ÓRDENES Y FORMAS CUADRÁTICAS

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

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

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

(2) *La función 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 $C(D)$ es igual al número de clase $h(D)$.*

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

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 $\mathfrak{h} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$. 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 (1).** Recordemos que el Lemma 7.5 mostrado en la sesión anterior, nos dice que $[1,\tau]$ es un ideal fraccionario propio del order $\mathcal{O}' = [1, a\tau]$. 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 sesión anterior, tenemos que $D = f^2 d_K$. Por ende

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

donde $\mathcal{O}_K = [1, w_K]$ (ver primer resultado de la charla anterior). 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 $\frac{b+d\sqrt{d_K}}{2} \in \mathbb{Z}$. Se sigue que $[1, a\tau] = [1, fw_K]$. Dado que en la sesión anterior se demostró que $\mathcal{O} = [1, fw_K]$, escribimos $\mathcal{O}' = \mathcal{O}$. Concluimos que $[a, (-b+\sqrt{D})/2]$ es un ideal propio de $\mathcal{O}$.

0.3. **Equivalencias para (2).** 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 $\lambda \in K^*$.

Partamos demostrando (1) ssi (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 nustro 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. Pero dos formas cuadráticas primitivas definido positivas de igual discriminante y raíz son iguales (ver ejercicio 7.12). Con esto concluimos la primera equivalencia.

Demostremos ahora (2) ssi (3). Asumamos (2) y consideremos $\lambda = r\tau + s \in K^*$. Entonces $\lambda[1,\tau'] = (r\tau+s)[1, (p\tau+q)/(r\tau+s)] = [r.\tau+s.1, p.\tau+s.1]$. Note que $[1,\tau] \supset [r.\tau+s.1, p.\tau+s.1]$. Si llamamos $x = r.\tau+s.1$ e $y = p.\tau+s.1$ entonces $[r.\tau+s.1, p.\tau+s.1] \supset [-r.x+p.y, s.x+(-q).y] =$

$[1,\tau]$. 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 $\lambda = r\tau + s$. Inversamente, 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 $g \in \mathrm{SL}_2(K)$.

0.4. **Demostración de (2).** 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 (1) del Teorema 0.1. Demostremos la sobreyectividad. Sea $\mathfrak{a}$ un $\mathcal{O}$-ideal fraccionario. Por lo visto en la sesión anterior, 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 $f(x,y) = ax^2 + bxy + cy^2$ es una forma cuadrática primitiva definida positiva y de discriminante $b^2 - 4ac = D$. Para el detalle de la positividad y del discriminante véase el ejercicio 7.12. 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 definido positivas de discriminante D y asumamos que $\mathrm{mcd}(a,a',(b+b')/2) = 1$. 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) $B \equiv b \pmod{2a}$,
(ii) $B \equiv b' \pmod{2a'}$,
(iii) $B^2 \equiv D \pmod{4aa'}$.

Usemos la función ψ para demostrar que $\overline{F(x,y)} = \overline{f(x,y)} * \overline{g(x,y)}$. 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 $\Delta = (-B+f\sqrt{d_K})/2$ y usando las conguencias (i) y (ii) obtenemos que los $\mathcal{O}$-ideales anteriores se escriben como $[a,\Delta]$, $[a',\Delta]$ y $[aa',\Delta]$. Estaúltima afimación se debe a que $[a,z+n.a] = [a,z]$, para cualquier $z \in K$. Luego 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

$$\Delta^2 = \frac{B^2 - 2Bf\sqrt{d_K} + f^2 d_K}{4} = \frac{B^2 + D - 2Bf\sqrt{d_K}}{4} \equiv \frac{2B^2 - 2Bf\sqrt{d_K}}{4} \equiv -B\Delta \pmod{aa'}, \tag{0.4}$$

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 $\mathrm{mcd}(a,a',(b+b')/2) = 1$. Concluimos que $\mathrm{mcd}(a,a',B) = 1$. Por lo tanto existen $x,y,z \in \mathbb{Z}$ tales que $\Delta = xa\Delta + ya'\Delta - zB\Delta$, de donde $[aa', a\Delta, a'\Delta, -B\Delta] = [aa',\Delta]$. Con esto se concluye lo pedido.

Observación 0.1. La ley de grupos deducida por Dirichlet no es más que la ley de grupos en $C(\mathcal{O})$. En otras palabras la biyección ψ es un isomorfismo de grupos.

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

Lema 0.1. *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 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 se traduce como $\overline{\mathfrak{a}}$ es el inverso de $\mathfrak{a}$ en el grupo de clases $C(\mathcal{O})$.*

Si m es representado por $f(x, y)$, entonces $m = d^2a$, donde a es propiamente representado por $f(x, y)$. Como se demostró en la clase 2, podemos asumir que $f(x, y) = ax^2 + bxy + cy^2$, cambiando $f(x, y)$ por una forma equivalente de ser necesario. Entonces $\psi(\overline{f(x, y)})$ es la clase de $\mathfrak{a} = a[1, \tau]$. Luego

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

de donde $N(d\mathfrak{a}) = d^2a = m$. Por lo tanto m es representado por la norma de ideales N. Demostremos la propiedad recíproca. Asumamos que $N(\mathfrak{a}) = m$. Por lo demostrado en el lema 7.5, expuesto en la sesión anterior, podemos considerar $\mathfrak{a} = \alpha[1, \tau]$, donde $a\tau^2 + b\tau + c = 0$ y $\text{mcd}(a, b, c) = 1$. 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 deinido positiva tal que $\psi(\overline{f(x, y)}) = \overline{\mathfrak{a}} \in C(\mathcal{O})$. Debemos probar que $f(x, y)$ representa a m. Note que $a\mathfrak{a} = \alpha a[1, \tau]$. Luego por (a) y (b) en el Lemma 0.1 tenemos 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 $N(\mathfrak{a}) = N(\alpha)/a$.

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 normal compleja

$$m = N(\mathfrak{a}) = N(\alpha)/a = \frac{1}{a}(p^2 - bpq + acq^2), \tag{0.6}$$

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

$$m = \frac{1}{a}((as+bq)^2 - b(as+bq)q + acq^2) = \frac{1}{a}(a^2s^2 + absq + acq^2) = as^2 + bsq + cq^2 = f(s, q), \tag{0.7}$$

de donde se sigue el resultado.

Observación 0.2. Sea $\mathfrak{a} = [\alpha, \beta]$ un $\mathcal{O}$-ideal con $\text{Im}(\beta/\alpha) > 0$. Entonces $f(x, y) = \frac{N(\alpha x - \beta y)}{N(\mathfrak{a})}$ es una forma cuadrática. Es un ejercicio probar que de esta manera de induce el inverso de ψ.

Corolario 0.1. *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 la exposición 2 se demostró que para M fijo, toda forma cuadrática primitiva represneta e un número k de manera que $\text{mcd}(m, k) = 1$. Luego, por (2) y (3), 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 $N(\mathfrak{a}) = k$. □

Ejemplo 0.1. La construcción anterior **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 $C(D) \neq \{1\}$.

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