CENTRO DE INVESTIGACIÓN Y DE ESTUDIOS AVANZADOS

DEL INSTITUTO POLITÉCNICO NACIONAL

UNIDAD ZACATENCO

DEPARTAMENTO DE CONTROL AUTOMÁTICO

Campos de funciones ciclotómicos con número de clases de divisores uno

T E S I S

QUE PRESENTA

Elizabeth Ramírez Ramírez

Para obtener el grado de

Maestra en Ciencias

en la Especialidad de Control Automático

Directora de Tesis:

Dra. Martha Rzedowski Calderón

México, D.F. Noviembre, 2014

A mis padres y hermanos.

A Eduardo Israel, Abril Paola,
Balam Alejandro y Mabel Itzae.

A la memoria de César Ramírez †

"Algunos misterios siempre escaparán a la mente humana.
Para convencernos de ello, sólo hay que echar un vistazo
a las tablas de los números primos, y ver que no reina
ni orden, ni reglas."
Évariste Galois

"Tenemos mucho tiempo por delante
para crear los sueños que aún
ni siquiera imaginamos soñar."
Steven Spielberg

Agradecimientos

Agradecezco profundamente a la Dra. Martha Rzedowski Calderón por todo el apoyo brindado durante la realización de este trabajo y por animarme siempre a seguir adelante. Al Dr. Gabriel Villa Salvador por sus enseñanzas y sugerencias para mejorar este trabajo. A la Dra. Myriam Rosalía Maldonado Ramírez por sus consejos y apoyo.

Al CINVESTAV y de manera especial al Departamento de Control Automático por la oportunidad brindada. A mis profesores por sus enseñanzas.

A mis padres y a mis hermanos Israel, Tere, René, Janet y a Tanize, por su apoyo incondicional, por soportarme en los momentos difíciles y por creer en mi siempre.

A Miguel, Anaid, Mónica, Kernel, Carlos, Xavier y Arturo por escucharme siempre y por sus palabras de aliento.

Al CONACyT.

Índice general

Resumen IX

Abstract XI

Introducción XIII

1. Preliminares 1

1.1. Generalidades 1

1.2. Valuaciones en campos de funciones racionales 2

1.3. Divisores 3

1.4. Adéles, diferenciales y el teorema de Riemann-Roch 8

2. Campos ciclotómicos 15

2.1. Campos de funciones ciclotómicos 15

2.2. Ramificación en $\mathfrak{p}_\infty$ 27

2.3. Subcampo real maximal 30

3. Fórmulas del diferente y del género 35

3.1. Extensiones de campos de funciones 35

3.2. Discriminante, diferente y género 38

3.3. Caso K_M y K_M^+ 46

4. Campos con número de clases de divisores uno 51

4.1. Campos de funciones algebraicas 51

4.2. Campos de funciones ciclotómicos 59

A. Método de Newton y lema de Abhyankar **75**

A.1. Método de Newton 75

A.2. Lema de Abhyankar 76

Conclusiones **77**

Bibliografía **79**

Resumen

Sea K un campo de funciones racionales sobre el campo finito $\mathbb{F}_q$ con q elementos. Usando las ideas de Carlitz, Hayes construyó la máxima extensión abeliana de K. En dicha construcción, usa campos de funciones ciclotómicos K_M.

El propósito de esta tesis es determinar los campos de funciones ciclotómicos con número de clases de divisores igual a uno. Para ello se presentan fórmulas para el diferente y para el género de los campos de funciones ciclotómicos K_M y de sus subcampos reales maximales K_M^+. El problema se reduce a encontrar la descomposición de $M = \prod_{i=1}^{r} P_i^{n_i}$ como producto de potencias de polinomios mónicos irreducibles de manera que al aplicar dichas fórmulas a los campos de funciones ciclotómicos y a sus subcampos reales maximales tengan género cero.

Abstract

Let K be a rational function field over the finite field $\mathbb{F}_q$ with q elements. Using the ideas of Carlitz, Hayes constructed the maximal abelian extension of K. In this construction he uses cyclotomic function fields K_M.

The purpose of this dissertation is to determine the cyclotomic function fields with divisor class number one. For this, we present formulas for the different and the genus of cyclotomic function fields K_M and their maximal real subfields K_M^+. The problem is reduced to finding the decomposition of $M = \prod_{i=1}^{r} P_i^{n_i}$ as a product of powers of monic irreducible polynomials so that the application of these formulas to cyclotomic function fields and to their maximal real subfields render genus equal to zero.

Introducción

La teoría de campos de funciones ciclotómicos se inicia con el trabajo de Kummer en las décadas de 1840 y 1850, sobre el último teorema de Fermat y las leyes de reciprocidad. En 1958 Iwasawa introdujo la teoría de $\mathbb{Z}_p$-extensiones y unos años después Kubota y Leopoldt inventaron las L-funciones p-ádicas, las cuales fueron interpretadas en términos de $\mathbb{Z}_p$-extensiones por Iwasawa.

Dentro de la teoría algebraica de números se estudian los campos numéricos que son extensiones finitas del campo de los números racionales $\mathbb{Q}$ y los campos de funciones algebraicas en una variable. Dados k un campo cualquiera, $k[T]$ el anillo de polinomios con coeficientes en k y $k(T)$ el campo de cocientes de $k[T]$, entonces un campo de funciones es una extensión finita de $k(T)$.

Se tienen varias analogías entre los campos numéricos y los campos de funciones, a saber:

Campos numéricos	Campos de funciones
$\mathbb{Z}$ es un dominio de factorización única	$k[T]$ es dominio de factorización única
$\mathbb{Q}$ es el campo cociente de $\mathbb{Z}$	$K = k(T)$ es el campo de cocientes de $k[T]$
$\mathbb{P}_{\mathbb{Q}} = \{\mathfrak{p} \in \mathbb{Z} \mid \mathfrak{p}$ es primo$\} \cup$ {el valor absoluto usual}.	$\mathbb{P}_K = \{P(T) \in k[T] \mid P(T)$ es irreducible $\} \cup \{\frac{1}{T}\}$.

Existen algunos campos de funciones análogos a los campos de números ciclotómicos los cuales fueron descubiertos por Carlitz en la década de los años treinta del siglo pasado. Esta analogía se profundizó en 1973, cuando Hayes publicó una exposición de las ideas de Carlitz sobre polinomios ciclotómicos y mostró que ésta contiene una teoría de los campos de clases para los campos de funciones racionales congruentes. Drinfeld y Hayes, generalizaron esta idea para obtener una teoría explicíta de campos de clases para cualquier campo de funciones congruentes, es decir una construcción explícita de toda extensión abeliana de dicho campo.

De igual forma los campos ciclotómicos y los campos de funciones ciclotómicos poseen ciertas analogías:

$\mathbb{Q}$	$k = \mathbb{F}_q[T]$
$W_n = \{\xi \in \overline{\mathbb{Q}} \mid \xi^n = 1\}$	$\Lambda_M = \{u \in \overline{k} \mid u^M = 0\}$
$\cong \prod_{i=1}^{r} W_{\mathfrak{p}_i^{\alpha_i}}$ donde $n = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_r^{\alpha_r}$ y $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ son números primos.	$\cong \prod_{i=1}^{r} \Lambda_{P_i^{\alpha_i}}$ donde $M = \prod_{i=1}^{r} P_i^{\alpha_i}$ y $P_1, \ldots, P_r$ son polinomios irreducibles.

El presente trabajo se basa en el artículo de Kida-Murabayashi [10]. En él se presenta una fórmula para el género del subcampo real maximal de campos de funciones ciclotómicos y se aplica ésta para determinar los campos de funciones ciclotómicos y los subcampos reales maximales con número de clases de divisores igual a uno.

En el capítulo 1, se dan las definiciones y propiedades básicas de valuaciones aplicadas a campos de funciones. Asimismo se tiene lo referente a divisores, clases de divisores, adéles, diferenciales y el teorema de Riemann-Roch.

En el capítulo 2 se desarrolla el tema de campos de funciones ciclotómicos sobre campos de funciones racionales con campo de constantes finito. Se presentan las propiedades de la ramificación del primo infinito y del subcampo real maximal de un campo de funciones ciclotómicos.

En el capítulo 3 se da una introducción a las extensiones de campos de funciones, las definiciones y las propiedades del discriminante, del diferente y del género, los cuales permiten introducir la fórmula de Riemann-Hurwitz. Finalmente, se obtienen fórmulas para el diferente y el género de los campos de funciones racionales y de sus subcampos reales maximales.

Por último, en el capítulo 4, se obtienen algunas condiciones para que un campo de funciones algebraicas tenga número de clases de divisores igual a uno. Posteriormente, se obtiene el resultado que garantiza que el número de clases de divisores es uno si y sólo si el género es cero, el cual es válido tanto para un campo de funciones ciclotómico, como para su subcampo real maximal. Para ello sólo se deben aplicar las fórmulas para el diferente y para el género obtenidas en el capítulo 3.

Capítulo 1

Preliminares

En el presente capítulo se da una introducción a la teoría de valuaciones y se hace un estudio de valuaciones en campos de funciones racionales. Posteriormente se dan definiciones y propiedades de divisores, entre los cuales destacan el teorema de Riemann y la definición del género de un campo de funciones algebraicas. Finalmente, se tratan los temas de adéles y de diferenciales, los cuales permiten demostrar el teorema de Riemann-Roch. También se prueba que un campo de funciones racionales tiene número de clases de divisores igual a uno.

1.1. Generalidades

Definición 1.1.1. Sea k un campo arbitrario. Un *campo de funciones* K sobre k es una extensión finitamente generada de k con grado de trascendencia 1.

Aquí suponemos que k es algebraicamente cerrado en K, es decir, si

$$\bar{k} = \{\alpha \in K \mid \alpha \text{ es algebraico sobre } K\},$$

entonces $\bar{k} = k$. En este caso a k se le llama el *campo de constantes* de K.

Definición 1.1.2. Sea $v : K^* \to \mathbb{Z}$ una valuación discreta de K^* que es *trivial* en k^*, es decir, $v(\alpha) = 0$ para $\alpha \in k^*$. Sean $\mathcal{O}_v = \{x \in K \mid v(x) \geq 0\}$ el anillo de valuación de v y $\mathcal{P}_v = \{x \in K \mid v(x) > 0\}$ el ideal maximal de $\mathcal{O}_v$. Al campo $k(v) := \mathcal{O}_v/\mathcal{P}_v$ se le llama el *campo residual* de v. Se tiene que $[k(v) : k] < \infty$ y a $[k(v) : k]$ se le llama el *grado* de v.

Por otro lado, si $\mathcal{O} \subseteq K$ es un subanillo de K, que es de valuación, con $k \subseteq \mathcal{O}$ y coc $\mathcal{O} = K$, entonces $\mathcal{O}$ da lugar a una valuación v. Si $\mathcal{P}$ es el ideal maximal de $\mathcal{O}$ se denota $k(\mathcal{P}) = k(v)$ y $d(\mathcal{P}) = d_K(\mathcal{P}) = f_{\mathcal{P}} = [k(v) : k]$ al grado de $\mathcal{P}$.

Nota 1.1.3. Cada uno de los tres objetos: el anillo de valuación $\mathcal{O}$, la valuación v y el ideal máximal $\mathcal{P}$ de $\mathcal{O}$, determina a los otros dos. A todos ellos de manera indistinta los nombraremos "lugar".

Se tiene que si v es una valuación de K, entonces $v|_{k(T)}$ es una valuación de $k(T)$, donde $T \in K \setminus k$, es decir, T es trascendente sobre k y por tanto $[K : k(T)]$ es finito.

Recíprocamente, dada una valuación v en $k(T)$, v se puede extender a una valuación en K y el número de tales extensiones es menor o igual a $[K : k(T)]$.

1.2. Valuaciones en campos de funciones racionales

En esta sección consideraremos el campo de funciones racionales $K = k(T)$. Sea $P = P(T) \in k[T]$ un polinomio mónico e irreducible. Si $\alpha = \alpha(T) \in k(T)^*$, escribimos

$$\alpha(T) = P(T)^s \frac{u(T)}{v(T)},$$

con $u(T),\ v(T) \in k[T]$ y $(P(T), u(T)) = 1 = (P(T), v(T))$ y $s \in \mathbb{Z}$.

Sea $v_P : K^* \to \mathbb{Z}$ dado por $v_P(\alpha) = s$, y definimos $v_P(0) = \infty$. Entonces v_P es una valuación.

El anillo de valuación asociado a P es $\mathcal{O}_P = \{\alpha \in k(T) \mid v_P(\alpha) \geq 0\}$, es decir,

$$\mathcal{O}_P = \left\{ \frac{a(T)}{b(T)} \in K \middle| (b(T), P(T)) = 1 \right\} = \left\{ \frac{a(T)}{b(T)} \in K \middle| P(T) \nmid b(T) \right\} = k[T]_P.$$

El ideal máximo de $\mathcal{O}_P$ es $\mathcal{P}_P = \{\alpha \in k(T) \mid v_P(\alpha) > 0\}$, es decir,

$$\mathcal{P}_P = \left\{ \frac{a(T)}{b(T)} \;\middle|\; P(T) \mid a(T),\ P(T) \nmid b(T) \right\} = P \cdot \mathcal{O}_P.$$

Notemos que $\mathcal{O}_P \neq k(T)$, pues $\frac{1}{P} \notin \mathcal{O}_P$.

Si $Q = Q(T) \in k[T]$ es un polinomio mónico e irreducible con $P(T) \neq Q(T)$, se tiene $v_P(P) = 1$ y $v_Q(P) = 0$. Por lo que v_P y v_Q son inequivalentes. Además, si $\alpha \in k^*$, entonces $v_P(\alpha) = 0$, es decir, v_P es trivial sobre k.

El campo residual es

$$\mathcal{O}_P/\mathcal{P}_P \cong k[T]_{(P)}/(P)k[T]_{(P)} \cong k[T]/(P)$$

y $k[T]/(P)$ es una extensión finita de grado igual al grado del polinomio $P(T)$.

Sea $y = \dfrac{1}{T}$, entonces $k(y) = k(T) = K$. Cada polinomio $Q(y) \in k[y]$ mónico e irreducible tiene una valuación asociada. En particular para $y \in k[y]$ y se denota la valuación asociada por $v_y = v_\infty$.

Sea $\alpha(T) \in K^*$, $\alpha(T) = \dfrac{a(T)}{b(T)}$ con $a(T),\ b(T) \in k[T]$. Entonces

$$\alpha(T) = \frac{a(\frac{1}{y})}{b(\frac{1}{y})} = \frac{y^{-\mathrm{gr}_T a} a_1(y)}{y^{-\mathrm{gr}_T b} b_1(y)} = y^{-\mathrm{gr}_T a + \mathrm{gr}_T b} \frac{a_1(y)}{b_1(y)},$$

donde $a_1(y),\ b_1(y) \in k[y]$ y $(a_1(y), y) = (b_1(y), y) = 1$.

Entonces $v_\infty(\alpha(T)) = v_y\Big(y^{-\mathrm{gr}_T a + \mathrm{gr}_T b} \dfrac{a_1(y)}{b_1(y)}\Big) = -\mathrm{gr}_T a + \mathrm{gr}_T b = -\mathrm{gr}_T(\alpha(T))$.

Ahora el anillo de valuación es

$$\mathcal{O}_\infty = \left\{ \frac{a(T)}{b(T)} \middle| \mathrm{gr}_{\ T} b \geq \mathrm{gr}_{\ T} a \right\} = k[y]_{(y)},$$

el ideal máximo es

$$\mathcal{P}_\infty = \left\{ \frac{a(T)}{b(T)} \middle| \mathrm{gr}_{\ T} b > \mathrm{gr}_{\ T} a \right\} = yk[y]_{(y)}$$

y el campo residual es $\mathcal{O}_\infty/\mathcal{P}_\infty \cong k[y]_{(y)}/yk[y]_{(y)} \cong k[y]/(y) \cong k$. Luego el grado del campo residual sobre k es 1.

Observemos que v_∞ no es equivalente a ningún v_P de antes, pues si $P(T) \in k[T]$ es un polinomio mónico e irreducible, entonces $v_P(P) = 1$ y $v_\infty(P) < 0$.

Teorema 1.2.1. *$\{v_P, v_\infty \mid P(T) \in k[T]$ es mónico e irreducible$\}$ son todas las valuaciones en $k(T)$ tales que $v(a) = 0$ para todo $a \in k^*$.*

Demostración. Ver [17], teorema 2.4.1, pp.37. □

Usualmente se denotará por $\mathfrak{p}_\infty, \mathfrak{p}_P$ a los lugares correspondientes a v_∞, v_P respectivamente.

1.3. Divisores

Sea L un campo de funciones algebraicas sobre el campo finito $k = \mathbb{F}_q$ con q elementos como campo de constantes y sea $\mathbb{P}_L$ el conjunto de lugares de L, esto es:

$$\mathbb{P}_L = \{\mathcal{P} \mid \mathcal{P} \text{ es un lugar de } L\}.$$

Si $\mathcal{P} \in \mathbb{P}_L$, la valuación correspondiente se denotará por $v_\mathcal{P}$.

Definición 1.3.1. Sea D_L el grupo abeliano libre generado por todos los lugares $\mathbb{P}_L$ de L. A D_L se le llama el *grupo de divisores* de L y los lugares se llaman *divisores primos* de L.

Nota 1.3.2. Consideraremos al grupo de divisores como grupo multiplicativo.

Si $\mathfrak{A}$ es un divisor, éste puede escribirse de forma única como $\prod_{\mathcal{P}\in\mathbb{P}_L} \mathcal{P}^{v_{\mathcal{P}}(\mathfrak{A})}$, donde $v_{\mathcal{P}}(\mathfrak{A}) \in \mathbb{Z}$ y $v_{\mathcal{P}}(\mathfrak{A}) = 0$ para casi todo $\mathcal{P}$.

Definición 1.3.3. El *divisor identidad* $\eta := \prod_{\mathcal{P}\in\mathbb{P}_L} \mathcal{P}^0$ es el que satisface $v_{\mathcal{P}}(\eta) = 0$ para cada lugar $\mathcal{P}$.

Definición 1.3.4. Un divisor $\mathfrak{A}$ es llamado *entero* si $v_{\mathcal{P}}(\mathfrak{A}) \geq 0$ para cada lugar $\mathcal{P}$.

Definición 1.3.5. Un divisor $\mathfrak{A}$ *divide* a un divisor $\mathfrak{B}$ si existe un divisor entero $\mathfrak{C}$ tal que $\mathfrak{B} = \mathfrak{A}\mathfrak{C}$, es decir, si $v_{\mathcal{P}}(\mathfrak{B}) \geq v_{\mathcal{P}}(\mathfrak{A})$ para todo $\mathcal{P}$. Cuando $\mathfrak{A}$ divide $\mathfrak{B}$ se escribe $\mathfrak{A}|\mathfrak{B}$.

Definición 1.3.6. Los divisores $\mathfrak{A}$ y $\mathfrak{B}$ son *primos relativos o coprimos* si $v_{\mathcal{P}}(\mathfrak{A}) \neq 0$ implica $v_{\mathcal{P}}(\mathfrak{B}) = 0$.

Nota 1.3.7. Dado un lugar $\mathcal{P}$, $f_{\mathcal{P}} = [k(\mathcal{P}) : k]$ denota el grado de $\mathcal{P}$, donde $k(\mathcal{P})$ es el campo residual.

Definición 1.3.8. Sea $\mathfrak{A}$ un divisor. Se define el *grado* de $\mathfrak{A}$, como

$$d(\mathfrak{A}) = d_L(\mathfrak{A}) = \sum_{\mathcal{P}\in\mathbb{P}_L} f_{\mathcal{P}} v_{\mathcal{P}}(\mathfrak{A}),$$

donde $\mathfrak{A} = \prod_{\mathcal{P}\in\mathbb{P}_L} \mathcal{P}^{v_{\mathcal{P}}(\mathfrak{A})}$.

Nota 1.3.9. Dado $x \in L^*$ existe un número finito de lugares $\mathcal{P}$ tal que $v_{\mathcal{P}}(x) \neq 0$.

Consideramos la función grado

$$d : D_L \to \mathbb{Z}$$

Si $\mathfrak{A}, \mathfrak{B} \in D_L$, entonces

$$d(\mathfrak{A}\mathfrak{B}) = \sum_{\mathcal{P}} f_{\mathcal{P}} v_{\mathcal{P}}(\mathfrak{A}\mathfrak{B}) = \sum_{\mathcal{P}} f_{\mathcal{P}} (v_{\mathcal{P}}(\mathfrak{A}) + v_{\mathcal{P}}(\mathfrak{B})) = \sum_{\mathcal{P}} f_{\mathcal{P}} v_{\mathcal{P}}(\mathfrak{A}) + \sum_{\mathcal{P}} f_{\mathcal{P}} v_{\mathcal{P}}(\mathfrak{B}) = d(\mathfrak{A}) + d(\mathfrak{B}).$$

Por lo tanto d es un homomorfismo de grupos. Además $\operatorname{Im} d = \{\mathfrak{A} \in D_L \mid d(\mathfrak{A}) \in \mathbb{Z}\} = m\mathbb{Z}$, $m \in \mathbb{N}$, es decir, $\operatorname{Im} d \cong \mathbb{Z}$.

Definición 1.3.10. Al conjunto

$$D_{L,0} = \ker d = \{\mathfrak{A} \in D_L \mid d(\mathfrak{A}) = 0\}$$

se le llama *grupo de divisores de L de grado* 0.

Definición 1.3.11. Dado $x \in L^*$, $(x)_L = \prod_{\mathfrak{P}} \mathfrak{P}^{v_{\mathfrak{P}}(x)}$ se llama *divisor principal* de x en L.
El conjunto

$$P_L = \{(x)_L \mid x \in L^*\}$$

es el *grupo de divisores principales* de L.

Tenemos la siguiente sucesión exacta corta.

$$1 \longrightarrow D_{L,0} \longrightarrow D_L \xrightarrow{d} m\mathbb{Z} \longrightarrow 0$$

Esto implica que $D_L/D_{L,0} = D_L/\ker d \cong \operatorname{Im} d \cong \mathbb{Z}$ y como $\mathbb{Z}$ es libre, de la sucesión exacta tenemos $D_L \cong D_{L,0} \oplus \mathbb{Z}$.

Como veremos más adelante, $P_L \subseteq D_{L,0}$, luego d induce un epimorfismo $\tilde{d} : D_{L,0}/P_L \to m\mathbb{Z}$ y

$$\ker \tilde{d} = \{\mathfrak{A} \text{ mód } P_L \mid d(\mathfrak{A}) = 0\} \cong D_{L,0}/P_L.$$

La función grado puede ser definida en una clase $C \in D_{L,0}/P_L$ como $\tilde{d}(C) = d(\mathfrak{A})$, donde $\mathfrak{A} \in C$. Esta definición no depende del representante $\mathfrak{A}$, pues si $\mathfrak{A}$ y $\mathfrak{B}$ determinan la misma clase C de $D_{L,0}/P_L$, entonces existe $x \in L^*$ tal que $\mathfrak{A} = \mathfrak{B}(x)_L$ y $d(\mathfrak{A}) = d(\mathfrak{B}) + d((x)_L) = d(\mathfrak{B}) + 0 = d(\mathfrak{B})$.

Definición 1.3.12. El *grado de una clase* $C \in D_{L,0}/P_L$ se define por $\tilde{d}(C) = d(\mathfrak{A})$, donde $\mathfrak{A}$ es un divisor que pertenece a C.

Nota 1.3.13. Si k es finito, el grupo $\frac{D_{L,0}}{P_L}$ es finito.

Demostración. Ver [17], ejercicio 3.6.26, pp. 91. □

Definición 1.3.14. El grupo

$$C_{L,0} = D_{L,0}/P_L$$

es el *grupo de clases de divisores de grado 0 de L*, también es llamado simplemente *grupo de clases de divisores de L* y

$$h_L := \left|\frac{D_{L,0}}{P_L}\right|$$

es el *número de clases de divisores de L.*

Sea

$$C_L = \frac{D_L}{P_L}.$$

Como $P_L < D_{L,0}$, se tiene la sucesión exacta corta:

$$1 \longrightarrow C_{L,0} \longrightarrow C_L \xrightarrow{\tilde{d}} m\mathbb{Z} \longrightarrow 0\,.$$

Aquí $m\mathbb{Z} \cong \mathbb{Z}$ y es libre de torsión. Por lo tanto

$$C_L \cong C_{L,0} \oplus \mathbb{Z}.$$

En particular C_L nunca es un grupo finito.
Ahora consideramos la sucesión exacta

$$1 \longrightarrow k^* \longrightarrow L^* \xrightarrow{i} P_L \longrightarrow 1$$

donde $i(x) = (x)_L$, entonces i es un epimorfismo, es decir, Im $i = P_L$ y en consecuencia la sucesión

$$1 \longrightarrow k^* \longrightarrow L^* \xrightarrow{i} D_L \xrightarrow{\pi} C_L \longrightarrow 1$$

es exacta, donde π es la proyección natural.
Ahora, $\ker i = \{x \in L^* \mid (x)_L = \eta\} = \{x \in L^* \mid v_\mathfrak{P}(x) = 0\ \forall \mathcal{P} \in D_L\}$. Entonces por el primer teorema de isomorfismo

$$P_L \cong L^*/k^*.$$

En lo que sigue, sea L un campo de funciones algebraicas sobre el campo finito $k = \mathbb{F}_q$ con q elementos como campo de constantes. Sea S un conjunto de divisores primos de L. Entonces

$$\Gamma(\mathfrak{A} \mid S) = \{x \in L \mid v_\mathfrak{P}(x) \geq v_\mathfrak{P}(\mathfrak{A})\ \forall \mathcal{P} \in S\}\,.$$

Se tiene que $\Gamma(\mathfrak{A} \mid S)$ es un espacio vectorial sobre k.

Nota 1.3.15. Si $\mathfrak{A} \mid \mathfrak{B}$, entonces $\Gamma(\mathfrak{B} \mid S) \subseteq \Gamma(\mathfrak{A} \mid S)$. También si $S \subseteq S_1$, entonces $\Gamma(\mathfrak{A} \mid S_1) \subseteq \Gamma(\mathfrak{A} \mid S)$. Y si $\mathfrak{A}$, $\mathfrak{B}$ son divisores tales que $\mathfrak{A}\mathfrak{B}^{-1} = \mathfrak{C} = \prod_{\mathfrak{P}} \mathfrak{P}^{v_\mathfrak{P}(\mathfrak{C})}$ es tal que $v_\mathfrak{P}(\mathfrak{C}) = 0$ para todo $\mathcal{P} \in S$, entonces $\Gamma(\mathfrak{A} \mid S) = \Gamma(\mathfrak{B} \mid S)$.

Ahora sea S fijo y consideremos un divisor $\mathfrak{A}$. Sea $\mathfrak{A}_0 := \prod_{\mathcal{P} \in S} \mathfrak{P}^{v_\mathfrak{P}(\mathfrak{A})}$. Entonces $\Gamma(\mathfrak{A}_0 \mid S) = \Gamma(\mathfrak{A} \mid S)$, es decir, $\mathfrak{A}_0$ tiene soporte en S y sus componentes son iguales a las de $\mathfrak{A}$.

Teorema 1.3.16. *Sea S un conjunto finito y supongamos $\mathfrak{A} \mid \mathfrak{B}$. Entonces*

$$\dim_k = \frac{\Gamma(\mathfrak{A} \mid S)}{\Gamma(\mathfrak{B} \mid S} = d(\mathfrak{B}_0) - d(\mathfrak{A}_0) = d(\mathfrak{B}_0\mathfrak{A}_0^{-1}).$$

Demostración. Ver [17], teorema 3.1.9, pp. 57. □

Definición 1.3.17. Sea $\mathbb{P}_L = \{\mathcal{P} \mid \mathcal{P} \text{ es un lugar de } L\}$. Sea $\mathfrak{A}$ un divisor de L. Definimos

$$\begin{aligned}\mathcal{L}(\mathfrak{A}) = \Gamma(\mathfrak{A} \mid \mathbb{P}_L) &= \{x \in L^* \mid \mathfrak{A} \mid (x)_L\} \cup \{0\} \\ &= \{x \in L \mid v_\mathfrak{P}(x) \geq v_\mathfrak{P}(\mathfrak{A}) \text{ para todo } \mathcal{P} \in \mathbb{P}_L\}.\end{aligned}$$

Se tiene que $\mathcal{L}(\mathfrak{A})$ es un k espacio vectorial. Y si $\mathfrak{A} \mid \mathfrak{B}$, $\mathcal{L}(\mathfrak{A}) \supseteq \mathcal{L}(\mathfrak{B})$.

Teorema 1.3.18. *Para cualquier divisor $\mathfrak{A}$, $\ell(\mathfrak{A}) = \dim_k \mathcal{L}(\mathfrak{A}) < \infty$. Si $\mathfrak{A} \mid \mathfrak{B}$, entonces $\ell(\mathfrak{A}) + d(\mathfrak{A}) \leq \ell(\mathfrak{B}) + d(\mathfrak{B})$.*

Demostración. Ver [17], teorema 3.1.11, pp. 59. □

Nota 1.3.19. Se tiene que $\mathcal{L}(\eta) = k$, pues si $x \in \mathcal{L}(\eta)$, entonces $v_\mathfrak{P}(x) \geq 0$ para todo $\mathcal{P}$. Si x fuera trascendente, existiría $\mathcal{P}$ tal que $v_\mathfrak{P}(x) < 0$. Entonces $x \in k$ y recíprocamente. En particular, tenemos

$$\ell(\eta) = 1.$$

Definición 1.3.20. Sea $x \in L\backslash\{0\}$. Entonces $(x)_L = \prod_{\mathcal{P}} \mathcal{P}^{v_\mathfrak{P}(x)} = \frac{\mathcal{Z}_x}{\eta_x}$, donde $\mathcal{Z}_x = \prod_{\mathcal{P},\, v_\mathfrak{P}(x)>0} \mathcal{P}^{v_\mathfrak{P}(x)}$ y $\eta_x = \prod_{\mathcal{P},\, v_\mathfrak{P}(x)<0} \mathcal{P}^{-v_\mathfrak{P}(x)}$. Decimos que $\mathcal{Z}_x$ es el *divisor de ceros* de x y η_x es el *divisor de polos* de x.

Teorema 1.3.21. *Si x es trascendente, $d(\mathcal{Z}_x) = d(\eta_x) = N = [L : k(x)]$.*

Demostración. Ver [17], teorema 3.2.7, pp. 62. □

Corolario 1.3.22. *Si $x \in L^*$, entonces $d((x)_L) = 0$.*

□

Observemos que como $d((x)_L) = 0$, tenemos $P_L \subseteq D_{L,0}$.

Proposición 1.3.23. *Si $x \in L$ es trascendente, entonces existe $Q \in \mathbb{Z}$ que depende únicamente de x, tal que $\ell(\eta_x^{-m}) + d(\eta_x^{-m}) \geq Q$ para todo $m \in \mathbb{Z}$.*

Demostración. Ver [17], proposición 3.3.1, pp. 67. □

Teorema 1.3.24. *(**Riemann**). Sea x un elemento trascendente de L y sea*

$$1 - g = \sup\{Q \mid \ell(\eta_x^{-m}) + d(\eta_x^{-m}) \geq Q \ \forall m \in \mathbb{Z}\}.$$

Entonces para cualquier divisor $\mathfrak{A} \in D_L$, se tiene $\ell(\mathfrak{A}) + d(\mathfrak{A}) \geq 1 - g$.

Demostración. Ver [17], teorema 3.3.2, pp. 67. □

Nota 1.3.25. Como $1 - g$ es la máxima cota inferior de $\{\ell(\mathfrak{A}) + d(\mathfrak{A}) \mid \mathfrak{A} \in D_K\}$, $g = g_L$ es independiente de x y se llama el *género* de L.

Ahora $\ell(\eta) + d(\eta) = 1 + 0 \geq 1 - g$. Por lo tanto

$$g \geq 0.$$

1.4. Adéles, diferenciales y el teorema de Riemann-Roch

Definición 1.4.1. Denotamos por $L_{\mathcal{P}}$ a la completación de L en el lugar $\mathcal{P}$. Una *repartición* o *adéle* es una función
$\varphi : \mathbb{P}_L \to \cup_{\mathcal{P} \in \mathbb{P}_L} L_{\mathcal{P}}$ dada por $\mathcal{P} \mapsto \varphi(\mathcal{P}) = \xi_{\mathcal{P}}$, tal que $\xi_{\mathcal{P}} \in L_{\mathcal{P}}$ y $v_{\mathcal{P}}(\xi_{\mathcal{P}}) = v_{\mathcal{P}}(\varphi(\mathcal{P})) \geq 0$ para casi todo $\mathcal{P}$.

Una repartición se puede escribir como $\xi = (\xi_{\mathcal{P}})_{\mathcal{P}}$. Al espacio de todas las reparticiones se le denota

$$\mathfrak{X} = \mathfrak{X}_L,$$

el cual es una k-álgebra de manera natural, ya que dados $a \in k$ y $\xi,\ \theta \in \mathfrak{X}$ se tiene:

- $(\xi + \theta)_{\mathcal{P}} = \xi_{\mathcal{P}} + \theta_{\mathcal{P}}$,
- $(\xi\theta)_{\mathcal{P}} = \xi_{\mathcal{P}} \cdot \theta_{\mathcal{P}}$,
- $(a \cdot \xi)_{\mathcal{P}} = a\xi_{\mathcal{P}}$.

Así pues $\mathfrak{X}$ es un espacio vectorial y a la vez un anillo.
Ahora sea $\phi : L \hookrightarrow \mathfrak{X}$ dado por $x \mapsto \phi(x) = \xi_x$ y $(\xi_x)_{\mathcal{P}} = x$ para todo $\mathcal{P} \in \mathbb{P}_L$.

Las valuaciones $v_{\mathcal{P}}$ de L se pueden extender a $\mathfrak{X}$ de la siguiente forma:
Dado $\xi \in \mathfrak{X}$, se tiene $v_{\mathcal{P}}(\xi) := v_{\mathcal{P}}(\xi_{\mathcal{P}})$. Se cumple lo siguiente para $\xi,\ \theta \in \mathfrak{X}$:

- $v_{\mathfrak{P}}(\theta \cdot \xi) = v_{\mathfrak{P}}(\theta) + v_{\mathfrak{P}}(\xi)$,
- $v_{\mathfrak{P}}(\xi_x) = v_{\mathfrak{P}}((\xi_x)_{\mathfrak{P}}) = v_{\mathfrak{P}}(x)$.

Definición 1.4.2. Sean $\mathfrak{A}$ un divisor y ξ una repartición. Se dice que $\mathfrak{A}$ *divide* a ξ y se pone $\mathfrak{A} \mid \xi$ si $v_{\mathfrak{P}}(\xi) \geq v_{\mathfrak{P}}(\mathfrak{A})$ para todo $\mathcal{P} \in \mathbb{P}_L$.

Dos reparticiones $\xi,\ \theta$ son *congruentes módulo* $\mathfrak{A}$ y se pone $\xi \equiv \theta \pmod{\mathfrak{A}}$ si $\mathfrak{A} \mid \xi - \theta$.

Sea

$$\begin{aligned}\mathfrak{X}(\mathfrak{A}) &:= \{\xi \in \mathfrak{X} \mid \mathfrak{A} \mid \xi\} \\ &= \{\xi \in \mathfrak{X} \mid v_{\mathfrak{P}}(\xi) \geq v_{\mathfrak{P}}(\mathfrak{A}) \text{ para todo } \mathcal{P} \in \mathbb{P}_L\}.\end{aligned}$$

Entonces $\mathfrak{X}(\mathfrak{A})$ es un k-espacio vectorial.

Tenemos ahora el siguiente resultado:

Teorema 1.4.3. *Si $\mathfrak{A}$ y $\mathfrak{B}$ son divisores tales que $\mathfrak{A} \mid \mathfrak{B}$, entonces $\mathfrak{X}(\mathfrak{A}) \supseteq \mathfrak{X}(\mathfrak{B})$ y*

$$\dim_k \frac{\mathfrak{X}(\mathfrak{A})}{\mathfrak{X}(\mathfrak{B})} = d(\mathfrak{B}) - d(\mathfrak{A}).$$

Demostración. Ver [17], teorema 3.3.16, pp. 71. □

Sea L un campo de funciones. Sean $\mathfrak{A}$ y $\mathfrak{B}$ divisores tales que $\mathfrak{A} \mid \mathfrak{B}$. Entonces la siguiente sucesión de k espacios vectoriales es exacta.

$$0 \longrightarrow \frac{\mathcal{L}(\mathfrak{A})}{\mathcal{L}(\mathfrak{B})} \longrightarrow \frac{\mathfrak{X}(\mathfrak{A})}{\mathfrak{X}(\mathfrak{B})} \longrightarrow \frac{\mathfrak{X}(\mathfrak{A}) + L}{\mathfrak{X}(\mathfrak{B}) + L} \longrightarrow 0$$

En particular

$$\begin{aligned}\dim_k \frac{\mathfrak{X}(\mathfrak{A}) + L}{\mathfrak{X}(\mathfrak{B}) + L} &= (\ell(\mathfrak{B}) + d(B)) - (\ell(\mathfrak{A}) + d(\mathfrak{A})) \\ \dim_k \frac{\mathfrak{X}}{\mathfrak{X}(\mathfrak{A}) + L} &= \delta(\mathfrak{A}^{-1}) = \ell(\mathfrak{A}) + d(\mathfrak{A}) + g - 1.\end{aligned}$$

Definición 1.4.4. Sea L/k un campo de funciones arbitrario. Una *diferencial* o *diferencial de Weil en L*, ω, es una función k lineal $\omega : \mathfrak{X}_L \to k$ tal que existe un divisor $\mathfrak{A}$ tal que $\ker \omega \supseteq \mathfrak{X}_L(\mathfrak{A}) + L$. En este caso decimos $\mathfrak{A}^{-1} | \omega$. En otras palabras, $\mathfrak{B} \mid \omega$ si y sólo si $\omega(\mathfrak{X}(\mathfrak{B}^{-1}) + L) = 0$.

Definición 1.4.5. La diferencial ω se llama *holomorfa* o *del primer tipo* si $\eta \mid \omega$.

Si $\mathfrak{B} \mid \mathfrak{A}$, entonces $\mathfrak{A}^{-1} \mid \mathfrak{B}^{-1}$. Con esto se tiene $\mathfrak{X}(\mathfrak{B}^{-1}) + L \subseteq \mathfrak{X}(\mathfrak{A}^{-1}) + L$. Por lo tanto si $\mathfrak{A} \mid \omega$, entonces $\mathfrak{B} \mid \omega$.

Sea

$$D(\mathfrak{A}) = \{\omega \mid \omega \text{ es diferencial y } \mathfrak{A} \mid \omega\}.$$

Entonces

$$D(\mathfrak{A}) \cong \left(\frac{\mathfrak{X}}{\mathfrak{X}(\mathfrak{A}^{-1}) + L}\right).$$

Luego $\dim_k D(\mathfrak{A}) = \dim_k \dfrac{\mathfrak{X}}{\mathfrak{X}(\mathfrak{A}^{-1}) + L} = \delta(\mathfrak{A}) = \ell(\mathfrak{A}^{-1}) + d(\mathfrak{A}^{-1}) + g - 1$.

Se tienen las siguientes propiedades:

1. $\dim_k D(\eta) = \delta(\eta) = g$.
2. Si $\mathfrak{A}_1 | \omega_1,\ \mathfrak{A}_2 | \omega_2$, sean $\omega = \omega_1 + \omega_2$ y $\mathfrak{A} = \text{mcd}(\mathfrak{A}_1, \mathfrak{A}_2)$. Entonces $\mathfrak{A} \mid \omega$.
3. Si ω es una diferencial y $x \in L$, se define $(x\omega)(\tau) := \omega(x\tau)$, con $\tau \in \mathfrak{X}$. Observemos que si $\mathfrak{A} \mid \omega$ y $x \neq 0$, entonces $(x)_L \mathfrak{A} \mid x\omega$. Entonces se tienen las siguientes propiedades:
   - $(xy)\omega = x(y\omega)$,
   - $(x + y)\omega = x\omega + y\omega$,
   - $x(\omega_1 + \omega_2) = x\omega_1 + x\omega_2$.

   Con esto, el conjunto de las diferenciales en L es un L espacio vectorial.

Dada una diferencial $\omega_0 \neq 0$, toda diferencial ω se puede escribir de manera única como $\omega = x\omega_0$ para algún $x \in L$. Por lo tanto, la dimensión sobre L del espacio de diferenciales en L es igual a uno.

Teorema 1.4.6. *Para cada diferencial $\omega \neq 0$, existe un único divisor $(\omega)_L$ tal que $\mathfrak{A} \mid \omega$ si y sólo si $\mathfrak{A} \mid (\omega)_L$.*

Demostración. Ver [17], teorema 3.4.9, pp. 78. □

Sea $\omega \neq 0$ y $C := \overline{(\omega)}_L \in D_L/P_L = C_L$. Si $\mathfrak{A} \in C$, entonces $\mathfrak{A} = (x)_L(\omega)_L = (x\omega)_L$ para algún $x \in L^*$. Por lo tanto todos los elementos de C son divisores de diferenciales. Por otro lado toda diferencial es de la forma $x\omega$, con $x \in L$, la cual tiene divisor $(x\omega)_L = (x)_L(\omega)_L$. Entonces $C = \{(\omega)_L \mid \omega \text{ es diferencial no cero}\}$. A $C = W$ se le llama la *clase canónica*.

Definición 1.4.7. Sean C una clase y $\mathfrak{A} \in C$. Si $\mathfrak{A}_1, \ldots, \mathfrak{A}_n \in C$, con $\dfrac{\mathfrak{A}_i}{\mathfrak{A}} = (x_i)_L$ para $1 \leq i \leq n$. Se dice que $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$ son *linealmente independientes* si $x_1, \ldots, x_n$ son linealmente independientes sobre k.

Esta definición es independiente del divisor $\mathfrak{A}$ y de los elementos $x_1, \ldots, x_n$ seleccionados.

Definición 1.4.8. Se define

$$N(C) = \text{ máximo número de divisores enteros de } C \text{ linealmente independientes.}$$

Se tiene la siguiente proposición:

Proposición 1.4.9. *$N(C) = \ell(\mathfrak{A}^{-1})$ para todo $\mathfrak{A} \in C$. En particular $N(C) < \infty$.*

Demostración. Ver [17], proposición 3.5.3, pp. 82. □

Ahora veremos el teorema de Riemann-Roch, el cual se origina de la teoría de superficies de Riemann.

Teorema 1.4.10. ***(Riemann-Roch)*** *Sea C cualquier clase. Se tiene*

$$N(C) = d(C) - g + 1 + N(WC^{-1}),$$

con W la clase canónica. Equivalentemente, para cualquier divisor $\mathfrak{A}$,

$$\ell(\mathfrak{A}^{-1}) = d(\mathfrak{A}) - g + 1 + \ell((\omega)_L^{-1}\mathfrak{A})$$

con ω cualquier diferencial no cero.

En otras palabras $\delta(\mathfrak{A}) = \ell(\mathfrak{A}^{-1}) + d(\mathfrak{A}^{-1}) + g - 1 = \ell((\omega)_L^{-1}\mathfrak{A}) = N(WC^{-1})$, para todo $\mathfrak{A} \in C$.

Demostración. Dado $\mathfrak{A} \in C$,

$$N(C) = \mathfrak{A}^{-1} = d(\mathfrak{A}) - g + 1 + \delta(\mathfrak{A}).$$

Además $\delta(\mathfrak{A}) = \dim_k D(\mathfrak{A})$, donde

$$D(\mathfrak{A}) = \{\omega \mid \omega \neq 0,\ \mathfrak{A} \mid \omega\} \cup \{0\} = \left\{\omega \mid \omega \neq 0,\ (\omega)_L\mathfrak{A}^{-1} \text{ es divisor entero}\right\} \cup \{0\}.$$

Por lo tanto $\delta(\mathfrak{A})$ es el máximo número de diferenciales $\omega_1, \ldots, \omega_n$ linealmente independientes sobre k y tales que $(\omega_1)_L\mathfrak{A}^{-1}, \ldots, (\omega_n)_L\mathfrak{A}^{-1}$ son divisores enteros. Es decir

$$\delta(\mathfrak{A}) = \dim_k \frac{\mathfrak{X}}{\mathfrak{X}(\mathfrak{A}^{-1}) + L} = N(WC^{-1}) = \ell((\omega)_L^{-1}\mathfrak{A}).$$

□

Corolario 1.4.11. *Sea W la clase canónica. Entonces $g = N(W)$ = máximo número de diferenciales holomorfas linealmente independientes y $d(W) = 2g - 2$. En particular, la dimensión de las diferenciales holomorfas es g.*

Demostración. $\ell(\mathfrak{A}^{-1}) = d(\mathfrak{A}) - g + 1 + \ell((\omega)^{-1}\mathfrak{A})$. Sea $\mathfrak{A} = \eta$, entonces $1 = 0 - g + 1 + N(W)$. Por lo tanto $N(W) = g$.
Sea ahora $\mathfrak{A} \in W^{-1}$, luego $\mathfrak{A}^{-1} \in W$. Entonces $N(W) = g = d(W) - g + 1 + N(WW^{-1}) = d(W) - g + 1 + N(P_L)$. Luego $N(P_L) = \ell(\eta) = 1$. Esto implica que $d(W) = g + g - 1 - 1 = 2g - 2$. □

Corolario 1.4.12. *Si $\mathfrak{A}$ es un divisor tal que $d(\mathfrak{A}) > 2g-2$ o bien $d(\mathfrak{A}) = 2g-2$ y $\mathfrak{A} \notin W$, entonces*

$$\ell(\mathfrak{A}^{-1}) = d(\mathfrak{A}) - g + 1.$$

En particular,

$$\ell(\mathfrak{A}^{-1}) \geq g - 1.$$

Demostración. Si $d(\mathfrak{A}) > 2g - 2$, entonces $d(W^{-1}\mathfrak{A}) > 2g - 2 - (2g - 2) = 0$. Luego $\ell(W^{-1}\mathfrak{A}) = 0$. Ahora si $d(\mathfrak{A}) = 2g - 2$ y $\mathfrak{A} \notin W$, entonces $d(W^{-1}\mathfrak{A}) = 0$ y $W^{-1}\mathfrak{A} \neq P_L$. Como $W^{-1}\mathfrak{A}$ es de grado cero, pero $W^{-1}\mathfrak{A} \neq \eta$, se tiene $\ell(W^{-1}\mathfrak{A}) = 0$.

Se concluye en cualquier caso que $\ell(\mathfrak{A}^{-1}) = d(\mathfrak{A}) - g + 1$. □

Corolario 1.4.13. *Si W' es una clase y g' es un entero tales que $N(C) = d(C) - g' + 1 + N(W'C^{-1})$ para toda clase C, entonces $W' = W$ y $g' = g$. Es decir, W y g están determinadas por el teorema de Riemann-Roch.*

Demostración. Ver [17], corolario 3.5.7, pp. 84. □

Corolario 1.4.14. *Para cualquier clase C, se tiene $N(C) \leq \max\{0, d(C) + 1\}$.*

Demostración. Si $N(C) = 0$, ya terminamos. Supongamos que $N(C) > 0$, entonces existe un divisor entero $\mathfrak{A} \in C$ tal que

$$N(C) = N(P_L\mathfrak{A}) \leq N(P_L) + d(\mathfrak{A}) = 1 + d(\mathfrak{A}) = 1 + d(C).$$

□

Ejemplo 1.4.15. Sea $K = k(T)$ el campo de funciones racionales. Sea $\mathfrak{A}$ un divisor de grado 0, es decir, $\mathfrak{A} \in D_{L,0}$. Se escribe $\mathfrak{A} = \prod_{i=1}^{r} \mathfrak{p}_i^{\alpha_i}$, donde cada $\mathfrak{p}_i$ $(1 \leq i \leq r)$ es un divisor primo de K. Se tiene

$$\sum_{i=1}^{r} \alpha_i d(\mathfrak{p}_i) = d(\mathfrak{A}) = 0.$$

Elegimos $\mathfrak{p}_r$ como $\mathfrak{p}_\infty$, esto es, el lugar correspondiente a la valuación v_∞. Cada $\mathfrak{p}_i$, $(1 \leq i \leq r-1)$ está asociado a algún polinomio irreducible $P_i(T)$ de $k[T]$. Se tiene $d(\mathfrak{p}_\infty) = 1$. Por lo tanto

$$\alpha_r = -\sum_{i=0}^{r} \alpha_i \text{gr } P_i.$$

Ahora, para una valuación $v \neq v_{P_i}, v_\infty$, tenemos $v(P_i) = 0$, $v_{P_i}(P_i) = 1$ y $v_\infty(P_i) = -\text{gr } P_i$.
Por lo tanto el divisor de P_i es $(P_i)_K = \dfrac{\mathfrak{p}_i}{\mathfrak{p}_\infty^{\text{gr } P_i}}$, donde $\mathfrak{p}_i$ es el divisor correspondiente a v_{P_i}.
Por lo tanto

$$\left(\prod_{i=1}^{r-1} (P_i(T))^{\alpha_i}\right)_K = \prod_{i=1}^{r-1} (P_i(T))^{\alpha_i} \prod_{i=1}^{r-1} \frac{\mathfrak{p}_i^{\alpha_i}}{\mathfrak{p}_\infty^{\alpha_i \text{ gr } P_i}} = \left(\prod_{i=1}^{r-1} \mathfrak{p}_i^{\alpha_i}\right) \mathfrak{p}_\infty^{-\sum_{i=1}^{r-1} \alpha_i \text{ gr } P_i} = \prod_{i=1}^{r-1} \mathfrak{p}_i^{\alpha_i} = \mathfrak{A},$$

es decir, $\mathfrak{A}$ es principal ya que $\mathfrak{A} = (\alpha(T))_K$, donde $\alpha(T) = \prod_{i=1}^{r-1} P_i(T)^{\alpha_i} \in k(T)^*$.

Notemos que si $r = 0$, entonces

$$\mathfrak{A} = \eta = (1)_K,\ 1 \in k^*.$$

Con esto se tiene que $D_{K,0} = P_K$.
Por lo tanto $C_{K,0} = D_{K,0}/P_K = \{1\}$ y así

$$h_K = 1.$$

Con esto se ha probado que un campo de funciones racionales tiene número de clases de divisores igual a 1.
Por último, como $d(\mathfrak{p}_\infty) = 1$, la función grado es suprayectiva, es decir, $d(D_K) = \mathbb{Z}$ y $C_K \cong \mathbb{Z}$.

Proposición 1.4.16. *Si el campo de constantes de L es un campo finito, entonces el número de clases de divisores de L, h_L, es finito.*

Demostración. Sea $n \in \mathbb{N}$, $n \geq g$. Sea $\mathfrak{B} \in D_L$ tal que $d(\mathfrak{B}) = n$ y sea $C_{L,n} := \{C \in C_L \mid d(C) = n\}$. El mapeo $C_{L,0} \to C_{L,n}$ dado por $[\mathfrak{A}] \mapsto [\mathfrak{A} + \mathfrak{B}]$ es biyectivo. Así, para probar que $h_L = |C_{L,0}|$ es finito, basta probar que $C_{L,n}$ es finito. Sea $C \in C_{L,n}$. Como $d(C) = n > g$, tenemos por el teorema de Riemann-Roch que $N(C) \geq d(C) - g + 1 = n - g + 1 > g - g + 1 = 1$. Por lo tanto, hay al menos un divisor entero $\mathfrak{A}$ en C. Tenemos

$$\mathfrak{A} = \prod_{\mathcal{P} \in \mathbb{P}_L} \mathcal{P}^{\alpha_\mathcal{P}},$$

con $\alpha_\mathcal{P} \geq 0$. Luego, basta probar que $S := \{\mathcal{P} \in \mathbb{P}_L \mid d(\mathcal{P}) \leq n\}$ es finito.

Sabemos que existe $T \in L$, elemento trascendente, de manera que $[L : K] < \infty$, donde $K = \mathbb{F}_q(T)$. Sea $S_0 := \{\mathfrak{p} \in \mathbb{P}_L \mid d(\mathfrak{p}) \leq n\}$. Dado $\mathcal{P} \in S$ existe un único divisor $\mathfrak{p} \in S_0$ tal que $\mathcal{P} \mid \mathfrak{p}$ y dado $\mathfrak{p} \in S_0$ existen a lo más un número finito de $\mathcal{P} \in S$, encima de $\mathfrak{p}$.

Por lo tanto sólo debemos ver que S_0 es finito. Como los lugares de $\mathbb{F}_q(T)$, (excepto el polo de T), corresponden a polinomios mónicos irreducibles $P(T) \in \mathbb{F}_q[T]$ del mismo grado, la finitud de S_0 se sigue. □

Capítulo 2

Campos ciclotómicos

Dado $K = \mathbb{F}_q(T)$ un campo de funciones racionales, se define el módulo de Carlitz-Hayes Λ_M y se obtienen algunas de sus propiedades, las cuales son necesarias para definir el campo de funciones ciclotómico $K_M = K(\Lambda_M)$. Se observa que la extensión K_M/K es de Galois, abeliana y geométrica. Posteriormente se trabaja el tema de ramificación en $\mathfrak{p}_\infty$ y se tiene que $\mathfrak{p}_\infty$ es moderadamente ramificado en K_M/K. Finalmente se obtiene el subcampo real maximal K_M^+ de K_M.

2.1. Campos de funciones ciclotómicos

Sea $K = \mathbb{F}_q(T)$ el campo de funciones racionales sobre el campo finito $\mathbb{F}_q$ con q elementos y sea $R_T = \mathbb{F}_q[T]$ el anillo de polinomios. Sea $\bar{K}$ una cerradura algebraica de K.

Sea $A = End_{\mathbb{F}_q} = \left\{\varphi : \bar{K} \to \bar{K} \mid \varphi(a+b) = \varphi(a) + (b),\ \varphi(\alpha a) = \alpha\varphi(a)\ \forall \alpha \in \mathbb{F}_q \text{ y } \forall a, b \in \bar{K}\right\}$.

Entonces A es una $\mathbb{F}_q$-álgebra que consiste de los $\mathbb{F}_q$ endomorfismos del grupo aditivo de $\bar{K}$.

Vamos a considerar dos elementos de A:

1. Sea φ el automorfismo de Frobenius de $\bar{K}$ sobre $\mathbb{F}_q$, es decir $\varphi : \bar{K} \to \bar{K}$ está dado por $u \mapsto u^q$.

2. Sea μ_T la multiplicación por T, esto es, $\mu_T : \bar{K} \to \bar{K}$ está dado por $u \mapsto Tu$.

Si $f(T) \in R_T = \mathbb{F}_q[T]$, la sustitución $T \to \varphi + \mu_T$ es el endomorfismo dado como sigue:
Si $f(T) = a_n T^n + \cdots + a_1 T + a_0$, $f(\varphi + \mu_T)(u) = a_n(\varphi + \mu_T)^n(u) + a_{n-1}(\varphi + \mu_T)^{n-1}(u) + \cdots + a_1(\varphi + \mu_T)(u) + a_0(u)$, es decir, $\xi : R_T \to A$ está dado por $\xi(T) = \varphi + \mu_T$ y $\xi(f(T)) = f(\varphi + \mu_T)$.

La función ξ es un homomorfismo de anillos y $(\varphi+\mu_T)^0 = \mathbf{1}_{\bar{K}}$, por lo tanto $(\varphi+\mu_T)^0(u) = \mathbf{1}(u) = u$. Así pues $\bar{K}$ obtiene una estructura de R_T-módulo.

Si $u \in \bar{K}$ y $M \in R_T$, denotamos $u^M := M(\varphi+\mu_T)(u)$, es decir, $M \circ u = \xi(M)(u) = M(\varphi+\mu_T)(u)$.

Notemos que dados $u \in \bar{K}$ y $M, N \in R_T$, se tiene $u^{M+N} = u^M + u^N$ y $\left(u^M\right)^N = u^{MN} = u^{NM} = \left(u^N\right)^M$.

Si $\alpha \in \mathbb{F}_q$, entonces $u^\alpha = \alpha(\varphi+\mu_T)(u) = \alpha(u) = \alpha u$. Por lo tanto la estructura de R_T-módulo respeta la estructura de $\mathbb{F}_q$-álgebra de $\bar{K}$.

Observación: $(\varphi \circ \mu_T)(u) = \varphi(Tu) = T^q u^q$ y $\left(\mu_T^q \circ \varphi\right)(u) = \mu_T^q(u^q) = T^q u^q$, entonces $\varphi \circ \mu_T = \mu_T^q \circ \varphi$. En particular $\varphi \circ \mu_T \neq \mu_T \circ \varphi$.

Teorema 2.1.1. *Si $M = a_d T^d + \cdots + a_1 T + a_0$ con $a_d \neq 0$. Entonces $u^M = \sum_{i=0}^{d} \begin{bmatrix} M \\ i \end{bmatrix} u^{q^i}$ donde $\begin{bmatrix} M \\ i \end{bmatrix}$ es un polinomio en R_T de grado $(d-i)\,q^i$. Además $\begin{bmatrix} M \\ 0 \end{bmatrix} = M$, $\begin{bmatrix} M \\ d \end{bmatrix} = a_d$ y $\begin{bmatrix} M \\ i \end{bmatrix} = a_i + \sum_{n=i+1}^{d} a_n h_n(i,T)$ donde cada $h_n(i,T) = \sum_{0 \le j_1 \le \ldots \le j_{n-1} \le i} T^{q^{j_1}+q^{j_2}+\cdots+q^{j_{n-1}}}$ es un polinomio de grado $(n-i)q^i$.*

Demostración. Primero veremos el caso u^{T^n}. Por inducción sobre n veremos que

$$u^{T^n} = \sum_{i=0}^{n-1} \left(\sum_{0 \le j_1 \le \ldots \le j_{n-1} \le i} T^{q^{j_1}+q^{j_2}+\cdots+q^{j_{n-1}}} \right) u^{q^i} + u^{q^n},$$

es decir

$$u^{T^n} = \sum_{i=0}^{n-1} h_n(i,T) u^{q^i} + u^{q^n}. \tag{2.1}$$

Para $n = 1$, tenemos $u^T = (\varphi+\mu_T)(u) = u^q + Tu = Tu + u^q$ y $\sum_{i=0}^{n-1} h_n(i,T)\,u^{q^i} + u^{q^n} = h_1(0,T)\,u^{q^0} + u^q$, $h_1(0,T) = \sum_{0 \le j_1 \le \ldots \le j_1 = j_{1-0} \le 0} T^{q^{j_1}+\cdots+q^{j_{1-0}}} = T^{q^0} = T^1 = T$.

Por lo tanto la ecuación (2.1) se cumple para $n = 1$.

Supongamos que se cumple la ecuación (2.1) para $n \ge 1$. Para $n+1$ tenemos

$$u^{T^{n+1}} = \left(u^{T^n}\right)^T = (\mu_T + \varphi)\left(u^{T^n}\right) = Tu^{T^n} + \left(u^{T^n}\right)^q = \sum_{i=0}^{n} \left(\sum_{0 \le j_1 \le \ldots \le j_{n-i+1} \le i} T^{q^{j_1}+q^{j_2}+\cdots+q^{j_{n-i+1}}} u^{q^i} \right) + u^{q^{n+1}}.$$

Por lo tanto $u^{T^{n+1}} = \sum_{i=0}^{n} h_{n+1}(i,T)\,u^{q^i} + u^{q^{n+1}}$ y la ecuación (2.1) se cumple para $u^{T^{n+1}}$.
Definimos $h_n(i,T) = 1$ si $i = n$ y $h_n(i,T) = 0$ si $i > n$.

Ahora sea $M = a_0 + a_1T + \cdots + a_dT^d = \sum_{n=0}^{d} a_nT^n$, donde $a_n \neq 0$. Entonces

$$u^M = u^{\sum_{n=0}^{d} a_nT^n} = \sum_{n=0}^{d} a_n u^{T^n} = \sum_{n=0}^{d} a_n \left(\sum_{i=0}^{n-1} h_n(i,T) u^{q^i} + u^{q^n} \right)$$
$$= \sum_{n=0}^{d} a_n \left(\sum_{i=0}^{n} a_n h_n(i,T) u^{q^i} \right) = \sum_{i=0}^{d} \left(\sum_{n=i}^{d} a_n h_n(i,T) \right) u^{q^i}$$

Por lo tanto para $0 < i < d$ tenemos:

$$\begin{bmatrix} M \\ i \end{bmatrix} = \sum_{n=i}^{d} a_n h_n(i,T) = a_i + \sum_{n=i+1}^{d} a_n h_n(i,T).$$

Finalmente

$$\begin{bmatrix} M \\ 0 \end{bmatrix} = \sum_{n=0}^{d} a_n h_n(0,T) = \sum_{n=0}^{d} a_n T^n = M$$
$$\begin{bmatrix} M \\ d \end{bmatrix} = \sum_{n=0}^{d} a_n h_n(d,T) = a_d h_d(d,T) = a_d$$

□

La extensión se visualiza como sigue:

$$\begin{array}{ccc} & & \bar{K} \\ & & | \\ R_T = \mathbb{F}_q[T] & \text{——} & K = \mathbb{F}_q(T) \end{array}$$

Definición 2.1.2. Sea Λ_M el conjunto de elementos en $\bar{K}$ correspondientes a los elementos de M torsión de $\bar{K}$, es decir, $\Lambda_M = \left\{ u \in \bar{K} \mid u^M = 0 \right\}$= conjunto de ceros del polinomio u^M en u. Λ_M es llamado el *módulo de Carlitz-Hayes de M*.

Proposición 2.1.3. *Λ_M es un R_T-submódulo de $\bar{K}$.*

Demostración. Como R_T es un anillo conmutativo, si $u \in \Lambda_M$ y $N \in R_T$, se tiene $N \circ u = u^N \in \Lambda_M$ pues $M \circ u^N = \left(u^N\right)^M = u^{NM} = u^{MN} = \left(u^M\right)^N = N \circ \left(u^M\right) = N \circ (0) = 0$. Por lo tanto Λ_M es un R_T-módulo de $\bar{K}$. □

Nota 2.1.4. Si $\alpha \in \mathbb{F}_q^*$, entonces $\Lambda_M = \Lambda_{\alpha M}$, pues $u^{\alpha M} = \left(u^M\right)^\alpha = \alpha \circ \left(u^M\right) = 0 \Leftrightarrow u^M = 0$.

De esto siempre podemos considerar, sin pérdida de generalidad, polinomios mónicos.

Proposición 2.1.5. *u^M es un polinomio separable en u de grado q^d, donde $M \in R_T$ es de grado d. Por tanto Λ_M es un $\mathbb{F}_q$-espacio vectorial de dimensión d.*

Demostración. Sea $M = a_d T^d + \cdots + a_1 T + a_0$. Entonces $u^M = \sum_{i=0}^{d} \begin{bmatrix} M \\ i \end{bmatrix} u^{q^i}$. Por lo tanto $\frac{d}{du}\left(u^M\right) = \begin{bmatrix} M \\ 0 \end{bmatrix} = M \neq 0$, donde $\frac{d}{du}\left(u^M\right)$ es constante respecto a u. Así u^M es un polinomio separable de grado q^d. Por lo tanto $|\Lambda_M| = \mathrm{gr}_u u^M = q^d$. Como Λ_M es un $\mathbb{F}_q$-módulo tenemos $\dim_{\mathbb{F}_q} \Lambda_M = d$. □

Proposición 2.1.6. *Si $M = \prod_{i=1}^{r} P_i^{\alpha_i}$, entonces $\Lambda_M \cong \bigoplus_{i=1}^{r} \Lambda_{P_i^{\alpha_i}}$ como R_T-módulos.*

Demostración. Observemos que Λ_M es un R_T-módulo y que R_T es un dominio de ideales principales.

Todo R_T módulo de torsión A se descompone como $A = \bigoplus_P A(P)$, donde la suma recorre los elementos primos de R_T y $A(P) = \{a \in A \mid P^n \circ a = 0 \text{ para algún } n \in \mathbb{N}\}$.

En nuestro caso $A = \Lambda_M$. Entonces

$$\begin{aligned} A(P) &= \left\{u \in \Lambda_M | u^{P^n} = 0 \text{ para algún } n \in \mathbb{N}\right\} \\ &= \begin{cases} 0 & \text{if } P \notin \{P_1, \dots P_r\}, \\ \Lambda_{P_i^{\alpha_i}} & \text{si } P = P_i \; i \leq i \leq r. \end{cases} \end{aligned}$$

Luego $\Lambda_M \cong \bigoplus_{i=1}^{r} \Lambda_{P_i^{\alpha_i}}$. □

Proposición 2.1.7. *Si $M = P^n$, con $P \in R_T$ irreducible y $n \in \mathbb{N}$. Entonces Λ_M es un R_T-módulo cíclico.*

Demostración. Por inducción sobre n. Para $n = 1$, sea $\xi \in \Lambda_P \setminus \{0\}$. Sea $\phi : R_T \to \Lambda_P$ dado por $N \mapsto \xi^N$. Entonces $\phi \neq 0$, ya que $\phi(1) = \xi^1 = \xi \neq 0$. Por otro lado $\phi(P) = \xi^P = 0$, entonces $P \in \ker\phi$ y así $(P) \subseteq \ker\phi$. Como R_T es dominio de ideales principales y P es un polinomio irreducible no cero, (P) es maximal. Por lo tanto, de $(P) \subseteq \ker\phi \subsetneq R_T$, concluimos $(P) = \ker\phi$. Esto implica que $R_T/(P) = R_T/\ker\phi \cong \phi(R_T)$ es submódulo de Λ_P. Por otro lado $|\phi(R_T)| = |R_T/\ker\phi| = |R_T/(P)| = q^d = |\Lambda_P|$, donde d es el grado de P. Entonces $\phi(R_T) = \Lambda_P$ y ϕ es suprayectivo. Luego $\Lambda_P \cong R_T/(P)$.

Λ_P es cíclico por las siguientes razones:

- $\Lambda_P = R_T \cdot \xi = \left\{\xi^N \mid N \in R_T\right\} = \phi(R_T)$
- En general $R_T/(S)$ es un R_T-módulo cíclico con generador $1 + (S)$ y recíprocamente, si $A = R_T \cdot a$ es R_T-módulo cíclico, $A \cong R_T/(I)$ donde $I = \{N \in R_T \mid N \cdot a = 0\}$ es el anulador de a.

Supongamos que el resultado es cierto para $n \geq 1$. Sea $\theta : \Lambda_{P^{n+1}} \to \Lambda_{P^n}$ dado por $u \mapsto u^P$. Entonces θ es un R_T-homomorfismo y $\ker\theta = \Lambda_P$. Por lo tanto $\Lambda_{P^{n+1}}/\Lambda_P \cong \theta(\Lambda_{P^{n+1}})$ submódulo de Λ_{P^n} y $|\theta(\Lambda_{P^{n+1}})| = |\Lambda_{P^{n+1}}/\Lambda_P| = \dfrac{q^{d(n+1)}}{q^d} = q^{nd} = |\Lambda_{P^n}|$ por lo tanto θ es suprayectiva y $\Lambda_{P^{n+1}/\Lambda_P} \cong \Lambda_{P^n}$.

Sea $\lambda \in \Lambda_{P^{n+1}}$ tal que $\theta(\lambda) = \lambda^P$ sea generador de Λ_{P^n} como R_T-módulo. Sea $\mu \in \Lambda_{P^{n+1}}$, $\theta(\mu) = \mu^P = \left(\lambda^P\right)^A$ para algún $A \in R_T$. Como $\mu^P - \lambda^{PA} = \left(\mu - \lambda^A\right)^P = 0$, tenemos $\mu - \lambda^A \in \ker\theta = \Lambda_P$. Como $\theta\left(\lambda^{P^n}\right) = \lambda^{P^{n+1}} = 0$ entonces $\lambda^{P^n} \in \Lambda_P$.

Ahora $\lambda^{P^n} \neq 0$ pues si no fuera así, tendríamos $\left(\lambda^P\right)^{P^{n-1}} = \left(\lambda^{P^n}\right) = 0$, pero λ^P es generador de Λ_{P^n}, por lo que $\left(\lambda^P\right)^{P^{n-1}} \neq 0$. Por lo tanto λ^{P^n} es generador de Λ_P y como $\mu - \lambda^A \in \Lambda_P$, existe $B \in R_T$ tal que $\mu - \lambda^A = \left(\lambda^{P^n}\right)^B$, luego $\mu = \lambda^{P^n B} + \lambda^A = \lambda^{A + P^n B} \in \langle\lambda\rangle$. Entonces λ genera a $\Lambda_{P^{n+1}}$ como R_T-módulo y con esto $\Lambda_{P^{n+1}}$ es R_T-módulo cíclico. □

Teorema 2.1.8. *Para $M \in R_T \setminus \{0\}$, $\Lambda_M \cong R_T/(M)$ como R_T-módulos. En particular Λ_M es R_T-módulo cíclico.*

Demostración. Por la proposición 2.1.6, $\Lambda_M \cong \bigoplus_{i=1}^{r} \Lambda_{P_i^{\alpha_i}}$ donde $M = \prod_{i=1}^{r} P_i^{\alpha_i}$. Por la proposición 2.1.7, cada $\Lambda_{P_i^{\alpha_i}}$ es R_T-cíclico y $\Lambda_{P_i^{\alpha_i}}$ es la P_i componente primaria de Λ_M. Como $\left(P_i, P_j\right) = 1$ a pares, Λ_M es R_T-cíclico. (De hecho si λ_i es generador de $\Lambda_{P_i^{\alpha_i}}$, entonces $\lambda = \lambda_1 + \cdots + \lambda_r$ es generador de Λ_M).

Sea λ generador de Λ_M y sea $\theta : R_T \to \Lambda_M$ dado por $A \mapsto \lambda^A$, para todo $A \in R_T$. Se tiene que θ es suprayectivo y $R_T/\ker\theta \cong \Lambda_M$ donde $\ker\theta = \left\{A \in R_T \mid \lambda^A = 0\right\} = \operatorname{an}(\lambda) = \operatorname{an}(\Lambda_M)$. Se tiene $M \in \ker\theta$ ya que como $\lambda \in \Lambda_M$, $\theta(M) = \lambda^M = 0$. Por lo que $(M) \subseteq \ker\theta$.

Finalmente, si $d = \operatorname{gr} M$, $|R_T/\ker\theta| = |\Lambda_M| = q^d$. Entonces $\ker\theta = (M)$ y $R_T/(M) = R_T/\ker\theta \cong \Lambda_M$. □

Definición 2.1.9. Para $M \in R_T \setminus \{0\}$, se define $\Phi(M) = |(R_T/(M))^*|$. Es decir,

$$\Phi(M) = \left|\{N \in R_T \mid (N, M) = 1,\ \operatorname{gr} N < \operatorname{gr} M\}\right|$$

es la *cardinalidad del grupo de unidades* de $R_T/(M)$.

La función Φ es el análogo de la función ϕ de Euler en $\mathbb{N}$, donde

$$\phi(n) = |\{m \in \mathbb{N} \mid (m,n) = 1,\ m < n\}|.$$

Entonces para $M, N \in R_T$ se tiene:

1. Si $(M,N) = 1$, entonces
$$\Phi(MN) = \Phi(M)\,\Phi(N).$$

Demostración. Como M y N son primos relativos tenemos por el teorema chino del residuo $R_T/(MN) \cong R_T/(M) \times R_T/(N)$, así $(R_T/(MN))^* \cong (R_T/(M))^* \times (R_T/(N))^*$. Tomando cardinalidad $|(R_T/(MN))^*| = |(R_T/(M))^*| \times |(R_T/(N))^*|$. Por lo tanto $\Phi(MN) = \Phi(M)\,\Phi(N)$. □

2. Si P es irreducible, entonces $\Phi(P) = q^d - 1$, donde $d = \operatorname{gr} P$, donde $d = \operatorname{gr} P$.

Demostración. Tenemos $R_T/(P) = \mathbb{F}_q[T]/(P) \cong \mathbb{F}_q(\alpha)$ donde α es raíz del polinomio irreducible P. Notemos que $\left|\mathbb{F}_q(\alpha)\right| = q^d$ donde $d = \operatorname{gr} P$, entonces $|R_T/(P)| = q^d$. Ahora para $M \in R_T \setminus \{0\}$ tenemos $\Phi(M) = |(R_T/(M))^*|$ y $(R_T/(P))^* = (R_T/(P)) \setminus \{0\}$ pues $R_T/(P)$ es campo. Entonces $\Phi(P) = |(R_T/(P))^*| = q^d - 1$. □

3. Si P es irreducible, entonces $\Phi(P^n) = \left|R_T/\left(P^{n-1}\right)\right| \Phi(P) = q^{(n-1)d}(q^d - 1)$, donde $d = \operatorname{gr} P$.

Demostración. Sea $\psi : (R_T/(P^n))^* \to (R_T/(P))^*$ dado por $f + (P^n) \mapsto f + (P)$. ψ está bien definida, es homomorfismo y es suprayectiva. Además

$$\begin{aligned}
\ker\psi &= \{f + (P^n) \in (R_T/(P^n))^* \mid f - 1 \in (P)\} \\
&= \{f + (P^n) \in (R_T/(P^n))^* \mid f - 1 = Pg,\ g \in R_T\} \\
&= \{f + (P^n) \mid f = 1 + Pg,\ g \in R_T\} \\
&= \{1 + Pg + (P^n) \mid g \in R_T\}.
\end{aligned}$$

Luego por el primer teorema de isomorfismo $(R_T/(P^n))^*/\ker\psi \cong (R_T/(P))^*$.
Ahora determinemos la cardinalidad de $\ker\psi$.
$1 + Pg + (P^n) = 1 + Pg_1 + (P^n) \Leftrightarrow P(g - g_1) \in (P^n) \Leftrightarrow P(g - g_1) = P^n l \Leftrightarrow g - g_1 = P^{n-1} l \Leftrightarrow g + \left(P^{n-1}\right) = g_1 + \left(P^{n-1}\right)$. Luego $|\ker\psi| = \left|R_T/\left(P^{n-1}\right)\right| = q^{d(n-1)}$. Entonces $\dfrac{|(R_T/(P^n))^*|}{\left|R_T/\left(P^{n-1}\right)\right|} = \left|(R_T/(P^n))^*/\ker\psi\right| = |(R_T/(P))^*| = \Phi(P)$. Por lo tanto $|(R_T/(P^n))^*| = \left|\left(R_T/\left(P^{n-1}\right)\right)\right| \Phi(P)$, es decir $\Phi(P^n) = \left|R_T/\left(P^{n-1}\right)\right| \Phi(P) = q^{d(n-1)}\left(q^d - 1\right) = \dfrac{q^{dn}}{q^d}\left(q^d - 1\right) = q^{dn} - q^{d(n-1)}$. □

4. De la parte 3, se tiene que en general si M se descompone como $M = \prod_{i=1}^{r} P_i^{n_i}$, donde $d_i = \operatorname{gr} P_i$ y $P_i^{n_i}$ son potencias de polinomios irreducibles distintos, entonces

$$\Phi(M) = |(R/(M))^*| = \prod_{i=1}^{r} \left| \left(R/\left(P_i^{n_i}\right)\right)^* \right| = \prod_{i=1}^{r} q^{d_i(n_i-1)}\left(q^{d_i}-1\right).$$

Proposición 2.1.10. *El R_T-módulo cíclico Λ_M tiene exactamente $\Phi(M)$ generadores. De hecho, si λ es generador de Λ_M, entonces λ^A, $A \in R_T$ es generador si y sólo si $(A, M) = 1$.*

Demostración. Sea λ un generador de Λ_M. Si $(A, M) = 1$, sean $\lambda_1 \in \Lambda_M$ y $B \in R_T$ tales que $\lambda_1 = \lambda^B$. Sean $S,\ U \in R_T$ tales que $SA + UM = 1$. Entonces $B = SAB + UMB$. Con esto se tiene que

$$\lambda_1 = \lambda^B = \lambda^{SAB+UMB} = \lambda^{SAB} + \left(\lambda^M\right)^{UB} = \left(\lambda^A\right)^{SB} + 0 = \left(\lambda^A\right)^{SB}.$$

Por lo que podemos concluir que λ^A es un generador de Λ_M. Para el recíproco, si λ^A es un generador de Λ_M, entonces existe $B \in R_T$ tal que $\lambda^{AB} = \lambda$. Esto implica que $\lambda^{AB-1} = 0$. Como λ es un generador, tenemos que si $\lambda^C = 0$ para algún $C \in R_T$, entonces M divide a C y por lo tanto M divide a $AB - 1$. Con esto tenemos que $AB \equiv 1(\text{mód } M)$ y $(A, M) = 1$.

□

Definición 2.1.11. El polo de T en $K = \mathbb{F}_q(T)$, $\mathfrak{p}_\infty$ definido por $(T)_K = \dfrac{\mathfrak{p}_0}{\mathfrak{p}_\infty}$ se llama el *"primo infinito"* de K.

Definición 2.1.12. Sea $M \in R_T \setminus \{0\}$. Al campo $K_M = K(\Lambda_M)$ generado sobre $K = \mathbb{F}_q(T)$ al adjuntarle el módulo de Carlitz-Hayes $\Lambda_M = \left\{u \in \bar{K} \mid u^M = 0\right\}$ se le llamará el *campo de funciones ciclotómico* determinado por Λ_M sobre K.

Proposición 2.1.13. *$K(\Lambda_M)/K$ es una extensión de Galois.*

Demostración. Como $\Lambda_M \cong R_T/(M)$ es cíclico, digamos generado por λ, entonces $\Lambda_M = \lambda^{R_T} = \left\{\lambda^A \mid A \in R_T\right\}$, entonces $K(\lambda) = K(\Lambda_M)$, ya que si $\xi \in \Lambda_M$ es de la forma $\xi = \lambda^A$ para algún $A \in R_T$, entonces $\xi = \lambda^A = A(\varphi + \mu_T)(\lambda) = \sum_{i=0}^{\operatorname{gr} A} \begin{bmatrix} A \\ i \end{bmatrix} \lambda^{q^i} \in K(\lambda)$. Ahora bien, $K(\Lambda_M)$ es el campo de descomposición del polinomio separable $F(u) = u^M \in K[u]$, se sigue que $K(\Lambda_M)/K$ es una extensión de Galois. □

Observemos que si $M = a_d T^d + \ldots + a_1 T + a_0$, entonces $u^M = a_d u^{q^d} + \begin{bmatrix} M \\ d-1 \end{bmatrix} u^{q^{d-1}} + \cdots + \begin{bmatrix} M \\ 1 \end{bmatrix} u^q + Mu \in R_T[u]$, entonces los elementos de Λ_M son enteros sobre R_T y el coeficiente líder de u^M es

$a_d \in \mathbb{F}_q \setminus \{0\}$. Además $u^M = a_d\left[u^{q^d} + a_d^{-1}\begin{bmatrix} M \\ d-1 \end{bmatrix}u^{q^{d-1}} + \cdots + a_d^{-1}\begin{bmatrix} M \\ 1 \end{bmatrix}u^q + a_d^{-1}Mu\right] \in R_T[u]$ con coeficiente líder 1. Notemos que $\Lambda_M = \Lambda_{a_d^{-1}M}$ y $a_d^{-1}M$ es mónico. Así los elementos de Λ_M son enteros sobre R_T.

Definición 2.1.14. Para $M \in R_T \setminus \{0\}$ sea $G_M := \text{Gal}\ (K(\Lambda_M)/K)$ el *grupo de Galois* de $K(\Lambda_M)/K$.

Proposición 2.1.15. *La acción de G_M sobre $K(\Lambda_M)$ conmuta con la acción de R_T, es decir, si $u \in K(\Lambda_M)$, $\sigma \in G_M$ y $N \in R_T$, entonces $\sigma\left(u^N\right) = \sigma(u)^N$.*

Demostración. Si $K \subseteq L \subseteq K(\Lambda_M)$ es cualquier subcampo, $u \in L$ y $N \in R_T$, entonces $u^T = (\varphi + \mu_T)(u) = u^q + Tu \in L$, esto implica $u^N = N(\varphi + \mu_T)(u) = \sum \alpha_i (\varphi + \mu_T)^i (u) \in L$ por lo tanto L es R_T-módulo.

En particular si $u \in K(\Lambda_M)$, $u^N \in K(\Lambda_M)$ para todo $N \in R_T$. Ahora

$$\begin{aligned}
\sigma\left(u^N\right) &= \sigma\left(\sum_{i=0}^{\text{gr}\,N} \begin{bmatrix} N \\ i \end{bmatrix} u^{q^i}\right) \text{ donde } \begin{bmatrix} N \\ i \end{bmatrix} \in R_T \subseteq K \\
&= \sum_{i=0}^{\text{gr}\,N} \begin{bmatrix} N \\ i \end{bmatrix} (\sigma u)^{q^i} \text{ por ser } \sigma \text{ homomorfismo} \\
&= (\sigma u)^N .
\end{aligned}$$

□

Proposición 2.1.16. *G_M es un subgrupo de $(R_T/(M))^*$. En particular $K(\Lambda_M)/K$ es una extensión abeliana y $[K(\Lambda_M) : K] \leq \Phi(M)$.*

Demostración. Como $K(\Lambda_M) = K(\lambda)$, con λ generador de Λ_M. Entonces $\sigma \in G_M$ está determinado por $\sigma\lambda$ pues $\sigma \sum \alpha_i \lambda_i = \sum \alpha_i (\sigma\lambda)^i$. Ahora $\sigma\lambda$ es un conjugado de λ. Por lo tanto $\sigma\lambda \in \Lambda_M$, entonces $\sigma\lambda = \lambda^A$ para algún $A \in R_T$.

Veamos que $\sigma\lambda$ es generador de Λ_M. Sea $\xi \in \Lambda_M$, $\sigma^{-1}\xi = \lambda^B$ para algún $B \in R_T$. Entonces $\xi = \sigma\left(\lambda^B\right) = (\sigma\lambda)^B$. Por lo tanto $\sigma\lambda$ es generador de Λ_M y entonces $(A, M) = 1$. Por lo tanto A mód $M \in (R_T/(M))^*$.

Veamos que A no depende de λ. Si λ_1 es otro generador de Λ_M, es decir, $\lambda_1 = \lambda^C$ para algún $C \in R_T$, entonces $\sigma\lambda_1 = \sigma\left(\lambda^C\right) = \left(\lambda^A\right)^C = \lambda^{AC} = \lambda^{CA} = \left(\lambda^C\right)^A = \lambda_1^A$.

Finalmente, si $\sigma\lambda = \lambda^A = \lambda^{A_1}$, entonces $\lambda^{A-A_1} = 0$. Por lo tanto $A - A_1 \in (M)$, es decir $A \equiv A_1$ (mód M).

Ahora sea $\theta : G_M \to (R_T/(M))^*$ dado por $\theta(\sigma) = A$ mód M, donde $\sigma\lambda = \lambda^A$. Como A no depende de λ, θ está bien definida. Si $\Psi \in G_M$, entonces $\Psi(\lambda) = \lambda^B$ y $(\Psi \circ \sigma)(\lambda) = \Psi\left(\lambda^A\right) = (\Psi(\lambda))^A = \lambda^{BA} = \lambda^{AB}$. Por lo tanto $\theta(\Psi \circ \sigma) = BA$ mód $M = (B \text{ mód } M)(A \text{ mód } M) = \theta(\Psi)\theta(\sigma)$. Luego θ es homomorfismo de grupos. Si $\sigma \in \ker\theta$, es decir, $\theta(\sigma) = 1$ mód M, entonces $\sigma\lambda = \lambda^1 = \lambda$, es decir $\sigma = \mathbf{1}$. Por lo tanto θ es monomorfismo. Así tenemos que $G_M \subseteq (R_T/(M))^*$ y $|G_M| = [K(\Lambda_M) : K] \leq |(R_T/(M))^*| = \Phi(M)$. Como $(R_T/(M))^*$ es abeliano, tenemos que G_M es abeliano. □

Definición 2.1.17. Sea $S \in R_T$ mónico. Definimos el *polinomio ciclotómico* con respecto a S como

$$\Psi_S(u) = \prod_{\substack{(B,S)=1 \\ \text{gr } B < \text{gr } S}} \left(u - \lambda_S^B\right).$$

donde λ_S es generador de Λ_S. Entonces $\Psi_S(u) \in K(\Lambda_S)[u]$.

Proposición 2.1.18. *$\Psi_S(u) \in K[u]$, donde $S \in R_T$ es un polinomio mónico.*

Demostración. Sea $\sigma \in G_S = \text{Gal}(K(\Lambda_S)/K)$. Entonces $\sigma(\lambda_S) = \lambda_S^A$ con, $(A, S) = 1$. Por lo tanto

$$\sigma(\Psi_S(u)) = \prod_{\substack{(B,S)=1 \\ \text{gr } B < \text{gr } S}} \left(u - \lambda_S^{AB}\right).$$

Ahora, de $(A, S) = (B, S) = 1$, tenemos $(AB, S) = 1$. Luego si $AB = QS + B_1$, con $\text{gr } B_1 < \text{gr } S$, entonces $\lambda_S^{AB} = \lambda_S^{B_1}$ y si $AB \equiv AC \pmod{S}$, entonces $B_1 \equiv C_1 \pmod{S}$ y como $\text{gr } B_1 < \text{gr } S$ y $\text{gr } C_1 < \text{gr } S$, tenemos

$$\sigma(\Psi_S(u)) = \prod_{\substack{(B,S)=1 \\ \text{gr } B < \text{gr } S}} \left(u - \lambda_S^{AB}\right) = \prod_{\substack{(B_1,S)=1 \\ \text{gr } B_1 < \text{gr } S}} \left(u - \lambda_S^{B_1}\right) = \Psi_S(u).$$

Por lo tanto $\sigma(\Psi_S(u)) = \Psi_S(u)$ para todo $\sigma \in G_S$ y así $\Psi_S(u) \in K(\Lambda_S)[u]$. □

Nota 2.1.19. Observemos que $\text{gr}_u \Psi_S(u) = \Phi(S)$.

Proposición 2.1.20. *1. Si N y M son dos polinomios mónicos distintos en R_T, entonces*

$$(\Psi_N(u), \Psi_M(u)) = 1.$$

2. Si $M \in R_T \setminus \{0\}$, con $d = \text{gr } M$, entonces $\sum_{\substack{D|M \\ D \text{ mónico}}} \Phi(D) = q^d$.

3. $u^M = \prod_{\substack{D|M \\ D \text{ mónico}}} \Psi_D(u)$, *donde* M *es un polinomio mónico en* R_T.

Demostración. 1. Sea $D := (\Psi_M(u), \Psi_N(u))$ y supongamos $D \neq 1$. Sea $\lambda \in \bar{K}$ raíz de D. Entonces λ es raíz de $\Psi_M(u)$ y de $\Psi_N(u)$, esto es $\lambda = \lambda_M^A = \lambda_N^B$ con $(A, M) = 1 = (B, N)$, $\operatorname{gr} A < \operatorname{gr} M$ y $\operatorname{gr} B < \operatorname{gr} N$. Luego $\lambda = \lambda_{MN}^{AN} = \lambda_{NM}^{BM}$, entonces $AN = BM$. Como A y M son primos relativos, al igual que B y N tenemos $A \mid B$ y $B \mid A$, entonces $A = B$ salvo una constante. Por lo tanto $M = N$ que es una contradicción. Por lo tanto $D = (\Psi_M(u), \Psi_N(u)) = 1$.

2. Si $M = P^n$, con P irreducible y $\operatorname{gr} P = d$, entonces

$$\sum_{\substack{D|M \\ D \text{ mónico}}} \Phi(D) = \sum_{i=0}^{n} \Phi\left(P^i\right) = \sum_{i=1}^{n} \left(q^{id} - q^{(i-1)d}\right) + 1 = q^{nd} - 1 + 1 = q^{nd} = q^{\operatorname{gr} P^n}.$$

En general si $M = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$, entonces

$$\sum_{\substack{D|M \\ D \text{ mónico}}} \Phi(D) = \sum_{\substack{\beta_i = 0, \ldots, \alpha_i \\ i = 1, \ldots, r}} \Phi\left(P_1^{\beta_1}\right) \cdots \Phi\left(P_r^{\beta_r}\right) = \prod_{i=1}^{r} \sum_{\beta_i = 0}^{\alpha_i} \Phi\left(P_i^{\beta_i}\right) = \prod_{i=1}^{r} q^{\operatorname{gr} P_i^{\alpha_i}} = q^{\sum_{i=1}^{r} \operatorname{gr} P_i^{\alpha_i}} = q^{\operatorname{gr} M} = q^d.$$

3. Si $D \mid M$, con D mónico, entonces $\Psi_D(u) \mid u^M$ y como para $D_1 \neq D_2$ mónicos, $(\Psi_{D_1}(u), \Psi_{D_2}(u)) = 1$, entonces $\prod_{D|M} \Psi_D(u) \mid u^M$. Pero $\operatorname{gr}\left(\prod_{D|M} \Psi_D(u)\right) = \sum_{D|M} \Phi(D) = q^{\operatorname{gr} M} = \operatorname{gr} u^M$. Entonces $u^M = \prod_{D|M} \Psi_D(u)$.

□

Proposición 2.1.21. *Sean* $M = P^n$, P *polinomio mónico irreducible con* $d = \operatorname{gr} \mathrm{P}$ *y* $\mathfrak{p}$ *el divisor de* K *asociado a* P. *Entonces todo divisor primo de* K *diferente de* $\mathfrak{p}$ *y* $\mathfrak{p}_\infty$ *es no ramificado en* $K(\Lambda_{P^n})$ *y el índice de ramificación de* $\mathfrak{p}$ *en* $K(\Lambda_{P^n})/K$ *es* $e(\mathfrak{p}) = \Phi(P^n) = q^{nd} - q^{(n-1)d} = q^{(n-1)d}(q^d - 1) = [K(\Lambda_M) : K]$.

Demostración. Sea $\mathcal{O}_M$ la cerradura entera de R_T en $K(\Lambda_M)$, esto es,

$$\mathcal{O}_M = \{\alpha \in K(\Lambda_M) \mid \operatorname{Irr}(\alpha, u, K) \subset R_T[u]\}.$$

$$\begin{array}{ccc} \mathcal{O}_M & \longrightarrow & K(\Lambda_M) \\ \big| & & \big| \\ R_T = \mathbb{F}_q[T] & \longrightarrow & K = \mathbb{F}_q(T) \end{array}$$

Como R_T es dominio de Dedekind, se tiene que $\mathcal{O}_M$ es dominio de Dedekind. Los primos ramificados, diferentes al primo infinito $\mathfrak{p}_\infty$ son los que aparecen en el discriminante de $\mathcal{O}_M/R_T$, es decir, $\delta_{\mathcal{O}_M/R_T}$. Sea λ generador de Λ_{P^n}. Entonces $R_T[\lambda] \subseteq \mathcal{O}_M$. Sea $g(u) = \text{Irr}\,(\lambda, u, K) \in R_T[u] \subseteq K[u]$. Sea $f(u) = u^M = u^{P^n}$. Como $f(\lambda) = 0$, existe $h(u) \in K[u]$ tal que $f(u) = h(u)g(u)$. Así que $f'(u) = h'(u)g(u) + h(u)g'(u)$. Evaluando en λ: $M = f'(\lambda) = h'(\lambda)g(\lambda) + h(\lambda)g'(\lambda) = h(\lambda)g'(\lambda)$. En particular $(g'(\lambda))_{\mathcal{O}_M} \mid (M)\,\mathcal{O}_M = (P^n)_{\mathcal{O}_M}$. Como veremos en el capítulo 3, el diferente satisface $\mathfrak{D}_{\mathcal{O}_M|R_T} = \text{mcd}\,\{F'(\alpha) \mid \alpha \text{ es entero, } K(\Lambda_M) = K(\alpha),\ F(u) = \text{Irr}\,(\alpha, u, K)\}$, se tiene $\mathfrak{D}_{\mathcal{O}_M/R_T}$ divide a $(g'(\lambda))_{\mathcal{O}_M}$ que a su vez divide a P^n en $\mathcal{O}_M$, donde

$$P\mathcal{O}_M = (\mathfrak{p}_1 \cdots \mathfrak{p}_h)^e \tag{2.2}$$

y $P^n = (\mathfrak{p}_1 \ldots \mathfrak{p}_h)^{ne}$. Por lo tanto $\delta_{\mathcal{O}_M/R_T} = P^s$ para algún s. Así, el único primo finito ramificado puede ser P. Ahora calculemos $e = e_{K(\Lambda_M)/K}(\mathfrak{p}_i \mid P)$.

Se tiene $u^{P^n} = \left(u^{P^{n-1}}\right)^P = \sum_{i=0}^{d} \begin{bmatrix} P \\ i \end{bmatrix} \left(u^{P^{n-1}}\right)^{q^i} = u^{P^{n-1}} \left(\sum_{i=0}^{d} \begin{bmatrix} P \\ i \end{bmatrix} \left(u^{P^{n-1}}\right)^{q^i-1} \right) = u^{P^{n-1}} \cdot t(u)$.

Entonces $t(u) \in R_T[u]$ y

$$t(u) = \frac{u^{P^n}}{u^{P^{n-1}}} = \sum_{i=0}^{d} \begin{bmatrix} P \\ i \end{bmatrix} \left(u^{P^{n-1}}\right)^{q^i-1}. \tag{2.3}$$

Por tanto $t(\alpha) = 0 \Leftrightarrow \alpha \in \Lambda_{P^n} \setminus \Lambda_{P^{n-1}} \Leftrightarrow \alpha$ es generador de Λ_{P^n}. Por lo tanto

$$t(u) = \prod_{(A,M)=1} \left(u - \lambda^A\right) = P + \sum_{i=1}^{d} \begin{bmatrix} P \\ i \end{bmatrix} \left(u^{P^{n-1}}\right)^{q^i-1}.$$

Para $u = 0$ se tiene $t(0) = \pm \prod_{(A,M)=1} \lambda^A = P$. Ahora $u^A = u(F(u))$, para algún $F(u) \in R_T[u]$. Por lo tanto $\lambda^A = \lambda(F(\lambda))$ y esto implica que λ divide a λ^A en $\mathcal{O}_M$. Si $(A, M) = 1$, entonces λ^A también es generador y por simetría λ^A divide a λ en $\mathcal{O}_M$. Así tengo que $\lambda = \beta_A \lambda^A$ para algún $\beta_A \in \mathcal{O}_M^*$

Así, por la ecuación (2.3), $P = \beta_0 \lambda^{\Phi(M)}$, con $\beta_0 \in \mathcal{O}_M^*$. Luego por la ecuación (2.2), tenemos $(\mathfrak{p}_1 \ldots \mathfrak{p}_h)^e = (P)_{\mathcal{O}_M} = (\lambda)^{\Phi(M)}$. Como $v_{\mathfrak{p}_i}(\lambda) \geq 1$, se tiene $v_{\mathfrak{p}_i}((\mathfrak{p}_1 \ldots \mathfrak{p}_h)^e) = v_{\mathfrak{p}_i}\left(\lambda^{\Phi(M)}\right) \geq \Phi(M)$. Luego $e \geq \Phi(M) = |(R_T/(M))^*| \geq |G_M| = [K(\Lambda_M) : K] \geq e$. Entonces $e = \Phi(M) = [K(\Lambda_M) : K] = q^{nd} - q^{(n-1)d} = q^{(n-1)d}\left(q^d - 1\right)$. □

Teorema 2.1.22. *Sea $M \in R_T \setminus \{0\}$ mónico. Entonces*

1. $t(u) = \Psi_M(u) = \text{Irr}\,(\lambda, u, K)$.
2. $G_M = \text{Gal}\,(K(\Lambda_M)/K) \cong (R_T/(M))^*$.

3. $[K(\Lambda_M) : K] = \Phi(M)$.

4. *Si $M = P^n$, para algún polinomio irreducible P y $\mathfrak{p}$ es el divisor de K asociado a P, entonces $\mathfrak{p}$ es totalmente ramificado en $K(\Lambda_M)/K$.*

Demostración. Si $M = P^n$, se tiene $[K(\Lambda_{P^n}) : K] = \Phi(P^n)$. Por lo tanto $G_{P^n} \cong (R_T/(P^n))^*$ pues $G_{P^n} \subseteq (R_T/P^n)^*$ y ambos tienen el mismo orden, es decir, $\Phi(P^n)$. Además $e(\mathfrak{p}) = \Phi(P^n)$. Por lo tanto $\mathfrak{p}$ es totalmente ramificado y con esto se tiene la parte (4) del teorema. En general si $M = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$ donde P_i, $i = 1, \ldots, r$ son polinomios irreducibles distintos, entonces $\Lambda_M = \oplus_{i=1}^r \Lambda_{P_i^{\alpha_i}}$ como R_T módulos.

Los campos $K\left(\Lambda_{P_1^{\alpha_1}}\right), \ldots, K\left(\Lambda_{P_r^{\alpha_r}}\right)$ son linealmente disjuntos a pares pues P_i es totalmente ramificado en $K_{\Lambda_{P_i^{\alpha_i}}}/K$ y no ramificado en $\prod_{j \neq i} K\left(\Lambda_{P_j}^{\alpha_i}\right)$. Entonces se tiene que

$$[K(\Lambda_M) : K] = \prod_{i=1}^{r} [K\left(\Lambda_{P_i^{\alpha_i}}\right) : K] = \prod_{i=1}^{r} \Phi\left(P_i^{\alpha_i}\right) = \Phi\left(P_1^{\alpha_i} \ldots P_r^{\alpha_r}\right) = \Phi(M).$$

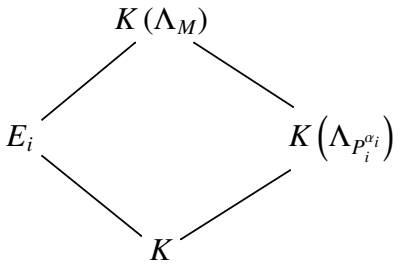
Ahora como $[K(\Lambda_M) : K] = \Phi(M)$, y $G_M \subseteq (R_T/(M))^*$, entonces se tiene $G_M \cong (R_T/(M))^*$. Con esto se tienen (2) y (3).

La parte (1) se sigue de $[K(\Lambda_M) : K] = \Phi(M)$ y del hecho de que $t(\lambda) = 0$ y $\mathrm{gr}_u(t(u)) = \Phi(M) = \mathrm{gr}_u \mathrm{Irr}(\lambda, u, K) = [K(\lambda) : K] = [K(\Lambda_M) : K]$. □

Corolario 2.1.23. *$K(\Lambda_M)/K$ es una extensión geométrica, es decir, el campo de constantes de $K(\Lambda_M)$ es el mismo que el de K, en este caso $\mathbb{F}_q$.*

Demostración. Sea $M = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$, donde $P_1, \ldots, P_r$ son polinomios irreducibles. Entonces $K(\Lambda_M) = \prod_{i=1}^{r} K\left(\Lambda_{P_i^{\alpha_i}}\right)$.

Para cada $1 \leq i \leq r$, sea $E_i = K\left(\Lambda_{M/P_i^{\alpha_i}}\right)$.



Entonces $\mathrm{Gal}(K(\Lambda_M)/E_i) \cong \mathrm{Gal}\left(K\left(\Lambda_{P_i^{\alpha_i}}\right)/K\right)$. Sea L la máxima extensión abeliana no ramificada de K contenida en $K(\Lambda_M)$, $K \subseteq L \subseteq K(\Lambda_M)$. Se tiene que $K(\Lambda_M)/E_i$ es totalmente

ramificada en P_i. Además E_iL/E_i es no ramificada, entonces $E_iL = E_i$ y por lo tanto $L \subseteq E_i$ para $1 \leq i \leq r$. Por lo tanto $K \subseteq L \subseteq \cap_{i=1}^{r} E_i = K$ y así $L = K$. Por tanto toda extensión propia S/K tal que $K \subsetneq S \subseteq K(\Lambda_M)$ es ramificada. Ahora sea $\mathbb{F}_{q^s}$ el campo de constantes de $K(\Lambda_M)$. El campo de constantes de $K = \mathbb{F}_q(T)$ es $\mathbb{F}_q$. Entonces $K = \mathbb{F}_q(T) \subseteq \mathbb{F}_{q^s}(T) \subseteq K(\Lambda_M)$. Se tiene que $\mathbb{F}_{q^s}(T)/\mathbb{F}_q(T)$ es no ramificada. Luego $\mathbb{F}_{q^s}(T) = \mathbb{F}_q(T)$, es decir, $1 = [\mathbb{F}_{q^s}(T) : \mathbb{F}_q(T)] = [\mathbb{F}_{q^s} : \mathbb{F}_q] = s$. □

Proposición 2.1.24. *Sea $M = P^n$, con P polinomio mónico e irreducible en R_T y $n \in \mathbb{N}$. Entonces $\Psi_{P^n}(u) = \frac{u^{P^n}}{u^{P^{n-1}}}$ es un polinomio de Eisenstein en P, es decir, es de la forma $\Psi_{P^n}(u) = \alpha_d u^d + \cdots + \alpha_1 u + \alpha_0 \in R_T$, donde $P \mid \alpha_i$ para $0 \leq i \leq d-1$, $P \nmid \alpha_d$ y $P^2 \nmid \alpha_0$.*

Demostración. Ver [17], proposición 12.3.18, pp. 429. □

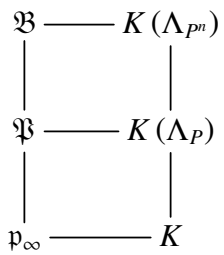
Corolario 2.1.25. *$\Psi_{P^n}(u)$ es irreducible en R_T.*

Demostración. Por la proposición 2.1.24, Ψ_{P^n} es un polinomio de Eisenstein en P. Entonces satisface el criterio de Eisenstein y por lo tanto es irreducible. □

2.2. Ramificación en $\mathfrak{p}_\infty$

Proposición 2.2.1. *Sea $M = P^n$, con $P \in R_T$ mónico e irreducible y $\operatorname{gr} P = d$. Entonces $\mathfrak{p}_\infty$ se descompone en $\Phi(P^n)/(q-1)$ divisores primos en $K(\Lambda_{P^n})$. El índice de ramificación es $e_\infty = q-1$ y cada uno de los divisores primos de $K(\Lambda_M)$ tiene grado 1, luego el grado relativo es $f_\infty = 1$.*

Demostración. Sea $\mathfrak{B}$ un primo de $K(\Lambda_{P^n})$ sobre $\mathfrak{p}_\infty$. Como la extensión es de Galois de grado $\Phi(P^n)$, basta probar que $e_\infty = e_{\mathfrak{B}} = q-1$ y $f_\infty = f_{\mathfrak{B}} = 1$. Sea $\mathfrak{P}$ el divisor primo de $K(\Lambda_P) \subseteq K(\Lambda_{P^n})$ bajo $\mathfrak{B}$, es decir, $\mathfrak{B} \cap K(\Lambda_P) = \mathfrak{P}$.



Se probará primero que $e_{\mathfrak{P}} = q-1$, $f_{\mathfrak{P}} = 1$ y después que $\mathfrak{P}$ se descompone totalmente en $K(\Lambda_{P^n})/K(\Lambda_P)$.

Sea $g(u) = \frac{u^P}{u} = \Psi_P(u)$. Entonces $K(\Lambda_P) = K(\lambda)$, donde λ es cualquier raíz de $g(u)$. Así se tiene:

$g(u) = \sum_{i=0}^{d} \begin{bmatrix} P \\ i \end{bmatrix} u^{q^i-1} = h\left(u^{q-1}\right)$, donde $h(u) = \sum_{i=0}^{d} \begin{bmatrix} P \\ i \end{bmatrix} u^{\frac{q^i-1}{q-1}}$ y $\mathrm{gr}_T \begin{bmatrix} P \\ i \end{bmatrix} = (d-i)q^i$.

Sea K_∞ la completación de K en $\mathfrak{p}_\infty$ y sea v_∞ la valuación correspondiente. Entonces

$$v_\infty\left(\begin{bmatrix} P \\ i \end{bmatrix}\right) = -(d-i)q^i = -\mathrm{gr}_T\left(\begin{bmatrix} P \\ i \end{bmatrix}\right).$$

Escribamos

$$h(u) = \sum_{j=0}^{\frac{q^d-1}{q-1}} f_j(T)u^j,$$

con $f_j(T) \neq 0 \Leftrightarrow j = \dfrac{q^i-1}{q-1}$ para algún i.

Construiremos el polígono de Newton correspondiente a $h(u)$ en K_∞. Los vértices de los coeficientes están dados por

$$\left(j, v_\infty\left(f_j(T)\right)\right) = \left(\frac{q^i-1}{q-1}, -(d-i)q^i\right) = \beta_i,$$

donde $j = \dfrac{q^i-1}{q-1}$.

La pendiente entre β_i y β_{i+1} es:

$$s_i = \frac{-(d-(i+1))q^{i+1} + (d-i)q^i}{\frac{q^{i+1}-1}{q-1} - \frac{q^i-1}{q-1}} = -d(q-1) + q + i(q-1) < s_i + 1.$$

Por lo tanto vemos que las pendientes se incrementan con i. De esta forma vemos que $\beta_0, \beta_1, \ldots, \beta_d$ son los vértices del polígono de Newton correspondiente a $h(u)$ en K_∞. (Ver apéndice A.1).

Se observa que la pendiente entre β_0 y β_1 es $s_0 = -d(q-1) + q$.

Como $\dfrac{q^1-1}{q-1} - \dfrac{q^0-1}{q-1} = 1 - 0 = 1$, $h(u)$ tiene una raíz θ en K_∞, con $v_\infty(\theta) = d(q-1) - q$.

Ahora como $g(u) = h\left(u^{q-1}\right)$, $K(\Lambda_P)_\mathfrak{P} = K_\infty(\lambda)$, donde λ es raíz de $u^{q-1} - \theta$, es decir, $\lambda^{q-1} = \theta$.

Sea $v_\mathfrak{P}$ la valuación en $K(\Lambda_P)_\mathfrak{P}$ sobre v_∞, la valuación en K_∞. Se tiene: $v_\mathfrak{P}\left(\lambda^{q-1}\right) = (q-1)v_\mathfrak{P}(\lambda)$ y $v_\mathfrak{P}(\lambda^{q-1}) = v_\mathfrak{P}(\theta) = e_\infty v_\infty(\theta) = e_\infty(d(q-1) - q)$. Entonces $(q-1)v_\mathfrak{P}(\lambda) = e_\infty(d(q-1) - q)$.

Como $(q-1, d(q-1) - q) = 1$ y como $q-1 \mid e_\infty(d(q-1) - q)$, se tiene $q-1 \mid e_\infty$.

Por otro lado, $e_\infty \leq e_\infty \cdot f_\infty = [K(\Lambda_P)_\mathfrak{P} : K_\infty] = [K_\infty(\lambda) : K_\infty] \leq q-1 \leq e_\infty$, entonces $e_\infty = q-1$ y por lo tanto $K(\Lambda_P)_\mathfrak{P}/K_\infty$ es totalmente ramificada y se tiene $e_\infty = q-1$ y $f_\infty = 1$.

Veamos ahora que $\mathfrak{P}$ se descompone totalmente en $K(\Lambda_{P^n})/K(\Lambda_P)$. Sea β raíz de $g(u)$, $v_\mathfrak{P}(\beta) =$

$d(q-1)-q$. Se tiene $u^P = ug(u)$, luego $u^{P^n} = \left(u^{P^{n-1}}\right)^P = u^{P^{n-1}} g\left(u^{P^{n-1}}\right)$, es decir, $\Psi_{P^n}(u) = \Psi_P\left(u^{P^{n-1}}\right) = \frac{u^{P^n}}{u^{P^{n-1}}}$.

Con esto, $K(\Lambda_{P^n})$ se obtiene de $K(\Lambda_P)$ adjuntándole cualquier raíz de $g\left(u^{P^{n-1}}\right)$. Así $K(\Lambda_{P^n})$ se obtiene de $K(\Lambda_P)$ adjuntándole una raíz de $u^{P^{n-1}} - \beta$.

Equivalentemente, esto se puede ver como sigue:

Si β_{P^n} es generador de Λ_{P^n}, entonces $\beta_{P^n}^{P^{n-1}} = \beta_{P^n/P^{n-1}} = \beta_P = \beta$ es generador de Λ_P.

Ahora calcularemos el polígono de Newton de $u^{P^{n-1}} - \beta$. Se tiene:

$$u^{P^{n-1}} - \beta = \sum_{i=0}^{(n-1)d} \begin{bmatrix} P^{n-1} \\ i \end{bmatrix} u^{q^i} - \beta.$$

Sean

$$\gamma_{-1} = (0, v_{\mathfrak{P}}(-\beta)) = (0, d(q-1)-q),$$
$$\gamma_i = \left(q^i, v_{\mathfrak{P}}\left(\begin{bmatrix} P^{n-1} \\ i \end{bmatrix}\right)\right) = \left(q^i, e(\mathfrak{P} \mid \mathfrak{p}_\infty)\, v_\infty\left(\begin{bmatrix} P^{n-1} \\ i \end{bmatrix}\right)\right) = \left(q^i, -(q-1)\left((d(n-1)-i)\, q^i\right)\right),$$

donde $0 \leq i \leq (n-1)d$.

Entonces la pendiente de γ_{-1} a γ_0 es $t_{-1} = -dn(q-1)+q$. La pendiente de γ_i a γ_{i+1} es $t_i = -(q-1)d(n-1)+i(q-1)+q < t_{i+1}$ para $0 \leq i \leq d(n-1)$. Por lo tanto las pendientes se incrementan y $t_{-1} = -dn(q-1)+q < -(q-1)d(n-1)+q = t_0$. Con esto, $\gamma_{-1}, \gamma_0, \gamma_1, \ldots, \gamma_{(n-1)d}$ son los vértices del polígono de Newton de $u^{P^n} - \beta$.

El segmento de γ_{-1} a γ_0 muestra que $u^{P^{n-1}} - \beta$ tiene una $(s - r = 1 - 0 = 1)$ raíz en $K(\Lambda_P)_{\mathfrak{P}}$.

Como la extensión es de Galois, $K(\Lambda_{P^n})_{\mathfrak{B}} = K(\Lambda_P)_{\mathfrak{P}}$, es decir, $u^{P^{n-1}} - \beta$ se descompone en $K(\Lambda_P)_{\mathfrak{P}}$ y por lo tanto $f(\mathfrak{B} \mid \mathfrak{P}) = e(\mathfrak{B} \mid \mathfrak{P}) = 1$. □

Ahora se probará el caso general usando el lema de Abhyankar. (Véase apéndice A.2).

Teorema 2.2.2. *Sea $M \in R_T \setminus \{0\}$. Entonces $\mathfrak{p}_\infty$ es moderadamente ramificado en $K(\Lambda_M)/K$. De hecho $e_\infty = q-1$, $f_\infty = 1$ y $h_\infty = \frac{\Phi(M)}{q-1}$.*

Demostración. Si $M = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$, entonces $K(\Lambda_M) = \prod_{i=1}^{r} K\left(\Lambda_{P_i^{\alpha_i}}\right)$. Luego por la proposición 2.2.1, tengo que $e_{\Lambda_{P_i^{\alpha_i}}}(\mathfrak{p}_\infty) = q-1$ y la ramificación es moderada pues $p = \text{caract } K \nmid (q-1)$. Por el lema de Abhyankar, $e_\infty = e_{K(\Lambda_M)}(\mathfrak{p}_\infty) = \text{ mcm } [q-1, \ldots, q-1] = q-1$. Además

$$\begin{array}{ccc} K\left(\Lambda_{P_1^{\alpha_1}}\right) & \xrightarrow{f_2'} & K\left(\Lambda_{P_1^{\alpha_1} P_2^{\alpha_2}}\right) \\ {\scriptstyle f_1}\downarrow & \nearrow_{f} & \downarrow{\scriptstyle f_1'} \\ K & \xrightarrow[f_2]{} & K\left(\Lambda_{P_2^{\alpha_2}}\right) \end{array}$$

Se tiene (ver teorema 12.14, pp. 212, de [14]) tengo $f_1' = 1$, luego $f = f_2 f_1' = 1$ y esto pasa para $i = 1, \ldots, r$ por lo que $f_\infty = d_{K(\Lambda_M)/K}(\mathfrak{p}_\infty) = 1$.

Finalmente, como $[K(\Lambda_M) : K] = e_\infty \cdot f_\infty \cdot h_\infty$, tenemos $h_\infty = \frac{\Phi(M)}{q-1}$ y éste es el número de divisores primos de $K(\Lambda_M)$ sobre $\mathfrak{p}_\infty$.

□

2.3. Subcampo real maximal

Proposición 2.3.1. *Se tiene $\mathbb{F}_q^* = G_0$, donde G_0 es el grupo de inercia de cualquier divisor primo $\mathfrak{P}$ de $K(\Lambda_M)$ sobre $\mathfrak{p}_\infty$.*

Demostración. Tenemos $f_\infty = d_{K(\Lambda_M)/K}(\mathfrak{P} \mid \mathfrak{p}_\infty) = 1$. Por lo tanto el grupo de inercia es igual al grupo de descomposición de $\mathfrak{P}$.
Suponemos que $M = P^n$, donde P es un polinomio mónico e irreducible. Entonces

$$G_M = G_{P^n} = \mathrm{Gal}\left(K\left(\Lambda_{P^n}\right)/K\right) \cong \left(R_T/\left(P^n\right)\right)^*.$$

Además $|G_M| = \Phi(P^n) = q^{nd} - q^{(n-1)d}$, donde $d = \mathrm{gr}\, P$. Por lo tanto $|G_{P^n}| = q^{(n-1)d}\left(q^d - 1\right)$. Por lo tanto el único subgrupo de G_{P^n} de orden $q^d - 1$ es cíclico y corresponde a $(R_T/(P))^*$. Luego por la unicidad del subgrupo cíclico de orden $q-1$ éste debe ser $\mathbb{F}_q^*$. Por otro lado, por el teorema 2.2.2 $|G_0| = e_\infty = q - 1$. Por lo que, en este caso, $G_0 = \mathbb{F}_q^*$.

Ahora para $M \in R_T \setminus \{0\}$ arbitrario, se considera $P \mid M$ y debe verse que existe $\lambda_0 \in \Lambda_P \subseteq \Lambda_M$ tal que $v_{\mathfrak{P}'}(\lambda_0) = -1$, donde $\mathfrak{P}' = \mathfrak{P} \cap K(\Lambda_P)$ y $\mathfrak{P}$ es un primo en $K(\Lambda_M)$ sobre $\mathfrak{p}_\infty$.

Consideremos el siguiente diagrama:

$$\begin{array}{ccc} \mathfrak{P} & \text{——} & K(\Lambda_M) \\ | & & | \\ \mathfrak{P}' & \text{——} & K(\Lambda_P) \\ | & & | \\ \mathfrak{p}_\infty & \text{———} & K \end{array}$$

Sabemos que $\mathfrak{p}_\infty$ tiene encima $q-1$ primos en $K(\Lambda_M)$, al igual que $\mathfrak{P}'$. Entonces $\mathfrak{P}'$ ya no puede ser ramificado. Luego, de existir tal λ_0, tenemos

$$v_{\mathfrak{P}}(\lambda_0) = e(\mathfrak{P} \mid \mathfrak{P}')\, v_{\mathfrak{P}'}(\lambda_0) = 1 \cdot (-1) = -1.$$

Entonces $\dfrac{1}{\lambda_0}$ es un elemento primo para $\mathfrak{P}|\mathfrak{p}_\infty$, pues $v_{\mathfrak{P}}\left(\frac{1}{\lambda_0}\right) = 1$.

Por último, si $\alpha \in \mathbb{F}_q^* \subseteq (R_T/(M))^* = \text{ Gal } (K(\Lambda_M)|K)$, entonces $\sigma_\alpha\left(\frac{1}{\lambda_0}\right) = \frac{1}{\alpha\lambda_0} = \alpha^{-1}\left(\frac{1}{\lambda_0}\right)$. Por lo tanto $\mathfrak{P}^{\sigma_\alpha} = \mathfrak{P}$. Con esto $\mathbb{F}_q^* \subseteq \mathrm{D}(\mathfrak{P} \mid \mathfrak{p}_\infty) = \mathrm{I}(\mathfrak{P}|\mathfrak{p}_\infty) = G_0$ y ambos tienen el mismo orden $q-1$. Por lo tanto $G_0 = \mathbb{F}_q^*$.

Ahora se debe encontrar λ_0:
Sea $\lambda \in \Lambda_P$, con $\lambda \neq 0$.

$$\lambda^P/\lambda = \lambda^{q^d-1} + \begin{bmatrix} P \\ d-1 \end{bmatrix}\lambda^{q^{d-1}-1} + \cdots + \begin{bmatrix} P \\ 1 \end{bmatrix}\lambda^{q-1} + P = 0,$$

donde $\begin{bmatrix} P \\ i \end{bmatrix} \in R_T$ es de grado $(d-i)\,q^i$, $(d = \text{gr } P)$. Dividiendo entre T^{q^d-1}:

$$\left(\tfrac{\lambda}{T}\right)^{q^d-1} + g_{d-1}\left(\tfrac{1}{T}\right)\left(\tfrac{\lambda}{T}\right)^{q^{d-1}-1} + \cdots + g_1\left(\tfrac{1}{T}\right)\left(\tfrac{\lambda}{T}\right)^{q-1} + g_0\left(\tfrac{1}{T}\right) = 0,$$

donde $g_i\left(\frac{1}{T}\right) \in \mathbb{F}_q\left[\frac{1}{T}\right]$ y $g_{d-i}\left(\frac{1}{T}\right) = \frac{1}{T^{q^d-q^{d-i}}}\begin{bmatrix} P \\ d-i \end{bmatrix}$ y

$$\begin{aligned} v_\infty(g_{d-i}(\tfrac{1}{T})) &= v_\infty\left(\begin{bmatrix} P \\ d-i \end{bmatrix}\right) - v_\infty\left(T^{q^d-q^{d-i}}\right) \\ &= -iq^{d-i} + q^d - q^{d-i} \\ &= q^d - (i+1)q^{d-i} > 0 \text{ para } 0 \leq i \leq d-1. \end{aligned}$$

En particular $v_\infty\left(g_{d-1}\left(\frac{1}{T}\right)\right) = q^d - 2q^{d-1} < q^d - (i+1)q^{d-i} = v_\infty\left(g_{d-i}\left(\frac{1}{T}\right)\right)$, $i \geq 2$.

Ahora, $\frac{\lambda}{T}$ es entero en $\mathfrak{P}' \mid \mathfrak{p}_\infty$, pues satisface un polinomio mónico con coeficientes en $\mathbb{F}_q[\frac{1}{T}]$. Por lo tanto es entero con respecto a $\frac{1}{T}$. Entonces $v_{\mathfrak{P}'}\left(\frac{\lambda}{T}\right) \geq 0$.
Por lo que si se tuviera $v_{\mathfrak{P}'}\left(\left(\frac{\lambda}{T}\right)^{q^{d-1}}\right) < v_{\mathfrak{P}'}\left(g_{d-1}\left(\frac{1}{T}\right)\right)$, entonces

$$v_{\mathfrak{P}'}\left(\left(\frac{\lambda}{T}\right)^{q^{d-1}}\right) < v_{\mathfrak{P}'}\left(g_{d-i}\left(\frac{1}{T}\right)\right) < v_{\mathfrak{P}'}\left(g_{d-i}\left(\frac{1}{T}\right)\cdot\left(\frac{\lambda}{T}\right)^{q^{d-i}-1}\right)$$

para todo $i > 0$. Entonces

$$\begin{aligned} \infty = v_{\mathfrak{P}'}(0) &= v_{\mathfrak{P}'}\left(\left(\frac{\lambda}{T}\right)^{q^d-1} + g_{d-1}\left(\frac{1}{T}\right)\left(\frac{\lambda}{T}\right)^{q^{d-1}-1} + \cdots + g_1\left(\frac{1}{T}\right)\left(\frac{\lambda}{T}\right)^{q-1} + g_0\left(\frac{1}{T}\right)\right) \\ &= v_{\mathfrak{P}'}\left(\left(\frac{\lambda}{T}\right)^{q^d-1}\right) \neq \infty, \end{aligned}$$

una contradicción. Por lo tanto: $\left(q^d-1\right)\left(v_{\mathfrak{P}'}(\lambda) - v_{\mathfrak{P}'}(T)\right) = v_{\mathfrak{P}'}\left(\left(\frac{\lambda}{T}\right)^{q^d-1}\right) \geq v_{\mathfrak{P}'}\left(g_{d-1}\left(\frac{1}{T}\right)\right) = e\left(\mathfrak{P}' \mid \mathfrak{p}_\infty\right) v_\infty\left(g_{d-1}\left(\frac{1}{T}\right)\right) = (q-1)\left(q^d - 2q^{d-1}\right)$.

Entonces se tiene:

$$\begin{aligned} v_{\mathfrak{P}'}(\lambda) &\geq \frac{(q-1)\left(q^d - 2q^{d-1}\right)}{q^d-1} + v_{\mathfrak{P}'}(T) \\ &= \frac{(q-1)\left(q^d - 2q^{d-1}\right)}{q^d-1} + e\left(\mathfrak{P}' \mid \mathfrak{p}_\infty\right) v_\infty(T) \\ &= \frac{(q-1)\left(q^d - 2q^{d-1}\right)}{q^d-1} + (q-1)(-1) \\ &= \frac{(q-1)\left(q^d - 2q^{d-1}\right)}{q^d-1} - (q-1) \\ &= \frac{(q-1)\left(q^d - 2q^{d-1} - \left(q^d-1\right)\right)}{q^d-1} \\ &= (q-1)\frac{1-2q^{d-1}}{q^d-1} > -2. \end{aligned}$$

Luego $v_{\mathfrak{P}'}(\lambda) \geq -1$. En particular, si $v_{\mathfrak{P}'}(\lambda) < 0$, entonces $v_{\mathfrak{P}'}(\lambda) = -1$. Se tiene: $[K(\Lambda_P) : \mathbb{F}_q(\lambda)] = q^{d-1}$. Por lo tanto gr $\mathcal{Z}_\lambda$ = gr $\eta_\lambda = q^{d-1}$. Además $e_\infty = q-1$ y $\left(q-1, q^{d-1}\right) = 1$. En el denominador de λ hay q^{d-1} primos $\mathfrak{q}$, tales que $v_{\mathfrak{q}'} = -1$. Observemos que $\lambda \in \mathcal{O}_P$. Sea $A \in R_T$ tal que $\sigma_{A^{-1}}(\mathfrak{q}) = \mathfrak{B}'$, $\sigma_A(\lambda) = \lambda'$ y $\sigma_A \in G_P$. Entonces $v_{\mathfrak{B}'}(\lambda^A) = v_{\mathfrak{B}'^{A^{-1}}}(\lambda) = v_{\mathfrak{q}}(\lambda) = -1$. Tómese $\lambda_0 = \lambda^A$.

□

Definición 2.3.2. Sea $M \in R_T \setminus \{0\}$. Sea $K_M^+ = K(\Lambda_M)^+ = K(\Lambda_M)^{G_0}$. A $K(\Lambda_M)^+$ se le llama el *subcampo real maximal* de $K(\Lambda_M)$.

Nota 2.3.3. Se tiene $[K(\Lambda_M) : K(\Lambda_M)^+] = |G_0| = q-1$ y $\mathfrak{p}_\infty$ se descompone totalmente en $\Phi(M)/(q-1)$ divisores primos en $K(\Lambda_M)^+/K$.

Proposición 2.3.4. *Sea $M = P^n$ para algún polinomio irreducible P. Entonces $\mathcal{O}_M = R_T[\lambda_M]$, donde λ_M es un generador de Λ_M.*

Demostración. Sea $\lambda = \lambda_M$. Como λ es entero, tenemos $R_T[\lambda] \subseteq \mathcal{O}_M$. Sea $\alpha \in \mathcal{O}_M$. Se tiene que $\left\{1, \lambda, \ldots, \lambda^{\Phi(M)-1}\right\}$ es una base de $K(\Lambda_M/K)$. Luego existen $a_0, a_1, \ldots, a_h \in K$ tales que $\alpha = a_0 + a_1\lambda + \cdots + a_h\lambda^h$, donde $h = \Phi(M) - 1$. Debemos verificar que $a_i \in R_T$ para $i = 0, \ldots, h$. De la demostración de la proposición 2.1.21 se tiene que $v_{\mathfrak{P}}(\lambda) = 1$, donde $\mathfrak{P}$ es el único divisor primo

de $K(\Lambda_M)$ sobre $\mathfrak{p}$ y $(P)_K = \frac{\mathfrak{p}}{\mathfrak{P}_\infty^{\operatorname{gr} P}}$. Luego $v_{\mathfrak{P}}\left(a_i\lambda^i\right) = i + \Phi(M)v_{\mathfrak{p}}(a_i) \equiv i \pmod{\Phi(M)}$. Así, cuando $i \neq j$, $a_i \neq 0$ y $a_j \neq 0$, se tiene $v_{\mathfrak{P}}\left(a_i\lambda^i\right) \neq v_{\mathfrak{P}}\left(a_j\lambda^j\right)$. Entonces

$$0 \leq v_{\mathfrak{P}}(\alpha) = \min_{a_i \neq 0}\left\{v_{\mathfrak{P}}\left(a_i\lambda^i\right)\right\} = \min_{a_i \neq 0}\left\{i + \Phi(M)v_{\mathfrak{P}}(a_i)\right\}$$

Por lo tanto $v(a_i) \geq 0$ para todo i.

Ahora, para cualquier $\sigma_A \in G_M$ tal que $\sigma_A(\lambda) = \lambda^A$, se tiene

$$\alpha^A = \sigma_A(\alpha) = a_0 + a_1\lambda^A + \cdots + a_h\left(\lambda^A\right)^h, \tag{2.4}$$

donde $A \pmod{M} \in (R_T/(M))^*$.

Si $\left\{\bar{A}_1, \ldots, \bar{A}_{\Phi(M)}\right\}$ es un conjunto de representantes de $(R_T/(M))^*$, se obtiene de la ecuación (2.4), denotando $\alpha_i = \alpha^{A_i}$ y $\lambda_i = \lambda^{A_i}$, que $(\alpha_1, \ldots, \alpha_{\Phi(n)})^T = [\lambda_i^j]_{\substack{1 \leq i \leq h+1 \\ 0 \leq j \leq h}}(a_0, \ldots, a_n)^T$

El determinante de la matriz $[\lambda_i^j]$ con $1 \leq i \leq h+1$ y $0 \leq j \leq h$, es un determinante de Vandermonde, así que $\det[\lambda_i^j] = \prod_{1 \leq t < l \leq h+1}(\lambda_l - \lambda_t) = \Delta$. Luego $a_i = \frac{b_i}{\Delta}$, donde $b_i \in \mathcal{O}_M$.

Para todo A mód $(R_T/(M))^*$, se tiene $\lambda = \beta_A\lambda^A$ y $P = \beta_0\lambda^{\Phi(M)}$ para algunos $\beta_A, \beta_0 \in \mathcal{O}_M^*$.

Entonces para cualquier divisor primo $\mathfrak{q}$ en $K(\Lambda_M)$ que no divida a $\mathfrak{p}$ ni a $\mathfrak{p}_\infty$ se tiene $v_{\mathfrak{q}}(\lambda) = v_q\left(\lambda^A\right) = 0$. De esto se sigue que el soporte del divisor de polos de a_i puede consistir únicamente de $\mathfrak{p}$ y de $\mathfrak{p}_\infty$. Como $v_{\mathfrak{p}}(a_i) \geq 0$, se tiene que $a_i \in R_T$. Entonces $\mathcal{O}_M = R_T[\lambda_M]$. □

Teorema 2.3.5. *Sea $M \in R_T \setminus \{0\}$ y sea P un polinomio irreducible que no divide a M. Entonces el mapeo $\varphi_P : \Lambda_M \to \Lambda_M$ dado por $\lambda \mapsto \lambda^P$ corresponde al símbolo de Artin $[\frac{K(\Lambda_M)/K}{P}]$.*

Demostración. Sea $(R_T)_P$ la localización de P, es decir, $(R_T)_P = \left\{\frac{f}{g} \mid f, g \in R_T,\ P \nmid g\right\}$.
Si $(P)_K = \frac{\mathfrak{p}}{\mathfrak{p}_\infty^{\operatorname{gr} P}}$, entonces

$$K(\mathfrak{p}) = (R_T)_{(P)}/P(R_T)_{(P)} \cong R_T/(P) \cong \mathbb{F}_{q^d},$$

donde $d = \operatorname{gr} P$.

Sea $\mathfrak{P}$ divisor primo en $K(\Lambda_M)$ que divide a $\mathfrak{p}$. Entonces $N(\mathfrak{p}) = \left|\mathbb{F}_{q^d}\right| = q^d$ y $\Lambda_M \subseteq \mathcal{O}_{\mathfrak{P}}$.
Entonces $[\frac{K(\Lambda_M)/K}{P}](\lambda) \equiv \lambda^{q^d} \pmod{\mathfrak{P}}$. Luego

$$u^P = u\Psi_P(u) = u\left(u^{q^d-1} + \beta_{q^d-2}u^{q^d-2} + \cdots + \beta_1 u + \beta_0\right).$$

Entonces P divide a β_i para todo $0 \leq i \leq q^d - 2$. Por lo tanto $\lambda^P \equiv \lambda^{q^d} \pmod{\mathfrak{P}}$. Ahora, $u^M = \prod_{A \bmod M}\left(u - \lambda^A\right)$. Derivando respecto a u se tiene

$$M = \sum_{A \bmod M}\left(\prod_{B \neq A, B \bmod M}\left(u - \lambda^B\right)\right),$$

que es constante respecto a u. Tomando $u = \lambda^C$ se obtiene $M = \prod_{C \neq B} \left(\lambda^C - \lambda^B\right)$. Como P no divide a M, se sigue que $\lambda^C \not\equiv \lambda^B \pmod{\mathfrak{P}}$ cuando $C \not\equiv B \pmod{M}$.
Por lo tanto $\lambda^P \equiv \lambda^Q \pmod{\mathfrak{P}}$ y esto implica $\lambda^P = \lambda^Q$.
Por último, de $\lambda^P \equiv [\frac{K(\Lambda_M)/K}{P}](\lambda) \equiv \lambda^{q^d}$ tenemos $\varphi_P = [\frac{K(\Lambda_M)/K}{P}]$.

□

Capítulo 3

Fórmulas del diferente y del género

En este capítulo empezamos con definiciones y propiedades de extensiones de campos de funciones para poder definir la conorma. Se sigue con definiciones y propiedades del discriminante y del diferente para extensiones de campos de funciones y posteriormente se trabaja sobre dominios de Dedekind. Por último se encuentran fórmulas para el diferente de K_M/K y de K_M/K_M^+, las cuales se utilizan para hallar fórmulas para g_M y g_M^+, los géneros de los campos K_M y K_M^+ respectivamente.

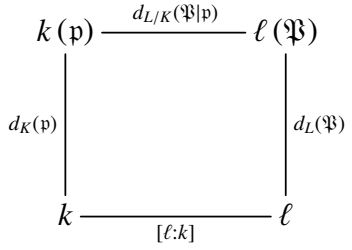
3.1. Extensiones de campos de funciones

Definición 3.1.1. Sean K/k y L/ℓ dos campos de funciones. Decimos que L es una *extensión de* K si $K \subseteq L$ y $\ell \cap K = k$.

Definición 3.1.2. Sea L/K una extensión de campos de funciones. Si $\mathfrak{p} \in \mathbb{P}_K$ y $\mathfrak{P} \in \mathbb{P}_L$ son tales que $\mathfrak{P}$ es una extensión de $\mathfrak{p}$, se define el *grado relativo* de $\mathfrak{P}$ sobre $\mathfrak{p}$ como $d_{L/K}(\mathfrak{P}|\mathfrak{p}) = [\ell(\mathfrak{P}) : k(\mathfrak{p})]$.

Proposición 3.1.3. *Sea L/K una extensión de campos. Si $d_L(\mathfrak{P}) = [\ell(\mathfrak{P}) : \ell]$ y $d_K(\mathfrak{p}) = [k(\mathfrak{p}) : k]$, entonces $d_L(\mathfrak{P})[\ell : k] = d_{L/K}(\mathfrak{P} \mid \mathfrak{p}) d_K(\mathfrak{p})$.*

Demostración. Se sigue del siguiente diagrama conmutativo



□

Además, del diagrama anterior tenemos que $d_{L/K}(\mathfrak{P} \mid \mathfrak{p}) < \infty \Leftrightarrow [\ell : k] < \infty$.

Consideremos una extensión L de K, $\mathcal{P}$ un lugar de L sobre K y $\mathcal{P}|_K = \mathfrak{p}$. Como las valuaciones son discretas y normalizadas, se tiene que $v_{\mathcal{P}} : L^* \to \mathbb{Z}$ y $v_{\mathfrak{p}} : K^* \to \mathbb{Z}$ son suprayectivas. Pero en general $v_{\mathcal{P}|_K}$ no es suprayectiva, así que $v_{\mathcal{P}}(K^*) = e\mathbb{Z}$, para algún $e \geq 1$. Por lo tanto $v_{\mathcal{P}}(x) = e v_{\mathfrak{p}}(x)$ para todo $x \in K$.

Definición 3.1.4. El número e obtenido en el párrafo anterior se llama *índice de ramificación* de $\mathcal{P}$ sobre $\mathfrak{p}$ y se denota $e = e(\mathcal{P}|\mathfrak{p}) = e_{L/K}(\mathcal{P}|\mathfrak{p})$.

Proposición 3.1.5. *Sea L/ℓ una extensión algebraica de K/k. Dado un lugar $\mathfrak{p} \in \mathbb{P}_K$, el número de extensiones de la valuación $v_{\mathfrak{p}}$ a L es finito.*

Demostración. Por el teorema de Riemman-Roch existe $x \in K \setminus k$ tal que el divisor de polos de $(x)_K$ es $\eta_{x,K} = \mathfrak{p}^n$ para algún $n \in \mathbb{N}$. Ahora $\mathfrak{P} \in \mathbb{P}_L$ extiende a $\mathfrak{p}$ si y sólo si $v_{\mathfrak{P}}(x) > 0$. Esto equivale a decir que $\mathfrak{P} \mid \eta_{x,L}$. Este último número es finito. □

Definición 3.1.6. Si L/ℓ es una extensión de K/k y si $\mathfrak{p} \in \mathbb{P}_K$, entonces si $\mathfrak{P}_1, \ldots, \mathfrak{P}_h$ son todas las extensiones de $\mathfrak{p}$ en L se define la *conorma* de K a L en $\mathfrak{p}$ por

$$\mathrm{con}_{K/L}(\mathfrak{p}) = \mathfrak{P}_1^{e_{L/K}(\mathfrak{P}_1|\mathfrak{p})} \cdots \mathfrak{P}_h^{e_{L/K}(\mathfrak{P}_h|\mathfrak{p})}.$$

Si $\mathfrak{A} \in D_K$ es un divisor, con $\mathfrak{A} = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_r^{\alpha_r}$ se define la *conorma* de $\mathfrak{A}$ como

$$\mathrm{con}_{K/L}(\mathfrak{A}) = \prod_{i=1}^{r} \mathrm{con}_{K/L}(\mathfrak{p}_i)^{\alpha_i}.$$

Teorema 3.1.7. *Para cualquier extensión L/ℓ de K/k, finita o infinita, si $\mathfrak{p} \in \mathbb{P}_K$ y $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$ son todas las extensiones de $\mathfrak{P}$ en L, entonces*

$$[L : K] = \sum_{i=1}^{h} e_{L/K}(\mathfrak{P}_i \mid \mathfrak{p})\, d_{L/K}(\mathfrak{P}_i \mid \mathfrak{p}).$$

Demostración. Si $[L : K] = \infty$, entonces $d_{L/K}(\mathfrak{p}_i \mid \mathfrak{p}) = \infty$ y la igualdad se cumple.

Supongamos que $[L : K] < \infty$. Sea $A := \sum_{i=1}^{h} e_{L/K}(\mathfrak{P}_i|\mathfrak{p}) d_{L/K}(\mathfrak{P}_i|\mathfrak{p})$ y sea $x \in K \setminus k$ tal que $(x)_K = \frac{\mathfrak{p}^{g+1}}{\mathfrak{q}} = \frac{\mathfrak{p}^{v_{\mathfrak{p}}(x)}}{\mathfrak{q}'}$, donde $\mathfrak{q}, \mathfrak{q}'$ son divisores enteros y $v_{\mathfrak{p}}(x) > 0$. Sea Entonces

$$(x)_L = \frac{(\mathcal{Z}_x)_L}{(\eta_x)_L} = \frac{\mathfrak{P}_1^{\alpha_1} \cdots \mathfrak{P}_h^{\alpha_h}}{(\eta_x)_L} = \frac{\mathfrak{P}_1^{v_{\mathfrak{P}_1}(x)} \cdots \mathfrak{P}_h^{v_{\mathfrak{P}_h}(x)}}{(\eta_x)_L}$$

$$\begin{aligned}
[L : \ell(x)] = d((\mathcal{Z}_x)_L) &= \sum_{i=1}^{h} v_{\mathfrak{P}_i}(x) d_L(\mathfrak{P}_i) \\
&= \sum_{i=1}^{h} v_{\mathfrak{p}}(x) e_{L/K}(\mathfrak{P}_i \mid \mathfrak{p}) d_L(\mathfrak{P}_i) \\
&= v_{\mathfrak{p}}(x) \left[\sum_{i=1}^{h} e_{L/K}(\mathfrak{P}_i \mid \mathfrak{p}) d_{L/K}(\mathfrak{P}_i \mid \mathfrak{p}) \right] \frac{d_K(\mathfrak{p})}{[\ell : k]} \\
&= v_{\mathfrak{p}}(x) \cdot A \cdot \frac{d_K(\mathfrak{p})}{[\ell : k]} \\
&= A \cdot \frac{d_K((\mathcal{Z}_x)_K)}{[\ell : k]} \\
&= A \cdot \frac{[K : k(x)]}{[\ell : k]} \\
&= A \cdot \frac{[K : k(x)]}{[\ell(x) : k(x)]} \\
[L : \ell(x)] &= A \cdot \frac{[K : k(x)]}{[\ell(x) : k(x)]}.
\end{aligned}$$

Entonces

$$A = \frac{[L : \ell(x)][\ell(x) : k(x)]}{[K : k(x)]} = \frac{[L : k(x)]}{[K : k(x)]} = [L : K].$$

□

Cuando L/K es una extensión de Galois se tiene que $d_{L/K}(\mathfrak{P}_i \mid \mathfrak{p}) = d_{L/K}\left(\mathfrak{P}_j \mid \mathfrak{p}\right)$ y $e_{L/K}(\mathfrak{P}_i \mid \mathfrak{p}) = e_{L/K}\left(\mathfrak{P}_j \mid \mathfrak{p}\right)$ para todo $1 \leq i, j \leq h$. Sean $f := d_{L/K}(\mathfrak{P}_i \mid \mathfrak{p})$, $e = e_{L/K}(\mathfrak{P}_i \mid \mathfrak{p})$, para todo $1 \leq i \leq h$. Entonces el teorema 3.1.7 toma la forma

$$[L : K] = efh.$$

Definición 3.1.8. Sea L/K una extensión de Galois con grupo de Galois $G = \mathrm{Gal}\,(L/K)$. Sea $\mathfrak{p} \in \mathbb{P}_K$ y $\mathfrak{P} \in \mathbb{P}_L$ una extensión de $\mathfrak{p}$. Se define:

1. $D = D_{L/K}(\mathfrak{P} \mid \mathfrak{p}) := \{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\}$ = *grupo de descomposición* de L/K.

2. $I = I_{L/K}(\mathfrak{P} \mid \mathfrak{p}) := \{\sigma \in G \mid \sigma x \equiv x \text{ mód } \mathfrak{P} \text{ para todo } x \in \mathcal{O}_{\mathfrak{P}}\}$ = *grupo de inercia* de L/K.

Nota 3.1.9. Como en el caso de campos numéricos se tiene $I \subseteq D$, $|I| = e = e_{L/K}(\mathfrak{P} \mid \mathfrak{p})$, $|D| = ef$, donde $f = d_{L/K}(\mathfrak{P} \mid \mathfrak{p})$. Además

$$D/I \cong \mathrm{Gal}\ (\ell(\mathfrak{P})/k(\mathfrak{p})) \text{ y } D \cong \mathrm{Gal}\,(L_{\mathfrak{P}} \mid K_{\mathfrak{p}}),$$

donde $L_{\mathfrak{P}}$ y $K_{\mathfrak{p}}$ son las completaciones de L y K en $\mathfrak{P}$ y $\mathfrak{p}$ respectivamente.

3.2. Discriminante, diferente y género

Sean L/K una extensión separable de campos de funciones, $\mathfrak{P}$ un lugar de L y $\mathfrak{p} := \mathfrak{P}\,|_K$. Sean $L_{\mathfrak{P}}$ y $L_{\mathfrak{p}}$ las respectivas completaciones. Se tiene que $[L_{\mathfrak{P}} : L_{\mathfrak{p}}] = e_{L/K}(\mathfrak{P} \mid \mathfrak{p})\, d_{L/K}(\mathfrak{P} \mid \mathfrak{p})$. Sea $\tilde{L}$ la cerradura de Galois de L/K y sea $\mathfrak{B}$ un lugar en $\tilde{L}$ sobre $\mathfrak{P}$.
Sea $\mathcal{O}_{\hat{\mathfrak{P}}} = \{x \in L_{\mathfrak{P}} \mid v_{\mathfrak{P}}(x) \geq 0\}$ la completación de $\mathcal{O}_{\mathfrak{P}}$ y $\hat{\mathfrak{B}} = \{x \in L_{\mathfrak{P}} \mid v_{\mathfrak{P}}(x) > 0\}$ la completación de $\mathfrak{p}$. Si $\mathrm{Tr} = \mathrm{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$ denota la traza de $L_{\mathfrak{P}}$ a $K_{\mathfrak{p}}$ se tiene:

Teorema 3.2.1. *Existe $m \in \mathbb{Z}$, $m \geq 0$ tal que si $x \in L_{\mathfrak{P}}$ satisface $v_{\mathfrak{P}}(x) \geq -m$, entonces $v_{\mathfrak{p}}(\mathrm{Tr}\,(x)) \geq 0$ y existe $x_0 \in L_{\mathfrak{P}}$ tal que $v_{\mathfrak{P}}(x_0) < -m$ y $v_{\mathfrak{p}}(\mathrm{Tr}\,(x_0)) < 0$.*

Demostración. Si $v_{\mathfrak{P}}(x) \geq 0$, entonces $x \in \mathcal{O}_{\mathfrak{P}}$. Por lo que $\mathrm{Tr}\,(x) \in \mathcal{O}_{\mathfrak{p}}$ y $v_{\mathfrak{p}}(\mathrm{Tr}\,x) \geq 0$.
Por otro lado, sea $y \in \mathcal{O}_{\mathfrak{p}}$ tal que $\mathrm{Tr}\,(y) \neq 0$. Este elemento y existe porque la extensión $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ es separable. Si $x \in K$ es tal que $v_{\mathfrak{p}}(x) < -v_{\mathfrak{p}}(\mathrm{Tr}\,(y))$ tenemos:

$$v_{\mathfrak{p}}(\mathrm{Tr}\,(xy)) = v_{\mathfrak{p}}(x\mathrm{Tr}\,(y)) = v_{\mathfrak{p}}(x) + v_{\mathfrak{p}}(\mathrm{Tr}\,(y)) < 0.$$

Sea

$$A = \{n \in \mathbb{Z} \mid v_{\mathfrak{p}}(x) \geq n \Rightarrow v_{\mathfrak{p}}(\mathrm{Tr}\,(x)) \geq 0\}.$$

Se observa que $0 \in A$, $\mathbb{N} \subseteq A$, pero existe $n \in \mathbb{Z}$ tal que $n < 0$ y $n \notin A$. También si $n_0 \notin A$ entonces $n_0 - 1 \notin A$ pues $v_{\mathfrak{P}}(x) \geq n_0$, entonces $v_{\mathfrak{P}}(x) \geq n_0 - 1$. Sea $t = \inf A$. Tenemos que $t \in \mathbb{Z}$ y $t \leq 0$. Sea $m = -t$. Entonces $m \geq 0$ y si $x \in L_{\mathfrak{P}}$ es tal que $v_{\mathfrak{P}}(x) \geq -m = t \in A$, entonces $v_{\mathfrak{p}}(\mathrm{Tr}\,(x)) \geq 0$. Por

otro lado, como $t-1 \notin A$, existe $x \in L_{\mathfrak{P}}$ tal que $v_{\mathfrak{P}}(x) \geq t-1 = -m-1$ y $v_{\mathfrak{p}}(\mathrm{Tr}\,(x)) < 0$.
Si $v_{\mathfrak{P}}(x) > t-1$, entonces $v_{\mathfrak{P}}(x) \geq t = -m$ y esto contradice que $t \in A$. Por lo tanto $v_{\mathfrak{P}}(x) = t-1 = -m-1 < -m$. □

Definición 3.2.2. El máximo entero no negativo que satisface las condiciones del teorema 3.2.1 se denota por $m(\mathfrak{P})$ y es llamado *exponente diferencial* de $\mathfrak{P}$ con respecto a K.

Teorema 3.2.3. *Se tiene que* $m(\mathfrak{P}) \geq e-1 = e_{L/K}(\mathfrak{P}|\mathfrak{p})-1$. *Si además* k *es perfecto, tenemos* $m(\mathfrak{P}) > e-1$ *si y sólo si la característica de* k *divide a* e. *En particular* $m(\mathfrak{P}) = 0$ *si* $\mathfrak{P}$ *no es ramificado.*

Demostración. Ver [17], teorema 5.6.3, pp. 148. □

Definición 3.2.4. Se dice que $\mathfrak{P}$ es *moderadamente ramificado* si $p \nmid e$ y *salvajemente ramificado* si $p \mid e$, donde p es la característica de k.

Teorema 3.2.5. *Se tiene que* $m(\mathfrak{P}) = 0$ *para todos excepto un número finito de lugares* $\mathfrak{P}$.

Demostración. Si $\mathfrak{P}$ es un lugar no ramificado separable, entonces $m(\mathfrak{P}) = e_{L/K}(\mathfrak{P} \mid \mathfrak{p}) - 1 = 1 - 1 = 0$. Entonces por el Teorema 3.2.3, el número de lugares $\mathfrak{P}$ que son ramificados o inseparables es finito. □

Definición 3.2.6. El divisor

$$\mathfrak{D}_{L/K} := \prod_{\mathfrak{P} \in \mathbb{P}_L} \mathfrak{P}^{m(\mathfrak{P})}$$

se llama el *diferente* de la extensión L/K y se tiene que $\mathfrak{P} \mid \mathfrak{D}_{L/K}$ si y sólo si $\mathfrak{P}$ es ramificado. El *discriminante* $\delta_{L/K}$ de la extensión L/K se define como la norma del diferente

$$\delta_{L/K} := N_{L/K}\left(\mathfrak{D}_{L/K}\right).$$

Ahora veremos diferentes y discriminantes en dominios de Dedekind. Recordemos que un dominio entero es un anillo conmutativo con unidad y sin divisores de cero.

Definición 3.2.7. Sea A un dominio entero y sea K el campo de cocientes de A. Entonces A es un *dominio de Dedekind* si satisface:

1. Cada ideal primo no cero $\mathfrak{P}$ es maximal.

2. A es noetheriano.

3. A es enteramente cerrado, es decir, si $x \in K$ satisface una relación $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$, con $a_i \in A$, entonces $x \in A$.

Sea A un dominio de Dedekind, luego todo ideal $\mathfrak{A} \neq 0$ de A se expresa como producto de ideales primos no cero de A de manera única.

Definición 3.2.8. Se definen los *divisores* de A como los ideales fraccionarios no cero de A, donde un *ideal fraccionario* $M \neq 0$ es un $A-$módulo contenido en K y tal que existe $\alpha \in A$, $\alpha \neq 0$ tal que $\alpha M \subseteq A$.

Un ideal fraccionario M es invertible si existe un ideal fraccionario M' tal que $MM' = A$.

Sea $K = \operatorname{coc} A$ y sea L/K una extensión separable con $[L : K] = n$.
Sea

$$\begin{aligned} B &= \{x \in L \mid x \text{ es entero sobre } A\} \\ &= \left\{x \in L \mid \text{ existe una relación } x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0, \text{ con } a_{n-1}, \ldots, a_0 \in A\right\}. \end{aligned}$$

Es decir, B es la cerradura entera de A en L.
Se tiene el siguiente diagrama:

$$\begin{array}{ccc} B & \text{———} & L \\ | & & | \\ | & & | \\ A & \text{———} & K \end{array}$$

Entonces B es un dominio de Dedekind y $\operatorname{coc} B = L$. Además B es un $A-$módulo libre de rango $n = [L : K]$. Esto es $B \cong A^n$ como $A-$módulo. Sea C un $A-$módulo libre generado por $\{e_1, \ldots, e_n\}$, es decir, $C = \bigoplus_{i=1}^{n} Ae_i$. Sea $\operatorname{Tr} : L \to K$ la traza, es decir, $\operatorname{Tr}(x) = \sum_{\sigma \in H} \sigma x$, donde $H = \left\{\sigma : L \to \overline{K} \mid \sigma \mid_K = \mathbf{1}_K\right\}$ y $|H| = n$. Como L/K es separable, tenemos Tr es suprayectiva.

Definición 3.2.9. Se define el *discriminante* como

$$\begin{aligned} \delta_{B/A} &= \langle \det \left[\operatorname{Tr}(e_i e_j)\right]_{1 \leq i,j \leq n} \rangle \\ &= \langle \det \left[\sigma e_i\right]_{1 \leq i \leq n, \sigma \in H} \rangle^2. \end{aligned}$$

Observamos que δ es independiente de la base $\{e_i, \ldots, e_n\}$ de B sobre A.

Definición 3.2.10. Para $M \subseteq L$, sea $M^* = \{y \in L \mid \text{Tr}\,(xy) \in A \text{ para todo } x \in L\}$. A M^* se le llama el *codiferente* de M sobre A.

Veamos algunas propiedades de M^*.

1. Se tiene $C \subseteq B \subseteq B^* \subseteq C^*$.

2. Como C^* es un $A-$módulo libre generado por la base dual de $\{e_1, \ldots, e_n\}$ con respecto a la forma bilineal no degenerada Tr (xy), entonces C^* es noetheriano. Por lo que B es finitamente generado como $A-$módulo. En particular B es noetheriano.

3. B es enteramente cerrado.

   Demostración. Sea $\alpha \in L$ tal que para cada $b_i \in B$ se satisface $\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 = 0$. Entonces como B es finitamente generado, $A[\alpha]$ es finitamente generado. Sea $A[\alpha] = \langle x_1, x_2, \ldots, x_n\rangle$. Entonces $\alpha x_i = \sum_{j=1}^{m} a_{ij}x_j$ para $1 \leq i \leq m$. Luego $\sum_{j=1}^{m} \left(\delta_{ij}\alpha - a_{ij}\right) x_j = 0$ donde

   $$\delta_{ij} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j. \end{cases}$$

   Ahora, si $M = [\delta_{ij}\alpha - a_{ij}]_{1\leq i,j\leq m}$, sea N la matriz adjunta de M. Entonces $NM = (\det M)\, I_n$ y $(\det M)\, x_i = 0$ para $1 \leq i \leq m$. Pero $1 \in A \subseteq A[\alpha]$, entonces $\det M = (\det M) \cdot 1 = 0$.
   Por otra parte tenemos que $\det M = \alpha^n + C_{n-1}\alpha^{n-1} + \cdots + C_1\alpha + C_0 = 0$, con $c_i \in A$. Con esto se tiene que $\alpha \in B$ y por lo tanto B es enteramente cerrado.

   □

4. Todo ideal primo no cero de B es maximal.

   Demostración. Sea $\mathfrak{P}$ ideal primo no cero de B y suponemos que $\mathfrak{P}$ no es maximal. Sea $\mathfrak{C}$ ideal maximal de B tal que $\mathfrak{P} \subsetneq \mathfrak{C} \subsetneq B$. Notemos que $\mathfrak{P} \cap A$ es un ideal primo no cero de A, entonces $\mathfrak{C} \cap A$ también lo es.
   Como A es un dominio de Dedekind y $\mathfrak{P} \cap A$ es ideal primo de A, entonces $\mathfrak{P} \cap A = \mathfrak{A} \cap A$.
   Ahora sea $x \in \mathfrak{C} \setminus \mathfrak{P}$. Entonces $x \in B$ y se cumple la relación $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$, con $a_i \in A$ y $a_0 \neq 0$. Entonces se tiene que $a_0 \in A \cap \mathfrak{C} = A \cap \mathfrak{P}$, es decir, $a_0 = -x\left(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_2x + a_1\right) \in \mathfrak{P}$.
   Como $x \notin \mathfrak{P}$ se tiene $x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_2x + a_1 \in \mathfrak{P}$. Así se tiene que $a_1 \in A \cap \mathfrak{C} = A \cap \mathfrak{P}$

y entonces $x\left(x^{n-2}+a_{n-1}x^{n-3}+\cdots+a_3x+a_2\right)\in\mathfrak{P}$.
Continuando de esta forma se tiene que $a_0,\ldots,a_{n-1}\in\mathfrak{P}$. Por lo tanto $x+a_{n-1}\in\mathfrak{P}$ y con esto $x\in\mathfrak{P}$ que contradice la elección de x. Por lo tanto $\mathfrak{P}$ es un ideal maximal. □

Con esto se tiene que B es un dominio de Dedekind.

Observamos que B^* es un $A-$módulo finitamente generado. Como $B\subseteq B^*\subseteq L$, el $B-$módulo B^* es finitamente generado y en consecuencia es un ideal fraccionario.

Por definición B^* es el máximo $B-$módulo contenido en L tal que $\mathrm{Tr}\,(B^*)\subseteq \mathrm{A}$. En particular $B\subseteq B^*$ pues $\mathrm{Tr}\,(B)\subseteq A$ y B^* es un ideal fraccionario de B.

Definición 3.2.11. Sean A un dominio de Dedekind y $K=\mathrm{coc}\,A$. Sea L/K una extensión finita separable y B la cerradura entera de A en L. Se define

$$\mathfrak{D}_{B/A}^{-1}=\{\alpha\in L\mid \alpha B^*\subseteq B\}.$$

Notemos que $\mathfrak{D}_{B/A}^{-1}$ es un $B-$módulo fraccionario y su inverso $\mathfrak{D}_{B/A}$ es un ideal de B llamado el *diferente* de B sobre A. La norma $N_{L/K}\mathfrak{D}_{B/A}$ se llama el *discriminante* de B sobre A.

Proposición 3.2.12. *1. Para una torre de campos $K\subseteq L\subseteq M$ se tiene $\mathfrak{D}_{M/K}=\mathfrak{D}_{M/L}\mathrm{con}_{L/M}\mathfrak{D}_{\mathrm{L/K}}$.*

2. Para un subconjunto multiplicativo S de A, entonces $\mathfrak{D}_{S^{-1}B/S^{-1}A}=S^{-1}\mathfrak{D}_{B/A}$.

3. Si $\mathfrak{P}|\mathfrak{p}$ son ideales primos de B y A respectivamente y $B_{\mathfrak{P}}$ y $A_{\mathfrak{p}}$ son las completaciones asociadas, entonces $\mathfrak{D}_{B/A}B_{\mathfrak{P}}=\mathfrak{D}_{B_{\mathfrak{P}}/A_{\mathfrak{p}}}$.

Demostración. 1. Sea $A\subseteq K$, $B\subseteq L$ cerradura entera de A en L y $C\subseteq M$ cerradura entera de A en M. Entonces basta ver que $\mathfrak{C}_{C/A}=\mathfrak{C}_{C/B}\mathfrak{C}_{B/A}$, donde $\mathfrak{C}_{C/A}=\{x\in L|\ \mathrm{Tr}\,(xC)\subseteq A\}$.
La inclusión $\subseteq$ se tiene por lo siguiente: $\mathrm{Tr}_{M/K}(\mathfrak{C}_{C/B}\mathfrak{C}_{B/A}C)=\mathrm{Tr}_{L/K}\mathrm{Tr}_{M/L}(\mathfrak{C}_{C/B}\mathfrak{C}_{B/A}C)=\mathrm{Tr}_{L/K}(\mathfrak{C}_{B/A}\mathrm{Tr}_{M/L}(\mathfrak{C}_{C/B}C))\subseteq A$.
Como $BC=C$, tenemos $\mathrm{Tr}_{M/K}(\mathfrak{C}_{C/A}C)=\mathrm{Tr}_{L/K}(B\mathrm{Tr}_{M/L}(\mathfrak{C}_{C/A}))\subseteq A$. Luego $\mathrm{Tr}_{M/L}(\mathfrak{C}_{C/A}C)\subseteq\mathfrak{C}_{B/A}$ y por lo tanto $\mathrm{Tr}_{M/L}\left(\mathfrak{C}_{B/A}^{-1}\mathfrak{C}_{C/A}C\right)=\mathfrak{C}_{B/A}^{-1}\mathrm{Tr}_{M/L}(\mathfrak{C}_{C/A}C)\subseteq B$. Esto implica que $\mathfrak{C}_{B/A}^{-1}\mathfrak{C}_{C/A}\subseteq\mathfrak{C}_{C/B}$ y así se tiene $\mathfrak{C}_{C/A}\subseteq\mathfrak{C}_{C/B}\mathfrak{C}_{B/A}$.

2. Si $x\in\mathfrak{D}_{B/A}^{-1}$, entonces $\mathrm{Tr}\,(xB)\subseteq A$. Esto implica que $\mathrm{Tr}\,(S^{-1}xB)=S^{-1}\mathrm{Tr}\,(xB)\subseteq S^{-1}A$ y viceversa.

3. Por la parte 2 de la proposición puedo suponer que A es un anillo de valuación discreta. Veamos que $\mathfrak{C}_{B/A}$ es denso en $\mathfrak{C}_{B_\mathfrak{P}/A_\mathfrak{p}}$. Para esto usamos la fórmula

$$\mathrm{Tr}_{L/K} = \sum_{\mathfrak{P}|\mathfrak{p}} \mathrm{Tr}_{L_\mathfrak{P}/K_\mathfrak{p}}$$

Sean $x \in \mathfrak{C}_{B/A}$ y $y \in B_\mathfrak{P}$. Por el teorema de aproximación se puede encontrar $\eta \in L$ cercano a y con respecto a $v_\mathfrak{P}$ y cercano a 0 con respecto a $v_{\mathfrak{P}'}$ para $\mathfrak{P}'|\mathfrak{p}$ y $\mathfrak{P}' \neq \mathfrak{P}$. Tenemos

$$\mathrm{Tr}_{L/K}(x\eta) = \mathrm{Tr}_{L_\mathfrak{P}/K_\mathfrak{p}}(x\eta) + \sum_{\mathfrak{P}' \neq \mathfrak{P}} \mathrm{Tr}_{L_{\mathfrak{P}'}/K_\mathfrak{p}}(x\eta).$$

Entonces $\mathrm{Tr}_{L_\mathfrak{P}/K_\mathfrak{p}}(x\eta)$ pertenece a $A_\mathfrak{p}$ ya que $\mathrm{Tr}_{L/K}(x\eta) \in A \subseteq A_\mathfrak{p}$. Lo mismo es cierto para $\mathrm{Tr}_{L_{\mathfrak{P}'}/K_\mathfrak{p}}(x\eta)$ ya que estos elementos son cercanos a 0 con respecto a $v_\mathfrak{p}$. Por lo tanto $\mathrm{Tr}_{L_\mathfrak{P}/K_\mathfrak{p}}(xy) \in A_\mathfrak{p}$. Con esto se tiene que $\mathfrak{C}_{B/A} \subseteq \mathfrak{C}_{B_\mathfrak{P}/A_\mathfrak{p}}$.
Recíprocamente, si $x \in \mathfrak{C}_{B_\mathfrak{P}/A_\mathfrak{p}}$ y si $\xi \in L$ es suficientemente cercano a x con respecto a $v_{\mathfrak{P}'}$, para $\mathfrak{P}' \neq \mathfrak{P}$, entonces $\xi \in \mathfrak{C}_{B/A}$. Esto se da porque si $y \in B$, entonces $\mathrm{Tr}_{L_\mathfrak{P}/K_\mathfrak{p}}(\xi y) \in A_\mathfrak{p}$, ya que $\mathrm{Tr}_{L_\mathfrak{P}/K_\mathfrak{p}}(xy) \in A_\mathfrak{p}$. De la misma manera $\mathrm{Tr}_{L_{\mathfrak{P}'}/K_\mathfrak{p}}(\xi y) \in A_\mathfrak{p}$ para $\mathfrak{P}'|\mathfrak{P}$, ya que hay elementos que son cercanos a 0. Por lo tanto $\mathrm{Tr}_{L/K}(\xi y) \in A_\mathfrak{p} \cap K = A$, es decir, $\xi \in \mathfrak{C}_{B/A}$. Con esto se tiene que $\mathfrak{C}_{B/A}$ es denso en $\mathfrak{C}_{B_\mathfrak{P}/A_\mathfrak{p}}$, es decir, $\mathfrak{C}_{B/A}B_\mathfrak{P} = \mathfrak{C}_{B_\mathfrak{P}/A_\mathfrak{p}}$ y así $\mathfrak{D}_{B/A}B_\mathfrak{P} = \mathfrak{D}_{B_\mathfrak{P}/A_\mathfrak{p}}$.

□

Teorema 3.2.13. $N_{L/K}(\mathfrak{D}_{L/K}) = \delta_{L/K}$.

Demostración. Sea S un subconjunto multiplicativo de A. Entonces

$$\delta_{S^{-1}B/S^{-1}A} = S^{-1}\delta_{B/A} \text{ y } \mathfrak{D}_{S^{-1}B/S^{-1}A} = S^{-1}\mathfrak{D}_{B/A}.$$

Entonces se puede suponer que A es un anillo de valuación discreta completo. Como A es un dominio de ideales principales, se tiene que B también lo es. Luego B admite una base entera $\{\alpha_1, \ldots, \alpha_n\}$. Así se tiene $\delta_{L/K} = (d(\alpha_1, \ldots, \alpha_n))$.
El codiferente $\mathfrak{C}_{B/A}$ es generado por la base dual $\{\alpha_1', \ldots, \alpha_n'\}$ que está caracterizada por $\mathrm{Tr}_{L/K}\left(\alpha_i\alpha_j'\right) = \delta_{ij}$. En otras palabras, $\mathfrak{C}_{B/A}$ es un ideal principal (β) y admite la $A-$base $\{\beta\alpha_1, \ldots, \beta\alpha_n\}$ del discriminante

$$d(\beta\alpha_1, \ldots, \beta\alpha_n) = \mathrm{N}_{L/K}(\beta)^2 d(\alpha_1, \ldots, \alpha_n).$$

Pero $(\mathrm{N}_{L/K}(\beta)) = \mathrm{N}_{L/K}(\mathfrak{C}_{B/A}) = \mathrm{N}_{L/K}\left(\mathfrak{D}_{L/K}^{-1}\right)$, y $(d(\alpha_1, \ldots, \alpha_n)) = \delta_{L/K}$.
Entonces se tiene

$$d(\alpha_1,\ldots,\alpha_n) = \det\left(\left(\sigma_i\alpha_j\right)\right)^2,\ d\left(\alpha_1',\ldots,\alpha_n'\right) = \det\left(\left(\sigma_i\alpha_j'\right)\right)^2,$$

para $\sigma_i \in \mathrm{Hom}_K\left(L,\overline{K}\right)$ y $\mathrm{Tr}\left(\alpha_i\alpha_j\right) = \delta_{ij}$.
Entonces $d(\alpha_1,\ldots,\alpha_n)\cdot d\left(\alpha_1',\ldots,\alpha_n'\right) = 1$. Así obtenemos $\delta_{L/K}^{-1} = \left(d(\alpha_1,\ldots,\alpha_n)^{-1}\right) = \left(d\left(\alpha_1',\ldots,\alpha_n'\right)\right) = (d(\beta\alpha_1,\ldots,\beta\alpha_n)) = \mathrm{N}_{L/K}\left(\mathfrak{D}_{L/K}\right)^{-2}\delta_{L/K}$.
Por lo tanto $\mathrm{N}_{L/K}\left(\mathfrak{D}_{L/K}\right) = \delta_{L/K}$. □

Teorema 3.2.14. *Sea A un dominio de Dedekind y $K = \mathrm{coc}\,\mathrm{A}$. Sea $L = K(\alpha)$ una extensión de campos finita y separable de grado n y sea B la cerradura entera de A en L. Si $B = A[\alpha]$, entonces $\mathfrak{D}_{B/A} = (P'(\alpha))$, donde $P(x) = \mathrm{Irr}(\alpha, x, K)$.*

Demostración. Ver [17], teorema 5.7.17, pp. 158. □

Proposición 3.2.15. *D_K = divisores de K = ideales fraccionarios de K.*
Sean $\mathfrak{A} \in D_K$, $\mathfrak{B} \in D_L$. Los siguientes enunciados son equivalentes:

1. $\mathrm{Tr}(\mathfrak{B}) \subseteq \mathfrak{A}$.
2. $\mathfrak{B} \subseteq \mathfrak{A}\mathfrak{D}_{L|K}^{-1}$.

Demostración. Si $\mathfrak{A} = 0$, entonces $\mathfrak{B} = 0$ y se tiene la equivalencia (1) $\Leftrightarrow$ (2).
Si $\mathfrak{A} \neq 0$, entonces
$\mathrm{Tr}(\mathfrak{B}) \subseteq \mathfrak{A} \Leftrightarrow \mathfrak{A}^{-1}\mathrm{Tr}(\mathfrak{B}) \subseteq \mathfrak{A}^{-1}\mathfrak{A} = A \Leftrightarrow \mathrm{Tr}\left(\mathfrak{A}^{-1}\mathfrak{B}\right) \subseteq A \Leftrightarrow \mathfrak{A}^{-1}\mathfrak{B} \subseteq \mathfrak{D}_{L|K}^{-1} \Leftrightarrow \mathfrak{B} \subseteq \mathfrak{A}\mathfrak{D}_{L|K}^{-1}$. □

Nota 3.2.16. Si $\mathfrak{p}$ es un ideal primo en A, entonces $\mathrm{con}_{A/B}\mathfrak{p} = \mathfrak{p}B = \mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_h^{e_h}$.

Definición 3.2.17. $\mathfrak{P}_i$ se llama *ramificado* si $e_i > 1$ y $\mathfrak{p}$ se llama *ramificado* si algún $e_i > 1$.

Teorema 3.2.18. *Sean $\mathfrak{P}$ un ideal primo de B y $\mathfrak{p} = \mathfrak{P} \cap A$. $\mathfrak{P}$ es ramificado si y sólo si $\mathfrak{P} \mid \mathfrak{D}_{B/A}$.*

Demostración. Ver [15], teorema 1, pp. 53. □

Corolario 3.2.19. *Sea $\mathfrak{p}$ primo de A. Entonces $\mathfrak{p}$ es ramificado si y sólo si $\mathfrak{p} \mid \delta_{B/A}$.*

Demostración. Se sigue del teorema 3.2.18, tomando normas. □

Corolario 3.2.20. *Casi todo $\mathfrak{P}$ de B y casi todo $\mathfrak{p}$ de A son no ramificados.*

Demostración. $\mathfrak{D}_{B/A}$ y $\delta_{B/A}$ son ideales, entonces son generados por un número finito de ideales primos y como $\mathfrak{P}$ es ramificado si y sólo si $\mathfrak{P} \mid \mathfrak{D}_{B/A}$, entonces el conjunto de tales $\mathfrak{P}$ es finito. □

Teorema 3.2.21. *Sea $\mathfrak{P}$ un ideal primo no cero de B y sea $\mathfrak{p} = \mathfrak{P} \cap A$. Sean $L(\mathfrak{P}) = B/\mathfrak{P}B$, $K(\mathfrak{p}) = A/\mathfrak{p}A$ los campos residuales. Se supone que $L(\mathfrak{P})/K(\mathfrak{p})$ es separable. Entonces si $\mathfrak{p}B = \mathfrak{P}^{e_1}\mathfrak{P}_2^{e_2}\dots\mathfrak{P}_h^{e_h}$, se tiene que el exponente de $\mathfrak{P}$ en $\mathfrak{D}_{B|A}$ es mayor o igual a $e_{\mathfrak{P}} - 1$. Se tiene la igualdad si y sólo si $p \nmid e_{\mathfrak{P}}$, donde p es la característica de $A/\mathfrak{p}A$.*

Demostración. Ver [15], proposición 13, pp. 58. □

Resumiendo, se tiene que si $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ son todos los primos de B ramificados, entonces $\mathfrak{D}_{B|A} = \mathfrak{P}_1^{e_1^*-1} \cdots \mathfrak{P}_r^{e_r^*-1}$, con $e_i^* = e_i$ si $p \nmid e_i$ y $e_i^* > e_i$ si $p \mid e_i$.
En el caso de campos de funciones se tiene que si L/K es una extensión finita, no tenemos de manera natural a A o B, pero tenemos $\mathcal{O}_{\mathfrak{p}}$ y $\mathcal{O}_{\mathfrak{P}}$ para cada primo $\mathfrak{P}$ de L y $\mathfrak{P}|_K = \mathfrak{p}$.
En este caso si $L_{\mathfrak{P}}$ y $K_{\mathfrak{p}}$ son las completaciones, entonces se tiene la siguiente situación:

$$\begin{array}{ccc} \hat{B} = \mathcal{O}_{\hat{\mathfrak{P}}} & \text{——} & L_{\mathfrak{P}} \\ \Big| & & \Big| \\ \hat{A} = \mathcal{O}_{\hat{\mathfrak{p}}} & \text{——} & K_{\mathfrak{p}} \end{array}$$

Tenemos $e_{\mathfrak{P}}$ = índice de ramificación de $\mathfrak{P}$ en B = índice de ramificación de $\hat{\mathfrak{P}}$ en $\hat{B}$. Además $L(\mathfrak{P}) = L_{\mathfrak{P}}(\hat{\mathfrak{P}})$ y $K(\mathfrak{p}) = K_{\mathfrak{p}}(\hat{\mathfrak{p}})$. Con esto puedo calcular $\mathfrak{D}_{\hat{B}|\hat{A}} = \hat{\mathfrak{P}}^{e_{\mathfrak{P}}^*-1}$. Así

$$\mathfrak{D}_{L/K} = \prod_{\mathfrak{P} \text{ ramificado}} \mathfrak{P}^{e_{\mathfrak{P}}^*-1}.$$

Ahora veremos la fórmula del género.

Teorema 3.2.22. *Sea L/K una extensión finita, geométrica y separable de campos de funciones. Sea ω una diferencial no cero de K y $\Omega = \operatorname{cotr}_{K/L}\omega$. Entonces $\Omega \neq 0$ y $(\Omega_L) = \mathcal{D}_{L/K}\operatorname{con}_{K/L}(\omega)_K$.*

Demostración. Ver [17], teorema 9.4.1, pp. 307. □

Corolario 3.2.23. ***(Fórmula de Riemann-Hurwitz)*** *Sea L/K una extensión finita, geométrica y separable de campos de funciones. Entonces*

$$2g_L - 2 = [L : K](2g_K - 2) + d_L(\mathfrak{D}_{L/K}).$$

Demostración.

$$\begin{aligned} 2g_L - 2 &= \mathrm{d}_L((\operatorname{cotr}\omega)_L) = \operatorname{gr}(\operatorname{con}_{K/L}(\omega)_K) + \mathrm{d}_L(\mathfrak{D}_{L/K}) \\ &= [L : K]\mathrm{d}_K((\omega)_K) + \mathrm{d}_L(\mathfrak{D}_{L/K}) \\ &= [L : K](2g_K - 2) + \mathrm{d}_L(\mathfrak{D}_{L/K}). \end{aligned}$$

□

3.3. Caso K_M y K_M^+

Calcularemos los diferentes de campos de funciones ciclotómicas y de sus subcampos reales maximales.

Sea $M \in R_T \setminus \{0\}$, M mónico y no constante, esto es $M \notin \mathbb{F}_q^*$. Sean $K = \mathbb{F}_q(T)$ y $K_M = K(\Lambda_M)$ el campo de funciones ciclotómico determinado por M. Sea K_M^+ el subcampo real maximal de K_M. Sea $\mathfrak{D}_{K_M/K}$ el diferente de la extensión K_M/K y sea g_M el género de K_M.

Teorema 3.3.1. ***(Fórmulas del diferente)*** *Sea $M = \prod_{i=1}^{r} P_i^{n_i}$ la factorización de $M \in R_T$ en potencias de irreducibles y $d_i = \operatorname{gr} P_i$. Los diferentes $\mathfrak{D}_{K_M/K}$ y $\mathfrak{D}_{K_M/K_M^+}$ están dados por las siguientes fórmulas:*

$$\mathfrak{D}_{K_M/K} = \prod_{i=1}^{r} con_{K_{P_i^{n_i}}/K_M} \mathfrak{P}_i^{s_i} \prod_{\mathfrak{B}_\infty|\mathfrak{p}_\infty} \mathfrak{B}_\infty^{q-2}, \tag{3.1}$$

$$\mathfrak{D}_{K_M/K_M^+} = \mathfrak{P}_1^{q-2} \prod_{\mathfrak{B}_\infty|\mathfrak{p}_\infty} \mathfrak{B}_\infty^{q-2} \; si \; r = 1, \tag{3.2}$$

$$\mathfrak{D}_{K_M/K_M^+} = \prod_{\mathfrak{B}_\infty|\mathfrak{p}_\infty} \mathfrak{B}_\infty^{q-2} \; si \; r \geq 2, \tag{3.3}$$

donde $\mathfrak{P}_i$ es el único divisor primo de $K_{P_i^{n_i}}$ sobre $\mathfrak{p}_i$, el divisor primo asociado a P_i y $\mathfrak{B}_\infty$ corre sobre los $\Phi(M)/(q-1)$ divisores primos de K_M que están sobre $\mathfrak{p}_\infty$ y $s_i = n_i\Phi(P_i^{n_i}) - q^{d_i(n_i-1)}$.

Demostración. Trataremos primero la contribución de los primos $\mathfrak{B}_\infty$ que se encuentran encima de $\mathfrak{p}_\infty$ al diferente. Como $\mathfrak{B}_\infty$ es moderadamente ramificado tanto en K_M/K como en K_M/K_M^+ y su índice de ramificación es $e_\infty = q-1$, $\mathfrak{B}_\infty$ aparece, tanto en el diferente de K_M/K como en el diferente de K_M/K_M^+, a la potencia $e_\infty - 1 = q-2$.

Se verá primero la prueba de la ecuación (3.1). Caso $r = 1$:
Sea $M = P^n$. Cualquier primo diferente de $\mathfrak{p}$ y $\mathfrak{p}_\infty$ es no ramificado. Por lo tanto falta determinar el valor de s. Para ello calculemos

$$(\mathfrak{D}_{K_M/K})_{\mathfrak{P}} = \mathfrak{D}_{(K_M)_{\mathfrak{P}}/K_{\mathfrak{p}}} = \mathfrak{P}^s$$

$(K_M)_{\mathfrak{P}}$ es generado sobre $K_{\mathfrak{p}}$ por una raíz λ de $\Psi_{P^n}(u) = \frac{u^{P^n}}{u^{P^{n-1}}}$. Por la Proposición 2.3.4 $\left\{\lambda^i\right\}_{i=1}^{\Phi(M)-1}$ es una base entera de $K(\Lambda_M)_{\mathfrak{P}}/K_{\mathfrak{p}}$ pues $\mathfrak{p}$ es totalmente ramificado en K_M/K. Por tanto $(\mathfrak{D}_{K_M/K})_{\mathfrak{P}} = \left(\Psi'_{P^n}(\lambda)\right)_{\mathfrak{P}}$. Ahora $u^{P^n} = u^{P^{n-1}}\Psi_{P^n}(u)$. Derivando respecto a u, $P^n = \left(u^{P^n}\right)' = P^{n-1}\Psi_{P^n}(u) + u^{P^{n-1}}\Psi'_{P^n}(u)$, así que $P^n = \lambda^{P^{n-1}}\Psi'_{P^n}(\lambda)$ y $\Psi'_{P^n}(\lambda) = \frac{P^n}{\lambda^{P^{n-1}}}$. Como $\lambda^{P^{n-1}} \in \Lambda_P$ y $\Psi_P(u) = \prod_{(A,P)=1}\left(u - \lambda_P^A\right)$, tenemos $P = \Psi_P(0) = \pm\prod_{(A,P)=1}\lambda_P^A = (\text{ unidad })\,\lambda_P^{\Phi(P)}$ y entonces se tiene $\left(\lambda^{P^{n-1}}\right)^{\Phi(P)} = (P)$.

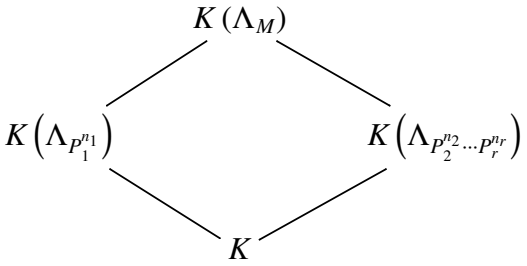
Así, si $\mathfrak{q}$ es el divisor de $K(\Lambda_P)$ que está encima de $\mathfrak{p}$, $v_{\mathfrak{q}}\left(\lambda^{P^{n-1}}\right) = \frac{v_{\mathfrak{q}}(P)}{\Phi(P)} = \frac{\Phi(P)}{\Phi(P)} = 1$, esto porque $\mathfrak{p}$ es totalmente ramificado en $K(\Lambda_P)/K$. Entonces

$$v_{\mathfrak{P}}\left(\lambda^{P^{n-1}}\right) = e(\mathfrak{P}/\mathfrak{q})v_{\mathfrak{q}}(\lambda^{P^{n-1}}) = \frac{\Phi(P^n)}{\Phi(P^{n-1})}.$$

Luego $s = v_{\mathfrak{P}}\left(\Psi'_{P^n}(\lambda)\right) = v_{\mathfrak{P}}\left(\frac{P^n}{\lambda^{P^{n-1}}}\right) = nv_{\mathfrak{P}}(P) - v_{\mathfrak{P}}\left(\lambda^{P^{n-1}}\right) = n\Phi(P^n) - \Phi(P^n)/\Phi(P^{n-1}) = n\Phi(P^n) - \frac{q^{(n-1)d}\left(q^d-1\right)}{(q^d-1)} = n\Phi(P^n) - q^{d(n-1)}$.

Hemos obtenido (3.1) para el caso $r = 1$. Ahora bien, $\mathfrak{P}$ es ramificado total y moderadamente en $K_{P^n}/K_{P^n}^+$ con índice de ramificación $e_{\mathfrak{P}} = q-1$, luego la contribución de $\mathfrak{P}$ al diferente es $e_{\mathfrak{P}} - 1 = q-2$. De donde se sigue (3.2).

Ahora supongamos $r \geq 2$. Los campos $K_{P_i^{n_i}}$, $1 \leq i \leq r$ son linealmente disjuntos a pares y las partes en la que el infinito no interviene $\left(\mathfrak{D}_{K_{P_i^{\alpha_i}}/K}\right)_{\infty}$ de los diferentes $\mathfrak{D}_{K_{P_i^{n_i}}/K}$ son primos relativos. Ahora si $r \geq 2$, consideremos el siguiente diagrama:



Entonces, tomando conormas sobre K_M, tenemos

$$\begin{aligned}(\mathfrak{D}_{K(\Lambda_M)/K})_{\infty} &= \left(\mathfrak{D}_{K(\Lambda_M)/K(\Lambda_{P_1})}\right)_{\infty}\ \text{con}_{K\left(\Lambda_{P_1^{n_1}}\right)/K(\Lambda_M)}\left(\mathfrak{D}_{K\left(\Lambda_{P_1^{n_1}}\right)/K}\right)_{\infty} \\ &= \left(\mathfrak{D}_{K(\Lambda_M)/K\left(\Lambda_{P_2^{n_2}\cdots P_r^{n_r}}\right)}\right)_{\infty}\ \text{con}_{K\left(\Lambda_{P_2^{n_2}\cdot P_r^{n_r}}\right)/K(\Lambda_M)}\left(\mathfrak{D}_{K\left(\Lambda_{P_2^{n_2}\cdots P_r^{n_r}}\right)/K}\right)_{\infty}.\end{aligned}$$

Notemos que los únicos primos que dividen a $\mathrm{con}_{K(\Lambda_{P_1^{n_1}})/K(\Lambda_M)}\left(\mathfrak{D}_{K(\Lambda_{P_1})/K}\right)_{\hat{\infty}}$ son los que se encuentran encima de $\mathfrak{p}_1$.

Los únicos divisores primos que dividen a $\left(\mathfrak{D}_{K\left(\Lambda_{P_2^{n_2}\cdots P_r^{n_r}}\right)/K}\right)_{\hat{\infty}}$ son los que se encuentran encima de $\mathfrak{p}_2, \ldots, \mathfrak{p}_r$.

Vemos que $\mathfrak{p}_1$ no se ramifica en $K\left(\Lambda_{P_2^{n_2}\cdots P_r^{n_r}}\right)/K$ y $\mathfrak{p}_i$ no se ramifica en $K\left(\Lambda_{P_1^{n_1}}\right)$, con $2 \leq i \leq r$. Además

$$\mathfrak{P}_1 \nmid \left(\mathfrak{D}_{K(\Lambda_M)/K\left(\Lambda_{P_1^{n_1}}\right)}\right)_{\hat{\infty}},$$

pues $\mathfrak{P}_1 \nmid \mathrm{con}_{K(\Lambda_{P_2^{n_2}\cdot P_r^{n_r}})/K(\Lambda_M)}\left(\mathfrak{D}_{K\left(\Lambda_{P_2^{n_2}\cdots P_r^{n_r}}\right)/K}\right)_{\hat{\infty}}$ y

$$\mathfrak{P}_2, \ldots, \mathfrak{P}_r \nmid \left(\mathfrak{D}_{K(\Lambda_M)/K\left(\Lambda_{P_2^{n_2}\cdots P_r^{n_r}}\right)}\right)_{\hat{\infty}},$$

pues $\mathfrak{P}_2, \ldots, \mathfrak{P}_r \nmid \mathrm{con}_{K\left(\Lambda_{P_i^{n_1}}\right)/K(\Lambda_M)}\left(\mathfrak{D}_{K\left(\Lambda_{P_1^{n_1}}\right)/K}\right)_{\hat{\infty}}$. Por lo tanto tenemos

$$\left(\mathrm{con}_{K\left(\Lambda_{P_1^{n_1}}\right)/K(\Lambda_M)}\left(\mathfrak{D}_{K\left(\Lambda_{P_1^{n_1}}\right)/K}\right)_{\hat{\infty}},\ \mathrm{con}_{K\left(\Lambda_{P_2^{n_2}\cdot P_r^{n_r}}\right)/K(\Lambda_M)}\left(\mathfrak{D}_{K\left(\Lambda_{P_2^{n_2}\cdots P_r^{n_r}}\right)/K}\right)_{\hat{\infty}}\right) = 1.$$

Entonces $\left(\left(\mathfrak{D}_{K(\Lambda_M)/K\left(\Lambda_{P_1^{n_1}}\right)}\right)_{\hat{\infty}},\ \left(\mathfrak{D}_{K(\Lambda_M)/K\left(\Lambda_{P_2^{n_2}\cdots P_r^{n_r}}\right)}\right)_{\hat{\infty}}\right) = 1$. Por lo tanto

$$\left(\mathfrak{D}_{K(\Lambda_M)/K\left(\Lambda_{P_1^{n_1}}\right)}\right)_{\hat{\infty}} = \mathrm{con}_{K\left(\Lambda_{P_2^{n_2}\cdot P_r^{n_r}}\right)/K(\Lambda_M)}\left(\mathfrak{D}_{K\left(\Lambda_{P_2^{n_2}\cdots P_r^{n_r}}\right)/K}\right)_{\hat{\infty}}$$

y

$$\mathrm{con}_{\mathrm{K}(\Lambda_1^{\alpha_1})/\mathrm{K}(\Lambda_\mathrm{M})}\left(\mathfrak{D}_{\mathrm{K}\left(\Lambda_{\mathrm{P}_1^{\mathrm{n}_1}}\right)/\mathrm{K}}\right)_{\hat{\infty}} = \left(\mathfrak{D}_{\mathrm{K}(\Lambda_\mathrm{M})/\mathrm{K}\left(\Lambda_{\mathrm{P}_2^{\mathrm{n}_2}\cdots\mathrm{P}_\mathrm{r}^{\mathrm{n}_\mathrm{r}}}\right)}\right)_{\hat{\infty}}.$$

Usando esto y el caso $r = 1$, podemos concluir (3.1).

Continuamos con la suposición $r \geq 2$ y consideramos λ generador de Λ_M. Entonces $K_M = K_M^+(\lambda)$. Sean O_M y O_M^+ las cerraduras enteras de R_T en K_M y K_M^+ respectivamente. Entonces el discriminante de O_M/O_M^+ divide al discriminante de λ, esto es

$$d(\lambda) = \left(\mathrm{N}_{K_M/K_M^+} f'(\lambda)\right) = \left(\prod_{a\in\mathbb{F}_q^*} a(q-1)\lambda^{q-2}\right) = \left(\lambda^{(q-1)(q-2)}\right),$$

donde

$$f(u) = \text{Irr } (\lambda, K_M^+; u) = \prod_{a \in \mathbb{F}_q^*} (u - a\lambda) = u^{q-1} - \lambda^{q-1}.$$

Por el corolario 1.9 de S. Galovich y M. Rosen en [5] se tiene que λ es una unidad de O_M si $r \geq 2$. Entonces el discriminante de O_M/O_M^+ es trivial y entonces la extensión es no ramificada fuera de $\mathfrak{p}_\infty$. Como la parte relativa a $\mathfrak{p}_\infty$ es la misma que la de la ecuación (3.2), entonces se tiene con esto la ecuación (3.3). □

Corolario 3.3.2. ***(Fórmulas del género)***
Sea $M = \prod_{i=1}^r P_i^{n_i}$, donde $P_1, \ldots, P_r$ son polinomios mónicos irreducibles, $n_i \in \mathbb{N}$, $d_i = \text{gr}\, P_\text{i}$ y $r \in \mathbb{N}$. Sean g_M y g_M^+ los géneros de los campos K_M y K_M^+ respectivamente. Entonces los géneros están dados por las siguientes fórmulas:

$$2g_M - 2 = -2\Phi(M) + \sum_{i=1}^{r} s_i \frac{\Phi(M)}{\Phi(P_i^{n_i})} d_i + (q-2)\frac{\Phi(M)}{q-1}, \tag{3.4}$$

$$2g_M^+ - 2 = (dn-2)\frac{\Phi(M)}{q-1} - d\frac{q^{d(n-1)}-1}{q-1} - d \text{ si } r = 1, \tag{3.5}$$

$$2g_M^+ - 2 = \frac{1}{q-1}\left\{(2g_M - 2) - \frac{\Phi(M)}{q-1}(q-2)\right\} \text{ si } r \geq 2. \tag{3.6}$$

En la ecuación (3.5) $d = d_1$ y $n = n_1$.

Demostración. Sea $\mathfrak{P}_i$ el único divisor primo de $K_{P_i^{n_i}}$ sobre P_i. Si el divisor primo $\mathfrak{P}_i$ de $K_{P_i^{n_i}}$ se descompone como $(\mathfrak{B}_1 \ldots \mathfrak{B}_{h_i})^{e_i}$ en K_M, entonces el grado de $\mathfrak{P}_i$ como un divisor de K_M es:

$$\text{d}_{K_M}\text{con}_{K\left(\Lambda_{P_i^{n_i}}\right)/K(\Lambda_M)} \mathfrak{P}_i = \text{d}_{K_M}\left((\mathfrak{B}_1 \ldots \mathfrak{B}_{h_i})^{e_i}\right) = (e_i f_i h_i)\, d_i = [K_M : K_{P_i^{n_i}}] d_i = \frac{\Phi(M)}{\Phi\left(P_i^{n_i}\right)} d_i,$$

donde f_i es el grado de inercia de $\mathfrak{B}_i$ sobre $\mathfrak{P}_i$. Por lo tanto el grado del diferente de K_M sobre K es

$$\sum_{i=1}^{r} s_i \frac{\Phi(M)}{\Phi\left(P_i^{n_i}\right)} d_i + (q-2)\frac{\Phi(M)}{q-1}.$$

Con esto se tiene la ecuación (3.4).

Ahora veremos el caso $r = 1$, es decir, $M = P^n$. Entonces:

$$\Phi(M) = q^{d(n-1)}\left(q^d - 1\right) \text{ y } s = nq^{d(n-1)}(q^d - 1) - q^{d(n-1)} = n\Phi(M) - q^{d(n-1)}.$$

Sustituyendo en la ecuación (3.4) se tiene:

$$2g_M - 2 = -2\Phi(M) + \left(n\Phi(M) - q^{d(n-1)}\right)d + (q-2)\frac{\Phi(M)}{q-1}.$$

Notemos que $[K_M : K_M^+] = q-1$ y $\mathrm{d}_{K_M}\left(\mathfrak{D}\left(K_M/K_M^+\right)\right) = (q-2)d + \frac{\Phi(M)}{q-1}(q-2)$. Entonces sustituyendo en la fórmula de Riemann-Hurwitz:

$$\begin{aligned}
2g_M - 2 &= [K_M : K_M^+]\,(2g_M^+ - 2) + \mathrm{d}_{K_M}\mathfrak{D}\left(K_{M/K_M^+}\right) \\
&= (q-1)\,(2g_M^+ - 2) + (q-2)d + \frac{\Phi(M)}{q-1}(q-2) \\
(q-1)\,(2g_M^+ - 2) &= 2g_M - 2 - (q-2)d - \frac{\Phi(M)}{q-1}(q-2) \\
&= -2\Phi(M) + \left(n\Phi(M) - q^{d(n-1)}\right)d - (q-2)d \\
&= (dn-2)\Phi(M) - dq^{d(n-1)} - dq + d + d \\
&= (dn-2)\Phi(M) - d\left(q^{d(n-1)} - 1\right) - d(q-1),
\end{aligned}$$

luego

$$2g_M^+ - 2 = (dn-2)\frac{\Phi(M)}{q-1} - d\frac{q^{d(n-1)}-1}{q-1} - d.$$

Con esto se tiene la fórmula (3.5).

Ahora suponemos que $r \geq 2$, es decir, $M = \prod_{i=1}^{r} P_i^{n_i}$.
Aquí $[K_M : K_M^+] = q-1$ y $\mathrm{d}_{K_M}\left(\mathfrak{D}\left(K_M/K_M^+\right)\right) = \frac{\Phi(M)}{q-1}(q-2)$. Sustituyendo en la fórmula de Riemann-Hurwitz:

$$\begin{aligned}
(q-1)\,(2g_M^+ - 2) &= 2g_M - 2 - \frac{\Phi(M)}{q-1}(q-2) \\
2g_M^+ - 2 &= \frac{1}{q-1}\left\{2g_M - 2 - \frac{\Phi(M)}{q-1}(q-2)\right\}.
\end{aligned}$$

Y así se tiene la ecuación (3.6). □

Capítulo 4

Campos con número de clases de divisores uno

En este capítulo trabajaremos con campos de funciones congruentes. Dado L un campo de funciones con el campo finito $\mathbb{F}_q$ como campo de constantes, veremos las condiciones que se deben cumplir para que el número de clases de divisores h_L sea uno. Para ello se introduce una función $S(q, g, 1)$ y usando la hipótesis de Riemann se prueban dos importantes resultados de Madan-Queen, los cuales condicionan el valor de q y g de tal forma que $h_L = 1$. Los resultados obtenidos se aplican a campos de funciones ciclotómicos, donde dado $M = \prod_{i=1}^{r} P_i^{n_i}$, con P_i polinomio irreducible de grado d_i se encuentran los valores de d_i y n_i, de tal forma que g_M o g_M^+ sean cero y con esto se garantiza que el número de clases de divisores de h_M sea igual a uno.

4.1. Campos de funciones algebraicas

Nota 4.1.1. Sea L un campo de funciones de género cero. El teorema de Riemann-Roch implica que $h_L = 1$. Además como consecuencia de la hipótesis de Riemann, L es un campo de funciones racionales. (Ver [17], proposición 7.3.1., pp. 97).

Veremos ahora unos criterios para que un campo de funciones sobre un campo finito tenga número de clases de divisores igual a uno.

Proposición 4.1.2. *Supongamos que L es un campo de funciones con campo de constantes $\mathbb{F}_q$, que $q > 4$ y que su género $g = g_L$ es distinto de cero. Entonces el número de clases de divisores $h = h_L$ es mayor que uno.*

Demostración. Se hará la prueba por contradicción.
Tenemos $q > 4$ y $g > 0$ y suponemos $h = 1$. Por el teorema 6.3.5 de [17], tenemos que $h = P_L(1)$, donde $P_L(u) = P_L(q^{-s})$ es el numerador de la función zeta de Riemann de un campo de funciones congruentes y es un polinomio de grado $2g$ cuyos ceros tienen valor absoluto $q^{1/2}$. Por lo tanto,

$$\begin{aligned} h &= \prod_{m=1}^{g} \left(1 - q^{1/2} e^{i\alpha_m}\right)\left(1 - q^{1/2} e^{-i\alpha_m}\right) \\ &= \prod_{m=1}^{g} \left(1 - 2q^{1/2}\cos\alpha_m + q\right) \geq \left(q^{1/2} - 1\right)^g. \end{aligned}$$

Veamos que la desigualdad es cierta:
Observemos primero que:

$$1 - 2q^{1/2}\cos\alpha_m + q \geq q^{1/2} - 1 \Leftrightarrow -q^{1/2} - 2q^{1/2}\cos\alpha_m + q \geq -2 \Leftrightarrow -2 \leq -q^{1/2}(1 + 2\cos\alpha_m) + q.$$

Ahora, sabemos que $\cos\alpha_m \leq 1$ y tenemos:
$\cos\alpha_m \leq 1 \Leftrightarrow 2\cos\alpha_m \leq 2 \Leftrightarrow 1 + 2\cos\alpha_m \leq 3 \Leftrightarrow q^{1/2}(1 + 2\cos\alpha_m) \leq 3q^{1/2} \Leftrightarrow -q^{1/2}(1 + 2\cos\alpha_m) \geq -3q^{1/2} \Leftrightarrow -q^{1/2}(1 + 2\cos\alpha_m) + q \geq -3q^{1/2} + q$.
Veamos que si $q \geq 4$ entonces $-3q^{1/2} + q \geq -2$:
Para esto, sea $f(x) = x - 3x^{1/2}$. Entonces $f'(x) = 1 - \frac{3}{2}x^{-1/2}$. Tenemos $f'(x) > 0 \Leftrightarrow 1 > \frac{3}{2\sqrt{x}} \Leftrightarrow x > \frac{9}{4}$. Observamos que $f(4) = -2$. Por lo tanto, como $q > 4$ tenemos $-3q^{1/2} + q \geq -2$, entonces $-q^{1/2}(1 + 2\cos\alpha_m) + q \geq -2$. Así $1 - 2q^{1/2}\cos\alpha_m + q \geq q^{1/2} - 1$.
Finalmente como $h = 1$, se tiene $q^{1/2} - 1 \leq 1$ de donde $q \leq 4$, una contradicción. □

Ahora suponemos que $\boldsymbol{g}$>**1** y que $\boldsymbol{q} \leq$ **4**. La hipótesis de Riemann es equivalente a la desigualdad

$$|N_1 - (q + 1)| \leq 2g\sqrt{q},$$

donde N_1 denota el número de primos de grado 1 de L.
Sea $\hat{L}$ la extensión de constantes de L de grado $2g - 1$. El campo $\mathbb{F}_q$ es perfecto, luego $g_{\hat{L}} = g_L = g$. Por la hipótesis de Riemann aplicada a $\hat{L}$ con campo de constantes $\mathbb{F}_{q^{2g-1}}$ y N_1' el número de divisores primos de grado 1 en $\hat{L}$, se tiene $\left|N_1' - \left(q^{2g-1} + 1\right)\right| \leq 2g\sqrt{q^{2g-1}}$. Por lo tanto

$$N_1 \geq q^{2g-1} + 1 - 2g\sqrt{q^{2g-1}}.$$

Si $d \mid 2g - 1$, un divisor de grado d en L se descompone en $(d, 2g - 1) = d$ divisores primos de grado $\frac{d}{(d,2g-1)} = 1$. (Ver teorema 6.2.1 de [17]).

Si un divisor primo de grado 1 en $\hat{L}$ se restringe a un primo de grado d, entonces $d \mid 2g-1$. (Ver proposición 3.1.3).

A lo más se pueden restringir al mismo lugar en L, $2g-1$ lugares de grado 1 en $\hat{L}$. Si $\mathfrak{P}_1, \ldots, \mathfrak{P}_s$ son primos de grado 1 que se restringen al mismo primo $\mathfrak{p}$ en L con $s \leq 2g-1$, entonces $\mathfrak{p}^{(2g-1)/d_L(\mathfrak{p})}$ es un divisor entero de grado $2g-1$ en L. Así, con a lo más $2g-1$ divisores de grado 1 en $\hat{L}$ obtenemos un divisor entero de grado $2g-1$ en L. Como hay N_1' lugares de grado 1 en $\hat{L}$, existen al menos

$$\frac{N_1'}{2g-1} \geq \frac{q^{2g-1}+1-2g\sqrt{q^{2g-1}}}{2g-1}$$

divisores enteros de grado $2g-1$ en L.

Entonces por el teorema 6.2.6 de [17], tenemos $A_n = h\left(\frac{q^{n-g+1}-1}{q-1}\right)$, donde A_n es el número de divisores enteros de grado n en L. Luego

$$A_{2g-1} = h\left(\frac{q^g-1}{q-1}\right) \geq \frac{q^{2g-1}+1-2g\sqrt{q^{2g-1}}}{2g-1}.$$

Por lo tanto

$$h \geq \frac{\left(q^{2g-1}+1-2g\sqrt{q^{2g-1}}\right)(q-1)}{(2g-1)(q^g-1)}.$$

Ahora tenemos que

$$h \geq R = \frac{\left(q^{2g-1}+1-2g\sqrt{q^{2g-1}}\right)(q-1)}{(2g-1)(q^g-1)}.$$

Sea $S(q,g,r) = (q-1)\left[q^{2g-1}+1-2g\sqrt{q^{2g-1}}\right] - r(2g-1)(q^g-1)$. Entonces

$$h \geq R = \frac{S(q,g,r) + r(2g-1)(q^g-1)}{(2g-1)(q^g-1)} = \frac{S(q,g,r)}{(2g-1)(q^g-1)} + r.$$

Luego si $S(q,g,r) > 0$ y como $(2g-1)(q^g-1) > 0$, se tiene $\frac{S(q,g,r)}{(2g-1)(q^g-1)} > 0$. Esto implica que $R > r$ y por lo tanto $h > r$.

Ahora,

$S(q,g,1) = (q-1)\left[q^{2g-1}+1-2g\sqrt{q^{2g-1}}\right] - (2g-1)(q^g-1)$. Derivando con respecto a g:

$$
\begin{aligned}
S'(q,g,1) &= (q-1)\Big[(2\ln q)\,q^{2g-1} - \Big(\big((2g\ln q)\ \sqrt{q^{2g-1}}\big) + 2\sqrt{q^{2g-1}}\Big)\Big] \\
&\quad - \Big[(2g-1)(\ln q)\,q^g + 2(q^g-1)\Big] \\
&= (q-1)\Big[(2\ln q)\Big(q^{2g-1}\Big) - (2g\ln q)\ \sqrt{q^{2g-1}} - 2\sqrt{q^{2g-1}}\Big] \\
&\quad - \Big[(2g\ln q)\,q^g - (\ln q)\,q^g + 2q^g - 2\Big] \\
&= (2\ln q)\,q^g\Big[\Big(q^{g-1}\Big)(q-1) - gq^{-1/2}(q-1) - g + \frac{1}{2}\Big] \\
&\quad - 2\sqrt{q^{2g-1}}\,(q-1) - 2q^g + 2 \\
&= (2\ln q)\,q^g\Big[\Big(q^{g-1}\Big)(q-1) - g\Big(q^{1/2} - q^{-1/2}\Big) - g + \frac{1}{2}\Big] \\
&\quad - 2\sqrt{q^{2g-1}}\,(q-1) - 2q^g + 2 \\
&= (2\ln q)\,q^g\Big[\Big(q^{g-1}\Big)(q-1) - g\Big(q^{1/2} - q^{-1/2}\Big) - g + \frac{1}{2}\Big] \\
&\quad - 2\sqrt{q^{2g+1}} + 2\sqrt{q^{2g-1}} - 2q^g + 2 \\
&= (2\ln q)\,q^g\Big[\Big(q^{g-1}\Big)(q-1) - g\Big(q^{1/2} - q^{-1/2} + 1\Big) + \frac{1}{2}\Big] \\
&\quad - 2q^g\Big(q^{1/2} - q^{-1/2} + 1\Big) + 2 \\
&= 2q^g\Big[\ln q\Big(q^{g-1}\Big)(q-1) - (g\ln q + 1)\Big(q^{1/2} - q^{-1/2} + 1\Big) + \frac{\ln q}{2}\Big] + 2.
\end{aligned}
$$

Sea $S_1(q,g,1) = \ln q\left(q^{g-1}\right)(q-1) - (g\ln q + 1)\left(q^{1/2} - q^{-1/2} + 1\right) + \dfrac{\ln q}{2}$. Entonces

$$
\begin{aligned}
S_1'(q,g,1) &= (\ln q)^2\left(q^{g-1}\right)(q-1) - \ln q\left(q^{1/2} - q^{-1/2} + 1\right) \\
&= \ln q\Big[\ln q\left(q^{g-1}\right)(q-1) - \left(q^{1/2} - q^{-1/2} + 1\right)\Big].
\end{aligned}
$$

Ahora, si $S_2(q,g,1) = \ln q\left(q^{g-1}\right)(q-1) - \left(q^{1/2} - q^{-1/2} + 1\right)$, entonces

$$
S_2'(q,g,1) = (\ln q)^2\left(q^{g-1}(q-1)\right) > 0.
$$

Entonces $S(q,g,1)$ es creciente como función de g para $q = 4$, $g \geq 2$; $q = 3$, $g \geq 3$; $q = 2$, $g \geq 5$.

Para ver esto, primero consideremos el caso en que $q = 4$ y $g \geq 2$, entonces $S_2(4,2,1) = 12\ln 4 - \frac{5}{2} > 0$. Esto implica que $S_1'(4,2,1) > 0$ y como $S_2'(q,g,1) > 0$ para $q = 4$, $g \geq 2$, entonces $S_1'(q,g,1)$ es creciente y positiva para $q = 4$, $g \geq 2$. Como $S_1(q,g,1)$ es creciente para $q = 4$, $g \geq 2$

y $S_1(4,2,1) > 0$, podemos concluir que $S(q,g,1)$ es creciente para $q = 4$, $g \geq 2$.

Ahora si $q = 3$ y $g \geq 3$, entonces $S_2(3,3,1) = 18\ln 3 - (\frac{2+\sqrt{3}}{\sqrt{3}}) > 0$. Además $S_1'(3,3,1) > 0$ y como $S_2'(q,g,1) > 0$ para $q = 3$, $g \geq 3$, se tiene $S_1'(q,g,1)$ es creciente y positiva para $q = 3$, $g \geq 3$. Luego $S_1(3,3,1) = \frac{37}{2}\ln 3 - (3\ln 3 + 1)(\frac{2+\sqrt{3}}{\sqrt{3}}) > 0$. Entonces $S'(3,3,1) > 0$ y como $S_1'(q,g,1) > 0$ para $q = 3$, $g \geq 3$, tenemos $S'(q,g,1)$ es creciente y positiva para $q = 3$, $g \geq 3$. Por lo tanto $S(q,g,1)$ es creciente para $q = 3$, $g \geq 3$.

Ahora veremos el caso en que $q = 2$, $g \geq 5$. Se tiene $S_2(2,5,1) = 16\ln 2 - (\frac{1+\sqrt{2}}{\sqrt{2}}) > 0$. Entonces $S_1'(2,5,1) > 0$ y como $S_2'(q,g,1) > 0$ para $q = 2$, $g \geq 5$, se sigue que $S_1'(q,g,1)$ es creciente y positiva para $q = 2$, $g \geq 5$. Luego $S_1(2,5,1) = \frac{33}{2}\ln 2 - (5\ln 2 + 1)(\frac{1+\sqrt{2}}{\sqrt{2}}) > 0$. Entonces $S'(2,5,1) > 0$ y como $S_1'(q,g,1) > 0$ para $q = 2$, $g \geq 5$, se tiene que $S'(q,g,1)$ es creciente y positiva para $q = 2$, $g \geq 5$. Por lo tanto $S(q,g,1)$ es creciente para $q = 2$, $g \geq 5$.

Por otra parte,

$$S(4,2,1) = 3(50 - 32) = 54 > 0$$

$$S(3,3,1) = 2\left(179 - 54\sqrt{3}\right) > 0$$

$$S(2,5,1) = 2\left(117 - 80\sqrt{2}\right) > 0$$

Con esto se ha probado el siguiente teorema:

Teorema 4.1.3. ***(Madan-Queen)*** *Sea L un campo de funciones de género g, que tiene al campo finito $\mathbb{F}_q$ como su campo de constantes. El número de clases de L, $h = h_L > 1$ si se satisface cualquiera de las siguientes condiciones:*

1. *$q = 4$ y $g \geq 2$;*
2. *$q = 3$ y $g \geq 3$;*
3. *$q = 2$ y $g \geq 5$.*

□

Este resultado se puede refinar con el siguiente teorema.

Teorema 4.1.4. *Sea L un campo de funciones de género g con $\mathbb{F}_q$ como su campo de constantes. Si $q = 3$ y $g = 2$, entonces $h = h_L > 1$.*

Antes de demostrar el teorema 4.1.4 consideramos lo siguiente.
De la sección 7.4 de [17], si $P_L(u)$ es el numerador de la función zeta de Riemann de un campo de funciones congruentes, entonces $P_L(u) = a_0 + a_1u + \cdots + a_{2g}u^{2g}$, donde $u = q^{-s}$, $a_{2g-i} = a_iq^{g-i}$ y $a_0 = 1$, $a_{2g} = q^g$. Además $a_i = A_i - (q+1)A_{i-1} + qA_{i-2}$. Entonces,

$$h = P_L(1) = \sum_{i=0}^{2g} a_i = \sum_{i=0}^{g-1} \left(\left(q^{g-i}+1\right)a_i\right) + a_g.$$

Sea $s_n = \sum_{i=1}^{2g} \omega_i^n$, donde $P_L(u) = \prod_{i=1}^{2g}(1-\omega_i u)$. Entonces por el teorema 7.3.5 de[17], se tiene que $-s_n = \sum_{d|n} d\,(N_d - n_d)$, donde N_d y n_d denotan el número de primos de grado d de L y de $\ell(x)$ respectivamente.
Ahora

$$\begin{aligned} u^{-2g}P_L(u) = u^{-2g}\prod_{i=1}^{2g}(1-\omega_i u) &= u^{-2g}\prod_{i=1}^{2g} u\left(u^{-1}-\omega_i\right) \\ &= \prod_{i=1}^{2g}\left(u^{-1}-\omega_i\right) = u^{-2g}\sum_{i=0}^{2g} a_iu_i \\ &= a_0u^{-2g} + a_1u^{-2g+1} + \cdots + a_{2g}, \end{aligned}$$

es decir, $\omega_1, \ldots, \omega_{2g}$ son las raíces de $u^{-2g}P_L(u) = Q_L(v)$, donde $v = u^{-1}$. Entonces se tiene que $Q_L(v) = b_0 + b_1v + \cdots + b_{2g}v^{2g} = \prod_{i=1}^{2g}(v-\omega_i)$ con $b_i = a_{2g-i} = q^{g-i}a_i$ y $b_{2g} = a_0 = 1$.

Por las identidades de Newton (teorema 7.1.4 [17]), tenemos $b_{2g-i} = a_i = (-1)^{2g-i}\sigma_i = (-1)^i\sigma_i$, donde σ_i es el $i-$ésimo polinomio elemental simétrico en $\omega_1, \ldots, \omega_{2g}$, por lo que $s_m + s_{m-1}a_1 + \cdots + s_1a_{m-1} + ma_m = 0$, donde $1 \le m \le 2g-1$. Por lo tanto,

$$\begin{aligned} s_1 + a_1 = 0, \text{ de donde } a_1 &= -s_1, \\ s_2 + s_1a_1 + 2a_2 = 0 \text{ y entonces } a_2 &= \frac{-s_2 - s_1a_1}{2} = \frac{s_1^2 - s_2}{2}, \\ a_3 &= \frac{-s_1^3 - 3s_1s_2 + 2s_3}{6}, \\ a_4 &= \frac{s_1^4 - 6s_1^2s_2 + 8s_1s_2 + 3s_2^2 - 6s_4}{24}, \text{ etc.} \end{aligned}$$

Por otro lado, por la fórmula de Dedekind (ver sección 7.5 de [17]),

$$n_d = \begin{cases} q+1 & \text{si } d = 1 \\ \frac{1}{d}\sum_{f|d}\mu(\frac{d}{f})q^f & \text{si } d > 1, \end{cases}$$

donde μ denota la función de Möbius y como $s_n = -\sum_{d|n} d\,(N_d - n_d)$, después de hacer las sustituciones necesarias, se obtiene:

$$
\begin{aligned}
a_1 &= N_1 - (q+1) \\
2a_2 = s_1^2 - s_2 &= (N_1 - (q+1))^2 + \left(\sum_{d|2} d\,(N_d - n_d)\right) \\
&= (N_1 - (q+1))^2 + ((N_1 - n_1) + 2\,(N_2 - n_2)) \\
&= \left(N_1^2 - 2N_1\,(q+1) + (q+1)^2\right) + \left((N_1 - (q+1)) + 2\left(N_2 - \frac{1}{2}\sum_{f|2}\mu\left(\frac{2}{f}\right)q^f\right)\right) \\
&= \left(N_1^2 - 2N_1\,(q+1) + (q+1)^2\right) + \left((N_1 - (q+1)) + 2\left(N_2 - \frac{1}{2}\left(\mu\left(\frac{2}{1}\right)q^1 + \mu\left(\frac{2}{2}\right)q^2\right)\right)\right) \\
&= N_1^2 - 2N_1\,(q+1) + (q+1)^2 + N_1 - (q+1) + 2N_2 - \left(-q + q^2\right) \\
&= N_1^2 - 2N_1\,(q+1) + (q+1)^2 + N_1 + 2N_2 - \left(1 + q^2\right) \\
&= N_1^2 - (2q+1)\,N_1 + 2N_2 + 2q.
\end{aligned}
$$

Nota 4.1.5. Observemos que de lo anterior se sigue que si $g = 1$, entonces $h = (q+1)a_0 + a_1 = (q+1)\cdot 1 + N_1 - (q+1) = N_1$.

Nota 4.1.6. Supongamos $h = 1$. Entonces para $g \geq 1$ se tiene $N_1 \leq 1$, pues si existieran $\mathfrak{p}_1, \mathfrak{p}_2$ divisores primos distintos de grado 1, como $h = 1$ se tendría que, $\frac{\mathfrak{p}_1}{\mathfrak{p}_2} = (x)$ sería divisor principal. Luego $[L : \ell(x)] = \mathrm{d}_L(\eta_x) = \mathrm{d}_L(\mathfrak{p}_2) = 1$ y por lo tanto $L = \ell(x)$ y $g = 0$, lo cual es absurdo.

Con esto como base se procederá a demostrar el teorema 4.1.4.

Demostración. Recordemos que $q = 3$ y $g = 2$. Tenemos $h = P_K(1) = \left(q^2+1\right)a_0 + (q+1)\,a_1 + a_2 = 10 + 4a_1 + a_2 = \dfrac{-6 + N_1 + N_1^2 + 2N_2}{2}$. Por lo tanto $h = 1$ si y sólo si

$$N_1^2 + N_1 + 2N_2 = 8. \tag{4.1}$$

Además, por la hipótesis de Riemann, los recíprocos de las raíces de $P_K(u)$ son $\sqrt{3}e^{\pm i\theta_1}$ y

$\sqrt{3}e^{\pm i\theta_2}$. Por lo tanto

$$\begin{aligned}
P_L(u) &= \left(1+\sqrt{3}e^{i\theta_1}u\right)\left(1+\sqrt{3}e^{-i\theta_1}u\right)\left(1+\sqrt{3}e^{i\theta_2}u\right)\left(1+\sqrt{3}e^{-i\theta_2}u\right)\\
&= \left(1-\sqrt{3}e^{-i\theta_1}u-\sqrt{3}e^{i\theta_1}u+3u^2\right)\left(1-\sqrt{3}e^{-i\theta_2}u-\sqrt{3}e^{i\theta_2}u+3u^2\right)\\
&= \left(1-\sqrt{3}\left((\cos\theta_1-i\operatorname{sen}\theta_1)+(\cos\theta_1+i\operatorname{sen}\theta_1)\right)u+3u^2\right)\\
&\quad \left(1-\sqrt{3}\left((\cos\theta_2-i\operatorname{sen}\theta_2)+(\cos\theta_2+i\operatorname{sen}\theta_2)\right)u+3u^2\right)\\
&= \left(1-2\sqrt{3}\cos\theta_1 u+3u^2\right)\left(1-2\sqrt{3}\cos\theta_2 u+3u^2\right)\\
&= 1+\left(-2\sqrt{3}\cos\theta_1\right)u+3u^2+\left(-2\sqrt{3}\cos\theta_2\right)u+\\
&\quad +\left(12\cos\theta_1\cos\theta_2u^2-6\sqrt{3}\cos\theta_2u^3+3u^2-6\sqrt{3}\cos\theta_1u^3+9u^4\right)\\
&= 1-2\sqrt{3}\left(\cos\theta_1+\cos\theta_2\right)u+\left(6+12\cos\theta_1\cos\theta_2\right)u^2-\\
&\quad -6\sqrt{3}\left(\cos\theta_1+\cos\theta_2\right)u^3+9u^4.
\end{aligned}$$

Comparando coeficientes se obtiene:

$$a_1 = N_1-(q+1) = N_1-4 = -2\sqrt{3}\left(\cos\theta_1+\cos\theta_2\right).$$

Despejando:

$$\cos\theta_1+\cos\theta_2 = -\frac{N_1-4}{2\sqrt{3}} = -\frac{(N_1-4)\sqrt{3}}{(2\sqrt{3})\sqrt{3}} = -\frac{(N_1-4)\sqrt{3}}{6}.$$

Por otro lado:

$2a_2 = N_1^2-(2q+1)N_1+2N_2+2q = N_1^2-7N_1+2N_2+6 = 24\cos\theta_1\cos\theta_2+12.$

Despejando:

$$\cos\theta_1\cos\theta_2 = \frac{N_1^2-7N_1+2N_2-6}{24}.$$

Sustituyendo la ecuación (4.1) se tiene:

$$\cos\theta_1\cos\theta_2 = \frac{N_1^2+N_1+2N_2-8N_1-6}{24} = \frac{8-8N_1-6}{24} = \frac{2-8N_1}{24} = \frac{1-4N_1}{12}.$$

Sea

$$\begin{aligned}
f(x) &= (x-\cos\theta_1)(x-\cos\theta_2) = x^2-x\cos\theta_2-x\cos\theta_1+\cos\theta_1\cos\theta_2\\
&= x^2-(\cos\theta_1+\cos\theta_2)x+\cos\theta_1\cos\theta_2\\
&= x^2+\left(\frac{(N_1-4)\sqrt{3}}{6}\right)x+\left(\frac{1-4N_1}{12}\right) = \frac{12x^2+2\sqrt{3}(N_1-4)x+(1-4N_1)}{12},
\end{aligned}$$

es decir, $\cos\theta_1$ y $\cos\theta_2$ son las raíces de $f(x)$.

Pero

$$0 \leq (1-\cos\theta_1)(1-\cos\theta_2) = f(1) = \frac{12 + 2\sqrt{3}(N_1 - 4) + (1 - 4N_1)}{12}$$
$$= \frac{(12 - 8\sqrt{3} + 1) + N_1(2\sqrt{3} - 4)}{12}.$$

Con esto vemos que $f(1)$ siempre es negativo. Por lo tanto $f(x)$ tiene una raíz mayor que uno. Esto es una contradicción.

Por lo tanto si $q = 3$ y $g = 2$ entonces $h > 1$. □

Finalmente usando el teorema 4.1.3 y el teorema 4.1.4 se tiene el siguiente resultado.

Proposición 4.1.7. ***(Madan-Queen)***. *Sea L un campo de funciones sobre el campo finito con q elementos ($q \leq 4$) y $g \geq 1$ su género. Si el número de clases de divisores de L es uno, entonces se tiene alguno de los siguientes casos:*

1. $q = 2$ *y* $g \leq 4$,
2. $q = 3$ *y* $g = 1$,
3. $q = 4$ *y* $g = 1$.

□

4.2. Campos de funciones ciclotómicos

En esta sección h_M y h_M^+ denotan los números de clases de divisores del campo de funciones ciclotómico $K_M = K(\Lambda_M)$ y de su subcampo real maximal K_M^+, respectivamente. Sea $M = \prod_{i=1}^{r} P_i^{n_i}$, donde los P_i son polinomios irreducibles de grado d_i.

Lema 4.2.1. *Sea K_M un campo de funciones ciclotómicos y N_1 el número de primos de grado* 1. *Entonces se tiene:*

$$N_1 \geq \frac{\Phi(M)}{q-1}.$$

Lo mismo se tiene para el subcampo real maximal K_M^+.

Demostración. Por la proposición 2.2.1, tenemos que el grado de los primos en K_M o en K_M^+ que están sobre el primo infinito $\mathfrak{p}_\infty$ es uno. Así que el número de primos de grado uno es mayor o igual que el número de primos que están sobre $\mathfrak{p}_\infty$, el cual es $h_\infty = \dfrac{\Phi(M)}{q-1}$. □

Teorema 4.2.2. *Para el campo de funciones ciclotómico K_M, el número de clases de divisores es $h_M = 1$ si y sólo si su género es $g_M = 0$. Lo mismo se cumple para K_M^+.*

Demostración. Supongamos $h_M = 1$. Si $\dfrac{\Phi(M)}{(q-1)} > 1$, entonces si $h_M = 1$, por el lema 4.2.1 y la nota 4.1.6 tenemos que $g_M = 0$.

Ahora consideramos el caso en que $\dfrac{\Phi(M)}{(q-1)} = 1$. Por definición de $\Phi(M)$, se tiene:

$$\frac{\Phi(M)}{(q-1)} = \frac{\prod_{i=1}^{r} q^{d_i(n_i-1)}\left(q^{d_i}-1\right)}{(q-1)} = 1$$

si y sólo si se tiene uno de los siguientes casos:

1. $q = 2$ y $r = 1$ se tiene $d_1 = n_1 = 1$.
2. $q = 2$ y $r = 2$ se tiene $d_1 = d_2 = 1$ y $n_1 = n_2 = 1$, pues únicamente hay dos primos de grado 1 distintos a $\mathfrak{p}_\infty$.
3. $q \geq 3$ y $r = 1$ se tiene $d_1 = n_1 = 1$.

Ahora calculemos el género en cada caso, usando la fórmula (3.4) del género.
Caso 1: $M = P_1$, $\Phi(M) = 1$ y $s = 0$. Entonces $2g_M - 2 = -2$, implica $g_M = 0$.
Caso 2: $M = P_1P_1'$, $\Phi(M) = 1$ y $s_1 = s_2 = 0$. Así $2g_M - 2 = -2$. Por lo que $g_M = 0$.
Caso 3: $M = P_1$, $\Phi(M) = q-1$ y $s = 1$. Así $2g_M - 2 = -2$. Luego $g_M = 0$.

Para el recíproco, si $g_M = 0$, entonces, como se había mencionado al principio de este capítulo, por el teorema de Riemann-Roch, K_M es un campo de funciones racionales y así por el ejemplo 1.4.15, $h_M = 1$. Para K_M^+ el argumento es análogo. □

El siguiente ejemplo ilustra que es posible tener un campo de funciones L de género $g_L \neq 0$ y número de clases de divisores $h_L = 1$.

Ejemplo 4.2.3. Sean $q = 2$, $Y^2 + Y = T^3 + T + 1$, $K = \mathbb{F}_2(T)$, $L = K(Y)$. Entonces $g_L = 1$, $h_L = 1$. (Ver [17], teorema 7.4.6, pp. 229).

Ahora, por el teorema 4.2.2, el problema se reduce a determinar los campos de género cero.

Lema 4.2.4. *Supongamos que L/F es una extensión finita, geométrica y separable de campos de funciones sobre un campo finito. Y sean g_L y g_F los géneros de L y F respectivamente. Entonces se tiene $g_L \geq g_F$.*

Demostración. Por la fórmula de Riemann-Hurwitz tenemos:

$$2g_L - 2 = (2g_F - 2)[L : F] + \text{grado del diferente} \geq (2g_F - 2)[L : F] \geq (2g_F - 2).$$

Con esto se concluye $g_L \geq g_F$. □

Lema 4.2.5. *Sea $M = \prod_{i=1}^{r} P_i^{n_i}$, donde los P_i son polinomios irreducibles de grado d_i. Si $q = 2$ y $g_M = 0$, entonces $r \leq 3$.*

Demostración. Si $n_i = 1$ y $d_i = 1$, el resultado se sigue.
Suponemos entonces que $n_i > 1$ o $d_i > 1$. Ahora,

$$s_i = n_i\Phi(P_i^{n_i}) - 2^{d_i(n_i-1)} \text{ y } \Phi(P_i^{n_i}) = 2^{d_i(n_i-1)}(2^{d_i-1}).$$

Luego,

$$\begin{aligned}\frac{s_i d_i}{\Phi(P_i^{n_i})} &= \frac{n_i\Phi(P_i^{n_i}) - 2^{d_i(n_i-1)}}{\Phi(P_i^{n_i})}d_i = (n_i-1)d_i + \frac{\Phi(P_i^{n_i}) - 2^{d_i(n_i-1)}}{\Phi(P_i^{n_i})}d_i \\ &= (n_i-1)d_i + \frac{2^{d_i(n_i-1)}(2^{d_i}-1-1)}{2^{d_i(n_i-1)}(2^{d_i-1})}d_i = (n_i-1)d_i + \left(\frac{2^{d_i}-2}{2^{d_i}-1}\right)d_i \\ &\geq \begin{cases} 1, \text{ si } d_i \geq 1 \text{ y } n_i > 1 \\ \frac{2}{3} \text{ si } d_i > 1 \text{ y } n_i \geq 1 \end{cases} \geq \frac{2}{3}.\end{aligned}$$

Con esto, procederemos a demostrar el lema.
Suponemos $q = 2$ y $r \geq 4$. Entonces sustituyendo en la fórmula (3.4) del género, tenemos:

$$\begin{aligned}2g_M - 2 &= -2\Phi(M) + \sum_{i=1}^{r} s_i \frac{\Phi(M)}{\Phi(P_i^{n_i})} \cdot d_i \\ &= \Phi(M)\left\{-2 + \sum_{i=1}^{r} \frac{s_i d_i}{\Phi(P_i^{n_i})}\right\} \\ &\geq \Phi(M)\left\{-2 + \frac{8}{3}\right\} = \Phi(M) \cdot \frac{2}{3} > 0\end{aligned}$$

Con esto se tiene, $2g_M > 2$, lo cual implica que $g_M > 1$, una contradicción. □

Lema 4.2.6. *Sea* $M = \prod_{i=1}^{r} P_i^{n_i}$, *donde los* P_i *son polinomios irreducibles de grado* d_i. *Si* $q \geq 3$ *y* $g_M^+ = 0$, *entonces* $r \leq 3$.

Demostración. Notemos primero que

$$\frac{s_i d_i}{\Phi(P_i^{n_i})} = \frac{n_i q^{d_i(n_i-1)}(q^{d_i}-1) - q^{d_i(n_i-1)}}{q^{d_i(n_i-1)}(q^{d_i}-1)} d_i \geq \frac{q^{d_i(n_i-1)}(q^{d_i}-1-1)}{q^{d_i(n_i-1)}(q^{d_i}-1)} d_i = d_i \frac{(q^{d_i}-2)}{q^{d_i}-1} \geq \frac{1}{2}.$$

Ahora supongamos que $q \geq 3$ y $r \geq 4$. De la fórmula (3.4) del género tenemos:

$$2g_M - 2 - (q-2)\frac{\Phi(M)}{q-1} = -2\Phi(M) + \sum_{i=1}^{r} s_i \frac{\Phi(M)}{\Phi(P_i^{n_i})} d_i$$

Usando la fórmula (3.6) del género,

$$2g_M^+ - 2 = \frac{1}{q-1}\left\{-2\Phi(M) + \sum_{i=1}^{r} \frac{s_i \Phi(M)}{\Phi(P_i^{n_i})} d_i\right\}.$$

Despejando:

$$\frac{q-1}{\Phi(M)}(2g_M^+ - 2) = -2 + \sum_{i=1}^{r} \frac{s_i d_i}{\Phi(P_i^{n_i})}.$$

Por lo tanto, $\frac{q-1}{\Phi(M)}(2g_M^+ - 2) \geq -2 + \frac{4}{2} = 0$. Esto implica que $2g_M^+ - 2 \geq 0$, entonces $2g_M^+ \geq 2$ y así $g_M^+ \geq 1$, una contradicción. □

Ahora podemos determinar los campos con número de clases de divisores uno. Primero se tratarán los subcampos reales maximales.
Para el caso $q = 2$ tenemos $e_\infty = 1$ y entonces $K_M^+ = K_M$, con esto de puede descartar este caso.

Lema 4.2.7. *Sean* $M = P^n$ *y* $d = \operatorname{gr} P$. *Si* $g_M^+ = 0$, *entonces* $(n, d) = \{(1,1), (1,2), (2,1)\}$.

Demostración. Supongamos $d(n-1) \geq 2$, entonces se tiene $dn > 2$ y $dn - d \geq 2$, de donde $dn - 2 \geq d$, luego $\frac{d}{dn-2} \leq 1$. Por la desigualdad

$$q^{d(n-1)}\left(q^d - 2\right) > q - 2,$$

tenemos,

$$q^{dn} - 2q^{d(n-1)} > q - 2$$
$$q^{dn} - q^{d(n-1)} > q^{d(n-1)} - 1 + q - 1$$
$$\frac{q^{dn} - q^{d(n-1)}}{q-1} > \frac{q^{d(n-1)} - 1}{q-1} + 1$$

$$\frac{q^{dn}-q^{d(n-1)}}{q-1} > \left(\frac{q^{d(n-1)}-1}{q-1}+1\right)\left(\frac{d}{dn-2}\right)$$
$$(dn-2)\frac{q^{dn}-q^{d(n-1)}}{q-1} - d\left(\frac{q^{d(n-1)}-1}{q-1}+1\right) > 0,$$

ya que $dn-2>0$. Por la fórmula del género (3.5) tenemos:

$$2g_M^+ - 2 = (dn-2)\frac{\Phi(M)}{q-1} - d\frac{q^{d(n-1)}-1}{q-1} - d > 0, \tag{4.2}$$

entonces $2g_M^+-2>0$. Pero esto no puede darse, porque por hipótesis $g_M^+=0$. Por lo que $d(n-1)<2$ y esto pasa si y sólo si $n=1$ ó $(n,d)=(2,1)$.
Si $n=1$, entonces de la ecuación (4.2) tenemos:

$$-2 = (d-2)\frac{q^d-1}{q-1} - d$$
$$(d-2)\frac{q^d-1}{q-1} - d + 2 = 0$$
$$(d-2)\left(\frac{q^d-1}{q-1}-1\right) = 0,$$

y esto pasa si y sólo si $d=1$ ó $d=2$. □

***Caso r =* 1:** por la fórmula (3.5), el recíproco del lema 4.2.7 es cierto. Por lo que tenemos tres casos para $g_{P^n}^+=0$:

- Para $(n,d)=(1,1)$, $P^n=P_1$, donde gr $P_1=1$,
- Para $(n,d)=(1,2)$, $P^n=P_2$, donde gr $P_2=2$,
- Para $(n,d)=(2,1)$, $P^n=P_1^2$, donde gr $P_1=1$

para $q\geq 3$.

Ahora consideremos el caso en que M contiene al menos dos factores primos. Usaremos la notación del lema 4.2.7.

Veamos el caso en que $\boldsymbol{q=3}$.
***Caso r =* 2:** Por el lema 4.2.4, sólo P_1, P_2 y P_1^2, donde gr $P_1=1$ y gr $P_2=2$, pueden ser factores de M.
Entonces se tiene el siguiente cuadro con el género g_M^+.

M	$\Phi(M)$	s_1	s_2	g_M	g_M^+
P_1P_1'	4	1	1	0	0
P_1P_2	16	1	7	7	2
$P_1P_1'^2$	12	1	9	4	1
P_2P_2'	64	7	7	65	25
$P_1^2P_2$	48	9	7	43	16
$P_1^2P_1'^2$	36	9	9	28	19

Cuadro 4.1: Género del campo K_M^+ $(q = 3, r = 2)$

Vemos que sólo en el caso en que $M = P_1P_1'$, con $P_1 \neq P_1'$ y gr $P_1 =$ gr $P_1' = 1$, se tiene $g_M^+ = 0$.

***Caso r* = 3:** P_1P_1' puede ser un factor de M. El otro factor no puede ser un polinomio de grado 2, pues si P_2 o P_1^2 es un factor de M, entonces el género del campo es mayor que cero por el cuadro 4.1 y el lema 4.2.4. Con esto sólo debemos calcular el género para el caso $M = P_1P_1'P_1''$, donde P_1, P_1', P_1'' son distintos a pares y de grado 1.
Entonces $\Phi(P_1P_1'P_1'') = 8$, $s_1 = s_2 = s_3 = 1$. Sustituyendo en la ecuación (3.4) se obtiene $g_M = 1$. Por último con la ecuación (3.6) tenemos que $g_M^+ = 0$.

Ahora veremos el caso en que $\boldsymbol{q} \geq \mathbf{4}$.
En este caso necesitamos el siguiente lema:

Lema 4.2.8. *Sean $q \geq 4$, $r \geq 2$ y suponemos que M es de uno de los siguientes tipos:*

1. $M = \prod_{i=1}^{r_1} P_{1,i}$ *con* $\operatorname{gr} P_{1,i} = 1$,
2. $M = \prod_{i=1}^{r_2} P_{2,i}$ *donde* $\operatorname{gr} P_{2,i} = 2$,
3. $M = \prod_{i=1}^{r_3} P_{1,i}$, *con* $\operatorname{gr} P_{1,i} = 1$.

Entonces el género g_M^+ es mayor que uno si y sólo si cumplen, según el caso, las siguientes desigualdades: $r_1 \geq 3$, $r_2 \geq 2$ y $r_3 \geq 2$.

Demostración. Para el caso 1 sustituimos $n_i = d_i = 1$ en la fórmula (3.4) del género y sea $r = r_1$. Entonces

$$\Phi(M) = \prod_{i=1}^{r} (q-1) = (q-1)^r$$
$$s_i = (q-1) - q^0 = q-2,$$

$$\begin{aligned} 2g_M - 2 &= -2(q-1)^r + r\left((q-2)\frac{(q-1)^r}{q-1}\right) + (q-2)\frac{(q-1)^r}{(q-1)} \\ &= -2(q-1)^r + r(q-2)(q-1)^{r-1} + (q-2)(q-1)^{r-1} \\ &= (q-1)^{r-1}\left[r(q-2) + (q-2) - 2(q-1)\right] \\ &= (q-1)^{r-1}(q(r-1) - 2r). \end{aligned}$$

Sustituyendo en la ecuación (3.6) se tiene:

$$\begin{aligned} 2g_M^+ - 2 &= \frac{1}{q-1}\left\{(q-1)^{r-1}(q(r-1) - 2r) - \frac{(q-1)^r}{q-1}(q-2)\right\} \\ &= \frac{1}{q-1}\left\{(q-1)^{r-1}(q(r-1) - 2r) - (q-1)^{r-1}(q-2)\right\} \\ &= (q-1)^{r-2}\{qr - 2q - 2r + 2\} \\ &= (q-1)^{r-2}\{(r-2)(q-2) - 2\}. \end{aligned}$$

Observamos que $g_M^+ = 0$ si y sólo si $r = 2$.

Con esto tenemos la prueba del caso 1.

Caso 2: sea $r = r_2$ y $M = \prod_{i=1}^{r} P_{2,i}$. En este caso $n_i = 1$ y $d_i = 2$. Entonces

$$\Phi(M) = \prod_{i=1}^{r} \left(q^2-1\right) = \left(q^2-1\right)^r$$
$$s_i = \left(q^2-1\right) - 1 = q^2 - 2.$$

Sustituyendo en la ecuación (3.4) tenemos:

$$\begin{aligned} 2g_M - 2 &= -2\left(q^2-1\right)^r + r\left(\left(q^2-2\right)\frac{\left(q^2-1\right)^r}{q^2-1}\cdot 2\right) + (q-2)\frac{\left(q^2-1\right)^r}{q-1} \\ &= -2\left(q^2-1\right)^r + 2r\left(q^2-2\right)\left(q^2-1\right)^{r-1} + (q-2)(q+1)\left(q^2-1\right)^{r-1} \\ &= \left(q^2-1\right)^{r-1}\left[2r\left(q^2-2\right) + (q+1)(q-2) - 2\left(q^2-1\right)\right] \\ &= \left(q^2-1\right)^{r-1}\left[q^2(2r-1) - q - 4r\right]. \end{aligned}$$

Sustituyendo en la ecuación (3.6):

$$\begin{aligned} 2g_M^+ - 2 &= \frac{1}{q-1}\left\{\left(q^2-1\right)^{r-1}\left[q^2(2r-1)-q-4r\right]-\frac{\left(q^2-1\right)^r}{q-1}(q-2)\right\} \\ &= \frac{1}{q-1}\left\{\left(q^2-1\right)^{r-1}\left(q^2(2r-1)-q-4r-(q+1)(q-2)\right)\right\} \\ &= (q+1)\left(q^2-1\right)^{r-2}\left(2(r-1)q^2-4r+2\right). \end{aligned}$$

Observamos que en este caso no es posible que $g_M^+ = 0$, pues $q \geq 4$.

Con esto tenemos la prueba del caso 2.

Ahora para el caso 3, sean $n_i = 2$, $d_i = 1$ y $r = r_3$. Entonces

$$\begin{aligned} \Phi(M) &= \prod_{i=1}^{r} q(q-1) = (q(q-1))^r \\ s_i &= 2 \cdot q(q-1) - q = 2q^2 - 3q. \end{aligned}$$

Por la ecuación (3.4), tenemos:

$$\begin{aligned} 2g_M - 2 &= -2q^r(q-1)^r + r\left[\left(2q^2-3q\right)\frac{q^r(q-1)^r}{q(q-1)}\right] + (q-2)\frac{q^r(q-1)^r}{q-1} \\ &= q^r(q-1)^{r-1}\left[(2q-3)r+q-2-2(q-1)\right] \\ &= q^r(q-1)^{r-1}\left[2qr-3r+q-2-2q+2\right] \\ &= q^r(q-1)^{r-1}\left((2r-1)q-3r\right). \end{aligned}$$

Luego de la ecuación (3.6), tenemos:

$$\begin{aligned} 2g_M^+ - 2 &= \frac{1}{q-1}\left\{q^r(q-1)^{r-1}\left((2r-1)q-3r\right)-\frac{q^r(q-1)^r}{q-1}(q-2)\right\} \\ &= \frac{1}{q-1}\left\{q^r(q-1)^{r-1}\left[(2r-1)q-3r-q+2\right]\right\} \\ &= q^r(q-1)^{r-2}\left[2(r-1)q-3r+2\right]. \end{aligned}$$

Observamos que también en este caso, puesto que $q \geq 4$, g_M^+ no puede ser cero. □

Ahora veamos el caso en que $\boldsymbol{r = 2}$**:**

Por el lema 4.2.8 debemos determinar el género para los siguientes cuatro casos:

1. $M = P_1 P_1'$,
2. $M = P_1 P_2$,
3. $M = P_1 P_1'^2$,
4. $M = P_1^2 P_2$,

donde gr P_1 = gr P_1' = 1 y gr $P_2 = 2$.
Para el primer caso, por el argumento en la prueba del lema 4.2.8, $g_M^+ = 0$.
Para el segundo caso, se tiene $d_1 = n_1 = n_2 = 1$, $d_2 = 2$. Así

$$\Phi(M) = (q-1)\left(q^2-1\right),\ s_1 = q-2 \text{ y } s_2 = q^2-2.$$

Sustituyendo en la ecuación (3.4), se tiene:

$$\begin{aligned}
2g_M - 2 &= -2(q-1)\left(q^2-1\right) + (q-2)\frac{(q-1)\left(q^2-1\right)}{q-1} \\
&\quad + \left(q^2-2\right)\frac{(q-1)\left(q^2-1\right)}{q^2-1}\cdot 2 + (q-2)\frac{(q-1)\left(q^2-1\right)}{q-1} \\
&= -2(q-1)\left(q^2-1\right) + 2(q-2)\left(q^2-1\right) + 2\left(q^2-2\right)(q-1) \\
&= (q-1)\left(2(q-2)(q+1) + 2\left(q^2-2\right) - 2\left(q^2-1\right)\right) \\
&= (q-1)\left(2q^2-2q-6\right) = 2(q-1)\left(q^2-q-3\right).
\end{aligned}$$

Ahora usando la ecuación (3.6).

$$\begin{aligned}
2g_M^+ - 2 &= \frac{1}{q-1}\left\{2(q-1)\left(q^2-q-3\right) - \frac{(q-1)\left(q^2-1\right)}{q-1}(q-2)\right\} \\
&= \frac{1}{q-1}\left\{(q-1)[2\left(q^2-q-3\right) - (q+1)(q-2)]\right\} \\
&= q^2-q-4.
\end{aligned}$$

Entonces $g_M^+ = 0$ si y sólo si $q^2-q-2 = (q-2)(q+1) = 0$, pero $q \geq 4$, así que este caso no se puede dar.
Para el caso en que $d_1 = d_2 = 1$, $n_1 = 1$ y $n_2 = 2$, tenemos

$$\Phi(M) = q(q-1)^2,\ s_1 = q-2 \text{ y } s_2 = 2q^2-3q.$$

Usando la ecuación (3.4) se tiene:

$$\begin{aligned}2g_M - 2 &= -2q\,(q-1)^2 + (q-2)\frac{q\,(q-1)^2}{q-1} + \left(2q^2-3q\right)\frac{q\,(q-1)^2}{q(q-1)} + (q-2)\frac{q\,(q-1)^2}{q-1}\\ &= -2q\,(q-1)^2 + q(q-2)(q-1) + q(2q-3)(q-1) + (q-2)q(q-1)\\ &= q(q-1)(2q-5).\end{aligned}$$

Ahora con la ecuación (3.6) tenemos:

$$\begin{aligned}2g_M^+ - 2 &= \frac{1}{q-1}\left\{q(q-1)(2q-5) - \frac{q\,(q-1)^2}{q-1}(q-2)\right\}\\ &= \frac{1}{q-1}\left\{q(q-1)(q-3)\right\} = q(q-3).\end{aligned}$$

Entonces $g_M^+ = 0$ si y sólo si $q^2 - 3q + 2 = (q-2)(q-1) = 0$. Pero $q \geq 4$, así que este caso no se puede dar.

Finalmente, para el caso en que $M = P_1^2 P_2$, donde $n_1 = 2$, $n_2 = 1$, $d_1 = 1$ y $d_2 = 2$ tenemos:

$$\Phi(M) = q(q-1)\left(q^2-1\right),\ s_1 = q(2q-3) \text{ y } s_2 = q^2 - 2.$$

Nuevamente sustituyendo en la ecuación (3.4) tenemos:

$$\begin{aligned}2g_M - 2 &= -2q(q-1)\left(q^2-1\right) + q(2q-3)\frac{q(q-1)\left(q^2-1\right)}{q(q-1)} + \left(q^2-2\right)\frac{q(q-1)\left(q^2-1\right)}{q^2-1}\cdot 2\\ &\quad + (q-2)\frac{q(q-1)\left(q^2-1\right)}{q-1}\\ &= -2q(q-1)\left(q^2-1\right) + q(2q-3)\left(q^2-1\right) + 2q(q-1)\left(q^2-2\right) + q(q-2)\left(q^2-1\right)\\ &= q(q-1)[-2\left(q^2-1\right) + (2q-3)(q+1) + 2\left(q^2-2\right) + (q-2)(q+1)]\\ &= q(q-1)[3q^2 - 2q - 7].\end{aligned}$$

Luego

$$\begin{aligned}2g_M^+ - 2 &= \frac{1}{q-1}\left\{q(q-1)\left(3q^2-2q-7\right) - \frac{q(q-1)\left(q^2-1\right)}{q-1}(q-2)\right\}\\ &= \frac{1}{q-1}\left\{q(q-1)[3q^2 - 2q - 7 - (q+1)(q-2)]\right\}\\ &= q\left(2q^2 - q - 5\right).\end{aligned}$$

Notemos que para $q \geq 4$, $q\left(2q^2 - q - 5\right) > 0$, luego este caso tampoco se puede dar.

Por los lemas 4.2.8 y 4.2.4, no es necesario considerar el caso $r \geq 3$.

Con estos resultados se tiene el siguiente teorema:

Teorema 4.2.9. *El número de clases de divisores h_M^+ del subcampo real maximal K_M^+ del campo de funciones ciclotómicos K_M es uno si y sólo si M es de uno de los siguientes tipos:*
(a) Si $q = 3$, entonces $M = P_1$, $M = P_2$, $M = P_1^2$, $M = P_1P_1'$, $M = P_1P_1'P_1''$, donde P_1, P_1', P_1'' son polinomios irreducibles de grado 1 y primos relativos a pares y P_2 es un polinomio irreducible de grado 2.
(b) Si $q \geq 4$, entonces $M = P_1$, $M = P_2$, $M = P_1^2$, $M = P_1P_1'$, donde P_1, P_1' son polinomios irreducibles de grado 1, $P_1 \neq P_1'$ y P_2 es un polinomio irreducible de grado 2.

Para campos de funciones ciclotómicos tenemos el siguiente resultado:

Teorema 4.2.10. *El número de clases de divisores h_M del campo de funciones ciclotómicos K_M es uno si y sólo si M es de uno de los siguientes tipos:*
(a) Si $q = 2$, entonces $M = P_1$, $M = P_2$, $M = P_1^2$, $M = P_1P_1'$, $M = P_1P_1'^2$, $M = P_1P_2$, $M = P_1P_1'P_2$, donde P_1, P_1', P_1'' son polinomios irreducibles de grado 1 distintos y P_2 es un polinomio irreducible de grado 2.
(b) Si $q = 3$, entonces $M = P_1$, $M = P_1P_1'$, donde P_1 y P_1' son polinomios irreducibles de grado 1 y $P_1 \neq P_1'$.
(c) Si $q \geq 4$, entonces $M = P_1$, donde P_1 es un polinomio irreducible de grado 1.

Demostración. Sea $M = \prod_{i=1}^{r} P_i^{n_i}$ la factorización de M. Empezaremos con el caso ***q=2*** y ***r=1***.
$M = P_1^{n_1}$. Haciendo $n = n_1$, $d = d_1$,

$$\Phi(M) = 2^{d(n-1)}\left(2^d - 1\right),$$
$$s = n \cdot 2^{d(n-1)}\left(2^d - 1\right) - 2^{d(n-1)}.$$

Sustituyendo $g_M = 0$ en la ecuación (3.4) de la fórmula del género se tiene:
$-2 = -2 \cdot 2^{d(n-1)}\left(2^d - 1\right) + \left(n \cdot 2^{d(n-1)} - 2^{d(n-1)}\right)d$ y esta igualdad se cumple si y sólo si $(d, n) = (1, 1)$ ó $(d, n) = (2, 1)$ ó $(d, n) = (1, 2)$.
Así $M = P_1, P_2$ o P_1^2, donde gr $P_1 = 1$ y gr $P_2 = 2$.

Ahora veamos el caso en que **r** ≥ 2. Para esto suponemos que $\boldsymbol{q = 2}$ y $\boldsymbol{r = 2}$. Vemos que sólo hay dos polinomios irreducibles de grado uno y uno de grado dos. Así hay sólo cinco casos posibles para ver si el género es cero. Los valores del género se reflejan en el siguiente cuadro:

M	$\Phi(M)$	s_1	s_2	g_M
P_1P_1'	1	0	0	0
P_1P_2	3	0	2	0
$P_1P_1'^2$	2	0	2	0
$P_1^2P_2$	6	2	2	2
$P_1^2P_1'^2$	4	2	2	1

Cuadro 4.2: Género del campo K_M $(q = 2, r = 2)$

Ahora para el caso en que $\boldsymbol{q = 2}$ y $\boldsymbol{r = 3}$, sólo se puede tener $M = P_1P_1'P_2$, donde gr $P_1 =$ gr $P_1' = 1$, gr $P_2 = 2$ y $P_1 \neq P_1'$. En este caso

$$\Phi(M) = 3,\ s_1 = s_2 = 0 \text{ y } s_3 = 2.$$

Entonces $2g_M - 2 = -2 \cdot 3 + 4 = -2$ y así $g_M = 0$.
Suponemos ahora que $\boldsymbol{q = 3}$. Por el Lema 4.2.4, sólo debemos calcular el género para los casos que se tienen en el teorema 4.2.9. Usamos la ecuación (3.4) para el género g_M. Entonces tenemos los resultados reflejados en el siguiente cuadro:

M	$\Phi(M)$	s_1	s_2	s_3	g_M
P_1	2	1			0
P_2	8	7			2
P_1^2	6	9			1
P_1P_1'	4	1	1		0
$P_1P_1'P_1''$	8	1	1	1	1

Cuadro 4.3: Género del campo K_M $(q = 3)$

Finalmente veremos el caso en que $\boldsymbol{q \geq 4}$.

- $M = P_1$. Entonces $\Phi(M) = q - 1$ y $s = q - 2$.

$$\begin{aligned} 2g_M - 2 &= -2(q-1) + q - 2 + q - 2 \\ &= -2. \end{aligned}$$

Así que $g_M = 0$.

- $M = P_2$. Entonces $\Phi(M) = q^2 - 1$ y $s = q^2 - 2$. Luego

$$\begin{aligned} 2g_M - 2 &= -2\left(q^2-1\right) + \left(q^2-2\right)\cdot 2 + (q-2)\frac{q^2-1}{q-1} \\ &= -2\left(q^2-1\right) + 2\left(q^2-2\right) + (q-2)(q+1) \\ &= q^2 - q - 4. \end{aligned}$$

  Entonces $g_M = \dfrac{(q-2)(q+1)}{2}$.

- $M = P_1^2$. Aquí $\Phi(M) = q(q-1)$, $s = 2q(q-1) - q$ y

$$\begin{aligned} 2g_M - 2 &= -2q(q-1) + (2q(q-1) - q) + (q-2)\frac{q(q-1)}{q-1} \\ &= -2q(q-1) + (2q(q-1) - q) + q(q-2) \\ &= q^2 - 3q. \end{aligned}$$

  Con esto $g_M = \dfrac{(q-1)(q-2)}{2}$.

- $M = P_1P_1'$, $\Phi(M) = (q-1)^2$ y $s_1 = s_2 = q-2$. Se tiene

$$\begin{aligned} 2g_M - 2 &= -2(q-1)^2 + 2\left[(q-2)\frac{(q-1)^2}{q-1}\right] + (q-2)\frac{(q-1)^2}{q-1} \\ &= (q-1)\left(3(q-2) - 2(q-1)\right) \\ &= (q-1)(q-4). \end{aligned}$$

  Luego, $g_M = \dfrac{(q-2)(q-3)}{2}$.

Los resultados anteriores se resumen en el siguiente cuadro:

M	$\Phi(M)$	s_1	s_2	g_M
P_1	$q-1$	$q-2$		0
P_2	q^2-1	q^2-2		$\dfrac{(q-2)(q+1)}{2}$

P_1^2	$q(q-1)$	$2q(q-1)-q$		$\frac{(q-1)(q-2)}{2}$
P_1P_1'	$(q-1)^2$	$q-2$	$q-2$	$\frac{(q-2)(q-3)}{2}$

Cuadro 4.4: Género del campo K_M $(q \geq 4)$

Vemos que los valores de g_M en el cuadro, excepto por el primero, son mayores que cero. Con esto tenemos la prueba del teorema. □

Ahora veremos algunos ejemplos.

Ejemplo 4.2.11. Si $q = 2$ y $M = T(T-1)$, entonces gr T = gr $(T-1) = 1$, $n_T = n_{T-1} = 1$.
$\Phi(M) = \left(2^{1(1-1)}(2^1-1)\right)^2 = \left(2^0\right)^2 = 1$, $s_T = s_{T-1} = 1 \cdot 1 - 2^0 = 0$.
Sustituyendo en la ecuación (3.4):
$2g_M - 2 = -2 - 1(0) = -2$. Entonces $2g_M = 0$ y por lo tanto $g_M = 0$. Por el lema 4.2.4, $g_M^+ = 0$. Luego por el teorema 4.2.2, $h_M = 1$ y $h_M^+ = 1$.

Ejemplo 4.2.12. Sean $q = 4$ y $M = T$. Entonces gr $T = n_T = 1$, $\Phi(M) = 4^0(4-1) = 3$ y $s = 3 - 4^0 = 2$. Sustituyendo en la ecuación (3.4):
$2g_M - 2 = -2 \cdot 3 + 2\frac{3}{3} + (4-2)\frac{3}{3} = -6 + 2 + 2 = -2$. Entonces $2g_M = 0$. Luego $g_M = 0$ y por el lema 4.2.4 y el teorema 4.2.2, $h_M = h_M^+ = 1$.

Ejemplo 4.2.13. Sean $q = 4$ y $M = T^2$. Entonces $d = 1$, $n = 2$, Luego $\Phi(M) = 4(3) = 12$ y $s = 2 \cdot 12 - 4 = 20$. Sustituyendo en la ecuación (3.4)

$$2g_M - 2 = -2 \cdot 12 + 20\left(\frac{12}{12}\right) + 2\left(\frac{12}{3}\right) = -24 + 20 + 8 = 4.$$

Entonces $2g_M = 6$ y $g_M = 3$. Con esto no podemos dar el valor de h_M, pero sí sabemos que $h_M > 1$. Ahora sustituyendo en la ecuación (3.5):

$$2g_M^+ - 2 = (2-2)^{\frac{12}{3}} - \frac{4-1}{4-1} - 1 = -2.$$

Entonces $2g_M^+ = 0 = g_M^+$. Luego por el teorema 4.2.2, $h_M^+ = 1$.

Ejemplo 4.2.14. Sean $q = 4$ y $M = T^2(T-1)$. Entonces $d_1 = d_2 = 1$, $n_1 = 2$ y $n_2 = 1$, $\Phi(M) = 4(4-1)\cdot 4^0(4-1) = 12\cdot 3 = 36$ y $s_1 = 2\cdot 12 - 4 = 20$, $s_2 = 3 - 4^0 = 2$.
Sustituyendo en la ecuación (3.4):

$$2g_M - 2 = -2\cdot 36 + 20\frac{36}{12} + 2\frac{36}{3} + 2\frac{36}{3} = 36.$$

Entonces $2g_M = 38$ y $g_M = 19$. Con esto no podemos dar el valor para h_M, pero sí sabemos que $h_M > 1$.
Sustituyendo ahora en la ecuación (3.6):

$$2g_M^+ - 2 = \frac{1}{3}\left\{36 - \frac{36}{3}(2)\right\} = \frac{1}{3}(36-24) = 4.$$

Entonces $2g_M^+ = 6$ y $g_M^+ = 3$. No podemos dar el valor de h_M^+, pero sabemos que $h_M^+ > 1$.

Apéndice A

Método de Newton y lema de Abhyankar

A.1. Método de Newton

Sea F un campo completo con respecto a una valuación discreta v con lugar $\mathcal{P}$. Sea $\bar{F}$ una cerradura algebraica de F. Sea $f(x) = a_0 + a_1x + \ldots + a_nx_n \in F[x]$ con $a_0a_n \neq 0$. A cada término de $f(x)$ se le asocia un punto $\mathbb{R} \times \mathbb{R}$ de la siguiente forma: Si $a_ix^i \neq 0$, es decir, $a_i \neq 0$, se toma $(i, v(a_i))$. Si $a_ix^i = 0$, es decir, $a_i = 0$, se toma el punto inexistente (i, ∞).
Se forma la cubierta convexa inferior del conjunto de puntos $\{(i, v(a_i)) \mid i = 0, 1, \ldots, n\}$. A este conjunto se le llama *polígono de Newton*.
Los vértices de esta cubierta inferior son: $\{(i_0 = 0, v(a_0)), (i_1, v(a_1)), \ldots, (i_m = n, v(a_n))\}$.

Primero se considera $S = \{i > 0 \mid a_i \neq 0\}$, si hay varios i con el mismo $v(a_i)$, se toma el que está más a la derecha.
Sea i_1 el máximo con la propiedad:

$$\frac{v(a_{i_1}) - v(a_0)}{i_1 - 0} = \text{mín} \left\{ \frac{v\left(a_j\right) - v(a_0)}{j - 0} \mid j \in S \right\}.$$

Sea i_2 el máximo con la propiedad:

$$\frac{v(a_{i_2}) - v(a_{i_1})}{i_2 - i_1} = \text{mín} \left\{ \frac{v\left(a_j - v_{a_{i_1}}\right)}{j - i_1} \mid j \in S, j > i_1 \right\}.$$

Se sigue con este proceso hasta terminar con los vértices.

Proposición A.1.1. *Supongamos que* $(r, v(a_r)) \leftrightarrow (s, v(a_s))$*, con* $s > r$*, es cualquier segmento del polígono de Newton de* $f(x)$ *y tiene pendiente* $\dfrac{v(a_s) - v(a_r)}{s - r} = -m$*. Entonces* $f(x)$ *tiene exactamente* $s - r$ *raíces* $\alpha_1, \alpha_2, \ldots, \alpha_{s-r}$ *en* F*, con valuación* $v(\alpha_1) = \ldots = v(\alpha_{s-r}) = m$*.*
Más aún, si $f_m(x) = \prod_{i=1}^{s-r}(x - \alpha_i) \in F[x]$*, entonces* $f_m(x) \mid f(x)$*.*

Demostración. Ver [17], pp. 431-433. □

A.2. Lema de Abhyankar

Teorema A.2.1. *Sea* E/F *una extensión finita y separable de campos de funciones. Sea* $E = F_1F_2$ *con* $F \subseteq F_i \subseteq E$*.*
Sea $\mathfrak{p}$ *un divisor primo de* F *y sea* $\mathfrak{P}$ *un divisor primo de* E *sobre* $\mathfrak{p}$*. Sean* $\mathfrak{P}_i := \mathfrak{P} \cap F_i$*,* $i = 1, 2$*. Si al menos una de las extensiones* $\mathfrak{P}_1/\mathfrak{p}$ *y/o* $\mathfrak{P}_2/\mathfrak{p}$ *tiene ramificación moderada, entonces*

$$e(\mathfrak{P}/\mathfrak{p}) = \operatorname{mcm}\left[e_1(\mathfrak{P}_1 \mid \mathfrak{p}), e_2(\mathfrak{P}_2 \mid \mathfrak{p})\right].$$

Demostración. Ver [17], pp. 434-435. □

Conclusiones

Este trabajo se desarrolló en el contexto de campos de funciones en una variable sobre el campo finito $\mathbb{F}_q$ con q elementos. Entre los conceptos introducidos están el número de clases de divisores h y el género g. Se estudió el tema de campos de funciones ciclotómicos, entre cuyos resultados principales están el grupo de Galois del campo ciclotómico K_M sobre el campo de funciones racionales $K = \mathbb{F}_q(T)$, el polinomio característico $\Psi_M(u)$ y el valor de Φ_M, para el polinomio mónico

$$M = \prod_{i=1}^{r} P_i^{n_i},$$

donde los P_i son polinomios irreducibles de grado d_i, así como la ramificación y el grupo de descomposición de $\mathfrak{p}_\infty$ y el subcampo real maximal K_M^+ de K_M. Aplicando las fórmulas para los diferentes de K_M y K_M^+ al teorema del género de Riemann-Hurwitz, se obtuvieron fórmulas para los géneros g_M y g_M^+ de K_M y K_M^+ respectivamente, las cuales están en términos de $\Phi(M)$ y s_i, donde

$$s_i = n_i \Phi(P_i^{n_i}) - q^{d_i(n_i-1)}.$$

Como vimos, para resolver el problema de determinar los campos de funciones ciclotómicos con número de clases de divisores uno, se empieza reduciendo las condiciones necesarias para que el número de clases de divisores h sea mayor que uno. Como se tiene que esto pasa si $g > 0$ y $q > 4$, se usa la hipótesis de Riemann para acotar la función

$$S(q, g, 1) = (q-1)\left[q^{2g-1} + 1 - 2g\sqrt{q^{2g-1}}\right] - (2g-1)(q^g - 1),$$

y ver cuándo es creciente.

Se sabe que si $g = 0$, entonces $h = 1$. Pero si $g \geq 1$, sólo es posible que $h = 1$ cuando: $q = 4,\ g = 1;\ q = 3,\ g = 1;\ q = 2,\ g = 1, 2, 3$. De esta forma las posibilidades para que el número de clases de divisores sea uno son mínimas.

Es de crucial importancia que, en el caso de los campos ciclotómicos K_M, se cumple

$$h_M = 1 \text{ si y solamente si } g_M = 0,$$

y lo mismo se cumple para sus subcampos reales K_M^+, ya que nuestro problema se redujo a determinar los campos de género cero. Esto no sucede en el caso general, como se muestra con un ejemplo de un campo L para el que $h_L = 1$, pero $g_L = 1$.

Una primera observación es que si $q = 2$ y $g_M = 0$, entonces el número r de polinomios irreducibles involucrados en la factorización de M cumple $r \leq 3$. Asimismo, si $q \geq 3$ y $g_M^+ = 0$, entonces $r \leq 3$.

Se trataron primero los subcampos reales maximales, observando que, cuando $q = 2$, $K_M^+ = K_M$ y se obtuvieron explícitamente los tipos de polinomios M que admiten $g_M^+ = 0$.

Finalmente, se determinaron los campos ciclotómicos cuyo número de clases de divisores es uno (o lo que es lo mismo, cuyo género es igual a cero), en términos de la factorización de M como producto de polinomios irreducibles. Cuando $q = 2$, M puede ser producto de hasta tres polinomios irreducibles de grados 1 y 2, con ciertas restricciones. Si $q = 3$, M puede ser producto de hasta dos polinomios irreducibles de grado 1 y, si $q = 4$, la única opción que tiene M es ser un polinomio irreducible de grado 1.

Bibliografía

[1] Artin, E. and Tate, J., Class field theory, W.A. Benjamin Inc., 1967.

[2] Carlitz, L., *A class of polynomials*, Trans. Amer. Math. Soc. **43** (1938), 137–168.

[3] Eichler, M., Introduction to the theory of algebraic numbers and functions, Academic Press, 1966.

[4] Galovich, S. and Rosen, M., *The class number of cyclotomic function fields*, J. Number Theory, **13** (1981), 363–375.

[5] Galovich, S. and Rosen, M., *Units and class groups in cyclotomic function fields*, J. Number Theory, **14** (1982), 156–184.

[6] Hayes, D. R., *Explicit class field theory for rational function fields*, Trans. Amer. Math. Soc. **189** (1974), 77–91.

[7] Iwasawa, K., Algebraic functions, American Mathematical Society, 1993.

[8] Jung, H. and Ahn, J., *Divisor class number one problem for abelian extensions over rational function fields*, J. Algebra, **310** (2007), 1–14.

[9] Kato, K., et. al., Number theory: introduction to class field theory, American Mathematical Society, 2011.

[10] Kida, M. and Murabayashi, N., *Cyclotomic function fields with divisor class number one*, Tokio J. Math, **14** No. 1 (1991), 45–56.

[11] MacRae, R. E., *On unique factorization in certain rings of algebraic functions*, J. Algebra, **17** (1971), 243–261.

[12] Madan, M. L. and Queen, C. S., *Algebraic function fields of class number one*, Acta Arith., **20**, (1972), 423-432.

[13] Neukirch, J., Algebraic number theory, Springer-Verlag, Berlin-New York, 1999.

[14] Rosen, M., Number theory in function fields, GTM 210, Springer-Verlag, New York-Berlin-Heidelberg, 2002.

[15] Serre, J. P., Local fields, GTM 67, Springer-Verlag, New York-Berlin-Heidelberg, 1979.

[16] Stichtenoth, H., Algebraic function fields and codes, Universitext, Springer-Verlag, Berlin-New York, 1993.

[17] Villa Salvador, G. D., Topics in the theory of algebraic function fields, Mathematics: Theory & Applications, Birkhäuser Boston, Inc., Boston, MA, 2006.

[18] Whashington L. C., Introduction to Cyclotomic Fields, GTM 83, Springer-Verlag, New York, 1997.