UNIVERSIDAD MICHOACANA DE SAN NICOLÁS DE HIDALGO

FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS

"Matemático Luis Manuel Rivera Guitiérrez"

Compactificación del Espacio Moduli de Curvas Elípticas

TESIS
que para obtener el título de

Licenciado en Ciencias Físico-Matemáticas

presenta:

José Luis Sánchez Ponce

Asesor:
Dr. Luis Abel Castorena Martínez
Instituto de Matemáticas, UNAM campus Morelia.

Morelia, Michoacán, Octubre de 2008

Este trabajo está dedicado a mis padres José Luis y Eva, también a mis hermanos y amigos.

Agradezco con especial cariño a Yuri, también a mis amigos Chucho, Néstor y Jaime de quienes he aprendido y disfrutado de su amistad.

Agradezco el apoyo y dedicación de mi asesor el Dr. Luis Abel Castorena Martínez y las aportaciones de mis sinodales: Dr. Jorge Luis López López, Dr. Francisco Domínguez Mota, Dra.Gloria Andablo Reyes, Dra. María Luisa Pérez Seguí y Dr. Luis Valero Elizondo.

Agradezco el apoyo económico para esta tesis brindado por: Proyecto UNAM PAPIIT IN104906-2 "Teoría de Brill Noether para curvas especiales y aplicaciones".

Índice general

Capítulo 1

Introducción.

El objetivo de esta tesis consiste en estudiar uno de los problemas clásicos del moduli, utilizando sólo variable compleja con un poco de la Teoría Geométrica de Invariantes. Lo que pretendemos explicar es la manera de compactificar el moduli de Toros Complejos, que es lo mismo que el moduli de Curvas Elípticas no singulares sobre $\mathbb{C}$. Sin entrar en detalles técnicos nosotros consideramos la siguiente situación:

Sea $\mathcal{T}$ un conjunto de objetos geométricos. Queremos encontrar un espacio $\mathcal{M}$ con ciertas propiedades algebraicas y geométricas, cuyos puntos clasifica elementos de $\mathcal{T}$, o más generalmente, clases de equivalencia de tales elementos bajo una relación de isomorfismo. La estructura (de *esquema*) algebraica y geométrica de $\mathcal{M}$ debe ser de un modo natural, de tal forma que los objetos geométricos en T varien en una familia algebraica cuyos objetos tengan la misma dimensión, y que el *moduli* de T varie algebraicamente en $\mathcal{M}$. Dicho de otra manera dada una familia $\pi : \mathcal{C} \to B$ cuyas fibras $\{\pi^{-1}(b) : b \in B\}$ son elementos de $\mathcal{T}$ y la aplicación $B \to \mathcal{M}$ que asigna a cada $b \in B$ la clase de equivalencia $[\pi^{-1}(b)]$ en $\mathcal{M}$ deberá ser algebraica. En esta tesis estudiamos el siguiente problema:

Para cada $t \in \mathbb{C}$, sea C_t la curva cúbica dada como los ceros del polinomio $y^2z - x(x - tz)(x - t\lambda z)$. Sea $\mathcal{T} = \{C_t : t \in \mathbb{C}\}$. No es difícil convencerse que para $t \neq 0$ la curva C_t es isomorfa a la curva C_1, la cual es una curva cúbica no singular(curva elíptica no singular). Notemos que la curva C_0 dada por los ceros del polinomio $zy^2 - x^3$ es racional, es decir, admite una parametrización del tipo $(s^2, s^3, 1)$ y tiene una singularidad de tipo *cúspide* en el punto $(0, 0, 1)$. En este caso no parece existir una estructura algebraica $\mathcal{M}$ con una aplicación $B \to \mathcal{M}$ tal que para todo $t \neq 0$ le asigna un solo valor, a saber la clase de equivalencia $[C_t]$(pues para $t \neq 0$ todas las C_t son isomorfas) y el valor $[C_0]$ para $t = 0$ que en este caso es una curva singular. Esto lo que nos sugiere es: O hacemos mas "pequeño" el espacio T, es decir, podemos consierar $\{C_t : t \neq 0\}$, en este caso todos los elementos de T son no singulares, pero esto es una solución un poco débil a nuestro problema. La otra opción es *completar* $\mathcal{M}$ admitiendo a C_0 como un elemento de T y de tal manera que tengamos una buena aplicación

algebraica $B \to \mathcal{M}$. Por ejemplo consdieremos la familia $\mathcal{F}$ donde los elementos de $\mathcal{F}$ son curvas $C_t = \{([x : y : z] : y^2z = x(x - z)(x - tz))\}$. Las curvas C_t son , para $|t|$ suficientemente pequeño, curvas suaves no isomorfas de género uno. La curva "especial"C_0(tomar $t = 0$) es una curva irreducible con una singularidad de tipo nodo (localmente un nodo tiene forma analítica del tipo $xy = 0$). Esta curva C_0 es un ejemplo de "curva estable". Examinaremos el significado de estas definiciones en los capítulos de la tesis. Notemos que en este caso tenemos una familia de curvas sobre el disco agujerado $D^* = D-\{0\}$, donde $D = \{t \in \mathbb{C} : |t| < 1\}-\{0\}$, es decir, tenemos una aplicación $f : \mathcal{F} \to D-\{0\}$ tal que para cada $t \in D-\{0\}$, $f^{-1}(t) := C_t$ es una curva de género uno. La filosofía del teorema de extensión de Riemann de variable compleja nos sugiere que dicha aplicación f se puede extender a todo D al considerar la imagen inversa del 0, esto es al considerar la "curva estable"$C_0 = f^{-1}(0)$. En la primera familia que hemos tomado se tiene que $C_0 = C_1$ y completamos dicha familia a una familia con moduli constante. En la segunda familia $\mathcal{F}$ que hemos considerado tenemos que la única posibilidad para extender dicha familia es considerar la curva estable C_0, es decir, no tenemos un espacio moduli $\mathcal{M}$ completo, a menos que admitamos el elemento singular C_0. Para trabajar en esta construcción necesitamos la Teoría Geométrica de invariantes. El trabajo de esta tesis es ver que mediante este proceso podemos compactificar el espacio moduli de curvas elípticas agregando un elemento "estable".

En el capítulo 2 se habla sobre Curvas Elípticas y Superficies de Riemann. En este se introduce formalmente los objetos y estructuras algebraicas y complejas que serán tratadas. En este también se empieza por clarificar la correspondencia natural que existe entre la familia de Toros Complejos y Curvas Elípticas.

En el capítulo 3 se introducen las funciones definidas sobre el Toro Complejo, llamadas funciones elípticas y se prueba la existencia de tales, a travez de la función p de Weierstrass. Después obtenemos una ecuación polinomial cúbica en las variables p y p' que permite encajar al Toro $\mathbb{C}/L$ en $\mathbb{C}P^2$, de manera que $\mathbb{C}/L$ se vea como curva algebraica y así obtener la correspondencia unívoca entre Toros Complejos y Curvas Elípticas. Después se observa que la familia de Toros (salvo isomorfismo) se identifica con la variedad $\mathbb{H}/\Gamma$, y por medio de la función j-invariante, definida en $\mathbb{H}$ y además invariante bajo la acción de Γ en $\mathbb{H}$, obtenemos que $\mathbb{H}/\Gamma$ es isomorfo a $\mathbb{C}$. Así $\mathbb{C}$ parametriza a la familia de los Toros complejos.

En el capítulo 4 se desarrollan los elementos básicos sobre la Teoría Geométrica de Invariantes con el objetivo de obtener la compactificación de la familia X de curvas elípticas no singulares (cúbicas). El proceso consiste en darle a X estructura de variedad proyectiva. Después notar que $G = SL(2, \mathbb{Z})$ actúa de manera natural sobre X, y que esta acción corresponde a la relación de isomorfismo entre curvas elípticas. Después notar que las cúbicas no singulares corresponden a los puntos estables de X bajo la acción de G. Por último tenemos que identificar en X los puntos que son semiestables y no estables, pues estos, deacuerdo al Teorema Fundamental de GIT compactifican de manera natural a la variedad

X^s/G(= elípticas no singulares).

Capítulo 2

Superficies de Riemann.

La idea básica de una Superficie de Riemann es que es un espacio que localmente luce a un abierto del plano complejo.

2.1. Definición de una Superficie de Riemann.

Definición. Sea S un espacio topológico, entonces S es llamada una $n-$ *variedad* si S es Hausdorff, conexo y si cada $s \in S$ tiene una vecindad U homeomorfa a un abierto de $\mathbb{R}^n$.

Una $2-variedad$ es también llamada una $superficie$.

Cualquier superficie ($2-variedad$) esta cubierta por una familia de abiertos U_i tal que para cada U_i existe un homeomorfismo $\phi_i : U_i \longrightarrow W_i$, donde $W_i \subseteq \mathbb{C}$ es abierto. El conjunto de parejas $\mathcal{A} = \{(U_i, \phi_i)\}$ es llamado un $atlas$ para S; si $s \in U_i$, (U_i, ϕ_i) es llamada una *carta* en s y $z_i = \phi_i(s)$ una *cordenada local* en s.

Si (U_i, ϕ_i) y (U_j, ϕ_j) son cartas para $s \in S$ con coordenadas locales $z_i = \phi_i(s)$ y $z_j = \phi_j(s)$, entonces $z_i = (\phi_i \circ \phi_j^{-1})(z_j)$ es llamado el *cambio de coordenada local* para s correspondiente a las cartas (U_i, ϕ_i) y (U_j, ϕ_j).

Las funciones

$$\phi_i \circ \phi_j^{-1} : \phi_j(U_i \cap U_j) \subseteq \mathbb{C} \longrightarrow \phi_i(U_i \cap U_j) \subseteq \mathbb{C}$$

están definidas siempre que $U_i \cap U_j \neq \varnothing$ y son llamadas las $funciones\ cambios\ de\ coordenadas$.

Un atlas $\mathcal{A} = \{(U_i, \phi_i)\}$ es llamado *analítico* si todas las funciones cambios de coordenadas son funciones analíticas (en el sentido usual de función de variable compleja).

Con el propósito de referirse a funciones analíticas o meromorfas en S, sin tener

que especificar la dependencia de estos conceptos sobre un atlas particular, decimos que dos atlas analíticos $\mathcal{A} = \{(U_i, \phi_i)\}$ y $\mathcal{B} = \{(V_j, \psi_j)\}$ son compatibles si, siempre que $(U_i, \phi_i) \in \mathcal{A}$ y $(V_j, \psi_j) \in \mathcal{B}$ y $U_i \cap V_j \neq \varnothing$, entonces

$$\phi_i \circ \psi_j^{-1} : \psi_j(U_i \cap V_j) \subseteq \mathbb{C} \longrightarrow \phi_i(U_i \cap V_j) \subseteq \mathbb{C}$$

sea una función analítica con inversa analítica (tales funciones son llamadas biholomorfismos). Nótese que $\mathcal{A}$ y $\mathcal{B}$ son compatibles si y sólo si $\mathcal{A} \cup \mathcal{B}$ es un atlas analítico para S. También es evidente que la relación dada por atlas compatibles es una relación de equivalencia. Una clase de equivalencia de atlas analíticos es llamada una *estructura compleja en S*.

Definición. Una superficie con estructura compleja es llamada una $Superficie$ *de Riemann.*

Para referirnos a la estructura compleja de una superficie es suficiente especificar un atlas representante de la clase.

2.2. Algunas Superficies de Riemann.

1) Sea $S = \mathbb{C}$, que es conexo, Hausdorff y homeomorfo a $\mathbb{R}^2$ y sea $\mathcal{A} = \{(\mathbb{C}, id : \mathbb{C} \longrightarrow \mathbb{C})\}$ un atlas para S; claramente $\mathcal{A}$ es un atlas analítico para $\mathbb{C}$ y además cualquier atlas analítico $\mathcal{A}' = \{(U_i, \phi_i)\}$ es un atlas compatible con $\mathcal{A} = \{(\mathbb{C}, id : \mathbb{C} \longrightarrow \mathbb{C})\}$, así $\mathbb{C}$ es una superficie de Riemann (con una única estructura compleja).

2) Cualquier abierto A de una superficie de Riemann S es también una superficie de Riemann, pues si $\mathcal{A} = \{(U_i, \phi_i)\}$ es un atlas analítico para S, entonces $\mathcal{B} = \{(U_i \cap T, \psi_i)\}$ es un atlas analítico para T, donde ψ_i denota la restricción de ϕ_i en $U_i \cap T$. Además si $\mathcal{A}' = \{(U'_j, \phi'_j)\}$ es un atlas para S compatible con $\mathcal{A}$, entonces $\mathcal{B}' = \{(U'_j \cap T, \psi'_j)\}$ es un atlas compatible con $\mathcal{B}$, donde ψ'_j denota la restricción de ϕ'_j en $U'_j \cap T$. Es decir, atlas compatibles en S, inducen atlas compatibles en T.

Proposición 1 *Si $\mathcal{A} = \{(U_i, \phi_i)\}$ es un atlas analítico para S, y si para cada i, $\{V_{ij}\}$ es una familia de subconjuntos abiertos de U_i tal que $\bigcup\{V_{ij}\} = U_i$, entonces si denotamos por ψ_{ij} la restricción de ϕ_i en V_{ij}, tenemos que $\mathcal{A}' = \{(V_{ij}, \psi_{ij})\}$ es un atlas analítico compatible con $\mathcal{A}$.*

Demostración: Es claro que S es cubierto por todos los conjuntos V_{ij}. Como las funciones cambios de coordenadas para el atlas $\mathcal{A} \cup \mathcal{A}'$ son las restricciones de las funciones cambios de coordenadas del atlas $\mathcal{A}$ ó en algunos casos la identidad, entonces $\mathcal{A}'$ en un atlas analítico compatible con $\mathcal{A}$. □

3) Sea $S = \Sigma = \mathbb{C} \cup \{\infty\}$. Sabemos que Σ es homeomorfa a $S^2 = \{\bar{x} \in \mathbb{R}^3 : \|\bar{x}\| = 1\}$. Sea $U_1 = \mathbb{C}$ con $\phi_1 = id : \mathbb{C} \longrightarrow \mathbb{C}$ y $U_2 = \Sigma \setminus \{0\}$ con

$\phi_2 = J : \Sigma \setminus \{0\} \longrightarrow \mathbb{C}$ dada por $J(z) = 1/z$, para $z \in \mathbb{C} - \{0\}$ y $J(\infty) = 0$. Claramente $\Sigma = U_1 \cup U_2$ y ϕ_1, ϕ_2 son homeomorfismos.

Ahora $\phi_1 \circ \phi_2^{-1} : \mathbb{C} \setminus \{0\} \longrightarrow \mathbb{C} \setminus \{0\}$ está dada por $(\phi_1 \circ \phi_2)(z) = 1/z$ y $\phi_2 \circ \phi_1^{-1} : \mathbb{C} \setminus \{0\} \longrightarrow \mathbb{C} \setminus \{0\}$ dada también por $(\phi_2 \circ \phi_1^{-1})(z) = 1/z$, entonces se tiene que $\{(U_i, \phi_i)\}$, $i \in \{1, 2\}$ es un atlas analítico para Σ. Por tanto Σ en una superficie de Riemann y es llamada *la esfera de Riemann*.

2.3. El Toro Complejo.

Sean $w_1, w_2 \in \mathbb{C}$, $w_2 \neq 0$ y tal que $w_1/w_2 \notin \mathbb{R}$ (i,e. w_1 y w_2 son $\mathbb{R} -$ *linealmente independientes*).

Sea $L = \mathbb{Z}w_1 \oplus \mathbb{Z}w_2 = \{nw_1 + mw_2 : n, m \in \mathbb{Z}\}$. Entonces L es llamada la *retícula* generada por w_1 y w_2. Además es claro que L es un subgrupo normal de $\mathbb{C}$ (normal ya que $\mathbb{C}$ es abeliano). Ahora consideramos la relación usual en $\mathbb{C}$ inducida por L:
Sean a y b en $\mathbb{C}$, decimos que a está relacionado con b *módulo* L y escribimos $a \sim b \ mod \ L$ si $a - b \in L$, equivalentemente $a \in b + L := \{a + l : l \in L\}$. Claramente $\sim$ es una relación de equivalencia y denotamos $[a] = \{b \in \mathbb{C} : a \sim b\}$. Ahora denotamos por $\mathbb{C}/L$ al conjunto de clases de equivalencia. Entonces definiendo la suma en $\mathbb{C}/L$ como $[a] + [b] := [a + b]$ para $a, b \in \mathbb{C}$, entonces $\mathbb{C}/L$ tiene estructura de grupo abeliano.

Ahora nuestro interés se concentra en darle una estructura compleja a $\mathbb{C}/L$. Para esto recordemos lo siguiente:
Si X es un espacio topológico, Y es un conjunto no vacío cualquiera tal que existe una función sobre $f : X \longrightarrow Y$, entonces Y es un espacio topológico definiendo que $A \subseteq Y$ es abierto si y sólo si $f^{-1}(A) \subseteq X$ es abierto. Con esta construcción $f : X \longrightarrow Y$ es una función continua.

Consideramos la proyección canónica $\Pi : \mathbb{C} \longrightarrow \mathbb{C}/L$ dada por $\Pi(z) = [z]$ que es claramente sobre. Entonces si definimos que $A \subseteq \mathbb{C}/L$ es abierto si y sólo si $\Pi^{-1}(A) \subseteq \mathbb{C}$ es abierto, $\mathbb{C}/L$ es un espacio topológico y Π es continua.

Proposición 2 *$\mathbb{C}/L$ es un espacio conexo Hausdorff.*

Demostración: Como $\Pi : \mathbb{C} \longrightarrow \mathbb{C}/L$ es continua y $\mathbb{C}$ es conexo, entonces $\Pi(\mathbb{C})$ es conexo, pero $\Pi(\mathbb{C}) = \mathbb{C}/L$, entonces $\mathbb{C}/L$ es conexo.

Ahora sean $s_1 = [z_1]$ y $s_2 = [z_2]$ dos puntos distintos en $\mathbb{C}/L$ y sea

$$d = inf|z_1 - (z_2 + w)| > 0, w \in L$$

pues L es discreto. Sean $V_1 = \{z \in \mathbb{C} : |z - z_1| < d/2\}$ y $V_2 = \{z \in \mathbb{C} : |z - z_2| < d/2\}$. Ahora se afirma que $(V_1 + w) \cap V_2 = \varnothing$ para todo $w \in L$; si no, sea $z \in V_1$ y $w \in L$ tal que $z + w \in V_2$, aplicando la desigualdad del triángulo obtenemos que

$$|z_1-(z_2+w)| \leqq |z_1-(z+w)|+|(z+w)-(z_2+w)| = |z_1-(z+w)|+|z-z_2| < \frac{d}{2}+\frac{d}{2} = d,$$

contradiciendo la definición de d. Como Π es abierta, $\Pi(V_1)$ y $\Pi(V_2)$ son abiertos que contienen a s_1 y s_2 respectivamente, además es claro que $\Pi(V_1) \cap \Pi(V_2) = \varnothing$, pues si no, entonces existe $[x] \in \Pi(V_1) \cap \Pi(V_2)$ y esto implica que existen a_1 y a_2 en V_1 y V_2 respectivamente tales que $x \sim a_1$ y $x \sim a_2$, entonces $a_1 \sim a_2$ y por tanto $a_2 = a_1 + w$ y así $a_2 \in (V_1 + w) \cap V_2$. Contradicción.

Por lo tanto $\Pi(V_1)$ y $\Pi(V_2)$ son vecindades disjuntas de s_1 y s_2 respectivamente. Entonces $\mathbb{C}/L$ es Hausdorff.□

Definición. Si $L = \mathbb{Z}w_1 \oplus \mathbb{Z}w_2$, el conjunto

$$P_L := \{sw_1 + tw_2 : 0 \leq s, t \leq 1\} \subseteq \mathbb{C}$$

es llamado el *paralelogramo fundamental* para la retícula L. (Ver figura 2.1).

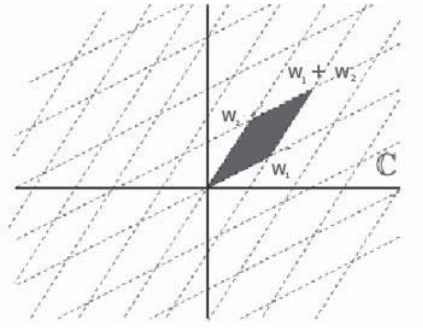


Figura 2.1: El Paralelogramo Fundamental asociado a w_1 y w_2.

Como $\mathbb{C}$ es un $\mathbb{R}$-espacio vectorial de dimensión dos y w_1 y w_2 son $\mathbb{R}-$*linealmente independientes*, entonces dado cualquier $z \in \mathbb{C}$, existen k_1 y k_2 elementos en $\mathbb{R}$ tal que $z = k_1w_1 + k_2w_2$.Entonces si n_1 y n_2 representan el mayor entero que sea menor que k_1 y k_2 respectivamente (la parte entera), entonces podemos escribir que $k_1 = n_1 + \alpha_1$ y $k_2 = n_2 + \alpha_2$, donde $0 \leq \alpha_1, \alpha_2 \leq 1$ y por tanto

$$z = (n_1 + \alpha_1)w_1 + (n_2 + \alpha_2)w_2 = \alpha_1w_1 + \alpha_2w_2 + (n_1w_1 + n_2w_2),$$

n_1 y n_2 enteros y $\alpha_1w_1+\alpha_2w_2 \in P$. Por lo tanto cualquier $z \in \mathbb{C}$ está relacionado *(mod L)* con algún elemento en P_L.

Proposición 3 *Sea $L = \mathbb{Z}w_1 \oplus \mathbb{Z}w_2$, entonces $\mathbb{C}/L$ es un espacio compacto.*

Demostración: Como hemos observado que cualquier $z \in \mathbb{C}$ está relacionado *(mod L)* con algún elemento en P_L, entonces $\Pi(P_L) = \mathbb{C}/L$, donde Π es la aplicación canónica de $\mathbb{C}$ sobre $\mathbb{C}/L$. Pero P_L es compacto y Π es continua. Por lo tanto $\Pi(P_L) = \mathbb{C}/L$ es compacto. $\square$

Teorema 1 *Si $L = \mathbb{Z}w_1 \oplus \mathbb{Z}w_2$, el espacio $\mathbb{C}/L$ es una superficie de Riemann.*

Demostración: Como L es discreto, entonces $\delta = inf|w| > 0$ donde $w \in L \setminus \{0\}$. Ahora para $\alpha \in \mathbb{C}$, consideramos $U_\alpha := \{z \in \mathbb{C} : |z - \alpha| \ < \frac{\delta}{4}\}$. También consideramos la aplicación canónica $\Pi : \mathbb{C} \longrightarrow \mathbb{C}/L$ dada por $z \longmapsto [z]$.

Ahora si a y b están en U_α y $a \sim b$ *(mod L)*, entonces existe $w \in L$ tal que $a - b = w$ y por tanto

$$|w| = |a - b| = |a - \alpha + \alpha - b| \leq |a - \alpha| + |b - \alpha| < \frac{\delta}{4} + \frac{\delta}{4} = \frac{\delta}{2} < \delta$$

Por lo tanto $w = 0$ y así $a = b$. Con esta observación se concluye que Π_{U_α} la restraicción de Π en U_α, denotada por $\Pi_\alpha : U_\alpha \longrightarrow \Pi(u_\alpha)$ es una biyección continua y como Π es abierta, entonces Π_α es un homeomorfismo.

Ahora denotamos $V_\alpha := \Pi_\alpha(U_\alpha)$ y $\phi_\alpha = \Pi_\alpha^{-1}$ la inversa de Π_α; entonces V_α es un abierto en $\mathbb{C}/L$ y $\phi_\alpha : V_\alpha \longrightarrow U_\alpha$ es un homeomorfismo sobre un abierto en $\mathbb{C}$. Es claro que $\{V_\alpha\}$ es una cubierta.

Veamos ahora que $\{(V_\alpha, \phi_\alpha)\}_{\alpha \in \mathbb{C}}$ es un atlas analítico para $\mathbb{C}/L$. Para esto observamos primero que para cualesquiera U_α y U_β, existe a lo más un $w \in L$ tal que $U_\alpha \cap U_\beta + w \neq \varnothing$, donde $U_\beta + w := \{u + w : u \in U_\beta\}$; pues si w_1, $w_2 \in L$ son tales que existen $z_1 \in U_\alpha \cap U_\beta + w_1$ y $z_2 \in U_\alpha \cap U_\beta + w_2$ y escribimos $z_1 = a + w_1$ y $z_2 = b + w_2$ con a y b en U_β, entonces podemos escribir que

$$|w_1 - w_2| = |(z_1 - a) - (z_2 - b)| = |(z_1 - z_2) - (a - b)| \leq |z_1 - z_2| + |a - b| < \frac{\delta}{2} + \frac{\delta}{2} = \delta$$

Por lo tanto como $w_1 - w_2 \in L$, entonces $w_1 - w_2 = 0$ i.e. $w_1 = w_2$.

Ahora supóngase que $\alpha, \beta \in \mathbb{C}$ son tales que $V_\alpha \cap V_\beta \neq \varnothing$ y consideramos $\phi_\beta \circ \phi_\alpha^{-1} : \phi_\alpha(V_\alpha \cap V_\beta) \longrightarrow \phi_\beta(V_\alpha \cap V_\beta)$.

Sea $z \in \phi_\alpha(V_\alpha \cap V_\beta)$ y $z' = (\phi_\beta \circ \phi_\alpha^{-1})(z)$, entonces

$$\Pi_\beta(z') = (\Pi_\beta \circ \phi_\beta \circ \phi_\alpha^{-1})(z) = \phi_\alpha^{-1}(z) = \Pi_\alpha(z)$$

Por lo tanto $\Pi(z') = \Pi(z)$, entonces $z \sim z'$ *(mod L)* i.e. $z' = z + w$, algún w que posiblemente depende de z; ahora como $z \in U_\alpha$ y $z' \in U_\beta$, entonces tenemos que $z' \in U_\beta \cap U_\alpha + w$ y como ya observamos este w es único y sólo depende de

α y β, no de z. Por lo tanto la aplicación $\phi_\beta \circ \phi_\alpha^{-1}$ es de la forma $z \longmapsto z + w$, con w constante, así es holomorfa.

Concluimos que $\{(V_\alpha, \phi_\alpha)\}_{\alpha \in \mathbb{C}}$ es un atlas analítico para $\mathbb{C}/L$. Por lo tanto $\mathbb{C}/L$ es una superficie de Riemann. $\square$

Toda Superficie de Riemann compacta S tiene asociado un número entero $g \geq 0$ llamado el *género de S*. Este invariante es topológico y cuenta el número de asas que tiene S.

Teorema 2 *(Abel-Jacobi). Si S es una superficie de Riemann compacta de género 1, entonces S es un toro complejo, es decir existen $w_1, w_2 \in \mathbb{C}$ con $\frac{w_1}{w_2} \notin \mathbb{R}$ tal que $S \cong \mathbb{C}/L$, donde $L = \mathbb{Z}w_1 \oplus \mathbb{Z}w_2$.* $\square$

2.4. Funciones analíticas y meromorfas en Superficies de Riemann.

Sean S_1 y S_2 superficies de Riemann. Entonces una función continua $f : S_1 \longrightarrow S_2$ es llamada *analítica* si siempre que (U_1, ϕ_1) y (U_2, ϕ_2) sean cartas (claro que para atlas fijos) de S_1 y S_2 tal que $U_1 \cap f^{-1}(U_2) \neq \varnothing$, entonces la función

$$\phi_2 \circ f \circ \phi_1^{-1} : \phi_1(U_1 \cap f^{-1}(U_2)) \subseteq \mathbb{C} \longrightarrow \mathbb{C}.$$

es una función analítica. Ver figura 2.2.

Como f es continua, $f^{-1}(U_2)$ es abierto en S_1, entonces $\phi_1(U_1 \cap f^{-1}(U_2)) \subseteq \mathbb{C}$ es abierto pues ϕ_1 es un homeomorfismo.

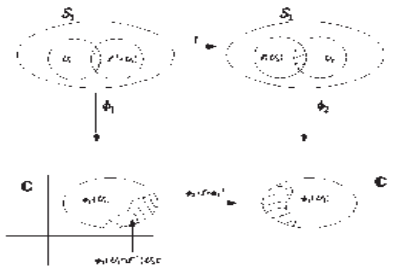


Figura 2.2: Función holomorfa entre Superficies de Riemann.

Teorema 3 *Si* $f : S_1 \longrightarrow S_2$ *y* $g : S_2 \longrightarrow S_3$ *son funciones analíticas entre superficies de Riemann, entonces* $g \circ f : S_1 \longrightarrow S_3$ *es también analítica.*

Demostración: Por la proposición 1, podemos escoger tres atlas $\mathcal{A}_i$ en S_i $(i = 1, 2, 3)$ de tal forma que para cada $(U_1, \phi_1) \in \mathcal{A}_1$ exista $(U_2, \phi_2) \in \mathcal{A}_2$ con $f(U_1) \subseteq U_2$, y para $(U_2, \phi_2) \in \mathcal{A}_2$ exista $(U_3, \phi_3) \in \mathcal{A}_3$ con $g(U_2) \subseteq U_3$. Ahora como $\phi_2 \circ f \circ \phi_1^{-1}$ y $\phi_3 \circ g \circ \phi_2^{-1}$ son analíticas (en abiertos de $\mathbb{C}$), entonces

$$\phi_3 \circ g \circ f \circ \phi_1^{-1} = (\phi_3 \circ g \circ \phi_2^{-1}) \circ (\phi_2 \circ f \circ \phi_1^{-1})$$

es también analítica.

Teorema 4 *Si* $\Pi : \mathbb{C} \longrightarrow \mathbb{C}/L$ *es la proyección,* $z \longmapsto z + L$*, entonces* Π *es holomorfa.*

Demostración: Π es por construcción continua.

Ahora $\{\mathbb{C}, \phi\}$ es el atlas de $\mathbb{C}$, donde $\phi = id : \mathbb{C} \longrightarrow \mathbb{C}$ y $\{U_\gamma, \phi_\gamma\}$ es el atlas de $\mathbb{C}/L$ ya mencionado, donde V es cualquier disco abierto en $\mathbb{C}$ con diámetro menor a $\delta/2$ y $\delta := inf|w| > 0$ donde $w \in L \setminus \{0\}$. Entonces sabemos que $\phi_\gamma \circ \Pi$ se restringe a la identidad $\phi_\gamma \circ \Pi_\gamma$ en cada V. Por lo tanto $\phi_\gamma \circ \Pi \circ \phi^{-1} : V \longrightarrow V$ es la identidad que es analítica. Así Π es holomorfa. □

2.5. Curvas Elípticas.

Las curvas elípticas son uno de los objetos matemáticaos más ricos en estructura y, gracias a los múltiples enfoques con los que pueden ser tratadas, estas curvas tienen muchas aplicaciones en diferentes áreas. Algunas de estas áreas son por ejemplo la Teoría de Números, Criptografía y Geometría Algebraica. El ojetivo de esta sección es introducir de manera formal las curvas elípticas y algunos ejemplos de estas, y poder darle a estas naturalmente una estructura compleja.

2.5.1. Ecuación de Weierstrass.

Definamos de manera elemental una curva elíptica:

Definición: Sea K un campo de característica distinta de 2 ó 3. Una *curva elíptica* E es la gráfica de una ecuación de la forma

$$y^2 = x^3 + Ax + B$$

con $A, B \in K$. En este caso decimos que la curva está definida sobre K. Esta ecuación es llamada la ecuación de Weierstrass de la curva elíptica.

Para ayudar a la intuición presentamos algunos dibujos de curvas elípticas sobre los números reales:

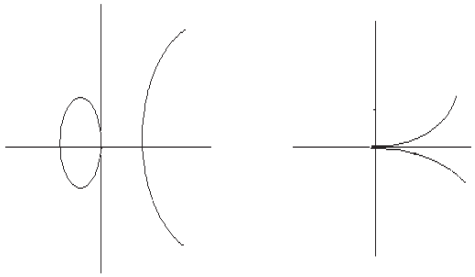


Figura 2.3: Ejemplos de curvas elípticas en el plano real. La primera corresponde a la ecuación $y^2 = x^3 - x$, la segunda a la ecuación $y = x^3$.

La ecuación de Weierstrass generalizada de la curva elíptica, a saber

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

es utilizada cuando se trabaja sobre campos de característica 2 ó 3. Si el campo no es de característica 2 podemos dividir la ecuación anterior por 2 y completar los cuadrados para reescribirla como

$$y_1^2 = x^3 + a_2'x^2 + a_4'x + a_6',$$

donde $y_1^2 = y + \dfrac{a_1x}{2} + \dfrac{a_3}{2}$ y a_2', a_4', a_6' son constantes. Si el campo no es de característica 3 podemos hacer el cambio de variable $x_1 = x + \dfrac{a_2'}{3}$ y obtener la forma de Weierstrass $y_1^2 = x_1^3 + Ax_1 + B$ para algunas constantes A, B.

Finalmente, si comenzamos con la ecuación $cy^2 = dx^3 + ax + b$, con $c, d \neq 0$, haciendo el cambio de variables $y_1 = c^2dy$, $x_1 = cdx$ recuperamos la forma de Weierstrass de la ecuación.

2.5.2. Curvas Singulares.

Sea E la curva de la ecuación $y^2 = f(x)$, $f(x) = x^3 + ax + b$.

Si escribimos la ecuación como $F(x, y) = y^2 - f(x) = 0$ y tomamos las derivadas

parciales $\dfrac{\partial F}{\partial x} = -f'(x)$, $\dfrac{\partial F}{\partial y} = y^2$, entonces por la definición $(x_0, y_0) \in E$ es un *punto singular de* E si y sólo si ambas parciales se anulan en (x_0, y_0).

Si (x_0, y_0) no es un punto singular de E, decimos que (x_0, y_0) es *no singular*. E es una *curva no singular* si y sólo si todos sus puntos son no singulares. Esto significa que todo punto en la curva tiene una línea tangente bien definida. Ahora supóngase que (x_0, y_0) es un punto singular en E, es decir, las derivadas parciales se anulan simultáneamente en (x_0, y_0), entonces $y_0 = 0$ y entonces $f(x_0) = 0$, por lo tanto $f(x)$ y $f'(x)$ tienen como raíz común a x_0. Así x_0 es raíz doble de $f(x)$. Inversamente, si $f(x)$ tiene una raíz doble x_0, entonces $(x_0, 0)$ es un punto singular en E. Es decir E es singular si y sólo si $f(x)$ tiene alguna raíz x_0 con multiplicidad ≥ 2.

Existen dos posibiliades para la singularidad, estas ocurren dependiendo si $f(x)$ tiene una raíz doble o una raíz triple.

i) En el caso en que $f(x)$ tiene una raíz doble, una ecuación típica (salvo cambio de coordenadas) es

$$y^2 = x^2(x+1)$$

El punto $(0, 0)$ es la "singularidad doble" (i.e, cero es raíz doble de $f(x) = x^2(x+1)$) de la curvatura E asociada. Veamos el comportamiento local de E cerca del $(0, 0)$. Para esto:

Sea $t = \dfrac{y}{x}$, así $y^2 = t^2x^2$, entonces la ecuación inicial se ve como $t^2x^2 = x^2(x+1)$, por tanto $t^2 = x + 1$, y así $x = t^2 - 1$ y $y = t^3 - t$.

Consideramos ahora $h(t) = (x(t), y(t)) = (t^2 - 1, t^3 - t)$, y entonces $h'(t) := (x'(t), y'(t)) = (2t, 3t^2)$ está bien definida cuando $x(t) \neq 0$ i.e, $t \neq \pm 1$. Pero

$$\lim_{t \to 1} h'(t) = (2, 3)$$

y

$$\lim_{t \to -1} h'(t) = (-2, 3).$$

Por lo tanto el punto $(0, 0)$ es doble y posee dos tangentes distintas, dadas por los vectores $(2, 3)$ y $(-2, 3)$.Ver Figura.

ii) El caso en que $f(x)$ tiene una raíz triple, entonces la curva E tiene como ecuación (salvo traslación)

$$y^2 = x^3,$$

y luce como una "parábola semicúbica" con una cúspide en el origen. El punto $(0, 0)$ es una singularidad en E, y como el cero es raíz triple de $f(x) = x^3$, $(0, 0)$ es llamado un punto triple de E.

El comportamiento local de E en el punto $(0,0)$ es más simple, pues E se parametriza con $x(t) = t^2$ y $y(t) = t^3$. Entonces $x'(t) = 2t$ y $y'(t) = 3t^2$.Por lo tanto $y = 0$ es la única tangente a $(0,0)$. (Ver figura 2.4).

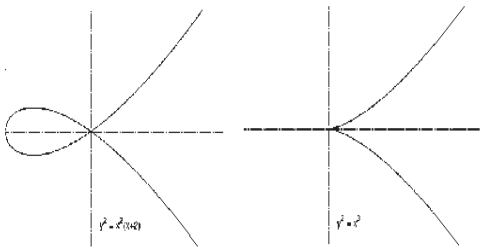


Figura 2.4: Ejemplos de curvas elípticas singulares.

Estas curvas analizadas, que representan hasta "equivalencia" la familia de curvas elípticas singulares son de suprema importancia para nuestro objetivo, y surgen finalmente en el capítulo 4 en el proceso de conclusión.

2.5.3. El Discriminante.

Sea $f(x) \in \mathbb{C}[x]$ un polinomio. Si factorizamos a $f(x)$ sobre $\mathbb{C}$

$$f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3),$$

entonces definimos el *discriminante de* $f(x)$ como

$$\Delta_f = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2$$

De la definición del discriminante de $f(x)$, se observa que $\Delta_f = 0$, si y sólo si, $f(x)$ tiene raices repetidas.

Sea E una curva elíptica, con ecuación $y^2 = x^3 + ax + b$.

Definamos el *discriminante de* E y lo escribimos como Δ_E a $\Delta_E := \Delta_f$, $f(x) = x^3 + ax + b$. Entonces E es una curva no-singular si y sólo si $\Delta_E \neq 0$.

Proposición 4 *Sea* $f(x) = x^3 + ax + b$, *entonces* $\Delta_f = 4a^3 + 27b^2$. $\square$

2.5.4. Curvas en el Plano Proyectivo.

Si escribimos a $\mathbb{C}P^2 = \mathbb{A}^2 \cup \mathbb{C}P^1$, entonces una *curva algebraica* en el plano afín $\mathbb{A}^2$ es el conjunto de soluciones de una ecuación de la forma

$$f(x, y) = 0,$$

donde $f(x, y) \in \mathbb{C}[x, y]$ es un polinomio en dos variables.

Las curvas elípticas son un particular ejemplo de curvas algebraicas, son solución de una ecuación de la forma

$$y^2 - x^3 - ax - b = 0,$$

con a, b constantes.

Para definir curvas de esta naturaleza en $\mathbb{C}P^2$, necesitaremos usar polinomios en tres variables, pues los puntos en $\mathbb{C}P^2$ están representados por ternas. Además cada punto en $\mathbb{C}P^2$ puede ser representado por distintas coordenadas homogéneas. Es así que requerimos de "polinomios homogeneos"para definir curvas en $\mathbb{C}P^2$.

Definición. Sea $F(X, Y, Z) \in \mathbb{C}[X, Y, Z]$ un polinomio en tres variables, entonces $F(X, Y, Z)$ es llamado un *polinomio homogéneo de grado d* si este satisface la identidad

$$F(tX, tY, tZ) = t^d F(X, Y, Z),$$

$\forall t \in \mathbb{C}$.

La definición de que $F(X, Y, Z)$ es un polinomio homogéneo de grado d es equivalente a decir que $F(X, Y, Z)$ es una combinación lineal de monomios $X^i Y^j Z^k$ con $i + j + k = d$.

Definición. *Una curva proyectiva C* en el plano proyectivo $\mathbb{C}P^2$ es el conjunto de soluciones de una ecuación polinomial de laforma $F(X, Y, Z) = 0$, donde $F(X, Y, Z) \in \mathbb{C}[X, Y, Z]$ es un polinomio homogéneo no constante. El *grado de la curva C* es el grado del polinomio $F(X, Y, Z)$.

Entonces para checar que algún punto $P \in \mathbb{C}P^2$ está en la curva C, sólo se verifica que $F(a, b, c) = 0$, donde $[a, b, c]$ es cualquier representación homogénea de P. Esto es obvio ya que cualquier otra representación homogénea de P se ve como $[ta, tb, tc]$, para algún $t \in \mathbb{C}^*$, así $F(a, b, c)$ son ambos cero ó ambos distintos de cero.

Sea $C \subseteq \mathbb{C}P^2$ una curva dada por un polinomio homogéneo de grado d,

$$C : F(X, Y, Z) = 0$$

Supóngase que $P = [a, b, c]$ es un punto en C y que $c \neq 0$, entonces el punto $(\frac{a}{c}, \frac{b}{c}) \in \mathbb{A}^2$ es un punto que satisface $F(\frac{a}{c}, \frac{b}{c}, 1) = 0$. Es decir, si definimos un

polinomio a partir de $F(X,Y,Z)$ dado por $f(x,y) = F(X,Y,1)$, entonces los siguientes conjuntos están en biyección

$$\{[a,b,c] \in C : c \neq 0\} \leftrightarrow \{(x,y) \in \mathbb{A}^2 : f(x,y) = 0\}$$

$$[a,b,c] \longmapsto (\frac{a}{c}, \frac{b}{c})$$

La curva de la ecuación $f(x,y) = 0$ está en $\mathbb{A}^2$, y es llamada la *parte afín* de la curva proyectiva C.

Los puntos $P = [a,b,0]$ en C son llamados los *puntos al infinito* de C.

El proceso de reemplazar el polinomio homogéneo $F(X,Y,Z)$ por el polinomio $f(x,y) = F(X,Y,1)$ es llamado la *deshomogenización* de $F(X,Y,Z)$ (con respecto a la variable Z). Intentemos invertir este proceso.

Supóngase que C_0 es una curva afín dada por una ecuación polinomial $f(x,y) = 0$ Entonces queremos encontrar una curva C proyectiva tal que C_0 sea la parte afín de esta curva C, es decir un polinomio homogéneo $F(X,Y,Z)$ tal que $f(x,y) = F(X,Y,1)$. Esto es simple.

Sea $f(x,y)$ un polinomio, lo escribimos como $f(x,y) = \sum a_{ij}x^iy^j$, entonces el *grado de f* es definido como el máximo de los $i+j$ tales que $a_{ij} \neq 0$, y escribimos el grado de f como $\partial(f)$.

Sea $f(x,y) = \sum a_{ij}x^iy^j$ un polinomio no cero, entonces definimos la *homogenización de f(x,y)* como el polinomio dado por

$$F(X,Y,Z) = \sum_{i,j} a_{ij}X^iY^jZ^{d-i-j}$$

donde $d = \partial(f)$ el grado de f. Es claro que $F(X,Y,Z)$ es un polinomio homogéneo de grado d, y que $f(x,y) = F(X,Y,1)$. Además como existe $a_{ij} \neq 0$ tal que $i+j = d$, entonces $Z^{d-i-j} = 1$. Por lo tanto $F(X,Y,0)$ no es el polinomio cero, es decir la curva definida por $F(X,Y,Z) = 0$ no contiene a todos los puntos al infinito. Así hemos visto que hay una correspondencia biyectiva entre las curvas afines en $\mathbb{C}P^2$ y las curvas proyectivas en $\mathbb{C}P^2$ que no contienen la linea al infinito.

Para una curva $C : F(X,Y,Z) = 0$ y $P \in C$, decimos que $P = [a,b,c]$ es un punto *singular* de C si

$$\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = 0.$$

Si $P = [a,b,c]$ es un punto de la curva C y $c \neq 0$, entonces P es singular en C si y sólo si $P_0 = (\frac{b}{a}, \frac{c}{a})$ es singular en la curva afín $C_0 = F(1,Y,Z) = 0$.

Analogamente se verifica para los otros casos en donde $a \neq 0$ ó $b \neq 0$. Es decir una curva proyectiva es no singular si y sólo si ésta es no singular al verla en cada uno de los planos afines.

Decimos que $C : F(X, Y, Z) = 0$ es una *curva no singular* (o suave) si esta es no singular en todos sus puntos.

Los siguientes resultados nos permiten poder tratar a las curvas elípticas desde otro enfoque, y en el cual desarrollaremos gran parte de nuestro objetivo, el de clasificar la Familia de curvas elípticas.

Proposición 5 *Si C es una curva afín no singular dada por un polinomio $f(x, y)$. Entonces C es una superficie de Riemann.*

Demostración: Sea $p = (x_0, y_0) \in C$. Si $\dfrac{\partial f}{\partial y}(p) \neq 0$, entonces por el Teorema de la Función implícita, existe una función $g_p(x)$ tal que en una vencidad U_p de p, C es la gráfica $y = g_p(x)$. Por lo tanto la proyección $\Pi_x : U_p \longrightarrow C$ que manda (x, y) a x es un homeomorfismo sobre su imagen. Además $\Pi_x(U)$ es abierto en $\mathbb{C}$. Analogamente, si $\dfrac{\partial f}{\partial x}(p) \neq 0$, entonces hacemos una construcción idéntica usando la otra proyección Π_y.

Como C es una curva no singular, entonces para cada $p \in C$ se tiene que al menos una de sus parciales no se anulan, y así $\{U_p\}_{p \in C}$ es una cubierta para C.

Veamos que cualesquiera dos cartas son compatibles. Supóngamos primero que estas se obtienen por la proyección Π_x. Entonces, si hay intersección no vacía con sus dominios, la composición de una de estas con la inversa de la otra es la identidad, que ciertamente es holomorfa. De igual manera para el caso en que las cartas se obtienen ambas por la proyección Π_y.

Ahora supongamos que una carta se obtiene de Π_x y otra de Π_y y sea $p = (x_0, y_0)$ un punto en común en U. Como cerca de p, C es localmente de la forma $y = g(x)$ para alguna función holomorfa g, entonces en $\Pi_x(U)$, cerca de x_0 se tiene que el inverso de Π_x manda a x a $(x, g(x))$. Por lo tanto la composición $\Pi_y \circ \Pi_x^{-1}$ manda x a $g(x)$, la cual es holomorfa. Esto prueba que cualesquiera dos cartas son compatibles.

Por último C es un espacio Hausdorff, pues $\mathbb{C}^2$ lo es y C es conexo ya que $f(x, y)$ es no singular y en particular irreducible. Con esto concluimos que C es una superficie de Riemann. □

El espacio $\mathbb{C}P^2$ puede ser cubierto por los conjuntos $U_0 = \{[x, y, z] : x \neq 0\}$; $U_1 = \{[x, y, z] : y \neq 0\}$; $U_2 = \{[x, y, z] : z \neq 0\}$

Cada conjunto U_i es homeomorfo al punto afín $\mathbb{C}^2$. El homeomorfismo para

U_0 está dado por mandar $[x, y, z]$ a $(\frac{y}{x}, \frac{z}{x}) \in \mathbb{C}^2$; el inverso es el que manda $(a, b) \in \mathbb{C}^2$ a $[1, a, b] \in \mathbb{C}P^2$. Para los otros es análogo.

Definimos $D_0 = \{p \in U_0 : \|\phi_0(p)\| = 1\}$ y analogamente a D_1 y D_2. Entonces $\mathbb{C}P^2$ está cubierto por los conjuntos D_i, los cuales son compactos. Por lo tanto $\mathbb{C}P^2$ es compacto.

Sea ϕ_0 el homeomorfismo de U_0 a $\mathbb{C}^2$ que manda $[x, y, z]$ a $(\frac{y}{x}, \frac{z}{x})$.
Sea $F(X, Y, Z) \in \mathbb{C}[X, Y, Z]$ un polinomio homogéneo no singular, y sea $\mathcal{X}$= $\{[X, Y, Z] \in \mathbb{C}P^2 : F(X, Y, Z) = 0\}$.
Definimos $\mathcal{X}_i$= $\mathcal{X} \cap U_i$ y notamos que los U_i cubren a $\mathcal{X}$. Como cada $\mathcal{X}_i$ se puede ver como una curva afín en $\mathbb{C}^2$ no singular, entonces por la proposición 5, cada $\mathcal{X}_i$ es una superficie de Riemann, y así obtenemos cartas complejas para $\mathcal{X}$. Además es fácil ver que cualesquiera dos de estas cartas con intersección no vacía son compatibles. Por lo tanto $\mathcal{X}$ resulta ser una Superficie de Riemann. Como $\mathcal{X}$ es el conjunto de ceros de una función continua, $\mathcal{X}$ es cerrado, y así $\mathcal{X}$ es compacto pues $\mathbb{C}P^2$ lo es.
La fórmula del grado nos dice que si $\mathcal{X}$ es una curva proyectiva no singular de grado d, entonces el género de $\mathcal{X}$ está dado por

$$g_{\mathcal{X}} = \frac{(d-1)(d-2)}{2}.$$

Entonces con el anterior análisis, usando la fórmula del grado y el Teorema de Abel-Jacobi, concluimos el siguiente Teorema.

Teorema 5 *Sea $\mathcal{X}$ una curva proyectiva no singular de grado 3. Entonces $\mathcal{X}$ es un Toro Complejo.* □

2.6. Apéndice A: El Toro Topológico

Sea $I = [0, 1] \times [0, 1] \subseteq \mathbb{R}^2$. Definimos la relación " $\sim$ " en I dada de la siguiente forma:

Para (a_1, a_2) y (b_1, b_2) en I, decimos que $(a_1, a_2) \sim (b_1, b_2)$ sii

$$b_1 = a_1 + t$$

y

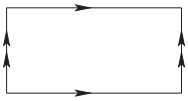
$$b_2 = a_2 + t,$$

con $t \in \{0, 1\}$.

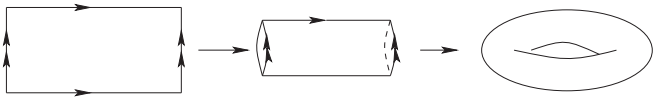
Es fácil ver que $\sim$ es de equivalencia en I y para $\bar{x} \in I$, denotamos por $[\bar{x}]$ la clase de $\bar{x}$ (respecto a $\sim$) y $I/\sim := \{[\bar{x}] : x \in I\}$.

Ahora consideramos $\pi : I \longrightarrow I/\sim$, donde $\pi(\bar{x}) = [\bar{x}]$, que es claramente sobre. Entonces si $A \subseteq I/\sim$, decimos que A es abierto en $I/\sim$ sii $\pi^{-1}(A)$ es abierto en I. De esta manera $I/\sim$ es un espacio topológico y π es una función continua, y como I es compacto y conexo, entonces $I/\sim$ también lo es.

$I/\sim$ es llamado el toro topológico y suele denotarse por la figura



Geométricamente $I/\sim$ se ve como:



2.7. Apéndice B: El Espacio Proyectivo $\mathbb{C}P^n$

Consideramos a $\mathbb{C}^{n+1}$ y $V := \mathbb{C}^{n+1} - \{(0, 0, ..., 0)\}$.

Decimos que dos vectores $z, w \in V$ son equivalentes y escribimos $z \sim w$, si y sólo si existe $\lambda \in \mathbb{C}^*$ tal que $z = \lambda w$. Claramente esta es una relación de equivalencia en V y denotamos por $[z] := \{w \in V : w \sim z\}$.

El espacio proyectivo complejo $n-$dimensional es el conjunto definido como $\mathbb{C}P^n := \{[z] : z \in V\}$. Si $z = (z_0, z_1, ..., z_n) \in V$, escribimos $[z] = [z_0 : z_1 : ... : z_n]$ las cuales llamamos *coordenadas homogeneas de z.*

Denotemos por $A^n(\mathbb{C}) := \{[z] \in \mathbb{C}P^n : z = (z_0, z_1, ..., z_n) \in \mathbb{C}^{n+1}, z_0 \neq 0\}$.

Observación: La aplicación

$$\mathbb{C}^n \longrightarrow A^n(\mathbb{C}) \subseteq \mathbb{C}P^n$$

$$(z_1, ..., z_n) \longmapsto [1, z_1, ..., z_n]$$

es una biyección, con inversa

$$A^n(\mathbb{C}) \longrightarrow \mathbb{C}^n$$

$$[z_0, z_1, ..., z_n] \longmapsto (\frac{z_1}{z_0}, \frac{z_2}{z_0}, ..., \frac{z_n}{z_0}).$$

$A^n(\mathbb{C}) \subseteq \mathbb{C}P^n$ es llamada *la parte $finita$*, y $\mathbb{C}P^n \setminus A^n(\mathbb{C})$ es llamada *la parte $infinita$* (o los puntos al infinito).

Observación: La aplicación

$$\mathbb{C}P^{n-1} \longrightarrow \mathbb{C}P^n \setminus A^n\mathbb{C}$$

$$[z_1, ..., z_n] \longmapsto [0, z_1, ..., z_n]$$

es una biyección.

Capítulo 3

Moduli de Curvas Elípticas no singulares.

Este capítulo tiene como objetivo principal parametrizar la Familia de Toros Complejos hasta isomorfismo.

3.1. Funciones Elípticas y Propiedades.

En esta sección iniciaremos el estudio de las funciones definidas en el toro complejo.

Denotemos por $\hat{\mathbb{C}}$ a la esfera de Riemann ($\mathbb{C} \cup \{\infty\}$).

Definición. Sean $w_1, w_2 \in \mathbb{C}$ tal que $w_1/w_2 \notin \mathbb{R}$ y$L = \mathbb{Z}w_1 \oplus \mathbb{Z}w_2$, entonces una función $f : \mathbb{C} \longrightarrow \hat{\mathbb{C}}$ meromorfa es llamada elíptica respecto a L si:

$f(z + w) = f(z)\ \forall w \in L$.

Considerando el siguiente diagrama

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{f} & \mathbb{CP}^1 \\ & \searrow^{\pi} & \uparrow \tilde{f} \\ & & \mathbb{C}/L \end{array}$$

donde $\pi(z) = [z]$, sabemos que existe una única $\bar{f} : \mathbb{C}/L \longrightarrow \hat{\mathbb{C}}$ tal que el diagrama conmuta, entonces $\bar{f}$ es la aplicación $[z] \longmapsto f(z)$.

La unicidad de $\bar{f}$ sólo depende de f, esto nos permite referirnos sin cuidado a f como una función bien definida en $\mathbb{C}/L$.

Teorema 6 *Una función elíptica sin polos es constante.*

Demostración: Sea $P_L = \{sw_1 + tw_2 : 0 \leq s, t \leq 1\}$. Como f no tiene polos entonces f es entera, por lo que f es continua en $\mathbb{C}$ y por tanto $f(P_L) \subseteq \mathbb{C}$ es compacto. Pero $f(\mathbb{C}) = f(P_L)$, por lo tanto $f(\mathbb{C})$ es compacto y así acotado. Entonces f es entera y acotada y por teorema de Liouville, f es constante. □

Proposición 6 *Si $f(z)$ y $g(z)$ son funciones elípticas, entonces*
i)$f(z) + c$
ii)$1/f(z)$
iii)$f(z) \cdot g(z)$
iv)$f\prime(z)$
son también elípticas.

Demostración:
i) Es obvio.

ii) Supongamos que f es no constante. Como $f(z)$ es elíptica, entonces $\dfrac{1}{f(z+w)} = \dfrac{1}{f(z)}$ $\forall w \in L$.
Ahora los polos de $1/f(z)$ se corresponden con los ceros de $f(z)$ y estos forman un conjunto discreto en $\mathbb{C}$, pues si no:
Sea $R = \mathbb{C} - D$, $D = \{z \in \mathbb{C} : f(z) = \infty\}$, entonces f es analítica en R.
Sea $A = \{z \in \mathbb{C} : f(z) = 0\}$, entonces si A no es discreto en $\mathbb{C}$, existe $\{z_n\} \subseteq A$ sucesión infinita y convergente a un punto z. Como f es continua, entonces $z \in A$ y por el teorema 2.2, f es identicamente cero en R, por lo tanto $f(z)$ es la constante cero en $\mathbb{C}$ y esto contradice la hipótesis, por lo tanto A es discreto en $\mathbb{C}$ y así concluimos que $1/f(z)$ es meromorfa. Entonces $1/f(z)$ es elíptica.

iii) $f(z+w) \cdot g(z+w) = f(z) \cdot g(z)$ $\forall w \in L$.
Ahora los polos de $f(z) \cdot g(z)$ es la unión de los polos de $f(z)$ y $g(z)$ y como la unión finita de discretos es discreto, por lo tanto $f(z) \cdot g(z)$ es meromorfa y así elíptica.

iv) Los polos de $f'(z)$ se corresponden con los polos de $f(z)$.
Ahora sea $z_0 \in \mathbb{C}$ y $w \in L$, entonces.

$$f'(z_0 + w) = \lim_{z \to z_0 + w} \frac{f(z) - f(z_0 + w)}{z - (z_0 + w)}$$

y con el cambio $\bar{z} = z - w$,

$$f'(z_0 + w) = \lim_{\bar{z} \to z_0} \frac{f(\bar{z} + w) - f(z_0)}{\bar{z} - z_0} = \lim_{\bar{z} \to z_0} \frac{f(\bar{z}) - f(z_0)}{\bar{z} - z_0} = f'(z_0)$$

$\therefore f'(z)$ es elíptica.

Proposición 7 *Si $f(z)$ es una función elíptica, entonces la suma de los residuos de $f(z)$ dentro de P es igual a cero.*

Demostración: Como el conjunto de polos de f es discreto en $\mathbb{C}$, entonces sin pérdida de generalidad podemos suponer que es analítica en ∂P. Aplicando el teorema del residuo obtenemos que

$$\sum_P Res(f) = \frac{1}{2\pi i}\int_{\partial P} f(z)dz$$

Ahora

$$\int_{\partial P} f(z)dz = \int_0^{w_2} f(z)dz + \int_{w_2}^{w_1+w_2} f(z)dz + \int_{w_1+w_2}^{w_1} f(z)dz + \int_{w_1}^{0} f(z)dz$$

pero haciendo $w = z - w_2$, notamos que

$$\int_{w_2}^{w_1+w_2} f(z)dz = -\int_{w_1+w_2}^{w_2} f(z)dz = -\int_{w_1}^{0} f(w+w_2)dw = -\int_{w_1}^{0} f(w)dw$$

De manera similar se observa que

$$\int_{w_1+w_2}^{w_1} f(z)dz = -\int_0^{w_2} f(z)dz \therefore \int_{\partial P} f(z)dz = 0$$

y así concluimos que

$$\sum_P Res(f) = 0.\square$$

Lema 1 *Si $f(z)$ es elíptica no constante, entonces f es sobre en $\hat{\mathbb{C}}$.*

Demostración: Si $c = \infty$, el resultado es válido por el Teorema 1. Sea $c \neq \infty$. Ahora si $f(z) = c$ no tiene solución, entonces $1/f(z) - c$ es entera y por la proposición 1, es también elíptica, por tanto $1/f(z) - c$ es constante y así entonces $f(z)$ es constante. Lo cual es una contradicción. Por lo tanto $f(z)$ es sobre. $\square$

Para una función elíptica f, el conjunto $S(f) = \{z \in \mathbb{C} : f(z) = \infty\}$ es discreto pues f es meromorfa. Entonces si P_L denota el Paralelogramo Fundamental asociado a la retícula L se tiene que $S(f) \cap P_L$ es un conjunto finito pues P_L es compacto. Esto nos permite hacer la siguiente definición:

Definición. Si f es una función elíptica no constante, definimos el orden de f y escribimos $ord(f) := \#S \cap P_L$.

Proposición 8 *Si f es elíptica de $ord(f) = m$ y n es el número de ceros de f contando multiplicidades, entonces $n - m = 0$.*

Demostración: Sea $h(z) = f'(z)/f(z)$, por la proposición 1, $h(z)$ es elíptica. Ahora si a es un cero de orden k de f, entonces cerca de a $f(z) = g(z)(z-a)^k$ con $g(z)$ analítica y $g(a) \neq 0$, entonces $f'(z) = k(z-a)^{k-1} + (z-a)^k g'(z)$ y por tanto $\dfrac{f'(z)}{f(z)} = \dfrac{k}{z-a} + \dfrac{g'(z)}{g(z)}$, entonces $h(z)$ tiene un polo simple en a con residuo k. De igual manera se observa que si b es un polo de orden l de f, entonces b es un polo simple con residuo $-l$ para $h(z)$.
Como los ceros y polos de f son los únicos polos de $f'(z)/f(z)$ se concluye que la suma de los residuos de $f'(z)/f(z)$ dentro del paralelogramo es igual a $n-m$ y por la proposición 5 $n-m=0$. □

Corolario 1 *Si $ord(f) = n$, entonces f toma cada valor de $\hat{\mathbb{C}}$ exactamente n-veces contando multiplicidad.*

Demostración: Para $c = \infty$ es definición. Sea $c \in \mathbb{C}$, $f(z) = c \iff g(z) = f(z) - c = 0$, como el orden de $g(z)$ es igual al de $f(z)$, entonces por la proposición anterior $g(z)$ tiene exactamente n ceros en el paralelogramo. □

Corolario 2 *Si f es elíptica, entonces $ord(f) > 1$.*

Demostración: Si $ord(f) = 1$, entonces existe un único polo simple z_0 de f con residuo $b_1 \neq o$, es decir

$$\sum Res(f) = b_1 \neq 0$$

esto contradice la proposición 5.

Lema 2 *La serie*

$$\sum_{(m,n)\in\mathbb{Z}\times\mathbb{Z}} \frac{1}{(m^2+n^2)^s}$$

$s \in \mathbb{R}$ y $(m,n) \neq (0,0)$ converge si y sólo si $s > 1$.

Demostración: Considerando el criterio de la integral, observamos que la serie converge si y sólo si

$$I = \int_{x^2+y^2\geq 1} \frac{dxdy}{(x^2+y^2)^s}$$

converge.
En coordenadas polares $x = r\cos\theta$ y $y = r\sin\theta$, I se ve como:

$$I = \int_0^{2\pi}\int_1^{\infty} \frac{rdrd\theta}{r^{2s}} = 2\pi\int_1^{\infty} \frac{dr}{r^{2s-1}}$$

la cual converge si y sólo si $s > 1$. □

Lema 3 *Sea $L \subset \mathbb{C}$ una retícula y $L' = L - \{0\}$. La serie*

$$\sum_{w \in L'} |w|^{-s}, s > 2$$

converge.

Demostración: Por el Lema 2 y por el criterio de comparación es suficiente probar que

$$\frac{1}{|mw_1 + mw_2|^2} \leq k \frac{1}{(m^2 + n^2)}$$

para alguna constante $k > 0$, sólo dependiendo de w_1 y w_2. Para esto es equivalente probar que la función $f(x, y) = \dfrac{|xw_1 + yw_2|^2}{x^2 + y^2}$ $(x, y) \in \mathbb{R}^2 \backslash \{\bar{0}\}$ tiene un mínimo global positivo.

Ahora sea $\lambda \in \mathbb{R}$ $\lambda \neq 0$, entonces

$$f(\lambda x, \lambda y) = \frac{|(\lambda x)w_1 + (\lambda y)w_2|^2}{(\lambda x)^2 + (\lambda y)^2} = \frac{|\lambda|^2 |xw_1 + yw_2|^2}{\lambda^2 (x^2 + y^2)} = f(x, y).$$

Por lo tanto $f(x, y)$ se puede ver como una función cuyo dominio es $S^1 = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$, el cual es compacto, y como $f(x, y)$ es continua en S^1, por lo tanto $f(x, y)$ alcanza un mínimo global y este es positivo. □

Proposición 9 *La serie*

$$\frac{1}{z^2} + \sum_{w \in L'} [\frac{1}{(z - w)^2} - \frac{1}{w^2}]$$

converge normalmente en $\mathbb{C} - L$.

Demostración: Equivalentemente probaremos que la serie converge absolutamente y uniformemente en $\bar{U}_r(0) - L$, donde $\bar{U}_r(0)$ es el disco cerrado de radio r y centrado en cero.

Ahora supóngase que $w \in L$ y $2r \leq |w|$. Sea $z \in \bar{U}_r(0)$, es decir, $|z| \leq r$, entonces $|z - 2w| \leq |z| + 2|w| \leq r + 2|w| \leq \dfrac{|w|}{2} + 2|w| = \dfrac{5}{2}|w|$. Ya que $|w| - |z| \geq 0$, $|z - w| \geq ||w| - |z|| = |w| - |z| \geq |w| - \dfrac{|w|}{2} = \dfrac{|w|}{2}$.

Entonces

$$|\frac{1}{(z - w)^2} - \frac{1}{w^2}| = \frac{|z||z - 2w|}{|w|^2 |z - w|^2} \leq \frac{10r}{|w|^3}$$

$\forall z$.

Nótese que el caso $|w| < 2r$ sólo incluye un número finito de sumandos a la

serie.

Utilizando El criterio M de Weierstrass ya que

$$\sum_{w\in L'} \frac{10r}{|w|^3}$$

converge, concluímos que

$$\frac{1}{z^2} + \sum_{w\in L'} [\frac{1}{(z-w)^2} - \frac{1}{w^2}]$$

converge absolutamente y uniformemente en $\bar{U}_r(0) - L$, por lo tanto la serie converge normalmente en $\mathbb{C} - L$. $\square$

En particular dicha serie converge puntualmente y absolutamente en $\mathbb{C} - L$. Esto nos permite introducir la siguiente función.

Definición. La función definida por la expresión

$$p(z) = \frac{1}{z^2} + \sum_{w\in L'} [\frac{1}{(z-w)^2} - \frac{1}{w^2}]$$

para $z \notin L$ y

$$p(z) = \infty$$

para $z \in L$ es llamada la función de Weierstrass relativa a L. Como cada término de la serie es una función analítica en $\mathbb{C} - L$ y la convergencia es normal, entonces por el Teorema de la convergencia analítica concluimos que $p(z)$ es analítica en $\mathbb{C} - L$.

Ahora si $V(0)$ es una bola agujerada del cero que no contenga puntos de L, observamos que

$$p(z) = \frac{1}{z^2} + g(z)$$

donde

$$g(z) = \sum_{w\in L'} [\frac{1}{(z-w)^2} - \frac{1}{w^2}]$$

es analítica en $V(0)$ y por tanto $z_0 = 0$ es un polo de orden 2 para $p(z)$.

Analogamente si $a \in L - \{0\}$ y $V(a)$ es una bola centrada en a y no contiene puntos de L, entonces

$$p(z) = \frac{1}{(z-a)^2} + g_a(z)$$

donde

$$g_a(z) = \frac{1}{z^2} - \frac{1}{a} + \sum_{w\in L'-\{a\}} [\frac{1}{(z-w)^2} - \frac{1}{w^2}]$$

es analítica en $V(a)$ y por tanto a es un polo de orden 2 para $p(z)$.

De esta manera concluímos que $p(z)$ es meromorfa en $\mathbb{C}$ y sus polos se encuentran exactamente en la retícula L.

Ahora como $w \in L'$ si y sólo si $-w \in L'$, entonces $p(-z) = p(z)$ es decir $p(z)$ es una función par.

Lema 4 *La derivada de la función de Weierstrass es meromorfa en $\mathbb{C}$ y está dada por la fórmula:*

$$p'(z) = -2 \sum_{w \in L} \frac{1}{(z-w)^3}$$

$z \in \mathbb{C} - L$. Los puntos de L son los polos de $p'(z)$ y tienen orden 3.

Demostración: Debido a la convergencia normal de $p(z)$ en $\mathbb{C} - L$, sabemos que podemos diferenciar esta término a término y por tanto

$$p'(z) = -\frac{2}{z^3} + \sum_{w \in L'} -\frac{2}{(z-w)^3} = -2 \sum_{w \in L} \frac{1}{(z-w)^3}$$

para $z \in \mathbb{C} - L$. Nótese también que los puntos de L son exactamente los polos de $p'(z)$ y tienen orden 3 ya que para cada $w_0 \in L$

$$p'(z) = -\frac{2}{(z-w_0)^3} + \sum_{w \in L - \{w_0\}} -\frac{2}{(z-w)^3}$$

donde la parte que corresponde a la serie es analítica en alguna vecindad agujerada de w_0. □

Observación: $p'(z)$ es impar pues $p(z)$ es par.

Proposición 10 *La función de Weierstrass $p(z)$ para la retícula L es una función elíptica de orden dos y $p'(z)$ es una función elíptica de orden tres.*

Demostración: Sea $w_0 \in L$, entonces tenemos que $w \in L$ si y sólo si $w - w_0 \in L$ y como

$$p'(z) = -2 \sum_{w \in L} \frac{1}{(z-w)^3}$$

es absolutamente convergente, entonces

$$p'(z + w_0) = -2 \sum_{w \in L} \frac{1}{(z + w_0 - w)} = p'(z)$$

Así vemos que $p'(z)$ es periódica en L y el cero es el único polo *(mod 1)* de $p'(z)$, este es de orden 3. Por lo tanto $p'(z)$ es una función elíptica de orden tres.

Ahora de la igualdad $p'(z+w_0) - p'(z) = 0$ $w_0 \in L$, y tomando primitivas en ambos lados, concluímos que $\forall z \in \mathbb{C} - L$, $p(z+w_0) - p(z) = c_{w_0}$, c_{w_0} constante. Veamos que $c_{w_0} = 0$ $\forall w_0 \in L$.

Podemos suponer que w_0 se encuentra en una base para L, entonces $\frac{1}{2}w_0$ no está en L. Calculando para $z = -\frac{1}{2}w_0$ y usando que $p(z)$ es par, obtenemos que
$p(-\frac{1}{2}w_0 + w_0) - p(-\frac{1}{2}w_0) = p(\frac{1}{2}w_0) - p(\frac{1}{2}w_0) = 0$

Así concluimos que $p(z)$ es periódica en L y sabemos que es meromorfa en $\mathbb{C}$, con el cero el único polo de $p(z)$ *(mod L)*, este de orden dos. Por lo tanto $p(z)$ es una función elíptica de orden dos. □

Lema 5 *Un punto $a \in \mathbb{C}$ es cero de $p'(z)$, si y sólo si $a \notin L$ y $2a \in L$.*

Demostración: Supongamos que a es tal que $a \notin L$ y $2a \in L$, entonces $p'(a) = p'(a-2a)$ (pues $-2a \in L$), entonces $p'(a) = p'(-a) = -p'(a)$ (pues $p'(z)$ es impar), por tanto $p'(a) = 0$.

De esta manera si $L = \mathbb{Z}w_1 \oplus \mathbb{Z}w_2$, entonces $\frac{w_1}{2}, \frac{w_2}{2}$ y $\frac{w_3}{2} = \frac{w_1+w_2}{2}$ son ceros de $p'(z)$ y por la proposición 3, son los únicos ceros de $p'(z)$ *(mod L)* pues el orden de $p'(z)$ es tres. □

Notación. Si $L = \mathbb{Z}w_1 \oplus \mathbb{Z}w_2$ y $p(z)$ es la función de Weierstrass para L; escribimos $e_1 := p(\frac{w_1}{2})$, $e_2 := p(\frac{w_2}{2})$, $e_3 := p(\frac{w_3}{2})$.

Observación. e_1, e_2 y e_3 no dependen de la base escogida para L, pues como $S = [\frac{1}{2}w_1] \cup [\frac{1}{2}w_2] \cup [\frac{1}{2}w_3]$ es el conjunto de todos los ceros de $p'(z)$ en $\mathbb{C}$, entonces $p(S) = \{e_1, e_2, e_3\}$ es independiente de la elección de la base. $[w]$ denota la clase de w *módulo L.*

Corolario 3 *Para cada $c \in \mathbb{C} - \{e_1, e_2, e_3\}$ la ecuación $p(z) = c$ tiene dos soluciones simples y para $c \in \{e_1, e_2, e_3, \infty\}$ la ecuación tiene una solución doble.*

Demostración: Sabemos que el orden de $p(z)$ es dos, entonces $p(z)$ toma cada valor en $\hat{\mathbb{C}}$ dos veces (con multiplicidad).

Ahora si $c \in \mathbb{C}$, entonces $p(z) = c$ tiene solución doble si y sólo si $p'(z) = 0$ y esto si y sólo si $z \in S$. Por lo tanto $c \in \{e_1, e_2, e_3\}$. Para $c = \infty$ sabemos que $z = 0$ es solución doble de $p(z) = c$. □

Corolario 4 *e_1, e_2 y e_3 son distintos entre sí.*

Demostración: Sea $f_j(z) = p(z) - e_j$, $j = 1, 2, 3$, entonces f_j es una función elíptica de orden dos y por lo tanto $f_j(z) = 0$ tiene dos soluciones en $\mathbb{C}/L$.

Como $f_j(\frac{1}{2}w_j) = 0 = f_j'(\frac{1}{2}w_j)$, entonces f_j tiene un cero doble en $z = \frac{1}{2}w_j$ y por tanto no hay mas ceros *(mod L)*. En particular $f_j(\frac{1}{2}w_k) \neq 0$ para $j \neq k$, pero $f_j(\frac{1}{2}w_k) = e_k - e_j$. Por lo tanto $e_j \neq e_k$ para $j \neq k$. □

3.2. La ecuación diferencial para $p(z)$.

En esta sección obtendremos una importante ecuación que conecta $p(z)$ y $p'(z)$, obtenida a partir de la serie de Laurent de $p(z)$ cerca de $z_0 = 0$.

Definimos

$$G_k := \sum_{w \in L'} \frac{1}{w^k}$$

que sabemos es absolutamente convergente para $k > 2$.

Ahora si $k > 2$ y es impar, entonces $G_k = 0$ pues para cada $w \in L$, $-w \in L$ y por tanto $\frac{1}{w^k} + \frac{1}{(-w)^k} = 0$ pues k es impar.

Consideremos ahora para $z \in \mathbb{C} - L$, la función

$$C(z) = \frac{1}{z} + \sum_{w \in L'} (\frac{1}{z-w} + \frac{1}{w} + \frac{z}{w^2}).$$

$C(z)$ está bien definida pues dado $z \in \mathbb{C} - L$, se cumple que

$$|\frac{1}{z-w} + \frac{1}{w} + \frac{z}{w^2}| = |\frac{z^2}{w^2(z-w)}| \leq k|w|^{-3},$$

k una constante que depende de z. Por tanto se tiene que la serie

$$\sum_{w \in L'} \frac{1}{z-w} + \frac{1}{w} + \frac{z}{w^2}$$

es absolutamente convergente para $z \in \mathbb{C} - L$.

Sabemos que

$$\sum_{n=0}^{\infty} z^n$$

es absolutamente convergente para $|z| < 1$ y que

$$\sum_{n=0}^{\infty} z^n = \frac{1}{1-z}$$

Ahora sea $m = min\{|w| : w \in L'\}$ y $D = \{z \in \mathbb{C} : |z| < m\}$ el disco abierto de máximo radio centrado en cero y que no contiene puntos de L. Por tanto dado $w \in L - \{0\}$ y $z \in D$, tenemos que $\frac{|z|}{|w|} < 1$ y así la serie

$$-\frac{1}{w} - \frac{z}{w^2} - \frac{z^2}{w^3} - \cdots = -\frac{1}{w}\sum_{n=0}^{\infty}(\frac{z}{w})^n = -\frac{1}{w}(\frac{1}{1-\frac{z}{w}}) = \frac{1}{z-w}$$

es absolutamente convergente para $z \in D$ y $w \in L - \{0\}$.

Despejando de la serie vemos que

$$\frac{1}{z-w} + \frac{1}{w} + \frac{z}{w^2} = -\sum_{n=2}^{\infty}\frac{z^n}{w^{n+1}}.$$

Ahora sustituimos en el término de la serie de $C(z)$ y obtenemos que

$$C(z) = \frac{1}{z} + \sum_{w \in L'}(-\sum_{n=2}^{\infty}\frac{z^n}{w^{n+1}})$$

y como ambas series son absolutamente convergentes, podemos cambiar el orden de la sumatoria y así obtenemos que

$$C(z) = \frac{1}{z} - \sum_{n=2}^{\infty}(\sum_{w \in L'}\frac{z^n}{w^{n+1}}) = \frac{1}{z} - \sum_{n=2}^{\infty} z^n(\sum_{w \in L'}\frac{1}{w^{n+1}}) = \frac{1}{z} - \sum_{n=2}^{\infty} G_{n+1}z^n = \frac{1}{z} - \sum_{n=2}^{\infty} G_{2n}z^{2n-1}$$

para $z \in D$ pues $G_n = 0$ si n es par $(n > 2)$.

Ahora nótese que

$$p(z) = -C'(z) = \frac{1}{z^2} + \sum_{n=2}^{\infty}(2n-1)G_{2n}z^{2n-2}$$

y por lo tanto esta es la expresión de Laurent de $p(z)$ cerca de $z_0 = 0$ $(z \in D)$.

Ahora entonces se verifican los siguientes cálculos:

$$p'(z) = -\frac{2}{z^3} + 6G_4 z + 20G_6 z^3 + ...,$$

y por tanto

$$p'(z)^2 = \frac{4}{z^6} - \frac{24G_4}{z^2} - 80G_6 + z^2\phi_1(z),$$

$$4p(z)^3 = \frac{4}{z^6} + \frac{36G_4}{z^2} + 60G_6 + z^2\phi_2(z),$$

$$60G_4p(z) = \frac{60G_4}{z^2} + z^2\phi_3(z),$$

donde $\phi_1(z), \phi_2(z), \phi_3(z)$ son series de potencias convergentes en D.

De estas tres últimas ecuaciones obtenemos que:

$$p'(z)^2 - 4p(z)^3 + 60G_4p(z) + 140G_6 = z^2\phi(z),$$

donde $\phi(z) = \phi_1(z) - \phi_2(z) + \phi_3(z)$.

Ahora como $p(z)$ y $p'(z)$ son elípticas, entonces

$$f(z) = p'(z)^2 - 4p(z)^3 + 60G_4p(z) + 140G_6$$

es también elíptica. Pero $f(z) = z^2\phi(z)$ en D y $\phi(z)$ es analítica en D, entonces $f(z)$ se anula en $z_0 = 0$ y por tanto se anula en todo L, pero como $f(z)$es una expresión polinomial de $p(z)$ y $p'(z)$, entonces $f(z)$ sólo puede tener polos en L, por tanto $f(z)$ es constante y $f(z) = 0\ \forall z \in \mathbb{C}$. De esta manera obtenemos el siguiente resultado:

Teorema 7

$$p'(z) = 4p(z)^3 - 60G_4p(z) - 140G_6$$

para $z \in \mathbb{C} - L$ □

Haciendo

$$g_2 = 60G_4,$$

$$g_3 = 140G_6,$$

la ecuación se ve así:

$$p'(z) = 4p(z)^3 - g_2p(z) - g_3$$

$z \in \mathbb{C} - L$.

3.3. La función j-invariante.

En este capítulo no trabajaremos con una retícula fija. Nos interesa identificar la familia de los Toros Complejos (módulo relación de isomorfismo).

3.3.1. El Grupo Modular Elíptico.

Esta sección inicia con la siguiente relación de equivalencia para retículas:

Definición. Dos retículas $L \subset \mathbb{C}$, $L' \subset \mathbb{C}$ son llamadas equivalentes y denotado por $L \sim L'$, si existe un número complejo $a \neq 0$, tal que $L' = aL$.

Sabemos que dos retículas L, L' son equivalentes si y sólo si $\mathbb{C}/L \approx \mathbb{C}/L$ (isomorfismo complejo).

Como $\frac{w_2}{w_1} \notin \mathbb{R}$, podemos también suponer que $Im(\frac{w_2}{w_1}) > 0$.

De esta manera se concluye que si $L = \mathbb{Z}w_1 \oplus \mathbb{Z}w_2$, entonces $L \approx L'$, donde $L' = \mathbb{Z} \oplus \mathbb{Z}\tau$ y $\tau \in \mathbb{H}$, i.e, $Im\tau > 0$.

Ahora la pregunta es:

Cuándo dos retículas L y L' son equivalentes, donde $L = \mathbb{Z} \oplus \mathbb{Z}\tau$ y $L' = \mathbb{Z} \oplus \mathbb{Z}\tau'$, $\tau, \tau' \in \mathbb{H}$?. $\mathbb{H} := \{z \in \mathbb{C} : Im(z) > 0\}$.

Por definición $L \approx L'$ si existe un número complejo $a \neq 0$ con la propiedad $L' = \mathbb{Z} \oplus \mathbb{Z}\tau' = a(\mathbb{Z} \oplus \mathbb{Z}\tau) = aL$.

En particular como τ' y 1 son elementos de L' y $L' = aL$, entonces podemos escribir

$$\tau' = a(\alpha\tau + \beta)$$

y

$$1 = a(\gamma\tau + \delta),$$

donde $\alpha, \beta, \gamma, \delta$ son algunos enteros.

Ahora si dividimos estas dos ecuaciones, obtenemos que

$$\tau' = \frac{\alpha\tau + \beta}{\gamma\tau + \delta}.$$

Así se observa que el punto τ' se obtiene a partir de τ mediante una importante aplicación, una transformación de Möbius con coeficientes enteros.

Veamos que podemos saber más sobre estos coeficientes.

Para esto obtenemos el siguiente resultado:

Lema 6 *Sea $\tau, \tau' \in \mathbb{H}$ tal que*

$$\tau' = \frac{\alpha\tau + \beta}{\gamma\tau + \delta}$$

para $\alpha, \beta, \gamma, \delta$ enteros, entonces $\alpha\delta - \beta\gamma > 0$.

Demostración: Calculemos la parte imaginaria de

$$\tau' = \frac{\alpha\tau + \beta}{\gamma\tau + \delta}$$

$$Im(\tau') = \frac{1}{2i}[\frac{\alpha\tau + \beta}{\gamma\tau + \delta} - \frac{\alpha\bar{\tau} + \beta}{\gamma\bar{\tau} + \delta}] = \frac{1}{2i}\frac{(\alpha\tau + \beta)(\gamma\bar{\tau} + \delta) - (\alpha\bar{\tau} + \beta)(\gamma\tau + \delta)}{|\gamma\tau + \delta|^2}.$$

Si denotamos por $D = \alpha\delta - \beta\gamma$ el determinante de la matriz

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

entonces obtenemos que

$$Im(\tau') = Im(\frac{\alpha\tau + \beta}{\gamma\tau + \delta}) = \frac{D \cdot Im\tau}{|\gamma\tau + \delta|^2}.$$

Como en nuestro caso estamos interesados cuando τ y $\tau' \in \mathbb{H}$, entonces $\alpha\delta - \beta\gamma > 0$. $\square$

Regresamos otra vez a la suposición de que $L \approx L'$, es decir $L' = \mathbb{Z} \oplus \mathbb{Z}\tau' = a(\mathbb{Z} \oplus \mathbb{Z}\tau) = aL$, $a \neq 0$.

Ya vimos que $1, \tau' \in aL$ nos implican que

$$\tau' = a(\alpha\tau + \beta)$$

y

$$1 = a(\gamma\tau + \delta)$$

con $\alpha, \beta, \gamma, \delta$ enteros. Esto en un lenguaje matricial se escribe como

$$\begin{pmatrix} \tau' \\ 1 \end{pmatrix} = aM \cdot \begin{pmatrix} \tau \\ 1 \end{pmatrix},$$

con M una matriz 2×2 y coeficientes enteros.

Analogamente como a y $a\tau$ están en L', entonces podemos escribir esto matricialmente así:

$$a\begin{pmatrix} \tau \\ 1 \end{pmatrix} = N \cdot \begin{pmatrix} \tau' \\ 1 \end{pmatrix}$$

con N una matriz entera.

Ahora juntando estas dos expresiones matriciales obtenemos que

$$\begin{pmatrix} \tau \\ 1 \end{pmatrix} = N \cdot M \begin{pmatrix} \tau \\ 1 \end{pmatrix}$$

Como τ y 1 son $\mathbb{R} - linealmente\ independientes$, entonces $N \cdot M = I$, donde

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix};$$

Pues supóngase que $x, y \in \mathbb{R}^2$ son linealmente independientes y que cumplen con que

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix},$$

a,b,c,d reales, entonces

$$x = ax + by \Longrightarrow 0 = (a-1)x + by$$

$$y = cx + dy \Longrightarrow 0 = cx + (d-1)y$$

Como x, y son $\mathbb{R} - linealmente\ independientes$, entonces concluimos que $a = 1$, $b = 0$, $c = 0$ y $d = 1$.

Por tanto

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

Por tanto como $N \cdot M = I$, entonces $detN \cdot detM = 1$, entonces $detM = \pm 1$.Por el Lema 5 $detM = 1$.

Hasta ahora hemos visto que si

$$L' = \mathbb{Z} \oplus \mathbb{Z}\tau' = a(\mathbb{Z} \oplus \mathbb{Z}\tau) = aL,$$

entonces

$$\tau' = \frac{\alpha\tau + \beta}{\gamma\tau + \delta},$$

donde $\alpha, \beta, \gamma, \delta$ son enteros tal que $\alpha\delta - \beta\gamma = 1$

Ahora inversamante supóngase que τ', τ estan en $\mathbb{H}$ y que

$$\tau' = \frac{\alpha\tau + \beta}{\gamma\tau + \delta}$$

con $\alpha, \beta, \gamma, \delta$ enteros y γ, δ distintos de cero, entonces

$$L' = \mathbb{Z} \oplus \mathbb{Z}\tau' = \mathbb{Z}\frac{\gamma\tau + \delta}{\gamma\tau + \delta} + \mathbb{Z}\frac{\alpha\tau + \beta}{\gamma\tau + \delta} = \frac{1}{\gamma\tau + \delta}(\mathbb{Z}\gamma\tau + \delta \oplus \mathbb{Z}\alpha\tau + \beta) = \frac{1}{\gamma\tau + \delta}(\mathbb{Z} \oplus \mathbb{Z}\tau) = \frac{1}{\gamma\tau + \delta} \cdot L$$

Por lo tanto $L' \approx L$ para $a = \dfrac{1}{\gamma\tau + \delta}$.

Definición. El grupo modular elíptico.

$$\Gamma = \mathbf{SL}(2,\mathbb{Z}) := \{M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} : \alpha,\beta,\gamma,\delta \in \mathbb{Z}, \alpha\delta - \beta\gamma = 1\}$$

es el grupo de matrices 2×2 con coeficientes enteros y determinante uno. La operación de grupo es la multiplicación.

Con esta definición podemos ya presentar el siguiente resultado:

Teorema 8 *Dos retículas de la forma* $\mathbb{Z} \oplus \mathbb{Z}\tau$ *y* $\mathbb{Z} \oplus \mathbb{Z}\tau'$, $\tau, \tau' \in \mathbb{H}$ *son equivalentes si y sólo si existe una matriz* $M \in \Gamma$ *tal que* $\tau' = M\tau$. □

Naturalmente se introduce la siguiente definición:

La aplicación

$$\Gamma \times \mathbb{H} \longrightarrow \mathbb{H}$$
$$(M, \tau) \longrightarrow M\tau$$

define una acción de Γ en $\mathbb{H}$.

Definición. Decimos que dos puntos $\tau, \tau' \in \mathbb{H}$ son equivalentes y escribimos $\tau \sim \tau'$, si existe $M \in \Gamma$, tal que $\tau' = M\tau$.

Claramente esta es una relación de equivalencia en $\mathbb{H}$.

Usaremos frecuentemente la siguiente notación:

$$[\tau] := \{M \cdot \tau : M \in \Gamma\}, \tau \in \mathbb{H}$$

$$\mathbb{H}/\Gamma := \{[\tau] : \tau \in \mathbb{H}\}.$$

Ya con esta notación y usando el Teorema 3, podemos decir entonces que las clases de equivalencia de retículas se corresponden en biyección con $\mathbb{H}/\Gamma$.

Teorema 9 $\mathbb{H}/\Gamma$ *es una superficie de Riemann.*

Teorema 10 *La proyección canónica* $\Pi : \mathbb{H} \longrightarrow \mathbb{H}/\Gamma$ *es holomorfa.* □

Ahora nuestro siguiente gran propósito es conocer la estructura de $\mathbb{H}/\Gamma$.

Recordemos que

$$g_2(L) := 60G_4(L)$$

y

$$g_3(L) := 140G_6(L),$$

donde

$$G_k(L) := \sum_{w \in L - \{0\}} w^{-k}$$

es convergente para $k \geq 3$.

Los números $g_2(L)$ y $g_3(L)$ dependen por supuesto de la retícula L, pero para retículas equivalentes vemos que como

$$G_k(aL) = a^{-k}G_k(L),$$

entonces en particular

$$g_2(aL) = a^{-4}g_2(L)$$

y

$$g_3(aL) = a^{-6}g_3(L).$$

Denotemos $\Delta(L) := g_2^3(L) - 27g_3^2(L)$ y es llamado discriminante de L.

Como e_1, e_2 y e_3 son las tres raices de $p'(z)$ *(mod L)* y estas son todas distintas y $g_2(L)$, $g_3(L)$ son los coeficientes de la ecuación diferencial para $p'(z)$, entonces $g_2^3(L) - 27g_3^2(L) \neq 0$. Es decir, para cada retícula $L = \mathbb{Z}w_1 \oplus \mathbb{Z}w_2$, $\Delta(L) \neq 0$.

Entonces vemos que

$$\Delta(aL) = g_2^3(aL) - 27g_3^2(aL) = (a^{-4}g_2(L))^3 - 27(a^{-6}g_3(L))^2 = a^{-12}g_2^3(L) - a^{-12}(27g_3^2(L)) = a^{-12}\Delta(L)$$

Por lo tanto

$$\frac{g_2^3(aL)}{\Delta(aL)} = \frac{a^{-12}g_2^3(L)}{a^{-12}\Delta(L)} = \frac{g_2^3(L)}{\Delta(L)}$$

Así obtenemos una fórmula invariante para retículas equivalentes. Denotamos por

$$j(L) = \frac{g_2^3(L)}{\Delta(L)}$$

y por tanto

$$j(aL) = j(L), a \in \mathbb{C} - \{0\}$$

Esta invarianza en clases de equivalencia de retículas, nos sugiere trabajar directamente en $\mathbb{H}/\Gamma$.

Sea $\tau \in \mathbb{H}$ y $L = \mathbb{Z} \oplus \mathbb{Z}\tau$, entonces denotamos por

$$G_k(\tau) = \sum_{(m,n)\in(\mathbb{Z}\times\mathbb{Z})'} (m + n\tau)^{-k} := G_k(L),$$

donde $(\mathbb{Z} \times \mathbb{Z})' = \mathbb{Z} \times \mathbb{Z} - \{(0, 0)\}$

Analogamente definimos las siguientes funciones definidas en el semiplano superior $\mathbb{H}$:

$$g_2(\tau) := 60G_4(\tau),$$

$$g_3(\tau) := 140G_6(\tau),$$

$$\Delta(\tau) := g_2^3(\tau) - 27g_3^2(\tau)$$

y

$$j(\tau) = \frac{g_2^3(\tau)}{\Delta(\tau)}.$$

Como la propiedad $j(aL) = j(L)$ es equivalente a que

$$j(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}) = j(\tau), para \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma,$$

entonces hemos obtenido una función

$$j : \mathbb{H} \longrightarrow \mathbb{C}$$

invariante bajo la acción del grupo modular Γ en $\mathbb{H}$;

$$j(\tau) = \frac{g_2^3(\tau)}{g_2^3(\tau) - 27g_3^2(\tau)}.$$

$j(\tau)$ es llamada la función $j - invariante$.

Lema 7 *$G_k(\tau)$ define una función analítica en $\mathbb{H}$.*

Demostración: Por el Teorema de convergencia analítica es suficiente probar que

$$G_k(\tau) = \sum_{(m,n)\in(\mathbb{Z}\times\mathbb{Z})'} (m+n\tau)^{-k}$$

converge absolutamente y uniformemente en cualquier disco cerrado de $\mathbb{H}$, para $k > 2$.

Ahora entonces; sea $\tau_0 \in \mathbb{H}$ y sea $\delta = \frac{1}{2}Im(\tau_0) > 0$. También denotamos por $k(\tau_0) = \{\tau \in \mathbb{H} : |\tau - \tau_0| \leq \delta\}$.

Si $m, n \in \mathbb{Z}$, $n \neq 0$, $-\frac{m}{n} \in \mathbb{R}$ y por tanto $|\frac{m}{n} + \tau_0| \geq Im(\tau_0) = 2\delta$; entonces se vale que

$$|(m+n\tau) - (m+n\tau_0)| = |n||\tau - \tau_0| \leq |n|\delta \leq \frac{1}{2}|m+n\tau_0|,$$

entonces aplicando la desigualdad del triángulo concluímos que

$$|m+n\tau| \geq |m+n\tau_0| - |(m+n\tau) - (m+n\tau_0)| \geq \frac{1}{2}|m+n\tau_0|,$$

esto para todo $\tau \in k(\tau_0)$ y $(m,n) \in \mathbb{Z}\times\mathbb{Z}$.

Por lo tanto

$$\frac{1}{|m+n\tau|^k} \leq \frac{1}{|m+n\tau_0|^k}, k > 1$$

$\forall \tau \in k(\tau_0)$ y $\forall (m,n) \neq (0,0)$.

Aplicando el criterio M de Weierstrass concluimos que

$$\sum_{(m,n)\in(\mathbb{Z}\times\mathbb{Z})'} \frac{1}{(m+n\tau)^k}$$

converge absolutamente y uniformemente en $k(\tau_0)$, para $k > 2$. Por lo tanto

$$\sum_{(m,n)\in(\mathbb{Z}\times\mathbb{Z})'} (m+n\tau)^{-k}$$

define una función analítica en $\mathbb{H}$. $\square$

Corolario 5 *La función $j-$invariante es una función analítica en el semiplano superior $\mathbb{H}$.*

Demostración: Como $G_k(\tau)$ es analítica en $\mathbb{H}$ para $k > 2$, entonces es claro que $g_2(\tau) = 60G_4(\tau)$ y $g_3(\tau) = 140G_6(\tau)$ son analíticas en $\mathbb{H}$ y claro también $\Delta(\tau) = g_2^3(\tau) - 27g_3^2(\tau)$ es analítica en $\mathbb{H}$ y como $\Delta(\tau) \neq 0\ \forall \tau \in \mathbb{H}$, entonces $j(\tau) = g_2^3(\tau)/\Delta(\tau)$ es analítica en $\mathbb{H}$. $\square$

Teorema 11 *La función $j : \mathbb{H} \longrightarrow \mathbb{C}$ es sobreyectiva.*

Demostración: Como $j : \mathbb{H} \longrightarrow \mathbb{C}$ es holomorfa, entonces por el teorema del mapeo abierto, $j(\mathbb{H}) \subseteq \mathbb{C}$ es abierto, pues $\mathbb{H} \subseteq \mathbb{C}$ es abierto.

Ahora veamos que $j(\mathbb{H})$ es cerrado. Sea $\{j(\tau_n)\} \subseteq j(\mathbb{H})$ una sucesión infinita y convergente a un punto $b \in \mathbb{C}$, $j(\tau_n) \longrightarrow b$.

Podemos suponer que $\tau_n \in R_\gamma$. Ahora supóngase también que existe una constante $c > 0$ tal que

$$Im(\tau_n) \leq c$$

para toda n. Entonces el conjunto

$$\{\tau \in R_\gamma : Im(\tau) \leq c\}$$

es compacto por ser cerrado y acotado. Por lo tanto existe $\{\tau_{n_k}\}$ una subsucesión convergente de $\{\tau_n\}$,

$$\tau_{n_k} \longrightarrow \tau,$$

$\tau \in \mathbb{H}$ y $Im(\tau) \leq c$.

Por continuidad de j, se tiene que $j(\tau_{n_k}) \longrightarrow j(\tau)$, pero $j(\tau_{n_k})$ es una subsucesión de $j(\tau_n) \longrightarrow b$. Entonces $j(\tau) = b$, y así $b \in j(\mathbb{H})$.

Por lo tanto $j(\mathbb{H}) \subseteq \mathbb{C}$ es abierto, cerrado y por supuesto no vacío. Entonces $j(\mathbb{H}) = \mathbb{C}$, j es sobre.

El caso en que $Im(\tau_n) \longrightarrow \infty$ es imposible, pues si es así, entonces $j(\tau_n) \longrightarrow \infty$, pero hemos supuesto que $j(\tau_n)$ es convergente.$\square$

Definición. Sea E una curva elíptica no singular, con ecuación $y^2 = 4x^3 - g_2x - g_3$. Definimos el *j-invariante de E*, y denotamos por $j(E) := \dfrac{g_2^3}{g_2^3 - g_3^2}$.

Notar que el $j - invariante$ está bien definido, pues como E es no singular $g_2^3 - g_3^2 \neq 0$.

Teorema 12 *Sean E y E' dos curvas elípticas no singulares. Entonces E y E' son isomorfas si y sólo si tienen el mismo $j - invariante$ i,e. $j(E) = j(E')$.*

Demostración: Consideremos las ecuaciones de las curvas elípticas E y E'. $E := y^2 = 4x^3 - g_2x - g_3$ y $E' : y^2 = 4x^3 - g_2'x - g_3'$. Al homogeneizar tales ecuaciones obtenemos dos curvas proyectivas $X_1, X_2 \subset \mathbb{C}P^2$ no singulares isomorfas de grado 3, es decir, $X_1 \cong X_2$. Por lo tanto tales curvas son dos toros complejos isomorfos T_1, T_2, es decir, $T_1 = \mathbb{C}/(\mathbb{Z}+\tau_1\mathbb{Z}) \cong T_2 = \mathbb{C}/(\mathbb{Z}+\tau_2\mathbb{Z})$. Como $T_1 \cong T_2$, entonces existe una transformación de Möbius $\dfrac{az+b}{cz+d}$ tal que $\tau_2 = \dfrac{a\tau_1 + b}{c\tau_1 + d}$. Por propiedades del $j - invariante$ tenemos que $j(\tau_2) = j(\dfrac{a\tau_1 + b}{c\tau_1 + d}) = j(\tau_1)$. Por lo tanto $j(E) = j(E')$.

Supongamos ahora que E y E' son dos curvas elípticas con el mismo $j - invariante$, $j(E) = j(E')$. Sin perdida de generalidad podemos escribir las ecuaciones de Weierstrass de E y E' de la siguiente manera:

$$E := y^2 = 4x^3 - g_2x - g_3$$

y

$$E' : y^2 = 4x^3 - g_2'x - g_3'.$$

Por hipótesis $j(E) = \dfrac{g_2^3}{\Delta} = \dfrac{g_2^3}{g_2^3 - 27g_3^2} = j(E') = \dfrac{{g_2'}^3}{\Delta'} = \dfrac{{g_2'}^3}{{g_2'}^3 - 27{g_3'}^2}$. Notemos que si $g_2 = 0$, entonces $g_2' = 0$ y $g_3' \neq 0 \neq g_3'$ ya que $\Delta \neq 0$. Esto nos hace ver que existe un número complejo u tal que $u^6 = \dfrac{g_3}{g_3'}$, entonces es fácil ver que $\phi : E \longrightarrow E'$ dada por $\phi(x, y) = (u^2x, u^3y)$ determina un isomorfismo entre E y E'.

Si $g_2 \neq 0 \neq g_3$, entonces $g_2' \neq 0 \neq g_3'$. Utilizando la igualdad de los $j - invariantes$ se tiene que $g_2^3{g_3'}^2 = {g_2'}^3g_3^2$, es decir, $(\dfrac{g_2}{g_2'})^3 = (\dfrac{g_3}{g_3'})^2$. Tomando $u \in \mathbb{C}$ tal que $u^4 = \frac{g_2}{g_2'}$ de manera que $u^{12} = (\dfrac{g_3}{g_3'})^2$ y $u^6 = \pm\dfrac{g_3}{g_3'}$. Si el signo es negativo multiplicamos a u por una raíz cuarta primitiva de la unidad y u^4 no cambia

pero u^6 cambia solo de signo, en otras palabras, tenemos que $u^4 = \frac{g_2}{g_2'}$ y $u^6 = \frac{g_3}{g_3'}$.

La aplicación $\phi : E \to E'$, $\phi(x, y) = (u^2x, u^3y)$ determina el isomorfismo entre E y E'. $\square$

Finalmente hemos logrado llegar al Teorema que revela que la Familia de Toros Complejos (módulo isomorfismo), que es el mismo que el de curvas elípticas no singulares, está parametrizado por el conjunto $\mathbb{C}$ de los números complejos. Esto gracias a la función $j - invariante$.

Teorema 13 *La función* $\bar{j} : \mathbb{H}/\Gamma \longrightarrow \mathbb{C}$ *es un isomorfismo entre superficies de Riemann.*

Capítulo 4

Resultados Clásicos en Teoría Geométrica de Invariantes.

En este capítulo se desarrollan los conceptos y resultados clásicos de la Teoría Geométrica de Invariantes, que nos permiten conseguir la compactificación del espacio moduli de curvas elípticas no singulares. Para esto comenzamos con algunas definiciones básicas.

Definición. Sea R un anillo. El anillo A es una *R-álgebra* si A es un *R-módulo* tal que $r(ab) = a(rb)$ para todo $r \in R$ y todo $a, b \in A$. Una *R-subálgebra* de A es un *R-submódulo* A_1 de A.

Definición. Sean A y B dos *K-álgebras*. Un *$homorfismo$* (*$isomorfismo$*) *de K-álgebras* es un homomorfismo (isomorfismo) de anillos

$$\phi : A \longrightarrow B$$

tal que $\phi(ra) = r\phi(a)$ para todo $r \in K$ y $a \in A$.

Definición. Una *K-álgebra* A es *$finitamente\ generada$* si existe un entero no negativo n y un ideal I en $K[x_1, ..., x_n]$ tal que $A = K[x_1, ..., x_n]/I$.

Por ejemplo si K es un campo y $R = K[x_1, ..., x_n]$ el anillo de polinomios en $n - variables$ con coeficientes en K, entonces R es obviamente una *K-álgebra* finitamente generada.

Denotamos por Σ_n el grupo de permutaciones en $\{1, 2, ..., n\}$. Consideramos la acción de Σ_n en $K[x_1, ..., x_n]$ de la forma

$$\Sigma_n \times K[x_1, ..., x_n] \longrightarrow K[x_1, ..., x_n]$$

$$(\sigma, f(x_1, ..., x_n)) \longrightarrow \sigma(f) = f(x_{\sigma(1)}, ..., x_{\sigma(n)})$$

El conjunto de invariantes

$$R^{\Sigma_n} := \{f \in K[x_1, ..., x_n] : \sigma(f) = f \forall \sigma \in \Sigma_n\}$$

es un subanillo de $K[x_1, ..., x_n]$ y es llamado *el anillo de funciones simétricas*. Este subanillo contiene a las funciones elementales:

$$f_1(x_1, ..., x_n) = x_1 + ... + x_n$$

$$f_2(x_1, ...x_n) = \sum_{1 \leq i < j \leq n} x_i x_j$$

$$\vdots$$

$$f_n(x_1, ..., x_n) = x_1 x_2 \cdots x_n.$$

Además se prueba que R^{Σ_n} está generado como *K-álgebra* por $f_1, f_2, ..., f_n$, es decir, cada elemento de R^{Σ_n} puede escribirse de manera única como un polinomio en los f_i. Por lo tanto R^{Σ_n} es isomorfo al anillo $K[f_1, ..., f_n]$ y así R^{Σ_n} es isomorfo a $K[x_1, ..., x_n]$ como *K-álgebra*.

4.1. La acción natural de $GL(n, K)$ en K^n.

Sea $M_n(K)$ el espacio vectorial de las matrices $n \times n$ con coeficientes en K y $GL(n, K)$ el grupo de matrices invertibles, con el producto de matrices como operación.

Una natural pero muy importante acción será la multiplicación. Sea $G \subset GL(n, K)$ un grupo de matrices. Consideramos la acción de G en el espacio afín K^n dada por la multiplicación usual

$$G \times K^n \longrightarrow K^n$$

$$(A, (x_1, ..., x_n)) \longmapsto A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

Para ésta acción, es natural preguntarse sí K^n/G es variedad afín sobre K y sí la aplicación proyección

$$\pi : K^n \longrightarrow K^n/G$$

$$x \longmapsto O(x)$$

es un morfismo de variedades. Más adelante trataremos este problema con bastante generalidad, aunque primero consideremos algunos casos más simples.

Si $G \subset GL(n,K)$ es un grupo. Un polinomio $f \in K[x_1,...,x_n]$ se dice *invariante bajo* G si $f(x) = f(Ax)$ para todo $A \in G$.

Si $G = GL(n,K)$, entonces $K^n/G = \{\{0\}, K^n - \{0\}\}$, donde $0 := (0,0,...,0) \in K^n$. Esto se debe a que si vemos a K^n como un $K-$*espacio vectorial* y tomamos v_1 y $w_1 \in K^n - \{0\}$ y consideramos dos bases en K^n: $U = \{v_1, v_2, ..., v_n\}$ y $W = \{w_1, w_2, .., w_n\}$, y $T : K^n \longrightarrow K^n$ es la transformación lineal determinada por la regla $T(v_i) = w_i$, $i = 1, 2, ..., n$, entonces T es un isomorfismo lineal y por tanto $[T]_{\mathcal{B}} = A$, donde $\mathcal{B}$ es la base canónica en K^n y $A \in GL(n,K)$ es tal que $A \cdot v_1 = w_1 \cdot A$.

Entonces podemos identificar a K^n/G con el conjunto $\{0,1\} \subseteq K$ que es afín mediante el polinomio $f(x) = x^2 - x \in K[x]$, y

$$\phi : K^n \longrightarrow \{0,1\}$$

dado por

$$(x_1, \ldots, x_n) \longmapsto \begin{cases} 0 & \text{si } x_i = 0 \forall i \\ 1 & \text{si } no \end{cases}$$

es un morfismo de variedades que corresponde a la proyección

$$\pi : K^n \longrightarrow K^n/G$$

$$x \longmapsto O(x).$$

4.2. Cocientes de variedades afines por grupos algebaicos.

En esta sección se generaliza lo que se observó anteriormente sobre condiciones para que K^n/G tenga estructura de variedad afín sobre K y la proyección sea un morfismo.

Aunque las siguientes definiciones son dadas sobre cualquier campo K algebraicamente cerrado, eventualmente trabajaremos de manera concreta con el campo $\mathbb{C}$ de los números complejos.

Definición. Un grupo G se dice *algebraico sobre un campo* K si es una variedad algebraica sobre K y las operaciones de multiplicación e inversos son

morfismos algebraicos. Un grupo algebraico que es isomorfo a un subgrupo cerrado de $GL(n,K)$ se llama *grupo algebraico lineal*.

Definición. Sean G_1 y G_2 grupos algebraicos, un *homomorfismo de grupos algebraicos* es un homomorfismo de grupos $\phi : G_1 \longrightarrow G_2$, que es morfismo de variedades algebraicas.

Ejemplo. Los grupos $GL(n,K)$, $SL(n,K)$ y $PGL(n,K)$ son grupos algebraicos lineales.

Proposición 11 *Un grupo algebraico lineal G sobre K posee un único subgrupo maximal, normal, soluble y conexo. Este grupo de llama el radical de G.*

Definición. Un grupo algebraico lineal G se dice *reductivo* si su radical es isomorfo a un producto directo de copias de K^*.

Ejemplo. Los grupos $GL(n,K)$, $SL(n,K)$ y $PGL(n,K)$ son grupos reductivos. Los subgrupos finitos de $GL(n,K)$ son reductivos.

Ejemplo. El subgrupo de $GL(4,\mathbb{C})$ definido por

$$G = \{ \begin{pmatrix} 1 & \beta & \gamma & \beta\gamma \\ 0 & 1 & 0 & \gamma \\ 0 & 0 & \alpha & \alpha\beta \\ 0 & 0 & 0 & \alpha \end{pmatrix} : \alpha \in \mathbb{C}^*, \beta, \gamma \in \mathbb{C} \}$$

no es reductivo.

Definición. Una *acción de un grupo algebraico* G en una variedad X es un morfismo entre variedades

$$\sigma : G \times X \longrightarrow X$$

$$(g,x) \longmapsto g \cdot x$$

tal que, para todo $g_1, g_2 \in G$, $x \in X$,

$$g_1(g_2 x) = (g_1 g_2)x$$

y

$$e \cdot x = x,$$

donde e es el neutro de G.

Si $W \subset X$ es un subconjunto, decimos que W es $G-$*invariante* si $g \cdot w \in W$ $\forall g \in G$.

Supóngase que G es un grupo algrebaico lineal y actúa en una variedad X (afín

en K^{n+1} o proyectiva en KP^n), entonces decimos que G *actúa linealmente en* X si existe un homomorfismo de grupos algebraicos

$$\rho : G \longrightarrow GL(n+1, K)$$

tal que la acción de G en X es la inducida por la acción

$$G \times K^{n+1} \longrightarrow K^{n+1}$$

$$(g, (x_0, x_1, ..., x_n)) \longmapsto \rho(g)(x_0, ..., x_n)$$

Un homomorfismo de grupos algebraicos

$$\rho : G \longrightarrow GL(n+1, K)$$

es llamada una representación racional de G sobre K.

Si G actúa linealmente en X, también decimos que esta acción de G es lineal en X.

Definición. Un grupo algebraico lineal G se dice *geometricamente reductivo* (*linealmente reductivo*) si, para acción lineal de G en K^n, y cada punto $v \in K^n$, $v \neq 0$, invariante por la acción de G i.e, $g \cdot v = v \; \forall g \in G$, existe $f \in K[x_1, ..., x_n]$, homogeneo, invariante bajo G, de grado mayor o igual a uno (igual a uno) tal que $f(v) \neq 0$.

Teorema 14 *Si K es un campo algebraicamente cerrado y de característica igual a cero, entonces es equivalente que:*

1.- G es reductivo.

2.- G es geometricamente reductivo.

3.- G es linealmente reductivo.

Nagata y Miyata probaron en 1963 que en general se vale que si G es geometricamente reductivo, entonces G es reductivo; para característica cero, Weil probó que si G es reductivo, entonces G es linealmente reductivo; y es obvio que si G es linealmente reductivo, entonces G es geometricamente reductivo. Así se consigue la equivalencia.

También, en 1974 se probó por Haboush que en campos de característica arbitraria, se cumple que si G es reductivo,entonces G es geométricamente reductivo. Estas equivalencias serán fundamentalmente útiles en el caso de trabajar con $\mathbb{C}$.

Definición. Sea G un grupo algebraico y R una K-*álgebra. Una acción racional de* G *en* R es una aplicación

$$G \times R \longrightarrow R$$

$$(g, f) \longmapsto fg$$

que satisface las siguientes propiedades:

1) $\forall f \in R$ y $g_1, g_2 \in G$, se cumple que $f^{g_1 g_2} = (f^{g_1})^{g_2}$ y $f^e = f$ (i.e,$(f, g) \longrightarrow fg$ es una acción).

2) Dado $g \in G$, la aplicación $f \longrightarrow f^g$ es un automorfismo de $K-algebras$ de R.

3) Para cada elemento $r \in R$ existe un $K - subespacio\ vectorial$ W de R de dimensión finita n ($W \cong K^n$), el cual contiene a r, es invariante bajo G y sobre el cual G actúa linealmente (i.e, mediante un morfismo de grupos algebraicos $\rho : G \longrightarrow GL(n)$).

Un resultado fundamental para el caso de acciones en variedades afines es:

Teorema 15 *(Nagata). Sea* G *un grupo reductivo actuando racionalmente en una* K-álgebra *finitamente generada* A*. Entonces* $A^G = \{f \in A : f^g = f\ \forall g \in G\}$ *es una* K-álgebra *finitamente generada.*

La traducción del teorema de Nagata a la Geometría Algebraica, nos da el teorema central de acciones de grupos en variedades afines, que es:

Teorema 16 *Sea* G *un grupo reductivo actuando en una variedad afín* X*. Entonces existe una variedad afín* Y *y un morfismo* $\phi : X \longrightarrow Y$ *tal que*

1. ϕ *es* $G - invariante$*, es decir,*

$$\phi(gx) = x$$

$\forall g \in G$.

2. ϕ *es sobre.*

3. Si $U \subset Y$ *es abierto, entonces*

$$\phi^x : A(U) \longrightarrow A(\phi^{-1}(U))$$

$$f \longmapsto f \circ \phi$$

es un isomorfismo sobre $A(\phi^{-1}(U))$.

4. Si W_1 *y* W_2 *son subconjuntos* $G - invariantes$*, cerrados, disjuntos, entonces*

$$\phi(W_1) \cap \phi(W_2) = \varnothing$$

5. Si W es un subconjunto $G-$ invariante cerrado de X, entonces $\phi(W)$ es cerrado en Y.

Notar que en la hipótesis de el teorema no se pide que G actúe linealmente en X; y la variedad Y es una variedad afín.

4.3. Cocientes de Variedades Proyectivas por Grupos Algebraicos.

En esta sección se enuncia el principal Teorema de la Teoría Geométrica de Invariantes en el contexto de variedades proyectivas.

Para empezar daremos las siguientes definiciones que aplican en variedades afines o proyectivas.

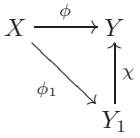
Trabajaremos suponiendo que G es un grupo algebraico actuando en X.

Definición. *Un buen cociente de X por G* es una pareja (Y, ϕ) donde Y es una variedad y $\phi : X \longrightarrow Y$ es un morfismo afín que satisface las condiciones 1-5 del Teorema 10.

Definición. *Un cociente categórico de X por G* es un par (ϕ, Y), donde Y es una variedad y ϕ es un morfismo tal que:

1. ϕ es constante en las órbitas de la acción.

2. Para cada variedad Y_1 y morfismo $\phi_1 : X \longrightarrow Y_1$ constante en órbitas, existe un único morfismo $\chi : Y \longrightarrow Y_1$ tal que $\chi \circ \phi = \phi_1$. Es decir, el siguiente diagrama conmuta:



Si (ϕ, Y) es un cociente categórico de X por G, y además para todo $y \in Y$, $\phi^{-1}(y)$ consiste de sólo una órbita, entonces (ϕ, Y) es llamado *espacio de órbitas.*

Proposición 12 *Si (Y, ϕ) es un buen cociente de X por G, entonces (Y, ϕ) es un cociente categórico.*

Definición. Un *cociente geométrico* es un buen cociente que además es un espacio de órbitas.

Proposición 13 *Sea (Y, ϕ) un buen cociente de X por G. Entonces se cumplen las siguientes afirmaciones:*

1. $\phi(x_1) = \phi(x_2)$ si y sólo si $\overline{O(x_1)} \cap \overline{O(x_2)} \neq \varnothing$.

2. Si la acción de G en X es cerrado, entonces (Y, ϕ) es un cociente geométrico.

Una acción lineal de G sobre X define una acción de G sobre el anillo de polinomios en $n+1$ variables con coeficientes en el campo:

$$G \times K[x_0, x_1, ..., x_n] \longrightarrow K[x_0, x_1, ..., x_n]$$

$$(g, f) \longmapsto fg$$

donde $fg(x_0, x_1, ..., x_n) = f(g(x_0, x_1, ..., x_n))$. Recordemos que el polinomio f se dice invariante por la acción si $f = f^g \ \forall g \in G$.

Definición. Decimos que $x \in \divideontimes$ es:

1. $Semi - estable$ si existe f, polinomio invariante, homogeneo, de grado mayor o igual que uno tal que $f(x) \neq 0$. Denotaremos el conjunto de puntos semi-estables de X por X^{ss}.

2. *Estable* si es semi-estable,

$$dim O(x) = dim G,$$

y $O(x)$ es cerrada en X^{ss}. El conjunto de puntos estables de X lo denotaremos por X^s.

3. Los puntos que no son semi-estables se denominan *inestables*. Este conjunto se llama el *cono nulo*, y se denota por CN.

Teorema Fundamental de Teoría Geométrica de Invariantes en Variedades Proyectivas:

Teorema 17 *Sea G un grupo reductivo actuando linealmente sobre una variedad proyectiva X, entonces*

1. Existe un buen cociente (Y, ϕ) de X^{ss} por G donde Y es proyectivo.

2. Existe $Y^s \subset Y$ abierto tal que $\phi^{-1}(Y^s) = X^s$ y (Y^s, ϕ) es un cociente geométrico de X^s por G.

3. Si $x_1, x_2 \in X^{ss}$, entonces

$$\phi(x_1) = \phi(x_2) \text{ si y sólo si } \overline{O(x_1)} \cap \overline{O(x_2)} \cap X^{ss} \neq \varnothing$$

La parte más importante del Teorema es el hecho de que Y es una variedad proyectiva. Esto nos permite pensar a Y como una compactificación natural del cociente X^s/G.

4.4. Subgrupos a un parámetro.

El objetivo de esta sección es enunciar un criterio que caracterice cuando un punto es estable o semiestable, evitando los cálculos que se desprenden de aplicar directamente la definición, pues este es por lo general muy difícil.

Supondremos que G es un grupo reductivo que está actuando en una variedad X en $\mathbb{C}P^n$, y que tal acción se extiende a una acción de G en $\mathbb{C}^{n+1}$ que deja invariante al cono sobre X.

Teorema 18 *Sean $x \in X$ y $\bar{x} \in \mathbb{C}^{n+1}$ un punto sobre x. Entonces:*

1) x es semi-estable si y sólo si $0 \notin \overline{O(\tilde{x})}$;

2) x es estable si y sólo si el morfismo

$$\sigma_{\tilde{x}} : G \longrightarrow \mathbb{C}^{n+1},$$

$$\sigma_{\tilde{x}}(g) = g\tilde{x}$$

es propio.

Definición. Un *subgrupo a un parámetro de G* es un homomorfismo de grupos algebraicos

$$\lambda : \mathbb{C}^* \longrightarrow G.$$

Sea λ un subgrupo a un parámetro de G. Entonces dado $t \in \mathbb{C}^*$, la aplicación

$$\lambda(t) : \mathbb{C}^{n+1} \longrightarrow \mathbb{C}^{n+1}$$

$$\tilde{x} \longmapsto \lambda(t)\tilde{x}$$

es lineal, la cual podemos diagonalizar sobre $\mathbb{C}$: Es decir, existe una base $e_0, ..., e_n$ en $\mathbb{C}^{n+1}$ tal que

$$\lambda(t)e_i = \alpha_i(t)e_i$$

con $\alpha_i(t) \in \mathbb{C}^*$. Además para cada $i \in [0, n]$, la aplicación

$$\alpha_i : \mathbb{C}^* \longrightarrow \mathbb{C}^*$$

$$t \longmapsto \alpha_i(t)$$

es morfismo de grupos. Por lo tanto $\alpha_i(t) = t^{r_i}$ con algún $r_i \in \mathbb{Z}$. Hemos visto entonces que dado t

$$\lambda(t)e_i = t^{r_i}e_i$$

para algunos $r_i \in \mathbb{Z}$.

Identifiquemos a $\mathbb{C}^*$ como un abierto en la línea proyectiva $\mathbb{C}P^1 = \mathbb{C}^* \cup \{0, \infty\}$. Si $X \subset \mathbb{C}P^n$ es una variedad proyectiva y $\psi : \mathbb{C}^* \longrightarrow X$ es un morfismo, entonces existe una única extensión

$$\bar{\psi} : \mathbb{C}P^1 \longrightarrow X \subset \mathbb{C}P^n,$$

donde $\bar{X}$ denota la cerradura (Zariski) en $\mathbb{C}P^n$. Así podemos entonces definir las expresiones

$$\lim_{t\to 0} \psi(t)$$

y

$$\lim_{t\to \infty} \psi(t).$$

Entonces se deduce que ψ es propio si y sólo si $\lim_{t\to\infty} \psi(t)$ y $\lim_{t\to 0} \psi(t)$ no existen en X.

Ahora escribimos $\tilde{x} = \sum \tilde{x_i}e_i$ en esta base, de tal forma que

$$\lambda(t)\tilde{x_i} = \sum t^{r_i}\tilde{x_i}e_i,$$

y definimos

$$\mu(x, \lambda) = max\{-r_i : \tilde{x_i} \neq 0\}$$

= único entero μ tal que $\lim_{t\to 0} t^{\mu}\lambda(t)\tilde{x}$ existe y es distinto de 0.

Note que

$$\mu(x, \lambda) > 0 \Longleftrightarrow \lim_{t\to 0} \lambda(t)\tilde{x} \text{no existe},$$

$$\mu(x, \lambda) = 0 \Longleftrightarrow \exists \lim_{t\to 0} \lambda(t)\tilde{x} \neq 0.$$

Con las anteriores observaciones y usando el teorema 12 obtenemos el siguiente resultado:

Teorema 19 *Sea G un grupo reductivo actuando linealmente en una variedad proyectiva X en $\mathbb{C}P^n$, entonces*

x es semi-estable $\Longleftrightarrow$ $\mu(x, \lambda) \geq 0$ para todo subgrupo a un parámetro λ de G,

x es estable $\Longleftrightarrow$ $\mu(x, \lambda) > 0$ para todo subgrupo a un parámetro λ de G.

Teorema 20 *Supóngase que $SL(\mathbb{C}, n)$ actúa linealmente sobre una variedad proyectiva X. Un punto $x \in X$ es estable (semi-estable) para esta acción si y sólo si $\mu(gx, \lambda) > 0$ (≥ 0) para todo $g \in SL(\mathbb{C}, n)$ y todo subgrupo a un parámetro λ de $SL(\mathbb{C}, n)$ de la forma $\lambda(t) = diag(t^{r_1}, ..., t^{r_n})$ con $\sum r_i = 0$, $r_1 \geq r_2 \geq ... \geq r_n$, no todos los r_i iguales a cero.* $(*)_n$

4.5. Compactificación de las cúbicas planas.

En esta sección consideramos el caso en donde $G = SL(\mathbb{C}, 3)$ y X es la familia de las curvas cúbicas planas.

Cualquier curva de estas esta determinada por uno y sólo un polinomio $f(x) \in \mathbb{C}[x_0, x_1, x_2]$, donde $f(x)$ es homogéneo de grado 3.

Entonces si escribimos

$$\begin{gathered} f = a_{30}x_1^3 + a_{21}x_1^2x_2 + a_{12}x_1x_2^2 + a_{03}x_2^3 + \\ a_{20}x_0x_1^2 + a_{11}x_0x_1x_2 + a_{02}x_0x_2^2 \\ + a_{10}x_0^2x_1 + a_{01}x_0^2x_2 \\ + a_{00}x_0^3, \end{gathered}$$

notamos que f esta univocamente determinado por sus coeficientes hasta multiplo escalar. Es decir, X está en corresondencia con $\mathbb{C}P^9$. Así vemos de manera natural la estructura de variedad proyectiva de X.

Recordemos que un punto $x \in \mathbb{C}P^2$ es un punto singular de la curva definida por f y todas sus derivadas parciales se anulan en x.

Nosotros queremos distinguir entre *puntos dobles y puntos triples* y referirnos a *tangentes* a la curva en punto doble.

Definición:

1) $(1, 0, 0)$ es un punto triple $\iff a_{00} = a_{10} = a_{01} = a_{20} = a_{11} = a_{02} = 0$.

2) $(1, 0, 0)$ es un punto doble $\iff$ la tangente a $(1, 0, 0)$ son las lineas definidas por la ecuación

$$a_{20}x_1^2 + a_{11}x_1x_2 + a_{02}x_2^2.$$

Se puede notar que

1) $(1, 0, 0)$ es *singular* $\iff a_{00} = a_{10} = a_{01} = 0$.

2) Para cualquier $g \in SL(\mathbb{C}, 3)$, x es un punto singular (doble o triple) de f si y sólo si gx es un punto singular (doble o triple) de $g \cdot x$; además g preserva tangentes.

Teorema 21 *(Criterio de estabilidad y semi-estabilidad.) Una curva cúbica plana es estable si y sólo si, esta es no singular; y es semi-estable si y sólo si esta no tiene puntos triples ni puntos dobles con una única tangente.*

Demostración: Sabemos por el teorema 20 que una curva cúbica es no estable (no semi-estable) si y sólo si esta es equivalente bajo la acción de $SL(\mathbb{C},3)$ a una para la cual $\mu(f,\lambda) \leq 0$ (< 0) para todo $\lambda : \mathbb{C}^* \longrightarrow SL(\mathbb{C},3)$ subgrupo a un parámetro de la forma $(*)_3$.

También tenemos que

$$\mu(f,\lambda) = max\{(3-i-j)r_0 + ir_1 + jr_2 : a_{ij} \neq 0\}$$

Consideremos primero la condición para semi-estabilidad. Notemos que si $\mu(f,\lambda) < 0$ entonces $a_{00} = a_{10} = a_{01} = a_{20} = a_{11} = 0$. Entonces si $a_{02} = 0$, $(1,0,0)$ es punto singular de f, y si $a_{02} \neq 0$, entonces $(1,0,0)$ es un punto doble con una única tangente dada por $a_{02}x_2^2$. Por lo tanto si f no tiene puntos triples ni dobles con una única tangante, entonces f es semi-estable.

Inversamente, si $a_{00} = a_{10} = a_{01} = a_{20} = a_{11} = 0$, entonces tomamos $r_0 = 3$, $r_1 = -1$, $r_2 = -2$, y así $\mu(f,\lambda) < 0$. Esto prueba la segunda parte del teorema.

Ahora consideramos la condición para estabilidad. Supóngase que f tiene un punto singular x. Podemos además suponer que $x = (1,0,0)$, entonces $a_{00} = a_{10} = a_{01} = 0$. Tomemos $r_0 = 2$, $r_1 = r_2 = -1$, y así obtenemos que $\mu(f,\lambda) \leq 0$, por tanto f es no estable.

Sólo falta ahora ver que si $\mu(f,\lambda) \leq 0$ para algún λ de la forma $(*)_3$, entonces f tiene un punto singular. Supóngase que $\mu(f,\lambda) \leq 0$, entonces $a_{00} = a_{10} = 0$. Si $a_{01} = 0$ hemos terminado pues entonces $(1,0,0)$ es un punto singular de f. Si $a_{01} \neq 0$, entonces como $\mu(f,\lambda) \leq 0$, obtenemos que $2r_0 + r_2 \leq 0$, entonces $r_1 = r_0$ y $r_2 = -2r_0$. Para estos valores r_i, se tiene que

$$\mu(f,\lambda) = max\{(3-3j) : a_{ij} \neq 0\},$$

entonces $\mu(f,\lambda) \leq 0$ si y sólo si $a_{i0} = 0$ $\forall i$. Entonces podemos escribir que $f = x_2 f'$ para algún polinomio f' de grado 2. Por lo tanto f es singular en todo punto tal que $x_2 = f' = 0$. $\square$

Conclusión:

Usando el Teorema principal de GIT, sabemos que la compactificación de X^s (el conjunto de puntos estables) se logra agregando a este los puntos de X^{ss}/X^s, i,e. los que sean semiestables pero no estables, y gracias al Teorema de clasificación de estabilidad y semi-estabilidad, concluimos que la compactificación del conjunto de curvas elípticas no singulares X^s se obtiene agregando a este las curvas que sean singulares y cuya singularidad satisfaga la condición para semi-estabilidad. Además nos interesamos sólo en tales de estas curvas que también sean irreducibles.

Como vimos en la sección de curvas singulares, una curva E dada por la ecuación $y^2 = x^3 + ax + b$ es singular si y sólo si el discriminante $\Delta_E = 4a^3 + 27b^2 = 0$ ó equivalentemente el polinomio $f(x) = x^3 + ax + b$ tiene alguna raíz con multiplicidad ≥ 2. Entonces las curvas dadas por $E_1 : y^2 = x^3$ y $E_2 : y^2 = x^2(x+1)$ representan (hasta equivalencia) las clases de curvas singulares. La primera representa el caso típico de una curva dada por un polinomio con una única raíz, esta es llamada curva *nodal*. La segunda representa el caso típico dado por un polinomio con dos raíces. Sin embargo la curva asociada a la ecuación $y^2 = x^3$, llamada curva *cuspidal*, no cumple la condición de semi-estabilidad, pues el punto $(0, 0)$ es una singularidad de E_1 con una tangente doble, a saber la recta $y = 0$.

Finalmente, consideremos la curva dada por $y^2 = x^2(x + 1)$. Esta curva es singular unicamente en el punto $(0, 0)$, y por el ya vimos que pasaban dos rectas tangentes, una dada por la dirección del vector $(2, 3)$ y otra por el vector $(-2, 3)$. Esto prueba que esta curva es un punto semi-estable y el único hasta equivalencia. Por lo tanto la curva dada por la ecuación $y^2 = x^2(x + 1)$ logra la compactificación de la Familia de Curvas Elípticas no singulares (Ver Figura 4.1).

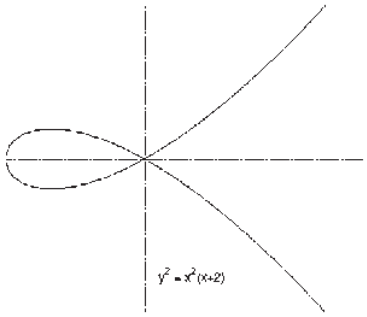


Figura 4.1: La curva nodal de de la ecuación $y^2 = x^2(x + 1)$.

Bibliografía

[1] Joseph H. Silverman Jonh Tate. *Rational Points on Elliptic Curves.* Springer, 2000.

[2] Rick Miranda. *Algebraic Curves and Riemann Surfaces.* Graduate Studies in Mathematics. Board, 1991.