ÓRDENES Y FORMAS CUADRÁTICAS

CLAUDIO BRAVO

Esta sección tiene por objetivo principal demostrar un resultado el cual relaciona formas cuadráticas primitivas definidas positivas y órdenes en cuerpos cuadráticos imaginarios. Recordemos que $C(D)$ denota el conjunto de clases de formas cuadráticas primitivas definidas positivas de discriminante D. Análogamente $C(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$ denota al grupo de clases de ideales del orden cuadrático $\mathcal{O}$. El teorema principal de esta exposición es el siguiente:

Teorema 0.1. *Sea $\mathcal{O}$ el orden de discriminante $D < 0$ en el cuerpo cuadrático imaginario $K = \mathbb{Q}(\sqrt{D})$.*

(I) *Si $f(x,y) = ax^2 + bxy + cy^2$ es una forma cuadrática primitiva definida positiva de discriminante D, entonces $[a, (-b + \sqrt{D})/2]$ es un ideal propio de $\mathcal{O}$.*

(II) *La función ϕ que asigna a $f(x,y)$ el ideal $[a, (-b + \sqrt{D})/2]$ induce un isomorfismo entre $C(D)$ y $C(\mathcal{O})$. Luego el orden de $C(\mathcal{O})$ es igual al número de clase $h(D)$.*

(III) *Un entero positivo m es representado por la forma cuadrática $f(x,y)$ si y solamente si m es la norma $N(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}|$ de un ideal $\mathfrak{a}$ en la clase de $\phi(f(x,y))$.*

Ejemplo 0.2. La afirmación (II) **no** vale para cuerpos cuadráticos reales. En efecto, sea $K = \mathbb{Q}(\sqrt{3})$. Entonces $\mathcal{O}_K = \mathbb{Z}[\sqrt{3}]$ es un DFU, luego un DIP. Por ende $C(\mathcal{O}_K) = \{1\}$. No obstante $\pm(x^2 - 3y^2) = \pm N(x + y\sqrt{3})$ no son equivalentes. Por ende $C(D) \neq \{1\}$.

Demostración: Dividimos esta demostración en pequeñas subsecciones. □

0.1. Generalidades. Sea $f(x,y) = ax^2 + bxy + cy^2$ como en el teorema. Las raíces de $f(x,1)$ son complejas, pues $D = b^2 - 4ac < 0$. Luego existe una única τ raíz de $f(x,1)$ en el conjunto $\mathfrak{h} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$. Llamaremos a τ la raíz de $f(x,y)$. Como $a > 0$, se tiene que $\tau = \frac{-b+\sqrt{D}}{2a}$. Luego $[a, (-b + \sqrt{D})/2] = [a, a\tau] = a[1, \tau]$, con $\tau \in K$.

0.2. Demostración de (I). Recordemos que el Lemma 2.12 de la sesión 3 nos dice que $[1, \tau]$ es un ideal fraccionario propio del orden $\mathcal{O}' = [1, a\tau]$. Luego $a[1, \tau]$ es un ideal propio contenido en $\mathcal{O}'$, pues cada uno de los generadores $a, a\tau$ es un elemento de $\mathcal{O}'$. Si $f = [\mathcal{O}_K : \mathcal{O}]$ es el conductor de $\mathcal{O}$ y d_K es el discriminante de K entonces, por lo visto en la definición 1.7 de la sesión 3, tenemos que $D = f^2 d_K$. Por ende

$$a\tau = \frac{-b + \sqrt{D}}{2} = \frac{-b + f\sqrt{d_K}}{2} = -\frac{b + fd_K}{2} + f\frac{d_K + \sqrt{d_K}}{2} = -\frac{b + fd_K}{2} + fw_K, \tag{0.1}$$

donde $\mathcal{O}_K = [1, w_K]$ (ver Teorema 1.3 de la sesión 3). Como $f^2 d_K = D = b^2 - 4ac$, si reducimos módulo 2 tenemos que $fd_K \equiv f^2 d_K \equiv b^2 \equiv b (\mathrm{mod}\ 2)$. Luego $\frac{b+fd_K}{2} \in \mathbb{Z}$. Se sigue que $[1, a\tau] = [1, fw_K]$. Dado que en la Proposición 1.5 de la sesión 3 se demostró que $\mathcal{O} = [1, fw_K]$, deducimos $\mathcal{O}' = \mathcal{O}$. Concluimos que $[a, (-b + \sqrt{D})/2]$ es un ideal propio de $\mathcal{O}$.

0.3. Equivalencias para (II). Sean $f(x,y)$ y $g(x,y)$ dos formas cuadráticas de discriminante D, y sean τ, τ' sus respectivas raíces. Probaremos que las siguientes afirmaciones son equivalentes

(1) $f(x,y)$ y $g(x,y)$ son equivalentes,

(2) $\tau' = \frac{p\tau+q}{r\tau+s}$, con $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.

(3) $[1, \tau] = \lambda[1, \tau']$, con $\lambda \in K^*$.

Para demostrar estas equivalencias haremos uso del siguiente lema técnico.

Lema 0.3. *Sea $f(x,y) = ax^2 + bxy + cy^2$ una forma cuadrática con coeficientes enteros. Sea τ una raíz de $f(x,1)$. Entonces:*

(a) *$f(x,y)$ es definida positiva si y solamente si $a > 0$ y $\tau \notin \mathbb{R}$.*

(b) *Cuando $f(x,y)$ es definida positiva y $mcd(a,b,c) = 1$, el discriminante de $f(x,y)$ es igual al discriminante del orden $\mathcal{O} = [1, a\tau]$.*

(c) *Dos formas cuadráticas primitivas definidas positivas de igual discriminante $D < 0$ e igual raíz son iguales.*

Demostración: Para demostar el item (a) note que $4af(x,y) = (2ax+by)^2 - Dy^2$. Si $a = 0$, se tiene que $f(1,0) = 0$ y por ende la forma cuadrática $f(x,y)$ no es definida positiva. Por otro lado, si $a \neq 0$, se tiene que $f(x,0) = ax^2$ y $f(\frac{-by}{2a}, y) = -\frac{Dy^2}{4a}$. Estas dos últimas igualdades nos permiten concluir que $f(x,y)$ es definida positiva si y solamente si $a > 0$ y $D < 0$. Note que la segunda condición es equivalente a que $\tau \notin \mathbb{R}$ por definición de τ.

La afirmación (b) se demuestra por un cálculo directo. En efecto, se sigue de la Proposición 1.8 de la charla 3, que el discriminante $D(\mathcal{O})$ del orden cuadrático $\mathcal{O} = [1, a\tau]$ es

$$D(\mathcal{O}) = \left(\det \begin{pmatrix} 1 & a\tau \\ 1 & a\overline{\tau} \end{pmatrix}\right)^2.$$

Es decir $D(\mathcal{O}) = a^2(\tau - \overline{\tau})^2 = a^2(\tau^2 - 2\tau\overline{\tau} - \overline{\tau}^2) = -ab(\tau + \overline{\tau}) - 4ac = b^2 - 4c = D$, dado que $a\tau\overline{\tau} = aN(\tau) = c$ y $a(\tau + \overline{\tau}) = a\mathrm{tr}(\tau) = -b$. En lo que sigue denotamos por D tanto al discriminante de la forma cuadrática $f(x,y)$ como al discriminante del orden $\mathcal{O}$.

Finalmente demostramos la afirmación (c). Sean $f(x,y)$ y $g(x,y)$ dos formas cuadráticas primitivas definidas positivas de igual discriminante $D < 0$, y sean τ, τ' sus raíces respectivas. Podemos escribir $f(x,y)$ como $f(x,y) = y^2 f(\frac{x}{y}, 1) = ay^2(\frac{x}{y} - \tau)(\frac{x}{y} - \overline{\tau})$. Por lo tanto, si $\tau = \tau'$, obtenemos que $f(x,y) = ay^2(\frac{x}{y} - \tau')(\frac{x}{y} - \overline{\tau}') = \frac{a}{a'}g(x,y)$, de donde se deduce que $b = \frac{a}{a'}b'$ y $c = \frac{a}{a'}c'$. Las dos igualdades anteriores implican que el discriminante de $g(x,y)$ es $\frac{a^2}{a'^2}D$. Concluimos que $\frac{a}{a'} \in \{1, -1\}$. Como $a, a' > 0$ concluimos que $a = a'$, de donde se sigue que $f(x,y) = g(x,y)$. □

Usando el lema anterior demostramos (1) si y solamente si (2). Asuma que $f(x,y) = g(px+qy, rx+sy)$, con p, q, r, s como en (2). Entonces $0 = f(\tau, 1) = g(p\tau+q, r\tau+s) = (r\tau+s)^2 g((p\tau+q)/(r\tau+s), 1)$. Por otro lado es sabido, de un primer curso de variable compleja, que

$$\mathrm{Im}\left(\frac{p\tau+q}{r\tau+s}\right) = \det \begin{pmatrix} p & q \\ r & s \end{pmatrix} |r\tau+s|^{-2}\mathrm{Im}(\tau). \tag{0.2}$$

En nuestro caso, dicho número es igual a $|r\tau+s|^{-2}\mathrm{Im}(\tau) > 0$. Por la unicidad de τ' concluimos (2). Inversamente, supongamos que se cumple (2). Entonces por los cálculos anteriores $f(x,y)$ y $g(px+qy, rx+sy)$ tienen la misma raíz. Empleando el item (c) del Lema 0.3 deducimos la identidad (2). Con esto concluimos la primera equivalencia.

Demostremos ahora (2) si y solamente si (3). Asumamos (2) y consideremos $\lambda = r\tau+s \in K^*$. Entonces $\lambda[1,\tau'] = (r\tau+s)[1, (p\tau+q)/(r\tau+s)] = [r.\tau+s.1, p.\tau+q.1]$. Note que $[1,\tau] \supset [r\tau+s, p\tau+q]$. Si llamamos $x = r.\tau+s.1$ e $y = p.\tau+q.1$ entonces, por el mismo argumento dado anteriormente, obtenemos $[r.\tau+s.1, p.\tau+q.1] \supset [-r.x+p.y, s.x+(-q).y]$. De un cálculo directo se deduce que $[-r.x+p.y, s.x+(-q).y] = [1,\tau]$. Concluimos que $\lambda[1,\tau'] = [1,\tau]$. Inversamente, supongamos válida la afirmación (3), es decir supongamos que $[1,\tau] = [\lambda, \lambda\tau']$, para algún $\lambda \in K^*$. Como $\lambda, \lambda\tau' \in [1,\tau]$ existen $p, q, r, s \in \mathbb{Z}$ tales que $\lambda\tau' = p\tau+q$ y $\lambda = r\tau+s$. Recíprocamente, como $1, \tau \in [\lambda, \lambda\tau']$ existen $p', q', r', s' \in \mathbb{Z}$ tales que $\tau = p'\lambda\tau' + q'\lambda$ y $1 = r'\lambda\tau' + s'\lambda$. Reemplazando estas ecuaciones en las condiciones derivadas de la primera contención es sencillo concluir que

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix}\begin{pmatrix} p' & q' \\ r' & s' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Por ende $g = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$. En particular, $\det(g) \in \{\pm 1\}$. Además de las dos primeras condiciones obtenemos que $\tau' = \frac{p\tau+q}{r\tau+s}$. Concluimos a partir de la identidad (0.2) que $\det(g) > 0$ y por ende $g \in \mathrm{SL}_2(\mathbb{Z})$.

0.4. Demostración de (II). Se deduce de la equivalencia entre (1) y (3) en la subsección anterior, que existe una función inyectiva $\psi : C(D) \to C(\mathcal{O})$ definida por $\psi(\overline{f(x,y)}) = \overline{a[1,\tau]}$, donde τ es la raíz de $f(x,1)$ y donde $\overline{(\cdot)}$ denota a la clase respectiva. Note que esta función está bien definida por la afirmación (I) del Teorema 0.1. Demostremos la sobreyectividad. Sea $\mathfrak{a}$ un $\mathcal{O}$-ideal fraccionario. Por lo visto en la Proposición 2.2 de la sesión 3, podemos escribir $\mathfrak{a} = [\alpha, \beta]$, con $\alpha, \beta \in K$. Note que β/α o $\alpha/\beta \in \mathfrak{h}$. Intercambiando α con β de ser necesario, podemos asumir que $\tau = \beta/\alpha \in \mathfrak{h}$. Sea ax^2+bx+c el polinomio minimal de τ sobre $\mathbb{Q}$. Racionalizando y cambiando signos de ser necesario, podemos asumir que $a, b, c \in \mathbb{Z}$, $a > 0$ y $\mathrm{mcd}(a,b,c) = 1$. Entonces, como se muestra en el Lema 0.3, la forma cuadrática $f(x,y) = ax^2+bxy+cy^2$ es primitiva, definida positiva y de discriminante $b^2 - 4ac = D$. Concluimos que $\psi(\overline{f(x,y)}) = \overline{a[1,\tau]} = \overline{[1,\tau]} = \overline{[1,\beta/\alpha]} = \overline{[\alpha,\beta]} = \overline{\mathfrak{a}}$.

0.5. Estructura de grupo en $C(D)$ y $C(\mathcal{O})$. En esta sección entenderemos el significado de la ley de grupo en $C(D)$ en términos de la ley de grupo en $C(\mathcal{O})$. En particular mostraremos que dicha ley de grupo no depende de la elección de los representantes. Este resultado estaba pendiente desde la sesión 2. Enunciemos la fórmula de Dirichlet. Sean $f(x,y) = ax^2+bxy+cy^2$, $g(x,y) = a'x^2+b'xy+c'y^2$ dos formas cuadráticas primitivas definidas positivas de discriminante D y asumamos que $\text{mcd}(a, a', (b+b')/2) = 1$. Entonces la ley de composición entre $f(x,y)$ y $g(x,y)$ es

$$F(x,y) = aa'x^2 + Bxy + \frac{B^2-D}{4aa'}y^2, \tag{0.3}$$

donde B es el único número módulo $2aa'$ que cumple con las siguientes congruencias:

(i) $B \equiv b (\text{mod } 2a)$,
(ii) $B \equiv b' (\text{mod } 2a')$,
(iii) $B^2 \equiv D (\text{mod } 4aa')$.

Usemos la función ψ para demostrar que dos hechos. El primero es que $\overline{F(x,y)}$ no depende de la elección de B, mientras que el segundo es que imagen vía la ley de composición de dos formas cuadráticas equivalentes a $f(x,y)$ y $g(x,y)$ respectivamente es una forma cuadrática equivalente a $F(x,y)$. En efecto, considere los $\mathcal{O}$-ideales "imagen" de f, g y F definidos por $[a, (-b+f\sqrt{d_K})/2]$, $[a', (-b'+f\sqrt{d_K})/2]$ y $[aa', (-B+f\sqrt{d_K})/2]$. Escribimos $\Delta = (-B+f\sqrt{d_K})/2$. Luego, usando las conguencias (i) y (ii), obtenemos que los $\mathcal{O}$-ideales anteriores se escriben como $[a,\Delta]$, $[a',\Delta]$ y $[aa',\Delta]$. Esta última afimación se debe a que $[a, z+n.a] = [a,z]$, para cualquier $n \in \mathbb{Z}$ y $z \in K$. Observe que si reemplazamos B por otro número B' que satisfaga las mismas conguencias, entonces, por el Lema 3.3 de la primera exposición, se tiene que $B = B' + 2naa'$, para algún $n \in \mathbb{Z}$. En particular $\Delta' = (-B'+f\sqrt{d_K})/2$ satisface que $[aa', \Delta'] = [aa', \Delta]$. Dado que ψ es una función bijectiva, concluimos que $\overline{F(x,y)}$ no depende de la elección de B, de donde se sigue la primera afimación. En lo que sigue demostramos el segunda afirmación. En efecto, la invariancia de clases de la ley de composición se traduce, via ψ, en la identidad $\overline{[a,\Delta][a',\Delta]} = \overline{[aa',\Delta]}$ en $C(\mathcal{O})$. Para demostrar esta última igualdad note que

$$\Delta^2 = \frac{B^2 - 2Bf\sqrt{d_K} + f^2 d_K}{4} = \frac{B^2 + D - 2Bf\sqrt{d_K}}{4} \equiv \frac{2B^2 - 2Bf\sqrt{d_K}}{4} \equiv -B\Delta (\text{mod } aa'). \tag{0.4}$$

Luego $[a,\Delta][a',\Delta] = [aa', a\Delta, a'\Delta, \Delta^2] = [aa', a\Delta, a'\Delta, -B\Delta]$. Note que si z divide simultaneamente a los enteros a, a', B, entonces de (i) y (ii) deducimos que z divide a b y b'. Por lo tanto z divide a $\text{mcd}(a, a', (b+b')/2) = 1$. Concluimos que $\text{mcd}(a, a', B) = 1$. Por lo tanto existen $x, y, z \in \mathbb{Z}$ tales que $\Delta = xa\Delta + ya'\Delta - zB\Delta$, de donde $[aa', a\Delta, a'\Delta, -B\Delta] = [aa', \Delta]$. Esto concluye lo afirmado.

Observación 0.4. La ley de composición deducida por Dirichlet no es más que la identidad inducida por la ley de grupos en $C(\mathcal{O})$.

0.6. Demostración de (III). Para demostrar (3) haremos uso de las siguientes propiedades básicas sobre la norma $N(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}|$.

Lema 0.5. *Sea $\mathcal{O}$ un orden cuadrático imaginario, entonces:*

(a) $N(\alpha\mathcal{O}) = N(\alpha)$, *para $\alpha \in \mathcal{O} \setminus \{0\}$. Note que la segunda norma es el cuadrado de la norma compleja.*
(b) $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$, *para cualquiera dos $\mathcal{O}$-ideales propios $\mathfrak{a}$ y $\mathfrak{b}$.*
(c) $\mathfrak{a}\overline{\mathfrak{a}} = N(\mathfrak{a})\mathcal{O}$, *para cualquier $\mathcal{O}$-ideal $\mathfrak{a}$. Note que esta identidad indica que $\overline{\mathfrak{a}}$ es el inverso de $\mathfrak{a}$ en el grupo de clases $C(\mathcal{O})$.*

Demostración: Dado que $\mathcal{O} = [1, a\tau]$, escribimos $\alpha = x + ya\tau$, donde $x, y \in \mathbb{Z}$. Sea $M_\alpha = \begin{pmatrix} x & -ayc \\ y & x - yb \end{pmatrix}$ la matriz asociada a la multiplicación por α sobre el $\mathbb{Z}$-módulo $\mathcal{O}$. Es un hecho, probado normalmente en un curso de Anillos y Módulos, que $|\mathcal{O}/\alpha\mathcal{O}| = \det(M_\alpha)$. Para más detalle vea el Ejercicio 7.15 de [Cox13]. De la igualdad anterior se deduce que $N(\alpha\mathcal{O}) = x^2 - bxy + acy^2 = N(x + ya\tau)$, de donde se sigue la identidad (a). Ahora consideremos un caso especial de la identidad (b) para probar. Supongamos que $\mathfrak{b} = \alpha\mathcal{O}$, con $\alpha \neq 0$. Afirmamos que $N(\alpha\mathfrak{a}) = N(\alpha)N(\mathfrak{a})$. En efecto, tenemos las inclusiones $\alpha\mathfrak{a} \subseteq \alpha\mathcal{O} \subseteq \mathcal{O}$ y usamos la sucesión exacta

$$\{0\} \to \alpha\mathcal{O}/\alpha\mathfrak{a} \to \mathcal{O}/\alpha\mathfrak{a} \to \mathcal{O}/\alpha\mathcal{O} \to \{0\},$$

para demostrar que $|\mathcal{O}/\alpha\mathfrak{a}| = |\mathcal{O}/\alpha\mathcal{O}||\alpha\mathcal{O}/\alpha\mathfrak{a}|$. Como el homomorfismo multiplicación por $\alpha \in K^*$ es un isomorfismo, concluimos la identidad deseada. Para demosotrar las igualdades (b) y (c) analizamos más en detalle la funcion norma. Sea $\mathfrak{a}$ un $\mathcal{O}$-ideal. Como se dijo en 0.4 podemos considerar $\mathfrak{a} = a[1,\tau]$, donde $a\tau^2 + b\tau + c = 0$, $a, b, c \in \mathbb{Z}$ y $\mathrm{mcd}(a,b,c) = 1$. Entonces

$$N(a[1,\tau]) = N([a, a\tau]) = |[1, a\tau]/[a, a\tau]| = |\mathbb{Z}/a\mathbb{Z}| = a. \tag{0.5}$$

Es más, si usamos la igualdad $\alpha\mathfrak{a} = \alpha a[1,\tau]$ obtenemos que $N(a)N(\mathfrak{a}) = N(\alpha)N(a[1,\tau])$. Por el cálculo anterior $N(a[1,\tau]) = a \in \mathbb{Z}$, de manera que la identidad anterior se escribe como $a^2N(\mathfrak{a}) = N(\alpha)a$. Por lo tanto

$$N(\mathfrak{a}) = N(\alpha)/a. \tag{0.6}$$

Por otro lado, en la continuación de la dem. de la Prop. 2.10 de la sesión 3, se demostró que $\mathfrak{a}\overline{\mathfrak{a}} = (N(\alpha)/a)\mathcal{O}$, de donde se sigue la identidad (c). Finalmente demostramos la identidad (b). En efecto, a partir de (c), se deduce

$$N(\mathfrak{ab})\mathcal{O} = \mathfrak{ab}\overline{\mathfrak{ab}} = N(\mathfrak{a})N(\mathfrak{b})\mathcal{O}.$$

Por lo tanto $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})u$, donde $u \in \mathcal{O}^* \cap \mathbb{Z}_{>0}$. Concluimos que $u = 1$, de donde se sigue (b). □

Comenzamos ahora con la demostración de la afirmación (3) del Teorema 0.1. En efecto, si m es representado por $f(x,y)$, entonces $m = d^2a$, donde a es propiamente representado por $f(x,y)$. Se sigue del Lema 3.4 de la primera sesión, que podemos asumir que $f(x,y) = ax^2 + bxy + cy^2$, al cambiar $f(x,y)$ por una forma equivalente de ser necesario. Entonces $\psi(\overline{f(x,y)})$ es la clase del ideal $\mathfrak{a} = a[1,\tau]$, cuya norma es $N(\mathfrak{a}) = |[1,a\tau]/[a,a\tau]| = a$, como se mostró en la identidad (0.5). Luego $N(d\mathfrak{a}) = d^2a = m$. Por lo tanto m es representado por la norma del ideal $d\mathfrak{a}$ el cual pertenece a la clase de $\phi(f(x,y))$.

Demostremos la propiedad recíproca. Asumamos que $N(\mathfrak{a}) = m$. Como se dijo en 0.4 y en el lema anterior, podemos considerar $\mathfrak{a} = \alpha[1,\tau]$, donde $a\tau^2+b\tau+c = 0$, $a,b,c \in \mathbb{Z}$ y $\mathrm{mcd}(a,b,c) = 1$. Es más, cambiando los signos de a y τ de ser necesario, podemos asumir que $a > 0$ y $\tau \in \mathfrak{h}$. Entonces $f(x,y) = ax^2 + bxy + cy^2$ es una forma cuadrática primitiva definida positiva tal que $\psi(\overline{f(x,y)}) = \overline{\mathfrak{a}} \in C(\mathcal{O})$. Debemos probar que $f(x,y)$ representa a m. Como muestra la igualdad (0.6) tenemos que $N(\mathfrak{a}) = N(\alpha)/a$. Por otro lado, como $\mathfrak{a} = \alpha[1,\tau] \subset \mathcal{O} = [1, a\tau]$, tenemos que existen $p,q,r,s \in \mathbb{Z}$ tales que $\alpha = p + qa\tau$ y $\alpha\tau = r + sa\tau$. Como $(p+qa\tau)\tau = r + sa\tau$ y $a\tau^2 = -b\tau - c$, obtenemos que $p = as + bq$. Por definición de $\mathfrak{a}$ y de la norma compleja

$$m = N(\mathfrak{a}) = N(\alpha)/a = \frac{1}{a}(p^2 - bpq + acq^2), \tag{0.7}$$

pero si se incluye la igualdad $p = as + bq$ en la ecuación anterior se obtiene

$$m = \frac{1}{a}((as+bq)^2 - b(as+bq)q + acq^2) = \frac{1}{a}(a^2s^2 + absq + acq^2) = as^2 + bsq + cq^2 = f(s,q), \tag{0.8}$$

de donde se sigue el resultado.

□

Corolario 0.6. *Sea $\mathcal{O}$ un orden en un cuerpo cuadrático imaginario. Sea M un entero no nulo. Entonces toda clase de ideales en $C(\mathcal{O})$ contiene un $\mathcal{O}$-ideal propio cuya norma es relativamente prima a M.*

Demostración: En el Lemma 3.5 de la primera exposición se demostró que dada una forma cuadrática primitiva $f(x,y)$ y un número entero fijo $M \in \mathbb{Z}\backslash\{0\}$, existe $k \in \mathbb{Z}$ propiamente representado por $f(x,y)$ de manera que $\mathrm{mcd}(M,k) = 1$. Luego, por (II) y (III), se sigue que para toda clase de ideales en $C(\mathcal{O})$ existe un $\mathcal{O}$-ideal propio $\mathfrak{a}$ en dicha clase tal que $N(\mathfrak{a}) = k$. □

Observación 0.7. Sea $\mathfrak{a} = [\alpha, \beta]$ un $\mathcal{O}$-ideal con $\mathrm{Im}(\beta/\alpha) > 0$. Entonces $f_{\mathfrak{a}}(x,y) = \frac{N(\alpha x - \beta y)}{N(\mathfrak{a})}$ es una forma cuadrática. Es más, de esta manera se induce la función inversa de ψ.

Esta afirmación merece una pequeña demostración la cual damos a continuación.
Demostración: Primero desarrollamos en términos de α, β la función $f_{\mathfrak{a}}(x,y)$. En efecto, note que $N(\alpha x - \beta y) = (\alpha x - \beta y)(\overline{\alpha}x - \overline{\beta}y) = N(\alpha)(x - ty)(x - \bar{t}y)$, donde $t = \frac{\beta}{\alpha}$. Por lo tanto $N(\alpha x - \beta y) = N(\alpha)(x^2 - \mathrm{tr}(t)xy + N(t)y^2)$. Concluimos que $f_{\mathfrak{a}}(x,y)$ es una forma cuadrática. Sea $p(x) = ax^2 + bx + c \in \mathbb{Z}[x]$ el polinomio irreducible de $t \in \mathbb{C}$, el cual asumimos que satisface

$\mathrm{mcd}(a,b,c) = 1$. Se sigue del Lema 2.11 de la exposición anterior y del Lemma 0.5(c), que $\frac{N(\alpha)}{a}\mathcal{O} = N(\mathfrak{a})\mathcal{O}$. Deducimos que $\frac{N(\alpha)}{a} = N(\mathfrak{a})$. Por lo tanto:

$$f_{\mathfrak{a}}(x,y) = \frac{N(\alpha)}{N(\mathfrak{a})}\left(x^2 - \mathrm{tr}(t)xy + N(t)y^2\right) = ax^2 + bxy + cy^2,$$

pues $\mathrm{tr}(t) = -b/a$ y $N(t) = c/a$. Por lo tanto $f_{\mathfrak{a}}(x,y)$ es una forma cuadrática primitiva con coeficientes enteros. Además, si escribimos $\tau = x + iy$, donde $x, y \in \mathbb{Q}$ e $y > 0$, deducimos que

$$D = \frac{N(\alpha)^2}{N(\mathfrak{a}^2)}(\mathrm{tr}(t)^2 - 4N(t)) = \frac{N(\alpha)^2}{N(\mathfrak{a}^2)}((t^2 + 2N(t) + \bar{t}^2) - 4N(t)) = \frac{N(\alpha)^2}{N(\mathfrak{a}^2)}((2x^2 - 2y^2) - 2x^2 - 2y^2).$$

Por lo tanto $D = -\frac{4N(\alpha)^2}{N(\mathfrak{a}^2)}y^2$, de donde se sigue que $D < 0$. Dado que siempre $a = N(\alpha)/N(\mathfrak{a})$ es un número entero positivo, por el Lema 0.3 concluimos que $f_{\mathfrak{a}}(x,y)$ es una forma cuadrática primitiva definida positiva con coeficientes enteros.

En lo que resta demostramos que $f_{\mathfrak{a}}(x,y)$ induce el inverso de la función ψ definida en 0.4. Primero demostramos que $\psi(\overline{f_{\mathfrak{a}}(x,y)}) = \overline{\mathfrak{a}}$. En efecto, la raíz de la forma $f_{\mathfrak{a}}(x,y)$ es $\tau = (\mathrm{tr}(t) + 2\sqrt{-y^2})/2 = x + iy$. Por lo tanto $\psi(\overline{f_{\mathfrak{a}}(x,y)}) = \overline{N(\alpha)/N(\mathfrak{a})[1,\tau]} = \overline{[1, x+iy]} = \overline{[1, \beta/\alpha]} = \overline{[\alpha,\beta]}$. Inversamente, sea $f(x,y)$ una forma cuadrática primitiva y definida positiva. Sabemos que $\psi(\overline{f(x,y)}) = \overline{a[1,\tau]}$, donde $\mathfrak{a} = a[1,\tau]$ es un $\mathcal{O}$-ideal. Demostramos que $f_{\mathfrak{a}}(x,y) = f(x,y)$. En efecto $\mathfrak{a} = [a, a\tau]$, de donde $N(\alpha) = a$, y por ende se sigue de un cálculo directo que

$$f_{\mathfrak{a}}(x,y) = \frac{a^2x^2 + abxy + acy^2}{a} = f(x,y).$$

Note que esta última igualdad es entre formas cuadráticas y no solamente entre sus clases módulo equivalencia. □

Agradecimientos: Al profesor Ricardo Menares, a Matías Alvarado, Anibal Aravena y Patricio Pérez por sus valiosos comentarios.

Referencias

[Cox13] David A. Cox. *Primes of the form x^2+ny^2*. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013. Fermat, class field theory, and complex multiplication. 0.6

E-mail address: claudio.bravo.c@ug.uchile.cl