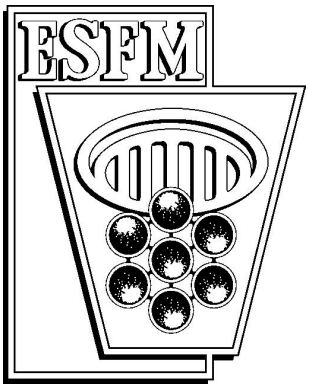


INSTITUTO POLITÉCNICO NACIONAL

Escuela Superior de Física y Matemáticas

Caracteres de Dirichlet en Campos de Funciones

TESIS

QUE PARA OBTENER EL GRADO DE
MAESTRO EN CIENCIAS

PRESENTA

JULIO CESAR SALAS TORRES

Directora de Tesis
Doctora Martha Rzedowski Calderón

Enero del 2005

A mis padres y hermanos...

A Dalila †

La lectura nunca fue un hábito
mas me acostumbré por la necesidad
por el hambre y mi pobreza.
Mi familia fue mi decisión
la fuerza que me dio en la voluntad
la energía que el pan no me daba
y la lucha contra la miseria
La decisión hace la realidad
el sueño nos hace miserables
y la perseverancia nos lleva al triunfo.

Tircis Salas Torres

Agradecimientos

Por su amistad y por ser un ejemplo a seguir, agradezco:

A mi asesora de tesis la Doctora Martha Rzedowski Calderón, por haber confiado en mí, motivándome a seguir adelante sin bajar los brazos, haberme tenido paciencia y guiarme en la realización de este trabajo...

Un agradecimiento muy especialmente a los Doctores Gabriel Villa Salvador y Pablo Lam Estrada por sus consejos y el apoyo incondicional que me han brindado...

A los Doctores José María Rocha Martínez, Roberto S. Acosta Abreu y José Germán González Santos por la revisión de este trabajo...

A los Doctores Arturo Zuñiga Segundo, César Alberto Escobar Gracia y al M. en C. Rubén Mancio Toledo por sus valiosos consejos...

A mis profesores por sus enseñanzas...

A mis padres por la confianza y el apoyo que siempre me han mostrado...

Agradezco el apoyo parcial para la realización de esta tesis al CONACyT, a través del proyecto $\# \ 36552 - E$.

Resumen

Sea k un campo de funciones racionales sobre un campo finito de característica p. Carlitz y Hayes han descrito una familia de extensiones de k las cuales son análogas a la familia de extensiones ciclotómicas $\mathbb{Q}(\zeta_n)$ sobre el campo $\mathbb{Q}$ de los números racionales. En este trabajo se analizan algunas propiedades aritméticas que comparten estas dos familias, se introduce la notación del subcampo real maximal de los campos de funciones ciclotómicos y se establece el resultado en característica p análogo al teorema clásico de Kronecker-Weber. Se introducen algunos hechos básicos acerca de los caracteres de Dirichlet y vemos cómo éstos pueden ser usados para obtener información sobre la aritmética de los campos numéricos.

El objetivo principal de esta tesis es desarrollar una teoría de caracteres de Dirichlet en campos de funciones y aplicarla a los campos de funciones ciclotómicos para obtener resultados en campos de funciones análogos a los establecidos en campos numéricos. En particular, se tiene que tanto el símbolo de Legendre como su análogo en campos de funciones son caracteres de Dirichlet.

Abstract

Let k be a rational function field over a finite field of characteristic p. Carlitz and Hayes have described a family of extensions of k, which is analogue to the family of cyclotomic extensions $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$, the field of rational numbers. In this work we analyze arithmetic properties that these two families share, we introduce the notation for the maximal real subfield of cyclotomic function fields and we establish the result in characteristic p analogous to the classical theorem of Kronecker-Weber. We introduce basic facts about Dirichlet characters and observe how these can be used to obtain information about the arithmetic of number fields. The main purpose of this thesis is to develop a theory of Dirichlet characters over function fields and apply it to cyclotomic function fields to obtain results in function fields analogous to the ones obtained in number fields. In particular, we have that both the Legendre Symbol and its function field analogue are Dirichlet characters.

Introducción

La teoría de campos ciclotómicos se inició propiamente con el trabajo de Kummer entre 1840 y 1850, sobre el Último Teorema de Fermat y Leyes de Reciprocidad, que pavimentó el camino para el desarrollo de la teoría algebraica de números en general. A mediados de la década de los cincuenta del siglo pasado, Iwasawa y Leopoldt retomaron la teoría de campos ciclotómicos. Poco después, Kubota y Leopoldt inventaron las L-funciones p-ádicas, que fueron interpretadas por Iwasawa en términos de $\mathbb{Z}_p$-extensiones. El desarrollo de esta teoría continúa en diversas direcciones.

Los caracteres de Dirichlet y sus L-series fueron introducidos por Dirichlet en 1831 para probar su teorema sobre la infinidad de primos en progresiones aritméticas. En 1962 Leopoldt utilizó los caracteres de Dirichlet para describir la aritmética de campos abelianos.

Es notable que el anillo de enteros $\mathbb{Z}$ tiene muchas propiedades en común con $R_T = \mathbb{F}_q[T]$, el anillo de polinomios en una variable sobre un campo finito. Ambos anillos son dominios de ideales principales, ambos anillos tienen campos residuales finitos, ambos anillos tienen una infinidad de primos y una finitud de unidades. Es natural entonces, esperar que haya resultados comunes para $\mathbb{Z}$ y R_T. Un campo de funciones algebraicas K en una variable sobre F es una extensión de F con grado de trascendencia uno. Cuando $F = \mathbb{F}_q$ es finito, decimos que K es un campo de funciones congruentes. Se conocen como campos globales a los campos numéricos y a los campos de funciones congruentes. El campo de funciones racionales $\mathbb{F}_q(T)$ es el análogo al campo de números racionales $\mathbb{Q}$, el anillo R_T es al análogo a $\mathbb{Z}$ y un campo de funciones congruentes es el análogo a una extensión finita de $\mathbb{Q}$. Sin embargo hay diferencias fundamentales entre ambas familias de campos: en los campos numéricos tenemos valores absolutos arquimedianos y en los campos de funciones no; el equivalente al anillo de enteros $\mathbb{Z}$ dentro de $\mathbb{Q}$ no tiene

un único similar en los campos de funciones, sino una infinidad, etc. Así, es importante tener en cuenta tanto la similitud entre estas familias de campos como sus diferencias fundamentales.

Por otro lado existen algunos campos de funciones análogos a los campos de números ciclotómicos los cuales descubrió Carlitz en la década de los años treinta del siglo pasado. Esta ingeniosa analogía no fue bien conocida hasta que en 1973, Hayes publicó una exposición de la idea de Carlitz y mostró que ésta contiene una teoría de campos de clases para los campos de funciones racionales. Drinfeld y Hayes, de manera independiente, generalizan esta idea para obtener una teoría explícita de campos de clases para cualquier campo de funciones congruentes, es decir, una construcción explícita de toda extensión abeliana de dicho campo. Esto es una solución completa al Problema 9 de Hilbert en el caso de campos de funciones.

El objetivo principal del presente trabajo es desarrollar una teoría de caracteres de Dirichlet en campos de funciones, paralela a la de campos numéricos, misma que aplicamos a la aritmética de campos de funciones.

En el Capítulo 1 se trata el tema de campos ciclotómicos dentro del contexto de campos numéricos. Se presentan conceptos y resultados que se consideraron importantes para la comprensión del tema. En el Capítulo 2 presentamos la teoría de campos ciclotómicos sobre campos de funciones racionales con campo de constantes finito, los conceptos y resultados son análogos a los del capítulo anterior. En el Capítulo 3 introducimos los hechos básicos acerca de los caracteres de Dirichlet y vemos como éstos pueden ser usados para obtener información sobre la aritmética de campos numéricos. En particular, se prueba que el símbolo de Legendre es un caracter de Dirichlet. Por último, en el Capítulo 4, que es la parte central de este trabajo, definimos caracteres de Dirichlet en el grupo de unidades de ciertos cocientes del anillo de polinomios sobre un campo finito, y los aplicamos a los campos de funciones ciclotómicos para obtener resultados análogos a los establecidos para campos numéricos en el capítulo anterior.

Contenido

Capítulo 1

Campos ciclotómicos

En este capítulo se trata el tema de campos ciclotómicos dentro del contexto de campos numéricos. En la primera sección se presentan algunos conceptos y resultados preliminares de teoría de números y en la segunda aparecen propiamente los campos ciclotómicos.

1.1 Resultados preliminares

Definición 1. Un **campo de números** o **campo numérico** es una extensión finita de $\mathbb{Q}$, el campo de los números racionales.

Siempre consideraremos que dichos campos estén contenidos en $\mathbb{C}$, el campo de los números complejos, es decir, supondremos que la cerradura algebraica $\overline{\mathbb{Q}}$ de $\mathbb{Q}$ está contenida en $\mathbb{C}$.

Definición 2. Sea K un campo numérico. Se define el **anillo de enteros** de K por $\vartheta_K = \{\alpha \in K | \operatorname{irr}(\alpha, \mathbb{Q}, x) \in \mathbb{Z}[x]\}$. Los elementos de ϑ_K se llaman **enteros algebraicos** de K.

Tenemos resultados tales como que $\vartheta_{\mathbb{Q}} = \mathbb{Z}$ o que ϑ_K es la cerradura entera de $\mathbb{Z}$ en K. Si $\alpha \in \vartheta_K$ se sigue $\mathbb{Z}[\alpha] \cong \mathbb{Z}^n$ como $\mathbb{Z}$-módulo (es decir, como grupo abeliano) donde $n = \operatorname{gr}(\operatorname{irr}(\alpha, \mathbb{Q}, x))$.

Definición 3. Cuando $\vartheta_K = \mathbb{Z}w_1 \oplus \cdots \oplus \mathbb{Z}w_n$, $\{w_1, \ldots, w_n\}$ se llama una **base entera** de K.

Definición 4. Se define el **discriminante** del campo K como $\delta(K) = \operatorname{disc}(K) := \operatorname{disc}\{w_1, \ldots, w_n\}$, donde $\{w_1, \ldots, w_n\}$ es cualquier base entera de K.

Teorema 1. *Sea $d \in \mathbb{Z}, d \neq 0, 1$, d libre de cuadrado, $K = \mathbb{Q}(\sqrt{d})$. Entonces, si $d \equiv 2, 3 \bmod 4$ tenemos que $\delta(K) = 4d$, $\{1, \sqrt{d}\}$ es base entera de ϑ_K y $\vartheta_K = \mathbb{Z}[\sqrt{d}] = \left\{a + b\sqrt{d} | a, b \in \mathbb{Z}\right\}$. Si $d \equiv 1 \bmod 4$ tenemos que $\delta(K) = d$, $\left\{1, \dfrac{1+\sqrt{d}}{2}\right\}$ es base entera de ϑ_K y $\vartheta_K = \mathbb{Z}\left[\dfrac{1+\sqrt{d}}{2}\right]$.*

Demostración: Ver [7] página 42.■

Definición 5. Sea K un campo numérico. Las **unidades** de K son los elementos de $E_K = \vartheta_K^* = \{x \in \vartheta_K | x^{-1} \in \vartheta_K\}$. Esto es, $\alpha \in \vartheta_K$ es unidad si existe $\beta \in \vartheta_K$ tal que $\alpha\beta = 1$. Tenemos que E_K es un grupo multiplicativo.

Sea K un campo numérico, $[K : \mathbb{Q}] = n$. Sea $\widetilde{K}$ la cerradura normal de $K/\mathbb{Q}$ y sean $\mathrm{id} = \sigma_1, \sigma_2, \ldots, \sigma_n$ los distintos monomorfismos de K en $\widetilde{K}$. Se tiene que la **norma** $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \mathrm{N}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \in \mathbb{Q}$ y la **traza** $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) \in \mathbb{Q}$, para toda $\alpha \in K$. En general, sean L/K una extensión $[L : K] = n$ e $\mathrm{id} = \sigma_1, \ldots, \sigma_n$ los distintos monomorfismos $\sigma : L \to \widetilde{L}$, $\widetilde{L}$ la cerradura normal de L/K, que satisfacen $\sigma|_K = \mathrm{id}_K$. Entonces, si $\alpha \in L$, $\mathrm{N}_{L/K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \in K$ y $\mathrm{Tr}_{L/K}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) \in K$. Finalmente, si $\alpha \in \vartheta_L$, $\mathrm{Tr}_{L/K}(\alpha), \mathrm{N}_{L/K}(\alpha) \in K \cap \vartheta_{\widetilde{L}} = \vartheta_K$.

Proposición 1. *Sea $\alpha \in \vartheta_K$. Entonces $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = 1$ si y sólo si α es unidad.*

Demostración: Ver [7] página 47.■

Teorema 2. *Sea $K = \mathbb{Q}(\sqrt{d})$, $d < 0$ y libre de cuadrado. Las unidades de K son:*

(i) $d = -1$, $E_K = \{1, -1, i, -i\}$.

(ii) $d=-3$, $E_K=\left\{\zeta_6^j|0\leq j\leq 5\right\}$, *donde* $\zeta_6=\dfrac{1+i\sqrt{3}}{2}$.

(iii) $d\neq -1,-3$, $E_K=\{\pm 1\}$.

Demostración: Ver [7] página 48.■

Si $d>0$ el problema es mucho más difícil. Para que $a+b\sqrt{d}$ sea unidad se debe tener, cuando $d\equiv 2,3 \bmod 4$, $\mathrm{N}(a+b\sqrt{d})=a^2-db^2=\pm 1$. Si $d\equiv 1 \bmod 4$, para que $a+b\left(\dfrac{1+\sqrt{d}}{2}\right)$ sea unidad se debe tener $\mathrm{N}\left(a+b\left(\dfrac{1+\sqrt{d}}{2}\right)\right)=\left(a+\dfrac{b}{2}\right)^2-\dfrac{db^2}{4}=\pm 1$ ó $(2a+b)^2-db^2=\pm 4$. Resulta ser que hay un número infinito de soluciones. Más aún, existe un $\omega\in\vartheta_K$, $\omega>1$ tal que todas las unidades de ϑ_K son $\{\pm\omega^n|\, n\in\mathbb{Z}\}$ por lo tanto $E_K=\vartheta_K^*\cong\{\pm 1\}\times\mathbb{Z}$.

Teorema 3. *Sea* $[K:\mathbb{Q}]=n$, $\alpha\in K$. *Si* $f(x)=\ \mathrm{irr}\,(\alpha,\mathbb{Q},x)$, *entonces* $\mathrm{disc}\,\{1,\alpha,\ldots,\alpha^{n-1}\}=(-1)^{\frac{n(n-1)}{2}}\,\mathrm{N}_{K/\mathbb{Q}}\left(f'(\alpha)\right)$.

Demostración: Ver [7] página 29.■

Definición 6. Sea $K/\mathbb{Q}$ un campo numérico, $[K:\mathbb{Q}]=n$. Sea $\sigma:K\to\sigma(K)$ un monomorfismo de K en $\widetilde{K}$ la cerradura de Galois de $K/\mathbb{Q}$. Si $\sigma(K)\subseteq\mathbb{R}$, σ se llama **real** y si $\sigma(K)\subseteq\mathbb{C}$, $\sigma(K)\nsubseteq\mathbb{R}$, σ se llama **complejo**.

Si σ es complejo, entonces el **complejo conjugado** $\overline{\sigma}$ de σ, que se define por $\overline{\sigma}(x+iy)=\overline{\sigma(x+iy)}$ es otro monomorfismo y $\overline{\sigma}\neq\sigma$ (de hecho $\overline{\sigma}=\sigma$ si y sólo si σ es real), por lo tanto hay un número par de encajes complejos. Sean r_1 igual al número de encajes reales y $2r_2$ igual al número de encajes complejos. Entonces $[K:\mathbb{Q}]=n=r_1+2r_2$.

Teorema 4 (Kronecker). *Sea* $[K:\mathbb{Q}]=n=r_1+2r_2$. *Entonces el signo de* $\delta(K)\in\mathbb{Z}$ *es* $(-1)^{r_2}$.

Demostración: Ver [7] página 44.■

Definición 7. Un dominio entero A (esto es, un anillo conmutativo con uno y sin divisores de cero) se llama **dominio de Dedekind** si:

i) A es enteramente cerrado en $K = \operatorname{coc} A$.

ii) Todo ideal primo no cero $\wp$ de A es ideal maximal.

iii) A es noetheriano.

Teorema 5. *Si K es un campo númerico, ϑ_K es dominio de Dedekind.*

Demostración: Ver [7] página 131.■

Definición 8. Sea A un dominio de Dedekind, $K = \operatorname{coc} A$. Un A-módulo $M \subseteq K$ se llama **ideal fraccional o ideal fraccionario** de A si existe $a \in A$, $a \neq 0$ tal que $aM \subseteq A$ (luego aM es ideal y como A es noetheriano, aM es finitamente generado).

Definición 9. Un ideal $\mathfrak{A}$ de ϑ_K se llama **invertible** si existe $\mathfrak{B}$ ideal fraccionario tal que $\mathfrak{AB} = \vartheta_K$.

Corolario 1. *Todo ideal $\mathfrak{A} \neq 0$ de ϑ_K es invertible.*

Demostración: Como ϑ_K es dominio de Dedekind, tenemos $\mathfrak{A} = \wp_1 \cdots \wp_r$, lo cual implica $\wp_1^{-1} \cdots \wp_r^{-1}\mathfrak{A} = \vartheta_K$, y como $\wp_i^{-1}$ es ideal fraccionario, tenemos $\wp_1^{-1} \cdots \wp_r^{-1}$ es ideal fraccionario.■

Corolario 2. *El conjunto de ideales fraccionarios no cero de ϑ_K forman un grupo.*

Demostración: Ver [7] página 154.■

Corolario 3. *El grupo de ideales fraccionarios no cero de ϑ_K forman un grupo abeliano libre $\mathcal{D}_K$ con generadores $\{\wp | \wp$ es ideal primo de $\vartheta_K,\ \wp \neq 0\}$, es decir $\mathcal{D}_K \cong \bigoplus_{\substack{\wp \text{ primo} \\ \wp \neq 0}} \mathbb{Z}$.*

Demostración: Ver [7] página 154 o [11] página 174.■

Definición 10. Si $\alpha \in K^*$, $(\alpha) = \{k\alpha | k \in \vartheta_K\}$ se llama **ideal fraccionario principal o ideal principal**. Tenemos $(\alpha)^{-1} = (\alpha^{-1})$. Sea P_K el grupo de los ideales fraccionarios principales, esto es $P_K = \{(\alpha) | \alpha \in K^*\}$. El grupo cociente $\mathrm{Cl}\,(K) = \mathcal{D}_K/P_K$ es el **grupo de clases** de K. Y por último $h_K = |\mathrm{Cl}\,(K)|$ es el **número de clases** de K.

Observación: El número de clases de K es uno si y sólo si ϑ_K es dominio de ideales principales si y sólo si ϑ_K es dominio de factorización única.

Definición 11. A los ideales fraccionarios no cero se les llama **divisores** de K y a los ideales no cero de ϑ_K se les llama **ideales enteros o divisores enteros**.

Definición 12. Sea $\wp$ un ideal primo de ϑ_K, $\wp \neq 0$. Se define el **grado de inercia** de $\wp$ por $f_\wp = [\vartheta_K/\wp : \mathbb{F}_p]$, donde $\wp \cap \mathbb{Z} = (p)$; $f_\wp$ también recibe el nombre de **grado** del primo $\wp$.

Definición 13. Sea $p \in \mathbb{Z}$ primo racional y sea $p\vartheta_K = \wp_1^{e_1} \cdots \wp_h^{e_h}$, $e_i \geq 1$. Se define el **índice de ramificación** de $\wp_i$ sobre p como e_i.
El divisor primo $\wp_i$ se llama **ramificado** si $e_i > 1$ y **no ramificado** si $e_i = 1$.
El primo racional $p \in \mathbb{Z}$ se llama **ramificado** si algún $e_i > 1$.

Observación: Si $p\vartheta_K = \wp_1^{e_1} \cdots \wp_h^{e_h}$, entonces $f_i = f_{\wp_i} = [\vartheta_K/\wp_i : \mathbb{Z}/p\mathbb{Z}]$.

Definición 14. Sea $f(x) = x^n + \cdots + a_0 \in \mathbb{Z}[x]$. Entonces el **discriminante** de $f(x)$ es $\delta(f) = \prod_{1 \leq i < j \leq n} (\alpha^{(i)} - \alpha^{(j)})^2$, donde $\alpha^{(1)}, \ldots, \alpha^{(n)}$ son las raíces de $f(x)$.

Observación: Si $f(x)$ es irreducible y α es raíz de $f(x)$, entonces $\delta(f) = \prod_{i<j} (\alpha^{(i)} - \alpha^{(j)})^2 = \mathrm{disc}\,\{1, \alpha, \ldots, \alpha^{n-1}\} = (-1)^{\frac{n(n-1)}{2}}\, \mathrm{N}_{K/\mathbb{Q}}\,(f'(\alpha))$.

Teorema 6. *Sea L/K extensión de campos númericos y sea $\mathfrak{B} = \{\alpha \in L | \ \mathrm{Tr}_{L/K}(\alpha x) \in \vartheta_K \text{ para toda } x \in \vartheta_L\}$. Entonces $\mathfrak{B}$ es un ideal fraccionario de ϑ_L y $\mathfrak{B}^{-1} \subseteq \vartheta_L$. El divisor $\mathfrak{D}_{L/K} = \mathfrak{B}^{-1}$ se llama el* **diferente** *de L/K.*

Demostración: Ver [7] página 209.■

Definición 15. El divisor $\partial_{L/K} = \mathrm{N}_{L/K}(\mathfrak{D}_{L/K}) \in \mathcal{D}_K$ se llama el **discriminante** de L/K.

Teorema 7. *Para una extensión* L/K, $\mathfrak{D}_{L/K} = \langle f'_\theta(\theta) | f_\theta = \mathrm{irr}\,(\theta, K, x), \theta \in \vartheta_L, L = K(\theta)\rangle$

Demostración: Ver [7] página 215.■

1.2 Campos ciclotómicos

Entenderemos por un **campo ciclotómico** al campo $\mathbb{Q}(\zeta_n)$, $n \in \mathbb{N}$, donde ζ_n es cualquier raíz n-ésima primitiva de la unidad (por ejemplo $\zeta_n = e^{2\pi i/n}$). Se tiene que $\mathbb{Q}(\zeta_n)$ es el campo de descomposición de $x^n - 1 \in \mathbb{Z}[x] \subseteq \mathbb{Q}[x]$. Sea $\Phi_n(x) = \prod_{\substack{0 \le i \le n \\ (i,n)=1}} (x - \zeta_n^i)$, $\Phi_n(x)$ es el **polinomio ciclotómico**. Se tiene que gr $(\Phi_n(x))$ coincide con $\varphi(n)$, donde $\varphi(n)$ es la **función φ de Euler**, la cual se define como $\varphi(1) = 1$ y si $n > 1$ $\varphi(n) = |\{i | 1 \le i < n, (i,n) = 1\}|$. Veamos algunos resultados:

Proposición 2. $\sum_{d|n} \varphi(d) = n$.

Demostración: Sea C_n un grupo cíclico de n elementos. Sea

$$A_t = \{x \in C_n | o(x) = t\},$$

si $t \nmid n$, entonces $A_t = \emptyset$, pero si $t|n$, se sigue que $|A_t| = \varphi(t)$ (C_n tiene un único subgrupo de orden t). Si $t_1 \neq t_2$, tenemos $A_{t_1} \cap A_{t_2} = \emptyset$, luego $C_n = \bigcup_{t=1}^{n} A_t$ (unión disjunta), por lo tanto

$$n = |C_n| = \sum_{t=1}^{n} |A_t| = \sum_{t|n} \varphi(t).\blacksquare$$

Proposición 3. $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

Demostración: Tenemos que

$$x^n - 1 = \prod_{i=1}^{n}(x - \zeta_n^i).$$

Ahora, para toda d que divide a n se sigue que $\Phi_d(x)$ divide a $x^n - 1$ pues: $\Phi_d(x) = \prod_{(j,d)=1} (x - \zeta_d^j)$.
Sean $d_1 \neq d_2$ (d_1 y d_2 que dividen a n) y supongamos δ es raíz tanto de $\Phi_{d_1}(x)$ como de $\Phi_{d_2}(x)$. Se tiene: $\delta = \zeta_{d_1}^{i_1} = \zeta_{d_2}^{i_2}$, $(i_1, d_1) = 1 = (i_2, d_2)$, entonces $\delta = \zeta_{d_1 d_2}^{i_1 d_2} = \zeta_{d_1 d_2}^{d_1 i_2}$ (pues $\zeta_d^j = \zeta_{d\frac{n}{d}}^{j\frac{n}{d}} = \zeta_n^{\frac{jn}{d}}$), lo que implica $i_1 d_2 = d_1 i_2$, y de $(i_1, d_1) = 1$ se tiene que i_1 divide a i_2 y recíprocamente i_2 divide a i_1, por lo tanto $i_2 = i_1$ y $d_1 = d_2$, lo cual no puede ser, por lo que $\Phi_{d_1}(x)$ y $\Phi_{d_2}(x)$ son primos relativos, y luego $\prod_{d|n} \Phi_d(x)$ divide a $x^n - 1$ y además ambos polinomios son mónicos.
Finalmente:

$$\text{gr}\left(\prod_{d|n} \Phi_d(x)\right) = \sum_{d|n} \varphi(d) = n$$

donde la última igualdad se tiene por la Proposición 2, por lo tanto

$$x^n - 1 = \prod_{d|n} \Phi_d(x). \blacksquare$$

Corolario 4. $\Phi_n(x) \in \mathbb{Z}[x]$.

Demostración: Por inducción:
Para $n = 1$, se tiene $\Phi_1(x) = x - 1 \in \mathbb{Z}[x]$.
Para $n > 1$, suponemos $\Phi_d(x) \in \mathbb{Z}[x]$ para $1 \leq d < n$,

$$x^n - 1 = \left(\prod_{\substack{d|n \\ d\neq n}} \Phi_d(x)\right) \Phi_n(x)$$

implica que $\Phi_n(x) \in \mathbb{Q}[x]$, pues tanto $x^n - 1$ como $\prod_{\substack{d|n \\ d\neq n}} \Phi_d(x)$ se encuentran en $\mathbb{Z}[x]$. Por el Lema de Gauss (ver [1]), se sigue que $\Phi_n(x) \in \mathbb{Z}[x]$. $\blacksquare$

Proposición 4. *Si* $(n,m)=1$, *entonces* $\mathbb{Q}(\zeta_n,\zeta_m)=\mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m)=\mathbb{Q}(\zeta_{nm})$.

Demostración: Tenemos $\zeta_n=\zeta_{nm}^m\in\mathbb{Q}(\zeta_{nm})$, análogamente $\zeta_m\in\mathbb{Q}(\zeta_{nm})$. Puesto que $(n,m)=1$, existen $x,\ y\in\mathbb{Z}$ de tal manera que $1=mx+ny$, luego $\zeta_{nm}=\zeta_{nm}^1=\zeta_{nm}^{mx+ny}=\zeta_{nm}^{mx}\zeta_{nm}^{ny}=\zeta_n^x\zeta_m^y\in\mathbb{Q}(\zeta_n,\zeta_m)$, por lo tanto

$$\mathbb{Q}(\zeta_n,\zeta_m)=\mathbb{Q}(\zeta_{nm}).\blacksquare$$

En la literatura (por ejemplo en [1] página 577) podemos encontrar resultados tales como, $\Phi_n(x)$ es irreducible, $[\mathbb{Q}(\zeta_n):\mathbb{Q}]=\varphi(n)$, si $(n,m)=1$ entonces $\mathbb{Q}(\zeta_n)\cap\mathbb{Q}(\zeta_m)=\mathbb{Q}$. Como consecuencia se tiene que $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ es de Galois con grupo $U_n=(\mathbb{Z}/n\mathbb{Z})^*$ e irr $(\zeta_n,x,\mathbb{Q})=\Phi_n(x)$.
Presentaremos a continuación la Fórmula de Inversión de Möbius.
Sea $\mu:\mathbb{N}\to k$, donde k es cualquier campo y μ está dada por

$$\mu(n)=\begin{cases}1 & \text{si} & n=1,\\ (-1)^r & \text{si} & n=p_1\cdots p_r,\\ & & p_i \text{ primos}\\ & & \text{distintos},\\ 0 & \text{en otro caso.} & \end{cases}$$

Se tiene $\displaystyle\sum_{d|n}\mu(d)=\epsilon(n)=\begin{cases}1 & \text{si} & n=1\\ 0 & \text{en otro caso.} & \end{cases}$

Proposición 5 (Fórmula de Inversión de Möbius). *Si* $f,g:\mathbb{N}\to k$, *con* k *cualquier campo y* $f(n)=\displaystyle\prod_{d|n}g(d)$, *entonces* $g(n)=\displaystyle\prod_{d|n}f(d)^{\mu(n/d)}$.

Demostración: Ver [7] página 88.$\blacksquare$

En particular, sean $f,g:\mathbb{N}\to\mathbb{Q}(x)$, $f(n)=x^n-1$, $g(d)=\Phi_d(x)$. Se tiene: $x^n-1=\displaystyle\prod_{d|n}\Phi_d(x)$, es decir $f(n)=\displaystyle\prod_{d|n}g(d)$, luego $g(n)=\displaystyle\prod_{d|n}f(d)^{\mu(n/d)}$, entonces $\Phi_n(x)=\displaystyle\prod_{d|n}(x^d-1)^{\mu(n/d)}$.

Nota: Si n es impar, $\mathbb{Q}(\zeta_{2n})=\mathbb{Q}(\zeta_n)$. Cuando consideremos $\mathbb{Q}(\zeta_m)$ supondremos $m\not\equiv 2 \bmod 4$. Tenemos $|U_n|=\varphi(n)$. Sean p un primo y $\alpha\geq 1$. Entonces

$$U_{p^\alpha}\cong\begin{cases}\mathbb{Z}/p^{\alpha-1}\mathbb{Z}\times\mathbb{Z}/(p-1)\mathbb{Z} & p>2\\ 1 & p=2,\alpha=1\\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2^{\alpha-2}\mathbb{Z} & p=2,\alpha\geq 2.\end{cases}$$

Si $(n,m)=1$, entonces $U_{nm}\cong U_n\times U_m$ y si $n=2^m p_1^{\alpha_1}\cdots p_r^{\alpha_r}$, entonces $U_n\cong U_{2^m}\times\prod_{i=1}^{r}U_{p_i^{\alpha_i}}=(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2^{m-2}\mathbb{Z})\times\prod_{i=1}^{r}\left(\mathbb{Z}/p_i^{\alpha_i-1}\mathbb{Z}\times\mathbb{Z}/(p_i-1)\mathbb{Z}\right)$.
Por lo tanto U_n es cíclico si y sólo si $n=2,4,p^\alpha,2p^\alpha$ $(p>2,\ \alpha\geq 1)$.
Mencionamos algunos resultados importantes: si K es un campo numérico $[K:\mathbb{Q}]=r_1+2r_2$, $\text{signo}(\delta(K))=(-1)^{r_2}$, $\delta(\mathbb{Q}(\zeta_n))=(-1)^{\varphi(n)/2}\dfrac{n^{\varphi(n)}}{\prod_{p|n}p^{\varphi(n)/(p-1)}}$.

Nota: Obtenemos el signo de $\delta(\mathbb{Q}(\zeta_p))$, para p un primo impar: $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ es de Galois y $\mathbb{Q}(\zeta_p)\not\subseteq\mathbb{R}$, luego $r_1=0$, $2r_2=[\mathbb{Q}(\zeta_p):\mathbb{Q}]=p-1$, $r_2=\dfrac{p-1}{2}$, por lo tanto $\operatorname{sgn}\delta(\mathbb{Q}(\zeta_p))=(-1)^{r_2}=(-1)^{\frac{p-1}{2}}$.

Nota: Sean K,E dos campos numéricos y supongamos que $(\delta(E),\delta(K))=1$ y que K y E son linealmente disjuntos sobre $\mathbb{Q}$ (esto es si $\{w_1,\ldots,w_n\}$ es base de $K/\mathbb{Q}$ y $\{v_1,\ldots,v_n\}$ es base de E sobre $\mathbb{Q}$, entonces $\{w_iv_j\}_{1\leq i\leq n}^{1\leq j\leq m}$ es base de $KE/\mathbb{Q}$). Entonces $\vartheta_{KE}=\vartheta_K\vartheta_E$ y $\delta(KE)=\delta(K)^{[E:\mathbb{Q}]}\delta(E)^{[K:\mathbb{Q}]}$.
También tenemos lo siguiente: sean $p\in\mathbb{Z}$ primo, $n\not\equiv 2 \bmod 4$, entonces p se ramifica en $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ si y sólo si $p|n$. Es decir, p es ramificado si y sólo si $p|n$ si y sólo si $p|\delta(K)$. Si $p\nmid n$, $e=1$, $f=o(p \bmod n)$, $g=\dfrac{\varphi(n)}{f}$. Si $p|n$, $p^a||n$ (esto es, $p^a|n$ y $p^{a+1}\nmid n$), $e=\varphi(p^a)$, $f=o(p \bmod \dfrac{\varphi(n)}{p^a})$, $g=\dfrac{\varphi(n/p^a)}{f}$.
En particular, p se descompone totalmente en $K/\mathbb{Q}$ si y sólo si $p\equiv 1 \bmod n$.
Sea $K=\mathbb{Q}(\zeta_n)$. Entonces $K^+=\mathbb{Q}(\zeta_n)\cap\mathbb{R}$ es el **subcampo real** de $\mathbb{Q}(\zeta_n)$, $[\mathbb{Q}(\zeta_n):\mathbb{Q}(\zeta_n)^+]=2$, $\mathbb{Q}(\zeta_n)^+=\mathbb{Q}(\zeta_n+\zeta_n^{-1})$. Se prueba $\vartheta_{K^+}=\mathbb{Z}[\zeta_n+\zeta_n^{-1}]$.
De lo más importante es el siguiente:

Teorema 8. *$\mathbb{Z}[\zeta_n]$ es el anillo de enteros de $\mathbb{Q}(\zeta_n)$.*

Demostración: Ver [7] página 83.■

Proposición 6. *Todo campo cuadrático está contenido en un ciclotómico.*

Demostración: Sea p primo. Si $p=2$, consideremos $\mathbb{Q}(\zeta_8)=\mathbb{Q}(\sqrt{2},i)=\mathbb{Q}(\sqrt{2},\sqrt{-2})$, luego $\sqrt{2},\sqrt{-2}\in\mathbb{Q}(\zeta_8)$, $i=\sqrt{-1}\in\mathbb{Q}(\zeta_8)$, donde $\zeta_8=e^{\frac{2\pi i}{8}}=e^{\frac{\pi i}{4}}=\dfrac{1+i}{\sqrt{2}}$, lo cual implica $\mathbb{Q}(\sqrt{2}),\mathbb{Q}(\sqrt{-2}),\mathbb{Q}(i)\subseteq\mathbb{Q}(\zeta_8)$. Sea p impar y

sea $K = \mathbb{Q}(\zeta_p)$, se tiene: $(-1)^{\frac{p-1}{2}} p^{p-2} = \delta(K) = \prod_{1\leq i<j\leq p-1} (\zeta_p^i - \zeta_p^j)^2$, luego $(-1)^{\frac{p-1}{4}} p^{\frac{p-3}{2}} \sqrt{p} = \pm \prod_{1\leq i<j\leq p-1} (\zeta_p^i - \zeta_p^j) \in \mathbb{Q}(\zeta_p)$, entonces $(-1)^{\frac{p-1}{4}} \sqrt{p} \in \mathbb{Q}(\zeta_p)$.
Si $p \equiv 1 \bmod 4$ entonces $\sqrt{p} \in \mathbb{Q}(\zeta_p)$, $\sqrt{-p} = \sqrt{-1}\sqrt{p} \in \mathbb{Q}(\zeta_4, \zeta_p) = \mathbb{Q}(\zeta_{4p})$ y si $p \equiv 3 \bmod 4$, entonces $\sqrt{-p} \in \mathbb{Q}(\zeta_p)$ y $\sqrt{p} \in \mathbb{Q}(\zeta_{4p})$, por lo tanto en cualquier caso $\sqrt{\pm p} \in \mathbb{Q}(\zeta_{4p})$. Ahora, si $d = \pm p_1 \cdots p_r$, entonces $\sqrt{d} = \sqrt{\pm 1}\sqrt{p_1} \cdots \sqrt{p_r} \in \mathbb{Q}(\zeta_8, \zeta_{p_1}, \ldots, \zeta_{p_r}) = \mathbb{Q}(\zeta_{8p_1 \cdots p_r})$. ■

Nota: Sea $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, $p_1 = 2$, de manera que $\alpha_1 = 0$ ó $\alpha_1 \geq 2$. Entonces $\dfrac{\varphi(n)}{2} = \dfrac{1}{2}\, p_1^{\alpha_1 - 1} \cdots p_r^{\alpha_r - 1}(p_1 - 1) \cdots (p_r - 1)$.
Si en la factorización de n hay al menos un primo $p \equiv 1 \bmod 4$, entonces $\dfrac{\varphi(n)}{2}$ es par.
Si en la factorización de n hay al menos dos primos impares $p \equiv 1 \bmod 2$, entonces $\dfrac{\varphi(n)}{2}$ es par.

Teorema 9 (Kronecker-Weber). *Toda extensión abeliana de $\mathbb{Q}$ está contenida en algún $\mathbb{Q}(\zeta_n)$. En particular se tiene que si $\mathbb{Q}_{ab}$ es la máxima extensión abeliana de $\mathbb{Q}$, entonces $\mathbb{Q}_{ab} = \mathbb{Q}(\zeta_\infty) = \bigcup_{n=1}^{\infty} \mathbb{Q}(\zeta_n)$.*

Demostración: Ver [7] página 256.■

En particular:

$$G = \mathrm{Gal}\,(\mathbb{Q}_{ab}/\mathbb{Q}) = \mathrm{Gal}\,(\mathbb{Q}(\zeta_\infty)/\mathbb{Q}) = \mathrm{Gal}\left(\bigcup_{n=1}^{\infty} \mathbb{Q}(\zeta_n)/\mathbb{Q}\right) =$$

$$= \lim_{\leftarrow} \mathrm{Gal}\,(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \lim_{\leftarrow} U_n.$$

Donde, como $U_n \cong \prod_p U_{p^{\alpha(p)}}$, tenemos

$$\lim_{\leftarrow} U_n = \prod_{p \text{ primo}} \lim_{\leftarrow} U_{p^\alpha}.$$

Luego, de la nota que sigue a la Proposición 5 y de que $\lim_{\leftarrow} C_{p^m} \cong \mathbb{Z}_p$ el anillo de los enteros p-ádicos, se sigue que

$$G = \mathrm{Gal}\,(\mathbb{Q}_{ab}/\mathbb{Q}) \cong (C_2 \times \mathbb{Z}_2) \times \prod_{p>2}(C_{p-1} \times \mathbb{Z}_p) = (C_2 \times \prod_{p>2} C_{p-1}) \times \widehat{\mathbb{Z}},$$

donde $\widehat{\mathbb{Z}} = \prod_{p\,\text{primo}} \mathbb{Z}_p$, el cual se conoce como el **anillo de Prüfer**.

Capítulo 2

Campos de funciones ciclotómicos

Se presenta en este capítulo la teoría de campos de funciones ciclotómicos sobre un campo de funciones racionales con campo de constantes finito. Los resultados son análogos a los del capítulo anterior.

2.1 Campos de funciones ciclotómicos

Sea $\mathbb{F}_q$ el campo finito de q elementos, $q = p^r$, p primo. Sea k el campo de funciones racionales sobre $\mathbb{F}_q$, $k = \mathbb{F}_q(T)$ y sea $R_T = \mathbb{F}_q[T]$. Aquí k "juega" el papel de $\mathbb{Q}$ y R_T el papel de $\mathbb{Z}$ con la diferencia de que hay varios anillos que corresponden a $\mathbb{Z}$ ($k = \mathbb{F}_q\left(\dfrac{aT+b}{cT+d}\right)$, $a, b, c, d \in \mathbb{F}_q$, $ad - bc \neq 0$ y si $T' = \dfrac{aT+b}{cT+d}$, $R_{T'} = \mathbb{F}_q[T']$ será otro "$\mathbb{Z}$"). Sea $n \in \mathbb{N}$. Entonces $\mathbb{F}_q(T^{1/n})$, $\mathbb{F}_q(T^n)$ son campos de funciones racionales y si $n > 1$,

$$\mathbb{F}_q(T^n) \subsetneqq \mathbb{F}_q(T) \subsetneqq \mathbb{F}_q(T^{1/n}).$$

De hecho

$$[\mathbb{F}_q(T) : \mathbb{F}_q(T^n)] = \left[\mathbb{F}_q(T^{1/n}) : \mathbb{F}_q(T)\right] = n.$$

En contraste, para $\mathbb{Q}$ se tiene que $A \subseteq \mathbb{Q}$, con A campo implica que A es igual a $\mathbb{Q}$ y si $\mathbb{Q} \subsetneqq B$ entonces $\mathbb{Q} \not\supseteq B$.

Sea k^{ac} una cerradura algebraica de k. Sea $\mathcal{A} = \mathrm{End}_{\mathbb{F}_q}(k^{ac})$. $\mathcal{A} = \{\rho : k^{ac} \to k^{ac} \mid \rho(a+b) = \rho(a) + \rho(b),\ \rho(\alpha a) = \alpha\rho(a)$ para toda $\alpha \in \mathbb{F}_q$ y para toda $a, b \in k^{ac}\}$. Es decir, $\mathcal{A}$ es la $\mathbb{F}_q$-álgebra ($\mathbb{F}_q$-módulo + anillo) de los $\mathbb{F}_q$-endomorfismos del grupo aditivo de k^{ac}. Vamos a considerar dos elementos de $\mathcal{A}$:

1. Sea φ el automorfismo de Fröbenius de k^{ac} sobre $\mathbb{F}_q$, es decir

$$\varphi : k^{ac} \to k^{ac}$$

donde $\varphi(u) = u^q$.

2. Sea μ_T la multiplicación por T, $\mu_T : k^{ac} \to k^{ac}$ donde $\mu_T(u) = Tu$.

Ahora, si $f(T) \in R_T = \mathbb{F}_q[T]$ la sustitución $T \mapsto \varphi + \mu_T$ en $f(T)$ nos da un elemento en $\mathcal{A}$, esto es: si $f(T) = a_n T^n + \cdots + a_1 T + a_0$, entonces $f(\varphi+\mu_T) : k^{ac} \to k^{ac}$, $f(\varphi+\mu_T)(u) = a_n(\varphi+\mu_T)^n(u) + \cdots + a_1(\varphi+\mu_T)(u) + a_0 u$, pues $(\varphi+\mu_T)^0 = \mathrm{id}_{k^{ac}}$, $(\varphi+\mu_T)^0(u) = u$. Por tanto obtenemos un homomorfismo de anillos $\xi : R_T \to \mathcal{A}$, $\xi(T) = \varphi + \mu_T$, $\xi(f(T)) = f(\varphi+\mu_T)$. Así pues k^{ac} obtiene una estructura de R_T-módulo de la manera siguiente: si $u \in k^{ac}$, $M \in R_T$, ponemos: $M \circ u = \xi(M)(u) = M(\varphi+\mu_T)(u)$, también usamos la notación

$$u^M := M(\varphi+\mu_T)(u).$$

Notemos: Si $M, N \in R_T$, entonces $u^{N+M} = u^N + u^M$ y $u^{NM} = (u^N)^M$. Si $\alpha \in \mathbb{F}_q$, $u \in k^{ac}$, $u^\alpha = \alpha(\varphi+\mu_T)^0(u) = \alpha(u) = \alpha u$, por lo tanto la estructura de R_T-módulo respeta la estructura de $\mathbb{F}_q$-álgebra de k^{ac}.

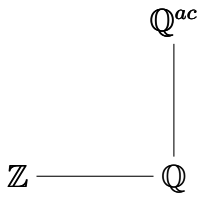
Nota: Observamos $(\varphi \circ \mu_T)(u) = \varphi(Tu) = T^q u^q$, mientras que $(\mu_T \circ \varphi)(u) = \mu_T(u^q) = Tu^q$ y $(\mu_T^q \circ \varphi)(u) = T^q u^q$, luego $\varphi \circ \mu_T = \mu_T^q \circ \varphi$. En particular $\varphi \circ \mu_T \neq \mu_T \circ \varphi$.

Proposición 7. *Si* $M = a_d T^d + \cdots + a_1 T + a_0 \in R_T$, $a_d \neq 0$, *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:* $\begin{bmatrix} M \\ 0 \end{bmatrix} = M$, $\begin{bmatrix} M \\ d \end{bmatrix} = a_d$.

Demostración: Ver [4] página 3.■

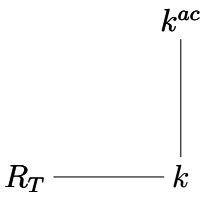
Nota: La acción, aunque técnicamente más complicada, es la correspondiente a la exponenciación en $(\mathbb{Q}^{ac})^*$. Más precisamente:

En el caso de campos numéricos,



$\mathbb{Z}$ actúa en $(\mathbb{Q}^{ac})^* = \mathbb{Q}^{ac}\backslash\{0\}$ por: $n \in \mathbb{Z}$, $u \in (\mathbb{Q}^{ac})^*$, $n \circ u = u^n$. Los campos ciclotómicos corresponden a: $\{u \in (\mathbb{Q}^{ac})^* | u^n = 1\} = \{\zeta_n^a\}_{a=0}^{n-1}$.

En nuestro caso,



R_T actúa en k^{ac} por "exponenciación": $M \in R_T$, $u \in k^{ac}$, $M \circ u = u^M$ los campos de funciones ciclotómicos corresponden a: $\{u \in k^{ac} | u^M = 0\}$.

Definición 16. Sea Λ_M el conjunto de elementos de k^{ac} que corresponden a la M-torsión de k^{ac}. Esto es $\Lambda_M = \{u \in k^{ac} | u^M = 0\}$ el conjunto de ceros del polinomio u^M en la variable u.

Puesto que R_T es conmutativo, si $u \in \Lambda_M$ y $N \in R_T$, entonces $N \circ u = u^N \in \Lambda_M$, en efecto: $M \circ u^N = (u^N)^M = u^{NM} = u^{MN} = (u^M)^N = 0^N = 0$, por lo tanto Λ_M es un R_T-submódulo de k^{ac}.

Nota: Si $\alpha \in \mathbb{F}_q \setminus \{0\}$, $\Lambda_M = \Lambda_{\alpha M}$, pues: $u^{\alpha M} = (u^M)^\alpha = \alpha(u^M) = 0$ si y sólo si $u^M = 0$.

Proposición 8. *Como polinomio en u sobre k, u^M es separable de grado q^d, $d = \text{gr}_T\ M$. Por tanto Λ_M es finito con q^d elementos y es por tanto un espacio vectorial de dimensión d sobre $\mathbb{F}_q$.*

Demostración: Sabemos $u^M = \sum_{i=0}^{d} \begin{bmatrix} M \\ i \end{bmatrix} u^{q^i}$. Derivando con respecto a u tenemos $(u^M)' = \begin{bmatrix} M \\ 0 \end{bmatrix} = M \neq 0$. Por tanto u^M es separable de grado q^d. Luego $|\Lambda_M| = \mathrm{gr}_u u^M = q^d$ y Λ_M es $\mathbb{F}_q$-módulo, luego $\dim_{\mathbb{F}_q} \Lambda_M = d$.■

Nota: Sabemos que en $\mathbb{Q}$: $W_n = \{\xi \in (\mathbb{Q}^{ac})^* | \xi^n = 1\} \cong \prod_{i=1}^{h} W_{p_i^{\alpha_i}}$ donde $n = p_1^{\alpha_1} \cdots p_h^{\alpha_h}$, $W_n = \mathbb{Z}/n\mathbb{Z}$ es $\mathbb{Z}$-cíclico. Esperamos obtener en k:

$$\Lambda_M = \{u \in k^{ac} | u^M = 0\} \cong \prod_{i=1}^{h} \Lambda_{P_i^{\alpha_i}}$$

donde $M = \prod_{i=1}^{h} P_i^{\alpha_i}$, con $P_1, \ldots, P_h$ polinomios irreducibles, Λ_M es R_T-cíclico.

Proposición 9. *Si* $M = \prod_{i=1}^{h} P_i^{\alpha_i}$, *entonces* $\Lambda_M \cong \bigoplus_{i=1}^{h} \Lambda_{P_i^{\alpha_i}}$ *como* R_T*-módulo.*

Demostración: Como Λ_M es un R_T-módulo y R_T es un dominio de ideales principales (D.I.P.), todo módulo de torsión A se descompone como: $A = \bigoplus_P A(P)$ donde $A(P)$ es la unión de las P^n-torsiones, variando $n \in \mathbb{N}$ y P recorre los elementos primos de R_T. Lo aplicamos para $A = \Lambda_M$

$$A(P) = \begin{cases} 0 & \text{si} \quad P \notin \{P_1, \ldots, P_h\} \\ \Lambda_{P_i^{\alpha_i}} & \text{si} \quad P = P_i \end{cases}$$

por lo tanto $\Lambda_M \cong \bigoplus_{i=1}^{h} \Lambda_{P_i^{\alpha_i}}$.■

Proposición 10. *Si* $M = P^n$, P *irreducible, entonces* Λ_M *es un* R_T*-módulo cíclico.*

Demostración: Por inducción sobre n. Para $n = 1$, sean $\xi \in \Lambda_P$, $\xi \neq 0$ y

$$\Psi : R_T \to \Lambda_P,$$

con $\Psi(N) = \xi^N$. Entonces $\Psi \neq 0$ pues $\Psi(1) = \xi^1 = \xi \neq 0$. Además $\Psi(P) = \xi^P = 0$, por lo que $P \in \ker \Psi$, luego $(P) \subseteq \ker \Psi$, como R_T es dominio de ideales principales y P es irreducible, $P \neq 0$, (P) es maximal, por lo tanto $P \subseteq \ker \Psi \subsetneq R_T$, luego $(P) = \ker \Psi$. Por lo tanto

$$R_T/(P) = R_T/\ker \Psi \cong \Psi(R_T).$$

Por otro lado $|\Psi(R_T)| = |R_T/(P)| = q^d = |\Lambda_P|$, entonces

$$\Psi(R_T) = \Lambda_P$$

y $\Lambda_P \cong R_T/(P)$. Ahora, para toda S, $R_T/(S)$ es R_T-cíclico pues 1 genera a $R_T/(S)$, por lo tanto Λ_P es cíclico.

Ahora supongamos cierto el resultado para $n \geq 1$, sea $\theta : \Lambda_{P^{n+1}} \to \Lambda_{P^n}$, con $u \mapsto u^P$. Entonces θ es un R_T-homomorfismo y $\ker \theta = \Lambda_P$. Por lo tanto

$$\Lambda_{P^{n+1}}/\Lambda_P \cong \theta(\Lambda_{P^{n+1}}) \text{ y } |\Lambda_{P^{n+1}}/\Lambda_P| = \frac{q^{d(n+1)}}{q^d} = q^{dn} = |\Lambda_{P^n}|,$$

luego θ es sobre y $\Lambda_{P^{n+1}}/\Lambda_P \cong \Lambda_{P^n}$. Sea $\lambda \in \Lambda_{P^{n+1}}$ tal que $\lambda^P = \theta(\lambda)$ genera a Λ_{P^n}. Probaremos que λ genera a $\Lambda_{P^{n+1}}$. Sea $\mu \in \Lambda_{P^{n+1}}$ y $\theta(\mu) = \mu^P = (\theta(\lambda))^A = \lambda^{PA}$, $A \in R_T$, $\mu^P - \lambda^{PA} = 0$ entonces $\mu - \lambda^A \in \Lambda_P = \ker \theta$. Ahora, $\lambda^{P^n} \in \Lambda_P$, pero $\lambda^{P^n} \neq 0$ pues λ^P genera a Λ_{P^n} y $0 \neq (\lambda^P)^{P^{n-1}} = \lambda^{P^n}$. Finalmente, Λ_P es un espacio 1-dimensional sobre $R_T/(P)$, $\lambda^{P^n} \neq 0$, por lo tanto existe $B \in R_T$ tal que $\mu - \lambda^A = (\lambda^{P^n})^B$ lo cual implica que

$$\mu = \lambda^{A+BP^n} \in \langle \lambda \rangle$$

por lo que λ genera a $\Lambda_{P^{n+1}}$ como R_T-módulo.■

Teorema 10. *Para $M \in R_T$, $\Lambda_M \cong R_T/(M)$ como R_T-módulo. En particular, Λ_M es R_T-cíclico.*

Demostración: Se tiene que

$$\Lambda_M \cong \bigoplus_{i=1}^{h} \Lambda_{P_i^{\alpha_i}},$$

donde $M = \prod_{i=1}^{h} P_i^{\alpha_i}$. Cada $\Lambda_{P_i^{\alpha_i}}$ es R_T-cíclico y además $\Lambda_{P_i^{\alpha_i}}$ es la P_i-componente primaria de Λ_M por lo tanto Λ_M es cíclico (de hecho, si λ_i es generador

de $\Lambda_{P_i^{\alpha_i}}$, $\lambda = \lambda_1 + \cdots + \lambda_h$ es generador de Λ_M). Ahora, sea λ un generador de Λ_M. Si

$$\theta : R_T \to \Lambda_M,$$

donde $\theta(A) = \lambda^A$, entonces θ es un epimorfismo y $\Lambda_M \cong R_T/(\ker\theta)$,

$$\ker\theta = \text{ ann }(\lambda) = \{A \in R_T | \lambda^A = 0\} = \text{ann}(\Lambda_M).$$

Observamos $M \in \ker\theta$ pues $\lambda^M = 0$, luego $(M) \subseteq \ker\theta$. Por otro lado $|R_T/(M)| = q^d$, $d = \text{ gr } M$, $|\Lambda_M| = q^d$ implica $\ker\theta = M$ y $R_T/(M) \cong \Lambda_M$.■

Definición 17. Para $M \in R_T$, $M \neq 0$ se define $\Phi(M) = |(R_T/(M))^*|$.

Proposición 11. *Si N, M son primos relativos, entonces $(R_T/(MN))^* \cong (R_T/(M))^* \times (R_T/(N))^*$*

Demostración: Como M y N son primos relativos tenemos a nivel de ideales que $(MN) = (M)(N) = (M)\cap(N)$. Luego por el Teorema Chino del Residuo $R_T/(M)\times R_T/(N) \cong R_T/(M)\cap(N) = R_T/(MN)$, por lo tanto $R_T/(MN) \cong R_T/(M) \times R_T/(N)$. De donde $(R_T/(MN))^* \cong (R_T/(M))^* \times (R_T/(N))^*$.■

Obsérvese que $\Phi(M)$ es la cardinalidad del grupo de unidades de $R_T/(M)$, $\Phi(M) = |\{N \in R_T | (M,N) = 1, \text{ gr } N < \text{ gr } M\}|$, Φ es como la función φ de Euler, cumple con

Proposición 12. *i) Si $(M,N) = 1$, entonces $\Phi(MN) = \Phi(M)\Phi(N)$.*

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

iii) Si P es irreducible, $\Phi(P^n) = |R_T/(P^{n-1})|\Phi(P) = q^{dn} - q^{d(n-1)}$.

Demostración: Probemos *i*). Tenemos que $(R_T/(MN))^* \cong (R_T/(M))^* \times (R_T/(N))^*$, que se sigue de la proposición anterior. Tomando cardinalidad tenemos $|(R_T/(M))^*||(R_T/(N))^*| = |(R_T/(MN))^*|$, por lo tanto $\Phi(MN) = \Phi(M)\Phi(N)$. Para ver *ii*), nos fijamos en $R_T/(P) = \mathbb{F}_q[T]/\langle P(T)\rangle \cong \mathbb{F}_q(\alpha)$ donde α es raíz de $P(T)$ el cual es un polinomio irreducible. Tenemos que $|\mathbb{F}_q(\alpha)| = q^d$, donde d es el grado del polinomio, luego $|R_T/(P)| = q^d$. Por otro lado, sabemos que para $M \in R_T\backslash\{0\}$ se tiene $\Phi(M) = |(R_T/(M))^*|$ y sabemos que $(R_T/(P))^* = (R_T/(P))\backslash\{0\}$ (pues $R_T/(P)$ es campo), lo que implica $\Phi(P) = |(R_T/(P))^*| = q^d - 1$. Por último probaremos *iii*), definimos

$\psi : (R_T/(P^n))^* \to (R_T/(P))^*$ dado por $f(T)+(P^n) \mapsto f(T)+(P)$. Tenemos que ψ está bien definido, ψ es un homomorfismo, ψ es suprayectivo. Entonces $\ker \psi = \{f(T)+(P^n) | f(T)-1 \in (P)\}$ $=\{f(T)+(P^n) | f(T)-1 = P(T)g(T),\ g(T) \in R_T\} = \{f(T)+(P^n) | f(T) = 1+P(T)g(T),\ g(T) \in R_T\} = \{1+P(T)g(T)+(P^n) | g(T) \in R_T\}$. Además, por el Primer Teorema de Isomorfismos, tenemos $(R_T/(P^n))^*/\ker \psi \cong (R_T/(P))^*$. Ahora, para ver cuántos elementos tiene $\ker \psi$ nos fijamos en $1+Pg+(P^n) = 1+Pg_1+(P^n)$ si y sólo si $P(g-g_1) \in (P^n)$ si y sólo si $P(g-g_1) = P^n l$ si y sólo si $g-g_1 = P^{n-1}l$ si y sólo si $g+(P^{n-1}) = g_1+(P^{n-1})$, por lo tanto $|\ker\psi| = |R_T/(P^{n-1})| = q^{d(n-1)}$. Luego $\dfrac{|(R_T/(P^n))^*|}{|R_T/(P^{n-1})|} = |(R_T/(P^n))^*/\ker\psi| = |(R_T/(P))^*| = \Phi(P)$, lo que implica $|(R_T/(P^n))^*| = |R_T/(P^{n-1})|\Phi(P)$, entonces $\Phi(P^n) = |R_T/(P^{n-1})|\Phi(P) = q^{d(n-1)}(q^d-1) = \dfrac{q^{dn}}{q^d}(q^d-1) = q^{dn} - q^{d(n-1)}$. ■

Proposición 13. *El R_T-módulo cíclico Λ_M tiene exactamente $\Phi(M)$ generadores. De hecho, si λ es cualquier generador y $A \in R_T$, entonces λ^A es generador si y sólo si $(A, M) = 1$.*

Demostración: Se tiene: $\Lambda_M \cong R_T/(M)$. Sea λ un generador. Si $(A, M) = 1$, sea $\xi \in \Lambda_M$. Se tiene $\xi = \lambda^B$, $B \in R_T$. Existen $S,\ U \in R_T$ tal que $1 = SA + UM$, luego $B = BSA + BUM$, $\xi = \lambda^B = \lambda^{BSA+BUM} = \lambda^{BSA} + \lambda^{BUM} = (\lambda^A)^{BS} + (\lambda^M)^{BU} = (\lambda^A)^{BS}$ por lo tanto λ^A es generador. Recíprocamente, si λ^A es generador, entonces existe $B \in R_T$ tal que $(\lambda^A)^B = \lambda$ implica $\lambda^{AB-1} = 0$. Pero λ es generador de Λ_M y ann $(\Lambda_M) = (M)$, lo que implica $M|AB-1$, entonces $AB \equiv 1 \bmod M$, por lo tanto $(A, M) = 1$.■

Definición 18. El polo de T, P_∞, será de ahora en adelante el "primo infinito" $(T)_k = \dfrac{P_0}{P_\infty}$.

Definición 19. Sea $M \in R_T \backslash \{0\}$. Al campo $k(\Lambda_M)$, que es el campo generado sobre $k = \mathbb{F}_q(T)$ al adjuntarle $\Lambda_M = \{u \in k^{ac} | u^M = 0\}$, se le llamará el **campo de funciones ciclotómico determinado por M sobre k.**

Nota: Puesto que $\Lambda_M \cong R_T/(M)$ es R_T-cíclico, digamos generado por $\lambda_M = \lambda$:

$$\Lambda_M = \lambda^{R_T} = \{\lambda^A | A \in R_T\},$$

tenemos

$$k(\Lambda_M) = k(\lambda).$$

En efecto, si $\xi \in \Lambda_M$, entonces $\xi = \lambda^A$ para algún $A \in R_T$, luego

$$\xi = A(\mu_T + \varphi)(\lambda) \in k(\lambda^q, \{T^s\lambda\}) = k(\lambda).$$

Ahora bien, como $k(\Lambda_M)$ es el campo de descomposición del polinomio separable $F(u) = u^M \in k[u]$, se sigue que $k(\Lambda_M)/k$ es Galois. Más aún, si

$$M(T) = a_d T^d + \cdots + a_1 T + a_0,$$

$$u^M = \left[\begin{array}{c} M \\ d \end{array} \right] u^{q^d} + \left[\begin{array}{c} M \\ d-1 \end{array} \right] u^{q^{d-1}} + \cdots + \left[\begin{array}{c} M \\ 1 \end{array} \right] u^q + Mu \in R_T[u],$$

por lo tanto los elementos de Λ_M son enteros sobre R_T (notemos que $\Lambda_M = \Lambda_{a_d^{-1}M}$ y que $a_d^{-1}M$ es mónico). Sea $G_M = \text{Gal}\,(k(\Lambda_M)/k)$.

Proposición 14. *La acción de G_M sobre $k(\Lambda_M)$ conmuta con la acción de R_T, esto es, si $u \in k(\Lambda_M)$, $\sigma \in G_M$, $N \in R_T$, tenemos $\sigma(u^N) = (\sigma(u))^N$.*

Demostración: Sea $u \in k(\Lambda_M)$. Primero veamos que $u^N \in k(\Lambda_M)$, en efecto, $u = \sum_{i=1}^{h} a_i u_i$, $a_i \in k$, $u_i \in \Lambda_M$, $u^N = \sum_{i=1}^{h} a_i u_i^N$, $a_i \in k$, $u_i^N \in \Lambda_M$. Por último: $\sigma(u^N) = \sigma\left(\sum_{i=0}^{\text{gr}\,N} \left[\begin{array}{c} N \\ i \end{array} \right] u^{q^i}\right) = \sum_{i=0}^{\text{gr}\,N} \left[\begin{array}{c} N \\ i \end{array} \right] (\sigma(u))^{q^i} = (\sigma(u))^N$. ■

Proposición 15. *El grupo 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: Sabemos $k(\Lambda_M) = k(\lambda)$. Por tanto $\sigma \in G_M$ está determinado por su acción en λ. Ahora bien, $\sigma(\lambda)$ es un conjugado de λ (es raíz de un mismo polinomio), por lo tanto $\sigma(\lambda) \in \Lambda_M$ luego $\sigma(\lambda) = \lambda^A$ para algún $A \in R_T$. Veamos que $\sigma(\lambda)$ debe ser un generador de Λ_M. Si

$\xi \in \Lambda_M$, $\sigma^{-1}\xi \in \Lambda_M$, entonces $\sigma^{-1}\xi = \lambda^B$ para algún $B \in R_T$, por lo tanto $\xi = \sigma(\lambda^B) = (\sigma(\lambda))^B$ luego $\sigma(\lambda)$ es generador de Λ_M y por tanto $(A, M) = 1$, lo que implica que $A \bmod M \in (R_T/(M))^*$. Veamos que A no depende del generador λ, si λ_1 es otro generador de Λ_M, $\lambda_1 = \lambda^B$ para algún $B \in R_T$, $\sigma(\lambda_1) = \sigma(\lambda^B) = \sigma(\lambda)^B = \lambda^{AB} = (\lambda^B)^A = \lambda_1^A$. Finalmente, $\sigma(\lambda) = \lambda^A = \lambda^{A_1}$ implica $\lambda^{A-A_1} = 0$, por lo tanto $M|A - A_1$, luego $A \equiv A_1 \bmod M$. Consideremos $\theta : G_M \to (R_T/(M))^*$ tal que $\theta(\sigma) = A \bmod M$ donde $\sigma(\lambda) = \lambda^A$. Si $\psi \in G_M$, con $\psi(\lambda) = \lambda^B$, entonces $(\psi \circ \sigma)(\lambda) = \psi(\sigma(\lambda)) = \psi(\lambda^A) = \psi(\lambda)^A = \lambda^{BA} = \lambda^{AB}$, luego $\theta(\psi \circ \sigma) = AB \bmod M = \theta(\psi)\theta(\sigma)$ por lo tanto θ es homomorfismo. Ahora, supongamos $\theta(\sigma) = 1 \bmod M$, es decir, $\sigma \in \ker\theta$, $\sigma(\lambda) = \lambda^1 = \lambda$. Luego $\sigma = \mathrm{id}$, por tanto θ es monomorfismo. Luego $G_M \subseteq (R_T/(M))^*$ y como $|G_M| = [k(\Lambda_M) : k] \leq |(R_T/(M))^*| = \Phi(M)$ y como $(R_T/(M))^*$ es abeliano, tenemos G_M es abeliano.■

Definición 20. Sea $S \in R_T$ mónico, definimos el **polinomio ciclotómico con respecto a** S:

$$\psi_S(u) = \prod_{\substack{(B,S)=1 \\ \mathrm{gr}\, B \leq \mathrm{gr}\, S}} (u - \lambda_S^B),$$

donde λ_S es generador de Λ_S. Entonces

$$\psi_S(u) \in k(\Lambda_S)[u].$$

Sea $\sigma \in G_S = \mathrm{Gal}\,(k(\Lambda_S)/k)$. Entonces $\sigma(\lambda_S) = \lambda_S^A$, $(A, S) = 1$,

$$\sigma(\psi_S(u)) = \prod_{\substack{(B,S)=1 \\ \mathrm{gr}\, B \leq \mathrm{gr}\, S}} (u - \lambda_S^{AB}).$$

Ahora, $(A, S) = 1 = (B, S)$ implica que $(AB, S) = 1$, donde $AB = QS + B_1$ con $\mathrm{gr}\, B_1 < \mathrm{gr}\, S$, $\lambda_S^{AB} = \lambda_S^{B_1}$ y si $AB \equiv AC \bmod S$, donde $AB = Q_1S + B_1$ y $AC = Q_2S + C_1$, entonces $B_1 \equiv C_1 \bmod S$, implica $B_1 = C_1$, por lo tanto

$$\prod_{\substack{(B,S)=1 \\ \mathrm{gr}\, B \leq \mathrm{gr}\, S}} (u - \lambda_S^{AB}) = \prod_{\substack{(B,S)=1 \\ \mathrm{gr}\, B \leq \mathrm{gr}\, S}} (u - \lambda_S^B) = \psi_S(u),$$

luego $\sigma(\psi_S(u)) = \psi_S(u)$, lo que implica que $\psi_S(u) \in k[u]$, gr $\psi_S(u) = \Phi(S)$. Para cualquier $R, S \in R_T$, escogemos los generadores de Λ_R, Λ_S y Λ_{RS} como λ_R, λ_S y λ_{RS} sujetos a: $\lambda_{RS}^R = \lambda_S$, $\lambda_{RS}^S = \lambda_R$.

Ejemplo: Sean $q = 2$, $N = T^2$, $M = T^3$, y $\Lambda_T = \{u \in k^{ac} | u^T = 0\} = \{u \in k^{ac} | (\varphi + \mu_T)(u) = 0\} = \{u \in k^{ac} | u^2 + Tu = 0\} = \{0, T\}$, tenemos $\psi_T(u) = u + T$. También nos fijamos en $\Lambda_N = \{u \in k^{ac} | u^N = 0\} = \{u \in k^{ac} | (\varphi + \mu_T)^2(u) = 0\} = \{u \in k^{ac} | (\varphi + \mu_T)(u^2 + Tu) = 0\} = \{u \in k^{ac} | u^4 + T^2u^2 + Tu^2 + T^2u = 0\} = \{u \in k^{ac} | (u^2 + Tu)(u^2 + Tu + T) = 0\} = \{0, T, \lambda_N, \lambda_N + T\}$, donde $\lambda_N^2 + T\lambda_N + T = 0$. Aquí se sigue que $\psi_N(u) = u^2 + Tu + T$, y en $\Lambda_M = \{u \in k^{ac} | u^M = 0\} = \{u \in k^{ac} | (\varphi + \mu_T)^3(u) = 0\} = \{u \in k^{ac} | (\varphi + \mu_T)(u^4 + (T^2 + T)u + T^2u) = 0\} = \{u \in k^{ac} | (u^4 + (T^2 + T)u^2 + T^2u)(u^4 + (T^2 + T)u^2 + T^2u + T) = 0\} = \{0, T, \lambda_N, \lambda_N + T, \lambda_M, \lambda_M + T, \lambda_M + \lambda_N, \lambda_M + \lambda_N + T\}$, donde $\lambda_M^4 + (T^2 + T)\lambda_M^2 + T^2\lambda_M + T = 0$, se tiene $\psi_M(u) = u^4 + (T^2 + T)u^2 + T^2u + T$.

Proposición 16. *Si* $M \in R_T \backslash \{0\}$, $d =$ gr M, *entonces* $\sum_{N|M} \Phi(N) = q^d$.

Demostración: Ver [12] Capítulo 12.■

Proposición 17. *i) Si* $N \neq M$, *entonces* $(\psi_M(u), \psi_N(u)) = 1$.

ii) $u^M = \prod_{N|M} \psi_N(u)$.

iii) $\psi_M(u) = \prod_{N|M} (u^M)^{\mu(M/N)}$ *donde* $\mu(D) = \begin{cases} 1 & \text{si } D = 1, \\ -1 & \text{si } D = P_1 \cdots P_r, \\ & P_i \text{ irreducibles} \\ & \text{distintos}, \\ 0 & \text{en otro caso}, \end{cases}$

iv) $\psi_M(u)$ *es irreducible.*

Demostración: *i*) Sea M diferente de N y supóngase que $\psi_M(u)$, $\psi_N(u)$ no son primos relativos, es decir sea Θ una raíz tanto de $\psi_M(u)$ como $\psi_N(u)$. Se tiene $\Theta = \lambda_M^{B_1} = \lambda_N^{B_2}$ con $(B_1, M) = 1 = (B_2, N)$, luego $\lambda_{MN}^{B_1 N} = \Theta = \lambda_{MN}^{MB_2}$ lo que implica que $B_1 N \equiv MB_2 \bmod MN$, luego $N|M$ y $M|N$, por tanto $M = aN$ para algún $a \in \mathbb{F}_q^*$, como M y N son mónicos, tenemos $N = M$ lo cual no puede ser, luego se tiene el resultado. *ii*) Tenemos que

$u^M = \prod_{B|M}(u - \lambda_M^B)$ y para todo N que divide a M, $\psi_N(u)$ divide a u^M pues $\psi_N(u) = \prod_{\substack{(N,B)=1 \\ \text{gr } B \leq \text{gr } N}} (u - \lambda_N^B)$ como para $N_1 \neq N_2$, $\psi_{N_1}(u)$, $\psi_{N_2}(u)$ son primos relativos (por el inciso anterior) tenemos que $\prod_{N|M} \psi_N(u)$ divide al polinomio u^M y ambos son mónicos. Finalmente, por la Proposición 16, $\text{gr}\left(\prod_{N|M} \psi_N(u)\right) = \sum_{N|M} \Phi(N) = q^d$. Por lo tanto $\prod_{N|M} \psi_N(u) = u^M$. Para las demostraciones de *iii*) y *iv*) ver [12] Capítulo 12.■

Nota: Denotaremos por ϑ_M a la cerradura entera de R_T en $k(\Lambda_M)$.

Proposición 18. *Sean $M = P^n$, P irreducible mónico en R_T, $d =$ gr P. Entonces todo divisor primo de k diferente de P y P_∞ no es ramificado en $k(\Lambda_M)/k$ y el índice de ramificación de P en $k(\Lambda_M)/k$ es $\Phi(P^n) = q^{dn} - q^{d(n-1)}$.*

Demostración: Consideremos

$$\begin{array}{ccc} \vartheta_M & \text{——} & k(\Lambda_M) \\ & & | \\ R_T & \text{————} & k \end{array}$$

Tenemos que ϑ_M es un dominio de Dedekind y $R_T[\Lambda_M] \subseteq \vartheta_M$. Los primos ramificados diferentes al primo infinito P_∞ son los que aparecen en el discriminante. Sea λ un generador de Λ_M. Sea $g(u) =$ irr $(\lambda, u, k) \in k[u]$, sea $f(u) = u^M$. Puesto que $f(\lambda) = 0$, $g(u)|f(u)$, luego $f(u) = g(u)h(u)$, para algún $h(u) \in k[u]$.

$$M = f'(u) = g'(u)h(u) + g(u)h'(u), \tag{2.1}$$

tomando $u = \lambda$ en (2.1)

$$M = g'(\lambda)h(\lambda) + 0,$$

se sigue que $(g'(\lambda))_{\vartheta_M}$ divide a $(M)_{\vartheta_M} = P^n$. Puesto que el diferente

$$\mathfrak{D}_{\vartheta_M/R_T} = \text{ m.c.d.}\left\{F'(\alpha)|\ \alpha \text{ es entero y } k(\Lambda_M) = k(\alpha),\ F(u) = \text{ irr }(\alpha, u, k)\right\},$$

tenemos $\mathfrak{D}_{\vartheta_M/R_T}$ divide a $(g'(\lambda))_{\vartheta_M}$, que a su vez divide a P^n con $P^n = (\mathcal{P}_1 \cdots \mathcal{P}_h)^{en}$, donde

$$P\vartheta_M = (\mathcal{P}_1 \cdots \mathcal{P}_h)^e. \tag{2.2}$$

Por lo tanto los únicos posibles primos ramificados en $k(\Lambda_M)/k$ son P y P_∞. Ahora, calculemos $e = e_{k(\Lambda_M)/k}(\mathcal{P}_i|P)$, se tiene

$$u^{P^n} = (u^{P^{n-1}})^P = \sum_{i=0}^{d} \left[\begin{array}{c} P \\ i \end{array}\right] (u^{P^{n-1}})^{q^i} =$$

$$u^{P^{n-1}} \left(\sum_{i=0}^{\text{gr } P} \left[\begin{array}{c} P \\ i \end{array}\right] (u^{P^{n-1}})^{q^i - 1} \right) = u^{P^{n-1}} t(u),$$

donde $t(u) \in R_T[u]$,

$$t(u) = \frac{u^{P^n}}{u^{P^{n-1}}} = \prod_{\alpha \in \Lambda_{P^n} \setminus \Lambda_{P^{n-1}}} (u - \alpha) = \prod_{\alpha \text{ generador de } \Lambda_M} (u - \alpha) = \prod_{\substack{(A,M)=1 \\ \text{gr } A \leq \text{gr } M}} (u - \lambda^A)$$

$= \psi_M(u)$, por lo tanto $t(u) = \displaystyle\prod_{\substack{(A,M)=1 \\ \text{gr } A \leq \text{gr } M}} (u - \lambda^A) = P + \sum_{i=1}^{d} \left[\begin{array}{c} P \\ i \end{array}\right] (u^{p^{n-1}})^{q^i - 1}.$

Ahora, $u^A = u(F(u))$ para algún $F(u) \in R_T[u]$, luego $\lambda^A = \lambda(F(\lambda))$, entonces $\lambda|\lambda^A$ en ϑ_M, para $(A, M) = 1$, λ^A también es generador. Por simetría $\lambda^A|\lambda$, por lo tanto

$$\lambda = \beta_A \lambda^A, \tag{2.3}$$

con $\beta_A \in \vartheta_M^*$. Para $u = 0$,

$$t(0) = \pm \prod_{\substack{(A,M)=1 \\ \text{gr } A \leq \text{gr } M}} \lambda^A = P.$$

Usando la ecuación (2.3) obtenemos $\pm P = \beta_0 \lambda^{\Phi(M)}$, para algún $\beta_0 \in \vartheta_M^*$.

Por lo tanto (2.2) nos da $(\mathcal{P}_1 \cdots \mathcal{P}_h)^e = (P)_{\vartheta_M} = (\lambda^{\Phi(M)})_{\vartheta_M} = (\lambda)_{\vartheta_M}^{\Phi(M)}$, la valuación $\nu_{\mathcal{P}_i}(\lambda) \geq 1$ implica $\nu_{\mathcal{P}_i}(\lambda^{\Phi(M)}) \geq \Phi(M)$, entonces $e \geq \Phi(M)$. Luego $e \geq \Phi(M) = |\,(R_T/(M))^*\,| \geq |G_M| = [k(\Lambda_M) : k] \geq e$. Concluimos que $e = \Phi(M) = [k(\Lambda_M) : k] = q^{dn} - q^{d(n-1)}$.■

Teorema 11. *Sea $M \in R_T \backslash \{0\}$, mónico. Entonces:*

i) $\psi_M(u) = \text{ irr } (\lambda, u, k)$ *(en particular $\psi_M(u)$ es irreducible).*

ii) $G_M = \text{ Gal } (k(\Lambda_M)/k) \cong (R_T/(M))^*$.

iii) $[k(\Lambda_M) : k] = \Phi(M)$.

iv) Si $M = P^n$ para algún polinomio irreducible P, entonces $\mathfrak{p}$ es totalmente ramificado en $k(\Lambda_M)/k$, donde $(P)_k = \dfrac{\mathfrak{p}}{\mathfrak{p}_\infty^{\text{gr } P}}$.

Demostración: Si $M = P^n$, se tiene $[k(\Lambda_M) : k] = \Phi(M)$ por lo tanto

$$G_M \cong (R_T/(M))^*,$$

pues $G_M \subseteq (R_T/(M))^*$ y ambos son del mismo orden. También, $\mathfrak{p}$ es totalmente ramificado pues su índice de ramificación es $e = \Phi(M)$ por lo tanto tenemos *iv*). Ahora, si $M = P_1^{\alpha_1} \cdots P_h^{\alpha_h}$, sabemos que

$$\Lambda_M = \bigoplus_{i=1}^{h} \Lambda_{P_i^{\alpha_i}}.$$

Si probamos $[k(\Lambda_M) : k] = \Phi(M)$ se tendrá que $G_M \cong (R_T/(M))^*$, pues $G_M \subseteq (R_T/(M))^*$ y ambos son del mismo orden. Luego tendremos *ii*) y *iii*), *i*) se seguirá de que $\psi_M(\lambda) = 0$ y $\text{gr}_u(\psi_M(u)) = \Phi(M) = \text{ gr } (\text{irr } (\lambda, u, k))$. Luego basta probar que $[k(\Lambda_M) : k] = \Phi(M)$. Ahora, $k(\Lambda_{P_1^{\alpha_1}}), \ldots, k(\Lambda_{P_h^{\alpha_h}})$ son linealmente disjuntos a pares pues P_i es totalmente ramificado en $k(\Lambda_{P_i^{\alpha_i}})$ y no ramificado en $\prod_{\substack{j=1 \\ j \neq i}}^{h} k(\Lambda_{P_j^{\alpha_j}})$, por lo tanto

$$[k(\Lambda_M) : k] = \prod_{i=1}^{h} [k(\Lambda_{P_j^{\alpha_j}}) : k] = \prod_{i=1}^{h} \Phi(p_i^{\alpha_i}) = \Phi(M).$$■

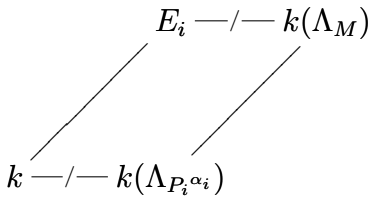
Ejemplo: Ahora sean $q = 2$, $M = T^3$ y $N = T^2$. El campo $k(\Lambda_M)$ es de Galois sobre k con grupo de Galois $G_M \cong (R_T/(M))^* \cong \mathbb{Z}/4\mathbb{Z}$. Este es un ejemplo de una extensión de k de grado cuatro (pues $\Phi(T^3) = 4$) con grupo de Galois cíclico, los elementos de G_M son $\{\sigma_1 = \text{ id }, \sigma_2, \sigma_3, \sigma_4\}$, un generador para este grupo cíclico es $\sigma_2 : \lambda_M \to \lambda_M^{T+1}$ el cual tiene orden cuatro en $(R_T/(M))^*$. Ahora como $N|M$ tenemos que $G_N < G_M$ como G_M es cíclico se sigue por teoría de grupos que $G_N = \text{ Gal }(k(\Lambda_N)/k)$ es cíclico y es isomorfo a $\mathbb{Z}/2\mathbb{Z}$, ya que $\Phi(T^2) = 2$.

Corolario 5. *La extensión $k(\Lambda_M)/k$ es geométrica, es decir, el campo de constantes de $k(\Lambda_M)$ es el mismo que el de k (que es $\mathbb{F}_q$).*

Demostración: Sea $\mathbb{F}_{q^s}$ el campo de constantes de $k(\Lambda_M)$, sea $M = P_1^{\alpha_1} \cdots P_h^{\alpha_h}$,

$$k(\Lambda_M) = \prod_{i=1}^{h} k(\Lambda_{P_i^{\alpha_i}}).$$

Para cada $1 \leq i \leq h$, sea $E_i = k(\Lambda_{M/P_i^{\alpha_i}})$



.

Tenemos Gal $(k(\Lambda_M)/E_i) \cong$ Gal $(k(\Lambda_{P_i{}^{\alpha_i}})/k)$. Sea R la máxima extensión de k no ramificada y contenida en $k(\Lambda_M)$,

$$k \subseteq R \subseteq k(\Lambda_M).$$

Se tiene que $k(\Lambda_M)/E_i$ es totalmente ramificada en P_i y E_iR/E_i es no ramificada. Esto implica $E_iR = E_i$, entonces $R \subseteq E_i$, por lo tanto

$$R \subseteq \bigcap_{i=1}^{h} E_i = k.$$

Luego $k = R$. Por tanto, si S es un campo $k \subseteq S \subseteq k(\Lambda_M)$ y $S \neq k$, entonces S/k es ramificada. Sea $S = \mathbb{F}_{q^s}(T)$. Tenemos S/k es no ramificada por ser extensión de constantes. Por lo tanto $S = k$, entonces $\mathbb{F}_{q^s} = \mathbb{F}_q$.■

Proposición 19. *Sea $M = P^n$, con $P \in R_T$ mónico e irreducible. Entonces $\psi_{P^n}(u) = \dfrac{u^{P^n}}{u^{P^{n-1}}}$ es un polinomio de Eisenstein en P.*

Demostración: Sea $\psi_{P^n}(u) = \prod_{\substack{(A,P)=1 \\ \text{gr } A \leq \text{gr } M}} (u - \lambda^A)$ (λ generador de Λ_{P^n}), sabemos P es totalmente ramificado en $k(\Lambda_M)/k$, luego

$$P\,\vartheta_M = \mathcal{P}^{\Phi(M)} \text{ y } \psi_{P^n}(0) = \pm \prod_{\substack{(A,P)=1 \\ \text{gr } A \leq \text{gr } M}} \lambda^A = P,$$

$$\Phi(M) = \nu_{\mathcal{P}}(P) = \nu_{\mathcal{P}}\left(\prod_{\substack{(A,P)=1 \\ \text{gr } A \leq \text{gr } M}} \lambda^A\right) = \sum_{\substack{(A,P)=1 \\ \text{gr } A \leq \text{gr } M}} \nu_{\mathcal{P}}\left(\lambda^A\right) =$$

$$= \sum_{\substack{(A,P)=1 \\ \text{gr } A \leq \text{gr } M}} \nu_{\mathcal{P}^A}(\lambda) = \sum_{\substack{(A,P)=1 \\ \text{gr } A \leq \text{gr } M}} \nu_{\mathcal{P}}(\lambda) = \Phi(M)\nu_{\mathcal{P}}(\lambda),$$

lo cual implica $\nu_{\mathcal{P}}(\lambda) = 1$. Tenemos

$$\psi_{P^n}(u) = u^{\Phi(M)} - f_{\Phi(M)-1}(\{\lambda^A\}_A)u^{\Phi(M)-1} + \cdots$$

$$\cdots \pm f_1(\{\lambda^A\}_A)u + (-1)^{\Phi(M)} f_0(\{\lambda^A\}_A),$$

con $f_i(\{\lambda^A\}_A)$ polinomios simétricos, entonces $\nu_{\mathcal{P}}(f_i(\{\lambda^A\}_A)) > 0$, implica P divide a f_i, finalmente $\nu_{\mathcal{P}}(f_0(\{\lambda^A\}_A)) = \pm P$.■

Corolario 6. *El polinomio $\psi_{P^n}(u)$ es irreducible.*

Demostración: Se sigue del criterio de Eisenstein.■

Definición 21. Consideramos una extensión de Galois L/k de campos globales (es decir, L/k son campos numéricos o campos de funciones con campos de constantes finitos). Si P es un primo de k no ramificado y $\mathcal{P}$ un primo en L tal que $\mathcal{P}$ divide a P y $L(\mathcal{P})/k(P)$ es la extensión de campos residuales (ver [11] página 41), entonces

$$\left[\frac{L/k}{\mathcal{P}}\right] : L(\mathcal{P}) \to L(\mathcal{P})$$

denota el automorfismo de Fröbenius. Si $\mathcal{P}^\sigma$ es un conjugado de $\mathcal{P}$,

$$\left[\frac{L/k}{\mathcal{P}^\sigma}\right] = \sigma \left[\frac{L/k}{\mathcal{P}}\right] \sigma^{-1}.$$

En el caso de que L/k sea abeliana, $\left[\frac{L/k}{\mathcal{P}}\right]$ no depende de $\mathcal{P}$, solamente de P (es decir, del primo en k). En este caso ponemos: $\left(\frac{L/k}{P}\right)$ el cual se llama el **símbolo de Artin** en P y $\left(\frac{L/k}{P}\right)$ está determinado por: $\left(\frac{L/k}{P}\right)(x) \equiv x^{q^d} \bmod \mathcal{P}$, para toda $x \in \vartheta_{\mathcal{P}}$ donde $\vartheta_{\mathcal{P}} = \{\xi \in L | \nu_{\mathcal{P}}(\xi) \geq 0\}$, $\nu_{\mathcal{P}}$ es la valuación asociada al primo $\mathcal{P}$ (ver [11] página 28), $d = \text{gr } P$ y $q^d = |k(\mathcal{P})|$.

Corolario 7. *Sea P un primo que no divide a M. Entonces $\varphi_P \in G_M$ dado por $\varphi_P(\lambda) = \lambda^P$, $\lambda \in \Lambda_M$ corresponde al símbolo de Artin* $\left(\frac{k(\Lambda_M)/k}{P}\right)$.

Demostración: Se tiene $k(P) \cong R_T/(P) \cong \mathbb{F}_{q^d}$ donde $d = \text{gr } P$. Entonces si $\mathcal{P}$ es primo en $k(\Lambda_M)$, tal que $\mathcal{P}$ divide a P,

$$\left(\frac{k(\Lambda_M)/k}{P}\right)(\lambda) \equiv \lambda^{q^d} \bmod \mathcal{P},$$

para $\lambda \in \vartheta_{\mathcal{P}}$, $\lambda \in \Lambda_M$. Como $u^P = u\Psi_P(u) = u(u^{q^d-1} + \cdots + \beta_1 u + \beta_0)$ y P divide a β_i para toda i, tenemos

$$\lambda^{\mathcal{P}} \equiv \lambda^{q^d} \bmod \mathcal{P},$$

$\lambda \in \Lambda_M$. Ahora: $u^M = \prod_{\substack{A \bmod M \\ \text{gr } A \leq \text{gr } M}} (u - \lambda^A)$. Tomando la derivada de u^M con respecto a u, tenemos $M = \sum_{A \bmod M} \prod_{\substack{B \bmod M \\ B \neq A}} (u - \lambda^B)$, constante en u. Tomemos $u = \lambda^C$,

$$M = \prod_{C \neq B} (\lambda^C - \lambda^B).$$

Puesto que P no divide a M, tenemos

$$\lambda^C \not\equiv \lambda^B \bmod P,$$

para toda $C \not\equiv B \bmod M$. Lo cual implica $\left(\frac{k(\Lambda_M)/k}{P}\right)(\lambda) = \lambda^P = \varphi_P(\lambda)$. ■

2.2 Ramificación en P_∞

Se desea probar lo siguiente:
Sea $M \in R_T \backslash \{0\}$. Entonces P_∞ se descompone en $\Phi(M)/(q-1)$ divisores primos de $k(\Lambda_M)$. Además $e_\infty = q - 1$ y el grado de cada primo encima de P_∞ es $f_\infty = 1$.

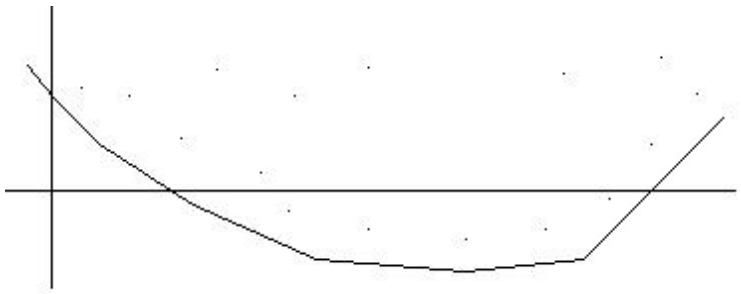
Para probar este resultado desarrollaremos el Método de Newton y probaremos el Lema de Abhyankar.
Primero, sea F un campo completo con respecto a una valuación discreta ν con lugar $\mathcal{P}$. Sea Ω una cerradura algebraica de F. Sea

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n,$$

$a_0, a_n \neq 0$. A cada sumando de $f(x)$ le asociamos un punto en $\mathbb{R} \times \mathbb{R}$ de la siguiente forma: si $a_i x^i \neq 0$, (es decir, $a_i \neq 0$) tomamos $(i, \nu(a_i))$ y si $a_i x^i = 0$, (es decir, $a_i = 0$) tomamos el punto inexistente $(i, \infty) = (i, \nu(a_i))$, (es decir, no escogemos ningún punto). Formamos la cubierta convexa inferior del conjunto de puntos

$$\{(i, \nu(a_i)) | i = 0, 1, \ldots, n\}$$

(la cual se llama **polígono de Newton**).



Más precisamente, los vértices de la cubierta son:

$$\{(0,\nu(a_0)),(i_1,\nu(a_{i_1})),\ldots,(n,\nu(a_n))\}$$

donde primero consideramos $S=\{i>0|a_i\neq 0\}$, i_1 es el máximo índice con la propiedad.

$$\frac{\nu(a_i)-\nu(a_0)}{i-0}=\text{ mín }\left\{\frac{\nu(a_j)-\nu(a_0)}{j-0}|j\in S\right\},$$

i_2 es el máximo índice tal que

$$\frac{\nu(a_i)-\nu(a_{i_1})}{i-i_1}=\text{ mín }\left\{\frac{\nu(a_j)-\nu(a_{i_1})}{j-i_1}|j\in S,j>i_1\right\},$$

etc.

Proposición 20. *Supongamos que* $(r,\nu(a_r))\leftrightarrow(s,\nu(a_s))$ *con* $r<s$ *es cualquier segmento del polígono de Newton de* $f(x)$ *la cual tiene pendiente* $\dfrac{\nu(a_s)-\nu(a_r)}{s-r}=-m$. *Entonces* $f(x)$ *tiene exactamente* $s-r$ *raíces* $\alpha_1,\ldots,\alpha_{s-r}$ *con* $\nu(\alpha_1)=\cdots=\nu(\alpha_{s-r})=m$. *Más aún* $f_m(x)=\prod_{i=1}^{s-r}(x-\alpha_i)\in F[x]$ *y* $f_m(x)|f(x)$.

Demostración: Ver [9] página 211.■

Volviendo a los campos de funciones, tenemos:

Proposición 21. *Sea* $M=P^n$, P *mónico e irreducible en* R_T, $d=\text{ gr }P$. *Entonces* P_∞ *se descompone en* $\Phi(M)/(q-1)$ *divisores primos en* $K(\Lambda_M)$.

El índice de ramificación es $e_\infty = q-1$ *y cada uno de estos primos tiene grado de inercia* $f_\infty = 1$.

Demostración: Sea $\mathfrak{B}$ un divisor primo en $k(\Lambda_M)$ sobre P_∞. Puesto que la extensión es de Galois, es suficiente probar que $e_{\mathfrak{B}} = q-1$ y $f_{\mathfrak{B}} = 1$. Sea $\mathfrak{p}$ el divisor primo de $k(\Lambda_P) \subseteq k(\Lambda_M)$ bajo $\mathfrak{B}$ es decir

$$\mathfrak{B} \cap k(\Lambda_P) = \mathfrak{p}.$$

Primero probemos que $e_{\mathfrak{B}} = q-1$ y $f_{\mathfrak{B}} = 1$ y después que $\mathfrak{p}$ se descompone totalmente en $k(\Lambda_M)/k(\Lambda_P)$. Sea $g(u) = \dfrac{u^p}{u} = \Psi_P(u)$ y $k(\Lambda_P)$ se obtiene de k al adjuntarle las raíces de $g(u)$. Ahora,

$$g(u) = \sum_{i=0}^{d} \left[\begin{array}{c} P \\ i \end{array} \right] u^{q^i-1} = h(u^{q-1}),$$

donde

$$h(u) = \sum_{i=0}^{d} \left[\begin{array}{c} P \\ i \end{array} \right] u^{\frac{q^i-1}{q-1}},\ \mathrm{gr}_T \left[\begin{array}{c} P \\ i \end{array} \right] = (d-i)q^i.$$

Sea k_∞ la completación de k en P_∞ y sea ν_∞ la valuación correspondiente. Entonces

$$\nu_\infty \left(\left[\begin{array}{c} P \\ i \end{array} \right] \right) = -(d-i)q^i = -\mathrm{gr}_T \left(\left[\begin{array}{c} P \\ i \end{array} \right] \right).$$

Pongamos $h(u) = \sum_{j=0}^{\frac{q^d-1}{q-1}} f_j(T)u^j$, tenemos $f_j(T) \neq 0$ si y sólo si $j = \dfrac{q^i-1}{q-1}$. Tomamos todos los vértices

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

La pendiente entre β_i y β_{i+1} es:

$$S_i = \frac{-(d-(i+1))q^{i+1} + (d-i)q^i}{\dfrac{q^{i+1}-1}{q-1} - \dfrac{q^i-1}{q-1}} = \cdots = -d(q-1) + q + i(q-1) < S_{i+1}$$

por lo tanto, las pendientes se incrementan con i, luego $\beta_0, \beta_1, \ldots, \beta_d$ son los vértices del polígono de Newton. La pendiente entre β_0 y β_1 es:

$$S_0 = -d(q-1) + q.$$

Como

$$\frac{q^1 - 1}{q-1} - 0 = 1 - 0 = 1,$$

$h(u)$ tiene una raíz θ en k_∞ con $\nu_\infty(\theta) = d(q-1) - q$. Ahora, puesto que $g(u) = h(u^{q-1})$, $k(\Lambda_P)_\mathfrak{p} = k_\infty(\lambda)$ donde λ es raíz de $u^{q-1} - \theta$, esto es $\lambda^{q-1} = \theta$. Sea $\nu_\mathfrak{p}$ la valuación en $k(\Lambda_P)$ sobre ν_∞. Se tiene

$$(q-1)\nu_\mathfrak{p}(\lambda) = \nu_\mathfrak{p}(\lambda^{q-1}) = \nu_\mathfrak{p}(\theta) = e_\infty \nu_\infty(\theta) = e_\infty(d(q-1) - q).$$

Puesto que $(d(q-1) - q, q-1) = 1$, tenemos $q-1 | e_\infty$ y por otro lado $(q-1) \geq [k(\Lambda)_\mathfrak{p} : k_\infty] = e_\infty f_\infty \geq e_\infty$, tenemos $e_\infty = q-1$, es decir $k(\Lambda_P)_\mathfrak{p}/k_\infty$ es totalmente ramificada ($e_\mathfrak{p} = q-1$, $f_\mathfrak{p} = 1$). Ahora veamos que $\mathfrak{p}$ se descompone totalmente en $k(\Lambda_{P^n})/k(\Lambda_P)$. Sea λ raíz de $g(u)$, $\nu_\mathfrak{p}(\lambda) = d(q-1) - q$,

$$\frac{u^{P^n}}{u^{P^{n-1}}} = \Psi_{P^n}(u) = \Psi_P(u^{P^{n-1}}) = g(u^{P^{n-1}})$$

$k(\Lambda_M)$ se obtiene de $k(\Lambda_P)$ adjuntándole cualquier raíz de $g(u^{P^{n-1}})$. Así $k(\Lambda_M)$ se obtiene de $k(\Lambda_P)$ adjuntándole una raíz de $u^{P^{n-1}} - \lambda$ (pues $\lambda \in \Lambda_P$ es generador, si λ_{P^n} es generador de Λ_M, $\lambda_{P^n}^{P^{n-1}} = \lambda_{P^n/P^{n-1}} = \lambda_P$ es generador de Λ_P). Calculemos el polígono de Newton de $u^{P^{n-1}} - \lambda$. Se tiene:

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

sean $\gamma_{-1} = (0, \nu_\mathfrak{p}(-\lambda)) = (0, d(q-1) - q)$ y $\gamma_i = \left(q^i, \nu_\mathfrak{p}\left(\begin{bmatrix} P^{n-1} \\ i \end{bmatrix}\right)\right) = (q^i, e(\mathfrak{p}|P_\infty))\nu_\infty\left(\begin{bmatrix} P^{n-1} \\ i \end{bmatrix}\right) = (q^i, -(q-1)(d(n-1)-i)q^i)$, $0 \leq i \leq (n-1)d$.
La pendiente de γ_{-1} a γ_0 es:

$$\frac{-(q-1)(d(n-1))q^0 - (d(q-1) - q)}{1-0} = -dn(q-1) + q = t_{-1}.$$

La pendiente de γ_i a γ_{i+1} es:

$\frac{-(q-1)(d(n-1)-(i+1))q^{i+1}+(q-1)(d(n-1)-i)q^i}{q^{i+1}-q^i} = -(q-1)d(n-1)+i(q-1)+q = t_i < t_{i+1}$, $t_{-1} = -dn(q-1)+q < -(q-1)d(n-1)+q = t_0$, por lo tanto $\gamma_{-1}, \gamma_0, \ldots, \gamma_{(n-1)d}$ son los vértices del polígono de Newton. El segmento de γ_{-1} a γ_0 muestra que $u^{P^{n-1}} - \lambda$ tiene una raíz en $k(\Lambda_P)_\mathfrak{p}$. Puesto que la extensión es de Galois, $k(\Lambda_M)_\mathfrak{B} = k(\Lambda_P)_\mathfrak{p}$, luego $f(\mathfrak{B}|\mathfrak{p}) = e(\mathfrak{B}|\mathfrak{p}) = 1$.■

Para probar esto mismo en el caso general necesitamos el Lema de Abhyankar. Para ello primero necesitamos:

Lema 1. *Supongamos G es un grupo finito y U es subgrupo normal de G, $|U| = p^n$ (con $p = 1$ o p primo) y supongamos G/U es cíclico de orden primo relativo a p. Sea $H_1 < G$ con $p^n || H_1|$. Entonces para todo $H_2 < G$ se tiene: $|H_1 \cap H_2| = (|H_1|, |H_2|)$.*

Demostración: Observemos que $|H_1 \cap H_2| ||H_i|$ $i = 1, 2$ implica

$$|H_1 \cap H_2| | (|H_1|, |H_2|).$$

Pongamos $|H_1| = a_1 p^n$, $|H_2| = a_2 p^m$, con $(a_1, p) = 1 = (a_2, p)$, $d = (a_1, a_2)$. Entonces $(|H_1|, |H_2|) = dp^m$, $(d, p) = 1$ luego $|H_1 \cap H_2| \leq dp^m$. Puesto que U es el p-subgrupo de Sylow de G, U contiene a cualquier subgrupo de orden p^m y si $V \subseteq H_2$, $|V| = p^m$, entonces $V \subseteq U \subseteq H_1$, lo que implica $V \subseteq H_1 \cap H_2$ por lo tanto $H_1 \cap H_2$ contiene un subgrupo de orden p^m. Sea $\pi : G \to G/U$ el epimorfismo natural $\pi(H_i) = \dfrac{H_i U}{U} \leq G/U$ tenemos

$$|\pi(H_i)| = \left|\frac{H_i U}{U}\right| = \frac{|H_i||U|}{|H_i \cap U||U|} = a_i.$$

Por tanto $\pi(H_i)$ es cíclico de orden a_i, para $i = 1, 2$, luego $\pi(H_1) \cap \pi(H_2)$ es cíclico de orden $d = (a_1, a_2)$ (pues G/U es cíclico), por lo tanto existe $x \in H_1 \cap H_2$ tal que $d | o(x)$, luego $|H_1 \cap H_2| \geq dp^m$. Concluimos $|H_1 \cap H_2| = (|H_1|, |H_2|)$. ■

Teorema 12 (Lema de Abhyankar). *Sea E/F una extensión finita y separable de campos de funciones, $E = F_1 F_2$ con $F \subseteq F_i \subseteq E$, $i = 1, 2$. Sean $\mathfrak{p}$ un divisor primo de F, $\mathfrak{P}$ primo en E tal que $\mathfrak{P}|\mathfrak{p}$ y $\mathfrak{P}_i = \mathfrak{P} \cap F_i$ la*

restricción de $\mathfrak{P}$ *a* F_i*, para* $i = 1, 2$*. Si al menos una de las extensiones* $\mathfrak{P}_1/\mathfrak{p}$ *o* $\mathfrak{P}_2/\mathfrak{p}$ *tiene ramificación moderada, entonces* $e(\mathfrak{P}|\mathfrak{p}) = [e(\mathfrak{P}_1|\mathfrak{p}), e(\mathfrak{P}_2|\mathfrak{p})]$.

Demostración: Sea $\widetilde{E}$ tal que $\widetilde{E}/F$ es finita y de Galois, $E \subseteq \widetilde{E}$ y sea $\mathfrak{B}$ primo en $\widetilde{E}$ tal que $\mathfrak{P}$ es la restricción de $\mathfrak{B}$ a E.
Sean $G = I(\mathfrak{B}|\mathfrak{p})$, $H_i = I(\mathfrak{B}|\mathfrak{P}_i)$, $i = 1, 2$. Sea $p =$ car F, si car $F \neq 0$ y sea $p = 1$, si car $F = 0$. Se tiene que alguno de $\mathfrak{P}_i|\mathfrak{p}$, $i = 1, 2$ tiene ramificación moderada, digamos $\mathfrak{P}_1|\mathfrak{p}$. Entonces: $(e(\mathfrak{P}_1|\mathfrak{p}), p) = 1$. Ahora, si U es el p-subgrupo de Sylow de G, entonces U es subgrupo normal de G (pues U es el primer grupo de ramificación, que es subgrupo normal del grupo de inercia G). Tenemos $U \subseteq H_1$ pues la ramificación salvaje está concentrada en $\mathfrak{B}/\mathfrak{P}_1$ y G/U es cíclico de orden primo relativo a p, luego se satisfacen las hipótesis del lema, por lo tanto

$$|H_1 \cap H_2| = (|H_1|, |H_2|).$$

Ahora, $E = F_1F_2$ implica

$$\text{Gal}\,(\widetilde{E}/E) = \text{Gal}\,(\widetilde{E}/F_1) \cap \text{Gal}\,(\widetilde{E}/F_2)$$

y

$$I(\mathfrak{B}|\mathfrak{P}) = I(\mathfrak{B}|\mathfrak{P}_1) \cap I(\mathfrak{B}|\mathfrak{P}_2) = H_1 \cap H_2,$$

luego
$e(\mathfrak{B}|\mathfrak{P}) = |I(\mathfrak{B}|\mathfrak{P})| = |H_1 \cap H_2| = (|H_1|, |H_2|) = (e(\mathfrak{B}|\mathfrak{P}_1), e(\mathfrak{B}|\mathfrak{P}_2)) = (e(\mathfrak{B}|\mathfrak{P})e(\mathfrak{B}|\mathfrak{P}_1), e(\mathfrak{B}|\mathfrak{P})e(\mathfrak{B}|\mathfrak{P}_2)) = e(\mathfrak{B}|\mathfrak{P})(e(\mathfrak{B}|\mathfrak{P}_1), e(\mathfrak{B}|\mathfrak{P}_2))$ lo que implica que

$$(e(\mathfrak{B}|\mathfrak{P}_1), e(\mathfrak{B}|\mathfrak{P}_2)) = 1.$$

Por otro lado $e(\mathfrak{P}|\mathfrak{p}) = e(\mathfrak{P}|\mathfrak{P}_1)e(\mathfrak{P}_1|\mathfrak{p}) = e(\mathfrak{P}|\mathfrak{P}_2)e(\mathfrak{P}_2|\mathfrak{p})$. Se tiene que $ax = by$ con $(x, y) = 1$, $a, b, x, y \in \mathbb{Z} \setminus \{0\}$ implica $[a, b] = ax = by$, entonces

$$e(\mathfrak{P}|\mathfrak{p}) = [e(\mathfrak{P}_1|\mathfrak{p}), e(\mathfrak{P}_2|\mathfrak{p})].\blacksquare$$

Teorema 13. *Sea* $M \in R_T$, $M \neq 0$*. Entonces* P_∞ *es moderadamente ramificado en* $k(\Lambda_M)/k$*. De hecho* $e_\infty = q - 1$ *y* $f_\infty = 1$, $g_\infty = \Phi(M)/(q - 1)$.

Demostración: Si $M = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$,

$$k(\Lambda_M) = \prod_{i=1}^{r} k(\Lambda_{P_i^{\alpha_i}}) \quad \text{y} \quad e(\mathfrak{P}_i|\mathfrak{p}_\infty) = q-1,$$

la ramificación es moderada pues

$$(p, q-1) = 1.$$

Por el Lema de Abhyankar, $e_\infty = [q-1, \ldots, q-1] = q-1$. Además, todos los grados de inercia relevantes son 1, entonces $f_\infty = 1$.■

Proposición 22. *Sean $M \in R_T \setminus \{0\}$ y P irreducible, $P \neq P_\infty$ tal que $P \nmid M$. Entonces en $k(\Lambda_M)/k$, $e_P = 1$ y $f_P = o(P \bmod M)$, $g_P = \Phi(M)/f_P$.*

Demostración: Sea $\lambda = \lambda_M$ generador de Λ_M. Entonces $k(\Lambda_M) = k(\lambda)$. Sea $\mathfrak{P}$ divisor primo de $k(\Lambda_M)$, $\mathfrak{P}|P$.

$$\vartheta_{\mathfrak{P}} = \{\xi \in k(\Lambda_M) | \nu_{\mathfrak{P}}(\xi) \geq 0\}$$

y

$$f_P = [\vartheta_{\mathfrak{P}}/\mathfrak{P} : (R_T)_P/P(R_T)_P] = [(\vartheta_M)_{\mathfrak{P}}/\mathfrak{P}(\vartheta_M)_{\mathfrak{P}} : R_T/P] =$$

$$= [\vartheta_M/\mathfrak{P}\vartheta_M : R_T/P]\,.$$

Se tiene que P no es ramificado en $k(\Lambda_M)/k$ y φ_P (que corresponde al símbolo de Artin), está dado por $\varphi_P(\lambda) = \lambda^P$. Tenemos $o(\varphi_P) = f_P$. Es decir, f_P es el mínimo tal que $\varphi_P^{f_P} = \text{id} \in G_M$, donde $G_M = \text{Gal}\,(k(\Lambda_M)/k)$. Luego $\varphi_P^f = \text{id}$ si y sólo si $\varphi_P^f(\lambda) = \lambda^{P^f} = \lambda$ si y sólo si $\lambda^{P^f-1} = 0$ si y sólo si $M|P^f - 1$ si y sólo si $P^f \equiv 1 \bmod M$ por lo que $f_P = o(P \bmod M)$. ■

Por lo tanto, tenemos el teorema general:

Teorema 14. *Sea $M = P_1^{\alpha_1} \cdots P_h^{\alpha_h}$ y consideramos $k(\Lambda_M)/k$. Si $P \neq P_1$, $\ldots$, P_h, P_∞, entonces $e_P = 1$, $f_P = o(P \bmod M)$, $g_P = \Phi(M)/f_P$. Si $P = P_i$, $1 \leq i \leq h$, entonces $e_{P_i} = \Phi(P_i^{\alpha_i})$, $f_{P_i} = o\left(P_i \bmod \dfrac{M}{P_i^{\alpha_i}}\right)$,*

$g_{P_i} = \dfrac{\Phi(M)}{\Phi(P_i^{\alpha_i}) f_P} = \dfrac{\Phi(M/P_i^{\alpha_i})}{o\left(P_i \bmod \dfrac{M}{P_i^{\alpha_i}}\right)}$. *Si* $P = P_\infty$, $e_\infty = q-1$, $f_\infty = 1$, $g_\infty = \Phi(M)/(q-1)$.

Demostración: Ver [12] Capítulo 12.■

Observación: Sea $M \in R_T$, $M \neq 0$. Si $A = \alpha \in \mathbb{F}_q^* \subseteq (R_T/(M))^*$ entonces $\sigma_A(\lambda) = \sigma_\alpha(\lambda) = \lambda^\alpha = \alpha\lambda$.

Proposición 23. *Se tiene que* $\mathbb{F}_q^*$ *es isomorfo al grupo de inercia de cualquier divisor primo de* $k(\Lambda_M)$ *sobre* P_∞.

Demostración: Ver [3] página 161.■

Definición 22. Sean $M \in R_T$, $M \neq 0$, y G_0 el grupo de inercia de cualquier divisor primo de $k(\Lambda_M)$ sobre P_∞. El campo $k(\Lambda_M)^+ = k(\Lambda_M)^{G_0}$, se llama el **subcampo real maximal** de $k(\Lambda_M)$.

Se tiene $[k(\Lambda_M) : k(\Lambda_M)^+] = q-1$ y P_∞ se descompone totalmente en $k(\Lambda_M)^+/k$ en $\Phi(M)/(q-1)$ divisores primos.

Para cualquier $M \in R_T$, recordemos que ϑ_M denota la cerradura entera de R_T en $k(\Lambda_M)$.

Proposición 24. *Supongamos que* $M = P^n$ *para algún polinomio irreducible* P. *Entonces* $\vartheta_M = R_T[\lambda_M]$ *donde* λ_M *es un generador de* Λ_M.

Demostración: Sea $\lambda = \lambda_M$. Como λ es entero, tenemos

$$R_T[\lambda] \subseteq \vartheta_M.$$

Sea $\alpha \in \vartheta_M$. Tenemos que $\{1, \lambda, \ldots, \lambda^{\Phi(M)-1}\}$ 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 $h = \Phi(M) - 1$. Queremos mostrar que $a_i \in R_T$ para $i = 0, \ldots, h$. Por la demostración de la Proposición 18 tenemos que $v_{\mathfrak{P}}(\lambda) = 1$ donde $\mathfrak{P}$ es el (único) divisor primo de $k(\Lambda_M)$ sobre $\mathfrak{p}$ y $(P)_k = \dfrac{\mathfrak{p}}{\mathfrak{p}_\infty^{\operatorname{gr} P}}$. Claramente,

$$v_{\mathfrak{P}}(a_i\lambda^i) = i + \Phi(M)v_{\mathfrak{p}}(a_i) \equiv i \bmod \Phi(M)$$

Así, cuando $i \neq j$, $a_i \neq 0$ y $a_j \neq 0$, tenemos $v_{\mathfrak{P}}(a_i\lambda^i) \neq v_{\mathfrak{P}}(a_j\lambda^j)$. De esto se sigue que

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

Por lo tanto, $v_{\mathfrak{P}}(a_i) \geq 0$ para toda i. Ahora, para cualquier $\sigma_A \in G_M$ tal que $\sigma_A(\lambda) = \lambda^A$, tenemos

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

donde $A \bmod M \in (R_T/(M))^*$. Si $\{\overline{A}_1, \ldots, \overline{A}_{\Phi(M)}\}$ es un conjunto de representantes de $(R_T/(M))^*$ obtenemos de (2.4), denotando $\alpha_i = \alpha^{A_i}$, $\lambda_i = \lambda^{A_i}$, que

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_{\Phi(M)} \end{pmatrix} = \begin{pmatrix} 1 & \lambda_1 & \lambda_1^2 & \cdots & \lambda_1^h \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \lambda_{h+1} & \lambda_{h+1}^2 & \cdots & \lambda_{h+1}^h \end{pmatrix} \begin{pmatrix} a_0 \\ \vdots \\ a_h \end{pmatrix}.$$

El determinante de la matriz $\left[\lambda_i^j\right]_{\substack{1 \leq i \leq h+1 \\ 0 \leq j \leq h}}$ es un determinante de Vandermonde, así que $\det\left[\lambda_i^j\right] = \prod_{1 \leq t < l \leq h+1} (\lambda_l - \lambda_t) = \Delta$. Luego

$$a_i = \frac{\det \begin{bmatrix} 1 & \lambda_1 & \cdots & \lambda_1^{i-1} & \alpha_1 & \lambda_1^{i+1} & \cdots & \lambda_1^h \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \lambda_{h+1} & \cdots & \lambda_{h+1}^{i-1} & \alpha_{h+1} & \lambda_{h+1}^{i+1} & \cdots & \lambda_{h+1}^h \end{bmatrix}}{\det \begin{bmatrix} 1 & \lambda_1 & \lambda_1^2 & \cdots & \lambda_1^h \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \lambda_{h+1} & \lambda_{h+1}^2 & \cdots & \lambda_{h+1}^h \end{bmatrix}} = \frac{b_i}{\Delta}$$

donde $b_i \in \vartheta_M$.
Por la demostración de la Proposición 18 (2.3), para toda $A \bmod (R_T/(M))^*$, tenemos

$$\lambda = \beta_A\lambda^A \text{ y } P = \beta_0\lambda^{\Phi(M)}$$

para algunos $\beta_A, \beta_0 \in \vartheta_M^*$. Entonces para cualquier divisor primo $\mathfrak{q}$ en $k(\lambda_M)$ que no divida a $\mathfrak{p}$ ni a $\mathfrak{p}_\infty$, tenemos

$$v_{\mathfrak{q}}(\lambda) = v_{\mathfrak{q}}(\lambda^A) = 0.$$

De esto se sigue que el soporte del divisor de polos de a_i puede consistir únicamente de $\mathfrak{p}$ y $\mathfrak{p}_\infty$. Puesto que $v_{\mathfrak{p}}(a_i) \geq 0$, tenemos que $a_i \in R_T$. Así $\vartheta_M = R_T[\lambda_M]$. ■

Otro resultado importante es la siguiente

Proposición 25. *Sean $M, N \in R_T \setminus \{0\}$ dos polinomios primos relativos. Entonces $\vartheta_M \vartheta_N = \vartheta_{MN}$.*

Demostración: Ver [12] Capítulo 12.■

Teorema 15. *Para cualquier $M \in R_T \setminus \{0\}$, sea $\lambda = \lambda_M$ un generador del R_T-módulo cíclico Λ_M. Entonces $\vartheta_M = R_T[\lambda]$.*

Demostración: Sea $M = \alpha P_1^{\alpha_1} \cdots P_h^{\alpha_h}$, donde $P_1, \ldots, P_h$ son polinomios mónicos irreducibles distintos en R_T. Usando las Proposiciones 24 y 25 obtenemos $\vartheta_M = \prod_{i=1}^{h} \vartheta_{P_i^{\alpha_i}} = \prod_{i=1}^{h} R_T[\lambda_{P_i^{\alpha_i}}] = R_T[\lambda]$. ■

2.3 Diferente y género

Sea $M \in R_T \setminus \{0\}$, M mónico, tal que $M \neq 1$. Sean $\mathfrak{D}_M$ el diferente de $k(\Lambda_M)/k$ y $g_{k(\Lambda_M)}$ el género de $k(\Lambda_M)$.

Proposición 26. *Sea $M = P^n$, P mónico irreducible, $d =$ gr P. Entonces $\mathfrak{D}_M = \mathfrak{p}^s \prod_{\mathfrak{B}|P_\infty} \mathfrak{B}^{q-2}$, donde $\mathfrak{p}$ es el único primo de $k(\Lambda_M)$ sobre P y $s = n\Phi(M) - q^{d(n-1)} = nq^{nd} - nq^{d(n-1)} - q^{d(n-1)} = nq^{nd} - (n+1)q^{d(n-1)}$ y $2g_{k(\Lambda_M)} - 2 = (dqn - dn - q)\left(\frac{\Phi(P^n)}{q-1}\right) - dq^{d(n-1)}$.*

Demostración: Se tiene que cualquier primo diferente a P y P_∞ es no ramificado. Por otro lado $e_\infty = q-1$, $f_\infty = 1$. Finalmente P es totalmente ramificado, por lo tanto $\mathfrak{D}_M = \mathfrak{p}^s \prod_{\mathfrak{B}|P_\infty} \mathfrak{B}^{q-2}$. Falta determinar s. Para ello calculemos $(\mathfrak{D}_M)_{\mathfrak{p}} = \mathfrak{D}_{k(\Lambda_M)_{\mathfrak{p}}/k_P} = \mathfrak{p}^s$. Tenemos $k(\Lambda_M)_{\mathfrak{p}}$ es generado sobre k_P por una raíz λ de $\Psi_{P^n}(u) = \frac{u^{P^n}}{u^{P^{n-1}}}$. Ahora, $\{\lambda^i\}_{i=0}^{\Phi(M)-1}$

es una base entera de $k(\Lambda_M)_{\mathfrak{p}}/k_P$ (pues $f = 1$ y λ es elemento primo), por lo tanto $(\mathfrak{D}_M)_{\mathfrak{p}} = (\Psi'_{P^n}(\lambda))_{\mathfrak{p}}$. Ahora, $u^{P^n} = u^{P^{n-1}}\Psi_{P^n}(u)$, $(u^{P^n})' = P^n = P^{n-1}\Psi_{P^n}(u) + u^{P^{n-1}}\Psi'_{P^n}(u)$ implica $P^n = \lambda^{P^{n-1}}\Psi'_{P^n}(\lambda)$, entonces $\Psi'_{P^n}(\lambda) = \dfrac{P^n}{\lambda^{P^{n-1}}}$. Ahora, $\lambda^{P^{n-1}} \in \Lambda_P$ y $\Psi_P(u) = \prod_{\substack{(A,P)=1 \\ \text{gr } A \leq \text{gr } P}} (u - \lambda_P^A)$, $\Psi_P(0) = P = \pm \prod_{\substack{(A,P)=1 \\ \text{gr } A \leq \text{gr } P}} \lambda_P^A =$(unidad)$\lambda_P^{\Phi(P)}$, lo que implica $((\lambda^{P^{n-1}})^{\Phi(P)}) = (P)$, entonces $\nu_{\mathfrak{p}_{\Lambda_{\mathfrak{p}}}}(\lambda^{P^{n-1}}) = \dfrac{\nu_{\mathfrak{p}_{\Lambda_{\mathfrak{p}}}}(P)}{\Phi(P)} = 1$, luego $\nu_{\mathfrak{p}}(\lambda^{P^{n-1}}) = e(k(\Lambda_{P^n})/k(\Lambda_P))\nu_{\mathfrak{p}_{\Lambda_{\mathfrak{p}}}}(\lambda^{P^{n-1}}) = \dfrac{\Phi(P^n)}{\Phi(P)}$. Entonces, $s = \nu_{\mathfrak{p}}(\Psi'_{P^n}(\lambda)) = \nu_{\mathfrak{p}}\left(\dfrac{P^n}{\lambda^{P^{n-1}}}\right) = n\nu_{\mathfrak{p}}(P) - \nu_{\mathfrak{p}}(\lambda^{P^{n-1}}) = n\nu_{\mathfrak{p}}(P) - \dfrac{\Phi(P^n)}{\Phi(P)} = n\Phi(P^n) - \dfrac{q^{nd} - q^{(n-1)d}}{q^d - 1} = n\Phi(P^n) - q^{(n-1)d}$.

Para el género se usa la Fórmula del Género de Riemann-Hurwitz (Ver [9] página 90) :

Sea L/k una extensión finita, separable y geométrica. Entonces

$$2g_L - 2 = [L : k](2g_k - 2) + \text{gr}\,\mathfrak{D}_{L/k}.$$

En nuestro caso tendremos $2g_{k(\Lambda_M)} - 2 = [k(\Lambda_M) : k](2g_k - 2) + \text{gr}\mathfrak{D}_{g_k(\Lambda_M)/k} = -2\Phi(M) + d(n\Phi(M) - q^{d(n-1)}) + \dfrac{\Phi(M)}{q-1}(q-2) = \dfrac{\Phi(M)}{q-1}(-2(q-1) + dn(q-1) + q - 2) - dq^{d(n-1)} = \dfrac{\Phi(M)}{q-1}((q-1)(-2+dn+1) - 1) - dq^{d(n-1)} = \dfrac{\Phi(M)}{q-1}((q-1)(dn-1) - 1) - dq^{d(n-1)} = \dfrac{\Phi(M)}{q-1}(qdn - q - dn) - dq^{d(n-1)}$. ■

Teorema 16 (Formulas del género y del diferente). *Sea $M \in R_T \setminus \mathbb{F}_q$, M mónico, $M = P_1^{\alpha_1} \cdots P_h^{\alpha_h}$ y sea $d_i = \text{gr } P_i$. Entonces se cumple que $\mathfrak{D}_M = \prod_{i=1}^{h}(\prod_{\mathfrak{p}|P_i} \mathfrak{p})^{s_i} \prod_{\mathfrak{B}|P_\infty} \mathfrak{B}^{q-2}$, donde $s_i = \alpha_i\Phi(P_i^{\alpha_i}) - q^{d_i(\alpha_i-1)}$ y $2g_{k(\Lambda_M)} - 2 = -2\Phi(M) + \sum_{i=1}^{h} d_i s_i \dfrac{\Phi(M)}{\Phi(P_i^{\alpha_i})} + (q-2)\dfrac{\Phi(M)}{q-1}$.*

Demostración: Para cada $1 \leq i \leq h$, en $k(\Lambda_M)/k(\Lambda_{P_i^{\alpha_i}})$, $\mathfrak{p}_i$ no es ramificado

y los primos encima de $\mathfrak{p}_i$ (de $k(\Lambda_{P_i^{\alpha_i}})/k$) son $\dfrac{\Phi(M)/\Phi(P_i^{\alpha_i})}{f_i}$ primos de grado de inercia f_i, por lo tanto en el diferente P_i contribuye con $\left(\prod_{\mathfrak{p}|P_i}\mathfrak{p}\right)^{s_i}$, el s_i es el de la proposición anterior y $\operatorname{gr}\prod_{\mathfrak{p}|P_i}\mathfrak{p} = d_i\dfrac{\Phi(M)/\Phi(P_i^{\alpha_i})}{f_i}f_i = d_i\dfrac{\Phi(M)}{\Phi(P_i^{\alpha_i})}$, de esto y de la Fórmula del Género de Riemann-Hurwitz se sigue el resultado.■

2.4 Máxima extensión abeliana A de k

Ahora estableceremos resultados análogos, en campos de funciones, al teorema de Kronecker-Weber.
El campo A consistirá de la composición de tres extensiones: E/k, K_T/k, y L_∞/k.

i) E/k es la únion de todas las extensiones de constantes de k. Más precisamente, como $k = \mathbb{F}_q(T)$, tenemos $E = \bigcup_{n=1}^{\infty}\mathbb{F}_{q^n}(T)$,

$$G_E = \operatorname{Gal}(E/k) = \operatorname{Gal}\left(\bigcup_{n=1}^{\infty}\mathbb{F}_{q^n}(T)/\mathbb{F}_q(T)\right) = \operatorname{Gal}(\varinjlim \mathbb{F}_{q^n}(T)/\mathbb{F}_q(T))$$

$$= \varprojlim \operatorname{Gal}\left(\mathbb{F}_{q^n}(T)/\mathbb{F}_q(T)\right) = \varprojlim \mathbb{Z}/n\mathbb{Z} = \widehat{\mathbb{Z}},$$

el cual es el anillo de Prüfer. Topológicamente, el grupo $G_E = \operatorname{Gal}(E/k)$ está generado por el automorfismo de Fröbenius, $\sigma : E \to E$ donde $u \mapsto u^q$, $G_E = \overline{\langle\sigma\rangle}$.

ii) K_T/k se define por $K_T = \bigcup_{M\in R_T} k(\Lambda_M)$, $\operatorname{Gal}\left(k(\Lambda_M)/k\right) \cong (R_T/(M))^*$ y

$$G_T = \operatorname{Gal}\left(K_T/k\right) = \operatorname{Gal}\left(\varinjlim_{M\in R_T}\left(k(\Lambda_M)/k\right)\right) \cong$$

$$\cong \varprojlim\left(\operatorname{Gal}\left(k(\Lambda_M)/k\right)\right) \cong \varprojlim (R_T/(M))^*.$$

Ahora bien, EK_T no puede ser la máxima extensión abeliana de k pues P_∞ es moderadamente ramificado en EK_T/k. Entonces necesitamos ciertas extensiones donde P_∞ sea salvajemente ramificado.

iii) Consideremos $T' = \dfrac{1}{T}$. Entonces $k = \mathbb{F}_q(T')$. Sea $F_n = k(\Lambda_{T^{-n-1}})$, $n \geq 1$. Se tiene que $[F_n : k] = q^n(q-1)$. Sea L_n el campo fijo por $\mathbb{F}_q^*$ contenido en F_n y sea $\lambda_{\frac{1}{T^{n+1}}}$ un generador del $R_{\frac{1}{T}} = \mathbb{F}_q\left[\dfrac{1}{T}\right]$-módulo $\Lambda_{T^{-n-1}}$. El único primo ramificado en L_n/k es P_∞ y es total y salvajemente ramificado. Entonces, si

$$L_\infty = \bigcup_{n=1}^{\infty} L_n = \lim_{\rightarrow} L_n, \text{ tenemos } G_\infty = \text{ Gal } (L_\infty/k) = \lim_{\leftarrow} \text{ Gal } (L_n/k)$$

$$\cong \{f\left(\frac{1}{T}\right) \in \mathbb{F}_q\left[\left[\frac{1}{T}\right]\right] | f(0) = 1\}.$$

Teorema 17. *La máxima extensión abeliana de k es $A = EK_TL_\infty$, su grupo de Galois es* Gal $(A/k) \cong G_E \times G_T \times G_\infty$, *donde* $G_E \cong \widehat{\mathbb{Z}} \cong \prod_{p \text{ primo}} \mathbb{Z}_p$; $G_T \cong \lim_{\substack{\leftarrow \\ M \in R_T}} (R_T/(M))^*$; $G_\infty \cong \{f\left(\dfrac{1}{T}\right) \in \mathbb{F}_q\left[\left[\dfrac{1}{T}\right]\right] | f(0) = 1\}$.

Demostración: Ver [4] página 25 o [11] página 281.■

2.5 Grupos de Galois de campos de funciones ciclotómicos

Determinaremos la estructura del grupo de Galois G_T. Para tal propósito obtendremos la estructura del grupo multiplicativo de unidades del R_T-módulo P^{p^t} para cualquier polinomio P mónico irreducible no constante en R_T y para cualquier $t \geq 1$. Aquí suponemos que P es un polinomio mónico irreducible no constante en R_T de grado d y $q = p^r$.

Teorema 18. *Si P es un polinomio irreducible en R_T y C_{q^d-1} es un grupo cíclico de orden q^d-1, entonces*

i) $(R_T/(P^p))^* \cong (\mathbb{Z}/p\mathbb{Z})^{\alpha_1} \times C_{q^d-1}$, *donde* $\alpha_1 = rd(p-1)$.

ii) Para cada entero positivo $t \geq 2$

$$(R_T/(P^{p^t}))^* \cong \prod_{i=1}^{t} (\mathbb{Z}/p^i\mathbb{Z})^{\alpha_i} \times C_{q^d-1},$$

donde $\alpha_i = rdp^{t-i-1}(p-1)^2$ *si* $1 \leq i \leq t-1$ *y* $\alpha_t = rd(p-1)$.

Demostración: Ver [4] página 36.■

Sea P un polinomio mónico irreducible no constante en R_T de grado d, tenemos que

$$\Lambda_P \subseteq \Lambda_{P^2} \subseteq \cdots \subseteq \Lambda_{P^n} \subseteq \cdots,$$

por lo tanto

$$k \subseteq k(\Lambda_P) \subseteq k(\Lambda_{P^2}) \subseteq \cdots \subseteq k(\Lambda_{P^n}) \subseteq \cdots,$$

es una torre de extensiones de campos. En particular, para cada $n \geq 1$ existe $t \geq 1$ tal que

$$k(\Lambda_{P^n}) \subseteq k(\Lambda_{P^{p^t}}).$$

Denotamos por $k(\Lambda_{P^\infty})$ la unión de los campos $k(\Lambda_{P^n})$, $n \geq 1$ y por $\mathbb{Z}_p^\infty$ al producto numerable de copias del anillo de enteros p-ádicos $\mathbb{Z}_p$. Se sigue que $\mathbb{Z}_p^\infty$ es un grupo profinito (ver [4] página 39).

Teorema 19. *Tenemos que* $\mathrm{Gal}\,(k(\Lambda_{P^\infty})/k) \cong \mathbb{Z}_p^\infty \times C_{q^d-1}$.

Demostración: Ver [4] página 39.■

Teorema 20. *Sea $\mathfrak{M}$ el conjunto de todos los polinomios mónicos irreducibles en R_T. Entonces,* $\mathrm{Gal}\,(K_T/k) \cong \mathbb{Z}_p^\infty \times \prod_{P\in\mathfrak{M}} C_{q^{d_P}-1}$ *donde $C_{q^{d_P}-1}$ es un grupo cíclico de orden $q^{d_P}-1$ con $d_P = \mathrm{gr}\,P$ para cada $P \in \mathfrak{M}$.*

Demostración: Ver [4] página 40.■

Capítulo 3

Caracteres de Dirichlet

En este capítulo se introducen los caracteres de Dirichlet, se relacionan con los caracteres de Galois (caracteres del grupo de Galois de un campo ciclotómico sobre $\mathbb{Q}$), lo que nos lleva al computo de los índices de ramificación vía caracteres. Se demuestra que dado cualquier grupo abeliano finito G, existe una extensión cíclica K de $\mathbb{Q}$ tal que el grupo de clases de ideales de K contiene un subgrupo isomorfo a G. Observamos que los conceptos y resultados del capítulo siguiente son, en buena parte, análogos a los de este capítulo y, hasta cierto punto, también las demostraciones. Elegimos presentar, en general, las demostraciones solamente en el Capítulo 4.

3.1 Caracteres de Dirichlet

Sea n un número natural. Un **caracter de Dirichlet** es un homomorfismo $\chi : U_n \to \mathbb{C}^*$. Decimos que χ está definido módulo n (mod n). Si $n|m$, definimos

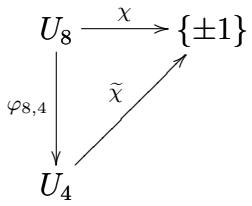
$$\varphi_{m,n} : U_m \to U_n$$

donde $x \bmod m \mapsto x \bmod n$. Si $\chi : U_n \to \mathbb{C}^*$ y $n|m$, tenemos $\chi \circ \varphi_{m,n}$ es un caracter módulo m y "casi" es el mismo que χ. Por lo tanto χ puede considerarse módulo n o módulo m. El mínimo n módulo el cual χ puede definirse se llama el **conductor** de χ y se denota por f_χ.

Ejemplos:

1) Sea $U_8 \cong \{1, 3, 5, 7\} \cong C_2 \times C_2$, $\chi : U_8 \mapsto \mathbb{C}^*$ con $\chi(1) = \chi(5) = 1$ y $\chi(3) = \chi(7) = -1$. Puesto que $\chi(a + 4) = \chi(a)$ para todo $a \in U_8$,

χ puede definirse módulo 4: $\widetilde{\chi} : U_4 = \{1,3\} = \{1,-1\}$, $\widetilde{\chi}(1) = 1$, $\widetilde{\chi}(-1) = -1$. El diagrama

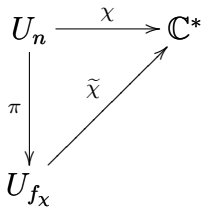


es conmutativo. Tenemos $f_\chi = 4$.

2) Consideremos $U_6 = \{1,5\} \cong U_3 = \{1,2\}$, $\chi : U_6 \to \mathbb{C}^*$, $\chi(1) = 1$, $\chi(5) = -1$, como tenemos el isomorfismo se puede definir $\chi : U_3 \to \mathbb{C}^*$, $\chi(1) = 1$, $\chi(2) = -1$, por lo tanto $f_\chi = 3$.

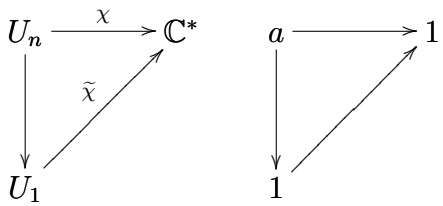
Observaciones:

1) Si $\chi : U_n \to \mathbb{C}^*$, es un caracter de Dirichlet, el conductor f_χ de χ, se definió como el mínimo f_χ tal que el diagrama



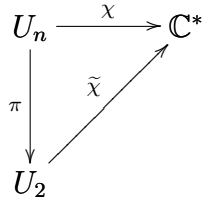
es conmutativo, esto es, $\chi = \widetilde{\chi} \circ \pi$, donde π es el epimorfismo natural; es decir, $f_\chi | n$ y $\pi : U_n \to U_{f_\chi}$, donde $x \bmod n \mapsto x \bmod f_\chi$. Observamos que el conductor f_χ de χ necesariamente divide a n.

2) Si $n = 1$, $U_1 = \{1\}$, $\chi : U_n \to \mathbb{C}^*, 1 \mapsto 1$ es el único caracter módulo 1 y χ es el **caracter trivial** para cualquier n : $(1|n)$



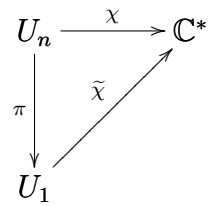
3) No puede haber un caracter de conductor 2.

Demostración: Supongamos que sí, es decir, sea χ un caracter de Dirichlet cuyo conductor f_χ es 2, entonces tenemos el siguiente diagrama



,

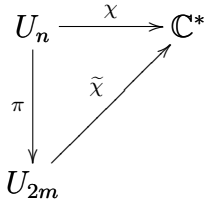
donde π es la proyección natural. Pero sabemos que $U_2 \cong U_1$. Es decir tendríamos



de donde χ es el caracter trivial, por lo que $f_\chi = 1$, lo cual no puede ser. Luego, no puede haber un caracter de Dirichlet cuyo conductor sea 2.■

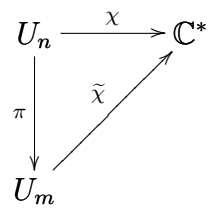
4) No puede haber un caracter de conductor $2m$ con m impar.

Demostración: Por contradicción supongamos que χ es un caracter de Dirichlet cuyo conductor f_χ es $2m$, con m impar entonces tenemos el siguiente diagrama



,

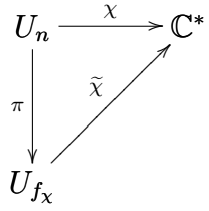
donde π es la proyección natural. Por otro lado sabemos que $U_{2m} \cong U_m$ para m impar. Luego tendríamos



implicaría que f_χ es m lo cual no puede ser. Luego, no puede haber un caracter de Dirichlet cuyo conductor sea $2m$ con m impar.■

5) Sean χ, φ dos caracteres de Dirichlet de conductores f_χ, f_φ. Supongamos que existe un n tal que $f_\chi | n$, $f_\varphi | n$ y $\chi, \varphi : U_n \to \mathbb{C}^*$ son iguales módulo n (es decir, $\chi(a \bmod n) = \varphi(a \bmod n)$, para todo a, $(a, n) = 1$). Entonces $\chi \equiv \varphi$ (es decir: $f_\chi = f_\varphi$ y $\varphi = \chi \bmod f_\chi$).

Demostración: Consideremos



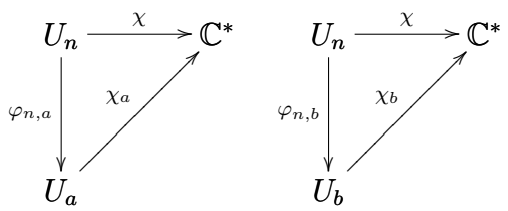
Tenemos $\widetilde{\chi} \circ \pi = \chi = \varphi$, $\widetilde{\varphi} \circ \pi = \varphi = \chi$, es decir, φ se puede definir módulo f_χ, lo cual implica $f_\varphi | f_\chi$. Por simetría $f_\chi | f_\varphi$, por lo tanto $f_\chi = f_\varphi$. ■

Definición 1. *Sea* $\chi : U_n \to \mathbb{C}^*$. *Si* $\chi(-1) = 1$, χ *se llama* **par**, *y si* $\chi(-1) = -1$, χ *se llama* **impar**.

Observación: En los dos ejemplos anteriores χ fue un caracter impar.

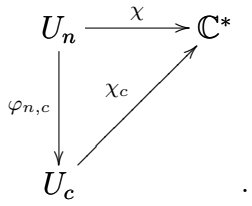
A veces es conveniente considerar un caracter $\chi : \mathbb{Z} \to \mathbb{C}$ si definimos $\chi(a) = 0$ para $a \in \mathbb{Z}$, $(a, f_\chi) \neq 1$ (χ así definido **no** es homomorfismo). Por tanto es importante hacer la convención con respecto al módulo de definición de χ, se considerará χ definido módulo su conductor. Tales caracteres (definidos módulo f_χ) se llaman **primitivos** (es decir, hacer $\chi(a) = 0$ tan poco como sea posible) y notemos que χ es periódico de **período** f_χ, es decir $\chi(a + f_\chi) = \chi(a)$ para todo $a \in \mathbb{Z}$.

Observación: Existencia del conductor. Sea $\chi : U_n \to \mathbb{C}^*$ un caracter de Dirichlet y sean $a|n$ y $b|n$ tales que $\chi = \chi_a \circ \varphi_{n,a} = \chi_b \circ \varphi_{n,b}$,



.

Sea $c = (a, b)$, sea d el producto de todos los primos p que dividen a n pero que no dividen a b, por lo tanto $c = (da, b)$.
Sean $x, y \in \mathbb{Z}$, $(x, n) = 1 = (y, n)$ y $x \equiv y \bmod c$. Existe $\alpha \in \mathbb{Z}$, $\alpha \equiv x \bmod da$, $\alpha \equiv y \bmod b$. Se verifica que $(\alpha, n) = 1$, $\chi(\alpha) = \chi_a \circ \varphi_{n,a}(\alpha) = \chi_{da} \circ \varphi_{n,da}(\alpha) = \chi_{da} \circ \varphi_{n,da}(x) = \chi(x)$, $\chi(\alpha) = \chi_b \circ \varphi_{n,b}(\alpha) = \chi_b \circ \varphi_{n,b}(y) = \chi(y)$, por lo tanto $\chi(x) = \chi(\alpha) = \chi(y)$, lo cual implica $\chi(x) = \chi(y)$, luego $\chi(x)$ se puede definir módulo c,



.

Observación: En el ejemplo 2), $\chi : U_6 \to \mathbb{C}^*$, $\chi(1) = 1$ y $\chi(5) = -1$, pero χ no tiene período 3 (y su conductor es 3), pues $\chi(1) = 1 \neq 0 = \chi(1+3) = \chi(4)$ módulo 6.

Cuando se hable de caracteres de U_n o de caracteres módulo n se incluirán los caracteres de conductores que dividen a n.
El caracter trivial es el caracter de conductor 1 y este es $\chi : \mathbb{Z} \to \mathbb{C}$, $\chi(a) = 1$ para todo $a \in \mathbb{Z}$.
Sean χ, ψ dos caracteres de conductores f_χ, f_ψ. Sea $\gamma : U_{[f_\chi, f_\psi]} \to \mathbb{C}^*$ donde $\gamma(a) = \chi(a)\psi(a)$. Entonces $\chi\psi$ es el caracter <u>primitivo</u> asociado a γ (γ no tiene por qué ser primitivo).

Ejemplos :

3) Sean $\chi : U_{12} \to \mathbb{C}^*$ donde $U_{12} = \{1, 5, 7, 11\}$, $\chi(1) = \chi(11) = 1$, $\chi(5) = \chi(7) = -1$ y $\psi : U_3 \to \mathbb{C}^*$ con $U_3 = \{1, 2\}$, $\psi(1) = 1$, $\psi(2) = -1$, $[f_\chi, f_\psi] = 12$,

$$\begin{array}{ccccc} & & \underline{\psi \bmod 12} & & \\ U_{12} & \to & U_3 & \to & \mathbb{C}^* \\ 1 & \mapsto & 1 & \mapsto & 1 \\ 5 & \mapsto & 2 & \mapsto & -1 \\ 7 & \mapsto & 1 & \mapsto & 1 \\ 11 & \mapsto & 2 & \mapsto & -1. \end{array}$$

Es decir ψ módulo 12: $\psi(1) = \psi(7) = 1$, $\psi(5) = \psi(11) = -1$. Ahora, $\gamma : U_{12} \to \mathbb{C}^*$,

$$\gamma(a) = \chi(a)\psi(a) = \begin{cases} 1 & a = 1 \\ 1 & a = 5 \\ -1 & a = 7 \\ -1 & a = 11. \end{cases}$$

Observamos

$$\begin{array}{ccccc} U_{12} & \to & U_4 & \to & \mathbb{C}^* \\ 1 & \mapsto & 1 & \mapsto & 1 \\ 5 & \mapsto & 1 & \mapsto & 1 \\ 7 & \mapsto & 3 & \mapsto & -1 \\ 11 & \mapsto & 3 & \mapsto & -1, \end{array}$$

con $U_{12} \to \mathbb{C}^*$, por lo tanto $\chi\psi : U_4 \to \mathbb{C}^*$, $(1 \mapsto 1,\ 3 \mapsto -1)$ es el producto y $f_{\chi\psi} = 4$. Nótese que $(\chi\psi)(3) = -1 \neq \chi(3)\psi(3)$.

4) Sea $\chi : U_n \to \mathbb{C}^*$ arbitrario y sea $\psi = \overline{\chi}$, $\psi(a) = \overline{\chi(a)} = \chi(a)^{-1}$ (pues $\chi(U_n) \subseteq$ raíces de 1) para $(a, f_\chi) = 1$, luego $\chi\overline{\chi}$ es el caracter trivial (es decir, $\chi\overline{\chi}(a) = 1$ para todo $a \in \mathbb{Z}$).

5) Si $(f_\chi, f_\psi) = 1$, entonces $f_{\chi\psi} = f_\chi f_\psi$. La demostración de este resultado se puede ver en el capítulo siguiente.

Los caracteres de Dirichlet se pueden pensar como caracteres de

$$\mathrm{Gal}\,(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong U_n$$

(y se llaman, en este caso, **caracteres de Galois**).
Ejemplo:

6) Consideramos $\chi : U_8 \to \mathbb{C}^*$ $(1, 5 \mapsto 1$ y $3, 7 \mapsto -1)$, $\ker\chi = \{1, 5 \mathrm{mod} 8\}$, este grupo es el grupo de Galois de $\mathbb{Q}(\zeta_8)/\mathbb{Q}(\zeta_4)$ pues $\mathrm{Gal}\,(\mathbb{Q}(\zeta_8)/\mathbb{Q}(\zeta_4))$ $\cong D_{8,4} = \{x \bmod 8 | x \equiv 1 \bmod 4\} = \{1, 5 \bmod 8\}$, por lo tanto χ es un caracter de

$$\frac{\mathrm{Gal}\ (\mathbb{Q}(\zeta_8)/\mathbb{Q})}{\mathrm{Gal}\ (\mathbb{Q}(\zeta_8)/\mathbb{Q}(\zeta_4))} \cong \mathrm{Gal}\ (\mathbb{Q}(\zeta_4)/\mathbb{Q}) \cong U_4,$$

$\chi : U_4 \to \mathbb{C}^*$ $(1 \mapsto 1,\ 3 \mapsto -1)$.

En general, sea χ un caracter módulo n, χ es un caracter de Gal $(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Sea $K = \mathbb{Q}(\zeta_n)^{\ker \chi} \subseteq \mathbb{Q}(\zeta_n)$. Tenemos K sólo depende de χ y se llama el **campo perteneciente a** χ. Si n es minimal, $n = f_\chi$. Más generalmente, si X es un grupo finito de caracteres de Dirichlet, sea $n := \text{m.c.m.}\{f_\chi | \chi \in X\}$. Así $X \subseteq$ caracteres de Gal $(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Sean $H := \bigcap_{\chi \in X} \ker \chi \subseteq U_n$ y $K = \mathbb{Q}(\zeta_n)^H$, K es el **campo perteneciente a** X. Entonces X es el conjunto de homomorfismos $\text{Gal}\,(K/\mathbb{Q}) \to \mathbb{C}^*$ y $[K : \mathbb{Q}] = |X|$, de hecho $X \cong \text{Gal}\,(K/\mathbb{Q})$ (véase el Corolario 8). Si X es cíclico generado por χ, entonces K es el campo perteneciente a χ.

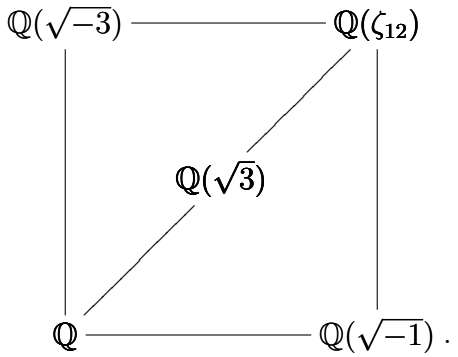
Ejemplos:

7) Sea X el grupo de caracteres de U_n tales que $\chi(-1) = 1$. Entonces $(\zeta_n \mapsto \zeta_n^{-1})$ está en el núcleo de cada $\chi \in X$, por lo tanto

$$\bigcap_{\chi \in X} \ker \chi = \langle J \rangle = \{\pm 1\},$$

$K = \mathbb{Q}(\zeta_n)^{\langle J \rangle} = \mathbb{Q}(\zeta_n)^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$. Por lo tanto el campo asociado a X es $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(\zeta_n)^+$. Similarmente, si χ es cualquier caracter, entonces el campo K que pertenece a χ satisface $K \subseteq \mathbb{R}$ si y sólo si $(\zeta_n \to \zeta_n^{-1}) \in \ker \chi$ si y sólo si $\chi(-1) = 1$.

8) Sea $\chi : U_{12} \to \mathbb{C}^*$ con $(1, 11 \mapsto 1; 5, 7 \mapsto -1)$ tenemos $\mathbb{Q}(\zeta_{12}) = \mathbb{Q}(\zeta_3)\mathbb{Q}(\zeta_4) = \mathbb{Q}(\sqrt{-3})\mathbb{Q}(\sqrt{-1})$

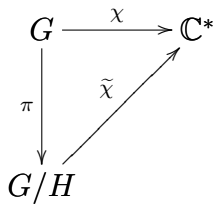


El campo K que pertenece a χ es una extensión cuadrática de $\mathbb{Q}$.

Además esta extensión es real ($\chi(-1) = 1$) por lo tanto $K = \mathbb{Q}(\sqrt{3})$. Otra forma: los otros campos cuadráticos $\mathbb{Q}(\zeta_3)/\mathbb{Q}$ y $\mathbb{Q}(\zeta_4)/\mathbb{Q}$ tienen conductor 3 y 4 respectivamente pero $f_\chi = 12 \neq 3, 4$.■

Recordemos que si G es un grupo abeliano finito y $\widehat{G} = \{f : G \to \mathbb{C}^* | \ f \text{ es caracter}\}$, entonces $\widehat{G} \cong G$ (isomorfismo no canónico) pero lo que sí tenemos es $\widehat{\widehat{G}} \cong G$ (isomorfismo canónico, si $g \in G$, $\widehat{g} : \widehat{G} \to \mathbb{C}^*$ está dado por $\widehat{g}(\chi) := \chi(g)$). De hecho tenemos un pareo (esto es, se respeta la operación en cada entrada, como en las funciones bilineales), $\varphi : G \times \widehat{G} \to \mathbb{C}^*$ donde $(g, \chi) \mapsto \langle g, \chi \rangle = \chi(g)$. Si $\langle g, \chi \rangle = 1$ para todo χ, entonces $\chi(g) = 1$ para todo $\chi \in \widehat{G}$. Sea $H = \langle g \rangle$. Entonces $\widehat{G}$ actúa como un conjunto de caracteres distintos de G/H pero hay a lo más $|G/H|$ de tales caracteres por lo tanto $|G/H| \geq |\widehat{G}| = |G|$, luego $|H| = 1$, entonces $g = 1$. Si $\langle g, \chi \rangle = 1$ para toda $g \in G$, entonces $\chi(g) = 1$ para toda $g \in G$, lo cual implica $\chi = 1$, por lo tanto φ es no degenerado.

Sea $H < G$ y sea $H^\perp = \{\chi \in \widehat{G} | \chi(h) = 1 \text{ para todo } h \in H\}$. Se tiene: $H^\perp \cong \widehat{(G/H)}$ pues toda $\chi \in H^\perp$



se factoriza, como en el diagrama, de manera única y viceversa. También, si $\mathcal{H} < \widehat{G}$, definimos $\mathcal{H}^\perp = \{g \in G | \chi(g) = 1 \text{ para todo } \chi \in \mathcal{H}\}$.

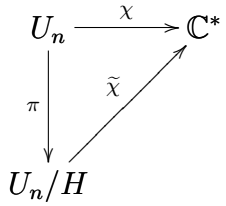
Proposición 27. $\widehat{H} \cong \widehat{G}/H^\perp$.

Demostración: Ver el siguiente capítulo o [14] página 23.■

Proposición 28. *Con la identificación* $\widehat{\widehat{G}} \cong G$, *se tiene* $(H^\perp)^\perp = H$.

Demostración: Ver el siguiente capítulo o [14] página 23.■

Sea X el grupo de caracteres de Dirichlet asociado a un campo K, es decir $K = \mathbb{Q}(\zeta_n)^H$, $H = \bigcap_{\chi \in X} \ker \chi$. Sea $\varphi : \mathrm{Gal}\,(K/\mathbb{Q}) \times X \to \mathbb{C}^*$ dado por $(\sigma, \chi) \mapsto \chi(\sigma)$, $\sigma \in \mathrm{Gal}\,(K/\mathbb{Q}) \cong U_n/H$. Si $\chi : U_n \to \mathbb{C}^*$, entonces $H \subseteq \ker \chi$, por lo tanto $\chi(H) = 1$, luego χ se factoriza:



Proposición 29. *El pareo φ es no degenerado, es decir, $\chi(\sigma) = 1$ para todo $\chi \in X$ implica $\sigma = \mathrm{id}_K$ y si $\chi(\sigma) = 1$ para todo $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, entonces $\chi = 1$.*

Demostración: Ver el siguiente capítulo o [14] página 23.■

Corolario 8. *Se tiene $X \cong \widehat{G} = \widehat{\mathrm{Gal}\,(K/\mathbb{Q})}$ y $|X| = [K : \mathbb{Q}]$.*

Demostración: Ver el siguiente capítulo o [14] página 23.■

Ahora, sean $L \subseteq K$, $\varphi : \mathrm{Gal}\,(K/\mathbb{Q}) \times X \to \mathbb{C}^*$ donde $\varphi((\sigma, \chi)) = \langle \sigma, \chi \rangle = \chi(\sigma)$. Si $Y = \{\chi \in X | \chi(g) = 1 \text{ para todo } g \in \mathrm{Gal}\,(K/L)\}$, entonces

$$Y \cong \mathrm{Gal}\,(K/L)^\perp \cong (G/\widehat{\mathrm{Gal}\,(K/L)}) \cong \widehat{\mathrm{Gal}\,(L/\mathbb{Q})}.$$

Recíprocamente, si $Y < X$, sea $L = K^{Y^\perp}$, donde

$$Y^\perp = \{g \in G | \chi(g) = 1 \text{ para todo } \chi \in Y\},$$

luego $\mathrm{Gal}\,(K/L) \cong \mathrm{Gal}\,(K/K^{Y^\perp}) \cong Y^\perp$, por lo tanto

$$Y = Y^{\perp\perp} = \mathrm{Gal}\,(K/L)^\perp \cong \widehat{\mathrm{Gal}\,(L/\mathbb{Q})}.$$

Se tiene también $Y \cong \widehat{\mathrm{Gal}\,(L/\mathbb{Q})} \cong \mathrm{Gal}\,(L/\mathbb{Q})$. El primer isomorfismo se expresa a través del pareo $\mathrm{Gal}\,(L/\mathbb{Q}) \times Y \to \mathbb{C}^*$ donde $(g, \chi) \mapsto \chi(g)$.

Proposición 30. *Existe una biyección entre los subgrupos de X y los subcampos de K, dada por:* $\begin{cases} \text{subgrupos de } X & & \text{subcampos de } K \\ Y & \mapsto & K^{Y^\perp} \\ \text{Gal}\,(K/L)^\perp & \hookleftarrow & L. \end{cases}$

Demostración: Ver el siguiente capítulo o [14] página 24.■

Lema 2. *Sean $G_1, G_2 < G$. Si $G_1 \subseteq G_2$, entonces $G_2^\perp \subseteq G_1^\perp$.*

Demostración: Tenemos $\chi \in G_2^\perp$ implica $\chi \in \widehat{G}$ y $\chi(g) = 1$ para todo $g \in G_2$ entonces $\chi \in \widehat{G}$ y $\chi(g) = 1$ para todo $g \in G_1$, luego $\chi \in G_1^\perp$.■

Por otro lado tenemos el siguiente

Lema 3. *Sea X_i correspondiente a K_i, $i = 1, 2$. Entonces:*

i) $X_1 \subseteq X_2$ si y sólo si $K_1 \subseteq K_2$.

ii) $\langle X_1, X_2 \rangle$ corresponde a $K_1 K_2$.

Demostración: Ver el siguiente capítulo.■

3.2 Cómputo de los índices de ramificación vía caracteres

Sea $n = p_1^{\alpha_1} \cdots p_h^{\alpha_h}$. Tenemos

$$U_n \cong \prod_{i=1}^{h} U_{p_i^{\alpha_i}},$$

por lo tanto, si $\chi : U_n \to \mathbb{C}^*$, entonces $\chi = \prod_{i=1}^{h} \chi_{p_i}$, donde $\chi_{p_i} : U_{p_i^{\alpha_i}} \to \mathbb{C}^*$, $\chi_{p_i} = \chi \circ \Phi^{-1} \circ g_i$, $\Phi : U_n \to \prod_{i=1}^{h} U_{p_i^{\alpha_i}}$ y $g_i : U_{p_i^{\alpha_i}} \to \prod_{i=1}^{h} U_{p_i^{\alpha_i}}$ donde $a \mapsto (1, \ldots, 1, a, 1, \ldots, 1)$. En efecto, si $a \in \mathbb{Z}$, $(a, n) = 1$,

$$\chi_{p_i}(a) = \chi(\Phi^{-1}(g_i(a \bmod n))) = \chi\Phi^{-1}((1, \ldots, 1, a, 1, \ldots, 1)) = \chi(b_i)$$

donde $b_i \equiv 1 \bmod p_j^{\alpha_j}$, $j \neq i$, $b_i \equiv a \bmod p_i^{\alpha_i}$, luego $(\prod_{i=1}^{h} \chi_{p_i})(a) = \prod_{i=1}^{h} \chi_{p_i}(a) = \prod_{i=1}^{h} \chi(b_i) = \chi(\prod_{i=1}^{h} b_i) = \chi(a)$.

Para X un conjunto de caracteres de Dirichlet y p un primo racional se denota: $X_p = \{\chi_p | \chi \in X\}$.

Ejemplo:

9) Consideremos $\chi : U_{12} \to \mathbb{C}^*$ ($\chi(1) = \chi(11) = 1$, $\chi(5) = \chi(7) = -1$). Tenemos $\chi = \chi_2\chi_3$, donde $\chi_2 : U_4 \to \mathbb{C}^*$ y $\chi_3 : U_3 \to \mathbb{C}^*$,

$$\Phi^{-1} \circ g_2 : U_4 \to U_3 \times U_4 \cong U_{12},$$

donde $1 \mapsto (1,1) \mapsto 1$, $3 \mapsto (1,3) = (7,7) \mapsto 7$ (pues $7 \equiv 1 \bmod 3$, $7 \equiv 3 \bmod 4$),

$$\Phi^{-1} \circ g_3 : U_3 \to U_{12},$$

donde $\Phi^{-1}(g_3(1)) = 1$, $\Phi^{-1}(g_3(2)) = 5$. Luego

$$\chi_2 = \chi \circ \Phi^{-1} \circ g_2,$$

está dado por $\chi_2(1) = 1$, $\chi_2(3) = \chi(7) = -1$,

$$\chi_3 = \chi \circ \Phi^{-1} \circ g_3,$$

está dado por $\chi_3(1) = 1$, $\chi_3(2) = \chi(5) = -1$. Si $X = \langle\chi\rangle$, entonces $X_2 = \langle\chi_2\rangle$, $X_3 = \langle\chi_3\rangle$, y $X_p = \{1\}$ si $p \neq 2, 3$.

Teorema 21. *Sea X un grupo de caracteres de Dirichlet y sea K el campo perteneciente a X. Sea p un primo racional y sea e su índice de ramificación en $K/\mathbb{Q}$. Entonces $e = |X_p|$.*

Demostración: Ver el siguiente capítulo o [14] página 24.■

Ejemplo:

10) Consideremos $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$. Como $3 \equiv 3 \mod 4$, el discriminante de $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ es $\delta(\mathbb{Q}(\sqrt{3})) = 12$ luego 2 y 3 son los únicos primos ramificados. Sea $\chi \bmod 12$, correspondiente a $\mathbb{Q}(\sqrt{3})$, $\chi : U_{12} \to \mathbb{C}^*$ ($1, 11 \mapsto 1$, $5, 7 \mapsto -1$). Tenemos $\chi = \chi_2\chi_3$ y si $X = \langle\chi\rangle$, entonces $X_2 = \{1, \chi_2\}$, $X_3 = \{1, \chi_3\}$. Luego $e_2 = 2$ y $e_3 = 2$.

Corolario 9. *Sean χ un caracter de Dirichlet y K el campo perteneciente a χ. Entonces p se ramifica en K si y sólo si $\chi(p) = 0$ (si y sólo si $p|f_\chi$). Más generalmente, sea L el campo perteneciente a un grupo de caracteres de Dirichlet X. Entonces p es no ramificado en $L/\mathbb{Q}$ si y sólo si $\chi(p) \neq 0$ para todo $\chi \in X$.*

Demostración: Ver el siguiente capítulo o [14] página 25.■

Teorema 22. *Sean X un grupo de caracteres de Dirichlet, K el campo perteneciente a X. Sean p un primo racional, $Y = \{\chi \in X | \chi(p) \neq 0\}$, $Z = \{\chi \in X | \chi(p) = 1\}$ ($Z < Y < X$). Entonces $e = [X : Y]$, $f = [Y : Z]$, $g = [Z : 1]$ son el índice de ramificación, el grado relativo y el número de primos arriba de p en $K/\mathbb{Q}$. De hecho, X/Y es isomorfo al grupo de inercia, X/Z es isomorfo al grupo de descomposición, Y/Z es un grupo cíclico de orden f el cual es isomorfo al grupo de Galois de la extensión de campos residuales.*

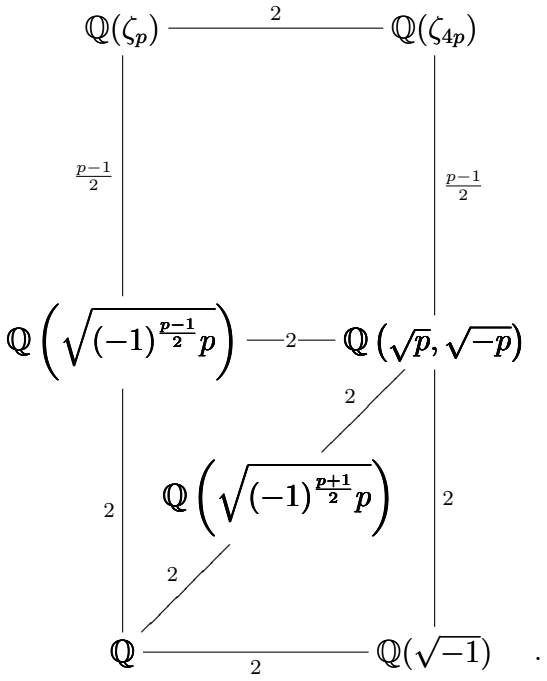
Demostración: Ver el siguiente capítulo o [14] página 25.■

Ejemplo:

11) Sea p primo, $p > 2$ y sea $K = \mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right) \subseteq \mathbb{Q}(\zeta_p)$, sean $\chi : U_p \to \mathbb{C}^*$ el caracter asociado a K y $X = \langle\chi\rangle$. Puesto que $|X| = [K : \mathbb{Q}] = 2$, tenemos $\chi^2 = 1$, $\chi \neq 1$, $f_\chi = p$ y $\chi(U_p) = \{\pm 1\}$, $K = \mathbb{Q}(\zeta_p)^{\ker\chi}$ donde $\ker\chi = \{\sigma \in \mathrm{Gal}\,(\mathbb{Q}(\zeta_p)/\mathbb{Q}) | \chi(\sigma) = 1\}$. Sea q cualquier primo racional $q \neq p$. Se tiene que q se descompone en $K/\mathbb{Q}$ si y sólo si $|Z| = 2$ ($Z = \{\varphi \in X | \varphi(q) = 1\}$) por lo tanto q se descompone en $K/\mathbb{Q}$ si y sólo si $\chi(q) = 1$. Ahora, si $q \equiv a^2 \bmod p$, $\chi(q) = \chi(a)^2 = 1$, luego $q \in \ker\chi$ y puesto que $|\ker\chi| = \dfrac{|U_p|}{2} = \dfrac{p-1}{2} = |\{t \in U_p | t = a^2\}|$, tenemos $\ker\chi = \{t \in U_p | t = a^2\}$, luego $\chi(q) = 1$ si y sólo si $q \equiv a^2 \mathrm{mod} p$ si y sólo si $\left(\dfrac{q}{p}\right) = 1$, por lo tanto $\chi(q) = \left(\dfrac{q}{p}\right)$.

En resumen $\mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right)$ corresponde a $\chi = \left(\dfrac{-}{p}\right)$, el símbolo de Legendre.

Es natural hacerse la siguiente pregunta:
¿A cuál caracter corresponde el campo $\mathbb{Q}\left(\sqrt{(-1)^{\frac{p+1}{2}}p}\right)$?



.

Sean $\chi : U_p \to \mathbb{C}^*$ con $\chi(q) = \left(\frac{q}{p}\right)$ y $\varphi : U_4 \to \mathbb{C}^*$, donde $\varphi(-1) = -1$, por lo que

$$\varphi(q) = \left\{ \begin{array}{rcl} 1 & \text{si} & q \equiv 1 \bmod 4 \\ -1 & \text{si} & q \equiv 3 \bmod 4 \\ & & \equiv -1 \bmod 4 \end{array} \right\} = (-1)^{\frac{q-1}{2}}.$$

Por tanto $\mathbb{Q}\left(\sqrt{(-1)^{\frac{p+1}{2}}p}\right)$ corresponde a $\chi\varphi$, $(\chi\varphi)(q) = (-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right)$ el conductor de $\chi\varphi$ es $4p = \left|\operatorname{disc}\mathbb{Q}\left(\sqrt{(-1)^{\frac{p+1}{2}}p}\right)\right|$.

Proposición 31. *Sea G un grupo abeliano finito. Entonces existen campos numéricos E y K tales que*

a) $\operatorname{Gal}(E/K) \cong G$,

b) E/K es no ramificada en todos los primos incluyendo a los primos infinitos.

Se puede escoger $E/\mathbb{Q}$ abeliana y $K/\mathbb{Q}$ cíclica.

Demostración: Sea $G = C_{n_1} \times \cdots \times C_{n_h}$ y sean $p_1, \ldots, p_h$ primos distintos tales que $p_i \equiv 1 \bmod 2n_i$, tenemos

$$\mathrm{Gal}\,(\mathbb{Q}(\zeta_{p_i})/\mathbb{Q}) \cong C_{p_i-1}.$$

Si ψ_i es un generador de $\widehat{U}_{p_i}(\cong C_{p_i-1})$, ψ_i es un caracter de conductor p_i y orden $p_i - 1$. Sea $\chi_i = \psi_i^{\frac{p_i-1}{n_i}}$. Tenemos $o(\chi_i) = n_i$, $f_{\chi_i} = p_i$ y como 2 divide a $\dfrac{p_i-1}{n_i}$, $\chi_i(-1) = 1$. Sea p_{h+1} otro primo impar y sea χ_{h+1} un caracter de conductor p_{h+1} y $\chi_i(-1) = -1$ (por ejemplo $\chi_{h+1} = \psi_{h+1}$ pues $\psi_i(-1) = -1$). Sea $\chi = \chi_1\chi_2\cdots\chi_h\chi_{h+1}$, pedimos que $n_1 \cdots n_h$ divida a $o(\chi_{h+1})$ (por ejemplo, $p_{h+1} \equiv 1 \bmod n_1 \cdots n_h$). Sea K el campo perteneciente a χ. Entonces $K/\mathbb{Q}$ es cíclica, pues

$$\mathrm{Gal}\,(K/\mathbb{Q}) \cong \langle\chi\rangle.$$

Ahora bien,

$$\chi(-1) = \chi_1(-1)\chi_2(-1)\cdots\chi_h(-1)\chi_{h+1}(-1) = 1\cdots 1(-1) = -1,$$

por lo tanto K es complejo, luego toda extensión de K es no ramificada en los primos infinitos. Sea $X = \langle\chi_1, \chi_2, \ldots, \chi_h, \chi_{h+1}\rangle$ y sea E el campo perteneciente a X. Por lo tanto $E/\mathbb{Q}$ es abeliana. Ahora bien, $f_{\chi_i} = p_i$ implica que $X_{p_i} = \langle\chi_i\rangle$, $1 \le i \le h+1$ y $X_p = \langle\chi\rangle_p = 1$ para todo $p \notin \{p_1, \ldots, p_h, p_{h+1}\}$, $e_{p_i}(E/\mathbb{Q}) = |X_{p_i}| = |\langle\chi_i\rangle|$ y como

$$e_{p_i}(K/\mathbb{Q}) = |\langle\chi_i\rangle|,$$

tenemos $e_{p_i}(E/K) = 1$, luego E/K es no ramificada en ningún primo. Ahora, $X = \langle\chi_1, \chi_2, \ldots, \chi_h, \chi_{h+1}\rangle = \langle\chi_1, \chi_2, \ldots, \chi_h, \chi\rangle$, pues

$$\chi = \chi_1\chi_2\cdots\chi_h\chi_{h+1}.$$

Tenemos

$$\mathrm{Gal}(E/K) \cong \widehat{\mathrm{Gal}(E/K)} \cong \widehat{\mathrm{Gal}(E/\mathbb{Q})}/\widehat{\mathrm{Gal}(E/K)}^{\perp} \cong X/\langle\chi\rangle$$

y

$$\langle \chi_1, \chi_2, \ldots, \chi_h \rangle \cong \bigoplus_{i=1}^{h} \langle \chi_i \rangle \cong \bigoplus_{i=1}^{h} \langle \psi_i^{\frac{p_i-1}{n_i}} \rangle \cong \bigoplus_{i=1}^{h} C_{n_i} \cong G.$$

Sea $\varphi : \langle \chi_1, \chi_2, \ldots, \chi_h \rangle \to X/\langle \chi \rangle$. Puesto que

$$X = \langle \chi_1, \chi_2, \ldots, \chi_h, \chi_{h+1} \rangle,$$

φ es suprayectiva. Si $\chi_1^{\alpha_1} \cdots \chi_h^{\alpha_h} \in \ker \varphi$, entonces $\chi_1^{\alpha_1} \cdots \chi_h^{\alpha_h} = \chi^{\alpha} = \chi_1^{\alpha} \cdots \chi_h^{\alpha} \chi_{h+1}^{\alpha}$ por lo tanto $\chi_{h+1}^{\alpha} = 1$ y $\alpha_i \equiv \alpha \bmod n_i$, habíamos pedido que $n_1 \cdots n_h$ divida a $o(\chi_{h+1})$ lo que implica que $n_1 \cdots n_h$ divide a α, por lo que n_i divide a α_i, que a su vez implica $\chi_i^{\alpha_i} = 1$, $i = 1, \ldots, h$, por tanto φ es inyectiva y

$$\langle \chi_1, \chi_2, \ldots, \chi_h \rangle \cong X/\langle \chi \rangle.$$

Concluimos Gal $(E/K) \cong G$.■

Nota: En la Proposición, E es la máxima extensión abeliana de $\mathbb{Q}$ no ramificada sobre K.

Ahora describiremos los campos de clases de Hilbert. Sean K un campo numérico y Cl (K) su grupo de clases. Sea L la máxima extensión abeliana no ramificada (incluyendo a ∞) de K. Se llama a L el **campo de clases de Hilbert de** K. Se tiene que L/K es Galois, finita y Gal $(L/K) \cong$ Cl (K), denotamos a L por H_K.
Un resultado fundamental de la teoría de campos de clases dice lo siguiente:

Teorema 23. *Si K es un campo de números y H_K es el campo de clases de Hilbert, entonces*

$$\text{Gal}\,(H_K/K) \cong \text{Cl}\,(K).$$

Además, como H_K contiene cualquier extensión abeliana no ramificada de K, entonces para una torre de campos $K \subseteq F \subseteq H_K$, $[F : K]$ divide a $h_K = [H_K : K]$.

Demostración: Ver [7] página 249.■

Lema 4. *Si A es un grupo abeliano finito y $B < A$, entonces A contiene un subgrupo isomorfo a A/B.*

Demostración: Directa de la estructura de los grupos abelianos finitamente generados o bien $A/B \cong \widehat{(A/B)} \cong B^{\perp} \subseteq \widehat{A} \cong A$.■

Teorema 24. *Dado cualquier grupo abeliano finito G, existe una extensión cíclica K de $\mathbb{Q}$ tal que el grupo de clases de ideales de K contiene un subgrupo isomorfo a G.*

Demostración: Por la Proposición 31, existen K y una subextensión de H_K/K con grupo de Galois G. Por lo tanto el grupo de clases de ideales tiene un grupo cociente isomorfo a G y por el Lema 4 se tiene el resultado.■

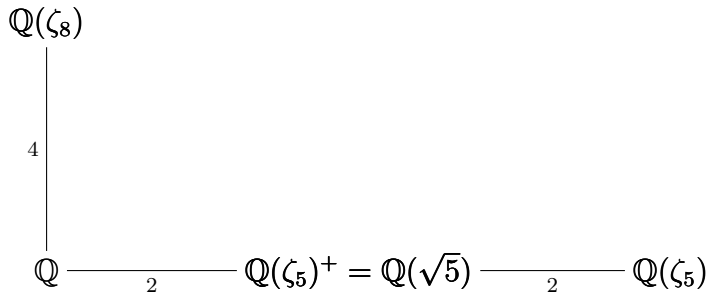
Teorema 25 (Fórmula del conductor-discriminante de Hasse). *Sea K el campo numérico asociado al grupo de caracteres de Dirichlet X. Entonces el discriminante de K está dado por: $\delta(K) = (-1)^{r_2} \prod_{\chi \in X} f_{\chi}$.*

Demostración: Ver [14] página 28.■

Ejemplos:

12) Sea $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1}) = \mathbb{Q}(\zeta_p)^{+}$. El grupo de caracteres de K es: $X = \{\chi \in \widehat{U}_p | \chi(-1) = 1\}$. Todos los caracteres de X (salvo el trivial) tienen conductor p. Hay $|X| - 1 = \dfrac{p-1}{2} - 1 = \dfrac{p-3}{2}$ caracteres pares no triviales y $r_2 = 0$, pues $K \subseteq \mathbb{R}$, por lo tanto $\delta(K) = p^{\frac{p-3}{2}}$. Similarmente, $\delta(\mathbb{Q}(\zeta_p)) = (-1)^{\frac{p-1}{2}} p^{p-2}$.

13) Sea $K_1 = \mathbb{Q}(\sqrt{10})$. Se tiene, $K_1 = \mathbb{Q}(\sqrt{10}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{5}) \subseteq \mathbb{Q}(\zeta_8, \zeta_5) = \mathbb{Q}(\zeta_{40})$, $\mathrm{Gal}\,(\mathbb{Q}(\zeta_{40})/\mathbb{Q}) \cong U_{40} \cong U_8 \times U_5 \cong (C_2 \times C_2) \times C_4 = G$.

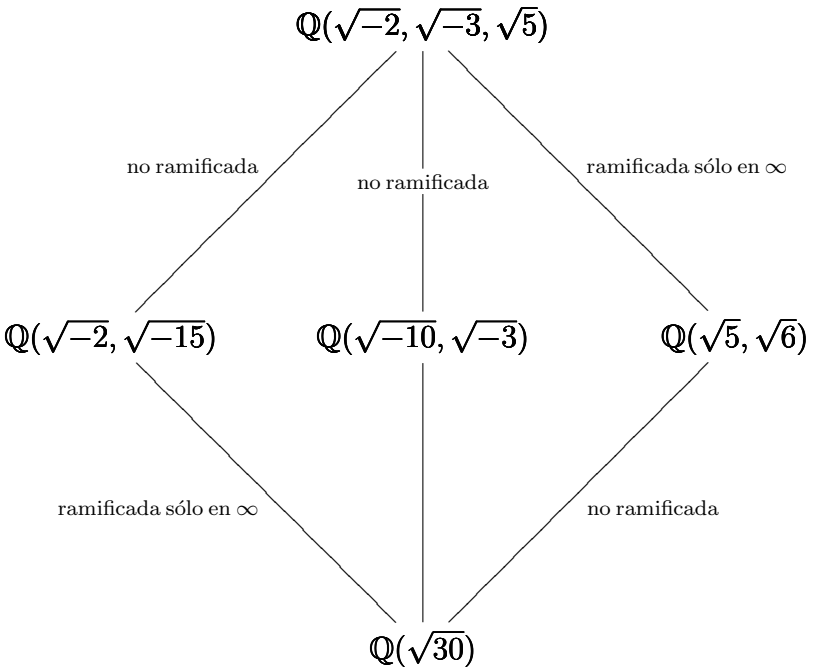


El grupo G tiene 7 subgrupos de orden 2 y por tanto 7 grupos cociente de índice 2. Se sigue que $\mathbb{Q}(\zeta_{40})$ tiene 7 subcampos cuadráticos: $\mathbb{Q}(\zeta_4)$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{-5}), \mathbb{Q}(\sqrt{10})$, $\mathbb{Q}(\sqrt{-10})$. Puesto que $\mathbb{Q}(\sqrt{10}) \nsubseteq \mathbb{Q}(\zeta_4), \mathbb{Q}(\zeta_8), \mathbb{Q}(\zeta_5) = \mathbb{Q}(\zeta_{10}), \mathbb{Q}(\zeta_{20})$, se sigue que si χ es el caracter correspondiente a $\mathbb{Q}(\sqrt{10})$, $f_\chi = 40$ (o bien, de $\delta(K_1) = 40$, se sigue $f_\chi = |40| = 40$). Por tanto, $\chi = \chi_2\chi_5$, $f_{\chi_2} = 8$, $f_{\chi_5} = 5$. Además $\chi(-1) = 1$, implica $\chi_2(-1) = \chi_5(-1) = \pm 1$. Si $\chi_2(-1) = \chi_5(-1) = -1$ se tendría que $\mathbb{Q}(\sqrt{-5}) \subseteq \mathbb{Q}(\zeta_5)$ lo cual es imposible (pues $\chi(-1) = -1$ significa que el campo asociado es complejo y $f_{\chi_5} = 5$). Por tanto $\chi_2(-1) = \chi_5(-1) = 1$, $\chi_2^2 = 1$, $\chi_5^2 = 1$ por lo tanto $\mathbb{Q}(\sqrt{2})$ es el campo asociado a χ_2 y $\mathbb{Q}(\sqrt{5})$ es el campo asociado a χ_5. Se sigue que si $Y = \langle \chi_2 \rangle \bigoplus \langle \chi_5 \rangle$, el campo asociado a Y es $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ luego $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ es la máxima extensión abeliana sobre $\mathbb{Q}$, que es no ramificada sobre $\mathbb{Q}(\sqrt{10})$ e ∞ es no ramificado pues $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ es real.

14) Sea ahora $K_2 = \mathbb{Q}(\sqrt{-5})$. Se tiene $\mathbb{Q}(\sqrt{-5}) \subseteq \mathbb{Q}(\zeta_{20}) = \mathbb{Q}(\zeta_4, \zeta_5)$ $\mathrm{Gal}(\mathbb{Q}(\zeta_{20})/\mathbb{Q}) \cong U_{20} \cong U_4 \times U_5 \cong C_2 \times C_4$, $\mathbb{Q}(\zeta_{20})$ tiene tres subcampos cuadráticos: $\mathbb{Q}(\sqrt{5}), \mathbb{Q}(\sqrt{-5})$ y $\mathbb{Q}(\zeta_4)$. Puesto que $K_2 \nsubseteq \mathbb{Q}(\zeta_5)$, si χ es el caracter correspondiente a K_2, $f_\chi = 20$ (o bien, de $\delta(K_2) = -20$, se sigue $f_\chi = |-20| = 20$). Si $\chi = \chi_2\chi_5$, $f_{\chi_2} = 4$, $f_{\chi_5} = 5$, $\chi(-1) = -1$ implica $\chi_2(-1) \neq \chi_5(-1)$. Como sólo hay un caracter cuadrático de conductor 5, tenemos $\chi_5(-1) = 1$ lo que implica $\chi_2(-1) = -1$, entonces el campo asociado a χ_2 es $\mathbb{Q}(\zeta_4)$ y el campo asociado a χ_5 es $\mathbb{Q}(\sqrt{5})$ por lo tanto el campo asociado a $Y = \langle \chi_2 \rangle \bigoplus \langle \chi_5 \rangle$ es $\mathbb{Q}(\sqrt{-1}, \sqrt{5})$ el cual es la máxima extensión abeliana de $\mathbb{Q}$ que es no ramificada sobre $\mathbb{Q}(\sqrt{-5})$ (∞ es no ramificado pues K_2 es complejo).

15) Sea $K_3 = \mathbb{Q}(\sqrt{30})$. Como $30 = 2 \cdot 3 \cdot 5$, tenemos $\mathbb{Q}(\sqrt{30}) \subseteq \mathbb{Q}(\zeta_8, \zeta_3, \zeta_5)$ $= \mathbb{Q}(\zeta_{120})$, $\mathrm{Gal}(\mathbb{Q}(\zeta_{120})/\mathbb{Q}) \cong U_8 \times U_3 \times U_5 \cong (C_2 \times C_2) \times C_2 \times C_4$.

Se tiene que $\mathbb{Q}(\zeta_{120})$ tiene $\dfrac{2^4-1}{2-1} = 15$ subcampos cuadráticos. Puesto que $\mathbb{Q}(\zeta_{120})$ es el mínimo campo ciclotómico conteniendo a $\mathbb{Q}(\sqrt{30})$, si χ es el caracter correspondiente a K_3, $f_\chi = 120$, $\chi = \chi_2\chi_3\chi_5$, $f_{\chi_2} = 8$, $f_{\chi_3} = 3$, $f_{\chi_5} = 5$. Puesto que sólo hay un caracter de conductor 3, $\chi_3(-1) = -1$. Como antes, tenemos $\chi_5(-1) = 1$ (pues sólo hay un caracter cuadrático de conductor 5). Puesto que $\chi(-1) = 1$, tenemos $\chi_2(-1) = -1$. Sea $Y = \langle\chi_2\rangle \bigoplus \langle\chi_3\rangle \bigoplus \langle\chi_5\rangle$. El campo perteneciente a χ_2 es $\mathbb{Q}(\sqrt{-2})$. El campo perteneciente a χ_3 es $\mathbb{Q}(\sqrt{-3})$. El campo perteneciente a χ_5 es $\mathbb{Q}(\sqrt{5})$. Por lo tanto el campo perteneciente a Y es $\mathbb{Q}(\sqrt{-2}, \sqrt{-3}, \sqrt{5})$. Ahora, $Y^+ = \{\varphi \in Y | \varphi(-1) = 1\} = \langle\chi_2\chi_3\rangle \bigoplus \langle\chi_5\rangle$. El campo perteneciente a $\chi_2\chi_3$ es $\mathbb{Q}(\sqrt{-2}\sqrt{-3}) = \mathbb{Q}(\sqrt{6})$. Por lo tanto, $\mathbb{Q}(\sqrt{5}, \sqrt{6})$ es la máxima extensión abeliana sobre $\mathbb{Q}$ no ramificada sobre $\mathbb{Q}(\sqrt{30})$ en ningún primo. $\mathbb{Q}(\sqrt{-2}, \sqrt{-3}, \sqrt{5})$ es la máxima extensión abeliana sobre $\mathbb{Q}$ no ramificada sobre $\mathbb{Q}(\sqrt{30})$ en ningún primo finito.



Capítulo 4

Caracteres de Dirichlet en campos de funciones

En este capítulo desarrollamos una teoría de caracteres de Dirichlet en campos de funciones y la aplicamos a los campos de funciones ciclotómicos para obtener resultados en campos de funciones análogos a los establecidos en el capítulo anterior para campos numéricos.

4.1 Caracteres de Dirichlet en campos de funciones

Un **caracter de Dirichlet en campos de funciones** es un homomorfismo

$$\Theta : (R_T/(N))^* \to \mathbb{C}^*,$$

con $N \in R_T \backslash \{0\}$ mónico. Decimos que Θ está definido módulo N. Ahora, si $N|M$ con $N, M \in R_T \backslash \{0\}$ mónicos,

$$\Phi_{M,N} : (R_T/(M))^* \to (R_T/(N))^*,$$

donde $A+(M) \mapsto A+(N)$. Si $\Theta : (R_T/(N))^* \to \mathbb{C}^*$, y $N|M$, tenemos $\Theta \circ \Phi_{M,N}$ es un caracter módulo M y "casi" es el mismo que Θ. Por lo tanto Θ puede considerarse módulo N o módulo M. El mínimo N (en tanto a grado) módulo el cual Θ puede definirse se llama el **conductor** de Θ y se denota F_Θ.

Ejemplos:

1) Sean $q = 2$,

$$\begin{array}{rcl} \Theta : (R_T/(T^3))^* & \to & \mathbb{C}^* \\ 1 & \mapsto & 1 \\ T+1 & \mapsto & -1 \\ T^2+1 & \mapsto & 1 \\ T^2+T+1 & \mapsto & -1. \end{array}$$

Puesto que $\Theta(T^2 + A) = \Theta(A)$ para toda $A \in (R_T/(T^3))^*$, Θ puede definirse módulo T^2,

$$\begin{array}{rcl} \widetilde{\Theta} : (R_T/(T^2))^* & \to & \mathbb{C}^* \\ 1 & \mapsto & 1 \\ T+1 & \mapsto & -1, \end{array}$$

$$\begin{array}{ccc} (R_T/(T^3))^* & \xrightarrow{\Theta} & \{\pm 1\} \\ \Big\downarrow{\scriptstyle \Phi_{T^3,T^2}} & \nearrow{\scriptstyle \widetilde{\Theta}} & \\ (R_T/(T^2))^* & & \end{array}$$

claramente $F_\Theta = T^2$.

2) Sean $q = 2$, $N = T^2 + T + 1$, $M = NT$ y $\omega = e^{2\pi i/3}$,

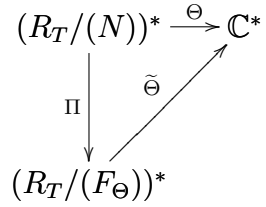
$$\begin{array}{rcl} \Theta : (R_T/(M))^* & \to & \mathbb{C}^* \\ 1 & \mapsto & 1 \\ T^2+1 & \mapsto & \omega \\ T+1 & \mapsto & \omega^2. \end{array}$$

Como tenemos el isomorfismo $(R_T/(NT))^* \cong (R_T/(N))^*$, se puede definir $\Theta : (R_T/(N))^* \to \mathbb{C}^*$, $\Theta(1) = 1$, $\Theta(T) = \Theta(T^2 + 1) = \omega$ y $\Theta(T + 1) = \omega^2$ por lo tanto $F_\Theta = T^2 + T + 1$.

Observaciones:

1) Si $\Theta : (R_T/(N))^* \to \mathbb{C}^*$, es un caracter de Dirichlet en campos de funciones, el **conductor** F_Θ de Θ, se definió como el mínimo F_Θ tal

que

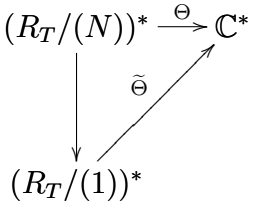


$\Theta = \widetilde{\Theta} \circ \Pi$, donde Π es el epimorfismo natural es decir, $F_\Theta | N$ y

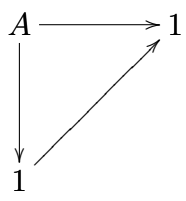
$$\Pi : (R_T/(N))^* \to (R_T/(F_\Theta))^*,$$

donde $A \bmod N \mapsto A \bmod F_\Theta$. Esto es, el conductor F_Θ de Θ necesariamente divide a N.

2) Si $N \in R_T \backslash \{0\}$ mónico, entonces $\Theta : (R_T/(N))^* \to \mathbb{C}^*, A \mapsto 1$ es el único caracter que se puede definir módulo 1 y Θ es el **caracter trivial**. Además este caracter es el único que tiene conductor 1.



dado por

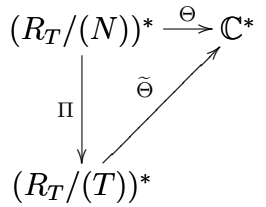


.

3) Recordemos que se tiene que si $(M, N) = 1$, entonces $(R_T/(NM))^* \cong (R_T/(N))^* \times (R_T/(M))^*$.

4) Con $q = 2$ no puede haber un caracter de conductor T ó $T + 1$.

Demostración: Supongamos que sí, es decir, sea Θ un caracter de Dirichlet cuyo conductor F_Θ es T, entonces tenemos el siguiente diagrama



,

donde Π es la proyección natural. Pero sabemos que $(R_T/(T))^* \cong \mathbb{F}_q^*$. Es decir tendríamos

$$\begin{array}{ccc} (R_T/(N))^* & \xrightarrow{\Theta} & \mathbb{C}^* \\ \Big\downarrow \Pi & \nearrow_{\widetilde{\Theta}} & \\ \mathbb{F}_2^* & & \end{array}$$

de donde Θ es el caracter trivial por lo que $F_\Theta = 1$ lo cual no puede ser. Luego, no puede haber un caracter de Dirichlet cuyo conductor sea T, el argumento es análogo para $T+1$.■

5) Sean $q = 2$ y $M \in R_T$ no cero mónico tal que $(M, T) = 1$. Entonces no existe ningún caracter Θ de tal forma que su conductor sea $F_\Theta = TM$. Análogamente, si en lugar de T se considera $T+1$.

Demostración: Por contradicción supongamos que Θ es un caracter de Dirichlet cuyo conductor F_Θ es TM, con $(M, T) = 1$ entonces tenemos el siguiente diagrama

$$\begin{array}{ccc} (R_T/(N))^* & \xrightarrow{\Theta} & \mathbb{C}^* \\ \Big\downarrow \Pi & \nearrow_{\widetilde{\Theta}} & \\ (R_T/(TM))^* & & \end{array} ,$$

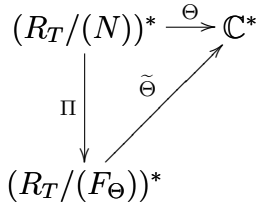
donde Π es la proyección natural. Pero sabemos que, en este caso, $(R_T/(TM))^* \cong (R_T/(M))^*$ para $(M, T) = 1$. Luego tendríamos

$$\begin{array}{ccc} (R_T/(N))^* & \xrightarrow{\Theta} & \mathbb{C}^* \\ \Big\downarrow \Pi & \nearrow_{\widetilde{\Theta}} & \\ (R_T/(M))^* & & \end{array}$$

implicaría que F_Θ es M lo cual no puede ser. Luego, no puede haber un caracter de Dirichlet cuyo conductor sea TM con $(M, T) = 1$. El argumento es análogo si tomamos a $T+1$ en lugar de T. ■

6) Sean Θ, Φ dos caracteres de Dirichlet de conductores F_Θ, F_Φ. Supongamos que existe un N tal que $F_\Theta|N$, $F_\Phi|N$ y $\Theta, \Phi : (R_T/(N))^* \to \mathbb{C}^*$ son iguales módulo N (es decir, $\Theta(A \bmod N) = \Phi(A \bmod N)$, para todo A, $(A, N) = 1$). Entonces $\Theta \equiv \Phi$ (es decir: $F_\Theta = F_\Phi$ y $\Phi = \Theta \bmod F_\Theta$).

Demostración: Consideremos



.

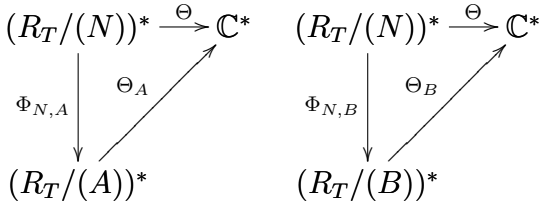
Tenemos $\widetilde{\Theta} \circ \Pi = \Theta = \Phi$, $\widetilde{\Phi} \circ \Pi = \Phi = \Theta$, es decir, Φ se puede definir módulo F_Θ, lo cual implica $F_\Phi|F_\Theta$. Por simetría $F_\Theta|F_\Phi$, por lo tanto $F_\Theta = F_\Phi$.■

Definición 2. *Entenderemos que un caracter* Θ *es* **par** *si* $\Theta(a) = 1$ *para toda* $a \in \mathbb{F}_q^*$.

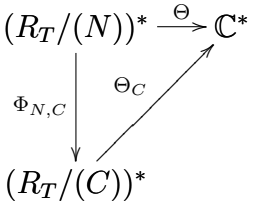
Tenemos que existen $\Phi(N)/(q-1) - 1$ caracteres pares no triviales sobre $(R_T/(N))^*$.

A veces es conveniente considerar un caracter $\Theta : R_T \to \mathbb{C}$ si definimos $\Theta(A) = 0$ para $A \in R_T$, $(A, F_\Theta) \neq 1$ (Θ así definido no es homomorfismo). Por tanto es importante hacer la convención con respecto al módulo de definición de Θ, se considerará Θ definido módulo su conductor. Tales caracteres (definidos módulo F_Θ) se llaman **primitivos** (es decir, hacer $\Theta(A) = 0$ tan poco como sea posible) y notemos que Θ es periódico de **período** F_Θ, es decir $\Theta(A + F_\Theta) = \Theta(A)$ para todo $A \in R_T$.

Observación: Existencia del conductor. Sea $\Theta : (R_T/(N))^* \to \mathbb{C}^*$ un caracter de Dirichlet y sean $A|N$ y $B|N$ tales que $\Theta = \Theta_A \circ \Phi_{N,A} = \Theta_B \circ \Phi_{N,B}$,



Sea $C = (A, B)$, sea D el producto de todos los primos P que dividen a N pero que no dividen a B, por lo tanto $C = (DA, B)$.
Sean $X, Y \in R_T$, $(X, N) = 1 = (Y, N)$ y $X \equiv Y \bmod C$. Existe $\alpha \in R_T$, $\alpha \equiv X \bmod DA$, $\alpha \equiv Y \bmod B$. Se verifica que $(\alpha, N) = 1$, $\Theta(\alpha) = \Theta_A \circ \Phi_{N,A}(\alpha) = \Theta_{DA} \circ \Phi_{N,DA}(\alpha) = \Theta_{DA} \circ \Phi_{N,DA}(X) = \Theta(X)$, $\Theta(\alpha) = \Theta_B \circ \Phi_{N,B}(\alpha) = \Theta_B \circ \Phi_{N,B}(Y) = \Theta(Y)$, por lo tanto $\Theta(X) = \Theta(\alpha) = \Theta(Y)$, lo cual implica $\Theta(X) = \Theta(Y)$, luego $\Theta(X)$ se puede definir módulo C.



Observación: En el ejemplo 2), $M = T^3 + T^2 + T$:

$$\begin{array}{ccc} \Theta : (R_T/(M))^* & \to & \mathbb{C}^* \\ 1 & \mapsto & 1 \\ T^2 + 1 & \mapsto & \omega \\ T + 1 & \mapsto & \omega^2, \end{array}$$

pero no tiene período $T^2 + T + 1$ (y su conductor es $T^2 + T + 1$), pues $\Theta(1) = 1 \neq 0 = \Theta(T^3) = \Theta(T^2 + T) = \Theta(1 + T^2 + T + 1)$ módulo M.

Cuando se hable de caracteres de $(R_T/(N))^*$ o de caracteres módulo N se incluirán los caracteres de conductores que dividen a N.
El caracter trivial es el caracter de conductor 1 y éste es $\Theta : R_T \to \mathbb{C}$, $\Theta(A) = 1$ para todo $A \in R_T$.
Sean Θ, Ψ dos caracteres de conductores F_Θ, F_Ψ. Sea $\Gamma : (R_T/([F_\Theta, F_\Psi]))^* \to \mathbb{C}^*$ donde $\Gamma(A) = \Theta(A)\Psi(A)$. Entonces $\Theta\Psi$ es el caracter primitivo asociado a Γ (Γ no tiene por qué ser primitivo).

Ejemplos:

3) Sean $q = 2$, $\zeta = \zeta_6 = e^{2\pi i/6}$, $\omega = \zeta_3 = e^{2\pi i/3}$, $M = T^2N$, con $N = T^2 + T + 1$ y

$$\begin{array}{ccc} \Theta : (R_T/(M))^* & \to & \mathbb{C}^* \\ 1 & \mapsto & 1 \\ T+1 & \mapsto & \zeta \\ T^2+1 & \mapsto & \zeta^2 \\ T^3+T^2+T+1 & \mapsto & -1 \\ T^3+T^2+1 & \mapsto & -\zeta \\ T^3+T+1 & \mapsto & -\zeta^2. \end{array}$$

y $\Psi : (R_T/(T^2))^* \to \mathbb{C}^*$ con $(R_T/(T^2))^* = \{1, T+1\}$, $\Psi(1) = 1$, $\Psi(T+1) = -1$, $[F_\Theta, F_\Psi] = M$,

$$\begin{array}{ccccc} & & \underline{\Psi \bmod M} & & \\ (R_T/(M))^* & \to & (R_T/(T^2))^* & \to & \mathbb{C}^* \\ 1 & \mapsto & 1 & \mapsto & 1 \\ T+1 & \mapsto & T+1 & \mapsto & -1 \\ T^2+1 & \mapsto & 1 & \mapsto & 1 \\ T^3+T^2+T+1 & \mapsto & T+1 & \mapsto & -1 \\ T^3+T^2+1 & \mapsto & 1 & \mapsto & 1 \\ T^3+T+1 & \mapsto & T+1 & \mapsto & -1. \end{array}$$

Es decir, Ψ módulo M: $\Psi(1) = \Psi(T^2+1) = \Psi(T^3+T^2+1) = 1$, $\Psi(T+1) = \Psi(T^3+T+1) = \Psi(T^3+T^2+T+1) = -1$. Ahora, sea $\Gamma : (R_T/(M))^* \to \mathbb{C}^*$, dada por

$$\Gamma(A) = \Theta(A)\Psi(A) = \begin{cases} 1 & \text{si} \quad A = 1 \\ \omega^2 & \text{si} \quad A = T+1 \\ \omega & \text{si} \quad A = T^2+1 \\ 1 & \text{si} \quad A = T^3+T^2+T+1 \\ \omega^2 & \text{si} \quad A = T^3+T^2+1 \\ \omega & \text{si} \quad A = T^3+T+1. \end{cases}$$

Observamos

$$\begin{array}{ccccc}
(R_T/(M))^* & \to & (R_T/(N))^* & \to & \mathbb{C}^* \\
1 & \mapsto & 1 & \mapsto & 1 \\
T+1 & \mapsto & T+1 & \mapsto & \omega^2 \\
T^2+1 & \mapsto & T & \mapsto & \omega \\
T^3+T^2+T+1 & \mapsto & 1 & \mapsto & 1 \\
T^3+T^2+1 & \mapsto & T+1 & \mapsto & \omega^2 \\
T^3+T+1 & \mapsto & T & \mapsto & \omega.
\end{array}$$

con $(R_T/(M))^* \to \mathbb{C}^*$, por lo tanto $\Theta\Psi : (R_T/(N))^* \to \mathbb{C}^*$, ($1 \mapsto 1$, $T \mapsto \omega$, $T+1 \mapsto \omega^2$) es el producto y $F_{\Theta\Psi} = N$. Nótese que $(\Theta\Psi)(T) = \omega \neq 0 = \Theta(T)\Psi(T)$.

4) Sea $\Theta : (R_T/(N))^* \to \mathbb{C}^*$ arbitrario y sea $\Psi = \overline{\Theta}$, $\Psi(A) = \overline{\Theta(A)} = \Theta(A)^{-1}$ (pues $\Theta((R_T/(N))^*) \subseteq$ raíces de 1) para $(A, F_\Theta) = 1$, luego $\Theta\overline{\Theta}$ es el caracter trivial (es decir, $\Theta\overline{\Theta}(A) = 1$ para todo $A \in R_T$).

5) Si $(F_\Theta, F_\Psi) = 1$, entonces $F_{\Theta\Psi} = F_\Theta F_\Psi$.
Demostración: Tenemos Θ y Ψ dos caracteres con $N = F_\Theta$, $M = F_\Psi$ sus respectivos conductores. Sea

$$\gamma : (R_T/[N, M])^* \to \mathbb{C}^*$$

dado por

$$\gamma(A \bmod [N, M]) = \Theta(A \bmod [N, M])\Psi(A \bmod [N, M]).$$

Definimos

$$\Psi_1 : (R_T/[N, M])^* \to \mathbb{C}^*$$

por $\Psi_1(A \bmod [N, M]) = \gamma(A \bmod [N, M])\Theta^{-1}(A \bmod [N, M])$
esto es $\Psi_1 = \gamma\Theta^{-1}$ y $(R_T/[[N, M], N])^* = (R_T/[N, M])^*$
y

$$\gamma(A \bmod [N, M])\Theta^{-1}(A \bmod [N, M]) = \Psi(A \bmod [N, M])$$

por lo tanto $\Psi_1 = \Psi(\bmod [N, M])$ lo que implica $F_{\Psi_1} = F_\Psi$. Observamos que en general

$$F_{\Theta\Psi}|[F_\Theta, F_\Psi].$$

Luego

$$M = F_{\Psi_1} = F_{\gamma\Theta^{-1}}|[F_\gamma, F_{\Theta^{-1}}],$$

por tanto

$$M|[F_\gamma, F_{\Theta^{-1}}] = [F_\gamma, F_\Theta] = \frac{F_\gamma N}{(F_\gamma, N)} = F_\gamma N_1,$$

donde $N_1 = \dfrac{N}{(F_\gamma, N)}$.

Supongamos $(M, N) = 1$. Entonces $(M, N_1) = 1$, luego $M|F_\gamma$. Análogamente $N|F_\gamma$. Por lo tanto, como $(M, N) = 1$, se tiene $NM|F_\gamma$. Como $F_\gamma = F_{\Theta\Psi}$ y $[N, M] = NM$, tenemos $F_\gamma|NM$. Concluimos $F_\gamma = NM$. Por lo tanto, $F_{\Theta\Psi} = F_\Theta F_\Psi$. ■

Los caracteres de Dirichlet en campos de funciones también se pueden pensar como caracteres de grupos de Galois de campos de funciones ciclotómicos pues $\mathrm{Gal}\,(k(\Lambda_N)/k) \cong (R_T/(N))^*$ (y se llaman, en este caso, **caracteres de Galois**).

Ejemplo:

6) Consideramos $q = 2$, $\Theta : (R_T/(T^3))^* \to \mathbb{C}^*$, $(1, T^2+1 \mapsto 1$ y $T+1, T^2+T+1 \mapsto -1)$, $\ker\Theta = \{1, T^2+1 \bmod T^3\}$, este grupo es el grupo de Galois de $k(\Lambda_{T^3})/k(\Lambda_{T^2})$ pues $\mathrm{Gal}\ (k(\Lambda_{T^3})/k(\Lambda_{T^2})) \cong \{A \bmod T^3 | A \equiv 1 \bmod T^2\} = \{1, T^2+1 \bmod T^3\}$, por lo tanto Θ es un caracter de

$$\frac{\mathrm{Gal}\ (k(\Lambda_{T^3})/k)}{\mathrm{Gal}\ (k(\Lambda_{T^3})/k(\Lambda_{T^2}))} \cong \mathrm{Gal}\ (k(\Lambda_{T^2})/k) \cong (R_T/(T^2))^*,$$

$\Theta : (R_T/(T^2))^* \to \mathbb{C}^*$ $(1 \mapsto 1,\ T+1 \mapsto -1)$.

En general, sea Θ un caracter módulo N, Θ es un caracter de $\mathrm{Gal}\,(k(\Lambda_N)/k)$. Sea $K = k(\Lambda_N)^{\ker\Theta} \subseteq k(\Lambda_N)$. Tenemos K sólo depende de Θ y se llama el **campo perteneciente a** Θ. Si N es minimal, $N = F_\Theta$. Más generalmente, si X es un grupo finito de caracteres de Dirichlet, sea

$$N := \text{ m.c.m. } \{F_\Theta | \Theta \in X\}.$$

Así X es un subconjunto de los caracteres de Gal $(k(\Lambda_N)/k)$. Sean

$$H := \bigcap_{\Theta \in X} \ker \Theta \subseteq (R_T/(N))^*$$

y $K = k(\Lambda_N)^H$, K es el **campo perteneciente a** X. Entonces X es el conjunto de homomorfismos Gal $(K/k) \to \mathbb{C}^*$ y $[K : k] = |X|$. De hecho

$$X \cong \text{Gal}\,(K/k).$$

Si X es cíclico generado por Θ, entonces K es el campo perteneciente a Θ.

Ejemplos

7) Sea $J = \{\sigma_\alpha \in \text{ Gal}\,(k(\Lambda_N)/k) | \alpha \in \mathbb{F}_q^*\}$ (ver observación que sigue al Teorema 14, en el capítulo 2) y sea $k(\Lambda_N)^+$ el campo fijo bajo J.

8) Sean $q = 3$, $M = T^2 + 1$. Tenemos $\Phi(M) = 8$, $(R_T/M)^* = \{1, T + 1, -T, -T + 1, -1, -T - 1, T, T - 1\}$ y $\Lambda_M = \{u \in k^{ac} | u^M = 0\} = \{u \in k^{ac} | ((\varphi + \mu_T)^2 + \text{id})(u) = 0\} = \{u \in k^{ac} | u^9 + (Tu)^3 + Tu^3 + T^2u + u = 0\}$, luego $u(u^8 + T^3u^2 + Tu^2 + T^2 + 1) = 0$, por lo tanto $\Psi_M(u) = u^8 + T^3u^2 + Tu^2 + T^2 + 1 = u^8 + (T^3 + T)u^2 + (T^2 + 1)$. Sea λ una raíz de $\Psi_M(u)$ y sean $\sigma_1 = \text{id}$, $\sigma_{-1} : \lambda \mapsto -\lambda$, $k(\Lambda_M)^+ = \{u \in k(\Lambda_M) | \sigma_{-1}(u) = u\}$. Puesto que $k(\Lambda_M) = \{A_0 + A_1\lambda + \cdots + A_7\lambda^7 | A_i \in k\}$, tenemos $k(\Lambda_M)^+ = \{A_0 + A_2\lambda^2 + A_4\lambda^4 + A_6\lambda^6 | A_i \in k\}$. Sea

$$\begin{array}{rcl} \Theta : (R_T/(M))^* & \to & \mathbb{C}^* \\ 1 & \mapsto & 1 \\ T + 1 & \mapsto & \zeta_8 \\ -T & \mapsto & \zeta_8^2 = i \\ -T + 1 & \mapsto & \zeta_8^3 \\ -1 & \mapsto & \zeta_8^4 = -1 \\ -T - 1 & \mapsto & \zeta_8^5 \\ T & \mapsto & \zeta_8^6 \\ T - 1 & \mapsto & \zeta_8^7, \end{array}$$

luego

$$\begin{array}{rcl} \Theta^2 : (R_T/(M))^* & \to & \mathbb{C}^* \\ 1 & \mapsto & 1 \\ T+1 & \mapsto & i \\ -T & \mapsto & -1 \\ -T+1 & \mapsto & -i \\ -1 & \mapsto & 1 \\ -T-1 & \mapsto & i \\ T & \mapsto & -1 \\ T-1 & \mapsto & -i. \end{array}$$

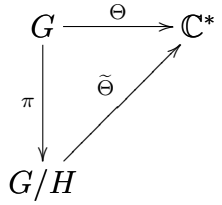
Por lo tanto $\ker \Theta^2 = \{1, -1\} \cong \{\sigma, \sigma_{-1}\} < G$, luego $k(\Lambda_M)^+ = k(\Lambda_M)^{\ker \Theta}$, entonces $k(\Lambda_M)^+$ es el campo perteneciente a Θ^2.

Recordemos que si G es un grupo abeliano finito y $\widehat{G} = \{f : G \to \mathbb{C}^* | \ f \text{ es caracter}\}$, entonces $\widehat{G} \cong G$ (isomorfismo no canónico) pero lo que sí tenemos es $\widehat{\widehat{G}} \cong G$ (isomorfismo canónico, si $g \in G$, $\widehat{g} : \widehat{G} \to \mathbb{C}^*$ está dado por $\widehat{g}(\Theta) := \Theta(g)$). De hecho tenemos un pareo

$$\varphi : G \times \widehat{G} \to \mathbb{C}^*$$

donde $(g, \Theta) \mapsto \langle g, \Theta \rangle = \Theta(g)$. Si $\langle g, \Theta \rangle = 1$ para todo Θ, entonces $\Theta(g) = 1$ para todo $\Theta \in \widehat{G}$. Sea $H = \langle g \rangle$. Entonces $\widehat{G}$ actúa como un conjunto de caracteres distintos de G/H pero hay a lo más $|G/H|$ caracteres por lo tanto $|G/H| \geq |\widehat{G}| = |G|$, luego $|H| = 1$, entonces $g = 1$. Si $\langle g, \Theta \rangle = 1$ para toda $g \in G$, entonces $\Theta(g) = 1$ para toda $g \in G$, lo cual implica $\Theta = 1$, por lo tanto φ es no degenerado.

Sea $H < G$ y sea $H^\perp = \{\Theta \in \widehat{G} | \Theta(h) = 1 \text{ para todo } h \in H\}$. Se tiene: $H^\perp \cong \widehat{(G/H)}$ pues toda $\Theta \in H^\perp$



se factoriza, como en el diagrama de manera única y viceversa. También, si $\mathcal{H} < \widehat{G}$, definimos $\mathcal{H}^\perp = \{g \in G | \Theta(g) = 1 \text{ para todo } \Theta \in \mathcal{H}\}$.

Proposición 32. $\widehat{H} \cong \widehat{G}/H^{\perp}$

Demostración: Sea res : $\widehat{G} \to \widehat{H}$ dada por $\Theta \mapsto \Theta|_H$, ker(res) $= H^{\perp}$. Entonces $\widehat{G}/H^{\perp}$ es isomorfo a un subgrupo de $\widehat{H}$. Por otro lado,

$$|\widehat{G}/H^{\perp}| = \frac{|\widehat{G}|}{|H^{\perp}|} = \frac{|G|}{|\widehat{(G/H)}|} = \frac{|G|}{|G/H|} = |H| = |\widehat{H}|,$$

lo cual implica que $\widehat{G}/H^{\perp} \cong \widehat{H}$. ■

Proposición 33. *Con la identificación* $\widehat{\widehat{G}} \cong G$, *se tiene* $(H^{\perp})^{\perp} = H$.

Demostración: Si $h \in H$, $\widehat{h} : \widehat{G} \to \mathbb{C}^*$ dada por $\Theta \mapsto \Theta(h)$, satisface $h(H^{\perp}) = 1$. Luego, si $\Theta \in H^{\perp}$, $\langle h, \Theta \rangle = \Theta(h) = 1$, entonces $h \in (H^{\perp})^{\perp}$, lo cual implica $H \subseteq (H^{\perp})^{\perp}$. Ahora, $|(H^{\perp})^{\perp}| = |\widehat{(\widehat{G}/H^{\perp})}| = |\widehat{G}/H^{\perp}| = \dfrac{|\widehat{G}|}{|H^{\perp}|} = \dfrac{|G|}{|\widehat{(G/H)}|} = \dfrac{|G|}{|G/H|} = |H|$, concluimos $(H^{\perp})^{\perp} = H$. ■

Sea X el grupo de caracteres de Dirichlet asociado a un campo K, es decir $K = k(\Lambda_N)^H$, $H = \bigcap_{\Theta \in X} \ker \Theta$. Sea

$$\varphi : \mathrm{Gal}\,(K/k) \times X \to \mathbb{C}^*$$

dado por $(\sigma, \Theta) \mapsto \Theta(\sigma)$, $\sigma \in \mathrm{Gal}\,(K/k) \cong (R_T/(N))^*/H$.
Si $\Theta : (R_T/(N))^* \to \mathbb{C}^*$, entonces $H \subseteq \ker \Theta$, por lo tanto $\Theta(H) = 1$, luego Θ se factoriza:

$$\begin{array}{ccc} (R_T/(N))^* & \xrightarrow{\Theta} & \mathbb{C}^* \\ \Big\downarrow{\scriptstyle \pi} & \nearrow{\scriptstyle \widetilde{\Theta}} & \\ (R_T/(N))^*/H & & \end{array} .$$

Proposición 34. *El pareo* φ *es no degenerado, es decir,* $\Theta(\sigma) = 1$ *para todo* $\Theta \in X$ *implica* $\sigma = \mathrm{id}_K$ *y si* $\Theta(\sigma) = 1$ *para todo* $\sigma \in \mathrm{Gal}(K/k)$, *entonces* $\Theta = 1$.

Demostración: Si $\Theta(\sigma) = 1$ para todo $\Theta \in X$, $\sigma \in \bigcap_{\Theta \in X} \ker \Theta = H$, $\sigma|_K = \text{id}_K$. Si $\Theta(\sigma) = 1$ para todo $\sigma \in G \cong (R_T/(N))^*/H$, entonces

$$\Theta : (R_T/(N))^* \to \mathbb{C}^*,$$

es trivial, es decir $\Theta = 1$. ■

Corolario 10. *Tenemos* $X \cong \widehat{G} = \widehat{\text{Gal}\,(K/k)}$ *y* $|X| = [K : k]$.

Demostración: Sea $\Phi : X \to \widehat{G}$, $\Phi(\Theta) = \langle \_, \Theta \rangle : G \to \mathbb{C}^*$,

$$\Phi(\Theta)(g) = \langle g, \Theta \rangle = \Theta(g).$$

Entonces, $\ker \Phi = \{\Theta \in X | \Theta(g) = 1 \text{ para todo } g \in G\} = \{1\}$, por lo tanto Φ es inyectiva. Ahora bien, sea $\psi : G \to \widehat{X}$ con $\psi(g) = \langle g, \_ \rangle$, análogamente ψ es inyectiva, luego $|G| \leq |\widehat{X}| = |X| \leq |\widehat{G}| = |G|$, por tanto Φ es un isomorfismo. ■

Ahora, sean $L \subseteq K$,

$$\varphi : \text{Gal}\,(K/k) \times X \to \mathbb{C}^*$$

donde $\varphi((\sigma, \Theta)) = \langle \sigma, \Theta \rangle = \Theta(\sigma)$. Si

$$Y = \{\Theta \in X | \Theta(g) = 1 \text{ para todo } g \in \text{Gal}\,(K/L)\},$$

entonces $Y \cong \text{Gal}\,(K/L)^\perp \cong (G/\widehat{\text{Gal}\,(K/L)}) \cong \widehat{\text{Gal}\,(L/k)}$.
Recíprocamente, si $Y < X$, sea $L = K^{Y^\perp}$, donde

$$Y^\perp = \{g \in G | \Theta(g) = 1 \text{ para todo } \Theta \in Y\},$$

luego $\text{Gal}\,(K/L) \cong \text{Gal}\,(K/K^{Y^\perp}) \cong Y^\perp$, por lo tanto

$$Y = Y^{\perp\perp} = \text{Gal}\,(K/L)^\perp \cong \widehat{\text{Gal}\,(L/k)}.$$

Se tiene también $Y \cong \widehat{\text{Gal}\,(L/k)} \cong \text{Gal}\,(L/k)$. El primer isomorfismo se expresa a través del pareo $\text{Gal}\,(L/k) \times Y \to \mathbb{C}^*$ donde $(g, \Theta) \mapsto \Theta(g)$.

Proposición 35. *Existe una biyección entre los subgrupos de* X *y los subcampos de* K *que contienen a* k*, dada por:*

$$\begin{cases} \text{subgrupos} & & \text{subcampos} \\ \text{de } X & & \text{de } K \\ Y & \mapsto & K^{Y^\perp} \\ \text{Gal}\,(K/L)^\perp & \hookleftarrow & L. \end{cases}$$

Demostración: Sean $\mathfrak{A} = \{Y | Y < X\}, \mathfrak{B} = \{L | k \subseteq L \subseteq K\}$, $\theta : \mathfrak{A} \to \mathfrak{B}$ dada por $Y \mapsto K^{Y^\perp}$ y $\delta : \mathfrak{B} \to \mathfrak{A}$ dada por $L \mapsto \mathrm{Gal}\,(K/L)^\perp$,

$$(\theta \circ \delta)(L) = \theta\left(\mathrm{Gal}\,(K/L)^\perp\right) = K^{(\mathrm{Gal}\,(K/L)^\perp)^\perp} = K^{\mathrm{Gal}\,(K/L)} = L,$$

$$(\delta \circ \theta)(Y) = \delta(K^{Y^\perp}) = \left(\mathrm{Gal}\,(K/K^{Y^\perp})\right)^\perp = (Y^\perp)^\perp = Y,$$

por lo tanto θ y δ son biyecciones inversas. ■

Proposición 36. *Sea X_i correspondiente a K_i, $i = 1, 2$. Entonces:*

i) $X_1 \subseteq X_2$ si y sólo si $K_1 \subseteq K_2$.

ii) $\langle X_1, X_2 \rangle$ corresponde a $K_1 K_2$.

Demostración: i) Primero supongamos $X_1 \subseteq X_2$, aplicando el Lema 2 (Capítulo 3), tenemos que $X_2^\perp \subseteq X_1^\perp$, luego

$$K_1 = K^{X_1^\perp} \subseteq K^{X_2^\perp} = K_2.$$

Recíprocamente, supongamos $K_1 \subseteq K_2$, esto implica que $\mathrm{Gal}\,(K/K_2) \subseteq \mathrm{Gal}\,(K/K_1)$, luego $\mathrm{Gal}\,(K/K_1)^\perp \subseteq \mathrm{Gal}\,(K/K_2)^\perp$, por lo tanto

$$X_1 \subseteq X_2.$$

ii) Sea $Y = \langle X_1, X_2 \rangle$. Entonces $K^{Y^\perp} = K_1 K_2$, en efecto, sean

$$Y = \langle X_1, X_2 \rangle = X_1 X_2 \text{ y } L = K_1 K_2.$$

Como $X_1 \subseteq Y$ y $X_2 \subseteq Y$, tenemos $K_1 \subseteq K^{Y^\perp}$, $K_2 \subseteq K^{Y^\perp}$, luego $L = K_1 K_2 \subseteq K^{Y^\perp}$. Ahora, como $L \supseteq K_1$ y $L \supseteq K_2$, se tiene $\mathrm{Gal}\,(K/L)^\perp \supseteq X_1$ y $\mathrm{Gal}\,(K/L)^\perp \supseteq X_2$, por lo tanto $\mathrm{Gal}\,(K/L)^\perp \supseteq X_1 X_2$, luego $L \supseteq K^{Y^\perp}$. ■

4.2 Cómputo de los índices de ramificación vía caracteres

Sea $N = P_1^{\alpha_1} \cdots P_h^{\alpha_h}$. Tenemos

$$(R_T/(N))^* \cong \prod_{i=1}^{h}(R_T/(P_i^{\alpha_i}))^*,$$

por lo tanto, si $\Theta : (R_T/(N))^* \to \mathbb{C}^*$, entonces $\Theta = \prod_{i=1}^{h} \Theta_{P_i}$, donde

$$\Theta_{P_i} : (R_T/(P_i^{\alpha_i}))^* \to \mathbb{C}^*,$$

$\Theta_{P_i} = \Theta \circ \Phi^{-1} \circ G_i$, $\Phi : (R_T/(N))^* \to \prod_{i=1}^{h}(R_T/(P_i^{\alpha_i}))^*$ y $Gi : (R_T/(P_i^{\alpha_i}))^* \to \prod_{i=1}^{h}(R_T/(P_i^{\alpha_i}))^*$ con $A \mapsto (1, \ldots, 1, A, 1, \ldots, 1)$. En efecto, si $A \in R_T$, $(A, N) = 1$, entonces

$$\Theta_{P_i}(A) = \Theta(\Phi^{-1}(G_i(A \bmod N))) = \Theta\Phi^{-1}((1, \ldots, 1, A, 1, \ldots, 1)) = \Theta(B_i)$$

donde $B_i \equiv 1 \bmod P_j^{\alpha_j}$, $j \neq i$, $B_i \equiv A \bmod P_i^{\alpha_i}$, luego $(\prod_{i=1}^{h} \Theta_{P_i})(A) = \prod_{i=1}^{h} \Theta_{P_i}(A) = \prod_{i=1}^{h} \Theta(B_i) = \Theta(\prod_{i=1}^{h} B_i) = \Theta(A)$.

Para X un conjunto de caracteres de Dirichlet en campos de funciones y P un polinomio irreducible, se denota: $X_P = \{\Theta_P | \Theta \in X\}$.

Ejemplo:

9) Sean $q = 2$, $M = T^2N$, con $N = T^2 + T + 1$ y

$$\Theta : (R_T/(M))^* \to \mathbb{C}^*$$

donde $(\Theta(1) = 1, \Theta(T+1) = \zeta, \Theta(T^2+1) = \zeta^2, \Theta(T^3+T^2+T+1) = -1, \Theta(T^3+T^2+1) = -\zeta, \Theta(T^3+T+1) = -\zeta^2, \zeta = e^{\frac{2\pi i}{6}})$. Ahora, tenemos $\Theta = \Theta_{P_1}\Theta_{P_2}$, donde $P_1 = T$ y $P_2 = N$, $\Theta_{P_1} : (R_T/(T^2))^* \to \mathbb{C}^*$ y $\Theta_{P_2} : (R_T/(N))^* \to \mathbb{C}^*$,

$$\Phi^{-1} \circ G_1 : (R_T/(T^2))^* \to (R_T/(M))^*,$$

con $1 \mapsto (1,1) \mapsto 1$, $T+1 \mapsto (T+1,1) = (T^3+T^2+T+1, T^3+T^2+T+1) \mapsto T^3+T^2+T+1$, pues $T^3+T^2+T+1 \equiv T+1 \bmod T^2$ y $T^3+T^2+T+1 \equiv 1 \bmod N$ y

$$\Phi^{-1} \circ G_2 : (R_T/(N))^* \to (R_T/(M))^*$$

con $1 \mapsto (1,1) \mapsto 1$, $T \mapsto (1,T) = (T^2+1, T^2+1) \mapsto T^2+1$, $T+1 \mapsto (1,T+1) \mapsto (T^3+T^2+1, T^3+T^2+1) \mapsto T^3+T^2+1$ pues $T^2+1 \equiv 1 \bmod T^2$, $T^2+1 \equiv T \bmod N$, $T^3+T^2+1 \equiv 1 \bmod T^2$ y $T^3+T^2+1 \equiv T+1 \bmod N$. Luego

$$\Theta_{P_1} = \Theta \circ \Phi^{-1} \circ G_1,$$

$(\Theta_{P_1}(1) = 1,\ \Theta_{P_1}(T+1) = \Theta(T^3+T^2+T+1) = -1)$,

$$\Theta_{P_2} = \Theta \circ \Phi^{-1} \circ G_2,$$

$(\Theta_{P_2}(1) = 1,\ \Theta_{P_2}(T) = \Theta(T^2+1) = \omega^2,\ \Theta_{P_2}(T+1) = \Theta(T^3+T^2+1) = -\omega)$. Tenemos $X = \langle\Theta\rangle$, $X_{P_1} = \langle\Theta_{P_1}\rangle$, $X_{P_2} = \langle\Theta_{P_2}\rangle$, $X_P = \{1\}$ si $P \neq T, N$.

Teorema 26. *Sea X un grupo de caracteres de Dirichlet en campos de funciones y sea K el campo perteneciente a X. Sea P un polinomio irreducible y sea e su índice de ramificación en K/k. Entonces $e = |X_P|$.*

Demostración: Sea $N = \text{m.c.m.}\,\{F_\Theta | \Theta \in X\}$, luego $K \subseteq k(\Lambda_N)$.
Sea $N = P^a M$, $(M,P) = 1$. Consideremos

$$L = K(\Lambda_M) = Kk(\Lambda_M) = k(\Lambda_N)^{Y^\perp},$$

donde Y, el grupo de caracteres de L, está generado por X y por los caracteres de $k(\Lambda_N)$ cuyo conductor divide a M (pues $k(\Lambda_M)$ es el campo perteneciente a los caracteres de $(R_T/(M))^*$ y L es el compuesto de K y $k(\Lambda_M)$). Si $\Phi \in Y$, $\Phi = \Theta\Psi$, $\Theta \in X$, $\Psi \in \widehat{(R_T/(M))^*}$, poniendo

$$\Theta = \Theta_P \Theta'$$

con $\Theta' = \prod_{Q|M} \Theta_Q \in (\widehat{R_T/(M)})^*$, se tiene $\Phi = \Theta_P(\Theta'\Psi) \in X_P \times (\widehat{R_T/(M)})^*$, lo cual implica $Y \subseteq X_P \times (\widehat{R_T/(M)})^*$. Recíprocamente, si $\Theta_P\Phi \in X_P \times (\widehat{R_T/(M)})^*$, como $\Theta_P \in X_P$, existe $\Theta \in X$ tal que $\Theta = \Theta_P \prod_{Q|M} \Theta_Q = \Theta_P\Theta'$, $\Theta_P\Phi = \Theta_P\Theta'((\Theta')^{-1}\Phi) = \Theta((\Theta')^{-1}\Phi) \in \langle X, (\widehat{R_T/(M)})^* \rangle = Y$. Por lo que

$$Y = X_P \times (\widehat{R_T/(M)})^*.$$

De $Y = X_P \times (\widehat{R_T/(M)})^*$ se sigue que $L = Fk(\Lambda_M)$, donde $F \subseteq k(\Lambda_{P^a})$ es el campo perteneciente a X_P. Tenemos

$$e = e_P(K/k) = e_P(L/k) = e_P(F/k) = [F : k] = |X_P|. \blacksquare$$

Ejemplo:

10) En el ejemplo anterior el índice de ramificación de $P_1 = T$ es $|X_{P_1}| = 2$ pues $o(\Theta_{P_1}) = 2$, el índice de ramificación de $P_2 = T^2 + T + 1$ es $|X_{P_2}| = 3$ pues $o(\Theta_{P_2}) = 3$ y, finalmente, el índice de ramificación de cualquier otro primo es 1.

Corolario 11. *Sea Θ un caracter de Dirichlet en campos de funciones y K el campo perteneciente a Θ. Entonces P se ramifica en K si y sólo si $\Theta(P) = 0$ (esto es, si y sólo si $P|F_\Theta$). Más generalmente, sea L el campo perteneciente a un grupo de caracteres de Dirichlet X. Entonces P es <u>no</u> ramificado en L/k si y sólo si $\Theta(P) \neq 0$ para todo $\Theta \in X$.*

Demostración: Tenemos P se ramifica en L/k si y sólo si $X_P \neq \{1\}$, si y sólo si existe $\Theta \in X$ tal que $\Theta_P \neq 1$, si y sólo si existe $\Theta \in X$ tal que $P|F_\Theta$, si y sólo si existe $\Theta \in X$ tal que $\Theta(P) = 0$. ■

Teorema 27. *Sean X un grupo de caracteres de Dirichlet, K el campo perteneciente a X. Sean $P \in R_T$ mónico irreducible no cero, $Y = \{\Theta \in X | \Theta(P) \neq 0\}$, $Z = \{\Theta \in X | \Theta(P) = 1\}$ (tenemos $Z < Y < X$). Entonces $e = [X : Y]$, $f = [Y : Z]$, $g = [Z : 1]$, son el índice de ramificación, el grado relativo y el número de primos arriba de P en K/k. De hecho, X/Y es*

isomorfo al grupo de inercia, X/Z es isomorfo al grupo de descomposición, Y/Z es un grupo cíclico de orden f el cual es isomorfo al grupo de Galois de la extensión de campos residuales.

Demostración: Sea L el subcampo de K perteneciente a Y, por el corolario anterior, L es el máximo subcampo de K donde P es no ramificado, por lo tanto L es el campo fijo del grupo de inercia de P, $\mathrm{Gal}\,(K/L) \cong I$ (grupo de inercia). Tenemos $L = K^{Y^\perp}$ y $Y = \mathrm{Gal}\,(K/L)^\perp$. Por tanto: $X/Y \cong \dfrac{\widehat{\mathrm{Gal}\,(K/k)}}{\mathrm{Gal}\,(K/L)^\perp} \cong \widehat{\mathrm{Gal}\,(K/L)} \cong \mathrm{Gal}\,(K/L) \cong I$. En particular,

$$e = |I| = |X/Y| = [X : Y].$$

Tenemos P es no ramificado en la extensión L/k y $Y \cong \widehat{\mathrm{Gal}\,(L/k)}$. Sea $N = \text{ m.c.m. } \{F_\Theta | \Theta \in Y\}$. Puesto que P es no ramificado en L/k, tenemos $\Theta(P) \neq 0$ y por tanto $P \nmid F_\Theta$ para todo $\Theta \in Y$, lo que implica $P \nmid N$ y $L \subseteq k(\Lambda_N)$. Sea $H = \mathrm{Gal}\,(k(\Lambda_N)/L)$. El automorfismo de Fröbenius para P en $k(\Lambda_N)$ está dado por: $\sigma_P(\lambda_N) = \lambda_N^P$, por lo tanto el automorfismo de Fröbenius de P en L es

$$\overline{\sigma}_P = \sigma_P \bmod H = \sigma_P \bmod \mathrm{Gal}\,(k(\Lambda_N)/L).$$

Si $\Theta \in Y$, entonces

$$\Theta(H) = \Theta(\mathrm{Gal}\,(k(\Lambda_N)/L)) = 1,$$

así $\Theta(\overline{\sigma}_P) = \Theta(P)$, por lo tanto $\Theta(\overline{\sigma}_P) = 1$ si y sólo si $\Theta(P) = 1$, luego

$$\langle \overline{\sigma}_P \rangle^\perp = \{\Theta \in Y | \Theta(P) = 1\} = Z,$$

bajo el pareo $\mathrm{Gal}\,(L/k) \times Y \to \mathbb{C}^*$. Por lo que

$$Y/Z = \frac{Y}{\langle \overline{\sigma}_P \rangle^\perp} = \frac{\widehat{\mathrm{Gal}\,(L/k)}}{\langle \overline{\sigma}_P \rangle^\perp} \cong \widehat{\langle \overline{\sigma}_P \rangle} \cong \langle \overline{\sigma}_P \rangle,$$

por lo tanto $[Y : Z] = f$. El campo fijo bajo el automorfismo de Fröbenius es el campo de descomposición E de P. Por otro lado, sabemos que $\mathrm{Gal}(L/E) = \langle \overline{\sigma}_P \rangle$, por tanto

$$E = L^{\langle \overline{\sigma}_P \rangle} \text{ le corresponde a } \mathrm{Gal}\,(L/E)^\perp = \langle \overline{\sigma}_P \rangle^\perp = Z,$$

luego E corresponde a Z y $g = [E : k] = |Z|$. Así, X/Z es isomorfo al grupo de descomposición.■

Ejemplo:

11) Sean P un polinomio irreducible en R_T y $d =$ gr P. Entonces

$$K = k\left(\sqrt[q-1]{(-1)^d P}\right) \subseteq k(\Lambda_P).$$

Sea $\Theta : (R_T/(P))^* \to \mathbb{C}^*$ el caracter asociado a K. Puesto que $X = \langle\Theta\rangle$ es de orden $[K : k] = |X| = q - 1$, tenemos $\Theta^{q-1} = 1$, $\Theta \neq \mathrm{id}$, $F_\Theta = P$ y $\Theta\left((R_T/(P))^*\right)$ coincide con el conjunto de raíces $(q-1)$-ésimas de 1. Tenemos $K = k(\Lambda_P)^{\ker\Theta}$, donde

$$\ker\Theta = \{\sigma \in \mathrm{Gal}\,(k(\Lambda_P)/k) | \Theta(\sigma) = 1\}.$$

Sea Q un polinomio irreducible tal que $Q \neq P$. Se tiene que Q se descompone totalmente en K/k si y sólo si $|Z| = q - 1$, por lo tanto Q se descompone en K/k si y sólo si $\Theta(Q) = 1$.

Por otro lado tenemos (ver [9] página 24) el análogo al símbolo de Legendre $\left(\frac{}{P}\right) = \left(\frac{}{P}\right)_{q-1}$ que está definido, para Q irreducible y $Q \neq P$, como el único elemento de $\mathbb{F}_q^*$ tal que $\left(\frac{Q}{P}\right) \equiv Q^{\frac{q^d-1}{q-1}} \bmod P$.

Ahora, si $Q \equiv B^{q-1} \bmod P$ para algún B, $\Theta(Q) = \Theta(B^{q-1}) = (\Theta(B))^{q-1} = 1$, por lo que $Q \in \ker\Theta$. Puesto que

$$|\ker\Theta| = \frac{|(R_T/(P))^*|}{q-1} = \frac{q^d-1}{q-1} = |((R_T/(P))^*)^{q-1}|,$$

tenemos $\ker\Theta = ((R_T/(P))^*)^{q-1}$, luego $\Theta(Q) = 1$ si y sólo si $Q \equiv B^{q-1} \bmod P$ si y sólo si $\left(\frac{Q}{P}\right) = 1$, por lo tanto $\ker\Theta = \left(\frac{}{P}\right)$.

En resumen $K = k\left(\sqrt[q-1]{(-1)^d P}\right)$ corresponde al caracter $\left(\frac{}{P}\right)$.

Proposición 37. *Sea G un grupo abeliano finito. Entonces existen campos de funciones E y K sobre $k = \mathbb{F}_q(T)$ tales que*

a) $\mathrm{Gal}\,(E/K) \cong G$,

b) E/K *es no ramificada en todos los divisores primos,*

c) E/k *es una extensión abeliana y* K/k *es una extensión cíclica.*

d) El campo de constantes tanto de E *como de* K *es* $\mathbb{F}_q$.

Demostración: Tenemos que $G \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_t\mathbb{Z}$. Sea $m_i = p^{t_i}a_i$, con $(a_i, p) = 1$ y $t_i \geq 0$ para $1 \leq i \leq h$. Sea $d_i' = o(p \bmod a_i)$ para $1 \leq i \leq h$, esto es $p^{d_i'} \equiv 1 \bmod a_i$. Supóngase $d_1 < d_2 < \cdots < d_h$, donde cada d_i' divide a d_i (por ejemplo, tomemos $d_1 = d_1'$, $d_i = 2d_{i-1}d_i'$, $i = 2, \ldots, h$). Sea $P_i \in R_T$ un polinomio irreducible mónico de grado d_i. Tal P_i existe pues $\mathbb{F}_{q^{d_i}} = \mathbb{F}_q(\alpha_i)$ para algún α_i y si $P_i = \mathrm{irr}\,(\alpha_i, T, \mathbb{F}_q)$, entonces $\mathbb{F}_q(\alpha_i) \cong R_T/(P_i)$. Tenemos que $(R_T/(P_i^{p^{t_i}}))^*$ contiene un elemento de orden $p^{t_i}a_i = m_i$. Como el grupo de caracteres de $(R_T/(P_i^{p^{t_i}}))^*$ es isomorfo al grupo $(R_T/(P_i^{p^{t_i}}))^*$, existe un caracter $\theta_i \bmod P_i^{p^{t_i}}$ de orden m_i. Así, Θ_i satisface $o(\Theta_i) = m_i$ y $F_{\Theta_i} = P_i^{s_i}$ con $s_i \leq p^{t_i}$.
Sea P_{h+1} otro polinomio mónico irreducible de grado $d_{h+1} > d_r$ tal que $a_1 \cdots a_h | q^{d_{h+1}} - 1$. Tal d_{h+1} existe pues $(a_1 \cdots a_h, q) = 1$. Sea Θ_{h+1} un caracter de Dirichlet definido $\bmod P_{h+1}^{p^t}$ para $t = t_1 + \cdots + t_h$ y orden $m_{h+1} = p^t(q^{d_{h+1}} - 1)$. Entonces $m_1 \cdots m_h = a_1 \cdots a_h p^{t_1 + \cdots + t_h} | m_{h+1}$. Sean $\Theta = \Theta_1 \cdots \Theta_h \Theta_{h+1}$ y K el campo correspondiente a $Y = \langle \Theta \rangle$. Sean $X = \langle \Theta_1, \ldots, \Theta_h, \Theta_{h+1} \rangle$ y E el campo correspondiente a Y. Tenemos

$$k \subseteq K \subseteq E \subseteq k(\Lambda_M),$$

donde $M = P_1^{\alpha_1} \cdots P_h^{\alpha_h} P_{h+1}^{\alpha_{h+1}}$ con $\alpha_i = p^{t_i}$, $1 \leq i \leq h$, y $\alpha_{h+1} = p^t$.
Así el campo de constantes de E y de K es $\mathbb{F}_q$. Esto prueba *d*). También, E/k es una extensión abeliana.
Se tiene que, el grupo $\mathrm{Gal}\,(K/k) \cong Y = \langle \Theta \rangle$ es cíclico. Esto prueba *c*). Tenemos $X = \langle \Theta_1, \ldots, \Theta_h, \Theta_{h+1} \rangle = \langle \Theta_1, \ldots, \Theta_h, \Theta \rangle$. Además, $o(\Theta) = o(\Theta_{h+1})$ $= m_{h+1}$ y como $m_1 \cdots m_h$ divide a m_{h+1}, Θ es de orden maximal.
De esto se sigue que $X/Y = X/\langle \Theta \rangle \cong \langle \Theta_1, \ldots, \Theta_h \rangle$. Por otra parte, si denotamos por k_X al campo perteneciente a X y por k_Y al campo perteneciente a Y, se tiene

$$X/Y = \frac{\widehat{\mathrm{Gal}\,(k_X/k)}}{\widehat{\mathrm{Gal}\,(k_Y/k)}} \cong \frac{\widehat{\mathrm{Gal}\,(k_X/k)}}{\left(\dfrac{\widehat{\mathrm{Gal}\,(k_Y/k)}}{\widehat{\mathrm{Gal}\,(k_X/k_Y)}}\right)} \cong \widehat{\mathrm{Gal}\,(k_X/k_Y)} \cong$$

$$\cong \widehat{\mathrm{Gal}\,(E/K)} \cong \mathrm{Gal}\,(E/K).$$

Así,

$$\mathrm{Gal}\,(E/K) \cong \langle \Theta_1, \ldots, \Theta_h \rangle \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_t\mathbb{Z} \cong G,$$

lo cual prueba a). Finalmente, los primos ramificados en E/k son $\mathfrak{p}_1, \ldots, \mathfrak{p}_h$, $\mathfrak{p}_{h+1}$ y $\mathfrak{p}_\infty$, donde

$$(P_i)_k = \frac{\mathfrak{p}_i}{\mathfrak{p}_\infty^{\mathrm{gr}\,P_i}}.$$

Nótese que el índice de ramificación de $\mathfrak{p}_\infty$ en K/k es $q-1$, así como en E/k. Por lo tanto $\mathfrak{p}_\infty$ es no ramificado en E/K. Finalmente, tenemos

$$X_{P_i} = \langle \Theta_i \rangle = Y_{P_i}.$$

Sabemos que el índice de ramificación en E/K de cualquier divisor primo en E sobre $\mathfrak{p}_i$ es $\dfrac{|X_{P_i}|}{|Y_{P_i}|} = 1$. Así E/K es no ramificado para cualquier divisor primo. Así probamos b) y por tanto la proposición.■

4.3 El campo de clases de Hilbert en campos de funciones

Desafortunadamente, en campos de funciones sobre campos finitos, la definición usual de la teoría de campos de clases de Hilbert no es muy buena. Si K es un campo de funciones sobre un campo finito, entonces la máxima extensión abeliana no ramificada de K es de dimensión infinita sobre K. Una opción para superar esta dificultad es la siguiente:

Consideremos P_∞ el primo infinito de k. Observemos que R_T consiste precisamente de los elementos de k cuyo único polo es P_∞. Sean K una extensión finita y separable de k, ϑ_K la cerradura entera de R_T en K y

$$S = \{\mathcal{P} \text{ primo en } K|\mathcal{P} \text{ está encima de } P_\infty\}.$$

Notemos que R_T es precisamente el conjunto de elementos de K cuyos polos son elementos de S. Sea K^{sep} una cerradura separable de K. Tenemos que ϑ_K es un dominio de Dedekind y su grupo de clases, que llamamos **grupo de clases de K respecto a S** y denotamos por $\text{Cl}(K)_S$ es finito.

Definición 23. El **campo de clases de Hilbert de K respecto a S**, al cual denotamos por $H_K(S)$ es la máxima extensión abeliana no ramificada contenida en K^{sep} en la que todo elemento $\mathcal{P}$ de S se descompone totalmente.

Teorema 28. *En las condiciones de arriba, $H_K(S)/K$ es una extensión de Galois finita y* $\text{Gal}\,(H_K(S)/K) \cong \text{Cl}(K)_S$.

Demostración: Ver [8] página 368.■

Teorema 29. *Dado cualquier grupo abeliano finito G, existe una extensión cíclica K de k tal que el grupo de clases de K contiene un subgrupo isomorfo a G.*

Demostración: Por la Proposición 37, existen campos de funciones E y K sobre k tales que $\text{Gal}\,(E/K) \cong G$. Sea $S = \{\mathcal{P} \text{ primo en } K|\mathcal{P} \text{ está encima de } P_\infty\}$. Por la demostración de la citada proposición, los primos en S se descomponen totalmente en K/k. Sean $H_K(S)$ el campo de clases de Hilbert con respecto a S y $\text{Cl}(K)_S$ el grupo de clases de K con respecto a S. Luego $E \subseteq H_K(S)$. Por el Teorema 28, tenemos $\text{Gal}\,(H_K(S)/K) \cong \text{Cl}(K)_S$. Por lo tanto, G es isomorfo a un cociente de $\text{Cl}(K)_S$ y por el Lema 4 en el Capítulo 3, G es isomorfo a un subgrupo de $\text{Cl}(K)_S$. Por otro lado, como $d = \text{m.c.d.}\,\{\text{gr}\,\mathcal{P}|\mathcal{P} \in S\} = 1$, tenemos, por la Proposición 14.1 de [9] que la siguiente sucesión es exacta:

$$0 \to \mathcal{D}(S)^0/P(S) \to \text{Cl}(K)^0 \to \text{Cl}(K)_S \to 0$$

donde $\mathcal{D}(S)$ es el grupo de divisores de K generado por S, $\mathcal{D}(S)^0$ es el grupo de divisores en $\mathcal{D}(S)$ de grado cero, $P(S)$ es el grupo de divisores principales en $\mathcal{D}(S)$ y $\text{Cl}(K)^0$ es el grupo de clases de divisores de grado cero de K. Así, $\text{Cl}(K)_S$ es un cociente de $\text{Cl}(K)^0$. Nuevamente por el Lema 4, $\text{Cl}(K)_S$ es

isomorfo a un subgrupo de $\mathrm{Cl}(K)^0$, que a su vez es un subgrupo de $\mathrm{Cl}(K)$, el grupo de clases de divisores de K. Por lo que concluimos que G es isomorfo a un subgrupo de $\mathrm{Cl}(K)$.■

Y por último, tenemos un análogo a la Fórmula del conductor- discriminante de Hasse. Consideramos el **discriminante** $\partial_{\vartheta_K/R_T} = \mathrm{N}_{K/k}(\mathfrak{D}_{\vartheta_K/R_T})$ donde ϑ_K es la cerradura entera de R_T en K.

Teorema 30. *Sea K el campo de funciones asociado al grupo de caracteres de Dirichlet X. Entonces el discriminante de K esta dado por:*

$$\partial_{\vartheta_K/R_T} = \prod_{\Theta \in X} F_\Theta.$$

Demostración: Ver [10] página 104.■

Ejemplo:

12) Sean $q = 3$, $M = T^2(T+1)$, $\zeta = \zeta_6$

$$\begin{array}{rcl} \Theta_T : (R_T/(T^2))^* & \to & \mathbb{C}^* \\ 1 & \mapsto & 1 \\ T-1 & \mapsto & \zeta \\ T+1 & \mapsto & \zeta^2 \\ -1 & \mapsto & -1 \\ -T+1 & \mapsto & -\zeta \\ -T-1 & \mapsto & -\zeta^2, \end{array}$$

$$\widetilde{\Theta}_T : (R_T/(M))^* \xrightarrow{\Pi_T} (R_T/(T^2))^* \xrightarrow{\Theta_T} \mathbb{C}^*$$

luego

$$\widetilde{\Theta}_T = \Theta_T \circ \Pi_T,$$

$$\begin{array}{rcl} \Theta_{T+1} : (R_T/(T+1))^* & \to & \mathbb{C}^* \\ 1 & \mapsto & 1 \\ -1 & \mapsto & -1 \end{array}$$

$$\widetilde{\Theta}_{T+1} : (R_T/(M))^* \xrightarrow{\Pi_{T+1}} (R_T/(T+1))^* \xrightarrow{\Theta_{T+1}} \mathbb{C}^*$$

$$\widetilde{\Theta}_{T+1} = \Theta_{T+1} \circ \Pi_{T+1}.$$

Sean $\Theta^* = \widetilde{\Theta}_T \circ \widetilde{\Theta}_{T+1}$ y $X = \langle \Theta^* \rangle$. El campo correspondiente a X es $K = k(\Lambda_M)$. Tenemos $X_T = \langle \Theta_T \rangle$ y $X_{T+1} = \langle \Theta_{T+1} \rangle$, luego $e_T = 6$ y $e_{T+1} = 2$. Observamos

$$Y(T+1) = \{\tau \in X | \tau(T+1) \neq 0\} = X_T$$
$$Z(T+1) = \{\tau \in X | \tau(T+1) = 1\} = \langle \widetilde{\Theta}_T^3 \rangle,$$

luego $e_{T+1} = 2$, $f_{T+1} = 3$ y $g_{T+1} = 2$. Ahora,

$$Y(T) = \{\tau \in X | \tau(T) \neq 0\} = X_{T+1}$$
$$Z(T) = \{\tau \in X | \tau(T) = 1\} = \{1\},$$

luego $e_T = 6$, $f_T = 2$ y $g_T = 1$. Para P_∞ tenemos $e_\infty = 2$, $f_\infty = 1$ y $g_\infty = 6$. Tenemos $\mathfrak{D}_M = \prod_{i=1}^{h} (\prod_{\mathfrak{p}|P_i} \mathfrak{p})^{s_i} \prod_{\mathfrak{B}|P_\infty} \mathfrak{B}^{q-2}$ (por el Teorema 16 del Capítulo 2), donde $M = P_1^{\alpha_1} \cdots P_h^{\alpha_h}$, $d_i = \text{ gr } P_i$ y $s_i = \alpha_i \Phi(P_i^{\alpha_i}) - q^{d_i(\alpha_i - 1)}$ para $1 \leq i \leq h$. Luego, en nuestro caso $M = T^2(T+1)$, $s_1 = 2\Phi(T^2) - 3 = 9$ y $s_2 = 1\Phi(T+1) - 3^0 = 1$, $\mathfrak{D}_M = \mathfrak{p}_T^9 \mathfrak{p}_{T+1,1} \mathfrak{p}_{T+1,2} \mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3 \mathfrak{P}_4 \mathfrak{P}_5 \mathfrak{P}_6$. Por lo tanto $\mathfrak{D}_{\vartheta_K/R_T} = \mathfrak{p}_T^9 \mathfrak{p}_{T+1,1} \mathfrak{p}_{T+1,2}$. Luego $\partial_{\vartheta_K/R_T} = \mathrm{N}_{K/k}(\mathfrak{D}_{\vartheta_K/R_T}) = T^{18}(T+1)^6$. Por otro lado, tenemos:

caracter	conductor del caracter
1	1
Θ_T	T^2
Θ_T^2	T^2
Θ_T^3	T
Θ_T^4	T^2
Θ_T^5	T^2
Θ_{T+1}	$T+1$
$\Theta_T \Theta_{T+1}$	$T^2(T+1)$
$\Theta_T^2 \Theta_{T+1}$	$T^2(T+1)$
$\Theta_T^3 \Theta_{T+1}$	$T(T+1)$
$\Theta_T^4 \Theta_{T+1}$	$T^2(T+1)$
$\Theta_T^5 \Theta_{T+1}$	$T^2(T+1)$.

Luego $\prod_{\Theta \in X} F_\Theta = 1T^2T^2TT^2T^2(T+1)T^2(T+1)T^2(T+1)T(T+1)T^2(T+1)T^2(T+1) = T^{18}(T+1)^6 = \partial_{\vartheta_{K/R_T}}$.

Con lo cual comprobamos, en este caso, la Fórmula del conductor-discriminante.

Conclusiones

Las clases de campos que hemos estudiado en este trabajo son parte de los llamados campos globales; esto es, unos son campos numéricos y los otros son extensiones finitas del campo de funciones racionales $\mathbb{F}_q(T)$ donde $\mathbb{F}_q$ es el campo finito de q elementos y T es una variable. Es por esto, que existen muchas propiedades aritméticas análogas que se cumplen en estos dos tipos de campos. Uno de los problemas en campos globales es poder construir una clase de campos de funciones congruentes que tengan propiedades aritméticas análogas a las de una clase de campos numéricos determinada y viceversa.

Hemos observado que, en efecto, la clase de campos ciclotómicos tiene una clase análoga en campos de funciones congruentes; a saber, la clase de campos de funciones ciclotómicos. Y esta analogía se da desde la forma en la que se determina la acción de R_T-módulo para determinar los elementos de torsión de k^{ac}, similar a la obtención de raíces de unidad. Así, se obtuvo la analogía en relación con su construcción, la función φ de Euler, el polinomio ciclotómico, el subcampo real, los grupos de Galois, la ramificación, el diferente, el discriminante, el número de clases, la máxima extensión abeliana, entre otras cosas. Pero también, y esto es la parte central del trabajo, se obtuvieron el desarrollo y las propiedades de los caracteres de Dirichlet en ambas clases de campos, notando que en efecto, tienen similitudes tanto en la definición como en sus propiedades, en particular, con respecto a la biyección entre subgrupos y subcampos, la ramificación, el símbolo de Legendre y los resultados vinculados al campo de clases de Hilbert.

En contraste, observamos lo siguiente (ver [14]). No se conoce si dado cualquier grupo abeliano finito, éste es el grupo de clases de algún campo numérico, pero lo que sí se sabe es que cualquier l-grupo abeliano finito es el l-subgrupo de Sylow del grupo de clases para algún campo de números. El resultado correspondiente para el conjunto de clases de divisores de grado 0

es falso para campos de funciones sobre campos finitos.

Se procuró obtener y presentar ejemplos que fueran ilustrando los conceptos y resultados, que fueran iluminando el camino y mostrando, hasta donde fue posible, el paralelismo entre ambas clases de campos.

Bibliografía

[1] Dummit, David S. & Foote, Richard M., *Abstract Algebra*, John Wiley & Sons, Inc., Second edition, 1999.

[2] Galovich, S. & Rosen, M. *The class number of cyclotomic function fields*, J. Number Theory 13, (1981), 363-375.

[3] Galovich, S. & Rosen, M. *Units and class groups in cyclotomic function fields*, J. Number theory 14, (1982), 156-184.

[4] Lam, Pablo, *Campos de funciones ciclotómicos y extensiones seudo-cogalois*, Tesis doctoral, CINVESTAV-IPN, México 1997.

[5] Lang, Serge, *Cyclotomic Fields*, Springer-Verlag, New York, GTM 59, 1978.

[6] Lang, Serge, *Algebraic Number Theory*, Springer-Verlag, New York, GTM 110, 1986.

[7] Mollin, Richard, *Algebraic Number Theory*, Chapman & Hall/CRC, London, 1999.

[8] Rosen, Michael, *The Hilbert class field in function fields*, Expos. Math, 5, (1987), 365-378.

[9] Rosen, Michael, *Number Theory in Function Fields*, Springer-Verlag, New York, GTM 210, 2002.

[10] Serre, Jean-Pierre, *Local Fields*, Springer-Verlag, New York, GTM 67, 1979.

[11] Villa Salvador, Gabriel Daniel, *Introducción a la Teoría de las Funciones Algebraicas*, México, Fondo de Cultura Económica, 2003.

[12] Villa Salvador, Gabriel Daniel, *Topics in the Theory of Algebraic Function Fields*, (en preparación).

[13] Villa Salvador, Gabriel Daniel & Lam, Pablo, *Some remarks on the theory of cyclotomic function fields*, Rocky Mountains, Journal of Mathematics, 31, (2001), 483-502.

[14] Washington, Lawrence C., *Introduction to Cyclotomic Fields*, Springer-Verlag, Second edition, GTM 83, 1982.

Índice