Una breve introducción a las superficies de género 1

Robert Auffarth

Sean $w_1, w_2 \in \mathbb{C}$ linealmente independientes como vectores sobre $\mathbb{R}$. Sea $L = \langle w_1, w_2 \rangle$ el subgrupo generado por ellos. Tomamos el grupo cuociente $X = \mathbb{C}/L$ con la topología cuociente inducida por $\mathbb{C}$ y la proyección natural $\pi : \mathbb{C} \to X$. Se puede ver que localmente π es un homeomorfismo, y localmente π^{-1} se puede tomar como una carta local, para así darle a $\mathbb{C}/L$ una estructura de superficie de Riemann. Esta superficie se llama *toro complejo*.

Notamos que un toro complejo es homeomorfo a $S^1 \times S^1$, y luego tiene género 1.

En estos apuntes estudiaremos algunas propiedades básicas de los toros complejos, y mostraremos que todo toro complejo es isomorfo a una curva elíptica.

1. Toros complejos y sus automorfismos

Sean $L, M \subset \mathbb{C}$ lattices en $\mathbb{C}$, y para $a \in \mathbb{C}$ consideremos la función $T_a : z \mapsto z + a$. Esta función induce una función holomorfa de $\mathbb{C}/L$ en $\mathbb{C}/L$ definida por $z + L \mapsto z + a + L$; es una función holomorfa biyectiva, y luego $T_a \in \mathrm{Aut}(\mathbb{C}/L)$.

Sean ahora $X = \mathbb{C}/L$, $Y = \mathbb{C}/M$ y $f : X \to Y$ holomorfa. Si componemos f con una traslación en Y, podemos suponer que $f(0 + L) = 0 + M$. Por la fórmula de Riemann-Hurwitz, tenemos que

$$\sum_{p \in X} (\mathrm{mult}_p f - 1) = 0,$$

y luego f es no ramificada. Esto implica que f es un cubrimiento en el sentido topológico, y entonces también lo es la composición $f \circ \pi$ (notamos que $\pi : \mathbb{C} \to X$ es el cubrimiento universal de X). Entonces, por la propiedad universal del cubrimiento universal, existe un homeomorfismo $g : \mathbb{C} \to \mathbb{C}$ tal que el siguiente diagrama conmuta:

$$\begin{tikzcd}
\mathbb{C} \arrow[r, "g"] \arrow[d, "\pi"'] \arrow[dr, phantom, "\circlearrowleft"] & \mathbb{C} \arrow[d, "\pi"] \\
X \arrow[r, "f"] & Y
\end{tikzcd}$$

Es fácil ver que g es holomorfa (de hecho es una función entera). Notamos además que para todo $z \in \mathbb{C}$ y para todo $l \in L$, tenemos que

$$\pi(g(z + l)) = f(z + l + L) = f(z + L) = \pi(g(z)),$$

y entonces $g(z + l) - g(z) \in M$ para todo $l \in L$. Así podemos suponer que $g(0) = 0$; si no, trasladamos la imagen de g por $-g(0) \in M$. Este cambio claramente no afecta el diagrama.

Entonces para todo $z \in \mathbb{C}$, $l \in L$, existe un $\omega(z, l) \in M$ tal que $\omega(z, l) = g(z + l) - g(z)$. Como $\mathbb{C}$ es conexo y $g(z + l) - g(z)$ es localmente constante (para l fijo), entonces $\omega(z, l)$ no depende de z. Si derivamos esta expresión con respecto a z, obtenemos que $g'(z + l) = g'(z)$ para todo z, y para todo $l \in L$. Esto implica que los valores que toma g' están dentro de un compacto, y por el Teorema de Louville, necesariamente g' es constante. Por lo tanto, g es lineal, y entonces existe $\gamma \in \mathbb{C}$ tal que $g(z) = \gamma z$ (recordemos que $g(0) = 0$). Notamos además que $\gamma L \subset M$. Tenemos entonces la siguiente proposición:

Proposición 1.1 *Toda función holomorfa $f : X \to Y$ está inducida por una función polinomial de grado uno $g(z) = \gamma z + a$, donde γ es tal que $\gamma L \subset M$. Podemos suponer que $a = 0$ si y solamente si $f(0+L) = 0+M$, y en este caso tenemos que f es un homomorfismo de grupos. Tenemos además que* $\deg f = [M : \gamma L]$, *y en particular f es un isomorfismo si y solamente si $\gamma L = M$.*

Tomemos ahora $f \in \mathrm{Aut}(X)$ con $f(0+L) = 0+L$. Entonces $f(z+L) = \gamma z + L$ para algún $\gamma \in \mathbb{C}$ tal que $\gamma L = L$. Se ve que γ necesariamente es de módulo 1, y de hecho es una raíz de la unidad. Notamos que dos posibilidades para γ son ± 1; de hecho todo toro complejo posee estos dos automorfismos.

Supongamos que γ no es real, y sea $l \in L \backslash \{0\}$ de longitud minimal. Entonces $\langle l, \gamma l \rangle = L$. Tenemos que $\gamma^2 l = a\gamma l + bl$ para algunos $a, b \in \mathbb{Z}$, y simplificando, tenemos que $\gamma^2 - a\gamma - b = 0$. Las únicas raíces de la unidad que satisfacen alguna ecuación cuadrática son las raíces cuartas y las raíces sextas, y entonces podemos suponer que o bien $\gamma = e^{i\pi/3}$ o $\gamma = i$ (si $\gamma = e^{2i\pi/3}$, entonces se puede demostrar que necesariamente el elemento $e^{i\pi/3} l$ también está en L).

En el primer caso, decimos que L es un lattice hexagonal; en el segundo caso decimos que L es un lattice cuadrado.

Sea ahora $\mathrm{Aut}_0(X) := \{f \in \mathrm{Aut}(X) \mid f(0+L) = 0+L\}$. Entonces

(a) Si L es hexagonal, tenemos que $\mathrm{Aut}_0(X) \cong \mathbb{Z}/6\mathbb{Z}$.
(b) Si L es cuadrado, tenemos que $\mathrm{Aut}_0(X) \cong \mathbb{Z}/4\mathbb{Z}$.
(c) Si L no es ni cuadrado ni hexagonal, tenemos que $\mathrm{Aut}_0(X) \cong \mathbb{Z}/2\mathbb{Z}$.

Si denotamos por $T(X) := \{f \mid f \text{ es traslación de } X\}$, entonces notamos que $T(X) \trianglelefteq \mathrm{Aut}(X)$. Además, $T(X) \cap \mathrm{Aut}_0(X) = \{\mathrm{id}\}$ y $T(X)\mathrm{Aut}_0(X) = \mathrm{Aut}(X)$, de donde obtenemos que $\mathrm{Aut}(X) \cong T(X) \rtimes \mathrm{Aut}_0(X) \cong X \rtimes \mathrm{Aut}_0(X)$.

2. Clases de isomorfismo de toros complejos

Se tiene que todo toro complejo es isomorfo a un toro inducido por algún lattice $\langle 1, \tau \rangle$, para τ en el semiplano superior $\mathbb{H}$; llamemos X_τ a tal toro. Queremos ver precisamente cuándo dos toros X_τ y X_σ son isomorfos.

Vimos en la sección anterior que $X_\tau \cong X_\sigma$ si y solamente si existe un $\gamma \in \mathbb{C}$ tal que $\gamma\langle 1, \tau \rangle = \langle 1, \sigma \rangle$. Si esto ocurre, entonces existen $a, b, c, d \in \mathbb{Z}$ tales que $\gamma = c\sigma + d$ y $\gamma\tau = a\sigma + b$. Entonces

$$\begin{pmatrix} \gamma\tau \\ \gamma \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \sigma \\ 1 \end{pmatrix}.$$

Sabemos que como $\gamma\langle 1, \tau \rangle = \langle 1, \sigma \rangle$, entonces tenemos que poder escribir 1 y σ como combinación lineal de γ y $\gamma\tau$ con coeficientes enteros. En tal caso, los coeficientes serían únicos, ya que γ y $\gamma\tau$ forman una base para $\mathbb{C}$ sobre $\mathbb{R}$. Vemos que

$$\frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} \gamma\tau \\ \gamma \end{pmatrix} = \begin{pmatrix} \sigma \\ 1 \end{pmatrix},$$

y como los coeficientes son únicos y pertenecen a $\mathbb{Z}$, necesariamente $ad - bc \in \{\pm 1\}$. Como τ y σ están en el semiplano superior, entonces necesariamente $ad - bc = 1$, y luego la matriz arriba pertenece a $\mathrm{SL}_2(\mathbb{Z})$.

Está claro que estas condiciones son suficientes también (si $\tau = (a\sigma+b)/(c\sigma+d)$ con $ad-bc = 1$, entonces definimos $\gamma := c\sigma + d$, y se tiene lo buscado), y entonces tenemos la siguiente proposición:

Proposición 2.1 *Dos toros complejos X_τ y X_σ son isomorfos si y solamente si existe* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in$ *$SL_2(\mathbb{Z})$ tal que*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \sigma = \tau,$$

donde la acción de $SL_2(\mathbb{Z})$ sobre $\mathbb{H}$ es la natural:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \sigma := \frac{a\sigma + b}{c\sigma + d}.$$

Esta no es una acción fiel (efectiva), pues el núcleo de esta acción corresponde al subgrupo $\{\pm \mathrm{id}\} \trianglelefteq \mathrm{SL}_2(\mathbb{Z})$. Por lo tanto, consideraremos que el grupo que actúa sobre $\mathbb{H}$ es realmente $\mathrm{SL}_2(\mathbb{Z})/\{\pm \mathrm{id}\} = \mathrm{PSL}_2(\mathbb{Z})$. En conclusión, hay una correspondencia $1-1$ entre las clases de isomorfismo de los toros complejos y el espacio $\mathbb{H}/\mathrm{PSL}_2(\mathbb{Z})$.

3. Dominios fundamentales en un toro complejo

Sea $L \subset \mathbb{C}$ un lattice en $\mathbb{C}$, $X = \mathbb{C}/L$ el toro asociado a L, y sea $G = \mathrm{Aut}_0(X)$ como antes. Observamos primero que si T_a es una traslación en X ($z + L \mapsto z + a + L$) de orden finito, entonces la función $\pi_a : X \to X/\langle T_a \rangle$ (la proyección a la superficie cuociente) es no ramificada, y por la fórmula de Riemann-Hurwitz se tiene que

$$0 = \deg \pi_a (2g - 2),$$

donde g es el género de $X/\langle T_a \rangle$. Notamos entonces que necesariamente $g = 1$, y luego el cuociente es homeomorfo a un toro.

Observamos que cuando estudiamos el subgrupo G, sin embargo, es distinto. Por la fórmula de Riemann-Hurwitz tenemos que

$$0 = \deg \pi (2g - 2) + \sum_{p \in X} (\mathrm{mult}_p \pi_G - 1),$$

donde $\pi_G : X \to X/G$ es la proyección natural y g es el género de la superficie cuociente. De otra forma, tenemos que

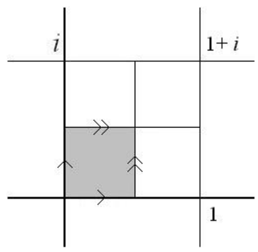
$$(2 - 2g) \deg \pi_G = \sum_{p \in X} (\mathrm{mult}_p \pi_G - 1).$$

Observamos que para todo lattice L, $0 + L$ siempre es un punto de ramificación de π_G (pues $0 + L$ es un punto fijo de todo automorfismo de G, y los otros puntos cerca de 0 son "rotados"). Por lo tanto, $g \neq 1$. Además, $g < 1$, ya que si no, entonces el lado derecho de la igualdad sería negativo. Por lo tanto, $g = 0$, y entonces X/G es homeomorfo a una esfera.

Nos concentraremos ahora en los automorfismos G y en los distintos tipos de lattice mencionados arriba; nuestro análisis se hará por casos:

1. L es un lattice cuadrado.

   En este caso, tenemos que $G = \langle h \rangle \cong \mathbb{Z}/4\mathbb{Z}$, donde $h(z + L) = iz + L$. Notamos que X es isomorfo al toro $\mathbb{C}/\langle 1, i \rangle$, y en tal toro tenemos que un dominio fundamental para la acción de G es de la forma $\{s + ti + \langle 1, i \rangle : s, t \in [0, 1/2]\}$:



En este caso,

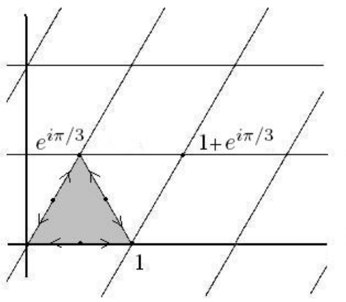
$$\mathrm{mult}_{0+L}\pi_G = \mathrm{mult}_{\frac{i+1}{2}+L}\pi_G = 4$$

$$\mathrm{mult}_{\frac{1}{2}+L}\pi_G = \mathrm{mult}_{\frac{i}{2}+L}\pi_G = 2$$

y $\mathrm{mult}_p\pi_G = 1$ para todo p distinto a estos puntos. Notamos que esta acción induce una función holomorfa $\pi_G : X \to \mathbb{P}^1$ de grado 4.

2. L es hexagonal.

   Tenemos que $G = \langle h \rangle \cong \mathbb{Z}/6\mathbb{Z}$, donde $h(z+L) = e^{\pi i/3}z + L$. Vemos que X es isomorfo al toro inducido por el lattice $\langle e^{\pi i/3}, 1\rangle$, y un dominio fundamental para la acción de G es $\{te^{\pi i/3} + s : s, t \in [0,1], s + t \leq 1\}$:

   Aquí tenemos que

$$\mathrm{mult}_{0+L}\pi_G = 6$$

$$\mathrm{mult}_{\frac{1}{2}+L}\pi_G = \mathrm{mult}_{\frac{e^{\pi i/3}}{2}+L}\pi_G = \mathrm{mult}_{\frac{1+e^{\pi i/3}}{2}+L}\pi_G = 2$$

$$\mathrm{mult}_{(2-\sqrt{3})(1+e^{\pi i/3})+L}\pi_G = \mathrm{mult}_{(2-2\sqrt{3})(1+e^{\pi i/3})+L} = 3$$

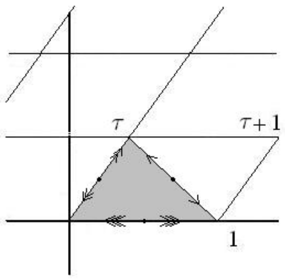
   y $\mathrm{mult}_p\pi_G = 1$ para todo otro $p \in X$. En este caso, notamos que tenemos entonces una función holomorfa $\pi_G : X \to \mathbb{P}^1$ de grado 6.

   Podemos ver que si dejamos que el subgrupo $H = \langle h^2 \rangle$ actúe sobre X, entonces la superficie cuociente también da la esfera, y

$$\mathrm{mult}_{0+L}\pi_H = \mathrm{mult}_{(2-\sqrt{3})(1+e^{\pi i/3})+L}\pi_H = \mathrm{mult}_{(2-2\sqrt{3})(1+e^{\pi i/3})+L}\pi_H = 3$$

   y $\mathrm{mult}_p\pi_H = 1$ para todo otro punto $p \in X$.

3. Si L no es ni cuadrado ni hexagonal, entonces solamente tenemos el automorfismo $z + L \mapsto -z + L$ (todo toro complejo tiene este automorfismo). En este caso, si $L = \langle 1, \tau \rangle$, un dominio fundamental para la acción de G sobre $\mathbb{C}/L$ es $\{s + t\tau : s, t \in [0,1], s + t \leq 1\}$:



En tal caso,

$$\mathrm{mult}_{0+L}\pi_G = \mathrm{mult}_{\frac{1}{2}+L}\pi_G = \mathrm{mult}_{\frac{\tau}{2}+L}\pi_G = \mathrm{mult}_{\frac{1+\tau}{2}+L}\pi_G = 2;$$

así, tenemos una función holomorfa $\pi_G : X \to \mathbb{P}^1$ de grado 2. Notamos que todo toro complejo posee esta función.

4. La función $\wp$ de Weierstrass y las curvas elípticas

Sea $L \subset \mathbb{C}$ un lattice en $\mathbb{C}$. Definimos la función $\wp$ de Weierstrass (que dependerá de L) como la función

$$\wp(z) := \frac{1}{z^2} + \sum_{w \in L\setminus\{0\}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right).$$

Tenemos que $\wp$ es una función meromorfa par en $\mathbb{C}$ con polos dobles en todo punto de L. Notamos que

$$\wp'(z) = -\frac{2}{z^3} - \sum_{w \in L\setminus\{0\}} \frac{2}{(z-w)^3},$$

y es fácil ver que $\wp'$ es una función meromorfa L-periódica. Tomando derivada entonces, notamos que para todo $w \in L$, $\wp(z+w) - \wp(z)$ es constante, y reemplazando $z = -w/2$, obtenemos que $\wp(z+w) - \wp(z) = 0$ para todo $z \in \mathbb{C}$; por lo tanto, $\wp$ también es L-periódica. Esto implica que $\wp$ y $\wp'$ son funciones meromorfas del toro complejo $\mathbb{C}/L$, y de hecho se puede demostrar que $\mathscr{K}(\mathbb{C}/L) = \mathbb{C}(\wp, \wp')$ (donde $\mathscr{K}(\mathbb{C}/L)$ es el cuerpo de las funciones meromorfas en $\mathbb{C}/L$).

Como $\wp$ tiene un polo de orden 2 en todo elemento de L, entonces $\deg \wp = 2$ (cuando vemos a $\wp$ como una función holomorfa $\mathbb{C}/L \to \hat{\mathbb{C}}$).

Sea ahora $G_k(L) := \sum_{w \in L\setminus\{0\}} \frac{1}{w^k}$ para $k \geq 2$ (estas series se llaman series de Eisenstein, y cuando no hay confusión, las denotaremos simplemente por G_k). Se puede demostrar que la serie de Laurent de $\wp$ en 0 es $\wp(z) = \frac{1}{z^2} + \sum_{n \in 2\mathbb{Z}_+} (n+1) G_{n+2} z^n$ para $|z| < \inf\{|w| : w \in L\setminus\{0\}\}$. Tenemos que en 0,

$$\wp(z) = \frac{1}{z^2} + 3G_4 z^2 + 5G_6 z^4 + \mathcal{O}(z^6)$$

y

$$\wp'(z) = -\frac{2}{z^3} + 6G_4 z + 20 G_6 z^3 + \mathcal{O}(z^5).$$

Se tiene que $(\wp'(z))^2$ y $4(\wp(z))^3 - 60G_4\wp(z) - 140G_6$ son de la forma

$$\frac{4}{z^6} - \frac{24G_4}{z^2} - 80G_6 + \mathcal{O}(z^2),$$

y luego su diferencia es una constante; esta constante además debe ser 0. Por lo tanto, tenemos que

$$(\wp'(z))^2 = 4(\wp(z))^3 - 60G_4\wp(z) - 140G_6.$$

Esto significa que $(\wp(z), \wp'(z))$ satisface la ecuación $y^2 = 4x^3 - ax - b$, con $a = 60G_4$ y $b = 140G_6$. Notamos que esta ecuación es no singular si y solamente si el polinomio $p(x) = 4x^3 - ax - b$ tiene 3 raíces distintas.

Proposición 4.1 *El polinomio $p(x) = 4x^3 - ax - b$ tiene 3 raíces distintas.*

Demostración Vemos que si $z_0 + L = -z_0 + L$ (y $z_0 \notin L$), entonces $\wp'(z_0) = \wp'(-z_0) = -\wp'(z_0)$, y luego $\wp'(z_0) = 0$; esto implica que en tal caso, $\wp(z_0)$ es raíz del polinomio $p(x)$. Supongamos que $L = \langle w_1, w_2 \rangle$; entonces notamos que $z_1 = w_1/2, z_2 = w_2/2$ y $z_3 = (w_1 + w_2)/2$ son puntos de $\mathbb{C}$ que cumplen tal igualdad. Además, como $\wp'(z_i) = 0$ para $i = 1, 2, 3$, entonces $\wp$ tiene multiplicidad 2 en cada z_i; esto muestra que necesariamente $\wp(z_i) \neq \wp(z_j)$ para todo $i \neq j$ (ya que $\wp$ es de grado 2), y luego las raíces de $p(x)$ son todas distintas.

□

Esto implica que la ecuación $y^2 = 4x^3 - ax - b$ es no singular, y por lo tanto el conjunto $\tilde{X} = \{(x, y) \in \mathbb{C}^2 : y^2 = p(x)\}$ es una superficie de Riemann.

Si agregamos "un punto en infinito" a $\tilde{X}$, obtenemos una superficie de Riemann compacta X. Mejor dicho, sea X la superficie de Riemann hiperelíptica dada por la ecuación $y^2 = p(x)$. Consideremos además la función $\phi : \mathbb{C}/L \to X$ tal que $z + L \mapsto (\wp(z + L), \wp'(z + L))$. Vemos que ϕ está bien definida.

Sea $(x, y) \in X \backslash \{\infty\}$ tal que $y \neq 0$. Entonces tenemos que existe una vecindad de x en $\mathbb{C}$ tal que $y = y(x)$ es una función holomorfa de x en tal vecindad con $(x, y(x)) \in X$ (Teorema de la Función Implícita), y luego $(x, y) \mapsto x$ es una carta local de X. Notamos que con esta carta, ϕ es holomorfa fuera de 0 y donde $\wp'(z) \neq 0$ (pues $z \mapsto z + L \mapsto (\wp(z), \wp'(z)) \mapsto \wp(z)$ es holomorfa). Si $\wp'(z + L) = 0$, entonces tenemos la carta $(x, y) \mapsto y$; con esta carta tenemos que ϕ en coordenadas locales es de la forma $z \mapsto \wp'(z)$, y esta función es holomorfa. Esto muestra que ϕ es holomorfa en $(\mathbb{C}/L) \backslash \{0 + L\}$.

Cerca de $0+L$, $\wp(z+L)$ es "grande", y vemos que una carta local definida alrededor de $\infty \in X$ es $(x, y) \mapsto y/x^2$. Con estas coordenadas, tenemos que ϕ es localmente de la forma $z \mapsto \wp'(z)/(\wp(z))^2$, y es fácil ver que esta función es holomorfa en 0. Por lo tanto, ϕ es holomorfa.

Como ϕ es una función holomorfa entre superficies de Riemann compactas, entonces es sobreyectiva. Además, por la fórmula de Riemann-Hurwitz, se tiene que ϕ es no ramificada. Notamos que si $z + L \in \mathbb{C}/L$, entonces $\wp(z + L) = \wp(-z + L)$ y $\wp'(-z + L) = -\wp'(z + L)$; esto muestra que como $\wp$ es de grado 2, entonces necesariamente tiene que ser inyectiva.

Concluimos entonces que ϕ es un isomorfismo entre $\mathbb{C}/L$ y X, y por lo tanto todo toro complejo puede verse como una curva elíptica.

Es interesante notar que como todo toro $\mathbb{C}/L$ tiene el automorfismo $z + L \mapsto -z + L$, podemos ver este automorfismo como un automorfismo de la curva elíptica asociada X: $(\wp(z), \wp'(z)) \mapsto (\wp(-z), \wp'(-z)) = (\wp(z), -\wp'(z))$. En otras palabras, corresponde al automorfismo $(x, y) \mapsto (x, -y)$.

De hecho, sabemos que si $\mathbb{C}/L$ y $\mathbb{C}/M$ son dos toros complejos isomorfos, entonces los isomorfismos entre ellos que fijan el 0 son de la forma $f : \mathbb{C}/L \to \mathbb{C}/M$ donde $z + L \mapsto \gamma z + M$, con $\gamma L = M$. Como $\wp_M(\gamma z) = \gamma^{-2}\wp_L(z)$ y $\wp'_M(\gamma z) = \gamma^{-3}\wp'_L(z)$ (donde $\wp_L$ es la función de Weierstrass que corresponde al lattice L, claramente), entonces obtenemos que el isomorfismo correspondiente entre sus curvas elípticas es $(x, y) \mapsto (\gamma^{-2}x, \gamma^{-3}y)$.

Hemos probado entonces la siguiente proposición:

Proposición 4.2 *Dado un toro complejo $\mathbb{C}/L$ para algún lattice L, entonces $\mathbb{C}/L$ es isomorfo (como superficie de Riemann) a una curva elíptica dada por $y^2 = 4x^3 - ax - b$, donde $a = 60\sum_{w\in L\setminus\{0\}} \frac{1}{w^4}$ y $b = 140\sum_{w\in L\setminus\{0\}} \frac{1}{w^6}$.*

Recíprocamente, dada una curva elíptica $y^2 = p(x)$ (no singular, con $\deg p(x) = 3$), sabemos que esta superficie tiene género 1; ¿Es posible determinar si tal superficie proviene de un toro complejo, y si es así, cuál es lattice que lo determina?

Sea $j : \mathbb{H} \to \mathbb{C}$ tal que $j(\tau) = 1728\frac{(60G_4(\tau))^3}{(60G_4(\tau))^3-27(140G_6(\tau))^2}$, donde $G_k(\tau)$ es la serie de Eisenstein que corresponde al lattice $L = \langle 1, \tau\rangle$. Notamos que el denominador de j no se anula, pues éste corresponde a un múltiplo del discriminante del polinomio $p(x)$ definido por L, y como $p(x)$ tiene raíces distintas, entonces su discriminante es no nulo. Se puede demostrar además que j es sobreyectiva.

Sea $y^2 = 4x^3 - a_2x - a_3$ una curva elíptica no singular con $a_2, a_3 \neq 0$ ($p(x)$ no tendría por qué tener esa forma, sin embargo, se puede obtener esta forma a través de un cambio de variables); entonces existe $\tau \in \mathbb{H}$ tal que

$$\frac{(60G_4(\tau))^3}{(60G_4(\tau))^3 - 27(140G_6(\tau))^2} = \frac{a_2^3}{a_2^3 - 27a_3^2}.$$

Entonces

$$\frac{a_2^3}{(60G_4(\tau))^3} = \frac{a_3^2}{(140G_6(\tau))^2}.$$

Sean $w_1 \in \mathbb{C}\setminus\{0\}$, $w_2 = \tau w_1$ y $L = \langle w_1, w_2\rangle$. Entonces se puede ver que $G_4(L) = w_2^{-4}G_4(\tau)$ y $G_6(L) = w_2^{-6}G_6(\tau)$. Luego, debemos elegir w_2 de tal manera que $w_2^{-4} = a_2/(60G_4(\tau))$ y $w_2^{-6} = a_3/(140G_6(\tau))$. Sin embargo, si satisfacemos la primera condición, entonces por la igualdad $\frac{a_2^3}{(60G_4(\tau))^3} = \frac{a_3^2}{(140G_6(\tau))^2}$, obtenemos que $w_2^{-6} = \pm a_3/(140G_6(\tau))$. Si el signo no coincide, entonces reemplazamos w_2 por iw_2. Por lo tanto, encontramos un lattice $L = \langle w_1, w_2\rangle$ tal que la curva elíptica generada por L es precisamente la curva elíptica dada por $y^2 = 4x^3 - a_2x - a_3$. En resumen:

Proposición 4.3 *Dada una curva elíptica (no singular), entonces existe un lattice en $\mathbb{C}$ de tal manera que $\mathbb{C}/L$ es isomorfo a la curva elíptica. Además, tal isomorfismo es el isomorfismo descrito antes usando la función $\wp$ de Weierstrass.*

Si $a_2 = 0$ podemos ver que el lattice buscado es de la forma $\gamma\langle 1, \zeta\rangle$ donde $\gamma \in \mathbb{C}$ y ζ es una raíz cúbica de la unidad. Si $a_3 = 0$, entonces el lattice buscado es de la forma $\gamma\langle 1, i\rangle$ para algún $\gamma \in \mathbb{C}$. Notamos que estos dos casos corresponden a los dos casos excepcionales en cuanto a los automorfismos.

5. X como grupo abeliano

Sea $L \subset \mathbb{C}$ un lattice y $f : \mathbb{C} \to \mathbb{C}$ meromorfa de periodo L. Sea P un paralelógramo fundamental de L (si $L = \langle w_1, w_2\rangle$, digamos que es el paralelógramo generado por w_1 y w_2), y sea $z_0 \in \mathbb{C}$ tal que la traslación $z_0 + \partial P$ no contiene ni ceros ni polos de f. Calculando, obtenemos que

$$\frac{1}{2\pi i}\int_{z_0+\partial P} \frac{zf'(z)}{f(z)}dz = \frac{w_1}{2\pi i}\int_\gamma \frac{f'(z)}{f(z)}dz - \frac{w_2}{2\pi i}\int_\eta \frac{f'(z)}{f(z)}dz,$$

donde $\gamma(t) = z_0 + tw_2$ y $\eta(t) = z_0 + tw_1$ para $t \in [0,1]$. Notamos que podemos subdividir γ (y análogamente η) en curvas γ_i sobre intervalos $[a_i, a_{i+1}]$, $i = 1, \ldots, n$, tales que $f \circ \gamma_i$ posee logaritmo (digamos $\log_i$, para mostrar que posiblemente tienen distintas ramas) para todo $i \leq n$. De este modo,

$$\int_\gamma \frac{f'(z)}{f(z)} dz = \sum_{i=1}^{n} \int_{\gamma_i} \frac{f'(z)}{f(z)} dz = \sum_{i=1}^{n} [\log_i(f(\gamma(a_{i+1}))) - \log_i(f(\gamma(a_i)))]$$

Notamos que esta suma es casi telescópica; sin embargo, no se anulan los elementos necesariamente, pues $\log_{i+1} - \log_i$ no es necesariamente la función 0. Sin embargo, estas funciones sí difieren por una constante (sus derivadas son iguales), y esta constante de hecho es un múltiplo entero de $2\pi i$. Por lo tanto,

$$\frac{1}{2\pi i} \int_\gamma \frac{f'(z)}{f(z)} dz \in \mathbb{Z}.$$

Análogamente, se tiene lo mismo para la curva η, y entonces concluimos que $\int_{z_0+\partial P} \frac{f'(z)}{f(z)} dz \in L$. Por otro lado, sabemos que esta integral es precisamente la suma de los ceros de f menos los polos de f (contados con multiplicidad). Por lo tanto, $\sum_{z \in P} (\mathrm{ord}_z f) z \in L$.

Como $\mathbb{C}/L$ es un grupo (topológico) abeliano, entonces podemos darle una estructura de grupo a X (la curva elíptica asociada a $\mathbb{C}/L$). Sean $z_1 + L, z_2 + L \in \mathbb{C}/L$, y consideremos la recta $ax + by + c = 0$ que pasa por $(\wp(z_1), \wp'(z_1))$ y $(\wp(z_2), \wp(z_2))$ (en $\mathbb{C}^2$). Sea $f(z) = a\wp(z) + b\wp'(z) + c$; notamos que es una función meromorfa en $\mathbb{C}$ con periodo L.

Si $b \neq 0$, entonces f tiene un polo triple en 0. Notamos que $z_1 + L$ y $z_2 + L$ son ceros de f, y luego existe solamente un otro cero $z_3 + L$ de f. Por el análisis anterior, como $0 + L$ es el único polo de f, tenemos que $z_1 + z_2 + z_3 + L = 0 + L$. Así, definimos la suma

$$(\wp(z_1), \wp'(z_1)) + (\wp(z_2), \wp'(z_2)) := (\wp(-z_3), \wp'(-z_3)) = (\wp(z_3), -\wp'(z_3)) = (\wp(z_1 + z_2), \wp'(z_1 + z_2)).$$

Usando esto, observamos que para todo $z + L \in \mathbb{C}/L$, se tiene que $(\wp(z), \wp'(z)) + \infty = \infty + (\wp(z), \wp'(z)) = (\wp(z), \wp'(z))$.

Si $b = 0$, entonces f tiene un polo doble en 0, y entonces $z_1 + L$ y $z_2 + L$ son los únicos ceros de f. Tenemos que $z_1 + z_2 + 0 + L = 0 + L$, y entonces ponemos $z_3 + L := 0 + L$. Así,

$$(\wp(z_1), \wp'(z_1)) + (\wp(z_2), \wp'(z_2)) = (\wp(0), \wp'(0)) = \infty.$$

Con esto, observamos entonces que X es un grupo abeliano con la suma definida, su elemento neutro es ∞ y la inversa de un elemento $(\wp(z), \wp'(z))$ es $(\wp(z), -\wp'(z))$.

Finalmente, vemos que el isomorfismo de superficies de Riemann $z + L \mapsto (\wp(z), \wp'(z))$ es también un isomorfismo de grupos. Como $\mathbb{C}/L$ es un grupo topológico, entonces también X es un grupo topológico.

Referencias

[1] Farkas, Hershel M. and Kra, Irwin: *Riemann Surfaces.* 2nd ed. Graduate Texts in Mathematics, 71, Springer-Velag New York (1980).

[2] Massey, William S.: *A Basic Course in Algebraic Topology.* Graduate Texts in Mathematics, 127, Springer-Velag New York (1991).

[3] Miranda, Rick: *Algebraic Curves and Riemann Surfaces.* Graduate Studies in Mathematics, v. 5, American Mathematical Society (1995).