\lambda| \leq |4|$ y $|1-r| \geq |2|$, se tiene que $|(1-r)^{-1} a_0 (1-\bar{r})^{-1} a_1^{-1}| = |a_0||a_1^{-1}|/|1-r|^2 \leq |8| < |4|$, lo cual implica que la última norma en la ecuación 3.1 es un cuadrado en virtud del Lema 2.6.4. \square

Si queremos probar que $H(\Lambda) = k^*$, tenemos que buscar elementos de $\mathcal{B}(\Lambda)$ con norma espinorial fuera de $N(k(a_1)^*)$, donde $\Lambda = \langle a_1 \rangle \perp \Lambda'$. El siguiente resultado nos ayuda a acotar la búsqueda.

Lema 3.3.3. Sea $\Lambda = \langle a_1 \rangle \perp \dots \perp \langle a_n \rangle = \mathcal{O}_D s_1 \perp \dots \perp \mathcal{O}_D s_n$ un \mathcal{O}_D -reticulado anti-hermitiano tal que $N(a_1), \dots, N(a_n)$ están en la misma clase de cuadrados. Sea $(s; \sigma) \in \mathcal{B}(\Lambda)$, es decir, $s = (1 - r)s_m - s_0$, donde

$$s_0 = \lambda_{m+1}s_{m+1} + \dots + \lambda_n s_n \in \mathcal{O}_D s_{m+1} \perp \dots \perp \mathcal{O}_D s_n, \quad \sigma = a_m(1 - \bar{r}) \text{ y } |1 - r| \geq |2|.$$

Si se satisface cualquiera de las siguientes condiciones

1. $|1 - r| > |2|$ y $|\lambda_{m+1}| < 1$, para $\mu(\Lambda) \geq \nu(8)$, y la extensión k/\mathbb{Q}_2 es no ramificada,
2. $|1 - r| = |2|$ y $|\lambda_{m+1}| \leq |2|$, para $\mu(\Lambda) \geq \nu(4\pi)$,
3. $|1 - r| > |2|$ o $|\lambda_{m+1}| < 1$, para $\mu(\Lambda) \geq \nu(16)$,

entonces $\theta[(s; \sigma)] \subset N(k(a_1)^*)$.

Demostración: Como en el Lema anterior, basta ver que para $a = h(s, s)$ se cumple que $N(a) \in N(a_m)k^{*2}$ pues $\sigma \in k(a)$. Como $s = (1 - r)s_m - s_0$ y tenemos que $a = (1 - r)a_m(1 - \bar{r}) + a_0$, donde $a_0 = h(s_0, s_0)$. Se sigue que

$$N(a) = N(a_m)N(1 - r)^2 N(1 + (1 - r)^{-1}a_0(1 - \bar{r})^{-1}a_m^{-1}). \quad (3.2)$$

Como $s_0 = \lambda_{m+1}s_{m+1} + \dots + \lambda_n s_n$, se tiene que $a_0 = \lambda_{m+1}a_{m+1}\overline{\lambda_{m+1}} + \dots + \lambda_n a_n \overline{\lambda_n}$ y por lo tanto $|(1 - r)^{-1}a_0(1 - \bar{r})^{-1}a_m^{-1}| = |a_0||a_m^{-1}|/|1 - r|^2 < |4|$ si se cumple cualquiera de las condiciones arriba. Esto implica que la última norma en la ecuación 3.2 es un cuadrado por el Lema 2.6.4. \square

El siguiente resultado nos permitirá elegir reticulados particulares en el cálculo de $H(\Lambda)$ para reticulados Λ arbitrarios.

Lema 3.3.4. Sea $\Lambda = \langle a_1 \rangle \perp \langle a_2 \rangle$ un \mathcal{O}_D -reticulado anti-hermitiano tal que $N(a_2) \in N(a_1)k^{*2}$ y la extensión $k(a_1)/k$ es ramificada. Entonces existe un \mathcal{O}_D -reticulado anti-hermitiano $L = \langle q \rangle \perp \langle \epsilon q \rangle$, donde $q \in D^*$ y $\epsilon \in k^*$, tal que $H(\Lambda) = H(L)$. De hecho, podemos suponer $q = q'$, para cualquier cuaternión $q' \in D^*$ con $N(q') \in N(a_1)k^{*2}$.

Demostración: Como $N(a_2) = N(a_1)b^2 = N(ba_1)$ para algún $b \in k^*$ y $k(a_1)/k$ es ramificada, podemos usar el Lema 4.3 en [2] para concluir que $\langle a_1 \rangle \perp \langle a_2 \rangle \cong \langle a_1 \rangle \perp \langle \xi ba_1 \rangle$, para algún $\xi \in k^*$. Por lo tanto, basta considerar $L = \langle q \rangle \perp \langle \epsilon q \rangle$, donde $q = a_1$ y $\epsilon = \xi b$. Finalmente, sea $q' \in D^*$ con $N(q') \in N(a_1)k^{*2}$, es decir, $N(q') = N(ca_1)$ para algún $c \in k^*$. Aplicando nuevamente el Lema 4.3 en [2] con $q = a_1$ obtenemos que $q' = \eta \epsilon c q \bar{\eta}$, para algún $\epsilon \in k^*$ y $\eta \in D^*$. Así, $\Lambda' = \langle q' \rangle \perp \langle \epsilon q' \rangle$ es isométrico a un re-escalamiento de L , luego $H(\Lambda') = H(L)$. \square

Observación 3.3.1. De la demostración de la descomposición de un reticulado en suma ortogonal de reticulados de rango 1 y 2 [2, §5] se desprende que un elemento $b = h(t, t)$, $t \in \Lambda$ descompone el reticulado (es decir, $\mathcal{O}_D t$ es sumando ortogonal) si tiene valor absoluto suficientemente grande, específicamente si $|b| = \mathbb{S}(t)$. Por lo tanto, si $\Lambda = \langle a_1 \rangle \perp \dots \perp \langle a_n \rangle$, para probar que $H(\Lambda) = k^*$, podemos buscar elementos representados por Λ de norma adecuada. Usaremos este hecho para probar el siguiente resultado, el cual es una mejora de la Proposición 6.9 en [2]

Recordemos que para un reticulado Λ , $\mu = \mu(\Lambda)$ es la diferencia minimal entre la valuación (denotada por ν) de las escalas de dos componentes consecutivos de rango 1.

Proposición 3.3.1. *Si $\Lambda = \langle a_1 \rangle \perp \dots \perp \langle a_n \rangle$ es un \mathcal{O}_D -reticulado anti-hermitiano, con $N(a_1), \dots, N(a_n) \in \pi k^{*2}$, para cualquier parámetro uniformizante π y $\mu = \nu(4)$, entonces $H(\Lambda) = k^*$.*

Demostración: Basta probar el caso $n = 2$. Así, podemos asumir que $\nu(a_2) - \nu(a_1) = \nu(4)$. Por el Lema 3.3.4 podemos suponer que el reticulado $\langle a_1 \rangle \perp \langle a_2 \rangle$, es de la forma $L = \langle q \rangle \perp \langle \epsilon q \rangle$, donde $\epsilon \in k^*$ y $\nu(\epsilon) = \nu(4)$. Además, podemos asumir que q es un parámetro uniformizante y, como las unidades de k son normas de K , podemos asumir que $q \in iK$. Probaremos que $H(L) = k^*$ de donde se sigue el resultado. Por la observación previa a la proposición, basta probar que L representa un elemento primo cuya norma no esté en la misma clase de cuadrados que π . Recordemos que si $K = k(j)$ y $q \in iK$, entonces $q\alpha = \bar{\alpha}q$ para cualquier $\alpha \in K$. Calculamos, para $\alpha \in \mathcal{O}_K$:

$$\begin{pmatrix} 1 & \alpha \end{pmatrix} \begin{pmatrix} q & 0 \\ 0 & \epsilon q \end{pmatrix} \begin{pmatrix} 1 \\ \bar{\alpha} \end{pmatrix} = (1 + \epsilon\alpha^2)q,$$

donde $N(1 + \epsilon\alpha^2) = 1 + \epsilon \operatorname{tr}(\alpha^2) + \epsilon^2 N(\alpha^2)$. Ahora, como $\nu(\epsilon) = \nu(4)$ y $\epsilon \in k^*$, podemos escribir $\epsilon = 4\epsilon$, con $\epsilon \in \mathcal{O}_k^*$. Así, tenemos que $N(1 + \epsilon\alpha^2) = 1 + 4\epsilon \operatorname{tr}(\alpha^2) + 16\epsilon^2 N(\alpha^2)$. Luego, por el Teorema de cuadrados locales (2.2.1) basta encontrar α tal que $1 + 4\epsilon \operatorname{tr}(\alpha^2)$ no sea un cuadrado. En efecto, sabemos por [10, §63] que existe $\Delta = 1 + 4\beta$ ($\beta \in \mathcal{O}_k^*$) unidad de defecto cuadrático minimal. Luego, basta elegir $\alpha \in \mathcal{O}_K$ tal que $\operatorname{tr}(\alpha^2) = \epsilon^{-1}\beta$. Sabemos que $\mathcal{O}_K = \mathcal{O}_k[\omega]$, donde $\omega = \frac{1+i}{2}$ (§2.6). Así, si $\eta \in \mathcal{O}_K$, con $\eta = a + b\omega$; $a, b \in \mathcal{O}_k$, entonces $\operatorname{tr}(\eta) = 2a + b$, de donde es claro que $\operatorname{tr}(\epsilon^{-1}\beta\omega) = \epsilon^{-1}\beta$. Ahora, como el cuerpo residual $\mathcal{O}_K/\pi\mathcal{O}_K$ es perfecto de característica 2, existe $\alpha \in \mathcal{O}_K$ tal que $\alpha^2 \equiv \epsilon^{-1}\beta\omega \pmod{\pi}$, de donde $\operatorname{tr}(\alpha^2) \equiv \epsilon^{-1}\beta \pmod{\pi}$ y $1 + 4\epsilon \operatorname{tr}(\alpha^2) \equiv 1 + 4\beta \pmod{4\pi}$. Por el Teorema de cuadrados locales $1 + 4\epsilon \operatorname{tr}(\alpha^2) = (1 + 4\beta)u^2 = \Delta u^2$, para algún $u \in \mathcal{O}_k^*$. Por lo tanto $1 + 4\epsilon \operatorname{tr}(\alpha^2)$ no es un cuadrado. Se concluye que $N(1 + \epsilon\alpha^2)$ no es cuadrado y por lo tanto $N(k(i)^*) \neq N(k((1 + \epsilon\alpha^2)q)^*)$. Así, $H(\Lambda) = k^*$ como queríamos probar.

□

El procedimiento anterior no se puede extender al caso en que $\mu > \nu(4)$ ya que, en este caso, $N(1 + \epsilon\alpha^2)$ es un cuadrado. Estos casos serán abordados exclusivamente sobre \mathbb{Q}_2 por otros métodos más adelante.

Capítulo 4

Algoritmo para calcular imágenes espinoriales

4.1. El Teorema de Tsukamoto

El siguiente resultado será utilizado en el algoritmo descrito en la sección siguiente. Específicamente, ocuparemos la caracterización de formas isotrópicas en dimensión 2. Recordemos que una forma anti-hermitiana es regular si el único vector ortogonal a todo el espacio es el vector 0. El discriminante de una forma anti-hermitiana sobre un álgebra de cuaterniones es la norma reducida de su matriz de Gram.

Teorema 4.1.1. [12, §10] *Sea k un cuerpo p -ádico¹ y D un álgebra de cuaterniones de división sobre k . Para formas anti-hermitianas sobre D , se tiene:*

1. *Dos formas regulares son isométricas si y sólo si ellas tienen la misma dimensión y el mismo discriminante.*
2. *Cada forma de dimensión > 3 es isotrópica.*
3. *En dimensión 1 todas las formas regulares son anisotrópicas. Hay formas de cualquier discriminante $\neq 1$.*
4. *Para cualquier dimensión > 1 hay formas de cualquier discriminante. En dimensión 2, una forma es isotrópica si y sólo si tiene discriminante 1. En dimensión 3, una forma es anisotrópica si y sólo si tiene discriminante 1.*

¹Aquí, p es cualquier lugar, aunque para nuestros propósitos, p siempre será diádico.

El siguiente resultado, junto con el Lema 3.1.1, nos permitirá construir de manera sencilla, rotaciones simples de tipo (B) para un reticulado binario, a partir de un cuaternión $r \in \mathcal{O}_D$.

Corolario 4.1.1.1. *Sea $r \in \mathcal{O}_D \setminus \{0\}$ y sean $a_1, a_2 \in \mathcal{O}_D \setminus \{0\}$ cuaterniones puros. Existe $\lambda \in \mathcal{O}_D \setminus \{0\}$ tal que $a_1 = ra_1\bar{r} + \lambda a_2\bar{\lambda}$ si y sólo si $NzNa_2 \in k^{*2}$ y $NzNa_2^{-1} \in \mathcal{O}_k$, donde $z = a_1 - ra_1\bar{r}$.*

Demostración: La existencia de $\lambda \in D^*$ tal que $a_1 = ra_1\bar{r} + \lambda a_2\bar{\lambda}$ es equivalente a que la forma anti-hermitiana cuya matriz de Gram es $\begin{pmatrix} z & 0 \\ 0 & -a_2 \end{pmatrix}$ sea isotrópica pues, para $x, y \in D^*$, $xz\bar{x} - ya_2\bar{y} = 0$ si y sólo si $z = \lambda a_2\bar{\lambda}$, donde $\lambda = x^{-1}y$. Ahora, por el Teorema de Tsukamoto, esto es equivalente a que su discriminante sea 1. Como el discriminante de una forma anti-hermitiana es la norma reducida de su matriz de Gram, concluimos que existe $\lambda \in D^*$ tal que $a_1 = ra_1\bar{r} + \lambda a_2\bar{\lambda}$ si y sólo si $NzNa_2 \in k^{*2}$. Finalmente, como $z = \lambda a_2\bar{\lambda}$ implica $Nz = Na_2N\lambda^2$, obtenemos que $\lambda \in \mathcal{O}_D$ si y sólo si $NzNa_2^{-1} \in \mathcal{O}_k$. \square

Observación 4.1.1. Notemos que el hecho de que a_1, a_2 sean cuaterniones puros es esencial en el Corolario anterior pues de otro modo la matriz $\begin{pmatrix} z & 0 \\ 0 & -a_2 \end{pmatrix}$ no define una forma anti-hermitiana.

4.2. El algoritmo

Crearemos un algoritmo para calcular $H(\Lambda)$ para reticulados binarios Λ que están en los casos I y II de la tabla 1.3, es decir, $\Lambda \cong \langle a_1 \rangle \perp \langle a_2 \rangle$, donde $N(a_2) \in N(a_1)k^{*2}$. Recuérdese que $\mu = \mu(\Lambda)$ es la diferencia minimal entre la valuación de las escalas de dos componentes consecutivos del reticulado como se define en el capítulo 1. Notemos que, para Λ en los casos I y II antes mencionados, la extensión $k(a_1)/k$ es ramificada por lo que tenemos a nuestra disposición el Lema 3.3.4.

El siguiente resultado es el que nos permitirá desarrollar un algoritmo para calcular $H(\Lambda)$ para los casos I y II de la tabla 1.3. Recordemos que, si $\Lambda = \Lambda_1 \perp \Lambda_2$, entonces $H(\Lambda_1), H(\Lambda_2) \subset H(\Lambda)$. Por lo tanto, para probar que $H(\Lambda) = k^*$, basta hacerlo para reticulados binarios.

Teorema 4.2.1. *Sea $\Lambda = \langle a_1 \rangle \perp \langle a_2 \rangle$ un \mathcal{O}_D -reticulado anti-hermitiano tal que $|2a_1| \geq |a_2|$ y $N(a_2) \in N(a_1)k^{*2}$. Entonces, son equivalentes:*

1. $H(\Lambda) = k^*$.
2. Existe $(s; \sigma) \in \mathcal{B}(\Lambda)$ tal que $N\sigma \notin N(k(a_1)^*)$.
3. Existen $r, \lambda \in \mathcal{O}_D$ tales que: $a_1 = ra_1\bar{r} + \lambda a_2\bar{\lambda}$ y $N(1 - \bar{r}) \notin N(k(a_1)^*)$.
4. Existe $r \in \mathcal{O}_D$ tal que: $\left(\frac{N(1-r), -Na_1}{p}\right) = -1$, $NzNa_2 \in k^{*2}$ y $NzN(a_2)^{-1} \in \mathcal{O}_k$, donde $z = a_1 - ra_1\bar{r}$.
5. Existe $r \in \mathcal{O}_D$ tal que: $\left(\frac{N(1-r), -Na_1}{p}\right) = -1$, $NzNa_1 \in k^{*2}$ y $NzN(\pi^t a_1)^{-1} \in \mathcal{O}_k$, donde $z = a_1 - ra_1\bar{r}$ y $\mu = \nu(\pi^t)$.

Demostración: $[1 \Rightarrow 2]$: Si $H(\Lambda) = k^*$, entonces en virtud de la Observación 3.2.2 existe una rotación $(s; \sigma) \in \mathcal{B}(\Lambda)$ tal que $\theta[(s; \sigma)] \notin N(k(a_1)^*)$.

$[2 \Rightarrow 3]$: La rotación $(s; \sigma)$ satisface $a_1 = h(s_1, s_1) = h((s; \sigma)(s_1), (s; \sigma)(s_1)) = ra_1\bar{r} + \lambda a_2\bar{\lambda}$ para ciertos $r, \lambda \in \mathcal{O}_D$. Por otra parte, sabemos que $\theta[(s; \sigma)] = N(\sigma)k^{*2}$ (ver §3.1), y que $\sigma = a_1(1 - \bar{r})$ (Lema 3.1.1). Esto concluye la demostración.

$[3 \Rightarrow 1]$: La ecuación $a_1 = ra_1\bar{r} + \lambda a_2\bar{\lambda}$ es equivalente a $h(s_1, s_1) = h(rs_1 + \lambda s_2, rs_1 + \lambda s_2)$. Así, por el Lema 3.1.1 tenemos que $(s; \sigma)$, con $s = s_1 - (rs_1 + \lambda s_2) = (1 - r)s_1 + \lambda s_2$ y $\sigma = a_1(1 - \bar{r})$, es una rotación simple. Además, sabemos que las rotaciones simples tienen norma espinorial $\theta[(s; \sigma)] = N(\sigma)k^{*2}$ (ver §3.1). Por lo tanto $H(\Lambda) = k^*$ en virtud del Corolario 3.2.1.2.

$[3 \Leftrightarrow 4]$: Es consecuencia directa del Lema 2.3.1 y el Corolario 4.1.1.1.

$[4 \Leftrightarrow 5]$: Es claro ya que $Na_2 \in N(a_1)k^{*2}$ y $\mu = \nu(a_2) - \nu(a_1) = \nu(\pi^t)$. □

Corolario 4.2.1.1. *Sea Λ como en el Teorema. Sea $\mu = \nu(\pi^t)$. Si $H(\Lambda) = k^*$, entonces $H(\Lambda') = k^*$ para todo $\Lambda' = \langle b_1 \rangle \perp \langle b_2 \rangle$ en el mismo caso que Λ de la tabla 1.3, que satisfaga $N(b_1), N(b_2) \in N(a_1)k^{*2}$ y $\mu(\Lambda') = \nu(\pi^s)$, para $s < t$.*

Observación 4.2.1. Por el Lema 3.3.2, en el Teorema anterior basta considerar rotaciones $(s; \sigma) \in \mathcal{B}(\Lambda)$ con $|\lambda| > |4|$, donde $s = (1 - r)s_1 - \lambda s_2$. Recordemos también que $|1 - r| \geq |2|$ para $(s; \sigma) \in \mathcal{B}(\Lambda)$. Además, podemos suponer $|a_1| \geq |i|$ por reescalamiento. Usaremos estos hechos en la siguiente Proposición, la cual nos

permitirá, junto con el Teorema anterior, crear un algoritmo para calcular imágenes espinoriales.

Recordemos que $e = \nu(2)/2$ es el índice de ramificación de la extensión k/\mathbb{Q}_2 , y t satisface $\mu = \nu(\pi^t)$.

Proposición 4.2.2. *Existe $r \in \mathcal{O}_D$ que cumple las condiciones en 5 del Teorema 4.2.1 si y sólo si existe $\alpha \in \mathcal{S} \oplus \mathcal{S}\omega \oplus \mathcal{S}i \oplus \mathcal{S}i\omega \subset \mathcal{O}_D$ que las cumple, donde \mathcal{S} es cualquier conjunto finito de representantes de $\mathcal{O}_k/\pi^u\mathcal{O}_k$, con $u = 6e + 1 + t$.*

Demostración: Si $r \in \mathcal{O}_D$ satisface las condiciones en 5 del Teorema 4.2.1, existe $(s; \sigma) \in \mathcal{B}(\Lambda)$, es decir, $s = (1 - r_0)s_1 - \lambda s_2$, con $|1 - r_0| \geq 2$ y $\sigma = a_1(1 - \bar{r}_0)$, tal que $N(1 - r_0) \notin N(k(a_1)^*)$. Es claro que $r_0 \in \mathcal{O}_D$ también satisface las condiciones en 5 de 4.2.1. Sea $\alpha \in \mathcal{O}_D$ un representante de la clase de r_0 módulo π^u como se describe arriba. Así, $r_0 = \alpha + \pi^u\beta$, con $\beta \in \mathcal{O}_D$ y $\alpha \in \mathcal{S} \oplus \mathcal{S}\omega \oplus \mathcal{S}i \oplus \mathcal{S}i\omega \subset \mathcal{O}_D$. Entonces $1 - r_0 = 1 - \alpha - \pi^u\beta$ y por lo tanto $N(1 - r_0) = N(1 - \alpha)N(1 - (1 - \alpha)^{-1}\pi^u\beta)$. Como $|1 - r_0| \geq |2|$, se tiene que $|1 - \alpha| \geq |2|$ y por lo tanto $N(1 - (1 - \alpha)^{-1}\pi^u\beta)$ es un cuadrado en virtud del Lema 2.6.4. Así,

$$\left(\frac{N(1 - r_0), -Na_1}{\mathfrak{p}} \right) = \left(\frac{N(1 - \alpha), -Na_1}{\mathfrak{p}} \right).$$

Por otra parte, si $z = a_1 - r_0 a_1 \bar{r}_0$ y $z' = a_1 - \alpha a_1 \bar{\alpha}$, entonces $z = z' - \pi^u\gamma$, con $\gamma \in \mathcal{O}_D$. Luego, $|z'| = |z|$, pues $|z| = |\pi^t \lambda a_1 \bar{\lambda}| > |16\pi^t a_1| \geq |\pi^{4e+t} i| > |\pi^u \gamma|$, donde asumimos que $|\lambda| > |4|$, $|a_1| \geq |i|$ (ver Obs. 4.2.1). Además se tiene que $Nz = Nz'N(1 - z'^{-1}\pi^u\gamma)$ con

$$|z'^{-1}\pi^u\gamma| < |\pi^{-(4e+t)} i^{-1} \pi^{6e+1+t}| = |\pi^{2e+1} i^{-1}| = |4\pi i^{-1}| < |4|.$$

Por lo tanto,

$$NzNa_1 \text{ es un cuadrado} \Leftrightarrow Nz'Na_1 \text{ es un cuadrado.}$$

Finalmente, como $|z'| = |z|$, es decir, $|Nz|_k = |Nz'|_k$ se tiene que

$$|Nz/\pi^{2t}N(a_1)|_k \leq 1 \Leftrightarrow |Nz'/\pi^{2t}N(a_1)|_k \leq 1.$$

□

Con los resultados obtenidos hasta ahora, estamos en condiciones de construir un algoritmo como sigue:

1. Cambiamos Λ por $L = \langle q \rangle \perp \langle \epsilon q \rangle$ como en el Lema 3.3.4, donde q es elegido de modo que $|q| \geq |i|$.
2. Fijamos un conjunto (finito) de representantes \mathcal{S} de $\mathcal{O}_k/\pi^u \mathcal{O}_k$.
3. Para los finitos $r = a + b\omega + ci + di\omega \in \mathcal{S} \oplus \mathcal{S}\omega \oplus \mathcal{S}i \oplus \mathcal{S}i\omega \subset \mathcal{O}_D$, verificamos si se cumplen las hipótesis en 5 del Teorema 4.2.1.
4. Concluimos que $H(\Lambda) = k^*$ si algún r satisface las hipótesis en 5 del Teorema 4.2.1. De otro modo, concluimos que $H(\Lambda) = N(k(a_1)^*)$ gracias a la Proposición 4.2.2.

Observación 4.2.2. El algoritmo depende sólo de a_1 y de μ . Por lo tanto, para el reticulado L de arriba, sólo nos interesa q y la valuación de ϵ . Esto implica que también podemos multiplicar ϵ por cualquier elemento de \mathcal{O}_k^* .

Observación 4.2.3. Como la condición $|2a_1| \geq |a_2|$ en 4.2.1 y 3.3.1 es esencial, el algoritmo no funciona, para $\mu < \nu(2)$, si la extensión k/\mathbb{Q}_2 es ramificada, a no ser que se obtenga k^* para $\mu < \nu(2)$.

4.3. Implementación del algoritmo

Implementamos el algoritmo descrito en la sección precedente para $k = \mathbb{Q}_2$: En este caso, $\mathcal{O}_k = \mathbb{Z}_2$, $\mathcal{O}_D = \mathbb{Z}_2 \oplus \mathbb{Z}_2\omega \oplus \mathbb{Z}_2i \oplus \mathbb{Z}_2i\omega$ y $\mathcal{O}_k/\pi^u \mathcal{O}_k \cong \mathbb{Z}/2^u \mathbb{Z}$.

1. Cambiamos Λ por $L = \langle q \rangle \perp \langle \epsilon q \rangle$ como en el Lema 3.3.4, donde q es elegido de modo que $|q| \geq |i|$: Tenemos dos posibilidades para la clase de cuadrados de a_1 .
 - a) Si $Na_1 \in \alpha \mathbb{Q}_2^{*2}$, con α unidad, buscamos q tal que $Nq \equiv \alpha \pmod{8}$. Así, $Nq = \alpha(1 + 8\alpha^{-1}\beta)$, para algún $\beta \in \mathcal{O}_D$, de donde se obtiene que $Nq \in N(a_1)\mathbb{Q}_2^{*2}$ y $|q| = 1$.

- b) Si $Na_1 \in \alpha\mathbb{Q}_2^{*2}$, con α parámetro uniformizante, buscamos q tal que $Nq \equiv \alpha \pmod{16}$. Así, $Nq = \alpha(1 + 16\alpha^{-1}\beta)$, para algún $\beta \in \mathcal{O}_D$, de donde se obtiene que $Nq \in N(a_1)\mathbb{Q}_2^{*2}$ y $|q| = |i|$.

En ambos casos se obtiene q con $|q| \geq |i|$.

2. Fijamos un conjunto (finito) de representantes \mathcal{S} de $\mathcal{O}_k/\pi^u\mathcal{O}_k$:

Como $\mathcal{O}_k/\pi^u\mathcal{O}_k \cong \mathbb{Z}/2^u\mathbb{Z}$, podemos elegir $\mathcal{S} = \{0, 1, \dots, 2^u - 1\}$.

3. Para los finitos $r = a + b\omega + ci + di\omega \in \mathcal{S} \oplus \mathcal{S}\omega \oplus \mathcal{S}i \oplus \mathcal{S}i\omega \subset \mathcal{O}_D$, verificamos si se cumplen las hipótesis en 5 de 4.2.1. Esta verificación se lleva a cabo usando las funciones *hilbert_symbol*(\cdot, \cdot, \cdot), *is_square*(\cdot) y (\cdot).*ordp*(\cdot) del programa Sage [14] la cuales se explican brevemente a continuación:

- a) La función *hilbert_symbol*(α, β, p) calcula el símbolo de Hilbert sobre \mathbb{Q}_p . Por ejemplo, si ejecutamos *hilbert_symbol*(2, 5, 2) el programa entrega -1 ya que 2 es parámetro uniformizante en \mathbb{Q}_2 y 5 es unidad de defecto cuadrático minimal en \mathbb{Q}_2 (ver apéndice).
- b) La función *is_square*(α) nos dice si α es un cuadrado en un anillo. Por ejemplo, si ejecutamos *is_square*(17) el programa entrega **False** ya que por defecto el programa asume que el anillo es \mathbb{Q} . Pero como estamos trabajando sobre \mathbb{Q}_2 , tenemos que decirle al programa que considere los elementos allí. Para esto, definimos $R = \mathbb{Q}_p(2, 20, 'capped-rel')$ (es decir, $R = \mathbb{Q}_2$). Luego, para decirle al programa que vea 17 como elemento de \mathbb{Q}_2 escribimos *R*(17). Entonces, si ejecutamos *is_square*(*R*(17)) el programa nos entrega **True**.
- c) La función (α).*ordp*(\cdot) nos entrega la valuación de α en \mathbb{Q}_p . Por ejemplo, si ejecutamos (*R*(2/3)).*ordp*(\cdot) el programa nos entrega 1 pues al escribir *R*(2/3) le decimos al programa que considere 2/3 como elemento de \mathbb{Q}_2 . Si ejecutamos (*R*(9/8)).*ordp*(\cdot) el programa nos entrega -3 . Notemos que $|\alpha|_{\mathbb{Q}_2} \leq 1$ es equivalente a *ord*₂(α) ≥ 0 .

Sabemos que la norma de $r = a + b\omega + ci + di\omega \in \mathcal{O}_D$ es $N(a, b, c, d, \pi) = a^2 + ab - b^2 - \pi(c^2 + cd - d^2)$. Por lo tanto, basta escribir $z = q - r\bar{q} = z_0 + z_1\omega + z_2i + z_3i\omega$ para obtener $Nz = N(z_0, z_1, z_2, z_3, \pi)$ y así, crear un algoritmo en el programa

Sage [14] como se muestra en el siguiente ejemplo a continuación (Notar que $Nz.subs()$ nos permite sustituir valores en la expresión que define a Nz):

Algorithm 1 Caso I, $u = -5$, $\mu = \nu(4)$ (ver tabla 1.3)

```

for  $a, b, c, d \in \mathcal{S}$  do
  if  $\text{hilbert\_symbol}(N(a - 1, b, c, d, 2), -5, 2) == -1$  and  $\text{R}(Nz.subs(a = a, b = b, c = c, d = d) * 5).is\_square()$  and  $\text{R}(Nz.subs(a = a, b = b, c = c, d = d)/2^4).ordp() >= 0$  then
    return  $H(\Lambda) = \mathbb{Q}_2^*$ 
  end if
end for
return  $H(\Lambda) = N(\mathbb{Q}_2(q)^*)$ 

```

4. Como en el ejemplo, concluimos que $H(\Lambda) = \mathbb{Q}_2^*$ si algún r satisface las hipótesis en 5 del Teorema 4.2.1. De otro modo, concluimos que $H(\Lambda) = N(\mathbb{Q}_2(a_1)^*)$ gracias a la Proposición 4.2.2.

Recordemos que si $H(\Lambda) = \mathbb{Q}_2^*$ para un reticulado binario, se tiene que $H(\Lambda) = \mathbb{Q}_2^*$ para un reticulado de cualquier rango. Por otra parte, si $H(\Lambda) \neq \mathbb{Q}_2^*$ para reticulados binarios, esto no implica, en principio, que esto ocurra para reticulados de rango mayor. En estos casos, reduciremos el problema al caso binario o ternario usando el Lema 3.3.1.

Usando las funciones descritas en la implementación del algoritmo, establecemos los siguientes lemas que serán de gran utilidad en el capítulo 5, en el cual se calculan imágenes espinoriales. Los primeros 2 lemas a continuación serán utilizados en el próximo capítulo para mejorar nuestro conjunto de generadores $\mathcal{B}(\Lambda)$.

Lema 4.3.1. *Para cada $q \in \{j + k, i + j\}$ y $t \in \{3, 4\}$, existe $r \in \mathcal{O}_D$ tal que:*

1. $|1 - r| = |2|$,
2. $NzNq \in \mathbb{Q}_2^{*2}$,
3. $NzN(2^t q)^{-1} \in \mathbb{Z}_2^*$,

donde $z = q - rq\bar{r}$.

q	t	r
$j+k$	3	$-1 - 4i - 4i\omega$
$j+k$	4	$-1 - 8i - 8i\omega$
$i+j$	3	$-1 - 4i\omega$
$i+j$	4	$-1 - 8i\omega$

Demostración: Es un cálculo directo comprobar que los elementos $r \in \mathcal{O}_D$ mostrados en la tabla de arriba satisfacen las condiciones 1-3 en el Lema.

□

Lema 4.3.2. Para cada $q \in \{j+k, i+j\}$ y $t \in \{3, 4\}$, existe $r \in \mathcal{O}_D$ tal que:

1. $|1-r| = |i|$,
2. $NzNq \in \mathbb{Q}_2^{*2}$,
3. $NzN(2^t q)^{-1} \in \mathbb{Z}_2^*$,

donde $z = q - r\bar{r}$.

Demostración: Es un cálculo directo comprobar que los elementos $r \in \mathcal{O}_D$ mostrados en la tabla de abajo satisfacen las condiciones 1-3 en el Lema.

q	t	r
$j+k$	3	$1 - 14\omega - i - 10i\omega$
$j+k$	4	$1 - 6\omega - 13i - 6i\omega$
$i+j$	3	$1 - 2\omega - i$
$i+j$	4	$-1 - 6\omega - 3i$

□

Usando el algoritmo descrito en esta sección encontramos elementos $r \in \mathcal{O}_D$ (ver los 2 lemas a continuación) que satisfacen las condiciones 5 del Teorema 4.2.1 para reticulados en particular, lo que nos permitirá concluir en el siguiente capítulo que $H(\Lambda) = \mathbb{Q}_2^*$ para cualquier reticulado en algunos casos de la tabla 1.3. Recordemos que, en esta sección, el cuerpo base es \mathbb{Q}_2 .

Lema 4.3.3. Sea $\Lambda = \langle a_1 \rangle \perp \langle a_2 \rangle$ un \mathcal{O}_D -reticulado anti-hermitiano como en el Teorema 4.2.1. Para $a_1 \in \{j+k, i+j\}$ y $t \in \{1, 2\}$ existe $r \in \mathcal{O}_D$ que satisface las condiciones en 5 del Teorema 4.2.1.

Demostración: Es un cálculo directo comprobar que los elementos $r \in \mathcal{O}_D$ mostrados en la tabla de abajo, satisfacen las condiciones pedidas para $t = 2$ y por lo tanto para $t = 1$ en virtud del Corolario 4.2.1.1. Aquí, $i_2^2 = 2$.

t	a_1	r	$N(1-r)$	z	$NzNa_1$
2	$j+k$	$1+2i_2\omega$	$2 \cdot 2^2$	$4(-1+2\omega-4i_2-7i_2\omega)$	$2^4 \cdot 5^2$
2	$i+j$	$1+2i_2+2i_2\omega$	$-2 \cdot 2^2$	$4(1-2\omega+3i_2+3i_2\omega)$	$2^4(1+8 \cdot 20)$

□

Lema 4.3.4. Sea $\Lambda = \langle a_1 \rangle \perp \langle a_2 \rangle$ un \mathcal{O}_D -reticulado anti-hermitiano como en el Teorema 4.2.1. Para $a_1 \in \{i_\pi\}_\pi$, donde $\pi \in \{\pm 2, \pm 10\}$, $i_\pi^2 = \pi$ y $t \in \{1, 2, 3, 4\}$ existe $r \in \mathcal{O}_D$ que satisface las condiciones en 5 del Teorema 4.2.1.

Demostración: Es un cálculo directo comprobar que los elementos $r \in \mathcal{O}_D$ mostrados en la tabla de abajo, satisfacen las condiciones pedidas para $t = 4$ y por lo tanto para $t < 4$ en virtud del Corolario 4.2.1.1.

t	π	r	$N(1-r)$	z	$NzNa_1$
4	± 2	$15+8\omega$	$5 \cdot 2^2(1+8 \cdot 5^{-1} \cdot 7)$	$-592i_\pi+304i_\pi\omega$	$2^{10}(1+8 \cdot 38)$
4	± 10	$15+8\omega$	$5 \cdot 2^2(1+8 \cdot 5^{-1} \cdot 7)$	$-592i_\pi+304i_\pi\omega$	$2^{10} \cdot 5^2(1+8 \cdot 38)$

□

Los siguientes lemas se demuestran mediante una búsqueda por Sage [14] como se describe al comienzo de la sección y nos permitirán concluir en el próximo capítulo que $H(\Lambda) \neq \mathbb{Q}_2^*$ en ciertos casos.

Lema 4.3.5. No existe $r = a + b\omega + ci + di\omega \in \mathbb{Z} \oplus \mathbb{Z}\omega \oplus \mathbb{Z}i \oplus \mathbb{Z}i\omega \subset \mathcal{O}_D$, con $0 \leq a, b, d, c < 2^{t+3}$ que cumpla las condiciones en 5 del Teorema 4.2.1 para $t \in \{3, 4\}$ y $a_1 \in \{j+k, j+i\}$.

Lema 4.3.6. No existe $\eta = a + b\omega + ci + di\omega \in \mathbb{Z} \oplus \mathbb{Z}\omega \oplus \mathbb{Z}i \oplus \mathbb{Z}i\omega \subset \mathcal{O}_D$, con $0 \leq a, b, d, c < 4$ tal que $|\eta| = |i|$ y $T(\xi) \equiv 1 \pmod{2}$, donde $\xi = 2(\eta a_1 \bar{\eta})^{-1} a_1$ y $a_1 \in \{j+k, j+i\}$.

Capítulo 5

Cálculo de imágenes espinoriales sobre \mathbb{Q}_2

A través de todo el capítulo, consideramos \mathcal{O}_D -reticulados anti-hermitianos, con $D = \left(\frac{\pi, \Delta}{\mathbb{Q}_2}\right)$. La Proposición 3.3.1 nos entrega $H(\Lambda)$ para el subcaso $\mu = \nu(4)$ del caso II descrito en la tabla 1.3. Esto da origen a la siguiente tabla, la cual contiene los únicos casos desconocidos hasta el momento (ver §1):

Casos	A	μ	$H(\Lambda)$
I	$\{-\tilde{u}\}$	$0 < \mu \leq \nu(16)$?
II	$\{\tilde{\pi}\}$	$\nu(4) < \mu \leq \nu(16)$?

Tabla 5.1: Casos desconocidos.

En virtud del Lema 3.3.4, es suficiente, para formas binarias, considerar los reticulados en la siguiente tabla:

Casos	Λ
I	$\langle q \rangle \perp \langle \epsilon q \rangle$ donde $\epsilon \in \mathbb{Q}_2^*$, $0 < \nu(\epsilon) \leq \nu(16)$ y $N(q) \in -u\mathbb{Q}_2^{*2}$
II	$\langle i \rangle \perp \langle \epsilon i \rangle$ donde $\epsilon \in \mathbb{Q}_2^*$, $\nu(4) < \nu(\epsilon) \leq \nu(16)$

Tabla 5.2: Casos desconocidos binarios.

Aquí, $q = q_u$ recorre un sistema de representantes con $N(q) \in -u\mathbb{Q}_2^{*2}$, para u recorriendo las unidades de defecto cuadrático no minimal, e $i = i_\pi$ recorre un

sistema de representantes con $N(i) = -\pi\mathbb{Q}_2^{*2}$, para π recorriendo los parámetros uniformizantes de \mathbb{Q}_2 .

Usando el algoritmo descrito en el capítulo anterior, realizaremos los cálculos para los casos I y II. Notar que 5 es unidad de defecto cuadrático minimal en \mathbb{Q}_2 y que $\Delta \in 5\mathbb{Q}_2^{*2}$ para cualquier unidad Δ de defecto cuadrático minimal (ver §2.2).

Observación 5.0.1. Al cambiar el parámetro uniformizante π no cambiamos el álgebra de división $D = \left(\frac{\pi, \Delta}{k}\right)$, es decir, $\left(\frac{\pi_1, \Delta}{k}\right) = \left(\frac{\pi_2, \Delta}{k}\right)$ para cualquier par de parámetros uniformizantes π_1, π_2 de k . Por lo tanto $i = i_\pi$ está en el mismo álgebra para todo π . A continuación se muestra una tabla con una posible elección de los distintos parámetros uniformizantes en D (módulo cuadrados) en función de i_2 . Recordemos que $\omega = \frac{1+i}{2}$:

π	i_π
-2	$i_2\omega$
10	$i_2(2 + \omega)$
-10	$i_2(2\omega - 1)$

Notar que $i_\pi j = -ji_\pi$ para cada π .

5.1. Caso I

Consideramos $\Lambda = \langle a_1 \rangle \perp \dots \perp \langle a_n \rangle$, donde $N(a_m) \in -u\mathbb{Q}_2^{*2}$, $\forall m = 1, \dots, n$ y $u \in \mathbb{Z}_2^*$ es una unidad de defecto cuadrático no minimal independiente de m . Como $\mathbb{Z}_2^*/\mathbb{Z}_2^{*2} = \{\pm 1, \pm 5\}$ y un cuaternión puro no puede tener norma -1 , tenemos dos opciones para u : $u = -5$ ó $u = -1$.

Por la discusión desarrollada al comienzo del capítulo, para reticulados binarios consideramos $\Lambda = \langle q \rangle \perp \langle \epsilon q \rangle$, donde puede elegirse cualquier cuaternión puro $q \in \mathcal{O}_D^0$ que satisfaga $N(q) \in -u\mathbb{Q}_2^{*2}$, y donde $\epsilon = \epsilon\pi^t$, con $\epsilon \in \mathbb{Z}_2^*$ y $t \in \{1, 2, 3, 4\}$. Más aún, podemos fijar el parámetro uniformizante en \mathbb{Q}_2 pues u es independiente de π y el algoritmo es independiente de la unidad ϵ arriba (ver Obs. 4.2.2). Por lo tanto, fijamos $\pi = 2$ para este caso y entonces, para reticulados binarios, consideramos el reticulado $\Lambda = \langle q \rangle \perp \langle 2^t q \rangle$, donde elegimos $q = j + k$ en el caso $u = -5$ y $q = i + j$ en el caso $u = -1$, y donde $t \in \{1, 2, 3, 4\}$.

Proposición 5.1.1. *Si $\Lambda = \langle a_1 \rangle \perp \dots \perp \langle a_n \rangle$ es un \mathcal{O}_D -reticulado anti-hermitiano, tal que $N(a_1), \dots, N(a_n) \in -u\mathbb{Q}_2^{*2}$ y la diferencia minimal entre la valuación de las escalas de dos componentes consecutivos es $0 < \mu < \nu(8)$, entonces $H(\Lambda) = \mathbb{Q}_2^*$.*

Demostración: Basta probarlo para reticulados binarios. Por la discusión previa a la Proposición asumimos que $\Lambda = \langle q \rangle \perp \langle 2^t q \rangle$, con $q = j + k$ en el caso $u = -5$ y $q = i + j$ en el caso $u = -1$, y donde $t \in \{1, 2\}$. Por el Corolario 4.2.1.1 basta probar el resultado para $t = 2$. Por el Lema 4.3.3 existe $r \in \mathcal{O}_D$ que satisface las condiciones del Teorema 4.2.1 y por lo tanto concluimos que $H(\Lambda) = \mathbb{Q}_2^*$. □

Para abordar los casos en que $\nu(8) \leq \mu \leq \nu(16)$ necesitaremos los siguientes resultados. Recordemos que, por el Ejemplo 2.6.1 se tiene que

$$\mathcal{O}_D/i^t\mathcal{O}_D \cong \begin{cases} (\mathbb{Z}/2^s\mathbb{Z}) \oplus (\mathbb{Z}/2^s\mathbb{Z})\tilde{\omega} \oplus (\mathbb{Z}/2^s\mathbb{Z})\tilde{i} \oplus (\mathbb{Z}/2^s\mathbb{Z})\tilde{i}\tilde{\omega} & , t = 2s \text{ par} \\ (\mathbb{Z}/2^{s+1}\mathbb{Z}) \oplus (\mathbb{Z}/2^{s+1}\mathbb{Z})\tilde{\omega} \oplus (\mathbb{Z}/2^s\mathbb{Z})\tilde{i} \oplus (\mathbb{Z}/2^s\mathbb{Z})\tilde{i}\tilde{\omega} & , t = 2s + 1 \text{ impar.} \end{cases}$$

Lema 5.1.1. *Si $r \in \mathcal{O}_D$ satisface la ecuación*

$$j + k = r(j + k)\bar{r} + \epsilon\pi^t\lambda(j + k)\bar{\lambda}, \quad (5.1)$$

donde $\epsilon \in \mathbb{Z}_2^*$, $\lambda \in \mathcal{O}_D$, $t \geq 2$ entonces $1 - r \in i\mathcal{O}_D$.

Demostración: Sea $r = a_0 + a_1\omega + a_2i + a_3i\omega$. Entonces,

$$\begin{aligned} r(j + k)\bar{r} &= (-2a_0a_2 - a_0a_3 - a_1a_2 - 3a_1a_3 - a_2^2 - a_2a_3 + a_3^2)\pi - a_0^2 - a_0a_1 + a_1^2 + (5.2) \\ & 2((2a_0a_2 + a_0a_3 + a_1a_2 + 3a_1a_3 + a_2^2 + a_2a_3 - a_3^2)\pi + a_0^2 + a_0a_1 - a_1^2)\omega + \\ & ((-a_2^2 + 4a_2a_3 + a_3^2)\pi - a_0(a_0 + 6a_1 + 2a_2 - 4a_3) - a_1(4a_1 + 6a_2 - 2a_3))i + \\ & ((2a_2^2 + 2a_2a_3 + 3a_3^2)\pi + 2a_0(a_0 + a_1 + 2a_2 + a_3) + a_1(3a_1 + 2a_2 - 4a_3))i\omega. \end{aligned}$$

Recordemos que estamos considerando en este caso $\pi = 2$. Además $j + k = -1 + 2\omega - i + 2i\omega$. Probaremos que $a_0 \equiv 1 \pmod{2}$ y $a_1 \equiv 0 \pmod{2}$. En efecto, usando la ecuación 5.2 y reduciendo módulo 2, la ecuación 5.1 se traduce en las ecuaciones:

$$1 \equiv a_0^2 + a_0a_1 + a_1^2 \pmod{2}$$

$$1 \equiv a_0^2 \pmod{2}$$

$$0 \equiv a_1^2 \pmod{2},$$

de donde $a_0 \equiv 1 \pmod{2}$ y $a_1 \equiv 0 \pmod{2}$.

□

Lema 5.1.2. *Si $r \in \mathcal{O}_D$ satisface la ecuación*

$$i + j = r(i + j)\bar{r} + \epsilon\pi^t\lambda(i + j)\bar{\lambda}, \quad (5.3)$$

donde $\epsilon \in \mathbb{Z}_2^*$, $\lambda \in \mathcal{O}_D$, $t \geq 2$ entonces $1 - r \in i\mathcal{O}_D$.

Demostración: Sea $r = a_0 + a_1\omega + a_2i + a_3i\omega$. Entonces,

$$\begin{aligned} r(i + j)\bar{r} = & (a_0a_3 + a_1a_2 + a_1a_3 - a_2^2 - a_2a_3 + a_3^2)\pi - a_0^2 - a_0a_1 + a_1^2 + & (5.4) \\ & 2((-a_0a_3 - a_1a_2 - a_1a_3 + a_2^2 + a_2a_3 - a_3^2)\pi + a_0^2 + a_0a_1 - a_1^2)\omega + \\ & ((-a_2^2 - a_3^2)\pi + a_0^2 + 2a_0a_1 - 2a_0a_2 + 4a_0a_3 + 2a_1^2 - 6a_1a_2 + 2a_1a_3)i + \\ & ((-2a_2a_3 - a_3^2)\pi - 2a_0a_1 + 4a_0a_2 + 2a_0a_3 - a_1^2 + 2a_1a_2 - 4a_1a_3)i\omega. \end{aligned}$$

Recordar que, como en el Lema anterior consideramos $\pi = 2$. Además, $i + j = -1 + 2\omega + i$. Probaremos que $a_0 \equiv 1 \pmod{2}$ y $a_1 \equiv 0 \pmod{2}$. En efecto, usando la ecuación 5.4 y reduciendo módulo 2, la ecuación 5.3 se traduce en las ecuaciones:

$$1 \equiv a_0^2 + a_0a_1 + a_1^2 \pmod{2}$$

$$1 \equiv a_0^2 \pmod{2}$$

$$0 \equiv a_1^2 \pmod{2},$$

de donde $a_0 \equiv 1 \pmod{2}$ y $a_1 \equiv 0 \pmod{2}$.

□

Observación 5.1.1. Usando las ecuaciones 5.2, 5.4 y reduciendo módulo 4 en las

ecuaciones 5.1, 5.3 respectivamente, se puede probar en ambos casos que $a_3 \equiv 0$ (2). Este hecho nos permite disminuir la cantidad de cálculos al utilizar el algoritmo.

Lema 5.1.3. *Sea $\Lambda = \mathcal{O}_D s_1 \perp \mathcal{O}_D s_2 = \langle a_1 \rangle \perp \langle a_2 \rangle$ un \mathcal{O}_D -reticulado anti-hermitiano tal que $N(a_1), N(a_2) \in -u\mathbb{Q}_2^{*2}$, donde u es unidad de defecto cuadrático no minimal, y $\nu(8) \leq \mu \leq \nu(16)$. Existe un reticulado L de rango 2 tal que $H(L) = H(\Lambda)$ y subconjuntos $\mathcal{B}_1(L), \mathcal{B}_2(L) \subset \mathcal{B}(L)$, tales que:*

1. $A(L) \cup \mathcal{B}_l(L)$ genera $\mathcal{U}^+(L)$, para $l = 1, 2$.
2. Las rotaciones $(s; \sigma) \in \mathcal{B}_1(L)$, donde $s = (1-r)s_1 - \lambda s_2$, satisfacen $|1-r| = |i|$.
3. Las rotaciones $(s; \sigma) \in \mathcal{B}_2(L)$, donde $s = (1-r)s_1 - \lambda s_2$, satisfacen $|\lambda| = 1$.

Demostración: Recordemos que $u \in \{-5, -1\}$.

Por el Lema 3.3.4 tenemos que $L = \mathcal{O}_D s_1 \perp \mathcal{O}_D s_2 = \langle q \rangle \perp \langle \epsilon 2^t q \rangle$, donde $\epsilon \in \mathbb{Z}_2^*$ y $t \in \{3, 4\}$ satisface $H(L) = H(\Lambda)$, donde elegimos $q = j + k$ para $u = -5$ y $q = i + j$ para $u = -1$. Sea $\phi \in \mathcal{B}(L)$ tal que $\phi(s_1) = r s_1 + \lambda s_2$. Por los lemas 5.1.2 y 5.1.1 se tiene que $|1-r| \in \{|i|, |2|\}$. Así, para probar que existe $\mathcal{B}_1(L)$, basta probar¹ que si ϕ es tal que $|1-r| = |2|$, existe $(s; \sigma) \in \mathcal{B}(L)$ tal que $|1-r''| = |i|$ y $|1-r'| = |i|$, donde r', r'' están definidos por $(s; \sigma)\phi(s_1) = r'' s_1 + \lambda'' s_2$, $(s; \sigma)(s_1) = r' s_1 + \lambda' s_2$, para ciertos $\lambda', \lambda'' \in \mathcal{O}_D$. En efecto, calculando $(s; \sigma)\phi(s_1) = (s; \sigma)(r s_1 + \lambda s_2)$ obtenemos que

$$1 - r'' = 1 - r + [r q (1 - \bar{r}') + \lambda \epsilon 2^t q \bar{\lambda}'] (1 - \bar{r}')^{-1} q^{-1} (1 - r') \quad (5.5)$$

$$\lambda'' = \lambda + [r q (1 - \bar{r}') + \lambda \epsilon 2^t q \bar{\lambda}'] (1 - \bar{r}')^{-1} q^{-1} \lambda'. \quad (5.6)$$

Por Lema 4.3.2 existe $r' \in \mathcal{O}_D$ (ver tabla 5.3 en la página siguiente) tal que

$$|1 - r'| = |i|, \quad NzN(\epsilon 2^t q) \in \mathbb{Q}_2^{*2} \quad y \quad NzN(\epsilon 2^t q)^{-1} \in \mathbb{Z}_2,$$

donde $z = q - r' q \bar{r}'$. Así, por el Corolario 4.1.1.1 existe $\lambda' \in \mathcal{O}_D$, tal que $q = r' q \bar{r}' + \epsilon 2^t \lambda' q \bar{\lambda}'$. Por lo tanto $(s; \sigma)$ con $s = (1-r')s_1 - \lambda' s_2$, $\sigma = q(1-\bar{r}')$ define una

¹Esto debido a que, en tal caso, existe un segundo elemento $(s'; \sigma') \in \mathcal{B}_1(L)$ definido por $s' = s_1 - (s; \sigma)\phi(s_1)$, $\sigma' = q(1-\bar{r}'')$ tal que $(s'; \sigma')(s; \sigma)\phi(s_1) = s_1$.

rotación generadora de tipo (B) en virtud del Lema 3.1.1. Notar que $(s; \sigma) \in \mathcal{B}(L)$ con $|1 - r'| = |i|$. Por otra parte, como

$$\begin{aligned} |[rq(1 - \bar{r}') + \lambda \epsilon 2^t q \bar{\lambda}'] (1 - \bar{r}')^{-1} q^{-1} (1 - r')| &= \\ |rq(1 - \bar{r}') + \lambda \epsilon 2^t q \bar{\lambda}'] &= |1 - \bar{r}'| = |i| \end{aligned}$$

y $|1 - r| = |2|$, se tiene que $|1 - r''| = |i|$. Por lo tanto, existe el conjunto $\mathcal{B}_1(L)$.

u	q	r'
-5	$j + k$	$1 - 6\omega - 13i - 6i\omega$
-1	$i + j$	$-1 - 6\omega - 3i$

Tabla 5.3: r' para construir $\mathcal{B}_1(L)$.

Para probar la existencia de $\mathcal{B}_2(L)$, basta probar² que si $\phi \in \mathcal{B}(L)$ es tal que $|\lambda| < 1$, existe $(s; \sigma) \in \mathcal{B}(L)$ tal que $|\lambda'| = 1$ y $|\lambda''| = 1$, donde $\lambda, \lambda', \lambda''$ son definidos por $\phi, (s; \sigma)$ y $(s; \sigma)\phi$ respectivamente, como en el caso anterior. De la ecuación 5.6 se observa que $|\lambda''| = 1$ si $|\lambda| < 1$ y $|\lambda'| = 1$. Por otra parte, para asegurar que $(s; \sigma) \in \mathcal{B}(L)$, es decir, $|1 - r'| \geq |2|$ basta escoger $r' \in \mathcal{O}_D$ tal que $|1 - r'| = |i|$ si $|1 - r| = |2|$, o $r' \in \mathcal{O}_D$ tal que $|1 - r'| = |2|$ si $|1 - r| = |i|$, debido a la ecuación 5.5. Por los lemas 4.3.1, 4.3.2 existe $r' \in \mathcal{O}_D$ (ver tabla 5.4 en la siguiente página) tal que

$$|1 - r'| = |i|, \text{ si } |1 - r| = |2|, \quad |1 - r'| = |2|, \text{ si } |1 - r| = |i|,$$

$$NzN(\epsilon 2^t q) \in \mathbb{Q}_2^{*2} \quad \text{y} \quad NzN(\epsilon 2^t q)^{-1} \in \mathbb{Z}_2^*,$$

donde $z = q - r'q\bar{r}'$. Así, por el Corolario 4.1.1.1 existe $\lambda' \in \mathcal{O}_D$ con $|\lambda'| = 1$, tal que $q = r'q\bar{r}' + \epsilon 2^t \lambda' q \bar{\lambda}'$. Por lo tanto $(s; \sigma)$ con $s = (1 - r')s_1 - \lambda's_2$, $\sigma = q(1 - \bar{r}')$ define una rotación generadora de tipo (B) en virtud del Lema 3.1.1 y esta rotación satisface $|\lambda'| = 1$. Por lo tanto, existe el conjunto $\mathcal{B}_2(L)$. □

²Esto debido a que, en tal caso, existe un segundo elemento $(s'; \sigma') \in \mathcal{B}_2(L)$ definido por $s' = s_1 - (s; \sigma)\phi(s_1)$, $\sigma' = q(1 - \bar{r}'')$ tal que $(s'; \sigma')(s; \sigma)\phi(s_1) = s_1$.

u	q	t	$ 1-r $	r'
-5	$j+k$	3	$ i $	$-1-4i-4i\omega$
-5	$j+k$	3	$ 2 $	$1-14\omega-i-10i\omega$
-5	$j+k$	4	$ i $	$-1-8i-8i\omega$
-5	$j+k$	4	$ 2 $	$1-6\omega-13i-6i\omega$
-1	$i+j$	3	$ i $	$-1-4i\omega$
-1	$i+j$	3	$ 2 $	$1-2\omega-i$
-1	$i+j$	4	$ i $	$-1-8i\omega$
-1	$i+j$	4	$ 2 $	$-1-6\omega-3i$

Tabla 5.4: r' para construir $\mathcal{B}_2(L)$.

Observación 5.1.2. Notemos que para un reticulado Λ como en el Lema anterior, podemos cambiar $\mathcal{B}(\Lambda)$ por $\mathcal{B}_l(\Lambda)$, $l = 1, 2$ en el Teorema 4.2.1. Así, para los generadores en $\mathcal{B}_2(L)$ tenemos que, si $z = q - rq\bar{r}$, entonces $|z| = |2^t|$ pues $|z| = |2^t \lambda q \bar{\lambda}|$.

La observación anterior nos dice que podemos reducir bastante el conjunto finito \mathcal{S} que aparece en la Proposición 4.2.2, establecemos esta mejora como una proposición, cuya demostración es análoga a la demostración de la Proposición 4.2.2 y la incluimos para mayor claridad.

Proposición 5.1.2. *Existe $r \in \mathcal{O}_D$ que cumple las condiciones en 5 del Teorema 4.2.1 para $t \in \{3, 4\}$ y $Na_1 \in -u\mathbb{Q}_2^{*2}$, con u unidad de defecto cuadrático no minimal si y sólo si existe $\alpha = a + b\omega + ci + di\omega \in \mathbb{Z} \oplus \mathbb{Z}\omega \oplus \mathbb{Z}i \oplus \mathbb{Z}i\omega \subset \mathcal{O}_D$, con $0 \leq a, b, d, c < 2^{t+3}$, que las cumple.*

Demostración: Si $r \in \mathcal{O}_D$ satisface las condiciones en 5 del Teorema 4.2.1, existe $(s; \sigma) \in \mathcal{B}(\Lambda)$, es decir, $s = (1 - r_0)s_1 - \lambda s_2$, con $|1 - r_0| \geq 2$ y $\sigma = a_1(1 - \bar{r}_0)$, tal que $N(1 - r_0) \notin N(k(a_1)^*)$. Es claro que $r_0 \in \mathcal{O}_D$ también satisface las condiciones en 5 de 4.2.1. Sea $\alpha = a + b\omega + ci + di\omega \in \mathcal{O}_D$ un representante de la clase de r_0 módulo 2^{t+3} . Así, $r_0 = \alpha + 2^{t+3}\beta$, con $\beta \in \mathcal{O}_D$ y donde podemos considerar $a, b, c, d \in \mathbb{Z}$ tales que $0 \leq a, b, d, c < 2^{t+3}$ puesto que \mathbb{Z} es denso en \mathbb{Z}_2 . Entonces $1 - r_0 = 1 - \alpha - 2^{t+3}\beta$ y por lo tanto $N(1 - r_0) = N(1 - \alpha)N(1 - (1 - \alpha)^{-1}2^{t+3}\beta)$. Como $|1 - r_0| \geq |2|$ (ver Obs. 4.2.1), entonces $|1 - \alpha| \geq |2|$ y por lo tanto $N(1 - (1 - \alpha)^{-1}2^{t+3}\beta)$ es un

cuadrado. Así,

$$\left(\frac{N(1-r_0), -Na_1}{\mathfrak{p}} \right) = \left(\frac{N(1-\alpha), -Na_1}{\mathfrak{p}} \right).$$

Por otra parte, si $z = a_1 - r_0 a_1 \bar{r}_0$ y $z' = a_1 - \alpha a_1 \bar{\alpha}$, entonces $z = z' - 2^{t+3}\gamma$, con $\gamma \in \mathcal{O}_D$. Luego, $|z'| = |z| = |2^t|$ (ver Obs. 5.1.2) y $Nz = Nz'N(1 - z'^{-1}2^{t+3}\gamma)$ con $|z'^{-1}2^{t+3}\gamma| \leq |8|$. Por lo tanto,

$$NzNa_1 \text{ es un cuadrado} \Leftrightarrow Nz'Na_1 \text{ es un cuadrado.}$$

Finalmente, como $|z| = |z'|$, es decir, $|Nz|_k = |Nz'|_k$ se tiene que

$$|Nz/2^{2l}N(a_1)|_k = 1 \Leftrightarrow |Nz'/2^{2l}N(a_1)|_k = 1.$$

□

Corolario 5.1.2.1. *Si $\Lambda = \langle a_1 \rangle \perp \langle a_2 \rangle$ es un \mathcal{O}_D -reticulado anti-hermitiano tal que $N(a_1), N(a_2) \in -u\mathbb{Q}_2^{*2}$, con u unidad de defecto cuadrático no minimal y $\mu = \nu(a_2) - \nu(a_1)$ satisface $\nu(8) \leq \mu \leq \nu(16)$, entonces $H(\Lambda) = N(\mathbb{Q}_2(a_1)^*)$.*

Demostración: Es una consecuencia directa de la Proposición y los lemas 3.3.4, 4.3.5. □

Necesitamos un último Lema previo a la siguiente Proposición, el cual nos ayudará a resolver el caso I cuando $\mu = \nu(8)$.

Lema 5.1.4. *Existe $\eta = a + b\omega + ci + di\omega \in \mathcal{O}_D$, que cumple las condiciones*

1. $|\eta| = |i|$,
2. $T(\xi) \equiv 1 \pmod{2}$, donde $\xi = 2(\eta a_1 \bar{\eta})^{-1} a_1$ y $a_1 \in \{j+k, j+i\}$

si y sólo si existe $\eta = a + b\omega + ci + di\omega \in \mathbb{Z} \oplus \mathbb{Z}\omega \oplus \mathbb{Z}i \oplus \mathbb{Z}i\omega \subset \mathcal{O}_D$, con $0 \leq a, b, c, d < 4$, que las cumple.

Demostración: Sea $\eta \in \mathcal{O}_D$ y sea $\alpha \in \mathcal{O}_D$ un representante de la clase de η módulo 4 del tipo descrito en el enunciado. Así, $\eta = \alpha + 4\beta$, donde $\beta \in \mathcal{O}_D$ y $\alpha = a + b\omega + ci + di\omega \in \mathbb{Z} \oplus \mathbb{Z}\omega \oplus \mathbb{Z}i \oplus \mathbb{Z}i\omega \subset \mathcal{O}_D$, con $0 \leq a, b, c, d < 4$ (\mathbb{Z} es denso en \mathbb{Z}_2). Es claro que

$$|\eta| = |i| \Leftrightarrow |\alpha| = |i|.$$

Por otra parte, se tiene que

$$\eta a_1 \bar{\eta} = \alpha a_1 \bar{\alpha} + 4(\alpha a_1 \bar{\beta} + \beta a_1 \bar{\alpha} + 4\beta a_1 \bar{\beta}),$$

de donde

$$N(\eta a_1 \bar{\eta}) = N(\alpha a_1 \bar{\alpha}) N(1 + 4(\alpha a_1 \bar{\alpha})^{-1}(\alpha a_1 \bar{\beta} + \beta a_1 \bar{\alpha} + 4\beta a_1 \bar{\beta})).$$

Aquí, $1 + 4(\alpha a_1 \bar{\alpha})^{-1}(\alpha a_1 \bar{\beta} + \beta a_1 \bar{\alpha} + 4\beta a_1 \bar{\beta}) \in \mathcal{O}_D^*$ pues $4(\alpha a_1 \bar{\alpha})^{-1}(\alpha a_1 \bar{\beta} + \beta a_1 \bar{\alpha} + 4\beta a_1 \bar{\beta}) \in 2\mathcal{O}_D$ si $|\alpha| = |i|$. Luego $N(1 + 4(\alpha a_1 \bar{\alpha})^{-1}(\alpha a_1 \bar{\beta} + \beta a_1 \bar{\alpha} + 4\beta a_1 \bar{\beta})) \equiv 1 \pmod{2}$. Finalmente, como $(\eta a_1 \bar{\eta})^{-1} = -\eta a_1 \bar{\eta} N(\alpha a_1 \bar{\alpha})^{-1} N(1 + 4(\alpha a_1 \bar{\alpha})^{-1}(\alpha a_1 \bar{\beta} + \beta a_1 \bar{\alpha} + 4\beta a_1 \bar{\beta}))^{-1}$ obtenemos que

$$2(\eta a_1 \bar{\eta})^{-1} a_1 \equiv 2(\alpha a_1 \bar{\alpha})^{-1} a_1 \pmod{2},$$

por lo cual

$$T(\xi) \equiv 1 \pmod{2} \Leftrightarrow T(\xi_\alpha) \equiv 1 \pmod{2},$$

donde $\xi_\alpha = 2(\alpha a_1 \bar{\alpha})^{-1} a_1$. □

Proposición 5.1.3. *Si $\Lambda = \langle a_1 \rangle \perp \dots \perp \langle a_n \rangle$ es un \mathcal{O}_D -reticulado anti-hermitiano, tal que $N(a_1), \dots, N(a_n) \in -u\mathbb{Q}_2^{*2}$, con u unidad de defecto cuadrático no minimal y la diferencia minimal entre la valuación de las escalas de dos componentes consecutivos es $\nu(8) \leq \mu \leq \nu(16)$, entonces $H(\Lambda) = N(\mathbb{Q}_2(a_1)^*)$.*

Demostración: Consideramos por separado los casos $\mu = \nu(16)$, $\mu = \nu(8)$.

Caso 1: $\mu = \nu(16)$.

Por el Lema 3.3.3 basta considerar rotaciones $(s; \sigma) \in \mathcal{B}(\Lambda)$ tales que $|1 - r| = |2|$

y $|\lambda_2| = 1$. En este caso, por el Lema 3.3.1 nos podemos reducir a calcular $H(\Lambda)$ para $n = 2$ en el enunciado de la proposición. En este caso, por el Lema 5.1.3 sabemos que podemos cambiar Λ por un reticulado L tal que $H(L) = H(\Lambda)$ y un conjunto de generadores de $\mathcal{U}^+(L)$ es $\mathcal{A}(L) \cup \mathcal{B}_1(L)$. Se concluye que $H(\Lambda) = N(\mathbb{Q}_2(a_1)^*)$ pues, por el Lema 3.3.3, las rotaciones en $\mathcal{B}_1(L)$ tienen norma espinorial en $N(\mathbb{Q}_2(a_1)^*)$.

Caso 2: $\mu = \nu(8)$.

Por el Lema 3.3.3, podemos asumir que las rotaciones $(s; \sigma) \in \mathcal{B}(\Lambda)$ satisfacen una de las siguientes condiciones:

1. $|1 - r| = |i|$, $|\lambda_2| = 1$,
2. $|1 - r| = |2|$, $|\lambda_2| \in \{1, |i|\}$.

Por el Lema 3.3.1 podemos reducir los casos en que $|\lambda_2| = 1$ a considerar reticulados de rango 2 y el caso en que $|1 - r| = |2|$, $|\lambda_2| = |i|$ a considerar reticulados de rango 3 con³ $|\lambda_3| = 1$. Para los reticulados de rango 2, el Corolario 5.1 nos dice que $H(\Lambda) = N(\mathbb{Q}_2(a_1)^*)$. Probaremos que para reticulados Λ de rango 3 tales que $(s; \sigma) \in \mathcal{B}(\Lambda)$ satisface $|1 - r| = |2|$, $|\lambda_2| = |i|$, $|\lambda_3| = 1$ también obtenemos $\theta[(s; \sigma)] \subset N(\mathbb{Q}_2(a_1)^*)$. En efecto, por el Lema 3.3.4 podemos asumir que $\Lambda = \langle a_1 \rangle \perp \langle 8\epsilon_2 a_1 \rangle \perp \langle 64\epsilon_3 a_1 \rangle$, con $\epsilon_2, \epsilon_3 \in \mathbb{Z}_2^*$. Así, por el Lema 3.1.1 sabemos que $r, \lambda_2, \lambda_3 \in \mathcal{O}_D$ con $|1 - r| \geq |2|$ definen un elemento $\phi \in \mathcal{B}(\Lambda)$ si y sólo si satisfacen la ecuación

$$z = 8\lambda_2\epsilon_2 a_1 \bar{\lambda}_2 + 64\lambda_3\epsilon_3 a_1 \bar{\lambda}_3,$$

donde $z = a_1 - r a_1 \bar{r}$. Podemos reescribir lo anterior de la siguiente manera:

$$z = 8\lambda_3(\epsilon_2 \eta a_1 \bar{\eta} + 8\epsilon_3 a_1) \bar{\lambda}_3,$$

donde $\eta = \lambda_3^{-1} \lambda_2$. Recordemos que, en este caso, $|\lambda_2| = |i|$ y $|\lambda_3| = 1$. Así, por el Corolario 4.1.1.1, lo anterior equivale a la existencia de $r, \eta \in \mathcal{O}_D$, con $|\eta| = |i|$ tales que $NzN(\epsilon_2 \eta a_1 \bar{\eta} + 8\epsilon_3 a_1) \in \mathbb{Q}_2^{*2}$, $NzN(8(\epsilon_2 \eta a_1 \bar{\eta} + 8\epsilon_3 a_1)^{-1}) \in \mathbb{Z}_2$. Pero sabemos que

³Si $|\lambda_3| < 1$, entonces nos podemos reducir a considerar reticulados de rango 2 (ver Lema 3.3.1).

$|\epsilon_2 \eta a_1 \bar{\eta} + 8\epsilon_3 a_1| = |2|$, por lo tanto,

$$NzN(8(\epsilon_2 \eta a_1 \bar{\eta} + 8\epsilon_3 a_1)^{-1}) \in \mathbb{Z}_2 \Leftrightarrow Nz/2^8 \in \mathbb{Z}_2.$$

Por otra parte, $N(\epsilon_2 \eta a_1 \bar{\eta} + 8\epsilon_3 a_1) = N(\epsilon_2 \eta a_1 \bar{\eta})N(1 + 8\epsilon(\eta a_1 \bar{\eta})^{-1}a_1)$, donde $\epsilon = \epsilon_2^{-1}\epsilon_3 \in \mathbb{Z}_2^*$. En tal caso, como $|8\epsilon(\eta a_1 \bar{\eta})^{-1}a_1| = |4|$, podemos escribir, $8\epsilon(\eta a_1 \bar{\eta})^{-1}a_1 = 4\epsilon\xi$ con $\xi = 2(\eta a_1 \bar{\eta})^{-1}a_1 \in \mathcal{O}_D^*$ y se tiene que

$$N(1 + 4\epsilon\xi) = 1 + 4\epsilon \text{tr}(\xi) + 16\epsilon^2 N(\xi).$$

Como $T(\xi) = 2x + y$, con $x, y \in \mathbb{Z}_2$ se tiene que $N(1 + 4\epsilon\xi) \in \{\mathbb{Q}_2^{*2}, 5\mathbb{Q}_2^{*2}\}$. Así, $N(\epsilon_2 \eta a_1 \bar{\eta} + 8\epsilon_3 a_1) \in \{N(a_1)\mathbb{Q}_2^{*2}, 5N(a_1)\mathbb{Q}_2^{*2}\}$, donde $N(\epsilon_2 \eta a_1 \bar{\eta} + 8\epsilon_3 a_1) \in 5N a_1 \mathbb{Q}_2^{*2}$ si y sólo si $T(\xi) \equiv 1 \pmod{2}$. Esta última condición no se satisface por los lemas 5.1.4 y 4.3.6. Por lo tanto, en este caso, tenemos un análogo al Teorema 4.2.1: $H(\Lambda) = \mathbb{Q}_2^*$ si y sólo si existe $r \in \mathcal{O}_D$, con $|1 - r| = |2|$ tal que:

1. $\left(\frac{N(1-r), -Na_1}{p}\right) = -1$,
2. $NzNa_1 \in \mathbb{Q}_2^{*2}$,
3. $|z| = |16|$.

El Corolario 5.1 implica que no existe $r \in \mathcal{O}_D$ que satisfaga las condiciones arriba. Por lo tanto concluimos que $H(\Lambda) = N(\mathbb{Q}_2(a_1)^*)$.

□

5.2. Caso II

Por la discusión realizada al comienzo del capítulo, consideraremos reticulados Λ de la forma $\langle i \rangle \perp \langle \epsilon i \rangle$, donde $\epsilon \in \mathbb{Q}_2^*$ y $\nu(4) < \nu(\epsilon) \leq \nu(16)$. En este caso, el cálculo depende del parámetro uniformizante, por lo que escribiremos $i = i_\pi$ para mayor claridad.

Proposición 5.2.1. *Si $\Lambda = \langle a_1 \rangle \perp \dots \perp \langle a_n \rangle$ es un \mathcal{O}_D -reticulado anti-hermitiano, con $N(a_1), \dots, N(a_n) \in \pi\mathbb{Q}_2^{*2}$, y la diferencia minimal entre la valuación de las escalas de dos componentes consecutivos es μ , con $\nu(4) < \mu \leq \nu(16)$, entonces $H(\Lambda) = \mathbb{Q}_2^*$.*

Demostración: Basta probarlo para $n = 2$. Por Lema 3.3.4 podemos suponer que el subreticulado $\langle a_1 \rangle \perp \langle a_2 \rangle$ es de la forma $L_t = \langle i_\pi \rangle \perp \langle \epsilon \pi^t i_\pi \rangle$, con $\epsilon \in \mathbb{Z}_2^*$, $t \in \{3, 4\}$, es decir, $L_t = \mathcal{O}_D s_1 + \mathcal{O}_D s_2$, donde $h(s_1, s_1) = i_\pi$, $h(s_2, s_2) = \epsilon \pi^t i_\pi$ y $h(s_1, s_2) = 0$. Además, como $i_\pi^2 = \pi$ y $\pi \mathbb{Q}_2^{*2} \in \{\pm 2\mathbb{Z}_2^{*2}, \pm 10\mathbb{Z}_2^{*2}\}$, basta considerar los casos $i = i_\pi$, para $\pi \in \{\pm 2, \pm 10\}$. Es claro que si $H(L_t) = \mathbb{Q}_2^*$, entonces $H(\Lambda) = \mathbb{Q}_2^*$. El Lema 4.3.4 junto con el Teorema 4.2.1 nos dicen que $H(L_t) = \mathbb{Q}_2^*$. \square

Concluimos esta sección con una tabla, la cual contiene todos los cálculos de la norma espinorial cuando el cuerpo es \mathbb{Q}_2 :

s	$ A $	α	μ	$H(\Lambda)$	Referencia
-	> 1	-	-	\mathbb{Q}_2^*	Obs. 3.2.1
0	1	$-\tilde{\Delta}$	-	$\mathbb{Z}_2^* \mathbb{Q}_2^{*2}$	Tabla 1.2
0	1	$-\tilde{u}$	$\mu \geq \nu(8)$	$N(\mathbb{Q}_2(a_m)^*)$	Prop. 5.1.3 + Tabla 1.2
0	1	$-\tilde{u}$	$0 < \mu < \nu(8)$	\mathbb{Q}_2^*	Prop. 5.1.1
0	1	$\tilde{\pi}$	$\mu > \nu(16)$	$N(\mathbb{Q}_2(a_m)^*)$	Tabla 1.2
0	1	$\tilde{\pi}$	$0 < \mu < \nu(16)$	\mathbb{Q}_2^*	Prop. 5.2.1 + Prop.3.3.1 + Tabla 1.2
$\neq 0$	-	-	-	\mathbb{Q}_2^*	Tabla 1.2

Tabla 5.5: Cálculos completos sobre \mathbb{Q}_2 para reticulados arbitrarios (no modulares) de cualquier rango.

5.3. Aplicaciones

Caso I con $u = -1, \mu = \nu(8)$.

Consideremos $\Lambda = \langle i + j \rangle \perp \langle 8(i + j) \rangle$, donde $D = \left(\frac{2,5}{\mathbb{Q}}\right)$. D ramifica sólo en 2 y 5. Además, Λ es unimodular para $p \neq 7$. Así, $H(\Lambda_p) = \mathbb{Z}_p^* \mathbb{Q}_p^{*2}$ para $p \neq 2, 5, 7$ por [8] y $H(\Lambda_5) = \mathbb{Z}_5^* \mathbb{Q}_5^{*2}$ por [6]. Luego, el cuerpo de clase espinorial Σ_Λ satisface $\Sigma_\Lambda \subset \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{7})$. Por otra parte, como el álgebra se descompone en infinito y la forma cuadrática asociada es indefinida, se tiene que en cada género espinorial hay sólo una clase y Σ_Λ satisface $\Sigma_\Lambda \subset \mathbb{R}$. De lo anterior y el hecho de que $H(\Lambda_2) = N(\mathbb{Q}_2(i + j)^*) = N(\mathbb{Q}_2(\sqrt{7}))$ (ver Tabla 5.5), se concluye que $\Sigma_\Lambda \subset \mathbb{Q}(\sqrt{7})$. Para $p = 7$ el álgebra se descompone y la forma cuadrática asociada a $\langle i + j \rangle$ tiene

discriminante $N(i + j) = -7$. Por lo tanto, el reticulado cuadrático asociado a Λ tiene una descomposición del tipo

$$\langle a \rangle \perp \langle -7a \rangle \perp \langle 8a \rangle \perp \langle -56a \rangle,$$

donde $a \in \mathbb{Z}_7^*$. Por lo tanto, si $\langle a \rangle \perp \langle 8a \rangle = \mathbb{Z}_7 e_1 \perp \mathbb{Z}_7 e_2$, consideramos la rotación $\tau_{e_1} \tau_{3e_1 + e_2}$, obteniendo $\theta(\tau_{e_1} \tau_{3e_1 + e_2}) = 3\mathbb{Q}_7^{*2}$. Esto nos dice que Σ_Λ es descompuesto en 7 pues $3 \notin N(\mathbb{Q}_7(\sqrt{7})^*)$. Concluimos que $\Sigma_\Lambda = \mathbb{Q}$ y por lo tanto el número de clases de Λ es 1, es decir, Λ satisface el principio de Hasse.

Caso II con $\pi = 2, \mu = \nu(2^t)$.

Consideremos $\Lambda = \langle i \rangle \perp \langle 2^t i \rangle$, para $t > 0$, donde $D = \left(\frac{2,5}{\mathbb{Q}}\right)$. D ramifica solamente en 2 y en 5. Entonces, como para $p \neq 2$, Λ es unimodular, se tiene que $H(\Lambda_p) = \mathbb{Z}_p \mathbb{Q}_p^{*2}$ para todo $p \neq 2$, por los cálculos en [8] para $p \neq 5$, y por [6, Teorema 4] para $p = 5$. Así, el cuerpo de clase espinorial Σ_Λ puede ramificar sólo en 2 e ∞ y se tiene que $\Sigma_\Lambda \subset \mathbb{Q}(\sqrt{-1}, \sqrt{2})$. Notemos también que el álgebra D se descompone en infinito y la forma cuadrática correspondiente al reticulado Λ es indefinida. Esto último implica que hay solamente una clase en cada género espinorial y que $\Sigma_\Lambda \subset \mathbb{R}$. Por otra parte, para $p = 2$, la Tabla 5.5 nos dice que $H(\Lambda_2) = \mathbb{Q}_2^*$ para $t \leq 4$ y $H(\Lambda_2) = N(\mathbb{Q}_2(i)^*)$ para $t > 4$, lo cual implica que Σ_Λ se descompone en 2 para $t \leq 4$ y Σ_Λ ramifica en 2 para $t > 4$. Por lo tanto $\Sigma_\Lambda = \mathbb{Q}$ para $t \leq 4$ y $\Sigma_\Lambda = \mathbb{Q}(\sqrt{2})$ para $t > 4$. En el primer caso, tenemos principio de Hasse para Λ , y en el segundo el número de clases de Λ es 2.

Apéndice A

Tabla de símbolos de Hilbert $\left(\frac{\alpha, \beta}{p}\right)$

Consideramos $k_p = \mathbb{Q}_2$ en todo lo que sigue. Como $\left(\frac{\alpha, \beta}{p}\right) = \left(\frac{\alpha\eta^2, \beta\lambda^2}{p}\right)$, $\forall \eta, \lambda \in \mathbb{Q}_2^*$, basta calcular $\left(\frac{\alpha, \beta}{p}\right)$ para $\alpha, \beta \in \{\pm 1, \pm 2, \pm 5, \pm 10\}$ pues $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2} = \{\pm 1, \pm 2, \pm 5, \pm 10\}$.

Los cálculos se encuentran en la siguiente tabla y son justificados posteriormente:

$\left(\frac{\cdot}{p}\right)$	1	-1	2	-2	5	-5	10	-10
1	1	1	1	1	1	1	1	1
-1	1	-1	1	-1	1	-1	1	-1
2	1	1	1	1	-1	-1	-1	-1
-2	1	-1	1	-1	-1	1	-1	1
5	1	1	-1	-1	1	1	-1	-1
-5	1	-1	-1	1	1	-1	-1	1
10	1	1	-1	-1	-1	-1	1	1
-10	1	-1	-1	1	-1	1	1	-1

Es claro que $\left(\frac{1, \beta}{p}\right) = 1, \forall \beta \in \mathbb{Q}_2$. Por otra parte, en virtud de [10, 63:11a]:

$$\left(\frac{\pm 2, 5}{p}\right) = -1, \quad \left(\frac{\pm 10, 5}{p}\right) = -1, \quad \left(\frac{\pm 1, 5}{p}\right) = 1, \quad \left(\frac{\pm 5, 5}{p}\right) = 1.$$

De las Proposiciones 57:9, 57:10 de [10] se desprenden las siguientes propiedades

$$\left(\frac{\alpha, 1-\alpha}{p}\right) = \left(\frac{\alpha, -\alpha}{p}\right) = 1, \quad \left(\frac{\alpha, \beta}{p}\right) \left(\frac{\alpha, \gamma}{p}\right) = \left(\frac{\alpha, \beta\gamma}{p}\right), \quad \left(\frac{\alpha, \alpha\beta}{p}\right) = \left(\frac{\alpha, -\beta}{p}\right).$$

De la fórmula producto para el símbolo de Hilbert y el hecho de que $\left(\frac{u,v}{\mathbb{Q}_p}\right) \cong \mathbb{M}_2(\mathbb{Q}_p)$ para todo $p \neq 2$, donde $u, v \in \mathbb{Z}_2^*$, se obtiene que $\left(\frac{-1,-1}{p}\right) = -1$ ya que $\left(\frac{-1,-1}{\mathbb{R}}\right)$ es álgebra de división. Usando lo anterior y el hecho de que $\left(\frac{\alpha,\beta}{p}\right) = \left(\frac{\beta,\alpha}{p}\right)$ calculamos:

1. $\left(\frac{\cdot,-1}{p}\right)$:

$$\begin{aligned} \left(\frac{2,-1}{p}\right) &= \left(\frac{2,1-2}{p}\right) = 1, & \left(\frac{-2,-1}{p}\right) &= \left(\frac{-1,-1}{p}\right) \left(\frac{2,-1}{p}\right) = -1, \\ \left(\frac{5,-1}{p}\right) &= \left(\frac{-1,5}{p}\right) = 1, & \left(\frac{-5,-1}{p}\right) &= \left(\frac{-1,-1}{p}\right) \left(\frac{5,-1}{p}\right) = -1, \\ \left(\frac{10,-1}{p}\right) &= \left(\frac{5,-1}{p}\right) \left(\frac{2,-1}{p}\right) = 1, & \left(\frac{-10,-1}{p}\right) &= \left(\frac{-1,-1}{p}\right) \left(\frac{10,-1}{p}\right) = -1. \end{aligned}$$

2. $\left(\frac{\cdot,2}{p}\right)$:

$$\begin{aligned} \left(\frac{-2,2}{p}\right) &= 1, & \left(\frac{2,2}{p}\right) &= \left(\frac{-1,2}{p}\right) \left(\frac{-2,2}{p}\right) = -1, \\ \left(\frac{5,2}{p}\right) &= \left(\frac{2,5}{p}\right) = -1, & \left(\frac{-5,2}{p}\right) &= \left(\frac{-1,2}{p}\right) \left(\frac{5,2}{p}\right) = 1, \\ \left(\frac{10,2}{p}\right) &= \left(\frac{5,2}{p}\right) \left(\frac{2,2}{p}\right) = 1, & \left(\frac{-10,2}{p}\right) &= \left(\frac{-1,2}{p}\right) \left(\frac{10,2}{p}\right) = -1. \end{aligned}$$

3. $\left(\frac{\cdot,-2}{p}\right)$:

$$\begin{aligned} \left(\frac{-2,-2}{p}\right) &= \left(\frac{-1,-2}{p}\right) \left(\frac{2,-2}{p}\right) = -1, & \left(\frac{5,-2}{p}\right) &= \left(\frac{-2,5}{p}\right) = -1, \\ \left(\frac{-5,-2}{p}\right) &= \left(\frac{-1,-2}{p}\right) \left(\frac{5,-2}{p}\right) = 1, & \left(\frac{10,-2}{p}\right) &= \left(\frac{5,-2}{p}\right) \left(\frac{2,-2}{p}\right) = -1, \\ \left(\frac{-10,-2}{p}\right) &= \left(\frac{-1,-2}{p}\right) \left(\frac{10,-2}{p}\right) = 1. \end{aligned}$$

4. $\left(\frac{\cdot,-5}{p}\right)$:

$$\left(\frac{-5,-5}{p}\right) = \left(\frac{-1,-5}{p}\right) \left(\frac{5,-5}{p}\right) = -1, \quad \left(\frac{10,-5}{p}\right) = \left(\frac{5,-5}{p}\right) \left(\frac{2,-5}{p}\right) = -1,$$

$$\left(\frac{-10, -5}{p}\right) = \left(\frac{-1, -5}{p}\right) \left(\frac{10, -5}{p}\right) = 1.$$

5. $\left(\frac{\cdot, 10}{p}\right)$:

$$\left(\frac{10, 10}{p}\right) = \left(\frac{5, 10}{p}\right) \left(\frac{2, 10}{p}\right) = 1, \quad \left(\frac{-10, 10}{p}\right) = 1.$$

6. $\left(\frac{\cdot, -10}{p}\right)$:

$$\left(\frac{-10, -10}{p}\right) = \left(\frac{-1, -10}{p}\right) \left(\frac{10, -10}{p}\right) = -1.$$

Referencias

- [1] L.E. Arenas-Carmona, *Applications of spinor class fields: embeddings of orders and quaternionic lattices*, Ann. Inst. Fourier **53** (2003), 2021–2038.
- [2] ———, *Spinor norm for local skew-hermitian forms*, Contemporary Math. **344** (2004), 19–29.
- [3] ———, *Integral springer theorem for quaternionic forms*, Nagoya Math. **187** (2007), 157–174.
- [4] ———, *Representation fields for quaternionic skew-hermitian forms*, Arch. Math. **94** (2010), 351–356.
- [5] C.N. Beli, *Integral spinor norm groups over dyadic local fields*, Journal of Number Theory **102** (2003), 125–182.
- [6] S. Böge, *Spinorgeschlechter schiefhermitescher formen*, Arch. Math. **XXI** (1970), 172–184.
- [7] A. G. Earnest and J. S. Hsia, *Spinor norms of local integral rotations 2*, Pacific J. Math. **61** (1975), 71–86.
- [8] M. Kneser, *Klassenzahlen indefiniter quadratischen formen in drei oder mehr veränderlichen*, Arch. Math. **VII** (1956), 323–332.
- [9] ———, *Lectures on galois cohomology of classical groups*, TATA Institute of Fundamental Research, Bombay, 1969.
- [10] O.T. O’Meara, *Introduction to quadratic forms*, Classics in Mathematics, Springer, 1973.

- [11] V. P. Platonov, Bondarenko, and Rapinchuk, *Class numbers and groups of algebraic groups*, Math. USSR Izv. 14 (1980), 547–569.
- [12] W. Scharlau, *Quadratic and hermitian forms*, Academic Press, New York, 1985.
- [13] E. A. M. Seip-Hornix, *Clifford algebras of quadratic quaternion forms*, Proc. Kon. Ned. Akad. Wet. 68 (1965), 326–363.
- [14] W. Stein et al., *Sage mathematics software*, The Sage Development Team, <http://www.sagemath.org>, version 4.3 ed., 2009.
- [15] M. F. Vignéras, *Arithmétique des algèbres de quaternions*, Springer, Berlin, 1980.
- [16] Gordon E. Wall, *The structure of a unitary factor group*, Publications mathématiques de l'I.H.É.S. 1 (1959), 7–23.
- [17] Fei Xu, *Integral spinor norms in dyadic local fields 1*, Pacific J. Math. 157 (1993), 179–200.