UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

FORMAS CUADRATICAS BINARIAS Y EL GRUPO DE CLASES DE IDEALES

T E S I S

QUE PARA OBTENER EL TITULO DE

M A T E M A T I C O

P R E S E N T A :

GUSTAVO ORTIZ GONZALEZ

DIRECTOR DE TESIS: M. en C. MARIO PINEDA RUELAS

1997

VNIVERSIDAD NACIONAL
AVPNOMA DE
MEXICO

M. en C. Virginia Abrín Batule
Jefe de la División de Estudios Profesionales de la
Facultad de Ciencias
P r e s e n t e

Comunicamos a usted que hemos revisado el trabajo de Tesis:

"FORMAS CUADRATICAS BINARIAS Y EL GRUPO DE CLASES DE IDEALES"

realizado por GUSTAVO ORTIZ GONZALEZ

con número de cuenta 7328427-9 **, pasante de la carrera de** MATEMATICAS

Dicho trabajo cuenta con nuestro voto aprobatorio.

Atentamente

Director de Tesis **Propietario**	M. EN C. MARIO PINEDA RUELAS	
Propietario	DR. FELIPE DE JESUS ZALDIVAR CRUZ	
Propietario	DR. HUGO ALBERTO RINCON MEJIA	Hugo A. Rincón M.
Suplente	DR. JUAN MORALES RODRIGUEZ	
Suplente	DRA. BERTHA MARIA TOME ARREOLA	

Consejo Departamental de Matemáticas

DR. MANUEL FALCONI MAGAÑA

A mi esposa

ROCIO

y a mis hijos

GUSTAVO Y RODRIGO

Por el sacrificio del tiempo no dedicado a ellos.

A mis padres

MARINO Y ROSALIA

Por haberme dado la vida.

A mis hermanos

Cesar, Sergio, Teresa, Marina,
Jesús, Rafael, Gabriel, Germán,
Guadalupe, Martín y José Antonio

Por ser todos para uno.

A la familia

Rivera Hernández

Por su apoyo.

Introducción

El primer paso en el estudio de las formas cuadráticas fué probablemente el teorema de Fermat.

Un primo p es representable de manera única por la forma $f(x,y) = x^2 + y^2$ *si y sólo si* $p \equiv 1 \pmod 4$ *ó* $p = 2$.

De manera más general Fermat estudió la ecuación $x^2 + y^2 = m$, donde m no necesariamente es un número primo.

En los años que siguieron hasta 1800, Euler, Lagrange, Legendre y otros obtuvieron resultados análogos para una variedad de formas cuadráticas. Fué Gauss sin duda en su obra maestra "*Disquisitiones Arithmeticae*", el primero en dar una exposición coherente de la teoría de las formas cuadráticas binarias. Durante el siglo XIX, mientras se desarrollaba la teoría de ideales y números algebraicos, se vió que la teoría de formas cuadráticas binarias era sólo un caso especial de esas teorías más abstractas.

Las formas cuadráticas binarias tienen un atractivo (entre otros): éstas forman parte del caso cuadrático en la teoría de números algebraicos y los teoremas pueden probarse independientemente usando métodos elementales.

El objetivo de este trabajo es establecer una correspondencia entre dos grupos. Uno de ellos se construye introduciendo una relación de equivalencia en la clase de las formas cuadraticas binarias de discriminante Δ negativo fijo. El otro grupo es el grupo de clases de ideales de una extensión cuadrática imaginaria de discriminante Δ.

El primer capítulo está dedicado por supuesto, al estudio de las formas cuadráticas binarias de discriminante negativo Δ. Establecemos una relación de equivalencia en dicho conjunto y damos un algoritmo de composición de

formas cuadráticas binarias de discriminante Δ. De manera que el conjunto de clases de formas tiene estructura de grupo. El capítulo II lo dedicamos al estudio del grupo de clases de ideales de un campo cuadrático imaginario. En el capítulo III establecemos la correspondencia que existe entre el grupo de clases de formas cuadráticas binarias de discriminante Δ y el grupo de clases de ideales de de un campo cuadrático imaginario de discriminante Δ.

Quiero dar mi más sincero agradecimiento al M. en C. Mario Pineda Ruelas por su desinteresada ayuda, sus consejos y parte de su valioso tiempo dedicado a la dirección este trabajo.

Finalmente quiero dar mi gratitud al M. en C. Fernando Vallejo Aguirre y al M. en C. Armando Reyes Rodríguez, por sus acertados comentarios respecto a esta tesis y al M. en C. Pablo Mendoza Iturralde por haberme motivado a la realización de este trabajo.

CONTENIDO

CAPITULO I

FORMAS CUADRATICAS BINARIAS

CONCEPTOS BASICOS

Sea $\boldsymbol{K}[x_1,\ldots,x_n]$ el anillo de polinomios en las indeterminadas $x_1,\ldots,x_n$ con coeficientes en $\boldsymbol{K}$, donde $\boldsymbol{K}$ es un anillo con elemento unitario. Se define una **forma** como un polinomio $f(x_1,\ldots,x_n)\in \boldsymbol{K}[x_1,\ldots,x_n]$ donde todos los términos son del mismo grado. Las formas se clasifican de acuerdo al número de variables como binarias, ternarias,...,etc., y de acuerdo a su grado en las variables como lineales, cuadráticas, cúbicas,...,etc. Denotemos como $F^r\boldsymbol{K}[x_1,\ldots,x_n]$ al conjunto de formas de grado r. El conjunto que nos interesa es $F^2\boldsymbol{K}[x_1,\ldots,x_n]$ y como dijimos antes, este conjunto lo llamaremos, el conjunto de las **formas cuadráticas** con coeficientes en $\boldsymbol{K}$, de manera que si $f(x_1,\ldots,x_n)\in F^2\boldsymbol{K}[x_1,\ldots,x_n]$, entonces

$$f(x_1,\ldots,x_n)=\sum_{i,j=1}^{n} a_{ij}x_ix_j,$$

con $a_{ij}\in \boldsymbol{K}$. De ahora en adelante sólo consideramos $\boldsymbol{K}=\mathbf{Z}$.

Una forma $f(x_1,\ldots,x_n)$ se dice que es **definida positiva** o simplemente **positiva** si $f(d_1,\ldots,d_n) > 0$, para $(d_1,\ldots,d_n)\in \mathbf{Z}^n - \{0\}$. De modo semejante se dice que una forma es **definida negativa** o simplemente **negativa** si $f(d_1,\ldots,d_n) < 0$, con $(d_1,\ldots,d_n)\in \mathbf{Z}^n - \{0\}$. Es claro, por ejemplo, que $f(x,y,z) = 3x^2 + 2y^2 + 4z^2$ es positiva y que $g(x,y,z) = -4x^4 - 2y^4 - x^2y^2 - y^2z^2 - z^4$ es negativa, mientras que $h(x,y) = x^2 - y^2$ no es ni positiva ni negativa. A una forma que no es ni positiva ni negativa se le llama forma **indefinida**. Notemos que si $f(x_1,\ldots,x_n)$ es positiva, entonces $-f(x_1,\ldots,x_n)$ es negativa y viceversa. De aquí que no es necesario estudiar por separado las formas positivas y las negativas, ya que las propiedades de las de un tipo se deducen de las propiedades de las otras. De hecho todo este trabajo es dedicado al estudio de las formas cuadráticas positivas.

Consideremos la forma $f(x_1,\ldots,x_n)\in F^2\mathbf{Z}[x_1,\ldots,x_n]$. Diremos que dicha forma representa a $m\in \mathbf{Z}$ si existe $(b_1,\ldots,b_n)\in \mathbf{Z}^n$ tal que $f(b_1,\ldots,b_n) = m$. Por ejemplo, la forma $f(x,y) = x^2 + y^2$ representa a 5, pero no a 6; ya que las parejas $(\pm1,\pm2)$ y

$(\pm 2,\pm 1)$ en $\mathbf{Z}^2$ son tales que $f(\pm 1,\pm 2) = f(\pm 2,\pm 1) = 5$ y se puede demostrar fácilmente que la ecuación $x^2 + y^2 = 6$ no es soluble en $\mathbf{Z}$. Es obvio que toda forma cuadrática representa a cero. Si una forma $f(x_1,\ldots,x_n)\in F^2\mathbf{Z}[x_1,\ldots,x_n]$ es tal que $f(b_1,\ldots,b_n) = 0$ para algún $(b_1,\ldots,b_n)\in \mathbf{Z}^n - \{0\}$, entonces a dicha forma se le llama **la forma cero**. De esto se deduce que las formas definidas (positivas y negativas), no son formas cero. En lo que sigue sólo trataremos con formas **cuadráticas binarias**.

Sea $f(x,y) = ax^2+bxy+cy^2\in F^2\mathbf{Z}[x,y]$. Asociamos a f el número

$$\Delta_f = b^2 - 4ac \tag{1.1}$$

y lo llamaremos el **discriminante** de la forma. Notemos que $\Delta_f \equiv 0$ ó $1 \pmod 4$ ya que $\Delta_f \equiv b^2 \pmod 4$.

Una forma $f(x,y)\in F^2\mathbf{Z}[x,y]$ se dice que es **primitiva** si $mcd(a,b,c) = 1$, y **derivada** si $mcd(a,b,c) = d > 1$. Como dijimos antes, $f(x,y)\in F^2\mathbf{Z}[x,y]$ representa a $m\in\mathbf{Z}$ si existe $(x_0,y_0)\in\mathbf{Z}^2$ tal que $f(x_0,y_0)=ax_0^2+bx_0y_0+cy_0^2 = m$. Dicha representación es **primitiva** si $mcd(x_0,y_0)=1$.
Si $mcd(x_0,y_0)=d>1$, entonces $d^2 \mid m$, y de $x_0=dx'$ y $y_0=dy'$ se sigue

$$m=f(x_0,y_0)=ax_0^2+bx_0y_0+cy_0^2 = ad^2x'^2+bd^2x'y'+cd^2y'^2$$

y así $f(x',y')$ es una representación primitiva de $\frac{m}{d^2}$. Por lo tanto, existen números que son primitivamente representados por $f(x,y)$. Usaremos la palabra "representado" entendiendo que es primitivamente representado, a menos que se diga otra cosa.

Para una discusión más adecuada, veamos como podemos expresar $f(x,y)\in F^2\mathbf{Z}[x,y]$ en términos matriciales. Es una tarea bastante fácil verificar que si $f(x,y) = ax^2 + bxy + cy^2$, entonces

$$f(x,y) = (x,y)\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}. \tag{1.2}$$

Si $x = \begin{pmatrix} x \\ y \end{pmatrix}$ y $B_f = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$, entonces $f(x) = x^t B_f x$, donde x^t es el transpuesto del vector x. A la matriz B_f comunmente se le llama la **matriz asociada** a $f(x,y)$. Notemos que B_f es simétrica. Por otro lado, si consideramos el determinante de B_f tenemos que $det\, B_f = ac - \frac{b^2}{4}$, pero $\Delta_f = b^2 - 4ac$ así que

$$\Delta_f = -4 det\, B_f. \tag{1.3}$$

Las propiedades de $f(x,y) \in F^2\mathbf{Z}[x,y]$ están íntimamente relacionadas con el valor de su discriminante (en su defecto al determinante de la matriz asociada a la forma en cuestión). El siguiente resultado nos proporciona una caracterización de las formas cuadráticas binarias positivas.

Teorema 1.1. *$f(x,y) = ax^2+bxy+cy^2 \in F^2\mathbf{Z}[x,y]$ es positiva si y sólo si $det\, B_f > 0$, $a > 0$ y $c > 0$.*

Demostración. Si $f(x,y) = ax^2+bxy+cy^2 \in F^2\mathbf{Z}[x,y]$ es positiva, entonces $f(x,y) > 0$ para todo $(x,y) \in \mathbf{Z}^2 - \{0\}$, entonces en particular $f(1,0) = a > 0$ y $f(0,1) = c > 0$. Ahora tendremos que probar que $det\, B_f > 0$. Para esto notemos que

$$\begin{aligned} f(x,y) &= ax^2 + bxy + cy^2 \\ &= \frac{1}{4a}\left[(2ax + by)^2 + (4ac - b^2)y^2\right] \\ &= \frac{1}{4a}\left[(2ax + by)^2 + (4\, det\, B_f)y^2\right]. \end{aligned} \tag{1.4}$$

Así que $f(-b,2a) = 4a(det\, B_f)$. Dado que f es positiva y $a > 0$, se sigue por lo tanto que $det\, B_f > 0$.

Para probar la inversa, supongamos que $det\, B_f > 0$, $a > 0$ y $c > 0$, entonces de la igualdad en (1.4) se sigue inmediatamente que $f(x,y) > 0$. ■

Observemos que $f(x,y)$ es negativa si y sólo si $det\, B_f > 0$, $a < 0$ y $c < 0$. De modo que las formas definidas están caracterizadas por $det\, B_f > 0$ y $ac > 0$ ó $\Delta_f < 0$ y $ac > 0$.

Corolario 1.2. *La forma* $f(x,y) = ax^2+bxy+cy^2 \in F^2\mathbf{Z}[x,y]$ *es indefinida si y sólo si* $det\ B_f \leq 0$.

Demostración. De (1.3) y (1.4) tenemos

$$f(x,y) = \frac{1}{4a}\left[(2ax+by)^2 - \Delta_f y^2\right]. \tag{1.5}$$

Ahora bien, está claro que tenemos que eliminar la posibilidad $\Delta_f < 0$ y $ac \leq 0$. Para que $f(x,y) < 0$ se debe de tener $a < 0$, puesto que $\Delta_f < 0$. Pero $\Delta_f = b^2 - 4ac$ así que $b^2 < 4ac$ y por lo tanto $ac > 0$. Así que si $f(x,y)$ es indefinida, entonces $\Delta_f \geq 0$ o bien $det\ B_f \leq 0$.

Recíprocamente, supongamos $det\ B_f \leq 0$. Entonces $\Delta_f \geq 0$ y de (1.5) se sigue que $f(x,y)$ es indefinida. puesto que para cualquier $a \neq 0$ el valor de $f(x,y)$ en (1.5) en algunas ocasiones es positivo, y en otras negativo; dependiendo de los valores que tomen x y y. ■

Hasta ahora no hemos dicho nada acerca de la posibilidad de que $det\ B_f = 0$. Pues bien, si este fuera el caso, de (1.1) y (1.3) se tiene $b^2 = 4ac$. De manera que $b = \pm 2\sqrt{ac} \in \mathbf{Z}$ y b es par. Resumiendo: a y c son cuadrados perfectos ó $c = k^2a$ para alguna $k \in \mathbf{Z}$. Si a y c son cuadrados perfectos existen r, $s \in \mathbf{Z}$ tal que $a = r^2$, $c = s^2$. Así

$$f(x,y) = r^2x^2 \pm 2rsxy + s^2y^2 = (rx \pm sy)^2 = u^2.$$

En caso de que $c = k^2a$:

$$\begin{aligned} f(x,y) &= ax^2 \pm 2akxy + ak^2y^2 \\ &= a(x^2 \pm 2kxy + k^2y^2) \\ &= a(x \pm ky)^2 = av^2. \end{aligned}$$

Es claro que si $a = 0$ ó $c = 0$, entonces $b = 0$ y $f(x,y) = tw^2$. Si a y c son cero, entonces $f(x,y)$ es la forma identicamente cero. De manera que, las formas con discriminante cero no presentan mayor interés. Por lo tanto no serán consideradas dentro de este trabajo.

Podemos hablar indistintamente del determinante de la matriz asociada a la forma cuadrática $f(x,y)$ y del discriminante de dicha forma, debido a la igualdad $\Delta_f = -4det\,B_f$. Nosotros haremos uso de la expresión que más nos convenga en su momento.

Supongamos que $f(x,y) = ax^2+bxy+cy^2 \in F^2\mathbf{Z}[x,y]$ representa a $m \in \mathbf{Z}$, entonces de la ecuación en (1.5) tenemos que

$$m = f(x,y) = \frac{1}{4a}[(2ax+by)^2-\Delta_f y^2], \qquad (1.5a)$$

o bien

$$4am = (2ax+by)^2-\Delta_f y^2. \qquad (1.6)$$

Luego deducimos que si $f(x,y)$ es definida (positiva o negativa), entonces a y m tienen el mismo signo, y por lo tanto c también tiene el mismo signo que a y m. Por otra parte si $f(x,y)$ es indefinida, entonces m puede ser cualquier valor y tener ya sea signo positivo o negativo. En caso de que $\Delta_f = k^2$ para alguna $k \in \mathbf{Z}$, (1.5a) puede escribirse como

$$\begin{aligned} m &= \frac{1}{4a}[2ax+(b+k)y][2ax+(b-k)y] \\ &= \frac{1}{4a}[2ax+k'y][2ax+k''y], \end{aligned}$$

luego

$$4am = [2ax+k'y][2ax+k''y].$$

Y en dicha representación aparece el producto de factores lineales. Diremos que una forma cuadrática es **degenerada** si $\Delta_f = k^2$, de otro modo la forma es **no degenerada**. Asumiremos en el resto de este trabajo que Δ_f no es un cuadrado perfecto y por lo tanto las formas bajo consideración son no degeneradas.

Hablando de representaciones de un número, veremos que si $f(x,y) \in F^2\mathbf{Z}[x,y]$ es positiva y representa a $m \in \mathbf{Z}$, entonces sólo hay un número

finito de parejas $(x,y)\in \mathbf{Z}^2$ mediante las cuales m puede ser representado por $f(x,y)$.

Teorema 1.3. *Si $f(x,y)\in F^2\mathbf{Z}[x,y]$ es positiva y $m\in\mathbf{Z}$, entonces el número de representaciones de m mediante f es finito.*

Demostración. Demostraremos que existen un número finito de parejas (x,y) para las cuales $f(x,y) \le m$. Si $m = 0$, entonces $(x,y) = (0,0)$ es la única pareja mediante la cual $f(x,y)$ representa a cero.
Dado que una forma positiva no puede representar números negativos, entonces asumiremos que $m > 0$.
Si $f(x,y)$ no representa a m, el resultado es inmediato
De (1.4) se sigue que $(2ax+by)^2+4det\,B_f y^2 \le 4am$, de modo que $det\,B_f y^2 \le am$, lo cual se cumple si y sólo si

$$-\sqrt{\frac{am}{det\,B_f}} \le y \le \sqrt{\frac{am}{det\,B_f}}. \qquad (1.7)$$

Por lo tanto y sólo toma un número finito de valores enteros.
Por otro lado, para cada valor de y en ese conjunto se deduce de (1.4) que $(2ax+by)^2 \le 4am - 4det\,B_f y^2$, lo cual es equivalente a

$$\frac{-2\sqrt{am-det\,B_f y^2}-by}{2a} \le x \le \frac{2\sqrt{am-det\,B_f y^2}-by}{2a} \qquad (1.8)$$

y por tanto x toma solamente un número finito de valores enteros. ■

Es importante apuntar nuevamente que cuando $det\,B_f = 0$, no tiene sentido hablar de la representación de un número por dicha forma, en los términos del teorema 1.3. Ya que como se vió anteriormente, puede suceder que si $f(x,y) = m$, entonces:

$$m = (rx \pm sy)^2 = u^2 \qquad \text{ó} \qquad m = a(x \pm ky)^2 = av^2.$$

Así, en particular $f(x,y)$ representa a cero para un número infinito de valores. De esta manera $f(x,y)$ es en cualquier caso una forma cero, las cuales están

excluidas de este trabajo. De aquí en adelante usaremos indistintamente $f(x,y)$ ó f, de acuerdo a que las variables en cuestión tengan relevancia o no, en el asunto.

Sea $f(x,y)\in F^2\mathbf{Z}[x,y]$ una forma particular. Consideremos el conjunto

$$L_f = \{\, m\in\mathbf{N} :\ m \text{ es representado por } f(x,y)\,\}.$$

Por el principio del buen orden, $L_f\subseteq\mathbf{N}$ tiene un elemento mínimo, digamos m^*. Este hecho junto con el teorema 1.3 nos conducen a

Teorema 1.4. *Sea $f\in F^2\mathbf{Z}[x,y]$ positiva. Entonces el menor entero positivo representado por $f(x,y)$ puede encontrarse en un número finito de pasos.*

Demostración. Sea $f(x,y)=ax^2+bxy+cy^2\in F^2\mathbf{Z}[x,y]$. Por el teorema 1.1 $a>0$ y $c>0$. Supongamos sin pérdida de generalidad que $a\le c$. Puesto que a es representado por f tenemos que si $a=1$, entonces $1=a=f(1,0)=m^*$ y terminamos. Si $a>1$, hacemos $m=a-1$ en la demostración del teorema 1.3. De esta manera se encuentran todos los x,y tales que $f(x,y)\le m$, y como este conjunto es finito, entonces necesariamente f alcanza ahí el mínimo m^*.
La justificación es la siguiente:
Remitiendonos al teorema 1.3, hagamos $P_m=\sqrt{\dfrac{am}{det\,B_f}}$. De manera que en la representación de m se tiene que $y\in[-P_m,P_m]\cap\mathbf{Z}=Y_m$. Luego para cada $y\in Y_m$ hagamos $Q_m=\dfrac{\sqrt{am-det\,B_f y^2}}{a}$. De modo que $x\in\left[-Q_m-\dfrac{b}{2a}y, Q_m-\dfrac{b}{2a}y\right]\cap\mathbf{Z}=X_m$.
Es obvio que si $n<m$, entonces $P_n<P_m$ y $Q_n<Q_m$ por lo tanto

$$-Q_m-\frac{b}{2a}y\le -Q_n-\frac{b}{2a}y\le x\le Q_n-\frac{b}{2a}y\le Q_m-\frac{b}{2a}y.$$

Así que $X_n\subseteq X_m$ y $Y_n\subseteq Y_m$ y por lo tanto $X_n\times Y_n\subseteq X_m\times Y_m$. Entonces si el mínimo m^* se alcanza en $\bigcup_{y\in Y_m} X_m\times Y_m$, entonces no es posible encontrar un entero positivo menor que m^* en $\bigcup_{y\in Y_n} X_n\times Y_n$ ■

Notemos que existen al menos dos parejas en dicho conjunto, para las cuales f alcanza su valor menor en $\mathbf{N}$. Esto se debe a que

$$f(-x,-y) = a(-x)^2+b(-x)(-y)+c(-y)^2 = ax^2+bxy+cy^2 = f(x,y)$$
$$f(-x,y) = a(-x)^2+b(-x)y+cy^2 = ax^2-bxy+cy^2 = f(x,-y).$$

Por ejemplo, consideremos la forma cuadrática binaria $f(x,y) = 4x^2+6xy+5y^2$, cuya matriz simétrica asociada es $B_f = \begin{pmatrix} 4 & 3 \\ 3 & 5 \end{pmatrix}$ y $detB_f = 11 > 0$, de modo que f es positiva. Como $a = 4 > 1$, hacemos $m = 3$ en la demostración del teorema 1.3. De la desigualdad en (1.7) se tiene

$$-\sqrt{\frac{12}{11}} \leq y \leq \sqrt{\frac{12}{11}},$$

así que $y \in S_y = \{-1,0,1\}$.
Para $y = -1$, de la desigualdad (1.8) tenemos que $x \in \{0,1\}$. Luego, $f(0,-1) = 4$ y $f(1,-1) = 3$.
Para $y = 0$, se tiene que $x \in \{0\}$ y $f(0,0) = 0$.
Para $y = 1$, tenemos que $x \in \{-1,0\}$. Luego, $f(-1,1) = 3$ y $f(0,1) = 4$.
Por lo tanto $m^* = 3$ es el menor entero positivo representado por $f(x,y) = 4x^2+6xy+5y^2$. ■

EQUIVALENCIA DE FORMAS.

Dada la forma $f(x,y) = ax^2+bxy+cy^2 \in F^2\mathbf{Z}[x,y]$, consideremos el efecto de la transformación

$$x = \alpha x' + \beta y'$$
$$y = \gamma x' + \delta y',$$

con $\alpha, \beta, \gamma, \delta \in \mathbf{Z}$ y $\alpha\delta - \beta\gamma \neq 0$. Dicha transformación la podemos escribir simplemente como

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \tag{1.9}$$

Pues bien, sustituyendo (1.9) en la expresión para $f(x,y)$ en (1.2) se tiene

$$\begin{aligned} f(x,y) &= (x \quad y) \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\ &= (x' \quad y') \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}^t \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \\ &= f'(x',y'). \end{aligned}$$

Así, la matriz asociada a la forma cuadrática $f'(x',y')$ está dada por

$$B_{f'} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}^t \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix},$$

la cual es simétrica.

Si hacemos $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, **entonces** $f'(x',y')$ **lo podemos escribir como**

$$f'(x') = x'^t B_{f'} x' = x'^t M^t B_f M x',$$

donde $x' = \begin{pmatrix} x' \\ y' \end{pmatrix}$.

Es claro que $f'(x',y')$ se obtiene a partir de $f(x,y)$ mediante la transformación (1.9) y

$$f'(x',y') = a'x'^2 + b'x'y' + c'y'^2.$$

Se puede verificar fácilmente que

$$a' = a\alpha^2 + b\alpha\gamma + c\gamma^2 = f(\alpha,\gamma)$$

$$b' = 2(a\alpha\beta+c\gamma\delta)+b(\alpha\delta+\beta\gamma) \qquad (1.10)$$
$$c' = a\beta^2+b\beta\delta+c\delta^2 = f(\beta,\delta),$$

de manera que $f'(x',y') \in F^2\mathbf{Z}[x',y']$.
Calculando el discriminante de f' tenemos que

$$\Delta_{f'} = -4 det B_{f'}.$$

Pero

$$\begin{aligned} det B_{f'} &= det(M^t B_f M) \\ &= det M^t \, det B_f \, det M \\ &= (det M)^2 det B_f . \end{aligned} \qquad (1.10\alpha)$$

Concluimos que $det B_{f'} = det B_f$ si y sólo si $det M = \pm 1$. De manera que si Γ es el conjunto de matrices unimodulares de 2x2, es decir matrices enteras de 2x2 con determinante ± 1, entonces $M \in \Gamma$. Usando (1.3) vemos que si la matriz M de la transformación (1.9) está en Γ, entonces $\Delta_{f'} = \Delta_f$.
Por otra parte, si invertimos el proceso en (1.9) tenemos

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}^{-1} \begin{pmatrix} x \\ y \end{pmatrix}$$
$$= \frac{1}{\alpha\delta - \beta\gamma} \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

De esta igualdad se sigue que si $f(x,y) \in F^2\mathbf{Z}[x,y]$ representa a un entero m, entonces la forma $f'(x',y') \in F^2\mathbf{Z}[x',y']$, también representa a m si f' se obtiene a partir de f mediante una transformación del tipo (1.9) y el determinante de dicha transformación es ± 1.

Sean f y f' dos formas cuadráticas binarias arbitrarias. Diremos que f' es **equivalente** a f si existe una matriz $M \in \Gamma$ tal que $B_{f'} = M^t B_f M$. Escribiremos $f' \sim f$ para indicar que f' y f son equivalentes.
Puesto que $\mathbf{Z}[x,y] \cong \mathbf{Z}[x',y']$, entonces restringiremos todo nuestro trabajo en $F^2\mathbf{Z}[x,y]$. Es por esta razón que si f' y f son equivalentes, entonces escribiremos

f, $f' \in F^2\mathbf{Z}[x,y]$ entendiendo que la relación entre sus variables está dada por la transformación unimodular (1.9).
Hecha esta aclaración se tiene entonces que la relación $\sim$ en $F^2\mathbf{Z}[x,y]$ es de equivalencia. En efecto, pues si $f, g, h \in F^2\mathbf{Z}[x,y]$ entonces:

1) $f \sim f$ con $M = I$, donde como siempre I es la matriz identidad.

2) Si $f \sim g$, entonces existe $M \in \Gamma$ tal que

$$B_f = M^t B_g M,$$

así que

$$B_g = (M^t)^{-1} B_f M^{-1} = (M^{-1})^t B_f M^{-1},$$

y por lo tanto $g \sim f$.

3) Si $f \sim g$ y $g \sim h$, entonces existen $M_1, M_2, M_3 \in \Gamma$ tales que

$$B_f = M_1^t B_g M_1 \qquad \text{y} \qquad B_g = M_2^t B_h M_2,$$

donde B_f, B_g y B_h son las matrices simétricas asociadas a f, g y h respectivamente. Así

$$\begin{aligned} B_f &= M_1^t (M_2^t B_h M_2) M_1, \\ &= (M_1^t M_2^t) B_h (M_2 M_1) \\ &= (M_2 M_1)^t B_h (M_2 M_1) \\ &= M_3^t B_h M_3, \end{aligned}$$

donde $M_3 = M_2 M_1$. De manera que $f \sim h$, y de esta forma $\sim$ es transitiva.

Como consecuencia de lo anterior, se tiene

Teorema 1.5. *Sean $f, g \in F^2\mathbf{Z}[x,y]$ tales que $f \sim g$. Entonces $\Delta_f = \Delta_g$.*

Demostración. Se sigue de (1.10*a*). ■

No es cierto sin embargo que, si tenemos dos formas $f, g \in F^2\mathbf{Z}[x,y]$ tales que $\Delta_f = \Delta_g$, entonces se pueda concluir que $f \sim g$. De hecho uno de los problemas fundamentales en la teoría de formas cuadráticas, es el de decidir cuándo dos formas con el mismo discriminante son equivalentes. Un criterio que usaremos más adelante es el siguiente.

Lema 1.8. *Sean* $f_1(x,y) = a_1x^2+b_1xy+c_1y^2$ y $f_2(x,y) = a_2x^2+b_2xy+c_2y^2$ *en* $F^2\mathbf{Z}[x,y]$ *tales que* $\Delta_{f_1}=\Delta_{f_2}$. *Entonces* $f_1(x,y) \sim f_2(x,y)$ *si y sólo si existen* $\alpha, \gamma \in \mathbf{Z}$ *tales que*

$$\begin{aligned} a_1\alpha^2+b_1\alpha\gamma+c_1\gamma^2 &= a_2 \\ 2a_1\alpha+(b_1+b_2)\gamma &\equiv 0 \pmod{2a_2} \\ (b_1-b_2)\alpha+2c_1\gamma &\equiv 0 \pmod{2a_2}. \end{aligned}$$

Demostración. Si $f_1 \sim f_2$ entonces existe $M \in \Gamma$ con

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix},$$

tal que satisface las ecuaciones (1.10). Es decir

$$\begin{aligned} a_2 &= a_1\alpha^2+b_1\alpha\gamma+c_1\gamma^2 \\ b_2 &= 2(a_1\alpha\beta+c_1\gamma\delta)+b_1(\alpha\delta+\beta\gamma) \\ &= (2a_1\alpha+b_1\gamma)\beta+(b_1\alpha+2c_1\gamma)\delta, \end{aligned}$$

y $\alpha\delta-\beta\gamma = \pm 1$. Para el caso en que $\alpha\delta-\beta\gamma = 1$, podemos resolver el sistema en β, δ:

$$\begin{aligned} -\gamma\beta \quad + \quad \alpha\delta &= 1 \\ (2a_1\alpha+b_1\gamma)\beta+(b_1\alpha+2c_1\gamma)\delta &= b_2, \end{aligned}$$

cuya solución es:

$$\left.\begin{aligned}\beta &= \frac{(b_1-b_2)\alpha+2c_1\gamma}{-2a_2}\\ \delta &= \frac{2a_1\alpha+(b_1+b_2)\gamma}{2a_2}\end{aligned}\right\} \qquad (1.11)$$

Por lo tanto α y γ son tales que se satisfacen las congruencias pedidas.

Para ver que $c_2 = \dfrac{b_2^2-\Delta}{4a_2}$, tenemos que por las ecuaciones (1.10), $c_2 = f_1(\beta,\delta)$. De manera que

$$\begin{aligned}f_1(\beta,\delta) = a_1\beta^2+b_1\beta\delta+c_1\delta^2 &= a_1\left(\frac{(b_1-b_2)\alpha+2c_1\gamma}{-2a_2}\right)^2\\ &+ b_1\left(\frac{(b_1-b_2)\alpha+2c_1\gamma}{-2a_2}\right)\left(\frac{2a_1\alpha+(b_1+b_2)\gamma}{2a_2}\right)\\ &+ c_1\left(\frac{2a_1\alpha+(b_1+b_2)\gamma}{2a_2}\right)^2,\end{aligned}$$

lo cual al desarrollar y agrupar nos da

$$\begin{aligned}f_1(\beta,\delta) &= \frac{1}{4a^2}\ [\,a_1(b_2^2-\Delta)\alpha^2 + b_1(b_2^2-\Delta)\alpha\gamma + c_1(b_2^2-\Delta)\gamma^2]\\ &= \frac{b_2^2-\Delta}{4a_2^2}\,[\,a_1\alpha^2 + b_1\alpha\gamma + c_1\gamma^2]\\ &= \frac{b_2^2-\Delta}{4a_2^2}\ f_1(\alpha,\gamma) = \frac{b_2^2-\Delta}{4a_2}.\end{aligned}$$

El recíproco es ahora evidente, puesto que si existen α, $\gamma \in \mathbf{Z}$ tales que

$$\begin{aligned}a_1\alpha^2+b_1\alpha\gamma+c_1\gamma^2 &= a_2\\ 2a_1\alpha+(b_1+b_2)\gamma &\equiv 0 \pmod{2a_2}\\ (b_1-b_2)\alpha+2c_1\gamma &\equiv 0 \pmod{2a_2}.\end{aligned}$$

Entonces el par de congruencias nos conducen a encontrar β, $\delta \in \mathbf{Z}$ dadas por el sistema (1.11) y así se tiene que se satisfacen las ecuaciones (1.10) y por lo tanto $f_2(x,y) = a_2x^2+b_2xy+c_2y^2$ es equivalente a $f_1(x,y) = a_1x^2+b_1xy+c_1y^2$ en $F^2\mathbf{Z}[x,y]$. El caso $\alpha\delta-\beta\gamma=-1$, se resuelve de manera semejante. ■

En vista de que la relación ~ en $F^2\mathbf{Z}[x,y]$ nos proporciona una relación de equivalencia, entonces podemos partir dicho conjunto en clases de equivalencia, digamos $[f]$. Donde como siempre

$$[f] = \{\, g \in F^2\mathbf{Z}[x,y] : f(x,y) \sim g(x,y) \,\}.$$

Dado que siempre trabajaremos con formas primitivas, tenemos el siguiente

Teorema 1.7. *Si $f(x,y) \in F^2\mathbf{Z}[x,y]$ es primitiva, entonces todas las formas en $[f]$ también son primitivas.*

Demostración. Remitiendonos a las ecuaciones (1.10) vemos que, si $f(x,y) = ax^2+bxy+cy^2$ y $g(x,y) = a'x^2+b'xy+c'y^2 \in [f]$, entonces

$$\begin{aligned} a &= a'\alpha'^2+b'\alpha'\gamma'+c'\gamma'^2 = g(\alpha',\gamma') \\ b &= 2(a'\alpha'\beta'+c'\gamma'\delta')+b'(\alpha'\delta'+\beta'\gamma') \\ c &= a'\beta'^2+b'\beta'\delta'+c'\delta'^2 = g(\beta',\delta') \end{aligned}$$

para algunos α', β', γ', $\delta' \in \mathbf{Z}$. Puesto que $\boldsymbol{mcd}(a',b',c') \mid \boldsymbol{mcd}(a,b,c)$, entonces $\boldsymbol{mcd}(a',b',c') = 1$. Por lo tanto $g(x,y)$ es primitiva. ■

Queda claro que si una forma en una clase es positiva, entonces todas las formas en esa clase también son positivas; pues si $f' \sim f$, entonces $\Delta_{f'} = \Delta_f$ y por lo tanto tanto a' como c' son positivos.

FORMAS REPRESENTATIVAS.

Nuestra siguiente tarea consiste en seleccionar una forma representativa de cada clase de equivalencia.

Para simplificar la notación, la expresión $f(x,y)=ax^2+bxy+cy^2$ la escribiremos en ocasiones como (a,b,c), ya que una forma está completamente determinada por sus coeficientes. También adoptaremos las siguientes

definiciones. Las formas (a,b,c) y $(a,-b,c)$ que difieren solamente en el coeficiente central, diremos que son formas **opuestas**. Estas formas son equivalentes, ya que una de ellas se obtiene a partir de la otra mediante la transformación unimodular

$$M = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Decimos que las formas (a,b,c) y (c,b',c') son **adyacentes** si $b+b' \equiv 0 \pmod{2c}$. Se puede verificar mediante cálculo directo que si $\delta = \dfrac{b+b'}{2c}$ en la matriz de transformación $M = \begin{pmatrix} 0 & -1 \\ 1 & \delta \end{pmatrix}$ y $c' = a - b\delta + c\delta^2$, entonces las formas adyacentes (a,b,c) y (c,b',c') son equivalentes.

Poniendo $\delta = 0$ en la matriz **M**, se deduce inmediatamente $(a,-b,c) \sim (c,b,a)$.

Recordemos del teorema 1.1 que si $f(x,y) = ax^2+bxy+cy^2 \in F^2\mathbf{Z}[x,y]$ es positiva entonces $detB_f > 0$ ($\Delta_f < 0$) y $ac > 0$. Diremos que $f = (a,b,c) \in F^2\mathbf{Z}[x,y]$ es una **forma reducida** si

$$|b| \leq a \leq c.$$

Por ejemplo, $f(x,y) = x^2 + y^2$ es una forma reducida.

Llamaremos a $F^2_\Delta\mathbf{Z}[x,y]$ el conjunto de las formas cuadráticas binarias que tienen un discriminante Δ fijo dado. Es claro que si $f, g \in F^2_\Delta\mathbf{Z}[x,y]$, entonces $\Delta_f = \Delta_g = \Delta$. Nuevamente recordemos que si $f \sim g$, entonces $f, g \in F^2_\Delta\mathbf{Z}[x,y]$ y que si $f, g \in F^2_\Delta\mathbf{Z}[x,y]$, entonces para que $f \sim g$, se deben satisfacer las condiciones pedidas en el lema 1.6. Denotemos como $R^2_\Delta\mathbf{Z}[x,y]$ al conjunto de formas cuadráticas binarias reducidas que tienen un discriminante Δ fijo dado. Claramente

$$R^2_\Delta\mathbf{Z}[x,y] \subseteq F^2_\Delta\mathbf{Z}[x,y] \subseteq F^2\mathbf{Z}[x,y].$$

Teorema 1.8. *Si* $f=(a,b,c)\in R_{\Delta}^{2}\mathbf{Z}[x,y]$ *es positiva, entonces*

$$|b| \leq \sqrt{\frac{|\Delta|}{3}} = 2\sqrt{\frac{det\, B_f}{3}}. \qquad (1.12)$$

Demostración. Como $f=(a,b,c)\in R_{\Delta}^{2}\mathbf{Z}[x,y]$, entonces $|b| \leq a \leq c$, de manera que $|b|^2 \leq ac$. Así que $4b^2 \leq 4ac$. De donde

$$3b^2 \leq 4ac - b^2 = -\Delta = 4detB_f$$

dividiendo entre 3 y extrayendo raíz cuadrada se obtiene el resultado deseado. ■

Teorema 1.9. $|R_{\Delta}^{2}\mathbf{Z}[x,y]| < \infty$.

Demostración. Si $f=(a,b,c)\in R_{\Delta}^{2}\mathbf{Z}[x,y]$, entonces por el teorema 1.8 $|b| \leq \sqrt{\frac{|\Delta|}{3}}$, con Δ fijo. Así que b sólo puede tomar un número finito de valores en $\mathbf{Z}$. Como $\Delta = b^2 - 4ac$, entonces $4ac = b^2 - \Delta$ solamente tiene solución para un número finito de enteros a y c. Luego $\Delta = b^2 - 4ac$ determina sólo un número finito de ternas $(a,b,c)\in\mathbf{Z}^3$ para las cuales $f=(a,b,c)\in R_{\Delta}^{2}\mathbf{Z}[x,y]$. ■

Recordemos que si tenemos dos formas f y g en $F^2\mathbf{Z}[x,y]$ tales que $f \sim g$, entonces existe una matriz M de 2x2 con coeficientes enteros y $detM = \pm 1$, tal que

$$B_g = M^t B_f M.$$

Diremos que f y g son **estrictamente equivalentes** o bien **propiamente equivalentes** si $detM = +1$ y escribiremos esta equivalencia como $f \approx g$. Si $detM = -1$, entonces diremos que f y g son **impropiamente equivalentes**. Es claro que $\approx$ es una relación de equivalencia en $F^2\mathbf{Z}[x,y]$ y que, el ser $f \approx g$ implica que $f \sim g$, pero no necesariamente se tiene que si $f \sim g$, entonces se debe de tener que $f \approx g$.

Podemos ver que si $f = (a,b,c) \in R_{\Delta}^{2}\mathbf{Z}[x,y]$, entonces $g = (a,-b,c) \in R_{\Delta}^{2}\mathbf{Z}[x,y]$ y en este caso f y g son impropiamente equivalentes, ya que una de ellas se obtiene a partir de la otra mediante alguna de las siguientes transformaciones

$$M_1 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{ó} \qquad M_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

lo cual se puede corroborar por cálculo directo. De aquí que si $b \neq 0$, entonces las formas opuestas (a,b,c) y $(a,-b,c)$ son impropiamente equivalentes. También es importante notar que las formas adyacentes (a,b,c) y (c,b,a) son impropiamente equivalentes mediante la transformación

$$M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

A continuación mostraremos que cada forma de discriminante dado es estrictamente equivalente a una forma reducida del mismo discriminante. Antes de otra cosa, consideremos las transformaciones unimodulares

$$S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{y} \quad T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Puede mostrarse fácilmente que $S^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ para todo $n \in \mathbf{Z}$, y que $T^2 = -I$.

Si aplicamos S^n a $f = (a,b,c) \in F_{\Delta}^{2}\mathbf{Z}[x,y]$, es decir $(S^n)^t B_f S^n$, se obtiene una forma equivalente $f' = (a',b',c') \in F_{\Delta}^{2}\mathbf{Z}[x,y]$, donde $a' = a$, $b' = b+2an$, $c' = an^2 + bn + c$. Y al aplicar T a la misma f, o sea $T^t B_f T$ obtenemos $f'' = (c,-b,a)$. Queda claro que al aplicar S^n a f, el primer coeficiente de la forma no se altera ni cambia de posición y al aplicar T se intercambian las posiciones del primero y tercer coeficiente y únicamente cambia de signo el coeficiente central.

Teorema 1.10. *Sea $f = (a,b,c) \in F_{\Delta}^{2}\mathbf{Z}[x,y]$ positiva. Entonces existe $g = (a',b',c') \in R_{\Delta}^{2}\mathbf{Z}[x,y]$ tal que $f \sim g$.*

Primera demostración. Esta demostración consiste en dar un algoritmo de reducción para todos los casos posibles. Para esto consideremos todas las posibles permutaciones de los números a, $|b|$ y c. Dado que a y c son positivos se tiene :

Caso a) $a \leq |b| \leq c$.

Aplicamos a f la transformación $S^{\beta} = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}$ para obtener $a' = a$, $b' = b+2a\beta$, $c' = a\beta^2+b\beta+c$. Escojemos $\beta \in \mathbf{Z}$ de tal manera que $|b+2a\beta| \leq a$. Si $a' \leq c'$, entonces $g = (a', b', c') \in R^2_{\Delta}\mathbf{Z}[x,y]$. Si $a' > c'$, procedemos como en **d)**.

Caso b) $a \leq c \leq |b|$.

Aplicamos $S^{\beta} = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}$ a f para obtener $a' = a$, $b' = b+2a\beta$, $c' = a\beta^2+b\beta+c$. Escojemos $\beta \in \mathbf{Z}$ de tal manera que $|b+2a\beta| \leq a$. Si $a' \leq c'$, entonces $g = (a', b', c') \in R^2_{\Delta}\mathbf{Z}[x,y]$. De otra manera procedemos como en **d)**.

Caso c) $|b| \leq a \leq c$.

En este caso $g = f \in R^2_{\Delta}\mathbf{Z}[x,y]$.

Caso d) $|b| \leq c \leq a$.

Aplicamos $T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ a f y obtenemos la forma equivalente $f' = (c, -b, a)$ la cual es reducida.

Caso e) $c \leq a \leq |b|$.

Transformamos f mediante $T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ para obtener $f' = (c, -b, a)$. Haciendo $a' = c$, $c' = a$ nos permiten proceder como en **b)**.

Caso f) $c \leq |b| \leq a$.

Aplicamos $T=\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ a f y obtenemos $f'=(c,-b,a)$. Poniendo $a'=c$, $c'=a$ procedemos como en **a)**.

Es claro que las transformaciones aplicadas en cada caso, disminuyen la magnitud del coeficiente central (por lo menos no lo aumentan) de las sucesiones de formas. De esta manera obtenemos una sucesión decreciente de enteros positivos. Así que la sucesión de formas obtenidas a partir de la forma original es finita. Sean $M_1,M_2,\ldots,M_k$ la sucesión de matrices unimodulares que nos llevan de la forma original a la forma reducida equivalente, entonces es evidente que la matriz $M = M_1 \cdot M_2 \cdots M_k = \prod_{i=1}^{k} M_i$ transforma directamente g en f y como $detM_i = +1$, entonces $detM = +1$. Así que $f \sim g$ y $f \in R_{\Delta}^{2}\mathbf{Z}[x,y]$. ■

Segunda demostración. Este procedimiento consiste en partir del menor entero positivo representado por la forma original (teorema 1.4). Pues bien, sea $a = \min\{\, m \in \mathbf{N} : g(x,y) = m \,\}$. Entonces existen $\alpha, \gamma \in \mathbf{Z}$ tales que $g(\alpha,\gamma) = a$ es una representación primitiva de a, ya que si $\boldsymbol{mcd}(\alpha,\gamma) = d > 1$, entonces $g(\alpha/d,\gamma/d) = a/d^2 < a$. Esto contradice el hecho de que a es el menor entero positivo representado por $g(x,y)$. Luego entonces, existen $\beta, \delta \in \mathbf{Z}$ tales que $\alpha\delta - \beta\gamma = 1$ y la matriz $M=\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ es unimodular. Ahora bien, sea $h(x,y) \in F_{\Delta}^{2}\mathbf{Z}[x,y]$ tal que

$$B_h = M^t B_g M = \begin{pmatrix} a & k/2 \\ k/2 & s \end{pmatrix},$$

donde como siempre $B_g = \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix}$. Además, por las ecuaciones (1.10) se tiene que

$$s = g(\beta,\delta) \qquad \text{y} \qquad k = 2(A\alpha\beta + C\gamma\delta) + B(\alpha\delta + \beta\gamma),$$

por lo tanto $h = (a,k,s) \in F_\Delta^2\mathbf{Z}[x,y]$ y $h \sim g$.
Enseguida tenemos que para cualquier $r \in \mathbf{Z}$, la transformación $M_r = \begin{pmatrix} 1 & -r \\ 0 & 1 \end{pmatrix}$ es unimodular. Hagamos $f \in F_\Delta^2\mathbf{Z}[x,y]$ de tal manera que

$$B_f = M_r^t B_h M_r ,$$

es decir

$$B_f = \begin{pmatrix} 1 & 0 \\ -r & 1 \end{pmatrix}\begin{pmatrix} a & k/2 \\ k/2 & s \end{pmatrix}\begin{pmatrix} 1 & -r \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} a & k-2ar \\ k-2ar & ar^2 - kr + s \end{pmatrix}.$$

Si tomamos r tal que $|k-2ar| \leq a$, entonces $b = k - 2ar$, satisface $|b| \leq a$. Por otro lado, sea $c = ar^2 - kr + s$. Como $f(0,1) = c$, entonces c también es representado por h. Como $h \sim g$, entonces g también representa a c. De modo que $a \leq c$ y por lo tanto $|b| \leq a \leq c$, por transitividad $f \sim g$, y por lo tanto $f(x,y) \in R_\Delta^2\mathbf{Z}[x,y]$. ■

Por ejemplo, consideremos la forma $g = (4,6,5) \in F_{-44}^2\mathbf{Z}[x,y]$.
La transformación $M_1 = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$, nos lleva a la forma $g' = (4,-2,3)$ que a su vez, es equivalente a (3,2,4), mediante $M_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, y esta es reducida por definición. Así que la matriz de reducción que nos lleva de la forma original a la forma reducida está dada por

$$M = M_1 M_2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix},$$

de manera que $g = (4,6,5) \sim (3,2,4) = f \in R_{-44}^2\mathbf{Z}[x,y]$.

Notemos también que si f, f_1, $f_2 \in F_\Delta^2\mathbf{Z}[x,y]$ son tales que f, f_1 son impropiamente equivalentes y f_1, f_2 son impropiamente equivalentes, entonces

f, f_2 son propiamente (o estrictamente) equivalentes. Es claro que si $(a,b,c) \in R_\Delta^2\mathbf{Z}[x,y]$, entonces $(a,-b,c) \in R_\Delta^2\mathbf{Z}[x,y]$, pero si $b \neq 0$, entonces (a,b,c) y $(a,-b,c)$ son impropiamente equivalentes. De aquí que las formas reducidas opuestas están en clases de equivalencia distintas y por lo tanto el representante de cada clase es único. Esto lo apuntaremos en el teorema 1.11, donde sólo consideraremos el caso en el que el coeficiente central es positivo. El caso $b < 0$ se trata de manera semejante.

Es importante aclarar en este punto que si (a,b,c) y $(a,-b,c)$ son elementos de $R_\Delta^2\mathbf{Z}[x,y]$, entonces para que $(a,b,c) \sim (a,-b,c)$, es necesario tener $a = b$ ó $a = c$; puesto que $(a,a,c) \sim (a,-a,c)$ bajo la transformación $\mathrm{M} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ y $(a,b,a) \sim (a,-b,a)$ mediante $M_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ ó $M_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ y estas son las únicas formas estrictamente equivalentes en $R_\Delta^2\mathbf{Z}[x,y]$.

Veamos ahora cómo podemos construir un sistema completo de formas reducidas dado $\Delta < 0$. Supongamos que se nos da $\Delta < 0$, entonces por el teorema 1.8, asignamos a b los valores 0, ±1, ±2, ..., $\pm k = \pm\left[\sqrt{\frac{|\Delta|}{3}}\right]$. Donde $[\cdot]$ denota la función mayor entero. Entonces para cada valor asignado a b, descomponemos $\frac{b^2-\Delta}{4}$ en todas las maneras posibles como el producto de dos enteros a y c. Finalmente, eliminamos aquellas combinaciones para las cuales no se cumpla $|b| \leq a \leq c$. Luego, las formas restantes son precisamente $R_\Delta^2\mathbf{Z}[x,y]$.

Por ejemplo, supongamos que se nos da $\Delta = -95$, como $\left[\sqrt{\frac{|-95|}{3}}\right] = 5 = k$. Entonces elaboramos la siguiente tabla:

b	$b^2-\Delta$	$\frac{b^2-\Delta}{4} \in \mathbf{Z}$	descomposición en ac
0	95	***	***
±1	96	24	1·24, 2·12, 3·8, 4·6
±2	99	***	***
±3	104	26	1·26*, 2·13*

±4	111	***	***
±5	120	30	1·30*, 2·15*, 3·10*, 5·6

Las descomposiciones marcadas con * se rechazan, ya que no satisfacen la condición requerida. Así que

$$R^2_{-95}\mathbf{Z}[x,y] = \{ (1,1,24), (2,\pm1,12), (3,\pm1,8), (4,\pm1,6), (5,5,6) \}.$$

Teorema 1.11. *Sean* $f, f' \in R^2_\Delta\mathbf{Z}[x,y]$, *donde* $f = (a,b,c)$ *y* $f' = (a',b',c')$ *con* $b \geq 0$ *y* $b' \geq 0$. *Si* $f \sim f'$, *entonces* $f = f'$.

Demostración. Dado que $f \sim f'$, entonces de las ecuaciones (1.10) se tiene que existen $\alpha, \gamma \in \mathbf{Z}$ tales que $a' = a\alpha^2+b\alpha\gamma+c\gamma^2 = f(\alpha,\gamma)$ es una representación primitiva de a'. Sin pérdida de generalidad supongamos que $a \geq a'$. Haciendo uso de la desigualdad $\alpha^2+\gamma^2 \geq 2|\alpha\gamma|$ tenemos

$$\begin{aligned} a' &= a\alpha^2+b\alpha\gamma+c\gamma^2 \geq a(\alpha^2+\gamma^2)+b\alpha\gamma \\ &\geq a(\alpha^2+\gamma^2)-b|\alpha\gamma| \geq 2a|\alpha\gamma|-b|\alpha\gamma| \\ &\geq 2a|\alpha\gamma|-a|\alpha\gamma| = a|\alpha\gamma|. \end{aligned} \tag{1.13}$$

Así que $|\alpha\gamma| \leq 1$.
Si $|\alpha\gamma| \neq 0$, con α y γ no ambos cero, entonces

$$a' = a\alpha^2+b\alpha\gamma+c\gamma^2 = a\alpha^2+c\gamma^2 \geq a(\alpha^2+\gamma^2) \geq a. \tag{1.14}$$

Si $|\alpha\gamma| = 1$, de (1.13) se obtiene el mismo resultado. Por lo tanto $a = a'$.
Dado que $a = a' \leq c'$, podemos suponer $c > c'$. Entonces $c > a$. Esto elimina la posibilidad de que $|\alpha\gamma| = 1$, ya que si así lo fuera, se tendría que $c\gamma^2 > a\gamma^2$ y (1.13) implicaría que $a' > a|\alpha\gamma| = a$. Contrario a lo supuesto. Entonces $|\alpha\gamma| = 0$, y $\gamma = 0$, ya que si $\gamma \neq 0$, entonces tendríamos que $a' = a\alpha^2+c\gamma^2 > a\alpha^2+a\gamma^2 = a(\alpha^2+\gamma^2) \geq a$. De manera que $a' > a$, en contradicción con lo supuesto.
Ahora bien, por ser f y f' reducidas, entonces $|b| \leq a$ y $|b'| \leq a' = a$. Por hipótesis $b, b' \geq 0$, de manera que

$$0 \leq b \leq a \qquad \text{y} \qquad 0 \leq b' \leq a.$$

de donde

$$0 \le b + b' \le 2a, \tag{1.15}$$
$$-a \le b' - b \le a. \tag{1.16}$$

Como el determinante de la matriz de la transformación es $\alpha\delta - \beta\gamma = 1$, entonces $\alpha\delta = 1$, ya que $\gamma = 0$ y por (1.10) se tiene que $b' = 2a\alpha\beta + b$. De aquí que $b' - b = 2a\alpha\beta$. De manera que $b' - b$ es multiplo de $2a$ y por (1.16) se debe tener $b' - b = 0$, y por lo tanto $b' = b$.
Por último, de la igualdad $\Delta f = b^2 - 4ac = b'^2 - 4a'c' = \Delta f'$, se deduce fácilmente que $c = c'$. ■

Corolario 1.12. *A cada* $f \in F_\Delta^2\mathbf{Z}[x,y]$ *le corresponde una única* $g \in R_\Delta^2\mathbf{Z}[x,y]$ *tal que* $f \sim g$.

Demostración. Se sigue inmediatamente de los teoremas 1.10 y 1.11. ■

De todo esto podemos ver que para decidir si dos formas son estrictamente equivalentes (cuando la equivalencia no es evidente desde un principio), basta con encontrar la forma reducida correspondiente a cada una de ellas, luego concluir que dichas formas son estrictamente equivalentes si y sólo si sus formas reducidas correspondientes son idénticas. Por lo tanto $F_\Delta^2\mathbf{Z}[x,y]$ lo podemos partir en clases de equivalencia (en el sentido estricto), donde en cada clase elegimos como representante a un elemento adecuado de $R_\Delta^2\mathbf{Z}[x,y]$.

Corolario 1.13. $\{\,[f] : f \in F_\Delta^2\mathbf{Z}[x,y]\,\}$ *es finito.*

Demostración. Por el teorema 1.9, $|\,R_\Delta^2\mathbf{Z}[x,y]\,| < \infty$. De aquí la conclusión. ■

COMPOSICION DE FORMAS.

En esta sección definiremos en $\{\,[f]\,\} = \{\,[f] : f \in F_\Delta^2\mathbf{Z}[x,y]\,\}$, una operación binaria para dotar a este conjunto de una estructura de grupo. A ese grupo lo

llamaremos **el grupo de clases de formas** y lo denotaremos como $\mathbf{CLF}_\Delta$. Definimos la forma cuadrática binaria $f=(1,b,c)$ como la **forma principal**. Más adelante veremos que esta forma juega el papel de la identidad en $\mathbf{CLF}_\Delta$.

Consideremos $f_1=(a_1,b_1,c_1)$ y $f_2=(a_2,b_2,c_2)$ en $F_\Delta^2\mathbf{Z}[x,y]$. Veamos qué es lo que sucede si efectuamos el producto ordinario entre ellas

$$\begin{aligned} f_1 f_2 &= (a_1x_1^2+b_1x_1y_1+c_1y_1^2)(a_2x_2^2+b_2x_2y_2+c_2y_2^2) \\ &= a_1a_2x_1^2x_2^2+a_1b_2x_1^2x_2y_2+a_1c_2x_1y_2^2 \\ &\quad +b_1a_2x_1x_2^2y_1+b_1b_2x_1x_2y_1y_2+b_1c_2x_1y_1y_2^2 \\ &\quad +c_1a_2y_1^2x_2^2+c_1b_2x_2y_1^2y_2+c_1c_2y_1^2y_2^2. \end{aligned}$$

A simple vista, no parece ser que esta expresión sea una forma cuadrática binaria. Surge la pregunta entonces; ¿qué es lo que debemos hacer para que el producto en $F_\Delta^2\mathbf{Z}[x,y]$ sea cerrado y de esta manera poder dotar a $\{[f]\}$ de estructura de grupo? Para hacer esto, veremos que existen formas "especiales" representativas en $\{[f]\}$, con las cuales se da la estructura que queremos.

Observemos que si r es representado por $f\in F_\Delta^2\mathbf{Z}[x,y]$, entonces r es representado por $g\in[f]$. De esta manera la representación de un número es una propiedad de las clases y no de la forma individual. Ya que siempre tratamos con formas primitivas, lo puntualizamos en el siguiente:

Lema 1.14. *Sea $f=(a,b,c)\in F_\Delta^2\mathbf{Z}[x,y]$, primitiva y $m\in\mathbf{Z}$ fijo. Entonces, existen $u,v\in\mathbf{Z}$ tales que $\mathbf{mcd}(u,v)=1$ y $\mathbf{mcd}(f(u,v),m)=1$.*

Demostración. Sean:

$P=\prod p_i$	tal que	$p_i \mid a,$	$p_i \mid c,$	y	$p_i \nmid m,$
$Q=\prod q_j$	tal que	$q_j \nmid a,$	$q_j \nmid c,$	y	$q_j \mid m,$
$R=\prod r_k$	tal que	$r_k \mid a,$	$r_k \nmid c,$	y	$r_k \nmid m,$
$S=\prod s_t$	tal que	$s_t \nmid a,$	$s_t \mid c,$	y	$s_t \nmid m,$

donde p_i, q_j, r_k, s_l, son primos distintos. Dado que $\boldsymbol{mcd}(a,b,c) = 1$, entonces $\boldsymbol{mcd}(b,P) = 1$.
Escogemos $u,v \in \mathbf{Z}$ tales que
$\boldsymbol{mcd}(u,P) = \boldsymbol{mcd}(u,R) = \boldsymbol{mcd}(v,P) = \boldsymbol{mcd}(v,Q) = 1$, $u = \alpha Q$, $v = \beta R$, $uv = \gamma S$ y $s_i^2 \nmid uv$. Esto puede hacerse en un número infinito de modos y u, v siguen siendo primos uno a otro. Una de las maneras más simples de hacer esto, es poner $u = QS'$, $v = RS''$, donde $S = S'S''$ es cualquier descomposición de S en dos factores.

Si p, q, r, s denotan factores primos de P, Q, R, S respectivamente. Entonces como

$$\begin{aligned} d = f(u,v) &= au^2+buv+cv^2 && (1)\\ &= a\alpha^2Q^2+b\alpha\beta QR+c\beta^2R^2 && (2)\\ &= a\alpha^2Q^2+b\alpha\beta QR+c\beta^2R^2 && (3)\\ &= a\alpha^2Q^2+b\gamma S+c\beta^2R^2 && (4)\\ &= au^2+b\alpha\beta QR+c\beta^2R^2, && (5) \end{aligned}$$

se tiene que:

$d \equiv cv^2 \pmod q$ (por (2)), así que $\boldsymbol{mcd}(d,q) = 1$, por lo tanto $\boldsymbol{mcd}(d,Q) = 1$.
$d \equiv au^2 \pmod r$ (por (5)), así que $\boldsymbol{mcd}(d,r) = 1$, por lo tanto $\boldsymbol{mcd}(d,R) = 1$.
$d \equiv buv \pmod p$ (por (1)), así que $\boldsymbol{mcd}(d,p) = 1$, por lo tanto $\boldsymbol{mcd}(d,P) = 1$.
$d \equiv au^2$ ó $cv^2 \pmod s$, si u ó $v \equiv 0 \pmod s$, luego $\boldsymbol{mcd}(d,S) = 1$.

Sabemos que si $x \equiv y \pmod p$, entonces $\boldsymbol{mcd}(x,p) = \boldsymbol{mcd}(y,p)$. Por lo tanto

$$\boldsymbol{mcd}(d,P) = \boldsymbol{mcd}(d,R) = \boldsymbol{mcd}(d,P) = \boldsymbol{mcd}(d,Q) = 1. \qquad (*)$$

Si $\boldsymbol{mcd}(d,m) = h$, entonces $h \mid d$ y $h \mid m$, luego $m = \delta h$. Si λ es factor primo de h, entonces λ es factor de m. Supongamos que λ es factor de P ó Q ó R ó S. Se sigue por (*) que $\lambda = 1$. Si por otro lado suponemos que λ no es factor ni de P, ni de Q, ni de R, ni de S y además $\lambda \mid d$, entonces $\boldsymbol{mcd}(\lambda,P) = 1$. Por (*) se sigue nuevamente que $\lambda = 1$. Por lo tanto $\boldsymbol{mcd}(d,m) = 1$. ■

Lema 1.15. *Sea* $[f] \in \{[f]\}$ *y* $D \in \mathbf{N}$. *Entonces existe* $g \in [f]$ *tal que* $g = (a,b,c)$ *y* $\boldsymbol{mcd}(a,D) = 1$.

Demostración. Sea $f = (A,B,C)$ primitiva y $\mathbf{F} = \{ m \in \mathbf{N} : m$ es representado por $f \}$. Puesto que $A, C \in \mathbf{F}$, entonces $d \mid A$ y $d \mid C$. Para cualesquiera $(x_0,y_0) \in \mathbf{Z}\times\mathbf{Z} - \{0\}$ se tiene que $d \mid m = Ax_0^2 + Bx_0y_0 + Cy_0^2$. Así que $d \mid Bx_0y_0$ para $(x_0,y_0) \in \mathbf{Z}\times\mathbf{Z} - \{0\}$. Por lo tanto $d \mid B$ y $d \mid \boldsymbol{mcd}(A,B,C)$, lo cual es absurdo. De esta manera existe $a \in \mathbf{F}$ tal que $\boldsymbol{mcd}(a,D) = 1$.
Sean $\alpha, \gamma \in \mathbf{Z}$ tal que $f(\alpha,\gamma) = a$. Si $\boldsymbol{mcd}(\alpha,\gamma) = 1$, terminamos. Si $\boldsymbol{mcd}(\alpha,\gamma) = d_1 > 1$, entonces $f\left(\frac{\alpha}{d_1}, \frac{\gamma}{d_1}\right) = \frac{a}{d_1^2} = a_1 \in \mathbf{F}$. Es claro que $\boldsymbol{mcd}(a_1,D) = 1$.
Supongamos que $f(\alpha,\gamma) = a$ es una representación primitiva. Sea $1 = \alpha\delta - \beta\gamma$. Entonces $\mathbf{M} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma$ y $g(x,y) = \boldsymbol{x}^t \mathbf{M}^t \mathbf{B}_f \mathbf{M}\boldsymbol{x} \in [f]$ satisface el teorema. ■

Lema 1.16. *Sean* $[f_1], [f_2] \in \{ [f] \}$. *Entonces existen* $g_1 \in [f_1]$ *y* $g_2 \in [f_2]$ *tales que* $g_1 = (a_1,b,c_1)$, $g_2 = (a_2,b,c_2)$ *y* $\boldsymbol{mcd}(a_1,a_2) = 1$.

Demostración. Sean $f_1 = (A_1,B_1,C_1)$ y $f_2 = (A_2,B_2,C_2)$ representantes de las clases $[f_1]$ y $[f_2]$ en $\{ [f] \}$ respectivamente. Por definición $A_1 > 0$ y podemos escoger $A_2 \in \mathbf{N}$ de tal manera que $\boldsymbol{mcd}(A_1,A_2) = 1$. Esto lo podemos hacer por el lema 1.15.
Consideremos las transformaciones unimodulares

$$M_1 = \begin{pmatrix} 1 & k_1 \\ 0 & 1 \end{pmatrix} \quad \text{y} \quad M_2 = \begin{pmatrix} 1 & k_2 \\ 0 & 1 \end{pmatrix}.$$

Sean $g_1, g_2 \in F_\Delta^2 \mathbf{Z}[x,y]$, de manera que $B_{g_i} = M_i^t B_{f_i} M_i$ es decir, para $i = 1,2$ tenemos:

$$\begin{pmatrix} a_i & b_i/2 \\ b_i/2 & c_i \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ k_i & 1 \end{pmatrix} \begin{pmatrix} A_i & B_i/2 \\ B_i/2 & C_i \end{pmatrix} \begin{pmatrix} 1 & k_i \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} A_i & A_ik_i + B_i/2 \\ A_ik_i + B_i/2 & A_ik_i^2 + B_ik_i + C_i \end{pmatrix}.$$

Podemos hacer $a_i = A_i$, $b_i = 2A_ik_i + B_i$ y $c_i = A_ik_i^2 + B_ik_i + C_i$ con $i = 1,2$.

Dado que $\Delta = B_1^2 - 4A_1C_1 = B_2^2 - 4A_2C_2$, se tiene entonces que B_1 y B_2 tienen la misma paridad. Si $b_1 = b_2 = b$, entonces

$$2A_1k_1+B_1 = 2A_2k_2+B_2,$$

de modo que

$$A_1k_1-A_2k_2 = \frac{B_2 - B_1}{2}.$$

Esto siempre es cierto, pues $\boldsymbol{mcd}(A_1,A_2) = 1$. Por lo tanto $g_1 = (a_1,b,c_1) = f_1$, $g_2 = (a_2,b,c_2) = f_2$ y $\boldsymbol{mcd}(a_1,a_2) = 1$. ■

Lema 1.17. *Sean* $[g_1]$, $[g_2]$ *en* $\{[f]\}$. *Entonces existen* $f_1 \in [g_1]$ y $f_2 \in [g_2]$ *tales que*

$$f_1(x,y) = a_1x^2+bxy+a_2c_0y^2$$
$$f_2(x,y) = a_2x^2+bxy+a_1c_0y^2$$

y $\boldsymbol{mcd}(a_1,a_2) = 1$.

Demostración. Por el lema 1.16 sabemos que

$$f_1(x,y) = a_1x^2+bxy+c_1y^2, \qquad f_2(x,y) = a_2x^2+bxy+c_2y^2.$$

Como $\Delta = b^2-4a_1c_1 = b^2-4a_2c_2$, entonces $a_1c_1 = a_2c_2$. Así $a_1 \mid a_2c_2$. Dado que $\boldsymbol{mcd}(a_1,a_2) = 1$, se tiene $a_1 \mid c_2$ y $c_2 = a_1c_0$ para algún $c_0 \in \mathbf{Z}$. De la misma manera se puede probar que $c_1 = a_2c_0$. ■

Consideremos las formas en $F_\Delta^2\mathbf{Z}[x,y]$:

$$f_1(x_1,y_1) = a_1x_1^2 + bx_1y_1 + a_2c_0y_1^2$$
$$f_2(x_2,y_2) = a_2x_2^2 + bx_2y_2 + a_1c_0y_2^2,$$

con $\boldsymbol{mcd}(a_1,a_2) = 1$. Si efectuamos el producto ordinario de estas dos formas tenemos como en un principio

$$\begin{aligned} f_1(x_1,y_1)\cdot f_2(x_2,y_2) &= (a_1x_1^2 + bx_1y_1 + a_2c_0y_1^2)(a_2x_2^2 + bx_2y_2 + a_1c_0y_2^2) \\ &= a_1a_2x_1^2x_2^2 + a_1bx_1^2x_2y_2 + a_1^2c_0x_1^2y_2^2 \\ &+ a_2bx_1x_2^2y_1 + b^2x_1x_2y_1y_2 + a_1bc_0x_1y_1y_2^2 \\ &+ a_2^2c_0x_2^2y_1^2 + a_2bx_2y_1^2y_2 + a_1a_2c_0^2y_1^2y_2^2. \end{aligned}$$

Definimos

$$\begin{aligned} x_3 &= x_1x_2 - c_0y_1y_2 \\ y_3 &= a_1x_1y_2 + a_2x_2y_1 + by_1y_2. \end{aligned} \qquad (1.17)$$

Sea $f_3(x_3,y_3) = a_1a_2x_3^2 + bx_3y_3 + c_0y_3^2$. Entonces

$$\begin{aligned} f_3(x_3,y_3) &= a_1a_2x_1^2x_2^2 + a_1a_2c_0^2y_1^2y_2^2 + a_1bx_1^2x_2y_2 \\ &+ a_2bx_1x_2^2y_1 + b^2x_1x_2y_1y_2 + a_1bc_0x_1y_1y_2^2 \\ &+ a_2bc_0x_2y_1^2y_2 + a_1^2c_0x_1^2y_2^2 + a_2^2c_0x_2^2y_1^2. \\ &= f_1(x_1,y_1)\cdot f_2(x_2,y_2) \end{aligned}$$

y $f_3(x,y)\in F_\Delta^2\mathbf{Z}[x,y]$. De manera que las formas "especiales" que buscamos estan dadas por el lema 1.17. Sean $g_1=[g_1]$, $g_2=[g_2]\in\{\ [f]\ \}$ tales que si $f_1=(a_1,b,a_2c_0)\in[g_1]$ y $f_2=(a_2,b,a_1c_0)\in[g_2]$, entonces definimos

$$g_1g_2 = [g_1][g_2] = [f_1][f_2] = f_1f_2 = [(a_1a_2,b,c_0)].$$

Veremos que esta está bien definida.

Teorema 1.18. *Si f_1, f_2, g_1, $g_2\in F_\Delta^2\mathbf{Z}[x,y]$ son tales que $f_1 \sim g_1$ y $f_2 \sim g_2$, entonces*

$$f_1f_2 \sim g_1g_2.$$

Demostración. Podemos suponer que

$$\begin{aligned} f_1 &= (a_1,b,a_2c_0) \sim g_1 = (a_1',b',a_2'c_0'), \\ f_2 &= (a_2,b,a_1c_0) \sim g_2 = (a_2',b',a_1'c_0'), \end{aligned}$$

con $\mathbf{mcd}(a_1,a_2) = \mathbf{mcd}(a_1',a_2') = 1$.

Por definición tenemos que $f_1 f_2 = (a_1a_2, b, c_0)$ y $g_1 g_2 = (a_1'a_2', b', c_0')$. Queremos probar que $f_1 f_2 \sim g_1 g_2$, es decir que existen $x_3, y_3 \in \mathbf{Z}$ tales que

$$a_1a_2x_3^2 + bx_3y_3 + c_0y_3^2 = a_1'a_2' \tag{1.18}$$
$$2a_1a_2x_3 + (b + b')y_3 \equiv 0 \pmod{2a_1'a_2'} \tag{1.19}$$
$$(b - b')x_3 + 2c_0y_3 \equiv 0 \pmod{2a_1'a_2'}. \tag{1.20}$$

Como $f_1 \sim g_1$ y $f_2 \sim g_2$, entonces por el lema 1.6 sabemos que existen $x_1, y_1, x_2, y_2 \in \mathbf{Z}$ tales que

$$a_1x_1^2 + bx_1y_1 + a_2c_0y_1^2 = a_1' \tag{1.18-1}$$
$$2a_1x_1 + (b + b')y_1 \equiv 0 \pmod{2a_1'} \tag{1.19-1}$$
$$(b - b')x_1 + 2a_2c_0y_1 \equiv 0 \pmod{2a_1'}. \tag{1.20-1}$$

$$a_2x_2^2 + bx_2y_2 + a_1c_0y_2^2 = a_2' \tag{1.18-2}$$
$$2a_2x_2 + (b + b')y_2 \equiv 0 \pmod{2a_2'} \tag{1.19-2}$$
$$(b - b')x_2 + 2a_1c_0y_2 \equiv 0 \pmod{2a_2'}. \tag{1.20-2}$$

Sea

$$x_3 = x_1x_2 - c_0y_1y_2$$
$$y_3 = a_1x_1y_2 + a_2x_2y_1 + by_1y_2.$$

Es claro que con estos valores (1.18) y (1.19) son solubles. Sólo nos queda mostrar que (1.20) también es soluble.

Hagamos $B = (b - \sqrt{\Delta})\frac{x_2}{2} + c_0y_3$. Entonces

$$R = \left[(b - \sqrt{\Delta})\frac{x_1}{2} + a_2c_0y_1\right]\left[a_2x_2 + (b + \sqrt{\Delta})\frac{y_2}{2}\right]$$
$$= (b - \Delta)\frac{a_2x_1x_2}{2} + (b^2 - \Delta)\frac{x_1y_2}{4} + a_2^2c_0y_1x_2 + (b + \sqrt{\Delta})\frac{a_2c_0y_1y_2}{2}.$$

En esta expresión tenemos $(b^2 - \Delta)\frac{x_1y_2}{4} = a_1a_2c_0x_1y_2$, ya que $b^2 - \Delta = 4a_1a_2c_0$.

Así

$$R = (b-\Delta)\frac{a_2x_1x_2}{2} + a_1a_2c_0x_1y_2 + a_2^2c_0y_1x_2 + (b+\sqrt{\Delta})\frac{a_2c_0y_1y_2}{2}.$$

Por otro lado tenemos

$$\begin{aligned} a_2B &= a_2\left[(b-\sqrt{\Delta})\frac{x_3}{2} + c_0y_3\right] \\ &= a_2\left[(b-\sqrt{\Delta})\frac{(x_1x_2 - c_0y_1y_2)}{2} + c_0(a_1x_1y_2 + a_2x_2y_1 + by_1y_2)\right] \\ &= (b-\sqrt{\Delta})\frac{a_2x_1x_2}{2} + (b+\sqrt{\Delta})\frac{a_2c_0y_1y_2}{2} + a_1a_2c_0x_1y_2 + a_2^2c_0y_1x_2 = R. \end{aligned}$$

Por lo tanto

$$\left[(b-\sqrt{\Delta})\frac{x_1}{2} + a_2c_0y_1\right]\left[a_2x_2 + (b+\sqrt{\Delta})\frac{y_2}{2}\right] = a_2B. \qquad (*)$$

De manera similar se puede mostrar que

$$\left[a_1x_1 + (b+\sqrt{\Delta})\frac{y_1}{2}\right]\left[(b-\sqrt{\Delta})\frac{x_2}{2} + a_1c_0y_2\right] = a_1B. \qquad (*)$$

$$\left[(b-\sqrt{\Delta})\frac{x_1}{2} + a_2c_0y_1\right]\left[(b-\sqrt{\Delta})\frac{x_2}{2} + a_1c_0y_2\right] = (b-\sqrt{\Delta})\frac{B}{2}. \qquad (*)$$

$$c_0\left[a_1x_1 + (b+\sqrt{\Delta})\frac{y_1}{2}\right]\left[a_2x_2 + (b+\sqrt{\Delta})\frac{y_2}{2}\right] = (b+\sqrt{\Delta})\frac{B}{2}. \qquad (*)$$

Dado que $b'^2 = b^2 - 4a_1a_2c_0 + 4a_1'a_2'c_0'$, se tiene $b'^2 \equiv \Delta \pmod{a_1'a_2'}$. Entonces para cada una de las ecuaciones (*), podemos sustituir $\sqrt{\Delta}$ por b' y convertirlas en congruencias módulo $a_1'a_2'$. Como los lados izquierdos son todos congruentes con 0 módulo $a_1'a_2'$, entonces debemos de tener que $B \equiv 0 \pmod{a_1'a_2'}$ y es lo que buscabamos. ■

Como una aplicación del lema 1.17 veamos que sucede con el producto de $f_{e_1} = [(1,b,c)]$ y $f_{e_2} = [(1,b',c')]$. Por el lema 1.16, existen $g_1 = (1,B,c_1) \in f_{e_1}$ y $g_2 = (1,B,c_2) \in f_{e_2}$. Por el lema 1.17 existe $c_0 \in \mathbf{Z}$ tal que $g_1 \sim (1,B,c_0)$ y $g_2 \sim (1,B,c_0)$. Por lo tanto $f_{e_1} = f_{e_2}$.

El anterior comentario nos sugiere la unicidad del "neutro".

EL GRUPO DE CLASES DE FORMAS

El teorema 1.18 nos dice, en esencia, que las clases determinadas por la composición de dos formas individuales no depende de las formas en sí, sino unicamente de las clases a las cuales ellas pertenecen. Hemos llegado precisamente al objetivo principal de este capítulo.

Teorema 1.19. *Bajo la composición de formas* $\mathbf{CLF}_\Delta$ *es un grupo abeliano finito. La identidad del grupo es la clase principal y el inverso de la clase de una forma, es la clase de la forma opuesta.*

Demostración. Sean $f_1 = [f_1]$, $f_2 = [f_2]$, $f_3 = [f_3] \in \mathbf{CLF}_\Delta$ tales que

$$f_1 = (a_1,b,a_2c_0) = (a_1,b,a_3c_0) = (a_1,b,a_2a_3\,c_0'),$$
$$f_2 = (a_2,b,a_1c_0) = (a_2,b,a_3c_0) = (a_2,b,a_1a_3\,c_0'),$$
$$f_3 = (a_3,b,a_1c_0) = (a_3,b,a_2c_0) = (a_3,b,a_1a_2\,c_0').$$

Por definición $f_1 f_2 = [f_1][f_2] \in \mathbf{CLF}_\Delta$.

Ahora

$$\begin{aligned} f_1(f_2f_3) &= (a_1,b,a_2c_0)[(a_2,b,a_3c_0)(a_3,b,a_2c_0)] \\ &= (a_1,b,c_0)(a_2a_3,b,c_0) \\ &= (a_1,b,a_2a_3\,c_0')(a_2a_3,b,a_1\,c_0') \\ &= (a_1a_2a_3,b,c_0'). \end{aligned}$$

y

$$\begin{aligned} (f_1f_2)f_3 &= [(a_1,b,a_2c_0)(a_2,b,a_3c_0)](a_3,b,a_2c_0) \\ &= (a_1a_2,b,c_0)(a_3,b,a_2c_0) \\ &= (a_1a_2,b,a_3\,c_0')(\,a_3,b,\,a_1a_2\,c_0') \\ &= (a_1a_2a_3,b,\,c_0'). \end{aligned}$$

Por lo tanto $f_1(f_2f_3) = (f_1f_2)f_3$.
Recordemos que la forma principal tiene el aspecto $f_c = (1,b,c)$, entonces

$$(1,b,c)(a',b',c') = (1,B,a'c_0)(a',B,c_0) = (a',B,c_0) = (a',b',c').$$

De aquí que $f_e = [(1,b,c)]$ juega el papel del **neutro** en $\mathbf{CLF}_\Delta$. La unicidad del neutro es consecuencia de los lemas 1.16 y 1.17. Aunque tambien se puede deducir de la definición de grupo.

Recordemos nuevamente que la **opuesta** de la forma $f = (a,b,c)$ se define como $f_o = (a,-b,c) = (c,b,a)$. De manera que

$$\begin{aligned} ff_o = (a,b,c)(a,-b,c) &= (a,b,c)(c,b,a) = (a,b,cc_0)(c,b,ac_0) \\ &= (ac,b,c_0) = (ac,b,1) = (1,b,ac). \end{aligned}$$

Así que $f_o = [(a,-b,c)]$ funciona como el inverso de $f = [(a,b,c)]$ bajo dicha composición. La unicidad del inverso puede verse de la siguiente manera:
Supongamos que para $f \in \mathbf{CLF}_\Delta$ existen g, $h \in \mathbf{CLF}_\Delta$ tales que $fg = 1$ y $fh = 1$, entonces $fg = fh$. Como $fg = gf$, tenemos $g(fg) = g(fh)$. Así $(gf)g = (gf)h$. Por lo tanto $g = h$.

De todo lo anterior se sigue que $\mathbf{CLF}_\Delta$ forma un grupo bajo la composición.

Que dicho grupo es abeliano, es evidente a partir de la definición de la composición. Por último, del teorema 1.9 se sigue que dicho grupo es finito. ■

El anterior comentario nos sugiere la unicidad del "neutro".

EL GRUPO DE CLASES DE FORMAS

El teorema 1.18 nos dice, en esencia, que las clases determinadas por la composición de dos formas individuales no depende de las formas en sí, sino unicamente de las clases a las cuales ellas pertenecen. Hemos llegado precisamente al objetivo principal de este capítulo.

Teorema 1.19. *Bajo la composición de formas* $\mathbf{CLF}_\Delta$ *es un grupo abeliano finito. La identidad del grupo es la clase principal y el inverso de la clase de una forma, es la clase de la forma opuesta.*

Demostración. Sean $f_1 = [f_1]$, $f_2 = [f_2]$, $f_3 = [f_3] \in \mathbf{CLF}_\Delta$ tales que

$$f_1 = (a_1,b,a_2c_0) \sim (a_1,b,a_3c_0) \sim (a_1,b,a_2a_3c_0'),$$
$$f_2 = (a_2,b,a_1c_0) \sim (a_2,b,a_3c_0) \sim (a_2,b,a_1a_3c_0'),$$
$$f_3 = (a_3,b,a_1c_0) \sim (a_3,b,a_2c_0) \sim (a_3,b,a_1a_2c_0').$$

Por definición $f_1 f_2 = [f_1][f_2] \in \mathbf{CLF}_\Delta$.

Ahora

$$\begin{aligned} f_1(f_2f_3) &= (a_1,b,a_2c_0)[(a_2,b,a_3c_0)(a_3,b,a_2c_0)] \\ &\sim (a_1,b,c_0)(a_2a_3,b,c_0) \\ &\sim (a_1,b,a_2a_3c_0')(a_2a_3,b,a_1c_0') \\ &\sim (a_1a_2a_3,b,c_0'). \end{aligned}$$

y

$$\begin{aligned} (f_1f_2)f_3 &= [(a_1,b,a_2c_0)(a_2,b,a_3c_0)](a_3,b,a_2c_0) \\ &\sim (a_1a_2,b,c_0)(a_3,b,a_2c_0) \\ &\sim (a_1a_2,b,a_3c_0')(a_3,b,a_1a_2c_0') \\ &\sim (a_1a_2a_3,b,c_0'). \end{aligned}$$

Por lo tanto $f_1(f_2f_3) = (f_1f_2)f_3$.
Recordemos que la forma principal tiene el aspecto $f_e = (1,b,c)$, entonces

$$(1,b,c)(a',b',c') \sim (1,B,a'c_0)(a',B,c_0) \sim (a',B,c_0) \sim (a',b',c').$$

De aquí que $f_e = [(1,b,c)]$ juega el papel del **neutro** en $\mathbf{CLF}_\Delta$. La unicidad del neutro es consecuencia de los lemas 1.16 y 1.17. Aunque tambien se puede deducir de la definición de grupo.
Recordemos nuevamente que la **opuesta** de la forma $f = (a,b,c)$ se define como $f_o = (a,-b,c) \sim (c,b,a)$. De manera que

$$\begin{aligned} ff_o &= (a,b,c)(a,-b,c) \sim (a,b,c)(c,b,a) \sim (a,b,cc_0)(c,b,ac_0) \\ &\sim (ac,b,c_0) \sim (ac,b,1) \sim (1,b,ac). \end{aligned}$$

Así que $f_o = [(a,-b,c)]$ funciona como el inverso de $f = [(a,b,c)]$ bajo dicha composición. La unicidad del inverso puede verse de la siguiente manera:
Supongamos que para $f \in \mathbf{CLF}_\Delta$ existen g, $h \in \mathbf{CLF}_\Delta$ tales que $fg = 1$ y $fh = 1$, entonces $fg = fh$. Como $fg = gf$, tenemos $g(fg) = g(fh)$. Así $(gf)g = (gf)h$. Por lo tanto $g = h$.

De todo lo anterior se sigue que $\mathbf{CLF}_\Delta$ forma un grupo bajo la composición.

Que dicho grupo es abeliano, es evidente a partir de la definición de la composición. Por último, del teorema 1.9 se sigue que dicho grupo es finito. ■

CAPITULO II

EL GRUPO DE CLASES DE IDEALES

Sea $\{\alpha_1,...,\alpha_n\}$ **una base para una extensión finita** K **de** $\mathbf{Q}$. **Se sabe que existen exactamente** n **monomorfismos** $\sigma_j : K \to \mathbf{C}$ **y generalmente a los elementos** $\sigma_j(\alpha)$ **se les llama conjugados de** α. **Definimos el discriminante de una base para** K **sobre** $\mathbf{Q}$ **como**

$$\Delta[\alpha_1,...,\alpha_n] = (det[\sigma_j(\alpha_i)])^2.$$

Si se tuviera otra base $\{\beta_1,...,\beta_n\}$ de K sobre $\mathbf{Q}$, entonces se puede probar que

$$\Delta[\beta_1,...,\beta_n] = \{det(a_{ij})\}^2 \Delta[\alpha_1,...,\alpha_n],$$

donde (a_{ij}) es la matriz asociada al cambio de base.

Recordemos que un **entero algebraico** $\theta \in \mathbf{C}$, es un número algebraico que satisface un polinomio mónico $f(x) \in \mathbf{Z}[x]$ y denotamos al conjunto $\mathbf{E}$ como el conjunto de los enteros algebraicos. Se puede probar y no lo haremos aquí que $\mathbf{E}$ es un anillo (cf. [3] pag 68).

Para cualquier campo K escribimos

$$\mathbf{O}_K = K \cap \mathbf{E},$$

y llamamos a $\mathbf{O}_K$ el **anillo de enteros de** K. Un hecho de importancia es que si tenemos cualquier número $\alpha \in K$, entonces existe $r \in \mathbf{Z}$ con $r \neq 0$, tal que $r\alpha \in \mathbf{O}_K$. De aquí que K se puede ver siempre como una extensión simple de $\mathbf{Q}$ al cual le añadimos un entero algebraico apropiado, es decir $K = \mathbf{Q}(\beta)$, para algún $\beta \in \mathbf{O}_K$. Como en toda la literatura relacionada con teoría de los números algebraicos, llamaremos de aquí en adelante **entero racional** a cualquier elemento de $\mathbf{Z}$ y **entero** a secas a cualquier elemento de $\mathbf{O}_K$. En estos términos es bastante

fácil probar que los únicos enteros **algebraicos** que son números racionales son los enteros racionales, en otras palabras $\mathbf{O}_K \cap \mathbf{Q} = \mathbf{Z}$. Sea $\{\alpha_1,\ldots,\alpha_n\}$ una base entera de $\mathbf{O}_K$. Entonces todo w en $\mathbf{O}_K$ se puede expresar en forma única como

$$w = a_1\alpha_1+\cdots+a_n\alpha_n,$$

con $a_i \in \mathbf{Z}$. Podemos ver que si $\{\alpha_1,\ldots,\alpha_n\}$ es una base para K con $\alpha_i \in \mathbf{O}_K$, entonces $\Delta[\alpha_1,\ldots,\alpha_n] \in \mathbf{Z}$ y es distinto de cero (cf. [3] pag 175). Más aún, una base con las caracteristicas anteriores y de discriminante mínimo en $\mathbf{O}_K$ es una base entera de $\mathbf{O}_K$ y estas siempre existen para cualquier ideal $I \subseteq \mathbf{O}_K$. Es un hecho que cualesquiera dos bases enteras de $\mathbf{O}_K$, tienen el mismo discriminante ya que la matriz de cambio de base es unimodular. A este valor común se le llama **el discriminante** del campo K el cual es un entero racional diferente de cero. Es claro además que campos isomorfos, tienen el mismo discriminante.

Para cualquier $\alpha \in K$ se define la **norma** de α como

$$\mathbf{N}_K(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha),$$

y la **traza** de α como

$$\mathrm{Tr}_K(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha),$$

donde los σ_i, $i = 1,\ldots,n$, son los distintos monomorfismos de K en $\mathbf{C}$. Se abreviará a la norma y a la traza de α como $\mathrm{N}(\alpha)$ y $\mathrm{Tr}(\alpha)$ respectivamente. La norma satisface $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$, para cualquier $\alpha, \beta \in K$ y si $\alpha \in \mathbf{Q}$, entonces $\mathrm{N}(\alpha) = \alpha^n$ y $\mathrm{Tr}(a\alpha+b\beta) = a\mathrm{Tr}(\alpha)+b\mathrm{Tr}(\beta)$ para $a, b \in \mathbf{Q}$.

Sea $K/\mathbf{Q}$ una extensión cuadrática. Entonces si $K = \mathbf{Q}(\alpha)$ para alguna $\alpha \in \mathbf{C}$, se tiene que α es raiz de un polinomio irreducible

$$p(x) = ax^2+bx+c,$$

con $a,\ b,\ c \in \mathbf{Q}$. Podemos suponer sin pérdida de generalidad que $a,\ b,\ c \in \mathbf{Z}$, quitando denominadores si es necesario. Si hacemos $\Delta = b^2 - 4ac$, siempre es posible poner $\Delta = r^2 d$, con $r,\ d \in \mathbf{Z}$ y d libre de cuadrados. Por lo tanto

$$\mathbf{Q}(\alpha) = \mathbf{Q}\left(\frac{-b \pm \sqrt{\Delta}}{2a}\right) = \mathbf{Q}(\sqrt{\Delta}) = \mathbf{Q}(r\sqrt{d}) = \mathbf{Q}(\sqrt{d}).$$

De manera que todos los campos cuadráticos son de la forma $\mathbf{Q}(\sqrt{d})$, donde $d \in \mathbf{Z}$ es libre de cuadrados. Si $\alpha \in \mathbf{Q}(\sqrt{d})$, entonces $\alpha = a + b\sqrt{d}$. Luego los automorfismos de $\mathbf{Q}(\sqrt{d})$ son: $\sigma_1 =$ *identidad* y $\sigma_2 =$ *conjugación*, de modo que

$$\sigma_1(a + b\sqrt{d}) = a + b\sqrt{d},$$
$$\sigma_2(a + b\sqrt{d}) = a - b\sqrt{d}.$$

La norma y la traza de α en un campo cuadrático son bastante fáciles de calcular ya que $N(\alpha) = \alpha\overline{\alpha}$ y $Tr(\alpha) = \alpha + \overline{\alpha}$, donde como siempre $\overline{\alpha}$ es el conjugado de α en K. De manera que

$$N(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d,$$

y

$$Tr(a + b\sqrt{d}) = (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a.$$

Podemos ver que, $\alpha \in \mathbf{O}_K$ si y sólo si $N(\alpha),\ Tr(\alpha) \in \mathbf{Z}$. Esta afirmación es válida sólo en el caso cuadrático. Cuando $[K:\mathbf{Q}] > 2$ se cumple: si $\alpha \in \mathbf{O}_K$, entonces $N(\alpha),\ Tr(\alpha) \in \mathbf{Z}$.

Teorema 2.1. *Sea $d \in \mathbf{Z}$ libre de cuadrados. El anillo de enteros de $\mathbf{Q}(\sqrt{d})$ es:*

$$\mathbf{O}_{\mathbf{Q}(\sqrt{d})} = \begin{cases} \mathbf{Z}(\sqrt{d}) & \text{si } d \equiv 2,3 \pmod 4, \\ \mathbf{Z}(-\frac{1}{2} + \frac{1}{2}\sqrt{d}) & \text{si } d \equiv 1 \pmod 4. \end{cases}$$

Demostración. (cf. [3] pag 189). ■

Por lo anterior, una base para $\mathbf{O}_{\mathbf{Q}(\sqrt{d})}$ es $\{1, \sqrt{d}\}$ si $d \equiv 2$ ó $3 \pmod 4$ ó $\{1, -\frac{1}{2}+\frac{1}{2}\sqrt{d}\}$ si $d \equiv 1 \pmod 4$. Así que el discriminante de cualquier campo cuadrático está dado por:

$$\Delta = \begin{cases} \Delta[1,\sqrt{d}] = 4d & \text{si } d \equiv 2,3 \pmod 4, \\ \Delta[1,-\frac{1}{2}+\frac{1}{2}\sqrt{d}] = d & \text{si } d \equiv 1 \pmod 4. \end{cases}$$

Un campo cuadrático se dice que es **real** si $d > 0$, e **imaginario** si $d < 0$. Nosotros estaremos interesados exclusivamente en los campos imaginarios precisamente para establecer la relación que existe entre las formas cuadráticas binarias con discriminante negativo y ciertos objetos de dichos campos.

IDEALES EN CAMPOS CUADRATICOS

En lo que sigue $\mathbf{K} = \mathbf{Q}(\sqrt{d})$, con $d \in \mathbf{Z}$ libre de cuadrados. Sea $I \subseteq \mathbf{O}_{\mathbf{K}}$ un ideal. Por el teorema 2.1 I tiene a lo más dos generadores pues $[\mathbf{O}_{\mathbf{K}}: I]$ es finito. Supongamos que $I = <\alpha_1,\alpha_2>$. Consideremos $<\overline{\alpha}_1,\overline{\alpha}_2> \subseteq \mathbf{O}_{\mathbf{K}}$ el cual claramente es un ideal, lo denotaremos como $\overline{I}$ y lo llamaremos el **ideal conjugado** de I. Recordemos que un ideal I es un **ideal principal** si $I = <\alpha>$ para algún $\alpha \in \mathbf{O}_{\mathbf{K}}$ y que $<\alpha> = <\beta>$ si y sólo si α y β son asociados. Entonces $<1> = <\alpha>$ si y sólo si α es unidad, pero si un ideal contiene a 1 entonces ese ideal es precisamente todo el anillo $\mathbf{O}_{\mathbf{K}}$, luego $\mathbf{O}_{\mathbf{K}} = <1>$ es llamado el **ideal unidad** ó **ideal identidad**.

Lema 2.2. *Sea $I \subseteq \mathbf{O}_{\mathbf{K}}$ un ideal. Existen $\alpha \in \mathbf{Z}$ y β un entero algebraico tal que $I = <\alpha,\beta>$.*

Demostración. Supongamos que $I = <\alpha_1,\alpha_2>$ con $\alpha_1,\alpha_2 \in \mathbf{O}_{\mathbf{K}}$. Sea $\delta = \sqrt{d} \in \mathbf{Q}(\sqrt{d})$, con $d \in \mathbf{Z}$ libre de cuadrados. Los elementos de $\mathbf{O}_{\mathbf{K}}$ son de la forma $a+b\delta$ donde $a, b \in \mathbf{Z}$. Así $\alpha_1=a_1+b_1\delta$ y $\alpha_2=a_2+b_2\delta$ con $a_1, b_1, a_2, b_2 \in \mathbf{Q}$. Dado que $\alpha_1 x+\alpha_2 y = (a_1+b_1\delta)x + (a_2+b_2\delta)y = (a_1x+a_2y)+(b_1x+b_2y)\delta$, escogemos $x_1, y_1 \in \mathbf{Z}$ para los cuales $b_1x_1+b_2y_1 = 0$ y $a_1x_1+a_2y_1 = a > 0$ sea mínimo. Si $x_2, y_2 \in \mathbf{Z}$ son tales que $g = b_1x_2+b_2y_2 = mcd(b_1,b_2)$ y $b = a_1x_2+a_2y_2$, entonces hacemos $\beta = b+g\delta$ y por lo tanto $I = <a,\beta>$. ■

Sean $I, J \subseteq \mathbf{O}_K$ ideales tales que $I = \langle \alpha_1, \alpha_2 \rangle$ y $J = \langle \beta_1, \beta_2 \rangle$. Recordemos que se define la suma y producto de ideales como:

$$I+J = \{\alpha+\beta : \alpha \in I, \beta \in J\},$$
$$IJ = \{\alpha\beta : \alpha \in I, \beta \in J\}.$$

Es fácil probar que tanto $I+J$ como IJ son ideales de $\mathbf{O}_K$. Podemos ver también que tanto para la suma como para el producto de ideales, se da la conmutatividad y la asociatividad. Como caso especial $\langle\alpha\rangle\langle\beta\rangle = \langle\alpha\beta\rangle$, es decir, el producto de ideales principales es nuevamente un ideal principal.

Decimos que un ideal I divide a un ideal J si existe un ideal L tal que $J = IL$, y como siempre lo escribimos como $I \mid J$. Notemos que $\langle\alpha\rangle \mid \langle\beta\rangle$ si y sólo si $\alpha \mid \beta$.

Como consecuencia de la aritmética que gobierna a los ideales tenemos los siguientes resultados :

Lema 2.3. *Sea $J \subseteq \mathbf{O}_K$. Si existe $\gamma \in \mathbf{O}_K$ diferente de cero tal que $\gamma \mid \alpha$ para todo $\alpha \in J$, entonces $J = \gamma I$ para algún ideal $I \subseteq \mathbf{O}_K$.*

Demostración. Sea $\alpha \in J$. Entonces $\alpha = \gamma a_\alpha$ para algún $a_\alpha \in \mathbf{O}_K$ entonces $a_\alpha = \frac{\alpha}{\gamma} \in \mathbf{O}_K$. Sea $I = \langle a_\alpha \rangle = \left\langle \frac{\alpha}{\gamma} : \alpha \in J \right\rangle$. Es claro entonces que $J = \gamma I$. ■

Lema 2.4. *Si $\gamma I = \gamma J$, para algún $\gamma \in \mathbf{O}_K$ diferente de cero, entonces $I = J$.*

Demostración. Sea $\alpha \in I$ y $\gamma\alpha \in \gamma I = \gamma J$. Entonces existe $\beta \in J$ tal que $\gamma\alpha = \gamma\beta \in J$. Así $\alpha = \beta \in J$. Por lo tanto $I = J$. ■

Es claro que cualquier ideal puede verse como un $\mathbf{O}_K$-submódulo del campo K. Los submódulos de interés que nos dan una estructura de grupo están caracterizados por la siguiente propiedad:

Decimos que un $\mathbf{O}_K$-submódulo J de K es un **ideal fraccional** de $\mathbf{O}_K$ si existe un elemento distinto de cero $\rho \in \mathbf{O}_K$ tal que $\rho J \in \mathbf{O}_K$. En otras palabras $I = \rho J$ es un ideal de $\mathbf{O}_K$ y $J = \rho^{-1} I$; así los ideales fraccionales de $\mathbf{O}_K$ son subconjuntos de K de la forma $\rho^{-1} I$.

Lema 2.5 (Hurwitz) *Sean* $\alpha, \beta \in \mathbf{O}_K$. *Si existe* $g \in \mathbf{Z}$ *tal que* $g \mid N(\alpha)$, $g \mid N(\beta)$ *y* $g \mid Tr(\alpha\overline{\beta})$, *entonces* $g \mid \overline{\alpha}\beta$ *y* $g \mid \alpha\overline{\beta}$.

Demostración. Sea $\sigma = \alpha\overline{\beta}$. Entonces $\sigma \in \mathbf{O}_K$ y satisface la ecuación

$$\sigma^2 - Tr(\sigma)\,\sigma + N(\sigma) = 0.$$

Como $N(\sigma) = N(\alpha)N(\beta)$, entonces $g^2 \mid N(\sigma)$ y $g \mid Tr(\sigma)$. Así $\mu = \frac{\sigma}{g}$ satisface

$$\mu^2 - \frac{Tr(\sigma)}{g}\mu + \frac{N(\sigma)}{g^2} = 0.$$

Por lo tanto $\mu \in \mathbf{O}_K$ y consecuentemente $\overline{\mu} \in \mathbf{O}_K$. ■

Teorema 2.6. *Si* $I \subseteq \mathbf{O}_K$. *es un ideal (diferente del ideal cero), entonces el ideal conjugado* $\overline{I}$ *es tal que*

$$I\overline{I} = \langle \alpha \rangle.$$

Demostración. Supongamos que $I = \langle \alpha, \beta \rangle$ con $\alpha, \beta \in \mathbf{O}_K$, entonces $\overline{I} = \langle \overline{\alpha}, \overline{\beta} \rangle$. De manera que

$$I\overline{I} = \langle \alpha\overline{\alpha},\ \alpha\overline{\beta},\ \beta\overline{\alpha},\ \beta\overline{\beta} \rangle = \langle N(\alpha),\ \alpha\overline{\beta},\ \beta\overline{\alpha},\ N(\beta) \rangle.$$

Hagamos $J = \langle \alpha\overline{\alpha},\ \alpha\overline{\beta} + \beta\overline{\alpha},\ \beta\overline{\beta} \rangle = \langle N(\alpha),\ Tr(\alpha\overline{\beta}),\ N(\beta) \rangle$. Es claro que J es un ideal cuya base consiste en su totalidad de elementos de $\mathbf{Z}$. Por lo tanto $J = \langle g \rangle$ para alguna $g \in \mathbf{Z}$, pero $\langle g \rangle = J \subseteq I\overline{I}$. Por otra parte del lema 2.5 se sigue que como g divide a los generadores de J, entonces también divide a los generadores de $I\overline{I}$. Así $I\overline{I} \subseteq \langle g \rangle$, por lo tanto se tiene

$$\langle g \rangle \subseteq I\overline{I} \subseteq \langle g \rangle,$$

de manera que $I\bar{I} = \langle g \rangle$. ■

Corolario 2.7. *Sean I, J, L ideales de* $\mathbf{O}_K$ *con* $L \neq \langle 0 \rangle$. *Si* $IL = JL$, *entonces* $I = J$.

Demostración. Como $IL = JL$, entonces por el teorema 2.6 podemos multiplicar por $\bar{L}$ ambos miembros de la ecuación y obtener

$$IL\bar{L} = JL\bar{L},$$

o sea

$$I\langle g \rangle = J\langle g \rangle.$$

El resultado se sigue al aplicar el lema 2.4. ■

Teorema 2.8. *Sean I, J ideales de* $\mathbf{O}_K$. $I \mid J$ *si y sólo si* $J \subseteq I$.

Demostración. Si $I \mid J$ entonces existe un ideal L de $\mathbf{O}_K$ tal que $J = IL$. Luego, todo elemento $\beta \in J$ es de la forma $\beta = \sum \alpha_{ij}\alpha_i\gamma_j$ con $\alpha_i \in I$, $\gamma_j \in L$, de manera que $\alpha_i\gamma_j \in I$. Así $\beta \in I$ y por lo tanto $J \subseteq I$. Recíprocamente, supongamos $J \subseteq I$. Por el teorema 2.6 existe $\bar{I}$ tal que $I\bar{I}$ es principal. Entonces $J\bar{I} \subseteq I\bar{I} = \langle \alpha \rangle$. De todo esto se sigue que $J\bar{I}$ es divisible por α, luego por el lema 2.3 $J\bar{I} = \langle \alpha \rangle L$ para algun ideal L. Entonces

$$J\bar{I}I = \langle \alpha \rangle LI = \langle \alpha \rangle IL$$

luego

$$J\langle \alpha \rangle = \langle \alpha \rangle IL = IL\langle \alpha \rangle,$$

remitiendonos al lema 2.4 concluimos que $J = IL$. ■

Corolario 2.9. *Para todo* $\alpha \in I$, $I \mid \alpha$.

Demostración. Dado que $\langle \alpha \rangle \subseteq I$. El resultado se sigue del teorema 2.8. ■

Sea $<0> \neq I \subseteq \mathbf{O}_K$. Puesto que $\mathbf{O}_K/I$ es finito (cf [3] pag 176). Entonces definimos la **norma** de I como

$$N(I) = \left|\mathbf{O}_K/I\right|.$$

Claramente la norma de un ideal es siempre un número natural. Podemos ver también que $N(I) = 1$ si y sólo si $I = \mathbf{O}_K$.
Por otro lado $\mathbf{O}_K$ es de factorización única respecto a sus ideales. Entonces de aquí se deduce que $\left|\mathbf{O}_K/IJ\right| = \left|\mathbf{O}_K/I\right|\left|\mathbf{O}_K/J\right|$ y por lo tanto

$$N(IJ) = N(I)N(J).$$

Se puede probar que si $\{\alpha_1,\alpha_2\}$ es una $\mathbf{Z}$-base de K/Q contenida en I, entonces tenemos (cf. [6] pag 121)

$$N(I) = \sqrt{\frac{\Delta[\alpha_1,\alpha_2]}{\Delta}} = \frac{\left|\alpha_1\overline{\alpha}_2 - \overline{\alpha}_1\alpha_2\right|}{\sqrt{\Delta}}.$$

En particular si $I=<\alpha>$ para algún $\alpha \in \mathbf{O}_K$, entonces $N(I)=N(<\alpha>)=|N(\alpha)|$. La prueba consiste en dar una base entera adecuada contenida en I.
Decimos que un ideal I es **primitivo** si el único ideal fraccional en K que contiene a I es $\mathbf{O}_K$.

EL GRUPO DE CLASES DE IDEALES

Decimos que dos ideales I, J están en la misma clase o que son **equivalentes** si existen ideales principales $<\alpha>$ y $<\beta>$ de $\mathbf{O}_K$ tales que $<\alpha>I = <\beta>J$. Esto lo escribimos como $I \sim J$. Claramente esta relación es de equivalencia. Esta relación induce una partición en clases de ideales de $\mathbf{O}_K$. Sea $I \subseteq \mathbf{O}_K$ un ideal. Entonces denotaremos su clase de equivalencia como :

$$I = [I] = \{ J \subseteq \mathbf{O}_K : J \sim I \}.$$

Definimos el producto de dos clases de ideales como :

$$IJ = [I][J] = [IJ].$$

Es decir, el producto de dos clases de ideales, es la clase del producto de los representantes de cada clase. Trivialmente todos los ideales principales son equivalentes a $<1>\sim \mathbf{O}_K$, el inverso de una clase es la clase de la inversa y es precisamente la clase de $\bar{I}$.
Esta definición es consistente ya que si $I'\sim I$ y $J'\sim J$ entonces $I'J'\sim IJ$. Que $IJ = JI$ se sigue inmediatamente del hecho que $\mathbf{O}_K$ es un anillo conmutativo. Puesto que el producto de ideales es asociativo, entonces $I(JL) = (IJ)L$. La clase de los ideales principales funciona como una identidad, bajo el producto de ideales ya que $<\alpha>I\sim I$.

Lo antes expuesto nos describe un grupo.

Sea $\mathbf{CLI} = \{ [I] : I \text{ es ideal de } \mathbf{O}_K \}$ y sea $\mathbf{CLI}_\Delta$ el conjunto de clases de ideales de un campo de discriminante Δ. Entonces $\mathbf{CLI}_\Delta$ es un grupo abeliano finito (cf [3] pag 178). En general, si $[K:\mathbf{Q}] > 2$, entonces $\bar{I}$ no necesariamente funciona como el inverso de I, sin embargo en el caso cuadrático sí lo es.

Todo lo anterior nos indica que la clase de ideales bajo el producto, tiene estructura de grupo. A este grupo se le llama como es de esperarse **el grupo de clases de ideales** y lo denotaremos como **CLI**. Todo esto lo resumimos en

Teorema 2.10. *Si $K/\mathbf{Q}$ es un campo cuadrático imaginario de discriminante Δ, entonces $\mathbf{CLI}_\Delta$ es un grupo abeliano finito.*

CAPITULO III

EL GRUPO DE CLASES DE FORMAS Y EL GRUPO DE CLASES DE IDEALES DE UN CAMPO CUADRATICO (IMAGINARIO)

BASES ORDENADAS

Esta sección la iniciaremos conviniendo lo siguiente:

$I=\langle\alpha,\beta\rangle$ indica que $\{\alpha,\beta\}$ son generadores de I como O_K-módulo. $I=[\alpha,\beta]$ indica que $\{\alpha,\beta\}$ son generadores de I como $\mathbf{Z}$-módulo, es decir $[\alpha,\beta]$ es una base entera de I. Supongamos que $I=[\alpha,\beta]$.

Hasta ahora no hemos hecho distinción alguna entre las bases $\{\alpha,\beta\}$ y $\{\beta,\alpha\}$. Diremos que la base $\{\alpha,\beta\}$ está **ordenada** si

$$\frac{\Delta[\alpha,\beta]}{\sqrt{\Delta}} = \frac{1}{\sqrt{\Delta}}\begin{vmatrix}\alpha & \beta\\ \overline{\alpha} & \overline{\beta}\end{vmatrix} = \frac{\alpha\overline{\beta}-\overline{\alpha}\beta}{\sqrt{\Delta}} > 0. \tag{3.1α}$$

Si $I=[\alpha,\beta]$ sabemos que $N(I) = \dfrac{|\alpha\overline{\beta}-\overline{\alpha}\beta|}{\sqrt{\Delta}} = \pm\dfrac{\alpha\overline{\beta}-\overline{\alpha}\beta}{\sqrt{\Delta}}$. Si $\dfrac{\alpha\overline{\beta}-\overline{\alpha}\beta}{\sqrt{\Delta}} < 0$, entonces escojemos la base ordenada $\{\beta,\alpha\}$. Así, en lugar de tomar $|\alpha\overline{\beta}-\overline{\alpha}\beta| = N(I)|\sqrt{\Delta}|$, asentamos más fuertemente $\alpha\overline{\beta}-\overline{\alpha}\beta = N(I)\sqrt{\Delta}$. De aquí en adelante sólo consideraremos bases ordenadas.

Supongamos que tenemos dos bases $[\alpha,\beta]$ y $[\gamma,\delta]$ para un ideal I. Luego dichas bases están relacionadas mediante la transformación

$$\left.\begin{aligned}\alpha &= A\gamma + B\delta\\ \beta &= C\gamma + D\delta\end{aligned}\right\} \tag{3.1}$$

donde $A, B, C, D \in \mathbf{Z}$ y $AD-BC = +1$. De todo esto se tiene entonces

$$\begin{vmatrix}\alpha & \beta\\ \overline{\alpha} & \overline{\beta}\end{vmatrix} = \begin{vmatrix}A & B\\ C & D\end{vmatrix}\begin{vmatrix}\gamma & \delta\\ \overline{\gamma} & \overline{\delta}\end{vmatrix}. \tag{3.2}$$

De aquí que ambas bases son equivalentes si y sólo si existe una transformación unimodular para la cual se cumple (3.1) y (3.2).
Sea $\rho \in \mathbf{O}_K$ diferente de cero. El producto de ρ con $I = [\alpha,\beta]$ lo definimos como sigue:

$$\rho I = \rho[\alpha,\beta] = [\rho\alpha,\rho\beta] \tag{3.3}$$

Si calculamos $\frac{\Delta[\rho\alpha,\rho\beta]}{\sqrt{\Delta}}$, obtenemos

$$\frac{\Delta[\rho\alpha,\rho\beta]}{\sqrt{\Delta}} = \frac{1}{\sqrt{\Delta}}\begin{vmatrix}\rho\alpha & \rho\beta\\ \overline{\rho}\overline{\alpha} & \overline{\rho}\overline{\beta}\end{vmatrix} = \frac{\rho\alpha(\overline{\rho}\overline{\beta})-(\overline{\rho}\overline{\alpha})\rho\beta}{\sqrt{\Delta}} = N(\rho)\frac{\alpha\overline{\beta}-\overline{\alpha}\beta}{\sqrt{\Delta}}.$$

CORRESPONDENCIA ENTRE IDEALES Y FORMAS

Para establecer una correspondencia entre las clases de formas y las clase de ideales, recordemos que una forma $f = (a,b,c) \in F^2\mathbf{Z}[x,y]$ es primitiva, si $mcd(a,b,c) = 1$. De igual manera, decimos que un ideal $I = [\alpha,\beta]$ es **primitivo** si el único $\mathbf{O}_K$-módulo en K que lo contiene es $\mathbf{O}_K$.

Teorema 3.1. *Si $I = [\alpha,\beta]$ es un ideal en $\mathbf{O}_K$, entonces*

$$f(x,y) = \frac{1}{N(I)}N(\alpha x+\beta y) = ax^2+bxy+cy^2 \in F_\Delta^2\mathbf{Z}[x,y]. \tag{3.4}$$

Demostración. Por un lado tenemos

$$\begin{aligned} N(\alpha x+\beta y) &= (\alpha x+\beta y)(\overline{\alpha}x+\overline{\beta}y)\\ &= \alpha\overline{\alpha}x^2+(\alpha\overline{\beta}+\overline{\alpha}\beta)x+\beta\overline{\beta}y^2\\ &= N(\alpha)x^2+Tr(\alpha\overline{\beta})xy+N(\beta)y^2, \end{aligned}$$

y como para cualquier $\alpha \in I$, $<\alpha> \subseteq I$, entonces $N(I) \mid N(<\alpha>) = N(\alpha)$. De tal modo que

$$N(I) \mid N(\alpha x+\beta y).$$

Pero $N(I) \mid N(\alpha)$ y $N(I) \mid N(\beta)$, por lo tanto $N(I) \mid Tr(\alpha\overline{\beta})$.

Sean

$$a = \frac{N(\alpha)}{N(I)}, \quad b = \frac{Tr(\alpha\overline{\beta})}{N(I)}, \quad c = \frac{N(\beta)}{N(I)}.$$

Es claro que si hacemos $f(x,y) = ax^2+bxy+cy^2$, entonces $f(x,y)\in F^2\mathbf{Z}[x,y]$. Calculando el discriminante de f tenemos:

$$\begin{aligned}\Delta_f = b^2-4ac &= \left[\frac{Tr(\alpha\overline{\beta})}{N(I)}\right]^2 - 4\frac{N(\alpha)}{N(I)}\frac{N(\beta)}{N(I)} \\ &= \frac{1}{N^2(I)}\left[Tr^2(\alpha\overline{\beta}) - 4N(\alpha\beta)\right] \\ &= \frac{1}{N^2(I)}\left[(\alpha\overline{\beta}+\overline{\alpha}\beta)^2 - 4N(\alpha\beta)\right] \\ &= \frac{1}{N^2(I)}(\alpha\overline{\beta}-\overline{\alpha}\beta)^2 = \Delta.\end{aligned}$$

Por lo tanto $f(x,y)\in F_\Delta^2\mathbf{Z}[x,y]$. ■

La forma definida en (3.5) se dice que **pertenece** al ideal I, con base $[\alpha,\beta]$ y lo escribimos como $f = f[\alpha,\beta] = f(I)$ o bien $I \to f$.

Teorema 3.2. *Sea* $f(x,y) = ax^2+bxy+cy^2\in F_\Delta^2\mathbf{Z}[x,y]$. *Entonces el ideal* $I = \left[\alpha, \frac{b-\sqrt{\Delta}}{2}\right]$ *de* $\mathbf{O}_\Delta$ *es primitivo y* $f(x,y) = \frac{1}{N(I)}N(\alpha x+\beta y)$ *donde* $\alpha = a$ *y* $\beta = \frac{b-\sqrt{\Delta}}{2}$.

Demostración. Dado que $\Delta \equiv b^2 \pmod 4$, entonces $\frac{b^2-\Delta}{4}\in\mathbf{Z}$. Sea $\beta = \frac{b-\sqrt{\Delta}}{2}$, claramente $\beta\in\mathbf{O}_\Delta$ puesto que β satisface la ecuación

$$\beta^2 - b\beta + \frac{b^2-\Delta}{4} = 0.$$

Enseguida, usando (3.1α) vemos que $\frac{\Delta[\alpha,(b-\sqrt{\Delta})/2]}{\Delta} = \frac{a\sqrt{\Delta}}{\sqrt{\Delta}} = a > 0$. Por lo tanto dicha base es ordenada.

Para ver que I es primitivo, notemos que de otra manera existiría $u\in\mathbf{O}_\Delta$ con $u > 1$ tal que $u \mid \alpha$ y $u \mid \beta = \frac{b-\sqrt{\Delta}}{2}$. De manera que u también divide a $\overline{\beta} = \frac{b+\sqrt{\Delta}}{2}$

así que u divide a $\overline{\beta}-\beta=\sqrt{\Delta}$ ó bien $u^2 \mid \Delta$, lo cual contradice el hecho de ser Δ libre de cuadrados.
Finalmente, dado que $N(I)=a$, $N(\alpha)=a^2$, $Tr(\alpha\overline{\beta})=ab$ y $N(\beta)=ac$ podemos hacer referencia al teorema 3.1 y obtenemos la última afirmación. ■

Si $f=(a,b,c)\in F_\Delta^2\mathbf{Z}[x,y]$, e I esta dado por el teorema 3.2 entonces escribimos $I(f)=I(a,b,c)=[\alpha,\beta]$ y decimos que I es el ideal determinado por la forma f, o bien que f nos lleva a I $(f\rightarrow I)$.

Resumimos lo anterior de la siguiente manera: Si comenzamos con una forma primitiva $f=(a,b,c)\in F_\Delta^2\mathbf{Z}[x,y]$, de tal manera que $a>0$ y su discriminante genera una extensión $\mathbf{Q}(\sqrt{\Delta})$. Construimos el ideal $I(a,b,c)$ de base ordenada de acuerdo al teorema 3.2. Luego, a partir de este ideal reconstruimos la forma cuadrática $f'([\alpha,\beta])$ de acuerdo con el teorema 3.1. Entonces, solamente invirtiendo los pasos vemos que $f'=f$.
Por otro lado, si comenzamos con un ideal primitivo $I=[\alpha,\beta]$, construimos a partir de él, la forma cuadrática $f([\alpha,\beta])$ de acuerdo al teorema 3.1, de modo que

$$f([\alpha,\beta])=\frac{N(\alpha)x^2+Tr(\alpha\overline{\beta})xy+N(\beta)y^2}{N(I)}.$$

Si comenzamos con la forma $f([\alpha,\beta])$, obtenemos el ideal I'

$$I'=[\alpha',\beta']=\left[\frac{N(\alpha)}{N(I)},\frac{Tr(\alpha\overline{\beta})-N(I)\sqrt{\Delta}}{N(I)}\right].$$

Como $\Delta<0$, entonces $N(\alpha)>0$ y también $N(I)>0$.

Todo lo anterior nos dice que al menos existe una biyección entre $\mathbf{CLF}_\Delta$ y $\mathbf{CLI}_\Delta$, es decir que a formas equivalentes les corresponden ideales equivalentes y a ideales equivalentes les corresponden formas equivalentes:

Teorema 3.3. *Si f_1, $f_2\in F_\Delta^2\mathbf{Z}[x,y]$, son tales que $f_1=f_2$, $f_1\rightarrow L_1$ y $f_2\rightarrow L_2$, entonces $L_1=L_2$. Inversamente, sean L_1, L_2 ideales de $\mathbf{O}_\omega$ tales que $L_1=L_2$. Si $L_1\rightarrow f_1$ y $L_2\rightarrow f_2$, entonces f_1, $f_2\in F_\Delta^2\mathbf{Z}[x,y]$, y $f_1=f_2$.*

Demostración. Supongamos que $f_1 \sim f_2$, $f_1 \to L_1$ y $f_2 \to L_2$. De acuerdo entonces con el teorema 3.2 tenemos que $L_1(f)=I_1$ y que $L_2(f_2)=I_2$. Sean $I_1=[\alpha_1,\beta_1]$ e $I_2=[\alpha_2,\beta_2]$ las respectivas bases ordenadas y

$$f(x,y) = \frac{1}{N(I_1)} N(\alpha_1 x + \beta_1 y) = \frac{1}{N(I_1)} (\alpha_1 x + \beta_1 y)(\overline{\alpha}_1 x + \overline{\beta}_1 y)$$
$$g(x',y') = \frac{1}{N(I_2)} N(\alpha_2 x' + \beta_2 y') = \frac{1}{N(I_2)} (\alpha_2 x' + \beta_2 y')(\overline{\alpha}_2 x' + \overline{\beta}_2 y'),$$

de donde por (1.9) se tiene que

$$\begin{cases} x' = px + qy \\ y' = rx + sy \end{cases} \tag{3.6}$$

con $p, q, r, s \in \mathbb{Z}$, y $ps - qr = 1$.
Ahora bien, dado que f_1 y f_2 representan al mismo conjunto de números, por ser $f_1 \sim f_2$, así que $f_1(x,y)$ es numéricamente igual a $f_2(x',y')$. Entonces la ecuación $f_1(x,y) = 0$ debe de transformarse en la ecuación $f_2(x',y') = 0$. Luego, como $N(\alpha) = 0$ sólo si $\alpha = 0$, entonces se debe de tener

$$\alpha_1 x + \beta_1 y = 0 \qquad \text{y} \qquad \alpha_2 x' + \beta_2 y' = 0,$$

o sea que

$$\frac{x}{y} = -\frac{\beta_1}{\alpha_1} \qquad \text{y} \qquad \frac{x'}{y'} = -\frac{\beta_2}{\alpha_2}, \tag{3.7}$$

deben de coincidir bajo (3.6) o bien

$$\frac{x}{y} = -\frac{\overline{\beta}_1}{\overline{\alpha}_1} \qquad \text{y} \qquad \frac{x'}{y'} = -\frac{\beta_2}{\alpha_2}, \tag{3.8}$$

coinciden bajo (3.6).
tratando primero con (3.7) obtenemos

$$-\frac{\beta_2}{\alpha_2}=\frac{x'}{y'}=\frac{px+qy}{rx+sy}=\frac{p(x/y)+q}{r(x/y)+s}=\frac{p(-\beta_1/\alpha_1)+q}{r(-\beta_1/\alpha_1)+s}=\frac{-p\beta_1+q\alpha_1}{-r\beta_1+s\alpha_1}.$$

De manera que

$$\frac{\alpha_2}{s\alpha_1-r\beta_1}=\frac{\beta_2}{-q\alpha_1+p\beta_1}=\frac{\lambda}{\mu}.$$

Luego

$$\begin{cases}\mu\alpha_2 = (s\alpha_1-r\beta_1)\lambda,\\ \mu\beta_2 = (-q\alpha_1+p\beta_1)\lambda.\end{cases} \tag{3.9}$$

Tenemos enseguida

$$\mu I_2=[\mu\alpha_2,\mu\beta_2]=[\lambda(s\alpha_1-r\beta_1),\lambda(-q\alpha_1+p\beta_1)]=[s(\lambda\alpha_1)-r(\lambda\beta_1),-q(\lambda\alpha_1)+p(\lambda\beta_1)].$$

Como $ps-qr=1$**, entonces**

$$\mu I_2=[\lambda\alpha_1,\lambda\beta_1]=\lambda I_1.$$

Dado que $I_1=[\alpha_1,\beta_1]$ **e** $I_2=[\alpha_2,\beta_2]$ **son ambas bases ordenadas, así como también lo es** $\mu I_2=[\lambda\alpha_1,\lambda\beta_1]=\lambda I_1$**. De aquí que** $I_1=I_2$**. Por lo tanto** $L_1=L_2$**. Ahora veamos que la alternativa (3.8) es prácticamente imposible. Procedemos de la misma manera que para la alternativa (3.7), es decir**

$$-\frac{\beta_2}{\alpha_2}=\frac{x'}{y'}=\frac{px+qy}{rx+sy}=\frac{p(x/y)+q}{r(x/y)+s}=\frac{p(-\overline{\beta}_1/\overline{\alpha}_1)+q}{r(-\overline{\beta}_1/\overline{\alpha}_1)+s}=\frac{-p\overline{\beta}_1+q\overline{\alpha}_1}{-r\overline{\beta}_1+s\overline{\alpha}_1}.$$

De manera que

$$\frac{\alpha_2}{s\overline{\alpha}_1-r\overline{\beta}_1}=\frac{\beta_2}{-q\overline{\alpha}_1+p\overline{\beta}_1}=\frac{\lambda}{\mu}.$$

Luego

$$\begin{cases}\mu\alpha_2 = (s\overline{\alpha}_1-r\overline{\beta}_1)\lambda,\\ \mu\beta_2 = (-q\overline{\alpha}_1+p\overline{\beta}_1)\lambda.\end{cases} \tag{3.9α}$$

De lo cual se tiene en este caso

$$\mu I_2 = [\lambda\overline{\alpha}_1, \lambda\overline{\beta}_1] = \lambda \bar{I}_1.$$

Lo cual es imposible; puesto que la base para $\bar{I}_1$ no es ordenada.

Para la demostración en el sentido opuesto, veamos que si el ideal I tiene bases ordenadas $I = [\alpha_1,\beta_1] = [\alpha_2,\beta_2]$, se sigue del teorema 3.1 que $f_1([\alpha_1,\beta_1]) = f_1([\alpha_2,\beta_2])$. Entonces

$$\begin{cases} \alpha_2 = p\alpha_1 + q\beta_1 \\ \beta_2 = r\alpha_1 + s\beta_1 \end{cases} \tag{3.10}$$

donde $ps - rq = 1$. De modo que

$$\alpha_2 x + \beta_2 y = \alpha_1(px+ry) + \beta_1(qx+sy),$$

así que por (3.5) $f_2(x',y') = f_1(px+ry, qx+sy)$ o sea que $f_1([\alpha_1,\beta_1]) = f_2([\alpha_2,\beta_2])$. Finalmente, sean los ideales L_1 y L_2 tales que $L_1 = L_2$ o bien $\mu L_2 = \lambda L_2$, para algunos μ, $\lambda \in \mathbf{O}_K$. Dado que la base sólo afecta a f_1 dentro de una clase de equivalencia, se tiene que

$$\mu[\alpha_1,\beta_1] = \lambda[\alpha_2,\beta_2],$$

de manera que según el teorema 3.1

$$f_1([\alpha_1,\beta_1]) = f_1([\alpha_2,\beta_2]). \qquad \blacksquare$$

Una forma alternativa de leer el teorema anterior es la siguiente:

Teorema 3.4. *Existe una biyección entre* $\mathbf{CLF}_\Delta$ y $\mathbf{CLI}_\Delta$.

Demostración. Sea $\mathrm{H} : \mathbf{CLI}_\Delta \rightarrow \mathbf{CLF}_\Delta$ definida por

$$\mathbf{H}(I) = \frac{1}{\mathbf{N}(I)}\mathbf{N}(\alpha x + \beta y) = \frac{\mathbf{N}(\alpha)x^2 + \mathbf{Tr}(\alpha\bar{\beta})xy + \mathbf{N}(\beta)y^2}{\mathbf{N}(I)},$$

donde $I \in [I]$, $\{\alpha,\beta\}$ es una base entera ordenada contenida en I.
Afirmamos que H está bien definida; si tenemos un ideal $J \in [I]$ entonces $I \sim J$. Así que $\mu I = \lambda J$. Luego

$$\mathbf{H}(\mu I) = \frac{1}{\mathbf{N}(\mu I)}\mathbf{N}(\mu\alpha x + \mu\beta y) = \frac{1}{\mathbf{N}(\mu)\mathbf{N}(I)}\mathbf{N}(\mu(\alpha x + \beta y))$$
$$= \frac{1}{\mathbf{N}(\mu)\mathbf{N}(I)}\mathbf{N}(\mu)\mathbf{N}(\alpha x + \beta y) = \frac{1}{\mathbf{N}(I)}\mathbf{N}(\alpha x + \beta y) = \mathbf{H}(I).$$

De la misma manera se puede ver que $\mathbf{H}(\lambda J) = \mathbf{H}(J)$.
Pero como $\mu I = \lambda J$, entonces $\mathbf{H}(\mu I) = \mathbf{H}(\lambda J)$ y por lo tanto $\mathbf{H}(I) = \mathbf{H}(J)$. Así que H está bien definida.
H es suprayectiva por el teorema 3.2 y la inyectividad se sigue del teorema 3.3; puesto que para ideales L_1 y L_2 tales que $\mathbf{H}(L_1) \sim \mathbf{H}(L_2)$, se tiene $L_1 \sim L_2$. Por lo tanto H es biyectiva. ■

CLASES DE IDEALES Y CLASES DE FORMAS

Nos gustaría ir un poco más allá que simplemente conformarnos con una simple biyección. Es decir, quisieramos saber bajo qué condiciones la función H definida en el teorema anterior es un **homomorfismo**, o sea que, si tenemos las clases de ideales $[I]$ y $[J]$ en $\mathbf{CLI}_\Delta$, tales que $\mathbf{H}(I) = f$ y $\mathbf{H}(J) = g$, entonces $\mathbf{H}(IJ) = \mathbf{H}(I)\mathbf{H}(J)$.
Por los lemas 1.16 y 1.17 sabemos que si $[f]$, $[g] \in \mathbf{CLF}_\Delta$, entonces podemos encontrar $f_1 \in [f]$ y $f_2 \in [g]$ tales que

$$f_1(x,y) = a_1x^2 + bxy + a_2c_0y^2$$
$$f_2(x,y) = a_2x^2 + bxy + a_1c_0y^2$$

y $mcd(a_1,a_2) = 1$. Escribimos $f_1 = (a_1,b,a_2c_0)$ y $f_2 = (a_2,b,a_1c_0)$. Recordemos que

$$f_1 f_2 = (a_1 a_2, b, c_0).$$

Pues bien, sea H como en el teorema 3.4, por suprayectividad, f_1 es la imagen bajo H (por el teorema 3.2) del ideal $I_1 = [a_1, \lambda]$, donde $\lambda = \frac{b - \sqrt{\Delta}}{2} \in \mathbf{O_K}$. De manera analoga f_2 es la imagen bajo H de $I_2 = [a_2, \lambda]$.
Observemos que

$$\lambda^2 = \frac{1}{4}\left(b^2 - 2b\sqrt{\Delta} + b^2 - 4a_1a_2c_0\right) = b\lambda - a_1a_2c_0. \qquad (3.11)$$

Luego si $\alpha_1 \in I_1$ y $\alpha_2 \in I_2$, se debe de tener

$$\alpha_1 = a_1x_1 + \lambda y_1$$
$$\alpha_2 = a_2x_2 + \lambda y_2,$$

con $x_1, x_2, y_1, y_2 \in \mathbf{Z}$. De manera que

$$\alpha_1\alpha_2 = (a_1x_1 + \lambda y_1)(a_2x_2 + \lambda y_2) = a_1a_2x_1x_2 + \lambda(a_1x_1y_2 + a_2y_1x_2) + \lambda^2 y_1y_2.$$

Pero de la ecuación (3.11) se tiene que $\lambda^2 = b\lambda - a_1a_2c_0$, así que

$$\begin{aligned}\alpha_1\alpha_2 = (a_1x_1 + \lambda y_1)(a_2x_2 + \lambda y_2) &= a_1a_2x_1x_2 + \lambda(a_1x_1y_2 + a_2y_1x_2) + (b\lambda - a_1a_2c_0)y_1y_2 \\ &= a_1a_2(x_1x_2 - c_0y_1y_2) + \lambda(a_1x_1y_2 + a_2y_1x_2 + by_1y_2) \\ &= a_1a_2x_3 + \lambda y_3,\end{aligned}$$

donde

$$x_3 = x_1x_2 - c_0y_1y_2$$
$$y_3 = a_1x_1y_2 + a_2y_1x_2 + by_1y_2.$$

Entonces $\alpha_1\alpha_2 \in [a_1a_2, \lambda] = I_3$, y por lo tanto $I_1I_2 \subseteq I_3$.

Ahora bien, dado que $a_1a_2 \in I_1I_2$ y $a_1\lambda$, $a_2\lambda \in I_1I_2$ y $\mathbf{mcd}(a_1, a_2) = 1$, entonces $\lambda \in I_1I_2$ y por lo tanto cualquier combinación lineal de a_1a_2 y λ, también es un elemento de I_1I_2 y , así que $I_3 \subseteq I_1I_2$, por lo tanto $I_1I_2 = I_3$, o al menos pertenecen a la misma clase.

Si aplicamos H a I_3, tenemos

$$\begin{aligned} \mathrm{H}(I_3) = f_3 &= a_1a_2x_3^2 + bx_3y_3 + c_0y_3^2 \\ &= (a_1x_1^2 + bx_1y_1 + a_2c_0y_1^2)(a_2x_2^2 + bx_2y_2 + a_1c_0y_2^2) \\ &= \mathrm{H}(I_1)\mathrm{H}(I_2). \end{aligned}$$

Por lo tanto $\mathrm{H}(I_1I_2) = \mathrm{H}(I_1)\mathrm{H}(I_2)$.

De esta manera hemos probado

Teorema 3.5. $\mathbf{CLF}_\Delta \equiv \mathbf{CLI}_\Delta$.

BIBLIOGRAFIA

[1] D. A. Buell, *Binary Quadratic Forms, Classical Theory and Modern Computations,* Springer - New York, 1989.

[2] E. Hecke, *Lectures on the Theory of Algebraic Numbers,* Springer-Verlag New York, 1981.

[3] K. Ireland & M. Rossen, *A Classical Introduction to Modern Number Theory,* G.T.M. 84, Springer-Verlag, 1982.

[4] G. B. Mathews, *Theory of Numbers,* Chelsea, New York.

[5] I. Niven y H. Zuckerman, *Introducción a la teoría de los números,* Limusa, 1985.

[6] I. Stewart & D. Tall, *Algebraic Number Theory,* John Wiley & Sons, New York.