34

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

CAMPOS DE FUNCIONES Y CURVAS SOBRE CAMPOS FINITOS CON UN GRAN NUMERO DE PUNTOS RACIONALES

T E S I S

QUE PARA OBTENER EL TITULO DE:

M A T E M A T I C O

P R E S E N T A :

OCTAVIO PANIAGUA TABOADA

DIRECTOR DE TESIS: DR. HERBERT KANAREK BLANDO

FACULTAD DE CIENCIAS
UNAM

2002

FACULTAD DE CIENCIAS
SECCION ESCOLAR

Autorizo a la Dirección General de Bib
UNAM a difundir en formato electrónic
contenido de mi trabajo recep
NOMBRE: Octavio Paniagua
Taboada
FECHA: 15/VIII/2002
FIRMA:

M. EN C. ELENA DE OTEYZA DE OTEYZA
Jefa de la División de Estudios Profesionales de la
Facultad de Ciencias
Presente

Comunico a usted que hemos revisado el trabajo escrito:
Campos de funciones y curvas sobre campos finitos con un gran número de puntos racionales.

realizado por Paniagua Taboada Octavio

con número de cuenta 9561474-0 , quién cubrió los créditos de la carrera de: Matemáticas

Dicho trabajo cuenta con nuestro voto aprobatorio.

Atentamente

Director de Tesis Propietario	Dr. Herbert Kanarek Blando	H Kanarek
Propietario	Dr. Enrique Javier Elizondo Huerta	
Propietario	Dr. Alberto León Kushner Schnur	
Suplente	Dr. Pedro Luis del Angel Rodríguez	
Suplente	Dr. Francisco Marmolejo Rivas	

Consejo Departamental de

M. en C. José Antonio Gómez Ortega

FACULTAD DE CIENCIAS
CONSEJO DEPARTAMENTAL
DE
MATEMATICAS

Campos de funciones y curvas con un gran número de puntos racionales

Octavio Paniagua Taboada
Facultad de Ciencias, UNAM

septiembre de 2002

A Alina

Agradecimientos

Al doctor Herbert Kanarek, por haber dirigido esta tesis y a los doctores Javier Elizondo, León Kushner, Francisco Marmolejo y Pedro Luis del Ángel por sus valiosos comentarios y críticas al presente trabajo.

A mis padres Rolando y Sonia, por aguantarme tanto tiempo y apoyarme incondicionalmente.

A mis hermanos Alberto y Ricardo por ser un ejemplo a seguir durante toda mi vida. Los quiero mucho a los desgraciados. A mi cuñada Malena, flamante integrante de esta familia.

Especialmente a mi abuelita Cristina y a la memoria de mis demás abuelitos, donde quiera que se encuentren.

A todos mis tíos, tías, primos y primas.

A todos aquellos profesores que me participaron en mi formación sobretodo a Luis Colavita, Javier Páez, Javier Elizondo y León Kushner.

A todos mis amigos y compañeros, Óscar, Pepe, Paquito, Ana, Ivette, Mitolito, Manuel, Paloma, Sandra, Alexei, Zinnya, Héctor, Lourdes, Ale M., Ale Canela, Pablo, Monks, Ileana, Javier, Omar, Cruz, el barbas, el flaquito, Ara, Sael, Edgar, Pancho, Lalo, Era, Paulo, Selene, Paula... junto con mis amigos de generación Camille, Galo, Pablo, todos los demas hijos de Páez y todos aquellos que se me olvidó mencionar.

A la fundación Alberto y Dolores Andrade por su apoyo constante durante toda mi formación académica.

Índice General

Introducción

En el presente trabajo se analiza el artículo *A construction of curves over finite fields* de Luciane Quoos y Arnaldo García publicado en Acta Arithmetica (2001). El principal tema de estudio son cierto tipo de variedades algebraicas: curvas irreducibles $\mathcal{X}$, no singulares, proyectivas de género g sobre un campo finito $\mathbb{F}_q$ y su relación con los campos de grado de trascendencia uno sobre un campo K.

La teoría de ecuaciones diofantinas es una rama de la teoría de números que trata de la solución de ecuaciones polinomiales en números enteros o racionales. Esta área se llama así en honor de Diophantus de Alejandría, quien formuló y resolvió una gran cantidad de problemas. Un ejemplo muy conocido de ecuaciones diofantinas es la famosa curva de Fermat

$$X^n + Y^n = Z^n$$

Probablemente el más famoso de los teoremas de Fermat establece que para $n \geq 3$ esta ecuación no posee soluciones enteras no triviales. La teoría de ecuaciones sobre campos finitos es un tópico clásico de la teoría de números. En esta teoría las congruencias de la forma

$$y^2 \equiv f(x) \pmod{p \text{ un primo}}$$

donde $f(x)$ es un polinomio o un cociente de polinomios con coeficientes enteros, era uno de los principales objetos de estudio. E. Artin conjeturó una cota superior para el numero N de soluciones de tales congruencias.

Posteriormente un celebrado y famoso teorema de A. Weil demuestró, en particular, la conjetura de Artin y dice lo siguiente: *si $\mathcal{X}$ es una curva algebraica proyectiva, no singular, irreducible, de género g sobre F_q, entonces el número N de puntos F_q racionales satisface lo siguiente*

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

El interés en curvas sobre campos finitos con muchos puntos racionales fue renovado después de que Goppa construyó códigos lineales sobre dichas curvas. El objetivo de este trabajo es presentar con detalle los resultados de

este artículo, así como toda la teoría subyacente de campos de funciones y trabajar algunos de los ejemplos que se construyen en dicho artículo.

La teoría de los campos de funciones ocupa el papel principal en esta tesis. En este sentido teoremas como el de Riemann-Roch y de Hasse-Weil (en campos finitos), poseen una belleza a todas luces atrayente y tienen implicaciones fundamentales en la teoría de números y la geometría algebraica. Espero que el lector disfrute estos resultados como yo lo hice al revisar este material.

Octavio Paniagua

Capítulo 1

Preliminares

1.1 Principios de la teoría de los campos de funciones algebraicas

Definición 1.1.1. Un campo de funciones algebraicas F/K de una variable sobre K es una extensión de campos F/K tal que F es una extensión algebraica finita de $K(x)$ para algún elemento $x \in F$, el cual es trascendente sobre K.

El ejemplo más sencillo de campo de funciones es el el campo de funciones racional; F/K es llamado *racional* si $F = K(x)$ para algún $x \in F$ trascendente sobre K. Cualquier elemento $z \in K(x)\backslash\{0\}$ posee una única representación de la forma

$$z = a \prod_i p_i(x)^{n_i}$$

en la cual a es un elemento de K distinto de cero, los $p_i(x) \in K[x]$ son polinomios irreducibles, no asociados y mónicos, $n_i \in \mathbb{Z}$.

Un campo arbitrario de funciones F/K (el cual no es necesariamente racional) puede representarse como una extensión algebraica simple de un campo de funciones racional $K(x)$, i.e. $F = K(x, y)$ donde $g(y) = 0$ para algún polinomio irreducible $g(T) \in K(x)[T]$.

Observación 1.1.2. Los elementos de F que son trascendentes sobre K pueden ser caracterizados de la siguiente manera: $z \in F$ es trascendente sobre K si y sólo si $[F : K(z)] < \infty$. En efecto, si z es trascedente sobre K, entonces la extensión $K(x)(z)/K(z)$ debe de ser algebraica, pues en caso contrario la extensión F/K tendría grado de trascendencia dos, lo cual es imposible por la definición de F; luego $[F : K(z)] = [F : K(x)(z)][K(x)(z) : K(z)] < \infty$. La otra implicación es clara.

1.2 Anillos de valuación

Definición 1.2.1. Un anillo de valuación del campo de funciones F/K es un anillo $\mathcal{O} \subset F$ con las siguientes propiedades:

1. $K \subsetneq \mathcal{O} \subsetneq F$ y
2. Para todo $z \in F$, $z \in \mathcal{O}$ o $z^{-1} \in \mathcal{O}$

La defincón anterior está motivada por la observación de que en el caso del campo de funciones racional $K(x)$, dado un polinomio irreducible $p(x) \in K[x]$, la localización con respecto al ideal primo generado por $p(x)$, es un anillo de valuación:

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

Es inmediato verificar que $\mathcal{O}_{p(x)}$ es un anillo de valuación de $K(x)/K$.

Definimos además el conjunto

$$\hat{K} := \{z \in F \mid z \quad \text{es algebraico sobre } K\}$$

que llamaremos la *cerradura algebraica* de K *en* F. Al campo $\hat{K}$ le llamaremos el *campo de constantes* de F. En el caso $\hat{K} = K$ diremos que K es el *campo pleno de constantes* o *todo el campo de constantes.*

Proposición 1.2.2. *Sea $\mathcal{O}$ un anillo de valuación del campo de funciones F/K, entonces*

1. *$\mathcal{O}$ es un anillo local, con ideal máximo $P := \mathcal{O} \backslash \mathcal{O}^*$, donde $\mathcal{O}^*$ denota las unidades de $\mathcal{O}$.*
2. *Para $0 \neq x \in F$, $x \in P$ si y sólo si $x^{-1} \notin \mathcal{O}$.*
3. *En el caso del campo de constantes $\hat{K}$ de F/K tenemos $\hat{K} \subseteq \mathcal{O}$ y además $\hat{K} \cap P = 0$.*

Demostración. (1) Es suficiente demostrar que P es un ideal, pues su complemento son unidades y esto implica que P en un ideal máximo y $\mathcal{O}$ es un anillo local. Veamos que P es un ideal de $\mathcal{O}$. Sea $x \in P$, $z \in \mathcal{O}$. Entonces $xz \notin \mathcal{O}^*$, de lo contrario x sería una unidad. Sean ahora $x, y \in P$. Sin pérdida de generalidad supongamos que $x\,y^{-1} \in \mathcal{O}$. Entonces $1 + x\,y^{-1} \in \mathcal{O}$ y $x + y = y(1 + x\,y^{-1}) \in P$. Por lo tanto P es un ideal de $\mathcal{O}$.

(2) Se sigue inmediatamente de la definición.

(3) Tomemos $z \in \hat{K}$. Supongamos que $z \notin \mathcal{O}$. Entonces debe ocurrir que $z^{-1} \in \mathcal{O}$ el cual es también algebraico sobre K. Por lo tanto existen

elementos $a_1, \ldots, a_s \in K$ tales que $a_s(z^{-1})^s + \cdots + a_1 z^{-1} + 1 = 0$, de manera que $z^{-1}(a_r(z^{-1})^{s-1} + \cdots + a_1) = -1$. Por lo tanto $z = -(a_r(z^{-1})^{s-1} + \cdots + a_1) \in K[z^{-1}] \subseteq \mathcal{O}$, por lo tanto $z \in \mathcal{O}$. La afirmación $K \cap P = 0$ es clara. □

Lema 1.2.3. *Sea $\mathcal{O}$ un anillo de valuación del campo de funciones F/K, P su ideal máximo y $0 \neq x \in P$. Sean $x_1, \ldots, x_n \in P$ tales que $x_1 = x$ y $x_i \in x_{i+1}P$ para $i = 1, \ldots, n-1$. Entonces $n \leq [F : K(x)] < \infty$.*

Demostración. De la observación 1.1.2 y la proposición 1.2.2 se sigue que $[F : K(x)] < \infty$, por lo que es suficiente probar que $x_1, \ldots, x_n$ son linealmente independientes sobre $K(x)$. Supongamos que existe una combinación lineal no trivial $\sum_{i=i}^{n} h_i x_i = 0$, con $h_i \in K[x]$. Es claro que podemos suponer que los $h_i \in K[x]$ y además que x no divide a todos los h_i. Definamos $a_i = h_i(0)$, es decir el término constante y ahora vamos a definir un índice $j \in \{1, \ldots, n\}$ con la condición $a_j \neq 0$ pero $a_i = 0$ para todo $i > j$. Obtenemos entonces

$$-h_j x_j = \sum_{i \neq j} h_i x_i$$

con $h_i \in \mathcal{O}$ para $1 \leq i \leq n$ (pues $x = x_1 \in P$), $x_i \in x_j P$ para $i < j$ y $h_i = x\, g_i$ para $i > j$ donde g_i es un polinomio en x. Si dividimos la igualdad anterior por x_j obtenemos

$$-h_j = \sum_{i<j} h_i \frac{x_i}{x_j} + \sum_{i>j} \frac{x}{x_j} g_i x_i$$

Todos los sumandos de la derecha pertenecen a P, por lo tanto $h_j \in P$. Por otra parte, $h_j = a_j + x g_j$ con $g_j \in K[x] \subseteq \mathcal{O}$ y $x \in P$, por lo tanto $a_j = h_j - x g_j \in P \cap K$. Como $a_j \neq 0$, tenemos una contradicción a la proposición 1.2.2. □

Proposición 1.2.4. *Sea $\mathcal{O}$ un anillo de valuación del campo de funciones F/K y P su ideal máximo. Entonces*

1. *P es un ideal principal.*

2. *Si $P = t\mathcal{O}$ entonces todo $0 \neq z \in F$ tiene una representación única de la forma $z = t^n u$ para alguna $n \in \mathbb{Z}$, $u \in \mathcal{O}^*$.*

3. *$\mathcal{O}$ es un dominio de ideales principales. Más aún, si $P = t\mathcal{O}$ y $\{0\} \neq I \subseteq \mathcal{O}$ es un ideal, entonces $I = t^n\mathcal{O}$ para alguna $n \in \mathbb{N}$, es decir. I es una potencia de P.*
   Un anillo con las propiedades arriba descritas es llamado anillo de valuación discreta.

Demostración. (1) Supongamos que P no es principal y escojamos un elemento $0 \neq x_1 \in P$. Dado que $P \neq \mathcal{O}x_1$ existe un elemento $x_2 \in P \backslash \mathcal{O}x_1$. Entonces $x_2 x_1^{-1} \notin \mathcal{O}$, por lo tanto $x_2^{-1} x_1 \in P$, por lo que $x_1 \in x_2 P$. Por recursión obtenemos una sucesión infinita de elementos $x_1, x_2, x_3, \cdots \in P$ tales que $x_i \in x_{i+1}P$ para todo $i \geq 1$, lo cual es una contradicción al lema 1.2.3.

(2) La unicidad de la representación $z = t^n u$ con $u \in \mathcal{O}^*$ es clara. Sólo debemos probar la existencia. Como z ó $z^{-1} \in \mathcal{O}$ supongamos que $z \in \mathcal{O}$. Si $z \in \mathcal{O}^*$ entonces $z = t^0 z$. Supongamos ahora que $z \in P$. Entonces existe una m máxima ($m \geq 1$) tal que $z \in t^m \mathcal{O}$, pues la longitud de la sucesión

$$x_1 = z, \quad x_2 = t^{m-1}, \quad x_3 = t^{m-2}, \ldots, x_m = t$$

es acotada por el lema 1.2.3. Escribimos entonces $z = t^m u$ con $u \in \mathcal{O}^*$, u debe ser unidad, de lo contrario se contradice la maximalidad de m.

(3) Sea $\{0\} \neq I \subsetneq \mathcal{O}$ un ideal. El conjunto $B := \{k \in \mathbb{N} \mid t^k \in I\}$ es no vacío (de hecho si $0 \neq x \in I$ entonces $x = t^k u$ con $u \in \mathcal{O}^*$ y $t^k = xu^{-1} \in I$). Sea $n = \text{mín}(B)$. Entonces afirmamos que $I = t^n \mathcal{O}$. La inclusión $t^n \mathcal{O} \subseteq I$ es clara, pues $t^n \in I$. Sea ahora $0 \neq y \in I$. Entonces $y = t^s w$ con $w \in \mathcal{O}^*$, por lo tanto $s \geq 0$, $t^s \in I$ y $s \geq n$. Por lo tanto $y = t^n t^{s-n} w \in t^n \mathcal{O}$. □

Definición 1.2.5. Sea F/K un campo de funciones.

1. Un *lugar* P del campo de funciones F/K es el ideal máximo de algún anillo de valuación $\mathcal{O}$ de F/K. Cualquier elemento $t \in P$ tal que $P = t\mathcal{O}$ es llamado elemento primo o parámetro local para P.

2. $\mathbb{P}_F := \{ P \mid P \text{ es un lugar de } F/K \}$.

Si $\mathcal{O}$ es un anillo de valuación de F/K y P su ideal máximo, entonces es claro que $\mathcal{O}$ está determinado de forma única por P, esto es $\mathcal{O} = \{ z \in F \mid z^{-1} \notin P \}$. De modo que llamaremos $\mathcal{O}_P := \mathcal{O}$ *el anillo de valuación* del lugar P. Existe otra forma útil de describir a los lugares en términos de valuaciones.

Definición 1.2.6. *Una valuación discreta* de F/K es una función $v : F \to \mathbb{Z} \cup \{\infty\}$ que satisface las siguientes propiedades:

1. $v(x) = \infty$ si y sólo si $x = 0$.

2. $v(xy) = v(x) + v(y)$ para todo $x, y \in F$.

3. $v(x + y) \geq \text{mín } \{v(x), v(y)\}$ para todo $x, y \in F$.

4. Existe un elemento $z \in F$ con $v(z) = 1$.

5. $v(a) = 0$ para cualquier $0 \neq a \in K$.

Para el símbolo ∞ definiremos las siguientes operaciones: $\infty + \infty = \infty + n = n + \infty = \infty$ e $\infty > m$ para toda $m, n \in \mathbb{Z}$. De (1), (2) y (4) es inmediato que esta función es suprayectiva. La propiedad (3) es llamada la desigualdad del triángulo. Una versión más fuerte de esta desigualdad puede ser demostrada:

Lema 1.2.7 (Desigualdad estricta del triángulo). *Sea v una valuación discreta de F/K y $x, y \in F$ tales que $v(x) \neq v(y)$. Entonces $v(x+y) = \min\{v(x), v(y)\}$.*

Demostración. Notemos primeramente que para todo $0 \neq a \in K$ tenemos $v(ax) = v(x)$. En particular $v(x) = v(-x)$. Dado que $v(x) \neq v(y)$, supongamos sin pérdida de generalidad que $v(x) < v(y)$. Si $v(x+y) \neq \min\{v(x), v(y)\}$, entonces $v(x+y) > v(x)$ por una parte, pero $v(x) = v((x+y)-y) \geq \min\{v(x+y), v(y)\} > v(x)$, lo cual es una contradicción. □

Ahora es posible asociar valuaciones a los ideales $P \in \mathbb{P}_F$.

Observación 1.2.8. A cualquier lugar P le asociamos una función $v_P : F \to \mathbb{Z} \cup \{\infty\}$ la cual resultará ser una valuación discreta de F/K: sea t un elemento primo para P. Entonces como ya sabemos todo $0 \neq z \in F$ tiene una representación única de la forma $z = t^n u$, con $u \in \mathcal{O}^*$ y $n \in \mathbb{Z}$. Definimos $v_P(z) := n$ y $v_P(0) := \infty$. La definición tiene sentido dado que depende únicamente en P, no en la elección del elemento primo t. Si t' es otro elemento primo para P entonces $P = t\mathcal{O} = t'\mathcal{O}$, de manera que $t = t'w$ para alguna $w \in \mathcal{O}^*$. Entonces $t^n u = (t'^n w^n)u = t'^n(w^n u)$ con $w^n u \in \mathcal{O}_P^*$ y es claro que v_P cumple con las propiedades de una valuación discreta.

Teorema 1.2.9. *Sea F/K un campo de funciones algebraicas.*

1. *Para cualquier lugar $P \in \mathbb{P}_F$, la funcion v_p definida anteriormente es una valuación discreta de F/K. Más aún tenemos lo siguiente:*

$$\mathcal{O}_P = \{z \in F \mid v_P(z) \geq 0\},$$
$$\mathcal{O}_P^* = \{z \in F \mid v_P(z) = 0\}$$
$$P = \{z \in F \mid v_P(z) > 0\}.$$

   Un elemento $x \in F$ es un elemento primo para P si y sólo si $v_P(x) = 1$.

2. *Recíprocamente, supongamos que v es una valuación discreta de F/K. Entonces el conjunto $P := \{z \in F \mid v(z) > 0\}$ es un lugar de F/K, y $\mathcal{O}_P = \{z \in F \mid v(z) \geq 0\}$ es el correspondiente anillo de valuación.*

3. *Todo anillo de valuación $\mathcal{O}$ de F/K es un subanillo propio y máximo de F.*

Demostración. Es claro que v_P posee las propiedades (1), (2), (4) y (5) de la definición 5. Sólo nos resta probar la desigualdad del triángulo. Para esto consideremos $x, y \in F$ con $v_P(x) = n$, $v_P(y) = m$. Sin pérdida de generalidad supongamos que $n \leq m < \infty$, entonces $x = t^n u_1$ y $y = t^m u_2$, con $u_1, u_2 \in \mathcal{O}^*$. Entonces $x + y = t^n(u_1 + t^{m-n}u_2) = t^n z$ con $z \in \mathcal{O}_P$. Si $z = 0$ entonces $v_P(x+y) = \infty > \text{mín}\{n, m\}$. En otro caso $z = t^k u$, con $k \geq 0$ y $u \in \mathcal{O}^*$. De manera que

$$v_P(x+y) = v_P(t^{n+k}u) = n + k \geq n = \text{ mín } \{v_P(x), v_P(y)\}$$

Las demás propiedades son claras así como (2). Veamos (3). Sea $\mathcal{O}$ un anillo de valuación de F/K, P su ideal máximo, v_P la valuación discreta asociada a P y $z \in F \backslash \mathcal{O}$. Mostraremos que $F = \mathcal{O}[z]$. Sea y un elemento arbitrario no cero de F. Entonces $v_P(yz^{-k}) \geq 0$ para k suficientemente grande. De modo que $w := yz^{-k} \in \mathcal{O}$ y $y = wz^k \in \mathcal{O}[z]$. □

Si consideramos ahora P un lugar de F/K y $\mathcal{O}_P$ su anillo de valuación, el anillo cociente $\mathcal{O}_P/P$ es un campo, dado que P es un ideal máximo. Por otra parte, también sabemos que $K \subseteq \mathcal{O}_P$ y $K \cap P = \{0\}$, de manera que existe de forma natural una inclusión canónica de K en $\mathcal{O}_P/P$. Pero este argumento también se aplica a $\hat{K}$, por lo que podemos considerar a $\hat{K}$ como un subcampo de $\mathcal{O}_P/P$ también.

El teorema anterior nos dice que valuaciones discretas y anillos de valuación de un campo de funciones, en esencia, nos dan la misma información. Ahora, en el campo $\mathcal{O}_P/P$ denotaremos para un elemento $x \in \mathcal{O}_P$ su clase módulo P por $x(P)$ y para un elemento $x \in F \backslash \mathcal{O}_P$ definimos su clase módulo P por $x(P) = \infty$ (notemos que el símbolo ∞ tiene otro sentido diferente que en la definición de valuación discreta). Esto nos lleva a la siguiente definición.

Definición 1.2.10. Sea $P \in \mathbb{P}_F$.

1. $F_P := \mathcal{O}_P/P$ es el campo de clases residuales de P. La aplicación $\phi : F \to F_P \cup \{\infty\}$ tal que $x \mapsto x(P)$ es llamado la aplicación de clases residuales con respecto a P.

2. $deg\, P := [F_P : K]$ es llamado el *grado* de P.

Cuando $deg\, P = 1$ tenemos que $F_P = K$. El grado de un lugar siempre es finito, como se prueba en la siguiente proposición. En particular si K es algebraicamente cerrado, todo lugar tiene grado 1 y podemos pensar a cada elemento $x \in F$ como una función

$$x : \mathbb{P}_F \to K \cup \{\infty\}$$

$$P \mapsto x(P)$$

Por esta razón a F/K se le llama campo de funciones. Los elementos de K interpretados como funciones, son constantes. A K se le llama el campo de constantes de F/K. A continuación establecemos una cota para el grado de P.

Proposición 1.2.11. *Si P es un lugar de F/K y $0 \neq x \in P$ entonces*

$$deg\, P \leq [F : K(x)] < \infty$$

Demostración. Notemos que $[F : K(x)] < \infty$ por la observación 1.1.2. Entonces es suficiente mostrar que cualesquiera elementos $z_1, \ldots, z_n \in \mathcal{O}_P$ cuyas clases residuales $z_1(P), \ldots, z_n(P) \in F_P$ son linealmente independientes sobre K, son linealmente independientes sobre $K(x)$. Supongamos que existe una combinación lineal no trivial

$$\sum_{i=1}^{n} \phi_i z_i = 0$$

donde $\phi_i \in K(x)$. Podemos suponer que $\phi_i \in K[x]$ y que x no divide a todos, es decir, $\phi_i = a_i + xg_i$, $a_i \in K$ y no toda $a_i = 0$. Dado que $x \in P$ y $g_i \in \mathcal{O}_P$, tenemos $\phi_i(P) = a_i(P) = a_i$. Entonces si evaluamos la aplicación de clases residuales en la combinación lineal anterior, tenemos

$$0 = 0(P) = \sum_{i=1}^{n} \phi_i(P) z_i(P) = \sum_{i=1}^{n} a_i z_i(P)$$

lo cual contradice la independencia lineal de $z_1(P), \ldots, z_n(P) \in F_P$. □

Corolario 1.2.12. *El campo $\hat{K}$ de F/K es una extensión finita de K*

Demostración. Usaremos el hecho de que $\mathbb{P}_F \neq \varnothing$, que será demostrado en el corolario 1.2.15. Sea $P \in \mathbb{P}_F$. Como $\hat{K}$ está encajado en F_P, mediante la proyección $\pi : \mathcal{O}_P \to F_P$, se sigue que $[\hat{K} : K] \leq [F_P : K] < \infty$. □

Definición 1.2.13. Sea $x \in F$ y $P \in \mathbb{P}_F$. Decimos que P es un *cero* de x de orden $m = v_P(x)$, si $v_P(x) > 0$; P es un *polo* de x de orden $m = v_P(x)$, si $v_P(x) < 0$.

Ahora enunciamos el siguiente teorema sobre la existencia de lugares dado un campo de funciones F/K

Teorema 1.2.14. *Sea F/K un campo de funciones y R un subanillo de F con $K \subseteq R \subsetneq F$. Supongamos que $\{0\} \neq I \subsetneq R$ es un ideal propio de R. Entonces existe un lugar $P \in \mathbb{P}_F$ tal que $I \subseteq P$ y $R \subseteq \mathcal{O}_P$.*

Demostración. Consideremos el siguiente conjunto

$$\mathcal{F} := \{S \mid S \quad \text{es un subanillo de } F \text{ tal que } R \subseteq S \text{ y } IS \neq S\}$$

$\mathcal{F}$ es claramente no vacío pues $R \in \mathcal{F}$. La familia $\{\mathcal{F}, \subseteq\}$ es un conjunto parcialmente ordenado bajo la inclusión. Sea ahora $\{S_\alpha\}_{\alpha \in I} \subseteq \mathcal{F}$ una cadena en $\mathcal{F}$ y consideremos la unión de todos los elementos en la cadena $T := \cup_{\alpha \in I}\{S_\alpha\}$, el cual es un subanillo de F con $R \subseteq T$. Debemos comprobar que $IT \neq T$. Supongamos lo contrario, entonces podemos escribir al 1 como $1 = \sum_{i=1}^{n} a_i s_i$ con $a_i \in I$, $s_i \in T$. Como $\{S_\alpha\}_{\alpha \in I}$ es una cadena existe un $S_0 \in \{S_\alpha\}$ tal que $s_1, \ldots, s_n \in S_0$, por lo tanto $1 \in IS_0$ lo cual es una contradicción.

Por el lema de Zorn $\mathcal{F}$ contiene un elemento máximo $\mathcal{O}$. Veamos que $\mathcal{O}$ es un anillo de valuación de F/K. Dado que $I \neq \{0\}$ e $I\mathcal{O} \neq \mathcal{O}$ tenemos que $\mathcal{O} \subsetneq F$ e $I \subseteq \mathcal{O}\backslash\mathcal{O}^*$. Supongamos que existe un elemento $z \in F$ con la propiedad de que $z \notin \mathcal{O}$ y $z^{-1} \notin \mathcal{O}$. Entonces por la maximalidad de $\mathcal{O}$, tenemos $I\mathcal{O}[z] = \mathcal{O}[z]$ y además $I\mathcal{O}[z^{-1}] = \mathcal{O}[z^{-1}]$ y por lo tanto podemos encontrar $a_0, \ldots, a_n, b_0, \ldots, b_m \in I\mathcal{O}$ con lo siguiente:

$$1 = a_0 + a_1 z + \cdots + a_n z^n \qquad y \tag{1.1}$$

$$1 = b_0 + b_1 z^{-1} + \cdots + b_m z^{-m} \tag{1.2}$$

Donde claramente $n \geq 1$ y $m \geq 1$. Supongamos que m, n son escogidos mínimos y $m \leq n$. Al multiplicar (1.1) por $1 - b_0$ y (1.2) por $a_n z^n$ obtenemos

$$1 - b_0 = (1 - b_0)a_0 + \cdots + (1 - b_0)a_n z^n$$

$$0 = (b_0 - 1)a_n z^n + \cdots + b_m z^{n-m}$$

Al sumar estas dos ecuaciones tenemos $1 = c_0 + c_1 z + \cdots + c_{n-1} z^{n-1}$ con coeficientes $c_i \in I\mathcal{O}$. Esta es una contradicción a la minimalidad de n en (1.1). De modo que, hemos demostrado que $\mathcal{O}$ es un anillo de valuación de F/K y sea P su ideal máximo. □

Corolario 1.2.15. *Sea F/K un campo de funciones, $z \in F$ trascendente sobre K. Entonces z tiene al menos un cero y un polo. En particular $\mathbb{P}_F \neq \varnothing$.*

Demostración. Consideremos el anillo $R = K[z]$ y el ideal $zK[z]$. Por el teorema 1.2.14, existe un lugar $P \in \mathbb{P}_F$ con $z \in P$, por lo tanto P es un cero de z. El mismo argumento demuestra que para z^{-1} existe un cero $Q \in \mathbb{P}_F$, de modo que Q es un polo de z. □

1.3 El campo de funciones racional

Consideremos ahora un campo K un elemento x trascendente sobre K y el campo de funciones $K(x)/K$. Vamos a examinar con detalle sus lugares.

Proposición 1.3.1.

1. *Sea $p(x)$ un polinomio irreducible y mónico. La localización*

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

es un anillo de valuación de $K(x)/K$, cuyo ideal máximo P está dado por

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

y tiene como elemento primo al polinomio $p(x)$.

2. *El anillo siguiente es también un anillo de valuación de $K(x)/K$*

$$\mathcal{O}_\infty = \left\{ \frac{f(x)}{g(x)} \mid deg\, f(x) \leq deg\, g(x) \right\}$$

cuyo ideal máximo es

$$P_\infty = \left\{ \frac{f(x)}{g(x)} \mid deg\, f(x) < deg\, g(x) \right\}$$

entonces $deg\, P_\infty = 1$. Un elemento primo para P_∞ es $t = 1/x$. La correspondiente valuación está dada por $v_\infty(f(x)/g(x)) = deg\, g(x) - deg\, f(x)$.

3. *K es el campo pleno de constantes de $K(x)/K$.*

Demostración. (1) Verificar que $p(x)$ es un elemento primo para $P_{p(x)}$ es inmediato, así como el hecho de que $\mathcal{O}_{p(x)}$ es un anillo de valuación con ideal máximo $P_{p(x)}$. La correspondiente valuación discreta claramente puede ser descrita de la siguiente manera: dado $z \in K(x)$, $z = p(x)^n(f(x)/g(x))$, donde $p(x) \nmid f(x)$, entonces $v_P(z) = n$. Además tenemos que el campo de clases residuales $K(x)_P = \mathcal{O}_P/P$ es isomorfo a $K[x]/(p(x))$; en efecto, consideremos $\psi : K[x] \to \mathcal{O}_P/P$, dado por $f(x) \mapsto f(x) \mod P$. El núcleo de esta aplicación es claramente $(p(x))$ y para ver que es sobre tomemos $z \in \mathcal{O}_P$; entonces $z = f(x)/g(x)$, donde $p(x) \nmid g(x)$ y por lo tanto $1 = up + vg$, donde $u, v \in K[x]$. De manera que $z = fup/g + fu$ y por lo tanto $z \equiv fu \mod P$. Esto demuestra

además que $deg\ P = deg\ p(x)$. En el caso particular $p(x) = x - \alpha$, con $\alpha \in K$, el grado de P es uno y en este caso vamos a denotar por P_α al lugar $P_{x-\alpha}$.

(2) Sólo veremos que $1/x$ es un elemento primo para P_∞, el resto de las afirmaciones son inmediatas. Consideremos $z = f(x)/g(x) \in P_\infty$, i.e. $deg\ f < deg\ g$. Entonces

$$z = \frac{1}{x}\frac{xf}{g}, \quad \text{con } deg\,(xf) \leq deg\ g$$

lo cual demuestra que $1/x$ genera a P_∞. Ahora, los campos de funciones $K(x)/K$ y $K(\frac{1}{x})/K$ son K-isomorfos. Al lugar ∞ de $K(x)/K$ le corresponde el lugar (x) de $K(\frac{1}{x})/K$ mediante este isomorfismo. Entonces el grado de $P_\infty = 1$.

(3) Escojamos un lugar P de grado uno. El campo $\hat{K}$ de $K(x)$ está encajado en el campo de clases residuales $K(x)_P$, por lo tanto $K \subseteq \hat{K} \subseteq K(x)_P \cong K$. □

Teorema 1.3.2. *Los únicos lugares de $K(x)/K$ son de la forma P, donde P está generado por un polinomio mónico irreducible sobre $K[x]$ o P_∞.*

Demostración. Sea P un lugar de $K(x)/K$. Dos casos son posibles:

(1) $x \in \mathcal{O}_P$, por lo tanto $K[x] \subseteq \mathcal{O}_P$. Entonces $I = K[x] \cap P$ es un ideal primo de $K[x]$ y por lo tanto es igual a cero o es el generado por un polinomio mónico irreducible $p(x)$, pero la aplicación de clases residuales induce un encaje $K[x]/I \hookrightarrow K(x)_P$, pues si $I = K[x] \cap P = 0$, entonces para todo elemento $g \in K[x]$, tenemos $g \notin P \Rightarrow 1/g \in \mathcal{O}_P$ y tendríamos entonces $\mathcal{O}_P = F$, lo cual no puede ser. Si $g(x) \in K[x]$ tal que $p(x) \nmid g(x)$, entonces $g(x) \notin P$ y entonces $1/g(x) \in \mathcal{O}_P$. Por lo tanto $\mathcal{O}_{p(x)} \subsetneq \mathcal{O}_P$ y como los anillos de valuación son máximos, se tiene la igualdad.

(2) $x \notin \mathcal{O}_P$, por lo tanto $K[x^{-1}] \subseteq \mathcal{O}_P$. Además $1/x \in P \cap K[1/x]$. Sea $u = 1/x$ e $I = P \cap K[u]$. I es un ideal de $K[u]$ que contiene a u por lo tanto $I = \langle u \rangle$. Ahora si $g(u) \in K[u]$, no es divisible por u entonces $g \notin P$. De donde, para todo $f(u) \in K[u]$ se tiene que $\frac{f(u)}{g(u)} \in \mathcal{O}_P$ y entonces

$$\begin{aligned}
\mathcal{O}_P &\supseteq \left\{ \frac{a_0 + a_1 u + \cdots + a_n u^n}{b_0 + b_1 u + \cdots + b_m u^m}, b_0 \neq 0 \right\} \\
&= \left\{ \frac{a_0 x^{m+n} + a_1 x^{m+n-1} + \cdots + a_n x^m}{b_0 x^{m+n} + b_1 x^{m+n-1} + \cdots + b_m x^n}, b_0 \neq 0 \right\} \\
&= \left\{ \frac{f(x)}{g(x)}, deg\ f \leq deg\ g \right\} = P_\infty
\end{aligned}$$

De nueva cuenta por el argumento de la maximalidad $\mathcal{O}_P = \mathcal{O}_\infty$. □

1.4 Independencia de valuaciones

El resultado principal de esta sección es el teorema de aproximación débil, en una sección posterior se dará un teorema más fuerte de aproximación.

Teorema 1.4.1 (Teorema de aproximación débil). *Sea F/K un campo de funciones, $P_1, \ldots, P_n \in \mathbb{P}_F$ lugares distintos de F/K, $x_1, \ldots, x_n \in F$ y $r_1, \ldots, r_n \in \mathbb{Z}$. Entonces existe $x \in F$ tal que*

$$v_{P_i}(x - x_i) = r_i \text{ para } i = 1, \ldots, n.$$

Demostración. No demostraremos este teorema pues, vamos a probar una versión más general llamado teorema de aproximación fuerte. La demostración de este teorema se puede consultar en [Sti]. □

Un corolario importante de este teorema es el siguiente.

Corolario 1.4.2. *Cualquier campo de funciones tiene una infinidad de lugares.*

Demostración. Supongamos que sólo existe una cantidad finita de lugares $P_1, \ldots, P_n$. Entonces, por el teorema de aproximación débil podemos encontrar un elemento no cero $x \in F$ con $v_{P_i}(x) > 0$ para $i = 1, \ldots, n$. Tenemos que x es trascedente sobre K pues tiene ceros, pero x no tiene ningún polo, lo cual es una contradicción, pues x es un elemento trascendente. □

Otra consecuencia importante del teorema de aproximación débil es el siguiente resultado.

Proposición 1.4.3. *Sea F/K un campo de funciones y $P_1, \ldots, P_k$ ceros del elemento $x \in F$. Entonces*

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

Demostración. Para simplificar notación sea $v_i := v_{P_i}$, $d_i := deg P_i$ y $e_i := v_i(x)$. Por el teorema de aproximación débil, para cada i existe un elemento t_i tal que

$$v_i(t_i) = 1 \text{ y } v_k(t_i) = 0 \text{ para } k \neq i.$$

Tomemos ahora $s_{i1}, \ldots, s_{id_i} \in \mathcal{O}_{P_i}$ tal que $s_{i1}(P_i), \ldots, s_{id_i}(P_i)$ es una base del campo residual F_{P_i} sobre K. De nuevo, por aproximación débil podemos encontrar $z_{ij} \in F$ tal que lo siguiente ocurre para toda i, j:

$$v_i(s_{ij} - z_{ij}) > 0 \text{ y } v_k(z_{ij}) \geq e_k \text{ para } k \neq i.$$

Afirmamos que los elementos

$$t_i^a \cdot z_{ij},\ 1 \leq i \leq r,\ 1 \leq j \leq d_i,\ 0 \leq a < e_i$$

son $K(x)$-linealmente independientes. Su número está dado por $\sum_{i=1}^{r} d_i e_i = \sum_{i=1}^{r} v_{P_i}(x) \cdot deg P_i$, de modo que la proposición se sigue de esta afirmación. Supongamos que existe una combinación lineal no trivial

$$\sum_{i=1}^{r} \sum_{j=1}^{d_i} \sum_{a=0}^{e_i-1} \phi_{ija} t_i^a z_{ij} = 0$$

sobre $K(x)$. Podemos suponer, sin pérdida de generalidad que $\phi_{ija} \in K[x]$ y que no todos los ϕ_{ija} son divisibles por x. Entonces existen índices $k \in \{1, \ldots, r\}$ y $c \in \{0, \ldots, e_k - 1\}$ tales que

$$x \mid \phi_{kja} \quad \text{para todo } a < c \text{ y todo } j \in \{1, \ldots, d_k\} \quad \text{y}$$

$$x \nmid \phi_{ikc} \quad \text{para algún } j \in \{1, \ldots, d_k\}.$$

Si multiplicamos la igualdad anterior por t_k^{-c} obtenemos

$$\sum_{i=1}^{r} \sum_{j=1}^{d_i} \sum_{a=0}^{e_i-1} \phi_{ija} t_i^a t_k^{-c} z_{ij} = 0 \tag{1.3}$$

Para $i \neq k$ todos los sumandos de (1.3) anterior están en P_k pues

$$\begin{aligned} v_k(\phi_{ija} t_i^a t_k^{-c} z_{ij}) &= v_k(\phi_{ija}) + a v_k(t_i) - c v_k(t_k) + v_k(z_{ij}) \\ &\geq 0 + 0 - c + e_k > 0. \end{aligned}$$

Ahora, si $i = k$ y $a < c$ tenemos

$$v_k(\phi_{kja} t_k^{a-c} z_{kj}) \geq e_k + a - c + 0 \geq e_k - c > 0,$$

Notemos que $x \mid \phi_{kja}$ y por lo tanto $v_k(\phi_{kja}) \geq e_k$. Además $v_k(s_{kj}) = 0$, para todo j pues $\{s_{k1}, \ldots, s_{kd_k}\}$ es una base para F_{P_k}. Por otro lado $v_k(s_{kj}) = v_k(z_{kj})$, por la condición $v_i(s_{ij} - z_{ij}) > 0$ y la desigualdad estricta del triángulo. Para $i = k$ y $a > c$, tenemos

$$v_k(\phi_{kja} t_k^{a-c} z_{kj}) \geq a - c > 0.$$

Afirmación. Las condiciones $\{s_{k1}, \ldots, s_{kd_k}\}$ base de F_{P_k} y $v_i(s_{ij} - z_{ij}) > 0$ implican que $z_{k1}(P_k), \ldots, z_{kd_k}(P_k)$ forman una base de F_{P_k}/K. En efecto, si suponemos que eso no ocurre, entonces existe una combinación lineal no trivial $\sum_{j=1}^{d_k} a_j z_{kj} = 0$ con $a_j \in \mathcal{O}_{P_k}$. Si consideramos ahora la siguiente combinación lineal $\sum_{j=1}^{d_k} a_j (s_{ij} - z_{kj})$, ésta pertence a P_k por la desigualdad estricta del triángulo, por lo tanto es igual a cero en F_{P_k} y entonces tenemos una combinación lineal no trivial igual a cero de las s_{jk}, lo cual no puede ocurrir, pues éstas eran una base.

Combinando esto con (1.3) tenemos lo siguiente

$$\sum_{j=1}^{d_k} \phi_{kjc}(P_k) \cdot z_{kj}(P_k) = 0$$

sobre K. Esto es una contradicción pues $z_{k1}(P_k), \ldots, z_{kd_k}(P_k)$ forman una base de F_{P_k}/K, por la afirmación anterior. □

Este resultado será usado varias veces más adelante y posee un corolario importante.

Corolario 1.4.4. *En un campo de funciones F/K, cualquier elemento $0 \neq x \in F$ tiene sólo un número finito de ceros y polos.*

Demostración. Si x es constante, entonces no tiene ceros ni polos. Si x es trascendente sobre K, el número de ceros está acotado superiormente por $[F : K(x)]$ por la proposición anterior. El mismo argumento muestra que x^{-1} tiene sólo un número finito de ceros. □

1.5 Divisores

El campo $\hat{K}$ de un campo de funciones es una extensión finita de K por el corolario 1.2.12 y F puede ser visto como campo de funciones sobre $\hat{K}$. De manera que la siguiente suposición no es crítica para la teoría.

De ahora en adelante, F/K denotará un campo de funciones algebraicas en una variable tal que $\hat{K}$ es todo el campo de constantes de F/K.

Definición 1.5.1. El grupo abeliano libre generado por los lugares de F/K es denotado por $\mathcal{D}_F$, lo llamaremos el *grupo de divisores* de F/K.

Los elementos de $\mathcal{D}_F$ son llamados divisores de F/K. En otras palabras podemos decir que un divisor es una suma formal del tipo

$$D = \sum_{P \in \mathbb{P}_F} n_P P \text{ con } n_P \in \mathbb{Z}, \text{ casi todo } n_P = 0.$$

El soporte de D está definido por

$$supp\, D := \{P \in \mathbb{P}_F \mid n_P \neq 0\}$$

Un divisor de la forma $D = P$ con $P \in \mathbb{P}_F$ será llamado un divisor primo. Dos divisores $D = \sum n_P P$ y $D' = \sum n'_P P$ se suman entrada por entrada:

$$D + D' = \sum_{P \in \mathbb{P}_F} (n_P + n'_P) P$$

Para $Q \in \mathbb{P}_F$ y $D = \sum n_P P \in \mathcal{D}_F$ definimos $v_Q(D) := n_Q$, por lo que $supp\, D = \{P \in \mathbb{P}_F \mid v_P(D) \neq 0\}$ y $D = \sum_{P \in supp\, D} v_P(D)P$.

Introducimos un orden parcial en $\mathcal{D}_F$ de la siguiente forma

$$D_1 \leq D_2 \Leftrightarrow v_P(D_1) \leq v_P(D_2) \quad \text{para todo } P \in \mathbb{P}_F$$

Un divisor $D \geq 0$ es llamado *positivo*. El grado de un divisor está definido por

$$deg\, D := \sum_{P \in \mathbb{P}_F} v_P(D)\, deg\, P$$

y esto da un homomorfismo $deg : \mathcal{D}_F \to \mathbb{Z}$. Por el corolario 1.4.4 todo elemento no cero $x \in F$ sólo tiene un número finito de polos y ceros en $\mathbb{P}_F$, de manera que la siguiente definición tiene sentido.

Definición 1.5.2. Sea $0 \neq x \in F$ y denotemos por Z (respectivamente N) el conjunto de ceros (polos) de x en $\mathbb{P}_F$. Definimos

$$(x)_0 := \sum_{P \in Z} v_P(x)P$$

como el divisor cero del elemento x. De manera análoga definimos

$$(x)_\infty := \sum_{P \in N} (-v_P(x))P$$

como el divisor polo de x y el divisor principal de x está dado por

$$(x) := (x)_0 - (x)_\infty.$$

Claramente $(x)_0 \geq 0$, $(x)_\infty \geq 0$ y los elementos $0 \neq x \in F$ que son constantes están caracterizados por

$$x \in K \Leftrightarrow (x) = 0$$

Definición 1.5.3. El conjunto

$$\mathcal{P}_F := \{(x) \mid 0 \neq x \in F\}$$

es llamado el grupo de *divisores principales* de F/K. Este es un subgrupo de $\mathcal{D}_F$, pues por la caracterización hecha de estos divisores, si $0 \neq x, y \in F$, tenemos $(xy) = (x) + (y)$. De manera que tiene sentido hablar del grupo cociente $Pic_F := \mathcal{D}_F/\mathcal{P}_F$ llamado el grupo de Picard. Para un divisor $D \in \mathcal{D}_F$, su clase en Pic_F la denotaremos por $[D]$. Decimos que dos divisores D, D' son equivalentes $D \sim D'$ si $[D] = [D']$, es decir, si $D = D' + (x)$ para algún $0 \neq x \in F$. Es fácil verificar que ésta es una relación de equivalencia.

La siguiente definición desempeña un papel fundamental en la teoría de campos de funciones algebraicas.

Definición 1.5.4. Para un divisor $A \in \mathcal{D}_F$ definimos

$$\mathcal{L}(A) := \{x \in F \mid (x) \geq -A\} \cup \{0\}$$

Esta definición tiene la siguiente interpretación, si

$$A = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j$$

con $n_i > 0$, $m_j > 0$, entonces $\mathcal{L}(A)$ consiste de elementos $x \in F$ tales que

1. x tiene ceros de orden $\geq m_j$ en Q_j, para $j = 1, \ldots, s$ y
2. x puedo tener polos únicamente en los lugares $P_1, \ldots, P_r$ con el orden del polo en P_i acotado por n_i $(i = 1, \ldots, r)$.

Observación 1.5.5. Sea $A \in \mathcal{D}_F$. Entonces

1. $x \in \mathcal{L}(A) \iff v_P(x) \geq -v_P(A)$ para todo $P \in \mathbb{P}_F$.
2. $\mathcal{L}(A) \neq \{0\} \iff$ existe un divisor $A' \geq 0$ tal que $A' \sim A$.

La demostración de estas afirmaciones se sigue inmediatamente de las definiciones.

Lema 1.5.6. *Sea $A \in \mathcal{D}_F$. Entonces*

1. *$\mathcal{L}(A)$ es un K-espacio vectorial.*
2. *Si A' es un divisor equivalente a A entonces $\mathcal{L}(A) \cong \mathcal{L}(A')$ como K-espacios vectoriales.*

Demostración. Sean $x, y \in \mathcal{L}(A)$ y $a \in K$. Entonces para todo $P \in \mathbb{P}_F$, tenemos $v_P(x+y) \geq \min\{v_P(x), v_P(y)\} \geq -v_P(A)$, por lo que $x+y \in \mathcal{L}(A)$. Se tiene $ax \in \mathcal{L}(A)$ por la observación anterior y por el hecho de que si $a \in K \backslash \{0\}$ entonces $v_P(a) = 0$; el caso $a = 0$ es trivial. Veamos la segunda parte del lema. Por hipótesis tenemos que existe $0 \neq z \in F$ tal que $A = A' + (z)$. Definamos $\phi : \mathcal{L}(A) \to F$ dada por $x \mapsto xz$. Esta función es K-lineal y su imagen está contenida en $\mathcal{L}(A')$ claramente. De la misma manera, si ahora definimos la función $\phi' : \mathcal{L}(A') \to F$ tal que $x \mapsto xz^{-1}$, ésta es K-lineal, su imagen está contenida en $\mathcal{L}(A)$ y además es inversa de ϕ. Por lo tanto ϕ es un isomorfismo entre $\mathcal{L}(A)$ y $\mathcal{L}(A')$. □

Los siguientes dos lemas son importantes para el ulterior desarrollo de la teoría.

Lema 1.5.7. *1.* $\mathcal{L}(0) = K$

2. Si $A < 0$ *entonces* $\mathcal{L}(A) = \{0\}$

Demostración. (1) Tenemos que para todo $x \in K\backslash\{0\}$, el divisor $(x) = 0$, por lo que $K \subseteq \mathcal{L}(0)$. Recíprocamente si $0 \neq x \in \mathcal{L}(0)$ entonces $(x) \geq 0$. Esto quiere decir que x no tiene ningún polo y por lo tanto $x \in K$.

(2) Ahora supongamos que existe un elemento $0 \neq x \in \mathcal{L}(A)$. Entonces $(x) \geq -A > 0$ y el elemento x tendría un cero pero ningún polo, lo cual es imposible. □

Lema 1.5.8. *Sean* A, B *divisores de* F/K *con* $A \leq B$. *Entonces tenemos* $\mathcal{L}(A) \subseteq \mathcal{L}(B)$, *por lo que tiene sentido el cociente* $\mathcal{L}(B)/\mathcal{L}(A)$ *y además*

$$dim(\mathcal{L}(B)/\mathcal{L}(A)) \leq degB - degA.$$

Demostración. $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ es trivial. Para probar la otra afirmación del lema supongamos que $B = A+P$ (podemos hacerlo sin pérdida de generalidad, el caso general se demuestra fácilmente por inducción). Escojamos $t \in F$ tal que $v_P(t) = v_P(B) = v_P(A) + 1$. Si $x \in \mathcal{L}(B)$ tenemos $v_P(x) \geq -v_P(B) = -v_P(t)$, de manera que $xt \in \mathcal{O}_P$ y tenemos un mapeo K-lineal $\psi : \mathcal{L}(B) \to F_P$, dado por $x \mapsto (xt)(P)$. Ahora, x está en el núcleo de ψ si y sólo si $v_P(xt) > 0$, es decir, $v_P(x) \geq -v_P(A)$. De manera que $Ker(\psi) = \mathcal{L}(A)$ y entonces ψ induce una aplicación K-lineal bien definida de $\mathcal{L}(B)/\mathcal{L}(A)$ en F_P. Por lo tanto

$$dim(\mathcal{L}(B)/\mathcal{L}(A)) \leq dim\ F_P = degB - degA$$

□

Proposición 1.5.9. *Para todo divisor* $A \in \mathcal{D}_F$ *el espacio* $\mathcal{L}(A)$ *tiene dimensión finita sobre* K. *Más precisamente, si* $A = A_+ - A_-$ *con divisores positivos* A_+ *y* A_-, *entonces*

$$dim\mathcal{L}(A) \leq deg\ A_+ + 1$$

Demostración. Dado que $\mathcal{L}(A) \subseteq \mathcal{L}(A_+)$, es suficiente demostrar que

$$dim\mathcal{L}(A_+) \leq deg\ A_+ + 1$$

Para esto notemos que el lema anterior nos dice que $dim(\mathcal{L}(A_+))/\mathcal{L}(0)) \leq deg\ A_+$ y dado que $\mathcal{L}(0) = K$ como se demostró anteriormente en el lema 1.5.7, la $dim(\mathcal{L}(A_+)) = dim(\mathcal{L}(A_+)/\mathcal{L}(0)) + 1$ la demostración está concluida. □

Definición 1.5.10. Para $A \in \mathcal{D}_F$, el entero $dim\, A := dim\, \mathcal{L}(A)$ es llamado la dimensión del divisor A.

El teorema que a continuación se enuncia establece que todo elemento $0 \neq x \in F$ tiene tantos ceros como polos, contados adecuadamente.

Teorema 1.5.11. *Todo divisor principal tiene grado cero. Más precisamente, sea $x \in F \backslash K$ y $(x)_0$ $(x)_\infty$ el divisor cero y polo respectivamente de x. Entonces*

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

Demostración. Sea $n = [F : K(x)]$ y sea

$$B := (x)_\infty = \sum_{i=1}^{r} -v_{P_i}(x) P_i$$

donde $P_1, \ldots, P_r$ son los polos de x. Entonces

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

por la proposición 1.4.3 ; mostraremos que $n \leq deg\, B$. Escojamos una base $u_1, \ldots, u_n$ de $F/K(x)$ y un divisor $C \geq 0$ tal que $(u_i) \geq -C$ para $i = 1, \ldots, n$. Tenemos entonces

$$dim(lB + C) \geq n(l+1) \quad \text{para todo } l \geq 0$$

lo cual se sigue inmediatamente del hecho de $x^i u_j \in \mathcal{L}(lB + C)$ para $0 \leq i \leq l$, $1 \leq j \leq n$ (notemos que estos elementos son linealmente independientes sobre K puesto que $u_1, \ldots, u_n$ son linealmente independientes sobre $K(x)$). Definamos $c = deg\, C$ y tenemos $n(l+1) \leq dim(lB + C) \leq l\, deg\, B + c + 1$ por la proposición 1.5.9. Por lo tanto

$$l(deg\, B - n) \geq n - c - 1$$

para toda $l \in \mathbb{N}$. El lado derecho de la desigualdad anterior es independiente de l, por lo que esta desigualdad sólo es posible cuando $deg\, B \geq n$ Hemos demostrado que $deg\, (x)_\infty = [F : K(x)]$. Como $(x)_0 = (x^{-1})_\infty$, concluimos que $deg\, (x)_0 = deg\, (x^{-1})_\infty = [F : K(x^{-1})] = [F : K(x)]$. □

Una parte importante para el desarrollo de la teoría es el siguiente corolario.

Corolario 1.5.12. *1. Sean A, $A' \in \mathcal{D}_F$ divisores tales que $A \sim A'$. Entonces $dim\, A = dim\, A'$ y $deg\, A = deg\, A'$.*

2. *Si* $deg A < 0$ *entonces* $dim A = 0$.

3. *Para un divisor* A *de grado cero, las siguientes afirmaciones son equivalentes:*

   (a) A *es principal*

   (b) $dim A \geq 1$

   (c) $dim A = 1$

Demostración. (1) Se sigue inmediatamente del lema 1.5.6 y el teorema 1.5.11.

(2) Supongamos $dim\, A > 0$. Por la observación 1.5.5 existe un divisor $A' \sim A$ con $A \geq 0$, entonces $deg\, A = deg\, A' \geq 0$.

(3) (a) $\Rightarrow$ (b) Si $A = (x)$ es principal entonces $x^{-1} \in \mathcal{L}(A)$, de manera que $dim\, A \geq 1$. (b) $\Rightarrow$ (c) Supongamos ahora que $dim\, A \geq 1$ y $deg\, A = 0$. Entonces $A \sim A'$ con algún $A' \geq 0$. Las condiciones $A' \geq 0$ y $deg\, A' = 0$, implican $A' = 0$, por lo tanto $dim\, A' = dim\, A = dim\, 0 = 1$ por el lema 1.5.7. (c) $\Rightarrow$ (a) Supongamos que $dim\, A = 1$ y $deg\, A = 0$. Tomemos $0 \neq z \in \mathcal{L}(A)$, entonces $(z) + A \geq 0$. Como $deg((z) + A) = 0$ se sigue que $(z) + A = 0$, por lo tanto $A = -(z) = (z^{-1})$ es principal. □

Ejemplo 1.5.13. Consideremos de nueva cuenta el campo de funciones racionales $F = K(x)$ con K un campo cualquiera. Para $0 \leq z \in K(x)$ tenemos $z = af(x)/g(x)$ con $a \in K^*$, $f(x)$, $g(x) \in K[x]$ mónicos y primos relativos. Sean ahora

$$f(x) = \prod_{i=1}^{r} p_i(x)^{n_i},\ g(x) = \prod_{j=1}^{s} q_j(x)^{m_j}$$

las descomposiciones en polinomios mónicos irreducibles de $f(x)$ y $g(x)$. Entonces el divisor principal de z en $\mathcal{D}_K(x)$ corresponde a

$$(z) = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j + (deg\, g - deg\, f)P_\infty$$

donde P_i, respectivamente Q_j son los lugares de $p_i(x)$ y $q_j(x)$. De manera que en un campo de funciones arbitrario, los divisores principales son los sustitutos para la descomposición en polinomios irreducibles que ocurre en el campo de funciones racional.

La siguiente proposición es fundamental en la definición del género de un campo de funciones algebraicas.

Proposición 1.5.14. *Existe una constante* $\gamma \in \mathbb{Z}$ *tal que, para todos los divisores* $A \in \mathcal{D}_F$ *ocurre lo siguiente:*

$$deg\, A - dim\, A \leq \gamma$$

Demostración. El énfasis en esta proposición es que γ sólo depende del campo de funciones F/K. Para empezar, notemos lo siguiente

$$A_1 \leq A_2 \Rightarrow deg\, A_1 - dim\, A_1 \leq deg\, A_2 - dim\, A_2, \tag{1.4}$$

por el lema 1.5.8. Tomamos un elemento $x \in F \backslash K$ y consideremos el divisor $B := (x)_\infty$. Al igual que en la prueba del teorema 1.5.11 existe un divisor $C \geq 0$ tal que $dim(lB + C) \geq (l+1)\, deg\, B$ para todo $l \geq 0$. Por otra parte, $dim(lB + C) \leq dim(lB) + deg\, C$ por el lema 1.5.8. Combinando estas desigualdades obtenemos

$$dim(lB) \geq (l+1) deg\, B - deg\, C = deg(lB) + ([F : K(x)] - deg\, C)$$

Por lo tanto

$$deg(lB) - dim(lB) \leq \gamma \quad \text{para toda } l > 0 \tag{1.5}$$

con algún $\gamma \in \mathbb{Z}$. Queremos mostrar que 1.5 se cumple cuando sustituimos en lugar de lB cualquier divisor $A \in \mathcal{D}_F$.

Afirmación. Dado un divisor A, existen divisores A_1, D y un entero $l \geq 0$ tal que $A \leq A_1$, $A_1 \sim D$ y $D \leq lB$.

Esta afirmación es fácil de verificar: Sean $A_1 \geq A$ tal que $A_1 \geq 0$. Entonces

$$\begin{aligned} dim(lB - A_1) &\geq dim(lB) - deg\, A_1 \\ &\geq deg(lB) - \gamma - deg\, A_1 \\ &> 0 \end{aligned}$$

para l suficientemente grande. Entonces existe un elemento $0 \neq z \in \mathcal{L}(lB - A_1)$. Definiendo $D := A_1 - (z)$ obtenemos $A_1 \sim D$ y $D \leq A_1 - (A_1 - lB) = lB$ como queríamos. Si ahora usamos esta afirmación la proposición si sigue fácilmente:

$$\begin{aligned} deg\, A - dim\, A &\leq deg\, A_1 - dim\, A_1 \\ &= deg\, D - dim\, D \\ &\leq deg(lB) - dim(lB) \\ &\leq \gamma \end{aligned}$$

Que es justamente lo que deseábamos demostrar. □

Ahora con la proposición anterior la siguiente definición tiene sentido.

Definición 1.5.15. El género g de F/K está definido por

$$g := \text{máx}\{degA - dimA + 1 \mid A \in \mathcal{D}_F\}$$

Observación 1.5.16. El género g de un campo de funciones es un entero no negativo. Esto es fácil de ver, simplemente en la definición de género sustituyamos $A = 0$ y entonces $deg(0) - dim(0) + 1 = 0$. Por lo tanto $g \geq 0$.

Teorema 1.5.17 (Teorema de Riemann). *Sea F/K un campo de funciones de género g.*

1. *Para todo divisor $A \in \mathcal{D}_F$,*

$$dim\, A \geq deg\, A + 1 - g$$

2. *Existe un entero c, que depende de F/K, tal que*

$$dim\, A = deg\, A + 1 - g$$

siempre que $deg\, A \geq c$.

Demostración. La primera afirmación es justamente la definición del género. Escojamos ahora un divisor A_0 con $g = deg\, A_0 - dim\, A_0 + 1$ y definamos $c := deg\, A_0 + g$. Si $deg\, A \geq c$ entonces

$$dim(A - A_0) \geq deg(A - A_0) + 1 - g \geq c - deg\, A_0 + 1 - g \geq 1$$

Por lo tanto existe un elemento $0 \neq z \in \mathcal{L}(A - A_0)$. Consideremos el divisor $A' := A + (z)$ el cual es $\geq A_0$. Tenemos entonces

$$\begin{aligned} deg\, A - dim\, A &= deg\, A' - dim\, A' \\ &\geq deg\, A_0 - dim\, A_0 \\ &= g - 1 \end{aligned} \tag{1.6}$$

Por lo tanto $dim\, A \leq deg\, A + 1 - g$. □

Ejemplo 1.5.18. Vamos a mostrar, con los teoremas anteriormente desarrollados, que el campo de funciones racional $K(x)/K$, tiene género cero. Denotemos por P_∞ el polo divisor de x. Consideremos para $r \geq 0$, el espacio vectorial $\mathcal{L}(rP_\infty)$. Desde luego, los elementos $1, x, \ldots, x^r$ están en $\mathcal{L}(rP_\infty)$, por lo tanto

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

para r suficientemente grande. Por lo tanto, $g \leq 0$, pero ya sabíamos que $g \geq 0$ por la observación 1.5.16 por lo tanto tenemos la afirmación.

Capítulo 2

El teorema de Riemann-Roch

En este sección F/K denotará un campo de funciones de género g.

2.1 El espacio de adeles

Definición 2.1.1. Para $A \in \mathcal{D}_F$, $i(A) := dim\, A - deg\, A + g - 1$ es llamado el índice de especialidad de A.

El teorema de Riemann establece que $i(A)$ es un entero no negativo y que además $i(A) = 0$ si $deg\, A$ es suficientemente grande. Es este capítulo daremos una interpretación de $i(A)$ como la dimensión de ciertos espacios vectoriales. Con este fin vamos a introducir la siguiente definición.

Definición 2.1.2. Un adel de F/K es un mapeo $\alpha : \mathbb{P}_F \to F$ de manera que $P \mapsto \alpha_P$ y $\alpha_P \in \mathcal{O}_P$ para casi toda $P \in \mathbb{P}_F$. Por lo que podemos pensar a un adel como un elemento del producto directo $\prod_{P \in \mathbb{P}_F} F$ y por lo tanto usaremos la notación $\alpha = (\alpha_P)_{P \in \mathbb{P}_F}$.

El siguiente conjunto

$$\mathcal{A}_F := \{\alpha \mid \alpha \text{ es un adel de } F/K\}$$

es llamado el espacio de adeles de F/K y tiene estructura de F-espacio vectorial de manera natural. Diremos que el *adel principal* de un elemento $x \in F$ es el adel cuyas componentes son todas iguales a x; este elemento es, en efecto, un adel pues dado $x \in F$, éste tiene a lo más un número finito de polos. Esto nos da una forma de encajar $F \hookrightarrow \mathcal{A}_F$. Las valuaciones v_P de F/K se extienden de manera natural a $\mathcal{A}_F$ definiendo $v_P(\alpha) := v_P(\alpha_P)$. Por definición de adel, $v_P(\alpha) \geq 0$ para casi toda $P \in \mathbb{P}_F$.

Definición 2.1.3. Para $A \in \mathcal{D}_F$ definimos

$$\mathcal{A}_F(A) := \{\alpha \in \mathcal{A}_F \mid v_P(\alpha) \geq -v_P(A) \quad \text{para toda } P \in \mathbb{P}_F\}$$

El cual es un K-subespacio de $\mathcal{A}_F$.

Teorema 2.1.4. *Para todo divisor $A \in \mathcal{D}_F$ el índice de especialidad es*

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

Demostración. La demostración de este teorema es bastante larga. Daremos la idea de la prueba y referimos a [Sti] para la demostración completa. La demostración consiste en varios pasos:

(1) Sean $A_1, A_2 \in \mathcal{D}_F$ y $A_1 \leq A_2$, entonces $\mathcal{A}_F(A_1) \subseteq \mathcal{A}_F(A_2)$ y además

$$dim(\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)) = deg\, A_2 - deg\, A_1 \tag{2.1}$$

(2) Sean $A_1, A_2 \in \mathcal{D}_F$, con $A_1 \leq A_2$ como antes

$$dim\,((\mathcal{A}_F(A_2) + F)/(\mathcal{A}_F(A_1) + F)) =$$

$$= (deg\, A_2 - dim\, A_2) - (deg\, A_1 - dim\, A_1) \tag{2.2}$$

(3) Si B es un divisor tal que $dim\, B = deg\, B + 1 - g$ entonces

$$\mathcal{A}_F = \mathcal{A}_F(B) + F \tag{2.3}$$

Una vez que hemos probado estos pasos, consideramos un divisor arbitrario A. Por el teorema de Riemann, existe un divisor $A_1 \geq A$ tal que $dim\, A_1 = deg\, A_1 + 1 - g$; por (2.3), $\mathcal{A}_F = \mathcal{A}_F(A_1) + F$ y por (2.2), tenemos

$$\begin{aligned} dim(\mathcal{A}_F/\mathcal{A}_F(A) + F) &= dim((\mathcal{A}_F(A_1) + F)/(\mathcal{A}_F(A) + F)) \\ &= (deg\, A_1 - dim\, A_1) - (deg\, A - dim\, A) \\ &= (g - 1) + dim\, A - deg\, A = i(A). \end{aligned}$$

□

Corolario 2.1.5. $g = dim\,(\mathcal{A}_F/(\mathcal{A}_F(0) + F))$.

Demostración. $i(0) = dim(0) - deg(0) + g - 1 = 1 - 0 + g - 1 = g.$ □

A continuación introducimos el concepto de diferencial de Weil, que nos lleva a una segunda interpretación para el índice de especialidad de un divisor.

Definición 2.1.6. Un *diferencial de Weil* de F/K es una aplicación K-lineal $\omega : \mathcal{A}_F \to K$ que se hace cero en $\mathcal{A}_F(A) + F$ para algún divisor $A \in \mathcal{D}_F$. Llamaremos

$$\Omega_F := \{\omega \mid \omega \text{ es un diferencial de Weil de } F/K\}$$

el módulo de diferenciales de F/K. Si $A \in \mathcal{D}_F$ sea

$$\Omega_F(A) := \{\omega \in \Omega_F \mid \omega \text{ se hace cero en } \mathcal{A}_F(A) + F\}$$

Notemos que Ω_F tiene estructura de K-espacio vectorial de manera natural. A continuación damos otra interpretación del índice de especialidad.

Lema 2.1.7. *Para todo $A \in \mathcal{D}_F$ se cumple que $dim\ \Omega_F(A) = i(A)$.*

Demostración. $\Omega_F(A)$ es de manera natural isomorfo a las formas lineales sobre $\mathcal{A}_F/(\mathcal{A}_F(A) + F)$. Dado que $\mathcal{A}_F/(\mathcal{A}_F(A) + F)$ tiene dimensión $i(A)$, por el teorema 2.1.4, el lema se sigue inmediatamente. □

A continuación vamos a definir el producto de elementos de F con diferenciales.

Definición 2.1.8. Para $x \in F$ y $\omega \in \Omega_F$ definimos $x\omega : \mathcal{A}_F \to K$ por

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

Es de rutina verificar que $x\omega$ es un diferencial de Weil de F/K. De hecho, si ω se anula en $\mathcal{A}_F(A) + F$ entonces $x\omega$ se anula en $\mathcal{A}_F(A + (x)) + F$. Entonces la definición anterior le da claramente a Ω_F una estructura de espacio vectorial sobre F.

Los siguientes proposición y lema, son resultados técnicos importantes para la demostración del teorema de Riemann-Roch.

Proposición 2.1.9. *Ω_F es un espacio vectorial de dimensión uno sobre F.*

Demostración. Sea $0 \neq \omega_1 \in \Omega_F$. Debemos demostrar que para todo $\omega_2 \in \Omega_F$ existe $z \in F$ tal que $\omega_2 = z\,\omega_1$. Supongamos que $\omega_2 \neq 0$. Sean $A_1, A_2 \in \mathcal{D}_F$ tales que $\omega_1 \in \Omega_F(A_1)$ y $\omega_2 \in \Omega_F(A_2)$. Consideremos ahora un divisor B de grado suficientemente grande tal que

$$dim(A_i + B) = deg(A_i + B) + 1 - g$$

para $i = 1, 2$. Esto, desde luego es posible por el teorema de Riemann. Consideremos ahora las siguientes aplicaciones lineales: $\phi_i : \mathcal{L}(A_i + B) \to \Omega_F(-B)$

dada por $x \mapsto x\omega_i$ para $i = 1, 2$ Las cuales están bien definidas, pues si $\alpha \in \mathcal{A}_F(-B)$ y $x_i \in \mathcal{L}(A_i + B)$ tenemos lo siguiente

$$v_P(\alpha) \geq v_P(B)$$

y

$$v_P(x_i) + v_P(B) \geq -v_P(A_i)$$

Al sumar las dos desigualdades obtenemos

$$v_P(\alpha\, x_i) = v_P(\alpha) + v_P(x_i) \geq -v_P(A_i)$$

porlo tanto el diferencial $x_i\omega \in \Omega_F(-B)$. Más aún, las funciones ϕ_i son inyectivas. Si $0 \neq x \in ker\, \phi_i$, tenemos que $(1/x)\,\alpha$ es un adel para toda $\alpha \in \mathcal{A}_F$. Al evaluar en este adel obtenemos para toda $\alpha \in \mathcal{A}_F$

$$x\,\omega_i((1/x)\,\alpha) := \omega_i(x\,(1/x)\,\alpha) = \omega_i(\alpha) = 0$$

es decir, ω_i es idénticamente cero, lo cual es una contradicción. Por lo tanto $x = 0$. Afirmamos ahora lo siguiente:

Afirmación. Para el divisor B se cumple lo siguiente

$$\phi_1(\mathcal{L}(A_1 + B)) \cap \phi_2(\mathcal{L}(A_2 + B)) \neq 0$$

Empezamos con un hecho bastante conocido de álgebra lineal: Si U_1, U_2 son dos subespacios de un espacio vectorial V de dimensión finita, entonces

$$dim(U_1 \cap U_2) \geq dim\, U_1 + dim\, U_2 - dim\, V \tag{2.4}$$

Definamos entonces $U_i := \phi_i(\mathcal{L}(A_i + B)) \subseteq \Omega_F(-B)$. Como

$$\begin{aligned} dim\, \Omega_F(-B) = i(-B) &= dim(-B) - deg(-B) + g - 1 \\ &= deg\, B + g - 1 \end{aligned}$$

(notemos que aquí usamos el hecho de que podemos considerar a $B > 0$ y por lo tanto $dim(-B) = 0$). Llegamos entonces a lo siguiente

$$\begin{aligned} &dim\, U_1 + dim\, U_2 - dim\, \Omega_F(-B) \\ &= deg(A_1 + B) + 1 - g + deg(A_2 + B) + 1 - g - (deg\, B + g - 1) \\ &= deg\, B + (deg\, A_1 + deg\, A_2 + 3(1 - g)) \end{aligned}$$

el término entre paréntesis es independiente de B, de manera que

$$dim\, U_1 + dim\, U_2 - dim\, \Omega_F(-B) > 0$$

si el grado de B es suficientemente grande. Por (2.4) tenemos que $U_1 \cap U_2 \neq 0$, lo que prueba la afirmación. Usando la afirmación, la prueba de esta proposición es inmediata: escojamos $x_1 \in \mathcal{L}(A_1 + B)$ y $x_2 \in \mathcal{L}(A_2 + B)$ tales que $x_1\omega_1 = x_2\omega_2 \neq 0$. Entonces $\omega_2 = (x_1 x_2^{-1})\omega_1$ como queríamos. □

Otro objetivo es asociarle un divisor a todo diferencial de Weil $\omega \neq 0$. Para esto consideremos el siguiente conjunto de divisores.

$$M(\omega) := \{A \in \mathcal{D}_F \mid \omega \quad \text{se anula en } \mathcal{A}_F(A) + F\}$$

El siguiente lema nos permitirá definir la noción de divisor canónico.

Lema 2.1.10. *Sea $0 \neq \omega \in \Omega_F$. Entonces existe un único divisor $W \in M(\omega)$ tal que $A \leq W$ para todo $A \in M(\omega)$.*

Demostración. Por el teorema de Riemann existe c constante tal que para todo $A \in \mathcal{D}_F$ tal que $deg\, A \geq c$ se tiene $i(A) = 0$. Como $dim(\mathcal{A}_F/(\mathcal{A}_F(A) + F)) = i(A)$ por el teorema 2.1.4, tenemos que $deg\, A < c$ para todo $A \in M(\omega)$. De manera que podemos escoger un divisor $W \in M(\omega)$ de grado máximo. Supongamos que W no cumple la conclusión del lema; entonces existe un divisor $A_0 \in M(\omega)$ con $A_0 \not\leq W$, es decir, $v_Q(A_0) > v_Q(W)$ para algún $Q \in \mathbb{P}_F$. Afirmamos ahora que $W + Q \in M(\omega)$ lo cual contradice la maximalidad de W. Para demostrar esta afirmación, consideremos un adel $\alpha = (\alpha_P) \in \mathcal{A}_F(W+Q)$. Podemos escribir a $\alpha = \alpha' + \alpha''$ donde

$$\alpha'_P := \begin{cases} \alpha_P & \text{si } P \neq Q \\ 0 & \text{si } P = Q \end{cases}$$

y

$$\alpha''_P := \begin{cases} 0 & \text{si } P \neq Q \\ \alpha_Q & \text{si } P = Q \end{cases}$$

Entonces $\alpha' \in \mathcal{A}_F(W)$ y $\alpha'' \in \mathcal{A}_F(A_0)$, por lo que $\omega(\alpha) = \omega(\alpha') + \omega(\alpha'') = 0$. De manera que ω se anula en $\mathcal{A}_F(W + Q) + F$ y la afirmación está probada. La unicidad de W es ahora inmediata. □

El lema anterior nos permite definir lo siguiente.

Definición 2.1.11. 1. El divisor (ω) de un diferencial de Weil $\omega \neq 0$ es el único divisor de F/K que satisface

   (a) ω se anula en $\mathcal{A}_F((\omega)) + F$.

   (b) Si ω se hace cero en $\mathcal{A}_F(A) + F$ entonces $A \leq (\omega)$.

2. Para $0 \neq \omega \in \Omega_F$ y $P \in \mathbb{P}_F$ definimos $v_P(\omega) := v_P((\omega))$.

3. Un lugar P se dice que es un *cero* (*polo*) de ω si $v_P(\omega) > 0$ (respectivamente si $v_P(\omega) < 0$. Se dice que ω es regular en P si $v_P(\omega) \geq 0$ y se dice que ω es *regular* (u *holomorfo*) si es regular en todo $P \in \mathbb{P}_F$.

4. Un divisor W es llamado *divisor canónico* de F/K si $W = (\omega)$ para algún $\omega \in \Omega_F$.

Observación 2.1.12. Se sigue inmediatamente de la definición que

$$\Omega_F(A) = \{\omega \in \Omega_F \mid \omega = 0 \text{ ó } (\omega) \geq A\}$$

y que

$$\Omega_F(0) = \{\omega \in \Omega_F \mid \omega \text{ es regular}\}$$

Como una consecuencia del lema 2.1.7 y la definición tenemos que

$$dim\, \Omega_F(0) = g$$

Hasta el momento tenemos estas interpretaciones del índice de especialización.

Proposición 2.1.13.

1. *Para* $0 \neq x \in F$ *y* $\omega \in \Omega_F$ *tenemos* $(x\omega) = (x) + (\omega)$
2. *Cualesquiera dos divisores canónicos de* F/K *son equivalentes.*

Demostración. Si ω se anula en $\mathcal{A}_F(A) + F$ entonces $x\omega$ se anula en $\mathcal{A}_F(A + (x)) + F$, por lo que

$$(\omega) + (x) \leq (x\omega)$$

Asimismo, $(x\omega) + (x^{-1}) \leq (x^{-1}x\omega) = (\omega)$, si combinamos estas desigualdades obtenemos

$$(\omega) + (x) \leq (x\omega) \leq -(x^{-1}) + (\omega) = (\omega) + (x)$$

Lo cual demuestra (1). El inciso (2) es una consecuencia de (1) y de la proposición 2.1.9. □

Una simple pero importante consecuencia es que los divisores canónicos de F/K forman una sola clase $[W]$ en el grupo de clases de divisores C_F. A esta clase se le llama la clase canónica de F/K.

Teorema 2.1.14. *Sea* A *un divisor arbitrario y* $W = (\omega)$ *un divisor canónico de* F/K. *Entonces la función* $\mu : \mathcal{L}(W - A) \to \Omega_F(A)$ *tal que* $x \mapsto x\omega$ *es un isomorfismo de* K*-espacios vectoriales.*

Demostración. Si $x \in \mathcal{L}(W - A)$ tenemos

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

por lo tanto $x\omega \in \Omega_F(A)$. Por lo que μ manda $\mathcal{L}(W - A)$ en $\Omega_F(A)$. Claramente μ es K-lineal e inyectiva. Para demostrar la suprayectividad consideremos

un diferencial $\omega_1 \in \Omega_F(A)$. Por la proposición 2.1.9, $\omega_1 = x\omega$ para algún $x \in F$. Pero tenemos que

$$(x) + W = (x) + (\omega) = (x\omega) = (\omega_1) \geq A,$$

de manera que $(x) \geq -(W - A)$, por lo tanto $x \in \mathcal{L}(W - A)$ y $\omega_1 = \mu(x)$. Hemos probado que $dim\,\Omega_F(A) = dim\,(W - A)$ y por otra parte ya sabíamos que $dim\,\Omega_F(A) = i(A)$, por lo tanto $i(A) = dim\,(W - A)$. □

Todos estos resultados los hemos desarrollado para obtener el Teorema de Riemann-Roch, que es por mucho el teorema más importante en la teoría de campos de funciones algebraicas.

Teorema 2.1.15 (Teorema de Riemann-Roch). *Sea $W \in \mathcal{D}_F$ un divisor canónico de F/K. Entonces para todo divisor $A \in \mathcal{D}_F$ se cumple*

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

Demostración. Este resultado es inmediato del teorema anterior y de la definición de $i(A)$. □

Corolario 2.1.16. *Para un divisor canónico W, tenemos*

$$deg\,W = 2g - 2 \quad y \quad dim\,W = g$$

Demostración. Si hacemos $A = 0$ por el teorema de Riemann-Roch tenemos

$$1 = dim\,0 = deg\,0 + 1 - g + dim(W - 0)$$

Entonces $dim\,W = g$. Ahora, si $A = W$ obtenemos

$$g = dim\,W = deg\,W + 1 - g + dim(W - W) = deg\,W + 2 - g$$

por lo tanto $deg\,W = 2g - 2$. □

Teorema 2.1.17. *Si A es un divisor de F/K de grado $\geq 2g - 1$, entonces*

$$dim\,A = deg\,A + 1 - g$$

Demostración. Tenemos que $dim\,A = deg\,A + 1 - g + dim(W - A)$, con W un divisor canónico. Como $deg\,A \geq 2g - 1$ y $deg\,W = 2g - 2$, se tiene $deg\,(W - A) < 0$. Por el lema 1.5.7 $dim(W - A) = 0$. □

2.2 Consecuencias del Teorema de Riemann-Roch

Como algunos de los resultados que provienen de este importante teorema, citaremos dos teoremas.

Teorema 2.2.1 (Teorema de aproximación fuerte). *Sea $S \subsetneq \mathbb{P}_F$ un subconjunto propio de $\mathbb{P}_F$ y $P_1, \ldots, P_r \in S$. Supongamos además que están dados $x_1, \ldots, x_r \in F$ y $n_1, \ldots n_r \in \mathbb{Z}$. Entonces existe un elemento $x \in F$ tal que*

$$v_{P_i}(x - x_i) = n_i \qquad (i = 1, \ldots, r), \quad y \quad v_P(x) \geq 0$$

para todo $P \in S \backslash \{P_1, \ldots, P_r\}$.

Demostración. Consideremos el adel $\alpha = (\alpha_P)_{P \in \mathbb{P}_F}$ tal que

$$\alpha_P := \begin{cases} x_i & \text{si } P = P_i,\ i = 1, \ldots, r. \\ 0 & \text{en otro caso} \end{cases}$$

Escojamos un lugar $Q \in \mathbb{P}_F \backslash S$. Para $m \in \mathbb{N}$ suficientemente grande tenemos

$$\mathcal{A}_F = \mathcal{A}_F\left(mQ - \sum_{i=1}^{r}(n_i + 1)P_i\right) + F$$

por los teoremas 2.1.17 y 2.1.4. Entonces existe un elemento $z \in F$ tal que $z - \alpha \in \mathcal{A}_F\left(mQ - \sum_{i=1}^{r}(n_i + 1)P_i\right)$. Esto quiere decir

$$v_{P_i}(z - x_i) > n_i \quad \text{para } i = 1, \ldots, r. \tag{2.5}$$

$$v_P(z) \geq 0 \quad \text{Si } P \in S \backslash \{P_1, \ldots, P_r\}. \tag{2.6}$$

Escogemos ahora $y_1, \ldots, y_r \in F$ tales que $v_{P_i}(y_i) = n_i$. De la misma manera construimos $y \in F$ tal que

$$v_{P_i}(y - y_i) > n_i \quad \text{para } i = 1, \ldots, r. \tag{2.7}$$

$$v_P(y) \geq 0 \quad \text{Si } P \in S \backslash \{P_1, \ldots, P_r\}. \tag{2.8}$$

Entonces tenemos, para $i = 1, \ldots, r$,

$$v_{P_i}(y) = v_{P_i}((y - y_i) + y_i) = n_i \tag{2.9}$$

Por (2.8) y la desigualdad estricta del triángulo. Si definimos $x := y + z$ tenemos

$$v_{P_i}(x - x_i) = v_{P_i}(y + (z - x_i)) = n_i \quad (i = 1, \ldots, r)$$

por (2.9). Para $P \in S \backslash \{P_1, \ldots, P_r\}$, se tiene $v_P(x) = v_P(y + z) \geq 0$ se cumple por (2.6) y (2.8) $\square$

Teorema 2.2.2 (Teorema de Clifford). *Para todo divisor A con $0 \leq deg\, A \leq 2g-2$ se tiene lo siguiente*

$$dim\, A \leq 1 + \frac{1}{2} deg\, A$$

Demostración. Revisar [Bri]. □

Ahora vamos a revisar los elementos $x \in F$ que tiene sólo un polo.

Proposición 2.2.3. *Sea $P \in \mathbb{P}_F$. Entonces, para todo $n \geq 2g$, existe un elemento $x \in F$ cuyo polo divisor $(x)_\infty = nP$.*

Demostración. Por el teorema 2.1.17, sabemos que $dim((n-1)P) = (n-1)deg\, P + 1 - g$ y $dim(nP) = n\, deg\, P + 1 - g$. Por lo tanto $\mathcal{L}((n-1)P) \subsetneq \mathcal{L}(nP)$. Cualquier elemento $x \in \mathcal{L}(nP) \backslash \mathcal{L}((n-1)P)$ tiene polo divisor nP, pues $v_P(x) \geq -n$, pero $v_P(x) < -n+1$, por lo que $v_P(x) = -n$ y $v_Q(x) \geq 0$ si $Q \neq P$. □

La siguiente proposición caracteriza por completo al campo de funciones racional.

Proposición 2.2.4. *Para un campo de funciones F/K las siguientes condiciones son equivalentes:*

1. *F/K es racional*
2. *F/K tiene género 0 y existe un divisor $A \in \mathcal{D}_F$ con $deg\, A = 1$.*

Demostración. (1) $\Rightarrow$ (2) Mostrado en el ejemplo 1.5.18.

(2) $\Rightarrow$ (1) Sea $g = 0$ y $deg\, A = 1$. Como $deg\, A \geq 2g-1$, tenemos que $dim\, A = deg\, A + 1 - g = 2$, por el teorema 2.1.17. Por lo tanto $A \sim A'$ para algún $A' \geq 0$. Dado que $dim\, A' = 2$ existe un elemento $x \in \mathcal{L}(A') \backslash K$, tal que $(x) \neq 0$ y $(x) + A' \geq 0$. Como $A' \geq 0$ y $deg\, A' = 1$, esto es posible sólo si $A' = (x)_\infty$, el polo divisor de x. Entonces

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

por el teorema 1.5.11. □

2.3 Componentes locales de los diferenciales

En la sección anterior consideramos el encaje diagonal $F \hookrightarrow \mathcal{A}_F$ el cual manda a cada elemento $x \in F$ al correspondiente adel principal. Ahora vamos a introducir, dado un lugar $P \in \mathbb{P}_F$, otro encaje $\iota_P : F \hookrightarrow \mathcal{A}_F$.

Definición 2.3.1. Sea $P \in \mathbb{P}_F$.

1. Para cada $x \in F$ sea $\iota_P(x) \in \mathcal{A}_F$ el adel cuya P-ésima componente es x y todas las demás 0
2. Para un diferencial de Weil $\omega \in \Omega_F$ definimos su componente local $\omega_P : F \to K$ por

$$\omega_P(x) := \omega(\iota_P(x))$$

De manera que ω_P es una función K-lineal. Tenemos la siguiente proposición.

Proposición 2.3.2. *Sean $\omega \in \Omega_F$ y $\alpha = (\alpha_P) \in \mathcal{A}_F$. Entonces $\omega_P(\alpha_P) \neq 0$ a lo más para un número finito de lugares P y además*

$$\omega(\alpha) = \sum_{P \in \mathbb{P}_F} \omega_P(\alpha_P)$$

En particular,

$$0 = \sum_{P \in \mathbb{P}_F} \omega_P(1)$$

Demostración. Podemos suponer que $\omega \neq 0$ y sea $W := (\omega)$ el divisor de ω. Entonces hay un conjunto finito $S \subseteq \mathbb{P}_F$ tal que

$$v_P(W) = 0 \text{ y } v_P(\alpha_P) \geq 0 \text{ para todo } P \notin S$$

Construyamos ahora el adel $\beta = (\beta_P)$ dado por:

$$\beta_P := \begin{cases} \alpha_P & \text{Si } P \notin S \\ 0 & \text{Si } P \in S \end{cases}$$

Entonces $\beta \in \mathcal{A}_F(W)$ y $\alpha = \beta + \sum_{P \in S} \iota_P(\alpha_P)$, de manera que $\omega(\beta) = 0$ y además

$$\omega(\alpha) = \sum_{P \in S} \omega_P(\alpha_P)$$

Para $P \notin S$, $\iota_P(\alpha_P) \in \mathcal{A}_F(W)$ y por lo tanto $\omega_P(\alpha_P) = 0$. □

La siguiente proposición nos muestra que cada diferencial de Weil está determinado de forma única por sus componentes locales.

Proposición 2.3.3.

1. *Sea $\omega \neq 0$ un diferencial de Weil de F/K y $P \in \mathbb{P}_F$. Entonces*

$$v_P(\omega) = \text{máx}\{r \in \mathbb{Z} \mid \omega_P(x) = 0 \quad \text{para todo } x \in F \text{ con } v_P(x) \geq -r\}$$

En particular, $\omega_P \neq 0$.

2. *Si* $\omega, \omega' \in \Omega_F$ *y* $\omega_P = \omega'_P$ *para algún* $P \in \mathbb{P}_F$ *entonces* $\omega = \omega'$.

Demostración. Por definición $v_P(\omega) = v_P(W)$ donde W es el divisor canónico de ω. Sea ahora $s := v_P(\omega)$. Si $x \in F$ con $v_P(x) \geq -s$ tenemos que $\iota_P(x) \in \mathcal{A}_F(W)$, por lo tanto $\omega_P(x) = \omega(\iota_P(x)) = 0$. Supongamos ahora que $\omega_P(x) = 0$ para cualquier $x \in F$ con $v_P(x) \geq -s-1$. Sea ahora $\alpha = (\alpha_Q)_{Q \in \mathbb{P}_F} \in \mathcal{A}_F(W+P)$. Entonces

$$\alpha = (\alpha - \iota_P(\alpha_P)) + \iota_P(\alpha_P)$$

con $\alpha - \iota_P(\alpha_P) \in \mathcal{A}_F(W)$ y $v_P(\alpha_P) \geq -s-1$, de modo que

$$\omega(\alpha) = \omega(\alpha - \iota_P(\alpha_P)) + \omega_P(\alpha_P) = 0$$

Por lo tanto ω se anula en $\mathcal{A}_F(W+P)$, una contradicción a la definición de W. Para (2) si $\omega_P = \omega'_P$ entonces $(\omega - \omega')_P = 0$, por lo tanto $\omega = \omega'$ por (1). □

2.4 Campos de funciones y curvas no singulares

Empezaremos esta sección recordando algunos conceptos sobre anillos de Dedekind y geometría algebraica.

Definición 2.4.1. Sean $(A, \mathfrak{m}_A)$, $(B, \mathfrak{m}_B)$ anillos locales contenidos en un campo K, decimos que B *domina a* A si $A \subseteq B$ y $\mathfrak{m}_B \cap A = \mathfrak{m}_A$.

A continuación citamos un resultado que nos será bastante útil.

Teorema 2.4.2. *Sea* A *un dominio noetheriano local de dimensión uno, con ideal máximo* $\mathfrak{m}$. *Entonces las siguientes condiciones son equivalentes*

1. A *es un anillo de valuación discreta.*
2. A *es enteramente cerrado (todo elemento de su campo de cocientes que es entero sobre* A, *pertenece a* A*).*
3. A *es un anillo regular local (dim* $A = dim(\mathfrak{m}/\mathfrak{m}^2)$*).*
4. $\mathfrak{m}$ *es un ideal principal.*

Demostración. Ver [A-M] □

Definición 2.4.3. Un *dominio de Dedekind* es un dominio noetheriano enteramente cerrado de dimensión uno.

Teorema 2.4.4. *La cerradura entera (esto es, los elementos de la extensión que son enteros sobre el dominio) de un dominio de Dedekind en una extensión finita de campos de su campo de cocientes es de nuevo un dominio de Dedekind.*

Demostración. Ver [Zar] o [Lor]. □

Vamos a suponer ahora que nuestro campo base K es algebraicamente cerrado y queremos establecer una conexión entre curvas no singulares con los campos de funciones F de grado de trascendencia uno sobre K (que llamaremos también campo de dimensión uno) y los anillos de valuación discreta de F/K. Si P es un punto sobre una curva no singular $\mathcal{V}$, entonces su anillo local $\mathcal{O}_P$ es un anillo regular de dimensión uno (ver [Har]) y por lo tanto un anillo de valuación discreta. Su campo de cocientes F es el campo de funciones de la variedad $\mathcal{V}$ y dado que $K \subseteq \mathcal{O}_P$, es un anillo de valuación discreta de F/K. De esta manera los anillos locales de $\mathcal{V}$ definen un subconjunto del conjunto C_F de todos los anillos de valuación discreta de F/K. Esto es precisamente lo que motiva la definición de una curva abstracta no singular. Antes de dar la definición concreta, revisemos algunos resultados previos.

Lema 2.4.5. *Sea $\mathcal{V}$ una variedad casi-proyectiva (un abierto no vacío de una variedad proyectiva), sean $P, Q \in \mathcal{V}$ y supongamos que $\mathcal{O}_Q \subseteq \mathcal{O}_P$ como subanillos de $K(\mathcal{V})$. Entonces $P = Q$.*

Demostración. Podemos en primera instancia encajar a $\mathcal{V}$ en un espacio proyectivo lo suficientemente grande $\mathbb{P}^n$. Ahora consideramos la cerradura de $\mathcal{V}$ en ese espacio proyectivo. Podemos suponer, después de un cambio adecuado de coordenadas, que ni P ni Q se encuentran en el hiperplano H_0 definido por $x_0 = 0$. Entonces $P, Q \in \mathcal{V} \cap (\mathbb{P}^n - H_0)$ y esta variedad es afín, de manera que podemos suponer desde el principio que $\mathcal{V}$ es afín. Denotemos por A el anillo coordenado afín de $\mathcal{V}$. Entonces existen ideales máximos $\mathfrak{m}, \mathfrak{n} \subseteq A$ tales que $\mathcal{O}_P = A_\mathfrak{m}$ y $\mathcal{O}_Q = A_\mathfrak{n}$. Si $\mathcal{O}_Q \subseteq \mathcal{O}_P$ debe ocurrir $\mathfrak{m} \subseteq \mathfrak{n}$. Pero $\mathfrak{m}$ es un ideal máximo y entonces $\mathfrak{m} = \mathfrak{n}$. Por lo tanto $P = Q$. □

Lema 2.4.6. *Sea F un campo de funciones de dimensión uno sobre K y sea $x \in F$. Entonces $\{R \in C_F \mid x \notin R\}$ es un conjunto finito.*

Demostración. Esta es una simple reformulación del hecho de que todo elemento $x \in F$ tiene sólo un número finito de polos, sin embargo vamos a probar este lema pues necesitamos una construcción en particular.

Dado que R es un anillo de valuación $x \notin R$ si y sólo si $1/x = y \in \mathfrak{m}_R$. Vamos a mostrar que el conjunto $\{R \in C_F \mid y \in \mathfrak{m}_R\}$ es finito. Si $y \in K$ no existe ningún R que cumpla esa condición, por lo tanto supongamos que $y \notin K$. Consideremos ahora el anillo $K[y]$, dado que K es algebraicamente cerrado y y trascendente sobre K, $K[y]$ es un anillo de polinomios; más aún,

dado que F es finitamente generado y de grado de trascendencia uno sobre K, el campo F es una extensión finita de $K(y)$. Denotemos por B la cerradura entera de $K[y]$ en F. Entonces B es un dominio de Dedekind y también una K-álgebra finitamente generada. Ahora si $y \in R$ para algún anillo de valuación discreta R de F/K entonces $K[y] \subseteq R$ y puesto que R es enteramente cerrado en F debe ocurrir también que $B \subseteq R$. Sea $\mathfrak{n} = \mathfrak{m}_R \cap B$. Entonces $\mathfrak{n}$ es un ideal máximo de B y es dominado por R. Por otra parte, tenemos que $B_{\mathfrak{n}}$ es también un anillo de valuación discreta de F/K y entonces $B_{\mathfrak{n}} = R$ por la maximalidad de los anillos de valuación discreta. Si además $y \in \mathfrak{m}_R$, entonces $y \in \mathfrak{n}$. Por otra parte, B es el anillo de coordenadas de alguna variedad afín Y (ver Hartshorne). Dado que B es un dominio de Dedekind Y tiene dimensión uno y es no singular. Pero si $y \in \mathfrak{n}$ entonces y como función regular sobre Y se hace cero en el punto de Y correspondiente a $\mathfrak{n}$. Como $y \neq 0$ se hace cero sólo en un número finito de puntos; éstos están en correspondencia 1-1 con los ideales máximos de B y $R = B_{\mathfrak{n}}$ está determinado por el ideal máximo $\mathfrak{n}$. Por lo tanto, $y \in \mathfrak{m}_R$ sólo para un número finito de $R \in C_F$. □

Corolario 2.4.7. *Cualquier anillo de valuación discreta de F/K es isomorfo al anillo local de un punto sobre una curva no singular afín.*

Demostración. Dado R, tomemos $y \in R \backslash K$, la construcción usada en la demostración del teorema anterior nos da esa curva. □

Podemos ahora introducir el concepto de curva abstracta no singular.

Definición 2.4.8. Una *curva abstracta no singular* es un conjunto abierto $U \subseteq C_F$, donde F es un campo de funciones de dimensión uno sobre K, con la siguiente topología: tomaremos como cerrados los subconjuntos finitos de todo el espacio, el total y el vacío.

Después de esta definición no es tan claro que C_F sea una variedad algebraica, de manera que vamos a agrandar nuestra categoría de variedades, añadiendo las curvas abstractas. En este contexto, dado $U \subseteq C_F$ definimos su anillo de funciones regulares $\mathcal{O}(U) = \cap_{P \in U} R_P$. Un elemento $f \in \mathcal{O}(U)$, define una función de U en K, dada por $R_P \mapsto f \pmod{P}$; notemos que $R/\mathfrak{m}_R$ es isomorfo a K para cualquier $R \in C_F$.

Definición 2.4.9. Un morfismo $\phi : \mathcal{X} \to \mathcal{Y}$ entre curvas abstractas o variedades es una aplicación continua tal que para cada abierto $V \subseteq Y$ y cada función regular $f : V \to K$, la composición $f \circ \phi$ es una función regular sobre $\phi^{-1}(V)$.

Puede parecernos poco natural el haber agrandado nuestra categoría de variedades, sin embargo, veremos que todo curva casi-proyectiva es isomorfa a una curva abstracta y viceversa. En particular, veremos que C_F es isomorfa a una curva proyectiva no singular.

Teorema 2.4.10. *Toda curva no singular casi-proyectiva es isomorfa a una curva abstracta no singular.*

Demostración. Sea F el campo de funciones de $\mathcal{Y}$. Entonces cada anillo local $\mathcal{O}_P$ de un punto $P \in \mathcal{Y}$ es un anillo de valuación discreta de F/K. Además por uno de los lemas que hemos probado tenemos que distintos puntos dan lugar a diferentes subanillos de F. Sea $U \subseteq C_F$ el conjunto de anillos locales de $\mathcal{Y}$ y sea $\phi : \mathcal{Y} \to U$ la aplicación biyectiva dada por $\phi(P) = \mathcal{O}_P$. Debemos mostrar que U es un abierto en C_F y para esto es suficiente probar que U contiene un abierto no vacío. Podemos suponer ahora que $\mathcal{Y}$ es afín, con anillo de coordenas A, K es finitamente generado como K-álgebra y F es el campo de cocientes de A, U es el conjunto de todas las localizaciones de A y sus ideales máximos. Dado que estos anillos locales son anillos de valuación discreta, U consiste en todos todos los anillos de valuación discreta de F/K que contienen a A. Sean ahora $x_1, \ldots, x_n$ un conjunto de generadores de A sobre K. Entonces $A \subseteq R_P$ si y sólo si para toda i, $x_i \in R_P$. De esta manera $U = \bigcap U_i$ donde $U_i = \{P \in C_F \mid x_i \in R_P\}$. Por uno de los teoremas anteriores $\{P \in C_F \mid x_i \notin R_P\}$ es un conjunto finito, por lo tanto cada U_i y por lo tanto también U es abierto. Entonces el conjunto U es una curva abstracta no singular. Para revisar que ϕ es un isomorfismo, necesitamos ver que las funciones regulares en cualquier abierto, son las mismas. Pero esto se sigue de la definción de funciones regulares sobre U y el hecho de que para cualquier abierto $V \subseteq Y$, se tiene $\mathcal{O}(V) = \cap_{P \in V} \mathcal{O}_{P,Y}$. □

Vamos a enunciar ahora un resultado sobre la extensión de morfismos de curvas a variedades proyectivas.

Proposición 2.4.11. *Sea $\mathcal{X}$ una curva abstracta no singular, sea $P \in \mathcal{X}$, Y una variedad proyectiva y sea $\phi : \mathcal{X} - P \to Y$ un morfismo. Entonces existe un único morfismo $\tilde{\phi} : \mathcal{X} \to Y$ que extiende a ϕ.*

Demostración. Ver [Har] □

Veamos ahora el resultado principal de esta sección.

Teorema 2.4.12. *Sea F un campo de funciones de dimensión uno sobre K. Entonces la curva abstracta no singular C_F es isomorfa a una curva proyectiva no singular.*

Demostración. Tomemos $P \in C_F$ un punto, entonces existe una curva afín V y un punto $Q \ni V$ tal que $R_P \cong \mathcal{O}_Q$ (revisar [Har]). Se sigue entonces que el campo de funciones de V es F y además V es isomorfo a un abierto de C_F. Hemos mostrado que todo punto $P \in C_F$ tiene una vecindad isomorfa a una variedad afín.

Como C_F es casi-compacta, podemos cubrirla con un número finito de subconjuntos abiertos U_i, cada uno de los cuales es isomorfo a una variedad afín V_i. Encajemos a V_i en $\mathbb{A}^{n_i}$ como un subconjunto abierto de $\mathbb{P}^{n_i}$ y sea Y_i la cerradura de V_i en $\mathbb{P}^{n_i}$. Entonces Y_i es una variedad proyectiva y tenemos un morfismo $\phi_i : U_i \to Y_i$ el cual es un isomorfismo de U_i sobre su imagen.

Por el lema anterior, podemos encontrar un morfismo $\bar{\phi}_i : C_F \to Y_i$ que extiende a ϕ_i. Sea ahora $\prod Y_i$ el producto directo de las variedades proyectivas Y_i. Entonces Y_i es también una variedad proyectiva. Sea $\phi : C_F \to \prod Y_i$ la aplicación diagonal, es decir, $\phi(P) = \prod \bar{\phi}(P)$ y sea Y la cerradura de la imagen. Entonces Y es una variedad proyectiva y $\phi : C_F \to Y$ es un morfismo cuya imagen es densa en Y (se sigue que Y es una curva). Debemos mostrar que ϕ es iso. Para cualquier punto $P \in C_F$, tenemos que $P \in U_i$ para alguna i, esto nos da un diagrama conmutativo

$$\begin{array}{ccc} C_F & \xrightarrow{\phi} & Y \\ \uparrow & & \downarrow \pi \\ U_i & \xrightarrow{\phi_i} & Y_i \end{array}$$

de morfismos dominantes, donde π es la proyección en el factor i-ésimo, de manera que tenemos una inclusión de anillos locales

$$\mathcal{O}_{\phi_i(P),Y_i} \hookrightarrow \mathcal{O}_{\phi(P),Y} \hookrightarrow \mathcal{O}_{P,C}$$

Los anillos de los extremos son isomorfos y por lo tanto el de enmedio también lo es. Hemos visto entonces que para cualquier $P \in C_F$ la aplicación $\phi_P^* : \mathcal{O}_{\phi(P),y} \to \mathcal{O}_{P,C_F}$ es un isomorfismo: Tomemos ahora Q cualquier punto de Y. Entonces $\mathcal{O}_Q$ es dominado por algún anillo de valuación discreta R de F/K (tomemos por ejemplo la localización de la cerradura entera de $\mathcal{O}_Q$ en el ideal máximo). Sin embargo, $R = R_P$ para algún $P \in C_F$ y además $\mathcal{O}_{\phi(P)} \cong R$ y por el teorema 6.4 debemos tener $Q = \phi(P)$. Esto muestra que ϕ es suprayectiva, además ϕ es claramente inyectiva pues a distintos puntos de C_F corresponden disitintos anillos de valuación de F. Entonces ϕ es un morfismo biyectivo de C_F en Y tal que para cada punto $P \in C_F$, se tiene ϕ_P^* es un isomorfismo y por lo tanto ϕ es un isomorfismo. □

De esta manera tenemos los siguientes corolarios.

Corolario 2.4.13. *Toda curva abstracta no singular es isomorfa a una curva casi-proyectiva. Toda curva casi-proyectiva no singular es isomorfa a un abierto de una curva proyectiva no singular.*

Corolario 2.4.14. *Toda curva es birracionalmente equivalente a un curva proyectiva no singular.*

Demostración. Después de los resultados anteriores esto es inmediato, pues si Y es una curva con campo de funciones F, entonces Y es birracionalmente equivalente con C_F la cual es no singular y proyectiva. □

Finalmente terminamos con un resultado muy importante que resume todos los anteriores.

Corolario 2.4.15. *Las tres siguientes categorías son equivalentes:*

1. *Curvas proyectivas no singulares y morfismos dominantes.*
2. *Curvas casi-proyectivas y aplicaciones racionales dominantes.*
3. *Campos de funciones de dimensión uno sobre K y K-homomorfismos.*

Demostración. Tenemos un funtor evidente de 1 a 2. Tenemos también el funtor $Y \to K(Y)$ de 2 a 3, el cual induce una equivalencia de categorías. Para finalizar necesitamos un funtor de 3 a 1.

A un campo de funciones F le asociamos la curva C_F, la cual por el teorema anterior es una curva proyectiva no singular. Si $F_1 \to F_2$ es un homomorfismo, entonces como $2 \cong 3$ tenemos una aplicación racional entre esas curvas. Esto puede ser representado mediante un morfismo $\phi : U \to C_{F_2}$, donde $U \subseteq C_{K_1}$. Por el teorema anterior ϕ se extiende a un morfismo $\bar{\phi} : C_{F_1} \to C_{F_2}$. Si $F_3 \to F_2 \to F_1$ son dos homomorfismos, se sigue de la unicidad del teorema anterior los morfismos $C_1 \to C_2 \to C_3$ y $C_1 \to C_3$ son compatibles. Por lo tanto $K \mapsto C_K$ es un funtor de 3 a 1 que es claramente inverso al funtor $1 \to 2 \to 3$ de manera que tenemos la equivalencia entre estas categorías. □

Podemos estudiar más en general la teoría de campos de funciones y su relación con las curvas algebraicas a través de la teoría de esquemas. Los esquemas proporcionan un marco satisfactorio para la teoría de campos de funciones. Los esquemas podemos pensarlos como parejas $(X, \mathcal{O}_X)$, que consisten de un espacio topológico X con una gavilla de anillos $\mathcal{O}_X$ tal que, para cada punto de X existe una vecindad U junto con la restricción $\mathcal{O}_U$ de la gavilla $\mathcal{O}_X$ a U es isomorfa a un esquema afín ($X = Spec(\mathcal{O})$). Para una descripción más precisa de estas ideas, recomendamos consultar [Neu].

Capítulo 3

Extensiones de campos de funciones

3.1 Extensiones algebraicas

En este sección se discutirán algunos conceptos vitales para la teoría como son la extensión algebraica de campos de funciones, la extensión de lugares, índices de ramificación y la igualdad fundamental $\sum e_i f_i = n$.

Definición 3.1.1.

1. Un campo de funciones algebraicas F'/K' es una extensión de F/K si F'/F es una extensión algebraica y $K \subseteq K'$.

2. La extensión algebraica F'/K' de F/K es llamada extensión de campos constante si $F' = FK'$, el campo compuesto de F y K'.

3. La extensión algebraica F'/K' de F/K es llamada extensión finita si $[F' : F] < \infty$.

Uno puede considerar también extensiones arbitrarias de campos de funciones (no necesariamente algebraicas), sin embargo, nos restringiremos únicamente a extensiones algebraicas por ser las más importantes. A continuación damos un lema importante.

Lema 3.1.2. *Sea F'/K' una extensión algebraica de F/K. Entonces se tiene lo siguiente:*

1. *K'/K es algebraica y $F \cap K' = K$.*

2. *F'/K' es una extensión finita de F/K si y sólo si $[K' : K] < \infty$.*

3. Sea $F_1 := FK'$. Entonces F_1/K' es una extensión constante de campos de funciones de F/K y F'/K' es una extensión finita de F_1/K'.

Demostración. Las parte 3 del lema es clara. Para 1, notemos que el grado de trascendencia de F' sobre K es $gr\, F'/K = gr\, F'/F + gr\, F/K = 0 + 1$, por lo que $gr\, F'/K = gr\, F'/K' + gr\, K'/K = 1 + 0$ y entonces K'/K es algebraica. Finalmente si $x \in F$ y $x \in K'$ entonces x es algebraico sobre K, pertenece a F y dado que $K = \hat{K}$, tenemos la afirmación. Para verificar 2 supongamos primero que F'/K' es una extensión finita de F/K. Entonces podemos considerar a F' como un campo de funciones sobre K, donde K' es todo el campo de constantes de F'. Por el corolario 1.2.12 concluimos que $[K' : K] < \infty$. Por el contrario supongamos ahora que $[K' : K] < \infty$. Tomemos $x \in F \backslash K$. Entonces $F'/K'(x)$ es una extensión de campos finita (pues x es trascendente sobre K') y además

$$[K'(x) : K(x)] \leq [K' : K] < \infty$$

Por lo tanto

$$[F' : K(x)] = [F' : K'(x)][K'(x) : K(x)] < \infty$$

Dado que $K(x) \subseteq F \subseteq F'$ tenemos $[F' : F] < \infty$. □

Definición 3.1.3. Sea F'/K' una extensión algebraica de F/K. Un lugar $P' \in \mathbb{P}_{F'}$ se dice que yace sobre $P \in \mathbb{P}_F$ si $P \subseteq P'$. También se dice que P' es una extensión de P o que P yace bajo P' y escribimos para denotar esta situación $P' \mid P$.

Lema 3.1.4. *Para todo $P' \in \mathbb{P}_{F'}$, tal que $\mathcal{O}_P \subsetneq \mathcal{O}_{P'}$ se tiene $F \cap \mathcal{O}_{P'} \neq F$.*

Demostración. En particular, veremos que

$$\mathcal{O}_P \subseteq \mathcal{O}_{P'} \Rightarrow \mathcal{O}_P = F \cap \mathcal{O}_{P'} \tag{3.1}$$

Claramente $F \cap \mathcal{O}_{P'}$ es un subanillo de F con $\mathcal{O}_P \subseteq F \cap \mathcal{O}_{P'}$. Entonces $F \cap \mathcal{O}_{P'} = \mathcal{O}_P$ o bien $F \cap \mathcal{O}_{P'} = F$ por la maximalidad de $\mathcal{O}_P$. Supongamos que $F \cap \mathcal{O}_{P'} = F$, es decir, $F \subseteq \mathcal{O}_{P'}$. Tomemos un elemento $z \in F' \backslash \mathcal{O}_{P'}$. Puesto que F'/F es algebraica, existe una ecuación

$$z^n + c_{n-1}z^{n-1} + \cdots + c_1 z + c_0 = 0 \tag{3.2}$$

con $c_i \in F$. Tenemos $v_{P'}(z^n) = n v_{P'}(z) < 0$ pues $z \notin \mathcal{O}_P$, por lo tanto

$$v_{P'}(z^n) < v_{P'}(c_i z^i) \quad \text{para } i = 0, \ldots, n-1$$

Pues supusimos que $F \subseteq \mathcal{O}_{P'}$. La desigualdad estricta del triángulo nos indica

$$v_{P'}(z^n + c_{n-1}z^{n-1} + \cdots + c_1 z + c_0) = n v_{P'}(z) \neq v_{P'}(0)$$

Esta contradicción a (3.1) demuestra (3.2). □

Proposición 3.1.5. *Sea F'/K' una extensión algebraica de F/K. Sea $P \in \mathbb{P}_F$ (resp. $P' \in \mathbb{P}_{F'}$) y sea $\mathcal{O}_P \subseteq F$ (resp. $\mathcal{O}_{P'} \subseteq F'$) y denotemos la valuación correspondiente por v_P (resp. $v_{P'}$). Entonces las siguientes afirmaciones son equivalentes.*

1. *$P' \mid P$.*
2. *$\mathcal{O}_P \subseteq \mathcal{O}_{P'}$.*
3. *Existe un entero $e \geq 1$ tal que $v_{P'}(x) = ev_P(x)$ para todo $x \in F$.*

Más aún, si $P' \mid P$ entonces

$$P = P' \cap F$$

Por esta razón P es llamado la restricción de P' a F.

Demostración. $1 \Rightarrow 2$. Supongamos que $P' \mid P$, pero que $\mathcal{O}_P \nsubseteq \mathcal{O}_{P'}$. Entonces existe una $u \in F$ tal que $v_P(u) \geq 0$ y $v_{P'}(u) < 0$. Como $P \subseteq P'$ se debe tener que $v_P(u) = 0$. Escojamos $t \in F$ con $v_P(t) = 1$, entonces $t \in P'$ y $r := v_{P'}(t) > 0$. De manera que

$$v_P(u^r t) = r v_P(u) + v_P(t) = 1,$$

$$v_{P'}(u^r t) = r v_{P'}(u) + v_{P'}(t) \leq -r + r = 0$$

Esto quiere decir que $u^r t \in P \backslash P'$, una contradicción a $P \subseteq P'$.

$2 \Rightarrow 1$. Supongamos ahora que $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$. Sea $y \in P$ entonces $y^{-1} \notin \mathcal{O}_P$ por la proposición 1.2.2, por lo tanto $y^{-1} \notin \mathcal{O}_{P'}$ por (3.1). Al aplicar otra vez la proposición 1.2.2 concluimos que $(y^{-1})^{-1} = y \in P'$, por lo tanto $P \subseteq P'$. $2 \Rightarrow 3$. Sea $u \in F$ un elemento tal que $v_P(u) = 0$, entonces $u, u^{-1} \in \mathcal{O}_P \subseteq \mathcal{O}_{P'}$, por lo que $v_{P'}(u) = 0$. Tomemos $t \in F$ con $v_P(t) = 1$ y sea $e = v_{P'}(t)$. Como $P \subseteq P'$ tenemos que $e \geq 1$. Sea $0 \neq x \in F$ y $v_P(x) = r \in \mathbb{Z}$. Entonces $v_P(xt^{-r}) = 0$ y tenemos entonces

$$v_{P'}(x) = v_{P'}(xt^{-r}) + v_{P'}(t^r) = 0 + r v_{P'}(t) = e v_P(x)$$

$3 \Rightarrow 2$ Si $x \in \mathcal{O}_P \Rightarrow v_P(x) \geq 0 \Rightarrow v_{P'}(x) = e v_P(x) \geq 0 \Rightarrow x \in \mathcal{O}_{P'}$. Hemos probado la equivalencia entre las tres afirmaciones y que además $\mathcal{O}_P = \mathcal{O}_{P'} \cap F$ si $P' \mid P$ y la afirmación $P = P' \cap F$ es ahora trivial por la afirmación 3. □

Una consecuencia de esta proposición es que existe un encaje canónico del campo de clases residuales $F_P = \mathcal{O}_P/P$ en el campo de clases residuales $F'_{P'} = \mathcal{O}_{P'}/P'$ dado por

$$x(P) \mapsto x(P') \quad \text{para } x \in \mathcal{O}_P$$

Definición 3.1.6. Sea F'/K' una extensión algebraica de F/K y sea $P' \in \mathbb{P}_{F'}$ un lugar de F'/K' que yace sobre $P \in \mathbb{P}_F$.

1. El entero $e(P' \mid P) = e$ con $v_{P'}(x) = ev_P(x)$ para todo $x \in F$ es llamado *el índice de ramificación* de P' sobre P. Decimos que $P' \mid P$ es ramificada si $e(P' \mid P) > 1$ y $P' \mid P$ es no ramificada si $e(P' \mid P) = 1$.

2. $f(P' \mid P) := [F'_{P'} : F_P]$ es llamado el *grado relativo* de P' sobre P.

Notemos que $f(P' \mid P)$ puede ser finito o infinito, sin embargo, el índice de ramificación es siempre un natural.

Proposición 3.1.7. *Sea F'/K' una extensión algebraica de F/K y P' un lugar de F'/K' que yace sobre $P \in \mathbb{P}_F$. Entonces*

1. $f(P' \mid P) < \infty \iff [F' : F] < \infty$.

2. *Si F''/K'' es una extensión algebraica de F'/K' y P'' es una extensión de P' entonces*

$$e(P'' \mid P) = e(P'' \mid P')e(P' \mid P),$$
$$f(P'' \mid P) = f(P'' \mid P')f(P' \mid P).$$

Demostración. Consideremos los encajes naturales $K \subseteq F_P \subseteq F'_{P'}$ y $K \subseteq K' \subseteq F'_{P'}$ donde $[F_P : K] < \infty$ y $[F'_{P'} : K'] < \infty$. Se sigue que

$$[F'_{P'} : F_P] < \infty \iff [K' : K] < \infty.$$

Notemos que la última condición es equivalente a $[F' : F] < \infty$ por el lema 3.1.2. La afirmación sobre los índices de ramificación es inmediata de las definiciones y $f(P'' \mid P) = f(P'' \mid P')f(P' \mid P)$ se sigue de las inclusiones $F_P \subseteq F'_{P'} \subseteq F''_{P''}$. □

Proposición 3.1.8. *Sea F'/K' una extensión algebraica de F/K.*

1. *Para cualquier lugar $P' \in \mathbb{P}_{F'}$ existe exactamente un lugar $P \in \mathbb{P}_F$ tal que $P' \mid P$ el cual es $P = F \cap P'$.*

2. *Recíprocamente para cada $P \in \mathbb{P}_F$ lugar de F existe al menos uno y a lo más un número finito de lugares $P' \in \mathbb{P}_{F'}$ extensiones de P.*

Demostración. La demostración se basa en la siguiente afirmación

$$\text{existe algún } z \in F,\ z \neq 0 \text{ con } v_{P'}(z) \neq 0. \tag{3.3}$$

Supongamos que esto es falso. Tomemos $t \in F'$ con $v_{P'}(t) > 0$, dado que F'/F es algebraica existe una ecuación

$$c_n t^n + c_{n-1}t^{n-1} + \cdots + c_1 t + c_0 = 0$$

con $c_i \in F$, $c_0 \neq 0$. Por hipótesis $v_{P'}(c_0) = 0$ y $v_{P'}(c_i t^i) = v_{P'}(c_i) + i v_{P'}(t) > 0$ para $i = 1, \ldots, n$, lo cual contradice la desigualdad estricta del triángulo. Definamos ahora $\mathcal{O} := \mathcal{O}_{P'} \cap F$ y $P := P' \cap F$. Por (3.3) es evidente que $\mathcal{O}$ es un anillo de valuación de F/K y P es su ideal correspondiente. La unicidad es trivial.

Supongamos ahora que tenemos un lugar P de F/K. Tomemos $x \in F \backslash K$ cuyo único cero sea P (lo cual es posible por la proposición 2.2.3). Para $P' \in \mathbb{P}_{F'}$ afirmamos que

$$P' \mid P \iff v_{P'}(x) > 0$$

Como x tiene sólo un número finito de ceros en F'/K' la parte 2 es una consecuencia inmediata de la afirmación anterior. Ahora, si $P' \mid P$ entonces $v_{P'}(x) = e(P' \mid P) v_P(x) > 0$. Recíprocamente si $v_{P'}(x) > 0$ sea Q el lugar de F/K que yace bajo P'; entonces $v_Q(x) > 0$, por lo tanto $Q = P$, pues P era el único cero de x en F/K. □

La proposición anterior nos permite definir un homomorfismo de $\mathcal{D}_F$ en $\mathcal{D}_{F'}$.

Definición 3.1.9. Sea F'/K' una extensión algebraica de F/K. Para un lugar $P \in \mathbb{P}_F$ definimos su conorma (con respecto a F'/F) de la siguiente manera

$$Con_{F'/F}(P) := \sum_{P'|P} e(P' \mid P) P'$$

Esta conorma puede extenderse a un homomorfismo de $\mathcal{D}_F$ en $\mathcal{D}_{F'}$ de la siguiente manera:

$$Con_{F'/F}(\sum n_P P) := \sum n_P Con_{F'/F}(P)$$

La conorma se comporta bien en torres de campos. Si $F \subseteq F' \subseteq F''$ una consecuencia inmediata de las fórmulas para el índice de ramificación es

$$Con_{F''/F}(A) = Con_{F''/F'}(Con_{F'/F}(A))$$

Para todo $A \in \mathcal{A}_F$. Una propiedad interesante de la conorma es que manda divisores principales en divisores principales.

Proposición 3.1.10. *Sea F'/K' una extensión algebraica del campo de funciones F/K. Para cualquier $0 \neq x \in F$, sean $(x)_0^F$, $(x)_\infty^F$, $(x)^F$ y respectivamente sean $(x)_0^{F'}$, $(x)_\infty^{F'}$, $(x)^{F'}$, los ceros, polos y divisor principal de $x \in \mathcal{D}_F$ y en $\mathcal{D}_{F'}$. Entonces*

$$Con_{F'/F}((x)_0^F) = (x)_0^{F'},\ Con_{F'/F}((x)_\infty^F) = (x)_\infty^{F'},\ Con_{F'/F}((x)^F) = (x)^{F'}.$$

Demostración. De la definición de divisor principal tenemos lo siguiente

$$(x)^{F'} = \sum_{P' \in \mathbb{P}_{F'}} v_{P'}(x)P' = \sum_{P \in \mathbb{P}_F} \sum_{P'|P} e(P' \mid P) v_P(x) P'$$

$$= \sum_{P \in \mathbb{P}_F} v_P(x) Con_{F'/F}(P) = Con_{F'/F}(\sum_{P \in \mathbb{P}_F} v_P(x)P)$$

$$= Con_{F'/F}((x)^F).$$

Si consideramos ahora sólo la parte positiva o negativa del divisor principal, obtenemos el resultado para esos casos. □

Esta proposición nos dice que la conorma induce un homomorfismo entre los grupos de Picard $Con_{F'/F} : Pic_F \to Pic_{F'}$. Ahora veremos un lema que nos será bastante útil.

Lema 3.1.11. *Sea K'/K una extensión finita de campos y sea x trascendente sobre K. Entonces*

$$[K'(x) : K(x)] = [K' : K]$$

Demostración. Podemos suponer que $K' = K(\alpha)$ para algún elemento $\alpha \in K'$. Tenemos claramente que $[K'(x) : K(x)] \leq [K' : K]$ pues $K'(x) = K(x)(\alpha)$. Para verificar la otra desigualdad, debemos probar que el polinomio irreducible $\phi(T) \in K[T]$ de α permanece irreducible sobre $K(x)$. Supongamos que esto es falso, entonces $\phi(T) = g(T)h(T)$ con $g(T)$, $h(t) \in K(x)[T]$, ambos polinomios mónicos y de grado menor que el grado de $\phi(T)$. Como $\phi(\alpha) = 0$, α debe ser raíz de alguno de los dos polinomios $g(T)$ o $h(T)$. Supongamos que es raíz de $g(T)$. Este polinomio es de la forma

$$g(T) = T^r + c_{r-1}(x)T^{r-1} + \cdots + c_0(x)$$

con $c_i(x) \in K(x)$ y $r < deg\,\phi$ y además

$$\alpha^r + c_{r-1}(x)\alpha^{r-1} + \cdots + c_0(x) = 0$$

multiplicamos por el común denominador y obtenemos

$$g_r(x)\alpha^r + g_{r-1}(x)\alpha^{r-1} + \cdots + g_0(x) = 0$$

para polinomios $g_i \in K[x]$. Podemos suponer que no todos los g_i son divisibles por x. Si hacemos ahora $x = 0$ obtenemos una ecuación no trivial para α sobre K de grado menor que $deg\,\phi$, lo cual es una contradicción. □

Teorema 3.1.12. *Sea F'/K' una extensión finita de campos de F/K, $P \in \mathbb{P}_F$ y $P_1, \ldots P_m$ todas las extensiones de P en F'. Sea $e_i := e(P_i \mid P)$ el índice de ramificación y $f_i := f(P_i \mid P)$ el grado relativo de $P_i \mid P$. Entonces*

$$\sum_{i=1}^{m} e_i f_i = [F' : F]$$

Demostración. Consideremos, de nueva cuenta, $x \in F$ tal que P es su único cero en F/K con $v_P(x) = r > 0$. Por la observación hecha en la demostración de la proposición 3.1.8 los lugares $P_1, \ldots, P_m$ son exactamente los ceros de x en F'. Ahora vamos a evaluar el grado $[F' : K(x)]$ de dos maneras distintas.

$$\begin{aligned}
[F' : K(x)] &= [F' : K'(x)][K'(x) : K(x)] \qquad (3.4)\\
&= (\sum_{i=1}^{m} v_{P_i}(x) deg\, P_i)[K' : K]\\
&= \sum_{i=1}^{m} (e_i v_P(x))[F'_{P_i} : K'][K' : K]\\
&= r \sum_{i=1}^{m} e_i [F'_{P_i} : F_P][F_P : K]\\
&= r deg\, P \sum_{i=1}^{m} e_i f_i.
\end{aligned}$$

Por otra parte tenemos

$$[F' : K(x)] = [F' : F][F : K(x)] = [F' : F] r\, deg\, P \qquad (3.5)$$

Dado que rP es el cero divisor de x en F/K, al comparar (3.4) y (3.5) tenemos el resultado. □

Corolario 3.1.13. *Sea F'/K' una extensión finita de F/K. Entonces para cualquier divisor $A \in \mathcal{D}_F$,*

$$deg\, Con_{F'/F}(A) = \frac{[F' : F]}{[K' : K]}\, deg\, A$$

Demostración. Es suficiente probar el resultado para un divisor primo $P \in \mathbb{P}_F$.

Tenemos

$$\begin{aligned} deg\, Con_{F'/F}(P) &= deg\left(\sum_{P'|P} e(P' \mid P)\, P'\right) \\ &= \sum_{P'|P} e(P' \mid P)\,[F'_{P'} : K'] \\ &= \sum_{P'|P} e(P' \mid P)\,\frac{[F'_{P'} : K]}{[K' : K]} \\ &= \frac{1}{[K' : K]} \sum_{P'|P} e(P' \mid P)[F'_{P'} : F_P][F_P : K] \\ &= \frac{1}{[K' : K]} \left(\sum_{P'|P} e(P' \mid P)\, f(P' \mid P)\right) deg\, P \\ &= \frac{[F' : F]}{[K' : K]}\, deg\, P \end{aligned}$$

□

Para finalizar esta sección vamos a proporcionar un criterio de irreducibilidad muy útil; un caso particular de la siguiente proposición es conocido como criterio de Eisenstein.

Proposición 3.1.14. *Sea F/K un campo de funciones y sea $\psi(T)$ un polinomio*

$$\psi(T) = a_n T^n + a_{n-1} T^{n-1} + \cdots + a_0$$

cuyos coeficientes $a_i \in F$. Supongamos que existe un lugar $P \in \mathbb{P}_F$ tal que se cumple alguna de las dos siguientes condiciones:

1. *$v_P(a_n) = 0$, $v_P(a_i) \geq v_P(a_0) > 0$ para $i = 1, \ldots, n-1$ y además $mcd(n, v_P(a_0)) = 1$.*
2. *$v_P(a_n) = 0$, $v_P(a_i) \geq 0$, para $i = 1, \ldots, n-1$, $v_P(a_0) < 0$ y por otra parte $mcd(n, v_P(a_0)) = 1$.*

Entonces $\psi(T)$ es irreducible en $F[T]$. Si $F' = F(y)$ con y una raíz del polinomio $\psi(T)$, entonces P tiene una única extensión $P' \in \mathbb{P}_{F'}$ y tenemos $e(P' \mid P) = n$ y $f(P' \mid P) = 1$.

Demostración. Sea F' una extensión tal que $F' = F(y)$ con $\psi(y) = 0$. Tenemos que el grado de $F'/F \leq deg\, \psi(T) = n$ y la igualdad se da si y sólo si $\psi(T)$ es irreducible. Sea P' una extensión de P. Ya que $\psi(y) = 0$ tenemos

$$-a_n y^n = a_0 + \cdots + a_{n-1} y^{n-1} \tag{3.6}$$

Supongamos que ocurre (1). Dado que $v_{P'}(a_n) = 0$ y $v_{P'}(a_i) > 0$ para $i = 1, \ldots, n-1$, se tiene $v_{P'}(y) > 0$ (pues si $v_{P'}(y) < 0$, llegamos a $nv_{P'}(y) = (n-1)v_{P'}(y)$, lo cual no puede ser). Si denotamos por $e = e(P' \mid P)$ sabemos que $v_{P'}(a_0) = e\, v_P(a_0)$ y $v_{P'}(a_i y^i) = e\, v_P(a_i) + i\, v_{P'}(y) > e\, v_P(a_0)$ para $i = 1, \ldots, n-1$. Por la desigualdad estricta del triángulo la ecuación (3.6) implica

$$n\, v_{P'}(y) = e\, v_P(a_0).$$

Puesto que el $mcd(n, v_P(a_0)) = 1$, tenemos que $n \mid e$ y por lo tanto $n \leq e$. Por otra parte, tenemos $e \leq [F' : F] \leq n$, lo cual nos lleva a

$$n = e = [F' : F]$$

Todas las demás afirmaciones de esta proposición se siguen de esta igualdad y la demostración en el caso (2) es análoga. □

3.2 Subanillos de campos de funciones

Definición 3.2.1. Un subanillo de F/K campo de funciones es un anillo R tal que $K \subseteq R \subseteq F$, y R no es un campo.

Una observación inmediata de esta definición es que si R es un subanillo de F/K entonces $K \subsetneq R \subsetneq F$. Podemos encontrar dos ejemplos clásicos que son los siguientes:

1. $R = \mathcal{O}_P$ para algún $P \in \mathbb{P}_F$.
2. $R = K[x_1, \ldots, x_n]$ donde $x_1, \ldots, x_n \in F \backslash K$.

El anillo $\mathcal{O}_P$ es obviamente un subanillo; para verificar que $K[x_1, \ldots, x_n]$ es también un subanillo, nos falta mostrar que no es campo. Para esto escojamos un lugar $P \in \mathbb{P}_F$ tal que $v_P(x_1) \geq 0, \ldots, v_P(x_n) \geq 0$. Sea $x = x_1$ y $d := deg\, P$. Dado que las clases residuales $1, x(P), \ldots, x^d(P) \in \mathcal{O}_P/P$ son linealmente dependientes sobre K podemos encontrar $\alpha_0, \ldots, \alpha_d \in K$ tales que el elemento $z = \alpha_0 + \alpha_1 x + \cdots + \alpha_d x^d$ es no cero y además $v_P(z) > 0$ (nótese que x es trascendente sobre K pues $x \notin K$). Entonces $z \in K[x_1, \ldots, x_n]$, pero $z^{-1} \notin K[x_1, \ldots, x_n]$ pues $v_P(y) \geq 0$ para cualquier $y \in K[x_1, \ldots, x_n]$.

Un ejemplo más general que 1 está dado en la siguiente definición.

Definición 3.2.2. Sea $\varnothing \neq S \subsetneq \mathbb{P}_F$, definimos

$$\mathcal{O}_S := \{z \in F \mid v_P(z) \geq 0 \text{ para todo } P \in S\}$$

es decir la intersección de todos los anillos de valuación $\mathcal{O}_P$ con $P \in S$. Cualquier anillo $R \subseteq F$ que sea de la forma $\mathcal{O}_S$ para algún $\varnothing \neq S \subsetneq \mathbb{P}_F$ es llamado *anillo de holomorfía* de F/K.

Veamos algunos resultados inmediatos.

Lema 3.2.3.

1. *Cualquier anillo de valuación $\mathcal{O}_P$ es un anillo de holomorfía.*
2. *Cualquier anillo de holomorfía es un subanillo de F/K.*
3. *Para cualquier $P \in \mathbb{P}_F$ y $\varnothing \neq S \subsetneq \mathbb{P}_F$ tenemos lo siguiente*

$$\mathcal{O}_S \subseteq \mathcal{O}_P \iff P \in S$$

En consecuencia $\mathcal{O}_S = \mathcal{O}_T \iff S = T$.

Demostración. La demostración de 1 es clara. (2) Únicamente debemos probar que $\mathcal{O}_S$ no es un campo. Sea $P_0 \in S$, dado que $S \neq \mathbb{P}_F$, podemos encontrar por aproximación fuerte un elemento no cero $z \in F$, tal que

$$v_{P_0}(z) > 0 \quad \text{y} \quad v_P(z) \geq 0 \quad \text{para toda } P \in S$$

Entonces $z \in \mathcal{O}_S$, pero $z^{-1} \notin \mathcal{O}_S$. (3) Supongamos que $P \notin S$, de nuevo, por aproximación fuerte podemos encontrar un elemento no cero $x \in F$ tal que

$$v_P(x) > 0 \quad \text{y} \quad v_Q(x) \geq 0 \text{para todo } Q \in S.$$

El único problema es cuando $P \cup S = \mathbb{P}_F$, en ese caso tomamos $x \in \mathcal{O}_S$ que tenga al menos un cero en S, dado que x debe tener un polo, tenemos que $v_P(x) < 0$. Un elemento que satisfaga las condiciones anteriores, está en $\mathcal{O}_S$, pero no en $\mathcal{O}_P$. Esto quiere decir que $P \notin S$ implica $\mathcal{O}_S \not\subseteq \mathcal{O}_P$. Las otras afirmaciones son claras. □

Revisemos ahora un concepto fundamental concerniente a los subanillos de campos de funciones.

Definición 3.2.4. Sea R subanillo de F/K.

1. Un elemento $z \in F$ se dice que es *entero sobre* R si $f(z) = 0$ para algún polinomio mónico $f(X) \in R[X]$.
2. El conjunto

$$B_F(R) := \{z \in F \mid z \text{ es entera sobre } R\}$$

es llamado *la cerradura entera* de R en F.

3. Sea $F_0 \subseteq F$ el campo de cocientes de R. El anillo R es llamado *enteramente cerrado* si $B_{F_0}(R) = R$, i.e. todo $z \in F_0$ que es entero sobre R ya se encuentra en R.

Teorema 3.2.5. *Sea $\mathcal{O}_S$ un anillo de holomorfía de F/K. Entonces*

1. *F es el campo de cocientes de $\mathcal{O}_S$.*
2. *$\mathcal{O}_S$ es enteramente cerrado.*

Demostración. (1) Sea $x \in F$, no cero. Por el teorema de aproximación fuerte, existe un elemento $z \in F$ tal que

$$v_P(z) \geq \text{máx}\{0, v_P(x^{-1})\} \text{ para todo } P \in S.$$

Claramente $z \in \mathcal{O}_S$ y $y := zx \in \mathcal{O}_S$, por lo que $x = yz^{-1}$ está en el campo de cocientes de $\mathcal{O}_S$.

(2) Sea $u \in F$ entero sobre $\mathcal{O}_S$. Tomemos una relación entera de u

$$u^n + a_{n-1}u^{n-1} + \cdots + a_0 = 0$$

con $a_i \in \mathcal{O}_S$. Debemos mostrar que $v_P(u) \geq 0$ para todo $P \in S$. Supongamos que esto no ocurre, así que $v_P(u) < 0$, para algún $P \in S$. Como $v_P(a_i) \geq 0$, tenemos

$$v_P(u^n) = n\, v_P(u) < v_P(a_i u^i)$$

para $i = 1, \ldots, n-1$. Entonces la desigualdad estricta del triángulo nos da una contradicción a la ecuación entera. □

Teorema 3.2.6. *Sea R un subanillo de F/K y*

$$S(R) = \{P \in \mathbb{P}_F \mid R \subseteq \mathcal{O}_P\}$$

entonces

1. *$\varnothing \neq S(R) \subsetneq \mathbb{P}_F$.*
2. *La cerradura entera de R en F $B_F(R) = \mathcal{O}_{S(R)}$. En particular $B_F(R)$ es un subanillo enteramente cerrado de F/K.*

Demostración. (1) Dado que R no es un campo, podemos encontrar un ideal propio no trivial $I \subsetneq R$ y por el teorema 1.2.14, existe un lugar P y un anillo de valuación tales $\mathcal{O}_P \supseteq R$ y $P \supseteq I$. Por lo tanto $\varnothing \neq S(R)$. Por otro lado, consideremos un elemento $x \in R$ que sea trascendente sobre K. Cualquier lugar Q que sea polo de x no pertenece a $S(R)$.

(2) Como $R \subseteq \mathcal{O}_{S(R)}$ y $\mathcal{O}_{S(R)}$ es un anillo enteramente cerrado, tenemos que $B_F(R) \subseteq \mathcal{O}_{S(R)}$. Para probar la otra inclusión, consideremos $z \in \mathcal{O}_{S(R)}$. Afirmamos que

$$z^{-1}\, R[z^{-1}] = R[z^{-1}] \tag{3.7}$$

Supongamos que (3.7) es falsa, es decir $z^{-1}\,R[z^{-1}]$ es un ideal propio de $R[z^{-1}]$, por el teorema 1.2.14 podemos encontrar un lugar $Q \in \mathbb{P}_F$ tal que

$$R[z^{-1}] \subseteq \mathcal{O}_Q \quad \text{y } z^{-1} \in Q.$$

Se sigue entonces que $Q \in S(R)$ y $z \notin \mathcal{O}_Q$, lo cual es una contradicción a $z \in \mathcal{O}_{S(R)}$. Por lo tanto tenemos (3.7). De (3.7) obtenemos una relación

$$1 = z^{-1} \sum_{i=0}^{s} a_i (z^{-1})^i \tag{3.8}$$

con $a_0, \ldots, a_s \in R$. Si multiplicamos (3.8) por z^{s+1} obtenemos

$$z^{s+1} - \sum_{i=0}^{s} a_i z^{s-i} = 0$$

y ésta es una ecuación entera de z sobre R. □

Como una consecuencia de los teoremas anteriores, tenemos el siguiente corolario.

Corolario 3.2.7. *Un subanillo R de F/K que tenga como campo de cocientes a F es enteramente cerrado si y sólo si es un anillo de holomorfía.*

Proposición 3.2.8. *Sea $\mathcal{O}_S$ un anillo de holomorfía de F/K. Entonces existe una correspondencia uno a uno entre S y el conjunto de ideales máximos de $\mathcal{O}_S$, dada por*

$$P \mapsto M_P := P \cap \mathcal{O}_S \quad \textit{(para } P \in S\textit{)}$$

Mas aún la aplicación $\phi : \mathcal{O}_S/M_P \to F_P$ dada por

$$x + M_P \mapsto x + P$$

es un isomorfismo

Demostración. Para $P \in S$ consideremos el homomorfismo de anillos $\Phi : \mathcal{O}_S \to F_P$ definido como $x \mapsto x + P$. Afirmamos que este homomorfismo es epi. Para esto sea $z + P \in \mathbb{F}_P$ con $z \in \mathcal{O}_P$. Por el teorema de aproximación fuerte, existe un $x \in F$ que satisface

$$v_P(x - z) > 0 \text{ y } v_Q(x) \geq 0 \text{ para todo } Q \in S \backslash \{P\}$$

Entonces es fácil ver por la condición anterior que $v_P(x) \geq 0$ y por lo ttanto $x \in \mathcal{O}_S$ y $\Phi(x) = z + P$. El núcleo de Φ es $M_P = P \cap \mathcal{O}_S$, por lo tanto Φ induce un isomorfismo $\phi : \mathcal{O}_S/M_P \to F_P$. Dado que F_P es un campo, el ideal

M_P es un ideal máximo de $\mathcal{O}_S$ y el teorema de aproximación fuerte muestra que $M_P \neq M_Q$. Únicamente resta probar que todo ideal máximo de $\mathcal{O}_S$ es de la forma $P \cap \mathcal{O}_S$ con algún $P \in S$. Sea $M \subseteq \mathcal{O}_S$ un ideal máximo. Por el teorema 1.2.14 existe un lugar $P \in \mathbb{P}_F$ con

$$M \subseteq P \text{ y } \mathcal{O}_S \subseteq \mathcal{O}_P$$

El lema 3.2.3 muestra que $P \in S$. Como $M \subseteq P \cap \mathcal{O}_S$ y M es un ideal máximo de $\mathcal{O}_S$, tenemos que $M = P \cap \mathcal{O}_S$. □

En la primera proposición 1.2.4 vimos que $\mathcal{O}_P$ era un dominio de ideales principales. Se puede demostrar usando el teorema de aproximación fuerte que $\mathcal{O}_S$ es siempre un dominio de Dedekind. Los anillos de holomorfía en general no son dominios de ideales principales, no obstante, cuando el conjunto S es finito siguen siendo dominios de ideales principales.

Proposición 3.2.9. *Si $S \subsetneq \mathbb{P}_F$ es un conjunto finito no vacío de lugares de F/K, entonces tenemos que $\mathcal{O}_S$ es un dominio de ideales principales.*

Demostración. Sea $S = \{P_1, \ldots P_k\}$ y sea $I \neq 0$ un ideal contenido en $\mathcal{O}_S$. Para $i = 1, \ldots, k$ escojamos $x_i \in I$ tal que

$$v_{P_i}(x_i) = n_i \leq v_{P_i}(u) \quad \text{para todo } u \in I$$

Esto es posible, desde luego, porque $v_{P_i}(u) \geq 0$ para todo $u \in I$ y cualquier $I \neq 0$. Por el teorema de aproximación fuerte, podemos encontrar $z_i \in F$ tal que

$$v_{P_i}(z_i) = 0 \quad \text{y } v_{P_j}(z_i) > n_j \text{ para } j \neq i.$$

Claramente $z_i \in \mathcal{O}_S$ por lo tanto el elemento $x = \sum_{i=1}^{n} x_i z_i \in I$. Por la desigualdad estricta del triángulo tenemos $v_{P_i}(x) = n_i$ para $i = 1, \ldots, k$. El resultado se sigue si podemos probar que $I \subseteq x\mathcal{O}_S$. Consideremos un elemento $z \in I$. Definamos $y = x^{-1}z$, entonces

$$v_{P_i}(y) = v_{P_i}(z) - n_i \geq 0 \quad \text{para } i = 1, \ldots, k.$$

De manera que $y \in \mathcal{O}_S$ y $z = xy \in x\mathcal{O}_S$. □

3.3 Bases locales enteras

El objetivo de esta sección es estudiar la cerradura entera de un subanillo de F/K en una extensión de F. Siempre vamos a considerar la situación siguiente: F/K es un campo de funciones con campo de constantes K y $F \subseteq F'$ es una extensión finita de campos.

A continuación daremos un resultado que se generaliza en álgebra conmutativa (ver por ejemplo [Mat]).

Proposición 3.3.1. *Sea R un subanillo de F/K enteramente cerrado cuyo campo de cocientes es F, i.e., R es un anillo de holomorfía de F/K. Sea $z \in F'$ y $\phi(T) \in F[T]$ su polinomio mínimo. Entonces z es entero sobre R si y sólo si $\phi(T) \in R[T]$.*

Demostración. Por definición $\phi(T)$ es el único polinomio irreducible mónico con coeficientes en F tal que $\phi(z) = 0$. Si $\phi(T) \in R[T]$ entonces obviamente z es entero sobre R. Supongamos ahora que $z \in F'$ entero sobre R. Tomemos un polinomio mónico $f(T) \in R[T]$ con $f(z) = 0$. Como $\phi(T)$ es el polinomio mínimo de z sobre F existe otro polinomio $\psi(T)$ tal que $f(T) = \phi(T)\psi(T)$. Sea ahora F''/F' un campo de descomposición para $\phi(T)$ y sea R'' la cerradura entera de R en F''. Dado que todas las raíces de $\phi(T)$ son raíces de $f(T)$, se encuentran en R''. Los coeficientes de $\phi(T)$ son combinaciones polinomiales de las raíces, por las fórmulas de Vieta, de manera que $\phi(T) \in R''[T]$. Pero $\phi(T) \in F[T]$ y $F \cap R'' = R$ pues R es enteramente cerrado, luego $\phi(T) \in R[T]$. □

Corolario 3.3.2. *Con la misma notación usada en la proposición anterior, consideremos $Tr_{F'/F} : F' \to F$ la traza de F' en F y sea $x \in F'$ entero sobre R. Entonces $Tr_{F'/F}(x) \in R$.*

Demostración. Recordaremos en primera instancia algunas propiedades de la traza que ocuparemos más adelante antes de probar este corolario. Supongamos que tenemos una extensión de campos M/L de grado n. La traza de un elemento $z \in M$ se define como la traza de la transformación lineal $\mu_z : M \to M$, dada por $\mu_z(x) = zx$. Si M/L no es separable, la función traza es idénticamente cero (ver [Mor]). Entonces podemos suponer en adelante que la extensión es separable. Esta aplicación $Tr_{M/L} : M \to L$ es L-lineal y no es idénticamente cero. Podemos describir a la traza de la siguiente manera: sea Ψ una cerradura algebraica de L. Un encaje de M/L en Ψ es un homomorfismo de campos $\sigma : M \to \Psi$ tal que $\sigma(a) = a$ para todo $a \in L$. Dado que M/L es separable, existen exactamente n encajes distintos $\sigma_1, \ldots, \sigma_n$ de M/L en Ψ y para $x \in M$ tenemos

$$Tr_{M/L}(x) = \sum_{i=1}^{n} \sigma_i(x)$$

Si $\phi(T) = T^r + a_{r-1}T^{r-1} + \cdots + a_0 \in L[T]$ es el polinomio mínimo de x sobre L, tenemos

$$Tr_{M/L}(x) = -sa_{r-1}, \text{ donde } s = [M : L(x)] \tag{3.9}$$

La traza se comporta bien en cadenas de campos, es decir, si $L \subseteq M \subseteq H$, entonces

$$Tr_{H/L}(x) = Tr_{M/L}(Tr_{H/M}(x))$$

De manera que (3.9) y la proposición 3.3.1 nos dan como resultado inmediato este corolario. □

Proposición 3.3.3. *Sea M/L una extensión finita y separable; consideremos una base $\{z_1, \ldots, z_n\}$ de M/L. Entonces existen elementos $z_1^*, \ldots, z_n^* \in M$ únicamente determinados tales que*

$$Tr_{M/L}(z_i z_j^*) = \delta_{ij}$$

donde δ_{ij} denota la delta de Kronecker. El conjunto $\{z_1^*, \ldots, z_n^*\}$ es también una base de M/L y es llamada la base dual de $\{z_1, \ldots, z_n\}$ con respecto a la traza.

Demostración. Consideremos el espacio dual M^* de M sobre L, es decir, es el conjunto de formas L-lineales $\lambda : M \to L$. Del álgebra lineal sabemos que M^* tiene dimensión n sobre. Para $z \in M$ y $\lambda \in M^*$ definimos $z\lambda \in M^*$ por $(z\lambda)(w) := \lambda(zw)$. Esta definición dota a M^* una estructura de M-espacio vectorial de dimensión uno (pues $dim_L(M^*) = [M : L]dim_M(M^*)$). Como en este caso $Tr_{M/L}$ no es la función cero, cualquier $\lambda \in M^*$ tiene una única representación de la forma $\lambda = zTr_{M/L}$, $z \in M$. En particular, las formas lineales $\lambda_j \in M^*$ dadas por $\lambda_j(z_i) := \delta_{ij}$ $(i = 1, \ldots, n)$ pueden ser escritas como $\lambda_j = z_j^* Tr_{M/L}$ con $z_j^* \in M$. Esto quiere decir que

$$Tr_{M/L}(z_i z_j^*) = (z_j^* Tr_{M/L})(z_i) = \lambda_j(z_i) = \delta_{ij}$$

Puesto que $\lambda_1, \ldots, \lambda_n$ son linealmente independientes sobre L, lo mismo ocurre con $z_1^*, \ldots, z_n^*$ y por lo tanto constituyen una base de M/L. □

Teorema 3.3.4. *Sea R un subanillo de F/K con campo de cocientes F y F'/F una extensión finita y separable de grado n. Sea R' la cerradura entera de R en F'. Entonces tenemos*

1. *Para cualquier base $\{x_1, \ldots, x_n\}$ de F'/F existen elementos $a_i \in R \backslash \{0\}$ tales que $a_1 x_1, \ldots, a_n x_n \in R'$. Por lo tanto existen bases de F'/F que están contenidas en R'.*

2. *Si $\{z_1, \ldots, z_n\} \subseteq R'$ es una base de F'/F y $\{z_1^*, \ldots, z_n^*\}$ denota la base dual con respecto a la traza, entonces*

$$\sum_{i=1}^{n} Rz_i \subseteq R' \subseteq \sum_{i=1}^{n} Rz_i^*$$

3. *Si, además R es un dominio de ideales principales, entonces existe una base $\{u_1, \ldots, u_n\}$ de F'/F con la propiedad*

$$R' = \sum_{i=1}^{n} Ru_i$$

Demostración. (1) Debemos mostrar que, para cualquier $x \in F'$ existe algún elemento $0 \neq a \in R$ tal que ax satisface una ecuación entera sobre R. Dado que F'/F es algebraica y F es el campo de cocientes de R, existen elementos $a_i, b_i \in R$ con $a_i \neq 0$ y

$$x^r + \frac{b_{r-1}}{a_{r-1}}x^{r-1} + \cdots + \frac{b_1}{a_1}x + \frac{b_0}{a_0} = 0$$

Si multiplicamos esta ecuación por a^r, donde $a = a_0 a_1 \cdots a_{r-1}$, obtenemos lo siguiente

$$(ax)^r + c_{r-1}(ax)^{r-1} + \cdots + c_1(ax) + c_0 = 0$$

con $c_i \in R$, por lo tanto $ax \in R'$.

(2) Sea ahora $\{z_1, \ldots, z_n\}$ una base de F'/F tal que toda $z_i \in R'$ y sea $\{z_1^*, \ldots, z_n^*\}$ la base dual. Tenemos que en particular todo $z \in F'$ puede ser representado en la forma

$$z = e_1 z_1^* + \cdots + e_n z_n^* \quad \text{con } e_i \in F.$$

Si $z \in R'$ entonces $zz_j \in R'$ para $j = 1, \ldots, n$ y por el corolario 3.3.2 tenemos que $Tr_{F'/F}(zz_j) \in R$. Por otra parte

$$Tr_{F'/F}(zz_j) = Tr_{F'/F}\left(\sum_{i=1}^{n} e_i z_j z_i^*\right) = \sum_{i=1}^{n} e_i Tr_{F'/F}(z_j z_i^*) = e_j$$

y concluimos que $e_j \in R$, por lo tanto $R' \subseteq \sum_{i=1}^{n} Rz_i^*$.

(3) Escojamos una base $\{y_1, \ldots, y_n\}$ de F'/F con $R' \subseteq \sum_{i=1}^{n} Ry_i$ (esto es posible por 2). Para $1 \leq k \leq n$ definamos

$$R_k = R' \cap \sum_{i=1}^{k} Ry_i \tag{3.10}$$

Deseamos construir de forma inductiva un conjunto $u_1, \ldots, u_n$ tales que $R_k = \sum_{i=1}^{k} Ru_i$. Para $k = 1$ tenemos $R_1 = R' \cap Ry_1$; consideremos ahora el conjunto

$$I_1 = \{a \in F \mid ay_1 \in R'\}$$

El cual está contenido en R, dado que $R' \subseteq \sum_{i=1}^{n} Ry_i$. Más aún I_1 es claramente un ideal de R, entonces $I_1 = a_1 R$ por ser R un dominio de ideales principales. Si definimos $u_1 = a_1 y_1$ es fácil verificar que $R_1 = Ru_1$. Supongamos que para $k \geq 2$ hemos encontrado $u_1, \ldots, u_{k-1}$ tales que $R_{k-1} = \sum_{i=1}^{k-1} Ru_i$. Sea ahora

$$I_k = \{a \in F \mid \text{ existen } b_1, \ldots, b_{k-1} \in R \text{ con}$$

$$b_1y_1 + \cdots + b_{k-1}y_{k-1} + ay_k \in R'\}$$

De nueva cuenta, I_k es un ideal de R y entoces $I_k = a_kR$. Escojamos $u_k \in R'$ de la manera siguiente

$$u_k = c_1y_1 + \cdots + c_{k-1}y_{k-1} + a_ky_k$$

Con $c_1, \ldots, c_{k-1} \in R$. Claramente $R_k \supseteq \sum_{i=1}^{k} Ru_i$. Para probar la inclusión contraria sea $w \in R_k$. Escribamos

$$w = d_1y_1 + \cdots + d_ky_k \text{ con } d_i \in R$$

Entonces $d_k \in I_k$ y por lo tanto $d_k = da_k$ con $d \in R$ y

$$w - du_k \in R' \cap \sum_{i=1}^{k-1} Ry_i = R_{k-1} = \sum_{i=1}^{k-1} Ru_i$$

Hasta ahora hemos probado que $R' = R_n = \sum_{i=1}^{n} Ru_i$. Puesto que R' contiene una base de F'/F por 1, los elementos $u_1, \ldots, u_n$ son linealmente independientes sobre F y constituye una base de F'/F.

□

Tenemos el siguiente corolario.

Corolario 3.3.5. *Sea F'/F una extensión finita y separable del campo de funciones F/K y sea $P \in \mathbb{P}_F$ un lugar de F/K. Entoces la cerradura entera $\mathcal{O}'_P$ de $\mathcal{O}_P$ en F' es*

$$\mathcal{O}'_P = \bigcap_{P'|P} \mathcal{O}_{P'}$$

Existe una base $\{u_1 \ldots, u_n\}$ de F'/F tal que

$$\mathcal{O}'_P = \sum_{i=1}^{n} \mathcal{O}_P u_i$$

Cualquier base $\{u_1 \ldots, u_n\}$ de esta forma es llamada una base entera de $\mathcal{O}'_P$ sobre $\mathcal{O}_P$ (o base local entera de F'/F para el lugar P)

Demostración. Este corolario es claro por el teorema 3.3.4 y por el teorema 3.2.5 (notemos que tanto $\mathcal{O}_P$ como $\mathcal{O}'_P$ son dominios de ideales principales. □

Un importante teorema sobre la existencia de bases enteras es el siguiente

Teorema 3.3.6. *Sea F/K un campo de funciones y F'/F finita y separable. Entonces cualquier base $\{z_1 \ldots, z_n\}$ de F'/F es una base entera para casi todo $P \in \mathbb{P}_F$.*

Demostración. Consideremos la base dual $\{z_1^*, \ldots, z_n^*\}$ de $\{z_1, \ldots, z_n\}$. Los polinomios mínimos de $z_1, \ldots, z_n, z_1^*, \ldots, z_n^*$ sobre F involucran sólo un número finito de coeficientes. Sea $S \subseteq \mathbb{P}_F$ el conjunto de los polos de todos estos coeficientes. S es finito y si $P \notin S$ tenemos que

$$z_1, \ldots, z_n, z_1^*, \ldots, z_n^* \in \mathcal{O}'_P \tag{3.11}$$

Por lo tanto

$$\sum \mathcal{O}_P z_i \subseteq \mathcal{O}'_P \subseteq \sum \mathcal{O}_P z_i^* \subseteq \mathcal{O}'_P \subseteq \sum \mathcal{O}_P z_i$$

La primera y la tercera de estas inclusiones son obvias por (3.11); la segunda y la cuarta son inmediatas por el teorema 3.3.4 (2). Notemos que $\{z_1, \ldots, z_n\}$ es la base dual de $\{z_1^*, \ldots, z_n^*\}$. Por lo tanto $\{z_1, \ldots, z_n\}$ es una base entera para todo $P \notin S$. □

3.4 Fórmula de Riemann-Hurwitz

Consideremos F/F' extensión finita y separable. Sea $P \in \mathbb{P}_F$ y sea $\mathcal{O}'_P := B_{F'}(\mathcal{O}_P)$ la cerradura entera de $\mathcal{O}_P$ en F', al conjunto

$$\mathcal{C}_P := \{z \in F' \mid Tr_{F'/F}(z\mathcal{O}'_P) \subseteq \mathcal{O}_P\}$$

le llamaremos el módulo complementario sobre $\mathcal{O}_P$. Observemos que la traza no es idénticamente cero pues la extensión es separable.

Proposición 3.4.1.

1. *$\mathcal{C}_P$ es un $\mathcal{O}'_P$-módulo y $\mathcal{O}'_P \subseteq \mathcal{C}_P$.*

2. *Si $\{z_1, \ldots, z_n\}$ es una base entera para $\mathcal{O}'_P$ sobre $\mathcal{O}_P$ entonces*

$$\mathcal{C}_P = \sum_{i=1}^{n} \mathcal{O}_P z_i^* \text{ con } \{z_1^*, \ldots, z_n^*\} \text{ la base dual}$$

3. *Existe un elemento $t \in F'$ que desde luego depende de P tal que $\mathcal{C}_P = t\mathcal{O}'_P$ y $v_{P'}(t) \leq 0$ para todo $P' \mid P$. Si $t' \in F'$ entonces*

$$\mathcal{C}_P = t'\mathcal{O}'_P \text{ si y sólo si } v_{P'}(t') = v_{P'}(t) \text{ para todo } P' \mid P$$

4. *$\mathcal{C}_P = \mathcal{O}'_P$ para casi todo $P \in \mathbb{P}_F$.*

Demostración. Es un $\mathcal{O}'_P$-módulo porque si tomamos $a \in \mathcal{O}'_P$ y $z \in \mathcal{C}_P$ entonces $Tr_{F'/F}(za\mathcal{O}'_P) \subseteq Tr_{F'/F}(z\mathcal{O}'_P) \subseteq \mathcal{O}_P$. Consideremos ahora $z \in \mathcal{C}_P$ como $\{z_1^*, \ldots, z_n^*\}$ es una base de F'/F existen $x_1, \ldots, x_n \in F$ tales que $z = \sum_{i=1}^n x_i z_i^*$, como $z \in \mathcal{C}_P$ y $z_1, \ldots, z_n \in \mathcal{O}'_P$ entonces $Tr_{F'/F}(zz_j) \in \mathcal{O}_P$ para $1 \leq j \leq n$. Por otra parte

$$Tr_{F'/F}(zz_j) = Tr_{F'/F}\left(\sum_{i=1}^n x_i z_i^* z_j\right)$$

$$= \sum_{i=1}^n x_i Tr_{F'/F}(z_i^* z_j) = x_j$$

por las propiedades de la base dual. Por lo tanto $x_j \in \mathcal{O}_P$ y $z \in \sum_{i=1}^n \mathcal{O}_P z_i^*$. Recíprocamente, sea ahora $z \in \sum_{i=1}^n \mathcal{O}_P z_i^*$, $u \in \mathcal{O}'_P$, $z = \sum_{i=1}^n x_i z_i^*$ y $u = \sum_{j=1}^n y_j z_j$ con $x_i, y_j \in \mathcal{O}_P$. Entonces tenemos

$$Tr_{F'/F}(zu) = Tr_{F'/F}\left(\sum_{i,j=1}^n x_i y_j z_i^* z_j\right)$$

$$= \sum_{i,j=1}^n x_i y_j Tr_{F'/F}(z_i^* z_j) = \sum_{i=1}^n x_i y_i \in \mathcal{O}_P.$$

Por lo tanto $z \in \mathcal{C}_P$. Por 2. $\mathcal{C}_P = \sum_{i=1}^n \mathcal{O}_P u_i$ con $u_i \in F'$ (base dual). Sea $x \in F$ tal que $v_P(x) \geq 0$ y $v_P(x) \geq -v_{P'}(u_i)$ para todo $P' \mid P$ e $i = 1, \ldots, n$. Entonces

$$v_{P'}(xu_i) = e(P' \mid P)v_P(x) + v_{P'}(u_i) \geq 0$$

para todo $P' \mid P$ e $i = 1, \ldots, n$ por lo tanto $x\mathcal{C}_P \subseteq \mathcal{O}'_P$. Es fácil verificar que $x\mathcal{C}_P$ es un ideal de $\mathcal{O}'_P$ y por lo tanto $x\mathcal{C}_P = y\mathcal{O}'_P$ para algún $y \in \mathcal{O}'_P$, porque $\mathcal{O}'_P$ es un DIP por la proposición 3.3.5. Sea ahora $t := x^{-1}y$ y tenemos entonces que $\mathcal{C}_P = t\mathcal{O}'_P$, pero $\mathcal{O}'_P \subseteq \mathcal{C}_P$, de manera que $y = \sum_{i=1}^n u_i a_i$ con $v_{P'}(a_i) \geq 0$ y $v_{P'}(xu_i) \geq 0$. En consecuencia

$$v_{P'}(xa_iu_i) \geq 0 \iff -v_{P'}(xa_iu_i) \leq 0 \iff v_{P'}(x^{-1}a_iu_i) \leq 0$$

Por lo tanto $v_{P'}(t) \leq 0$ para todo $P' \mid P$. Finalmente tenemos

$$t\mathcal{O}'_P = t'\mathcal{O}'_P \iff tt'^{-1} \in \mathcal{O}'_P \text{ y } t^{-1}t' \in \mathcal{O}'_P$$

$$\iff v_{P'}(tt'^{-1}) \geq 0 \text{ y } v_{P'}(t^{-1}t') \geq 0$$

$$\iff v_{P'}(t) = v_{P'}(t') \text{ para todo } P' \mid P$$

Finalmente, para la última parte escojamos una base $\{z_i, \ldots, z_n\}$ de F'/F. Por el teorema 3.3.6 $\{z_i, \ldots, z_n\}$ y $\{z_i^* \ldots, z_n^*\}$ son bases enteras para casi toda $P \in \mathbb{P}_F$. Por (2) entonces tenemos que $\mathcal{C}_P = \mathcal{O}'_P$ para casi toda P. □

Definición 3.4.2. Consideremos $P \in \mathbb{P}_F$ y $\mathcal{O}'_P$ la cerradura entera de $\mathcal{O}_P$ en F'. Sea $\mathcal{C}_P = t\mathcal{O}'_P$ el módulo complementario sobre $\mathcal{O}_P$. Definimos ahora para $P' \mid P$ el exponente del *diferente* de P' sobre P por

$$d(P' \mid P) := -v_{P'}(t)$$

Por la proposición anterior está bien definido y $d(P' \mid P) \geq 0$. Más aún, se tiene que $d(P' \mid P) = 0$ para casi todo $P \in \mathbb{P}_F$. De manera que podemos definir el divisor

$$Diff(F'/F) := \sum_{P \in \mathbb{P}_F} \sum_{P' \mid P} d(P' \mid P)P'$$

Llamado el *diferente* de F'/F. Notemos que $Diff(F'/K)$ es un divisor de F' y $Diff(F'/K) \geq 0$.

Observación 3.4.3. Notemos la siguiente caracterización del módulo $\mathcal{C}_P$, la cual se sigue inmediatamente de las definiciones.

$$z \in \mathcal{C}_P \iff v_{P'}(z) \geq -d(P' \mid P) \quad \text{para todo } P' \mid P.$$

Definición 3.4.4. Sea

$$\mathcal{A}_{F'/F} := \{\alpha \in \mathcal{A}_{F'} \mid \alpha_{P'} = \alpha_{Q'} \quad si\ P' \cap F = Q' \cap F\}$$

Este conjunto es un F'-subespacio de $\mathcal{A}_{F'}$ y el homomorfismo traza puede ser extendido a una aplicación F-lineal de $\mathcal{A}_{F'/F}$ en $\mathcal{A}_F$ de la siguiente manera

$$(Tr_{F'/F}(\alpha))_P := Tr_{F'/F}(\alpha_{P'}) \quad \text{para } \alpha \in \mathcal{A}_{F'/F}$$

donde P' es cualquier lugar que yace sobre P. Notemos que $\alpha_{P'} \in \mathcal{O}_{P'}$ para casi todo $P' \in \mathbb{P}_{F'}$. Por lo tanto $Tr_{F'/F}(\alpha_{P'}) \in \mathcal{O}_P$ para casi todo P, por el corolario 3.3.2. Notemos también que la traza de un adel principal $z \in F'$ es claramente el adel principal de $Tr_{F'/F}(z)$. Para un divisor $A' \in \mathcal{D}_{F'}$ definimos

$$\mathcal{A}_{F'/F}(A') := \mathcal{A}_{F'}(A') \cap \mathcal{A}_{F'/F}.$$

Teorema 3.4.5. *Para todo diferencial de Weil ω de F/K existe un único diferencial de Weil ω' de F'/K' tal que*

$$Tr_{K'/K}(\omega'(\alpha)) = \omega(Tr_{F'/F}(\alpha)) \tag{3.12}$$

para todo $\alpha \in \mathcal{A}_{F'/F}$. Este diferencial es llamado la cotraza de ω en F'/F y es denotado por $Cotr_{F'/F}(\omega)$. Si $\omega \neq 0$ y $(\omega) \in \mathcal{D}_F$ es el divisor canónico de ω entonces

$$(Cotr_{F'/F}(\omega)) = Con_{F'/F}((\omega)) + Diff(F'/F)$$

Si usamos la noción de componentes locales de un diferencial de Weil, la ecuación (3.12) puede ser reemplazada por las siguientes condiciones locales: para todo $P \in \mathbb{P}_F$ y todo $y \in F'$

$$\omega_P(Tr_{F'/F}(y)) = Tr_{K'/K}(\sum_{P'|P} \omega'_{P'}(y)) \tag{3.13}$$

La equivalencia entre (3.12) y (3.13) se sigue de la proposición 2.3.2, la cual establece que $\omega(\gamma)$ es la suma de todas sus componentes locales $\omega_P(\gamma_P)$ para cualquier adel $\gamma = (\gamma_P)_{P\in\mathbb{P}_F}$.

Para la demostración del teorema, necesitamos probar previamente dos lemas importantes.

Lema 3.4.6. *Para todo $C' \in \mathcal{D}_{F'}$ tenemos $\mathcal{A}_{F'} = \mathcal{A}_{F'/F} + \mathcal{A}_{F'}(C')$.*

Demostración. Sea $\alpha = (\alpha_{P'})_{P'\in\mathbb{P}_{F'}}$ un adel de F'. Para todo $P \in \mathbb{P}_F$ existe por el teorema de aproximación fuerte un elemento $x_P \in F'$ con

$$v_{P'}(\alpha_{P'} - x_P) \geq -v_{P'}(C') \quad \text{para todo } P' \mid P$$

Definimos ahora $\beta = (\beta_{P'})_{P'\in\mathbb{P}_{F'}}$ con $\beta_{P'} = x_P$ si $P' \mid P$. Entonces $\beta \in \mathcal{A}_{F'/F}$ y $\alpha - \beta \in \mathcal{A}_{F'}(C')$. Dado que $\alpha = \beta + (\alpha - \beta)$ tenemos el lema. □

Lema 3.4.7. *Sea M/L una extensión de campos finita y separable. Sea V un M-espacio vectorial y $\mu : V \to L$ una aplicación L-lineal. Entonces existe un único homomorfismo M-lineal $\mu' : V \to M$ tal que $Tr_{M/L} \circ \mu' = \mu$.*

Demostración. Consideremos el espacio de formas lineales $M^* = \{\lambda : M \to L \mid \lambda \text{ es } L\text{-lineal}\}$ como espacio vectorial sobre M con esta operación: $(z\lambda)(w) = \lambda(zw)$ para $\lambda \in M^*$ y $z, w \in M$. Como ya vimos, la dimensión de M^* sobre M es uno, así que cualquier $\lambda \in M^*$ tiene una representación única de la forma $\lambda = zTr_{M/L}$ con $z \in M$. Dado un elemento $v \in V$, definimos la aplicación $\lambda_v : M \to L$ por $\lambda_v(a) := \mu(av)$ la cual es claramente L-lineal. Por lo tanto $\lambda_v = z_v Tr_{M/L}$ con un único elemento $z_v \in M$ y definimos $\mu'(v) := z_v$. De manera que se cumple lo siguiente

$$\mu(av) = (\mu'(v)Tr_{M/L})(a) = Tr_{M/L}(a\mu'(v)) \tag{3.14}$$

para todo $a \in M$ y $v \in V$; además $\mu'(v)$ está determinado de forma única. Usando esto podemos verificar fácilmente que $\mu' : V \to M$ es M-lineal. Si hacemos además $a = 1$ en (3.14) obtenemos que $\mu = Tr_{M/L} \circ \mu'$ lo cual demuestra la existencia de $\mu' : V \to M$ con las propiedades deseadas.

Veamos la unicidad. Si suponemos que existe otro $\mu^* : V \to M$ tal que $Tr_{M/L} \circ \mu' = Tr_{M/L} \circ \mu^*$ y $\mu^* \neq \mu'$. Entonces la imagen de $\mu' - \mu^*$ es todo M por ser M-lineal y entonces tenemos que $Tr_{M/L} \circ (\mu' - \mu^*) = 0$, lo cual es una contradicción pues la extensión era separable. □

Demostración del teorema anterior. En primera instancia deseamos mostrar la existencia de un diferencial de Weil tal que

$$Tr_{K'/K}(\omega'(\alpha)) = \omega(Tr_{F'/F}(\alpha))$$

se cumple para todo $\alpha \in \mathcal{A}_{F'/F}$. Si $\omega = 0$ simplemente definimos $\omega' = 0$. Supongamos entonces que $\omega \neq 0$. Por brevedad definamos también

$$W' := Con_{F'/F}((\omega)) + Diff(F'/F)$$

La construcción del diferencial ω' la haremos en tres pasos.

1. Definimos ahora una aplicación K-lineal $\omega_1 : \mathcal{A}_{F'/F} \to K$ dado por $\omega_1 := \omega \circ Tr_{F'/F}$ y que tiene las siguientes propiedades:

   (a) $\omega_1(\alpha) = 0$ si $\alpha \in \mathcal{A}_{F'/F}(W') + F'$.

   (b) Si $B' \in \mathcal{D}_{F'}$ es un divisor tal que $B' \not\leq W'$, entonces existe un adel $\beta \in \mathcal{A}_{F'/F}(B')$ con $\omega_1(\beta) \neq 0$.

   Veamos que ω_1 cumple (a) y (b). ω_1 es obviamente K-lineal y ω_1 se anula en F' pues ω se anula en F. Sea ahora $\alpha \in \mathcal{A}_{F'/F}(W')$. Para probar que $\omega_1(\alpha) = 0$ necesitamos verificar únicamente que para todo $P \in \mathbb{P}_F$ y $P' \mid P$ se cumple

   $$v_P(Tr_{F'/F}(\alpha_{P'})) \geq -v_P(\omega) \tag{3.15}$$

   pues ω se anula en $\mathcal{A}_F((\omega))$ por definición del divisor $((\omega))$. Escojamos ahora un elemento $x \in F$ con $v_P(x) = v_P(\omega)$. Entonces

   $$v_{P'}(x\alpha_{P'}) = v_{P'}(x) + v_{P'}(\alpha_{P'}) \geq e(P' \mid P)v_P(\omega) - v_{P'}(W')$$

   $$= v_{P'}(Con_{F'/F}((\omega)) - W') = -v_{P'}(Diff(F'/F)) = -d(P' \mid P)$$

   donde $-d(P' \mid P)$ denota el exponente del diferente. Pero esto implica por la observación 3.4.3 que $x\alpha_{P'} \in \mathcal{C}_P$, el módulo complementario sobre $\mathcal{O}_P$ y por lo tanto $v_P(Tr_{F'/F}(x\alpha_{P'})) \geq 0$. Como $Tr_{F'/F}(x\alpha_{P'}) = xTr_{F'/F}(\alpha_{P'})$ y $v_P(x) = v_P(\omega)$, la afirmación (3.15) se cumple.

   Ahora supongamos que tenemos $B' \not\leq W'$; esto quiere decir que exite $P_0 \in \mathbb{P}_F$ tal que

   $$v_{P^*}(Con_{F'/F}((\omega)) - B') < -d(P^* \mid P_0) \tag{3.16}$$

   para algún $P^* \mid P_0$. Denotemos por $\mathcal{O}'_{P_0}$ la cerradura entera de P_0 en F' y $\mathcal{C}_{P_0}$ el módulo complementario sobre $\mathcal{O}_{P_0}$. Consideremos ahora el conjunto

   $$J := \{z \in F' \mid v_{P^*}(z) \geq v_{P^*}(Con_{F'/F}((\omega)) - B') \text{ para todo } P^* \mid P\}$$

Por el teorema de aproximación fuerte tenemos que existe un elemento $u \in J$ que satisface $v_{P'}(Con_{F'/F}((\omega)) - B')$ para todo $P' \mid P$. Tenemos entonces que $J \notin \mathcal{C}_{P_0}$ por la observación 3.4.3, hecha en la definición del diferente. Pero por otra parte, $J\mathcal{O}'_{P_0} \subseteq J$ y entonces

$$Tr_{F'/F}(J) \notin \mathcal{O}_{P_0} \tag{3.17}$$

Escojamos ahora $t \in F$ con la propiedad de que $v_{P_0}(t) = 1$. Para alguna $r \geq 0$ se cumple $t^r J \subseteq \mathcal{O}'_{P_0}$ (esto es inmediato de la definición de J). Por lo tanto $t^r Tr_{F'/F}(J) = Tr_{F'/F}(t^r J) \subseteq \mathcal{O}_{P_0}$. Es inmediato verificar que $t^r Tr_{F'/F}(J)$ es un ideal de $\mathcal{O}_{P_0}$ y en consecuencia, $t^r Tr_{F'/F}(J) = t^s \mathcal{O}_{P_0}$ con $s \geq 0$. Al multiplicar por una potencia adecuada tenemos $Tr_{F'/F}(J) = t^m \mathcal{O}_{P_0}$ para alguna $m \in \mathbb{Z}$. Por (3.17) $m \leq -1$ y por lo tanto

$$t^{-1}\mathcal{O}_{P_0} \subseteq Tr_{F'/F}(J) \tag{3.18}$$

Ahora, por la proposición 2.3.3 en la sección de componentes locales de los diferenciales de Weil, podemos encontrar un elemento $x \in F$ con

$$v_{P_0}(x) = -v_{P_0}(\omega) - 1 \quad \text{y } \omega_{P_0}(x) \neq 0 \tag{3.19}$$

Ahora escojamos $y \in F$ tal que $v_{P_0}(y) = v_{P_0}(\omega)$, de manera que $xy \in t^{-1}\mathcal{O}_{P_0}$. Por (3.18) existe una $z \in J$ tal que $Tr_{F'/F}(z) = xy$. Consideremos ahora el adel definido por

$$\beta_{P'} := \begin{cases} 0 & \text{Si } P' \nmid P_0 \\ y^{-1}z & \text{Si } P' \mid P_0 \end{cases}$$

Se sigue de la definición de J que si $P' \mid P_0$

$$v_{P'}(\beta) = -v_{P'}(y) + v_{P'}(z)$$

$$\geq -v_{P'}(Con_{F'/F}((\omega))) + v_{P'}(Con_{F'/F}((\omega)) - B')$$

$$-v_{P'}(B')$$

Por lo tanto $\beta \in \mathcal{A}_{F'/F}(B')$. Finalmente, hemos demostrado que $\omega_1(\beta) = \omega(Tr_{F'/F}(\beta)) = \omega_{P_0}(x) \neq 0$ por (3.19). Esto prueba (b).

2. Definamos ahora $\omega_2 : \mathcal{A}_{F'} \to K$ como sigue. Si $\alpha \in \mathcal{A}_{F'}$ existen adeles $\beta \in \mathcal{A}_{F'/F}$ y $\gamma \in \mathcal{A}_{F'}(W')$ tales que $\alpha = \beta + \gamma$ por el lema 3.4.6 Definimos

$$\omega_2(\alpha) := \omega_1(\beta)$$

Esta definición no depende de la elección de β y γ. Si α tiene dos representaciones $\alpha = \beta + \gamma = \beta_1 + \gamma_1$, con $\beta, \beta_1 \in \mathcal{A}_{F'/F}$ y $\gamma, \gamma_1 \in \mathcal{A}_{F'}(W')$ entonces

$$\beta_1 - \beta = \gamma - \gamma_1 \in \mathcal{A}_{F'/F} \cap \mathcal{A}_{F'}(W')$$

Por lo tanto $\omega_1(\beta_1) - \omega_1(\beta) = \omega_1(\beta_1 - \beta) = 0$ por el paso 1. La aplicación ω_2 es obviamente K-lineal y por (a) y (b) del paso anterior y tiene las siguientes propiedades

(a) $\omega_2(\alpha) = 0$ si $\alpha \in \mathcal{A}_{F'}(W') + F'$

(b) Si $B' \in \mathcal{D}_{F'}$ es un divisor con $B' \not\leq W'$ entonces existe un adel $\beta \in \mathcal{A}_{F'}(B')$ con $\omega_2(\beta) \neq 0$.

Hemos construido, hasta este momento, una aplicación K-lineal $\omega_2 : \mathcal{A}_{F'} \to K$ que se anula en $\mathcal{A}_{F'}(B') + F'$. No obstante, ω_2 no es un diferencial de F'/K' si K' es estrictamente más grande que K; de manera que necesitamos levantar ω_2 a una aplicación K'-lineal, lo cual se hace en este último paso.

3. Por el lema 3.4.7 existe un homomorfismo K'-lineal $\omega' : \mathcal{A}_{F'} \to K'$ tal que $Tr_{K'/K} \circ \omega' = \omega_2$. De la definición de ω_1 y ω_2, obtenemos inmediatamente para $\alpha \in \mathcal{A}_{F'/F}$

$$Tr_{K'/K}(\omega'(\alpha)) = \omega_2(\alpha) = \omega_1(\alpha) = \omega(Tr_{F'/F}(\alpha))$$

Esto prueba (3.12) y sólo resta probar

(a) $\omega'(\alpha) = 0$ para $\alpha \in \mathcal{A}_{F'}(W') + F'$.

(b) Si $B' \in \mathcal{D}_{F'}$ es un divisor con $B' \not\leq W'$, entonces existe un adel $\beta \in \mathcal{A}_{F'}(B')$ con $\omega'(\beta) \neq 0$.

Como ω' es K'-lineal, la imagen de $\mathcal{A}_{F'}(W') + F'$ bajo ω' es cero o bien todo K'. Si fuera todo K' existe un $\alpha \in \mathcal{A}_{F'}(W') + F'$ tal que $Tr_{K'/K}(\omega'(\alpha)) \neq 0$ puesto que $Tr_{K'/K} : K' \to K$ no es idénticamente cero. Por la construcción de ω' tenemos que $\omega_2 = Tr_{K'/K} \circ \omega'$ y por lo tanto $\omega_2 = 0$ lo cual es una contradicción a (a). Por el inciso (b) del paso anterior, existe un adel $\beta \in \mathcal{A}_{F'}(B')$ con la propiedad $\omega_2(\beta) \neq 0$ y entonces la propiedad (b) en este paso es inmediata.

De manera que hemos mostrado la existencia de un diferencial de Weil ω' de F'/K' que satisface (3.12) y cuyo divisor canónico es

$$(\omega') = W' = Con_{F'/F}((\omega)) + Diff(F'/F)$$

Para probar la unicidad de ω', supongamos que existe otro diferencial ω^* de F'/K' que satisface (3.12), es decir,

$$Tr_{K'/K}(\omega^*(\alpha)) = Tr_{K'/K}(\omega'(\alpha)) = \omega(Tr_{F'/F}(\alpha))$$

para todo $\alpha \in \mathcal{A}_{F'/F}$. Si definimos $\eta = \omega^* - \omega'$ tenemos

$$Tr_{K'/K}(\eta(\alpha)) = 0 \quad \text{para todo } \alpha \in \mathcal{A}_{F'/F} \tag{3.20}$$

Pero η es un diferencial de Weil de F'/K', por lo tanto η se anula en $\mathcal{A}_{F'}(C')$ para algún divisor $C' \in \mathcal{A}_{F'}$. Por el lema 3.4.6 tenemos que $Tr_{K'/K}(\eta(\alpha)) = 0$ para todo $\alpha \in \mathcal{A}_{F'}$. Esto implica que $\eta = 0$ y por lo tanto $\omega' = \omega^*$. □

Veamos ahora algunas propiedades básicas de la aplicación cotraza $\omega \mapsto Cotr_{F'/F}(\omega)$.

Proposición 3.4.8.

1. *Si ω_1, ω_2 son diferenciales de Weil de F/K y $x \in F$, entonces*

$$Cotr_{F'/F}(\omega_1 + \omega_2) = Cotr_{F'/F}(\omega_1) + Cotr_{F'/F}(\omega_2)$$

y

$$Cotr_{F'/F}(x\omega) = xCotr_{F'/F}(\omega)$$

2. *Sea F''/F' otra extensión finita y separable. Entonces*

$$Cotr_{F''/F}(\omega) = Cotr_{F''/F'}(Cotr_{F'/F}(\omega))$$

Para todo diferencial de Weil ω de F/K.

Demostración. Dada la unicidad del teorema 3.4.5, es suficiente por lo tanto mostrar que

$$Tr_{K'/K}((Cotr_{F'/F}(\omega_1) + Cotr_{F'/F}(\omega_2))(\alpha)) = (\omega_1 + \omega_2)(Tr_{F'/F}(\alpha))$$

se cumple para todo $\alpha \in \mathcal{A}_{F'/F}$. La demostración de esta afirmación es inmediata de la linealidad de la traza. De la misma manera podemos probar que $Cotr_{F'/F}(x\omega) = xCotr_{F'/F}(\omega)$, así como la afirmación 2. □

Corolario 3.4.9. *Supongamos que tenemos una cadena de extensiones finitas y separables $F \subseteq F' \subseteq F''$, entonces se cumple lo siguiente.*

1. $Diff(F''/F) = Con_{F''/F'}(Diff(F'/F)) + Diff(F''/F')$.

2. $d(P'' \mid P) = e(P'' \mid P')d(P' \mid P) + d(P'' \mid P')$ *si* P'', P' *y* P *son lugares de* F'', F' F *respectivamente, con* $P \subseteq P' \subseteq P''$.

Demostración. La afirmación 2 es simplemente una reformulación de 1, como puede verificarse rápidamente. De manera que sólo vamos a demostrar 1. Sea $\omega \neq 0$ un diferencial de Weil, entonces por el teorema 3.4.5 el divisor de $Cotr_{F''/F}(\omega)$ es

$$(Cotr_{F''/F}(\omega)) = Con_{F''/F}((\omega)) + Diff(F''/F) \tag{3.21}$$

Por otra parte la proposición 3.4 nos dice

$$\begin{aligned}(Cotr_{F''/F}(\omega)) &= (Cotr_{F''/F'}(Cotr_{F'/F}(\omega))) \\ &= (Cotr_{F''/F'}(Con_{F'/F}((\omega)) + Diff(F'/F)) \\ &= Con_{F''/F'}(Con_{F'/F}((\omega)) + Diff(F'/F)) + Diff(F''/F') \\ &= Con_{F''/F}((\omega)) + Con_{F''/F'}(Diff(F'/F)) + Diff(F''/F') \end{aligned} \tag{3.22}$$

Si ahora comparamos (3.21) y (3.22) obtenemos 1. □

Una consecuencia simple, pero muy importante es el siguiente teorema.

Teorema 3.4.10 (Fórmula de Riemann-Hurwitz). *Sea* F/K *un campo de funciones de género* g *y* F'/F *una extensión finita y separable. Denotemos por* K' *el campo de constantes de* F' *y por* g' *su género. Entonces*

$$2g' - 2 = \frac{[F' : F]}{[K' : K]}(2g - 2) + deg\, Diff(F'/F)$$

Demostración. Tomemos $\omega \neq 0$ un diferencial de Weil. Entonces por el teorema 3.4.5 tenemos

$$(Cotr_{F'/F}(\omega)) = Con_{F'/F}((\omega)) + Diff(F'/F)$$

Entonces si calculamos el grado al divisor anterior y recordamos que el grado de un divisor canónico es $2g - 2$ (respectivamente $2g' - 2$) y por el corolario 3.1.13 tenemos lo siguiente

$$\begin{aligned} 2g' - 2 &= deg\, Con_{F'/F}((\omega)) + deg\, Diff(F'/F) \\ &= \frac{[F' : F]}{[K' : K]}(2g - 2) + deg\, Diff(F'/F) \end{aligned}$$

□

Cualquier campo de funciones puede ser visto siempre como una extensión de un campo de funciones racional $K(x)$. Esta fórmula del género es una herramienta poderosa que nos permite calcular el género de las diferentes extensiones $F/K(x)$.

3.5 El diferente

Durante esta sección supondremos todo el tiempo que el campo K (y por lo tanto K') es perfecto.

El siguiente teorema nos da una relación entre el índice de ramificación y el exponente del diferente.

Teorema 3.5.1 (Teorema de Dedekind del diferente). *Sean $P \in \mathbb{P}_F$ y $P' \in \mathbb{P}_{F'}$ tales que $P' \mid P$ entonces*

1. $d(P' \mid P) \geq e(P' \mid P) - 1$.
2. $d(P' \mid P) = e(P' \mid P) - 1$ *si y sólo si* $e(P' \mid P)$ *no es divisible por* $\operatorname{char} K$.

Para la demostración de este teorema necesitaremos de dos lemas previos.

Lema 3.5.2. *Sea F_1/F una extensión algebraica de campos de funciones, $P \in \mathbb{P}_F$ y $P_1 \in \mathbb{P}_{F_1}$, con $P_1 \mid P$. Consideremos σ un automorfismo de F_1/F. Entonces $\sigma(P_1) = \{\sigma(z) \mid z \in P_1\}$ es un lugar de F_1 y además tenemos*

1. $v_{\sigma(P_1)}(y) = v_{P_1}(\sigma^{-1}(y))$ *para todo* $y \in F'$.
2. $\sigma(P_1) \mid P$.
3. $e(\sigma(P_1) \mid P) = e(P_1 \mid P)$ *y* $f(\sigma(P_1) \mid P) = f(P_1 \mid P)$.

Demostración. Claramente $\sigma(\mathcal{O}_{P_1})$ es un anillo de valuación de F_1 con $\sigma(P_1)$ como su ideal máximo por ser σ un automorfismo. Además el correspondiente anillo de valuación $\mathcal{O}_{\sigma(P_1)} = \sigma(\mathcal{O}_{P_1})$. Consideremos ahora $t_1 \in F_1$ un elemento primo para P_1, es decir, $P_1 = t_1\mathcal{O}_{P_1}$; entonces $\sigma(P_1) = \sigma(t_1)\sigma(\mathcal{O}_{P_1})$, de manera que $\sigma(t_1)$ es un elemento primo para $\sigma(P_1)$

1. Sea $0 \neq y \in F_1$ y supongamos que $y = \sigma(z)$. Escribimos a z como $z = t_1^r u$ con $r = v_{P_1}(z)$ y $u \in \mathcal{O}_{P_1} \backslash P_1$ y tenemos $y = \sigma(t_1)^r \sigma(u)$ donde $\sigma(u) \in \mathcal{O}_{\sigma(P_1)} \backslash \sigma(P_1)$ y $\sigma(t_1)$ es un elemento primo para $\sigma(P_1)$. Por lo tanto $v_{\sigma(P_1)}(y) = r = v_{P_1}(z) = v_{P_1}(\sigma^{-1}(y))$.
2. $\sigma(P_1)$ yace sobre P pues $\sigma(P_1) \supseteq \sigma(P) = P$.
3. Sea $x \in F$ un elemento primo para P. Entonces
$$e(\sigma(P_1) \mid P) = v_{\sigma(P_1)}(x) = v_{P_1}(\sigma^{-1}(x)) = v_{P_1}(x) = e(P_1 \mid P).$$
El automorfismo σ de F'/F induce un isomorfismo $\hat{\sigma}$ de las clases residuales $F_{1_{P_1}}$ en $F_{1_{\sigma(P_1)}}$ dado por
$$\hat{\sigma}(z + P_1) = \sigma(z) + \sigma(P_1)$$
y $\hat{\sigma}$ es la identidad en F_P, por lo tanto $f(P_1 \mid P) = f(\sigma(P_1) \mid P)$.

□

Lema 3.5.3. *Sea $P \in \mathbb{P}_F$ y sean $P_1, \ldots, P_r \in \mathbb{P}_{F'}$ todas las extensiones de P en F'. Consideremos la clase residual $k := \mathcal{O}_P/P$ y $k_i := \mathcal{O}_{P_i}/P_i \supseteq k$ y los correspondientes proyecciones en las clases residuales $\pi : \mathcal{O}_P \to k$ y respectivamente $\pi_i : \mathcal{O}_{P_i} \to k_i$ para $i = 1, \ldots, r$. Entonces para cada $u \in \mathcal{O}'_P$ (la cerradura entera de $\mathcal{O}_P$ en F')*

$$\pi(Tr_{F'/F}(u)) = \sum_{i=1}^{r} e(P_i \mid P) Tr_{k_i/k}(\pi_i(u)).$$

Demostración. Ver [Sti]. □

Demostración del teorema 3.5.1. (1) Denotemos nuevamente por $\mathcal{O}'_P$ a la cerradura entera de $\mathcal{O}_P$ en F' y $\mathcal{C}_P$ el módulo complementario sobre $\mathcal{O}_P$. Queremos probar

$$Tr_{F'/F}(t\mathcal{O}'_P) \subseteq \mathcal{O}_P \tag{3.23}$$

para todo elemento $t \in F'$ que satisfaga

$$v_{P'}(t) = 1 - e(P' \mid P) \quad \text{para todo } P' \mid P \tag{3.24}$$

Notemos que (3.23) implica que $t \in \mathcal{C}_P$ y la caracterización de $\mathcal{C}_P$ dada en la observación 3.4.3 nos dice $1 - e(P' \mid P) \geq -d(P' \mid P)$, así tenemos que $d(P' \mid P) \geq e(P' \mid P) - 1$. Para probar (3.23), consideremos una extensión finita de Galois F^*/F tal que $F \subseteq F' \subseteq F^*$ y escojamos $n = [F' : F]$ automorfismos $\sigma_1, \ldots, \sigma_n$ de F^*/F cuyas restricciones a F' sean distintas. Para $z \in \mathcal{O}'_P$ tenemos

$$Tr_{F'/F}(tz) = \sum_{i=1}^{n} \sigma_i(tz) \tag{3.25}$$

Fijemos ahora P^* un lugar de F^* que yazca sobre P y definamos ahora $P_i^* = \sigma_i^{-1}(P^*)$ y $P'_i = P_i^* \cap F'$. Notemos que $\sigma_i(z)$ es entero sobre $\mathcal{O}_P$, pues $z \in \mathcal{O}'_P$ y por lo tanto $v_{P^*}(\sigma_i(z)) \geq 0$. Obtenemos entonces

$$\begin{aligned} v_{P^*}(\sigma_i(tz)) &= v_{P^*}(\sigma_i(t)) + v_{P^*}(\sigma_i(z)) \\ &\geq v_{P^*}(\sigma_i(t)) = v_{P_i^*}(t) \\ &= e(P_i^* \mid P'_i)(1 - e(P'_i \mid P)) \\ &> -e(P_i^* \mid P) = -e(P^* \mid P) \end{aligned}$$

Si usamos (3.25) concluimos

$$-e(P^* \mid P) < v_{P^*}(Tr_{F'/F}(tz)) = e(P^* \mid P) v_P(Tr_{F'/F}(tz))$$

lo cual implica que $v_P(Tr_{F'/F}(tz)) \geq 0$ y por lo tanto tenemos (3.23).

(2) Mantenemos la notación del último lema y por brevedad escribimos $e_i := e(P_i \mid P)$ y sea $P' = P_1$ y $e = e(P_1 \mid P)$. Debemos mostrar que

$$d(P' \mid P) = e - 1 \iff char\ K \text{ no divide a } e \tag{3.26}$$

Primero supongamos que e no es divisible por $char\ K$. Supongamos que $d(P' \mid P) \geq e$. Entonces existe alguna $w \in F$; tal que

$$v_{P'}(w) \leq -e \text{ y } Tr_{F'/F}(w\mathcal{O}'_P) \subseteq \mathcal{O}_P \tag{3.27}$$

Dado que K es perfecto la extensión k_1/k es separable y podemos encontrar $y_0 \in \mathcal{O}'_P$ tal que $Tr_{k_1/k}(\pi_1(y_0)) \neq 0$. Por el teorema de aproximación fuerte existe un elemento $y \in F'$ tal que

$$v_{P'}(y - y_0) > 0$$

y

$$v_{P_i}(y) \geq \quad \text{máx}\{1, e_i + v_{P_i}(w)\} \text{ para } 2 \leq i \leq r \tag{3.28}$$

Entonces $y \in \mathcal{O}'_P$ y por el lema 3.5.3 tenemos

$$\pi(Tr_{F'/F}(y)) = e(Tr_{k_1/k}(\pi_1(y)) + \sum_{i=2}^{r} e(P_i \mid P) Tr_{k_i/k}(\pi_i(y))$$

$$= e(Tr_{k_1/k}(\pi_1(y)) \neq 0$$

Aquí usamos el hecho de que $char\ K$ no divide a e y por lo tanto $e \neq 0$ en k. Concluimos ahora que

$$v_P(Tr_{F'/F}(y)) = 0$$

Ahora escojamos $x \in F$ tal que $v_P(x) = 1$. Entonces

$$Tr_{F'/F}(x^{-1}y) = x^{-1}Tr_{F'/F}(y) \notin \mathcal{O}_P \tag{3.29}$$

Por otro lado, $x^{-1}yw^{-1} \in \mathcal{O}'_P$ pues

$$v_{P'}(x^{-1}yw^{-1}) = -e + v_{P'}(y) - v_{P'}(w) \geq 0$$

y también

$$v_{P_i}(x^{-1}yw^{-1}) = -e + v_{P_i}(y) - v_{P_i}(w) \geq 0$$

para todo $i = 2, \ldots r$, por (3.27) y (3.28). De manera que $x^{-1}y \in w\mathcal{O}'_P$ y $Tr_{F'/F}(x^{-1}y) \in \mathcal{O}_P$ por (3.27), lo cual contradice (3.29).

Para demostrar el recíproco, supongamos ahora que $char\ K$ divide a e y tenemos que mostrar que $d(P' \mid P) \geq e$. Escojamos $u \in F'$ tal que

$$v_{P'}(u) = -e \text{ y } v_{P_i}(u) \geq -e_i + 1 \quad (i = 2, \ldots, r). \tag{3.30}$$

Ahora denotemos nuevamente con x un elemento primo para P. Para todo $z \in \mathcal{O}'_P$ tenemos

$$v_{P'}(xuz) \geq 0 \quad \text{y} \quad v_{P_i}(xuz) > 0$$

para $i = 2, \ldots, r$. Por lo tanto, $xuz \in \mathcal{O}'_P$ y por el lema 5.3

$$\pi(Tr_{F'/F}(xuz)) = e(Tr_{k_1/k}(\pi_1(xuz)) + \sum_{i=2}^{r} e(P_i \mid P) Tr_{k_i/k}(\pi_i(xuz))$$

$$= e(Tr_{k_1/k}(\pi_1(xuz))) = 0$$

Se sigue entonces que $xTr_{F'/F}(uz) = Tr_{F'/F}(xuz) \in P = x\mathcal{O}_P$ y por lo tanto $Tr_{F'/F}(uz) \in \mathcal{O}_P$ para todo $z \in \mathcal{O}'_P$. Concluimos que $u \in \mathcal{C}_P$ y que $-e = v_{P'}(u) \geq -d(P' \mid P)$ por (3.30) y por la observación 3.4.3. □

Veamos ahora algunas consecuencias del teorema de Dedekind. Recordemos que una extensión de lugares $P' \mid P$ se dice ramificada si $e(P' \mid P) > 1$; en otro caso se dice que $P' \mid P$ es no ramificada.

Definición 3.5.4. Sea F'/F una extensión de campos de funciones y $P \in \mathbb{P}_F$.

1. Una extensión P' de P en F' se dice que es *mansamente (respect. salvajemente ramificada)* si $e(P' \mid P) > 1$ y *char* K no divide a $e(P' \mid P)$ (respect. si *char* K divide a $e(P' \mid P)$).

2. Decimos que P es *ramificado (respect. no ramificado)* si existe al menos un $P' \in \mathbb{P}_{F'}$ tal que $(P' \mid P)$ es ramificada (respect. si $(P' \mid P)$ es no ramificada para todo $(P' \mid P)$. El lugar P es *mansamente ramificado* en F'/F si es ramificado en F'/F y ninguna extensión de P es salvajemente ramificada. Si al menos hay una extensión es salvajemente ramificada de P, decimos que P es *salvajemente ramificado*.

3. P es *totalmente ramificado* en F'/F si existe sólo una extensión P' de P en F'/F y el índice de ramificación es $e(P' \mid P) = [F' : F]$.

4. F'/F se dice *ramificada (respect. no ramificada)* si al menos un lugar $P \in \mathbb{P}_F$ es ramificado (respect. si todo $P \in \mathbb{P}_F$ es no ramificado).

5. F'/F se dice que es *mansa* si ningún lugar $P \in \mathbb{P}_F$ es salvajemente ramificado en F'/F.

Corolario 3.5.5. *Sea F'/F una extensión finita y separable de campos de funciones.*

1. *Si $P \in \mathbb{P}_F$ y $P' \in \mathbb{P}_{F'}$ son tales que $P' \mid P$, entonces $P' \mid P$ es ramificada si y sólo si $P' \leq Diff(F'/F)$. Si $P' \mid P$ es ramificada, entonces*

$$d(P' \mid P) = e(P' \mid P) - 1 \iff P' \mid P \text{ es mansamente ramificada}$$

$$d(P' \mid P) \geq e(P' \mid P) \iff P' \mid P \text{ es salvajemente ramificada}$$

2. *Casi todos los lugares $P \in \mathbb{P}_F$ son no ramificados en F'/F.*

Demostración. Este corolario es inmediato del teorema de Dedekind. □

Veamos ahora un resultado importante consecuencia de la fórmula del género de Hurwitz.

Corolario 3.5.6. *Sea F'/F una extensión finita y separable de campos de funciones, que tienen el mismo campo de constantes. Sea g (respect. g') el género de F/K (F'/K). Entonces*

$$2g' - 2 \geq [F' : F](2g - 2) + \sum_{P \in \mathbb{P}_F} \sum_{P' \mid P} (e(P' \mid P) - 1) \, deg \, P'$$

La igualdad se cumple si y sólo si F'/F es mansa.

Demostración. Clara por los teoremas 3.4.10 y 3.5.1. □

Otro par de corolarios inmediatos son los siguientes.

Corolario 3.5.7. *Sea F'/F una extensión finita y separable de campos de funciones, que poseen el mismo campo de constantes y sea g (respect. g') el género de F/K (F'/K). Entonces $g' \geq g$.*

Corolario 3.5.8. *Sea $F/K(x)$ una extensión separable y finita del campo de funciones racional de grado $[F : K(x)] > 1$ tal que K es el campo de constantes de F. Entonces $F/K(x)$ es ramificada.*

Demostración. Por la fórmula de Riemann-Hurwitz tenemos

$$2g' - 2 = -2[F' : K(x)] + deg \, Diff(F'/K(x))$$

donde g es el género de F/K. Por lo tanto

$$deg \, Diff(F'/K(x)) \geq 2([F : K(x)] - 1) > 0$$

La afirmación se cumple pues cualquier lugar en el soporte del diferente se ramifica por corolario 3.5.5. □

Teorema 3.5.9. *Sea $F' = F(y)$ una extensión finita y separable de campos de funciones, de grado $[F' : F] = n$. Sea $P \in \mathbb{P}_F$ tal que polinomio mínimo $\phi(T)$ de y sobre F tiene coeficientes en $\mathcal{O}_P$, es decir, y sea entero sobre $\mathcal{O}_P$ y sean $P_1, \ldots, P_r$ todas las extensiones de P en $\mathbb{P}_{F'}$. Entonces*

1. *$d(P_i \mid P) \leq v_{P_i}(\phi'(y))$ para $1 \leq i \leq r$.*
2. *El conjunto $\{1, y, \ldots, y^{n-1}\}$ es una base entera de F'/F en el lugar P si y sólo si $d(P_i \mid P) = v_{P_i}(\phi'(y))$ para $1 \leq i \leq r$.*

Demostración. Ver [Bri]. □

3.6 Extensiones constantes

Vamos a considerar un campo de funciones algebraicas F/K con campo de constantes K el cual supondremos siempre que es perfecto. Pensemos en una extensión algebraica $K \subseteq K'$. El campo compuesto $F' = FK'$ es un campo de funciones sobre K' y su campo de constantes es una extensión finita de K'. Lo que no es claro en primera instancia es que K' sea el campo pleno de constantes de F'. Así que empezamos esta sección respondiendo esa pregunta.

Lema 3.6.1. *Sea $\Psi \supseteq F$ un campo algebraicamente cerrado y $\alpha \in \Psi$ algebraico sobre K. Entonces $[K(\alpha) : K] = [F(\alpha) : F]$.*

Demostración. La desigualdad $[K(\alpha) : K] \leq [F(\alpha) : F]$ es inmediata, de modo que sólo tenemos que probar que el polinomio mínimo $\phi(T) \in K[T]$ de α permanece irreducible en $F[T]$. Supongamos que no es así; entonces $\phi(T) = g(T)h(T)$ con polinomios mónicos $g(T), h(T) \in F[T]$ de grado ≥ 1. Cualquier raíz de $g(T)$ y $h(T)$ en Φ es también una raíz de $\phi(T)$ y por lo tanto algebraica sobre K. Por lo tanto todos los coeficientes de $g(T)$ y de $h(T)$ son algebraicos sobre K por las fórmulas de Vieta. Por otra parte, estos coeficientes son elementos de F. Como K es algebraicamente cerrado en F, concluimos que $g(T), h(T) \in K[T]$, lo cual contradice la irreducibilidad de $\phi(T)$ sobre K. □

Proposición 3.6.2. *Sea $F' = FK'$ una extensión constante de campos de funciones de F (de grado finito o infinito), entonces*

1. *K' es todo el campo de constantes de F'.*
2. *Cualquier subconjunto de F que es linealmente independiente sobre K, permanece linalmente independiente sobre K'.*
3. *$[F : K(x)] = [F' : K'(x)]$ para cualquier $x \in F \backslash K$.*

Demostración. (1) Consideremos un elemento $\gamma \in F'$ el cual es algebraico sobre K'. Entonces es algebraico también sobre K y existe un número finito de elementos $\alpha_1, \ldots, \alpha_r \in K'$ tal que $\gamma \in F(\alpha_1, \ldots, \alpha_r) = K(\alpha)$ para algún $\alpha \in K'$ (en este punto usamos el hecho de que K es perfecto). Dado que γ es algebraico sobre K, podemos encontrar $\beta \in F'$ con $K(\alpha, \gamma) = K(\beta)$. Entonces tenemos que $F(\beta) = F(\alpha, \gamma) = F(\alpha)$ (pues $\gamma \in F(\alpha_1, \ldots, \alpha_r) = F(\alpha)$) y por el lema anterior

$$[K(\beta) : K] = [F(\beta) : F] = [F(\alpha) : F] = [K(\alpha) : K]$$

Esto implica que $K(\alpha) = K(\beta)$ y entonces $\gamma \in K(\alpha) \subseteq K'$. (2) Sean $y_1, \ldots, y_r \in F$ elementos linealmente independientes sobre K y consideremos ahora una combinación lineal

$$\sum_{i=1}^{r} \gamma_i y_i = 0 \quad \text{con } \gamma_i \in K' \tag{3.31}$$

Tomemos $\alpha \in K'$ tal que $\gamma_1, \ldots, \gamma_r \in K(\alpha)$ y escribamos

$$\gamma_i \sum_{j=1}^{n-1} c_{ij}\alpha^j \quad \text{con } c_{ij} \in K,\ n = [K(\alpha) : K]$$

De (3.31) tenemos

$$0 = \sum_{i=1}^{r} \left(\sum_{j=0}^{n-1} c_{ij}\alpha^j \right) y_i = \sum_{j=0}^{n-1} (c_{ij}y_i)\alpha^j \tag{3.32}$$

Con $\sum_{j=0}^{n-1} c_{ij}y_i \in F$. Puesto que $[F(\alpha) : F] = [K(\alpha) : K]$ por el lema anterior, se sigue los elementos $1, \alpha, \ldots, \alpha^{n-1}$ son linealmente independientes sobre F y (3.32) implica

$$\sum_{j=0}^{n-1} c_{ij}y_i = 0 \quad \text{para } j = 0, \ldots, n-1$$

Dado que los elementos $y_1, \ldots, y_r$ son linealmente independientes sobre K se sigue que $c_{ij} = 0$ y por lo tanto (3.31) es la combinación lineal trivial. (3) Claramente $[F' : K'(x)] \leq [F : K(x)]$. Por lo tanto sólo resta probar que un cualesquiera elementos $z_1, \ldots, z_s \in F$ que son linealmente independientes sobre $K(x)$ permanecen linealmente independientes sobre $K'(x)$. Supongamos que esto no ocurre, es decir existe una combinación lineal no trivial

$$\sum_{i=1}^{s} f_i(x)z_i = 0 \tag{3.33}$$

con $f_i(x) \in K'(x)$, no todos cero. Si multiplicamos todos por el común denominador, podemos suponer que todos los $f_i(x) \in K'[x]$. Entonces (3.33) establece una dependencia lineal del conjunto $A = \{x^j z_i \mid 1 \leq i \leq s,\ j \geq 0\}$ sobre K'. La parte 2 de esta proposición implica que este conjunto es linealmente dependiente sobre K también; de manera que $z_1, \ldots, z_s$ son linealmente dependientes sobre $K(x)$, lo cual es una contradicción. □

El siguiente teorema resume las propiedades más importantes de las extensiones constantes.

Teorema 3.6.3. *En una extensión algebraica constante $F' = K'F$ de F/K se cumple lo siguiente.*

1. *F'/F es no ramificado, i.e., $e(P' \mid P) = 1$ para todo $P \in \mathbb{P}_F$ y todo $P' \in \mathbb{P}_{F'}$ tal que $P' \mid P$.*

2. *F'/K' tiene el mismo género que F/K.*

3. *Para todo divisor $A \in \mathcal{D}_F$ tenemos que $deg\, Con_{F'/F}(A) = deg\, A$.*

4. *Para todo divisor $A \in \mathcal{D}_F$, $dim\, Con_{F'/F}(A) = dim\, A$. Más aún, cualquier base de $\mathcal{L}(A)$ es también una base de $\mathcal{L}(Con_{F'/F}(A))$.*

5. *Si W es un divisor canónico de F/K entonces $Con_{F'/F}(W)$ es también un divisor canónico de F'/K'.*

6. *La aplicación conorma $Con_{F'/F} : Pic_F \to Pic_{F'}$ del grupo de clases divisoras de F en el grupo de clases divisoras de F' es inyectivo.*

7. *El campo de clases residuales $F_{P'}$ de cualquier lugar $P' \in \mathbb{P}_{F'}$ es el campo compuesto $F_P K'$ de K' y del campo de clases residuales F_P, donde $P = P' \cap P$.*

8. *Si K'/K es de grado finito, cualquier base de K'/K es una base entera de F'/F para todo $P \in \mathbb{P}_F$.*

Demostración. Vamos a demostrar primero (1) y (2) en el caso de una extensión finita y posteriormente probaremos (8). Podemos suponer que $K' = K(\alpha)$ y en este caso $F' = F(\alpha)$ y el polinomio mínimo de $\phi(T)$ de α sobre K permanece irreducible sobre F por el lema 3.6.1. Sea ahora $P \in \mathbb{P}_F$ y $P' \in \mathbb{P}_{F'}$ con $P' \mid P$. El exponente del diferente $d(P' \mid P)$ satisface que

$$0 \leq d(P' \mid P) \leq v_{P'}(\phi'(\alpha))$$

Por el teorema 3.5.9. Como α es separable sobre K se cumple que $\phi'(\alpha) \neq 0$ y como $\phi'(\alpha) \in K'$ implica que $v_{P'}(\phi'(\alpha)) = 0$. De manera que tenemos

$$d(P' \mid P) = v_{P'}(\phi'(\alpha)) = 0 \tag{3.34}$$

Por el teorema de Dedekind, concluimos que $P' \mid P$ es no ramificada. La fórmula del género de Riemann-Hurwitz nos da

$$2g' - 2 = \frac{[F' : F]}{[K' : K]}(2g - 2) + deg\, Diff(F'/F) \tag{3.35}$$

donde g (resp. g') denota el género de F/K (resp. de F'/K'). Como $K' = K(\alpha)$ tenemos que $[F' : F] = [K' : K]$ y $Diff(F'/F) = 0$ por (3.34) y por lo tanto $2g' - 2 = 2g - 2$ por (3.35) y entoces tenemos 1 y 2 en el caso de una extensión constante finita.

Ahora probaremos 8. En este caso podemos suponer que $K' = K(\alpha)$ y sea ahora $n = [K' : K]$. De (3.34) y del teorema 3.5.9, tenemos que $1, \alpha, \ldots, \alpha^{n-1}$ es una base entera de F'/F para todo $P \in \mathbb{P}_F$. Obviamente para cualquier otra base $\gamma_1, \ldots, \gamma_n$ de K'/K

$$\sum_{i=0}^{n-1} \mathcal{O}_P \alpha^i = \sum_{j=1}^{n} \mathcal{O}_P \gamma_j$$

de manera que $\gamma_1, \ldots, \gamma_n$ es también una base entera. De ahora en adelante supondremos que F'/F es una extensión algebraica arbitraria.

(1) Sea $P' \in \mathbb{P}_{F'}$ una extensión de P. Escojamos $t \in F'$ un elemento primo primo para P'. Podemos tomar un campo intermedio $K \subseteq K_1 \subseteq K'$ tal que el grado de $[K_1 : K]$ es finito y $t \in F_1 \doteq FK_1$. Sea ahora $P_1 = P \cap F_1$. Entonces $v_{P'}(t) = 1 = e(P' \mid P) v_{P_1}(t)$ y por lo tanto $e(P' \mid P_1) = 1$. Por otra parte ya hemos demostrado que $e(P_1 \mid P) = 1$, de manera que $e(P' \mid P) = e(P' \mid P_1) e(P_1 \mid P) = 1$.

(3) Es suficiente probar el resultado para un divisor primo $P \in \mathbb{P}_F$. Escojamos $x \in F$ tal que P sea el único cero de x en F (tal elemento existe por la proposición 1.6.5, de manera que el divisor cero $(x)_0^F$ de $x \in \mathcal{D}_F$ tiene la forma $(x)_0^F = rP$ con $r > 0$. Se sigue de la proposición 3.1.9 que

$$(x)_0^{F'} = Con_{F'/F}((x)_0^F) = r Con_{F'/F}(P)$$

Usamos ahora el hecho de que $[F' : K'(x)] = deg\,((x)_0^{F'})$ y obtenemos

$$\begin{aligned} r deg\, Con_{F'/F}(P) &= [F' : K'(x)] \\ &= [F : K(x)] \\ &= deg((x)_0^F) = r deg\, P \end{aligned}$$

De esta manera tenemos (3).

(2) Como primer paso mostraremos que

$$dim\, A \leq dim\, Con_{F'/F}(A) \tag{3.36}$$

se cumple para todo $A \in \mathcal{D}_F$. Si $\{x_1, \ldots, x_r\}$ es una base del espacio $\mathcal{L}(A)$ entonces $x_i \in \mathcal{L}(Con_{F'/F}(A))$ por la proposición 3.1.9 y los elementos $x_1, \ldots, x_r$ son linealmente independientes sobre K' por la proposición 3.6.1, lo cual prueba (3.36). Sea g (resp. g') el género de F/K (resp. el género de F'/K') escojamos ahora un divisor $C \in \mathcal{D}_F$ que satisfaga

$$deg\, C \geq \text{ máx } \{2g - 1, 2g' - 1\} \tag{3.37}$$

Por el teorema de Riemann-Roch tenemos

$$dim\, C = deg\, C + 1 - g \tag{3.38}$$

y

$$dim\, Con_{F'/F}(C) = deg\, C + 1 - g' \tag{3.39}$$

En esta parte hemos usado el hecho de que $deg\, Con_{F'/F}(C) = deg\, C$ por (3). Ahora (3.36), (3.37) y (3.38) implican que $g' \leq g$. Para demostrar la otra desigualdad $g \leq g'$ consideremos una base $\{u_1, \ldots, u_s\}$ de $\mathcal{L}(Con_{F'/F}(C))$. Entonces tomamos un campo intermedio $K \subseteq K_0 \subseteq K'$ con $[K_0 : K] < \infty$ y $u_1, \ldots, u_s \in F_0 = K_0 F$. Claramente $u_1, \ldots, u_s \in \mathcal{L}(Con_{F_0/F}(C))$ y entonces

$$dim\, Con_{F_0/F}(C) \geq dim\, Con_{F'/F}(C) \tag{3.40}$$

Ya hemos mostrado que F_0/K_0 tiene género g (pues es una extensión constante finita) y el teorema de Riemann-Roch nos dice

$$dim\, Con_{F_0/F}(C) = deg\, C + 1 - g \tag{3.41}$$

Si ahora combinamos (3.38), (3.39) y (3.40) tenemos $g \leq g'$, por lo tanto $g = g'$. (4) Supongamos primero que $deg\, A \geq 2g - 1$. Como $g' = g$ por el teorema de Riemann-Roch y (3) tenemos

$$dim\, Con_{F'/F}(A) = deg\, Con_{F'/F}(A) + 1 - g$$

$$deg\, A + 1 - g = dim\, A$$

El mismo argumento que usamos para demostrar (3.36) muestra que cualquier base de $\mathcal{L}(A)$ es también una base de $\mathcal{L}(Con_{F'/F}(A))$. Consideremos ahora un divisor arbitrario $A \in \mathcal{D}_F$ y una base $\{x_1, \ldots, x_r\}$ de $\mathcal{L}(A)$. Puesto que $x_1, \ldots, x_r \in \mathcal{L}(Con_{F'/F}(A))$ y puesto que son linealmente independientes sobre K', es suficiente probar que todo $z \in \mathcal{L}(Con_{F'/F}(A))$ es una K'-combinación

lineal de $x_1, \ldots, x_r$. Escojamos ahora divisores primos $P_1 \neq P_2$ de F/K y definamos $A_1 := n_1 P_1$ y $A_2 := n_2 P_2$ con $n_1, n_2 \geq 0$ tales que $deg\, A_i \geq 2g-1$ para $i = 1, 2$. Entonces

$$A = \text{mín}\ \{n_1, n_2\} \text{ y } \mathcal{L}(A) = \mathcal{L}(A_1) \cap \mathcal{L}(A_2).$$

Extendemos $\{x_1 \ldots, x_r\}$ a una base $\{x_1 \ldots, x_r, y_1, \ldots, y_m\}$ del espacio vectorial $\mathcal{L}(A) \neq \mathcal{L}(A_1)$ y $\{x_1 \ldots, x_r, z_1, \ldots, z_n\}$ de $\mathcal{L}(A) \neq \mathcal{L}(A_2)$ respectivamente. Los elementos

$$x_1, \ldots, x_r, y_1, \ldots, y_m, z_1, \ldots, z_n \tag{3.42}$$

son linealmente independientes sobre K, veámoslo. Si tenemos una combinación lineal

$$\sum_{i=1}^{r} a_i x_i + \sum_{j=1}^{m} b_j y_j + \sum_{k=1}^{n} c_k z_k = 0$$

con $a_i,\ b_j,\ c_k \in K$. Entonces

$$\sum_{i=1}^{r} a_i x_i + \sum_{j=1}^{m} b_j y_j = -\sum_{k=1}^{n} c_k z_k \in \mathcal{L}(A_1) \cap \mathcal{L}(A_2) = \mathcal{L}(A)$$

Puesto que $\{x_1, \ldots, x_r\}$ es una base de $\mathcal{L}(A)$ y $x_1 \ldots, x_r, y_1, \ldots, y_m$ son linealmente independientes, esto implica que $b_j = 0$ para toda j y entoces también por la independencia lineal de los elementos $x_1, \ldots, x_r, z_1, \ldots, z_n$ se sigue que $a_i = c_k = 0$ para toda i y toda k. Recordando que los elementos de F que son linealmente independientes sobre K permanecen linealmente independientes sobre K' por la proposición 3.6.1 concluimos que los elmentos (3.42) son linealmente independientes sobre K'.

Sea ahora $z \in \mathcal{L}(Con_{F'/F}(A))$. Como $deg\, A_i \geq 2g-1$, la afirmación (4) vale para A_i y escribimos

$$z = \sum_{i=1}^{r} d_i x_i + \sum_{j=1}^{m} e_j y_j = \sum_{i=1}^{r} f_i x_i + \sum_{k=1}^{n} g_k z_k \tag{3.43}$$

con $d_i,\ e_j,\ f_i,\ g_k \in K'$. Como $x_1, \ldots, x_r, y_1, \ldots, y_m, z_1, \ldots, z_n$ son linealmente independientes, las dos representaciones en (3.43) coinciden, por lo tanto $e_j = g_k = 0$ para toda j y toda k. De manera que z es una combinación lineal de $x_1, \ldots, x_r$ sobre K'.

(5) Si W es un divisor canónico de F/K entonces $deg\, W = 2g-2$ y $dim\, W = g$, pero por todo lo que ya se ha probado tenemos

$$deg\, Con_{F'/F}(W) = 2g-2 \text{ y } dim\, Con_{F'/F}(W) = g.$$

Estas dos propiedades caracterizan por completo a los divisores canónicos, por la proposición 1.6.2.

(6) Puesto que $Con_{F'/F} : Pic_F \to Pic_{F'}$ es un homomorfismo, debemos mostrar que el núcleo es cero. Consideremos un divisor $A \in \mathcal{D}_F$ cuya conorma en F' es principal. Esto implica que

$$deg\, Con_{F'/F}(A) = 0 \text{ y } dim\, Con_{F'/F}(A) = 1$$

Entonces $deg\, A = 0$ y $dim\, A = 1$ por (3) y (4). Esto implica que A es principal, por el corolario 1.4.12.

(7) Sea $z(P') \in F'_{P'}$ donde $z \in \mathcal{O}_{P'}$. Existe un campo intermedio $K \subseteq K_1 \subseteq K'$ con $z \in F_1 = K_1F$ y $[K_1 : K] < \infty$. Sea $P_1 = P' \cap F_1$ y sean $P_2, \ldots, P_r$ los otros lugares de F_1/K_1 que yacen sobre P. Tomemos $u \in F_1$ tal que

$$v_{P_1}(z - u) > 0 \text{ y } v_{P_i}(u) \geq 0 \text{ para } 2 \leq i \leq r$$

Entonces $z(P') = u(P')$ y entonces u se encuentra en la cerradura entera de $\mathcal{O}_P$ en F_1 por el corolario 3.3.5. Por (8)

$$u = \sum_{i=1}^{n} \gamma_i x_i \text{ con } \gamma_i \in K_1,\ x_i \in \mathcal{O}_P.$$

Por lo tanto,

$$z(P') = u(P') = \sum_{i=1}^{n} \gamma_i x_i(P) \in F_1 K'.$$

□

El siguiente corolario nos da una fórmula para el grado de la conorma de un divisor en una extensión algebraica arbitraria de campos de funciones.

Corolario 3.6.4. *Sea F'/K' una extensión algebraica de F/K. Entonces para todo divisor $A \in \mathcal{D}_F$,*

$$deg\, Con_{F'/F}(A) = [F' : FK']\, deg\, A$$

Demostración. Por el lema 3.1.2 sabemos que $[F' : FK'] < \infty$ y FK'/K' es una extensión constante de F/K y como

$$Con_{F'/F}(A) = Con_{F'/FK'}(Con_{FK'/F}(A))$$

obtenemos

$$deg\, Con_{F'/F}(A) = [F' : FK']\, deg\, Con_{FK'/K'}(A) = [F' : FK']\, deg\, A$$

por el corolario 3.1.13 y el teorema 3.6.3. □

Corolario 3.6.5. *Sea $P \in \mathbb{P}_F$ un lugar de F/K de grado r y $\bar{F} = F\bar{K}$ la extensión constante de F/K con la cerradura algebraica $\bar{K}$ de K. Entonces*

$$Con_{\bar{F}/F}(P) = \bar{P}_1 + \cdots + \bar{P}_r$$

con distintos lugares $\bar{P}_i$

Demostración. Es una consecuencia inmediata del teorema anterior, partes (1) y (3). □

Proposición 3.6.6. *Sea F/K un campo de funciones con campo de constantes K. Supongamos que F'/F es una extensión finita con campo de constantes K'. Sea $\Phi \supseteq \bar{K}$ la cerradura algebraica de K. Entonces*

$$[F' : F] = [F'\bar{K} : F\bar{K}][K' : K] \tag{3.44}$$

En el caso especial $F' = F(y)$, si $\phi(T) \in F[T]$ es el polinomio mínimo de y sobre F, entonces las siguentes condiciones son equivalentes:

1. *$K' = K$.*
2. *$\phi(T)$ es irreducible en $F\bar{K}[T]$.*

Demostración. Dado que $F \subseteq FK' \subseteq F'$, se cumple

$$[F' : F] = [F' : FK'][FK' : F] \tag{3.45}$$

La extensión K'/K es separable y de grado finito, por lo tanto $K' = K(\alpha)$ para algún $\alpha \in K'$ y el lema 3.6.1 implica

$$[FK' : F] = [K' : K] \tag{3.46}$$

La proposición 3.6.2, (3) muestra que para todo $x \in F \backslash K$,

$$[FK' : K(x)] = [F\bar{K} : \bar{K}(x)] \text{ y } [F' : K'(x)] = [F'\bar{K} : \bar{K}(x)].$$

Lo cual implica

$$[F' : FK'] = [F'\bar{K} : F\bar{K}] \tag{3.47}$$

Si sustituimos (3.47) y (3.46) en (3.45) obtenemos (3.44).

Consideremos ahora el caso $F' = F(y)$. Notemos que $[F' : F] = deg\,\phi(T)$ y $[F'\bar{K} : F\bar{K}]$ es igual al grado del polinomio mínimo de y sobre $F\bar{K}$ (el cual divide a $\phi(T)$ en $F\bar{K}[T]$). La equivalencia entre (1) y (2) es por lo tanto una consecuencia inmediata de (3.44). □

Un polinomio $\phi(T) \in K(x)[T]$ (sobre el campo de funciones racional $K(x)$) se dice que es absolutamente irreducible si $\phi(T)$ es irreducible en el anillo de polinomios $\bar{K}(X)[T]$ (donde $\bar{K}$ denota la cerradura algebraica de K). El siguiente corolario es un caso especial de la proposición anterior.

Corolario 3.6.7. *Sea $F = K(x, y)$ un campo de funciones y $\phi(T) \in K(x)[T]$ el polinomio mínimo de y sobre $K(x)$. Las siguientes condiciones son equivalentes:*

1. *K es todo el campo de constantes de F.*
2. *$\phi(T)$ es absolutamente irreducible*

3.7 Extensiones de Galois

Las extensiones de Galois que estudiaremos tienen propiedades muy útiles que, desde luego, no necesariamente se cumplen en una extensión arbitraria. Recordemos que una extensión de campos finita M/L se dice que es una *extensión de Galois* si el grupo de automorfismos $Aut(M/L) = \{\sigma : M \to M \mid \sigma(a) = a$ para toda $a \in L$ y σ isomorfismo $\}$ tiene orden $[M : L]$. En tal caso llamaremos a $Aut(M/L)$ el *grupo de Galois* de M/L y lo denotaremos por $Gal(M/L)$.

Una extensión de campos de funciones se dice que es de Galois si F'/F es de Galois de grado finito. Comenzaremos con un teorema que nos dice que tipo de acción tiene el grupo de Galois en las extensiones de los lugares

Teorema 3.7.1. *Sea F'/K' una extensión de Galois de F/K y sean P_1 y P_2 extensiones de un lugar $P \in \mathbb{P}_F$. Entonces $P_2 = \sigma(P_1)$ para algún $\sigma \in Gal(F'/F)$. En otras palabras, la acción del grupo de Galois es transitiva en el conjunto de extensiones de P.*

Demostración. Supongamos que el enunciado es falso, es decir, que $\sigma(P_1) \neq P_2$ para todo $\sigma \in G := Gal(F'/F)$. Por el teorema de aproximación fuerte, existe un elemento $z \in F'$ tal que $v_{P_2}(z) > 0$ y $v_Q(z) = 0$ para todo $Q \in \mathbb{P}_{F'}$ con $Q \mid P$ y $Q \neq P_2$. Sea $N_{F'/F} : F' \to F$ la aplicación norma. Tenemos entonces lo siguiente

$$v_{P_1}(N_{F'/F}(z)) = v_{P_1}\left(\prod_{\sigma \in G} \sigma(z)\right) = \sum_{\sigma \in G} v_{P_1}(\sigma(z))$$

$$= \sum_{\sigma \in G} v_{\sigma^{-1}(P_1)}(z) = \sum_{\sigma \in G} v_{\sigma(P_1)}(z) = 0 \qquad (3.48)$$

puesto que P_2 no se encuentra dentro de los lugares $\sigma(P_1)$, $\sigma \in G$ (nótese que aquí usamos el lema 3.5.2). Por otro lado

$$v_{P_2}(N_{F'/F}(z)) = \sum_{\sigma \in G} v_{\sigma(P_2)}(z) > 0 \tag{3.49}$$

Pero $N_{F'/F}(z) \in F$, por lo tanto

$$v_{P_1}(N_{F'/F}(z)) = 0 \iff v_P(N_{F'/F}(z)) = 0 \iff v_{P_2}(N_{F'/F}(z)) = 0$$

Lo cual es una contradicción a (3.48) y (3.49). □

Corolario 3.7.2. *Con la notación como en el teorema anterior, con F'/F una extensión de Galois. Sean $P_1, \ldots, P_r$ todos los lugares de F' que yacen sobre P. Entonces tenemos*

1. *$e(P_i \mid P) = e(P_j \mid P)$ y $f(P_i \mid P) = f(P_j \mid P)$ para toda $i, \ldots, j$. Por lo tanto definimos $e(P) = e(P_j \mid P)$ y $f(P) = f(P_i \mid P)$ y llamamos a $e(P)$ (resp. $f(P)$) el índice de ramificación de P (resp. el grado relativo de P) en F'/F.*
2. *$e(P)f(P)r = [F' : F]$.*
3. *Los coeficientes del diferente $d(P_i \mid P)$ y $d(P_j \mid P)$ son iguales para toda i, j.*

Demostración. La parte (1) es inmediata por el teorema anterior y el lema 3.5.2, mientras que (2) es una consecuencia directa de (1) y del teorema 3.1.11. Para demostrar (3) consideremos la cerradura entera

$$\mathcal{O}'_P = \bigcap_{i=1}^{r} \mathcal{O}_{P_i}$$

de $\mathcal{O}_P$ en F' y el módulo complementario

$$\mathcal{C}_P = \{z \in F' \mid Tr_{F'/F}(z\mathcal{O}'_P) \subseteq \mathcal{O}_P\}$$

Sea ahora $\sigma \in Gal(F'/F)$. Es claro que $\sigma(\mathcal{O}'_P) = \mathcal{O}_{P'}$ y que $\sigma(\mathcal{C}_P) = \mathcal{C}_P$ (usamos el hecho de que $Tr_{F'/F}(\sigma(u)) = Tr_{F'/F}(u)$ para $u \in F'$). Escribimos a $\mathcal{C}_P = t\mathcal{O}'_P$ y obtenemos $\sigma(t)\mathcal{O}'_P = \sigma(\mathcal{C}_P) = \mathcal{C}_P = t\mathcal{O}'_P$, de tal manera que

$$-d(P_i \mid P) = v_{P_i}(t) = v_{P_i}(\sigma(t))$$

para toda i (por la proposición 3.4.2 y la definición del exponente del diferente). Consideremos ahora dos lugares P_i, P_j que yazcan sobre P. Escojamos $\sigma \in G(F'/F)$ tal que $\sigma(P_i) = P_j$. Entonces

$$-d(P_i \mid P) = v_{P_i}(\sigma(t)) = v_{\sigma^{-1}(P_i)}(t) = v_{P_j}(t) = -d(P_j \mid P)$$

□

Hay extensiones de Galois que son particularmente interesantes como las extensiones de Kummer y las extensiones de Artin-Schreier. En el presente trabajo únicamente describiremos las extensiones de Kummer, puesto que utilizaremos éstas en el método del siguiente capítulo para construir curvas con muchos puntos racionales. El siguiente resultado es debido a Hasse.

Proposición 3.7.3. *Sea F/K un campo de funciones en el cual K contiene una raíz primitiva n-ésima de la unidad (con $n > 1$ y n primo relativo con la característica del campo K). Supongamos que $u \in F$ es un elemento que satisface*

$$u \neq w^d \text{ para todo } w \in F \text{ y } d \mid n,\ d > 1 \tag{3.50}$$

Sea ahora

$$F' = F(y) \text{ con } y^n = u \tag{3.51}$$

Dicha extensión F' es llamada una extensión de Kummer de F. Entonces se cumple lo siguiente

1. *El polinomio $\phi(T) = T^n - u$ es el polinomio mínimo de y sobre F (en particular es irreducible sobre F). La extensión F'/F es de Galois de grado n, su grupo de Galois es cíclico y todos los automorfismos de F'/F están dados por $\sigma(y) = \zeta y$, donde $\zeta \in K$ es una raíz n-ésima de la unidad.*

2. *Sea $P \in \mathbb{P}_F$ y $P' \in \mathbb{P}_{F'}$ una extensión de P. Entonces*

$$e(P' \mid P) = \frac{n}{r_P} \text{ y } d(P' \mid P) = \frac{n}{r_P} - 1$$

donde

$$r_P := mcd(n, v_P(u)) > 0$$

3. *Si K' es el campo de constantes de F' y g (resp. g') es el género de F (resp. de F'), entonces*

$$g' = 1 + \frac{n}{[K' : K]} \left(g - 1 + \frac{1}{2} \sum_{P \in \mathbb{P}_F} (1 - \frac{r_P}{n}) deg\, P \right)$$

con r_P definido como en 2.

Notemos primero que toda extensión cíclica F'/F de grado n es una extensión de Kummer, siempre que n sea primo relativo con la característica del campo y que F contenga a todas las raíces n-ésimas de la unidad. Este hecho es conocido de la teoría de Galois.

Demostración. La demostración de (1) se sigue de la teoría de Galois. Ver [Mor].

(2) Caso 1. Supongamos que $r_P = 1$, entonces de (3.51) obtenemos

$$nv_{P'}(y) = v_{P'}(y^n) = v_{P'}(u) = e(P' \mid P)v_P(u),$$

lo cual implica $e(P' \mid P) = n$, como n y $v_P(u)$ son primos relativos. Como n no es divisible por *char* K, el teorema de Dedekind nos dice $d(P' \mid P) = n - 1$

Caso 2. Supongamos que $r_P = n$, es decir, $v_P(u) = ln$ con $l \in \mathbb{Z}$. Escojamos $t \in F$ con $v_P(t) = l$ y definamos $y_1 := t^{-1}y$ y $u_1 := t^{-n}u$. Entonces $y_1^n = u_1$, $v_P(u_1) = 0$ y el polinomio irreducible de y_1 sobre F es

$$\psi(T) = T^n - u_1 \in F[T]$$

Entonces y_1 es entero sobre $\mathcal{O}_P$ y por el teorema 3.5.9 tenemos

$$0 \leq d(P' \mid P) \leq v_{P'}(\psi'(y_1))$$

Y tenemos que $\psi'(y_1) = ny_1^{n-1}$, de manera que $v_{P'}(\psi'(y_1)) = (n-1)v_{P'}(y_1) = 0$ y $d(P' \mid P) = 0$ por el teorema de Dedekind, $e(P' \mid P) = 1$ y tenemos (2) en este caso particular.

Caso 3. $1 < r_P < n$. Consideremos el campo intermedio siguiente

$$F_0 = F(y_0) \quad \text{con } y_0 = y^{n/r_P}$$

Entonces $[F' : F_0] = n/r_P$ y $[F_0 : F] = r_P$. El elemento y_0 satisface la ecuación

$$y_0^{r_P} = u \tag{3.52}$$

sobre F. Sea $P_0 = P' \cap F_0$. El caso 2 se aplica a F_0/F y por lo tanto $e(P_0 \mid P) = 1$. Por (3.52)

$$v_{P_0}(y_0) = \frac{v_P(u)}{r_P}$$

Este entero es primo relativo con n/r_P, así que el caso 1 se aplica a la extensión $F' = F_0(y)$ (notemos que $y^{n/r_P} = y_0$). Por lo tanto $e(P' \mid P_0) = n/r_P$ y

$$e(P' \mid P) = e(P' \mid P_0)e(P_0 \mid P) = n/r_P$$

(3) El grado del diferente $Diff(F'/F)$ es

$$\begin{aligned} deg\, Diff(F'/F) &= \sum_{P \in \mathbb{P}_F} \sum_{P' \mid P} d(P' \mid P) deg\, P' \\ &= \sum_{P \in \mathbb{P}_F} (\frac{n}{r_P} - 1) \sum_{P' \mid P} deg\, P' \end{aligned} \tag{3.53}$$

Notemos que para un lugar fijo $P \in \mathbb{P}_F$, el índice de ramificación $e(P) = e(P' \mid P)$ no depende de la elección de P' y entonces tenemos

$$\sum_{P'|P} deg\, P' = \frac{1}{e(P)} deg\, (\sum_{P'|P} e(P' \mid P)P')$$

$$= \frac{1}{e(P)} deg\, Con_{F'/F}(P) = \frac{r_P}{n} \frac{n}{[K' : K]} deg\, P$$

$$= \frac{r_P}{[K' : K]} \deg P$$

por la parte (2) y por el corolario 3.1.13 y si sustituimos esto en (3.53) se muestra que

$$deg\, Diff(F'/F) = \sum_{P \in \mathbb{P}_F} \frac{n - r_P}{r_P} \frac{r_P}{[K' : K]} deg\, P$$

$$\frac{n}{[K' : K]} \sum_{P \in \mathbb{P}_F} (1 - \frac{r_P}{n}) deg\, P$$

Y la fórmula de Riemann-Hurwitz demuestra (3). □

Un corolario del teorema anterior que vale la pena resaltar es el siguiente.

Corolario 3.7.4. *Sea F/K campo de funciones y $F' = F(y)$ con $y^n = u \in F$ donde char K no divide a n y K contiene una raíz primitiva n-ésima de la unidad. Supongamos que existe un lugar $Q \in \mathbb{P}_F$ tal que $mcd(v_Q(u), n) = 1$. Entonces K todo el campo de constantes de F', la extensión F'/F es cíclica de grado n y*

$$g' = 1 + n(g - 1) + \frac{1}{2} \sum_{P \in \mathbb{P}_F} (n - r_P) deg\, P$$

Demostración. De la hipótesis $mcd(v_Q(u), n) = 1$ se sigue fácilmente que u satisface la condición (3.50). Únicamente resta probar que el campo de constantes K' de F' no es más grande que K y entonces el corolario se sigue inmediatamente de la proposición anterior. Escojamos Q' extensión de Q en F'. La parte (2) de la proposición muestra que

$$e(Q' \mid Q) = [F' : F] = n \tag{3.54}$$

Supongamos ahora que $[K' : K] > 1$ y consideremos el campo intermedio $F_1 = FK' \neq F$ y el lugar $Q_1 = Q' \cap F_1$. Por (3.54) tenemos que $e(Q_1 \mid Q) = [F_1 : F] > 1$. Por otra parte, $e(Q_1 \mid Q) = 1$ puesto que F_1/F es una extensión constante. Esta contradicción demuestra $K' = K$. □

Observación 3.7.5. En las demostraciones anteriores, en ningún momento, usamos la hipótesis de que K tuviera una raíz primitiva n-ésima de la unidad. Por lo tanto, las afirmaciones de la proposición 3.7.4 partes (2) y (3) son ciertas en un caso más general, con la sencilla excepción de que $F(y)/F$ ya no es extensión de Galois si K no contiene a todas las raíces n-ésimas de la unidad.

Para finalizar este capítulo vamos a dar algunas definiciones y enunciar algunos resultados, que en el presente trabajo no son tan importantes, pero que son necesarios para la demostración del teorema de Hasse-Weil del siguiente capítulo.

Definición 3.7.6. Consideremos F'/F una extensión de Galois con grupo de Galois $G := Gal(F'/F)$. Sea $P \in \mathbb{P}_F$ y P' una extensión de P.

1. $G_Z(P'|P) := \{\sigma \in G \mid \sigma(P') = P'\}$ es el *grupo de descomposición* de P' sobre P.
2. $G_T(P'|P) := \{\sigma \in G \mid v_{P'}(\sigma z - z) > 0 \text{ para toda } z \in \mathcal{O}_{P'}\}$ es el *grupo de inercia* de P' sobre P.
3. El campo fijo $Z := Z(P'|P)$ de $G_Z(P'|P)$ es llamado el *campo de descomposición*, mientras que el campo fijo $T := T(P'|P)$ de $G_T(P'|P)$ se llama *campo de inercia* de P' sobre P.

Tenemos además $G_T(P'|P) \subseteq G_Z(P'|P)$ y ambos son subgrupos de G.

Teorema 3.7.7. *Con la notación de la definición anterior.*

1. *El grupo de descomposición $G_Z(P'|P)$ tiene orden $e(P'|P)\, f(P'|P)$.*
2. *El grupo de inercia $G_T(P'/P)$ es un subgrupo normal de $G_Z(P'|P)$ de orden $e(P'|P)$.*
3. *La extensión de clases residuales $F'_{P'}/F_P$ es también de Galois. Cualquier automorfismo $\sigma \in G_Z(P'|P)$ induce un automorfismo $\bar{\sigma}$ de $F'_{P'}$ sobre F_P, definiendo $\bar{\sigma}(z(P')) = \sigma(z)(P')$ para toda $z \in \mathcal{O}_{P'}$. La función $\phi : G_Z(P'|P) \to Gal(F'_{P'}|F_P)$, dada por $\sigma \mapsto \bar{\sigma}$ es un epimorfismo cuyo núcleo es el grupo de inercia $G_T(P'|P)$.*
4. *Sea P_Z (resp. P_T) la restricción de P' al campo de descomposición $Z = Z(P'|P)$ (resp. $T = T(P'|P)$). Entonces tenemos lo siguiente: $F \subseteq Z \subseteq T \subseteq F'$, además $P \subseteq P_Z \subseteq P_T \subseteq P'$ y tenemos las siguientes condiciones en los índices $e(P'|P_T) = e(P'|P) = [F' : T]$, $f(P'|P_T) = 1$; $f(P_T|P_Z) = f(P'|P) = [T : Z]$, $e(P_T|P_Z) = 1$ y finalmente $e(P_Z|P) = f(P_Z|P) = 1$.*

Demostración. Revisar por ejemplo [Sti]. □

Capítulo 4

El teorema de Hasse-Weil

4.1 La función zeta de un campo de funciones

Lema 4.1.1. *Para todo $n \geq 0$ existen sólo un número finito de divisores positivos de grado n.*

Demostración. Un divisor positivo es suma finita de divisores positivos primos. Por lo tanto es suficiente probar que el conjunto $S = \{P \in \mathbb{P}_F \mid deg\, P \leq n\}$ es finito. Tomemos $x \in F \backslash \mathbb{F}_q$ y consideremos el conjunto $S_0 = \{P_0 \in \mathbb{P}_{\mathbb{F}_q(x)} \mid deg\, P_0 \leq n\}$. Es claro que $P \cap \mathbb{F}_q(x) \in S_0$ para todo $P \in S$ y por otra parte cualquier $P_0 \in S_0$ tiene un número finito de extensiones en F. Por lo tanto es suficiente mostrar que S_0 es finito. Pero los lugares de $\mathbb{F}_q(x)$ (exceptuando el polo de x) corresponden a polinomios mónicos irreducibles del mismo grado y sólo hay un número finito de estos polinomios puesto que $\mathbb{F}_q$ es finito. □

Recordemos la definición del grupo de Picard $Pic_F := \mathcal{D}_F/\mathcal{P}_F$. La clase de $A \in \mathcal{D}_F$ en el grupo de Picard Pic_F será denotada por $[A]$. Entonces $A \sim B \iff A \in [B] \iff [A] = [B]$. Divisores equivalentes tienen el mismo grado y dimensión como ya lo hemos visto; de manera que los enteros

$$deg\,[A] := deg\, A \text{ y } dim\,[A] := dim\,[A]$$

están bien definidos.

Definición 4.1.2. El conjunto

$$\mathcal{D}_F^0 := \{A \in \mathcal{D}_F \mid deg\, A = 0\}$$

el cual es obviamente un subgrupo de $\mathcal{D}_F$ es llamado el grupo de divisores de grado cero. Asimismo,

$$Pic_F^0 = \{[A] \in C_F \mid deg\,[A] = 0\}$$

es el grupo de clases divisoras de grado cero.

Proposición 4.1.3. *El grupo Pic_F^0 es finito. Su orden $h = h_F$ es llamado el número de clases de $F/\mathbb{F}_q$.*

Demostración. Sea $B \in \mathcal{D}_F$ de grado $n \geq g$ y consideremos el conjunto de clases divisoras

$$Pic_F^n = \{[C] \in C_F \mid deg\,[C] = n\}$$

La aplicación $\phi : Pic_F^0 \to Pic_F^n$ dada por $[A] \mapsto [A + B]$ es biyectiva, pues si $[A' + B] = [A + B] \Rightarrow A' + B = A + B + (x)$ con $x \neq$ y esto a su vez implica que $A' = A + (x)$ y por lo tanto ϕ es inyectiva. Consideremos ahora un divisor $C \in \mathcal{D}_F$ de grado n. Entonces el divisor $C - B$ tiene grado cero y por lo tanto $[C] = [C - B + B]$. Por lo tanto ϕ es suprayectiva. De modo que es suficiente verificar que Pic_F^n es finito.

Afirmamos ahora que para toda clase divisora $[C] \in Pic_F^n$ existe $A \geq 0$ con $A \in [C]$. Veámoslo, como $deg\,C = n \geq g$ tenemos por el teorema de Riemann

$$dim\,[C] \geq n + 1 - g \geq 1$$

y por la observación 1.5.5, como $dim\,C \geq 1$ existe $A \geq 0$ tal que $A \sim C$. Sólo hay un número finito de divisores de grado n por el lema anterior, lo cual implica la finitud de Pic_F^n. □

Damos a continuación una definición que nos servirá más adelante.

Definición 4.1.4. Definimos el entero $\partial > 0$ por

$$\partial := \min\{deg\,A \mid A \in \mathcal{D}_F \text{ y } deg\,A > 0\}$$

La imagen de la función grado $deg : \mathcal{D}_F \to \mathbb{Z}$ generado por ∂ y el grado de cualquier divisor de $F/\mathbb{F}_q$ es múltiplo de ∂.

A continuación definimos unos coeficientes que utilizaremos en muchos resultados posteriores.

$$A_n := \mid \{A \in \mathcal{D}_F \mid A \geq 0 \text{ y } deg\,A = n\} \mid$$

Por ejemplo, es claro que $A_0 = 1$ y A_1 es el número de lugares $P \in \mathbb{P}_F$ de grado uno.

Lema 4.1.5.

1. *$A_0 = 0$ si $\partial \nmid n$.*
2. *Para una clase divisora fija $[C] \in C_F$, tenemos*

$$\mid \{A \in [C] \mid A \geq 0\} \mid \quad = \frac{1}{q-1}(q^{dim[C]} - 1)$$

3. Para cualquier entero $n > 2g-2$ con $\partial \mid n$,

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

Demostración. La parte (1) es clara.

(2) Las condiciones $A \in [C]$ y $A \geq 0$ son equivalentes a

$$A = (x) + C \text{ para algún } x \in F \text{ con } (x) \geq -C,$$

es decir, $x \in \mathcal{L}(C)\backslash\{0\}$. Existe exactamente $q^{dim[C]}-1$ elementos (pues tenemos tantas copias de $\mathbb{F}_q$ como $dim\,[C]$ y estamos quitando el elemento cero) $x \in \mathcal{L}(C)\backslash\{0\}$ y dos de ellos dan el mismo divisor si y sólo si difieren por una constante $\alpha \neq 0, \alpha \in \mathbb{F}_q$, pues $v_P(x) = v_P(\alpha x)$ si $\alpha \in \mathbb{F}_q^*$.

(3) Hay $h = h_F$ clases de divisores de grado n a decir $[C_1], \ldots, [C_h]$ entonces por (2) y el teorema de Riemann-Roch

$$\mid \{A \in [C_j]; A \geq 0\} \mid \; = \frac{1}{q-1}(q^{n+1-g}-1)$$

Claramente cualquier divisor de grado n se encuentra en una de las clases divisoras $[C_1], \ldots, [C_h]$. Por lo tanto

$$A_n = \sum_{i=1}^{h} \mid \{A \in [C_j]; A \geq 0\} \mid = \frac{h}{q-1}(q^{n+1-g}-1).$$

□

Definición 4.1.6. La serie de potencias

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

es llamada la *función Zeta* de $F/\mathbb{F}_q$. Notemos que $Z(t)$ es una serie de potencias sobre el campo de los complejos. Ahora veremos que esta serie de potencias converge en una vecindad del cero.

Proposición 4.1.7. *La serie de potencias $Z_F(t) = \sum_{n=0}^{\infty} A_n t^n$ es convergente para $\mid t \mid < q^{-1}$. Más precisamente si $\mid t \mid < q^{-1}$*

1. Si $F/\mathbb{F}_q$ tiene género $g = 0$ entonces

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

2. Si $g \geq 1$, entonces $Z(t) = F(t) + G(t)$, donde

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

($[C]$ recorre todas las clases divisoras $[C] \in \mathrm{Pic}_F$ con $0 \leq deg\,[C] \leq 2g-2$) 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. (1) Caso $g = 0$. En primera instancia mostraremos que todo campo de funciones de género cero tiene como número de clases $h = 1$, i.e. cada divisor de A de grado cero, es principal. Este hecho se sigue del teorema de Riemann-Roch, pues $0 > 2g - 2$, entonces $dim\,A = deg\,A + 1 - g = 1$ y por lo tanto, podemos encontrar $0 \neq x \in F$ tal que $(x) \geq -A$. Ambos son divisores de grado cero y entonces $A = -(x) = (x^{-1})$ es principal. Si ahora aplicamos el lema 4.1.5 obtenemos

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

para $|qt| < 1$. (2) Para $g \geq 1$ obtenemos ahora

$$\sum_{n=0}^{\infty} A_n t^n = \sum_{deg\,[C] \geq 0} |\,\{A \in [C]; A \geq 0\}\,|\, t^{deg\,[C]} = \sum_{deg\,[C] \geq 0} \frac{q^{dim\,[C]} - 1}{q-1} t^{deg\,[C]}$$

$$= \frac{1}{q-1} \sum_{0 \leq deg\,[C] \leq 2g-2} q^{dim\,[C]}\, t^{deg\,[C]} + \frac{1}{q-1} \sum_{deg\,[C] > 2g-2} q^{deg\,[C]+1-g}\, t^{deg\,[C]}$$

$$- \frac{1}{q-1} \sum_{deg\,[C] \geq 0} t^{deg\,[C]} = F(t) + G(t),$$

con

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

y

$$(q-1)G(t) = \sum_{n=\frac{2g-2}{\partial}+1}^{\infty} hq^{n\partial+1-g}t^{n\partial} - \sum_{n=0}^{\infty} ht^{n\partial}$$
$$= hq^{1-g}(qt)^{2g-2+\partial}\frac{1}{1-(qt)^{\partial}} - h\frac{1}{1-t^{\partial}}$$

□

Corolario 4.1.8. *La función $Z(t)$ puede ser extendida a una función racional sobre $\mathbb{C}$ y tiene un polo simple en $t = 1$.*

Demostración. Este hecho es evidente, pues $\frac{1}{1-t^{\partial}}$ tiene un polo simple en $t = 1$. □

Ahora deseamos estudiar el comportamiento de la función zeta de $F/\mathbb{F}_q$ bajo extensiones constantes finitas y para esto es conveniente a menudo tener una representación de $Z(t)$ como un producto infinito. Recordemos del análisis complejo que un producto infinito $\prod_{i=1}^{\infty}(1+a_i)$ (con $a_i \neq -1$, $a_i \in \mathbb{C}$) converge con límite $a \in \mathbb{C}$ si $\lim_{n\to\infty}\prod_{i=1}^{n}(1+a_i) = a \neq 0$. El producto es llamado absolutamente convergente si $\sum_{i=1}^{\infty}|a_i| < \infty$. Del análisis sabemos que la convergencia absoluta implica la convergencia del producto y que además el límite de un producto absolutamente convergente es independiente del orden los factores. Más aún, si el producto $\prod_{i=1}^{\infty}(1+a_i) = a$ convergente absolutamente entonces $\prod_{i=1}^{\infty}(1+a_i)^{-1}$ converge absolutamente y $\prod_{i=1}^{\infty}(1+a_i)^{-1} = a^{-1}$.

Proposición 4.1.9 (Producto de Euler). *Para $|t| < q^{-1}$ la función zeta puede ser representada como un producto infinito absolutamente convergente.*

$$Z(t) = \prod_{P\in\mathbb{P}_F}(1-t^{deg\,P})^{-1}. \tag{4.1}$$

en particular $Z(t) \neq 0$ para $|t| < q^{-1}$.

Demostración. El lado derecho de (4.1) converge absolutamente para $|t| < q^{-1}$, pues $\sum_{P\in\mathbb{P}_F}|t|^{deg\,P} \leq \sum_{n=0}^{\infty}A_n|t|^n < \infty$ por la proposición 4.1.7. Por otra parte, cada factor de (4.1) puede ser escrito como una serie geométrica y obtenemos

$$\prod_{P\in\mathbb{P}_F}(1-t^{deg\,P})^{-1} = \prod_{P\in\mathbb{P}_F}\sum_{n=0}^{\infty}|t|^{deg\,(nP)}$$
$$= \sum_{A\in\mathcal{D}_F, A\geq 0}t^{deg\,A} = \sum_{n=0}^{\infty}A_nt^n = Z(t)$$

□

Para los siguientes resultados vamos a denotar por $\bar{\mathbb{F}}_q$ la cerradura algebraica de $\mathbb{F}_q$ y vamos a considerar la extensión constante $\bar{F} = F\bar{\mathbb{F}}_q$ de $F/\mathbb{F}_q$. Para cualquier $r \geq 1$ existe exactamente una extensión de grado r a decir $\mathbb{F}_{q^r}/\mathbb{F}_q$ con $\mathbb{F}_{q^r} \subseteq \bar{\mathbb{F}}_q$, y definimos

$$F_r := F\mathbb{F}_{q^r} \subseteq \bar{F}.$$

Lema 4.1.10.

1. *F_r/F es una extensión cíclica de grado r (es una extensión de Galois, con grupo de Galois cíclico y de orden r. El grupo de Galois $Gal(F_r/F)$ es generado por el automorfismo de Frobenius σ el cual actúa en $\mathbb{F}_{q^r}$ por $\sigma(\alpha) = \alpha^q$.*

2. *$\mathbb{F}_{q^r}$ es el campo pleno de constantes de F_r.*

3. *$F_r/\mathbb{F}_{q^r}$ tiene el mismo género que $F/\mathbb{F}_q$.*

4. *Sea $P \in \mathbb{P}_F$ un lugar de grado n. Entonces $Con_{F_r/R}(P) = P_1 + \cdots + P_d$, con $d := mcd(n, r)$ distintos lugares $P_i \in \mathbb{P}_{F_r}$ y el grado $deg\, P_i = n/d$.*

Demostración. (1) Es conocido de la teoría de Galois que $\mathbb{F}_{q^r}/\mathbb{F}_q$ es cíclica y de orden r y su grupo de Galois está generado por el endomorfismo de Frobenius $\alpha \mapsto \alpha^q$; ver, por ejemplo [Mor]. Como $[\mathbb{F}_{q^r} : \mathbb{F}_q] = [F_r : F]$ por el lema 3.6.1, la afirmación (1) se sigue inmediatamente.

(2) y (3) Son inmediatas de la proposición 3.6.2 y el teorema 3.6.3.

(4) P es no ramificado en F_r/F por el teorema 3.6.3. Consideremos algún lugar $P' \in \mathbb{P}_{F_r}$ que yazca sobre P. El campo de clases residuales de P' es el campo compuesto $\mathbb{F}_{q^r}$ con el campo F_P por el teorema 3.6.3. Denotemos por $u := mcm(n, r)$. Dado que $F_P = \mathbb{F}_{q^n}$ esta composición es $\mathbb{F}_{q^n}\mathbb{F}_{q^r} = \mathbb{F}_{q^u}$. Por lo tanto $deg\, P' = [\mathbb{F}_{q^u} : \mathbb{F}_{q^r}] = n/d$. □

Para el siguiente resultado, necesitamos de una igualdad polinomial: si $m \geq 1$ y $r \geq 1$ son enteros, sea $d = mcd(m, r)$ entonces

$$(X^{r/d} - 1)^d = \prod_{\xi^r = 1} (X - \xi^m), \tag{4.2}$$

donde ξ corre sobre todas las raíces r-ésimas de la unidad en $\mathbb{C}$. Ambos son polinomios mónicos del mismo grado y cada raíz (r/d)-ésima de la unidad es una raíz de ellos, con multiplicidad d. Por lo tanto los polinomios son iguales. Sustituimos ahora $X = t^{-m}$ en (4.2), multiplicamos por t^{mr} y obtenemos

$$(1 - t^{mr/d})^d = \prod_{\xi^r = 1} (1 - (\xi t)^m \tag{4.3}$$

Proposición 4.1.11. *Sea $Z(t)$ (respec. $Z_r(t)$) la función zeta de F (respec. de $F_r = F\mathbb{F}_{q^r}$). Entonces:*

$$Z_r(t^r) = \prod_{\xi^r=1} Z(\xi t) \tag{4.4}$$

para toda $t \in \mathbb{C}$ y ξ corre sobre todas las raíces r-ésimas de la unidad.

Demostración. Es suficiente demostrarlo para $|t| < q^{-1}$. En esta región la representación del producto de Euler nos da

$$Z_r(t^r) = \prod_{P \in \mathbb{P}_F} \prod_{P'|P} (1 - t^{r deg\, P'})^{-1} \tag{4.5}$$

Para un lugar fijo $P \in \mathbb{P}_F$ sea $m := deg\, P$ y $d := mcd(r, m)$, entonces

$$\prod_{P'|P} (1 - t^{r deg\, P'}) = (1 - t^{rm/d})^d = \prod_{\xi^r=1} (1 - (\xi t)^m) = \prod_{\xi^r=1} (1 - (\xi t)^{deg\, P})$$

Por el lema anterior y (4.5) tenemos

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

□

Corolario 4.1.12 (K. Schmidt). $\partial = 1$.

Demostración. Para $\xi^\partial = 1$ tenemos lo siguiente

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

puesto que ∂ divide el grado de P para todo $P \in \mathbb{P}_F$. Por lo tanto $Z_\partial(t^\partial) = Z(t)^\partial$ por la proposición anterior tiene un polo simple en $t = 1$ por el corolario 1.7 y entonces la función $Z(t^\partial)$ tiene un polo de orden ∂ en $t = 1$. Por lo tanto $\partial = 1$. □

Corolario 4.1.13.

1. *Cualquier campo de funciones $F/\mathbb{F}_q$ de género $g = 0$ es racional y su función $Z(t)$ es*

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

2. *Si $F/\mathbb{F}_q$ tiene género $g \geq 1$ su función zeta puede escribirse como $Z(t) = F(t) + G(t)$, donde*

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

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

Demostración. Cualquier campo de funciones de género cero con un divisor de grado 1 es racional. Las demás afirmaciones se siguen de la proposición 4.1.7 y del hecho $\partial = 1$. □

Proposición 4.1.14. *La función zeta de $F/\mathbb{F}_q$ satisface la siguiente ecuación funcional*

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

Demostración. Para $g = 0$ esto es claro por el corolario 4.1.13. Supongamos entonces que $g \geq 1$. Escribamos $Z(t) = F(t) + G(t)$ como en el corolario 4.1.13. Tomemos W un divisor canónico de F, entonces

$$\begin{aligned}
(q-1)F(t) &= \sum_{0 \leq deg\,[C] \leq 2g-2} q^{dim\,[C]} t^{deg\,[C]} \\
&= \sum_{0 \leq deg\,[C] \leq 2g-2} q^{deg\,[C]+1-g+dim\,[W-C]} t^{deg\,[C]} \\
&= q^{g-1} t^{2g-2} \sum_{0 \leq deg\,[C] \leq 2g-2} q^{deg\,[C]-(2g-2)+dim\,[W-C]} t^{deg\,[C]-(2g-2)} \qquad (4.6) \\
&= q^{g-1} t^{2g-2} \sum_{0 \leq deg\,[C] \leq 2g-2} q^{dim\,[W-C]} \left(\frac{1}{qt}\right)^{deg[W-C]} \\
&= q^{g-1} t^{2g-2} (q-1) F\left(\frac{1}{qt}\right)
\end{aligned}$$

Para esta parte usamos el hecho de que $deg\,[W] = 2g-2$. Si $[C]$ corre por todas las clases divisoras con $0 \leq deg\,[C] \leq 2g-2$ también lo hace $[W-C]$ pero en orden contrario. Para la función $G(t)$ hacemos un cálculo similar y obtenemos

$$\begin{aligned}
& q^{g-1} t^{2g-2} G\left(\frac{1}{qt}\right) \\
&= \frac{h}{q-1} q^{g-1} t^{2g-2} \left(q^g \left(\frac{1}{qt}\right)^{2g-1} \frac{1}{1-q\frac{1}{qt}} - \frac{1}{1-\frac{1}{qt}} \right) \qquad (4.7)
\end{aligned}$$

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

Si sumamos (4.6) y (4.7), obtenemos la ecuación funcional para $Z(t)$. □

Definición 4.1.15. El polinomio $L(t) := L_F(t) := (1-t)(1-qt)Z(t)$ es llamado el *L-polinomio* de $F/\mathbb{F}_q$.

Por el corolario 1.12 tenemos que $L(t)$ es un polinomio de grado $\leq 2g$ y notemos también que $L(t)$ contiene toda la información de los números A_n, $n \geq 0$ pues

$$L(t) = (1-t)(1-qt)\sum_{n=0}^{\infty} A_n t^n \tag{4.8}$$

Teorema 4.1.16.

1. $L(t) \in \mathbb{Z}[t]$ *y* $\deg L(t) = 2g$.
2. $L(t) = q^g t^{2g} L(1/qt)$ *(ecuación funcional).*
3. $L(1) = h$, *el número de clases de* $F/\mathbb{F}_q$.
4. *Si escribimos a* $L(t) = a_0 + a_1 t + \cdots + a_{2g}t^{2g}$, *entonces se cumple lo siguiente*
   (a) $a_0 = 1$ *y* $a_{2g} = q^g$.
   (b) $a_{2g-i} = q^{g-i}a_i$ *para* $0 \leq i \leq g$.
   (c) $a_1 = N - (q+1)$ *donde* N *es el número de lugares* P *de* $\mathbb{P}_F$ *de grado* 1.
5. $L(t)$ *se factoriza en* $\mathbb{C}[t]$ *de esta manera*

$$L(t) = \prod_{i=1}^{2g}(1-\alpha_i t) \tag{4.9}$$

Los números complejos $\alpha_i, \ldots, \alpha_{2g}$ *son enteros algebraicos y pueden ser ordenados de forma tal que* $\alpha_i \alpha_{g+i} = q$ *para* $i = 1, \ldots, 2$.

6. *Si* $L_r(t) = (1-t)(1-q^r t)Z_r(t)$ *denota el polinomio de la extensión* $F_r = F\mathbb{F}_{q^r}$, *entonces*

$$L_r(t) = \prod_{i=1}^{2g}(1-\alpha_i^r t) \text{ con } \alpha_i \text{ dadas por } (4.9).$$

Demostración. Todas estas afirmaciones son triviales para el caso $g = 0$.

(1) Ya se señaló que $L(t)$ es un polinomio de grado $\leq 2g$ en (4) mostraremos que su término principal es q^g y por lo tanto $deg\ L(t) = 2g$. Ahora $L(t) \in \mathbb{Z}[t]$ por (4.9) comparando todos los coeficientes. (2) Es la ecuación funcional de la función zeta, pues

$$L(t) = (1-t)(1-qt)Z(t) = (1-t)(1-qt)q^{g-1}t^{2g-2}Z(\frac{1}{qt}) \text{ y}$$

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

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

(3) Por el corolario 1.12, tenemos

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

Por lo tanto, $L(1) = h$.

(4) Escribimos a $L(t) = a_0 + a_1 t + \cdots + a_{2g}t^{2g}$. La ecuación funcional nos implica

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

y entonces $a_{2g-i} = q^{g-i}a_i$, para $i = 0, \ldots, g$ y por lo tanto también (2) está demostrado. Comparando los coeficientes de t^0 y de t^1 en 1.12 tenemos que $A_0 = a_0$ y $a_1 = A_1 - (q+1)A_0$. Como $A_0 = 1$ y $A_1 = N$ tenemos que $a_0 = 1$ y $a_1 = N - (q+1)$. Finalmente tenemos $a_{2g} = q^g a_0 = q^g$ por (2).

(5) Consideremos el polinomio recíproco

$$L^{\perp} := t^{2g}L(\frac{1}{t}) = a_0 t^{2g} + a_1 t^{2g-1} + \cdots + a_{2g} = t^{2g} + a_1 t^{2g-1} + \cdots + q^g \quad (4.10)$$

El polinomio $L^{\perp}(t)$ es mónico y posee sus coeficientes en $\mathbb{Z}$, así que sus raíces $\alpha_1, \ldots, \alpha_{2g} \in \mathbb{C}$ son enteros algebraicos y podemos escribir entonces

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

Entonces es claro que

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

Notemos que las raíces de $L^{\perp}(t)$ son los inversos de las raíces de $L(t)$. La ecuación funcional implica $L^{\perp}(\alpha) = 0 \iff L^{\perp}(q/\alpha)$ pues

$$L(1/t) = q^g t^{-2g} L(\frac{t}{q}) \text{ y } L^{\perp}(t) = t^{2g} L(\frac{1}{q}) = q^g L(t/q)$$

entonces $L^{\perp}(\frac{q}{t}) = (\frac{q}{t})^{2g} L(\frac{t}{g})$ y dado que $\alpha \neq 0$ tenemos esa afirmación. Podemos además acomodar las raíces de $L^{\perp}(t)$ como

$$\alpha_1, q/\alpha_1, \ldots, \alpha_k, q/\alpha_k, q^{1/2}, \ldots, q^{1/2}, -q^{1/2}, \ldots, -q^{1/2},$$

donde $q^{1/2}$ aparece m veces y $-q^{1/2}$ aparece n veces y por las fórmulas de Vieta tenemos

$$\alpha_1 \frac{q}{\alpha_1} \cdots \alpha_k \frac{q}{\alpha_k} (q^{1/2})^n (-q^{1/2})^m$$

por lo tanto n es par y como $m + n + 2k = 2g$ (por la potencia del polinomio) entonces m es también par y podemos entonces reacomodar las $\alpha_1, \ldots, \alpha_g$ de tal manera que $\alpha_i \alpha_{g+i} = q$ para $i = 1, \ldots, g$.

(6) Por la prop 4.1.11 obtenemos de la definición $L_r(t) = (1-t)(1-q^r t) Z_r(t)$ y entonces

$$L_r(t^r) = (1 - t^r)(1 - q^r t^r) Z_r(t^r) = (1 - t^r)(1 - q^r t^r) \prod_{\xi^r = 1} Z(\xi t)$$

$$(1 - t^r)(1 - q^r t^r) \prod_{\xi^r = 1} \frac{L(\xi t)}{(1 - \xi t)(1 - g\xi t)} = \prod_{\xi^r = 1} L(\xi t)$$

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

Por lo tanto $L_r(t) = \prod_{i=1}^{2g} (1 - \alpha_i^r t)$. □

El teorema anterior muestra que el número

$$N(F) = N = \quad | \{ P \in \mathbb{P}_F \mid deg\, P = 1 \} | \tag{4.11}$$

puede ser calculado de manera fácil si se conoce el polinomio $L(t)$ de $F/\mathbb{F}_q$. En el caso más general podemos considerar

$$N_r(F) = N_r = \quad | \{ P \in \mathbb{P}_F \mid deg\, P = r \} |$$

donde $F_r = F\mathbb{F}_{q^r}$ es la extensión constante de $F/\mathbb{F}_q$ de grado r.

Corolario 4.1.17. *Para cualquier $r \geq 1$*

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

donde $\alpha_1, \ldots, \alpha_{2g} \in \mathbb{C}$ son los recíprocos de las raíces de $L(t)$. En particular para

$$N(F) = N_1 = q + 1 - \sum_{i=1}^{2g} \alpha_i$$

Demostración. Por el teorema anterior (4) tenemos que $N_r - (q^r + 1)$ es el coeficiente de t en el L-polinomio $L_r(t)$. Por otro lado, dado que $L_r(t) = \prod_{i=1}^{2g}(1 - \alpha_i^r t)$ este mismo coeficiente es justamente $-\sum_{i=1}^{2g} \alpha_i^r$. □

Corolario 4.1.18. *Sea $L(t) = \sum_{i=0}^{2g} a_i t^i$ el L-polinomio de $F/\mathbb{F}_q$ y sea $S_r := N_r - (q^r + 1)$, entonces tenemos*

1. $L'(t)/L(t) = \sum_{r=1}^{\infty} S_r t^{r-1}$
2. $a_0 = 1$ *y*

$$i a_i = S_i a_0 + S_{i-1} a_1 + \cdots + S_1 a_{i-1} \tag{4.12}$$

para $i = 1, \ldots, g$.

Por lo tanto, dados $N_1, \ldots, N_g$ podemos determinar a $L(t)$ por (4.12) y las ecuaciones $a_{2g-i} = q^{g-i} a_i$ para $i = 0, \ldots, g$.

Demostración. Escribamos $L(t) = \prod_{i=1}^{2g}(1 - \alpha_i t)$ y tenemos entonces

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

$$= \sum_{r=1}^{\infty} (\sum_{i=1}^{2g} -\alpha_i^r) t^{r-1} = \sum_{r=1}^{\infty} S_r t^{r-1}$$

por el corolario anterior y la definición de S_r. (2) Sabemos que $a_0 = 1$ y por (1) tenemos que

$$a_1 + 2a_2 t + \cdots + 2g a_{2g} t^{2g-1} = (a_0 + a_1 t + \cdots + a_{2g} t^{2g}) \sum_{r=1}^{\infty} S_r t^{r-1}$$

comparando los coeficientes de los términos $t^0, t^1, \ldots, t^{g-1}$, tenemos este resultado. □

4.2 La cota de Hasse-Weil

Con toda la notación del teorema anterior, sea $F/\mathbb{F}_q$ un campo de funciones de género g, $Z_F(t) = L_F(t)/(1-t)(1-qt)$ su función zeta, $\alpha_1, \ldots, \alpha_{2g}$ las raíces recíprocas de $L_F(t)$, $N(F) = |\{P \in \mathbb{P}_F \mid deg\, P = 1\}|$; $F_r = F\mathbb{F}_{q^r}$ es la extensión constante de grado r y $N_r = N(F_r)$.

Teorema 4.2.1 (Teorema de Hasse-Weil). *Los recíprocos de las raíces de $L_F(t)$ satisfacen*

$$|\alpha_i| = q^{1/2}$$

para $i = 1, \ldots, 2g$.

Antes de probar el teorema, daremos una consecuencia importante.

Teorema 4.2.2 (Cota de Hasse-Weil). *El número N de lugares de $F/\mathbb{F}_q$ de grado 1, puede ser estimado por*

$$|N - (q+1)| \leq 2gq^{1/2} \tag{4.13}$$

Demostración. El corolario 4.1.17 nos da $N - (q+1) = -\sum_{i=1}^{2g} \alpha_i$ y por el teorema de Hasse-Weil este resultado es inmediato. □

A continuación enunciaremos algunos resultados que son necesarios para probar el teorema de Hasse-Weil. Esta demostración del teorema de Hasse-Weil es debida a Bomberi.

Lema 4.2.3. *Sea $m \geq 1$. Entonces el teorema de Hasse-Weil se cumple para $F/\mathbb{F}_q \iff$ se cumple para la extensión constante $F_m/\mathbb{F}_{q^m}$.*

Demostración. Los recíprocos de las raíces de $L_F(t)$ son $\alpha_1, \ldots, \alpha_{2g}$, por el teorema 4.1.16, los recíprocos de las raíces de $L_m(t)$ son $\alpha_1^m, \ldots, \alpha_{2g}^m$. Entonces este lema se sigue inmediatamente porque $|\alpha_i| = q^{1/2} \iff |\alpha_i^m| = (q^m)^{1/2}$. □

Lema 4.2.4. *Supongamos que existe $c \in \mathbb{R}$ tal que para todo $r \geq 1$ se tiene*

$$|N_r - (q^r + 1)| \leq cq^{r/2} \tag{4.14}$$

Entonces el teorema de Hasse-Weil se cumple para $F/\mathbb{F}_q$.

Demostración. El corolario 4.1.17, establece que $N_r - (q^r + 1) = -\sum_{i=1}^{2g} \alpha_i^r$ entonces por (4.14) tenemos

$$|\sum_{i=1}^{2g}| \leq cq^{1/2} \tag{4.15}$$

para $r \geq 1$. Consideremos la función meromorfa

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

Sea $\rho = \min\{|\alpha_i^{-1}| \mid 1 \leq i \leq 2g\}$. El radio de convergencia de $H(t)$ alrededor de cero es precisamente ρ pues $\alpha_1^{-1}, \ldots, \alpha_{2g}^{-1}$ son las únicas singularidades de $H(t)$. Por otra parte, para $|t| < r$ tenemos

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

Por (4.15) esta serie converge para $|t| < q^{-1/2}$, i.e. $|tq^{1/2}| < 1$, entonces $q^{-1/2} \leq \rho$. Esto implica que $q^{1/2} \geq |\alpha_i|$ para $i = 1, \ldots, 2g$. Como $\prod_{i=1}^{2g} \alpha_i = q^g$ tenemos que $|\alpha_i| = q^{1/2}$. Notemos que las desigualdades (4.14) son equivalentes a la existencia de constantes $c_1 > 0$ y $c_2 > 0$ tales que

$$N_r \leq q^r + 1 + c_1 q^{r/2} \tag{4.16}$$

$$N_r \geq q^r + 1 - c_2 q^{r/2} \tag{4.17}$$

para $r \geq 1$ por el lema 4.2.3 el teorema de Hasse-Weil se cumple para alguna extensión constante de F. Por lo tanto se suficiente probar que las desigualdades anteriores se cumplen bajo ciertas hipótesis adicionales que pueden hacerse en una extensión algebraica apropiada. □

Proposición 4.2.5. *Supongamos que $F/\mathbb{F}_q$ satisface la siguiente hipótesis*

$$q \text{ es cuadrado y } q > (g+1)^4$$

entonces el número $N = N(F)$ de lugares de $F/\mathbb{F}_q$ de grado uno puede ser estimado por

$$N < (q+1) + (2g+1)q^{1/2}$$

Demostración. Supongamos que existe un lugar $Q \in \mathbb{P}_F$ grado uno (de otra forma $N = 0$ lo cumple). Definamos $q_0 = q^{1/2}$ y $m = q_0 - 1$ y $n = 2g + q_0$. Entonces es inmediato que $r := q - 1 + (2g+1)q^{1/2} = m + nq_0$. □

Proposición 4.2.6. *Supongamos que $F/\mathbb{F}_q$ satisface las siguienes condiciones*

(1) q es un cuadrado y (2) $q > (g+1)^4$.

Entonces el número de lugares $N = N(F)$ de $F/\mathbb{F}_q$ de grado uno puede ser estimado por

$$N < (q+1) + (2g+1)q^{1/2}$$

Demostración. Supongamos que existe un lugar $Q \in \mathbb{P}_F$ de grado uno (de otra forma $N = 0$ y el enunciado se cumple trivialmente). Definimos ahora $q_0 = q^{1/2}$, $m = q_0 - 1$ y $n = 2g + q_0$. Entonces es inmediato que $r := q - 1 + (2g + 1)q^{1/2} = m + nq_0$. Definamos ahora $T := \{i \mid 0 \leq i \leq m \text{ e } i \text{ es un número polo de } Q\}$. Para cada $i \in I$ escojamos un elemento $u_i \in F$, cuyo polo divisor sea iQ. Entonces el conjunto $\{u_i \mid i \in T\}$ es una base de $\mathcal{L}(mQ)$. Consideremos el espacio vectorial $\mathcal{L} := \mathcal{L}(mQ)\mathcal{L}(nQ)^q \subseteq \mathcal{L}(rQ)$ (por definición $\mathcal{L}$ consiste de todas las sumas finitas $\sum x_j y_j^q$ con $x_j \in \mathcal{L}(mQ)$ y $y_i \in \mathcal{L}(nQ)$), desde luego $\mathcal{L}$ es un $\mathbb{F}_q$-espacio vectorial y $\mathcal{L} \subseteq \mathcal{L}(rQ)$. Deseamos construir $x \in L^*$ $(x \neq 0)$ tal que $x(P) = 0$ para todo $P \in \mathbb{P}_F$ con $deg\, P = 1$ y $P \neq Q$. Supongamos que encontramos a tal elemento x. Entonces todos los lugares de grado uno, excepto Q son ceros de x y el divisor cero $(x)_0$ tiene grado $deg\,(x)_0 \geq N - 1$ y como $x \in \mathcal{L} \subseteq \mathcal{L}(rQ)$, $deg\,(x)_0 = deg\,(x)_\infty \leq r = q + (2g + 1)q^{1/2}$ si combinamos estas dos desigualdades, obtenemos $N \leq q + (2g + 1)q^{1/2}$. Ahora vamos a probar algunas afirmaciones para asegurar la existencia del elemento x.

Afirmación (1). Todo $y \in \mathcal{L}$ puede ser escrito de manera única de la forma

$$y = \sum_{i \in T} u_i z_i^{q_0} \tag{4.18}$$

con $x_i \in \mathcal{L}(nQ)$ no todas las $x_i = 0$.

Para cualquier índice con $x_i \neq 0$ tenemos

$$v_Q(u_i x_i^q) \equiv v_Q(u_i) \equiv -1 \pmod{q_0}$$

Ahora, como $m = q_0 - 1$, los números $i \in T$ son distintos módulo q_0. Entonces la desigualdad estricta del triángulo nos da

$$v_Q\left(\sum_{i \in T} u_i x_i^{q_0}\right) = \min\{v_Q(u_i x_i^q) \mid i \in T\} \neq \infty.$$

Esta contradicción demuestra la afirmación 1. □

Consideremos ahora la función $\lambda : \mathcal{L} \to \mathcal{L}((q_0 m + n)Q)$ dado por

$$\lambda\left(\sum_{i \in T} u_i z_i^{q_0}\right) = \sum_{i \in T} u_i^{q_0} z_i$$

con $z_i \in \mathcal{L}(nQ)$ por la afirmación 1, esta aplicación está bien definida; λ no es $\mathbb{F}_q$−lineal, pero es un homomorfismo del grupo aditivo de $\mathcal{L}$ en $\mathcal{L}((q_0 m + n)Q)$.

Afirmación (2). El núcleo de λ no es cero. Como λ es un homomorfismo de $\mathcal{L}$ en $\mathcal{L}((q_0 m + n)Q)$ es suficiente demostrar que $dim\, \mathcal{L} > dim\, \mathcal{L}((q_0 m + n)Q)$, donde dim denota la dimensión como $\mathbb{F}_q$-espacios vectoriales.

Por la afirmación 1 y el teorema de Riemann-Roch, tenemos que

$$dim\, L = dim(mQ)\, dim(nQ) > (m+1-g)(n+1-g)$$

por otro lado, como $q_0 m + n = q_0(q_0-1) + (2g+q)$ por el teorema de Riemann-Roch se sigue que $dim\, \mathcal{L}((q_0 m+n)Q) = (2g+q)+1-g = g+q+1$. De esta manera, podemos concluir la afirmación 2 si probamos que

$$(m+1-g)(n+1-g) > g+q+1$$

Con este fin, consideremos las siguientes equivalencias

$$\begin{aligned} &(m+1-g)(n+1-g) > g+q+1 \\ \iff &(q_0-g)(2g+q_0+1-g) > g+q+1 \\ \iff &q-g^2+q_0-g > g+q+1 \\ \iff &q_0 > g^2+2g+1 = (g+1)^2 \\ \iff &q > (g+1)^4 \end{aligned}$$

y dado que supusimos que $q > (g+1)^4$, tenemos la afirmación 2.

Afirmación (3). Sea $0 \neq x \in \mathcal{L}$ un elemento del núcleo de λ y $P \neq Q$ un lugar de grado uno.

Notemos que para todo $y \in \mathcal{L}$ se tiene $y(P) \neq \infty$ porque Q es el único polo de y. Más aún como $\mathbb{F}_q$ es el campo de clases residuales de P, tenemos que $y(P)^q = y(P)$ (por el teorema de Lagrange). Sea ahora $x \in \mathcal{L}$ con $\lambda(x) = 0$. Escribamos a $x = \sum_{i \in T} u_i z_i^{q_0}$ y obtenemos

$$x(P)^{q_0} = \left(\sum u_i(P) z_i(P)^{q_0}\right)^{q_0}$$

$$= \sum_{i \in T} u_i^{q_0}(P) z_i(P)^q = \left(\sum u_i^{q_0} z_i\right)(P) = \lambda(x)(P) = 0$$

Con esto demostramos la afirmación 3 y la proposición 4.2.6 está completa.

La proposición anterior nos proporcionó una cota superior para los números N_r (en una extensión de campos apropiada). Con el propósito de obtener una cota inferior, necesitamos un lema de la teoría de grupos.

Lema 4.2.7. *Sea G un grupo que es el producto directo*

$$G = \langle \sigma \rangle \times G' \tag{4.19}$$

de un grupo cíclico $\langle \sigma \rangle$ y un subgrupo $G' \subseteq G$ tal que $ord\, G' = m$, $ord(\sigma) = n$ y $m \mid n$. Supongamos que H es un subgrupo $H \subseteq G$ tal que $ord\, H = nc$ y $ord\,(H \cap G') = e$. Entonces existen c subgrupos $U \subseteq H$ con las siguientes propiedades

$$U \text{ es cíclico de orden } n \text{ y } U \cap G' = \{1\} \tag{4.20}$$

Demostración. Sea $\tau \in G'$ y consideremos el sugrupo cíclico que está generado por $\langle \sigma\tau \rangle \subseteq G$. Como $\sigma\tau = \tau\sigma$ puesto que G es un producto directo, tenemos además que $(\tau, 1)(1, \sigma) = (\tau, \sigma)$, $ord(\sigma) = n$ y $ord(\tau) \mid m$, de manera que $ord(\sigma\tau) = n$. Más aún, $\langle \sigma\tau \rangle \cap G = \{1\}$ y además $\langle \sigma\tau \rangle \neq \langle \sigma\tau' \rangle$ para $\tau' \neq \tau$ (todo esto se sigue inmediatamente del hecho de que G es un producto directo) porque los elementos $\lambda \in G$ tienen una representación única de la forma $\lambda = \sigma^i\rho$ con $0 \leq i < n$ y $\rho \in G'$. Hemos encontrado entonces $m = ord\, G'$ subgrupos distintos $U \subseteq G$ con las propiedades (4.20).

De la definición de producto directo, tenemos que $G' \lhd G$ y entonces $H/H \cap G' \cong HG'/G'$. Por otra parte, (4.20) implica que $HG' = G$ y entonces $H/H \cap G' \cong G/G'$ es cíclico de orden n. Sea ahora $\lambda_0 \in H$ cuyo orden módulo $H \cap G'$ sea n y escribamos $\lambda_0 = \sigma^a\tau'$ con $\tau' \in G'$ y $a \in \mathbb{Z}$. El exponente a es primo relativo con n (de lo contrario habría un entero $1 \leq d \leq n$ con $\sigma^{ad} = 1$ y entonces $\lambda_0^d = \tau'^d \in H \cap G'$, lo cual es una contradicción pues el orden de λ_0 módulo $H \cap G'$ sería menor que n). Por lo tanto una potencia adecuada $\lambda = \lambda_0^t$ tiene una representación de la forma $\lambda = \sigma\tau_0$ con $\tau_0 \in G'$.

Sea ahora $H \cap G' = \{\psi_1, \ldots, \psi_e\}$ y definamos

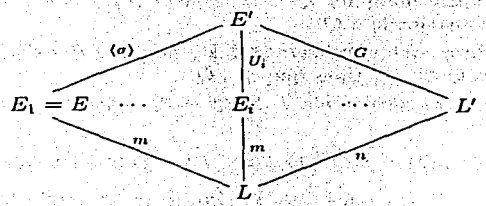
$$U^{(j)} := \langle \sigma\tau_0\psi_j \rangle$$

para $j = 1, \ldots, e$. Los subgrupos $U^{(j)} \subseteq H$ con cíclicos de orden n, distintos y además $U^{(j)} \cap G' = \{1\}$. Nos falta demostrar que H no contiene otros subgrupos cíclicos U de orden n con $U \cap G' = \{1\}$. Sea ahora U un subgrupo que satisface (4.20). De la misma forma encontramos un generador de la forma específica $\sigma\tau_1$ con $\tau_1 \in G'$. Como $\sigma\tau_1 \in H$ y $\sigma\tau_0 \in H$, tenemos

$$\tau_0\tau_1\tau_0^{-1} = (\tau\tau_0)^{-1}(\sigma\tau_1) \in H \cap G' = \{\psi_1, \ldots, \psi_e\}$$

Entonces $\tau_1 = \tau_0\psi_j$ para algún j y $U = \langle \sigma\tau_1 \rangle = \langle \sigma\tau_0\psi_j \rangle = U^{(j)}$. □

Consideremos la siguiente situación: sea E/L una extensión de Galois de campos de funciones de grado $[E : L] = m$ y supongamos que $\mathbb{F}_q$ es el campo de constantes de E y de L. Escojamos $n > 0$ con $m \mid n$ y sea $E' := E\mathbb{F}_{q^n}$ (resp. $L' = L\mathbb{F}_{q^n} \subseteq E'$) la correspondiente extensión constante de grado n. Entonces E'/L es de Galois con grupo de Galois $G' = \langle \sigma \rangle \times G$ donde G es el grupo de Galois $G := Gal(E'/L') \cong Gal(E/L)$ y σ es el automorfismo de Frobenius de E'/E. Por el lema anterior G' contiene exactamente m subgrupos cíclicos $U \subseteq G'$ con $ord\, U = n$ y $U \cap G = \{1\}$ con digamos $U_1, \ldots, U_m$. Podemos suponer que $U_1 = \langle \sigma \rangle$. Definamos como E_i el campo fijo de U_i $(i = 1, \ldots, m)$. Entonces $E_1 = E$ y tenemos el siguiente diagrama



Denotemos ahora por $g(E_i)$, el género de E_i y por $N(E_i)$ (respec. $N(L)$) el número de lugares de grado uno de E_i (resp de L).

Proposición 4.2.8. *Bajo las hipótesis anteriores se tiene*

1. $\mathbb{F}_q$ *es todo el campo de constantes de* E_i *para* $1 \leq i \leq m$.
2. $E' = E_i\mathbb{F}_{q^n}$ *y* $g(E_i) = g(E)$ *para* $i = 1, \ldots, m$.
3. $mN(L) = \sum_{i=1}^{m} N(E_i)$.

Demostración. (1), (2) Notemos primero que $U_i \cap G = \{1\}$. Entonces de la teoría de Galois sabemos que E' es el campo compuesto de E_i y L', por lo tanto $E' = E_iL' = E_iL\mathbb{F}_{q^n} = E_i\mathbb{F}_{q^n}$ es la extensión constante de E_i con $\mathbb{F}_{q^n}$. Como $[E' : E_i] = ord\, U_i = n$ de modo que $\mathbb{F}_q$ es el campo de constantes de E_i. El género es invariante bajo extensiones constantes como ya lo vimos, por lo tanto $g(E_i) = g(E') = g(E)$ para $i = 1, \ldots, m$.

(3) Consideremos ahora los conjuntos $X = \{P \in \mathbb{P}_L \mid deg\, P = 1\}$ y para $i = 1, \ldots, m$, $X_i = \{Q \in \mathbb{P}_E, \deg Q = 1\}$, de manera que debemos demostrar la siguiente afirmación

$$\left|\bigcup_{i=1}^{m} X_i\right| = m|X_i| \tag{4.21}$$

Sea ahora $P \in X$. Escojamos una extensión $P' \in \mathbb{P}_{E'}$ y sea $P_1 := P' \cap E$. El grado relativo $f(P_1 \mid P)$ divide a m, dado que E/L es de Galois. Por lo tanto $f(P_1 \mid P)$ divide también a n y el campo de clases residuales de P' es $\mathbb{F}_{q^n}$ por el teorema 3.6.3. Esto quiere decir que el grado relativo de $P' \mid P$ es $f(P' \mid P) = n$. Sea $e = e(P' \mid P)$ el índice de ramificación de P en E'/L y r el número de lugares en $\mathbb{P}_{E'}$ que yacen sobre P (como E'/L es de Galois, e depende solamente de P) y tenemos entonces

$$mn = [E' : L] = e(P' \mid P)f(P' \mid P)r = enr$$

por lo tanto $m = er$ y (4.21) se reduce a las siguientes afirmaciones.

Afirmación (1). Para cualquier $Q \in X_i$ con $Q \mid P$, existe exactamente un lugar $Q' \in \mathbb{P}_{E'}$ que extiende a Q.

Afirmación (2). Para cualquier lugar $Q' \in \mathbb{P}_{E'}$ con $Q' \mid P$, existen exactamente e distintos lugares $Q \in \cup_{i=1}^{m}$ tales que $Q' \mid Q$.

Demostración de la afirmación 1. Si $Q' \in \mathbb{P}_{E'}$ yace sobre el lugar $Q \in X_i$ y $Q \mid P$, entonces

$$f(Q' \mid Q) = f(Q' \mid Q)f(Q \mid P) = f(Q' \mid P) = n$$

Notemos que $f(Q \mid P) = 1$ pues $Q \in X_i$. Por lo tanto $f(Q' \mid Q) = [E' : E_i]$ lo cual implica que Q' es la única extensión de Q en $E' \mid E_i$.

Demostración de la afirmación 2. Sea ahora $Q \in \mathbb{P}_{E'}$ tal que $Q' \mid P$. Sea $H \subseteq Gal(E'/L)$ el grupo de descomposición de Q' sobre P $Z \subseteq E'$ el campo fijo por H y $P_Z := Q' \cap Z$. Entonces

$$ord\, H = e(Q' \mid P)f(Q' \mid P) = en$$

y $f(P_Z \mid P) = 1$, por el teorema 3.7.7. En particular se sigue que $\mathbb{F}_q$ es el todo el campo de constantes de Z. Por la teoría de Galois, el campo fijo de $H \cap G$ es el compuesto de Z y L'. Tenemos ahora $ZL' = ZL\mathbb{F}_{q^n}$ y $[Z\mathbb{F}_{q^n} : Z] = n$ puesto que $\mathbb{F}_q$ es todo el campo de constantes de Z. De esta manera

$$ord(H \cap G) = [E' : Z]/[ZL' : Z] = ne/n = e$$

Dado que P_Z es no ramificado en $ZL' = Z\mathbb{F}_{q^n}$, se sigue también que $T := ZL'$ es el campo de inercia y $H \cap G$ es el grupo de inercia de $Q' \mid P$. Aplicamos ahora el lema 4.2.7 y tenemos exactamente e de los grupos cíclicos $U_{i_1}, \ldots, U_{i_e}$. Sea $Q_{ij} = Q' \cap E_j$. Como E_{ij} contiene el campo de descomposición de Q' sobre P, Q' es el único lugar de E' que yace sobre Q_{ij}. Por otro lado $e(Q \mid Q_{ij}) = 1$ pues es una extensión constante de E_{ij}. Esto implica que $f(Q' \mid Q_{ij}) = [E' : E_{ij}] = n = f(Q' \mid P)$ y por lo tanto $deg\, Q_{ij} = 1$. De esta manera hemos construido e lugares distintos $Q_{ij} \in \cup_{i=1}^{m} X_i$ tal que $Q' \mid Q_{ij}$.

Supongamos ahora que $Q \in X_i$ para algún $i \in \{1, \ldots, m\}$ y $Q' \mid Q$. Entonces $f(Q' \mid Q) = n$. Tenemos además que $U_i = Gal(E'/E_i)$ está contenido en el grupo de descomposición H de Q' sobre P, es decir, U_i es uno de los grupos anteriormente mencionados U_{i_j} y Q es el correspondiente Q_{ij}, $j \in \{1, \ldots, e\}$. Esto demuestra la afirmación 2 y con ello concluimos la demostración de esta proposición. □

Para finalizar la demostración del teorema de Hasse-Weil, necesitamos del siguiente lema.

Lema 4.2.9. *Supongamos que $z \in F$ satisface $v_P(z) \not\equiv 0 \pmod{p}$ para algún $P \in \mathbb{P}_F$. Entonces z es un elemento separante para F/K. En particular F/K es separablemente generado.*

Demostración. Revisar [Sti]. □

Fin de la demostración del teorema de Hasse-Weil. Como se mencionó antes necesitamos establecer una cota superior para $N_r = N(F_r)$. Escojamos un subcampo racional $F_0 = \mathbb{F}_q(t) \subseteq F$ tal que F/F_0 es separable y finita; consideremos también una extensión E/F tal que E/F_0 sea de Galois (notemos que existe un elemento separable por el lema 4.2.9). Es posible que el campo de constantes de E sea una extensión propia $\mathbb{F}_{q^d}$ de $\mathbb{F}_q$. En este caso, vamos a considerar los campos $F\mathbb{F}_{q^d}$ y $F_0\mathbb{F}_{q^d} = \mathbb{F}_{q^d}(t)$ en lugar de F y de F_0. La extensión $E/F_0\mathbb{F}_{q^d}$ es de Galois y suficiente probar Hasse-Weil para $F\mathbb{F}_{q^d}$ Podemos ahora cambiar la notación y suponer que $\mathbb{F}_q$ es el campo de constantes de E y más aún, podemos suponer que q es cuadrado y $q > (g(E)+1)^4$.

Sea $m = [E : F]$ y $n = [E : F_0]$. Consideremos la extensión constante de campos $E' = E\mathbb{F}_{q^n}$, $F' := F\mathbb{F}_{q^n}$ y $F_0' = F_0\mathbb{F}_0\mathbb{F}_{q^n}$. Por el lema 4.2.7, existen exactamente m distintos subgrupos cíclicos $V_1, \ldots, V_m \subseteq Gal(E'/F)$ de orden n tal que $V_i \cap Gal(E'/F') = \{1\}$. Es claro que $V_i \cap Gal(E'/F_0') = \{1\}$ (esto se hace mostrando que E' es el compuesto de F_0' con el campo fijo de V_i), de manera que podemos suponer que $V_i = U_i$ para $i = 1, \ldots, m$. Denotemos ahora por E_i el campo fijo de U_i para $i = 1, \ldots, n$. Por la proposición 4.2.8 tenemos lo siguiente:

$$mN(F) = \sum_{i=1}^{m} N(E_i) \tag{4.22}$$

y por otra parte

$$nN(F_0) = \sum_{i=1}^{n} N(E_i) \tag{4.23}$$

Dado que supusimos que q es cuadrado y $q > (g(E)+1)^4$ tenemos la siguiente cota superior

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

para $1 \leq i \leq n$. Por la proposición 4.2.8, los lugares de $F_0 = \mathbb{F}_q(t)$ de grado 1 son el polo de t para cada $\alpha \in \mathbb{F}_q$ el cero de $t - \alpha$, entonces $N(F_0) = q + 1$ combinamos esto con (4.22) y (4.23) para obtener

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

Por lo tanto $N(F) \geq q + 1 - \frac{n-m}{m}(2g(E) + 1)q^{1/2}$. Notemos también que los números m, n y $g(E)$ son invariantes bajo extensiones de campos constantes, de manera que hemos establecido una cota inferior

$$N_r \geq q^r + 1 - c_2 q^{r/2}$$

para una constante $c_2 > 0$ y con esto terminamos la demostración del teorema de Hasse-Weil. □

El teorema de Hasse-Weil es referido frecuentemente como la hipótesis de Riemann para campos de funciones. Esto se debe a que podemos tomar la función Zeta $Z_F(t)$ como un análogo de la función ζ de Riemann

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \tag{4.24}$$

(donde $s \in \mathbb{C}$ y $Re(s) > 1$) de la siguiente manera. Definamos la norma absoluta de un divisor $A \in \mathcal{D}_F$ por $\mathcal{N}(A) := q^{deg\, A}$. La norma absoluta de un divisor propio $P \in \mathbb{P}_F$, $\mathcal{N}(P)$ es la cardinalidad de su campo de residuos F_p. Entonces la función

$$\zeta_F(s) := Z_F(q^{-s}) = Z_F(\frac{1}{q^s})$$

puede ser escrita como

$$\zeta_F(s) = \sum_{n=0}^{\infty} A_n q^{-sn} = \sum_{A \in \mathcal{D}_F,\, A \geq 0} \mathcal{N}(A)^{-s}$$

que es el análogo apropiado para (4.24). Se sabe que la función ζ de Riemann tiene una extensión meromorfa en el plano complejo. La hipótesis clásica de Riemann establece que además de los llamados ceros triviales $s = -2, -4, -6$, etc. todos los ceros de $\zeta(s)$ están en la línea crítica $R(s) = 1/2$. En el caso de campos de funciones el teorema de Hasse-Weil nos dice lo siguiente

$$\zeta_F(s) = 0 \Rightarrow Z_F(q^{-s}) = 0 \Rightarrow |q^{-s}| = q^{-1/2}$$

como $|q^{-s}| = q^{-Re(s)}$ tenemos que $\zeta_F(s) = 0 \Rightarrow Re(s) = 1/2$. Por esta razón el teorema de Hasse-Weil es visto como el análogo de la hipótesis clásica de Riemann.

Capítulo 5

Un método de construcción de curvas

Comenzaremos este capítulo con algunos antecedentes de variedades sobre campos que no son algebraicamente cerrrados.

Definición 5.0.10. Denotemos por $\bar{K}$ la cerradura algebraica de K. Una variedad afín $V \subseteq \mathbb{A}^n_{\bar{K}}$ se dice que *está definida sobre* K si su ideal $I(V) \subseteq \bar{K}[X_1, \ldots, X_n]$ es generado por polinomios $F_1, \ldots, F_r \in K[X_1, \ldots, X_n]$. Si V está definida sobre K, el conjunto

$$V(K) = V \cap \mathbb{A}^n_K = \{P = (a_1, \ldots, a_n) \in V \mid a_i \in K \text{ para todo } i\}$$

es llamado el conjunto de *puntos K-racionales.*

Existe una caracterización de los puntos racionales de una variedad en términos del grupo de Galois: Sea $Gal(\bar{K}/K)$ el grupo de Galois de $\bar{K}/K$. La acción de $Gal(\bar{K}/K)$ sobre $\bar{K}$ se extiende de manera natural a los conjuntos $\mathbb{A}^n_{\bar{K}}$, $\mathbb{P}^n_{\bar{K}}$, $\bar{K}[X_1, \ldots, X_n]$, etc. Por ejemplo, consideremos una variedad proyectiva $V \subseteq \mathbb{P}^n_{\bar{K}}$ (definida sobre K), un punto $P = (a_0 : \cdots : a_n) \in V$ y un automorfismo $\sigma \in Gal(\bar{K}/K)$; entonces $\sigma(P) = (\sigma(a_0) : \cdots : \sigma(a_n))$. Es claro que

$$V(K) = \{P \in V \mid \sigma(P) = P \text{ para todo } \sigma \in Gal(\bar{K}/K\}$$

Consideremos ahora una curva proyectiva $V \subseteq \mathbb{P}^n_{\bar{K}}$ la cual está definida sobre K (K perfecto). Entonces el campo $K(V)$ de funciones K-racionales es un campo de funciones de una variable sobre K. Un divisor $D = \sum_{P \in V} n_P P \in \mathcal{D}(V)$ *está definido* sobre K si $\sigma(D) = D$ para toda $\sigma \in Gal(\bar{K}/K)$. Los divisores de V definidos sobre K forman un subgrupo $\mathcal{D}(V/K) \subseteq \mathcal{D}(V)$. Si $D \in \mathcal{D}(V/K)$, el espacio $\mathcal{L}_K(D)$ está dado por

$$\mathcal{L}_K(D) = K(V) \cap \mathcal{L}(D)$$

es un K-espacio vectorial de dimensión finita y su dimensión sobre K es igual a la dimensión de $\mathcal{L}(D)$ (sobre $\tilde{K}$) por el teorema 3.6.3. Un divisor $Q \in \mathcal{D}(V/K)$ con $Q > 0$ es llamado un divisor primo de V/K si Q no puede ser escrito de la forma $Q = Q_1 + Q_2$, con $Q_1, Q_2 \in \mathcal{D}(V/K)$. Los divisores primos de V/K corresponden con los lugares del campo de funciones $K(V)/K$; bajo esta correspondencia, divisores primos de grado uno, i.e, *puntos K-racionales* de V corresponden a los lugares $K(V)/K$ de grado uno.

Ejemplo 5.0.11. Sea K un campo perfecto de característica $p \geq 0$ y consideremos el polinomio $g(X,Y) = aX^m + bY^n + c$, $a, b, c \in K\backslash\{0\}$, $m \geq n \geq 1$ y $p \nmid mn$. El polinomio $g(X,Y)$ es irreducible (esto se sigue del criterio de Eisenstein proposición 3.1.14). La curva afín $V = \{P \in \mathbb{A}^2_{\bar{K}} \mid g(P) = 0\}$ es no singular, ya que si $P = (\alpha, \beta) \in V$,

$$g_X(\alpha,\beta) = am\alpha^{m-1} \neq 0 \text{ ó } g_Y(\alpha,\beta) = bn\beta^{n-1} \neq 0$$

Sea ahora $G(X,Y,Z) = aX^m + bY^nZ^{m-n} + cZ^m$ la proyectivización de la curva V, entonces la cerradura en $\mathbb{P}^2$ de esta curva es

$$\bar{V} = \{(\alpha : \beta : \gamma) \in \mathbb{P}^2_{\bar{K}} \mid G(\alpha,\beta,\gamma) = 0\}$$

Consideremos los puntos al infinito, es decir, $P = (\alpha : \beta : 0)$ con $(\alpha, \beta) \neq (0,0)$ y $G(\alpha,\beta,0) = 0$.

Caso 1:$m > n$. De $G(\alpha,\beta,0)$ se sigue que $\alpha = 0$ por lo tanto $P = (0:1:0)$ es el único punto al infinito. Éste es un punto singular ya que $G_X(P) = G_Y(P) = G_Z(P) = 0$. Caso 2:$m = n$. Tenemos entonces $G(\alpha,\beta,0) = a\alpha^m + b\beta^m$, por lo que $\beta \neq 0$ y entonces podemos pensar que $\beta = 1$, es decir, $P = (\alpha : 1 : 0)$. La ecuación $a\alpha^m + b = 0$ tiene m raíces distintas $\alpha \in \bar{K}$, por lo tanto hay m puntos distintos al infinito de $\bar{V}$. Todos ellos son no singulares pues $G_Y(\alpha, 1, 0) = mb \neq 0$.

5.1 Extensiones cíclicas del campo racional

En esta sección se verá el caso particular de campos de funciones $F = K(x,y)$ que están definidos por una ecuación

$$y^n = a\prod_{i=1}^{s} p_i(x)^{n_i} \tag{5.1}$$

con $s > 0$,los polinomios $p_i(x) \in K[x]$, distintos e irreducibles, $a \neq 0$ y $0 \neq n_i \in \mathbb{Z}$. Además, vamos a suponer que las siguientes condiciones se cumplen

$$char\, K \nmid n, \quad mcd(n, n_i) = 1 \quad 1 \leq i \leq s \tag{5.2}$$

Tenemos entonces un caso particular del teorema de Riemann-Hurwitz para este tipo de extensiones.

Proposición 5.1.1. *Supongamos que $F = K(x, y)$ está definido por* (5.1) *y* (5.2), *entonces tenemos*

1. *K es el campo pleno de funciones de F, y $[F : K(x)] = n$. Si K contiene un raíz primitiva n-ésima de la unidad, entonces $F/K(x)$ es una extensión cíclica.*

2. *Denotemos por P_i y por P_∞ el cero y polo de $p_i(x)$, respectivamente en $K(x)$. Entonces los lugares $P_1, \ldots, P_s$ están totalmente ramificados en $F/K(x)$. Todos los lugares $Q_\infty \in \mathbb{P}_F$ con $Q_\infty \mid P_\infty$ tiene índice de ramificación $e(Q_\infty \mid P_\infty) = n/d$ donde*

$$d := mcd\left(n, \sum_{i=1}^{s} n_i \deg p_i(x)\right)$$

   Ningún otro lugar $P \in \mathbb{P}_{K(x)}$ que no sea $P_1, \ldots, P_s, P_\infty$ se ramifica en $F/K(x)$.

3. *El género de $F/K(x)$ es*

$$g = \frac{n-1}{2}\left(-1 + \sum_{i=1}^{s} \deg p_i(x)\right) - \frac{d-1}{2}$$

Demostración. Este resultado se sigue inmediatamente de la proposición 3.7.3, el corolario 3.7.4 y la observación 3.7.5 □

Ejemplo 5.1.2. Sea $F = K(x, y)$ con

$$y^n = (x^m - b)/(x^m - c)$$

donde $b, c \in K\backslash\{0\}$, $b \neq c$ y $char\, K \nmid mn$. Entonces (5.1) y (5.2) se cumplen y además

$$g = (n-1)(m-1)$$

Ejemplo 5.1.3. Consideremos ahora el campo de funciones $F = K(x, y)$ definido por la ecuación

$$ax^m + by^n = c, \quad a, b, c \in K\backslash\{0\}, \quad char\, K \nmid mn$$

tiene género

$$g = \frac{1}{2}((n-1)(m-1) + 1 - mcd(m, n))$$

En el caso particular de la curva de *tipo Fermat*, es decir el campo de funciones definido por

$$ax^n + by^n = c, \quad a, b, c \in K^*, \quad char\, K \nmid n$$

cuyo género es igual a $g = (n-1)(n-2)$.

Un caso particularmente interesante es el de las curvas máximas, es decir, aquellas curvas que tienen la cota de Hasse-Weil.

Ejemplo 5.1.4. Consideremos $K = \mathbb{F}_{q^2}$ el campo finito de cardinalidad q^2. Consideremos el campo de funciones $F = K(x, y)$ con

$$ax^{q+1} + by^n = c \quad a, b, c \in \mathbb{F}_q \backslash \{0\}, \quad n \mid q+1 \tag{5.3}$$

Sea $P_\alpha = P_{x-\alpha} \in \mathbb{P}_{K(x)}$ (resp. P_∞) el cero de $x - \alpha$ (resp. el polo de $x - \alpha$) y queremos determinar el número

$$N = N(F/\mathbb{F}_{q^2}) = \mid \{P \in \mathbb{P}_F;\ deg\ P = 1\} \mid$$

Vamos a hacer, en primera instancia, un cambio de variable para escribir a este campo de funciones en términos más conocidos. Hacemos la sustitución $x_1 = \gamma x$, $y_1 = \delta y$ con $\gamma^{q+1} = a/c$ y $\delta^n = -b/c$ y obtenemos entonces $F(x_1, y_1)$ con $y_1^n = x_i^{q+1} - 1$ (notemos que $\gamma, \delta, \in \mathbb{F}_{q^2}$ pues todos los elementos de $\mathbb{F}_q$ son $(q+1)-$potencias de elementos de $\mathbb{F}_{q^2}$). Por lo tanto podemos suponer desde el principio que $F = K(x, y)$ con

$$y^n = x^{q+1} - 1 \quad y \quad n \mid q+1 \tag{5.4}$$

Sea $P_\alpha \in \mathbb{P}_{K(x)}$ (resp. P_∞) el cero de $x - \alpha$ (resp. el polo de x en $K(x)$). Cualquier lugar $P \in \mathbb{P}_F$ de grado uno yace sobre P_∞ o sobre P_α para algún $\alpha \in K$, por lo tanto debemos estudiar la descomposición de P_α y P_∞ en $F/K(x)$.

Caso 1. $\alpha \in K$ y $\alpha^{q+1} = 1$. En este caso α es una raíz simple del polinomio $T^{q+1} - 1 \in K[T]$ y P_α es completamente ramificado en $F/K(x)$ por la proposición anterior. Por lo tanto P_α tiene una única extensión $P \in \mathbb{P}_F$ y $deg\ P = 1$.

Caso 2. $\alpha \in K$ y $\alpha^{q+1} \neq 1$. Vamos a determinar la descoposición de P_α en $F/K(x)$. El polinomio mínimo de y sobre $K(x)$ es $\phi(T) = T^n - (x^{q+1} - 1) \in K(x)[T]$, y

$$\phi_\alpha(T) = T^n - (\alpha^{q+1} - 1) \in K[T]$$

tiene n distintas raíces $\beta \in K = \mathbb{F}_{q^2}$ (en esta parte usamos el hecho de que $\alpha^{q+1} - 1 \in \mathbb{F}_q \backslash \{0\}$ y $n \mid q+1$). Para cualesquiera de esas raíces β, existe un único lugar $P_{\alpha,\beta} \in \mathbb{P}_F$ tal que $P_{\alpha,\beta} \mid P_\alpha$ y $y - \beta \in P_{\alpha,\beta}$ es de grado uno. Por lo tanto P_α tiene n extensiones distintas $P \in \mathbb{P}_F$ que cumplen $deg\ P = 1$.

Caso 3. $\alpha = \infty$. En este caso, no es posible aplicar directamente el teorema de Kummer, pues no todos los coeficientes del polinomio mínimo de y sobre $K(x)$ están en el anillo de valuación $\mathcal{O}_\infty$ de P_∞. Consideramos entonces el elemento $z := y/x^{\frac{q+1}{n}}$ que satisface la ecuación

$$z^n = 1 - (1/x)^{q+1}$$

Como $T^n - 1$ tiene n raíces distintas en K tenemos que P_∞ tiene n extensiones distintas $P \in \mathbb{P}_F$, todas de grado uno.

Existen $q+1$ elementos $\alpha \in \mathbb{F}_{q^2}$ que pertenecen al caso 1 y $(q^2-(q+1))$ elementos α se encuentran en el caso 2. Sumando las extensiones obtenemos que $F/\mathbb{F}_{q^2}$ tiene

$$N = (q+1) + n(q^2-(q+1)) + n = q+1+n(q^2-q)$$

lugares de grado uno. Por el primer ejemplo, el género de F es $g = (n-1)(q-1)/2$ y por lo tanto

$$q^2+1+2gq = q^2+1+q(n-1)(q-1) = q+1+n(q^2-q)$$

De manera que los campos de funciones que están definidos por (5.3) tiene la cota de Hasse-Weil

$$N = q^2+1+2gq$$

sobre F_{q^2}.

Ejemplo 5.1.5. El caso particular $H = \mathbb{F}_{q^2}(x,y)$ con

$$x^{q+1} + y^{q+1} = 1$$

es llamado el campo de funciones *hermitiano* y es un campo de funciones máximo. Como lo indica el ejemplo anterior. En este caso $g(X,Y) = X^{q+1} + Y^{q+1} - 1$. Vamos a determinar el número de puntos K-racionales $P = (\alpha : \beta : \gamma) \in \bar{V}(K)$. Sea primero $\gamma \neq 0$, es decir, $P = (\alpha : \beta : 1)$ Para todo $\alpha \in K$ con $\alpha^{q+1} \neq 1$ existen $q+1$ elementos distintos $\beta \in K$ con $G(\alpha,\beta,1) = 0$. Finalmente si $\gamma = 0$, existen $q+1$ puntos $P = (\alpha : 1 : 0) \in \bar{V}(K)$. De esta manera tenemos todos los puntos K-racionales de la curva hermitiana, los cuales totalizan q^3+1.

5.2 El método

Las curvas construidas a partir de este momento estarán dadas por ecuaciones afines sobre un campo finito con q elementos definidas por

$$y^m = h(x),$$

donde m divide a $q-1$ y $h(x) \in \mathbb{F}_q(x)$ una función racional. Para el método estudiado en este trabajo m será cualquier divisor de $q-1$ y $h(\alpha) = 1$ para casi todos los elementos de $\alpha \in \mathbb{F}_q$.

La forma de construir estas curvas consistirá en considerar ecuaciones de la forma

$$y^m = \frac{g(x)}{R(g(x))}$$

donde $R(g(x))$ es un polinomio asociado a $g(x)$ de tal forma que el cociente $\frac{g(x)}{R(g(x))}$ es casi siempre 1 cuando lo evaluamos en el campo finito en cuestión. Dado un polinomio $g(x) \in \mathbb{F}_q[x]$ de grado $\geq q$, definimos su polinomio reducido $R(g(x))$ el cual será de grado $\leq q-1$, que se obtiene de $g(x)$ realizando las siguientes operaciones en los monomios:

1. $R(x^j) = x^j$ si $j \leq q-1$.
2. $R(x^{q+j}) = x^{1+j}$ para toda $j \geq 0$.

Veamos los siguientes ejemplos de cálculo polinomio reducido.

Ejemplo 5.2.1. Consideremos los siguientes polinomios
$R(x^{2q-1}) = R(x^{q+q-1}) = R(x^{1+q-1}) = R(x^q) = x$
$R(x^{2q-2}) = R(x^{q+q-2}) = R(x^{1+q-2}) = R(x^{q-1}) = x^{q-1}$
$R(ax^{q^2} + x^{q+1} + bx + c) = R(ax^{q^2}) + R(x^{q+1}) + R(bx) + R(cx^0)$
$= ax + x^2 + bx + c$ Si $q \neq 2$ y $a, b, c \neq 0 \pmod q$.

Más en general, es inmediato verificar que si $n \equiv m \pmod{q-1}$ y $1 \leq n \leq q-1$, entonces $R(x^m) = x^n$ y precisamente por este hecho, para $\alpha \in \mathbb{F}_q$, $g(\alpha) = R(g(\alpha))$. En particular

$$g(\alpha) = 0 \iff R(g(\alpha)) = 0$$

Observación 5.2.2. La propiedad más importante entre un polinomio $g(x)$ y su reducido $R(g(x))$ es la siguiente

$$\frac{g(x)}{R(g(x))} = 1 \text{ para todo } \alpha \in \mathbb{F}_q \text{ con } g(\alpha) \neq 0$$

Esta observación es inmediata del hecho de que $\mathbb{F}_q^*$ tiene orden $q-1$, es un grupo bajo el producto y la relación que ocurre si $m \equiv n \pmod{q-1}$ entonces $x^m = x^n$ $(1 \leq n \leq q-1)$.

Las curvas absolutamente irreducibles, definidas por

$$y^m = \frac{g(x)}{R(g(x))} \text{ tal que } m \mid q-1 \tag{5.5}$$

son tales que su número N de puntos racionales sobre $\mathbb{F}_q$ satisface

$$N \geq m \#\{\alpha \in \mathbb{F}_q \mid g(\alpha) \neq 0\}.$$

Lo cual también es fácil de verificar pues, en $\mathbb{F}_q^*$ para cada divisor m de $q-1$ existe un subgrupo multiplicativo de orden m ($\mathbb{F}_q^*$ es un grupo cíclico para todo campo finito $\mathbb{F}_q$).

Los polinomios $g(x)$ que vamos a estar considerando siempre serán de la forma $g(x) = f(x)^r$ para algún $f(x) \in \mathbb{F}_q[x]$ y $r \geq 2$, esto es hecho con el objeto de que la curva tenga género pequeño. De esta manera las curvas $\mathcal{X}$ que estaremos considerando serán de la forma

$$y^m = \frac{f(x)^r}{R(f(x)^r)} \; m \mid q-1 \text{ y } r \geq 2 \tag{5.6}$$

La ecuación (5.6) nos define una extensión muy particular de campos de funciones $\mathbb{F}_q(x,y)/\mathbb{F}_q(x)$ y siempre ocurrirá que en esta extensión existe un lugar totalmente ramificado y por lo tanto tendremos que la ecuación (5.6) es totalmente irreducible (corolario 3.7.4).

El siguiente teorema nos da una caracterización del género de las curvas anteriormente expuestas.

Teorema 5.2.3. *Sea $f(x) \in \mathbb{F}_{q^n}[x]$ un polinomio separable y sea q^j una potencia de la característica tal que $q^j(deg\, f(x)) \geq q^n$. Supongamos también que el polinomio reducido $R(f(x)^{q^j})$ es también separable y que la curva $\mathcal{X}$ definida por*

$$y^m = \frac{f(x)^{q^j}}{R(f(x)^{q^j})} \text{ con } m \text{ divisor de } q^n - 1$$

es absolutamente irreducible.

Entonces el género g y el número N de puntos racionales sobre $\mathbb{F}_{q^n}$ de la curva $\mathcal{X}$ satisface

$$2g = (\delta + \delta' - 2c)(m-1) + c(m-d) + (m-d') \text{ y } N \geq (q^n - c_1)m$$

donde los coeficientes $\delta = deg\, f(x)$, $\delta' = deg\, R(f(x)^{q^j})$, $d = mcd(m, q^j - 1)$, $d' = mcd(m, q^j\delta - \delta')$ y los números c y c_1 están definidos por

$$\begin{aligned} c_1 &= \#\{\alpha \in \mathbb{F}_{q^n} \mid f(\alpha) = 0\} \\ c &= \#\{\alpha \in \bar{\mathbb{F}}_{q^n} \mid f(\alpha) = R(f(\alpha)) = 0\} \end{aligned}$$

y $\bar{\mathbb{F}}_{q^n}$ es la cerradura algebraica de $\mathbb{F}_q$.

Demostración. La afirmación sobre el género g de $\mathcal{X}$ se sigue de la fórmula de Riemann-Hurwitz aplicada a la extensión de campos $\mathbb{F}_{q^n}(x,y)/\mathbb{F}_{q^n}(x)$ de grado m. Los ceros comunes de $f(x)$ y de $R(f(x))$ en $\bar{\mathbb{F}}_q$ se ramifican con índice de ramificación m/d (pues cada uno de los lugares –los ceros comunes– son menores o iguales que el diferente), el infinito posee índice de ramificación

m/d' por el corolario 3.7.4 de las extensiones de Kummer y los demás ceros del numerador o el denominador, los cuales son $\delta + \delta' - 2c$ puntos son ceros simples y por lo tanto totalmente ramificados. De esta manera la fórmula de Riemann-Hurwitz nos da lo siguiente

$$2g - 2 = -2m + cd(\frac{m}{d} - 1) + d'(\frac{m}{d'} - 1) + (\delta + \delta' - 2c)(m - 1)$$

que es, después de algunas simplificaciones la afirmación del teorema. La afirmación sobre el número N se sigue inmediatamente de la observación 5.2.2. □

Debemos mencionar que el valor exacto de N se obtiene después de analizar la racionalidad de los puntos cuya primera coordenada es $x = \infty$ o $x = \alpha$, con $\alpha \in \mathbb{F}_q$ y $f(\alpha) = 0$. Si $\alpha \in \mathbb{F}_q$ es un cero de $f(x)$, entonces es un cero de multiplicidad $q^j - 1$ de la función racional $\frac{f(x)}{R(f(x))}$, dado que supusimos que los polinomios $f(x)$ y $R(f(x))$ son separables, podemos escribir a la curva $\mathcal{X}$ de la manera siguiente

$$y^m = \frac{f(x)^{q^j}}{R(f(x)^{q^j})} = (x - \alpha)^{q^j - 1} h(x)$$

con $h(x) \in \mathbb{F}_q[x]$ y $h(\alpha) \neq 0$. La ecuación anterior la podemos ahora reescribir como

$$\left(\frac{y^{m/d}}{(x - \alpha)^{\frac{q^j - 1}{d}}} \right)^d = h(x)$$

donde $d = mcd(m, q^j - 1)$. Denotamos ahora por z lo siguiente

$$z = \frac{y^{m/d}}{(x - \alpha)^{\frac{q^j - 1}{d}}}$$

De manera que tenemos las siguentes extensiones de campos de funciones $\mathbb{F}_{q^n}(x) \subset \mathbb{F}_{q^n}(x, z) \subset \mathbb{F}_{q^n}(x, y)$. Entonces para verificar la racionalidad de los puntos con $x = \alpha$, basta verificar que la ecuación $z^d = h(\alpha)$ posee d soluciones en el campo finito $\mathbb{F}_{q^n}$ y en ese caso tendremos d puntos racionales cuya primera coordenada será $x = \alpha$.

5.3 Aplicaciones del método

Las siguientes curvas se considerarán sobre $\mathbb{F}_{q^2}$.

Ejemplo 5.3.1. Consideremos la curva

$$y^m = \frac{(x^{q+1}+x+1)^q}{x^{q+1}+x^q+1} \quad m \text{ un divisor de } q^2-1.$$

Notemos primero algunos detalles: las raíces comunes del numerador y del denominador pertenecen a $\mathbb{F}_q$ y satisfacen la ecuación $x^2+x+1=0$, ($\alpha^q=\alpha$ si $\alpha \in \mathbb{F}_q$). Entonces tenemos tres casos a considerar pues $x^2+x+1=0$ si y sólo si $x^3=1$ y $x \neq 1$. Denotemos por $d = mcd(m, q-1)$. 1er Caso. $q \equiv 1 \pmod 3$, entonces $c = c_1 = 2$, por lo tanto

$$g = (q-2)(m-1) + (m-d)$$

y además

$$N = \begin{cases} (q^2-1)m, & \text{si } \frac{q-1}{d} \not\equiv 0 \pmod 3 \\ (q^2-1)m + 2d, & \text{si } \frac{q-1}{d} \equiv 0 \pmod 3 \end{cases}$$

Entonces tenemos puntos racionales cuya primera coordenada es $x = \alpha$ y $\alpha^2+\alpha+1=0$ si y sólo si existe $z \in \mathbb{F}_{q^2}$ tal que $z^d = -\alpha$, lo cual ocurre si y sólo si $3 \mid \frac{q-1}{d}$. De la misma manera, tenemos m puntos racionales cuya primera coordena es $x = \infty$ ya que la ecuación $z^m = 1$ tiene claramente soluciones en $\mathbb{F}_{q^2}$.

2do Caso. $q \equiv 0 \pmod 3$, entonces $c = c_1 = 1$ y tenemos

$$g = (q-1)(m-1) + \frac{m-d}{2}$$

por otra parte

$$N = q^2 m + d$$

El número de puntos racionales viene del hecho de que tenemos d puntos cuya primera coordenada es $x = 1$ y m puntos cuya primera coordenada es $x = \infty$.

3er Caso. $q \equiv 2 \pmod 3$, entonces $c = c_1 = 0$, por lo tanto

$$g = q(m-1)$$

y

$$N = (q^2+1)m$$

En este caso obtuvimos exactamente m puntos cuya primera coordenada es $x = \infty$.

Ejemplo 5.3.2. Supongamos primero que $p \neq 2$ y consideremos la curva definida por:

$$y^m = \frac{(x^{q+1}+x+1)^q}{x^{q+1}+x^q-1}, \text{ con } m \text{ un divisor de } q^2-1$$

De nueva cuenta las raíces comunes del numerador y el denominador son elementos en $\mathbb{F}_q$ que satisfacen $\alpha^2+\alpha-1=0$, es decir, $\left(2(\alpha+\frac{1}{2})\right)^2=5$. Por lo tanto, necesitamos que $p\neq 5$ y q un cuadrado tal que ocurra lo siguiente $p\equiv \pm 1 \pmod 5$. Tenemos entonces que ahora $c=c_1=2$. Entonces por el teorema 5.2.3 tenemos que el género

$$g=(q-2)(m-1)+(m-d),$$

donde $d=mcd(m,q-1)$. Denotemos por $o(\alpha)$ el orden del elemento α en $\mathbb{F}_q^*$ que cumpla además $\alpha^2+\alpha+1=0$, vemos que el número de puntos racionales sobre $\mathbb{F}_{q^2}$ satisface

$$N=\begin{cases}(q^2-1)m+2d & \text{si } o(\alpha)\mid \frac{4(q-1)}{d}\\ (q^2-1)m & \text{en caso contrario}\end{cases}$$

El número exacto de los puntos racionales se obtiene al analizar cuidadosamente las siguientes ecuaciones

$$z^d=\frac{(\alpha^q+1)^q}{\alpha^q}=\frac{\alpha+1}{\alpha}=\frac{1}{\alpha^2} \text{ si } x=\alpha \text{ y } \alpha^2+\alpha-1=0$$

y

$$z^m=1 \text{ los puntos cuya primera coordenada es } x=\infty$$

Por ejemplo, si $p=3$ y q es un cuadrado, entonces el orden del elemento α es igual a $o(\alpha)=8$ y obtenemos $2d$ puntos racionales extras si $\frac{q-1}{d}$. De esta manera para $q=9$ obtenemos una curva sobre $\mathbb{F}_{81}$ y $g=7$ con $N=164$, un nuevo récord para curvas sobre este campo y de este género (ver Quoos).

Bibliografía

[A-M] Atiyah, Michael, McDonald, I. *Introduction to Commutative Algebra*, Addison-Wesley, Reading, Massachusetts, 1969.

[Bri] Le Brigand, D. *Corps de fonctions.* DEA "Méthodes algébriques". Méthodes pour les corps glabaux. Notas, Institut de Mathématiques de Jussieu, 2001.

[Har] Hartshorne, R. *Algebraic Geometry.* (Graduate Texts in Mathematics), Springer-Verlag, New-York-Heidelberg-Berlin, 1977.

[Lid-Nie] Lidl, R., Niederreiter, H. *Finite Fields.* (Encyplopedia of Mathematics and its Applications), vol **20**. Addison-Wesley, Reading, Massachusetts, 1965.

[Lor] Lorenzini, D. *An Invitation to Arithmetic Geometry* (Graduate Studies in Mathematics), vol **9**. American Mathematical Society, Rhode Island. 1996.

[Mat] Matsumura, H. *Commutative Ring Theory* (segunda edición), traducido por Reid, M. Cambridge University Press, Cambridge. 1995.

[Mor] Morandi, P. *Field and Galois theory.* (Graduate Texts in Mathematics), vol **167**, Springer-Verlag, New York-Heildelberg-Berlin, 1996.

[Mrn] Moreno, C. *Algebraic Curves over Finite Fields.* (Cambridge Tracts in Mathematics), vol **97**. Cambridge University Press, Cambridge, 1991.

[Neu] Neurkich, J. *Algebraic Number Theory.* (A Series of Comprehensives Studies in Mathematics), vol **322**. Springer-Verlag, New York-Heildelberg-Berlin, 1999.

[Quo] Quoos, L., García, A. *A construction of curves over finite fields*, Acta Arith. **98**, no 2 2001, 181-195.

[Ste] Stepanov, S. *Arithmetic of Algebraic Curves.* Consultants Bureau, New York and London, 1994.

[Sti] Stichtenoth, H. *Algebraic funtion fields and codes*. Springer-Verlag, Berlin, 1993.

[Zar] Zariski O., Samuel, P. *Commutative Algebra*, vol I, Springer-Verlag, Berlin, 1975.