Rev.R.Acad.Cienc.Exact.Fis.Nat. (Esp)
Vol. 94, N.º 3, pp 397-416, 2000
Monográfico: Contribuciones al estudio algorítmico de problemas de moduli aritméticos

CORRESPODENCIA ENTRE FORMAS TERNARIAS ENTERAS Y ÓRDENES CUATERNIÓNICOS[1]

P. LLORENTE

Funes 3350. Departamento de Matemáticas. Facultad de Ciencias Exactas y Naturales. Universidad Nacional de Mar del Plata. 7600 Mar del Plata. Argentina. E-mail: llorente@argenet.com.ar

ABSTRACT

En este trabajo se interpreta, en términos de álgebras de Clifford, y se demuestra completamente la correspondencia entre formas ternarias enteras y órdenes cuaterniónicos descubierta por Brandt [3]. La demostración es constructiva y permite el cálculo efectivo. También se dan ejemplos de la correspondencia y de algunas aplicaciones de la misma. La exposición es esencialmente autocontenida.

INTRODUCCIÓN

Es sabido que existe una correspondecia inmediata entre las formas unarias enteras y los órdenes de cuerpos cuadráticos, y que una estrecha relación liga el estudio de las formas binarias enteras con la aritmética de tales órdenes. Si deseamos obtener una situación similar para formas ternarias y cuaternarias enteras, debemos sustituir los cuerpos cuadráticos por las álgebras de cuaterniones racionales y considerar sus órdenes. De mantenerse la similitud con las dimensiones más bajas, debería existir una correspondencia entre las formas ternarias enteras y los órdenes cuaterniónicos. Este es el tema central del presente estudio. Históricamente, el primero en considerar las álgebras de cuaterniones racionales fue Hermite [6], en 1854, en su estudio de las formas cuadráticas (ver Observación 1.21 más adelante), pero el desarrollo del tema que nos ocupa se produjo, en su mayor parte, entre los años 1920 y 1945. Latimer [7], en 1937, establece una correspondencia parcial entre formas ternarias enteras y órdenes cuaterniónicos (ver Sección 2.3) y finalmente Brandt [3], en 1941, presenta una correspondencia completa.

El objetivo principal de este trabajo es el estudio de esta correspondencia desde un punto de vista a la vez conceptual y algorítmico.

El trabajo consta de tres partes y el contenido de las mismas es el siguiente:

En la Parte 1 se reúnen las definiciones y los resultados previos necesarios. Muchos de ellos son bien conocidos pero, lamentablemente, no siempre existen referencias adecuadas que los incluyan en su totalidad. Tampoco las definiciones y las notaciones que utilizan los distintos autores suelen ser coherentes. Por tal motivo y para la comodidad del lector, hemos preferido intentar una exposición esencialmente autocontenida y en un estilo más clásico. Las dos primeras secciones contienen las definiciones y los resultados básicos sobre formas cuadráticas, espacios cuadráticos, álgebras de cuaterniones y el álgebra de Clifford. Las dos últimas están dedicadas a las formas ternarias enteras y a los órdenes cuaterniónicos, respectivamente.

La Parte 2 contiene los resultados fundamentales de este estudio. En la primera sección se construye y estudia el orden de Clifford asociado a una forma ternaria entera y en la siguiente se muestra que dicha asociación define una correspondencia entre las clases de formas ternarias enteras y las clases de órdenes cuaterniónicos (ver Teorema 2.16). En las dos secciones siguientes se relaciona esta correspondencia con las obtenidas por Latimer y por Brandt. La última sección está dedicada a las determinaciones algorítmicas efectivas.

En la Parte 3 se incluyen algunos ejemplos de la correspondencia y de algunas aplicaciones de la misma.

Los resultados establecidos en este trabajo tienen diversas consecuencias y aplicaciones. Tanto éstas, como la extensión de la correspondencia a situaciones más generales, deberán ser objeto de estudios futuros.

Debo agradecer a Gonzalo Tornaría por su valiosa colaboración en algunos tramos de este estudio y a Pilar Bayer por sus sugerencias y por su estímulo permanente.

[1] Este trabajo es parte del PROYECTO TEORÍA DE NÚMEROS, Subsidio EXA 100/97, Universidad Nacional de Mar del Plata, Argentina.

1. FORMAS CUADRÁTICAS Y CUATERNIONES

En lo que sigue reuniremos las definiciones y los resultados previos necesarios para estudiar la correspondencia entre formas ternarias enteras y órdenes cuaterniónicos.

1.1. Formas cuadráticas y espacios cuadráticos

Sea **A** un dominio de característica ≠2. Llamaremos *forma cuadrática* (o simplemente *forma*) sobre **A** a todo polinomio homogéneo de grado 2:

$$(1)\quad f = f(x_1,\ldots, x_n) = a_{11}x_1^2 + a_{12}x_1x_2 + \cdots + a_{nn}x_n^2$$

con coeficientes $a_{ij} \in \mathbf{A}$. Diremos que f es una forma unaria, binaria, ternaria o cuaternaria según que $n = 1, 2, 3$ o 4. Si $\mathbf{A} = \mathbf{Q}$, el cuerpo de los números racionales, diremos que f es una forma racional. Si $\mathbf{A} = \mathbf{Z}$, el anillo de los números enteros, diremos que f es una forma entera. Diremos que f es *diagonal* si $a_{ij} = 0$ para $i \neq j$, y la denotaremos $f = \mathrm{diag}(a_{11}, \ldots, a_{nn})$.

Definimos la *matriz* de la forma cuadrática f como

$$\mathbf{M}(f) = \begin{Vmatrix} a_{11} & a_{12}/2 & \cdots & a_{1n}/2 \\ a_{12}/2 & a_{22} & \cdots & a_{2n}/2 \\ \vdots & \vdots & \vdots & \vdots \\ a_{1n}/2 & a_{2n}/2 & \cdots & a_{nn} \end{Vmatrix}$$

que verifica

$$(2)\qquad f(x_1, \ldots, x_n) = {}^t\mathbf{x} \cdot \mathbf{M}(f) \cdot \mathbf{x},$$

donde ${}^t\mathbf{x} = \|x_1 \cdots x_n\|$ y ${}^tA$ denota la transpuesta de una matriz A.

Llamaremos *determinante* de f, y lo denotaremos $\det(f)$, al determinante de $\mathbf{M}(f)$. Una forma f es *regular* si $\det(f) \neq 0$ y *singular* en caso contrario. En este trabajo supondremos que toda forma cuadrática es regular.

Sean f y g dos formas cuadráticas sobre **A**. Diremos que *f representa a g* si existe una matriz **M** con coeficientes en **A** tal que $\mathbf{M}(g) = {}^t\mathbf{M} \cdot \mathbf{M}(f) \cdot \mathbf{M}$, en cuyo caso diremos que $g = \mathbf{M} \cdot f$. Las formas f y g son **A**-*equivalentes* si $g = \mathbf{M} \cdot f$ con $\mathbf{M} \in \mathbf{GL}(n, \mathbf{A})$. Llamaremos *automorfa* de la forma f a toda $\mathbf{M} \in \mathbf{GL}(n, \mathbf{A})$ tal que $f = \mathbf{M} \cdot f$. El conjunto de las automorfas de f es un subgrupo de $\mathbf{GL}(n, \mathbf{A})$.

Es claro que la **A**-equivalencia es una relación de equivalencia entre las formas cuadráticas sobre **A** que, por (2), se corresponde con los cambios lineales de las variables.

Una forma cuadrática sobre **A** es *diagonalizable* si es **A**-equivalente a una forma diagonal. Si **A** es un cuerpo, toda forma sobre **A** es diagonalizable, pero esto no es cierto en general.

Observación 1.1. *De las definiciones anteriores se sigue que si f y g son dos formas cuadráticas* **A**-*equivalentes, entonces* $\det(g) = a^2 \det(f)$, *donde $a \in \mathbf{A}$ es un elemento inversible en* **A**.

El estudio de las formas cuadráticas sobre **A** y el de sus clases de **A**-equivalencia puede realizarse considerando los *espacios cuadráticos* sobre **A**.

Sea V un **A**-módulo libre de rango n. Una aplicación F: $V \to \mathbf{A}$ se llama *cuadrática* si:

(i) $F(a\mathbf{x}) = a^2F(\mathbf{x})$ para todo $a \in \mathbf{A}$ y $\mathbf{x} \in V$.

(ii) La aplicación B_F: $V \times V \to \mathbf{A}$ tal que $B_F(\mathbf{x}, \mathbf{y}) = 1/2[F(\mathbf{x} + \mathbf{y}) - F(\mathbf{x}) - F(\mathbf{y})]$ es bilineal.

Un tal par (V, F) constituye un espacio cuadrático sobre **A**. Es claro que B_F es una forma bilineal simétrica que determina la función cuadrática F. En efecto, $F(\mathbf{x}) = B_F(\mathbf{x}, \mathbf{x})$ para todo $\mathbf{x} \in V$.

Sea $\{\mathbf{u}_1, \cdots \mathbf{u}_n\}$ una **A**-base de V. La función

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

es una forma cuadrática sobre **A** cuya matriz $\mathbf{M}(f)$ es la matriz $\|B_F(\mathbf{u}_i, \mathbf{u}_j)\|$ de la forma bilineal B_F en dicha base.

Recíprocamente, sea $f = f(x_1,\ldots, x_n)$ una forma cuadrática sobre **A** y definamos F: $\mathbf{A}^n \to \mathbf{A}$ tal que

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

donde $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ es una base dada de $\mathbf{A}^n$. Es claro que $(\mathbf{A}^n, F)$ es un espacio cuadrático sobre **A** tal que la matriz de la forma bilineal B_F en la base $\{\mathbf{e}_1,\ldots, \mathbf{e}_n\}$ es $\mathbf{M}(f)$. Denotaremos (V, f) a dicho espacio cuadrático y lo llamaremos *espacio cuadrático asociado a f*. Observemos que identificamos a f con la función cuadrática. En particular, B_f será la correspondiente forma bilineal.

Vemos así que existe una correspondencia entre formas cuadráticas sobre **A** y espacios cuadráticos sobre **A** *con una base fija,* y que al cambiar de base se obtienen todas las formas cuadráticas de una clase de **A**-equivalencia.

Si (V_1, F_1) y (V_2, F_2) son dos espacios cuadráticos sobre **A**, se llama *isometría* de (V_1, F_1) en (V_2, F_2) a toda aplicación **A**-lineal ϕ: $V_1 \to V_2$ tal que $F_1 = F_2 \circ \phi$. Si ϕ es un isomorfismo de **A**-módulos, (V_1, F_1) y (V_2, F_2) se llaman *isométricos* (o isomorfos). Es claro que las isometrías de espacios cuadráticos se corresponden con la re-

presentación de una forma cuadrática por otra, que espacios cuadráticos isométricos se corresponden con formas cuadráticas **A**-equivalentes y que las isometrías de un espacio cuadrático en sí mismo se corresponden con las automorfas de la forma cuadrática correspondiente.

Sea (V, F) un espacio cuadrático sobre **A**. Para todo submódulo libre V_1 de V, la restricción F_1 de F a V_1 es una aplicación cuadrática, de modo que (V_1, F_1) es un subespacio cuadrático.

Observación 1.2. *Sean* $\mathbf{A} \subset \mathbf{A}'$ *dominios. Toda forma cuadrática f sobre* **A** *puede considerarse también como una forma cuadrática sobre* $\mathbf{A}'$. *Los correspondientes espacios cuadráticos asociados a f se obtienen, uno del otro, por* extensión de escalares.

Si dos tales formas cuadráticas son **A**-*equivalentes, también son* $\mathbf{A}'$-*equivalentes, pero lo recíproco no es cierto en general.*

Por otra parte, si (V', F') *es un espacio cuadrático sobre* $\mathbf{A}'$ *y* $V \subset V'$ *es un* **A**-*módulo libre de base* $\{\mathbf{u}_1, \ldots, \mathbf{u}_k\}$, *con* $k \leq n$ *y donde* $\{\mathbf{u}_1, \ldots, \mathbf{u}_k\}$ *es un conjunto* $\mathbf{A}'$-*independiente de* V', *podemos considerar la restricción F de* F' *a V. En general,* (V, F) *no será un espacio cuadrático sobre* **A** *pues no necesariamente* $F(V) \subset \mathbf{A}$. *De todos modos, con abuso de lenguaje, diremos que* (V, F) *es el* espacio cuadrático obtenido por restricción de F' a V. *También lo denotaremos* (V, F'_V) *o, simplemente,* (V, F').

Dos elementos $\mathbf{x}$, $\mathbf{y}$ de V se dicen *ortogonales* si $B_F(\mathbf{x}, \mathbf{y}) = 0$. Una base de V es ortogonal si sus elementos son ortogonales dos a dos. En una tal base, la matriz de B_F es diagonal. Luego, si **A** es un cuerpo todo espacio cuadrático sobre **A** posee bases ortogonales, pero esto no es cierto en general.

Si $S \subset V$ es un subconjunto, el conjunto $S^\perp$, de los elementos ortogonales a todos los elementos de S, es un subespacio cuadrático. En particular, tomando $S = V$, se tiene $V^\perp$ llamado *radical* de V. Se dice que (V, F) es *no degenerado* si $V^\perp = \{\mathbf{0}\}$. Los espacios cuadráticos no degenerados se corresponden con las formas cuadráticas regulares que estamos considerando.

Dos subespacios cuadráticos (V_1, F_1) y (V_2, F_2) de (V, F) se dicen *ortogonales* si $V_1 \subset V_2^\perp$. Si $V = V_1 \oplus V_2$ como **A**-módulos y son ortogonales, escribiremos $V = V_1 \perp V_2$. En particular, si $\{\mathbf{u}_1, \cdots \mathbf{u}_r\}$ es una **A**-base de V_1 y $\{\mathbf{u}_{r+1}, \cdots \mathbf{u}_n\}$ es una **A**-base de V_2, con V_1 y V_2 ortogonales, escribiremos $V = \langle \mathbf{u}_1, \cdots \mathbf{u}_r \rangle \perp \langle \mathbf{u}_{r+1}, \cdots \mathbf{u}_n \rangle$.

Sea $\mathbf{A} \subset \mathbf{R}$ un subanillo del cuerpo de los números reales. Diremos que una forma cuadrática f sobre **A** es una forma *definida positiva* (*definida negativa*) si $f(x_1, \ldots, x_n) > 0$ $(f(x_1, \ldots, x_n) < 0)$ para todos los valores $x_1, \ldots, x_n$, no todos cero. Si f toma valores positivos y negativos, diremos que es una forma *indefinida.*

El estudio de las formas definidas negativas se reduce al de las formas definidas positivas. Por esta razón, sólo diremos de una forma que es *definida* o que es *indefinida,* y en el primer caso supondremos que es *definida positiva.*

Dos formas **A**-equivalentes representan los mismos elementos de **A** (considerados como formas unarias), luego son ambas definidas o ambas indefinidas.

Observaciones 1.3. *(1) Si f es una forma cuadrática definida entonces* $\det(f) > 0$.

En efecto, f puede pensarse como una forma sobre **R** (*Observación* 1.2) *y, por lo tanto,* **R**-*equivalente a una forma diagonal g. Siendo* $\det(g) > 0$, *por la Observación* 1.1, $\det(f) > 0$.

Observemos que lo recíproco no es cierto: el determinante de una forma indefinida puede tener cualquier signo. El razonamiento anterior muestra que en el caso de una forma definida negativa, el signo de su determinante es $(-1)^n$.

(2) Es interesante observar que una forma cuadrática regular sobre **A** *sólo puede ser definida o indefinida. En efecto, supongamos que f es una forma sobre* **A** *que no es indefinida y sea* **u** *un elemento del espacio cuadrático* (V, f) *sobre* **R** *tal que* $f(\mathbf{u}) = 0$. *Para todo* $k \in \mathbf{R}$ *y todo* $\mathbf{v} \in V$, $f(k\mathbf{u} + \mathbf{v}) = f(\mathbf{v}) + 2kB_f(\mathbf{u}, \mathbf{v})$ *tomaría distintos signos a menos que* $B_f(\mathbf{u}, \mathbf{v}) = 0$; *luego* $\mathbf{u} \in V^\perp = \{\mathbf{0}\}$ y f *es definida.*

1.2. Algebras de cuaterniones y álgebra de Clifford

Sean $\mathcal{P} \subset \mathbf{Z}$ el conjunto de los enteros primos $p > 1$ y $\mathcal{P}' = \mathcal{P} \cup \{\infty\}$. Para cada $p \in \mathcal{P}'$ sea $\mathbf{Q}_p$ el cuerpo de los números p-ádicos si $p \in \mathcal{P}$ y $\mathbf{Q}_\infty = \mathbf{R}$. En lo que sigue, K denotará al cuerpo $\mathbf{Q}$ o a uno de los cuerpos $\mathbf{Q}_p$ con $p \in \mathcal{P}'$.

Definición 1.4. *Llamaremos* álgebra de cuaterniones *sobre K a toda K-álgebra central y simple de dimensión* 4 *sobre K.*

Si $\mathcal{H}$ es un álgebra de cuaterniones sobre K, existen dos elementos a, b no nulos de K y una K-base $\{\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ de $\mathcal{H}$, donde $\mathbf{1} \in \mathcal{H}$ es la unidad del álgebra y se verifican las relaciones:

$$\mathbf{i}^2 = a, \quad \mathbf{j}^2 = b, \quad \mathbf{ij} = \mathbf{k} = -\mathbf{ji}. \tag{3}$$

Recíprocamente, dados dos elementos a, b no nulos de K, las relaciones (3) permiten definir una estructura de K-álgebra con unidad **1** sobre el K-espacio vectorial de base $\{\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$, que resulta un álgebra de cuaterniones sobre K (ver [9, p. 2]). Denotaremos $\mathcal{H}_K(a, b)$ al álgebra de cuaterniones sobre K definida por el par de elementos a, b. En el caso $K = \mathbf{Q}$, la denotaremos simplemente $\mathcal{H}(a, b)$.

Observación 1.5. *Si bien toda álgebra de cuaterniones $\mathcal{H}$ sobre K es de la forma $\mathcal{H}_K(a, b)$, los elementos a, b no están determinados unívocamente por $\mathcal{H}$.*

Por ejemplo, permutando $\mathbf{i}$ *con* $\mathbf{j}$ *se tiene que* $\mathcal{H}_K(a, b) = \mathcal{H}_K(b, a)$ *y tomando la base* $\{\mathbf{1}, s\mathbf{i}, t\mathbf{j}, st\mathbf{k}\}$, *donde* s, t *son elementos no nulos de* K, *se concluye que* $\mathcal{H}_K(a, b) = \mathcal{H}_K(as^2, bt^2)$, *de modo que* a, b *pueden reemplazarse por elementos equivalentes módulo cuadrados no nulos de* K.

Sea $\mathcal{H}$ un álgebra de cuaterniones sobre K y sea $\mathbf{u} \in \mathcal{H}$ un elemento inversible en $\mathcal{H}$. Es claro que la aplicación $\lambda_{\mathbf{u}}: \mathcal{H} \to \mathcal{H}$ tal que $\lambda_{\mathbf{u}}(\mathbf{x}) = \mathbf{u}\mathbf{x}\mathbf{u}^{-1}$ es un K-automorfismo de $\mathcal{H}$ que es llamado *automorfismo interior* (asociado a $\mathbf{u}$).

Lemma 1.6. *En un álgebra de cuaterniones sobre K, todo K-automorfismo es un automorfismo interior.*

Demostración. Es una consecuencia del Teorema de Skolem-Noether (ver [9, Teorema 2.1, p.6]). □

Toda álgebra de cuaterniones $\mathcal{H}$ sobre K posee un K-antiautomorfismo involutivo $\mathbf{u} \to \bar{\mathbf{u}}$ llamado *conjugación* (ver [9, p. 1]). En particular, $\mathcal{H}$ es K-isomorfa a $\mathcal{H}^{op}$ la K-álgebra opuesta de $\mathcal{H}$. Si $\mathcal{H} = \mathcal{H}_K(a, b)$ con base $\{\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$, la conjugación aplica dicha base en la base $\{\mathbf{1}, -\mathbf{i}, -\mathbf{j}, -\mathbf{k}\}$.

La conjugación permite definir, para todo $\mathbf{u} \in \mathcal{H}$, la *traza* (reducida) $T(\mathbf{u}) = \mathbf{u} + \bar{\mathbf{u}}$ y la *norma* (reducida) $N(\mathbf{u}) = \mathbf{u}\bar{\mathbf{u}}$, que verifican (ver [9, Lema 1.1, p. 2]):

Lemma 1.7. *(i)* $\mathbf{u}$ *es inversible en $\mathcal{H}$ si y sólo si* $N(\mathbf{u}) \neq 0$.

(ii) $N: \mathcal{H}^* \to K^*$ *es un homomorfismo del grupo de los elementos inversibles de $\mathcal{H}$* en el grupo multiplicativo de K.

(iii) $T: \mathcal{H} \to K$ *es K-lineal y* $B_T(\mathbf{u}, \mathbf{v}) = T(\mathbf{u}\mathbf{v})$ *define una aplicación bilineal no degenerada.*

Corolario 1.8. *Todo* $\mathbf{u} \in \mathcal{H}$ tal que $\mathbf{u} \notin K \cdot \mathbf{1}$ *es cuadrático sobre K con polinomio minimal:* $X^2 - T(\mathbf{u})X + N(\mathbf{u})$.

Denotaremos $\mathcal{H}^0$ al conjunto de los $\mathbf{u} \in \mathcal{H}$ tal que $T(\mathbf{u}) = 0$. Por el corolario anterior, $\mathcal{H}^0$ es el conjunto de los $\mathbf{u} \in \mathcal{H}$ tales que $\mathbf{u} \notin K \cdot \mathbf{1}$ y $\mathbf{u}^2 \in K \cdot \mathbf{1}$.

La norma N define, sobre el K-espacio vectorial $\mathcal{H}$, una estructura de espacio cuadrático $(\mathcal{H}, N)$ cuya forma bilineal asociada está dada por $B_N(\mathbf{u}, \mathbf{v}) = T(\mathbf{u}\bar{\mathbf{v}})/2$. Este espacio cuadrático resulta ser no degenerado; además se tiene:

Corolario 1.9. *Como espacio cuadrático:* $\mathcal{H} = \langle \mathbf{1} \rangle \perp \mathcal{H}^0$.

Finalmente se tiene (ver [9, Lema 3.1, p. 11]):

Proposición 1.10. *Sean $\mathcal{H}_1$ y $\mathcal{H}_2$ dos álgebras de cuaterniones sobre K. Las propiedades siguientes son equivalentes:*

(1) *$\mathcal{H}_1$ y $\mathcal{H}_2$ son isomorfas como álgebras.*

(2) *$\mathcal{H}_1$ y $\mathcal{H}_2$ son isométricos como espacios cuadráticos.*

(3) *$\mathcal{H}_1^0$ y $\mathcal{H}_2^0$ son isométricos como espacios cuadráticos.*

Nosotros estamos interesados en las álgebras de cuaterniones racionales, es decir, con $K = \mathbf{Q}$. Sea $\mathcal{H} = \mathcal{H}(a, b)$ una tal álgebra, donde a, b pueden suponerse, por la Observación 1.5, enteros no nulos. Para cada $p \in \mathcal{P}'$ se obtiene, por extensión de escalares, el álgebra de cuaterniones $\mathcal{H}_p = \mathcal{H}_{\mathbf{Q}_p}(a, b)$.

Toda álgebra de cuaterniones sobre K es isomorfa al álgebra de matrices $\mathbf{M}(2, K)$ o es un álgebra de división, según que existan o no elementos no nulos con norma cero. En el caso $K = \mathbf{R}$, existe (salvo isomorfismos) una única álgebra de cuaterniones de división: los *cuaterniones de Hamilton* $\mathcal{H}_{\mathbf{R}}(-1, -1)$. Lo mismo ocurre en el caso $K = \mathbf{Q}_p$ para $p \in \mathcal{P}$ (ver [9, Teorema 1.1, p. 31]).

Definición 1.11. *Diremos que $\mathcal{H}$ es* ramificada *en un $p \in \mathcal{P}'$ si $\mathcal{H}_p$ es de división. Diremos que $\mathcal{H}$ es* definida *si es ramificada en $p = \infty$; en caso contrario diremos que $\mathcal{H}$ es* indefinida.

El siguiente resultado muestra cómo la ramificación determina las álgebras de cuaterniones racionales (ver [9, Teorema 3.1, p. 74]).

Proposición 1.12. *El conjunto $S(\mathcal{H}) \subset \mathcal{P}'$ de los $p \in \mathcal{P}'$ donde $\mathcal{H}$ es ramificada es finito y su cardinal es par. Para todo $S \subset \mathcal{P}'$ finito y de cardinal par existe una única álgebra de cuaterniones $\mathcal{H}$ sobre* $\mathbf{Q}$, *salvo isomorfismos, tal que $S(\mathcal{H}) = S$. En particular, $\mathcal{H} \approx \mathbf{M}(2, \mathbf{Q})$ es de matrices si y sólo si $S(\mathcal{H})$ es vacío.*

Definición 1.13. *Llamaremos* discriminante *(reducido) de $\mathcal{H}$, y lo denotaremos $d(\mathcal{H})$, al producto de los $p \in \mathcal{P}$ donde $\mathcal{H}$ es ramificada, si algún tal p existe. En caso contrario, definimos $d(\mathcal{H}) = 1$.*

Corolario 1.14. *El discriminante $d(\mathcal{H})$ determina el álgebra de cuaterniones $\mathcal{H}$ sobre* $\mathbf{Q}$ *salvo isomorfismos. En particular, $\mathcal{H} \approx \mathbf{M}(2, \mathbf{Q})$ es de matrices si y sólo si $d(\mathcal{H}) = 1$.*

Para todo entero $d > 1$ libre de cuadrados existe una única álgebra de cuaterniones $\mathcal{H}$ sobre $\mathbf{Q}$, *salvo isomorfismos, tal que $d(\mathcal{H}) = d$, $\mathcal{H}$ es definida si y sólo si d es el producto de un número impar de primos.*

Observaciones 1.15. *(1) Dada $\mathcal{H}(a, b)$, el cálculo de $d = d(\mathcal{H})$ se realiza fácilmente utilizando el* símbolo de Hilbert. *En particular, $\mathcal{H}$ es definida si y sólo si $a < 0$ y $b < 0$ (ver [9, p. 32 y p. 79]).* Un método práctico para determinar *d es el siguiente (ver [3, p.31]):*

Podemos suponer que *a y b son enteros libres de cuadrados. Entonces resulta que $d \mid 2ab$ y para un primo $p > 2$ se tiene que $p \mid d$* si $p \mid a$ y $\left(\frac{b}{p}\right) = -1$ o $p \mid b$ y $\left(\frac{a}{p}\right) = -1$ *o $p \mid a$ y $p \mid b$ y $\left(\frac{m}{p}\right) = -1$ donde $m = ab/p^2$. Para decidir si d es par o impar se utiliza la última parte del Corolario* 1.14 *(que es consecuencia de la* fórmula del producto *para el símbolo de Hilbert) dado que los signos de a y b determinan si $\mathcal{H}$ es definida o indefinida.*

(2) Dado un entero $d > 1$ libre de cuadrados, existen muchos pares a, b tales que $d(\mathcal{H}(a, b)) = d$ (Observación 1.5*), aún tomando a y b enteros y libres de cuadrados. En realidad, no existe un tal par* canónico.

Sin embargo, desde un punto de vista computacional es conveniente trabajar, para cada discriminante d, en un álgebra $\mathcal{H}(a, b)$ bien determinada. Nosotros trabajaremos en el álgebra, que denotaremos $\mathcal{H}(d)$, así elegida:

$$\mathcal{H}(2) = \mathcal{H}(-1, -1)$$

$$\mathcal{H}(q) = \mathcal{H}(-1, -q) \quad \text{y} \quad \mathcal{H}(2q) = \mathcal{H}(-1, q) \quad \text{si } q \in \mathcal{P} \text{ y } q \equiv 3 \pmod 4$$

$$\mathcal{H}(q) = \mathcal{H}(-2, -q) \quad \text{y} \quad \mathcal{H}(2q) = \mathcal{H}(-2, q) \quad \text{si } q \in \mathcal{P} \text{ y } q \equiv 5 \pmod 8$$

$$\mathcal{H}(d) = \mathcal{H}(-p, -d) \quad o \quad \mathcal{H}(-p, d) \quad \textit{en todo otro caso,}$$

según que el número de factores primos de d sea impar o par y donde p es el menor elemento de $\mathcal{P}$ que no divide a d y verifica:

(i) $p \equiv 3 \pmod 4$ *si d es impar y* $p \equiv 3 \pmod 8$ *si d es par,*

(ii) para todo primo $q > 2$ que divide a d, $\left(\frac{-p}{q}\right) = -1$,

y todos los cálculos los realizaremos en la correspondiente base $\{\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$.

Observemos que esta elección no da, en general, la expresión más simple en términos de a y b. Por ejemplo, $\mathcal{H}(15) = \mathcal{H}(-7, 15) = \mathcal{H}(-3, 5)$.

El instrumento más adecuado para estudiar la relación entre formas ternarias y álgebras de cuaterniones es el álgebra de Clifford. Aunque esta álgebra puede definirse para cualquier espacio cuadrático sobre un cuerpo, aquí nos concentraremos en el caso que nos interesa, es decir, en espacios cuadráticos de dimensión 3 sobre **Q**.

Definición 1.16. *Sea (V, F) un espacio cuadrático sobre* **Q**. *Llamaremos* álgebra de Clifford *de (V, F), y la denotaremos C(V, F), al álgebra sobre* **Q** *que contiene a V como subespacio de modo que para todo* $\mathbf{u} \in V$, $\mathbf{u}^2 = F(\mathbf{u}) \cdot \mathbf{1}$ *en C(V, F), y que es* universal *respecto de esta propiedad.*

La propiedad universal de $C(V, F)$ significa que para toda álgebra C sobre **Q** que contenga a V como subespacio de modo que para todo $\mathbf{u} \in V$, $\mathbf{u}^2 = F(\mathbf{u}) \cdot \mathbf{1}$ en C, existe un *único* homomorfismo λ: $C(V, F) \to C$ de álgebras sobre **Q** que es la identidad sobre V. La existencia de $C(V, F)$ se prueba constructivamente y, entonces, su unicidad es consecuencia de su propiedad universal.

Definición 1.17. *Sea f una forma cuadrática sobre* **Q** *y sea (V, f) el espacio cuadrático asociado a f. Llamaremos* álgebra de Clifford de *f, y la denotaremos C(f), al álgebra de Clifford de (V, f).*

Sea f como en (1), con $n = 3$, una forma ternaria regular sobre **Q**. Veamos cómo se construye el álgebra de Clifford $C(f)$.

Nota. Para aligerar la notación, en todo lo que sigue (i, j, k) representará una permutación cíclica de $\{1, 2, 3\}$ y, a menos que se indique lo contrario, supondremos que i recorre los valores $i = 1, 2, 3$ (luego j y k recorren los valores correspondientes).

Sea (V, f) el espacio cuadrático asociado a f con base $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$.

Como **Q**-espacio vectorial $C(f)$ tiene base $\{\mathbf{1}, \mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{E}_1, \mathbf{E}_2, \mathbf{E}_3, \mathbf{E}\}$ donde $\mathbf{1} \in C(f)$ es la identidad del álgebra, $\mathbf{E}_i = \mathbf{e}_j\mathbf{e}_k$ y $\mathbf{E} = \mathbf{e}_1\mathbf{e}_2\mathbf{e}_3$. Por la propiedad universal de $C(f)$, para todo $\mathbf{x} \in V \subset C(f)$, $\mathbf{x}^2 = f(\mathbf{x})$. En particular, resulta que

$$\mathbf{e}_i^2 = a_{ii} \quad \text{y} \quad \mathbf{e}_i\mathbf{e}_j + \mathbf{e}_j\mathbf{e}_i = a_{ij} \tag{4}$$

y estas relaciones determinan el producto en $C(f)$.

$C(f)$ (como toda álgebra de Clifford) tiene una estructura de álgebra $\mathbf{Z}/2\mathbf{Z}$-graduada. La *parte par* de $C(f)$, que denotaremos $C_0(f)$, es la subálgebra de $C(f)$ de base $\{\mathbf{1}, \mathbf{E}_1, \mathbf{E}_2, \mathbf{E}_3\}$.

Proposición 1.18. *Para toda forma ternaria (regular) f sobre* **Q**, $C_0(f)$ *es un álgebra de cuaterniones sobre* **Q** *que es definida si y sólo si f es definida.*

Demostración. Es claro que $C(f)$ sólo depende de la clase de **Q**-equivalencia de f. Siendo **Q** un cuerpo, podemos suponer que f es diagonal. Los $a_{ii} = a_i$ son no nulos (por ser f regular) y pueden tomarse enteros (y libres de cuadrados si se lo desea). Tomando $\mathbf{i} = \mathbf{E}_1$, $\mathbf{j} = \mathbf{E}_2$ y $\mathbf{k} = -a_3\mathbf{E}_3$ y teniendo en cuenta (4), resulta que $\{\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ es una **Q**-base de $C_0(f)$ y $C_0(f) = \mathcal{H}(-a_2a_3, -a_1a_3)$. Es claro que $C_0(f)$ es un álgebra de cuaterniones definida si y sólo si los a_i tienen todos el mismo signo (ver Observación 1.15), es decir, si y sólo si f es definida. □

Observación 1.19. *Si $C = C(V, F)$, es claro que C^{op} posee las mismas propiedades que definen a C. Luego, por la propiedad universal de C, existe un único isomorfismo λ: $C \to C^{op}$ que es la identidad sobre V. Identificando a C^{op} con C como conjuntos, esto muestra que en C está definido un antiautomorfismo involutivo. En el caso en que $C = C(f)$ con f ternaria sobre* **Q**, *dicho antiautomorfismo está determinado por $\mathbf{e}_i\mathbf{e}_j \to \mathbf{e}_j\mathbf{e}_i$, y restringido al álgebra de cuaterniones $C_0(f)$ es la conjugación.*

Observación 1.20. *Hemos visto que a toda clase $\mathcal{F}$ de formas ternarias* **Q***-equivalentes le podemos hacer corresponder un álgebra de cuaterniones racionales. En efecto, tomando $f = \operatorname{diag}(a_1, a_2, a_3) \in \mathcal{F}$ resulta $C_0(f) = \mathcal{H}(-a_2a_3, -a_1a_3) = \mathcal{H}$ que sólo depende de $\mathcal{F}$. Observemos, de paso, que $\mathcal{H}$ no varía si realizamos cualquier permutación en el conjunto $\{a_1, a_2, a_3\}$, dado que la correspondiente forma diagonal y f son* **Q***-equivalentes.*

Considerando el espacio cuadrático $(\mathcal{H}, N)$ sobre **Q**, *resulta que $\mathcal{H} = \langle \mathbf{1} \rangle \perp \mathcal{H}^0$ (Corolario 1.9) y la forma cuadrática norma N sobre $\mathcal{H}^0$ es $N = \operatorname{diag}(a_2a_3, a_1a_3, a_1a_2a_3^2)$,* **Q***-equivalente a $g = \operatorname{diag}(a_2a_3, a_1a_3, a_1a_2)$ con $M(g) = \operatorname{adj} M(f)$ (matriz adjunta). Tomando $(\det(g))^{-1/2}g = \operatorname{diag}(1/a_1, 1/a_2, 1/a_3)$ se obtiene una forma* **Q***-equivalente a f. Es decir, se recupera $\mathcal{F}$.*

El objetivo central de este trabajo es el de estudiar correspondencias de este tipo para formas ternarias enteras.

Observación 1.21. *Hemos dicho que el álgebra de Clifford es el instrumento más adecuado para estudiar la relación entre formas ternarias y álgebras de cuaterniones, sin embargo, como ya hemos señalado en la Introducción, el primero en considerar estas álgebras fue Hermite. En efecto, en* [6], *estudiando las automorfas de una forma ternaria f obtiene una fórmula para* multiplicar *cuaternas de números racionales que, en esencia, equivale a la definición de un álgebra de cuaterniones racionales asociada a f.*

El álgebra de cuaterniones de Hermite asociada a una forma ternaria f está definida en términos de $\mathbf{M}(f) = \|a_{ij}\|$ y de adj $\mathbf{M}(f) = \|A_{ij}\|$ *del modo siguiente (ver [8, p. 283]): sobre la* **Q***-base $\{\mathbf{1}, \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3\}$ se define el producto mediante las relaciones:*

$$\mathbf{u}_i^2 = -A_{ii}, \quad \mathbf{u}_i\mathbf{u}_j = -A_{ij} + \sum_{s=1}^{3} a_{ks}\mathbf{u}_s, \tag{5}$$

$$\mathbf{u}_j\mathbf{u}_i = -A_{ij} - \sum_{s=1}^{3} a_{ks}\mathbf{u}_s.$$

Particularizando (5) *al caso en que $f = \operatorname{diag}(a_1, a_2, a_3)$, resulta que esta álgebra coincide con $C_0(f)$.*

1.3. Formas ternarias enteras

Desde ahora denotaremos $f = (a_1, a_2, a_3, a_{23}, a_{13}, a_{12})$ a la forma cuadrática ternaria (regular)

$$f = f(x_1, x_2, x_3) = \\ = a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_{23}x_2x_3 + a_{13}x_1x_3 + a_{12}x_1x_2,$$

que, salvo indicación expresa de lo contrario, supondremos entera.

Definición 1.22. *Llamaremos* discriminante *de f al entero*

$$\mathbf{D}(f) = 4\det(f) = 4a_1a_2a_3 + a_{23}a_{13}a_{12} - a_1a_{23}^2 - a_2a_{13}^2 - a_3a_{12}^2.$$

Si *f* y *g* son dos formas enteras, diremos que son *equivalentes,* y lo denotaremos $f \sim g$, si son **Z**-equivalentes. Un objeto $X(f)$ asociado a una forma entera *f* es un *invariante* si coincide para todas las formas de una clase (de formas equivalentes), es decir, si $f \sim g \Rightarrow X(f) = X(g)$.

Uno de los objetivos en el estudio de las formas enteras es el de hallar invariantes que faciliten la identificación de sus clases (ver Observaciones 1.37, más adelante), pero aquí sólo consideraremos aquellos que sean necesarios para nuestro estudio.

Sea *f* una forma ternaria entera. De la Observación 1.1 se sigue que $\mathbf{D}(f)$ es un invariante, y la propiedad universal del álgebra de Clifford nos permite asegurar que $d(f) = d(C_0(f))$ es, también, un invariante.

Si *f* es una forma ternaria entera, $\mathbf{D}(-f) = -\mathbf{D}(f)$. Luego, siendo *f* regular, resulta que *f* y $-f$ no son equivalentes. En la Sección 1.1 señalamos que el estudio de las formas definidas negativas se reduce al de las formas definidas positivas. Más generalmente, el estudio de $-f$ se reduce al de *f*. Por esta razón, desde ahora supondremos que: $\mathbf{D}(f) > 0$ *para toda forma ternaria entera f.* Esta convención incluye otras dos que hemos hecho antes: *f* es regular y si *f* es definida entonces *f* es definida positiva.

Observación 1.23. *Es claro que $-\mathbf{I}_3$ es una automorfa para toda forma ternaria f (cambio de signo de las variables). Luego, si f y g son dos formas ternarias enteras tales que $M \cdot f = g$ con $M \in \mathbf{M}(3, \mathbf{Z})$ (es decir: si f representa a g y, en particular, si son equivalentes), necesariamente* $\det M \neq 0$ *y, cambiando M por $M \cdot (-\mathbf{I}_3)$ si fuera necesario, siempre podremos suponer que* $\det M > 0$.

Además, si f′ y g′ son dos formas tales que $f' \sim f$ y $g' \sim g$, es decir, $f' = M_1 \cdot f$ y $g' = M_2 \cdot g$ con $M_1, M_2 \in \mathbf{GL}(3, \mathbf{Z})$, resulta que $M' \cdot f' = g'$ con $M' = M_2 \cdot M \cdot M_1^{-1}$ y, por la convención anterior, $\det M' = \det M > 0$. *Esto muestra que el concepto de «representar a» se extiende a clases de formas ternarias enteras.*

Definición 1.24. *Diremos que la forma ternaria entera* $f = (a_1, a_2, a_3, a_{23}, a_{13}, a_{12})$ *es* clásica *si sus tres últimos coeficientes son pares. En caso contrario diremos que* f *es* no clásica.

Observación 1.25. *Es claro que una forma ternaria entera* f *es clásica si y sólo si su matriz* $\mathbf{M}(f)$ *es entera. Esto muestra que la propiedad de una forma de ser clásica o no clásica es común a todas las formas de su clase.*

La definición anterior se extiende naturalmente a formas enteras en cualquier número de variables. Muchos autores llaman forma entera *a una forma* f *tal que su matriz* $\mathbf{M}(f)$ *es entera, es decir, a lo que nosotros llamamos* forma entera clásica. *Por ejemplo, parte del contenido de esta sección se encuentra en* [4] *pero formulado sólo para formas ternarias clásicas.*

Más adelante quedará de manifiesto que en el estudio de la correspondencia entre formas ternarias enteras y órdenes cuaterniónicos es esencial adoptar nuestra definición de forma entera (ver el Teorema 2.16 *y su Corolario* 2.18 *en la Sección 2.2).*

Definición 1.26. *Llamaremos* divisor *de la forma ternaria entera* f*, y lo denotaremos* $\sigma(f)$*, al máximo común divisor de los coeficientes de* f*. Diremos que* f *es* primitiva *si* $\sigma(f) = 1$.

Lema 1.27. $\sigma(f)$ *es un invariante.*

Demostración. Sean $g = M \cdot f$ una forma equivalente a f y (V, g) su espacio cuadrático asociado con base $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$. Si $g = (b_1, b_2, b_3, b_{23}, b_{13}, b_{12})$, resulta que

$$b_i = g(\mathbf{e}_i) = f(M \cdot \mathbf{e}_i) = f(\mathbf{u}_i) \quad \text{y}$$

$$b_{ij} = g(\mathbf{e}_i + \mathbf{e}_j) - g(\mathbf{e}_i) - g(\mathbf{e}_j) = f(\mathbf{u}_i + \mathbf{u}_j) - f(\mathbf{u}_i) - f(\mathbf{u}_j).$$

Dado que $\sigma(f)$ divide a $f(\mathbf{u})$ para todo $\mathbf{u} \in V$, $\sigma(f)$ divide a todos los coeficientes de g, por lo cual divide a $\sigma(g)$. Razonando de la misma forma, se obtiene que $\sigma(g)$ divide a $\sigma(f)$, y siendo ambos enteros positivos, se concluye que $\sigma(f) = \sigma(g)$ es un invariante. □

Definición 1.28. *Llamaremos* forma adjunta *de una forma ternaria entera* f*, y la denotaremos* ${}^a f$*, a la forma que verifica*

$$\mathbf{M}({}^a f) = \text{adj}\big(2\mathbf{M}(f)\big) = 4\ \text{adj}\mathbf{M}(f),$$

donde adj M *es la matriz adjunta de la matriz* M.

Proposición 1.29. *Si* f *es una forma ternaria entera, entonces:*

(i) $\mathbf{D}({}^a f) = 16\mathbf{D}(f)^2$.

(ii) ${}^a({}^a f) = 16\mathbf{D}(f)f$.

(iii) $f \sim g \Leftrightarrow {}^a f \sim {}^a g$ *para toda forma ternaria entera* g.

(iv) f y ${}^a f$ *son ambas definidas o ambas indefinidas.*

Demostración. La parte *(i)* es inmediata recordando que $\det(\text{adj}\ \mathbf{M}(f)) = (\det \mathbf{M}(f))^2$. De las propiedades de la adjunta de una matriz se sigue que

$$\mathbf{M}({}^a f) \cdot \mathbf{M}(f) = \mathbf{M}(f) \cdot \mathbf{M}({}^a f) = \mathbf{D}(f)\mathbf{I}_3. \tag{6}$$

Aplicando (6) a la forma ${}^a f$ y usando la parte *(i)*, se tiene que

$$\mathbf{M}\big({}^a({}^a f)\big) \cdot \mathbf{M}({}^a f) = \mathbf{M}({}^a f) \cdot \mathbf{M}\big({}^a({}^a f)\big) = 16\mathbf{D}(f)^2\mathbf{I}_3, \tag{7}$$

y la parte *(ii)* es consecuencia de (6) y (7).

Sea $g = M \cdot f$, con $M \in \mathbf{GL}(3, \mathbf{Z})$, una forma equivalente a f. Si $\tilde{M} = \text{adj}\ M$, se tiene que adj $\mathbf{M}(g) = {}^t\tilde{M} \cdot \text{adj}\ \mathbf{M}(f) \cdot \tilde{M}$. Luego ${}^a f \sim {}^a g$.

Recíprocamente, si ${}^a f \sim {}^a g$, aplicando lo anterior se tiene que ${}^a({}^a f) \sim {}^a({}^a g)$ y la parte *(iii)* resulta de *(i)* y *(ii)*, recordando que $\mathbf{D}(f) > 0$ y $\mathbf{D}(g) > 0$.

Siendo $\mathbf{M}(f)$ simétrica, de (6) se obtiene que

$$\mathbf{M}(\mathbf{M}(f) \cdot {}^a f) = {}^t\mathbf{M}(f) \cdot \mathbf{M}({}^a f) \cdot \mathbf{M}(f) =$$
$$= \mathbf{D}(f)\mathbf{M}(f) = \mathbf{M}\big(\mathbf{D}(f)f\big)$$

es decir,

$$\mathbf{M}(f) \cdot {}^a f = \mathbf{D}(f)f,$$

de donde se concluye la parte *(iv)*. □

El lema 1.27 y la parte *(iii)* de la proposición anterior permiten definir un nuevo invariante que nos será de utilidad:

Corolario 1.30. $\omega(f) = \sigma({}^a f)$ *es un invariante.*

En general, la forma ternaria f no será la adjunta ${}^a g$ de una forma ternaria entera. Si lo es, diremos que f *posee antiadjunta* y llamaremos *antiadjunta de* f a la forma g. La proposición siguiente da condiciones necesarias y suficientes para que f posea antiadjunta, muestra que ésta es única y da una forma de calcularla.

Proposición 1.31. *Sea* f *una forma ternaria entera. Entonces* $f = {}^a g$ *para alguna forma ternaria entera* g *si y sólo si* $\mathbf{D}(f) = k^2$ *es un cuadrado y* $4k \mid \omega(f)$*. En tal caso,* $g = {}^a f/4k$.

Demostración. Supongamos que $f = {}^a g$. Por Proposición 1.29 se tiene que

$$\mathbf{D}(f) = \mathbf{D}({}^a g) = 16\mathbf{D}(g)^2 = k^2$$

es un cuadrado, y

$$^af = {}^a({}^ag) = 16\mathbf{D}(g)g = 4kg,$$

luego $4k \mid \omega(f)$ y $g = {}^af/4k$.

Recíprocamente, si $\mathbf{D}(f) = k^2$ es un cuadrado y $4k \mid \omega(f)$, resulta que $g = {}^af/4k$ es una forma ternaria entera y

$$^ag = {}^a({}^af)/16k^2 = 16\mathbf{D}(f)f/16k^2 = f. \qquad \square$$

Definición 1.32. *Sean f y g dos formas ternarias enteras. Diremos que g deriva de f, y lo denotaremos $g \lhd f$, si ${}^af$ representa a ${}^ag$. Si $M \cdot {}^af = {}^ag$ es una tal representación, llamaremos* índice de g *en f al entero positivo* $\imath(f, g) = |\det M|$. *Diremos que g es una forma* fundamental *si no deriva propiamente de otra, es decir, si $g \lhd f \Rightarrow \imath(f, g) = 1$.*

Observación 1.33. *(1) Estamos utilizando la convención hecha en la Observación* 1.23. *Razonando como allí, se verifica fácilmente que tanto los conceptos de* «derivar de» *y de* «índice» *como el de* «fundamental» *se extienden a clases de formas ternarias enteras.*

(2) Es claro que si f representa a g, es decir, $M \cdot f = g$, entonces $\operatorname{adj} M \cdot {}^af = {}^ag$ *y g deriva de f. En este caso,* $\imath(f, g) = (\det M)^2$ *es un cuadrado. Vemos así que el concepto de* «derivar de» *es una generalización del concepto de* «ser representada por».

Proposición 1.34. *Sean f y g dos formas ternarias enteras y $M \in \mathbf{M}(3, \mathbf{Z})$ con* $\det M = k > 0$. *Las afirmaciones siguientes son equivalentes:*

(i) $M \cdot {}^af = {}^ag$.

(ii) $g = (\operatorname{adj} M \cdot f)/k$.

(iii) $f = ({}^tM \cdot g)/k$.

Demostración. Sea $M \cdot {}^af = {}^ag$. Por Proposición 1.29,

$$16\mathbf{D}(g)^2 = \mathbf{D}({}^ag) = k^2\mathbf{D}({}^af) = 16k^2\mathbf{D}(f)^2,$$

luego, $\mathbf{D}(g) = k\mathbf{D}(f)$. Además,

$$16\mathbf{D}(f)(\operatorname{adj} M \cdot f) = \operatorname{adj} M \cdot {}^a({}^af) = {}^a({}^ag) = \\ = 16\mathbf{D}(g)g = 16\mathbf{D}(f)kg,$$

luego $\operatorname{adj} M \cdot f = kg$ y *(i)* $\Rightarrow$ *(ii)*.

Aplicando ${}^tM$ a la igualdad anterior, se tiene

$$k^2f = (k\mathbf{I}_3) \cdot f = {}^tM \cdot \operatorname{adj} M \cdot f = k({}^tM \cdot g),$$

lo que muestra que *(ii)* $\Rightarrow$ *(iii)*.

Finalmente, si $f = ({}^tM \cdot g)/k$ resulta que

$$M \cdot {}^af = M \cdot \operatorname{adj}({}^tM) \cdot {}^ag/k^2 = (k\mathbf{I}_3) \cdot {}^ag/k^2 = {}^ag,$$

es decir, *(iii)* $\Rightarrow$ *(i)* y la demostración queda completa□

Proposición 1.35. *Sea $f = (a_1, a_2, a_3, a_{23}, a_{13}, a_{12})$ una forma ternaria entera y sea $b_3 = 4a_1a_2 - a_{12}^2$ el tercer coeficiente de su forma adjunta. Si $a_1b_3 \neq 0$ entonces $C_0(f) \approx \mathcal{H}(-b_3, -a_1\mathbf{D}(f))$.*

Demostración. Diagonalizando f sobre $\mathbf{Q}$ con el simple método de *completar cuadrados* resulta que f es $\mathbf{Q}$-equivalente a $\operatorname{diag}(a_1, b_3/4a_1, \mathbf{D}(f)/b_3)$. Teniendo en cuenta la Proposición 1.18 y la Observación 1.20, resulta que

$$C_0(f) \approx \mathcal{H}(-b_3/4, -\mathbf{D}(f)/4a_1) \approx \mathcal{H}(-b_3, -a_1\mathbf{D}(f)). \qquad \square$$

Corolario 1.36. *Sea $f = (a_1, a_2, a_3, a_{23}, a_{13}, a_{12})$ una forma ternaria entera y sea $b_3 = 4a_1a_2 - a_{12}^2$ el tercer coeficiente de su forma adjunta. Entonces f es definida si y sólo si $a_1 > 0$ y $b_3 > 0$.*

Dada una forma ternaria entera f, la Proposición 1.35 permite determinar fácilmente su invariante $d(f) = d(C_0(f))$ utilizando, por ejemplo, el método dado en la primera de las Observaciones 1.15. En efecto, la condición $a_1b_3 \neq 0$ siempre se verifica módulo un cambio de variable lineal que no afecta el valor de $d(f)$.

Observaciones 1.37. *Los invariantes $\mathbf{D}(f)$, $d(f)$ y $\omega(f)$ permiten decidir, en muchos casos, que dos formas ternarias enteras no son equivalentes, pero su igualdad no alcanza para asegurar la equivalencia. Una útil partición de las clases de formas está dada por la* teoría de los géneros:

Para cada $p \in \mathcal{P}'$ sea $\mathbf{Z}_p$ el anillo de los enteros p-ádicos si $p \in \mathcal{P}$ y $\mathbf{Z}_\infty = \mathbf{R}$. Diremos que dos formas ternarias enteras están en el mismo género *si son $\mathbf{Z}_p$-equivalentes para todo $p \in \mathcal{P}'$. Es claro que formas equivalentes están en el mismo género.*

Existe un conjunto de invariantes (similar al de los caracteres de Gauss para el caso de formas binarias enteras) que junto con $\mathbf{D}(f)$, $d(f)$ y $\omega(f)$ permiten decidir si dos formas ternarias enteras están o no en el mismo género. Si un género contiene más de una clase de formas ternarias, estos invariantes tampoco permiten asegurar la equivalencia de dos formas.

1.4. Ordenes cuaterniónicos

Sea $\mathcal{H} = \mathcal{H}(a, b)$ un álgebra de cuaterniones sobre $\mathbf{Q}$ con $d = d(\mathcal{H}) > 1$.

Teniendo en cuenta el Corolario 1.8, es natural decir que un $\mathbf{u} \in \mathcal{H}$ es un *entero* si $T(\mathbf{u})$ y $N(\mathbf{u})$ son números

enteros. En tal caso, $\mathbf{u} \in \mathbf{Q} \cdot \mathbf{1}$ es un entero si y sólo si $\mathbf{u} \in \mathbf{Z} \cdot \mathbf{1}$. Contrariamente a lo que ocurre en el caso conmutativo, el conjunto de los enteros de $\mathcal{H}$ no es un subanillo.

Definición 1.38. *Llamaremos* red *de $\mathcal{H}$ a todo subgrupo $L \subset \mathcal{H}$ finitamente generado.*

Toda red $L \neq \{\mathbf{0}\}$ de $\mathcal{H}$ es un $\mathbf{Z}$-módulo libre de rango $r \leq 4$. Si $\{\mathbf{u}_1, \ldots, \mathbf{u}_r\}$ es una $\mathbf{Z}$-base de L, denotaremos $L = [\mathbf{u}_1, \ldots, \mathbf{u}_r]$. Es claro que $\{\mathbf{u}_1, \ldots, \mathbf{u}_r\}$ es un conjunto $\mathbf{Q}$-independiente de $\mathcal{H}$.

Definición 1.39. *Llamaremos* módulo *de $\mathcal{H}$ a toda red L de $\mathcal{H}$ que contiene una $\mathbf{Q}$-base de $\mathcal{H}$. Si $\{\mathbf{u}_0, \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3\}$ es una tal base, $L = [\mathbf{u}_0, \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3]$. Diremos que un módulo es* unitario *si $L \cap \mathbf{Q} \cdot \mathbf{1} = \mathbf{Z} \cdot \mathbf{1}$ y todos sus elementos tienen traza entera, en tal caso es posible tomar una* base unitaria *en la que $\mathbf{u}_0 = \mathbf{1}$. Diremos que un módulo es* entero *si es unitario y todos sus elementos son enteros.*

Definición 1.40. *Llamaremos* orden *de $\mathcal{H}$ a todo módulo $\mathcal{O}$ que sea un subanillo de $\mathcal{H}$. Diremos que un orden es* maximal *si no está contenido propiamente en un orden de $\mathcal{H}$. Diremos que un orden es* de Eichler *si es la intersección de dos órdenes maximales.*

Se tiene (ver [9, Proposición 4.2, p. 20]) la siguiente caracterización de los órdenes:

Proposición 1.41. *Un subconjunto $\mathcal{O} \subset \mathcal{H}$ es un orden si y sólo si $\mathcal{O}$ es un subanillo (con $\mathbf{1} \in \mathcal{O}$) de enteros de $\mathcal{H}$ que contiene una $\mathbf{Q}$-base de $\mathcal{H}$.*

Corolario 1.42. *Todo orden de $\mathcal{H}$ es un módulo entero y está contenido en un orden maximal.*

Observación 1.43. *Sea $\mathcal{O}$ un orden de $\mathcal{H}$. Si $\mathbf{u} \in \mathcal{O}$, es claro que $\bar{\mathbf{u}} = T(\mathbf{u}) - \mathbf{u} \in \mathcal{O}$. Luego $\mathcal{O}$ es cerrado por conjugación y ésta define un antiautomorfismo involutivo del anillo $\mathcal{O}$.*

Observación 1.44. *Consideremos el espacio cuadrático $(\mathcal{H}, N)$ sobre $\mathbf{Q}$ determinado por la forma norma. Hemos visto que la forma bilineal asociada a $2N$ es $B(u, v) = T(u\bar{v})$. Siendo $\det(2N) = (4ab)^2$ en la base $\{\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$, por la Observación 1.1 resulta que $\det(2N) = q^2$ con $q \in \mathbf{Q}$, $q \neq 0$ en cualquier base de $\mathcal{H}$.*

Dada una red $L \neq \{\mathbf{0}\}$ de $\mathcal{H}$, podemos considerar (Observación 1.2) el espacio cuadrático (L, N_L) restricción de N a L. Si $L = [\mathbf{u}_0, \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3]$ es un módulo, como los cambios de base en L están dados por elementos del $\mathbf{GL}(4, \mathbf{Z})$, es claro que $\det(2N_L)$ tomará el mismo valor en cualquiera de dichas bases. Esto justifica la siguiente definición.

Definición 1.45. *Llamaremos* discriminante *de un módulo $L = [\mathbf{u}_0, \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3]$ al número*

$$\mathbf{D}(L) = +\sqrt{\det(2N)} = +\sqrt{\det\|T(\mathbf{u}_i\bar{\mathbf{u}}_j)\|}.$$

Observación 1.46. *Sobre $\mathcal{H}$ se tiene definida la forma bilineal traza $B_T(u, v) = T(uv)$. Lo habitual es definir el discriminante de un módulo $L = [\mathbf{u}_0, \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3]$ como el número $+\sqrt{|\det\|T(\mathbf{u}_i\mathbf{u}_j)\||}$. Observando que $\det(B_T) = -(4ab)^2$ en la base $\{\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$, es claro que ambas definiciones coinciden.*

Es claro que si $L_1 \subset L_2$ son dos módulos de $\mathcal{H}$, entonces $\mathbf{D}(L_1) = \mathbf{D}(L_2)[L_2 : L_1]$. En particular, se tiene:

Corolario 1.47. *Si $\mathcal{O}$ es un orden de $\mathcal{H}$, $\mathbf{D}(\mathcal{O})$ es un entero. Si $\mathcal{O}_1 \subset \mathcal{O}_2$ son dos órdenes de $\mathcal{H}$, entonces $\mathbf{D}(\mathcal{O}_1) = \mathbf{D}(\mathcal{O}_2)[\mathcal{O}_2 : \mathcal{O}_1]$.*

El siguiente resultado (ver [9, Corolario 5.3, p. 84]) es importante para reconocer si un orden es o no maximal:

Proposición 1.48. *Un orden $\mathcal{O} \subset \mathcal{H}$ es maximal si y sólo si $\mathbf{D}(\mathcal{O}) = d(\mathcal{H})$.*

Definición 1.49. *Llamaremos* divisor *de un orden $\mathcal{O}$, y lo denotaremos $\sigma(\mathcal{O})$ al máximo entero $n > 0$ para el cual existe un orden $[\mathbf{1}, \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3]$ tal que $\mathcal{O} = [\mathbf{1}, n\mathbf{u}_1, n\mathbf{u}_2, n\mathbf{u}_3]$. Diremos que $\mathcal{O}$ es un orden primitivo si $\sigma(\mathcal{O}) = 1$.*

Definición 1.50. *Diremos que un módulo unitario L es* clásico *si todos sus elementos tienen traza par, en caso contrario diremos que L es* no clásico. *Un orden será clásico (o no clásico) si lo es como módulo.*

Ejemplo 1.51. *$\mathcal{O}_c = [\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}]$ es un orden clásico. Como veremos (Corolario* 2.18*) no es maximal.*

Hasta aquí hemos considerado los órdenes de una determinada álgebra de cuaterniones racionales. En nuestro estudio necesitaremos considerar órdenes cuaterniónicos en general. Para ello nos serán útiles las siguientes definiciones:

Definición 1.52. *Diremos que $\mathcal{O}$ es un* orden cuaterniónico *si $\mathcal{O} \subset \mathcal{H}$ es un orden de un álgebra de cuaterniones racionales $\mathcal{H}$. Si $\mathcal{H}$ es definida (indefinida) diremos que $\mathcal{O}$ es un orden cuaterniónico* definido (indefinido).

Si $\mathcal{O}_1 \subset \mathcal{H}_1$ y $\mathcal{O}_2 \subset \mathcal{H}_2$ son dos órdenes cuaterniónicos, diremos que $\mathcal{O}_1$ es equivalente *a $\mathcal{O}_2$, y lo denotaremos $\mathcal{O}_1 \sim \mathcal{O}_2$, si existe un isomorfismo $\lambda : \mathcal{H}_1 \to \mathcal{H}_2$ tal que $\lambda(\mathcal{O}_1) = \mathcal{O}_2$.*

Observación 1.53. *Es claro que $\mathcal{O}_1 \sim \mathcal{O}_2$ es una relación de equivalencia que, en el caso de órdenes contenidos en un $\mathcal{H}$, coincide con la definición habitual, esto es: existe un automorfismo (interior por Lema* 1.6*) $\lambda : \mathcal{H} \to \mathcal{H}$ tal que $\lambda(\mathcal{O}_1) = \mathcal{O}_2$.*

Por otra parte, puesto que la conjugación define un isomorfismo entre $\mathcal{H}$ y $\mathcal{H}^{op}$, resulta que todo orden cuaterniónico $\mathcal{O}$ es equivalente al orden $\mathcal{O}^{op}$ (comparar con Observación 1.43).

Observemos también que tanto el discriminante de un orden como las propiedades de ser definido, indefinido, primitivo, clásico o no clásico son invariantes *respecto de esta relación de equivalencia; es decir, coinciden para todos los órdenes de una clase.*

Definición 1.54. *Si $\mathcal{O}_1 \subset \mathcal{H}_1$ y $\mathcal{O}_2 \subset \mathcal{H}_2$ son dos órdenes cuaterniónicos, diremos que $\mathcal{O}_1$* está contenido en sentido amplio *en $\mathcal{O}_2$, y lo denotaremos $\mathcal{O}_1 \prec \mathcal{O}_2$, si existe un isomorfismo $\lambda : \mathcal{H}_1 \to \mathcal{H}_2$ tal que $\lambda(\mathcal{O}_1) \subset \mathcal{O}_2$. En tal caso definimos el* índice $[\mathcal{O}_2 : \mathcal{O}_1] = [\mathcal{O}_2 : \lambda(\mathcal{O}_1)]$.

Observaciones 1.55. *(1) Si $\mathcal{O}_1$ y $\mathcal{O}_2$ son dos órdenes cuaterniónicos, es claro que $\mathcal{O}_1 \sim \mathcal{O}_2$ si y sólo si $\mathcal{O}_1 \prec \mathcal{O}_2$ y $\mathcal{O}_2 \prec \mathcal{O}_1$.*

(2) Es inmediata la verificación de que los conceptos de «estar contenido en sentido amplio» *y de* «índice» *se extienden a clases de órdenes cuaterniónicos equivalentes.*

(3) Si $\mathcal{O}_1 \prec \mathcal{O}_2$ (como órdenes cuaterniónicos o como sus clases) resulta, como en el Corolario 1.47, *que $\mathbf{D}(\mathcal{O}_1) = \mathbf{D}(\mathcal{O}_2)[\mathcal{O}_2 : \mathcal{O}_1]$.*

Como hemos visto en la Observación 1.20, para establecer una correspondencia entre clases de formas ternarias racionales y álgebras de cuaterniones $\mathcal{H}$ sobre $\mathbf{Q}$ resulta fundamental la descomposición ortogonal $\mathcal{H} = \langle \mathbf{1} \rangle \perp \mathcal{H}^0$ del espacio cuadrático $(\mathcal{H}, N)$. Nos proponemos estudiar este tipo de descomposición en el caso de los espacios cuadráticos (L, N) obtenidos por restricción de la forma norma N a un orden o, más generalmente, a un módulo unitario L.

Nota: En todo lo que sigue, denotaremos $\mathbf{u}^* = \mathbf{u} - \frac{T(\mathbf{u})}{2}\mathbf{1}$ para todo elemento $\mathbf{u}$ de un álgebra de cuaterniones racionales $\mathcal{H}$.

Sea $L = [\mathbf{1}, \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3]$ un módulo unitario y sea $L^0 = L \cap \mathcal{H}^0$. En el caso en que L es un módulo clásico, $L^0 = [\mathbf{u}_1^*, \mathbf{u}_2^*, \mathbf{u}_3^*]$ es una subred de rango 3 de L y $L = \langle \mathbf{1} \rangle \perp L^0$ como espacio cuadrático. Si L es no clásico, una tal descomposición ortogonal no existe. De todos modos, podemos considerar los elementos $\mathbf{u}_i^*$ (que no necesariamente pertenecerán a L) y el módulo unitario $L^* = [\mathbf{1}, \mathbf{u}_1^*, \mathbf{u}_2^*, \mathbf{u}_3^*]$ que será clásico con $L^{*0} = [\mathbf{u}_1^*, \mathbf{u}_2^*, \mathbf{u}_3^*]$ y $L^* = \langle \mathbf{1} \rangle \perp L^{*0}$.

Lema 1.56. *Dado un módulo unitario $L = [\mathbf{1}, \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3]$, el módulo unitario $L^* = [\mathbf{1}, \mathbf{u}_1^*, \mathbf{u}_2^*, \mathbf{u}_3^*]$ depende sólo de L y no de la base unitaria utilizada para definirlo.*

Demostración. Sea $\{\mathbf{1}, \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ otra base unitaria de L y sean

$$\mathbf{v}_t = \alpha_t \mathbf{1} + \sum_{s=1}^{3} \alpha_{st}\mathbf{u}_s \qquad (t = 1, 2, 3).$$

Siendo $T(\mathbf{v}_t) = 2\alpha_t + \sum_{s=1}^{3} \alpha_{st} T(\mathbf{u}_s)$ resulta que $\mathbf{v}_t^* = \sum_{s=1}^{3} \alpha_{st}\mathbf{u}_s^*$. Luego, $L^* = [\mathbf{1}, \mathbf{v}_1^*, \mathbf{v}_2^*, \mathbf{v}_3^*]$. □

Definición 1.57. *Dado un módulo unitario $L = [\mathbf{1}, \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3]$, llamaremos* módulo clásico asociado a L *al módulo $L^* = [\mathbf{1}, \mathbf{u}_1^*, \mathbf{u}_2^*, \mathbf{u}_3^*]$.* Denotaremos (V_L^*, N^*) *o, simplemente, (V^*, N^*) al espacio cuadrático obtenido por restricción de la forma norma N a $V^* = [\mathbf{u}_1^*, \mathbf{u}_2^*, \mathbf{u}_3^*]$, de modo que, como espacio cuadrático, $L^* = \langle \mathbf{1} \rangle \perp V^*$.*

Es claro que si L es un módulo clásico, entonces $L^* = L$ y $V^* = L^0 = L \cap \mathcal{H}^0$. Además, del Lema 1.56 y de su demostración se sigue el siguiente:

Corolario 1.58. *Para toda base unitaria $\{\mathbf{1}, \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3\}$ de un módulo unitario L, $\{\mathbf{u}_1^*, \mathbf{u}_2^*, \mathbf{u}_3^*\}$ es una base de V^*.*

Observación 1.59. *Sea $L = [\mathbf{1}, \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3]$ un módulo unitario no clásico. Veamos cómo puede interpretarse el módulo clásico L^* asociado a L.*

El primero en considerar el problema (aunque sólo para órdenes maximales) fue Latimer [7]. *Su idea consiste en tomar $L^0 = L \cap \mathcal{H}^0$ y considerar el módulo clásico $L' = \langle \mathbf{1} \rangle \perp L^0$.*

Por hipótesis, alguno de los $\mathbf{u}_i$ tiene traza impar. Podemos suponer que $i = 1$ y que $T(\mathbf{u}_1) = 2t + 1$. Tomemos $\mathbf{v}_1 = \mathbf{u}_1 - t\mathbf{1}$ y, para $j > 1$, $\mathbf{v}_j = \mathbf{u}_j^*$ si $T(\mathbf{u}_j)$ es par y $\mathbf{v}_j = (\mathbf{u}_j - \mathbf{v}_1)^*$ en caso contrario. Es claro que $\{\mathbf{1}, \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ es una base de L tal que $T(\mathbf{v}_1) = 1$ y $T(\mathbf{v}_2) = T(\mathbf{v}_3) = 0$. A una tal base Latimer la llama base normal *de L. Es claro que $L^0 = [\mathbf{v}_1', \mathbf{v}_2', \mathbf{v}_3']$ con $\mathbf{v}_1' = 2\mathbf{v}_1 - \mathbf{1}$, $\mathbf{v}_2' = \mathbf{v}_2$ y $\mathbf{v}_3' = \mathbf{v}_3$, es una subred de rango 3 de L y que $L' = [\mathbf{1}, \mathbf{v}_1', \mathbf{v}_2', \mathbf{v}_3']$ es un submódulo de L con $[L : L'] = 2$.*

Como veremos, para establecer su correspondencia parcial entre formas ternarias enteras y órdenes cuaterniónicos Latimer utiliza el espacio cuadrático (L^0, N). Sin embargo, para conseguir una correspondencia completa necesitaremos que el módulo clásico asociado a L tenga el mismo discriminante que L, mientras que ahora tenemos que $\mathbf{D}(L') = 2\mathbf{D}(L)$.

Una manera natural *de sumergir a L' en un módulo clásico que lo contenga como submódulo de índice 2 es tomando $[\mathbf{1}, \mathbf{v}_1'/2, \mathbf{v}_2', \mathbf{v}_3'] = [\mathbf{1}, \mathbf{v}_1^*, \mathbf{v}_2^*, \mathbf{v}_3^*] = L^*$.*

Observemos que si L es entero (en particular, si L es un orden), L' es entero, pero L^* no será entero en general.

De la observación anterior y la definición de discriminante de un módulo se tiene:

Corolario 1.60. *Si L^* es el módulo clásico asociado a un módulo unitario L, entonces* $\mathbf{D}(L^*) = \mathbf{D}(L)$ *y* $4\mathbf{D}(N^*) = \mathbf{D}(L)^2$.

Observación 1.61. *Hemos visto (Observación* 1.15*) que, desde un punto de vista computacional, trabajaremos con el álgebra de cuaterniones $\mathcal{H} = \mathcal{H}(d)$ y en la correspondiente base $B_c = \{\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$. Del mismo modo, al trabajar con un módulo unitario L de $\mathcal{H}$ lo haremos en su* base normal de Hermite *(relativa a la base B_c), esto es en la base $B = \{\mathbf{1}, \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3\}$ tal que si $A = \|\alpha_{ij}\|$ es la matriz del cambio de la base B* a la base *B_c, dicha matriz verifica:*

(1) A *es triangular superior,*

(2) $\alpha_{ii} > 0$,

(3) $0 \le \alpha_{ij} < \alpha_{ii}$,

es decir, A está en su forma normal superior de Hermite.

Lo importante es que dicha base es única, lo que permite, por ejemplo, determinar fácilmente si dos módulos unitarios son iguales o no.

Observemos que a partir de la base normal de Hermite de un módulo unitario L es posible definir una base canónica *del módulo clásico asociado a L. Esto permite dar otra demostración del Lema* 1.56.

2. ESTUDIO DE LA CORRESPONDENCIA

Aquí comenzamos el estudio de la correspondencia entre formas ternarias enteras y órdenes cuaterniónicos.

2.1. El orden de Clifford de una forma ternaria entera

Sean $f = (a_1, a_2, a_3, a_{23}, a_{13}, a_{12})$ una forma ternaria racional (regular) y (V, f) el espacio cuadrático asociado con base $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$. Recordemos que el álgebra de Clifford $C(f)$ tiene base $\{\mathbf{1}, \mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{E}_1, \mathbf{E}_2, \mathbf{E}_3, \mathbf{E}\}$ y que su producto está determinado por las relaciones (4). El álgebra de cuaterniones $C_0(f)$ es la subálgebra de $C(f)$ de base $\{\mathbf{1}, \mathbf{E}_1, \mathbf{E}_2, \mathbf{E}_3\}$. Recordando la convención hecha sobre los índices (i, j, k) a continuación de la Definición 1.17, un simple cálculo muestra el siguiente:

Lema 2.1. *El producto en $C_0(f)$ está determinado por las expresiones:*

(a) $\mathbf{E}_i^2 = -a_j a_k + a_{jk}\mathbf{E}_i$. *Luego,* $T(\mathbf{E}_i) = a_{jk}$ *y* $N(\mathbf{E}_i) = a_j a_k$.

(b) $\mathbf{E}_i\mathbf{E}_j = a_{ij}a_k - a_k\mathbf{E}_k$

(c) $\mathbf{E}_j\mathbf{E}_i = -a_{ik}a_{jk} + a_{ik}\mathbf{E}_i + a_{jk}\mathbf{E}_j + a_k\,\mathbf{E}_k$

Corolario 2.2. *f es entera si y sólo si* $[\mathbf{1}, \mathbf{E}_1, \mathbf{E}_2, \mathbf{E}_3]$ es un orden de $C_0(f)$. □

Definición 2.3. *Llamaremos orden de Clifford de la forma ternaria entera f, y lo denotaremos $\mathcal{O}(f)$, al orden* $[\mathbf{1}, \mathbf{E}_1, \mathbf{E}_2, \mathbf{E}_3]$ *de $C_0(f)$, y llamaremos* base de Clifford *a su base* $\{\mathbf{1}, \mathbf{E}_1, \mathbf{E}_2, \mathbf{E}_3\}$.

Observación 2.4. *Sean f una forma ternaria y $\mathcal{O}(f) = [\mathbf{1}, \mathbf{E}_1, \mathbf{E}_2, \mathbf{E}_3]$ su orden de Clifford, dado en su base de Clifford. Del Lema 2.1 se sigue que $\mathcal{O}(-f) = [\mathbf{1}, -\mathbf{E}_1, -\mathbf{E}_2, -\mathbf{E}_3] = \mathcal{O}(f)$. Este hecho refuerza nuestra convención de considerar sólo formas ternarias enteras f con* $\mathbf{D}(f) > 0$.

Corolario 2.5. *Sea f entera, entonces f es clásica si y sólo si $\mathcal{O}(f)$ es un orden clásico y f es primitiva si y sólo si $\mathcal{O}(f)$ es un orden primitivo.*

Definición 2.6. *Si $f = ng$ con $n \in \mathbf{Z}$ $(n \neq 0)$ y g es entera primitiva, entonces* $\mathcal{O}(g) = [\mathbf{1}, \mathbf{E}_1/n, \mathbf{E}_2/n, \mathbf{E}_3/n]$ donde $\mathcal{O}(f) = [\mathbf{1}, \mathbf{E}_1, \mathbf{E}_2, \mathbf{E}_3]$.

Corolario 2.7. *La matriz de la forma norma en $\mathcal{O}(f)$ en la base de Clifford es:*

$$\begin{pmatrix} 1 & a_{23}/2 & a_{13}/2 & a_{12}/2 \\ a_{23}/2 & a_2a_3 & (a_{23}a_{13} - a_3a_{12})/2 & (a_{12}a_{23} - a_2a_{13})/2 \\ a_{13}/2 & (a_{23}a_{13} - a_3a_{12})/2 & a_1a_3 & (a_{12}a_{13} - a_1a_{23})/2 \\ a_{12}/2 & (a_{12}a_{23} - a_2a_{13})/2 & (a_{12}a_{13} - a_1a_{23})/2 & a_1a_2 \end{pmatrix}.$$

Desde ahora supondremos que f es entera. Nos proponemos estudiar el módulo clásico $\mathcal{O}(f)^* = [\mathbf{1}, \mathbf{E}_1^*, \mathbf{E}_2^*, \mathbf{E}_3^*]$ asociado a $\mathcal{O}(f) = [\mathbf{1}, \mathbf{E}_1, \mathbf{E}_2, \mathbf{E}_3]$ y, en particular, el espacio cuadrático (V^*, N^*).

Lema 2.8. *Sea $M = \|\alpha_{st}\| \in \mathbf{GL}(3, \mathbf{Z})$ la matriz del cambio de una base $\{\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3\}$ de V a la base $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$; esto es:*

$$\mathbf{u}_t = \sum_{s=1}^{3} \alpha_{st}\mathbf{e}_s \qquad (t = 1, 2, 3).$$

Si $\mathbf{U}_i^*$ está definido a partir de $\{\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3\}$ tal como $\mathbf{E}_i^*$ está definido a partir de $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$, entonces $\mathrm{Adj}(M)$ *es la matriz del cambio de la base $\{\mathbf{U}_1^*, \mathbf{U}_2^*, \mathbf{U}_3^*\}$ de V^* a la base $\{\mathbf{E}_1^*, \mathbf{E}_2^*, \mathbf{E}_3^*\}$.*

Demostración. Es un simple cálculo a partir de (4) y razonando como en la demostración del Lema 1.56. □

Siendo $T(\mathbf{E}_i^*) = 0$, es claro que $\mathbf{E}_j^*\,\mathbf{E}_i^* = \overline{\mathbf{E}_i^*\mathbf{E}_j^*}$. Luego, del Lema 2.1 se obtiene:

Lema 2.9. *El producto de elementos de $\mathcal{O}(f)^*$ está determinado por las expresiones:*

$$\mathbf{E}_i^*\mathbf{E}_j^* = \left(\frac{a_{ij}a_k}{2} - \frac{a_{ik}a_{jk}}{4}\right) + \frac{a_{ik}}{2}\,\mathbf{E}_i^* + \frac{a_{jk}}{2}\,\mathbf{E}_j^* + a_k\mathbf{E}_k^*.$$

Proposición 2.10. *Como formas ternarias enteras,* $4N^* = {}^af$.

Demostración. La proposición se sigue del Lema 2.9 y de la definición de ${}^af$, observando que $N(\mathbf{E}_i^*) = -\mathbf{E}_i^{*2} = a_j a_k - \frac{a_{jk}^2}{4}$.

Recordando que $\mathbf{D}({}^af) = 16\mathbf{D}(f)^2$, de la proposición anterior y el Corolario 1.60 se obtiene:

Corolario 2.11. *Para toda forma ternaria entera* f, $\mathbf{D}(\mathcal{O}(f)) = \mathbf{D}(f)$.

2.2. El teorema fundamental

Sean $\mathcal{F}_+$ el conjunto de todas las clases $\bar{f}$ de formas ternarias enteras f con $\mathbf{D}(f) > 0$ y Ω el conjunto de todas las clases $\bar{\mathcal{O}}$ de órdenes cuaterniónicos $\mathcal{O}$ con $d > 1$. De la propiedad universal del álgebra de Clifford se sigue:

Proposición 2.12. *La aplicación* $\Psi: \mathcal{F}_+ \to \Omega$ *que a la clase de una forma* f *le hace corresponder la clase de su orden de Clifford* $\mathcal{O}(f)$ *está bien definida.*

En esta sección nos proponemos estudiar la aplicación Ψ.

Sea $\mathcal{O} = [\mathbf{u}_0 = \mathbf{1}, \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3] \subset \mathcal{H}$ un orden cuaterniónico con $d > 1$. Se tiene:

$$\mathbf{u}_s\mathbf{u}_t = \sum_{r=0}^{3} \pi(s, t, r)\mathbf{u}_r \qquad (s, t = 1, 2, 3)$$

donde los $\pi(s, t, r)$ son enteros por definición de orden.

Sea $\mathcal{O}^* = [\mathbf{1}, \mathbf{u}_1^*, \mathbf{u}_2^*, \mathbf{u}_3^*]$ el correspondiente módulo clásico asociado a $\mathcal{O}$. Siendo $T(\mathbf{u}_i^*) = 0$, es claro que $\mathbf{u}_j^*\mathbf{u}_i^* = \overline{\mathbf{u}_i^*\mathbf{u}_j^*}$ luego, el producto entre elementos de $\mathcal{O}^*$ queda determinado por los doce coeficientes $\pi^*(i, j, r) \in \mathbf{Q}$ tales que:

$$\mathbf{u}_i^*\mathbf{u}_j^* = \sum_{r=0}^{3} \pi^*(i, j, r)\mathbf{u}_r^*. \tag{8}$$

Lema 2.13. *Con la convención hecha sobre los índices* (i, j, k):

(i) Sean $b_i = \pi^*(j, k, i)$. *Los tres* b_i *son enteros no nulos.*

(ii) Se verifican las tres igualdades $\pi^*(i, j, j) = \pi^*(k, i, k)$.

(iii) $2\pi^*(i, j, j)$ *es un entero de la misma paridad que* $T(\mathbf{u}_i)$.

Demostración. Es claro que $b_i = \pi^*(j, k, i) = \pi(j, k, i)$ son enteros. Si $b_i = 0$, entonces $\{\mathbf{1}, \mathbf{u}_j^*, \mathbf{u}_k^*\}$ generarían sobre $\mathbf{Q}$ un subanillo de $\mathcal{H}$ de grado 3 sobre $\mathbf{Q}$, lo que contradice al Corolario 1.8. Luego *(i)* queda probada. Igualando el coeficiente de $\mathbf{u}_k^*$ en

$$\mathbf{u}_i^*(\mathbf{u}_i^*\mathbf{u}_j^*) = -N(\mathbf{u}_i^*)\mathbf{u}_j^* = \sum_{r=0}^{3} \pi^*(i, j, r)\mathbf{u}_i^*\mathbf{u}_r^* \tag{9}$$

de *(i)* se obtiene fácilmente *(ii)*. Por último, *(iii)* es consecuencia del hecho que $\pi^*(i, j, j) = \pi(i, j, j) - T(\mathbf{u}_i)/2$. □

Proposición 2.14. *Para todo orden cuaterniónico* $\mathcal{O} = [\mathbf{1}, \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3]$ *con* $d > 1$ *existe una forma ternaria entera* f *tal que* $\mathbf{D}(f) > 0$ *y* $\mathcal{O}$ *es equivalente a* $\mathcal{O}(f)$.

Demostración. Sean b_i definidos como en la parte *(i)* del lema anterior y sean $a_i = \varepsilon b_i$, $a_{jk} = 2\varepsilon\pi^*(i, j, j)$, con $\varepsilon = \pm 1$ a determinar. Por el lema anterior, $f = (a_1, a_2, a_3, a_{23}, a_{13}, a_{12})$ es una forma ternaria entera. Determinamos ε de modo que $\mathbf{D}(f) > 0$ y aseguramos que $\mathcal{O}$ es equivalente a $\mathcal{O}(f)$.

En efecto, sean $\mathbf{v}_i = \varepsilon\mathbf{u}_i + \varepsilon t_i\mathbf{1}$ con $t_i = (a_{jk} - T(\mathbf{u}_i))/2$. Por la parte *(iii)* del lema anterior los t_i son enteros, de modo que $\mathcal{O} = [\mathbf{1}, \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3]$. Comparando las expresiones para $\mathbf{v}_i^2$, $\mathbf{v}_i\mathbf{v}_j$ y $\mathbf{v}_j\mathbf{v}_i$ con las correspondientes para la base de Clifford de $\mathcal{O}(f)$ dadas en el Lema 2.1, se concluye que $\mathcal{O}$ es equivalente a $\mathcal{O}(f)$. □

Observación 2.15. *(1) En el caso definido, igualando el coeficiente de* $\mathbf{u}_j^*$ *en* (9), *resulta que* $b_j b_k = N(\mathbf{u}_i^*) + \pi^*(i, j, j)^2 > 0$, *lo que prueba que los enteros* b_i *son no nulos y tienen un mismo signo* ε. *La tabla de los productos de los* $\mathbf{v}_i$ *es similar a la del Lema* 2.1 *o está* invertida, *es decir, es similar a la correspondiente a* $\mathcal{O}(f)^{op}$, *en cuyo caso parece natural tomar la base conjugada* $\mathcal{O} = [\mathbf{1}, \bar{\mathbf{v}}_1, \bar{\mathbf{v}}_2, \bar{\mathbf{v}}_3]$. *En el caso indefinido ocurre algo similar.*

(2) No sólo hemos probado que todo orden cuaterniónico $\mathcal{O} = [\mathbf{1}, \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3]$ *es equivalente a un* $\mathcal{O}(f)$, *sino también que* ajustando las trazas *de los* $\mathbf{u}_i$ *(o, eventualmente, de los* $-\mathbf{u}_i$, de los $\bar{\mathbf{u}}_i$ o de los $-\bar{\mathbf{u}}_i$*) la equivalencia se obtiene aplicando la base de* $\mathcal{O}$ *en la base de Clifford de* $\mathcal{O}(f)$.

Ahora estamos en condiciones de probar el resultado central de este trabajo:

Teorema 2.16. *La aplicación* $\Psi: \mathcal{F}_+ \to \Omega$ *que a la clase de una forma* f *le hace corresponder la clase de su orden de Clifford* $\mathcal{O}(f)$, *es biyectiva.*

Las clases de formas definidas (indefinidas) se corresponden, por Ψ, *con las clases de órdenes definidos (indefinidos), las clases de formas primitivas se corresponden con las clases de órdenes primitivos y las clases de formas clásicas se corresponden con las clases de órdenes clásicos.*

Demostración. Hemos visto que Ψ es una aplicación bien definida (Proposición 2.12) y que es sobre (Proposición 2.14). Sólo resta probar que Ψ es inyectiva.

Supongamos que f y f' son dos formas ternarias enteras de discriminante positivo tales que $\mathcal{O}(f) \sim \mathcal{O}(f')$. Sean (V, f) y (V', f') los espacios cuadráticos asociados, y sean $\mathcal{O}(f) = [\mathbf{1}, \mathbf{E}_1, \mathbf{E}_2, \mathbf{E}_3]$ y $\mathcal{O}(f') = [\mathbf{1}, \mathbf{E}'_1, \mathbf{E}'_2, \mathbf{E}'_3]$ expresados en las correspondientes bases de Clifford. Siendo $\mathcal{O}(f) \sim \mathcal{O}(f')$, $\mathcal{O}(f) = [\mathbf{1}, \mathbf{U}_1, \mathbf{U}_2, \mathbf{U}_3]$ donde los $\mathbf{U}_i$ poseen idénticas propiedades algebraicas que los $\mathbf{E}'_i$. Por el Corolario 1.58, $\{\mathbf{E}_1^*, \mathbf{E}_2^*, \mathbf{E}_3^*\}$ y $\{\mathbf{U}_1^*, \mathbf{U}_2^*, \mathbf{U}_3^*\}$ son bases de (V^*, N^*). Luego, por la Proposición 2.10 resulta que ${}^af \sim {}^af'$ y, por la Proposición 1.29 *(iii)*, $f \sim f'$. Luego Ψ es inyectiva.

La última parte del teorema es consecuencia de la Proposición 1.18 y el Corolario 2.5. □

Del teorema anterior y el Corolario 2.11 se sigue:

Corolario 2.17. *Si* $\Psi(\bar{f}) = \overline{\mathcal{O}}$ *entonces* $\mathbf{D}(\bar{f}) = \mathbf{D}(\overline{\mathcal{O}})$.

Corolario 2.18. *Ningún orden clásico es maximal. En efecto, a la clase de un orden maximal le corresponde una clase de formas primitivas no clásicas.*

Demostración. Sea $\mathcal{O} = \mathcal{O}(f)$ un orden maximal en un álgebra de cuaterniones $\mathcal{H}$. Es claro que $\mathcal{O}$ (y luego f) debe ser primitivo. Por Proposición 1.48, $\mathbf{D}(\mathcal{O}) = d(\mathcal{H})$ es un entero libre de cuadrados. Siendo $\mathbf{D}(\mathcal{O}) = \mathbf{D}(f)$ (Corolario 2.11), f es una forma no clásica pues en caso contrario $\det \mathbf{M}(f)$ es entero y $4 \mid \mathbf{D}(f)$. □

Sean f_1 y f_2 dos formas ternarias enteras. Es claro que si la forma f_2 representa a la forma f_1 entonces existe una isometría entre los correspondientes espacios cuadráticos y, por la propiedad universal del álgebra de Clifford, una aplicación de $C(f_1)$ en $C(f_2)$ que, restringida a sus partes pares, muestra que $\mathcal{O}(f_1) \prec \mathcal{O}(f_2)$. Sin embargo, es posible que $\mathcal{O}(f_1) \prec \mathcal{O}(f_2)$ sin que la forma f_2 represente a la forma f_1, como muestra la proposición siguiente (comparar con *(2)* de las Observaciones 1.33).

Proposición 2.19. $\Psi(\bar{f}_1) \prec \Psi(\bar{f}_2) \Leftrightarrow \bar{f}_1 \lhd \bar{f}_2$.

Demostración. Sean f_1 y f_2 dos formas ternarias enteras y sean (V_1^*, N_1^*) y (V_2^*, N_2^*) los correspondientes espacios cuadráticos obtenidos a partir de $\mathcal{O}(f_1)^*$ y $\mathcal{O}(f_2)^*$. Razonando como en las demostraciones de los lemas 1.56 y 2.8 se prueba que $\mathcal{O}(f_1) \prec \mathcal{O}(f_2)$ si y sólo si existe una isometría de (V_2^*, N_2^*) en (V_1^*, N_1^*), y esto ocurre (por Proposición 2.10) si y sólo si ${}^af_2$ representa a ${}^af_1$, es decir, si y sólo si $f_1 \lhd f_2$. □

Corolario 2.20. *Sea* $\Psi(\bar{f}) = \overline{\mathcal{O}}$ *entonces* $\overline{\mathcal{O}}$ *es maximal si y sólo si* $\bar{f}$ *es fundamental.*

Teniendo en cuenta la Proposición 1.48 y los corolarios 2.17 y 2.20, resulta:

Corolario 2.21. *Una forma ternaria entera f (de discriminante positivo) es fundamental si y sólo si* $\mathbf{D}(f) = d(f)$.

Observación 2.22. *Sean* $\mathcal{O}_1$ *y* $\mathcal{O}_2$ *dos órdenes cuaterniónicos. Diremos que* $\mathcal{O}_1$ *es isomorfo a* $\mathcal{O}_2$, *y lo denotaremos* $\mathcal{O}_1 \approx \mathcal{O}_2$, *si existe un isomorfismo de anillos con unidad* F: $\mathcal{O}_1 \to \mathcal{O}_2$. *Es posible, entonces, considerar las* clases de isomorfía *de órdenes cuaterniónicos. Es claro que, en general,* $\mathcal{O}_1 \sim \mathcal{O}_2 \Rightarrow \mathcal{O}_1 \approx \mathcal{O}_2$. *Es interesante destacar que vale la recíproca. En efecto, basta observar que el argumento utilizado para probar la inyectividad de* Ψ *en el teorema anterior permite demostrar que* $\mathcal{O}(f_1) \approx \mathcal{O}(f_2) \Rightarrow f_1 \sim f_2$.

Una manera de enunciar este hecho es la siguiente:

Corolario 2.23. *Sean* $\mathcal{O}_1 \subset \mathcal{H}_1$ *y* $\mathcal{O}_2 \subset \mathcal{H}_2$ *órdenes en álgebras de cuaterniones racionales. Todo isomorfismo de anillos con unidad* F: $\mathcal{O}_1 \to \mathcal{O}_2$ *se extiende a un único isomorfismo de álgebras* λ: $\mathcal{H}_1 \to \mathcal{H}_2$.

2.3. La correspondencia de Latimer

El primero en establecer una correspondencia entre clases de formas ternarias enteras y clases de órdenes cuaterniónicos fue Latimer [7], en 1937. Su correspondencia es parcial pues se limita a considerar el conjunto $\Omega_m \subset \Omega$ de las clases de órdenes maximales, con la definición habitual de equivalencia (ver Observación 1.53).

La presentación de Latimer es inversa de la desarrollada en las secciones anteriores. En efecto, él parte de un orden maximal $\mathcal{O} = [\mathbf{1}, \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3]$ contenido en un álgebra de cuaterniones racionales $\mathcal{H}$ de discriminante d. Para ello utiliza una caracterización de los órdenes maximales debida a Brandt [2] que, esencialmente, puede considerarse equivalente a nuestro Corolario 2.20. Su propósito es el de asignarle a $\mathcal{O}$ una forma ternaria entera utilizando una descomposición similar a la descomposición ortogonal $\mathcal{H} = \langle \mathbf{1} \rangle \perp \mathcal{H}^0$ del espacio cuadrático $(\mathcal{H}, N)$.

Con este fin, define sus *bases normales* $\{\mathbf{1}, \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ de $\mathcal{O}$, obtiene la correspondiente base $\{\mathbf{v}'_1, \mathbf{v}'_2, \mathbf{v}'_3\}$ para $\mathcal{O}^0 = \mathcal{O} \cap \mathcal{H}^0$ (ver Observación 1.59) y la forma ternaria entera

$$(10) \qquad f = f(x_1, x_2, x_3) = N(x_1\mathbf{v}'_1 + x_2\mathbf{v}'_2 + x_3\mathbf{v}'_3)$$

Observa que $\mathbf{D}(f) = d^2$ y que f es clásica si y sólo si d es par. Finalmente, le asigna a $\mathcal{O}$ la forma f si d es par y la forma $2f$ si d es impar.

Observación 2.24. *Latimer no da ninguna justificación para esta elección, pero parece claro que desea trabajar sólo con formas clásicas, tal como lo hace Dickson en* [4], *y poder utilizar los caracteres allí definidos para determinar los géneros de formas ternarias enteras.*

Los autores que trabajan sólo con formas clásicas llaman impropiamente primitivas *a las formas* $2f$ *cuando* f *es una forma entera primitiva no clásica, y ésta es la manera de incluir tales formas* f *en sus estudios.*

De todos modos, desde nuestro punto de vista, parece más natural *(y equivalente para todos los fines) asignar a* $\mathcal{O}$ *la forma* f *de* (10) *en todos los casos.*

Se prueba fácilmente que la aplicación $\mathcal{L}: \Omega_m \to \mathcal{F}_+$ que a la clase de un orden cuaterniónico maximal $\mathcal{O}$ le hace corresponder la clase de la forma f (o $2f$) dada en (10) está bien definida.

Sea $\Omega_m(d)$ el conjunto de las clases de órdenes cuaterniónicos maximales $\mathcal{O}$ con $\mathbf{D}(\mathcal{O}) = d$. Latimer prueba que $\mathcal{L}(\Omega_m(d)) \subset \mathcal{G}_d$ donde $\mathcal{G}_d$ es un género de formas ternarias enteras (ver Observación 1.37) determinado por d.

Sea $\mathcal{F}_{\mathcal{L}} = \cup_d \mathcal{G}_d$, donde d recorre el conjunto de los discriminantes de álgebras de cuaterniones racionales, es decir, el conjunto de los enteros $d > 1$ libres de cuadrados. Entonces considera $\mathcal{L}: \Omega_m \to \mathcal{F}_{\mathcal{L}}$.

Latimer prueba la inyectividad de la aplicación $\mathcal{L}$ a partir del siguiente:

Lema 2.25 (Latimer). *Sean* $\mathcal{O}_1$ *y* $\mathcal{O}_2$ *dos órdenes maximales en un álgebra de cuaterniones racionales* $\mathcal{H}$. *Entonces* $\mathcal{O}_1 = \mathcal{O}_2$ *si y sólo si* $\mathcal{O}_1^0 = \mathcal{O}_2^0$.

Observación 2.26. *La demostración del lema anterior es trabajosa y está precedida por un interesante estudio de las bases de un álgebra de cuaterniones racionales* $\mathcal{H}$ *que sean* «canónicas» *y permitan determinar bases normales particulares para un orden maximal* $\mathcal{O} \subset \mathcal{H}$ *dado. Este estudio está relacionado con la construcción de* $\mathcal{H}(d)$ *realizada en la segunda de las Observaciones* 1.15.

Sea $\mathcal{H}$ *un álgebra de cuaterniones racionales con* $d = d(\mathcal{H}) > 1$. *Para todo primo* $q \in \mathcal{P}$ *que verifica las condiciones (i) y (ii) que allí se establecieron,* $\mathcal{H} = \mathcal{H}(-q, -d)$ *si es definida y* $\mathcal{H} = \mathcal{H}(-q, d)$ *si es indefinida (recordemos que ésta es la definición de* $\mathcal{H}(d)$ *con* q *el menor de tales primos).*

El cuerpo $K = \mathbf{Q}(\mathbf{i}) \subset \mathcal{H}$ *es el cuerpo cuadrático* $\mathbf{Q}(\sqrt{-q})$. *Sea* $E \subset K$ *el anillo de los enteros de K. Luego* $E = [\mathbf{1}, \sigma]$, *con* $\sigma = (\mathbf{1} + \mathbf{i})/2$, *es el (único) orden maximal de K.*

Para todo orden maximal $\mathcal{O} \subset \mathcal{H}$, $\mathcal{O} \cap E = [\mathbf{1}, c\sigma]$ *será un orden de K de determinado conductor* $c \geq 1$. *Latimer muestra que existen infinitos primos q, que verifican las condiciones (i) y (ii), para los cuales* $c = 1$, *es decir,* $E \subset \mathcal{O}$. *Entonces prueba que existen* $\mathbf{u}_2 = c_2\mathbf{j}$, *con* $0 < c_2 \in \mathbf{Z}$, *y* $\mathbf{u}_3$, *con* $T(\mathbf{u}_3) = 0$, *tales que* $\mathcal{O} = [\mathbf{1}, \sigma, \mathbf{u}_2, \mathbf{u}_3]$. *Claramente, ésta es una base normal de* $\mathcal{O}$. *En realidad, el resultado de Latimer es mucho más preciso y completo (ver* [7, *Teorema* 4]).

Utilizando resultados de Artin y de él mismo, Latimer concluye que, en el caso indefinido, los géneros de formas ternarias $\mathcal{G}_d$ contienen una única clase de formas. Luego, la inyectividad de $\mathcal{L}$ implica el siguiente:

Corolario 2.27. *En el caso indefinido, para cada discriminante* d *existe una única clase de órdenes cuaterniónicos maximales.*

Observación 2.28. *El Corolario* 2.27 *puede ser obtenido a partir de los corolarios* 2.20 *y* 2.21 *utilizando resultados de la teoría de formas cuadráticas ternarias enteras.*

En el caso indefinido, la sobreyectividad de la aplicación $\mathcal{L}$ es consecuencia de las observaciones previas al Corolario 2.27. Para probar la sobreyectividad de $\mathcal{L}$ en el caso definido, Latimer no utiliza ni el álgebra de Clifford ni el álgebra de cuaterniones de Hermite (ver Observacion 1.21), sino un trabajo de Fueter [5] donde se calculan las relaciones que determinan el producto de un álgebra de cuaterniones racionales $\mathcal{H}$ de discriminante d en términos de una base de un orden maximal de $\mathcal{H}$. También necesita un resultado de Brandt [1] y realizar una serie de prolijos cálculos a partir de una forma f tal que $\bar{f} \in \mathcal{G}_d$.

Así obtiene su resultado fundamental:

Teorema 2.29 [Latimer]. *La aplicación* $\mathcal{L}: \Omega_m \to \mathcal{F}_{\mathcal{L}}$ *es biyectiva.*

Observación 2.30. *A pesar de que la correspondencia dada por Latimer es parcial e insatisfactoria, cabe destacar que la establece entre* clases, *como la dada en el Teorema* 2.16, *y que se apoya en la idea de asociarle a un orden un módulo unitario clásico. Por otra parte, algunas ideas contenidas en su artículo, como las comentadas en la Observación* 2.26, *resultan útiles tanto para determinar el cardinal de* $\Omega_m(d)$ (ver [9, p. 26]) *como en otras aplicaciones.*

2.4. La correspondencia de Brandt

El 21 de octubre de 1941, H. Brandt dio una conferencia en la Universidad de Jena que, por muchos motivos, puede considerarse fundamental. Dicha conferencia consta de tres partes (ver [3]). En la primera establece

una correspondencia entre formas ternarias enteras y órdenes cuaterniónicos; en la segunda estudia la composición de ideales en un álgebra de cuaterniones racionales y define el hoy llamado *grupoide de Brandt;* en la tercera define y estudia lo que él llama *matrices de Hecke* y que en la actualidad se denominan *matrices de Brandt.* En esta sección sólo nos ocuparemos de la primera parte de la conferencia de Brandt, haciendo una breve descripción de su correspondencia y comparándola con los resultados de las secciones anteriores.

Brandt parte de una forma ternaria entera $f = f(x_1, x_2, x_3)$ y considera el álgebra de cuaterniones de Hermite asociada $\mathcal{H}$ (ver Observación 1.21). Llama *forma norma de Hermite* a la forma cuadrática $H = H(x_0, x_1, x_2, x_3)$ que representa al espacio cuadrático $(\mathcal{H}, N)$ en la base $\{\mathbf{1}, \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3\}$ de Hermite, y observa que $H = x_0^2 + F(x_1, x_2, x_3)$, donde F es la forma ternaria que verifica $\mathbf{M}(F) = \text{adj}\,\mathbf{M}(f)$, es decir, *la adjunta de f en sentido clásico* (y no en el sentido de la Definición 1.28).

Si f es clásica, de (5) resulta que $[\mathbf{1}, \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3]$ es un orden de $\mathcal{H}$. Recíprocamente, si $\mathcal{O} \subset \mathcal{H}$ es un orden clásico y la forma norma N se expresa en una base de $\mathcal{O}$ correspondiente a la descomposición ortogonal $\mathcal{O} = \langle \mathbf{1} \rangle \perp \mathcal{O}^0$, resulta que $N = x_0^2 + G(x_1, x_2, x_3)$ y, por un resultado del mismo Brandt [1], G es *la adjunta en sentido clásico* de una forma ternaria entera g.

Brandt observa que si la forma f o el orden $\mathcal{O}$ son no clásicos, la forma cuadrática H no es entera y la construcción de Hermite debe ser «extendida para que siga valiendo lo mismo». Entonces define una nueva forma norma, *ajustando* convenientemente los coeficientes de H, de modo que la correspondencia anterior se extienda a todos los casos.

Finalmente muestra que si $f \sim f'$ entonces $H \sim H'$ y se obtiene *el mismo* orden.

Brandt no es totalmente explícito en esta parte de su conferencia. Si bien formalmente su correspondencia es entre clases de formas ternarias enteras y órdenes cuaterniónicos, tácitamente identifica órdenes isomorfos. Por otra parte, sus ajustes en los coeficientes de la forma norma de Hermite significan también ajustes en los elementos de la base de Hermite. Más claro en este sentido es Pall [8], que al comienzo de su artículo precisa y completa algunos aspectos del estudio de Brandt (y donde llama *forma norma de Brandt* a la extensión que éste hizo de la forma norma de Hermite). Aunque el interés de Pall no se centra en la correspondencia entre formas ternarias enteras y órdenes cuaterniónicos, tal vez no sería injusto llamarla *correspondencia de Brandt-Pall.*

Para relacionar el trabajo de Brandt con los resultados obtenidos en las secciones anteriores debemos comenzar observando que sus ideas se corresponden con las contenidas en la Observación 1.20 , que están vinculadas con la Proposición 2.10, y no con la construcción de un módulo clásico asociado a un orden.

Tampoco Brandt utiliza el álgebra de Clifford, pero sí el álgebra de cuaterniones de Hermite $\mathcal{H}$ asociada a una forma ternaria entera f, dada en una base $\{\mathbf{1}, \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3\}$. Si comparamos (5) con el Lema 2.9 y la demostración de la Proposición 2.10 , notamos que $\{\mathbf{1}, \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3\}$ resulta ser una base de $\mathcal{O}(f)^*$.

Cuando se trata de encontrar el orden $\mathcal{O}$ correspondiente a una forma f, los ajustes que realiza Brandt deben entenderse (como lo hace Pall [8]) semejantes a los *ajustes de las trazas* señalados en la segunda de las Observaciones 2.15. En general, un módulo unitario L no queda determinado por su módulo clásico asociado L^*. Sin embargo, de los resultados de las secciones anteriores no es difícil deducir que un orden $\mathcal{O}$ sí queda determinado por $\mathcal{O}^*$. Entonces, los ajustes de las trazas de los $\mathbf{u}_i$ pueden realizarse de una manera esencialmente única para obtener un orden $\mathcal{O}$, y éste resulta equivalente a $\mathcal{O}(f)$.

Recíprocamente, cuando se parte de un orden $\mathcal{O}$, los ajustes que realiza Brandt sobre los coeficientes de la forma norma de Hermite tienen como propósito el de hallar una expresión de la forma $N(x_0, x_1, x_2, x_3) = x_0^2 + F(x_1, x_2, x_3)$, tal que F sea *la adjunta en sentido clásico* de una forma ternaria entera f. Teniendo en cuenta la Proposición 2.10 y la definición de ${}^a f$, se obtiene que N^* es *la adjunta de f en sentido clásico.* Luego, la construcción de Brandt es esencialmente equivalente a la construcción de $\mathcal{O}^*$.

Teniendo en cuenta los comentarios anteriores y la Observación 2.22 (o su Corolario 2.23) podemos concluir que la correspondencia de Brandt, si bien conceptualmente es distinta, coincide con la dada por el Teorema 2.16.

2.5. Determinación efectiva de la correspondencia

La correspondencia Ψ: $\mathcal{F}_+ \longrightarrow \Omega$ dada por el Teorema 2.16 puede ser determinada efectivamente mediante algoritmos *Ordft*$[f]$ y *Ftord*$[\mathcal{O}]$ que calculan $\Psi(\bar{f})$ y $\Psi^{-1}(\overline{\mathcal{O}})$, respectivamente, y que pueden ser implementados en un ordenador. Como veremos, los resultados de las secciones anteriores permiten obtener dos versiones distintas para cada uno de ellos. En esta sección daremos un esquema de dichos algoritmos y haremos algunas observaciones sobre su implementación.

Como hemos mencionado en las Observaciones 1.15 y 1.61, todas las computaciones se realizarán en la base $B_c = \{\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ de la correspondiente álgebra de cuaterniones $\mathcal{H} = \mathcal{H}(d) = \mathcal{H}(a, b)$ y los módulos unitarios L de $\mathcal{H}$ se darán en su base normal de Hermite relativa a B_c. Esto permitirá trabajar con distintos L simultáneamente.

Algoritmo 2.31. *Ordft*1 [f].

La *entrada* del algoritmo es una forma ternaria entera f. Se calcula $d = d(f)$ y se trata de obtener un orden $\mathcal{O} \sim \mathcal{O}(f)$ contenido en $\mathcal{H} = \mathcal{H}(\mathrm{d}) = \mathcal{H}(a, b)$.

Utilizando el Corolario 2.7, se calcula la matriz M_1 de la forma norma N en la base de Clifford $\{\mathbf{1}, \mathbf{E}_1, \mathbf{E}_2, \mathbf{E}_3\}$ de $\mathcal{O}(f)$. Por otra parte, la matriz de N en la base B_c de $\mathcal{H}$ es $M_2 = \mathrm{diag}(1, -a, -b, ab)$, de modo que existe una matriz $M \in \mathbf{GL}(4, \mathbf{Q})$ tal que ${}^tM \cdot M_2 \cdot M = M_1$. Entonces $\|\mathbf{1}\ \mathbf{i}\ \mathbf{j}\ \mathbf{k}\| \cdot \mathrm{M} = \|\mathbf{1}\ \mathbf{E}_1\ \mathbf{E}_2\ \mathbf{E}_3\|$ y, por la Proposición 1.10, $\mathcal{O} = [\mathbf{1}, \mathbf{E}_1, \mathbf{E}_2, \mathbf{E}_3]$ es el orden buscado. La *salida* del algoritmo es el módulo $\mathcal{O}$ expresado en su base normal de Hermite.

Algoritmo 2.32. *Ordft*2 [f].

La *entrada* del algoritmo es una forma ternaria entera $f = (a_1, a_2, a_3, a_{23}, a_{13}, a_{12})$. Se calcula $d = d(f)$ y se trata de obtener un orden $\mathcal{O} \sim \mathcal{O}(f)$ contenido en $\mathcal{H} = \mathcal{H}(d) = \mathcal{H}(a, b)$.

Se calcula la matriz $M_1 = \mathrm{adj}\ \mathbf{M}(f)$ que, por la Proposición 2.10, es la matriz de la forma norma N_0 sobre $\mathcal{H}^0$ en la base $\{\mathbf{E}_1^*, \mathbf{E}_2^*, \mathbf{E}_3^*\}$ obtenida a partir de la base de Clifford $\{\mathbf{1}, \mathbf{E}_1, \mathbf{E}_2, \mathbf{E}_3\}$ de $\mathcal{O}(f)$. Por otra parte, la matriz de N_0 en la base $\{\mathbf{i}, \mathbf{j}, \mathbf{k}\}$ de $\mathcal{H}^0$ es $M_2 = \mathrm{diag}(-a, -b, ab)$, de modo que existe una matriz $M \in \mathbf{GL}(3, \mathbf{Q})$ tal que ${}^tM \cdot M_2 \cdot M = M_1$. Entonces, por la Proposición 1.10, $\|\mathbf{i}\ \mathbf{j}\ \mathbf{k}\| \cdot M = \|\mathbf{E}_1^*\ \mathbf{E}_2^*\ \mathbf{E}_3^*\|$ y, por el Lema 2.1, $\mathbf{E}_i = a_{jk} + \mathbf{E}_i^*$. Luego, $\mathcal{O} = [\mathbf{1}, \mathbf{E}_1, \mathbf{E}_2, \mathbf{E}_3]$ es el orden buscado. La *salida* del algoritmo es el módulo $\mathcal{O}$ expresado en su base normal de Hermite.

Algoritmo 2.33. *Ftord*1 [f].

Este algoritmo se basa en la demostración de la Proposición 2.14 que es constructiva. La *entrada* es un orden $\mathcal{O} = [\mathbf{1}, \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3] \subset \mathcal{H} = \mathcal{H}(d)$ y se trata de obtener una forma ternaria entera f tal que $\mathcal{O} \sim \mathcal{O}(f)$.

Se calculan los $\mathbf{u}_i^*$, los coeficientes $\pi^*(i, j, r)$ de (8) y con ellos la forma ternaria entera f. La *salida* del algoritmo es la forma f o su *reducida* si $\mathcal{H}$ es definido (ver Observación 2.36, más adelante). □

Algoritmo 2.34. *Ftord*2 [f].

La *entrada* del algoritmo es un orden $\mathcal{O} = [\mathbf{1}, \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3] \subset \mathcal{H} = \mathcal{H}(d)$ y se trata de obtener una forma ternaria entera g tal que $\mathcal{O} \sim \mathcal{O}(g)$.

Se calculan los $\mathbf{u}_i^*$ y con ellos la forma ternaria

$$f = f(x_1, x_2, x_3) = 4N(x_1\mathbf{u}_1^* + x_2\mathbf{u}_2^* + x_3\mathbf{u}_3^*)$$

que, por la Proposición 2.10 , es la adjunta de la forma g buscada. Entonces g se calcula a partir de f como indica la Proposición 1.31. La *salida* del algoritmo es la forma g o su *reducida* si $\mathcal{H}$ es definido (ver Observación 2.36, más adelante).

Para implementar los algoritmos anteriores es preciso disponer de al menos un par de *«paquetes»* de programas que permitan calcular con formas ternarias y en un álgebra de cuaterniones racionales.

Algoritmos 2.35. *Formas ternarias.*

Lo estrictamente necesario para implementar los algoritmos que dan la correspondencia Ψ: $\mathcal{F}_+ \to \Omega$ se reduce a lo siguiente:

1. Cambios de expresiones.

Una forma ternaria f puede expresarse de al menos tres maneras diferentes: mediante sus coeficientes $f = (a_1, a_2, a_3, a_{23}, a_{13}, a_{12})$, mediante su matriz $\mathbf{M}(f)$ y como polinomio $f = f(x_1, x_2, x_3)$ como en (1). En general resulta conveniente utilizar la primera de estas expresiones, pero es necesario tener algoritmos que permitan pasar de una expresión a otra. Así será sencillo, por ejemplo, implementar un algoritmo que calcule la forma ternaria $M \cdot f$ a partir de la matriz $M \in \mathbf{GL}(3, \mathbf{Q})$ y la forma ternaria f.

2. Cálculo de invariantes.

Algoritmos que calculen $\mathbf{D}(f)$, $\sigma(f)$, $\omega(f)$ y $d(f)$. Los tres primeros se obtienen directamente a partir de las definiciones y el último utilizando la Proposición 1.35 y la primera de las Observaciones 1.15. También resultará útil un algoritmo que determine si una forma ternaria entera es definida o indefinida aplicando el Corolario 1.36.

3. Cálculo de adjuntas y antiadjuntas

Sea f una forma ternaria entera. Para calcular ${}^af$ es suficiente utilizar la definición. Para determinar si f posee o no una antiadjunta y para calcular la antiadjunta de f se utiliza la Proposición 1.31.

Observación 2.36. *En el caso de formas ternarias enteras* definidas *es posible definir un representante canónico en cada clase de formas, al que se denomina* forma reducida *(ver* [4, p.155-179]). *Existe también un algoritmo* Reduce(f), *fácilmente implementable, para calcular la forma reducida $f_r \sim f$ (y, si fuera necesario, también la matriz $M \in \mathbf{GL}(3, \mathbf{Z})$ tal que $M \cdot f = f_r$). Por otra parte, la definición de forma reducida permite construir tablas de formas ternarias enteras definidas.*

La existencia de una buena definición de forma reducida y del algoritmo *Reduce*(f) *implica que, en el caso definido, sea más conveniente trabajar con formas ternarias enteras que con órdenes cuaterniónicos, dado que resulta mucho más fácil decidir la equivalencia de formas que la de órdenes.*

Algoritmos 2.37. *Cuaterniones.*

Un esquema de los algoritmos necesarios es el siguiente:

1. Operaciones con cuaterniones

Dada un álgebra de cuaterniones racionales $\mathcal{H} = \mathcal{H}(a, b)$, sus elementos se representan mediante sus coordenadas (x_0, x_1, x_2, x_3) en la base $B_c = \{\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ correspondiente y se implementan fácilmente algoritmos que realicen todas las operaciones básicas: suma, producto por un racional, producto no conmutativo, conjugación, cálculo de la traza y de la norma, componentes de un elemento en una base dada, automorfismo interior asociado a un elemento, etc.

2. Cálculo del álgebra $\mathcal{H}(d)$

Las Observaciones 1.15 permiten implementar algoritmos que calculen el invariante $d = d(\mathcal{H})$, correspondiente a un álgebra de cuaterniones $\mathcal{H} = \mathcal{H}(a, b)$, y definan el álgebra $H(d)$ a partir del invariante d.

3. Operaciones con módulos unitarios

Algoritmos que, dado un módulo unitario $L = [\mathbf{1}, \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3] \subset \mathcal{H}(d)$, calculen su discriminante $\mathbf{D}(L)$, den su base normal de Hermite, determinen si un elemento de $\mathcal{H}$ pertenece a L y si L es un orden. Con ellos no será difícil la implementación de otros que determinen si dos módulos unitarios son iguales o si uno es un submódulo de otro. También es conveniente poder calcular la intersección de dos módulos unitarios.

Observación 2.38. *Al tratar de implementar los algoritmos Ordft1[f] y Ordft2[f] se observa que es preciso disponer de otro algoritmo previo Mateq(F_1, F_2) que calcule una matriz $M \in \mathbf{GL}(n, \mathbf{Q})$ tal que $M \cdot F_1 = F_2$ cuando dos formas cuadráticas $\mathbf{Q}$-equivalentes F_1 y F_2 en n variables son dadas (al menos para $n = 3$ y $n = 4$).*

Tal vez éste sea el punto más delicado en la implementación de la correspondencia Ψ. En efecto, hasta donde alcanza nuestro conocimiento, actualmente no se dispone de un algoritmo Mateq(F_1, F_2) eficiente. Con Jordi Quer estamos trabajando en este sentido pero aún no hemos conseguido resultados plenamente satisfactorios. El algoritmo que utilizamos consta de dos pasos: 1) Se calculan formas diagonales $G_1 \sim F_1$ y $G_2 \sim F_2$ con las correspondientes matrices $M_1 = Mateq(F_1, G_1)$ y $M_2 = Mateq(F_2, G_2)$ (con lo que el problema queda reducido al caso de formas diagonales). 2) Se calcula $M_3 = Mateq(G_1, G_2)$ utilizando, esencialmente, el Teorema de Witt (que permite reducir el problema a uno equivalente con menor número de variables). Claramente, $Mateq(F_1, F_2) = M_1 \cdot M_3 \cdot M_2^{-1}$.

La necesidad de utilizar este procedimiento implica que el algoritmo Ordft2[f] es preferible al Ordft1[f].

Observación 2.39. *Es posible obtener un Ftord3[$\mathcal{O}$] utilizando los ajustes de Brandt* [3] y un *Ordft3[f] utilizando los resultados de Pall* [8]. *Cronológicamente, éstos son los primeros que hemos implementado. Naturalmente, las tres versiones de los algoritmos producen idénticos resultados.*

También es fácil de implementar un algoritmo que calcule la clase de formas ternarias $\mathcal{L}(\mathcal{O})$ que la correspondencia de Latimer asigna a la clase de un orden cuaterniónico maximal $\mathcal{O}$ dado.

3. EJEMPLOS

Los resultados establecidos en las secciones anteriores tienen diversas consecuencias y aplicaciones. La correspondencia Ψ y la posibilidad de su cálculo efectivo permiten utilizar la teoría de las formas enteras en el estudio de la aritmética de los órdenes cuaterniónicos, y recíprocamente. Por ejemplo, siguiendo el esquema utilizado para formas binarias, las escasas tablas de formas ternarias enteras de las que se dispone están calculadas a partir de $\mathbf{D}(f)$. En el caso de formas binarias, esto significa *agrupar* las formas vinculadas a un mismo orden cuadrático (que está determinado por su discriminante), pero la situación es muy diferente para formas ternarias. En efecto, existen formas ternarias enteras f y g tales que $\mathbf{D}(f) = \mathbf{D}(g)$ pero $d(f) \neq d(g)$. Un estudio más profundo de la correspondencia Ψ debe ayudar a encontrar el método más adecuado de disponer futuras tablas de formas ternarias enteras.

En las próximas secciones nos limitaremos a desarrollar ejemplos de la correspondencia y de algunas de sus posibles aplicaciones.

Nota: En todo lo que sigue, $\{\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ será la base del álgebra de cuaterniones racionales $\mathcal{H}(d)$ en la que estemos operando y, para aligerar la notación, para todo $q \in \mathbf{Q}$ denotaremos con q al elemento $q\mathbf{1}$ de $\mathcal{H}$(d).

3.1. Órdenes maximales

En esta sección daremos dos ejemplos de la correspondencia Ψ en el caso de órdenes cuaterniónicos $\mathcal{O} \subset \mathcal{H}$ maximales, es decir, con $\mathbf{D}(\mathcal{O}) = d(\mathcal{H})$ (Proposición 1.48). El primero con $\mathcal{H}$ indefinida y el segundo con $\mathcal{H}$ definida. También calcularemos las clases de formas asociadas por la correspondencia de Latimer a dichos órdenes.

Ejemplo 3.1. *Órdenes de discriminante* $\mathbf{D} = 6$.

En este primer ejemplo desarrollaremos con algún detalle el cálculo de la correspondencia en ambos sentidos. Estando en el caso indefinido, sabemos que existe una única clase de órdenes cuaterniónicos de discriminante $\mathbf{D} = 6$ (Corolario 2.27). Trabajaremos en el álgebra de cuaterniones $\mathcal{H} = \mathcal{H}(6) = \mathcal{H}(-1, 3)$.

Comencemos por determinar un orden maximal de $\mathcal{H}$. Si consideramos el orden $\mathcal{O}' = [\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}]$, observamos

que $\mathbf{D}(\mathcal{O}') = 12$, luego $\mathcal{O}'$ es un suborden de índice 2 de un orden maximal $\mathcal{O}$ (Corolarios 1.42 y 1.47). Observando que $\mathbf{u}_3 = (\mathbf{1} + \mathbf{i} + \mathbf{j} + \mathbf{k})/2$ es un entero, es fácil verificar que

$$\mathcal{O} = [\mathbf{1}, \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3] = [\mathbf{1}, \mathbf{i}, \mathbf{j}, (\mathbf{1} + \mathbf{i} + \mathbf{j} + \mathbf{k})/2]$$

es un orden maximal de $\mathcal{H}$ dado en su base normal de Hermite. Nos proponemos calcular $\Psi^{-1}(\overline{\mathcal{O}})$.

Sea $\mathcal{O}^* = [\mathbf{1}, \mathbf{u}_1^*, \mathbf{u}_2^*, \mathbf{u}_3^*]$ el módulo clásico asociado a $\mathcal{O}$. Calculando los productos $\mathbf{u}_i^*\mathbf{u}_j^*$ y expresándolos en la base de $\mathcal{O}^*$ tenemos:

$$\mathbf{u}_1^*\mathbf{u}_2^* = -\mathbf{u}_1^* - \mathbf{u}_2^* + 2\mathbf{u}_3^*$$
$$\mathbf{u}_3^*\mathbf{u}_1^* = -1/2 + 1/2\,\mathbf{u}_1^* + \mathbf{u}_2^* - \mathbf{u}_3^*$$
$$\mathbf{u}_2^*\mathbf{u}_3^* = 3/2 - \mathbf{u}_1^* + 1/2\,\mathbf{u}_2^* - \mathbf{u}_3^*.$$

Operando como en la demostración de la Proposición 2.14, obtenemos la forma

$$f = (1, -1, -2, 2, 2, -1),$$

con $\mathbf{D}(f) = 6$, y los ajustes de las trazas: $\mathbf{v}_1 = -\mathbf{u}_1 + 1$, $\mathbf{v}_2 = -\mathbf{u}_2 + 1$ y $\mathbf{v}_3 = -\mathbf{u}_3$ (en este caso $\varepsilon = -1$). Si calculamos la tabla de los productos de los $\mathbf{v}_i$ comprobamos que coincide con la que define el producto en $\mathcal{O}(f)^{op}$ (ver Observaciones 2.15). Tomando la base conjugada tenemos:

$$\mathcal{O} = [\mathbf{1}, \mathbf{1}+\mathbf{i}, \mathbf{1}+\mathbf{j}, (-\mathbf{1}+\mathbf{i}+\mathbf{j}+\mathbf{k})/2] \sim [\mathbf{1}, \mathbf{E}_1, \mathbf{E}_2, \mathbf{E}_3] = \mathcal{O}(f)$$

donde la equivalencia se obtiene aplicando una base en la otra. Luego, $\Psi^{-1}(\overline{\mathcal{O}}) = \overline{f}$.

Recíprocamente, si queremos hallar la clase de órdenes maximales de $\mathcal{H}$ a partir de una clase de formas ternarias, debemos encontrar una forma g con $\mathbf{D}(g) = 6$. Si inspeccionamos la tabla de Dickson (ver [4, p. 150-151]) debemos tener en cuenta que él trabaja sólo con formas clásicas. Siendo g no clásica (Corolario 2.18), en la tabla se encontrará la forma impropiamente primitiva $2g$ (ver Observación 2.24), de modo que $g = (-1, -1, 2, 0, 0, -1)$. Sea $G = {}^a g/4 = (-2, -2, 3/4, 0, 0, 2)$ la adjunta de g en sentido clásico y sean

$$M_1 = \begin{Vmatrix} 1 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{Vmatrix}, \quad M_2 = \begin{Vmatrix} 1 & -3/2 & -3/2 \\ 0 & 1/2 & -1/2 \\ 1 & -1 & -1 \end{Vmatrix}, \quad M = \begin{Vmatrix} -2 & 1 & 3/2 \\ -1 & 1 & 1/2 \\ -1 & 0 & 1/2 \end{Vmatrix}.$$

Entonces $M_1 \cdot G = G_1 = \mathrm{diag}(-2, -6, 3)$ y $M_2 \cdot G_1 = N_0 = \mathrm{diag}(1, -3, -3)$, la forma norma de $\mathcal{H}^0$ en la base $\{\mathbf{i}, \mathbf{j}, \mathbf{k}\}$. Aplicando la matriz $M = (M_1 \cdot M_2)^{-1}$ a $\|\mathbf{i}\ \mathbf{j}\ \mathbf{k}\|$ obtenemos $\|\mathbf{E}_1^*\ \mathbf{E}_2^*\ \mathbf{E}_3^*\|$, donde $\{\mathbf{1}, \mathbf{E}_1^*, \mathbf{E}_2^*, \mathbf{E}_3^*\}$ es la base de $\mathcal{O}(g)^*$. Como las trazas de los $\mathbf{E}_i$ están dadas por los tres últimos coeficientes de g (Lema 2.1), tenemos que

$$\mathcal{O}(g) = \mathcal{O}'' =$$
$$= [\mathbf{1}, -2\mathbf{i} - \mathbf{j} - \mathbf{k}, \mathbf{i} + \mathbf{j}, (-\mathbf{1} + 3\mathbf{i} + \mathbf{j} + \mathbf{k})/2] \subset \mathcal{H}.$$

Expresando a $\mathcal{O}''$ en su base normal de Hermite resulta que $\mathcal{O}'' = \mathcal{O}$.

Luego $\Psi(\overline{g}) = \overline{\mathcal{O}}$ y, necesariamente, $f \sim g$.

Por último, calculemos la clase $\mathcal{L}(\overline{\mathcal{O}})$ de formas ternarias asignada a $\overline{\mathcal{O}}$ por la correspondencia de Latimer. Es claro que $\{\mathbf{1}, (\mathbf{1} + \mathbf{i} + \mathbf{j} + \mathbf{k})/2, \mathbf{i}, \mathbf{j}\}$ es una base normal de $\mathcal{O}$. Luego $\mathcal{O}^0 = [\mathbf{i} + \mathbf{j} + \mathbf{k}, \mathbf{i}, \mathbf{j}] = [\mathbf{i}, \mathbf{j}, \mathbf{k}]$ y $\mathcal{L}(\overline{\mathcal{O}}) = \overline{N}_0$.

Ejemplo 3.4. *Órdenes de discriminante* $\mathbf{D} = 11$.

Se trata de determinar los órdenes maximales de $\mathcal{H} = \mathcal{H}(11) = \mathcal{H}(-1, -11)$. Hemos elegido este discriminante por tratarse del menor d para el que $\mathcal{H}(d)$ posee más de un orden maximal.

Siendo $\mathcal{H}$ definida, hemos visto (Observación 2.36) que es más conveniente trabajar con formas ternarias. En este caso, la inspección de una tabla o el cálculo directo nos muestra que existen dos clases de formas ternarias con $\mathbf{D} = 11$. Las formas reducidas correspondientes son:

$$(11) \quad f_1 = (1, 1, 3, 0, -1, 0) \quad \text{y} \quad f_2 = (1, 1, 4, 1, 1, 1).$$

En consecuencia, $\mathcal{H}$ posee dos órdenes maximales que, expresados en sus bases normales de Hermite son:

$$\mathcal{O}_1 = [\mathbf{1}, 3\mathbf{i}, (13\mathbf{i} + \mathbf{j})/6, (\mathbf{1} + \mathbf{k})/2] \quad \text{y}$$
$$(12) \quad \mathcal{O}_2 = [\mathbf{1}, 12\mathbf{i}, (6 + 103\mathbf{i} + \mathbf{j})/12, (211\mathbf{i} + \mathbf{j} + 6\mathbf{k})/24]$$

y $\Omega_m(11) = \{\overline{\mathcal{O}_1}, \overline{\mathcal{O}_2}\}$.

En cuanto a la correspondencia de Latimer, formas definidas por (10) y correspondientes a $\mathcal{O}_1$ y a $\mathcal{O}_2$ son, respectivamente

$$\ell_1' = (11, 9, 5, 13, 0, 0) \quad \text{y}$$
$$\ell_2' = (295, 144, 78, 211, 302, 412),$$

que son equivalentes a las formas reducidas

$$\ell_1 = (1, 3, 11, 0, 0, -1) \quad \text{y} \quad \ell_2 = (3, 4, 4, -3, -2, -2).$$

Estas resultan ser las únicas clases de formas ternarias primitivas de discriminante $\mathbf{D} = 121$, y ambas están en el mismo género. En rigor, siendo d impar, $\mathcal{L}(\overline{\mathcal{O}_1}) = \overline{2\ell_1}$ y $\mathcal{L}(\overline{\mathcal{O}_2}) = \overline{2\ell_2}$ (ver Observación 2.24).

3.2. Determinación de subórdenes

Dado un orden cuaterniónico $\mathcal{O}$, denotaremos $\mathcal{O}(m, n)$ a sus subórdenes, donde m es el índice del suborden y $n > 0$ es un entero que distingue a los distintos subórdenes

de $\mathcal{O}$ de índice m. En esta sección nos proponemos determinar los subórdenes de índices $m = 2$ y 3 de los órdenes maximales $\mathcal{O}_1$ y $\mathcal{O}_2$ dados en (12).

En general, para determinar los subórdenes de índice m de un orden cuaterniónico $\mathcal{O} = [\mathbf{1}, \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3]$ con $\mathbf{D}(\mathcal{O}) = \mathrm{D}$ puede procederse en dos pasos: 1) se determinan todos los submódulos unitarios L de $\mathcal{O}$ de índice m; 2) se seleccionan aquellos submódulos unitarios L que sean órdenes.

En el Paso 1, deberían aplicarse a $\|\mathbf{u}_1\ \mathbf{u}_2\ \mathbf{u}_3\|$ todas las matrices $M \in \mathbf{M}(3,\mathbf{Z})$, con $\det M = m$. Sin embargo, si dos de tales matrices M_1 y M_2 son *equivalentes a derecha* (esto es: existe una $U \in \mathbf{GL}(3, \mathbf{Z})$ tal que $M_1 = M_2 \cdot U$), entonces determinan el mismo L. Hermite [6] obtiene representantes canónicos para las clases de matrices U equivalentes a derecha. En el caso $m = p \in \mathcal{P}$ primo, éstos son (ver [8, p. 309]) las $p^2 + p + 1$ matrices:

$$(13)\quad \begin{Vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & p \end{Vmatrix}, \quad \begin{Vmatrix} 1 & 0 & 0 \\ 0 & p & a \\ 0 & 0 & 1 \end{Vmatrix} \quad \text{y} \quad \begin{Vmatrix} p & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{Vmatrix},$$

con $a, b = 0, 1, \ldots, p - 1$.

Por otra parte, los subórdenes de índice m del orden cuaterniónico $\mathcal{O}$ también pueden estudiarse a partir de una forma ternaria f tal que $\Psi(f) = \overline{\mathcal{O}}$ utilizando la Proposición 2.19. En el caso $m = p \in \mathcal{P}$ primo, habrá que aplicar las matrices de (13) a la forma ${}^{a}f$ para hallar las formas ternarias que derivan de f.

Ejemplo 3.2. *Subórdenes de índice $m = 2$.*

Calculemos, en primer lugar, las clases de órdenes con $\mathbf{D} = 22$. Para ello observamos que existen tres clases de formas ternarias enteras con $\mathbf{D} = 22$, de las cuales sólo dos tienen invariante $d = 11$. (La tercera tiene invariante $d = 2$ y se corresponde con la clase del suborden de índice $m = 11$ de la clase de órdenes maximales con $\mathbf{D} = 2$; la forma reducida correspondiente es $g_3 = (1, 2, 3, 0, -1, 0)$.) Las formas reducidas correspondientes son:

$$g_1 = (1, 1, 6, -1, -1, 0) \quad \text{y} \quad g_2 = (2, 2, 2, 1, 1, 2).$$

Las dos clases de órdenes con $\mathbf{D} = 22$ son, por lo tanto, las clases de

$$\mathcal{O}(g_1) = [\mathbf{1}, 276\mathbf{i}, (46 + 5529\mathbf{i} + \mathbf{j})/92, (3 + 230\mathbf{i} + \mathbf{k})/6] \quad \text{y}$$

$$(14)\quad \mathcal{O}(g_2) = [\mathbf{1}, 12\mathbf{i}, (6 + 103\mathbf{i} + \mathbf{j})/12, (1 + 18\mathbf{i} + \mathbf{k})/2].$$

Las formas reducidas correspondientes a las clases de las formas adjuntas de f_1 y f_2 de (11) son

$$(15)\quad \begin{aligned} F_1 &= (4, 11, 12, 0, -4, 0) \quad \text{y} \\ F_2 &= (3, 15, 15, -14, -2, -2). \end{aligned}$$

Aplicando las siete matrices de (13) con $p = 2$ a estas formas se obtiene, en ambos casos, que sólo tres dan formas ternarias enteras que poseen antiadjunta. Para F_1, una de dichas antiadjuntas es equivalente a g_1 y las otras dos son equivalentes a g_2. Para F_2, las tres antiadjuntas son equivalentes a g_2. Así pues, la manera en que g_1 y g_2 derivan de f_1 y f_2 queda representada por el grafo siguiente:

$$(g.1)\quad \begin{array}{ccc} & \xrightarrow{1} & g_1 \\ f_1 & & \\ & \xrightarrow{2} & \\ & \xrightarrow{3} & g_2 \\ f_2 & & \end{array}$$

De lo anterior podemos concluir que se verifican las siguientes relaciones de inclusión en sentido amplio:

$$(16)\quad \overline{\mathcal{O}(g_1)} \prec \overline{\mathcal{O}_1}, \quad \overline{\mathcal{O}(g_2)} \prec \overline{\mathcal{O}_1} \quad \text{y} \quad \overline{\mathcal{O}(g_2)} \prec \overline{\mathcal{O}_2}.$$

Calculando los subórdenes de índice $m = 2$ de $\mathcal{O}_1$ y $\mathcal{O}_2$ dados en (12) con el procedimiento descrito al comienzo de esta sección se obtienen:

$$\mathcal{O}_1(2, 1) = [\mathbf{1}, 3\mathbf{i}, (4\mathbf{i} + \mathbf{j})/3, (3 + 13\mathbf{i} + \mathbf{j} + 3\mathbf{k})/6]$$

$$\mathcal{O}_1(2, 2) = [\mathbf{1}, 6\mathbf{i}, (13\mathbf{i} + \mathbf{j})/6, (1 + 6\mathbf{i} + \mathbf{k})/2]$$

$$\mathcal{O}_1(2, 3) = [\mathbf{1}, 6\mathbf{i}, (31\mathbf{i} + \mathbf{j})/6, (1 + 6\mathbf{i} + \mathbf{k})/2]$$

$$\mathcal{O}_2(2, 1) = [\mathbf{1}, 12\mathbf{i}, (6 + 103\mathbf{i} + \mathbf{j})/12, (1 + 18\mathbf{i} + \mathbf{k})/2]$$

$$\mathcal{O}_2(2, 2) = [\mathbf{1}, 24\mathbf{i}, (6 + 103\mathbf{i} + \mathbf{j})/12, (499\mathbf{i} + \mathbf{j} + 6\mathbf{k})/24]$$

$$\mathcal{O}_2(2, 3) = [\mathbf{1}, 24\mathbf{i}, (6 + 247\mathbf{i} + \mathbf{j})/12, (211\mathbf{i} + \mathbf{j} + 6\mathbf{k})/24].$$

Calculando, para cada uno, la forma reducida correspondiente por Ψ se observa que $\mathcal{O}_1(2, 3) \sim \mathcal{O}(g_1)$ y los otros cinco son equivalentes a $\mathcal{O}(g_2)$. Luego, la manera en que están dadas las inclusiones de (16) queda representada por un grafo similar a (*g*.1).

Ejemplo 3.3. *Subórdenes de índice $m = 3$.*

Procedemos igual que en el ejemplo anterior. Existen tres clases de formas ternarias enteras con $\mathbf{D} = 33$ y $d = 11$. Las formas reducidas correspondientes son:

$$h_1 = (1, 1, 11, 0, 0, -1), \quad h_2 = (1, 3, 3, 0, 0, -1) \quad \text{y}$$

$$h_3 = (2, 2, 3, 2, 2, 1).$$

Luego, las tres clases de órdenes cuaterniónicos con $\mathbf{D} = 33$ son las clases de

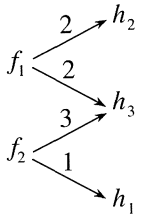
$$\mathcal{O}(h_1) = [\mathbf{1}, 6\mathbf{i}, (1 + 6\mathbf{i} + \mathbf{j})/2, (2 + 23\mathbf{i} + \mathbf{k})/4]$$

$$(17)\quad \mathcal{O}(h_2) = [\mathbf{1}, 3\mathbf{i}, (\mathbf{i} + \mathbf{j})/2, (1 + \mathbf{k})/2] \quad \text{y}$$

$$\mathcal{O}(h_3) = [\mathbf{1}, 45\mathbf{i}, (1283\mathbf{i} + \mathbf{j})/30, (1 + 60\mathbf{i} + \mathbf{k})/2].$$

Aplicando las trece matrices de (13) con $p = 3$ a las formas F_1 y F_2 de (15) se obtiene, en ambos casos, que sólo cuatro dan formas ternarias enteras que poseen antiadjunta. Para F_1, dos de dichas antiadjuntas son equivalentes a h_2 y las otras dos son equivalentes a h_3. Para F_2, una de las antiadjuntas es equivalente a h_1 y las otras tres son equivalentes a h_3. Luego, la manera en que h_1, h_2 y h_3 derivan de f_1 y f_2 queda representada por el grafo siguiente:

(*g*.2)



En este caso podemos concluir que se verifican las siguientes relaciones de inclusión en sentido amplio:

(18) $\overline{\mathcal{O}(h_1)} \prec \overline{\mathcal{O}_2}$, $\overline{\mathcal{O}(h_2)} \prec \overline{\mathcal{O}_1}$, $\overline{\mathcal{O}(h_3)} \prec \overline{\mathcal{O}_1}$ y $\overline{\mathcal{O}(h_3)} \prec \overline{\mathcal{O}_2}$.

Calculando los subórdenes de índice $m = 3$ de $\mathcal{O}_1$ y $\mathcal{O}_2$ dados en (12), con el procedimiento conocido, se verifica que la manera en que están dadas las inclusiones de (18) queda representada por un grafo similar a (*g*.2).

3.3. Órdenes de Eichler

Es claro que la propiedad de un orden de ser *de Eichler* (ver Definición 1.40) se extiende a clases de órdenes cuaterniónicos. Sea $\mathcal{O}$ un orden cuaterniónico con $d(\mathcal{O}) = d$ y sean $\overline{\mathcal{O}_u}$ y $\overline{\mathcal{O}_v}$ elementos (no necesariamente distintos) de $\Omega_m(d)$. Denotaremos $\overline{\mathcal{O}} = \mathcal{E}(\overline{\mathcal{O}_u}, \overline{\mathcal{O}_v})$ para indicar que $\overline{\mathcal{O}}$ es de Eichler y que $\mathcal{O}$ se obtiene como intersección de órdenes equivalentes a $\mathcal{O}_u$ y a $\mathcal{O}_v$. En esta sección nos proponemos mostrar que las clases de órdenes halladas en los ejemplos 3.3 y 3.4 son de Eichler, expresándolas en la forma $\mathcal{CE}(\overline{\mathcal{O}_u}, \overline{\mathcal{O}_v})$ con $\overline{\mathcal{O}_u}$ y $\overline{\mathcal{O}_v}$ pertenecientes al conjunto $\Omega_m(11)$ determinado en el Ejemplo 3.2.

Ejemplo 3.4. *Ordenes de Eichler de* $\mathbf{D} = 22$.

Como hemos visto, las clases de órdenes de $\mathbf{D} = 22$ son las clases de $\mathcal{O}(g_1)$ y $\mathcal{O}(g_2)$ dados en (14). Teniendo en cuenta (16), si $\overline{\mathcal{O}(g_1)}$ es de Eichler sólo podrá expresarse en la forma $\mathcal{E}(\overline{\mathcal{O}_1}, \overline{\mathcal{O}_1})$. Es natural considerar el submódulo $\mathcal{O}_1(2, 3) \sim \mathcal{O}(g_1)$ de $\mathcal{O}_1$ (ver Ejemplo 3.3). Para todo $\mathbf{u} \in \mathcal{O}_1(2, 3)$, el automorfismo $\lambda_\mathbf{u}$ de $\mathcal{O}_1$ deja invariante a $\mathcal{O}_1(2, 3)$ y tomando $\mathbf{u} = (6 + 5\mathbf{i} - \mathbf{j})/6$, con $N(\mathbf{u}) = 2$, se obtiene que $\mathcal{O}_1(2, 3) = \mathcal{O}_1 \cap \lambda_\mathbf{u}(\mathcal{O}_1)$. Luego, $\overline{\mathcal{O}(g_1)} = \mathcal{E}(\overline{\mathcal{O}_1}, \overline{\mathcal{O}_1})$.

Si $\overline{\mathcal{O}(g_2)}$ es de Eichler, según (16) podría expresarse en cualquiera de las formas $\mathcal{E}(\overline{\mathcal{O}_1}, \overline{\mathcal{O}_1})$, $\mathcal{E}(\overline{\mathcal{O}_1}, \overline{\mathcal{O}_2})$ y $\mathcal{E}(\overline{\mathcal{O}_2}, \overline{\mathcal{O}_2})$. Una búsqueda similar a la realizada para $\mathcal{O}(g_1)$ no es posible pues $\mathcal{O}(g_2)$ no posee elementos de norma 2. Calculando

$$\mathcal{O}' = \mathcal{O}_1 \cap \mathcal{O}_2 = [\mathbf{1}, 12\mathbf{i}, (13\mathbf{i} + \mathbf{j})/6, (1 + 18\mathbf{i} + \mathbf{k})/2],$$

se obtiene que $\mathbf{D}(\mathcal{O}') = 44$. Luego, por el Corolario 1.47, $[\mathcal{O}_1 : \mathcal{O}'] = [\mathcal{O}_2 : \mathcal{O}'] = 4$. Tomando $\mathbf{v} = (\mathbf{1} + \mathbf{k})/2 \in \mathcal{O}_1$, con $N(\mathbf{v}) = 3$, y $\mathbf{w} = (3 - 8\mathbf{i} - 2\mathbf{j} + 3\mathbf{k})/6 \in \mathcal{O}'$, con $N(\mathbf{w}) = 6$, se obtiene que $\mathcal{O}(g_2) \sim \lambda_\mathbf{v}(\mathcal{O}_1) \cap \lambda_\mathbf{w}(\mathcal{O}_2)$. Luego, $\overline{\mathcal{O}(g_2)} = \mathcal{E}(\overline{\mathcal{O}_1}, \overline{\mathcal{O}_2})$.

Ejemplo 3.5. *Órdenes de Eichler de* $\mathbf{D} = 33$.

Las clases de órdenes de $\mathbf{D} = 33$ son las clases de $\mathcal{O}(h_1)$, $\mathcal{O}(h_2)$ y $\mathcal{O}(h_3)$ dados en (17). Teniendo en cuenta (18), para las dos primeras razonamos como en el ejemplo anterior para el caso de $\mathcal{O}(g_1)$. Tomando $\mathbf{x} = (36 - 5\mathbf{i} + \mathbf{j} - 6\mathbf{k})/24$, con $N(\mathbf{x}) = 3$, en el único suborden de $\mathcal{O}_2$ equivalente a $\mathcal{O}(h_1)$, se tiene que $\mathcal{O}(h_1) \sim \mathcal{O}_2 \cap \lambda_\mathbf{x}(\mathcal{O}_2)$. Luego, $\overline{\mathcal{O}(h_1)} = \mathcal{E}(\overline{\mathcal{O}_2}, \overline{\mathcal{O}_2})$.

Por otra parte, el elemento $\mathbf{v}$ del ejemplo anterior pertenece a uno de los dos subórdenes de $\mathcal{O}_1$ equivalentes a $\mathcal{O}(h_2)$. Resulta que $\lambda_\mathbf{x}$ transforma uno de estos subórdenes en el otro y $\mathcal{O}(h_2) \sim \mathcal{O}_1 \cap \lambda_\mathbf{v}(\mathcal{O}_1)$. Luego, $\overline{\mathcal{O}(h_2)} = \mathcal{E}(\overline{\mathcal{O}_1}, \overline{\mathcal{O}_1})$.

Finalmente, $\mathcal{O}(h_3) \sim \lambda_\mathbf{w}(\mathcal{O}_1) \cap \lambda_\mathbf{u}(\mathcal{O}_2)$, donde $\mathbf{u}$ y $\mathbf{w}$ son los elementos del ejemplo anterior. Luego, $\overline{\mathcal{O}(h_3)} = \mathcal{E}(\overline{\mathcal{O}_1}, \overline{\mathcal{O}_2})$.

Observación 3.6. *En ambos ejemplos, las relaciones de inclusión en sentido amplio, deducidas del grafo que representa la manera en que las clases de formas ternarias del discriminante considerado derivan de las clases de formas fundamentales, determina la expresión de una clase de órdenes de Eichler como intersección de clases de órdenes maximales.*

REFERENCIAS

1. H. Brandt (1924), *Der Kompositionsbegriff bei den quaternären quadratischen Formen,* Math. Ann. **91**, 300-315.
2. H. Brandt (1928), *Idealtheorie in Quaternionenalgebren,* Math. Ann. **99**, 1-29.
3. H. Brandt (1943), *Zur Zahlentheorie der Quaternionen,* Jber. Deutsch. Math.-Verein. **53**, 23-57.
4. L. E. Dickson (1930), *Studies in the theory of numbers,* The University of Chicago Press, Chicago.
5. R. Fueter (1935), *Zur Theorie Brandtschen Quaternionenalgebren,* Math. Ann. **110**, 650-661.
6. C. Hermite (1854), *Sur la théorie des formes quadratiques,* Journal für Mathematik **47**, 307-342.
7. C. G. Latimer (1937), *The classes of integral sets in a quaternion algebra,* Duke Math. J. **3**, 237-247.
8. G. Pall (1946), *On generalized quaternions,* Trans. Amer. Math. Soc. **59**, 280-332.
9. M. F. Vignéras (1980), *Arithmétique des Algèbres de Quaternions,* **LNM**, **800**, Springer.