UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

LAS CONJETURAS DE WEIL PARA CURVAS ELÍPTICAS

T E S I S

QUE PARA OBTENER EL TITULO DE:

M A T E M A T I C O

P R E S E N T A :

FRANCISCO XAVIER PORTILLO BOBADILLA

DIRECTOR DE TESIS: DR. JAVIER ELIZONDO HUERTA

1996

VNIVERSIDAD NACIONAL
AVPNOMA DE
MEXICO

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

Comunicamos a usted que hemos revisado el trabajo de Tesis:

Las conjeturas de Weil para curvas elípticas

realizado por FRANCISCO XAVIER FORTILLO BOBADILLA

con número de cuenta 9034202-4 , pasante de la carrera de Matemáticas.

Dicho trabajo cuenta con nuestro voto aprobatorio.

Atentamente

Director de Tesis Propietario	Dr. E. Javier Elizondo Huerta
Propietario	Dr. Sevin Recillas Pishmish
Propietario	Dra. Laura Hidalgo Solís
Suplente	Dr. Emilio Lluis Riera
Suplente	Dr. Marcelo Alberto Aguilar González

Consejo Departamental de Matemáticas

M. en C. Alejandro Bravo Mojica

Las Conjeturas de Weil para Curvas Elípticas

Francisco Xavier Portillo Bobadilla

Indice

1 Introducción: Breve Historia de las Conjeturas de Weil

La historia de las conjeturas de Weil es un ejemplo maravilloso de la imaginación y el desarrollo matemático, en ella se conjugan y unifican varias áreas de la matemática antigua y moderna. Y aunque la esencia de las ideas que culminaron con su demostración se debe principalmente a seis gigantes de la matemática: E.Artin, F.K.Schimidt, H.Hase, A.Weil, A.Grothendiek y P.Deligne. El embrión que produciría estas ideas se remonta a más de dos siglos antes de la culminación de ésta. Y atañe desde luego a los geniales matemáticos de esa época, principalmente Euler, Gauss, Einseisten y Jacobi.

1.1 Congruencias y su número de soluciones

El problema nació al cuestionarse acerca del número de soluciones que tendría una congruencia como por ejemplo $f(x) \equiv 0 \ mod(p)$, donde x se mueve sobre los números $\{1, 2, \ldots, p-1\}$ y f es un polinomio.

Esta pregunta es muy natural que uno puede formularla con cierto razgo de ingenuidad en un primer curso de Teoría de Números, cuando es introducido a las congruencias y sus propiedades. Sin embargo, dar una respuesta aceptable no es nada trivial, y en su búsqueda, los matemáticos han desarrollado una maquinaria sumamente compleja, con la esperanza de acercarse a una solución. Como es de esperarse, en esta búsqueda también, muchas preguntas se fueron abriendo, y algunas conjeturas se formularon.

El primer caso notable que se planteo fue el de buscar las soluciones a la congruencia $x^2 \equiv a \ mod(p)$.

Para p fija su solución es relativamente sencilla. Y ésta se da si y solamente si $a^{(p-1)/2} \equiv 1 \ mod(p)$.

Generalizando un poco más la pregunta el siguiente teorema nos responde cuando existe una solución a la congruencia $x^n \equiv a \ mod(p)$ con p fija, y además nos especifica el número de soluciones.

Teorema 1.1. Sea p un número primo, y $d = (n, p-1)$ entonces $x^n \equiv a \ mod(p)$ tiene d soluciones si y unicamente si $a^{(p-1)/d} \equiv 1 \ mod(p)$

Si ahora movemos el primo p a lo largo de todos los primos y fijamos a, la pregunta se torna más difícil. Es decir, si nos dan un sólo primo p, gracias al teorema anterior podemos verificar facilmente si a es residuo cuadrático, pero el teorema no nos sirve de nada para decir cuales son esos primos. (!!)

Es aquí realmente cuando empiezan los dolores de cabeza, que si no fuera gracias a la aparición de Euler y Gauss que formulan y prueban lo que hoy en día son conocidas como las leyes de la reciprocidad cuadrática, el problema todavía probablemente nos atormentería.

Definición 1.2. El símbolo (a/p) es igual a 1, si a es residuo cuadrático de p, igual a -1, si no es residuo cuadrático, y si $p|a$ entonces igual a 0.

Una de las propiedades importante de (a/p) es que es un caracter multiplicativo del campo $\mathbb{F}_p$. Es decir, un homomorfismo del grupo multiplicativo de $\mathbb{F}_p$ en el grupo multiplicativo de $\mathbb{C}$. De la definición y del teorema anteriores se ve claramente que el símbolo (a/b) cumple:

Proposición 1.3. *a)* $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ mod(p)$

b) Si $a \equiv b \ mod(p)$ *entonces* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Hasta aquí puede no quedar muy clara la utilidad del símbolo $\left(\frac{a}{p}\right)$, sin embargo, la siguientes propiedades conocidas como las leyes de la reciprocida cuadrática, formuladas por Euler en su artículo *Observationes circa divisionem quadratorum per numeros primos* que según el libro de Ireland y Rosen [KM90] fueron formuladas en algún año posterior a 1746 y demostradas por primera vez por Gauss el 8 de Abril de 1796 darían la respuesta satisfactoria a la pregunta para qué primos la ecuación $x^2 \equiv a \ mod(p)$ tiene solución.

Es interesante saber que hasta el propio Gauss se congratuló de este resultado, estando sumamente orgulloso que lo llamó el *Theorema Aureum*, y además se preocupo en dar 6 pruebas diferentes de él.

Proposición 1.4. *Leyes de la Reciprocidad Cuadrática.*

Sean p y q números primos impares. Entonces:

a) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$

b) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$

c) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$

Nota 1.5. Podemos apreciar que el inciso c) es la herramienta suficientemente general que nos ayuda a resolver $x^2 \equiv a \ mod(p)$ para p variable.

Sin perdida de generalidad, sea $a = q$ un primo. Estamos interesados en evaluar $\left(\frac{q}{p}\right)$ para toda $p \neq q$. Pero esto, es equivalente a evaluar

$$\left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Haciéndolo por casos vemos que si p es de la forma $4k+1$ entonces $(q/p) = (p/q)$. Es decir, basta encontrar todos los $(q-1)/2$ residuos cuadráticos, que podemos denotar $\{\eta_1, \dots, \eta_{\frac{q-1}{2}}\}$ del primo fijo q y verificar por la proposición 1.4 que p se encuentre, en alguna de las series $\{\eta_i + mq : m \in \mathbb{Z}\}$.

Trabajando de una manera similar, si p es de la forma $4k+3$, se llega al resultado de que si q es residuo cuadrático módulo p si y sólo si $p \equiv \pm b^2$, donde b es primo.

La siguiente proposición nos termina de justificar la afirmación inicial de la nota anterior:

Proposición 1.6. *Sea $m = 2^e p_1^{e_1} \cdots p_n^{e_n}$ la descomposición primaria de m, y supongamos $(a, m) = 1$. Entonces $X^2 \equiv a \ mod(m)$ es soluble si y sólo si lo siguiente se satisface:*

a) Si $e = 2$, entonces $a \equiv 1 \ mod(4)$.

Si $e \geq 3$, entonces $a \equiv 1 \ mod(8)$

b) Si para toda i tenemos que $a^{\frac{p_i-1}{2}} \equiv 1 \ mod(p_i)$.

Una prueba se puede ver en [KM90, pag 50].

Siguiendo el exitoso ejemplo de las leyes de la reciprociadad cuadrática, los matemáticos fueron en busca de leyes equivalentes para resolver en general la congruencia $X^n \equiv a \ mod(p)$ para el caso con p variable.

En el caso $n = 3$ y $n = 4$, esta investigación dio lugar a las leyes de la reciprocidad cúbica y bicuadrática que fueron formuladas y planteadas por Gauss, pero que sus demostraciones se debieron primeramente al joven Einseistein. Es importante destacar que Gauss nunca completó la prueba de la reciprocidad bicuadrática, él mismo Gauss le escribió a Humboldt en 1846 que el talento matemático de Einseistein era de una naturaleza que sólo unos pocos poseían en una centuria. Desgraciadamente, su muerte a los 29 años interrumpió su brillante carrera.

1.2 Sumas de Gauss y Caracteres

En su afán por calcular las leyes de la reciprocidad, Gauss introdujo lo que ahora son conocidas como las sumas de Gauss, que generalizadas a cualquier caracter χ se escriben:

$$g_a(\chi) = \sum_t \chi(t)\zeta^{at}$$

donde la suma es sobre todas las $t \in \mathbb{F}_p$ y $\zeta = e^{\frac{2\pi i}{p}}$ con $a \in \mathbb{F}_p$.

En su sexta prueba de la reciprocidad cuadrática, Gauss hizo uso de la serie $g_a(\chi)$ donde $\chi(t) = \left(\frac{t}{p}\right)$. Las siguientes proposiciones nos exponen las principales propiedades de las sumas de Gauss.

Proposición 1.7. *Si $a \neq 0$ y $\chi \neq \varepsilon$ donde varepsilon es el caracter trivial (todo lo manda a la unidad), entonces tenemos que*

$$g_a(\chi) = \chi(a^{-1})g_1(\chi)$$

Además $g_a(\varepsilon) = 0$ si $a \neq 0$ y $g_0(\varepsilon) = p$.

Proposición 1.8. *Sea $g(\chi) = g_1(\chi)$. Si $\chi \neq \varepsilon$ entonces $|g(\chi)| = \sqrt{p}$.*

Ejemplo 1.9. Si $\chi(t) = \left(\frac{t}{p}\right)$ entonces las 2 proposiciones anteriores se resumen en las siguientes afirmaciones:

a) $g_a = (a/b)g_1$

b) $g_1^2 = (-1)^{(p-1)/2}p$

El inciso a) es inmediato de la primera proposición de las últimas 2. El inciso b) surge observando que

$$\overline{\left(\frac{t}{p}\right)} = \left(\frac{t}{p}\right)$$

donde la barra indica el conjugado complejo, así se tiene que

$$g\left(\overline{\left(\frac{t}{p}\right)}\right) = g\left(\left(\frac{t}{p}\right)\right)$$

Comparando $\overline{g(\chi)}$ con $g(\overline{\chi})$ ($\overline{\chi}$ el caracter que manda a a hacia $\overline{\chi(a)}$), llegamos a la igualdad

$$\overline{g(\chi)} = \chi(-1)g(\overline{\chi})$$

y por tanto:

$$g_1^2 = g_1\left(\left(\frac{p}{t}\right)\right) g_1\left(\left(\frac{\overline{p}}{t}\right)\right) = g_1\left(\overline{\left(\frac{t}{p}\right)}\right) g_1\left(\left(\frac{\overline{t}}{p}\right)\right) = g_1\left(\left(\frac{t}{p}\right)\right)\overline{g_1\left(\left(\frac{t}{p}\right)\right)}\left(\frac{-1}{p}\right)$$
$$= \left(\frac{-1}{p}\right) p = (-1)^{\frac{p-1}{2}} p$$

El siguiente ejemplo evidencia la tremenda utilidad de las sumas de Gauss, para computar las leyes de reciprocidad.

Ejemplo 1.10. Sea $p^* = (-1)^{\frac{p-1}{2}} p$,donde $g = \sum_{t\in\mathbb{F}_p}\left(\frac{t}{q}\right)\zeta^t$, $\zeta = e^{\frac{2\pi i}{p}}$. Entonces

$$g^{q-1} = (g^2)^{\frac{q-1}{2}} = (p^*)^{\frac{q-1}{2}} \equiv \left(\frac{p^*}{q}\right) \ (mod\ q)$$

$$\Rightarrow g^q \equiv \left(\frac{p^*}{q}\right) g$$

Pero además

$$\left(\sum_{t\in\mathbb{F}_q}\left(\frac{t}{q}\right)\zeta^t\right)^q = \sum_{t\in\mathbb{F}_q}\left(\frac{t}{q}\right)^q \zeta^{qt} = \sum_{t\in\mathbb{F}_q}\left(\frac{t}{q}\right)\zeta^{qt}$$

y por lo tanto, $g^q = g_q$. De donde,

$$g_q = \left(\frac{p^*}{q}\right) g$$

y observando que $\left(\frac{q}{p}\right) g = g_q$, y además

$$\left(\frac{p^*}{q}\right) = \left(\frac{-1}{q}\right)^{\frac{p-1}{2}}\left(\frac{p}{q}\right) = (-1)^{\frac{q-1}{2}\frac{p-1}{2}}\left(\frac{p}{q}\right)$$

se sigue la ley de la reciprocidad en 1.4 c).

Exitosamente Gauss y Einseinstein aplicaron las sumas de Gauss para obtener y demostrar las leyes de las reciprocidades cúbica y bicuadrática. Un poco después, Jacobi observo que usando las propiedades básicas de las sumas de Gauss, se podía estimar correctamente el número de soluciones en casos más generales. Pensemos en la ecuación $x^2 + y^2 = 1$ sobre el campo $\mathbb{F}_q$, el círculo unitario alrededor del origen en $\mathbb{A}^2_{\mathbb{F}_q}$. Denotemos el número de soluciones de dicha ecuación a ese número como $N(x^2 + y^2 = 1)$. Entonces

$$N(x^2 + y^2 = 1) = \sum_{a+b=1} N(x^2 = a)N(y^2 = b)$$

donde $N(y^2 = b)$ y $N(x^2 = a)$ son los número de soluciones a las ecuaciones que contienen dentro del paréntesis, con a y b en $\mathbb{F}_q$. Por otro lado tenemos que

$$N(x^2 = a) = 1 + \left(\frac{a}{b}\right)$$

y sustituyendo obtenemos

$$N(x^2 + y^2 = 1) = p + \sum_a \left(\frac{a}{p}\right) + \sum_b \left(\frac{b}{p}\right) + \sum_{a+b=1} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

$$p + \sum_{a+b=1} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Es decir, el problema se ha reducido a calcular la suma $\sum_{a+b=1} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

De manera análoga, al tratar de calcular el número $N(x^3+y^3 = 1)$ Jacobi encontró que era necesario evaluar suma:

$$\sum_i \sum_j \sum_{a+b=1} \chi^i(a)\chi^j(b)$$

Sin duda, fueron estos casos particulares los que lo llevaron a definir las ahora llamadas sumas de Jacobi:

Definición 1.11. Sean χ y λ caracteres en $\mathbb{F}_p$, la suma de Jacobi se define como

$$J(\chi, \lambda) = \sum_{a+b=1} \chi(a)\lambda(b).$$

El siguiente teorema, que Einseinstein demostró en su artículo *Beiträge sur Kreistheilung* en 1844, no sólo resuelve el problema de calcular el valor de las sumas $J(\chi, \lambda)$, y por tanto de conocer $N(x^2+y^2=1)$ y $N(x^3+y^3=1)$, si no también nos muestra una sorprendente relación entre las sumas de Jacobi y las de Gauss, que se puede resumir en el siguiente teorema.

Teorema 1.12. a) $J(\varepsilon, \varepsilon) = p$
b) $J(\varepsilon, \chi) = 0$ con $\varepsilon \neq \chi$
c) $J(\chi, \chi^{-1}) = -\chi(-1)$ con $\varepsilon \neq \chi$
d) Si $\chi\lambda \neq \varepsilon$ entonces

$$J(\chi, \lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\lambda)}$$

Es decir, Jacobi no sólo construye la herramienta necesaria (y suficiente) para resolver las congruencias

$$x^2 + y^2 = 1 \ , \ x^3 + y^3 = 1$$

sino que además empuja al planteamiento de encontrar la solución de la ecuación $x^n+y^n = 1$ con $n \in \mathbb{Z}$, Y en consecuencia a resolver las congruencias

$$x_1^k + \cdots + x_r^k \equiv 0$$

Einseistein, generalizó las sumas de Jacobi y dió una versión más general del teorema. Se recomienda al lector interesado consultar el libro de Ireland y Rosen [KM90, pp 98-101].

Definición 1.13. Sean $\chi_1, \ldots, \chi_n$ caracteres de $\mathbb{F}_p$. Una suma de Jacobi es definida como

$$J(\chi_1, \ldots, \chi_n) = \sum_{t_1+\cdots+t_n=1} \chi_1(t_1) \cdots \chi_n(t_n)$$

Al dar la anterior definición Einseistein pensaba en descomponer $N(x_1^k + \cdots + x_r^k = 1)$ como la suma

$$\sum_{a_1+\cdots+a_r=1} N(x_1^k = a_1) \cdots N(x_r^k = a_r)$$

Resolver esa suma fue un problema abierto para aquella generación de matemáticos (Euler, Gauss, Einseistein, Jacobi) y pocos se ocuparon de ella durante años;

hasta que Hardi y Littlewood en su trabajo sobre al problema de Waring, y con la intensión de obtener propiedades de sus "Series Singulares"se toparon con la necesidad de hacer una evaluación asintótica de la congruencia

$$x_1^k \cdots x_r^k = 0$$

cuando p tiende a infinito.

Desde luego, tuvieron que recurrir a el método de Jacobi para evaluar dicha congruencia. Fue de esta manera que los matemáticas volvieron nuevamente los ojos al antiguo problema planteado. Generalizando aún más, se planteo encontrar las soluciones a la ecuación

$$a_1 x_1^{k_1} + \cdots + a_r x_r^{k_r} = 0$$

con $a_1, a_2, \ldots, a_r$ en $\mathbb{F}_q$, con $q = p^r$, p primo.

Este problema no fue resuelto sino hasta 1949, con los trabajos separados y casi simultáneos de Hue-Vandiver y A.Weil.

Similares resultados fueron obtenidos por Daverport (1931) y Mordel (1933) para la ecuación $x^k = f(y)$ donde f es un polinomio.

2 Observaciones Preliminares

El propósito de este capítulo es el de prover las definiciones, los resultados y las observaciones indispensables para desarrollar más adelante nuestro estudio de las curvas Elípticas.

La discusión abarcará cuestiones generales que superan el ámbito de las curvas elípticas, pero que representan la herramienta necesaria para realizar su estudio.

Así, por la temática que hemos elegido presentar en estas *Observaciones Preliminares,* no será extraño saltar de una definición general, como puede ser la de puntos singulares en una variedad, a la presentación de un morfismo que sólo tenga sentido sobre variedades en campos finitos (*morfismo de Frobenius).*

De esta manera el centro unificador del capítulo es el hecho de que toda discusión incluida en éste es necesaria.

El lector que tenga conocimiento de los temas que a continuación mencionamos puede, sin ningun problema, proseguir con el siguiente capítulo. Estos temas se refieren a:

- Resultados sobre morfismos de curvas.
- Definición del grado de un morfismo.
- Valuaciones sobre una curva.
- Resultados sobre curvas.
- Divisores (definición y resultas básicos).
- Espacio de diferenciales de una curva.
- Teorema de Riemman-Roch. (Enunciación)
- Teorema Fundamental de Max Noether.
- Mapeo de Frobenius.

2.1 Geometria Algebraica

Notación 2.1. Dado $\mathbb{K}$ un campo denotaremos $\overline{\mathbb{K}}$ su cerradura algebraica.

Notación 2.2. Dado $\mathbb{K}$ un campo denotaremos por $A^n_{\mathbb{K}}$ al conjunto de puntos $P = (x_1, \ldots, x_n)$, con $x_1, \ldots, x_n \in \mathbb{K}$, es decir, al espacio afín asociado a $\mathbb{K}$.

Notación 2.3. Si $\mathbb{K}$ es un campo y V una variedad definida por el conjunto de polinomios $\mathcal{P}$ con coeficientes en $\mathbb{K}$, entonces la variedad definida por $\mathcal{P}$ se denotará $V(\mathbb{K})$ si es considerada en el afín $A^n_{\mathbb{K}}$ o se denotará $V(\overline{\mathbb{K}})$ si es considerada en el afín $A^n_{\overline{\mathbb{K}}}$. Seguiremos denotando como V a la variedad definida por $\mathcal{P}$ mientras no sea importante dar una distinción entre los dos conjuntos o no exista riesgo de confusión.

Como es natural $V \subset \mathbf{A}^n_{\overline{\mathbb{K}}}$ es una variedad, si es el cero de polinomios en $\overline{\mathbb{K}}[X_1, \ldots, X_n]$. Decimos que V está definida sobre $\mathbb{K}$ si los polinomios pertenecen al anillo $\mathbb{K}[X_1, \ldots, X_n]$.

En el caso proyectivo, $V \subset \mathbb{P}^n$ es variedad si es el cero de polinomios homogeneos irreducibles en $S = \overline{\mathbb{K}}[X_0, \ldots, X_n]$. Donde S es considerado como un anillo graduado sobre $\overline{\mathbb{K}}$.

Notación 2.4. Dada una variedad V proyectiva o afín, denotaremos por $I(V)$ al ideal de la varidad, por $K[V]$ a su anillo de cordenadas y por $K(V)$ a su campo de funciones.

Notación 2.5. Dada V una variedad y $P \in V$ un punto, denotaremos al anillo local en P como O_P y a su anillo local máximal como μ_P.

Definición 2.6. Sea V una variedad definida sobre $\mathbb{K}$. Un punto $P \in V$ es no singular si

$$\dim_{\mathbb{K}} \frac{\mu_P}{\mu_P^2} = \dim V$$

donde la dimensión del lado izquierdo es su dimensión como $\mathbb{K}$-módulo y la del lado derecho es la $Altura(I(V))$. Ver [Atiya].

Observación 2.7. Esta definición de puntos no singulares es equivalente sobre variedades afines, a pedir que el rango de la matriz

$$\left(\frac{\partial f_i}{\partial X_j}(P)\right)_{1\leq i\leq m, 1\leq j\leq n}$$

sea igual a n menos $dim(V)$, donde $f_1, f_2, \ldots, f_m \in K[X]$ son los generadores de V y n la dimensión del espacio. Ver [Har77, I.5].

Ejemplo 2.8. Considere la curva $C : y^2 - x^3 = 0$ en $\mathbb{A}^2_{\mathbb{C}}$ y sea $P = (0,0)$. Entonces $\dim C = 1$, pero

$$\frac{\mu_P}{\mu_P^2} \cong \{ax + by : (a,b) \in \mathbb{C}^2\}$$

de donde

$$\dim_{\mathbb{K}} \left(\frac{\mu_P}{\mu_P^2}\right) = 2$$

Y por lo tanto C es singular en P.

Nota 2.9. La desigualdad $\dim(\mu_P/\mu_P^2) \geq \dim(V)$ siempre se cumple. [Har77, I.5.2]

Ejemplo 2.10. Si $V : x^2 - 2 = 0$ entonces $V(\mathbb{Q}) = \emptyset$ pero $V = \{\sqrt{2}, -\sqrt{2}\}$

Definición 2.11. Si $V \subset \mathbb{A}^n$ es una variedad afín, denotaremos por $\overline{V}$ a la cerradura proyectiva en $\mathbb{P}^N$ de V, es decir, a la cerradura topológica de la imagen del mapeo

$$V \subset \mathbb{A}^n \xrightarrow{\phi_i} \mathbb{P}^n$$

donde ϕ_i es la identificación canónica de $\mathbb{A}^n$ con el abierto $U_i = \{P \in \mathbb{P}^n : x_i \neq 0\}$.

Como $P = [a_0, \ldots, a_n] \in \mathbb{P}^n$, con $a_0 \neq 0$ satisface F homogeneo si y sólo si $(a_1/a_0, \ldots, a_n/a_0) \in \mathbb{A}^n$ satisface $F(1, X_1, \ldots, X_n)$, y al revés $P =$

$(a_1, \ldots, a_n) \in \mathbb{A}^n$ satisface $g \in \mathbb{K}[X_1, \ldots, X_n]$ si y sólo si $[1, a_1, \ldots, a_n] \in \mathbb{P}^n$ satisface $X_0^e g(X_1/X_0, \ldots, X_n/X_0)$; y además se cumple que

$$F(X_0, \ldots, X_n) = X_0^e F(1, X_0, \ldots, X_n) ,$$

donde $e = \deg F(1, X_0, \ldots, X_n)$, vemos que el mapeo ϕ_i es un homeomorfismo de U_i en $\mathbb{A}^n$ y por lo tanto la siguiente proposición es válida.

Proposición 2.12. *a) Si V es una variedad afín. Entonces se cumple:*

$$V = \overline{V} \cap \mathbb{A}^n$$

b) Si V es una variedad proyectiva. Entonces se cumple:

$$V \cap \mathbb{A}^n = \emptyset \quad o \quad V = \overline{V \cap \mathbb{A}^n}$$

Demostración. Clara de que ϕ_i es homeomorfismo, y de la identificación de $\mathbb{A}^n$ con U_i. □

Terminaré este capítulo presentándoles las siguientes definiciones.

Definición 2.13. Decimos que una función $f \in k(V)$ es regular en P si $f \in O_P$. Si para todo $P \in U$, f es regular en P entonces decimos que f es regular en U, donde U es cualquier subconjunto del espacio.

Definición 2.14. Un mapeo $\phi : V \to Y$, donde V y Y son variedades algebraicas, es un morfismo si es continuo bajo la topología de Zariski y además si para cada abierto $W \subset Y$, el morfismo de campos $\phi^*|_W : K(W) \to K(V)$ manda funciones regulares en funciones regulares.

2.2 Curvas

Definición 2.15. Sea $\mathbb{K}$ un campo y G un grupo totalmente ordenado, una valuación de $\mathbb{K}$ en G es un mapeo $v : \mathbb{K} \to G$, tal que para todo par $x,y \in \mathbb{K}$ cumple:

a) $v(xy) = v(x) + v(y)$

b) $v(x + y) \geq min(v(x), v(y))$

Observación 2.16. El conjunto $R = \{x \in \mathbb{K} : v(x) \geq 0\} \cup \{0\}$ es un anillo local con ideal máximal $\mu = \{x \in \mathbb{K} : v(x) > 0\}$. Si R es un dominio entero con campo de cocientes $\mathbb{K}$, R es una valuación sobre $\mathbb{K}$ si existe una valuación v de $\mathbb{K}$, tal que R es su anillo de valuación.

Es también fácil mostrar que $k = \{x \in \mathbb{K} : v(x) = 0\}$ es un campo (Si $x \in k$ entonces $v(1/x) = v(x) + v(1/x) = v(1) = 0$). Así podemos también decir que R es una valuación sobre $\mathbb{K}/k$, con $k \subset R$.

Definición 2.17. R es un anillo de valuación discreta si $G = \mathbb{N}$.

Ejemplo 2.18. Dada una curva C algebraica y un punto $P \in C$ no singular. Definimos la valuación normal (o canónica) sobre $K(C)$, como el mapeo

$$ord_P : k(C) \to \mathbb{Z} \cup \{\infty\}$$

dado por la extensión del mapeo

$$Ord_P : O_P \to \mathbb{N} \cup \{\infty\}$$

donde

$$Ord_P(x) = max\{n \in \mathbb{N} : x \in \mu_P^n\}$$

con μ_P el ideal maximal de O_P, y para $f/g \in K(C)$ definimos $ord_P(f/g)$ como

$$ord_P\left(\frac{f}{g}\right) = Ord_P(f) - ord_P(g)$$

Nota 2.19. Es rutina demostrar que el mapeo, definido arriba, es en efecto una valuación, aunque más importante es la observación de que O_P es un anillo de valuación discreta.

Definición 2.20. Sean C y P como arriba $f \in K(C)$, decimos que $ord_P(f)$ es el orden de f en P, y que f tiene un cero en P si $ord_P(f) > 0$ o que tiene un polo en P si $ord_P(f) < 0$.

Observación 2.21. Es claro que si f es una función regular entonces $ord_P(f) \geq 0$. Pues existe un abierto U tal que $P \in U$ y $f = g/h$, con g y h polinomios, y $h(P) \neq 0$ y por lo tanto $f \in O_P$.

Observación 2.22. Veamos que el conjunto $A(f) = \{P \in C : ord_P(f) > 0\}$ es finito para $f \neq 0$ fija. Como f es función racional en C, existe un abierto denso $U \in C$, tal que $P \in U$ y f se escribe de la forma g/h, con $g,h \in K[C]$ donde $h \notin I(P)$, entonces los puntos donde $g(P) = 0$ son los puntos donde $g/h \in \mu_P$. De donde, si $f \neq 0$ entonces $g \neq 0$, pero g es un polinomio y por lo tanto sólo existe un número finito de puntos $\{P_1, \ldots, P_n\} \subset U$ donde $f = 0$, es decir donde $ord_P(f) > 0$. Y como claramente U es igual a C menos un número finito de puntos, se sigue que $A(f)$ es finito.

Corolario 2.23. *Toda función $f \in K(C)$ tiene solamente un número finito de polos y ceros.*

Demostración. Se sigue de que $ord_P(f) < 0$ si y sólo si $ord_P(1/f) > 0$. □

Nota 2.24. En general, es cierto que si $\mathbb{K}$ es un campo y v una valuación el conjunto

$B = \{R \subset \mathbb{K} :$ tal que R es un anillo de valuación de $v\}$ es finito.

Es decir, toda valuación tiene un número finito de anillos de valuación. Esta demostración general puede verse en [Har77, I.6.5] o [Sha74, III.1]

2.3 Morfismos de Curvas

Proposición 2.25. *Sea $V \in \mathbb{P}^n$ una variedad proyectiva, C una curva y sea $P \in C$ un punto al que se le puede asociar una valuación v sobre $\mathbb{Z}$, tal que O_P es su anillo de valuación sobre $\mathbb{K}(C)$. Si $\phi : \{C - P\} \to V$ es un morfismo entonces existe un único morfismo $\overline{\phi} : C \to V$ que extiende a ϕ.*

Demostración. Como $V \subset \mathbb{P}^n$, basta con demostrar que existe un morfismo $\overline{\phi}$ que extiende a ϕ para el caso $V = \mathbb{P}^n$.

Sea

$$U = \mathbb{P}^n - \{X_i = 0\}_{i=0}^n$$

donde X_i son las coordenadas de $\mathbb{P}^n$. Podemos suponer por inducción que $\phi(V - P) \cap \mathbb{P}^n \neq \emptyset$, de lo contrario existe i tal que $\phi(V - P) \subset H_i \cong \mathbb{P}^{n-1}$, donde H_i es el hiperplano definido por $X_i = 0$.

Las funciones X_i/X_j son regulares sobre U, de donde componiendo con ϕ obtenemos las funciones regulares

$$f_{ij} = \phi \circ \frac{X_i}{X_j}$$

sobre un abierto de C. Y por lo tanto, pertenecientes al conjunto $\mathbb{K}(C)$.

Así las cosas, si v es una valuación asociada a O_P, ésta es una valuación que se extiende a $\mathbb{K}(C)$. Sea $r_i = v(f_{i0})$, de donde dado que

$$\frac{X_i}{X_j} = \frac{X_i/X_0}{X_j/X_0}$$

entonces tenemos $v(f_{ij}) = r_i - r_j$.

Escojamos s tal que r_s es mínimo. Entonces definimos $\overline{\phi}(P) = (f_{0s}(P), \ldots, f_{ns}(P))$ y $\overline{\phi}(Q) = \phi(Q)$ para $Q \neq P$. Note que $\overline{\phi}$ está bien definido en $\mathbb{P}^n$, dado que $f_{ss}(P) = 1$. Basta demostrar que $\overline{\phi}$ es morfismo. La unicidad sigue del siguiente lema cuya prueba se encuentra en [Har77, I.4.1].

Lema 2.26. *Sean X y Y variedades, ϕ y ψ morfismos de X en Y que coinciden en un abierto $U \subset X$. Entonces $\phi = \psi$.*

Ahora sea $U_k \subset \mathbb{P}^n$ el abierto $X_k \neq 0$, su anillo de coordenadas claramente es

$$\mathbb{K}[\frac{X_0}{X_k}, \ldots, \frac{X_n}{X_k}]$$

Es decir, para cualquier abierto $V \subset U_k$, las funciones regulares son enviadas bajo cualquier morfismo en funciones regulares, y por lo tanto $\overline{\phi}$ es un morfismo. □

Corolario 2.27. *Sea C una curva, $V \subset \mathbb{P}^n$ una variedad, $P \in C$ un punto no singular y $\phi : C \to V$ un mapeo racional. Entonces ϕ es regular en C.*

Demostración. Existe un abierto $U \in C$ donde ϕ es regular, si $P \in U$ el corolario sigue. Si $P \notin U$, entonces, por la proposición 2.25, ϕ se extiende de manera única a un morfismo de $\overline{\phi} : U \cup \{P\} \to \mathbb{P}^n$, ahora como además se cumple que $\phi(P) = \overline{\phi}(P)$, entonces se tiene que ϕ es regular en P. □

Ejemplo 2.28. Sea $C/\mathbb{K}$ una curva lisa y $f \in \mathbb{K}$ una función racional. Entonces f define un mapeo racional,

$$\overline{f} : C \longrightarrow \mathbb{P}^1$$

$$P \longmapsto [f(P), 1]$$

que por el corolario anterior es un morfismo, el cual está dado explícitamente por la fórmula

$$f(P) = \begin{cases} [f(P), 1] & \text{si } f \text{ es regular en } P \\ [1, 0] & \text{si } f \text{ tiene polo en } P \end{cases}$$

Análogamente, si tenemos $\phi : C \to \mathbb{P}^1$ una función racional, es también un morfismo, entonces si $U \subset \mathbb{P}^1$ es el abierto $\mathbb{P} - \{[1, 0]\}$, su anillo de

coordenadas $\mathbb{K}[X]$ es el anillo de polinomios en la variable X, y además a todo punto $Q \in \mathbb{P}^1$ podemos verlo en la forma $[X, 1]$.

Pero la variable $X \in \mathbb{K}[X]$ define una función regular sobre U. De ahí que como ϕ es un morfismo, $\overline{X} = X \circ \phi$ es regular en un abierto de C. Es decir, $\overline{X}$ es una función racional en C.

Ademas el morfismo $\overline{\overline{X}} : C \to$ definido como

$$P \to [\overline{X}, 1]$$

es justamente el morfismo ϕ, esto se nota viendo que la imagen de ϕ en U puede escribirse de la forma $[\mu(P), 1]$, donde μ es función del punto P y que por tanto $\overline{X}(P) = \mu(P)$ para toda $P \in U$, y finalmente aplicando el lema 2.26 tenemos el resultado sobre la coincidencia de los morfismos en toda C.

Comentario 2.29. De esta manera tenemos una correspondencia uno a uno

$$\mathbb{K}(C) \cup \{\infty\} \longleftrightarrow \{\text{mapeos } \phi : C \to \mathbb{P} \text{ definidos sobre } \mathbb{K}\}$$

El símbolo ∞ lo incluimos, porque de las observaciones anteriores obtuvimos una correspondencia uno a uno

$$\mathbb{K}(C) \longleftrightarrow \{\text{mapeos } \phi : C \to \mathbb{P} \text{ tal que } \phi(C) \cap U \neq 0\}$$

Y por tanto, contamos todos los mapeos $\phi : C \to \mathbb{P}$ excepto el mapeo constante $\infty(P) = [0, 1]$. De esta manera identificamos al mapeo $\infty(P)$ con el símbolo ∞.

Volviendo a nuestra discusión general, el siguiente teorema demostrado en [Har77, II.6.8] y en [Sha74, 2.I.5;teo.4] nos será también de mucha utilidad.

Teorema 2.30. Sea $\phi : C_1 \to C_2$ un morfismo de curvas. Entonces ϕ es constante o es suprayectivo.

Sean $C_1/\mathbb{K}$ y $C_2/\mathbb{K}$ dos curvas sobre $\mathbb{K}$ y sea $\phi : C_1/\mathbb{K} \to C_2/\mathbb{K}$ un morfismo, entonces tenemos el homomorfismo de campos $\phi^* : \mathbb{K}(C_2) \to \mathbb{K}(C_1)$ que da lugar a la inclusión de campos $\phi^*\mathbb{K}(C_2) \subset \mathbb{K}(C_1)$. Así se puede demostrar que si $\phi \neq 0$ entonces $[\mathbb{K}(C_1) : \phi^*\mathbb{K}(C_2)]$ es un número finito. De donde definimos el grado de un morfismo no constante de curvas $\phi : C_1 \to C_2$ como el número

$$\deg \phi = [\mathbb{K}(C_1) : \phi^*\mathbb{K}(C_2)] .$$

Decimos que ϕ es separable si la extensión es separable.

De manera análoga, definimos $\deg_s \phi$ y $\deg_i \phi$ los grados separables e inseparables de ϕ como los grados separable e inseparables de la extensión $\mathbb{K}(C_1)/\mathbb{K}(C_2)$.

Es evidente, de la definición que

$$\deg \phi = \deg_s \phi * \deg_i \phi$$

Nuevamente en [Har77, I.6.1] vemos el siguiente resultado.

Proposición 2.31. *Las siguientes categorías son equivalentes:*

1) Curvas Proyectivas no singulares y morfismos dominantes (suprayectivos).

2) Campos de funciones de dimensión 1 sobre $\mathbb{K}$ *y* $\mathbb{K}$*-homomorfismos.*

De esta manera, si $\phi : C_1 \to C_2$ es un mapeo de curvas proyectivas de grado 1. Entonces

$$\phi^* : \mathbb{K}(C_2) \to \mathbb{K}(C_1)$$

es un $\mathbb{K}$-isomorfismo. Aplicando el cofuntor que manda $\mathbb{K}(C_i) \to C_i$ y $\phi^* \to \phi$ tenemos que ϕ es un morfismo.

Análogamente $(\phi^*)^{-1} : \mathbb{K}(C_1) \to \mathbb{K}(C_2)$ define un morfismo

$$\mu : C_2 \to C_1$$

que además cumple con

$$\phi \circ \mu(P) = P \text{ para toda } P \in C_2$$

y

$$\mu \circ \phi(P) = P \text{ para toda } P \in C_1$$

con lo que ϕ es un homomorfismo.

De ahí que hemos demostrado la siguiente proposición.

Proposición 2.32. *Si* $\phi : C_1 \to C_2$ *es un mapeo de curvas proyectivas de grado 1 entonces* ϕ *es un isomorfismo.*

2.4 Ramificaciones (Definiciones y resultados)

Definición 2.33. Sea $\phi : C_1 \to C_2$ un mapeo de curvas no singulares y sea $P \in C_1$ un punto. Definimos el índice de ϕ en P, denotado como $e_\phi(P)$, al número dado por

$$e_\phi(P) = ord_P(\phi^* t_{\phi(P)})$$

donde $t_{\phi(p)}$ es un parámetro de uniformización en $\phi(P)$.

Decimos que ϕ no está ramificada o no se ramifica en C si $e_\phi(P) = 1$ para todo punto $P \in C_1$.

Ejemplo 2.34. Si $\phi : C_1 \to C_2$ es un isomorfismo, entonces $e_\phi(P) = 1$, esto es ϕ no se ramifica. (El converso no es cierto).

Proposición 2.35. *Sea $\phi : C_1 \to C_2$ un mapeo sobre curvas no singulares, entonces se cumple:*

a) Para todo $Q \in C_2$

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg \phi$$

b) Para casi todo $Q \in C$ (excepto un número finito)

$$\#\phi^{-1}(Q) = deg_s(\phi)$$

donde $\#\phi^{-1}(Q)$ es la cardinalidad del conjunto $\phi^{-1}(Q)$.

c) Sea $\psi : C_2 \to C_3$ otro mapeo como arriba. Entonces para $P \in C_1$

$$e_{\psi \circ \phi}(P) = e_\phi(P) e_\psi(\phi P)$$

Ver el libro de Silverman [Sil85, II.2.6] para prueba del inciso c) y referencias de las pruebas de a) y b).

Corolario 2.36. *$\phi : C_1 \to C_2$ es no ramificado si y solo si $\#\phi^{-1}(Q) = deg(\phi)$ para toda $Q \in C_2$.*

Demostración. Trivial por el inciso a) de arriba. □

2.5 Divisores

Definición 2.37. El conjunto de divisores de una curva C es el grupo libre sobre $\mathbb{Z}$ generado por los puntos de C. Y lo denotamos por $Div(C)$

Ejemplo 2.38. Si f es una función racional sobre C, entonces definimos el divisor de f, $div(f) \in Div(C)$ como

$$div(f) = \sum_{P \in C} ord_P(f)(P)$$

Obviamente $div(f)$ es un divisor ya que $ord_P(f) = 0$ para todo $P \in C$, salvo un número finito de puntos. Ver 2.23.

Definición 2.39. Un divisor D es principal, si existe una función $f \in \mathbb{K}(C)$ tal que $D = div(f)$.

Claramente el conjunto de los divisores principales forma un subgrupo de $Div(C)$, que denotaremos $Pri(C)$.

Definición 2.40. Decimos que un divisor D es linealmente equivalente o esta relacionado con $\overline{D}$ si $D - \overline{D}$ es principal. Escribiremos $D \sim \overline{D}$ para indicar la equivalencia lineal.

Definición 2.41. El grado de un divisor $D = \sum_{P \in C} n_P(P)$, es el número

$$deg(D) = \sum_{P \in C} n_P$$

Ejemplo 2.42. El conjunto de los divisores de grado cero

$$Div^0(C) = \{D \in Div(C) : deg(D) = 0\}$$

es un subgrupo de $Div(C)$.

Definición 2.43. Decimos que $D = \sum_{P \in C} n_P(P)$ es efectivo si $n_P \geq 0$ para todo $P \in C$. Análogmente si $n_P \leq 0$ para toda $P \in C$ decimos que D es no positivo, o no nulificable.

Ejemplo 2.44. Todos los divisores principales de una curva, son efectivos y no positivos. [Har77, II.6.10] o [Sha74, 2.III.2]. Además si $div(f) = 0$, entonces f no tiene polos, de donde el morfismo $f : C \to \mathbb{P}^1$ dado por

$$P \to [1, f(P)]$$

no cubre el punto $[0, 1]$, vease 2.28, y por lo tanto el mapeo es constante por la proposición 2.27. De donde $f \in \mathbb{K}$.

Definición 2.45. El grupo de Picard de una curva C se define como el cociente

$$Pic(C) = \frac{Div(C)}{Pri(C)}.$$

Aprovechándonos de que todo divisor principal de una curva C es de grado cero, podemos definir la parte de grado cero del grupo de Picard como

$$Pic^0(C) = \frac{Div^0(C)}{Pri(C)}.$$

Resumiendo tenemos que la siguiente sucesión es exacta

$$1 \to \overline{\mathbb{K}} \to \overline{\mathbb{K}}(C) \to^{div} Div^0 \to Pic^0(C) \to 0.$$

donde $\overline{\mathbb{K}}$ es la cerradura algebraica de $\mathbb{K}$.

Ejemplo 2.46. Si $C = \mathbb{P}^1$ entonces $\mathrm{Pic}^0(C) = 0$, es decir

$$1 \to \overline{\mathbb{K}} \to \overline{\mathbb{K}}(C) \to^{div} Div^0 \to 0.$$

es exacta.

Esto se sigue de que si $D = \sum_{i=0}^{m} n_{P_i} P_i \in Div^0(\mathbb{P}^1)$. Definimos la función racional f como

$$f(P) = \prod_{i=0}^{m} (x_i Y - y_i X)^{n_{P_i}}$$

donde $P_i = (x_i, y_i)$ para $1 \leq i \leq m$. Así notamos que f tiene ceros y polos en los puntos P_i, con multiplicidades $ord_P(f) = n_P$ para todo $P \in C$. Es decir, se ha mostrado que $D = div(f)$.

Comentario 2.47. En el siguiente capítulo veremos que la estructura de grupo de una curva elíptica E es precisamente el grupo $Pic^0(E)$. Dicho de otra manera, la variedad Jacobiana de E resulta ser la misma E.

Para terminar esta subsección definiremos 2 mapeos importantes. Sea $\phi : C_1 \to C_2$ un mapeo dado, entonces definimos

$$\phi^* : Div(C_2) \to Div(C_1)$$

como

$$(Q) \to \sum_{P \in \phi^{-1}(Q)} \cdot e_\phi(P)(P)$$

y definimos

$$\phi_* : Div(C_1) \to Div(C_2)$$

por

$$(P) \to (\phi(P)).$$

Claramente haciendo $\mathbb{Z}$-lineal estos mapeos obtenemos 2 morfismos de grupos.

Proposición 2.48. *Sea $\phi : C_1 \to C_2$ un mapeo no constante de curvas no singulares. Entonces se satisfacen las siguientes condiciones:*

a) $deg(\phi^* D) = deg(\phi) deg(D)$. $\forall D \in Div(C_2)$

b) $\phi^*(div(f)) = div(\phi^* f)$. $\forall f \in \overline{\mathbb{K}}(C_2)$

c) $deg(\phi_* D) = deg(D)$. $\forall D \in Div(C_1)$

d) $\phi_*(div(f) = div(\phi_* f)$. $\forall f \in \overline{\mathbb{K}}(C_1)$

Demostración. a) Utilizando que $deg(\phi) = \sum_{P \in \phi_{-1}(Q)} e_\phi(P)$ para toda $Q \in C_2$

b) Sigue de las definiciones y de la igualdad

$$ord_P(\phi^* f) = e_\phi(P)\, ord_{\phi(P)}(f)$$

para toda $P \in C_1$.

c) Clarísimo por la definición del mapeo ϕ_*.

d) Ver el libro de Serre "Local Fields"[Ser79, I.14] o "Algebraic Number Theory"de Lang [Lan70, 1.22] . □

2.6 Formas Diferenciales

Sea Ω_C el espacio de formas diferenciales de una curva C, definido como el conjunto de símbolos dx con $x \in \overline{\mathbb{K}}(C)$, tal que cumple con las siguientes igualdades:

$$d(x + y) = dx + dy$$

$$d(xy) = ydx + xdy$$

$$dc = 0 \ \ \forall c \in \overline{\mathbb{K}}$$

De esta manera, Ω_C es un $\overline{\mathbb{K}}(C)$-espacio vectorial.

Sea $\phi : C_1 \to C_2$ un mapeo no constante. Entonces el mapeo $\phi^* : \mathbb{K}(C_2) \to \mathbb{K}(C_1)$ induce de manera natural un mapeo:

$$\phi^* : \Omega_{C_2} \to \Omega_{C_1}$$

dado por

$$\phi^*(\sum f_i dx_i) = \sum \phi^* f_i d(\phi^* x_i).$$

Observación 2.49. Ω_C es de dimensión 1 como $\overline{\mathbb{K}}(C)$-espacio vectorial. [Mat80, 27.A.B], [Rob73, II,3.4] o [Sha74, III.4.thm.3]

Además, si $x \in \overline{\mathbb{K}}(C)$, entonces dx es una $\mathbb{K}(C)$ base para Ω_C si y solo si $\mathbb{K}(C)/\mathbb{K}(x)$ es una extensión finita separable. Más aún, si t es un parámetro de uniformización en un punto $P \in C$ entonces $\mathbb{K}(C)/\mathbb{K}(t)$ es una extención finita separable [Sil85, II.1.4], y por tanto, dt es un generador de Ω_C.

Definición 2.50. Sea $w = gdt \in \Omega_C$, con t parámetro de uniformización y $g \in \mathbb{K}(C)$. El divisor asociado a w es el divisor $div(g)$. Es decir:

$$div(w) = \sum_{P \in C} ord_P \left(\frac{dw}{dt} \right)$$

donde dw/dt es entendida como la función g.

Observación 2.51. El divisor $div(w)$ no depende del parámetro de uniformización elegido. Sean t y $\bar{t}$ dos parámetros de uniformización en P. Entonces podemos encontrar dos funciones $f,g \in \mathbb{K}(C)$ tal que $dt = gd\bar{t}$ y $d\bar{t} = fdt$. Donde naturalmente $gf = I_{\mathbb{K}(C)}$, y utilizando que si t y $\bar{t}$ son regulares en P entonces dt y $d\bar{t}$ son también regulares en P [Rob73, II.3.10] tenemos que g y f son constantes, ejemplo 2.44. Y por tanto: $ord_P(dw/dt) = ord_P(cdw/d\bar{t}) = ord_P(dw/d\bar{t})$, c constante.

Definición 2.52. Una diferencial w es regular u holomorfa si $div(w)$ es efectivo. Es no nulificable si $-div(w)$ es efectivo.

Comentario 2.53. Como Ω_C es un espacio vectorial sobre $\overline{\mathbb{K}}$ de dimensión 1, entonces si w_1, w_2 son 2 diferenciales no nulos tenemos que

$$div(w_1) \sim div(w_2)$$

Es decir, la imagen del conjunto

$$div(\Omega_C) = \{D \in Div(C) : D = div(w), w \in \Omega_C\}$$

en $Pic(C)$ es únicamente un elemento que llamamos la clase de divisores canónicos. A cada elemento de esta clase lo llamaremos un divisor canónico.

Ejemplo 2.54. En $\mathbb{P}^1$ la clase de los divisores canónicos es la de los divisores de grado -2. Considere la función racional $f : \mathbb{P}^1 \to \overline{\mathbb{K}}$ dada por:

$$[x, y] \to \frac{x}{y}$$

es suficiente demostrar que $div(f) = -2([0, 1])$. Sea $P = [\lambda, \mu] \in \mathbb{P}^1$, entonces tenemos que $(\mu X - \lambda Y) = I(P)$, y si $\mu \neq 0$ podemos escribir $I(P) = (X - \eta Y)$ y por tanto si $P \neq [1, 0]$ tenemos que $X/Y - \eta$ es un parámetro de uniformización en P.

De donde se sigue que

$$d\left(\frac{X}{Y}\right) = d\left(\frac{X}{Y} + \eta\right) = d\left(\frac{X + \eta Y}{Y}\right)$$

y por lo tanto

$$ord_P\left(d\left(\frac{X}{Y}\right)\right) = 0.$$

Ahora si $P = [1, 0]$, entonces Y/X es un parámetro de uniformización y así:

$$d\left(\frac{X}{Y}\right) = d\left(\frac{Y}{X}\left(\frac{X}{Y}\right)^2\right) = \left(\frac{X}{Y}\right)^2 d\left(\frac{Y}{X}\right) + 2d\left(\frac{X}{Y}\right).$$

Lo que implica que

$$d\left(\frac{X}{Y}\right) = -\left(\frac{X}{Y}\right)^2 d\left(\frac{Y}{X}\right)$$

Y como

$$ord_P\left(\frac{X}{Y}\right)^2 = -2$$

Obtenemos que

$$Div\left(\frac{X}{Y}\right) = -2[1,0].$$

Los siguientes resultados enriqueceran más la discusión sobre la relación entre extensiones separables, paráuetros de uniformización y diferenciales.

Observación 2.55. Sea $x \in \mathbb{K}(C)$ tal que $\mathbb{K}(C)/\mathbb{K}(x)$ es una extensión separable y $x(P) = 0$. Entonces para toda $f \in \overline{\mathbb{K}}(C)$

$$ord_P(fdx) = ord_P(f) + ord_P(x) - 1$$

Ver demostración en [Sil85, pp 36].

Comentario 2.56. Si f es regular en C entonces df/dx es también regular en C. Ver Hartshorne [Har77, IV.2.1].

Proposición 2.57. *Sea $\phi : C_1 \to C_2$ un mapeo no constante de curvas. Entonces ϕ es separable si y sólo si el mapeo*

$$\phi^* : \Omega_{C_2} \to \Omega_{C_1}$$

es inyectivo.

2.7 Teorema de Riemman-Roch

En las secciones anteriores considerando a una curva C y a una función racional $f \in \mathbb{K}(C)$ nos interesamos en los polos y ceros de f en C, y según vimos, esto dió lugar al divisor:

$$Div(f) = \sum_{P \in C} n_P(P)$$

donde claramente podíamos numerar los puntos $\{P_1, P_2, \ldots, P_m\}$ tales que $n_{P_i} \neq 0$.

Ahora invirtiendo el proceso fijamos los puntos (un número finito) y las multiplicidades de los puntos y nos podemos preguntar acerca de las funciones que sólo tienen polos en los puntos dados y cuya multiplicidad no sobrepasa las multiplicidades dadas, esto es, si $\{n_{P_i}\}_{i=1}^{i=m}$ son las multiplicidades de los polos (numeros positivos); entonces nos preguntamos por las funciones f tales que:

$$Div(f) \geq -\sum_{i=0}^{i=m} n_{P_i}(P_i)$$

En general, si D es un divisor de la curva, podemos considerar el conjunto

$$\mathcal{L}(D) = \{f \in \mathbb{K}(C) : div(f) \geq -D\} \cup \{0\}.$$

Y se muestra que $\mathcal{L}(D)$ es un $\mathbb{K}$-espacio vectorial finitamente generado. Ver [Har77, II.5.19].

Ejemplo 2.58. Si $D = 0$, entonces

$$\mathcal{L}(D) = \{\text{el conjunto de las funciones regulares de } C\}$$

Además como $f \in \mathcal{L}(0)$ no puede tener ceros entonces tampoco tiene polos, pues $deg(f) = 0$ de ahí que $div(f) = 0$ y por lo tanto f es constante. 2.44.

Ejemplo 2.59. Consideremos $degD < 0$, entonces si $f \in \mathbb{K}(C)$ y $f \neq 0$ podemos ver que

$$-degD = deg(-D) \geq deg(f) = 0$$

lo que no puede ocurrir, y por tanto

$$\mathcal{L}(D) = 0$$

y obviamente $\ell(D) = \dim_{\mathbb{K}} \mathcal{L}(D) = 0$.

Observación 2.60. Si $D \sim \overline{D}$ entonces $\mathcal{L}(D) \cong \mathcal{L}(\overline{D})$.

Tomemos $g \in \mathbb{K}(C)$ tal que $D - \overline{D} = div(g)$, así definamos el mapeo $g : \mathcal{L}(D) \to \mathcal{L}(\overline{D})$ dado por:

$$f \to fg.$$

Nótese que está bien definido: si $div(f) \geq -D$ entonces:

$$div(fg) = div(f) + div(g) = div(f) + D - \overline{D} \geq -D + D - \overline{D} \geq -\overline{D}.$$

y además $g^{-1} : \mathcal{L}(\overline{D}) \to \mathcal{L}(D)$ es el mapeo:

$$f \to f\frac{1}{g}.$$

Así tenemos que claramente el mapeo g es un isomorfismos de espacios vectoriales.

Ejemplo 2.61. Si K_C es un divisor canónico de C, digamos $K_C = div(w)$, entonces $\mathcal{L}(K_C)$ es el conjunto de funciones tales que

$$div(f) \geq -div(w)$$

es decir, el conjunto de funciones tal que $div(fw)$ es holomorfo. En el caso de que $w = dt$ con t parámetro de uniformización, entonces $\mathcal{L}(K_C)$ es el conjunto de diferenciales con f constante. Por la proposición 2.58.

A continuación uno de los teoremas más importantes en la geometría algebraica de curvas: *El Teorema de Riemman-Roch.*

Teorema 2.62. (Riemman-Roch) Sea C una curva no singular y K_C un divisor canónico en C. Entonces existe un entero $g \geq 0$, tal que para cualquier divisor $D \in Div(C)$

$$\ell(D) - \ell(K_C - D) = degD - g + 1$$

Una prueba que utiliza teoría de cohomologia y dualidad de Serre aparece en Hartshorne [Har77, IV.1], para una prueba con métodos más elementales ver [Lan82, ch.1]. Otra prueba bastante geométrica la encontramos en el libro de William Fulton [Ful69, 8.6].

Nota 2.63. El número g obtenido es conocido como el género de la curva y coincide con el viejo concepto de género topológico que representa intuitivamente el número de "hoyos"que tiene una curva. Así por medios algebraícos vemos que el número de hoyos en una superficie incide sobre su espacio de funciones $\mathcal{L}(D)$.

Corolario 2.64. *a)* $\ell(K_C) = g$
b) $deg K_C = 2g - 2$
c) Si $deg D > 2g - 2$ *entonces*

$$\ell(D) = deg D - g + 1$$

Demostración. a) Tomando en *Riemman-Roch* $D = 0$ y viendo que $\mathcal{L}(0) = 0$, se obtiene el resultado.

b) Haciendo $D = K_C$ y utilizando el inciso a) para sustituir $\ell(K_C)$ con g se obtiene lo que queremos.

c) Si $deg > 2g - 2$, entonces por b) y el ejemplo 2.59 tenemos que $\ell(D - K_C) = 0$ y por tanto la validez buscada. □

Ejemplo 2.65. Si $C = \mathbb{P}^1$ sabemos que $deg(K_C) = -2$ por 2.54, y por tanto sabemos que el genero de $\mathbb{P}^1$ es 0. Dicho topologicamente no tiene "hoyos".

Ejemplo 2.66. En el siguiente capítulo veremos que las curvas elípticas son curvas de genero 1. Por lo tanto, invirtiendo el proceso del ejemplo anterior, tendremos que $deg K_C = 0$ para todo divisor canónico K_C. En conclusión toda diferencial de una curva elíptica es no nulificable y holomorfa.

Ejemplo 2.67. En una esfera de Riemman ($g = 0$) la dimensión del espacio de funciones racionales que tienen polos en $\{P_1, \ldots, P_m\}$ con multipliciades a lo más $\{n_1, \ldots, n_2\}$ es igual a:

$$\sum_{i=1}^{i=m} n_i + 1.$$

Analogamente, si f es una función en una curva, con $g = 0$ y $div(f)$ su divisor, la dimensión $\mathcal{L}(-div(f))$ es igual a 1. Lo que quiere decir que las funciones que tienen los mismos ceros y los mismos polos que f son las funciones kf donde $k \in \mathbb{K}$.

Ejemplo 2.68. Si E es una curva elíptica (g=1). Entonces no existen funciones $f \in \mathbb{K}(E)$ con sólo un polo simple que no sean constantes. Sea $D = (Q)$. Entonces usando el inciso c) del corolario anterior tenemos que $\ell(D) = 1$. Pero el espacio $\mathcal{L}(D)$ incluye todas las constantes, de donde, todas las funciones con a lo más un polo simple no tienen ninguno.

2.8 Indice de Intersección

Consideremos dos conjuntos algebraicos $X,H \in \mathbb{P}^n$, donde H es una hipersuperficie y $dim X = r$, que se intersecten adecuadamente, esto es, que su intersección no tenga componentes de dimensión r.

De esta manera, tendríamos

$$Y \cap H = Z_1 \cup Z_2 \cup \cdots \cup, Z_s \text{ con } \dim Z_j = r-1, Z_j \text{ irreducibles}$$

[Har77, I.7.2].

Así dada una componente Z_j estamos interesados en construir un número que nos mida *qué tan fuerte* es la intersección en dicha componente. Un número que sea *cero* para toda variedad Z de dimensión $r-1$, que no pertenezca al conjunto $\{Z_j\}$, y que sea positivo para toda Z_j, siendo además igual a 1 si los conjuntos Y y H se cruzan transversalmente en Z_j y mayor o igual que 2 si Y y H se tocan tangencialmente en Z_j.

Parecerá que pedimos mucho a este número como para poder construirlo, sin embargo, se puede construir y lo denotaremos:

$$i(Y,H,Z_j)$$

Definición 2.69. Si $\mathcal{P}$ es un primo minimal de un S-módulo graduado M. Definimos la multiplicidad de M en $\mathcal{P}$ como la longitud de $M_{\mathcal{P}}$ sobre $S_{\mathcal{P}}$. Y la denotaremos $\mathcal{M}_{\mathcal{P}}$.

Definición 2.70. El número $i(Y,H,Z_j)$ será el número $\mathcal{M}_{\mathcal{P}_j}(S/I(Y)+I(H))$, donde $\mathcal{P}_j$ es el primo minimal correspondiente a la componente Z_j.

Ejemplo 2.71. Sean $X,H \subset \mathbb{P}^2$ curvas proyectivas entonces las componentes Z_j son los puntos de intersección.

Así, de ahora en adelante pensaremos a X y a H como curvas proyectivas y a Z_j como puntos.

Proposición 2.72. *Sean C_1, C_2 curvas proyectivas definidas por F_1 y F_2 (polinómios) y $P_1,\ldots,P_m$ sus puntos de intersección entonces:*

a) $i(C_1,C_2,P) = 0$ Si y sólo si $P \neq P_i$ para $1 \leq i \leq m$.

b) $i(C_1,C_2,P) = i(C_2,C_1,P)$

c) Si $F_1 = G_1G_2$ y si S_1 y S_2 son curvas definidas por G_1 y G_2 entonces

$$i(C_1,C_2,P) = i(S_1,C_2,P) + i(S_2,C_2,P)$$

Demostración. a) Sean $\mathcal{P}_1, \ldots, \mathcal{P}_m$ los primos correspondientes a los punto $P_1, \ldots, P_m$. Entonces $(F_1, F_2) \subset \mathcal{P}_i$ para toda i (y además si $(F_1, F_2) \subset \mathcal{P}$, con $I(P) = \mathcal{P}$, se tiene $\mathcal{P} = \mathcal{P}_i$ para una i). Sea

$$n_i = max\{n \in \mathbb{Z} : (F_1, F_2) \in \mathcal{P}_i^n\}$$

Entonces si S es el anillo graduado de $\mathbb{P}^2$, obtenemos la siguientes contensiones de S-módulos:

$$\frac{S}{(F_1, F_2)} = \frac{S}{\prod_{i=1}^{i=m} \mathcal{P}_i^{n_i}} \supset \frac{S}{\mathcal{P}_m^{n_m - 1} \prod_{i=1}^{i=m-1} \mathcal{P}_i^{n_i}} \supset \cdots \frac{S}{\mathcal{P}_1^2} \supset \frac{S}{\mathcal{P}_1} \supset 0$$

La igualdad del lado izquierdo se obtiene gracias a que $(F_1, F_2) = \cap \mathcal{P}_i^{n_i}$, ver Eisenbud [Eis95, cor 2.12], ver también comentario inicial al capítulo 3 del mismo libro.

Es claro también que esta cadena es una serie de composición, cuya altura es igual a $\sum_{i=0}^{i=m} n_i$.

Ahora, localizando sobre $\mathcal{P}$ (el ideal de un punto) en la cadena de arriba y utilizando que $\mathcal{P} \cap \mathcal{P}_i = 0$ si $\mathcal{P} \neq \mathcal{P}_i$ obtenemos la cadena de $S_{\mathcal{P}}$ módulos:

$$\left(\frac{S}{F_1, F_2}\right)_{\mathcal{P}} = \frac{S}{\mathcal{P}_i^{n_i}} \supset \frac{S}{\mathcal{P}_i^{n_i - 1}} \supset \cdots \supset \frac{S}{\mathcal{P}_i} \supset 0$$

si $\mathcal{P} = \mathcal{P}_i$ para algún i, o bien la cadena trivial

$$0 \supset 0$$

si $\mathcal{P} \neq \mathcal{P}_i$ para todo i.

De donde sigue el resultado buscado.

b) Trivial de la definición.

c) Se sigue localizando la siguiente sucesión exacta:

$$0 \to \frac{S}{(F_1, G_1)} \to \frac{S}{(F_1, G_1 G_2)} \hookrightarrow \frac{S}{(F_1, F_2)} \to 0$$

dada por

$$Z \to G_2 Z \hookrightarrow G_1 Z.$$

□

Definición 2.73. Se define el divisor de intersección de dos curvas C_1,$C_2 \in \mathbb{P}^2$, como el divisor:

$$R_1 \cdot R_2 = \sum_{P \in \mathbb{P}^2} i(C_1, C_2, P)(P)$$

siendo R_1 y R_2 los polinomios que definen a las curvas.

Claramente por el inciso a) de la proposición anterior $R_1 \cdot R_2$ es en realidad un elemento de $Div(C_1)$ y de $Div(C_2)$.

Las propiedades sobre $i(C_1, C_2, P)$ estipuladas en la proposición anterior se traducen a las siguientes propiedades entre los divisores de intersección:

Proposición 2.74. *a)* $R_1 \cdot R_2 = R_2 \cdot R_1$
b) $R_1 \cdot FG = R_1 \cdot F + R_2 \cdot G$
c) $F \cdot G = F \cdot (AF + G)$

Demostración. Todo es claro menos c), el cual se sigue del isomorfismo:

$$\frac{S}{(F,G)} \cong \frac{S}{(F, AF+G)}.$$

□

Definición 2.75. Sean C_1,C_2 dos curvas que intersectan a C, decimos que C_2 intersecta a C en un ciclo mayor que C_1 si

$$F_2 \cdot F \geq F_1 \cdot F$$

donde F_i son los polinomios que generan a C_i y F el que genera a C.

Considerando la definición de arriba, es natural preguntarse si existe una curva S definida por $G = 0$, que tenga justamente como divisor de intersección a:

$$D = F_2 \cdot F \dot{-} F_1 \cdot F$$

Pero encontrar dicha curva es equivalente a pedir que exista una ecuación, con A y B polinómios (formas) tales que $F_2 = AF + BF_1$, con grados $\deg H - \deg F$ y $\deg H - \deg G$ respectivamente. Así tendriamos

$$F_2 \cdot F = (AF + BF_1) \cdot F = (BF) \cdot F = B \cdot F + F_1 \cdot F$$

Siendo la curva generada por B la que buscamos.

Teorema 2.76. Max Noether's Fundamental Theorem. Si F,G,H son curvas proyectivas en $\mathbb{P}^2$. Asumiendo que F y G no tienen componentes en común. Entonces existe una equación $H = AF + BG$ con A,B polinomios de grados $\deg H - \deg F$, $\deg H - \deg G$ respectivamente, si se cumple cualquiera:

a) F y G se intersectan transversalmente en todo punto $P \in F \cap G \cap H$.

b) P es no singular en F y $i(P, F, P) \geq i(G, F, P)$.

c) F y G tienen tangentes distintas en P y

$$\mu_P(H) \geq \mu_P(F) + \mu_P(G) - 1$$

Corolario 2.77. *Sean C_1, C_2 y C curvas en $\mathbb{P}^2$. Si*

a) C_1 y C_2 se intersectan en $\deg C_1 \deg C_2$ puntos distintos, y C cruza a través de esos puntos

b) Todos los puntos de $C_1 \cap C_2$ son no singulares en C_1 y $C \cdot C_1 \geq C_2 \cdot C_1$. Entonces existe una curva D tal que

$$D \cdot C_1 = C \cdot C_1 - C_2 \cdot C_1$$

Demostración. a) Sigue directamente del inciso a) del teorema, y utilizando el teorema de Bezout para ver que todo punto $P \in F \cap G$ tiene índice de multiplicidad 1.

b) Es exactamente la misma afirmación del inciso b) del teorema, en el caso de curvas. □

Ejemplo 2.78. Sea C una cúbica irreducible y C_1 y C_2 otras dos cúbicas. Entonces suponiendo que $C_1 \cdot C = \sum_{i=1}^{9} P_i$ donde P_i son no singulares en C (no necesariamente distintos) y suponiendo que $C_2 \cdot C = \sum_{i=1}^{8} P_i + Q$. Entonces $Q = P$.

Demostración. Sea L una línea que pase por P_9, entonces $C \cdot L = P_9 + T + R$ de esta manera: $C_2 L \cdot C = C_1 \cdot C + Q + T + R$. Así por el inciso b) del corolario 2.77, existe una recta M, tal que $M \cdot C = Q + T + R$ y por tanto $M = L$, de donde forzosamente $Q = P_9$. □

2.9 Mapeo de Frobenius

Consideremos en esta sección $\mathbb{K}$ un campo con $char(\mathbb{K}) = p$, y sea $q = p^s$, entonces si C es una curva en $\mathbb{P}^n$ definimos como la curva $C^{(q)}$ a la curva

generada por el ideal $I(I(C)^{(q)})$ donde $I(C)^{(q)}$ es la imagen de $I(C)$ bajo el mapeo

$$q : \mathbb{K}[C] \to \mathbb{K}[C] \qquad f \to f^{(q)}$$

Ahora definimos el q^{th}-mapeo de Frobenius $\phi : C \to C^{(q)}$ al mapeo dado por

$$P = [X_0, \ldots, X_n] \to P^{(q)} = [X_0^q, \ldots, X_n^q]$$

Como $q = p^s$ tenemos que el mapeo esta bien definido, dado que $f^{(q)}(P^{(q)}) = (f(P))^q$. Aún más si $\mathbb{K}$ es un campo finito con q elementos entonces trivialmente tendríamos que $C = C^{(q)}$ y además el q^{th}-morfismo de Frobenius es justamente el mapeo identidad $\phi : C \to C$. Es decir, el conjunto de puntos racionales sobre $\mathbb{K}$, de donde $C(\mathbb{K}) = Ker(1 - \phi)$.

De la definición y usando el teorema 2.27 vemos que ϕ es suprayectivo. El siguiente teorema nos conduce a un corolario importante.

Teorema 2.79. Sea $\mathbb{K}$ un campo de característica $p > 0$, $q = p^r$, $C/\mathbb{K}$ una curva y $\phi : C \to C_1$ el q^{th}-morfismo de Frobenius. Entonces

a) $\phi^*\mathbb{K}(C^{(q)}) = \mathbb{K}(C)^q = \{f^q : f \in \mathbb{K}(C)\}$

b) ϕ es puramente inseparable.

c) $\deg \phi = q$

Para la prueba ver el libro de Joseph Silverman [Sil85, II.2.11].

Corolario 2.80. *Todo mapeo $\psi : C_1 \to C_2$ de curvas proyectivas sobre un campo de característica $p > 0$ se factoriza como*

$$C_1 \to^{\phi} C_1^{(q)} \to^{\lambda} C_2$$

donde $q = deg_i(\psi)$, y ϕ es el q^{th}-morfismo de Frobenius.

Demostración. Sea K la cerradura separable de $\psi^*\mathbb{K}(C_2)$ en $\mathbb{K}(C_1)$. Entonces $\mathbb{K}(C_1)/K$ es puramente inseparable de grado $q = p^r$, y entonces $\mathbb{K}(C_1)^q \subset K$. Pero por 2.79.

$$\mathbb{K}(C_1)^q = \phi^*\mathbb{K}(C_1^{(q)}) \text{ y } [\mathbb{K}(C_1) : \mathbb{K}(C_1^{(q)})] = q$$

De donde comparando grados $K = \mathbb{K}(C_1^{(q)})$. De esta forma se tiene la siguiente torre de extenciones

$$\mathbb{K}(C_2)/\mathbb{K}(C_1^{(q)})/\mathbb{K}(C_1)$$

por lo que utilizando la proposición 2.31 se sigue el resultado. □

3 Geometría de Curvas Elípticas

En este capítulo estudiaremos la geometría de las curvas elípticas, mencionando algunos invariantes importantes, y presentando la estructura de grupo sobre estas curvas.

Empezaremos el capítulo por dar dos definiciones alternativas para una curva Elíptica. Una será más explicita ya que se da en terminos de una ecuación cúbica concreta, a saber,

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2z + a_4XZ^2 + a_6Z^3$$

donde $a_1, a_2, \ldots, a_6$ son elementos del campo.

Y la otra será más abstracta y se definirá utilizando el invariante de una curva g (género) que vimos en el capítulo anterior, cuando discutimos el teorema de *Riemman-Roch*, el cual utilizaremos después para demostrar la equivalencia de ambas definiciones.

Más adelante, presentaremos dos maneras diferentes de presentar la estructura de grupo sobre las curvas Elípticas. La primera construcción será totalmente geométrica: por medio de trazo de rectas describiremos la forma de sumar dos puntos, además de que escogeremos el elemento especial O y la obtención del inverso. La segunda forma será puramente algebraica y la haremos haciendo una identificación entre los divisores de grado cero del grupo de Picard de la curva y los puntos de esta, así resultará que el grupo sobre la curva será justamente isomorfo al grupo de Picard de grado cero de ella.

Finalmente, cerraremos nuestro capítulo con el estudio de las isogenias de una curva elíptica, las propiedades y las herramientas indispensables para que en el siguiente capítulo estemos en condiciones de probar las "Conjeturas de Weil para curvas elípticas".

3.1 Ecuación de Weiestrass para curvas elípticas

Definición 3.1. Una curva elíptica E es una curva proyectiva en $\mathbb{P}^2$ isomorfa a una curva dada por la ecuación de Weiestrass

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

donde $a_1, a_2, \ldots, a_6 \in \mathbb{K}$.

Será costumbre de ahora en adelante ver nuestra curva elíptica E en el afín $Z \neq 0$, en ese caso, la curva elíptica se transformará en la ecuación:

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

donde $x = \frac{X}{Z}$ y $y = \frac{Y}{Z}$, nos representa el cambio de coordenadas que pasa de una ecuación a otra.

Muchas veces, también es util para realizar cálculos con mayor facilidad trasladar nuestra curva al origen, en ese caso tendremos la ecuación:

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

o considerar que la curva elíptica E es no singular, en cuyo caso obtendríamos (después de trasladar al origen) la mini ecuación:

$$y^2 + a_1xy = x^3 + a_2x^2$$

Nota 3.2. Podemos apreciar en la ecuación de Weiestrass que el único punto que queda en la línea al infinito ($Z = 0$) es el único punto $[0, 1, 0]$. Dado que $Z = 0$ implica $X = 0$.

Nota 3.3. Es importante notar que los únicos cambios de coordenadas que preservan la forma de la ecuación de Weiestrass son de la forma

$$x = u^2\bar{x} + r \quad y = u^3\bar{y} + u^2s\bar{x} + t$$

Naturalmente, al aplicarle un cambio de coordenadas a una curva elíptica es necesario ser lo suficiente cuidadoso para no alterarle la forma de Weiestrass cuando sean necesario. Como caso particular, es fácil ver que una traslación no nos altera la forma, por lo tanto, no existirá ningún impedimento par trasladar al origen la ecuación de Weiestrass.

Definición 3.4. Sea $char(\mathbb{K}) \neq 2$. Entonces completando cuadrado del lado izquierdo de la ecuación de Weiestrass y sustituyendo y por $\frac{1}{2}(y - a_1x + a_3)$ obtenemos la ecuación:

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

donde

$$b_2 = a_1^2 + 4a_2$$

$$b_1 = 2a_1 + a_1a_3$$

$$b_6 = a_3^2 + 4a_6$$

y definimos

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$$

$$c_4 = b_2^3 - 24b_4$$

$$c_6 = b_2^3 + 36b_2b_4 - 216b_6$$

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

$$j = c_4^3/\Delta$$

$$w = dx/(2y + a_1x + a_3) = dy/(3x^2 + 2a_2x + a_4 - a_1).$$

Llamamos a Δ el discriminante de la ecuación de Weiestrass, a j el j-invariante de una curva elíptica E y a w el invariante diferencial de E.

Observación 3.5. La igualdad

$$\frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}$$

se desprende (naturalmente) de la ecuación

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

aplicando de ambos lados el operador diferencial d, y utilizando las reglas de derivación.

Ejemplo 3.6. El invariante diferencial

$$\frac{dx}{2y + a_1 + a_3}$$

nos representa en $\mathbb{P}^2$, es decir, en coordenadas homogéneas a la diferencial

$$\frac{Z}{2Y + a_1X + a_3Z} d\left(\frac{X}{Z}\right) \in \Omega_C$$

donde claramente $\frac{X}{Z}$ es un parámetro de uniformización en $P = [0, Y, 1]$ con

$$Y = -\frac{a_3 + \sqrt{b_6}}{2}$$

Análogamente

$$\frac{dy}{3x^2 + 2a_2x + a_4 + a_1y}$$

representa a la diferencial homogénea

$$\frac{Z^2}{3X^2 + a_2XZ + a_4Z^2 - a_1YZ} d\left(\frac{Y}{Z}\right)$$

donde $\frac{Y}{Z}$ es parámetro de uniformizacion en los puntos $P = [x, 0, 1]$ donde x se mueve en las soluciones de la ecuación:

$$x^3 + a_2x^2 + a_4x + a_6 = 0$$

La siguiente proposición justifica el hecho de que se haya nombrado a j el j-ésimo invariante.

Proposición 3.7. *a) La curva dada por la ecuación de Weiestrass puede ser caracterizada como sigue:*

i) Es no singular si $\Delta \neq 0$.

ii) Tiene un nodo si $\Delta = 0$ *y* $c_4 \neq 0$.

iii) Tiene una cúspide si $\Delta = 0$ *y* $c_4 = 0$.

b) Dos curvas elípticas son isomorfas sobre $\overline{\mathbb{K}}$ *si y sólo si tienen el mismo* j*-invariante.*

c) Sea $j_0 \in \overline{\mathbb{K}}$. *Entonces existe una curva elíptica definida sobre* $\mathbb{K}(j_0)$, *con* j *invariante igual a* j_0.

Demostración. Silverman, *The Aritmetic of Elliptic Curves* [Sil85, III.1.4]. □

Otra forma adecuada de representar las curvas elípticas es por medio de la ecuación de Legendre

$$y = x(x-1)(x-\lambda),$$

la cual la podemos obtener si $char(\mathbb{K}) \neq 2$ poniendo la ecuación de Weiestrass en la forma

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

donde b_2, b_4, b_6 son como en la definición 3.4. luego remplazando (x, y) por $(4x, 8y)$ tenemos factorizando la ecuación cúbica

$$y^2 = (x-e_1)(x-e_2)(x-e_3)$$

y de esa manera volviendo a sustituir por

$$x = (e_2-e_1)\bar{x} + e_1 \quad y = (e_2-e_1)^{\frac{3}{2}}\bar{y}$$

obtenemos la forma de Legendre con

$$\lambda = \frac{e_3-e_1}{e_2-e_1} \in \overline{\mathbb{K}}$$

Proposición 3.8. *a) El discriminante Δ de E_λ esta dado por la ecuación*

$$\Delta = 2^4(\lambda-1)^2\lambda^2$$

b) El j-invariante de E_λ es

$$j(E_\lambda) = \frac{2^8(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$$

c) Existe una asociación

$$\mathbb{K} - \{0,1\} \to \overline{\mathbb{K}}$$

$$\lambda \to j(E_\lambda)$$

que es sobreyectiva y exactamente 6 a 1, excepto para $j = 0$ y $j = 1278 = 2^8$. donde la asociación es 3 a 1 y 2 a 1.

Demostración. a) Se sigue observando que de E_λ obtenemos las cantidades $b_2 = -4(\lambda + 1)$, $b_4 = 2\lambda$, $b_6 = 0$ y $b_8 = -\lambda^2$, y sustituyendo en la definición de Δ.

b) Como arriba, se calcula $b_4 = 2^4(\lambda^2 - \lambda + 1)$ y se sustituye en la definición de j.

c) Se sigue observando que si E_μ y E_λ son dos curvas en la forma de Legrende con el mismo j invariante entonces μ toma la forma de las seis posiblidades

$$\mu \in \{\lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda}\}$$

Ver [Sil85, pag 72] para una descripción más detallada. Naturalmente vemos que $j(E_\lambda) = 0$ ocurre sólo si $\lambda^2 - \lambda + 1 = 0$, es decir si $\lambda = \frac{\lambda-1}{\lambda}$, con lo que automáticamente las ternas $(\lambda, \frac{\lambda-1}{\lambda}, \frac{1}{1-\lambda})$ y $(\frac{1}{\lambda}, \frac{\lambda}{\lambda-1}, 1-\lambda)$ nos dan el mismo valor μ y por lo tanto la asociación:

$$\mathbb{K} - \{0, 1\} \to \overline{\mathbb{K}}$$

es 2 a 1.

Análogamente, si $j(E_\lambda) = 2^8$ se tiene que $\lambda = 1$ y por lo tanto sólo podemos obtener los 3 valores siguientes $\mu = -1, 2, 1/2$. □

Definición 3.9. Definimos al conjunto E_{ns} como el conjunto de los puntos no singulares de una curva elíptica.

3.2 La Curva Elíptica; Curva de Género 1

Definición 3.10. Una curva elíptica es un par (E, O), donde E es una curva de genero 1, y $O \in E$. Escribimos $E/\mathbb{K}$ si E es definida sobre $\mathbb{K}$ como curva y $O \in E(\mathbb{K})$.

Proposición 3.11. *Sea E una curva no singular dada por la ecuación de Weiestruss. Entonces el invariante diferencial w de E, es no nulificable y no cero, es decir $div(w) = 0$.*

Demostración. Recordemos que

$$w = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{2y + a_2x + a_3}$$

con $x_0 \in \mathbb{K}$. Entonces sea $P = (x_0, y_0)$ y sea

$$\pi_y : E \to \mathbb{P}^1$$

el mapeo dado por

$$[X, Y, Z] \mapsto [X, Z]$$

Es decir, la proyección desde el punto $P = [0, 1, 0] \in E$. Entonces π_y está bien definido para todo punto $P \in E$, excepto $P = [0, 1, 0]$, y además π_y es un mapeo de grado finito. Debemos también observar que la función x, considerando coordenadas no homogéneas, es equivalente a la función $\frac{X}{Z}$ en coordenadas homogéneas.

Primeramente estimaremos $ord_P(w)$ con $P \neq [0, 1, 0]$. Sea Q el punto $Q = [x_0, 1] \in \mathbb{P}^1$ (notar que ${\pi_y}^{-1}([1, 0]) = [0, 1, 0]$)

Tenemos que $t = \frac{X - x_0 Z}{Z}$ es un parámetro de uniformización en Q. Claramente $\pi_y^*(t) = x - x_0$ considerando coordenadas no homogeneas.

Ahora la cardinalidad de $\pi_y^{-1}(Q)$ está dada por el número de soluciones al polinomio cuadrático $F(x_0, y)$. Y además, por la proposición 2.35, tenemos

$$\sum_{P \in \pi_y^{-1}(Q)} ord_P(x - x_0) = 2$$

de donde $ord_P(x - x_0) = 2$ si y solamente si $F(x_0, Y)$ tiene doble solución, es decir si y sólo si

$$ord_P\left(\frac{\partial F}{\partial y}(x_0, y_0)\right) = 1$$

cumpliéndose por lo tanto, siempre, con $ord_P(x - x_0) = 1$ o 2, la igualdad

$$ord_P(w) = ord_P(x - x_0) - ord_P\left(\frac{\partial F}{\partial y}\right) - 1 = 0$$

Ahora, como x es una función regular, en todo punto de E, excepto en $P = [0, 1, 0]$, y $\deg \sum_{Q \in E - P} ord_Q(x) = 2$ Entonces, $ord_P(x) = -2$, ya que debe cumplirse $\deg \div x = 0$.

Siguiendo un razonamiento similar se puede ver que $ord_P(y) = -3$. Por lo tanto, existen funciones $f, g \in \mathbb{K}(E)$ con $ord_P(f) = ord_P(g) = 0$, tal que $x = t^{-2} f$ y $y = t^{-3} g$, con t parámetro de uniformización en P.

Y de esa manera, sustituyendo x y y por $t^{-2}f$ y $t^{-3}g$ en la ecuación que define a w, tenemos,

$$w = \frac{-2f + t\frac{df}{dt}}{2g + a_1 tf + a_3 t^3} dt$$

de donde como f es regular entonces dt/df es también regular; y por tanto si $char(\mathbb{K}) \neq 2$ se evidencia que $ord_P(w) = 0$. Y si $char(\mathbb{K}) = 2$ trabajando de manera análoga con la ecuación de w en términos de dy se sigue el resultado. □

Proposición 3.12. *Si E es una curva singular dada por la ecuación de Weiestrass entonces existe un mapeo racional*

$$\phi : E \to \mathbb{P}^1$$

de grado 1.

Demostración. Supongamos sin perdida de generalidad que E pasa por el punto $(0,0) \in E$. Entonces, como E es sigular se puede escribir de la forma:

$$E : y^2 + a_1 xy = x^3 + a_2 x^2$$

Entonces el mapeo racional

$$\phi : E \to \mathbb{P}^1 \quad [x, y, z] \mapsto [x, y]$$

tiene grado 1.

Dividiendo la ecuación que define a E por x^2, tenemos que

$$x = \left(\frac{y}{x}\right)^2 + a_1 \frac{y}{x} - a_2$$

y dividiento por y

$$y = \left(\frac{y}{x}\right)^{-1} x^2 + a_3 \left(\frac{y}{x}\right)^{-1} x + a_1 x.$$

Por lo que, como $\mathbb{K}(y/x)$ es el campo de funciones del abierto $U = \mathbb{P} - [0, 1]$, el morfismo de campos

$$\phi : \mathbb{K}\left(\frac{y}{x}\right) \to \mathbb{K}(E)$$

es un isomorfismo.

De donde, E y $\mathbb{P}^1$ son birracionales, y por lo tanto ϕ es un mapeo racional de grado 1. □

Proposición 3.13. *Sea E una curva Elíptica sobre $\mathbb{K}$. Entonces*
a) Existen funciones $x, y \in \mathbb{K}(E)$ de manera que el mapeo

$$\phi : E \to \mathbb{P}^2$$

dado por

$$\phi(P) = [x(P), y(P), 1]$$

da un isomorfismo de $E/\mathbb{K}$ sobre una curva cuya ecuación es

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

donde $a_1, a_2, \ldots, a_6 \in \mathbb{K}$. Y además $\phi(O) = [0, 1, 0]$.
b) Toda variedad no singular dada por una curva elíptica C como arriba es una curva elíptica definida sobre $\mathbb{K}$ y con origen $O = [0, 1, 0]$.

Demostración. Por el teorema de Riemman-Roch $\mathcal{L}(nO)$ tiene dimensión n sobre $\mathbb{K}(E)$.

Así $\mathcal{L}(2O)$ es un espacio de 2 dimensiones, en el que sus elementos se pueden expresar como $\{k + k_1x\}$ donde x es una función con polo doble en O y k,$k_1 \in \mathbb{K}$. Análogamente, se tiene que

$$\mathcal{L}(3O) \cong \mathcal{L}(2O) \oplus \mathcal{L}(3O - P - Q)$$

con $P, Q \in E$ y $P \neq O$ y $Q \neq O$.

Así, si escogemos la función $x \in \mathcal{L}(2O)$ con doble polo en O y una función $y \in \mathcal{L}(3O)$, tal que $y \neq 0$ y $y \notin \mathcal{L}(2O)$. Entonces las 7 funciones $1, x, y, x^2, xy, y^2, x^3$ estan en $\mathcal{L}(6O)$. Pero $\mathcal{L}(6O) = 6$ y por lo tanto, existen coeficientes $A_1, A_2, \ldots, A_7 \in \mathbb{K}$, al menos algunos distintos de cero tales que

$$A_1 + A_2x + A_3y + A_4x^4 + A_5xy + A_6y^2 + A_7x^3 = 0$$

Podemos notar también que $A_7A_6 \neq 0$, pues de no serlo así entonces tendriamos cada término con distinta polaridad y por lo tanto todos los A_j serían cero.

Sustituyendo x,y por $-A_6A_7x$ y $A_6A_7^2y$ y dividiendo entre $A_6^3A_7^4$. Obtenemos una ecuación como la de Weiestrass. Así naturalmente el mapeo buscado es $\phi : E \to C$, con $\phi(P) = [x(P), y(P), 1]$. Así, basta mostrar que $\phi : E \to C$ es un mapeo grado 1, ya que en dicho caso, como E es no singular éste sería un isomorfismo.

Ahora como x tiene un único polo doble en O, entonces el morfismo

$$x : E \to \mathbb{P}^1 \qquad P \to [x(P), 1]$$

es de grado 2.

Esto se sigue de que la imagen inversa del punto $[1, 0]$ (ver ??) es el punto O contando doblemente.

El mapeo $x : E \to \mathbb{P}^1$ se puede ver como la composición $x = \pi_y \circ \phi$ donde $\pi_y : C \to \mathbb{P}^1$ es la proyección desde $P = [0, 1, 0]$, esto es

$$\pi_y : [x, y, z] \to [x, y]$$

y este mapeo es también de grado 2.

Entonces de la igualdad $\deg x = \deg \pi_y \deg \phi$ se sigue que $\deg \phi = 1$.

Pero C no puede ser singular, de serlo, entonces por la proposición anterior, existe un mapeo racional $\psi : C \to \mathbb{P}^1$ de grado 1, y por lo tanto $\psi \circ \phi : E \to \mathbb{P}^1$ es un mapeo de grado 1 entre 2 curvas no singulares y por lo tanto un isomorfismo. (Ver proposición 2.27) Pero eso, no puede ser, ya que estas curvas poseen diferente género.

b) Se sigue por el corolario a *Riemman-Roch* y del hecho que $div(w) = 0$ que el género de C es 1. De esa forma, C junto con el punto $O = [0, 1, 0]$ definen una curva elíptica. □

3.3 La Ley de Grupo para las Curvas Elípticas

Como anticipamos en la introducción a este capítulo, en esta sección introduciremos la Ley de Grupo en 2 formas diferentes:

Para la primera, es muy importante tener en mente el teorema de Bezout sobre las multiplicidades de la intersección de curvas, éste nos dice que la suma de los índices de intersección sobre los puntos de la intersección es igual al grado de las curvas.

Así las cosas, una recta $L \subset \mathbb{P}^n$ intersecta a E en exactamente 3 puntos P,Q,R (que pueden ser iguales, ya que estamos contando multiplicidades). Por ejemplo, la recta $Z = 0$ intersecta a E unicamente en el punto $O = [0, 1, 0]$ con una triple multiplicidad, siendo este un punto de inflección, y en ese sentido, un punto especial que nos posibilitará la construcción de la estructura de grupo en E.

Definición 3.14. Ley de Operación. Sea P,$Q \in E$. Construimos la operación $\oplus : E \to E$ siguiendo el procedimiento:

Trazemos la línea L que pasa por P y Q (si $P = Q$, L será tangente a E), entonces ésta intersecta a E en un tercer punto R. Ahora, conectemos a R y O con otra línea L, entonces sea $P \oplus Q$ el tercer punto de intersección de L con E.

Proposición 3.15. *La Ley de Operación tiene las siguientes propiedades:*
a)Si una línea intersecta a E en los puntos P,Q,R, entonces

$$(P \oplus Q) \oplus R = O$$

b) $P \oplus O = P$ para toda $P \in E$.
c) $P \oplus Q = Q \oplus P$ para todas P,$Q \in E$.
d) Sea $P \in E$, entonces existe un punto en E, denotado por $\ominus P$ tal que:

$$P \oplus (\ominus P) = O$$

e)Sean P,Q,$R \in E$. Entonces

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$$

En otras palabras, la ley de operación definida, provee a la curva elíptica de una extructura de grupo

Demostración. a) Como L pasa por P, Q y R, entonces $P \oplus Q$ es el otro punto de la línea que une R y O, de donde si M une $P \oplus Q$ con R ésta tiene como tercer punto de intersección a O y como O tiene grado 3 entonces su tangente no toca ningún punto en la curva, excepto al punto O y así $(P \oplus Q) \oplus R = O$.

b) Sea L una recta pasando por P y O, entonces intersecta en otro punto R (no necesariamente distinto), ahora como obviamente L une a R con O, se sigue el resultado.

c) Trivial por construcción.

d) Consideremos la línea que une P con O, entonces sea $\ominus P$ el otro punto de intersección con E, entonces naturalmente $P \oplus (\ominus P) = O$

e) Este es el inciso más difícil. Para demostrarlo utilizaremos los divisores de intersección: Escojamos las rectas L_1, M_1 y L_2 tal que

$$L_1 \cdot C = P + Q + \hat{S}$$

$$M_1 \cdot C = O + \hat{S} + S$$

$$L_2 \cdot C = S + R + \hat{T}$$

Análogamente escojamos las rectas M_2, L_3, M_3 tal que

$$M_1 \cdot C = R + Q + \hat{U}$$

$$L_1 \cdot C = O + \hat{U} + U$$

$$M_2 \cdot C = U + P + T$$

Basta demostrar que $T = \hat{T}$. Consideremos las cúbicas $C_1 = L_1L_2L_3$ y $C_2 = M_1M_2M_3$, de donde aplicando el resultado del ejemplo 2.78 tenemos que $T = \hat{T}$. □

A partir de ahora, con el fin de simplificar la notación en lugar de usar los símbolos $\oplus$ y $\ominus$, utilizaremos la notación más agradable $+$ y $-$.

También denotaremos la suma m-veces de un punto P como

$$mP = P + \cdots + P \ (m \text{ veces})$$

Si consideramos fijo $m \in \mathbb{Z}$ entonces definimos de manera natural el mapeo

$$[m] : E \to E \qquad P \mapsto mP$$

Este mapeo jugará un rol muy importante de ahora en adelante, siendo un morfismo de curvas que es también un homomorfismo de grupos (ver siguiente sección). Y de esa forma tendremos una representación

$$[\ ] : \mathbb{Z} \to Aut(E, E) = End(E)$$

Observación 3.16. El grupo $Pic^0(E)$ hereda su estructura a E.

Sean P, $Q \in E$ entonces los divisores $D = (P) - (O)$ y $\bar{D} = (Q) - (O)$, son linealmente equivalentes si y sólo si $P = Q$. Ya que $D \sim \bar{D} \iff$ existe $f \in \mathbb{K}(E)$ con $div\,(F) = (P) - (Q)$

$\iff P = Q$ (por el ejemplo 2.68).

De donde, existe un mapeo bien definido de

$$G : E \to Pic^0(E)$$

e inversamente si $D \in Pic^0(E)$, por el corolario a *Riemman-Roch*,

$$\mathcal{L}(D + (O)) = 1$$

de donde existe $f \in \mathbb{K}(E)$ tal que $div\,(f) \geq -D - (O)$ y como $\deg div\,(f) = 0$ se tiene

$$div\,(f) = D + (O) - (P) \text{ con } P \in E$$

y así se sigue que $D \sim (P) - (O)$, y por ende G es biyectiva.

Ahora, heredándole la estructura de grupo de $Pic^0(E)$ a E, observamos nuevamente que E es una variedad abeliana.

Proposición 3.17. *Si E es dada por una ecuación de Weiestrass, entonces el grupo geométrico en E, coincide con el grupo algebraico $Pic^0(E)$.*

Demostración. Basta ver que

$$G(P + Q) = G(P) + G(Q)$$

donde la suma de la izquierda es la del grupo geométrico y la de la derecha la inducida por $Pic^0(E)$. A continuación una hermosa prueba debida a Silverman: Sea

$$f(X, Y, Z) = aX + bY + cZ = 0$$

la recta que pasa por P, Q y S, y sea

$$g(X, Y, Z) = dX + eY + fZ = 0$$

la recta de S a O.

De esta manera, recordando que la línea $Z = 0$ intersecta a E en O con multiplicidad 3, Silverman obtiene

$$div\left(\frac{f}{z}\right) = (P) + (Q) + (S) - 3(O)$$

y

$$div\left(\frac{g}{z}\right) = (P + Q) + (S) - 2(O)$$

y en consecuencia

$$div\left(\frac{f}{g}\right) = (P + Q) - (Q) - (P) + (O)$$

de donde $G(P + Q) = G(P) + G(Q)$. □

Corolario 3.18. *Sea E una curva elíptica. El divisor $D = \sum_i n_i P_i \in Div(E)$ es principal si y sólo si* $\deg D = 0$ *y* $\sum n_i P_i = O$.

Demostración. Claramente si D es principal, entonces $\deg D = 0$.

Pero D es principal si y sólo si $D \sim O$ y dado que $\deg D = 0$ esto es si y sólo si $\sum_i (n_i P_i - n_i O) \sim O$ pero esto por definición de la suma en la curva elíptica, unicamente y necesariamente ocurre si $\sum n_i P_i = O$. □

3.4 Isogenias

Ya hemos estudiado de manera individual las curvas elípticas, ahora estamos interesados en estudiar los mapeos entre ellas.

Definición 3.19. Sean E_1 y E_2 curvas elípticas. Una isogenia entre E_1 y E_2 es un morfismo

$$\phi : E_1 \to E_2$$

que satisface que $\phi(O) = O$.

Decimos que E_1 son isogeniamente equivalentes si exite una isogenia entre ellas tal que $\phi(E_1) = E_2$.

Observación 3.20. Dada una isogenia $\phi : E_1 \to E_2$ entonces ésta cumple con $\phi(E_1) = \{O\}$ o con $\phi(E_1) = E_2$. De esta manera tenemos que $\phi \neq 0$ es un mapeo finito de curvas, y por lo tanto podemos hablar de grados separables e inseparables de ϕ.

Nota 3.21. Se puede demostrar que los mapeos $\ominus : E \to E$ dado por $P \mapsto -P$ y $\oplus : E \times E \to E$ son morfismos [Sil85, teo 3.6].

De aquí se sigue, que el conjunto de isogenias $\phi : E_1 \to E_2$, tienen extructura de grupo con la ley de operación:

$$(\phi + \psi)(P) = \phi(P) + \psi(P)$$

y estructura de anillo con la composición.

Definición 3.22. Denotamos por $Hom(E_1, E_2)$ al conjunto de homorfismos del grupo de E_1 a el grupo E_2.

Observación 3.23. Entonces todo elemento perteneciente al $Hom(E_1, E_2)$ es una isogenia, pues E_1 es no singular y entonces si $\phi \neq 0$ tenemos que ϕ es suprayectiva y es un morfismo 2.27.

Si $\phi = 0$ entonces se tiene trivialmente que ϕ es morfismo.

Ejemplo 3.24. El homomorfismo $[m] : E \to E$ define una isogenea.

Proposición 3.25. *a) Sea $E/\mathbb{K}$ una curva elíptica y sea $m \in \mathbb{Z}$, $m \neq 0$. Entonces el mapeo de multiplicación*

$$[m] : E \to E$$

es no constante.

b) Sean E_1 y E_2 dos curvas elípticas. Entonces el grupo

$$Hom(E_1, E_1)$$

es un $\mathbb{Z}$-módulo libre de torsión.

Demostración. a) Ver [Sil85, pag 72] o corolario 3.36.

b) Sigue inmediatamente de a) si consideramos que $[m] \circ \phi = 0$ si y sólo si $m = 0$ o $\phi = 0$. □

Definición 3.26. El m-subgrupo de torsión de E es el subgrupo

$$E[m] = \ker [m]$$

Y el grupo de torsión es el conjunto de puntos de orden finito

$$E_{tors} = \cup_{m=1}^{\infty} E[m]$$

Observación 3.27. Dado que por la proposición anterior $[m] \neq 0$ entonces el grupo $E[m]$ es finito 3.25. Aún más demostraremos (siguiente capítulo) que este grupo posee exactamente m^2 elementos.

Definición 3.28. La traslación τ_Q : es el isomorfismo dado por

$$\tau_Q : E \to E$$

$$P \to P + Q$$

Claramente tenemos que $\tau_Q \circ \tau_{-Q}$.

Teorema 3.29. El isomorfismo siguiente es cierto

$$Hom(E_1, E_2) \cong \{\text{isogenias } \phi : E_1 \to E_2 \}$$

Ya vimos, que todo homomorfismo $\phi \in Hom(E_1, E_2)$ nos define una isogenia (observación 3.23), basta por tanto, demostrar que dada una isogenia $\phi : E_1 \to E_2$ se tiene que

$$\phi(P + Q) = \phi(P) + \phi(Q) \text{ para todos } P,Q \in E$$

Si $\phi(P) = O$ para todo $P \in E_1$ no hay nada que probar, de otra manera, si $\phi \neq O$ induce un homomorfismo

$$\phi_* : Pic^0(E_1) \to Pic^0(E_2)$$

dado por

$$\sum n_i(P_i) \to \sum n_i(\phi(P_i))$$

de donde, utilizando el siguiente diagrama conmutativo

con los isomorfismos $E_i \cong Pic^0(E_i)$ dados en la contrucción de la estructura de grupo en E_i, se sigue que ϕ es composición de morfismos y por tanto es morfismo.

Corolario 3.30. *Si* $\phi : E_1 \to E_2$ *entonces* $\ker \phi = \phi^{-1}(O)$ *es un subgrupo finito.*

Demostración. Por el teorema anterior es subgrupo. De donde se sigue la proposición. □

Nota 3.31. Conversamente, se puede demostrar que si G es un subgrupo finito de E_1 entonces existe una curva E_2 y una isogenia $\phi : E_1 \to E_2$ tal que

$$G \cong \ker \phi.$$

Teorema 3.32. Sea $\phi : E_1 \to E_2$ una isogenia no constante.

a) Para $Q \in E_2$,

$$\sharp\phi^{-1}(Q) = deg_s \phi$$

y además, para todo $P \in \phi^{-1}(Q)$,

$$e_\phi(P) = deg_i(\phi).$$

b) El mapeo

$$\ker \phi \to Aut\left[\overline{\mathbb{K}}(E_1)/\phi^*\overline{\mathbb{K}}(E_2)\right]$$

$$T \to \tau_T^*$$

es un isomorfismo, donde τ_T es la traslación por T y τ_T^* es un automorfismo inducido sobre $\overline{\mathbb{K}}(E_2)$.

c) Asumiendo que ϕ es separable. Entonces ϕ es no ramificado,

$$\sharp \ker \phi = \deg_s \phi$$

y $\overline{\mathbb{K}}(E_1)$ es una extensión de Galois sobre $\phi^*(E)$.

Demostración. Ver [Sil85, 4.10]. □

Corolario 3.33. *Sean*

$$\phi : E_1 \to E_2 \ , \ \psi : E_1 \to E_3$$

dos isogenias no constantes, donde asumimos que ϕ es separable. Entonces si

$$\ker \phi \subset \ker \psi,$$

exite una isogenia

$$\lambda : E_2 \to E_3$$

tal que $\psi = \lambda \circ \phi$.

Demostración. Por el teorema 3.32 como ϕ es separable, entonces $\phi^*\overline{\mathbb{K}}(E_1)$ es una extensión de Galois, i.e.

$$Aut(\overline{\mathbb{K}}(E_2)/\phi^*\overline{\mathbb{K}}(E_1)) = [\overline{\mathbb{K}}(E_2) : \phi^*\overline{\mathbb{K}}(E_1)]$$

Entonces la inclusión $\ker \phi \subset \ker \psi$ implica que el grupo de Galois $Aut(\overline{\mathbb{K}}(E_2)/\phi^*\overline{\mathbb{K}}(E_1))$ fija al subcampo $\psi^*\overline{\mathbb{K}}(E_1)$. Así tenemos las siguientes inclusiones de campos

$$\psi^*\overline{\mathbb{K}}(E_1) \subset \phi^*\overline{\mathbb{K}}(E_1) \subset \overline{\mathbb{K}}(E_2)$$

de donde por la proposición 2.31, existe un mapeo

$$\lambda : E_2 \to E_3$$

satisfaciendo naturalmente la igualdad

$$\phi^*(\lambda^* \mathbb{K}(E_3)) = \psi^* \mathbb{K}(E_3)$$

lo que implica que $\psi = \lambda \circ \phi$. Y el resultado se sigue de observar que λ es isogenia

$$\lambda(O) = \lambda(\phi(O)) = \psi(O).$$

□

3.5 El Invariante Diferencial

En la primera sección definimos al invariante diferencial w de una curva elíptica y más adelante en la sección 2 demostramos que $div(w) = 0$, siendo este resultado de gran utilidad para ver que las Curvas Elíptica definidas por la ecuación de Weiestrass son curvas de género 1. Esto nos posibilitó una construcción más algebraica de la estructura de Grupo en estas curvas. En este capítulo presentaremos resultados importantes acerca del invariante w que nos ayudarán a profundizar nuestro estudio de estas curvas y los mapeos entre ellas, en concreto, el corolario 3.37 muestra que el mapeo $(1 - \phi)$ es separable, ésto nos será muy útil para evaluar el número de puntos de los conjuntos $E(\mathbb{K}_n)$. Con $\mathbb{K}$ un campo finito. Y por tanto para demostrar la conjetura de Weil en el caso de curvas elípticas.

Teorema 3.34. Sean E y $\bar{E}$ dos curvas elípticas, sea w el invariante diferencial de E y

$$\phi, \psi : E \to \bar{E}$$

dos isogeneas. Entonces

$$(\phi + \psi)^* w = \phi^* w + \psi^* w$$

donde los mapeos ϕ^* y ψ^* están definidos después del comentario 2.47.

(Naturalmente el signo + en el lado derecho representa la suma en el grupo $Hom(E, \bar{E})$, mientras que en el lado izquierdo representa la suma en el espacio vectorial Ω_E.)

Una prueba de este teorema se puede encontrar en Silverman [Sil85, III.5.2]. Nosotros estamos interesados en las siguientes notables consecuencias.

Corolario 3.35. *Sea w el invariante diferencial de una curva elíptica E. Sea $m \in \mathbb{Z}$. Entonces*

$$[m]^* w = mw.$$

Demostración. Es claro que para $m = 0$ y $m = 1$ que el corolario se cumple. Entonces por inducción y usando el teorema tenemos:

$$[m+1]^* w = [m]^* w + [1]^* w = (m+1)w$$

□

Corolario 3.36. *Sea $E/\mathbb{K}$ una curva elíptica, $m \in \mathbb{Z}$, con $m \neq 0$. Asumiendo que $char(\mathbb{K}) = 0$ o $(char(\mathbb{K}), m) = 1$ tenemos que $[m]$ es un mapeo finito y un endomorfismo separable.*

Demostración. Sea w el invariante diferencial de E. Entonces $[m]^* w = mw \neq 0$. De aquí que $[m] \neq [0]$. De donde $[m]$ es sobre y por lo tanto es finito y $[m]^*$ es inyectivo por lo que se sigue de la proposición 2.57 que $[m]$ es separable. □

Corolario 3.37. *Sea $char(\mathbb{K}) = p > 0$, E una curva elíptica sobre $\mathbb{F}_q$, y $\phi : E \to E$ el q^{th}-mapeo de Frobenius. Sean $m,n \in \mathbb{Z}$, entonces el mapeo*

$$m + n\phi : E \to E$$

es separable si y sólo si $(p, m) = 1$. En particular el mapeo $(1 - \phi)$ es separable.

Demostración. Sea w el invariante diferencial de E. Vimos en 2.57 que un mapeo ψ es inseparable si y sólo si $\psi^* w = 0$. De donde como el mapeo de Frobenius ϕ es inseparable obtenemos

$$(m + n\phi)^* w = mw + n\phi^* w = mw$$

y por lo tanto si $(p, m) = 1$ tenemos que $(m + n\phi)^* \neq 0$. □

3.6 La Isogenia Dual

Si consideramos $\phi : E_1 \to E_2$ una isogenia. Hemos visto que esta isogenia nos induce un homomorfismo

$$\phi^* : Pic^0(E_2) \to Pic^0(E_2)$$

Entonces aprovechando los isomorfismos de grupo $E_2 \cong Pic^0(E_2)$ y $E_1 \cong Pic^0(E_1)$ esto nos induce una isogenia

$$\widehat{\phi} : E_2 \to E_1$$

Definición 3.38. A la isogenia $\widehat{\phi}$ la llamaremos la isogenia dual de ϕ.

El siguiente teorema, nos muestra una relación intrínseca entre las isogenias ϕ y $\widehat{\phi}$ y el grado $\deg \phi$.

Teorema 3.39. Sea $\phi : E_1 \to E_2$ una isogenia no constante de grado m.

a) Entonces existe una isogenia única

$$\widehat{\phi} : E_2 \to E_1$$

que satisface $\widehat{\phi} \circ \phi = [m]$.

b) Como grupo de homomorfismos, $\widehat{\phi}$ es igual a la composición

$$E_2 \to Div^0(E_2) \xrightarrow{\phi^*} Div^0(E_1) \xrightarrow{sum} E_1$$

$$Q \mapsto (Q) - (O) \qquad \sum n_P(P) \mapsto \sum [n_P]P$$

Demostración. En el inciso a) la unicidad de ϕ se sigue facilmente de la existencia. Por lo tanto, para demostrar a) y b) basta ver que el inciso b) con la isogenia dual $\widehat{\phi}$ definida arriba cumple que

$$\widehat{\phi} \circ \phi = [\deg \phi] = [m].$$

Observe que si $\phi \neq 0$ entonces para todo $Q \in E$ se tiene que $\phi^{-1}(Q) \neq \emptyset$. Así usando el teorema 3.32

$$\begin{aligned}\widehat{\phi}(Q) &= sum(\phi^*(Q-O)) \\ &= sum\left(\sum_{P\in\phi^{-1}(Q)} e_\phi(P)(P) - \sum_{S\in\ker\phi} e_\phi(S)(S)\right) \\ &= \sum_{P\in\phi^{-1}(Q)} [e_\phi(P)(P)](P) - \sum_{S\in\ker\phi} [e_\phi(S)](S)\end{aligned}$$

Pero como dado cualquier $P \in \phi^{-1}(Q)$ se tiene la igualdad de conjuntos

$$\{P+T : T \in \ker\phi\} = \phi^{-1}(Q)$$

entonces

$$\begin{aligned}\widehat{\phi}(Q) &= \sum_{T\in Ker\phi} (e_\phi(T+P) - e_\phi(T)(T)) \\ &= [\deg_i \phi]\left(\sum_{P\in Ker\phi} (T+P) - (P)\right) \\ &= [\deg_i \phi] \circ [\deg_s \phi](P) \\ &= [\deg \phi](P)\end{aligned}$$

Pero como $P \in \phi^{-1}(Q)$ entonces se ha mostrado que

$$\widehat{\phi} \circ \phi(P) = \widehat{\phi}(Q) = [m](P)$$

□

Teorema 3.40. Sea $\phi : E_1 \to E_2$ una isogenea.

a) Si $m = \deg\phi$ entonces

$$\widehat{\phi} \circ \phi = [m] \qquad \text{sobre } E_1$$

$$\phi \circ \widehat{\phi} = [m] \qquad \text{sobre } E_2$$

b) Sea $\lambda : E_2 \to E_3$ otra isogenea. Entonces

$$\widehat{\lambda \circ \phi} = \widehat{\phi} \circ \widehat{\lambda}$$

c) Sea $\lambda : E_2 \to E_3$ otra isogenea. Entonces

$$\widehat{\lambda + \phi} = \widehat{\lambda} + \widehat{\phi}$$

d) Para toda $m \in \mathbb{Z}$

$$\widehat{[m]} = [m] \text{ y } \deg [m] = m^2$$

e) $\deg \widehat{\phi} = \deg \phi$

f) $\widehat{\widehat{\phi}} = \phi$

Demostración. a) Ya sabemos por 3.39 que $\widehat{\phi} \circ \phi = [m]$. Ahora considerando la composición

$$\phi \circ \widehat{\phi} \circ \phi = \phi \circ [m] = [m] \circ \phi$$

De donde como ϕ es sobreyectiva por la proposición 2.27 se sigue a).

b) Sean $\deg \phi = m$ y $\deg \lambda = n$.

Componiendo nuevamente se tiene

$$\widehat{\phi} \circ \widehat{\lambda} \circ \lambda \circ \phi = \widehat{\phi} \circ [n]\phi = [n] \circ \widehat{\phi} \circ \phi = [nm]$$

y utilizando la unicidad de la isogenia se ve la afirmación.

c) Ver Silverman [Sil85, III.6.2].

d) El resultado es evidente para $m = 0$ y $m = 1$. Entonces por inducción y utilizando el inciso c)

$$\widehat{[m+1]} = \widehat{[m] + [1]} = \widehat{[m]} + \widehat{[1]} = [m+1]$$

el resultado es evidente para toda $m \in \mathbb{Z}$.

e) Por el inciso de arriba y mirando que

$$[m^2] = [\deg \widehat{\phi} \circ \phi] = [\deg \phi \ \deg \widehat{\phi}] = [\deg \widehat{\phi}] \circ [m]$$

el resultado se evidencía. □

4 Conjeturas de Weil

4.1 Preparando la demostración

Consideremos $\mathbb{K}$ un campo finito con q elementos y pensemos en $\overline{\mathbb{K}}$ su cerradura algebraica. Entonces si V es una variedad definida por los polinomios $f_1, f_2, \ldots, f_n$ con coeficientes en $\mathbb{K}$, la entenderemos naturalmente como una variedad encajada en $\mathbb{P}^N_{\overline{\mathbb{K}}}$ esto es, los puntos de la variedad con coordenadas homogéneas en $\overline{\mathbb{K}}$. Por otro lado, sea $V(\mathbb{K}_n)$ el conjunto de puntos de V con cordenadas en $\mathbb{K}_n$, llamados los puntos racionales de V respecto a $\mathbb{K}_n$, la extensión de grado n de $\mathbb{K}$. Resulta interesante tener en mente la idea geométrica de que los conjuntos $V(\mathbb{K}_n)$ nos van "llenando" la curva $V \subset \mathbb{P}^N_{\overline{\mathbb{K}}}$, de tal manera que resulta interesante preguntarse hasta que punto la sucesión de conjuntos $V(\mathbb{K}_n)$ llena a V. Siguiendo esta idea podemos definir una función, que llamaremos *zeta*, que nos conserve este tipo de información.

Definimos la función *zeta* como la siguente serie de potencias:

$$Z(V/\mathbb{K}, T) = \exp(\sum_{n=1}^{\infty} \sharp V(\mathbb{K}_n) T^n/n)$$

esta función tiene sentido como serie, dado que cada término $\sharp V(\mathbb{K}_n)$ es finito debido a la finitud de $\mathbb{K}_n$ y además se pueden definir las funciones $\exp x$ y $\log x$ como series formales. Por otro lado, aplicando $\log x$ a la funcion $Z(V/\mathbb{K}, T)$, podemos recuperar los valores $\sharp V(\mathbb{K}_n)$ derivando las veces que sea necesario y multiplicando por el término

$$\frac{1}{(n-1)!}.$$

Ahora ya definida la funcion $Z(V/\mathbb{K}, T)$ estamos en condiciones de formular las conjeturas de Weil para esta función, la cual cumplirá con las 3 propiedades siguientes: racionalidad, de la ecuación funcional y la Hipótesis de Riemann. Las conjeturas de Weil quedaron estableciadas así:

Conjetura 4.1. *(Conjeturas de Weil). Sea $\mathbb{K}$ un campo finito con q elementos y $V/\mathbb{K}$ una variedad proyectiva de dimensión n. Entonces se cumple:*
a) La Racionalidad.

$$Z(V/\mathbb{K}, T) \in \mathbb{Q}(T)$$

b) La Ecuación Funcional. Existe un entero ε (La característica de Euler) tal que:

$$Z(V/\mathbb{K}, 1/q^n T) = \pm q^{n\varepsilon/2} T^{\varepsilon} Z(V/\mathbb{K}, T)$$

c) La Hipótesis de Riemann. Existe una factorización

$$Z(V/\mathbb{K}, T) = \frac{P_1(T) \dots P_{2n-1}(T)}{P_0(T) P_2(T) \dots P_{2n}(T)}$$

con cada $P_i(T) \in \mathbb{Z}[T]$. Además $P_0(T) = 1 - T$, $P_{2n}(T) = 1 - q^n T$, y para cada $1 \leq i \leq 2n-1$, $P_i(T)$ se factoriza sobre $\mathbb{C}$ como:

$$P_i(T) = \prod_j (1 - \alpha_{ij} T)$$

con $|\alpha_{ij}| = q^{i/2}$.

Observación 4.2. Es natural preguntarse por qué definir a la función $Z(V/\mathbb{K}, T)$ como se definió y no de una manera más simple, como por ejemplo la serie $\sum_{n=1}^{\infty} \sharp V(\mathbb{K}_n) T^n/n$. La respuesta está dada un poco por lo que nos gustaría demostrar; es decir, las propiedades de la función *zeta* que nos gustaría que tuvieran validez. La idea intuitiva, para elegir $Z(V/\mathbb{K}, T)$, es la siguiente: la serie $\sum_{n=1}^{\infty} \sharp V(\mathbb{K}_n) T^n/n$ es muy parecida a la serie $\log T$ lo que las diferencía son los coeficientes. Esta diferencia podría ser bastante para tener 2 funciones profundamente distintas. Sin embargo, no es tampoco tan desatinada la siguiente pregunta:

Podemos expresar a la serie $\sum_{n=1}^{\infty} \sharp V(\mathbb{K}_n) T^n/n$ en terminos de $\log Q(T)$, donde $Q(T)$ sea una función amable: esto es, una función racional, que cumpla con la Hipótesis de Riemman, etc? .

Si esto ultimo fuera posible entonces tendríamos un equivalente de la conjetura de Weil y si quisieramos que la función *zeta* fuera racional, etc, bastaría con aplicar una exp a la serie $\log Q(T)$. Como en efecto se hizo cuando se definió $Z(V/\mathbb{K}, T)$.

Para ilustrar estas consideraciones calculemos $Z(\mathbb{P}^N_{\mathbb{K}}/\mathbb{K}, T)$. Dado que $\mathbb{K}$ tiene q elementos entonces cada extensión $\mathbb{K}_n$ tiene q^n elementos entonces si N es la dimensión del espacio proyectivo tenemos que el numero de coordenadas homogéneas sobre el campo $\mathbb{K}_n$ es $q^{n(N+1)} - 1$. Además estas coordenadas

están agrupadas en clases de equivalencias con $q^n - 1$ elementos, de esta manera sabemos que

$$\sharp V(\mathbb{P}^N_{Kn}) = \frac{q^{n(N+1)} - 1}{q^n - 1} = \sum_{i=1}^{N} q^{ni}$$

de donde

$$\begin{aligned} \log Z(\mathbb{P}^N_{\overline{\mathbb{K}}}/\mathbb{K}, T) &= \sum_{n=1}^{\infty} \left(\sum_{i=1}^{N} q^{ni} \right) \\ &= \sum_{i=0}^{N} -\log(1 - q^i T) \end{aligned}$$

Con lo que finalmente se obtiene que

$$Z(\mathbb{P}^N_{\overline{\mathbb{K}}}/\mathbb{K}, T) = \frac{1}{(1-T)(1-qT)\dots(1-q^iT)}$$

que es una función racional con coeficientes enteros y que se puede verificar facilmente que cumple con las conjeturas de Weil.

4.2 El Módulo de Tate

Recordemos que definimos el grupo $E[m]$ como el kernel del mapeo $[m]$. Sabemos también que $\deg[m] = m^2$, estos resultados nos dan la posibilidad de describir explícitamente los subgrupos $E[m]$ cuando tenemos que la $char(\mathbb{K}) = 0$ o bien que es primo con respecto a m. En ese caso hemos mostrado en 3.36 que el mapeo $[m]$ es separable y por lo tanto por la proposición 3.32 $\sharp E[m] = m^2$, de donde considerando que $E[m]$ es un grupo abeliano, vemos que

$$E[m] \cong \left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right) \times \left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right).$$

Comentario 4.3. Si $char(\mathbb{K}) = p$ entonces tenemos 2 posibilidades para los módulos $E[p^e]$:

$$E[p^e] = \frac{\mathbb{Z}}{p^e\mathbb{Z}}$$

o bien

$$E[p^e] = 0$$

Esto se desprende utilizando la p^{th} potencia del mapeo ϕ de Frobenius, siendo este mapeo una isogenia grado p; así dividiendo el mapeo $[p]$ tenemos que $[p] = \phi \circ \widehat{\phi}$ de donde

$$\sharp E[p^e] = \deg_s [p^e] \tag{1}$$

$$= (\deg_s \phi \circ \widehat{\phi})^e \tag{2}$$

y como el ϕ es inseparable entonces:

$$\sharp E[p^e] = (\deg_s \widehat{\phi})^e$$

Pero sabemos que $\deg \widehat{\phi} = \deg \phi = p$, y por lo tanto $\deg_s \widehat{\phi} = p$ si $\widehat{\phi}$ es separable o $\deg_s \widehat{\phi} = 1$ si $\widehat{\phi}$ es insepable; de donde se deduce ya facilmente que $E[p^e]$ sólo puede tener las 2 formas mencionadas.

Comentario 4.4. Existe una representación natural del grupo de Galois $G_{\frac{\mathbb{K}}{\mathbb{K}}}$ (el grupo de los automorfismos de $\overline{\mathbb{K}}$ que dejan fijo al campo $\mathbb{K}$) en los automorfismos de $E[m]$. Dado ψ un automorfismo en $G_{\frac{\mathbb{K}}{\mathbb{K}}}$ y P un punto en $E[m]$ entonces el punto $\psi(P)$ se encuentra también en $E[m]$, pues $[m] \circ \psi(P) = \psi \circ [m](P) = 0$. Pero realmente la representación

$$G_{\frac{\mathbb{K}}{\mathbb{K}}} \to Aut(E[m]) \cong GL_2(\frac{\mathbb{Z}}{m\mathbb{Z}})$$

con m fija no será del todo util para estudiar y obtener conclusiones en nuestro analisis de la función *zeta*, lo mejor será la unión de estas representaciones respecto a un primo fijo ℓ.

De esta forma, utilizando una idea análoga a la de la construcción de los números $\mathbb{Z}_\ell$ como la completación de $\mathbb{Z}$ con respecto al ideal $\ell\mathbb{Z}$ nos construye el módulo de Tate.

Definición 4.5. Sea E una curva elíptica y $\ell \in \mathbb{Z}$ un primo. El (ℓ-ádico) módulo de Tate en E es el grupo

$$T_\ell(E) = \lim_{\leftarrow n} E[\ell^n]$$

tomando el límite inverso con respecto a los mapeos naturales $[\ell]$

$$E[\ell^{n+1}] \xrightarrow{[\ell]} E[\ell^n]$$

Como cada módulo $E[\ell^n]$ es un $\mathbb{Z}/\ell\mathbb{Z}$ módulo, se ve facilmente que el módulo de Tate tiene una estructura de $\mathbb{Z}_\ell$-módulo, ya que los número $\mathbb{Z}_\ell$ actúan de manera natural en cada término $E[\ell^n]$. Se puede apreciar también que el módulo $T_\ell(E)$ respeta la tópologia ℓ-ádica.

Ejemplo 4.6. Análogamente a como se construye el módulo de Tate para una curva elíptica, podemos construir el módulo de Tate para un campo $\mathbb{K}$. Consideremos a μ_{ℓ^n} el conjunto de las ℓ^n raíces de la unidad en $\mathbb{K}$, entonces tomemos el límite inverso del mapeo:

$$\ell : \mu_{\ell^{n+1}} \to \mu_{\ell^n}$$

el grupo de Galois $G_{\frac{\mathbb{K}}{\mathbb{K}}}$ actua sobre cada grupo μ_{ℓ^n} dado que $y^m(x^m - 1) + (y^m - 1) = 0$. De donde se obtiene la representación

$$G_{\frac{\mathbb{K}}{\mathbb{K}}} \to T_\ell(\mu) \cong \mathbb{Z}_\ell$$

siendo la ultima parte de la expresión un isomorfismo de grupos.

Ejemplo 4.7. Para ilustrar el ejemplo anterior consideremos el campo $\mathbb{C}$, entonces el conjunto de raíces m-esimas de la unidad lo podemos pintar como un círculo unitario en el plano, de esa manera, los conjuntos μ_{ℓ^n} son grupos de ℓ^n puntos sobre el círculo unitario. Al ir aumentando el valor de n vamos llenando el círculo de puntos, y de esa manera vemos que al obtener el límite de Tate guardamos la información de muchisimos puntos del circulo unitario, que finalmente nos cubren de manera densa el conjunto de unidades de $\mathbb{C}$.

Tener presente este ejemplo es de gran utilidad para guiar nuestra intuición en nuestro estudio de curvas elípticas, en cierta forma al obtener el módulo de Tate estamos llenando nuestra curva de puntos. En las siguientes secciones veremos cómo este módulo de Tate se convertirá en la herramienta más importante para construir nuestra demostración de las conjeturas de Weil.

Proposición 4.8. *El módulo de Tate tiene la siguiente estructura.*

1) Si $\ell \neq char(\mathbb{K})$ entonces $T_\ell(E) = \mathbb{Z}_\ell \times \mathbb{Z}_\ell$.

2) Si $p = char(\mathbb{K})$ entonces $T_p(E) = 0$ o bien $T_p(E) = \mathbb{Z}_p$.

Demostración. Siguen inmediatamente de la construcción de Tate y de las consideraciones iniciales en la sección incluyento el comentario 4.3. □

Sea ϕ un homomorfismo de la curva elíptica E_1 en la curva E_2, entonces ϕ restringido a los conjuntos $E[m]$, con m entero, nos produce un homomorfismo de grupos de $E_1[m]$ en $E_2[m]$. Lo cual nos induce de manera natural un homomorfismo de modulos

$$\phi_\ell : T_\ell(E_1) \to T_\ell(E_2)$$

donde el morfismo ϕ_ℓ actúa coordenada a coordenada, como el mapeo ϕ.

Esta observación nos sugiere el siguiente mapeo

$$Hom(E_1, E_2) \to Hom(T_\ell(E_1), T_\ell(E_2))$$

dado por $\phi \to \phi_\ell$, que en realidad, es un homomorfismo de anillos, ya que ϕ_ℓ es $\mathbb{Z}_\ell$-lineal.

En el caso de que $E_1 = E_2 = E$, entonces ϕ_ℓ se convierte en un endomorfismo de $T_\ell(E)$ y con el cual obtenemos el homomorfismo de anillos

$$End(E) \to End(T_\ell(E))$$

dado por

$$\phi \to \phi_\ell$$

4.3 El Apareo de Weil

Antes de construir el mapeo, hagamos algunas observaciones sobre la forma en que el grupo de Galois $G_{\frac{\mathbb{K}}{\mathbb{K}}}$, actúa sobre los espacios afines y proyectivos, los espacios de polinomios y de funciones y finalmente sobre variedades. Estas observaciones nos serán útiles para demostrar que el Apareo de Weil es compatible con la acción del grupo $G_{\frac{\mathbb{K}}{\mathbb{K}}}$.

Definición 4.9. El grupo de Galois $G_{\frac{\mathbb{K}}{\mathbb{K}}}$ actúa sobre un punto $P = (x_1, x_2, \ldots, x_n) \in \mathbb{A}^n$, coordenada a coordenada, esto es

$$P^\sigma = (x_1^\sigma, x_2^\sigma, \ldots, x_n^\sigma)$$

para $\sigma \in G_{\frac{\mathbb{K}}{\mathbb{k}}}$.

Es claro de esta definición, que los puntos $\mathbb{A}^n(\mathbb{K})$ son justamente los puntos fijos bajo la acción de $G_{\frac{\mathbb{K}}{\mathbb{k}}}$. O dicho de otra forma

$$\mathbb{A}^n(\mathbb{K}) = \{P \in \mathbb{A}^n : P = P^\sigma, \ \ \sigma \in G_{\frac{\mathbb{K}}{\mathbb{k}}}\}$$

Resulta inmediato que para cualquier variedad $V \subset \mathbb{A}^n$, se cumple

$$V(\mathbb{K}) = \{P \in V : P = P^\sigma, \ \ \sigma \in G_{\frac{\mathbb{K}}{\mathbb{k}}}\}$$

Una observación menos trivial es el hecho de que si $f \in \mathbb{K}[X]$, entonces $(f(P))^\sigma = f(P^\sigma)$. Más en general para $f \in \overline{\mathbb{K}}[X]$ se cumple naturalmente que $f(P)^\sigma = f^\sigma(P^\sigma)$, donde entendemos la aplicación $\sigma : \overline{\mathbb{K}}[X] \to \overline{\mathbb{K}}[X]$, como la acción de σ en los coeficientes de f.

Observación 4.10. Si V es una variedad definida sobre $\mathbb{K}$, esto es que sea cero de polinomios en $\mathbb{K}[X]$. El mapeo σ definido sobre $\mathbb{K}[X]$, como en la observación anterior, mapea al ideal $I(V)$ en sí mismo, ya que todo $f \in I(V)$ se escribe como $f = gh$ donde g tiene todos sus coeficientes en $\mathbb{K}$ y además $g \in I(V)$, y por lo tanto se da la igualdad $f^\sigma = g^\sigma h^\sigma = g(h^\sigma)$.

De esta observación se desprende que el grupo de Galois, actúa de manera natural sobre el anillo de coordenadas de una variedad definida sobre $\mathbb{K}$, y por lo tanto actúa sobre las funciones racionales de la curva, definiendo

$$\left(\frac{f}{g}\right)^\sigma = \frac{f^\sigma}{g^\sigma} \ ,$$

Una vez tomadas en cuenta estas observaciones construyamos el aparco de Weil para curvas elípticas.

Sea $T \in E[m]$ un punto en la curva elíptica, por el corolario 3.18 existe $f \in \mathbb{K}[X]$, tal que

$$div\,(f) = m(T) - m(O)$$

entonces si T' es otro punto tal que $[m](T') = T$ es claro por el mismo corolario que también existe una función g tal que

$$div\,(g) = [m]^*(T) - [m]^*(0) = \sum_{R \in E[m]} (R+T) - (R)$$

Naturalmente se observa que $div\,(g^m) = div\,(f \circ [m])$, de donde multiplicando adecuadamente por $\lambda \in \mathbb{K}^*$ podemos considerar $g^m = f \circ [m]$.

Ahora, sea S otro punto en $E[m]$, puede ser $S = T$, y sea $X \in E$ otro punto, entonces se tiene que

$$g^m(X+S) = f([m](X) + [m](s)) = f([m](X) + (0)) = f([m](X)) = g^m(X)$$

De donde se define el mapeo de Weil

$$e_m(S,T) : E[m] \times E[m] \to \mu_m$$

como

$$e_m(S,T) = \frac{g(X+S)}{g(X)}$$

donde X es cualquier punto sobre E, y μ_m el conjunto de las m-raíces de la unidad en $\overline{\mathbb{K}}$.

Teorema 4.11. El e_m-aparco de Weil es

a) Bilinear:

$$e_m(S_1 + S_2, T) = e_m(S_1, T)e_m(S_2, T) \tag{3}$$
$$e_m(S, T_1 + T_2) = e_m(S, T_1)e_m(S, T_2) \tag{4}$$

b) Alternante:

$$e_m(S,T) = (e_m(T,S))^{-1}$$

c) No degenerado: Si $e_m(S,T) = 1$ para toda $S \in E[m]$, entonces $T = 0$.

d) Compatible con los mapeos [m]:

$$e_{mm'}(S,T) = e_m([m']S, T)$$

e) Galois invariante:

$$e_m(S,T)^\sigma = e_m(S^\sigma, T^\sigma)$$

Demostración. a) La linealidad en el primer término es una fácil consecuencia de que la construcción de $e_m(S,T)$ no depende de la elección del punto X en E, así tenemos que

$$\begin{aligned} e_m(S_1S_2,T) &= \frac{g(X+S_1+S_2)}{g(x)} \\ &= \frac{g(X+S_1+S_2)g(X+S_1)}{g(X+S_1)g(X)} \\ &= e_m(S_1,T)e_m(S_2,T) \end{aligned}$$

La linearidad en el segundo es más complicada.

Sea h una función tal que:

$$div\,(h) = (T_1+T_2) - (T_1) - (T_2) + (0) \quad ,$$

y sean f_1,f_2 y f_3 las funciones *efes* definidas como en la construcción del Apareo de Weil, para los puntos T_1, T_2 y T_1+T_2 respectivamente, entonces las funciones f_3/f_1f_2 y h^m tienen el mismo divisor.

Similarmente, si g_1,g_2 y g_3 son las funciones *ges* para los puntos T_1, T_2 y T_1+T_2 vemos que la función $g_3^m = f_3 \circ [m]$, tiene el divisor asociado

$$\sum_{R\in E[m]} m(R+T_1'+T_2') - m(R)$$

con $[m]T_1' = T_1$ y $[m]T_2' = T_2$.

Calculando el divisor de $h^m \circ [m]$ obtenemos

$$\sum_{R\in E[m]} m(R+T_1'+T_2') - m(R+T_1') - m(R+T_2') + m(R))$$

de donde sumandole los divisores de $div\,(g_1^m)$ y $div\,(g_2^m)$, y sacando raíz m-ésima, al producto $g_1^mg_2^mh^m\circ[m]$, obtenemos que $div\,(g_3) = div\,(g_1g_2(h\circ[m]))$, de donde se sigue que

$$\frac{g_3(X+S)}{g_3(X)} = \frac{g_1(X+S)g_2(X+S)h([m]X+[m]S)}{g_1(X)g_2(X)h([m]X)} = e_m(S,T_1)e_m(S,T_2)$$

y por lo tanto a) se cumple.

b) Como consecuencia inmediata de la linealidad tenemos la siguiente igualdad

$$e_m(S+T,S+T) = e_m(S,S)e_m(S,T)e_m(T,S)e_m(T,T)$$

por lo que basta demostrar que $e_m(T,T) = 1$ para toda $T \in E[m]$.

Actuando en consecuencia y siendo $\tau_P : E \to E$ la traslación por P tenemos

$$\begin{aligned} div\left(\prod_{i=0}^{i=m-1} f \circ \tau_{[i]T}\right) &= m \sum_{i=0}^{i=m-1} (T + [-i]T) - ([-i]T) \\ &= m([m]T) - m(0) = 0 \end{aligned}$$

De donde $\prod_{i=0}^{i=m-1} f \circ \tau_{[i]T}$ es constate, y por lo tanto componiendo con [m], se llega a que el producto $\prod_{i=0}^{i=m-1} g^m \circ \tau_{[i]T}$ es constante, y sacando raíz m-ésima obtenemos que $\prod_{i=0}^{i=m-1} g \circ \tau_{[i]T}$ también es constante.

Ahora evaluando este último producto en los puntos X y $T+X$, obtenemos finalmente que

$$g(X+T) = g(X)$$

c) Recordemos del capítulo de isogeneas que existe un isomorfismo entre el grupo de puntos del $\ker\phi$ y el grupo de automorfismos del campo $\overline{\mathbb{K}}(E_1)$ que dejan fijo al subcampo $\phi^*\overline{\mathbb{K}}(E_2)$, y además éste está dado por el mapeo $T \to \tau_T$.

Aplicando dicho teorema a la isogenea $[m]$ y al subgrupo $E[m]$, con $E = E_1 = E_2$, y suponiendo que $e_m(S,T) = 0$ para toda $S \in E[m]$, y por tanto que $g(X+S) = g(X)$ para toda S, es decir, la función g es fija bajo la acción de los automorfismos τ_S, entonces $g \in [m]^*\overline{\mathbb{K}}(E)$ y de ahí que exista una función $h \in \overline{\mathbb{K}}(E)$, tal que $g = h \circ [m]$, y de esta manera

$$h^m \circ [m] = g^m = f \circ [m]$$

y obviamente

$$div\,(h^m) = m(T) - m(0)$$

que equivalentemente $div\,(h) = (T) - (0)$, y como una curva elíptca no puede tener sólo un polo, entonces tenemos que T=0.

d) Sean g y $\bar{g}$ las funciones que definen a e_m y a $e_{mm'}$ respectivamente. Observando que los divisores $div\,(g)$ y $div\,(g \circ [m'])$ son iguales tenemos que $\bar{g} = cg \circ [m']$, donde $c \in \overline{\mathbb{K}}$, y por tanto

$$\begin{aligned} e_{mm'}(S,T) &= \frac{g \circ [m'](X+S)}{g \circ [m'](X)} \\ &= \frac{g(Y+[m']S)}{g(Y)} = e_m([m']S,T) \end{aligned}$$

e) Sea $\sigma \in G_{\frac{\mathbb{K}}{\mathbb{K}}}$ y f y g las funciones definidas como arriba, entonces f^σ y g^σ son las funciones correspondientes al punto T^σ de esa manera

$$\begin{aligned} e_m(S,T^\sigma) &= \frac{g^\sigma(X+S)}{g^\sigma(X)} \\ &= \left(\frac{g(X+S)}{g(X)}\right)^\sigma = (e_m(S,T))^\sigma \end{aligned}$$

□

Corolario 4.12. *Existen puntos S y T en $E[m]$ tal que $e_m(S,T)$ es una raíz primitiva de μ_m. Además, si $E[m] \subset \mathbb{K}(E)$ se tiene que $\mu_m \subset \mathbb{K}^*$.*

Demostración. Conforme movemos S y T en el subgrupo $E[m]$, vamos obteniendo un subgrupo μ_d de μ_m, ya que e_m es un homomorfismo. De donde

$$1 = (e_m(S,T))^d = e_m([d]S,T)$$

y como el aparco Weil no es degenerado vemos que $[d]S = 0$ para toda $S \in E[m]$ y por lo tanto $d = m$.

En particular, si $E[m] \subset \mathbb{K}(E)$ utilizando la invarianza del aparco de Weil bajo la acción de $G_{\frac{\mathbb{K}}{\mathbb{K}}}$ y el hecho de que $S\,, T \in E[m]$ son invariantes también bajo $G_{\frac{\mathbb{K}}{\mathbb{K}}}$ tenemos que la m-ésima raíz $e_m(S,T)$ es invariante si observamos que

$$(e_m(S,T))^\sigma = e_m(S^\sigma, T^\sigma) = e_m(S,T)$$

□

Proposición 4.13. *Sea $S \in E_1[m]$ y sea $T \in E_2[m]$, si $\phi : E_1 \to E_2$ es una isogenea de E_1 entonces*

$$e_m(S, \hat{\phi}(S)) = e_m(\phi(S), T)$$

donde $\hat{\phi}$ es la dual de ϕ.

Demostración. De la subsección de isogeneas sabemos que la isogenia $\hat{\phi}$ se puede ver como la composicion de los siguientes homomorfismos:

$$E_2 \to Div^0(E_2) \to Div^0(E_1) \to E^1$$

$$Q \to (Q) - (0) \sum n_P(P) \to \sum [n]_P(P)$$

y la proposición sigue de esta propiedad sin demasiada complicación como se puede ver en el libro de Silverman [Sil85, III.8.2] □

Proposición 4.14. *Existe un apareo que es alternante, bilinear, no dejenerado, Galois invariante*

$$e : T_\ell(E) \times T_\ell(E) \to T_\ell(\mu_\ell)$$

y además que las isogeneas ϕ y $\hat{\phi}$ son adjuntas para el apareo.

Demostración. Construiremos el apareo de Weil de módulos

$$e : T_\ell(E) \times T_\ell(E) \to T_\ell(\mu_\ell)$$

que consiste en pegar todos los aparcos $e_{\ell^n} : E[\ell^n] \times E[\ell^n] \to \mu_{\ell^n}$ es decir, el apareo e actuara en cada subgrupo $E[\ell^n]$ como el apareo e_{ℓ^n}. Por lo tanto, basta demostrar que los aparcos e_{ℓ^n} son compatibles con el limite inverso, es decir es suficiente observar que se cumple

$$(e_{\ell^{n+1}}(S,T))^\ell = e_{\ell^n}([\ell]S, [\ell]T))$$

Pero por la linealidad tenemos que

$$(e_{\ell^{n+1}}(S,T))^\ell = e_{\ell^{n+1}}(S, [\ell]T)$$

y utilizando la compatibilidad de e_m con los mapeos $[\ell]$ obtenemos

$$e_{\ell^{n+1}}(S, [\ell]T) = e_{\ell^n}([\ell]S, [\ell]T)$$

□

4.4 La Demostración de la Conjetura.

Antes de dar la demostración, es necesario hacer las siguientes observaciones que probaremos ayudados por la herramienta construida en las secciones y subsecciones anteriores, en especial: el módulo de Tate y el pareo de Weil nos resultarán de gran ayuda.

Proposición 4.15. *Si $\phi \in End(E)$, ℓ es primo con $(char(\mathbb{K}), \ell) = 1$, o bien $char(\mathbb{K}) = 0$, entonces a)*

$$deg\phi = det\phi_\ell$$

b)

$$Tr(\phi_\ell) = 1 + \deg\phi - \deg(1 - \phi)$$

donde $Tr(\phi_\ell)$ y $det(\phi_\ell)$ son la traza y el determinante respectivamente de la matriz de 2×2 definida por el endomorfismo ϕ_ℓ.

Demostración. Antes que nada hay que notar que si la $char(\mathbb{K})$ es primo relativo con ℓ o es 0 entonces el módulo $T_\ell(E)$ es isomorfo con $\mathbb{Z}_\ell \times \mathbb{Z}_\ell$, de donde podemos encontrar un $\mathbb{Z}_\ell$-base de vectores v_1 y v_2, de tal forma que los endomorfismos de $T_\ell(E)$ se pueden ver como matrices de 2×2.

Por nuestra sección anterior existe un mapeo no degenerado, alternante y bilinear:

$$e : T_\ell(E) \times T_\ell(E) \to T_\ell(\mu_\ell)$$

de donde:

$$\begin{aligned} e(v_1, v_2)^{\deg\phi} &= e([\deg\phi]v_1, v_2) \\ &= e(\hat{\phi}_\ell \circ \phi_\ell v_1, v_2) \\ &= e(\phi_\ell v_1, \phi_\ell v_2) \\ &= e(av_1 + cv_2, bv_1 + dv_2) \\ &= e(v_1, v_2)^{ad-bc} \\ &= e(v_1, v_2)^{det(\phi_\ell)} \end{aligned}$$

Y como e es no degenerada entonces podemos concluir que $deg\phi = det(\phi_\ell)$ y además, haciendo uso de la siguiente identidad

$$Tr(A) = 1 + \det(A) - det(1 - A)$$

donde A es una matriz de 2×2, se deduce trivialmente el inciso b). □

Comentario 4.16. La proposición anterior nos permite asociarle a los elementos de $End(T_\ell(E))$ los números $Tr(\phi_\ell)$ y $det(\phi_\ell)$ que pertenecen a uno de los anillos más estudiados, $\mathbb{Z}$. Lo cual no es inmediatamente un hecho natural dado que $T_\ell(E)$ tiene estructura de $\mathbb{Z}_\ell$-módulo, dicho en otras palabras, los números $ad - bc$ y $a + d$ convergen en los naturales, pensados como series sobre $\mathbb{Z}$ con respecto al ideal $\ell\mathbb{Z}$.

Consideremos ahora el q^{th}-mapeo ϕ de Frobenius, donde $q = char(\mathbb{K})$, recordamos de las sección del mapeo de Frobenius 2.9 que $E(\mathbb{K}) = Ker(1-\phi)$, análogamente podemos ver que $E(\mathbb{K}_n) = Ker(1 - \phi^n)$, de donde obtenemos la importante observación más general:

$$\sharp E(\mathbb{K}_n) = \sharp Ker(1 - \phi_p^n) = \sharp deg(1 - \phi_p^n)$$

para toda $n > 0$.

Siendo la última igualdad válida dado que el mapeo $1 - \phi_p^n$ es separable por la proposición 3.37.

En particular se cumple:

$$\sharp E(\mathbb{K}) = deg(1 - \phi) \ .$$

Así haciendo

$$T = \begin{pmatrix} T & 0 \\ 0 & T \end{pmatrix}$$

y tomando en cuenta lo anterior, podemos calcular el determinante de la mátriz $T - \phi_\ell$, es decir podemos obtener el *Polinomio Característico* de ϕ_ℓ, y de esa manera, según la observación y la proposición anteriores, calcular los números $\sharp E(\mathbb{K}_n)$, que son indispensables para describir la función $Z(E/\mathbb{K}, T)$. Así:

$$\begin{aligned} det(T - \phi_\ell) &= T^2 + Tr(\phi_\ell)T + det(\phi_\ell) && (5) \\ &= (T - \alpha)(T - \beta) && (6) \end{aligned}$$

donde α y β son raíces complejas conjugadas pues la traza y el determinante involucrados en la segunda parte de la ecuación son enteros.

De esta manera evaluando en $T = 1$ tenemos que

$$det(1 - \phi_\ell) = (1 - \alpha)(1 - \beta)$$

de donde se llega a que:

$$\sharp E(\mathbb{K}) = (1-\alpha)(1-\beta) = 1-\alpha-\beta+p$$

observando que

$$\alpha\beta = det(\phi_\ell) = deg(\phi) = p$$

(Recordar: el mapeo de Frobenius es de grado p).

Análogamente podemos calcular $\sharp E(\mathbb{K}_n)$:

Triangularizando la mátriz ϕ_ℓ quedan en la diagonal los número α y β, y elevando a la n-ésima potencia tenemos que

$$det(T-\phi_\ell^n) = (T-\alpha^n)(T-\beta^n)$$

de donde

$$\sharp E(\mathbb{K}_n) = 1-\alpha^n-\beta^n+p^n$$

y de esta manera estamos en condiciones de probar el Teorema Principal.

Teorema 4.17. (Conjeturas de Weil) Sea $\mathbb{K}$ un campo finito con q elementos y $E/\mathbb{K}$ una curva elíptica. Entonces existe una $a \in \mathbf{N}$ tal que:

$$Z(E/\mathbb{K},T) = \frac{1-aT+qT^2}{(1-T)(1-qT)}$$

además

$$Z(E/\mathbb{K},\frac{1}{q}T) = Z(E/\mathbb{K},T)$$

y

$$1-aT+qT^2 = (1-\alpha T)(1-\beta T)$$

con $|\alpha| = |\beta| = \sqrt{q}$.

Demostración. Por la observación anterior tenemos que:

$$\log Z(E/\mathbb{K},T) = \sum_{n=1}^{\infty}(1-\alpha^n-\beta^n+p^n)\frac{T^n}{n} \tag{7}$$

$$= \sum_{n=1}^{\infty}\frac{T^n}{n} + \sum_{n=1}^{\infty}\alpha^n\frac{T^n}{n} + \sum_{n=1}^{\infty}\beta^n\frac{T^n}{n} + \sum_{n=1}^{\infty}p^n\frac{T^n}{n} \tag{8}$$

$$= -log(1-T) + log(1-\alpha T) + log(1-\beta T) \tag{9}$$

$$- log(1-qT) \tag{10}$$

$$= log\left(\frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qt)}\right) \tag{11}$$

de donde trivialmente

$$Z(E/\mathbb{K},T) = \frac{(1-aT+qT^2)}{(1-T)(1-qT)}$$

con $-\alpha-\beta=a$ y $q=\alpha\beta$, siendo inmediatas todas las afirmaciones del teorema, con excepción de la segunda igualdad del enunciado del teorema *(hipótesis de Riemman)* que se sigue inmediatamente comparando $Z(E/\mathbb{K},\frac{1}{q}T)$ y $Z(E/\mathbb{K},T)$. □

Referencias

[Eis95] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry.* Number 150 in GTM. Springer-Verlag, New York, 1st edition, 1995.

[Ful69] W. Fulton. *Algebraic Curves.* Brandeis University, New York, Amsterdam, 1969.

[Har77] R. Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1977.

[KM90] K.Ireland and M.Rosen. *A Clasical Introduction to Modern Number Theory*, volume 84 of *GTM.* Springer-Verlag, New York, 1990.

[Lan70] S. Lang. *Algebraic Number Theory.* Addison-Wesley, 1970.

[Lan82] S. Lang. *Introduction to Algebraic and Abelian functions.* Springer-Verlag, 2nd edition, 1982.

[Mat80] H. Matsumura. *Commutative Algebra*, volume 271. Benjamin/Cummings, 2nd edition, 1980.

[Rob73] A. Robert. *Elliptic Curves*, volume 326 of *LNM.* Springer-Verlag, New York, NY, 1973.

[Ser79] J.-P. Serre. *Local Fields.* Springer-Verlag, 1979.

[Sha74] I. Shafarevich. *Basic Algebraic Geometry.* Springer-Verlag, New York, NY, 1974.

[Sil85] Joseph H. Silverman. *The Arithmetic of Elliptic Curves.* Number 106 in GTM. Springer-Verlag, New York, 1985.

Instituto de Matemáticas
Ciudad Universitaria, UNAM
México D.F. 04510
México

portillo@math.unam.mx