Trabajo monográfico

Las Conjeturas de Weil

Mariano Rodríguez

Orientador:

Gonzalo Tornaría
Facultad de Ciencias, UDELAR

Licenciatura en Matemática
Universidad de la República
Montevideo, Uruguay

Resumen

En este trabajo monográfico estudiamos la prueba de las Conjeturas de Weil para curvas, concluyendo con la demostración de la Cota de Hasse-Weil. También calculamos para un par de curvas sus funciones Zeta asociadas, y así obteniendo fórmulas para la cantidad de puntos de la curva sobre cualquier extensión del cuerpo de base. Para probar las Conjeturas de Weil utilizamos técnicas de la Teoría de Cuerpos de Funciones en una variable, junto a herramientas de cuerpos finitos y Teoría de Galois.

Índice general

Introducción

La Teoría de Números tiene sus raices fuertemente situadas en el estudio de las ecuaciones diofánticas, es decir, ecuaciones polinómicas en varias variables con coeficientes enteros; el estudio de estas ecuaciones ha llevado a la creación y desarrollo de varias áreas, como lo son la Teoría Algebraica de Números y la Geometría Aritmética. Del estudio de las ecuaciones diofánticas, surgió también el estudio de ecuaciones diofánticas en $\mathbb{Z}/n\mathbb{Z}$; en este caso, se tienen resultados de gran importancia, como lo son las Leyes de Reciprocidad, por ejemplo, la Ley de Reciprocidad Cuadrática trata dado un primo q el comportamiento de la ecuación $x^2 \equiv q \pmod{p}$ al variar el primo p. Esta resolución nos ayuda a entender cómo se comporta para cuando n no es primo. Una de las ecuaciones diofánticas que han tenido más impacto es $x^n + y^n = z^n$, la cual fue conjeturada en 1637 por Pierre de Fermat que no tiene soluciones tal que $n \geq 3$ y $xyz \neq 0$. Conocido como el Último Teorema de Fermat, fue un disparador para la creación y desarrollo de muchas áreas, como los son las curvas elípticas, las formas cuadráticas y la formas modulares. Este problema tardó 358 años en ser resuelto, y fue gracias a la conexión encontrada entre esta ecuación y las curvas elípticas, esta conexión junto a la Conjetura de Taniyama-Shimura (1957), que sería probada parcialmente por Andrew Wiles en 1995, probó el Último Teorema de Fermat. La Conjetura de Taniyama-Shimura fue probada por completo en 2001, utilizando las ideas de Wiles. Este teorema es conocido hoy en día como Teorema de Modularidad, y hay conjeturas generalizando esto para curvas de mayor género y variedades abelianas de mayor dimensión; estas conjeturas son parte del Programa de Langlands, que busca conectar el mundo de las formas automorfas con las representaciones de grupos de Galois absolutos de cuerpos de números. Todo esto muestra la importancia de las curvas elípticas en la Teoría de Números, las cuales son un objeto central en este trabajo.

Una curva elíptica sobre un cuerpo K está definida por una ecuación de la forma:

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

con $a_1, a_2, a_3, a_4, a_6 \in K$, cuya variedad proyectiva que define es no singular y contiene un punto distinguido. A estas curvas se les puede asignar una ley de grupo abeliano, al cual Herni Poincaré conjetura en 1901 que es un grupo finitamente generado si $K = \mathbb{Q}$. Esto fue probado en principio por Louis Mordell en 1922 para $K = \mathbb{Q}$ y fue probado para cuerpos de números por André Weil en 1929. En 1921 Emil Artin conjeturó en su tesis de doctorado que dada una curva elíptica E sobre un cuerpo finito $\mathbb{F}_q$ con N puntos proyectivos se tiene que:

$$|N - (q + 1)| \leq 2\sqrt{q}$$

La intuición detras de esta conjetura surge de que la curva E es una variedad de dimensión 1 y $q+1$ es la cantidad de puntos de una recta proyectiva sobre $\mathbb{F}_q$, por lo tanto la desigualdad nos dice que una curva elíptica tiene una cantidad de puntos que no difiere mucho de la cantidad de puntos de una recta proyectiva. Esto fue probado por Helmut Hasse en 1933, en una versión un poco más general, para curvas hiperelípticas y André Weil generalizó el resultado para curvas proyectivas en 1949 de la siguiente manera: Sea C una curva proyectiva lisa sobre $\mathbb{F}_q$ con N puntos proyectivos y género g, luego

$$|N-(q+1)| \leq 2g\sqrt{q}$$

Esto es consecuencia de una serie de resultados para curvas proyectivas lisas sobre cuerpos finitos. Las Conjeturas de Weil son una generalización de estos resultados para variedades proyectivas lisas sobre cuerpos finitos, propuestas por el mismo André Weil en el mismo artículo en el que probó los resultados para curvas. Estas conjeturas tardaron 25 años en ser resueltas por completo, y fueron varios los matemáticos que colaboraron para ello.

Consideremos una variedad lisa X sobre $\mathbb{F}_q$ de dimensión d, notaremos N_m a la cantidad de puntos proyectivos de X definidos sobre $\mathbb{F}_{q^m}$. Definimos la función zeta asociada a X como:

$$Z_X(t) = \exp\left(\sum_{m=1}^{\infty} N_m \frac{t^m}{m}\right)$$

Esta función se puede ver que converge para $|t| < q^{-d}$. Una propiedad interesante de esta función es que su derivada logarítmica es la función generatriz de $\{N_m\}_{m\in\mathbb{N}}$, es decir:

$$\frac{\mathrm{d}}{\mathrm{dt}} \log Z_X(t) = \sum_{m=1}^{\infty} N_m t^{m-1}$$

Notemos que la Cota de Hasse-Weil habla sobre N_1, es decir, la cantidad de soluciones proyectivas sobre el cuerpo de base, pero al definir Z_X nos interesa la cantidad de puntos en toda extensión. Restrinjamos momentáneamente al caso de una curva elíptica, una de las claves para probar la Cota de Hasse-Weil es que se puede probar que existe $\alpha \in \mathbb{C}$ tal que $|\alpha| = q^{1/2}$ y:

$$N_m = q^m + 1 - \alpha^m - \tilde{\alpha}^m \ \ \forall m \geq 1$$

con $\tilde{\alpha} = q/\alpha$, por lo tanto $|\tilde{\alpha}| = |\alpha| = q^{1/2}$. Esto nos relaciona entonces el valor N_1 que nos interesaba con N_m para todo m. Luego:

$$|N_m - q^m - 1| = |\alpha^m + \tilde{\alpha}^m| \leq 2|\alpha|^m = 2q^{m/2}$$

y esto precisamente prueba la Cota de Hasse-Weil para una curva elíptica sobre cualquier extensión del cuerpo base. Luego de enunciar las Conjeturas de Weil veremos como esto se generaliza.

Teorema 0.1 (Conjeturas de Weil). *Sea X una variedad proyectiva lisa sobre $\mathbb{F}_q$ de dimension d. Se tiene que:*

- *Racionalidad: Z_X es una función racional:*
$$Z_X(t) = \frac{\prod_{i=1}^{d} P_{2i-1}(t)}{\prod_{i=0}^{d} P_{2i}(t)} = \prod_{i=0}^{2d} (-1)^{i+1} P_i(t)$$
con $P_i(t) \in \mathbb{Z}[t]$, $P_0(t) = 1 - t$, $P_{2d}(t) = 1 - q^d t$ y si $1 \leq i \leq 2d-1$ se tiene que $P_i(t) = \prod_j (1 - \alpha_{ij} t)$.
- *Ecuación funcional: Z_X satisface la ecuación funcional:*
$$Z_X\left(\frac{1}{q^d t}\right) = \pm q^{d\chi/2} t^{\chi} Z_X(t)$$
con χ la característica de Euler de X. Además, en algún orden, los valores $\alpha_{i1}, \alpha_{i2}, \ldots$ son iguales a $q^d/\alpha_{2n-i,1}, q^d/\alpha_{2n-i,2}, \ldots$.
- *Hipótesis de Riemann: Si $1 \leq i \leq 2d-1$: $|\alpha_{ij}| = q^{i/2}$.*
- *Números de Betti: Supongamos que X es la reducción módulo p de alguna variedad proyectiva Y definida sobre un cuerpo de números. Luego $\deg P_i$ es el i-ésimo número de Betti de Y, viendo a Y como una variedad compleja.*

Para entender la razón detras de esta "Hipótesis de Riemann", consideremos la siguiente función ζ_X:
$$\zeta_X(s) = \prod_{x \in X_{(0)}} \frac{1}{1 - N(x)^{-s}} = \sum_{c \in Z_0(X)^+} \frac{1}{N(c)^s}$$
con $X_{(0)}$ los puntos cerrados de X (órbitas de puntos por la acción de $\mathrm{Gal}\left(\overline{\mathbb{F}_q}/\mathbb{F}_q\right)$), y $N(x)$ el cardinal de la menor extensión de $\mathbb{F}_q$ sobre la que x esta definido (menor extensión sobre la cual los puntos de la órbita están definidos), es decir, podemos escribir $N(x) = q^{\deg(x)}$, con $\deg(x)$ el grado de x como punto cerrado. Por otro lado:
$$Z_0(X)^+ = \left\{ \sum_{x \in X_{(0)}} n_x x : \ n_x \geq 0 \ \forall x \in X_{(0)} \quad \text{y} \quad n_x = 0 \quad \text{para casi todo } x \in X_{(0)} \right\}$$
y $N\left(\sum_{x \in X_{(0)}} n_x x\right) = \prod_{x \in X_{(0)}} N(x)^{n_x}$. Luego se tiene lo siguiente:

Teorema 0.2.
$$\zeta_X(s) = Z_X(q^{-s})$$

Demostración. Aplicando logaritmo a $\zeta_X(s)$ se tiene:
$$\begin{aligned}
\log \zeta_X(s) &= \sum_{x \in X_{(0)}} -\log(1 - N(x)^{-s}) = \sum_{x \in X_{(0)}} \sum_{n=1}^{\infty} \frac{N(x)^{-sn}}{n} \\
&= \sum_{n=1}^{\infty} \sum_{x \in X_{(0)}} \frac{N(x)^{-sn}}{n} = \sum_{n=1}^{\infty} \sum_{x \in X_{(0)}} \frac{q^{-n \deg(x) s}}{n} \\
&= \sum_{n=1}^{\infty} \sum_{x \in X_{(0)}} \deg(x) \frac{q^{-n \deg(x) s}}{n \deg(x)} = \sum_{m=1}^{\infty} \sum_{\substack{x \in X_{(0)} \\ \deg(x) | m}} \deg(x) \frac{q^{-ms}}{m}
\end{aligned}$$

Notemos entonces que:

$$\sum_{\substack{x\in X_{(0)}\\ \deg(x)|m}} \deg(x) = N_m$$

Por lo tanto:

$$\zeta_X(s) = \exp\left(\sum_{m=1}^{\infty} N_m \frac{q^{-ms}}{m}\right) = Z_X(q^{-s})$$

■

En el caso que X sea una curva ($d = 1$), se tiene que $\zeta_X(s)$ es cero si y sólo si $q^{-s} = \alpha_{1j}^{-1}$ para algún j, y luego:

$$q^{-1/2} = |\alpha_{1j}^{-1}| = |q^{-s}| = q^{-\Re s} \implies \Re s = \frac{1}{2}$$

A pesar de haber tratado con una definición de ζ_X a partir de los puntos cerrados de la variedad, la idea de la función ζ asociada a una curva surgió de una manera un poco distinta, gracias a Emil Artin. Si C es una curva lisa en $\mathbb{F}_q$, se puede probar que el anillo de funciones regulares $\mathbb{F}_q[C]$ es un dominio de Dedekind, por lo tanto a C se le puede asignar también la función zeta de Dedekind:

$$\zeta_{\mathbb{F}_q[C]}(s) = \sum_{\substack{I\lhd\mathbb{F}_q[C]\\ I\neq 0}} \frac{1}{N(I)^s}$$

con $N(I) = \#\mathbb{F}_q[C]/I$. Por otro lado, al ser $\mathbb{F}_q[C]$ un dominio de Dedekind los ideales primos de $\mathbb{F}_q[C]$ están en correspondencia con las valuaciones de $\mathbb{F}_q(C)$, que a su vez (ver sección 4 del capítulo 1) están en correspondencia con los puntos cerrados de C; además en la correspondencia son compatibles las normas de los ideales primos con las normas de los puntos cerrados. Utilizando esto podemos ver que:

$$\zeta_{\mathbb{F}_q[C]} = \zeta_C$$

Esto es uno de los primeros pasos para notar las analogías entre cuerpos de funciones sobre cuerpos finitos y cuerpos de números. Por más que no hablaremos de estas analogías en este trabajo, estarán subyacentes y son interesantes de tener en mente a la hora de trabajar con cuerpos de funciones.

Como mencionabamos previamente, las Conjeturas de Weil fueron probadas a lo largo de 25 años. Bernard Dwork probó la racionalidad en 1960 utilizando análisis p-ádico, y luego Alexander Grothendieck probó la ecuación funcional y la conexión con los Números de Betti en 1965 utilizando la propiedades de la Cohomología Étale. La Cohomología Étale fue una herramienta desarrollada por Alexander Grothendieck y Michael Artin para poder resolver las Conjeturas de Weil, y casi 10 años más tarde, en 1974 Pierre Deligne resuelve la Hipótesis de Riemann, para así poder concluir las Conjeturas de Weil, utilizando la Cohomología Étale. Una teoría de cohomología con las propiedades era intuida desde que André Weil propuso las Conjeturas, pues el mismo llego a las Conjeturas bajo ciertas heuristicas, para las cuales el intuía que se precisaba una teoría de cohomología con ciertas propiedades.

Veamos ahora como se generaliza el hecho mencionado para curvas elípticas de que:

$$N_m = q^m + 1 - \alpha^m - \tilde{\alpha}^m$$

Consideremos una factorización de Z_X:

$$Z_X(t) = \frac{\prod_i (1 - \alpha_i t)}{\prod_i (1 - \beta_i t)}$$

PROPOSICIÓN 0.3.

$$N_m = \sum_i \beta_i^m - \sum_i \alpha_i^m$$

DEMOSTRACIÓN. Recordemos que:

$$\frac{\mathrm{d}}{\mathrm{dt}} \log Z_X(t) = \sum_{m=1}^{\infty} N_m t^{m-1}$$

Por otro lado:

$$\begin{aligned}\frac{\mathrm{d}}{\mathrm{dt}} \log Z_X(t) &= \frac{\mathrm{d}}{\mathrm{dt}} \left(\sum_i \log(1 - \alpha_i t) - \sum_i \log(1 - \beta_i t) \right) = \sum_i \frac{\beta_i}{1 - \beta_i t} - \sum_i \frac{\alpha_i}{1 - \alpha_i t} \\ &= \sum_i \sum_{m=1}^{\infty} \beta_i^m t^{m-1} - \sum_i \sum_{m=1}^{\infty} \alpha_i^m t^{m-1} = \sum_{m=1}^{\infty} \left(\sum_i \beta_i^m - \sum_i \alpha_i^m \right) t^{m-1}\end{aligned}$$

Luego por el principio de identidad de series de potencias se tiene que:

$$N_m = \sum_i \beta_i^m - \sum_i \alpha_i^m$$

■

Es más, la existencia de α_i, β_i tal que $N_m = \sum_i \beta_i^m - \sum_i \alpha_i^m$ es equivalente a la factorización dada para Z_X, y por lo tanto implicaría su racionalidad. Para el caso de dimensión 1, si X es una curva de genero g, la ecuación que se tiene es:

$$Z_X(t) = \frac{\prod_i (1 - \alpha_i t)}{(1 - t)(1 - qt)}$$

Por lo tanto la igualdad de N_m se simplifica a:

$$N_m = q^m + 1 - \sum_{i=1}^{2g} \alpha_i^m$$

por lo que se tiene una forma, relativamente sencilla, de contar la cantidad de soluciones proyectivas para una curva sobre un cuerpo finito. En la última sección de este trabajo calcularemos los α_{1i} y daremos fórmulas explícitas para N_m para ciertas curvas. En este caso ademas se tiene que $|\alpha_i| = q^{1/2}$ para todo i, por lo tanto:

$$|N_m - q^m - 1| = \left| \sum_{i=1}^{2g} \alpha_i^m \right| \leq 2g q^{m/2}$$

En este trabajo monográfico estudiamos las pruebas de la Conjetura de Weil para curvas, es decir, cuando $d = 1$. Este caso fue el primero, probado por Weil en 1949, y la razón por la cual esta prueba que estudiaremos no se generaliza es que las curvas proyectivas lisas tienen cuerpos de funciones en una variable, propiedad que no vale en dimensiones más altas.

Capítulo 1

Curvas y cuerpos de funciones

Dedicamos este capítulo a introducir los cuerpos de funciones, su relación con las curvas proyectivas lisas sobre $\mathbb{F}_q$, y culminamos con un teorema fundamental para trabajar con lugares y divisores: el Teorema de Riemann-Roch.

Definición 1.1. Dado un cuerpo K se dice que F/K es un *cuerpo de funciones en una variable* si F es una extensión de K con grado de trascendencia 1. Llamamos *cuerpo de constantes* de F/K al cuerpo de elementos algebraicos de F sobre K, denotado $\tilde{K}$.

A lo largo de este capítulo, a menos que se aclare lo contrario, cuando hablemos de cuerpos de funciones asumiremos siempre que son en una variable, y supondremos que el cuerpo de constantes de F/K satisface $\tilde{K} = K$.

Ejemplo 1.2. Los siguientes ejemplos son fundamentales para motivar la mayoría de definiciones y resultados que veremos en este capítulo:

- El más sencillo es $F = K(x)$ el cuerpo de funciones racionales de K.
- Otro ejemplo muy importante, que aunque no se tratará en esta monografía es muy útil para generar intuición, es el cuerpo de funciones meroformas de una superficie de Riemann compacta.
- Por otro lado tenemos el ejemplo que motiva este trabajo: si C una curva proyectiva sobre K dada por los ceros de un polinomio $f \in K[x, y]$ irreducible, luego se define $K(C)$ como el cuerpo de fracciones de $K[C] := K[x, y]/(f)$ y se tiene que $K(C)/K$ es un cuerpo de funciones. Para ver que es un cuerpo de funciones basta ver que $K(C)$ es una extensión finita de $K(x)$ visto dentro de $K(C)$.

1. Anillos de valuación y lugares

En esta sección enunciaremos sin prueba resultados, que se pueden encontrar en [ST].

Definición 1.3. Un *anillo de valuación* en F/K es un anillo $\mathcal{O}$ tal que $K \subsetneq \mathcal{O} \subsetneq F$ y tal que para todo $z \in F^\times$ se tiene que $z \in \mathcal{O}$ o $z^{-1} \in \mathcal{O}$.

Ejemplo 1.4. El ejemplo más sencillo de anillo de valuación es el siguiente en $K(x)/K$: consideremos $p(x) \in K[x]$ irreducible, luego es fácil ver que

$$\mathcal{O}_{p(x)} = \left\{ \frac{f(x)}{g(x)} \in K(x) : p(x) \nmid g(x) \right\}$$

es un anillo de valuación. Notemos que si $I = (p(x)) \implies \mathcal{O}_{p(x)} = K[x]_I$, es decir, las localizaciones por ideales primos de $K[x]$ da lugar a anillos de valuación.

Proposición 1.5. *Todo anillo de valuación en F/K es un anillo local.*

DEFINICIÓN 1.6. Un *lugar* P de un cuerpo de funciones F/K es un ideal maximal de un anillo de valuación $\mathcal{O}_P$ en F/K. Notamos $\mathcal{P}_F$ al *conjunto de lugares* de F/K.

TEOREMA 1.7. *Sea $P \in \mathcal{P}_F$, luego:*

(a) *P es un ideal principal de $\mathcal{O}_P$. Si $P = t\mathcal{O}_P$, se dice que t es un uniformizador (o elemento primo) de P (o de $\mathcal{O}_P$).*
(b) *Si t es un uniformizador de P, para todo $z \in F^\times$ existen únicos $n \in \mathbb{Z}$ y $u \in \mathcal{O}_P^\times$ tal que $z = t^n u$.*
(c) *Si $I \triangleleft \mathcal{O}_P$ y t un uniformizador, existe $n \in \mathbb{N}$ tal que $I = t^n\mathcal{O}_P$. Luego $\mathcal{O}_P$ es un dominio de ideales principales.*

A partir del resultado anterior, dado un lugar P elegimos un uniformizador $t \in F$ y definimos la *valuación asociada a P* como $v_P : F \to \mathbb{Z} \cup \{\infty\}$ de la siguiente manera: si $z = 0$ definimos $v_P(0) = \infty$; por otro lado si $z \neq 0$ existen $n \in \mathbb{Z}$ y $u \in \mathcal{O}_P^\times$ tales que $z = t^n u$ y definimos $v_P(z) = n$. Para ver que esto no depende de nuestra elección de uniformizador, basta ver que si $P = t\mathcal{O}_P = r\mathcal{O}_P$ se tiene que existe $u \in \mathcal{O}_P^\times$ tal que $r = tu$.

Es fácil probar que v_P cumple las siguientes propiedades:

1. $v_P(xy) = v_P(x) + v_P(y)$ para todo $x, y \in F$.
2. $v(x+y) \geq \min\{v(x), v(y)\}$ para todo $x, y \in F$, y si $v(x) \neq v(y)$ tenemos igualdad.
3. $v_P(a) = 0$ para todo $a \in K^\times$.
4. $v_P(x) = \infty \iff x = 0$.
5. Existe $t \in F$ tal que $v_P(t) = 1$.

Una función $v : F \to \mathbb{Z} \cup \{\infty\}$ que cumpla las propiedades anteriores se llama una *valuación discreta*. Luego, dado un anillo de valuación $\mathcal{O}_P$ le asignamos una valuación discreta v_P; y recíprocamente, dada una valuación discreta v, le asignamos el anillo de valuación $\mathcal{O} = \{z \in F : v(z) \geq 0\}$.

Ahora podemos expresar P y $\mathcal{O}_P$ en términos de v_P:

$$\begin{aligned} \mathcal{O}_P &= \{z \in F : \ v_P(z) \geq 0\} \\ \mathcal{O}_P^\times &= \{z \in F : \ v_P(z) = 0\} \\ P &= \{z \in F : \ v_P(z) > 0\} \end{aligned}$$

Sea $P \in \mathcal{P}_F$, luego $F_P := \mathcal{O}_P/P$ es el *cuerpo residual* de $\mathcal{O}_P$. Si $x \in \mathcal{O}_P$ notamos $x(P)$ a la clase de x en F_P, y si $x \in F \setminus \mathcal{O}_P$ notamos $x(P) := \infty$. Llamamos *mapa residual* a $F \to F_P \cup \{\infty\}$ con $x \mapsto x(P)$. Se puede ver que $K \subseteq \mathcal{O}_P$ y $K \cap P = \{0\}$, por lo que el mapa $\mathcal{O}_P \to F_P$ induce un encaje de K en F_P. Definimos entonces el *grado de un lugar* como $\deg P := [F_P : K]$.

PROPOSICIÓN 1.8. *Si $P \in \mathcal{P}_F$ y $x \in P \setminus \{0\} \implies \deg P \leq [F : K(x)] < \infty$.*

DEFINICIÓN 1.9. Sean $z \in F$ y $P \in \mathcal{P}_F$, luego decimos que P es un *cero de orden m* de z si $m = v_P(z) > 0$, y P es un *polo de orden m* de z si $m = -v_P(z) > 0$.

Como uno puede esperar, pensando en cuerpos de funciones como $K(x)$, no solo tenemos que existen lugares, sino que hay infinitos:

TEOREMA 1.10. *Todo cuerpo de funciones tiene infinitos lugares. En particular, si $z \in F \setminus K$ entonces z tiene al menos un cero y un polo.*

Concluimos esta sección con los siguientes resultados:

PROPOSICIÓN 1.11. *Sean $P_1, \ldots, P_r$ ceros de $x \in F$, luego:*

$$\sum_{i=1}^{r} v_{P_i}(x) \cdot \deg P_i \leq [F : K(x)]$$

COROLARIO 1.12. *Todo $z \in F^\times$ tiene finitos ceros y polos.*

DEMOSTRACIÓN. Si $x \in K \implies v_P(x) = 0$ para todo $P \in \mathcal{P}_F$. Si $x \in F \setminus K$, luego la cantidad de ceros de x esta acotada por $[F : K(x)] < \infty$ por la proposición anterior. Similarmente, x^{-1} tiene finitos ceros, lo que quiere decir que x tiene finitos polos. ■

2. Divisores

DEFINICIÓN 1.13. El *grupo de divisores* $\mathrm{Div}(F)$ de F/K es el grupo abeliano libre generado por $\mathcal{P}_F$. Esto quiere decir que si $D \in \mathrm{Div}(F)$, luego:

$$D = \sum_{P \in \mathcal{P}_F} n_P \cdot P$$

con $n_P \in \mathbb{Z}$ y para casi todo $P \in \mathcal{P}_F$ se tiene $n_P = 0$. Notaremos $v_P(D) := n_P$.

En $\mathrm{Div}(F)$ se tiene un orden parcial dado por $D_2 \geq D_1$ si $v_P(D_2) \geq v_P(D_1)$ para todo $P \in \mathcal{P}_F$. Similarmente, $D_2 > D_1$ si $D_2 \geq D_1$ y existe $P \in \mathcal{P}_F$ tal que $v_P(D_2) > v_P(D_1)$. Llamaremos a un divisor D *positivo* si $D > 0$.

Recordemos que tenemos una función $\deg : \mathcal{P}_F \to \mathbb{Z}$ que nos indica el grado de los lugares, esto induce un homomorfismo $\deg : \mathrm{Div}(F) \to \mathbb{Z}$ dado por:

$$\deg D := \sum_{P \in \mathcal{P}_F} v_P(D) \cdot \deg P$$

Anteriormente vimos que todo $x \in F$ tiene finitos polos y finitos ceros, esto motiva la siguiente definición:

DEFINICIÓN 1.14. Sea $x \in F^\times$, luego el *divisor principal* asociado a x es:

$$(x) := \sum_{P \in \mathcal{P}_F} v_P(x) \cdot P$$

Sean $x, y \in F$, como $v_P(x) + v_P(y) = v_P(xy)$ tenemos que $(x) + (y) = (xy)$, y esto induce una estructura de grupo en:

$$\mathrm{Princ}(F) := \{(x) \in \mathrm{Div}(F) : \ x \in F^\times\}$$

Ahora, como $\mathrm{Princ(F)} \leq \mathrm{Div}(F)$ podemos definir el grupo de clases de divisores:

$$\mathrm{Cl}(F) := \mathrm{Div}(F)/\mathrm{Princ(F)}$$

Si D_1, D_2 están en la misma clase notaremos $D_1 \sim D_2$.

A continuación damos una definición más antes de pasar a probar resultados acerca de estos objetos. Definiremos el espacio de Riemann-Roch que será fundamental a lo largo de este capítulo.

DEFINICIÓN 1.15. Sea $A \in \mathrm{Div}(F)$, el espacio de Riemann-Roch asociado a A es:

$$\mathscr{L}(A) := \{x \in F : \ (x) \geq -A\}$$

EJEMPLO 1.16. Tomemos $F = K(x)$ y veamos como es $\mathscr{L}(P)$ para algún $P \in \mathcal{P}_F$. Sea $p(x) \in K[x]$ polinomio irreducible y mónico, luego todo lugar de $K(x)$ es de la forma:

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)} \in K(x) : \ p(x) \nmid g(x) \right\}$$

$$P_\infty = \left\{ \frac{f(x)}{g(x)} : \ \mathrm{gr}(f(x)) \leq \mathrm{gr}(g(x)) \right\}$$

Además se tiene que $\deg P_{p(x)} = \deg p(x)$ y $\deg P_\infty = 1$. Sea entonces $P = P_{p(x)}$ y $r(x) \in \mathscr{L}(P)$, entonces podemos escribir a r como:

$$r(x) = f(x) \cdot p(x)^n$$

con $f(x) \in K[x]$, $p(x) \nmid f(x)$ y $n \geq -1$. Luego $g(x) \in K(x)$ pertenece a $\mathscr{L}(P)$ si y sólo si $p(x)g(x) \in K[x]$.

Más en general, $x \in \mathscr{L}(A)$ si y sólo si x tiene ceros de orden mayor igual a los polos de A y a lo sumo tiene polos de orden menor igual a los ceros de A.

PROPOSICIÓN 1.17. *Sea $A \in \mathrm{Div}(F)$, luego:*

(a) *$\mathscr{L}(A)$ es un K-espacio vectorial.*
(b) *Si $A \sim A'$, luego $\mathscr{L}(A) \cong \mathscr{L}(A')$.*

DEMOSTRACIÓN. (a) Sean $x, y \in \mathscr{L}(A)$, luego:

$$v_P(x+y) \geq \min\{v_P(x), v_P(y)\} \geq v_P(-A) \implies x + y \in \mathscr{L}(A)$$

Si $a \in K$: $v_P(ax) = v_P(x) \geq v_P(-A)$ y entonces $ax \in \mathscr{L}(A)$. Es fácil chequear que se cumplen las otras propiedades.

(b) Si $A \sim A'$ se tiene que existe $x \in F^\times$ tal que $A = A' + (x)$, luego podemos definir $\varphi : \mathscr{L}(A) \to \mathscr{L}(A')$ tal que $z \mapsto xz$. Veamos que esta bien definido:

$$v_P(xz) = v_P(x) + v_P(z) \geq v_P(x) - v_P(A) = -v_P(A')$$

Por otro lado, es claro que φ es una transformación lineal inyectiva, y si $z \in \mathscr{L}(A')$:

$$v_P(x^{-1}z) = -v_P(x) + v_P(z) \geq -v_P(x) - v_P(A') = -v_P(A)$$

por lo tanto $x^{-1}z \in \mathscr{L}(A)$ y $\varphi(x^{-1}z) = z$. Concluimos entonces que $\mathscr{L}(A) \cong \mathscr{L}(A')$. ■

DEFINICIÓN 1.18. Definimos $\ell(A) := \dim_K \mathscr{L}(A)$.

Es fácil chequear lo siguiente:

LEMA 1.19.

(a) *$\mathscr{L}(0) = K$ y si $A \in \mathrm{Div}(F)$ tal que $A < 0$, luego $\mathscr{L}(A) = \{0\}$.*

(b) *Si* $A \leq B$ *luego* $\mathscr{L}(A) \subseteq \mathscr{L}(B)$.

En particular si $A < 0$ tenemos que $\ell(A) = 0$, $\ell(0) = 1$ y si $A \leq B$ luego $\ell(A) \leq \ell(B)$. Y si $A \sim B$ como $\mathscr{L}(A) \cong \mathscr{L}(B) \implies \ell(A) = \ell(B)$.

PROPOSICIÓN 1.20. *Sean* A, B *divisores tal que* $A \leq B$ *luego*

$$\ell(B) - \ell(A) = \dim(\mathscr{L}(B)/\mathscr{L}(A)) \leq \deg(B) - \deg(A)$$

DEMOSTRACIÓN. Veamos primero que esto vale cuando $B = A + P$ con $P \in \mathcal{P}_F$, luego el resultado sigue por inducción. Sea $z \in F$ un uniformizador de P y $t = z^{v_P(B)}$, entonces $v_P(t) = v_P(B) = v_P(A) + 1$. Notemos que si $x \in \mathscr{L}(B)$ luego $v_P(x) \geq -v_P(t)$ por lo tanto $v_P(xt) \geq 0$. Podemos entonces definir la siguiente transformación lineal:

$$\begin{aligned} \varphi : \mathscr{L}(B) &\to F_P \\ x &\mapsto (xt)(P) \end{aligned}$$

Notemos lo siguiente:

$$x \in \operatorname{Ker}\varphi \iff xt \in P \iff v_P(x) \geq -v_P(t) + 1 = -v_P(A) \iff x \in \mathscr{L}(A)$$

Luego, como $\operatorname{Ker}\varphi = \mathscr{L}(A)$ tenemos que:

$$\dim(\mathscr{L}(B)/\mathscr{L}(A)) \leq \dim F_P = \deg P = \deg B - \deg A$$

■

TEOREMA 1.21. *Sea* A *un divisor y sean* $A_+, A_- \geq 0$ *de manera que* $A = A_+ - A_-$, *luego:*

$$\ell(A) \leq \deg A_+ + 1$$

En particular, $\ell(A) < \infty$ *para todo* $A \in \operatorname{Div}(F)$.

DEMOSTRACIÓN. Como $A_+ \geq 0$, aplicando la proposición anterior obtenemos:

$$\ell(A_+) - \ell(0) \leq \deg A_+ + \deg 0 \implies \ell(A_+) \leq \deg A_+ + 1$$

Por otro lado, como $A \leq A_+$ luego $\ell(A) \leq \ell(A_+) \leq \deg A_+ + 1 < \infty$. ■

El siguiente resultado es fundamental para poder decir más acerca de $\ell(A)$. Sea $x \in F^\times$, luego notaremos $(x)_0 := (x)_+$ y $(x)_\infty := (x)_-$.

TEOREMA 1.22. *Sea* $x \in F$, *luego* $\deg(x) = 0$. *Es más, se tiene:*

$$\deg(x)_0 = \deg(x)_\infty = [F : K(x)]$$

DEMOSTRACIÓN. Probaremos que $\deg(x)_0 = \deg(x)_\infty$. Por la Proposición 1.11 se deduce que $\deg(x)_\infty = \deg(x^{-1})_0 \leq [F : K(x^{-1})] = [F : K(x)]$. Queremos ver que $n := [F : K(x)] \leq \deg(x)_\infty$. Sea $u_1, \ldots, u_n$ una base de $F/K(x)$ y $C \geq 0$ divisor tal que $(u_i) \geq -C$ para todo $i = 1, \ldots, n$ (para ver que existe basta observar que hay finitos lugares P tal que existe i con $v_P(u_i) \neq 0$). Veamos que para todo $l \geq 0$ se tiene que $x^i u_j \in \mathscr{L}(l(x)_\infty + C)$ son linealmente independientes con $0 \leq i \leq l$ y $1 \leq j \leq n$. Por un lado:

$$v_P(x^i u_j) = i v_P(x) + v_P(u_j) \geq -l v_P((x)_\infty) - v_P(C) \implies x^i u_j \in \mathscr{L}(l(x)_\infty + C)$$

Que son linealmente independientes es una consecuencia inmediata de que $u_1, \ldots, u_n$ son linealmente independientes sobre $K(x)$. Por lo tanto:

$$n(l+1) \leq \ell(l(x)_\infty + C)$$

Ahora, aplicando el teorema anterior:

$$n(l+1) \leq \ell(l(x)_\infty + C) \leq l \deg(x)_\infty + \deg C + 1$$
$$\implies n - \deg C - 1 \leq l(\deg(x)_\infty - n)$$

Notemos que la expresión de la izquierda no depende de l y que la derecha es no positiva, luego como l puede ser arbitrariamente grande se llega a un absurdo si $\deg(x)_\infty < n$, por lo tanto $\deg(x)_\infty = n$. Esto por lo tanto también prueba que $\deg(x)_0 = \deg(x^{-1})_\infty = [F : K(x^{-1})] = [F : K(x)]$. Concluimos que $\deg(x) = 0$.

■

Corolario 1.23. *Sean $A \sim B$ divisores, luego $\ell(A) = \ell(B)$ y $\deg A = \deg B$. Si A es principal $\ell(A) = 1$; si $\deg A < 0$ luego $\ell(A) = 0$.*

Demostración. La primera afirmación ya la probamos y la segunda es clara. Supongamos $A = (x)$ con $x \in F^\times$, luego notemos que $(x^{-1}) = -(x)$, por lo tanto $x^{-1} \in \mathscr{L}(A)$, lo que implica que $\ell(A) \geq 1$. Notemos que $A + (x^{-1}) = 0$, luego $A \sim 0$, por lo tanto $\ell(A) = \ell(0) = 1$. Para la última afirmación basta recordar que si $\ell(A) > 0 \implies$ existe un divisor $A \geq 0$ tal que $A \sim A'$, por lo tanto si $\deg A < 0$ esto implica que $0 > \deg A = \deg A' \geq 0$ lo que es absurdo. ■

Ya vimos la cota superior $\ell(A) \leq \deg A_+ + 1$ para la dimensión del espacio de Riemann-Roch asociado a A, ahora veremos una cota inferior, que ayudará a determinar $\ell(A)$ con precisión bajo ciertas circumstancias.

Proposición 1.24. *Existe una constante $\gamma \in \mathbb{Z}$ dependiendo solo de F/K tal que para todo $A \in \mathrm{Div}(F)$:*

$$\deg A - \ell(A) \leq \gamma$$

Demostración. Recordemos que si $A \leq B$, luego:

$$\ell(B) - \ell(A) \leq \deg(B) - \deg(A) \implies \deg(A) - \ell(A) \leq \deg(B) - \ell(B)$$

Sea $x \in F \setminus K$ y consideremos $B = (x)_\infty$, luego, como vimos en la prueba del Teorema 1.22 existe $C \geq 0$ tal que $\ell(lB + C) \geq (l+1) \deg B$ para todo $l \geq 0$. Por otro lado:

$$\ell(lB + C) - \ell(lB) \leq \deg(lB + C) - \deg(lB) \implies \ell(lB + C) \leq \ell(lB) + \deg(C)$$

Entonces:

$$\begin{aligned} \ell(lB) \geq (l+1) \deg B - \deg C &= l \deg B + \deg B - \deg C \\ &= \deg(lB) + \deg(x)_\infty - \deg C \\ &= \deg(lB) + [F : K(x)] - \deg C \end{aligned}$$

Luego existe $\gamma \in \mathbb{Z}$ que depende sólo de x tal que $\deg(lB) - \ell(lB) \leq \gamma$ para todo $l > 0$ (en este caso $\gamma = \deg C - [F : K(x)]$). Teniendo esto basta probar la siguiente afirmación para concluir el resultado:

Afirmación: Dado un divisor A, existe un divisor D y un entero $l \geq 0$ tal que $A_+ \sim D$ y

$D \leq lB$. Luego como $A \leq A_+$ se puede ver que $\deg A - \ell(A) \leq \gamma$.
Prueba de la afirmación: Notemos que:

$$\ell(lB) - \ell(lB - A_+) \leq \deg A_+$$

Luego:

$$\ell(lB - A_+) \geq \ell(lB) - \deg A_+ \geq \deg(lB) - \gamma - \deg A_+ > 0$$

para un l suficientemente grande (pues $\deg B > 0$), por lo tanto existe un elemento no nulo $z \in \mathscr{L}(lB - A_+)$. Sea $D = A_+ - (z)$, luego $A_+ \sim D$:

$$D = A_+ - (z) \leq A_+ - (A_+ - lB) = lB$$

■

Esta proposición nos permite definir el invariante más importante de un cuerpo de funciones.

Definición 1.25. El *género* de un cuerpo de funciones F/K se define como:

$$g := \text{máx}\{\deg A - \ell(A) + 1 : \ A \in \text{Div}(F)\}$$

Notemos que el genero es un entero no negativo, para esto basta evaluar la expresión dentro del máximo en $A = 0$.

Teorema 1.26 (Teorema de Riemann). *Sea F/K un cuerpo de funciones de género g. Luego:*

(*a*) *Para todo $A \in \text{Div}(F)$:*

$$\ell(A) \geq \deg A + 1 - g$$

(*b*) *Existe una constante c que depende sólo de F/K tal que:*

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

cuando $\deg A \geq c$.

Demostración. La parte (a) es obvia. Para la (b) consideremos A_0 divisor tal que $g = \deg A_0 - \ell(A_0) + 1$ y sea $c := \deg A_0 + g$. Tomemos A tal que $\deg A \geq c$, luego:

$$\ell(A - A_0) \geq \deg(A - A_0) + 1 - g \geq 1$$

Por lo tanto existe $z \in \ell(A - A_0) \setminus \{0\}$. Sea $A' = A + (z) \geq A_0$, luego utilizando que $A' \sim A$:

$$\deg A - \ell(A) = \deg A' - \ell(A') \geq \deg A_0 - \ell(A_0) = g - 1$$

Luego $\ell(A) \leq \deg A + 1 - g$, y aplicando la parte (a) obtenemos la igualdad. ■

Esto nos da una herramienta muy interesante para calcular dimensiones de espacios de Riemann-Roch, aunque esto dependerá de dos cosas: poder calcular g y c. Determinar c es lo que vamos a hacer en las proxima sección, y probaremos el Teorema de Riemann-Roch que nos dice que nos podemos tomar $c = 2g - 1$, y este es un buen valor, es más, es el mejor valor de c posible, pues el resultado sería falso con $c \leq 2g - 2$.

Determinar el valor de g por otro lado es un problema difícil que no abordaremos en este trabajo, pero que involucra herramientas como Teoría de Galois y Teoría Algebraica de Números.

DEFINICIÓN 1.27. Dado un divisor A definimos el índice de especialidad:

$$i(A) := \ell(A) - \deg A - 1 + g$$

Luego, en términos de este índice, el resultado anterior nos dice que $i(A) \geq 0$ y se tiene que existe un entero $c > 0$ tal que $\deg A \geq c$ implica $i(A) = 0$.

COROLARIO 1.28. *Si $A \leq B$, luego $i(B) \leq i(A)$. Por lo tanto si $i(A) = 0$, entonces $i(B) = 0$.*

En la próxima sección abordaremos dos herramientas muy interesantes: los adeles y los diferenciales de Weil, y con esto podremos probar el Teorema de Riemann-Roch.

3. Adeles y diferenciales de Weil

DEFINICIÓN 1.29. Un elemento $\alpha \in \prod_{P \in \mathcal{P}_F} F$ es un adel de F/K si para casi todo $P \in \mathcal{P}_F$ se cumple $\alpha_P \in \mathcal{O}_P$, es decir, si $v_P(\alpha) := v_P(\alpha_P) \geq 0$. Definimos el espacio de adeles $\mathcal{A}_F$ como el conjunto de adeles sobre F/K.

PROPOSICIÓN 1.30. *$\mathcal{A}_F$ es un K espacio vectorial.*

DEMOSTRACIÓN. Chequearemos simplemente que combinaciones K lineales de adeles son adeles, el resto de propiedades son evidentes. Si $a, b \in K$ y $\alpha, \beta \in \mathcal{A}_F$:

$$v_P(a\alpha + b\beta) \geq \text{mín}\{v_P(a\alpha), v_P(b\beta)\} = \text{mín}\{v_P(\alpha), v_P(\beta)\}$$

Al ser α, β adeles, es claro que $a\alpha + b\beta$ tiene valuación no negativa para casi todos los lugares P, por lo tanto $a\alpha + b\beta \in \mathcal{A}_F$. ■

Sea $x \in F$, luego podemos considerar a x como el adel constante (para ver que x es un adel basta recordar que tiene finitos polos). Por lo tanto tenemos un encaje $F \hookrightarrow \mathcal{A}_F$.

Dado $A \in \text{Div}(F)$ definimos, de una manera similar al espacio de Riemann-Roch asociado a A, el siguiente subespacio de los adeles:

$$\mathcal{A}_F(A) := \{\alpha \in \mathcal{A}_F : \ v_P(\alpha) \geq -v_P(A) \ , \ \ \forall P \in \mathcal{P}_F\}$$

TEOREMA 1.31. *Si $A \in \text{Div}(F)$:*

$$i(A) = \dim(\mathcal{A}_F/(\mathcal{A}_F(A) + F))$$

DEMOSTRACIÓN. Primero enunciamos las afirmaciones que utilizamos para la prueba de este resultado:

1. Si $A \leq B$ divisores, luego $\mathcal{A}_F(A) \subseteq \mathcal{A}_F(B)$ y:
$$\dim(\mathcal{A}_F(B)/\mathcal{A}_F(A)) = \deg B - \deg A$$
2. Si $A \leq B$ divisores, luego:
$$\dim((\mathcal{A}_F(B) + F)/(\mathcal{A}_F(A) + F)) = i(A) - i(B)$$
3. Si B es tal que $i(B) = 0$, luego $\mathcal{A}_F = \mathcal{A}_F(B) + F$.

Luego de probar esto, la prueba sigue de la siguiente manera. Sea A un divisor, luego por el Teorema de Riemann existe $B \geq A$ tal que $i(B) = 0$, y entonces:

$$\dim(\mathcal{A}_F/(\mathcal{A}_F(A) + F)) = \dim((\mathcal{A}_F(B) + F)/(\mathcal{A}_F(A) + F)) = i(A) - i(B) = i(A)$$

■

Corolario 1.32.

$$\dim(\mathcal{A}_F/(\mathcal{A}_F(0)+F)) = g$$

A continuación probemos las tres afirmaciones de las que dependen los resultados anteriores.

Demostración de la Afirmación 1. Supongamos que $B = A + P$ con $P \in \mathcal{P}_F$, luego por inducción se tiene el caso general. Sea $t \in F$ tal que $v_P(t) = v_P(B) = v_P(A)+1$, y consideremos el mapa $\varphi : \mathcal{A}_F(B) \to F_P$ tal que $\varphi(\alpha) = (t\alpha_P)(P)$. Luego es fácil ver que $\operatorname{Ker}\varphi = \mathcal{A}_F(A)$ y se puede probar que φ es sobreyectiva, por lo tanto:

$$\mathcal{A}_F(B)/\mathcal{A}_F(A) \cong F_P \implies \dim(\mathcal{A}_F(B)/\mathcal{A}_F(A)) = \deg P = \deg B - \deg A$$

■

Demostración de la Afirmación 2. Se tiene la siguiente sucesión exacta, que aunque no mostraremos su exactitud, es algo sencillo:

$$0 \longrightarrow \mathscr{L}(B)/\mathscr{L}(A) \longrightarrow \mathcal{A}_F(B)/\mathcal{A}_F(A) \longrightarrow (\mathcal{A}_F(B)+F)/(\mathcal{A}_F(A)+F) \longrightarrow 0$$

definida con los morfismos obvios dados por componer proyecciones e inclusiones. La exactitud de la sucesión implica:

$$\begin{aligned}\dim((\mathcal{A}_F(B)+F)/(\mathcal{A}_F(A)+F)) &= \dim(\mathcal{A}_F(B)/\mathcal{A}_F(A)) - \dim(\mathscr{L}(B)/\mathscr{L}(A)) \\ &= \deg(B) - \deg(A) - (\ell(B)-\ell(A)) = i(B) - i(A)\end{aligned}$$

■

Demostración de la Afirmación 3. Sea B tal que $i(B) = 0$ y $\alpha \in \mathcal{A}_F$, luego podemos considerar $C \geq B$ tal que $\alpha \in \mathcal{A}_F(C)$. Entonces:

$$\dim((\mathcal{A}_F(C)+F)/(\mathcal{A}_F(B)+F)) = i(B) - i(C) = 0$$

Por lo tanto $\alpha \in A_F(C) + F = \mathcal{A}_F(B) + F$, por lo tanto $A_F(B) + F = \mathcal{A}_F$. ■

Ahora pasaremos a estudiar los diferenciales de Weil, que se encuentran muy relacionados con los adeles, pues estos diferenciales son funcionales lineales del espacio de adeles en K con ciertas condiciones en su núceo.

Definición 1.33. Un diferencial de Weil es un mapa lineal $\omega : \mathcal{A}_F \to K$ tal que existe un divisor A de manera que ω se anula en $\mathcal{A}_F(A) + F$. Notamos Ω_F al espacio de diferenciales de Weil; y notamos $\Omega_F(A)$ al espacio de diferenciales de Weil que se anulan en $\mathcal{A}_F(A) + F$.

Se puede ver que Ω_F es un K espacio vectorial, y $\Omega_F(A)$ un subespacio de Ω_F. También, como $\Omega_F(A)$ es isomorfo al espacio de funcionales lineales de $\mathcal{A}_F/(\mathcal{A}_F(A)+F)$, espacio de dimensión $i(A) < \infty$, luego $\dim \Omega_F(A) = i(A)$. Tomando un divisor A con $\deg A \leq -2$:

$$\dim \Omega_F(A) = \ell(A) - \deg A + g - 1 \geq g + 1 \geq 1$$

Por lo tanto $\Omega_F(A) \neq 0$ y $\Omega_F \neq 0$.

Algo interesante que veremos a continuación es que Ω_F no solo es un K espacio vectorial, sino que también es un F espacio vectorial de dimensión 1.

DEFINICIÓN 1.34. Sean $x \in F$ y $\omega \in \Omega_F$, definimos $x\omega : \mathcal{A}_F \to K$ de manera que:

$$(x\omega)(\alpha) := \omega(x\alpha)$$

Se puede ver que si ω se anula en $\mathcal{A}_F(A) + F$, luego $x\omega$ se anula en $\mathcal{A}_F(A + (x)) + F$. Esto da a Ω_F una estructura de F espacio vectorial.

LEMA 1.35. *Sean A, B divisores y $\omega \in \Omega_F(A) \setminus \{0\}$, entonces:*

$$\varphi : \mathscr{L}(A - B) \to \Omega_F(B)$$
$$x \mapsto x\omega$$

es inyectivo.

DEMOSTRACIÓN. Veamos primero que este mapa esta bien definido. Consideremos $x \in \mathscr{L}(A - B)$, es claro que $x\omega$ se anula en F ya que ω lo hace; por otro lado, si $\alpha \in \mathcal{A}_F(B)$ entonces:

$$v_P(x\alpha) = v_P(x)+v_P(\alpha) \geq v_P(B)-v_P(A)-v_P(B) = -v_P(A) \implies (x\omega)(\alpha) = \omega(x\alpha) = 0$$

ya que $\omega \in \Omega_F(A)$, por lo tanto el mapa esta bien definido. Sea ahora $x \in \mathscr{L}(A - B)$ tal que $x\omega = 0$ y supongamos que $x \neq 0$. Como $\omega \neq 0$ existe $\beta \in \mathcal{A}_F$ tal que $\omega(\beta) \neq 0$, tomemos entonces α tal que $\alpha = x^{-1}\beta$, entonces $(x\omega)(\alpha) = \omega(\beta) \neq 0$, lo que es absurdo, por lo tanto $x = 0$, y el mapa φ es inyectivo. ■

TEOREMA 1.36. *Ω_F es un F espacio vectorial de dimensión* 1.

DEMOSTRACIÓN. Sean $\omega_1, \omega_2 \in \Omega_F \setminus \{0\}$, y consideremos $A_1, A_2 \in \mathrm{Div}(F)$ tal que $\omega_i \in \Omega_F(A_i)$. Para $i = 1, 2$ definimos las funciones $\varphi_i : \mathscr{L}(A_i + B) \to \Omega_F(-B)$ tal que $x \mapsto x\omega_i$ para cierto divisor $B > 0$ que especificaremos luego. Sea $U_i = \mathrm{Im}\varphi_i$, y veamos que existe $\omega \in U_1 \cap U_2 \setminus \{0\}$; pues teniendo este diferencial se tiene que existen $x_1, x_2 \in F \setminus \{0\}$ tal que $\omega = x_1\omega_1 = x_2\omega_2 \implies \omega_2 = (x_2^{-1}x_1)\omega_1$, por lo que $\dim_F \Omega_F = 1$. Observemos lo siguiente:

$$i(-B) = \dim \Omega_F(-B) \geq \dim U_1 + U_2 = \dim U_1 + \dim U_2 - \dim U_1 \cap U_2$$
$$\implies \dim U_1 \cap U_2 \geq \dim U_1 + \dim U_2 - i(-B)$$

Para ver que existe el diferencial que buscamos basta probar que $\dim U_1 \cap U_2 \neq 0$. Como $B > 0 \implies \ell(-B) = 0$, por lo tanto $i(-B) = \deg B + g - 1$; por otro lado, como φ_i es inyectiva luego $\dim U_i = \ell(A_1 + B) \geq \deg(A_1 + B) + 1 - g$, por lo tanto:

$$\dim U_1 \cap U_2 \geq \deg B + \deg A_1 + \deg A_2 + 1 - g$$

Entonces basta elegir B con grado suficientemente grande para que $\dim U_1 \cap U_2 > 0$. ■

LEMA 1.37. *Sea $\omega \in \Omega_F \setminus \{0\}$, luego existe un único divisor W tal que $\omega \in \Omega_F(W)$ y tal que si $\omega \in \Omega_F(A)$ luego $A \leq W$.*

DEMOSTRACIÓN. Notamos $M(\omega)$ al conjunto de divisores tal que ω se anula en $\mathcal{A}_F(A)$. Luego para todo $A \in M(\omega)$ se tiene que $\omega \in \Omega_F(A) \setminus \{0\}$, por lo que $i(A) = \dim \Omega_F(A) > 0$. Recordemos que por el Teorema de Riemann existe $c > 0$ tal que $\deg A \geq c$ implica $i(A) = 0$, por lo tanto el grado de los divisores en $M(\omega)$ es acotado superiormente. Consideremos entonces $W \in M(\omega)$ un divisor de grado maximal en el conjunto.

Veamos que W es el divisor que buscamos. Supongamos existe $A \in M(\omega)$ tal que $A \not\leq W$, luego existe un lugar Q tal que $v_Q(A) > v_Q(W)$, veamos que $W + Q \in M(\omega)$, lo que es absurdo. Consideremos $\alpha \in \mathcal{A}_F(W + Q)$, luego podemos escribir $\alpha = \alpha' + \alpha''$ con $\alpha'_P = \alpha_P$ si $P \neq Q$ y $\alpha'_Q = 0$, y con $\alpha''_P = 0$ si $P \neq Q$ y $\alpha''_Q = \alpha_Q$. Finalmente, usando que $v_P(0) = \infty$ (nótese que aca nos referimos a $0 \in F$ y no a $0 \in \mathrm{Div}(F)$) es fácil ver que $\alpha' \in \mathcal{A}_F(W)$ y $\alpha'' \in \mathcal{A}_F(A)$, por lo que $\omega(\alpha) = 0$; esto implica que $W + Q \in M(\omega)$. ■

Definición 1.38. Dado $\omega \in \Omega(F) \setminus \{0\}$ definimos el divisor (ω) como el determinado por la prueba anterior. Decimos que un divisor W es canónico si existe un diferencial ω tal que $W = (\omega)$.

Proposición 1.39. *Sea $\omega \in \Omega(F) \setminus \{0\}$, entonces se tiene:*

1. *Si $A \in M(\omega)$ y $x \in F \setminus \{0\}$ luego $(x) + A \in M(x\omega)$.*
2. *Si $x \in F \setminus \{0\}$ se tiene que $(x\omega) = (x) + (\omega)$. Luego los divisores canónicos conforman una clase de divisores.*

Demostración. 1. Notemos que si $\alpha \in \mathcal{A}_F((x) + A)$ luego $x\alpha \in \mathcal{A}_F(A) \implies (x\omega)(\alpha) = \omega(x\alpha) = 0$, por lo que $(x) + A \in M(\omega)$.

2. Como $(\omega) \in M(\omega) \implies (x) + (\omega) \in M(x\omega)$, por lo que $(x) + (\omega) \leq (x\omega)$. Similarmente $(x^{-1}) + (x\omega) \leq (\omega) \implies (x\omega) \leq (x) + (\omega)$, por lo tanto $(x\omega) = (x) + (\omega)$. Recordemos que $\dim_F \Omega_F = 1$, luego dados dos divisores canónicos cualesquiera pertenecen a la misma clase; finalmente utilizando la propiedad anterior vemos que si un divisor canónico es equvialente a otro divisor D, luego este es canónico.

■

Finalmente presentamos el teorema que es la clave para probar el Teorema de Riemann-Roch.

Teorema 1.40 (Teorema de Dualidad). *Sea $A \in \mathrm{Div}(F)$ y $W = (\omega)$ un divisor canónico. Luego el mapa:*

$$\begin{aligned} \mu : \mathscr{L}(W - A) &\to \Omega_F(A) \\ x &\mapsto x\omega \end{aligned}$$

es un isomorfismo de K espacios vectoriales, y en particular $i(A) = \ell(W - A)$.

Demostración. En 1.35 vimos que este mapa es inyectivo. Consideremos ahora $\delta \in \Omega_F(A)$, luego existe $x \in F$ tal que $\delta = x\omega$. Observemos que

$$(x) + W = (x) + (\omega) = (x\omega) = (\delta) \geq A$$

por lo tanto $(x) \geq -(W - A) \implies x \in \mathscr{L}(W - A)$, por lo que $\mu(x) = \delta$. ■

Entonces tenemos como corolario:

Teorema 1.41 (Teorema de Riemann-Roch). *Sea W un divisor canónico y $A \in \mathrm{Div}(F)$, luego:*

$$\ell(A) = \deg A + 1 - g + \ell(W - A)$$

DEMOSTRACIÓN. Utilizando lo anterior obtenemos:

$$\ell(W - A) = i(A) = \ell(A) - \deg A + g - 1$$

■

COROLARIO 1.42. *Si W es un divisor canónico luego $\ell(W) = g$ y $\deg W = 2g - 2$.*

DEMOSTRACIÓN. Basta usar el Teorema de Riemann-Roch con W y evaluar en $A = 0$ y $A = W$. ■

Ahora podemos concluir la forma del Teorema de Riemann-Roch que nos será mas útil.

COROLARIO 1.43. *Si $A \in \mathrm{Div}(F)$ y $\deg A \geq 2g - 1$:*

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

DEMOSTRACIÓN. Notemos que si W es canónico $\deg(W - A) < 0$ y luego:

$$i(A) = \ell(W - A) = 0$$

■

Recordemos que previamente el Teorema de Riemann nos decía que existe una constante c tal que si $\deg A \geq c$ luego $\ell(A) = \deg A + 1 - g$, y ahora probamos que podemos tomar $c = 2g - 1$; es más, esta es la mejor constante que podemos tomar, pues si tomamos una menor se puede ver que cualquier divisor canónico sería un contraejemplo para el teorema.

4. Correspondencia entre curvas y cuerpos de funciones

Sean $C/\Bbbk$ una curva proyectiva lisa dada por $f \in \Bbbk[x, y]$, $\mathbb{K}$ una clausura algebraica de $\Bbbk$, y supongamos que $\Bbbk$ es un cuerpo perfecto, de esta manera $\mathbb{K}/\Bbbk$ es una extensión Galois. Sea $\Bbbk < L < \mathbb{K}$ un cuerpo intermedio, luego notamos $L[C] := L[x, y]/(f)$ al anillo de coordenadas de C/L, el cual es un dominio, y luego $L(C) := [L[C]]$ es su cuerpo de funciones (sobre L), el cual es un cuerpo de funciones sobre L en el sentido definido en 1.1. Notaremos $\mathcal{P}_L := \mathcal{P}_{L(C)}$, $\mathcal{P}_L^n = \{M \in \mathcal{P}_L : \deg M = n\}$ y $C(L)$ a los puntos proyectivos de C definidos en L.

Uno de los resultados más importante de esta sección es el siguiente:

TEOREMA 1.44. *Se tiene una correspondencia biyectiva entre $C(\mathbb{K})$ y $\mathcal{P}_{\mathbb{K}}$.*

Antes de ver la prueba de esta proposición veremos como asociarle a $P \in C(\mathbb{K})$ un lugar $M_P \in \mathcal{P}_{\mathbb{K}}$.

Sea $P \in C(\mathbb{K})$, y supongamos que es afín (se supone esto siempre a menos que se aclare lo contrario, pues ser afín o un punto impropio no afecta la construcción de M_P. Si el punto es impropio, a menos de un cambio de coordenadas se puede suponer que es afín, y si bien el cambio de coordenadas afecta a $\mathbb{K}[C]$, no afecta a $\mathbb{K}(C)$). Consideremos el mapa $\varphi_P : \mathbb{K}[C] \to \mathbb{K}$ tal que $[g] \mapsto g(P)$, este es un mapa sobreyectivo, por lo tanto $\operatorname{Ker}\varphi_P \lhd \mathbb{K}[C]$ es un ideal maximal, y luego la localización $\mathbb{K}[C]_{\operatorname{Ker}\varphi_P}$ es un anillo local. Notemos que se tiene una inclusión obvia $\iota : \mathbb{K}[C]_{\operatorname{Ker}\varphi_P} \to \mathbb{K}(C)$ ya que

$\mathbb{K}(C)$ es el cuerpo de fracciones de $\mathbb{K}[C]$. Notamos $\mathcal{O}_P := \iota\left(\mathbb{K}[C]_{\operatorname{Ker}\varphi_P}\right)$, el cual también es un anillo local, y notamos M_P a su ideal maximal. Nuestro objetivo ahora es ver que $\mathcal{O}_P$ es un anillo de valuación del cuerpo de funciones $\mathbb{K}(C)/\mathbb{K}$, para concluir que $M_P \in \mathcal{P}_{\mathbb{K}}$. Primero observemos que $\mathcal{O}_P$ es Noetheriano, pues $\mathbb{K}[x,y]$, lo es, y aplicar cocientes, localizaciones, y homomorfismos no afecta la Noetherianidad.

Observación 1.45. Sea $g = g_1/g_2 \in M_P$, luego como $M_P = \mathcal{O}_P \backslash \mathcal{O}_P^{\times}$, y los elementos no invertibles de $\mathbb{K}[C]_{\operatorname{Ker}\varphi_P}$ son los localizados de $\operatorname{Ker}\varphi_P$, se tiene que $g_1(P) = 0$.

Proposición 1.46. *Sea $P \in C(\mathbb{K})$, y supongamos que es un punto afín con $P = (a,b)$, luego $M_P = (x-a)_{\mathcal{O}_P}$ o $M_P = (y-b)_{\mathcal{O}_P}$.*

Demostración. Como $f(P) = 0$, existen $A, B \in \mathbb{K}[x,y]$ tal que:

$$f(x,y) = (x-a)A(x,y) + (y-b)B(x,y) \tag{1}$$

y al ser C lisa se tiene que:

$$\left(\frac{\partial f}{\partial x}(P), \frac{\partial f}{\partial y}(P)\right) = (A(P), B(P)) \neq (0,0)$$

Supongamos sin pérdida de generalidad que $B(P) \neq 0$, veamos que $M_P = (x-a)_{\mathcal{O}_P}$. Sea $g = g_1/g_2 \in M_P$, con $g_1/g_2 \in \mathbb{K}[C]_{\operatorname{Ker}\varphi_P}$, luego $g_2(P) \neq 0$, por lo tanto $g_2 \in \mathcal{O}_P^{\times}$. Suponemos entonces que $g \in M_P$, con $g \in \mathbb{K}[C]$, y sea $G \in \mathbb{K}[x,y]$ representante de g, luego $g = G + (f)$. Como $g(P) = f(P) = 0$ se tiene que $G(P) = 0$, por lo tanto existen $D, E \in \mathbb{K}[x,y]$ tal que $G(x,y) = (x-a)D(x,y) + (y-b)E(x,y)$. Ahora, despejando $y-b$ de 1 y sustituyendolo en la ecuación de $G(x,y)$ obtenemos:

$$\begin{aligned} G(x,y) &= (x-a)D(x,y) + \left(\frac{f(x,y) - (x-a)A(x,y)}{B(x,y)}\right) E(x,y) \\ &= (x-a)\left(D(x,y) - \frac{A(x,y)E(x,y)}{B(x,y)}\right) + f(x,y)\frac{E(x,y)}{B(x,y)} \end{aligned}$$

Por lo tanto el sumando de la izquierda es un representante de g (notar que $B \notin \operatorname{Ker}\varphi_P$), y luego $g \in (x-a)_{\mathcal{O}_P}$. Concluimos que $M_P \subseteq (x-a)_{\mathcal{O}_P}$, la otra inclusión es obvia. ∎

Notamos t_P al generador de M_P, y lo llamamos uniformizador de M_P (pues lo será en el sentido discutido previamente al probar que M_P es un lugar).

Teorema 1.47. *$\mathcal{O}_P$ es un anillo de valuación discreta de $\mathbb{K}(C)/\mathbb{K}$, y luego $M_P \in \mathcal{P}_{\mathbb{K}}$.*

Demostración. Primero veremos que si $I \lhd \mathcal{O}_P$ existe $n \in \mathbb{Z}$ tal que $I = (t^n)$ (para simplicar la notación utilizaremos $t := t_P$). Consideremos $I = (r) \lhd \mathcal{O}_P$, luego existe $n \in \mathbb{N}$ tal que $t^n \mid r$ y $t^{n+1} \nmid r$, pues de lo contrario $(r) \subsetneq (r/t) \subsetneq (r/t^2) \subsetneq \dots$ es una cadena creciente de ideales que no estabiliza, lo que es absurdo ya que $\mathcal{O}_P$ es Noetheriano. Sea $u \in \mathcal{O}_P$ tal que $r = ut^n$: como $t^{n+1} \nmid r$, luego $u \notin M_P$, es decir, $u \in \mathcal{O}_P^{\times}$, esto implica que $I = (t^n)$.
Sea ahora $z \in \mathbb{K}(C)$, luego como $\mathbb{K}[C] \subseteq \mathcal{O}_P$ (recordemos que P es afín) se tiene que $z = \frac{g}{h}$ con $g, h \in \mathcal{O}_P$. Sean $u, w \in \mathcal{O}_P^{\times}$ y $n, m \in \mathbb{N}$ tal que $a = ut^n$ y $b = wt^m$, luego si $v = u/w \in \mathcal{O}_P^{\times}$: $z = vt^{n-m}$. Dependiendo del signo de $n-m$ se tendrá que $z \in \mathcal{O}_P$ o $z^{-1} \in \mathcal{O}_P$. Concluimos que $\mathcal{O}_P$ es un anillo de valuación de $\mathbb{K}(C)/\mathbb{K}$ y por lo tanto que M_P es un lugar. ∎

Habiendo probado esto, tenemos el mapa $\Phi : C(\mathbb{K}) \to \mathcal{P}_{\mathbb{K}}$ tal que $P \mapsto M_P$, veremos que este mapa es una biyección.

Demostración de 1.44. Veamos primero que Φ es inyectiva. Sean $P, Q \in C(\mathbb{K})$ tal que $M_P = M_Q$ (esta suposición viene junto a $\mathcal{O}_P = \mathcal{O}_Q$, pues un lugar tiene su anillo de valuación asociado), luego $\mathcal{O}_P/M_P = \mathcal{O}_Q/M_Q$. Consideremos $\tau : \mathbb{K} \to \mathcal{O}_P/M_P$ tal que $u \mapsto [u]$, este mapa es un homomorfismo de cuerpos, por lo que es inyectivo. Luego si $\pi : \mathcal{O}_P \to \mathcal{O}_P/M_P$ proyección e $i : \mathbb{K} \to \mathcal{O}_P$ inclusión: $\tau = \pi \circ i$. Sea $P = (a, b)$ y $Q = (c, d)$, sabemos que $\pi(x - a) = 0 = \pi(x - c)$, por lo tanto $\pi(x) = \pi(a) = \pi(c)$, pero:

$$\tau(a) = \pi(a) = \pi(c) = \tau(c)$$

lo que implica que $a = c$; similarmente $b = d$, por lo tanto $P = Q$. Resta probar la sobreyectividad de Φ. Sea $M \in \mathcal{P}_{\mathbb{K}}$ y $\mathcal{O}$ su anillo de valuación. Notemos que como $[\mathcal{O}/M : \mathbb{K}] < \infty$ y $\mathbb{K}$ es algebraicamente cerrado, luego $\mathcal{O}/M \cong \mathbb{K}$, entonces el morfismo $\tau : \mathbb{K} \to \mathcal{O}/M$ tal que $u \mapsto [u]$ es un isomorfismo de cuerpos. Sea $\pi : \mathcal{O} \to \mathcal{O}/M$ proyección y consideremos $\phi = \tau^{-1} \circ \pi : \mathcal{O} \to \mathbb{K}$. A continuación es cuando surgirán las sutilezas de distinguir entre puntos afines e impropios. Separamos en varios casos:

1. Si $x, y \in \mathcal{O}$: sea $a := \phi(x)$ y $b := \phi(y)$. Si $P := (a, b)$ es fácil chequear que $M = M_P$. (en coordenadas proyectivas $P = (a : b : 1)$)
2. Si $x \in \mathcal{O}$, $y \notin \mathcal{O}$: sea $F(X, Y, Z)$ la homogenización de $f(x, y)$. En coordenadas proyectivas $x = X/Z$, $y = Y/Z$; consideremos $x' = X/Y = x/y$, $z' = Z/Y = 1/y$, luego podemos obtener un polinomio $f'(x', z')$, que tiene como homogeneizado a F. Ahora, como $y \notin \mathcal{O}$, luego $z' = 1/y \in \mathcal{O}$, y como $x, 1/y \in \mathcal{O}$ se tiene que $x' = x/y \in \mathcal{O}$. Definimos entonces $a := \phi(x')$, $b := \phi(z')$, entonces si $P = (a : 1 : b)$ se tiene que $M = M_P$.
3. Si $x \notin \mathcal{O}$, $y \in \mathcal{O}$: idem al caso anterior.
4. Si $x \notin \mathcal{O}$, $y \notin \mathcal{O}$: Tomemos $u = x/y$, sabemos que u o u^{-1} pertenecen a $\mathcal{O}$. Suponemos sin pérdida de generalidad que $u \in \mathcal{O}$, luego aplicando el mismo razonamiento que en el segundo punto se obtiene un P tal que $M = M_P$.

■

Esto prueba entonces la biyectividad entre $C(\mathbb{K})$ y $\mathcal{P}_{\mathbb{K}}$.

Consideremos $G = \mathrm{Gal}(\mathbb{K}/\Bbbk)$, luego se tienen las siguientes acciones:

- G actúa en $C(\mathbb{K})$ mediante $\sigma \cdot P \mapsto P^\sigma$.
- G actúa en $\mathcal{P}_{\mathbb{K}}$ mediante $\sigma \cdot M_P \to M_{P^\sigma}$.

Teniendo esto en cuenta, el mapa $\Phi : C(\mathbb{K}) \to \mathcal{P}_{\mathbb{K}}$ es G-equivariante, es decir, si $\sigma \in G$:

$$\Phi(P)^\sigma = M_{P^\sigma}$$

Sea $H < G$ de índice finito, y sea $L = \mathbb{K}^H$ el cuerpo fijo por H. Luego:

$$[L : \Bbbk] = [\mathbb{K}^H : \mathbb{K}^G] = [G : H] < \infty$$

por lo que L es una extensión finita de $\Bbbk$. Si G actúa en un conjunto A y $H < G$, notamos $\mathrm{Fix}_H(A)$ a los elementos fijos de A por toda la acción de H, y A_H a los elementos de

A que tienen como estabilizador a H. Entonces es fácil ver que la biyección Φ, al ser G-equivariante, se restringe a una biyección entre $\mathrm{Fix}_H(C(\mathbb{K}))$ y $\mathrm{Fix}_H(\mathcal{P}_{\mathbb{K}})$, además:

$$\mathrm{Fix}_H(C(\mathbb{K})) = C(L)$$
$$\mathrm{Fix}_H(\mathcal{P}_{\mathbb{K}}) = \Phi(C(L))$$

Esta biyección se puede restringir aún más, a una biyección entre $C(\mathbb{K})_H$ y $(\mathcal{P}_{\mathbb{K}})_H$. Finalmente, esto nos da una biyección entre los conjuntos:

$$C(\mathbb{K})_m := \{\mathscr{P} \subseteq C(\mathbb{K}) : \ \mathscr{P} \text{ órbita por } G \text{ de orden } m\}$$
$$\mathcal{P}_{\mathbb{K},m} := \{\mathscr{M} \subseteq \mathcal{P}_{\mathbb{K}} : \ \mathscr{M} \text{ órbita por } G \text{ de orden } m\}$$

Consideremos ahora el mapa $\Gamma : \mathcal{P}_{\mathbb{K},m} \to \mathcal{P}_{\Bbbk}^m$ tal que $\mathscr{M} \mapsto \Bbbk(C) \cap \bigcap \mathscr{M}$. Se puede ver que este mapa esta bien definido y que además es una biyección. Esto luego nos da entonces la biyección entre $C(\mathbb{K})_m$ y $\mathcal{P}_{\Bbbk}^m$, que será la correspondencia que más nos interesará utilizar para entender lo que esta pasando, en un sentido geométrico, en el próximo capítulo.

Para entender bien la función anterior comenzamos con la siguiente observación: sea $M_P \in \mathscr{M}$, luego

$$\mathscr{M} = \{M_{P^\sigma} : \ \sigma \in G\} = \{M_Q : \ Q \in G \cdot P\}$$

Al conjunto $G \cdot P$ lo llamamos un punto cerrado de $C/\mathbb{K}$ de grado m (el grado es el tamaño de la órbita por la acción de Galois). Sin embargo, se tiene:

$$\forall \sigma \in G : \Bbbk(C) \cap M_P = \Bbbk(C) \cap M_{P^\sigma}$$

Para probar esto basta ver que:

$$\mathcal{O} := \Bbbk(C) \cap \mathcal{O}_P$$

es un anillo de valuación discreto de $\Bbbk(C)/\Bbbk$, con ideal maximal $\Bbbk(C) \cap M_P$, que además cumple que $\forall \sigma \in G : \ \mathcal{O} = \Bbbk(C) \cap \mathcal{O}_{P^\sigma}$. Por lo tanto:

$$\Bbbk(C) \cap M_P = \Bbbk(C) \cap \bigcap_{\sigma \in G} M_{P^\sigma}$$

Ahora nos reducimos al cuerpo que nos interesará. Sea $\Bbbk = \mathbb{F}_q$ y $\mathbb{K} = \overline{\mathbb{F}_q}$, y tomemos una curva lisa $\mathbb{C}/\mathbb{F}_q$. Vimos que tenemos una correspondencia biyectiva entre $C\left(\overline{\mathbb{F}_q}\right)_m$ y $\mathcal{P}_{\mathbb{F}_q}^m$. Notemos que como $\mathbb{F}_q$ tiene solo una extensión de grado m se tiene que:

$$\begin{aligned} C\left(\overline{\mathbb{F}_q}\right)_m =& \{G \cdot P \in C\left(\overline{\mathbb{F}_q}\right) : \ P \text{ esta definido en } \mathbb{F}_{q^m} \text{ pero no en menores extensiones}\} \\ =& \{\text{Puntos cerrados de } C/\mathbb{F}_q \text{ de grado } m\} \end{aligned}$$

Luego tenemos:

Teorema 1.48. *Se tiene una correspondencia biyectiva entre los puntos cerrados de $C/\mathbb{F}_q$ de grado m y los lugares de $\mathbb{F}_q(C)/\mathbb{F}_q$ de grado m.*

Capítulo 2

Zetas locales y la Hipótesis de Riemann para cuerpos finitos

> With all of this, we have made great progress; but it is not enough. The purely algebraic theory of algebraic functions in any arbitrary field of constants is not rich enough so that one might draw useful lessons from it. The "classical" theory (that is, Riemannian) of algebraic functions over the field of constants of the complex numbers is infinitely richer; but on the one hand it is too much so, and in the mass of facts some real analogies become lost; and above all, it is too far from the theory of numbers. One would be totally obstructed if there were not a bridge between the two. And just as God defeats the devil: this bridge exists; it is the theory of the field of algebraic functions over a finite field of constants.
>
> André Weil, 1940, en una carta a su hermana Simone Weil

En este capítulo definiremos las funciones Zetas locales asociadas a un cuerpo de funciones Z_F, y veremos que si C es una curva proyectiva lisa sobre $\mathbb{F}_q$ y F es su cuerpo de funciones, luego $Z_F = Z_C$, con Z_C la función Zeta asociada a la curva C definida en la introducción. Luego probaremos las enunciados de las Conjeturas de Weil para Z_F.

1. Función zeta asociada a una curva proyectiva

Sea C una curva proyectiva lisa sobre $\mathbb{F}_q$, esta tiene un cuerpo de funciones asociado $\mathbb{F}_q(C)/\mathbb{F}_q$. Notemos que posiblemente $\mathbb{F}_q$ no es el cuerpo de constantes de $\mathbb{F}_q(C)$, supongamos este es $\mathbb{F}_{q^m}$, luego tomaremos como cuerpo de funciones de C a $\mathbb{F}_{q^m}(C)$. De esta manera podremos suponer que el cuerpo de constantes de $F = \mathbb{F}_q(C)$ es $\mathbb{F}_q$, esto será muy importante en este capítulo, por más que no lo sea en esta sección.

Definimos la función Zeta de $C/\mathbb{F}_q$ como:

$$Z_C(t) = \exp\left(\sum_{r=1}^{\infty} N_r \frac{t^r}{r}\right)$$

donde N_r es la cantidad de puntos proyectivos definidos sobre $\mathbb{F}_{q^r}$. Por otro lado, definiremos la función Zeta de $\mathbb{F}_q(C)/\mathbb{F}_q$ como:

$$Z_F(t) = \sum_{n=1}^{\infty} A_n t^n$$

con A_n siendo la cantidad de divisores mayores o iguales a 0 de grado n (probaremos que A_n es finito y que Z_F converge en un entorno de 0). Por más distantes que puedan

parecer Z_C y Z_F, se tiene que $Z_C = Z_F$. Recordemos primero algunas notaciones que vimos en la introducción.

DEFINICIÓN 2.1. Notamos $C_{(0)}$ al conjunto de puntos cerrados de C y $D_0(C)^+$ al conjunto de sumas formales $\sum_{x\in C_{(0)}} n_x x$ con $n_x \geq 0$ para todo $x \in C_{(0)}$, $n_x = 0$ para casi todo $x \in C_{(0)}$ y $n_x > 0$ para algún x. Si $x \in C_{(0)}$ notamos $N(x)$ al cardinal de la menor extensión en la que esta definida x (notemos que entonces $N(x) = q^{\deg(x)}$, con $\deg(x)$ el grado de x como punto cerrado), y esto se extiende a $D_0(C)^+$ mediante $N\left(\sum_{x\in C_{(0)}} n_x x\right) = \prod_{x\in C_{(0)}} N(x)^{n_x}$.

Similarmente, definimos $\mathrm{Div}(F)^+$ al conjunto de divisores mayores a 0.

TEOREMA 2.2.

$$Z_F = Z_C$$

DEMOSTRACIÓN. Notemos que $\mathrm{Div}(F)^+$ es el conjunto de divisores con valuación no negativa en todo lugar, y tal que existe un lugar en el que tiene valuación positiva. Por otro lado, recordemos que los lugares de grado m están en correspondencia con los puntos cerrados de grado m, por lo tanto:

$$\begin{aligned} Z_F(q^{-s}) = \sum_{n=1}^{\infty} A_n q^{-ns} &= \sum_{D\in \mathrm{Div}(F)^+} q^{-s\deg D} = \prod_{P\in\mathcal{P}_F} \frac{1}{1-q^{-s\deg P}} \\ &= \prod_{x\in C_{(0)}} \frac{1}{1-q^{-s\deg x}} = \prod_{x\in C_{(0)}} \frac{1}{1-N(x)^{-s}} = \zeta_C(s) \end{aligned}$$

Luego, por 0.2 se tiene que:

$$Z_F(q^{-s}) = \zeta_C(s) = Z_C(q^{-s}) \implies Z_F = Z_C$$

■

2. Función zeta asociada a un cuerpo de funciones

En esta sección $F/\mathbb{F}_q$ será un cuerpo de funciones con cuerpo de constantes $\mathbb{F}_q$. Al tomar un cuerpo de funciones así, se tiene que existe una curva proyectiva lisa tal que $F = \mathbb{F}_q(C)$.

Antes de definir la función zeta asociada a F precisaremos de algunos resultados.

LEMA 2.3. *Sea $n \in \mathbb{N}$, luego existen finitos divisores positivos en $F/\mathbb{F}_q$ de grado n.*

DEMOSTRACIÓN. Todo divisor positivo de grado n es suma finita de lugares de grado menor o igual a n, por lo tanto basta ver que el conjunto $S = \{P \in \mathbb{P}_F : \deg P \leq n\}$ es finito. Pero vimos que los lugares de grado m están en biyección con los puntos cerrados de grado m, y estos son finitos, por lo tanto S es finito. ■

OBSERVACIÓN 2.4. Si $A, B \in \mathrm{Div}(F)$ son divisores equivalentes, luego $\deg A = \deg B$ y $\ell(A) = \ell(B)$. Luego, dado $C \in \mathrm{Cl}(F)$ se puede hablar de $\deg C$ y $\ell(C)$.

DEFINICIÓN 2.5. Sea $n \in \mathbb{Z}$, luego:

$$\mathrm{Div}^n(F) := \{A \in \mathrm{Div}(F) : \deg A = n\} \quad \text{y} \quad \mathrm{Cl}^n(F) := \{C \in \mathrm{Cl}(F) : \deg C = n\}$$

Notemos que si $n = 0 : \mathrm{Div}^0(F) < \mathrm{Div}(F)$ y $\mathrm{Cl}^0(F) < \mathrm{Cl}(F)$.

PROPOSICIÓN 2.6. *Si* $\mathrm{Cl}^n(F) \neq \emptyset : |\mathrm{Cl}^n(F)| = \left|\mathrm{Cl}^0(F)\right| < \infty$.

DEMOSTRACIÓN. Sea $B \in \mathrm{Cl}^n(F)$ y $f : \mathrm{Cl}^0(F) \to \mathrm{Cl}^n(F)$ tal que $A \mapsto A + B$. Es claro que f es una biyección, luego $\mathrm{Cl}^0(F)$ y $\mathrm{Cl}^n(F)$ tienen igual cardinal para todo n tal que $\mathrm{Cl}^n(F) \neq \emptyset$. Sea $n \geq g$ tal que $\mathrm{Cl}^n(F) \neq \emptyset$, y sea $[B] \in \mathrm{Cl}^n(F)$. Como $\deg B \geq g$: $\ell(B) \geq \deg(B) + 1 - g \geq 1$, entonces existe $z \in \mathscr{L}(B) \setminus \{0\}$. Sea $A = B + (z) \geq 0$, luego $[A] = [B]$; ahora, toda clase de $\mathrm{Cl}^n(F)$ contiene un divisor positivo, y como hay finitos divisores positivos de grado n concluimos que $\mathrm{Cl}^n(F)$ es finito. ■

Llamamos a $h = h_F := \left|\mathrm{Cl}^0(F)\right|$ al *número de clases* de $F/\mathbb{F}_q$.

DEFINICIÓN 2.7. Dado $n \geq 0$:

$$A_n := |\{A \in \mathrm{Div}(F) : \ A \geq 0 \ \text{ y } \ \deg A = n\}|$$

Definimos $\partial := \mathrm{mín}\{\deg A : \ A \in \mathrm{Div}(F) \ \text{ y } \ \deg A > 0\}$.

Probaremos más adelante que $\partial = 1$, lo que equivale a que exista un punto de la curva C que define a F, que tenga coordenadas en $\mathbb{F}_q$. Para cuerpos de funciones genéricos esto no es cierto. Notemos también que si $A \in \mathrm{Div}(F)$ luego $\partial \mid \deg A$, y como existe $W \in \mathrm{Div}(F)$ divisor canónico: $\partial \mid \deg W = 2g - 2$.

LEMA 2.8. *Si* $[C] \in \mathrm{Cl}(F)$*:*

$$|\{A \in [C] : \ A \geq 0\}| = \frac{1}{q-1}\left(q^{\ell(C)} - 1\right)$$

Y si $n \geq 2g - 1$ *y* $\partial \mid n$*:*

$$A_n = \frac{h}{q-1}\left(q^{n+1-g} - 1\right)$$

DEMOSTRACIÓN. Sea $A \in [C]$, luego $A \geq 0 \iff$ existe $x \in \mathscr{L}(C) \setminus \{0\}$ tal que $A = C + (x)$. Además, si $x, y \in \mathscr{L}(C) \setminus \{0\}$ cumplen $C + (x) = C + (y) \implies (xy^{-1}) = 0$, y como xy^{-1} no tiene ceros ni polos se tiene que $xy^{-1} \in \mathbb{F}_q^{\times}$. Concluimos por lo tanto:

$$|\{A \in [C] : \ A \geq 0\}| = \frac{1}{q-1}\left(q^{\ell(C)} - 1\right)$$

Por otro lado, sea $\mathrm{Cl}^0(F) = \{[C_1], \ldots, [C_h]\}$, luego como cada divisor $A \geq 0$ de grado n esta en exactamente una de las clases $[C_i]$:

$$A_n = \sum_{i=1}^{h} \frac{1}{q-1}\left(q^{\ell(C)} - 1\right)$$

Aplicando Riemann Roch, pues $\deg[C_i] = n \geq 2g - 1$, obtenemos que $\ell(C) = n + 1 - g$, y entonces:

$$A_n = \sum_{i=1}^{h} \frac{1}{q-1}\left(q^{n+1-g} - 1\right) = \frac{h}{q-1}\left(q^{n+1-g} - 1\right)$$

■

DEFINICIÓN 2.9. La función *zeta asociada al cuerpo de funciones* $F/\mathbb{F}_q$ es:

$$Z(t) = Z_F(t) = \sum_{n=0}^{\infty} A_n t^n \in \mathbb{C}[[t]]$$

Por más que se define como una serie formal de potencias, veremos que converge en $|t| < q^{-1}$.

PROPOSICIÓN 2.10. *Sea* $|t| < q^{-1}$*, luego:*

(a) *Si* $g = 0$*:*

$$Z(t) = \frac{1}{q-1}\left(\frac{q}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}}\right)$$

(b) *Si* $g \geq 1:\ Z(t) = F(t) + G(t)$ *con:*

$$F(t) = \frac{1}{q-1} \sum_{0 \leq \deg[C] \leq 2g-2} q^{\ell([C])} t^{\deg[C]}$$

y

$$G(t) = \frac{h}{q-1}\left(q^{1-g}(qt)^{2g-2+\partial}\frac{1}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}}\right)$$

DEMOSTRACIÓN.

(a) Notemos que como $g = 0:\ 0 \geq 2g-1$, por lo tanto se tiene que:

$$A_n = \frac{h}{q-1}\left(q^{n+1} - 1\right)$$

si $\partial \mid n$ y $A_n = 0$ sino. Entonces:

$$\begin{aligned} Z(t) &= \frac{h}{q-1}\sum_{n=0}^{\infty}(q^{\partial n+1}-1)t^{\partial n} = \frac{h}{q-1}\left(q\sum_{n=0}^{\infty}(qt)^{\partial n} - \sum_{n=0}^{\infty}t^{\partial n}\right) \\ &= \frac{h}{q-1}\left(\frac{q}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}}\right) \end{aligned}$$

Por otro lado, notemos que si $[A] \in \mathrm{Cl}^0(F):\ \ell([A]) = \deg(A) + 1 - g = 1$, por lo tanto existe $z \in \mathscr{L}(A) \setminus \{0\}$ tal que $(z) \geq -A$. Pero recordemos que $\deg(z) = 0 = \deg A \implies (A) = (z)$, es decir, todo divisor de grado 0 es principal, por lo tanto $h = 1$. Concluimos que:

$$Z(t) = \frac{1}{q-1}\left(\frac{q}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}}\right)$$

(b) Calculemos $Z(t)$:

$$\begin{aligned} Z(t) = \sum_{n=0}^{\infty} A_n t^n &= \sum_{\deg[C]\geq 0} |\{A \in [C]:\ A \geq 0\}|\, t^{\deg[C]} = \sum_{\deg[C]\geq 0} \frac{q^{\ell([C])}-1}{q-1} t^n \\ &= \frac{1}{q-1}\sum_{0\leq\deg[C]\leq 2g-2} q^{\ell([C])}t^{\deg[C]} + \frac{1}{q-1}\left(\sum_{\deg[C]>2g-2} q^{\ell[C]}t^{\deg[C]} - \sum_{\deg[C]\geq 0} t^{\deg[C]}\right) \end{aligned}$$

Llamamos al primer sumando $F(t)$ y al segundo $G(t)$. Resta probar que $G(t)$ tiene la expresión indicada en el enunciado. Recordemos que $\mathrm{Cl}^n(F)$ y $\mathrm{Cl}^0(F)$ tienen el mismo cardinal siempre que $\partial \mid n$, de lo contrario $\mathrm{Cl}^n(F) = \emptyset$. Luego aplicando Riemann Roch obtenemos:

$$\begin{aligned}(q-1)G(t) &= \sum_{\deg[C]>2g-2} q^{\deg[C]+1-g}t^{\deg[C]} - h\sum_{\partial|n} t^{\partial n} \\ &= hq^{1-g}\sum_{\substack{n>2g-2 \\ \partial|n}} (qt)^n - h\frac{1}{1-t^\partial}\end{aligned}$$

Aplicando el cambio de variable $n = 2g-2+\partial m$, con $m \geq 1$. Notemos que este cambio de variable esta justificado ya que $\partial \mid 2g-2$. Luego:

$$\begin{aligned}(q-1)G(t) &= h\left(q^{1-g}\sum_{m=1}^{\infty}(qt)^{2g-2+\partial m} - \frac{1}{1-t^\partial}\right) \\ &= h\left(q^{1-g}(qt)^{2g-2+\partial}\frac{1}{1-(qt)^\partial} - \frac{1}{1-t^\partial}\right)\end{aligned}$$

■

Tenemos como corolario entonces la primera de las Conjeturas de Weil, la racionalidad de $Z(t)$. Próximamente seremos más especificos acerca del numerador y denominador de $Z(t)$, como se detalla en la Conjetura.

COROLARIO 2.11. *$Z(t)$ se extiende a una función racional en $\mathbb{C}$ con polos simples en $t = 1, q^{-1}$.*

DEFINICIÓN 2.12. Sea $r \geq 1$, luego notamos F_r al cuerpo compuesto dado por $F\mathbb{F}_{q^r}$.

LEMA 2.13. *Se tiene:*

(a) *La extensión F_r/F es una extensión de grado r.*
(b) *$F_r/\mathbb{F}_{q^r}$ es un cuerpo de funciones.*
(c) *$\mathbb{F}_{q^r}$ es el cuerpo de constantes de F_r.*
(d) *$F_r/\mathbb{F}_{q^r}$ tiene el mismo género que $F/\mathbb{F}_q$.*

DEMOSTRACIÓN. La prueba se encuentra en [ST]. ■

DEFINICIÓN 2.14. Decimos que $P' \in \mathcal{P}_{F_r}$ divide a $P \in \mathcal{P}_F$ si $P \subseteq P'$, y notamos $P' \mid P$.

LEMA 2.15. *Sea $P \in \mathcal{P}_F$ con $m = \deg P$. Existen exactamente $d = \mathrm{mcd}(m, r)$ lugares $P'_1, \ldots, P'_d \in \mathbb{P}_{F_r}$ tal que $P'_i \mid P$, y además estos cumplen $\deg P'_i = m/d$.*

DEMOSTRACIÓN. La prueba se encuentra en [ST]. ■

Notamos entonces $Z_r = Z_{F_r}$. A continuación veremos una identidad que nos relaciona Z con Z_r, y con la que podremos probar que $\partial = 1$.

PROPOSICIÓN 2.16. *Sea $|t| < q^{-1}$, luego:*

$$Z(t) = \prod_{P\in\mathbb{P}_F}(1-t^{\deg P})^{-1}$$

Además el producto converge absolutamente, por lo tanto $Z(t) \neq 0$ para todo $|t| < q^{-1}$.

DEMOSTRACIÓN. Bastará probar la identidad para $|t| < q^{-1}$, luego se extiende por continuación analítica.

Recordamos que un producto $\prod_i (1+a_i)^{-1} = a \neq 0$ converge absolutamente si y sólo si $\prod_i (1+a_i) = a^{-1} \neq 0$ converge absolutamente si y sólo si $\sum_i |a_i| < \infty$.

Luego, $\prod_{P\in\mathcal{P}_F}(1-t^{\deg P})^{-1}$ converge absolutamente $\iff \sum_{P\in\mathcal{P}_F} |t|^{\deg P} < \infty$:

$$\sum_{P\in\mathcal{P}_F} |t|^{\deg P} \leq \sum_{\substack{A\in \mathrm{Div}(F)\\ A\geq 0}} |t|^{\deg A} = \sum_{n=0}^{\infty} A_n |t|^n = Z(|t|) < \infty$$

Por otro lado:

$$\prod_{P\in\mathcal{P}_F} (1-t^{\deg P})^{-1} = \prod_{P\in\mathcal{P}_F} \sum_{n=0}^{\infty} t^{\deg(nP)} = \sum_{\substack{A\in \mathrm{Div}(F)\\ A\geq 0}} t^{\deg A} = \sum_{n=0}^{\infty} A_n t^n = Z(t)$$

■

PROPOSICIÓN 2.17. *Para todo $t \in \mathbb{C}$:*

$$Z_r(t^r) = \prod_{\zeta^r=1} Z(\zeta t)$$

DEMOSTRACIÓN.

$$Z_r(t^r) = \prod_{P\in\mathcal{P}_{F_r}} \left(1-t^{r\deg P}\right)^{-1} = \prod_{P\in\mathcal{P}_F} \prod_{P'|P} \left(1-t^{r\deg P'}\right)^{-1}$$

Sea $P \in \mathbb{P}_F$, $\deg P = m$ y $d = \mathrm{mcd}(m,r)$, luego:

$$\prod_{P'|P} \left(1-t^{r\deg P'}\right) = \prod_{P'|P} \left(1-t^{\frac{rm}{d}}\right) = \left(1-t^{\frac{rm}{d}}\right)^d$$

Notemos que $(X^{r/d}-1)^d = \prod_{\zeta^r=1}(X-\zeta^m)$ (basta ver que ambos son mónicos y tienen la mismas raices con igual multiplicicad). Sutituyendo $X = t^{-m}$:

$$(t^{\frac{-rm}{d}}-1)^d = \prod_{\zeta^r=1} (t^{-m}-\zeta^m)$$

y multiplicando por t^{mr}:

$$(1-t^{\frac{rm}{d}})^d = \prod_{\zeta^r=1} (1-(\zeta t)^m)$$

Juntando las igualdades que obtuvimos y utilizando que el producto de Euler converge absolutamente:

$$Z_r(t^r) = \prod_{P\in\mathcal{P}_F} \prod_{\zeta^r=1} (1-(\zeta t)^{\deg P})^{-1} = \prod_{\zeta^r=1} \prod_{P\in\mathcal{P}_F} (1-(\zeta t)^{\deg P})^{-1} = \prod_{\zeta^r=1} Z(\zeta t)$$

■

COROLARIO 2.18. *$\partial = 1$, i.e., existe un divisor D tal que* $\deg D = 1$.

DEMOSTRACIÓN. Sea ζ tal que $\zeta^{\partial} = 1$, luego como para todo $P \in \mathcal{P}_F$ se tiene que $\partial \mid \deg P$:

$$Z(\zeta t) = \prod_{P \in \mathcal{P}_F} (1 - (\zeta t)^{\deg P})^{-1} = \prod_{P \in \mathcal{P}_F} (1 - t^{\deg P})^{-1} = Z(t)$$

Entonces por la proposición anterior se tiene que $Z_\partial(t^\partial) = Z(t)^\partial$. Recordemos que $Z_\partial(t)$ tiene un polo simple en $t = 1$, y es fácil ver que $Z_\partial(t^\partial)$ también tiene un polo simple en $t = 1$. Por otro lado $Z(t)^\partial$ tiene un polo de orden ∂ en $t = 1$. Entonces como $Z_\partial(t^\partial) = Z(t)^\partial$ concluimos que $\partial = 1$. ■

Habiendo probado esto podemos simplicar las expresiones obtenidas al probar la racionalidad de Z.

COROLARIO 2.19. *Si $g = 0$ se tiene que $F/\mathbb{F}_q$ es un cuerpo de funciones racional, es decir, existe $t \in F$ tal que $F = \mathbb{F}_q(t)$:*

$$Z(t) = \frac{1}{(1-t)(1-qt)}$$

Si $g \geq 1$ se tiene que $Z(t) = F(t) + G(t)$ con:

$$F(t) = \frac{1}{q-1} \sum_{0 \leq \deg[C] \leq 2g-2} q^{\ell([C])} t^{\deg[C]}$$

y

$$G(t) = \frac{h}{q-1} \left(q^g t^{2g-1} \frac{1}{1-qt} - \frac{1}{1-t} \right)$$

DEMOSTRACIÓN. Lo único no trivial de este corolario es que si $g = 0$, luego F es un cuerpo de funciones racionales de $\mathbb{F}_q$. Esto es una consecuencia de la siguiente proposición. ■

PROPOSICIÓN 2.20. *Sea F/K un cuerpo de funciones con cuerpo de constantes K. Las siguientes condiciones son equivalentes:*

1. *F/K es racional, es decir, existe $t \in F$ tal que $F = K(t)$.*
2. *F/K tiene género 0 y $\exists A \in \mathrm{Div}(F)$ tal que* $\deg A = 1$.

DEMOSTRACIÓN. ((1) $\implies$ (2)) Para ver que existe $A \in \mathrm{Div}(F)$ tal que $\deg A = 1$ basta tomar el lugar asociado a t, es decir:

$$P_t = \left\{ \frac{f}{g} : \ f, g \in K[t], \ t \nmid g \right\}$$

Para ver que $g = 0$, consideremos el lugar:

$$P_\infty = \left\{ \frac{f}{g} : \ f, g \in K[t], \ \deg g > \deg f \right\}$$

Luego se puede ver que $1, t, \ldots, t^r \in \mathscr{L}(rP_\infty)$, por lo tanto:

$$r + 1 \leq \ell(rP_\infty) = \deg(rP_\infty) + 1 - g = r + 1 - g$$

para $r \geq 2g - 2$. Entonces como $g \geq 0 \implies g = 0$.

($(2) \implies (1)$) Notemos que $\deg A = 1 \geq 2g - 1 = -1$, por lo tanto aplicando Riemann-Roch se tiene que:

$$\ell(A) = \deg A + 1 - g = 2$$

Sea $y \in \mathscr{L}(A) \setminus \{0\}$, luego $A' := (y) + A \geq 0$ y $A' \sim A$. Como $\ell(A) = 2$, luego existe $x \in \mathscr{L}(A) \setminus \{K\}$, y por 1.10 $(x) \neq 0$. Entonces $(x) + A' \geq 0$, $\deg A = 1$ y $A' > 0$ (es más, A' es un lugar de grado 1), por lo tanto $A' = (x)_\infty$ y por 1.22:

$$[F : K(x)] = \deg(x)_\infty = \deg A' = 1$$

Concluimos que $F = K(x)$. ■

Concluimos esta sección probando otra de las conjeturas de Weil, la ecuación funcional de Z.

TEOREMA 2.21. *La función Z asociada a $F/\mathbb{F}_q$ satisface la ecuación funcional:*

$$Z(t) = q^{g-1}t^{2g-2}Z\left(\frac{1}{qt}\right)$$

DEMOSTRACIÓN. Si $g = 0$, basta sustituir 2.20. Si $g \geq 1$, utilizamos las expresiones $Z(t) = F(t) + G(t)$ de 2.20. Recordemos que si W es un divisor canónico de F: $\deg[W] = 2g - 2$, luego:

$$\{[C] \in \mathrm{Cl}(F) : \ 0 \leq \deg[C] \leq 2g - 2\} = \{[W - C] \in \mathrm{Cl}(F) : \ 0 \leq \deg[C] \leq 2g - 2\}$$

Para ver esto basta observar que $\mathrm{Cl}^n(F) \to \mathrm{Cl}^{2g-2-n}(F)$ tal que $[C] \mapsto [W - C]$ es una biyección. Por lo tanto, aplicando que $\deg[C] = -\deg[W - C] + 2g - 2$ y el teorema de Riemann-Roch:

$$\begin{aligned}
(q-1)F(t) &= \sum_{0 \leq \deg[C] \leq 2g-2} q^{\ell([C])} \cdot t^{\deg[C]} \\
&= \sum_{0 \leq \deg[C] \leq 2g-2} q^{\deg[C]+1-g+\ell([W-C])} \cdot t^{\deg[C]} \\
&= \sum_{0 \leq \deg[C] \leq 2g-2} q^{-\deg[W-C]+g-1+\ell([W-C])} \cdot t^{-\deg[W-C]+2g-2} \\
&= q^{g-1}t^{2g-2} \sum_{0 \leq \deg[C] \leq 2g-2} q^{\ell([W-C])} \cdot \left(\frac{1}{qt}\right)^{\deg[W-C]} \\
&= q^{g-1}t^{2g-2} \sum_{0 \leq \deg[C] \leq 2g-2} q^{\ell([C])} \cdot \left(\frac{1}{qt}\right)^{\deg[C]} \\
&= q^{g-1}t^{2g-2}(q-1)F\left(\frac{1}{qt}\right)
\end{aligned}$$

Por otro lado, utilizando la proposición anterior:

$$\begin{aligned} q^{g-1}t^{2g-2}G\left(\frac{1}{qt}\right) &= q^{g-1}t^{2g-2}\frac{h}{q-1}\left(q^g\frac{1}{(qt)^{2g-1}}\frac{1}{1-q\frac{1}{qt}}-\frac{1}{1-\frac{1}{qt}}\right) \\ &= \frac{h}{q-1}\left(\frac{1}{t}\frac{1}{1-\frac{1}{t}}-\frac{q^{g-1}t^{2g-2}}{1-\frac{1}{qt}}\right) \\ &= \frac{h}{q-1}\left(-\frac{1}{1-t}+q^gt^{2g-1}\frac{1}{1-qt}\right) \\ &= G(t) \end{aligned}$$

Concluimos que:

$$Z(t) = q^{g-1}t^{2g-2}Z\left(\frac{1}{qt}\right)$$

■

Esto prueba la segunda de las Conjeturas de Weil, la Ecuación Funcional.

3. L-polinomio

Determinar el L-polinomio de un cuerpo de funciones, como veremos más adelante será algo fundamental; en términos geométricos, si $C/\mathbb{F}_q$, conocer el L-polinomio, en particular sus raices, nos permitirá conocer con exactitud $|C(\mathbb{F}_{q^r})|$ para todo $r \in \mathbb{N}$.

Definición 2.22. El *L-polinomio* de $F/\mathbb{F}_q$ es $L(t) = (1-t)(1-qt)Z(t)$.

Proposición 2.23. *Sea L el L-polinomio de F, luego:*

(a) $L(t) \in \mathbb{Z}[t]$ *y tiene grado* $2g$.
(b) L *satisface la ecuación funcional:*

$$L(t) = q^gt^{2g}L\left(\frac{1}{qt}\right)$$

(c) $L(1) = h$.
(d) *Sea* $L(t) = a_0 + a_1t + \cdots + a_{2g}t^{2g}$, *entonces se tiene:*
   1. $a_0 = 1$ *y* $a_{2g} = q^g$.
   2. $a_{2g-i} = q^{g-i}a_i$ *para* $0 \leq i \leq 2g$.
   3. $a_1 = N - (q+1)$ *con N la cantidad de lugares de grado 1 de F. Notemos que* $N = A_1 = |\{A \in \mathrm{Div}(F) :\ A \geq 0 \ \ y \ \ \deg A = 1\}|$.

Demostración. Si $g = 0$ sabemos que $L(t) = 1$, por lo tanto las afirmaciones son triviales. Suponemos entonces $g \geq 1$:

(a) Para ver que $L(t)$ es un polinomio con coeficientes enteros basta comparar coeficientes con la igualdad $L(t) = (1-t)(1-qt)\sum A_nt^n$. Por otro lado, como $Z(t) = F(t)+G(t)$ con las expresiones dadas en el corolario 2.16, es fácil ver que $(1-t)(1-qt)Z(t)$ tiene grado a lo sumo $2g$. Veremos más adelante que $a_{2g} \neq 0$, por lo que tendremos que el grado de L es $2g$.

(b) Simplemente aplicamos la ecuación funcional de $Z(t)$:

$$\begin{aligned} L(t) &= (1-t)(1-qt)Z(t) = (1-t)(1-qt)q^{g-1}t^{2g-2}Z\left(\frac{1}{qt}\right) \\ &= \frac{(1-t)(1-qt)q^{g-1}t^{2g-2}}{\left(1-\frac{1}{qt}\right)\left(1-q\frac{1}{qt}\right)}\left(1-\frac{1}{qt}\right)\left(1-q\frac{1}{qt}\right)Z\left(\frac{1}{qt}\right) \\ &= \frac{(1-t)(1-qt)q^{g}t^{2g}}{(qt-1)(t-1)}L\left(\frac{1}{qt}\right) = q^g t^{2g} L\left(\frac{1}{qt}\right) \end{aligned}$$

(c) Utilicemos las expresiones dadas en el corolario 2.16 de $Z(t) = F(t)+G(t)$. Como F no tiene un polo en 1, se tiene que $(1-t)(1-qt)F(t)$ se anula en $t=1$. Luego basta calcular $(1-t)(1-qt)G(t)$ en $t=1$:

$$(1-t)(1-qt)G(t) = \frac{h}{q-1}\left(q^g t^{2g-1}(1-t) - (1-qt)\right)$$

al evaluar en $t=1$ nos queda que la expresión de la derecha es igual a h, por lo tanto $L(1) = h$.

(d) Sea $L(t) = a_0 + a_1 t + \cdots + a_{2g}t^{2g}$, luego aplicando la ecuación funcional tenemos que:

$$L(t) = q^g t^{2g} L\left(\frac{1}{qt}\right) = a_0 q^g t^{2g} + a_1 q^{g-1} t^{2g-1} + \cdots + \frac{a_{2g}}{q^g}$$

Entonces se puede ver que esta igualdad nos da la relación: $a_i q^{g-i} = a_{2g-i}$. Por otro lado, comparando coeficientes en $L(t) = (1-t)(1-qt)\sum_{n=0}^{\infty} A_n t^n$ vemos que $a_0 = 1$, y luego $a_{2g} = q^g$, lo que implica como se mencionó en la parte (a) que el grado de $L(t)$ es $2g$. Comparando coeficientes de manera similar obtenemos que: $a_1 = A_1 - (q+1)A_0 = A_1 - (q+1) = N - (q+1)$.

■

TEOREMA 2.24. *Si $L(t)$ factoriza en $\mathbb{C}$ como:*

$$L(t) = \prod_{i=1}^{2g}(1-\alpha_i t)$$

se tiene que los α_i son enteros algebraicos y se pueden ordenar de manera que $\alpha_i\alpha_{g+i} = q$ para $i = 1, \ldots, g$. Luego $\prod_{i=1}^{2g}\alpha_i = q^g$. Además, si $r \geq 1$ se tiene que L_r admite la factorización:

$$L_r(t) = \prod_{i=1}^{2g}(1-\alpha_i^r t)$$

DEMOSTRACIÓN. Sea $R(t) = t^{2g}L\left(\frac{1}{t}\right) = a_0 t^{2g} + a_1 t^{2g-1} + \cdots + a_{2g}$. Luego:

$$R(t) = t^{2g}\prod_{i=1}^{2g}\left(1-\frac{\alpha_i}{t}\right) = \prod_{i=1}^{2g}(t-\alpha_i)$$

Notemos que entonces los α_i son raices de R, que es un polinomio mónico con coeficientes enteros, por lo tanto los α_i son enteros algebraicos. Ahora, aplicando la ecuación funcional a $L(1/t)$ obtenemos:

$$R(t) = t^{2g}L\left(\frac{1}{t}\right) = t^{2g}q^g\left(\frac{1}{t}\right)^{2g} L\left(\frac{t}{q}\right) = \prod_{i=1}^{2g} q\left(1 - \frac{\alpha_i t}{q}\right) = \prod_{i=1}^{2g}(q - \alpha_i t)$$

Entonces las raices α_i están en biyección con q/α_i (notemos que $\alpha_i \neq 0$ ya que de lo contrario el grado de R es menor a $2g$), luego es claro que podemos reordenar los α_i para que cumplan $\alpha_i\alpha_{g+i} = q$.

Por otro lado, ahora veamos que pasa con $L_r(t)$. Evaluamos L_r en t^r para poder aplicar la identidad que relaciona Z_r con Z:

$$\begin{aligned} L_r(t^r) &= (1-t^r)(1-q^rt^r)Z_r(t^r) = (1-t)^r(1-q^rt^r)\prod_{\zeta^r=1} Z(\zeta t) \\ &= (1-t^r)(1-q^rt^r)\prod_{\zeta^r=1}\frac{L(\zeta t)}{(1-\zeta t)(1-q\zeta t)} \end{aligned}$$

Se puede ver que $1 - t^r = \prod_{\zeta^r=1}(1-\zeta t)$ y $1 - q^rt^r = \prod_{\xi^r=q}(1-\xi t) = \prod_{\zeta^r=1}(1-q\zeta t)$, entonces:

$$\begin{aligned} L_r(t^r) &= \prod_{\zeta^r=1} L(\zeta t) = \prod_{\zeta^r=1}\prod_{i=1}^{2g}(1-\alpha_i\zeta t) \\ &= \prod_{i=1}^{2g}\prod_{\zeta^r=1}(1-\alpha_i\zeta t) = \prod_{i=1}^{2g}(1-\alpha_i^r t^r) \end{aligned}$$

Luego $L_r(t) = \prod_{i=1}^{2g}(1-\alpha_i^r t)$. ■

Definición 2.25. Si $F/\mathbb{F}_q$ cuerpo de funciones notamos:

$$N = N(F) := |\{P \in \mathbb{P}_F : \deg P = 1\}|$$

Si $r \geq 1$ notamos:

$$N_r := N(F_r) = |\{P \in \mathbb{P}_{F^r} : \deg P = 1\}|$$

Con lo que probamos en esta sección se tiene lo siguiente: sea $a_1(p)$ el coeficiente asociado a t^1 en un polinomio p, luego:

$$a_1(L) = N - (q+1)$$

y:

$$a_1(L_r) = N_r - (q^r+1)$$

Por otro lado, si $p(t) = \prod_i(1-\beta_i t)$ se tiene que $a_1(p) = -\sum_i \beta_i$. Entonces concluimos que:

Corolario 2.26.

$$N(F) = q + 1 - \sum_{i=1}^{2g}\alpha_i$$

Y si $r \geq 1$*:*

$$N_r(F) = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r$$

Esto implica, desde el lado geométrico, que basta conocer $\alpha_1, \ldots, \alpha_{2g}$ para conocer $\#C(\mathbb{F}_{q^r})$ para todo $r \geq 1$.

4. Hasse-Weil

En esta sección probaremos el resultado más importante de este trabajo monográfico, esta es la cota de Hasse Weil para curvas lisas absolutamente irreducibles sobre $\mathbb{F}_q$.

TEOREMA 2.27 (Hasse-Weil, 1949). *Sea* $C/\mathbb{F}_q$ *una curva lisa absolutamente irreducible de género* g *luego:*

$$|\#C(\mathbb{F}_q) - (q+1)| \leq 2gq^{\frac{1}{2}}$$

En términos de cuerpos de funciones el resultado es:

TEOREMA 2.28. *Sea* $F/\mathbb{F}_q$ *un cuerpo de funciones de género* g *luego:*

$$|N - (q+1)| \leq 2gq^{\frac{1}{2}}$$

Dada la biyección que vimos entre puntos y lugares, es claro que ambos teoremas son equivalentes.

La prueba de este teorema que veremos viene dada por Enrico Bombieri, y el camino a seguir es el siguiente: Sea $F/\mathbb{F}_q$ un cuerpo de funciones:

1. Probar que existe $c \in \mathbb{R}$ tal que para todo $r \geq 1$:
$$|N_r - (q^r + 1)| \leq cq^{\frac{r}{2}}$$
2. Probar que los α_i definidos en la sección anterior tienen valor absoluto $q^{1/2}$ (análogo de la Hipótesis de Riemann).
3. Probar que basta tomar $c = 2g$ en la cota dada anteriormente.

Sabiendo que ese será el camino, vamos a recorrerlo de manera inversa.

TEOREMA 2.29. *Supongamos que* $|\alpha_i| = q^{1/2}$ *para todo* $i = 1, \ldots, 2g$*, luego para todo* $r \geq 1$*:*

$$|N_r - (q^r + 1)| \leq 2gq^{\frac{r}{2}}$$

DEMOSTRACIÓN. Recordemos de 2.26 que:

$$N_r = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r$$

Luego:

$$|N_r - (q^r + 1)| = \left| \sum_{i=1}^{2g} \alpha_i^r \right| \leq \sum_{i=1}^{2g} |\alpha_i|^r = 2gq^{r/2}$$

■

TEOREMA 2.30. *Supongamos que existe $c \in \mathbb{R}$ tal que:*

$$|N_r - (q^r + 1)| \leq cq^{\frac{r}{2}} \quad \forall r \geq 1$$

Luego $|\alpha_i| = q^{1/2}$ para todo $i = 1, \ldots, 2g$.

DEMOSTRACIÓN. Definimos:

$$H(t) = \sum_{i=1}^{2g} \frac{\alpha_i t}{1 - \alpha_i t}$$

Notemos que $H(t)$ tiene radio de convergencia:

$$\varrho = \min_{1 \leq i \leq 2g} \left\{ |\alpha_i|^{-1} \right\}$$

alrededor de $t = 0$. Por otro lado:

$$H(t) = \sum_{i=1}^{2g} \sum_{r=1}^{\infty} (\alpha_i t)^r = \sum_{r=1}^{\infty} \left(\sum_{i=1}^{2g} \alpha_i^r \right) t^r$$

Y como se tiene que $N_r - (q^r + 1) = -\sum_{i=1}^{2g} \alpha_i^r$, luego:

$$\left| -\sum_{i=1}^{2g} \alpha_i^r \right| = |N_r - (q^r + 1)| \leq cq^{r/2}$$

Por lo tanto, se tiene que $H(t)$ converge si $|tq^{1/2}| < 1 \iff |t| < q^{-1/2}$. Como $H(t)$ tiene radio de convergencia ϱ:

$$q^{-1/2} \leq \varrho \implies \forall i = 1, \ldots, 2g : \ |\alpha_i| \leq q^{1/2}$$

Recordemos que por 2.24:

$$\prod_{i=1}^{2g} \alpha_i = q^g$$

Entonces debe ser que $|\alpha_i| = q^{1/2}$. ■

5. Lema principal

Llamaremos "Lema principal" a:

LEMA 2.31 (Lema principal). *Existe $c \in \mathbb{R}$ tal que:*

$$|N_r - (q^r + 1)| \leq cq^{\frac{r}{2}} \quad \forall r \geq 1$$

Antes de probar esto, notaremos algo que por mas obvio que sea es esencial para la prueba del lema principal:

PROPOSICIÓN 2.32. *Sea $r \geq 1$, luego el teorema de Hasse-Weil vale para $F/\mathbb{F}_q$ si y sólo si vale para $F_r/\mathbb{F}_{q^r}$.*

DEMOSTRACIÓN. Esto es claro por 2.24. ■

Teniendo esto en cuenta, el lema principal lo probaremos para las potencias para los q tal que $q > (g+1)^4$ y tal que q es un cuadrado. Por lo tanto, no probaremos directamente el lema principal para los q que no cumplan lo anterior, pero si sabemos que estos q cumpliran la Hipótesis de Riemann, y por lo tanto cumplirán la cota de Hasse-Weil (lo que es más fuerte que el lema principal).

Dividiremos la prueba del lema principal en dos partes:

1. Probar la cota superior, es decir, probar que existe $c_1 \in \mathbb{R}$ tal que:
$$N_r \leq q^r + 1 + c_1 q^{\frac{r}{2}} \quad \forall r \geq 1$$
Desde el punto de vista geométrico: acota la cantidad de puntos de la curva.
2. Probar la cota inferior, es decir, probar que existe $c_2 \in \mathbb{R}$ tal que:
$$q^r + 1 - c_2 q^{\frac{r}{2}} \leq N_r \quad \forall r \geq 1$$
Desde el punto de vista geométrico: dice que existen puntos, lo que es algo "más difícil" de probar, como veremos.

5.1. Cota superior. Antes de probar la cota superior veremos algunas propiedades estandares de cuerpos de funciones.

DEFINICIÓN 2.33. Sea F/K un cuerpo de funciones, y $Q \in \mathcal{P}_F$, luego se dice que i es un *número polo* de Q si:
$$\exists x \in F : \ (x)_\infty = iQ$$
Recordemos que $\mathcal{P}_F^1 = \{Q \in \mathcal{P}_F : \ \deg Q = 1\}$.

LEMA 2.34. *Sea $Q \in \mathcal{P}_F^1$, luego i es un número polo de Q si y sólo si $\ell(iQ) = \ell((i-1)Q) + 1$.*

DEMOSTRACIÓN. Si i es un número polo existe $x \in \mathscr{L}(iQ)$ tal que $(x)_\infty = iQ$, y por lo tanto $x \in \mathscr{L}(iQ) \setminus \mathscr{L}((i-1)Q)$. Por otro lado, por 1.20:
$$\ell(iQ) - \ell((i-1)Q) \leq \deg(iQ) - \deg((i-1)Q) = 1$$
Luego, como vimos que $\mathscr{L}(iQ) \neq \mathscr{L}((i-1)Q)$ se tiene que $\ell(iQ) = \ell((i-1)Q) + 1$.

Ahora, si $\ell(iQ) = \ell((i-1)Q) + 1$, existe $x \in \mathscr{L}(iQ) \setminus \mathscr{L}((i-1)Q)$, y es fácil ver que $(x)_\infty = iQ$. ■

Sea $m \in \mathbb{N}$ y $Q \in \mathcal{P}_F^1$, definimos $T_Q = \{j : \ 0 \leq j \leq m, \ j \text{ número polo de } Q\}$. Por el lema anterior sabemos que para todo $j \in T_Q$ existe $u_j \in F$ tal que $(u_j)_\infty = jQ$, y se tiene la siguiente proposición:

PROPOSICIÓN 2.35. *$\{u_j : \ j \in T\}$ es una base de $\mathscr{L}(mQ)$.*

DEMOSTRACIÓN. Veamos primero que $\#T = \ell(mQ)$:
$$\ell(mQ) = \ell(mQ) - \ell(-Q) = \sum_{i=0}^{m} \ell(iQ) - \ell((i-1)Q)$$
$$= \sum_{\substack{0 \leq i \leq m \\ i \text{ número polo de } Q}} 1 = \#T$$

Basta entonces probar que $\{u_j : j \in T\}$ es linealmente independiente en $\mathscr{L}(mQ)$. Sean $\{a_j\}_{j\in T} \subseteq K$ tal que existe $i \in T : a_i \neq 0$. Como $a_j \in K$ se tiene que $v_Q(a_j) = 0$ si $a_j \neq 0$; luego si $i \neq j$ y $a_i \neq 0 \neq a_j$: $-i = v_Q(a_i u_i) \neq v_Q(a_j u_j) = -j$. Entonces se tiene que:

$$v_Q\left(\sum_{\substack{j\in T\\ a_j\neq 0}} a_j u_j\right) = \text{mín}\{v_Q(a_j u_j) : j \in T,\ a_j \neq 0\} < \infty$$

Y como $v_Q(0) = \infty$ se tiene que $\sum_{j\in T} a_j u_j \neq 0$. Por lo tanto el conjunto $\{u_j : j \in T\}$ es una base de $\mathscr{L}(mQ)$. ■

Ahora sí podemos probar la cota superior del lema principal.

TEOREMA 2.36. *Sea $F/\mathbb{F}_q$ cuerpo de funciones de manera que $q > (g+1)^4$ y q es un cuadrado, luego:*

$$N \leq q + 1 + (2g+1)q^{\frac{1}{2}}$$

DEMOSTRACIÓN. Sea $Q \in \mathcal{P}_F^1$ y establecemos unas constantes que nos serán útiles:

$$q_0 := q^{\frac{1}{2}}, \quad m := q_0 - 1, \quad n := 2g + q_0, \quad r := m + nq_0 = q - 1 + (2g+1)q^{\frac{1}{2}}$$

Notemos que, al ser q un cuadrado, q_0 es una potencia de la característica de F, y por lo tanto se tiene que: $(a+b)^{q_0} = a^{q_0} + b^{q_0}$ para todo $a, b \in F$; a su vez, si $a \in \mathbb{F}_q$ también sabemos que existe a^{1/q_0}. Sea $\{u_j : j \in T\}$ una base de $\mathscr{L}(mQ)$ como fue descrita en 2.35. Definimos el $\mathbb{F}_q$-espacio vectorial $\mathscr{L}$ como:

$$\mathscr{L} = \mathscr{L}(mQ)\cdot\mathscr{L}(nQ)^{q_0} := \left\{\sum_{i=1}^{s} x_i y_i^{q_0} : s \geq 1,\ x_1, \ldots, x_s \in \mathscr{L}(mQ),\ y_1, \ldots, y_s \in \mathscr{L}(nQ)\right\}$$

Sean $x \in \mathscr{L}(mQ), y \in \mathscr{L}(nQ)$, luego: $(xy^{q_0}) = (x) + q_0(y) \geq -(m + nq_0)Q$, por lo tanto $xy^{q_0} \in \mathscr{L}((m+nq_0)Q) = \mathscr{L}(rQ)$; aplicando que para todos $z_1, z_2 \in F$ se tiene que $v_Q(z_1 + z_2) \geq \text{mín}\{v_Q(z_1), v_Q(z_2)\}$ se tiene que: $\forall z \in \mathscr{L} : z \in \mathscr{L}(rQ)$.

<u>*Afirmación:*</u> Existe $z \in \mathscr{L} \setminus \{0\}$ tal que: $z(P) = 0$ para todo $P \in \mathcal{P}_F^1 \setminus \{Q\}$.

De probar que existe el elemento z mencionado en la afirmación se tiene que:

$$\deg(z)_0 \geq \#\mathcal{P}_F^1 \setminus \{Q\} = N - 1$$

Pero sabemos que $z \in \mathscr{L}(rQ)$, luego:

$$\deg(z)_0 = \deg(z)_\infty \leq r = q - 1 + (2g+1)q^{\frac{1}{2}}$$

Por lo tanto:

$$N \leq \deg(z)_0 + 1 \leq q + (2g+1)q^{\frac{1}{2}} \leq q + 1 + (2g+1)q^{\frac{1}{2}}$$

Comenzamos entonces la prueba de la afirmación. Esta se dividirá en tres pasos:

<u>*Paso 1:*</u> Para todo $z \in \mathscr{L}$ existen únicos $\{z_j\}_{j\in T} \subseteq \mathscr{L}(nQ)$ tal que:

$$z = \sum_{j\in T} u_j z_j^{q_0}$$

Esto luego implica que $\dim_{\mathbb{F}_q} \mathscr{L} = \ell(mQ)\ell(nQ)$ (basta tomar una base de $\mathscr{L}(nQ)$, y ver que el producto de esta con $\{u_j : j \in T\}$ da una base de $\mathscr{L}$).

Para ver su existencia sea $z = \sum_{i\in T} x_i y_i^{q_0}$ y $a_{ij} \in \mathbb{F}_q$ tal que:

$$x_i = \sum_j a_{ij}u_j \implies z = \sum_{i\in T}\sum_{j\in T} a_{ij}u_j y_i^{q_0} = \sum_{j\in T} u_j \left(\sum_{i\in T} a_{ij} y_i^{q_0}\right)$$

Luego:

$$\sum_{i\in T} a_{ij} y_i^{q_0} = \left(\sum_{i\in T} a_{ij}^{\frac{1}{q_0}} y_i\right)^{q_0}$$

Por lo tanto $z_j := \sum_{i\in T} a_{ij}^{\frac{1}{q_0}} y_i$ pertenece a $\mathscr{L}(nQ)$ y cumple $z = \sum_{j\in T} u_j z_j^{q_0}$. Para ver la unicidad, supongamos que existen $z_j \in \mathscr{L}(nQ)$ tal que $\sum_{j\in T} u_j z_j^{q_0} = 0$, luego si $z_j \neq 0$:

$$v_Q\left(u_j z_j^{q_0}\right) = v_Q(u_j) + q_0 v_Q(z_j 0) \equiv -i \text{ mód } q_0$$

Esto implica que si $i \neq j$ y $z_i \neq 0 \neq z_j$: $v_Q(u_i z_i^{q_0}) \neq v_Q(u_j z_j^{q_0})$. Luego:

$$\infty = v_Q(0) = v_Q\left(\sum_{\substack{j\in T\\ z_j\neq 0}} u_j z_j^{q_0}\right) = \text{mín}\left\{v_Q\left(u_j z_j^{q_0}\right) : j \in T,\ z_j \neq 0\right\} \neq \infty$$

lo que es absurdo.

<u>*Paso 2:*</u> Definimos el homomorfismo de grupos aditivos $\lambda : \mathscr{L} \to \mathscr{L}((mq_0 + n)Q)$ tal que:

$$\sum_{j\in T} u_j z_j^{q_0} \mapsto \sum_{j\in T} u_j^{q_0} z_j$$

Veremos que $\operatorname{Ker}\lambda \neq 0$. Notemos que como $\mathscr{L}$ y $\mathscr{L}((mq_0+n)Q)$ son espacios de dimensión finita sobre $\mathbb{F}_q$, entonces estos espacios son finitos; luego para ver que $\operatorname{Ker}\lambda \neq 0$ basta probar que $\dim\mathscr{L} > \ell((mq_0 + n)Q)$, pues si $\operatorname{Ker}\lambda = 0$ se tiene que λ es una inyección de $\mathscr{L}$ en $\mathscr{L}((mq_0 + n)Q)$, lo que es absurdo ya que $\#\mathscr{L} > \#\mathscr{L}((mq_0 + n))$.

En el paso 1 vimos que $\dim L = \ell(mQ)\ell(nQ)$, entonces por 1.26:

$$\begin{aligned}\ell(mQ)\ell(nQ) &\geq (\deg mQ + 1 - g)(\deg nQ + 1 - g)\\ &= (m + 1 - g)(n + 1 - g)\\ &= (q_0 - g)(q_0 + g + 1) = q - g^2 + q_0 - g\end{aligned}$$

Ahora, notemos que $mq_0 + n = (q_0 - 1)q_0 + 2g + q_0 = q + 2g \geq 2g - 1$, por lo tanto aplicando 1.43 obtenemos que:

$$\ell((mq_0 + n)Q) = \deg((mq_0 + n)Q) + 1 - g = 2g + q + 1 - g = q + 1 + g$$

Entonces:

$$\dim \mathscr{L} > \ell((mq_0+n)Q) \iff q - g^2 + q_0 - g > q + 1 + g$$
$$\iff q_0 > g^2 + 2g + 1 = (g+1)^2 \iff q > (g+1)^4$$

Aca se ve la importancia de la hipotésis $q > (g+1)^4$, y de que el género del cuerpo de funciones sea invariante respecto a los cambios de cuerpos de constantes (ver 2.13).

Paso 3: Sea $z \in \operatorname{Ker}\lambda \setminus \{0\}$, luego $z(P) = 0 \ \ \forall P \in \mathcal{P}_F^1$.

Dado $f \in \mathscr{L} \subseteq \mathscr{L}(rQ)$, como Q es su único polo, se tiene que $f(P) \neq \infty$ para todo $P \in \mathcal{P}_F^1 \setminus \{Q\}$ (esto quiere decir que $f \in \mathcal{O}_P$). Luego, como $\deg P = 1$ se tiene que $f(P) \in \mathbb{F}_q \implies f(P)^q = f(P)$. Sea $z = \sum_i u_i z_i^{q_0} \in \operatorname{Ker}\lambda \setminus \{0\}$, luego:

$$\begin{aligned} z(P)^{q_0} &= \left(\sum_i u_i(P) z_i(P)^{q_0}\right)^{q_0} \\ &= \sum_i u_i(P)^{q_0} z_i(P)^q \\ &= \sum_i u_i(P)^{q_0} z_i(P) \\ &= (\lambda(z))(P) = 0 \end{aligned}$$

■

Notemos que al tener que $g(F) = g(F_r)$, este teorema implica que:

$$\forall r \geq 1 : \ N(F_r) \leq q^r + 1 + (2g+1)q^{r/2}$$

5.2. Cota inferior. Antes de probar la cota superior veremos un lema de teoría de grupos, y citaremos unas propiedades acerca de extensiones de cuerpos de funciones.

LEMA 2.37. *Sea G' grupo tal que $G' = \langle\sigma\rangle \times G$ con $\langle\sigma\rangle$ subgrupo cíclico de orden n y G subgrupo de orden m tal que $m \mid n$ (notemos que $\langle\sigma\rangle$ y G son subgrupos de G' viéndolos como $\langle\sigma\rangle \times \{1\}$ y $\{1\} \times G$ respectivamente). Sea $H < G'$ subgrupo tal que $|H| = ne$ y $|H \cap G| = e$, luego existen exactamente e subgrupos $U < H$ cíclicos de orden n tal que $U \cap G = \{1\}$.*

DEMOSTRACIÓN. Se hará el siguiente abuso de notación en esta prueba: si $r \in \mathbb{N}$ y $g \in G$, notamos $\sigma^r g := (\sigma^r, g) \in \langle\sigma\rangle \times G$; notemos entonces que $(\sigma^r g)^s = \sigma^{rs} g^s$ y $(\sigma^{r_1} g_1)(\sigma^{r_2} g_2) = (\sigma^{r_1+r_2})(g_1 g_2)$. Consideremos el homomorfismo $\varphi : G' \to G'$ tal que $\sigma^r g \mapsto \sigma^r$, luego $\operatorname{Ker}\varphi = G$ y por lo tanto $G \triangleleft G'$. Como $H < G'$ y $G \triangleleft G'$:

$$H/H \cap G \cong HG/G \implies \frac{ne}{e} = \frac{|HG|}{m} \implies |HG| = nm$$

Pero $|G'| = nm \implies G' = HG$, y luego $G'/G \cong \langle\sigma\rangle$, por lo tanto $H/H \cap G$ es un grupo cíclico de orden n. Consideremos $\lambda_0 \in H$ de orden n módulo $H \cap G$. Sea $a \in \mathbb{Z}$ y $\tau_0 \in G$ tal que $\lambda_0 = \sigma^a \tau_0$; notemos que a es coprimo a n, pues de lo contrario existe $1 \leq d < n$ tal que $n \mid ad \implies \lambda^d = \tau_0^d \in H \cap G$, lo que es absurdo ya que λ_0 módulo $H \cap G$ tiene orden n. Entonces existe t tal que $at \equiv 1 \pmod{n}$, por lo tanto $\lambda := \lambda_0^t = \sigma\tau$ con $\tau = \tau_0^t \in G$,

y al ser t coprimo a n, el orden de λ módulo $H \cap G$ es n. Sea $H \cap G = \{h_1, \dots, h_e\}$ y definimos $U_j = \langle \lambda h_j \rangle$ para $j = 1, \dots, e$. Notemos que los subgrupos $U_j \subseteq H$ son cíclicos de orden n, si $i \neq j$ se tiene que $U_i \neq U_j$ (basta notar que si $g_1, g_2 \in G$: $\sigma^r g_1 = \sigma^s g_2$ si y sólo si $r = s$ y $g_1 = g_2$) y $U_j \cap G = \{1\}$.

Sea $U \subseteq H$ subgrupo cíclico de orden n tal que $U \cap G = \{1\}$, y consideremos un generador de la forma σh (podemos hallarlo de la manera que se encontro λ a partir de λ_0). Como $\sigma h, \sigma\tau \in H$, luego:

$$(\sigma h)^{-1}(\sigma\tau) = h^{-1}\tau \in H \cap G$$

Sea h_i tal que $h^{-1}\tau = h_i \implies \tau = h \cdot h_i$, luego:

$$U = \langle \sigma\tau \rangle = \langle \sigma h h_i \rangle = \langle \lambda h_i \rangle = U_i$$

■

Consideremos E/L una extensión Galois donde E y L son cuerpos de funciones de $\mathbb{F}_q$ con cuerpo de constantes $\mathbb{F}_q$. Luego E/L es una extensión finita; sea $m = [E : L]$ y $n > 0$ tal que $m \mid n$, luego definimos $E' := E \cdot \mathbb{F}_{q^n}$. Notemos que como $E' = E(\mathbb{F}_{q^n})$ y $\mathbb{F}_{q^n}$ es una extensión finita de $\mathbb{F}_q$, luego E' es una extensión algebraica de E por un conjunto finito, por lo tanto la extensión es finita y $E'/\mathbb{F}_q$ es un cuerpo de funciones. Sea $\alpha \in \mathbb{F}_{q^n}$ tal que $E' = E(\alpha)$, luego:

$$[E' : E] = [E(\alpha) : E] = \deg \mathrm{Irr}_{E,\alpha}$$

donde $\mathrm{Irr}_{E,\alpha}$ es el polinomio irreducible de α sobre E. Como $\alpha \in \mathbb{F}_{q^n}$ y $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$, luego $\deg \mathrm{Irr}_{\mathbb{F}_q,\alpha} \leq n \implies \mathrm{Irr}_{E,\alpha} \mid \mathrm{Irr}_{\mathbb{F}_q,\alpha}$, por lo tanto $[E' : E] \leq n$. Tenemos entonces lo siguiente:

$$|\operatorname{Aut}(E'/E)| \leq [E' : E] \leq n$$

Para probar entonces que E'/E es Galois basta ver que $|\operatorname{Aut}(E'/E)| \geq n$. Sea $\sigma : E' \to E'$ tal que:

$$z \in E \mapsto z \quad \text{y} \quad \alpha \in \mathbb{F}_{q^n} \mapsto \alpha^q$$

Este mapa se extiende por linearidad, y esta bien definido ya que $E \cap \mathbb{F}_{q^n} = \mathbb{F}_q$, y los elementos de $\mathbb{F}_q$ quedan fijos por el morfismo elevar a la q. Es claro que σ es inyectivo, y luego es sobreyectivo (por el teorema de las dimensiones); entonces $\sigma \in \operatorname{Aut}(E'/E)$. Por lo tanto $\langle \sigma \rangle \subseteq \operatorname{Aut}(E'/E)$, pero como $|\sigma| = n$, luego $n \leq |\operatorname{Aut}(E'/E)|$. Concluimos entonces que E'/E es una extensión Galois de grado n y $\operatorname{Gal}(E'/E) = \langle \sigma \rangle$.

Nos interesa ahora ver que E'/L es una extensión Galois. Notemos lo siguiente:

$$|\operatorname{Aut}(E'/L)| \leq [E' : L] = [E' : E][E : L] = |\sigma||G|$$

con $G = \operatorname{Gal}(E/L)$. Sea $F : \langle \sigma \rangle \times G \to \operatorname{Aut}(E'/L)$ tal que $(\sigma^s, g) \mapsto r$ con $r : E' \to E'$ tal que:

$$z \in E \mapsto g(z) \quad \text{y} \quad \alpha \in \mathbb{F}_{q^n} \mapsto \alpha^{q^m}$$

Se puede ver que F es un homomorfismo inyectivo, y esto nos da la desigualdad:

$$|\sigma||G| \leq |\operatorname{Aut}(E'/L)|$$

Por lo que concluimos que $|\operatorname{Aut}(E'/L)| = |\sigma||G|$, y por lo tanto F es un isomorfismo, es decir, tenemos que:

$$G' := \operatorname{Gal}(E'/L) \cong \langle\sigma\rangle \times G = \operatorname{Gal}(E'/E) \times \operatorname{Gal}(E/L)$$

Podemos entonces aplicar el lema anterior con $G' = H$, esto nos dice que existen $U_1, \ldots, U_m \subseteq G'$ subgrupos cíclicos de orden n tal que $U_i \cap G = \{1\}$. Notemos que $\langle\sigma\rangle$ es uno de estos subgrupos, por lo que podemos suponer que $U_1 = \langle\sigma\rangle$. Consideremos $E_i := (E')^{U_i}$, es decir, los cuerpos fijos por U_i.

Finalmente veamos que si $L' = L \cdot \mathbb{F}_{q^n}$, luego E'/L' es Galois; notemos que como para E'/E se tiene que $[L' : L] = n$ y $\operatorname{Gal}(L'/L)$ es cíclico de orden n generado por un automorfismo $\sigma : L' \to L'$ tal que $z \in L \mapsto z$ y $\alpha \in \mathbb{F}_{q^n} \mapsto \alpha^q$. Primero se tiene la siguiente desigualdad:

$$|\operatorname{Aut}(E'/L')| \leq [E' : L'] = \frac{[E' : L]}{[L' : L]} = \frac{n|G|}{n} = |G|$$

Para probar que es Galois basta entonces definir un mapa inyectivo $\rho : G \to \operatorname{Aut}(E'/L')$, que por la desigualdad anterior, podremos ver que es un isomorfismo de grupos. Definimos ρ mediante $g \mapsto \rho_g$ con $\rho_g : E' \to E'$ tal que $z \in E \mapsto g(z)$ y $\alpha \in \mathbb{F}_{q^n}$; es claro que es un homomorfismo inyectivo, y por lo tanto un isomorfimso, por lo tanto E'/L' es Galois con $\operatorname{Gal}(E'/L') \cong G$.

Antes de terminar probar el lema principal, citamos dos proposiciones que se pueden encontrar en [ST].

Proposición 2.38. *En el contexto de lo presentado anteriormente, notamos $g(F)$ al género de un cuerpo de funciones y $N(F)$ la cantidad de lugares de grado 1. Se cumple:*

- *F_q es el cuerpo de constantes de E_i para todo $1 \leq i \leq m$*
- *$E' = E_i \cdot F_{q^n}$ y $g(E_i) = g(E)$ para todo $1 \leq i \leq m$.*
- *$m \cdot N(L) = \sum_{i=1}^{m} N(E_i)$.*

Proposición 2.39. *Sea K un cuerpo perfecto de característica positiva y F/K un cuerpo de funciones con cuerpo de constantes K. Luego existe $z \in F$ tal que $F/K(z)$ es una extensión finita y separable.*

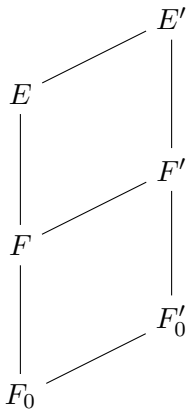
Ahora probaremos la cota inferior del lema prinicipal, así habiendo probado el análogo de la Hipótesis de Riemann y la cota de Hasse-Weil.

Teorema 2.40. *Sea $F/\mathbb{F}_q$ cuerpo de funciones de manera que $q > (g+1)^4$ y q es un cuadrado, luego existe $c_2 \in \mathbb{R}$ tal que:*

$$\forall r \geq 1 : \; N_r \geq q^r + 1 - c_2 q^{\frac{r}{2}}$$

Demostración. Por 2.39 existe $t \in F$ tal que $F_0 = \mathbb{F}_q(t)$ es una subextensión separable de F. Al ser F/F_0 una extensión finita y separable, su clausura Galois es finita; sea E clausura Galois, luego E es un cuerpo de funciones sobre $\mathbb{F}_q$. Sea $\mathbb{F}_{q^d}$ el cuerpo de constantes de $E/\mathbb{F}_q$; si $d \neq 1$ consideramos $F' = F\mathbb{F}_{q^d}$ y $F'_0 = F_0\mathbb{F}_{q^d} = \mathbb{F}_{q^d}(t)$, luego E/F'_0 es Galois; recordemos que por el lema 2.32 basta probar esta cota para $F/\mathbb{F}_{q^d}$. Suponemos entonces que el cuerpo de constantes de E es $\mathbb{F}_q$.

Sea $m := [E : F]$ y $n := [E : F_0]$, luego $m \mid n$. Consideremos $E' = E \cdot \mathbb{F}_{q^n}$, $F' = F \cdot \mathbb{F}_{q^n}$ y $F'_0 = F_0 \cdot \mathbb{F}_{q^n}$. Notemos que al ser E/F_0 Galois se tiene por lo visto anteriormente que las siguientes extensiones también son Galois: E'/F_0, E'/F'_0, E'/F y E'/F'. Tenemos entonces el siguiente diagrama de extensiones:



Además, los grupos de Galois de F'/F y F'_0/F_0 son cíclicos de orden n por lo visto previamente, digamos que $\mathrm{Gal}(F'/F) = \langle \sigma_1 \rangle$ y $\mathrm{Gal}(F'_0/F_0) = \langle \sigma_2 \rangle$, entonces:

$$\mathrm{Gal}(E'/F) \cong \langle \sigma_1 \rangle \times \mathrm{Gal}(E'/F') \quad \mathrm{y}\, \mathrm{Gal}(E'/F_0) \cong \langle \sigma_2 \rangle \times \mathrm{Gal}(E'/F'_0)$$

Podemos entonces aplicar entonces el lema 2.37 para los dos grupos anteriores, con $H = \mathrm{Gal}(E'/F)$ y $H = \mathrm{Gal}(E'/F_0)$ respectivamente; obtenemos entonces:

$$\exists! V_1, \ldots, V_m < \mathrm{Gal}(E'/F) \quad \text{cíclicos de orden } n\text{:} \quad \forall i = 1, \ldots, m : V_i \cap \mathrm{Gal}(E'/F') = \{1\}$$

y

$$\exists! U_1, \ldots, U_n < \mathrm{Gal}(E'/F_0) \quad \text{cíclicos de orden } n\text{:} \quad \forall i = 1, \ldots, n : U_i \cap \mathrm{Gal}(E'/F'_0) = \{1\}$$

Sea $\sigma \in V_i \cap \mathrm{Gal}(E'/F'_0)$, luego $\sigma \in V_i < \mathrm{Gal}(E'/F)$, por lo tanto σ deja fijo a los cuerpos F'_0 y F, luego deja fijo a $F'_0 \cdot F = F'$; sin embargo $V_i \cap \mathrm{Gal}(E'/F') = \{1\}$, por lo tanto $\sigma = 1$. Al tener entonces que $V_i \cap \mathrm{Gal}(E'/F'_0) = \{1\}$ y $V_i < \mathrm{Gal}(E'/F) < \mathrm{Gal}(E'/F'_0)$ se tiene que podemos reordenar los subgrupos $U_1, \ldots, U_n$ de manera que $V_i = U_i$ para $i = 1, \ldots, m$.

Sean $E_i := (E')^{U_i}$ los cuerpos fijos por U_i, luego por 2.38 se tiene que:

$$m \cdot N(F) = \sum_{i=1}^{m} N(E_i) \quad \mathrm{y} \quad n \cdot N(F_0) = \sum_{i=1}^{n} N(E_i)$$

Por otro lado, la cota superior de Hasse-Weil y que E_i, E tienen igual género por 2.38, nos dicen que:

$$\forall i : \; N(E_i) \leq q + 1 + (2g(E) + 1)q^{1/2}$$

Ahora, recordemos que $F_0 = \mathbb{F}_q(t)$, por lo tanto los lugares de grado 1 son fáciles de describir, pues se tratan de los lugares correspondientes a $t - \alpha$ para $\alpha \in \mathbb{F}_q$ y el lugar

correspondiente a $1/t$ (véase 1.16); luego $N(F_0) = q + 1$. Entonces:

$$\begin{aligned} n(q+1) = n \cdot N(F_0) &= \sum_{i=1}^{n} N(E_i) = \sum_{i=1}^{m} N(E_i) + \sum_{i=m+1}^{n} N(E_i) \\ &= m \cdot N(F) + \sum_{i=m+1}^{n} N(E_i) \\ &\leq m \cdot N(F) + (n-m)\left(q + 1 + (2g(E)+1)q^{1/2}\right) \end{aligned}$$

Luego:

$$\begin{aligned} m \cdot N(F) &\geq m(q+1) - (n-m)(2g(E)+1)q^{1/2} \\ \implies N(F) &\geq q + 1 - \frac{n-m}{m}(2g(E)+1)q^{1/2} \end{aligned}$$

Sea $c_2 = \frac{n-m}{m}(2g(E)+1)$, para concluir este teorema basta ver que c_2 es invariante bajo extensiones de cuerpos constantes, pero esto es claro, pues:

$$n = [E : F_0] = [E' : F'], \quad m = [E : F] = [E' : F'] \quad \text{y} \quad g(E) = g(E')$$

■

Concluimos entonces la prueba del lema principal, y por lo tanto del análogo de la Hipótesis de Riemann y de la cota de Hasse-Weil.

6. Ejemplos utilizando SAGE

En esta sección presentaremos dos curvas para las cuales calcularemos los correspondientes N_r para todo $1 \leq r \leq g$ utilizando SAGE, de esta manera podremos calcular el L-polinomio asociado y luego su función Z, es decir, dar su expresión racional. Habiendo calculado el L-polinomio, recordemos que los valores de los α_i son los inversos de las raices de L; en estos casos, trabajaremos con una curva de género 1 y una de género 2, por lo tanto como los L-polinomios tienen grado igual a 2 veces el género, es fácil hallar sus raices y luego los α_i. De tener curvas de género mayor o igual a 3, para hallar los α_i dependemos de la habilidad que tengamos para calcular raices de polinomios de grado mayor igual a 5; en general solo podremos obtener aproximaciones para los α_i, y por lo tanto también tendremos aproximaciones para los N_r. Sin embargo, notemos que poder hallar con exactitud los valores de N_r solo para curvas de género 1 y 2 no es poca cosa, pues las curvas de género 1 y 2 corresponden respectivamente a las curvas proyectivas lisas dadas por $y^2 = f(x)$ con $\deg f \in \{3, 4, 5, 6\}$. Si se tiene que una ecuación de menor grado, ya sea:

1. $y = f(x)$, $f(x) \in \mathbb{F}_q[x]$.
2. $y^2 = f(x)$, $f(x) \in \mathbb{F}_q[x]$ tal que $\deg f = 1, 2$.

Estas son isomorfas a $\mathbb{P}^1_{\mathbb{F}_q}$, y como el cuerpo de funciones de $\mathbb{P}^1_{\mathbb{F}_q}$ (visto como curva en $\mathbb{P}^2_{\mathbb{F}_q}$) es racional, luego ya sabemos que $Z_C(t) = 1/(1-t)(1-qt)$, por lo tanto sabemos que $N_r = q^r + 1$ para todo $r \geq 1$.

Antes de comenzar con los ejemplos mencionamos un resultado que nos permitirá hallar los coeficientes del L-polinomio de una curva a partir de saber la cantidad de puntos

proyectivos definidos en $\mathbb{F}_{q^i}$ para $1 \leq i \leq g$ (para $g = 1$ no lo utilizaremos, pues se sabe que $a_1 = N_1 - (q+1)$, pero para curvas de mayor grado si es necesario).

PROPOSICIÓN 2.41. *Sea $L(t) = \sum_{i=1}^{2g} a_i t^i$ el L-polinomio de $F/\mathbb{F}_q$. Definimos $S_r := N_r - (q^r + 1)$. Luego:*

$$ia_i = S_i a_0 + S_{i-1} a_1 + \ldots S_1 a_{i-1}$$

Recordemos que $a_{2g-i} = q^{g-i} a_i$ para $i = 0, \ldots, g$, $a_0 = 1$ y $a_{2g} = q^g$. Por lo tanto basta conocer $N_1, \ldots, N_g$ para obtener los coeficientes de L.

DEMOSTRACIÓN. Recordemos por 2.24 que $L(t) = \prod_{i=1}^{2g}(1 - \alpha_i t)$, y consideremos su derivada logarítmica:

$$\frac{L'(t)}{L(t)} = \sum_{i=1}^{2g} \frac{-\alpha_i}{1 - \alpha_i t}$$

y notemos que $\frac{1}{1-\alpha_i t} = \sum_{r=0}^{\infty}(\alpha_i t)^r$ para $|t| < \text{mín}\{|\alpha_i| : 1 \leq i \leq 2g\}$, por lo tanto:

$$\frac{L'(t)}{L(t)} = \sum_{i=1}^{2g}(-\alpha_i)\sum_{r=0}^{\infty}(\alpha_i t)^r = \sum_{r=0}^{\infty} t^r \left(\sum_{i=1}^{2g} -\alpha_i^{r+1}\right)$$

Como $N_r = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r \implies \sum_{i=1}^{2g} -\alpha_i^{r+1} = N_{r+1} - (q^{r+1} + 1) = S_{r+1}$. Por lo tanto:

$$L'(t) = L(t) \sum_{r=0}^{\infty} S_{r+1} t^r$$

Comparando coeficientes vemos que se cumple el resultado. ■

6.1. Curva de género 1. Consideremos la curva elíptica 83.a1, obtenida en [LMFDB] (L-functions and modular forms database), que tiene ecuación minimal $E : y^2 + xy + y = x^3 + x^2 + x$. Esta curva elíptica tiene discriminante -83, por lo tanto la curva tiene buena reducción, es decir, al reducirla módulo p, es una curva suave en todo primo $p \neq 83$. Tomemos $p = 163$, se puede calcular utilizando [SAGE] que la curva tiene 186 puntos definidos sobre $\mathbb{F}_p$, es decir, $N_1 = 186$. Sabemos que $a_0 = 1$, $a_1 = N_1 - (p+1) = 22$ y $a_2 = 163$, luego:

$$L(t) = 163t^2 + 22t + 1 \quad \text{y} \quad Z(t) = \frac{163t^2 + 22t + 1}{(1-t)(1-163t)}$$

Ahora hallamos las raices, y obtenemos que estas son:

$$\frac{-11 \pm i\sqrt{42}}{163}$$

Por lo tanto tomamos como α_1, α_2 a los inversos de estas raices:

$$\alpha_1 = \frac{163}{-11 + i\sqrt{42}} = -11 - i\sqrt{42} \quad \text{y} \quad \alpha_2 = \frac{163}{-11 - i\sqrt{42}} = -11 + i\sqrt{42}$$

Concluimos entonces que para esta curva:

$$N_r = 163^r + 1 - (-11 - i\sqrt{42})^r - (-11 + i\sqrt{42})^r$$

Sin embargo, notemos que el proceso hecho anteriormente se puede realizar para todo primo $p \neq 83$, pues la curva elíptica tiene buena reducción módulo estos primos.

Dado un primo $p \neq 83$ notamos $a_p := p + 1 - N_1$, luego se puede calcular nuevamente utilizando SAGE:

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53
a_p	-1	-1	-2	-3	3	-6	5	2	-4	-7	5	-11	-2	-8	0	6

Sin embargo, para $p = 83$ también se puede hallar la cantidad de puntos proyectivos, en este caso será 85, por lo que podemos definir $a_{83} = 85-83-1 = 1$. Es más, en general se puede probar que dada una curva elíptica E y un primo p de mala reducción:

- Si la reducción es multiplicativa split:

$$\#E(\mathbb{F}_{p^r}) = N_r = p^r + 1^r - 1^r = p^r \implies a_p = 1$$

- Si la reducción es multiplicativa no split:

$$\#E(\mathbb{F}_{p^r}) = N_r = p^r + 1^r - (-1)^r \implies a_p = -1$$

- Si la reducción es aditiva:

$$\#E(\mathbb{F}_{p^r}) = N_r = p^r + 1^r - 0^r = p^r + 1 \implies a_p = 0$$

Esto se parece mucho a las fórmulas que hallamos para curvas lisas, sin embargo los "α_i" en este caso no tienen valor absoluto $p^{1/2}$, ni hay una cantidad $2g$ de estos. Además esto nos dice que $|a_p| = |N_1 - p - 1| \leq 1$ si p es de mala reducción, de lo contrario la cota de Hasse-Weil nos dice que $|a_p| \leq 2\sqrt{p}$. No ahondaremos en los detalles de los tipos de reducciones, pero es interesante notar lo que sucede en dichos casos. Recordemos que la función Z_E de la curva elíptica E la definimos viendo la curva en un cuerpo finito, pero como ahora podemos definir E en $\mathbb{F}_p$ para todo primo p (por más que haya mala reducción, es decir, no sea lisa en $\mathbb{F}_{83}$), notaremos:

$$Z_{E,p}(t) = \exp\left(\sum_{m=1}^{\infty} \#E(\mathbb{F}_{p^m})\frac{t^m}{m}\right)$$

y:

$$L_{E,p} = (1-t)(1-pt)Z_{E,p}(t)$$

Utilizando esto, y las fórmulas para las cantidades de puntos para curvas elípticas sobre primos de mala reducción se obtiene:

- Si la reducción de E en p es multiplicativa split:

$$Z_{E,p}(t) = \frac{1-t}{(1-t)(1-pt)} \implies L_{E,p}(t) = 1 - t$$

- Si la reducción de E en p es multiplicativa no split:

$$Z_{E,p}(t) = \frac{1+t}{(1-t)(1-pt)} \implies L_{E,p}(t) = 1 + t$$

- Si la reducción de E en p es aditiva:

$$Z_{E,p}(t) = \frac{1}{(1-t)(1-pt)} \implies L_{E,p}(t) = 1$$

Se puede ver que en estos casos se tiene la regla general $L_{E,p}(t) = 1 - a_p t$. En caso que E tenga buena reducción en p, sabemos que:

$$L_{E,p}(t) = 1 - a_p t + pt^2$$

Se puede definir entonces la L-serie asociada a la curva elíptica E como:

$$L_E(s) = \prod_p L_{E,p}(p^{-s})^{-1}$$

la cual converge para $\Re(s) > \frac{3}{2}$, esto se puede probar utilizando que $|a_p| \leq 2\sqrt{p}$. El Teorema de Modularidad, del cual hablamos en la introducción, está relacionado a L_E, y dice que existe una forma modular nueva de peso 2, llamemosla f tal que:

$$L_E(s) = L_f(s)$$

Esto se puede usar para probar un caso de una conjetura que enunciaremos ahora. Definimos la funcion Λ_E asociada a E como:

$$\Lambda_E(s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L_E(s)$$

El valor N es el conductor de la curva elíptica.

CONJETURA 2.42 (Hasse-Weil). *Sea E una curva elíptica sobre un cuerpo de números K. Se tiene que $\Lambda_E(s)$ admite una continuación analítica para todo el plano complejo, y satisface la ecuación funcional:*

$$\Lambda_E(s) = \pm\Lambda_E(2 - s)$$

Esta conjetura fue probada para $K = \mathbb{Q}$ gracias al Teorema de Modularidad, y por lo tanto la prueba es indirecta. En esta se comprueba la conjetura ya que las L-series asociadas a formas modulares satisfacen las propiedades anteriores.

6.2. Curva de género 2 (de tipo GL_2). Consideramos la curva hiperelíptica 169.a.169.1 obtenida en [LMFDB], con ecuación $H : y^2 + (x^3 + x + 1)y = x^5 + x^4$. Esta curva tiene discriminante -13^2, por lo tanto tiene buena reducción para todo primo $p \neq 13$. Tomemos $p = 73$, se puede calcular utilizando [SAGE] que $N_1 = 74$ y $N_2 = 5044$. Sabemos que $a_0 = 1$, $a_1 = 73 + 1 - 74 = 0$ y $a_4 = 73^2$; como $a_{2g-i} = p^{g-i}a_i$, luego $a_3 = 73a_1 = 0$. Aplicando 2.41 hallamos a_2:

$$2a_2 = S_2a_0 + S_1a_1 = S_2 = 5044 - (73^2 + 1) = -286 \implies a_2 = -143$$

Luego:

$$L(t) = 73^2t^4 - 143t^2 + 1 \quad \text{y} \quad Z(t) = \frac{73^2t^4 - 143t^2 + 1}{(1 - t)(1 - 73t)}$$

Se puede partir L como:

$$L(t) = (73t^2 + 17t + 1)(73t^2 - 17t + 1)$$

Entonces las raices son:

$$\frac{-17 \pm i\sqrt{3}}{2 \cdot 73} \quad \text{y} \quad \frac{17 \pm i\sqrt{3}}{2 \cdot 73}$$

Calculando los inversos tenemos:

$$\alpha_1 = \frac{-17 - i\sqrt{3}}{2},\ \alpha_2 = \frac{-17 + i\sqrt{3}}{2}$$

$$\alpha_3 = \frac{17 + i\sqrt{3}}{2} \text{ y } \alpha_4 = \frac{17 - i\sqrt{3}}{2}$$

Por lo tanto concluimos que:

$$N_r = 73^r + 1 - \frac{1}{2^r}\left((-17 - i\sqrt{3})^r + (-17 + i\sqrt{3})^r + (17 - i\sqrt{3})^r + (17 + i\sqrt{3})^r\right)$$

Mediante un proceso similar al hecho con la curva elíptica, se puede definir la L-serie L_H asociada a H, y resulta que esta curva hiperelíptica es de tipo GL_2, esto quiere decir, existe una forma modular nueva de peso 2 tal que $L_H = L_f$. Por más que esta curva hiperelíptica sea de tipo GL_2, existen otras que no lo son, como lo es la siguiente.

6.3. Curva de género 2 (no tipo GL_2). Consideramos la curva hiperelíptica 249.a.249.1 obtenida en [LMFDB], con ecuación $H : y^2 + (x^3 + 1)y = x^2 + x$. Esta curva tiene discriminante $249 = 3 \cdot 83$, por lo tanto tiene buena reducción para todo primo $p \neq 3, 83$. Tomemos $p = 101$, se puede calcular utilizando [SAGE] que $N_1 = 81$ y $N_2 = 10329$. Sabemos que $a_0 = 1$, $a_1 = 81 + 1 - 101 = -19$ y $a_4 = 101^2$; como $a_{2g-i} = p^{g-i}a_i$, luego $a_3 = 73a_1 = -1387$. Aplicando 2.41 hallamos a_2:

$$2a_2 = S_2a_0 + S_1a_1 = (10329 - 101^2 - 1) + 19^2 = 488 \implies a_2 = 244$$

Luego:

$$L(t) = 101^2t^4 - 1387t^3 + 244t^2 - 19t + 1 \quad \text{y} \quad Z(t) = \frac{101^2t^4 - 1387t^3 + 244t^2 - 19t + 1}{(1 - t)(1 - 101t)}$$

Este L polinomio no es bicuadrático como en el anterior ejemplo, lo que complica un poco determinar sus raices exactas. En SAGE se puede hallar las expresiones algebraicas exactas de las raices, sin embargo estas son demasiado complicadas como para trabajar con ellas y encontrarles algun sentido. Por esta razón damos aproximaciones numéricas de estas raices:

$0{,}010375 - 0{,}121984i$, $0{,}010375 + 0{,}121984i$, $0{,}057608 - 0{,}056762i$ y $0{,}057608 + 0{,}056762i$

Viendo este problema encontrado para esta curva hiperelíptica que no es de tipo GL_2, esto puede sugerir que aquellas curvas que si son de GL_2 tienen L-polinomios que se pueden factorizar de maneras más sencillas, o tal vez tiendan a ser bicuadráticos.

Bibliografía

[LP] Bernstein et al. *An Introduction to the Langlands Program*. Springer Publishing Company, Incorporated, 2004. ISBN: 0817632115.

[BK] Bruno Kahn. *Zeta and L-Functions of Varieties and Motives*. London Mathematical Society Lecture Note Series. Cambridge University Press, 2020.

[LMFDB] The LMFDB Collaboration. *The L-functions and modular forms database*. `https://www.lmfdb.org`. [Online; accessed 30 March 2025]. 2025.

[SAGE] W. A. Stein et al. *Sage Mathematics Software*. `http://www.sagemath.org`. The Sage Development Team, 2025.

[ST] Henning Stichtenoth. *Algebraic Function Fields and Codes*. 2nd. Springer Publishing Company, Incorporated, 2008. ISBN: 3540768777.

[FV] Felipe Voloch. *Lecture notes in Topics in Algebra, Equations over finite fields*. `https://web.ma.utexas.edu/users/voloch/Preprints/finitefieldnotes.pdf`. 2001.