



LEY DE RECIPROCIDAD DE ARTIN

Daniel Camilo Rodriguez Ruiz

UNIVERSIDAD NACIONAL DE COLOMBIA
FACULTAD DE CIENCIAS
DEPARTAMENTO DE MATEMÁTICAS
SEDE BOGOTÁ
19 DE MARZO, 2021

LEY DE RECIPROCIDAD DE ARTIN

Daniel Camilo Rodríguez Ruiz

Trabajo Final de Maestría en Ciencias Matemáticas

Director:

John Jaime Rodríguez Vega, Profesor Asociado

UNIVERSIDAD NACIONAL DE COLOMBIA

FACULTAD DE CIENCIAS

DEPARTAMENTO DE MATEMÁTICAS

SEDE BOGOTÁ

19 DE MARZO, 2021

ARTIN RECIPROCITY LAW

Daniel Camilo Rodríguez Ruiz

Master Thesis in Mathematical Sciences

Director:

John Jaime Rodríguez Vega, Associate Teacher

NATIONAL UNIVERSITY OF COLOMBIA

SCIENCE FACULTY

DEPARTMENT OF MATHEMATICS

BOGOTÁ BRANCH

MARCH 19, 2021

*Dedicado a
mi madre, mi familia,
y a todas las personas que lo hicieron posible.*

AGRADECIMIENTOS

En primer lugar, quiero agradecer profundamente al profesor John Jaime Rodríguez Vega por no dudar en ningún momento el ser mi acompañante durante la realización de este trabajo, así como por su comprensión, paciencia, orientación y consejos que me dieron la fuerza suficiente para continuar en los momentos de dificultad que se presentaron.

También quiero agradecer a la Universidad Nacional de Colombia, por haberme aceptado durante todos mis estudios en matemáticas, y por permitirme aprender en todos los sentidos de la vida. A los maestros que me marcaron el camino muchas gracias.

Por otro lado, quiero agradecer a mi madre y a mi familia cercana, quienes siempre me brindan toda su ayuda y su cariño. Gracias a mi tía Daissy E. Alarcon que con su apoyo me permitió finalizar mis estudios.

Por último, quiero dar gracias a William Eduardo Peña por su compañía y ayuda en la lectura detallada de este trabajo, y por sus sugerencias en las correcciones. Y quiero agradecer a Andres F. Alvarez por su ánimo y apoyo.

A todos los que me ayudaron y me brindaron su apoyo, muchas gracias.

RESUMEN

En este trabajo final se presenta de una manera general la teoría de los cuerpos numéricos, en donde se muestran propiedades del anillo de enteros algebraicos y del grupo de clases de ideales. También se realiza un estudio detallado sobre la ramificación de un ideal primo en una extensión, luego, se introduce el símbolo de Artin, este es una generalización del símbolo de Legendre. A partir de algunas propiedades del símbolo de Artin se presenta una primera prueba de la ley de reciprocidad cuadrática.

Además, se define el homomorfismo de Artin y se enuncia el teorema de Artin para el cuerpo de clases de Hilbert. Por último, se estudia brevemente el grupo de clases de ideales generalizado y se enuncia el teorema de Artin, a partir de este se presenta otra prueba de la ley de reciprocidad cuadrática.

Palabras clave: Cuerpo numérico, ideal fraccionario, teorema de Kummer-Dedekind, símbolo de Artin, homomorfismo de Artin, ley de reciprocidad cuadrática, divisor primo, grupo de clases de ideales generalizado, teorema de Artin, símbolo de Legendre, ley de reciprocidad débil.

ABSTRACT

This thesis a general review of the theory of number fields is given. We study some properties of the ring of integers of a number field and also of the ideal class group. We also carried out a detailed study of the ramification of prime ideals in field extensions. Then we define Artin's symbol (which is a generalization of Legendre's symbol) and use some of its properties to give a first proof of the quadratic reciprocity law.

In addition we study the Artin homomorphism and state Artin's theorem for the Hilbert class field. Finally, we focus on the generalized ideal class group and state Artin's theorem in this context. This allow us to present another proof of the quadratic reciprocity law.

Key words: Number field, fractional ideal, Kummer-Dedekind's theorem, Artin's symbol, Artin's map, quadratic reciprocity law, prime divisor, generalized ideal class group, Artin's theorem, Legendre's symbol, weak reciprocity law.

INTRODUCCIÓN

La teoría algebraica de números es una rama de la teoría de números en la que se generaliza la noción de número entero, introduciendo así los cuerpos numéricos y los enteros algebraicos, y cuyo objetivo es estudiar las propiedades de estos conceptos, en particular la factorización en primos. Esta teoría surge de manera rigurosa en 1801 cuando Carl F. Gauss publica "*Disquisitiones arithmeticae*", en donde Gauss compila gran cantidad de resultados de teoría de números que ya se habían obtenido previamente, aunque en la mayor parte de este libro se introducen conceptos nuevos que se deben a Gauss. En este libro, Gauss introduce el concepto de congruencia, y con ayuda de este enuncia el famoso *Teorema Áureo* o *Ley de Reciprocidad Cuadrática* como se conoce en la actualidad, además realiza la primera prueba. La ley de reciprocidad cuadrática era muy importante para Gauss, quien lo siguió explorando profundamente mediante diferentes técnicas y logró realizar seis pruebas más. Esto llevó a que los matemáticos de la época también se interesaran en este teorema encontrando muchas pruebas diferentes, tanto así que, Lemmermeyer en [16] cita al menos 196 pruebas. Un objetivo importante para los matemáticos de la época era generalizar la ley de reciprocidad cuadrática, y fue Gauss quien enunció por primera vez la ley de reciprocidad bicuadrática, aunque Eisenstein fue el primero en demostrar la ley de reciprocidad cúbica y bicuadrática, después, otros nombres como Kummer, Hilbert, Hasse y Takagi enunciaron sus propias leyes de reciprocidad.

El problema de generalizar las leyes de reciprocidad adquirió una gran importancia en matemáticas, de este modo, Hilbert dio lugar en la lista de sus 23 problemas al noveno problema, que pide encontrar la ley de reciprocidad más general en un cuerpo numérico arbitrario, es decir, enunciar un teorema de reciprocidad que generalice todos los anteriores y realizar su prueba.

Por otro lado, uno de los objetivos de la teoría analítica de números es el estudio sobre la distribución de los números primos y la función zeta de Riemann, de manera más general estudia las L-funciones de Dirichlet. La teoría algebraica y analítica de números se relacionan de una manera muy estrecha cuando Dedekind generaliza la función zeta de Riemann a un cuerpo numérico, obteniendo información sobre la distribución de los ideales primos del anillo de enteros. Luego, Hecke generaliza las L-funciones de Dirichlet a los cuerpos numé-

ricos, estas son denominadas como las L-funciones de Hecke.

A finales del siglo XIX y principios del siglo XX se crea la teoría del cuerpo de clases, que trata de describir todas las extensiones abelianas de un cuerpo fijo K en términos de la estructura interna de K .

En 1923 Artin publica el artículo *Über eine neue Art von L-Reihen* donde intentaba generalizar los resultados de Hecke y Weber que se tienen para todas las extensiones abelianas, Artin buscaba generalizar estos resultados para extensiones no abelianas, para eso definió un nuevo tipo de L-función llamadas L-funciones de Artin. Además, enunció un teorema muy importante sobre las L-funciones, este teorema es llamado el teorema de Artin. La interpretación algebraica del teorema de Artin es conocida como la ley de reciprocidad de Artin, esta es la ley de reciprocidad más general en cualquier cuerpo, aunque cabe notar que Artin no tenía como objetivo encontrar la ley de reciprocidad más general pues su objetivo era mucho más analítico.

Este trabajo tiene por objetivo desarrollar las herramientas necesarias para comprender y enunciar la ley de reciprocidad de Artin, y obtener la ley de reciprocidad cuadrática como una consecuencia.

Además, se asume bastante familiaridad con los temas estándar de un curso de álgebra abstracta, puesto que en la totalidad del trabajo se usan estas herramientas algebraicas. Aunque en este documento no se prueban resultados nuevos, una característica importante de este es que en su gran mayoría las proposiciones y teoremas se prueban con detalle, haciendo posible una mejor lectura de cada tópico.

El contenido de este documento está dividido en tres capítulos, y las referencias principales son [7] y [17].

En el capítulo 1 se estudian las propiedades básicas de los cuerpos numéricos y de los enteros algebraicos, se introducen algunos conceptos básicos como la norma, la traza y el discriminante, estos se usan posteriormente. Los resultados más importantes de este capítulo y de los más usados en todo el documento son la finitud del cuerpo cociente del anillo de enteros algebraicos y un ideal propio no nulo, y el teorema fundamental de la aritmética en ideales, también se estudian brevemente los cuerpos finitos y el automorfismo de Frobenius. El capítulo finaliza con el concepto de ideal fraccionario, el teorema fundamental de la aritmética en ideales fraccionarios y el grupo de clases de ideales.

El capítulo 2 es fundamental en este documento, este se basa en el estudio de la ramificación de ideales primos en extensiones de cuerpos numéricos, también, se realiza un estudio cuidadoso de los cuerpos cuadráticos y ciclotómicos, donde se presentan gran parte de sus propiedades básicas. Se estudia la ramificación de ideales primos en extensiones de Galois

y se prueba el Teorema de Kummer-Dedekind, este exhibe la factorización de un ideal primo que no ramifica en una extensión de Galois. Además, se introduce el símbolo de Artin y sus propiedades, y se presenta una prueba poco usual de la ley de reciprocidad cuadrática. El capítulo finaliza con el homomorfismo de Artin y el teorema de Artin para el cuerpo de clases de Hilbert, y por último, se clasifican las extensiones abelianas y no ramificadas de un cuerpo numérico en términos de los subgrupos del grupo de clases de ideales.

El capítulo 3 es el más importante del documento, en este se presentan los divisores primos de un cuerpo como la clase de equivalencia de un valor absoluto no trivial, y un divisor primo se dice arquimediano o no arquimediano si lo son todos los valores absolutos que lo componen, además, los divisores primos no arquimedianos corresponden a los ideales primos del anillo de enteros mientras que los divisores primos arquimedianos corresponden a los homomorfismos del cuerpo en \mathbb{C} que fijan a \mathbb{Q} , con ayuda de este concepto se define un módulo en un cuerpo como un producto formal de todos los divisores primos con ciertas condiciones, así, se introduce el grupo de clases de ideales generalizado. Se enuncia el teorema de Artin, se define el símbolo de Legendre para la n -ésima potencia y se muestra la ley de reciprocidad débil, usando esto se demuestra la ley de reciprocidad cuadrática como consecuencia de la ley de reciprocidad de Artin.

ÍNDICE GENERAL

Agradecimientos	II
Resumen	III
Abstract	IV
Introducción	V
1. Preliminares	1
1.1. Cuerpos numéricos	1
1.2. Cuerpos finitos	13
1.3. Ideales fraccionarios	15
2. Ramificación	19
2.1. Definición y Propiedades	19
2.2. Cuerpos Cuadráticos	26
2.3. Cuerpos Ciclotómicos	32
2.4. Ramificación en extensiones de Galois	40
2.4.1. Teorema de Kummer-Dedekind	45
2.4.2. Símbolo de Artin	50
2.5. Ley de Reciprocidad Cuadrática	60
2.5.1. El Carácter Cuadrático de 2	61
2.5.2. Prueba de la Ley de Reciprocidad Cuadrática	63
2.6. El cuerpo de clases de Hilbert y el Homomorfismo de Artin	67
3. Teoría del Cuerpo de Clases	73
3.1. Un Poco de Historia	73
3.2. Divisores Primos	74
3.3. Grupo de Clases Generalizado	79
3.4. Teorema de Artin	84
3.5. Hacia las Leyes de Reciprocidad	88
Bibliografía	101

CAPÍTULO 1

PRELIMINARES

Este primer capítulo estudia algunas nociones básicas de los cuerpos numéricos, como lo son la norma, la traza y el discriminante. Se destaca el estudio de algunas propiedades del anillo de enteros, una de las más importantes es la factorización única de todo ideal no nulo en producto de ideales primos. Los cuerpos finitos ocupan un lugar importante en este capítulo por su importancia en los capítulos posteriores. Y para finalizar este capítulo se estudian las propiedades básicas de los ideales fraccionarios de un cuerpo numérico

En este capítulo una parte de las afirmaciones se presentan sin demostración, ya que estas afirmaciones son ampliamente conocidas en la literatura.

1.1. CUERPOS NUMÉRICOS

El estudio de la aritmética de los cuerpos numéricos es un tópico central de la teoría algebraica de números.

Definición 1.1.1. Un cuerpo numérico K se define como un subcuerpo de \mathbb{C} tal que su grado como extensión sobre \mathbb{Q} denotado por $[K : \mathbb{Q}]$ es finito.

Dado K un cuerpo numérico se define \mathcal{O}_K como el conjunto de enteros algebraicos de K , es decir $\alpha \in \mathcal{O}_K$ si $\alpha \in K$ y es raíz de algún polinomio mónico con coeficientes enteros.

En este caso, en [17] se prueba que el conjunto \mathcal{O}_K de enteros algebraicos de K resulta un subanillo de \mathbb{C} , tal anillo tiene por cuerpo de fracciones a K .

Dado K un cuerpo numérico tal que $n = [K : \mathbb{Q}]$, entonces existen $\sigma_1, \dots, \sigma_n$ homomorfismos de K en \mathbb{C} que fijan a \mathbb{Q} , con ayuda de estos homomorfismos se pueden caracterizar las extensiones normales.

Lema 1.1.1. Sean K, L cuerpos numéricos tales que L es una extensión finita de K .

1. Si σ es un homomorfismo de K en \mathbb{C} que fija a \mathbb{Q} , entonces σ se extiende a exactamente $[L : K]$ homomorfismos de L en \mathbb{C} que fijan a \mathbb{Q} .
2. Existen exactamente $[L : K]$ homomorfismos de L en \mathbb{C} que fijan a K .
3. Sea $\alpha \in L$. Si $\beta \in \mathbb{C}$ es una raíz del polinomio mínimo de α , entonces existe un homomorfismo de L en \mathbb{C} que fija a K y envía α en β .

Demostración. 1. Por inducción sobre $n = [L : K]$:

$n = 1$: Se tiene que $L = K$ y no hay nada que probar.

$n \geq 2$: Supóngase que la afirmación es verdadera para cualesquiera par de cuerpos numéricos K, L tales que L es una extensión finita de K y $[L : K] < n$.

Sea $\sigma : K \rightarrow \mathbb{C}$ un homomorfismo de K en \mathbb{C} que fija a \mathbb{Q} , entonces

$$\sigma : K \rightarrow K'$$

es un isomorfismo de cuerpos, donde $K' := \sigma(K)$.

De este modo, se induce el siguiente isomorfismo de anillos

$$\sigma' : K[x] \rightarrow K'[x]$$

inducido por σ .

Por hipótesis $K \subsetneq L$, luego existe $\alpha \in L - K$, y puesto que L es una extensión algebraica de K , existe $f(x) \in K[x]$ el polinomio mínimo de α .

De este modo, el polinomio $g(x) := \sigma'(f(x)) \in K'[x]$ es irreducible y

$$gr(g(x)) = gr(f(x)).$$

Sea $m := gr(g(x)) = gr(f(x)) = [K(\alpha) : K] \geq 2$, entonces $g(x)$ tiene m raíces distintas en \mathbb{C} . Sean β_1, \dots, β_m las raíces de $g(x)$, luego, para cada $i \in \{1, \dots, m\}$ existe un isomorfismo de anillos

$$\begin{aligned} \theta_i : K(\alpha) &\rightarrow K'(\beta_i) \\ \theta_i(\alpha) &= \beta_i \text{ y } \theta_i|_K = \sigma \end{aligned}$$

que extiende a σ . Así, al considerar $\theta_i : K(\alpha) \rightarrow \mathbb{C}$, se tiene que θ_i es un homomorfismo de $K(\alpha)$ en \mathbb{C} que fija a \mathbb{Q} y extiende a σ . Note que θ_i está determinado por sus valores en K y en α .

Esto implica que se tienen $m = [K(\alpha) : K]$ homomorfismos de $K(\alpha)$ en \mathbb{C} que fijan a \mathbb{Q} y extienden a σ .

De otro lado, $K \subsetneq K(\alpha) \subseteq L$ y $[K(\alpha) : K] \geq 2$, entonces

$$n = [L : K] = [L : K(\alpha)][K(\alpha) : K] \geq [L : K(\alpha)]2 > [L : K(\alpha)],$$

la hipótesis de inducción implica que cada uno de los m homomorfismos de $K(\alpha)$ en \mathbb{C} que fijan a \mathbb{Q} se extiende a $[L : K(\alpha)]$ homomorfismos de L en \mathbb{C} que fijan a \mathbb{Q} . Por lo tanto, el homomorfismo σ se extiende a $m[L : K(\alpha)] = [L : K]$ homomorfismos de L en \mathbb{C} que fijan a \mathbb{Q} .

Nótese que cada homomorfismo que extienda a σ debe ser uno de los anteriores: En efecto, sea τ un homomorfismo de L en \mathbb{C} que fija a \mathbb{Q} y que extiende a σ , sea $\alpha \in L - K$ el mismo de antes y

$$f(x) = x^m + \sum_{i=0}^{m-1} f_i x^i \in K[x]$$

su polinomio mínimo, entonces

$$g(x) = \sigma'(f(x)) = x^m + \sum_{i=0}^{m-1} \sigma(f_i) x^i \in K'[x] \subseteq \mathbb{C}[x],$$

luego

$$g(\tau(\alpha)) = (\tau(\alpha))^m + \sum_{i=0}^{m-1} \sigma(f_i) \tau(\alpha)^i = \tau \left(\alpha^m + \sum_{i=0}^{m-1} f_i \alpha^i \right) = \tau(f(\alpha)),$$

por lo tanto, $\tau(\alpha)$ es una raíz de $g(x)$, de modo que $\tau(\alpha) = \beta_i$ para algún $1 \leq i \leq m$, y así $\tau(\alpha) = \theta_i(\alpha)$ para algún $1 \leq i \leq m$, de este modo la restricción de τ a $K(\alpha)$ es el homomorfismo θ_i .

Para los elementos de $L - K(\alpha)$ se aplica de manera recurrente el razonamiento anterior. Esto muestra que τ debe ser uno de los $[L : K]$ homomorfismos construidos en la prueba inductiva.

2. Sea $\iota : K \rightarrow \mathbb{C}$ el homomorfismo inclusión, este fija los elementos de K . Por el item anterior, se sigue que ι se extiende a exactamente $[L : K]$ homomorfismos de L en \mathbb{C} que fijan a \mathbb{Q} , ya que al restringir estos homomorfismos a K son iguales al homomorfismo ι , se obtiene que cada uno de estos deja fijo el cuerpo K .
3. Basta tomar el homomorfismo idéntico

$$i_K : K \rightarrow K,$$

este induce el isomorfismo

$$\phi : K(\alpha) \rightarrow K(\beta),$$

el cual satisface que $\phi(\alpha) = \beta$ y la restricción de ϕ a K es i_K . De otro lado, se tiene que

$$\phi : K(\alpha) \longrightarrow \mathbb{C}$$

es un homomorfismo de $K(\alpha)$ en \mathbb{C} que fija a \mathbb{Q} , por ítem 1 se obtiene que este homomorfismo se extiende a un homomorfismo de L en \mathbb{C} tal que fija a K y envía α en β .

□

El siguiente teorema relaciona la normalidad de una extensión algebraica con los homomorfismos que dejan fijo a \mathbb{Q} .

Teorema 1.1.1. *Sean K, L cuerpos numéricos tales que L es una extensión finita de K . Entonces las siguientes condiciones son equivalentes:*

1. L es una extensión normal de K .
2. Todo homomorfismo de L en \mathbb{C} que fija a K es un automorfismo de L .
3. El grupo $\text{Gal}(L/K)$ tiene exactamente $[L : K]$ elementos.

Demostración. (1) \Rightarrow (2) : Sea $\sigma : L \longrightarrow \mathbb{C}$ un homomorfismo de L en \mathbb{C} que fija a K , entonces $\sigma(K) = K \subseteq L$.

Sea $\alpha \in L - K$, entonces $K \subsetneq K(\alpha) \subseteq L$. Por otro lado, sea $f(x) \in K[x] \subseteq \mathbb{C}[x]$ el polinomio mínimo de α , y $n := [K(\alpha) : K] = \text{gr}(f(x))$.

Sean $\alpha_1 := \alpha, \alpha_2, \dots, \alpha_n$ las n distintas raíces de $f(x)$, puesto que L es normal sobre K se tiene que $\alpha_1, \dots, \alpha_n \in L$. Ya que $\sigma(\alpha)$ es una raíz de $f(x)$, entonces $\sigma(\alpha) = \alpha_i \in L$ para algún $1 \leq i \leq n$. Esto implica que

$$\sigma(L) \subseteq L.$$

De otro lado,

$$\sigma : L \longrightarrow \sigma(L)$$

es un isomorfismo de anillos, y así,

$$\sigma(L) = L,$$

esto implica que σ es un automorfismo de L .

(2) \Rightarrow (1) : Sea $p(x) \in K[x]$ un polinomio irreducible tal que existe $\beta \in L$ raíz de $p(x)$, y sea $\gamma \in \mathbb{C}$ otra raíz de $p(x)$. El lema anterior implica que existe

$$\phi : L \longrightarrow \mathbb{C}$$

un homomorfismo de L en \mathbb{C} que fija a K y $\phi(\beta) = \gamma$.

Por hipótesis, se tiene que ϕ es un automorfismo de L , de donde se obtiene que $\gamma \in L$, y por lo tanto, $p(x)$ tiene todas sus raíces en L .

(1) \Rightarrow (3) : El teorema fundamental de la teoría de Galois implica que

$$|\text{Gal}(L/K)| = [L : K].$$

(3) \Rightarrow (2) : Por hipótesis se tiene que

$$|\text{Gal}(L/K)| = [L : K].$$

Sea

$$\mathcal{C} := \{\sigma : L \rightarrow \mathbb{C} : \sigma \text{ es un homomorfismo que fija a } K\},$$

el lema anterior implica que

$$|\mathcal{C}| = [L : K].$$

De otro lado, $\text{Gal}(L/K) \subseteq \mathcal{C}$, ya que todo automorfismo de L es un homomorfismo de L en \mathbb{C} . De esto se concluye que $\mathcal{C} = \text{Gal}(L/K)$. □

Corolario 1.1.1. Sean K, L cuerpos numéricos tales que L es una extensión finita de K , y sean $\alpha_1, \dots, \alpha_n \in L$.

Si $L = K(\alpha_1, \dots, \alpha_n)$ y para cada $1 \leq i \leq n$, L contiene todas las raíces del polinomio mínimo de α_i . Entonces L es una extensión normal de K .

Demostración. Ya que α_i es algebraico sobre K para cada $1 \leq i \leq n$, entonces

$$L = K(\alpha_1, \dots, \alpha_n) = K(\alpha_1) \cdots (\alpha_n) = K[\alpha_1] \cdots [\alpha_n] = K[\alpha_1, \dots, \alpha_n],$$

y así

$$L = \{f(\alpha_1, \dots, \alpha_n) : f(x_1, \dots, x_n) \in K[x_1, \dots, x_n]\}.$$

Sea $\sigma : L \rightarrow \mathbb{C}$ un homomorfismo de L en \mathbb{C} que fija a K , entonces $\sigma(\alpha_i) \in L$ para cada $1 \leq i \leq n$ ya que $\sigma(\alpha_i)$ resulta ser una raíz del polinomio mínimo de α_i .

Sea $f(\alpha_1, \dots, \alpha_n) \in L$, entonces $\sigma(f(\alpha_1, \dots, \alpha_n)) = f(\sigma(\alpha_1), \dots, \sigma(\alpha_n)) \in L$, y por lo tanto $\sigma(L) \subseteq L$.

Entonces $\sigma(L) = L$ ya que $\sigma : L \rightarrow \sigma(L)$ es un isomorfismo de anillos, así σ es un automorfismo de L , por lo tanto, todo homomorfismo de L en \mathbb{C} que fija K es un automorfismo de L , esto implica que L es una extensión normal de K . □

Corolario 1.1.2. Sean K, L cuerpos numéricos tales que L es una extensión finita de K . Entonces existe M un cuerpo numérico que es extensión finita de L , y además, M es una extensión normal de K , y por lo tanto M es una extensión normal de L .

Demostración. Por el teorema del elemento primitivo, se tiene que $L = K(\alpha)$ para algún $\alpha \in L$. Sean $\alpha_1 := \alpha, \alpha_2, \dots, \alpha_n$ las raíces del polinomio mínimo de α sobre K , defínase

$$M := K(\alpha_1, \dots, \alpha_n),$$

así, M es un cuerpo numérico que es extensión finita de K , y por el corolario anterior se tiene que M es una extensión normal de K .

De otro lado

$$M = K(\alpha_1, \dots, \alpha_n) = K(\alpha_1)(\alpha_2, \dots, \alpha_n) = L(\alpha_2, \dots, \alpha_n),$$

entonces M es una extensión finita de L . El corolario anterior implica que M es una extensión normal de L . \square

Por otro lado, con ayuda de estos homomorfismos se estudian algunas propiedades importantes de los cuerpos numéricos.

Definición 1.1.2. Sea K un cuerpo numérico tal que $n = [K : \mathbb{Q}]$, y sean $\sigma_1, \dots, \sigma_n$ los homomorfismos de K en \mathbb{C} que fijan a \mathbb{Q} .

1. Sea $\alpha \in K$, se define la norma de α en K relativa a \mathbb{Q} como

$$N_{\mathbb{Q}}^K(\alpha) := \sigma_1(\alpha) \cdots \sigma_n(\alpha).$$

2. Sea $\alpha \in K$, se define la traza de α en K relativa a \mathbb{Q} como

$$Tr_{\mathbb{Q}}^K(\alpha) := \sigma_1(\alpha) + \cdots + \sigma_n(\alpha).$$

3. Sean $\alpha_1, \dots, \alpha_n \in K$, se define el discriminante de $\alpha_1, \dots, \alpha_n$ como

$$disc(\alpha_1, \dots, \alpha_n) := \det(A)^2$$

donde $A = [a_{ij}]$ y $a_{ij} = \sigma_i(\alpha_j)$ para $1 \leq i, j \leq n$.

En [17] se prueban las siguientes propiedades básicas de la norma, la traza y el discriminante,

$$N_{\mathbb{Q}}^K(\alpha), Tr_{\mathbb{Q}}^K(\alpha) \in \mathbb{Q},$$

y si además $\alpha \in \mathcal{O}_K$, entonces

$$N_{\mathbb{Q}}^K(\alpha), Tr_{\mathbb{Q}}^K(\alpha) \in \mathbb{Z}.$$

Además,

$$disc(\alpha_1, \dots, \alpha_n) \in \mathbb{Q},$$

y si además $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$, entonces

$$disc(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}.$$

Por otro lado, sea K un cuerpo numérico donde $[K : \mathbb{Q}] = n$ y sea $\alpha \in K$, si $f(x)$ es el polinomio mínimo de α sobre \mathbb{Q} tal que $gr(f(x)) = n$, en [9] se prueban dos nuevas maneras de calcular el discriminante:

1.

$$disc(1, \alpha, \dots, \alpha^{n-1}) = \prod_{i>j} (\sigma_i(\alpha) - \sigma_j(\alpha))^2.$$

2.

$$disc(1, \alpha, \dots, \alpha^{n-1}) = (-1)^{\frac{n!}{2(n-2)!}} \prod_{i=1}^n f'(\beta_i),$$

donde β_1, \dots, β_n son las n raíces de $f(x)$, y $\sigma_1, \dots, \sigma_n$ son los homomorfismos de K en \mathbb{C} que fijan a \mathbb{Q} .

Proposición 1.1.1. *Sea K un cuerpo numérico tal que $[K : \mathbb{Q}] = n$, y sea $\alpha \in \mathcal{O}_K$. Entonces α es una unidad de \mathcal{O}_K si y solo si $N_{\mathbb{Q}}^K(\alpha) = \pm 1$.*

Demostración. Supóngase que α es una unidad de \mathcal{O}_K , es decir que existe $\beta \in \mathcal{O}_K$ tal que $\alpha\beta = 1$, entonces

$$N_{\mathbb{Q}}^K(\alpha\beta) = N_{\mathbb{Q}}^K(\alpha)N_{\mathbb{Q}}^K(\beta) = 1,$$

puesto que $\alpha, \beta \in \mathcal{O}_K$, la proposición anterior implica que $N_{\mathbb{Q}}^K(\alpha), N_{\mathbb{Q}}^K(\beta) \in \mathbb{Z}$, y por lo tanto $N_{\mathbb{Q}}^K(\alpha) = \pm 1$.

Recíprocamente, supóngase que $N_{\mathbb{Q}}^K(\alpha) = \pm 1$, y sean $\sigma_1, \dots, \sigma_n$ los n homomorfismos de K en \mathbb{C} que fijan a \mathbb{Q} , sin pérdida de generalidad se puede suponer que $\sigma_1(k) = k$ para todo $k \in K$, y así

$$\begin{aligned} N_{\mathbb{Q}}^K(\alpha) &= \sigma_1(\alpha) \cdots \sigma_n(\alpha) \\ &= \alpha\beta \\ &= \pm 1. \end{aligned}$$

Donde $\beta := \sigma_2(\alpha) \cdots \sigma_n(\alpha)$, además, $\sigma_i(\alpha) \in \mathcal{O}_K$ para todo $1 \leq i \leq n$, esto implica que $\beta \in \mathcal{O}_K$ y por lo tanto α es una unidad de \mathcal{O}_K . \square

La siguiente proposición es usada para mostrar cuando un entero algebraico es irreducible.

Proposición 1.1.2. *Sea K un cuerpo numérico, y sea $\alpha \in \mathcal{O}_K$. Si $N_{\mathbb{Q}}^K(\alpha) = \pm p$ donde $p \in \mathbb{Z}$ es primo, entonces α es irreducible.*

Demostración. Nótese que $\alpha \neq 0$ pues cada homomorfismo de K en \mathbb{C} es inyectivo, además α no es una unidad de \mathcal{O}_K .

Ahora, supóngase que α no es irreducible, es decir existen $\beta, \gamma \in \mathcal{O}_K$ no unidades tal que $\alpha = \beta\gamma$. Entonces

$$N_{\mathbb{Q}}^K(\beta)N_{\mathbb{Q}}^K(\gamma) = \pm p,$$

puesto que p es primo y $N_{\mathbb{Q}}^K(\beta), N_{\mathbb{Q}}^K(\gamma) \in \mathbb{Z}$ se obtiene que $N_{\mathbb{Q}}^K(\beta) = \pm 1$ o $N_{\mathbb{Q}}^K(\gamma) = \pm 1$. Esto implica que β o γ son unidades, ya que esto contradice la suposición se concluye que α es una unidad de \mathcal{O}_K . \square

Note que el concepto de norma de un elemento se puede extender a una extensión finita L de K .

Definición 1.1.3. Sean $K \subseteq L$ cuerpos numéricos tales que $[L : K] = m$, y sean $\sigma_1, \dots, \sigma_m$ los homomorfismos de L en \mathbb{C} que fijan a K .

1. Sea $\alpha \in L$, se define la norma de α en L relativa a K como

$$N_K^L(\alpha) := \sigma_1(\alpha) \cdots \sigma_m(\alpha).$$

2. Sea $\alpha \in L$, se define la traza de α en L relativa a K como

$$Tr_K^L(\alpha) := \sigma_1(\alpha) + \cdots + \sigma_m(\alpha).$$

En [17] se presentan las siguientes propiedades básicas de la norma y la traza relativas,

$$N_K^L(\alpha), Tr_K^L(\alpha) \in K,$$

y si además $\alpha \in \mathcal{O}_L$, entonces

$$N_K^L(\alpha), Tr_K^L(\alpha) \in \mathcal{O}_K. \quad (\text{E.1.1})$$

Por otro lado, dado K un cuerpo numérico, en [17] se prueba que \mathcal{O}_K es un \mathbb{Z} -módulo libre donde $rank(\mathcal{O}_K) = [K : \mathbb{Q}]$. Esta es una propiedad importante del anillo de enteros algebraicos puesto que determina su estructura aditiva.

Definición 1.1.4. Sea K un cuerpo numérico tal que $n = [K : \mathbb{Q}]$, una \mathbb{Z} -base de \mathcal{O}_K se llama base entera de K .

Sea $\{\eta_1, \dots, \eta_n\}$ una base entera de K , se define el discriminante de K como

$$disc(K) := disc(\eta_1, \dots, \eta_n).$$

Ejemplo 1.1.1. Sea $K := \mathbb{Q}(\sqrt{-5})$ un cuerpo numérico. Hallar la norma y la traza para cualquier $\alpha \in K$, el anillo \mathcal{O}_K de enteros algebraicos de K , y el discriminante de K .

Primero, sean σ_1 y σ_2 los homomorfismos de K en \mathbb{C} que fijan a \mathbb{Q} definidos como

$$\sigma_1(a + b\sqrt{-5}) := a + b\sqrt{-5} \text{ y } \sigma_2(a + b\sqrt{-5}) := a - b\sqrt{-5}$$

para cada $a + b\sqrt{-5}$. Así, para cada $\alpha = a + b\sqrt{-5} \in K$ se tiene que la norma y la traza de α están dadas por

$$N_{\mathbb{Q}}^K(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha) = a^2 + 5b^2 \text{ y } Tr_{\mathbb{Q}}^K(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) = 2a.$$

Luego, nótese que el polinomio mínimo de $\sqrt{-5}$ sobre \mathbb{Q} es $x^2 + 5$, y por lo tanto el conjunto $\{1, \sqrt{-5}\}$ es una \mathbb{Q} -base de K .

Se afirma que $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$:

En efecto, sea $h = a + b\sqrt{-5} \in \mathbb{Z} + \mathbb{Z}\sqrt{-5}$, entonces $h = a + b\sqrt{-5}$ es raíz del polinomio

$$p(x) = x^2 - 2ax + a^2 + 5b^2 \in \mathbb{Z}[x],$$

y así $h \in \mathcal{O}_K$.

Para la otra contención, sea $h = a + b\sqrt{-5} \in \mathcal{O}_K$ donde $a, b \in \mathbb{Q}$, puesto que

$$\text{Tr}_{\mathbb{Q}}^K(h) = 2a \in \mathbb{Z} \text{ y } N_{\mathbb{Q}}^K(h) = a^2 + 5b^2 \in \mathbb{Z},$$

entonces $2a = m$ y $a^2 + 5b^2 = n$ donde $n, m \in \mathbb{Z}$.

Ya que $b \in \mathbb{Q}$, entonces $b = \frac{r}{s}$ con $r, s \in \mathbb{Z}$, $s \neq 0$ y $\text{mcd}(r, s) = 1$; luego

$$\frac{20r^2}{s^2} = 4n - 4a^2,$$

y así $s^2 | 20$, de modo que $s = 0$ ó $s = 1$.

Luego, se puede escribir

$$a = \frac{m}{2} \text{ y } b = \frac{t}{2}$$

donde $t = 2r$ ó $t = r$ según el caso.

Puesto que $a^2 + 5b^2 = n$, entonces $m^2 + 5t^2 = 4n$, es decir $m^2 + t^2 \equiv 0 \pmod{4}$, pero esta congruencia solo se tiene si m y t son pares, de aquí se obtiene que $a, b \in \mathbb{Z}$ y por lo tanto $h \in \mathbb{Z} + \mathbb{Z}\sqrt{-5}$. Esto implica la igualdad deseada.

Ahora, nótese que $\{1, \sqrt{-5}\}$ es una \mathbb{Z} -base de \mathcal{O}_K , luego, el discriminante de K está dado por

$$\text{disc}(K) = \text{disc}(1, \sqrt{-5}) = \det(A)^2$$

donde

$$A = \begin{pmatrix} 1 & \sqrt{-5} \\ 1 & -\sqrt{-5} \end{pmatrix}.$$

Por lo tanto $\text{disc}(K) = -20$. Esto concluye el ejemplo.

Ejemplo 1.1.2. El recíproco de la proposición 1.1.2 no es cierto. Sea $K = \mathbb{Q}(\sqrt{-5})$, en el ejemplo anterior se mostró que $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$.

Sea $\alpha = 1 + \sqrt{-5} \in \mathcal{O}_K$, entonces α es irreducible pero $N_{\mathbb{Q}}^K(\alpha) = 6$, que no es primo.

En efecto, supóngase que α no es irreducible, es decir, existen $\beta, \gamma \in \mathcal{O}_K$ no unidades tal que $\alpha = \beta\gamma$. Entonces

$$N_{\mathbb{Q}}^K(\alpha) = 6 = N_{\mathbb{Q}}^K(\beta)N_{\mathbb{Q}}^K(\gamma),$$

de aquí se desprenden dos casos: Si $N_{\mathbb{Q}}^K(\beta) = 2$ y $N_{\mathbb{Q}}^K(\gamma) = 3$, o $N_{\mathbb{Q}}^K(\beta) = 3$ y $N_{\mathbb{Q}}^K(\gamma) = 2$. Si $\beta = a + b\sqrt{-5}$, entonces $N_{\mathbb{Q}}^K(\beta) = a^2 + 5b^2$. En el primer caso se obtiene que

$$a^2 \equiv 2 \pmod{5},$$

y en el segundo caso se obtiene que

$$a^2 \equiv 3 \pmod{5}.$$

Ya que los únicos cuadrados $(\text{mod } 5)$ son $0, 1, 4$, entonces los dos casos son falsos. Esto implica que α es irreducible.

Lema 1.1.2. Sean K un cuerpo numérico y \mathfrak{a} un ideal no nulo de \mathcal{O}_K , entonces \mathfrak{a} contiene un entero m no nulo.

Demostración. Sea $\beta \in \mathfrak{a} \subseteq \mathcal{O}_K$ no nulo, y sea

$$p(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1} + x^n \in \mathbb{Z}[x]$$

un polinomio de grado mínimo tal que $p(\beta) = 0$.

Entonces

$$\beta^n + b_{n-1}\beta^{n-1} + \cdots + b_1\beta + b_0 = 0,$$

de donde

$$b_0 = -\left(b_1\beta + \cdots + b_{n-1}\beta^{n-1} + \beta^n\right) \in \mathfrak{a}.$$

Defínase $m := b_0$, así $m = b_0 \in \mathbb{Z} \cap \mathfrak{a}$ y es no nulo. De lo contrario

$$\beta^n + b_{n-1}\beta^{n-1} + \cdots + b_1\beta = 0,$$

y puesto que β es no nulo, se obtiene que

$$\beta^{n-1} + b_{n-1}\beta^{n-2} + \cdots + b_2\beta + b_1 = 0,$$

esto contradice la manera en que se eligió el polinomio $p(x)$. □

El siguiente corolario permite definir la norma de un ideal del anillo de enteros algebraicos.

Corolario 1.1.3. Si K es un cuerpo numérico y \mathfrak{a} es un ideal no nulo de \mathcal{O}_K entonces el anillo cociente $\mathcal{O}_K/\mathfrak{a}$ es finito.

Demostración. Ya que \mathfrak{a} es un ideal no nulo de \mathcal{O}_K , el lema anterior implica que existe $m \in \mathbb{Z}$ no nulo tal que $m \in \mathfrak{a}$, considere la función

$$f : \mathcal{O}_K/m\mathcal{O}_K \longrightarrow \mathcal{O}_K/\mathfrak{a}$$

definida como $f(\bar{k}) := \bar{k}$, así f es sobreyectiva y por lo tanto $|\mathcal{O}_K/\mathfrak{a}| \leq |\mathcal{O}_K/m\mathcal{O}_K|$.

Ya que \mathcal{O}_K es un \mathbb{Z} -módulo libre de $\text{rank}(\mathcal{O}_K) = n$, se obtiene que $\mathcal{O}_K/m\mathcal{O}_K \cong (\mathbb{Z}/m\mathbb{Z})^n$ como \mathbb{Z} -módulos, así, se concluye que $\mathcal{O}_K/\mathfrak{a}$ es finito. □

Dado \mathfrak{a} un ideal no nulo de \mathcal{O}_K , se define su norma como $\|\mathfrak{a}\| := |\mathcal{O}_K/\mathfrak{a}|$, la norma de un ideal está bien definida pues es finita.

Definición 1.1.5. Sea R un dominio de integridad y K su cuerpo de fracciones, se dice que R es un dominio de Dedekind si satisface las siguientes condiciones:

1. R es integralmente cerrado en K , es decir, si $\alpha \in K$ es raíz de un polinomio mónico con coeficientes en R , entonces $\alpha \in R$.
2. R es Noetheriano, es decir, para cualquier cadena de ideales $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \dots$ de R existe $n \geq 1$ tal que $\mathfrak{a}_n = \mathfrak{a}_{n+i}$ para todo $i \geq 1$.
3. Cada ideal primo no nulo de R es maximal.

Teorema 1.1.2. Sea K un cuerpo numérico y \mathcal{O}_K su anillo de enteros algebraicos, entonces \mathcal{O}_K es un dominio de Dedekind, es decir:

1. \mathcal{O}_K es integralmente cerrado en K .
2. \mathcal{O}_K es Noetheriano.
3. Cada ideal primo no nulo de \mathcal{O}_K es maximal.

Demostración. 1. Sea $\alpha \in K$ una raíz del polinomio

$$p(x) := a_0 + a_1x + \dots + a_{n-1}x^{n-1} + x^n \in \mathcal{O}_K[x],$$

y defínase $W := \mathbb{Z}[a_0, a_1, \dots, a_{n-1}, \alpha]$.

W resulta ser un \mathbb{Z} -módulo finitamente generado pues para todo $0 \leq i \leq n-1$ se tiene que $\mathbb{Z}[a_i]$ es un \mathbb{Z} -módulo finitamente generado; además $\alpha W \subseteq W$, y así $\alpha \in \mathcal{O}_K$.

2. Sea $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \dots \subseteq \mathcal{O}_K$ una cadena ascendente de ideales de \mathcal{O}_K , entonces la cadena de subgrupos $0 \subseteq \mathfrak{a}_2/\mathfrak{a}_1 \subseteq \dots \subseteq \mathcal{O}_K/\mathfrak{a}_1$ se detiene ya que $\mathcal{O}_K/\mathfrak{a}_1$ es finito, luego existe $n \geq 1$ tal que $\mathfrak{a}_n = \mathfrak{a}_{n+i}$ para todo $i \geq 1$.
3. Sea \mathfrak{p} un ideal primo no nulo de \mathcal{O}_K , entonces $\mathcal{O}_K/\mathfrak{p}$ es un dominio de integridad finito, luego es un cuerpo y por lo tanto \mathfrak{p} es un ideal maximal de \mathcal{O}_K . □

A continuación, se presenta un ejemplo de que no todos los anillos \mathcal{O}_K son dominios de factorización única, aunque si son dominios de Dedekind.

Ejemplo 1.1.3. En los dominios de Dedekind no se tiene en general unicidad en la factorización de sus elementos.

Sea $K = \mathbb{Q}(\sqrt{-5})$, en el ejemplo 1.1.1 se mostró que $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$. Este anillo es un dominio de Dedekind donde no se tiene factorización única de sus elementos, ya que

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$$

son dos factorizaciones diferentes de 6 en elementos irreducibles.

1. $1 + \sqrt{-5}$ es un elemento irreducible de \mathcal{O}_K : Esto ya se probó en el ejemplo anterior.
2. $1 - \sqrt{-5}$ es un elemento irreducible de \mathcal{O}_K : Análogo al anterior.
3. 2 es un elemento irreducible de \mathcal{O}_K : Supóngase que 2 no es irreducible, es decir, existen $\alpha, \beta \in \mathcal{O}_K$ no unidades tal que $2 = \alpha\beta$. Entonces

$$4 = N_{\mathbb{Q}}^K(2) = N_{\mathbb{Q}}^K(\alpha)N_{\mathbb{Q}}^K(\beta),$$

luego, $N_{\mathbb{Q}}^K(\alpha) = 2$. Si $\alpha = a + b\sqrt{-5} \in \mathcal{O}_K$, entonces $a^2 \equiv 2 \pmod{5}$, esto es una contradicción. Por lo tanto 2 es irreducible.

4. 3 es un elemento irreducible de \mathcal{O}_K : Análogo al anterior.

Por ultimo, note que $\mathcal{O}_K^* = \{\pm 1\}$. Esto implica que ni 2 ni 3 son asociados a $1 + \sqrt{-5}$ ni a $1 - \sqrt{-5}$, y así las dos factorizaciones son diferentes.

Definición 1.1.6. Sea R un anillo, y sean $\mathfrak{a}, \mathfrak{b}$ ideales de R , se dice que \mathfrak{a} divide a \mathfrak{b} si existe \mathfrak{c} un ideal de R tal que $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$, y se denota por $\mathfrak{a}|\mathfrak{b}$.

Dado D un dominio de Dedekind, y $\mathfrak{a}, \mathfrak{b}$ dos ideales de D , en [17] se prueba que $\mathfrak{a}|\mathfrak{b}$ si y solo si $\mathfrak{b} \subseteq \mathfrak{a}$.

Una propiedad importante de los dominios de Dedekind es que tienen unicidad en la factorización en ideales primos de todo ideal no nulo.

Sea K un cuerpo numérico y \mathfrak{a} un ideal no nulo de \mathcal{O}_K , en [17] se prueba que

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

donde $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ son ideales primos de \mathcal{O}_K , y además, que esta factorización es única salvo el orden.

Luego agrupando y renombrando todos los ideales primos que son iguales, se obtiene una escritura de la forma

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}.$$

Definición 1.1.7. Sea K un cuerpo numérico y \mathcal{O}_K su anillo de enteros algebraicos. Sea \mathfrak{p} un ideal primo de \mathcal{O}_K , al cuerpo finito $\mathcal{O}_K/\mathfrak{p}$ se le llama cuerpo residuo de \mathfrak{p} .

1.2. CUERPOS FINITOS

En esta sección se introduce el concepto de un cuerpo finito, que se caracteriza por su tamaño.

En [10] se demuestran algunas propiedades de los cuerpos finitos.

Dado F un cuerpo finito, entonces:

1. La característica del cuerpo F es un primo p , es decir $\text{char}(F) = p$.
2. El subcuerpo primo P de F es isomorfo a $\mathbb{Z}/p\mathbb{Z}$. Donde el subcuerpo primo P se define como la intersección de todos los subcuerpos de F .
3. $|F| = p^k$, donde $k := [F : P]$.
4. Existe un cuerpo finito de tamaño p^k , y está conformado por todas las raíces del polinomio $x^{p^k} - x$ sobre P . Este cuerpo es único salvo isomorfismo.

De aquí en adelante, cuando se consideren F, K cuerpos numéricos tal que F es una extensión de Galois de K , se entiende que, F es una extensión finita, normal y separable de K .

A continuación, si se tiene una extensión de cuerpos finitos que es de Galois, el grupo de Galois resulta ser un grupo cíclico generado por el automorfismo de Frobenius.

Lema 1.2.1. Sean F un cuerpo finito y $p \in \mathbb{Z}$ un primo tales que $\text{char}(F) = p$. Entonces

$$\begin{aligned}\gamma : F &\rightarrow F \\ x &\mapsto \gamma(x) := x^p\end{aligned}$$

es un automorfismo de F , que fija a P .

Este automorfismo es llamado el automorfismo de Frobenius.

Demostración. Sean $x, y \in F$, entonces

$$\begin{aligned}\gamma(x + y) &= (x + y)^p \\ &= \sum_{r=0}^p \binom{p}{r} x^{p-r} y^r \\ &= x^p + \sum_{r=1}^{p-1} \binom{p}{r} x^{p-r} y^r + y^p \\ &= x^p + y^p \\ &= \gamma(x) + \gamma(y).\end{aligned}$$

Es decir $\gamma(x + y) = \gamma(x) + \gamma(y)$. Además

$$\gamma(xy) = (xy)^p = x^p y^p = \gamma(x)\gamma(y)$$

y así $\gamma(xy) = \gamma(x)\gamma(y)$. Por ultimo $\gamma(1) = 1^p = 1$, por lo tanto γ es un homomorfismo de anillos.

Ya que F es un cuerpo entonces γ es inyectivo, además, por el teorema de la dimensión se tiene que γ es sobreyectivo.

Por ultimo, sea $q \in P$, entonces $\gamma(q) = \gamma(q^1) = q\gamma(1) = q$, así se concluye que γ es un automorfismo de F que fija a P . \square

Proposición 1.2.1. Sean F un cuerpo finito y P su subcuerpo primo tales que $|F| = p^n$, donde $p \in \mathbb{Z}$ es primo y $n = [F : P]$. Entonces F es una extensión de Galois de P , y $Gal(F/P)$ es un grupo cíclico generado por el automorfismo de Frobenius.

Demostración. Por hipótesis, F es un cuerpo finito con $|F| = p^n$ donde $n = [F : P]$, entonces F es una extensión finita de P . También se tiene que F es el cuerpo de descomposición del polinomio $x^{p^n} - x$ sobre P , esto implica que F es una extensión normal de P . Y por ultimo, se tiene que P es un cuerpo perfecto por ser finito, entonces F es una extensión separable de P . Esto implica que F es una extensión de Galois de P .

Por lo tanto $|Gal(F/P)| = [F : P] = n$, y además se tiene que γ tiene orden n . En efecto, supóngase que existe $1 \leq l \leq n - 1$ tal que $\gamma^l = i_F$, entonces para todo $a \in F$ se tiene que

$$\gamma^l(a) = i_F(a),$$

es decir, para todo $a \in F$ se tiene

$$a^{p^l} = a.$$

Esto implica que el polinomio $x^{p^l} - x$ tiene p^l raíces diferentes, de modo que se llega a una contradicción. Por lo tanto $Gal(F/P)$ es un grupo cíclico generado por el automorfismo de Frobenius γ . \square

Proposición 1.2.2. Sean F, K cuerpos finitos tales que F es una extensión de K , entonces F es una extensión de Galois de K , y $Gal(F/K)$ es un grupo cíclico.

Demostración. Nótese que $[F : P] = [F : K][K : P]$, pero $[F : P]$ es finito, entonces $[F : K]$ es finito. Además, como F es extensión normal y separable de P , entonces F es extensión normal y separable de K , esto implica que F es una extensión de Galois de K .

Por otro lado, se tiene que $Gal(F/K)$ es un subgrupo de $Gal(F/P)$, de modo que $Gal(F/K)$ es un grupo cíclico, puesto que $Gal(F/P)$ es cíclico generado por el automorfismo de Frobenius γ de la proposición anterior.

Supóngase que $|F| = p^n$ y $|K| = p^m$, donde $[F : P] = n$, $[K : P] = m$ y $p \in \mathbb{Z}$ es primo, entonces $m|n$. Note que m es el menor entero positivo tal que $\gamma^m \in Gal(F/K)$.

En efecto, sea $k \in K$, entonces $k^{p^m} - k = 0$, por lo tanto

$$\gamma^m(k) = k^{p^m} = k,$$

y así, $\gamma^m \in \text{Gal}(F/K)$. Por un argumento similar al de la proposición anterior se tiene que m es el menor entero positivo con esta propiedad, esto implica que $\text{Gal}(F/K)$ es cíclico generado por γ^m . \square

1.3. IDEALES FRACCIONARIOS

En esta sección se introduce el concepto de ideal fraccionario en \mathcal{O}_K que generaliza la noción de ideal. También, se muestra que la colección de ideales fraccionarios resulta un grupo abeliano con el producto de ideales fraccionarios, esto permite definir el grupo de clases de ideales.

Definición 1.3.1. Sea K un cuerpo numérico y \mathcal{O}_K su anillo de enteros algebraicos, un ideal fraccionario de K es un conjunto no vacío de la forma $\alpha\mathfrak{a}$ donde $\alpha \in K$ es no nulo y \mathfrak{a} es un ideal no nulo de \mathcal{O}_K .

Nótese que si $\alpha = 1$, entonces todo ideal no nulo de \mathcal{O}_K es un ideal fraccionario de K .

Ya que K es el cuerpo de fracciones de \mathcal{O}_K , se tiene la inyección canónica $\mathcal{O}_K \hookrightarrow K$. Así se puede considerar a K como un \mathcal{O}_K -módulo.

Proposición 1.3.1. Sea K un cuerpo numérico y \mathcal{O}_K su anillo de enteros algebraicos, sea $\mathfrak{b} \subseteq K$ un \mathcal{O}_K -módulo. Entonces \mathfrak{b} es un ideal fraccionario de K si y solo si \mathfrak{b} es finitamente generado.

Demostración. Supóngase que \mathfrak{b} es un ideal fraccionario de K , entonces

$$\mathfrak{b} = \frac{r}{s}\mathfrak{a}$$

donde $r, s \in \mathcal{O}_K$ no nulos, y \mathfrak{a} es un ideal no nulo de \mathcal{O}_K . Ya que \mathcal{O}_K es noetheriano entonces $\mathfrak{a} = \langle u_1, \dots, u_n \rangle$ y por lo tanto se tiene que $\mathfrak{b} = \langle \frac{ru_1}{s}, \dots, \frac{ru_n}{s} \rangle$, es decir \mathfrak{b} es finitamente generado.

Ahora, supóngase que \mathfrak{b} es un \mathcal{O}_K -módulo finitamente generado, entonces

$$\mathfrak{b} = \left\langle \frac{r_1}{s_1}, \dots, \frac{r_n}{s_n} \right\rangle,$$

donde $\frac{r_i}{s_i} \in K$ para cada $1 \leq i \leq n$. Entonces se tiene que

$$\mathfrak{b} = \frac{1}{s} \langle s_2 \cdots s_n r_1, \dots, s_1 \cdots s_{n-1} r_n \rangle,$$

donde $s := s_1 \cdots s_n$, y por lo tanto \mathfrak{b} es un ideal fraccionario de K . \square

Se denota al conjunto de todos los ideales fraccionarios de K por I_K , además se extiende el producto de ideales a ideales fraccionarios como sigue:

Sean \mathfrak{b} y \mathfrak{b}' ideales fraccionarios de K , entonces $\mathfrak{b} = \alpha\mathfrak{a}$ y $\mathfrak{b}' = \alpha'\mathfrak{a}'$ donde $\alpha, \alpha' \in K$ y $\mathfrak{a}, \mathfrak{a}'$ son ideales de \mathcal{O}_K , entonces

$$\mathfrak{b}\mathfrak{b}' = (\alpha\mathfrak{a})(\alpha'\mathfrak{a}') = \alpha\alpha'\mathfrak{a}\mathfrak{a}'$$

Por lo tanto el producto de dos ideales fraccionarios de K es de nuevo un ideal fraccionario de K , además, por la siguiente proposición I_K resulta ser un grupo abeliano con este producto donde el elemento neutro es \mathcal{O}_K .

Proposición 1.3.2. *Sea K un cuerpo numérico y \mathcal{O}_K su anillo de enteros algebraicos, si \mathfrak{b} es un ideal fraccionario de K entonces \mathfrak{b} es invertible, es decir existe un ideal fraccionario de K denotado por \mathfrak{b}^{-1} tal que $\mathfrak{b}\mathfrak{b}^{-1} = \mathcal{O}_K$.*

Demostración. Defínase \mathfrak{b}^{-1} como $\mathfrak{b}^{-1} := \{\alpha \in K : \alpha\mathfrak{b} \subseteq \mathcal{O}_K\}$. □

Ejemplo 1.3.1. Sea $K = \mathbb{Q}(\sqrt{-5})$ un cuerpo numérico, anteriormente se vio que

$$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{-5}.$$

Sea

$$\mathfrak{b} := \frac{1 + \sqrt{-5}}{3}\mathcal{O}_K$$

un ideal fraccionario de K .

Para calcular el ideal fraccionario $\mathfrak{b}^{-1} = \{\alpha \in K : \alpha\mathfrak{b} \subseteq \mathcal{O}_K\}$ basta hallar el inverso de

$$\frac{1 + \sqrt{-5}}{3}$$

en K .

Entonces

$$\left(\frac{1 + \sqrt{-5}}{3}\right)^{-1} = \frac{1 - \sqrt{-5}}{2}.$$

Por lo tanto,

$$\mathfrak{b}^{-1} = \frac{1 - \sqrt{-5}}{2}\mathcal{O}_K.$$

La siguiente definición generaliza la divisibilidad entre ideales.

Definición 1.3.2. *Sea K un cuerpo numérico y \mathcal{O}_K su anillo de enteros algebraicos, y sean $\mathfrak{a}, \mathfrak{b}$ ideales fraccionarios de K . Se dice que \mathfrak{a} divide a \mathfrak{b} si existe \mathfrak{c} un ideal de \mathcal{O}_K tal que $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$, y se denota por $\mathfrak{a}|\mathfrak{b}$.*

Además, nótese que la divisibilidad entre ideales fraccionarios es una relación de orden.

La siguiente proposición es una generalización a ideales fraccionarios de la factorización única de un ideal no nulo en ideales primos.

Proposición 1.3.3. *Sea K un cuerpo numérico y \mathcal{O}_K su anillo de enteros algebraicos, si \mathfrak{b} es un ideal fraccionario de K , entonces $\mathfrak{b} = \prod_{i=1}^r \mathfrak{p}_i^{m_i}$ donde \mathfrak{p}_i son ideales primos de \mathcal{O}_K y $m_i \in \mathbb{Z}$ para cada $1 \leq i \leq r$. Además, la factorización es única salvo el orden.*

Demostración. Sea \mathfrak{b} un ideal fraccionario de K , entonces $\mathfrak{b} = \frac{e}{f} \mathfrak{a}$ donde $e, f \in \mathcal{O}_K$ no nulos, y \mathfrak{a} un ideal no nulo de \mathcal{O}_K . Ya que $e\mathfrak{a} = \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_t^{m_t}$ y $f\mathcal{O}_K = \mathfrak{q}_1^{n_1} \cdots \mathfrak{q}_v^{n_v}$ de forma única donde $\mathfrak{p}_i, \mathfrak{q}_j$ son ideales primos de \mathcal{O}_K para cada $1 \leq i \leq t$ y $1 \leq j \leq v$, luego como $(f\mathcal{O}_K)^{-1} = \frac{1}{f}\mathcal{O}_K$, entonces

$$\mathfrak{b} = \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_t^{m_t} \mathfrak{q}_1^{-n_1} \cdots \mathfrak{q}_v^{-n_v}.$$

Renombrando cada ideal se obtiene la factorización deseada; y la unicidad de tal factorización se obtiene de la unicidad en la factorización de $e\mathfrak{a}$ y $f\mathcal{O}_K$. \square

Definición 1.3.3. Sea K un cuerpo numérico y \mathcal{O}_K su anillo de enteros algebraicos, un ideal fraccionario \mathfrak{b} de K se dice principal si \mathfrak{b} como \mathcal{O}_K -submódulo de K es generado por un solo elemento, es decir $\mathfrak{b} = \alpha\mathcal{O}_K$ para algún $\alpha \in K - \{0\}$.

Se denota al conjunto de todos los ideales fraccionarios principales de K por P_K , además P_K resulta ser un subgrupo de I_K .

El cociente I_K/P_K es llamado grupo de clases de ideales de \mathcal{O}_K y se denota por $C(\mathcal{O}_K)$. Además, en [17] se prueba que este grupo tiene la propiedad de ser finito.

El cardinal del grupo $C(\mathcal{O}_K)$ es llamado el número de clases del cuerpo K , de tal forma que establece qué tan lejos están los ideales de \mathcal{O}_K de ser principales y así, ser un dominio de factorización única.

Proposición 1.3.4. *Sea K un cuerpo numérico y \mathcal{O}_K su anillo de enteros algebraicos. El anillo \mathcal{O}_K es un DIP si y solo si $C(\mathcal{O}_K)$ es el grupo trivial.*

Demostración. Supóngase que \mathcal{O}_K es un DIP, y sea $\mathfrak{b} \in I_K$, entonces $\mathfrak{b} = \alpha\mathfrak{a}$ donde $\alpha \in K$ y \mathfrak{a} es un ideal de \mathcal{O}_K . Luego, $\mathfrak{a} = e\mathcal{O}_K$ para algún $e \in \mathcal{O}_K$, esto implica que $\mathfrak{b} = \alpha'\mathcal{O}_K$ donde $\alpha' := \alpha e \in K$, y por lo tanto $\mathfrak{b} \in P_K$, es decir que $C(\mathcal{O}_K)$ es trivial.

Recíprocamente, supóngase que $C(\mathcal{O}_K)$ es trivial y sea \mathfrak{a} un ideal no nulo de \mathcal{O}_K , viendo este ideal como un elemento de I_K se tiene que $\mathfrak{a} = \alpha\mathcal{O}_K$ para algún $\alpha \in K$, esto implica que $\alpha \in \mathcal{O}_K$ y así \mathfrak{a} es un ideal principal de \mathcal{O}_K , es decir \mathcal{O}_K es un DIP. \square

Ejemplo 1.3.2. Sea $K = \mathbb{Q}(\sqrt{-5})$ un cuerpo numérico, en el ejemplo 1.1.3 se mostró que $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$ no es un dominio de factorización única, en este ejemplo se muestra explícitamente que no es un DIP.

En efecto, sea $\mathfrak{a} = 2\mathcal{O}_K + (1 + \sqrt{-5})\mathcal{O}_K$ el ideal de \mathcal{O}_K generado por 2 y $1 + \sqrt{-5}$, entonces \mathfrak{a} no es principal.

Supóngase que existe $x \in \mathcal{O}_K$ tal que $\mathfrak{a} = x\mathcal{O}_K$. Puesto que $2, 1 + \sqrt{-5} \in \mathfrak{a}$ entonces existen $k_1, k_2 \in \mathcal{O}_K$ tal que $2 = xk_1$ y $1 + \sqrt{-5} = xk_2$, esto implica que

$$N_{\mathbb{Q}}^K(2) = N_{\mathbb{Q}}^K(x)N_{\mathbb{Q}}^K(k_1) \text{ y } N_{\mathbb{Q}}^K(1 + \sqrt{-5}) = N_{\mathbb{Q}}^K(x)N_{\mathbb{Q}}^K(k_2).$$

Es decir,

$$N_{\mathbb{Q}}^K(x) \mid 4 \text{ y } N_{\mathbb{Q}}^K(x) \mid 6,$$

por lo tanto $N_{\mathbb{Q}}^K(x) \in \{\pm 1, \pm 2\}$.

Si $x = a + b\sqrt{-5} \in \mathcal{O}_K$, entonces $N_{\mathbb{Q}}^K(x) = a^2 + 5b^2$, esto implica que $x = \pm 1$, y así

$$\mathfrak{a} = \mathbb{Z} + \mathbb{Z}\sqrt{-5}.$$

Ahora, nótese que $1 \notin \mathfrak{a} = 2\mathcal{O}_K + (1 + \sqrt{-5})\mathcal{O}_K$. Ya que si $1 \in \mathfrak{a} = 2\mathcal{O}_K + (1 + \sqrt{-5})\mathcal{O}_K$ entonces

$$1 = 2(\lambda_1 + \lambda_2\sqrt{-5}) + (1 + \sqrt{-5})(\theta_1 + \theta_2\sqrt{-5})$$

donde $\lambda_1, \lambda_2, \theta_1, \theta_2 \in \mathbb{Z}$, entonces se obtiene el sistema de ecuaciones

$$\left. \begin{aligned} 2\lambda_1 + \theta_1 - 5\theta_2 &= 1 \\ 2\lambda_2 + \theta_1 + \theta_2 &= 0 \end{aligned} \right\}$$

que no tiene solución en \mathbb{Z} , por lo tanto $1 \notin \mathfrak{a}$. Esto es una contradicción, así se concluye que \mathfrak{a} no es un ideal principal y el grupo $C(\mathcal{O}_K)$ es no trivial.

CAPÍTULO 2

RAMIFICACIÓN

En este capítulo se presentan dos tópicos importantes de la teoría algebraica de números, uno de estos tópicos es la ramificación de ideales, es decir, se estudia la factorización de un ideal primo en una extensión finita. Se realiza un estudio cuidadoso de cuerpos numéricos particulares, aplicando allí la teoría que se va desarrollando. Un teorema importante de este capítulo es el teorema de Kummer-Dedekind, tal teorema es bastante útil para calcular la factorización en ideales primos.

El otro tópico central de este capítulo es el símbolo y el homomorfismo de Artin, usados para enunciar el teorema de Artin para el cuerpo de clases de Hilbert.

2.1. DEFINICIÓN Y PROPIEDADES

Sean K y L cuerpos numéricos tales que L es una extensión finita de K , y sean \mathcal{O}_K y \mathcal{O}_L los anillos de enteros algebraicos de K y L respectivamente. Sea \mathfrak{p} un ideal primo de \mathcal{O}_K , entonces el ideal generado por \mathfrak{p} en \mathcal{O}_L es

$$\mathfrak{p}\mathcal{O}_L = \{p_1l_1 + \cdots + p_nl_n \mid p_i \in \mathfrak{p}, l_i \in \mathcal{O}_L, 1 \leq i \leq n, n \geq 1\}.$$

Este ideal puede que ya no sea primo en \mathcal{O}_L , la teoría de la ramificación estudia la factorización de $\mathfrak{p}\mathcal{O}_L$ en ideales primos de \mathcal{O}_L .

Proposición 2.1.1. *Sean K y L cuerpos numéricos tales que L es una extensión de K , y sean \mathcal{O}_K y \mathcal{O}_L los anillos de enteros algebraicos de K y L respectivamente. Sean \mathfrak{p} un ideal primo de \mathcal{O}_K y \mathfrak{P} un ideal primo de \mathcal{O}_L , las siguientes condiciones son equivalentes:*

1. $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L$.
2. $\mathfrak{p}\mathcal{O}_L \subseteq \mathfrak{P}$.
3. $\mathfrak{p} \subseteq \mathfrak{P}$.
4. $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$.

5. $\mathfrak{P} \cap K = \mathfrak{p}$.

Demostración. (1) \Rightarrow (2) : Por definición.

(2) \Rightarrow (3) : Se tiene ya que $\mathfrak{p} \subseteq \mathfrak{p}\mathcal{O}_L$.

(3) \Rightarrow (4) : Supóngase que $\mathfrak{p} \subseteq \mathfrak{P}$, entonces $\mathfrak{p} = \mathfrak{p} \cap \mathcal{O}_K \subseteq \mathfrak{P} \cap \mathcal{O}_K$ es decir que $\mathfrak{p} \subseteq \mathfrak{P} \cap \mathcal{O}_K$. Note que $\mathfrak{P} \cap \mathcal{O}_K$ es un ideal de \mathcal{O}_K , pero por ser \mathfrak{p} un ideal primo de \mathcal{O}_K es maximal y por lo tanto se tiene la igualdad.

(4) \Rightarrow (5) : Supóngase que $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$, ya que $\mathcal{O}_K = \mathbb{A} \cap K$ donde \mathbb{A} son los enteros algebraicos de \mathbb{C} , entonces se tiene la igualdad.

(5) \Rightarrow (1) : Supóngase que $\mathfrak{P} \cap K = \mathfrak{p}$, entonces $\mathfrak{p} \subseteq \mathfrak{P}$ y por lo tanto $\mathfrak{p}\mathcal{O}_L \subseteq \mathfrak{P}$, es decir que $\mathfrak{P} | \mathfrak{p}\mathcal{O}_L$. \square

Si se tiene alguna condición de la proposición anterior se dice que el ideal \mathfrak{P} contiene \mathfrak{p} . Además, de la proposición anterior se tiene que los ideales primos de \mathcal{O}_L que contienen al ideal primo \mathfrak{p} de \mathcal{O}_K son los únicos que aparecen en la factorización de $\mathfrak{p}\mathcal{O}_L$.

Observación 2.1.1. Sean K y L cuerpos numéricos tales que L es una extensión finita de K , y sean \mathcal{O}_K y \mathcal{O}_L los anillos de enteros algebraicos de K y L respectivamente. Sea \mathfrak{p} un ideal primo de \mathcal{O}_K , ya que $\mathfrak{p}\mathcal{O}_L$ es un ideal de \mathcal{O}_L , entonces

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

donde $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ son los únicos ideales primos de \mathcal{O}_L que contienen a \mathfrak{p} .

Definición 2.1.1. Los enteros positivos e_i se llaman índices de ramificación de \mathfrak{p} en \mathfrak{P}_i para cada $1 \leq i \leq r$, y se denotan por $e_i := e_{\mathfrak{P}_i | \mathfrak{p}}$.

Observación 2.1.2. Sean K y L cuerpos numéricos tales que L es una extensión finita de K , y sean \mathcal{O}_K y \mathcal{O}_L los anillos de enteros algebraicos de K y L respectivamente. Sea \mathfrak{p} un ideal primo de \mathcal{O}_K , entonces

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

donde $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ son los ideales primos de \mathcal{O}_L que contienen a \mathfrak{p} . Ya que $\mathcal{O}_K/\mathfrak{p} \subseteq \mathcal{O}_L/\mathfrak{P}_i$ para cada $1 \leq i \leq r$, y como los cuerpos $\mathcal{O}_K/\mathfrak{p}$, $\mathcal{O}_L/\mathfrak{P}_i$ son finitos entonces $\mathcal{O}_L/\mathfrak{P}_i$ es una extensión finita de $\mathcal{O}_K/\mathfrak{p}$, así

$$[\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}] := f_i$$

Definición 2.1.2. Los enteros positivos f_i se llaman los grados inerciales de \mathfrak{P}_i sobre \mathfrak{p} para cada $1 \leq i \leq r$, y se denotan por $f_i := f_{\mathfrak{P}_i | \mathfrak{p}}$.

Notación 1. Sea R un anillo y \mathfrak{a} un ideal de R , se denota la norma de un ideal como

$$\|\mathfrak{a}\| := |R/\mathfrak{a}|.$$

Dado K un cuerpo numérico tal que $[K : \mathbb{Q}] := n$, en [17] y [1] se demuestran las siguientes propiedades de la norma de ideales.

1. Si $\mathfrak{a}, \mathfrak{b}$ son ideales de \mathcal{O}_K entonces

$$\| \mathfrak{a} \mathfrak{b} \| = \| \mathfrak{a} \| \| \mathfrak{b} \| .$$

2. Sea $\alpha \in \mathcal{O}_K$ no nulo, entonces

$$\| \alpha \mathcal{O}_K \| = |N_{\mathbb{Q}}^K(\alpha)|.$$

La siguiente proposición relaciona los índices de ramificación y los grados de inercia en la factorización de un primo en \mathbb{Z} .

Nótese que $(p\mathbb{Z})\mathcal{O}_K = p\mathcal{O}_K$, teniendo esto en cuenta se simplificará la notación.

Proposición 2.1.2. *Sea K un cuerpo numérico tal que $[K : \mathbb{Q}] = m$, y sea $p \in \mathbb{Z}$ un primo tal que su factorización en \mathcal{O}_K está dada por*

$$p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g},$$

donde $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ son ideales primos de \mathcal{O}_K . Si f_1, \dots, f_g son los grados inerciales de \mathfrak{P}_i sobre p , entonces

$$\sum_{i=1}^g e_i f_i = m.$$

Demostración. Puesto que $p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$, y para cada $1 \leq i \leq g$ se tiene

$$\| \mathfrak{P}_i \| = |\mathcal{O}_K / \mathfrak{P}_i| = |\mathbb{Z} / p\mathbb{Z}|^{[\mathcal{O}_K / \mathfrak{P}_i : \mathbb{Z} / p\mathbb{Z}]} = |\mathbb{Z} / p\mathbb{Z}|^{f_i} = p^{f_i},$$

entonces

$$\begin{aligned} \| p\mathcal{O}_K \| &= \| \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g} \| \\ &= \prod_{i=1}^g \| \mathfrak{P}_i \|^{e_i} \\ &= \prod_{i=1}^g (p^{f_i})^{e_i} \\ &= p^{\sum_{i=1}^g f_i e_i} \end{aligned}$$

y $\| p\mathcal{O}_K \| = |N_{\mathbb{Q}}^K(p)| = p^m$, así se concluye que

$$\sum_{i=1}^g e_i f_i = m.$$

□

Por otro lado, sean K y L cuerpos numéricos tales que L es una extensión finita de K con $[L : K] := n$, en [17] se prueba que si \mathfrak{a} es un ideal de \mathcal{O}_K , entonces

$$\| \mathfrak{a} \mathcal{O}_L \| = \| \mathfrak{a} \|^n .$$

Con ayuda de este hecho se puede probar el siguiente teorema, este es una generalización de la proposición 2.1.2.

Teorema 2.1.1. *Sean K y L cuerpos numéricos tales que L es una extensión finita de K y $[L : K] := n$. Sea \mathfrak{p} un ideal primo de \mathcal{O}_K y su factorización en \mathcal{O}_L*

$$\mathfrak{p} \mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

donde $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ son los ideales primos de \mathcal{O}_L que contienen a \mathfrak{p} .

Si f_1, \dots, f_r son los grados inerciales de \mathfrak{P}_i sobre \mathfrak{p} entonces

$$\sum_{i=1}^r e_i f_i = n .$$

Demostración. Puesto que $\mathfrak{p} \mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$, entonces

$$\| \mathfrak{P}_i \| = |\mathcal{O}_L / \mathfrak{P}_i| = |\mathcal{O}_K / \mathfrak{p}|^{[\mathcal{O}_L / \mathfrak{P}_i : \mathcal{O}_K / \mathfrak{p}]} = \| \mathfrak{p} \|^{f_i},$$

luego

$$\begin{aligned} \| \mathfrak{p} \mathcal{O}_L \| &= \| \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} \| \\ &= \prod_{i=1}^r \| \mathfrak{P}_i \|^{e_i} \\ &= \prod_{i=1}^r (\| \mathfrak{p} \|^{f_i})^{e_i} \\ &= \| \mathfrak{p} \|^{\sum_{i=1}^r f_i e_i}, \end{aligned}$$

por otro lado se tiene que $\| \mathfrak{p} \mathcal{O}_L \| = \| \mathfrak{p} \|^n$, de esta manera se concluye que

$$\sum_{i=1}^r e_i f_i = n .$$

□

Proposición 2.1.3. *Sea K un cuerpo numérico y \mathcal{O}_K su anillo de enteros algebraicos. Sea \mathfrak{a} un ideal no nulo de \mathcal{O}_K , si $\| \mathfrak{a} \| = p$ donde $p \in \mathbb{Z}$ es primo, entonces \mathfrak{a} es un ideal primo de \mathcal{O}_K .*

Demostración. Supóngase que \mathfrak{a} no es ideal primo de \mathcal{O}_K , entonces $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ donde $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ son ideales primos de \mathcal{O}_K , entonces

$$p = \| \mathfrak{a} \| = \| \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} \| = \| \mathfrak{p}_1 \|^{e_1} \cdots \| \mathfrak{p}_r \|^{e_r}$$

y por lo tanto p no es primo. □

Proposición 2.1.4. Sea K un cuerpo numérico y \mathcal{O}_K su anillo de enteros algebraicos. Sea \mathfrak{p} un ideal primo de \mathcal{O}_K , entonces existe un único $p \in \mathbb{Z}$ primo tal que $\mathfrak{p}|p\mathcal{O}_K$.

Demostración. Ya que \mathfrak{p} es un ideal primo de \mathcal{O}_K entonces $\mathfrak{p} \cap \mathbb{Z}$ es un ideal primo de \mathbb{Z} y por lo tanto existe $p \in \mathbb{Z}$ primo tal que $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, luego $p\mathbb{Z} \subseteq \mathfrak{p}$, esto implica que $\mathfrak{p}|p\mathcal{O}_K$.

Supóngase que existe otro $q \in \mathbb{Z}$ primo tal que $\mathfrak{p}|q\mathcal{O}_K$, así $q\mathbb{Z} \subseteq \mathfrak{p}$.
Ya que $\text{mcd}(p, q) = 1$ entonces $1 \in \mathfrak{p}$, esto es una contradicción. \square

Proposición 2.1.5. Sea K un cuerpo numérico tal que $[K : \mathbb{Q}] := n$ y \mathcal{O}_K su anillo de enteros algebraicos. Sean \mathfrak{p} un ideal primo de \mathcal{O}_K y $p \in \mathbb{Z}$ el único primo tal que $\mathfrak{p}|p\mathcal{O}_K$, entonces $\|\mathfrak{p}\| = p^e$ para algún $1 \leq e \leq n$.

Demostración. Como $\mathfrak{p}|p\mathcal{O}_K$ entonces $p\mathcal{O}_K = \mathfrak{p}\mathfrak{q}$ donde \mathfrak{q} es un ideal de \mathcal{O}_K , luego

$$\|p\mathcal{O}_K\| = \|\mathfrak{p}\mathfrak{q}\| = \|\mathfrak{p}\| \|\mathfrak{q}\|$$

pero $\|p\mathcal{O}_K\| = \|(p\mathbb{Z})\mathcal{O}_K\| = \|p\mathbb{Z}\|^n = |\mathbb{Z}/p\mathbb{Z}|^n = p^n$, luego, se concluye que $\|\mathfrak{p}\| = p^e$ para algún $1 \leq e \leq n$. \square

Definición 2.1.3. Sean K y L cuerpos numéricos tales que L es una extensión finita de K , y sean \mathcal{O}_K y \mathcal{O}_L los anillos de enteros algebraicos de K y L respectivamente. Sea \mathfrak{p} un ideal primo de \mathcal{O}_K y su factorización en \mathcal{O}_L

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

donde $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ son los ideales primos de \mathcal{O}_L que contienen a \mathfrak{p} .

Se dice que \mathfrak{p} ramifica en L si existe $1 \leq i \leq r$ tal que $e_i > 1$, en caso contrario, se dice que \mathfrak{p} no ramifica en L .

Además, se dice que L es una extensión no ramificada de K si todo ideal primo de \mathcal{O}_K no ramifica en L .

La siguiente proposición establece el comportamiento de los índices de ramificación y de los grados inerciales cuando se tiene alguna extensión intermedia.

Proposición 2.1.6. Sean L, K y M cuerpos numéricos tales que $K \subseteq M \subseteq L$. Sea \mathfrak{p} un ideal primo de \mathcal{O}_K , \mathfrak{Q} un ideal primo de \mathcal{O}_M que contiene a \mathfrak{p} , y \mathfrak{P} un ideal primo de \mathcal{O}_L que contiene a \mathfrak{Q} . Entonces

$$e_{\mathfrak{P}|\mathfrak{p}} = e_{\mathfrak{P}|\mathfrak{Q}}e_{\mathfrak{Q}|\mathfrak{p}} \quad \text{y} \quad f_{\mathfrak{P}|\mathfrak{p}} = f_{\mathfrak{P}|\mathfrak{Q}}f_{\mathfrak{Q}|\mathfrak{p}}.$$

Demostración. Puesto que $\mathcal{O}_K/\mathfrak{p} \subseteq \mathcal{O}_M/\mathfrak{Q} \subseteq \mathcal{O}_L/\mathfrak{P}$ son extensiones finitas, entonces

$$[\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}] = [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_M/\mathfrak{Q}] [\mathcal{O}_M/\mathfrak{Q} : \mathcal{O}_K/\mathfrak{p}],$$

esto es, $f_{\mathfrak{P}|\mathfrak{p}} = f_{\mathfrak{P}|\mathfrak{Q}}f_{\mathfrak{Q}|\mathfrak{p}}$.

Por otro lado, ya que $\mathfrak{p} \subseteq \mathfrak{Q} \subseteq \mathfrak{P}$, se tienen las siguientes factorizaciones

$$\begin{aligned}\mathfrak{p}\mathcal{O}_M &= \mathfrak{Q}^{e_{\mathfrak{Q}|\mathfrak{p}}} \mathfrak{Q}_1^{t_1} \cdots \mathfrak{Q}_x^{t_x}, \\ \mathfrak{Q}\mathcal{O}_L &= \mathfrak{P}^{e_{\mathfrak{P}|\mathfrak{Q}}} \mathfrak{P}_1^{u_1} \cdots \mathfrak{P}_y^{u_y}, \\ \mathfrak{p}\mathcal{O}_L &= \mathfrak{P}^{e_{\mathfrak{P}|\mathfrak{p}}} \mathfrak{R}_1^{v_1} \cdots \mathfrak{R}_z^{v_z}.\end{aligned}$$

Donde los \mathfrak{P}_i y \mathfrak{R}_i son ideales primos de \mathcal{O}_L que contienen a \mathfrak{Q} y \mathfrak{p} respectivamente, y los \mathfrak{Q}_i son ideales primos de \mathcal{O}_M que contienen a \mathfrak{p} .

Teniendo en cuenta que $\mathfrak{p}\mathcal{O}_L = (\mathfrak{p}\mathcal{O}_M)\mathcal{O}_L$, se obtiene que

$$\begin{aligned}\mathfrak{p}\mathcal{O}_L &= \left(\mathfrak{Q}^{e_{\mathfrak{Q}|\mathfrak{p}}} \mathfrak{Q}_1^{t_1} \cdots \mathfrak{Q}_x^{t_x} \right) \mathcal{O}_L \\ &= (\mathfrak{Q}\mathcal{O}_L)^{e_{\mathfrak{Q}|\mathfrak{p}}} \cdots (\mathfrak{Q}_x\mathcal{O}_L)^{t_x} \\ &= \mathfrak{P}^{e_{\mathfrak{P}|\mathfrak{Q}}} \mathfrak{P}_1^{e_{\mathfrak{P}|\mathfrak{Q}}} \cdots\end{aligned}$$

pero \mathfrak{Q} es el único ideal primo de \mathcal{O}_M que está contenido en \mathfrak{P} , y así, la factorización única de $\mathfrak{p}\mathcal{O}_L$ implica que $e_{\mathfrak{P}|\mathfrak{p}} = e_{\mathfrak{P}|\mathfrak{Q}} e_{\mathfrak{Q}|\mathfrak{p}}$. \square

Para terminar esta sección, el siguiente lema relaciona las extensiones no ramificadas con las extensiones intermedias.

Lema 2.1.1. Sean K, M, L cuerpos numéricos tales que $K \subseteq M \subseteq L$, y sea \mathfrak{p} un ideal primo de \mathcal{O}_K .

1. El ideal \mathfrak{p} no ramifica en L si y solo si \mathfrak{p} no ramifica en M y cada ideal primo de \mathcal{O}_M que contiene a \mathfrak{p} no ramifica en L .
2. L es una extensión no ramificada de K si y solo si L es una extensión no ramificada de M y M es una extensión no ramificada de K .

Demostración. 1. Supóngase que \mathfrak{p} no ramifica en L , es decir

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_g$$

donde \mathfrak{P}_i es un ideal primo de \mathcal{O}_L y $e_{\mathfrak{P}_i|\mathfrak{p}} = 1$ para cada $1 \leq i \leq g$.

Sea

$$\mathfrak{p}\mathcal{O}_M = \mathfrak{Q}_1^{e'_1} \cdots \mathfrak{Q}_h^{e'_h}$$

donde \mathfrak{Q}_i es un ideal primo de \mathcal{O}_M y $e'_i = e_{\mathfrak{Q}_i|\mathfrak{p}}$ para cada $1 \leq i \leq h$. Puesto que $(\mathfrak{p}\mathcal{O}_M)\mathcal{O}_L = \mathfrak{p}\mathcal{O}_L$, entonces

$$\mathfrak{p}\mathcal{O}_L = (\mathfrak{Q}_1\mathcal{O}_L)^{e'_1} \cdots (\mathfrak{Q}_h\mathcal{O}_L)^{e'_h};$$

ahora, si para cada $1 \leq i \leq h$ se tiene que $\mathfrak{Q}_i\mathcal{O}_L = \mathfrak{R}_{i1}^{e''_{i1}} \cdots \mathfrak{R}_{ir_i}^{e''_{ir_i}}$ es la factorización en ideales primos de \mathcal{O}_L , entonces

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{R}_{11}^{e'_{11} e''_{11}} \cdots \mathfrak{R}_{1r_1}^{e'_{1r_1} e''_{1r_1}} \cdots \mathfrak{R}_{hr_h}^{e'_{hr_h} e''_{hr_h}}.$$

De modo que, por la unicidad de la factorización se obtiene que cada \mathfrak{R}_{ij} es igual a \mathfrak{P}_d para un único $1 \leq d \leq g$, y así $r_1 + \cdots + r_h = g$. Además se obtiene que $e'_i = 1$ para cada $1 \leq i \leq g$, y $e''_{ij} = 1$ para cada $1 \leq i \leq h, 1 \leq j \leq r_i$. Esto implica que \mathfrak{p} no ramifica en M y cada ideal primo \mathfrak{Q}_i no ramifica en L .

Recíprocamente, supóngase que \mathfrak{p} no ramifica en M y cada ideal primo de \mathcal{O}_M que contiene a \mathfrak{p} no ramifica en L , es decir

$$\mathfrak{p}\mathcal{O}_M = \mathfrak{Q}_1 \cdots \mathfrak{Q}_h$$

donde \mathfrak{Q}_i es un ideal primo de \mathcal{O}_M y $e_{\mathfrak{Q}_i|\mathfrak{p}} = 1$ para cada $1 \leq i \leq h$, y

$$\mathfrak{Q}_i\mathcal{O}_L = \mathfrak{R}_{i1} \cdots \mathfrak{R}_{ir_i}$$

donde \mathfrak{R}_{ij} es un ideal primo de \mathcal{O}_L para cada $1 \leq i \leq h$ y $1 \leq j \leq r_i$.

Sea

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$$

donde \mathfrak{P}_i es un ideal primo de \mathcal{O}_L y $e_i = e_{\mathfrak{P}_i|\mathfrak{p}}$ para cada $1 \leq i \leq g$.

Ya que $(\mathfrak{p}\mathcal{O}_M)\mathcal{O}_L = \mathfrak{p}\mathcal{O}_L$, entonces

$$\begin{aligned} \mathfrak{p}\mathcal{O}_L &= (\mathfrak{Q}_1 \cdots \mathfrak{Q}_h)\mathcal{O}_L \\ &= (\mathfrak{Q}_1\mathcal{O}_L) \cdots (\mathfrak{Q}_h\mathcal{O}_L) \\ &= \mathfrak{R}_{11} \cdots \mathfrak{R}_{1r_1} \cdots \mathfrak{R}_{hr_h}. \end{aligned}$$

Luego, por la unicidad de la factorización se concluye que

$$\mathfrak{Q}_i\mathcal{O}_L = \mathfrak{P}_{i1} \cdots \mathfrak{P}_{ir_i}$$

donde $\mathfrak{P}_{ij} \in \{\mathfrak{P}_1, \dots, \mathfrak{P}_g\}$ para cada $1 \leq i \leq h$ y $1 \leq j \leq r_i$. Esto implica que para cada $1 \leq i \leq g$, el ideal \mathfrak{P}_i contiene a algún ideal primo de \mathcal{O}_M que contiene a \mathfrak{p} , es decir para cada $1 \leq i \leq g$ existe $1 \leq j \leq h$ tal que $\mathfrak{p} \subseteq \mathfrak{Q}_j \subseteq \mathfrak{P}_i$, aplicando la proposición 2.1.6 se obtiene que

$$e_{\mathfrak{P}_i|\mathfrak{p}} = e_{\mathfrak{P}_i|\mathfrak{Q}_j} e_{\mathfrak{Q}_j|\mathfrak{p}}$$

y por lo tanto

$$e_{\mathfrak{P}_i|\mathfrak{p}} = 1$$

para cada $1 \leq i \leq g$, es decir \mathfrak{p} no ramifica en L .

2. Supóngase que L es una extensión no ramificada de K , y sea \mathfrak{p} un ideal primo de \mathcal{O}_K . La parte 1 implica que \mathfrak{p} no ramifica en M y por lo tanto M es una extensión no ramificada de K . Por otro lado, sea \mathfrak{Q} un ideal primo de \mathcal{O}_M , y defínase $\mathfrak{p} := \mathfrak{Q} \cap \mathcal{O}_K$ un ideal primo de \mathcal{O}_K que está contenido en \mathfrak{Q} , por hipótesis el ideal \mathfrak{p} no ramifica en L y por

la parte 1 se obtiene que \mathfrak{Q} no ramifica en L , así se concluye que L es una extensión no ramificada de M .

Recíprocamente, supóngase que L es una extensión no ramificada de M y M es una extensión no ramificada de K . Sea \mathfrak{p} un ideal primo de \mathcal{O}_K y sea \mathfrak{Q} un ideal primo de \mathcal{O}_M que contiene a \mathfrak{p} , entonces \mathfrak{p} no ramifica en M y \mathfrak{Q} no ramifica en L , de modo que por la parte 1 se concluye que \mathfrak{p} no ramifica en L , y así se concluye que L es una extensión no ramificada de K .

□

2.2. CUERPOS CUADRÁTICOS

En esta sección se estudiarán los cuerpos cuadráticos para observar la teoría anterior en un caso particular.

Definición 2.2.1. Sea K un cuerpo numérico, se dice que K es un cuerpo cuadrático si el grado de K como extensión de \mathbb{Q} es 2, es decir $[K : \mathbb{Q}] = 2$.

Un cuerpo cuadrático K es de la forma $K = \mathbb{Q}(\sqrt{d})$, donde d es un entero libre de cuadrados. Este es un hecho fundamental de los cuerpos cuadráticos probado en [11].

Si $d > 0$ se dice que K es un cuerpo cuadrático real, y si $d < 0$ se dice que K es un cuerpo cuadrático imaginario.

Proposición 2.2.1. Sea K un cuerpo cuadrático, es decir $K = \mathbb{Q}(\sqrt{d})$ para algún $d \in \mathbb{Z}$ libre de cuadrados, y sea $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$. Entonces $N_{\mathbb{Q}}^K(\alpha) = a^2 - b^2d$ y $T_{\mathbb{Q}}^K(\alpha) = 2a$, donde $N_{\mathbb{Q}}^K(\alpha)$ y $T_{\mathbb{Q}}^K(\alpha)$ denotan la norma y la traza de α respectivamente.

Demostración. Como $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 2$, existen σ_1 y σ_2 homomorfismos de $\mathbb{Q}(\sqrt{d})$ en \mathbb{C} que dejan fijo a \mathbb{Q} .

Sea $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, entonces $\sigma_1(\alpha) = a + b\sqrt{d}$ y $\sigma_2(\alpha) = a - b\sqrt{d}$, y así

$$N_{\mathbb{Q}}^K(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2d$$

y

$$T_{\mathbb{Q}}^K(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) = (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a.$$

□

Proposición 2.2.2. Sea K un cuerpo cuadrático, es decir $K = \mathbb{Q}(\sqrt{d})$ para algún $d \in \mathbb{Z}$ libre de cuadrados, y sean \mathcal{O}_K su anillo de enteros algebraicos y $\alpha \in \mathbb{Q}(\sqrt{d})$. Probar que $\alpha \in \mathcal{O}_K$ si y solo si $T_{\mathbb{Q}}^K(\alpha), N_{\mathbb{Q}}^K(\alpha) \in \mathbb{Z}$.

Demostración. Supóngase que $\alpha \in \mathcal{O}_K$, sea $p(x) \in \mathbb{Z}[x]$ el polinomio mónico del cual α es raíz.

Si $gr(p(x)) = 1$, entonces $\alpha \in \mathbb{Z}$, y por lo tanto $N_{\mathbb{Q}}^K(\alpha), T_{\mathbb{Q}}^K(\alpha) \in \mathbb{Z}$.

Si $gr(p(x)) = 2$, entonces $\sigma_1(\alpha)$ y $\sigma_2(\alpha)$ son raíces de $p(x)$, luego

$$p(x) = (x - \sigma_1(\alpha))(x - \sigma_2(\alpha)) = x^2 - T_{\mathbb{Q}}^K(\alpha)x + N_{\mathbb{Q}}^K(\alpha),$$

y por lo tanto $N_{\mathbb{Q}}^K(\alpha), T_{\mathbb{Q}}^K(\alpha) \in \mathbb{Z}$.

Recíprocamente, sea $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ y supóngase que

$$T_{\mathbb{Q}}^K(\alpha) = 2a \in \mathbb{Z} \text{ y } N_{\mathbb{Q}}^K(\alpha) = a^2 - b^2d \in \mathbb{Z},$$

entonces

$$\alpha^2 - T_{\mathbb{Q}}^K(\alpha)\alpha + N_{\mathbb{Q}}^K(\alpha) = 0,$$

luego, α es raíz de $p(x) = x^2 - T_{\mathbb{Q}}^K(\alpha)x + N_{\mathbb{Q}}^K(\alpha) \in \mathbb{Z}[x]$ y así $\alpha \in \mathcal{O}_K$. \square

La siguiente proposición da una descripción explícita del anillo de enteros algebraicos de un cuerpo cuadrático.

Proposición 2.2.3. *Sea K un cuerpo cuadrático, es decir $K = \mathbb{Q}(\sqrt{d})$ para algún $d \in \mathbb{Z}$ libre de cuadrados, y sea \mathcal{O}_K su anillo de enteros algebraicos. Entonces $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\delta$ donde*

$$\delta = \begin{cases} \sqrt{d} & \text{si } d \equiv 2, 3 \pmod{4} \\ \frac{1 + \sqrt{d}}{2} & \text{si } d \equiv 1 \pmod{4} \end{cases}$$

Demostración. Sea $\alpha = a + b\sqrt{d} \in \mathcal{O}_K$ con $a, b \in \mathbb{Q}$, luego

$$T_{\mathbb{Q}}^K(\alpha) = 2a \in \mathbb{Z} \text{ y } N_{\mathbb{Q}}^K(\alpha) = a^2 - b^2d \in \mathbb{Z},$$

entonces $4b^2d \in \mathbb{Z}$.

Si $b = \frac{p}{q}$ con $p, q \in \mathbb{Z}$, $q \neq 0$ y $\text{mcd}(p, q) = 1$, entonces $q^2 | 4d$, luego, nótese que q no puede tener factores primos impares, y por lo tanto $q = 2^k$ donde $k \geq 0$. El hecho de que $q^2 | 4d$ implica que $k = 0$ o $k = 1$, pero en ambos casos se obtiene que $b = \frac{r}{2}$ para algún $r \in \mathbb{Z}$, y por lo tanto $2b \in \mathbb{Z}$.

Sean $m := 2a \in \mathbb{Z}$, $n := 2b \in \mathbb{Z}$, por lo tanto $m^2 - n^2d \equiv 0 \pmod{4}$, y así se tienen los siguientes casos:

Si $d \equiv 2, 3 \pmod{4}$ entonces $m^2 + 2n^2 \equiv 0 \pmod{4}$ ó $m^2 + n^2 \equiv 0 \pmod{4}$, de esto se deduce que m y n son pares. Así se concluye que $a, b \in \mathbb{Z}$, y

$$\mathcal{O}_K \subseteq \mathbb{Z} + \mathbb{Z}\sqrt{d}.$$

Si $d \equiv 1 \pmod{4}$ entonces $m^2 - n^2 \equiv \pmod{4}$, lo cual implica que $2|(m+n)$ o $2|(m-n)$, es decir que $m \equiv n \pmod{2}$, así $m = n + 2r$ para algún $r \in \mathbb{Z}$. Entonces

$$\begin{aligned}\alpha &= a + b\sqrt{d} \\ &= \frac{m}{2} + \frac{n}{2}\sqrt{d} \\ &= \frac{m + n\sqrt{d}}{2} \\ &= \frac{n + 2r + n\sqrt{d}}{2} \\ &= r + n \left(\frac{1 + \sqrt{d}}{2} \right)\end{aligned}$$

Y por lo tanto

$$\mathcal{O}_K \subseteq \mathbb{Z} + \mathbb{Z} \frac{1 + \sqrt{d}}{2}.$$

Por otro lado si $d \equiv 2, 3 \pmod{4}$ entonces $\sqrt{d} \in \mathcal{O}_K$ pues es raíz de $p(x) = x^2 - d$. Y si $d \equiv 1 \pmod{4}$ entonces $\frac{1-d}{4} \in \mathbb{Z}$, así $\frac{1+\sqrt{d}}{2} \in \mathcal{O}_K$ pues es raíz de $p(x) = x^2 - x + \frac{1-d}{4}$. De esto se concluye la igualdad. \square

Ahora se puede calcular el discriminante de un cuerpo cuadrático.

Proposición 2.2.4. Sea K un cuerpo cuadrático, es decir $K = \mathbb{Q}(\sqrt{d})$ para algún $d \in \mathbb{Z}$ libre de cuadrados, y sea \mathcal{O}_K su anillo de enteros algebraicos. Entonces $\{1, \sqrt{d}\}$ es una \mathbb{Z} -base de \mathcal{O}_K si $d \equiv 2, 3 \pmod{4}$, y $\{1, \frac{1+\sqrt{d}}{2}\}$ es una \mathbb{Z} -base de \mathcal{O}_K si $d \equiv 1 \pmod{4}$. Además se tiene que

$$\text{disc}(K) = \begin{cases} 4d & \text{si } d \equiv 2, 3 \pmod{4} \\ d & \text{si } d \equiv 1 \pmod{4} \end{cases}$$

donde $\text{disc}(K)$ denota el discriminante de K .

Demostración. La primera parte es consecuencia directa del hecho que $\{1, \sqrt{d}\}$ es una \mathbb{Q} -base de K .

Ahora, si $d \equiv 2, 3 \pmod{4}$, entonces

$$\begin{aligned}\text{disc}(K) &= \text{disc}(1, \sqrt{d}) \\ &= \begin{vmatrix} \sigma_1(1) & \sigma_1(\sqrt{d}) \\ \sigma_2(1) & \sigma_2(\sqrt{d}) \end{vmatrix}^2 \\ &= \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 \\ &= 4d.\end{aligned}$$

Y, si $d \equiv 1 \pmod{4}$, entonces

$$\begin{aligned} \text{disc}(K) &= \text{disc} \left(1, \frac{1 + \sqrt{d}}{2} \right) \\ &= \begin{vmatrix} \sigma_1(1) & \sigma_1\left(\frac{1 + \sqrt{d}}{2}\right) \\ \sigma_2(1) & \sigma_2\left(\frac{1 + \sqrt{d}}{2}\right) \end{vmatrix}^2 \\ &= \begin{vmatrix} 1 & \frac{1 + \sqrt{d}}{2} \\ 1 & -\frac{1 + \sqrt{d}}{2} \end{vmatrix}^2 \\ &= d. \end{aligned}$$

□

Por ultimo, se estudiará la factorización de un primo $p \in \mathbb{Z}$ en el anillo de enteros algebraicos de un cuerpo cuadrático K .

Sea $p \in \mathbb{Z}$ un primo, entonces $p\mathcal{O}_K = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$ donde $\mathfrak{q}_1, \dots, \mathfrak{q}_r$ son ideales primos de \mathcal{O}_K , y sean f_1, \dots, f_r los grados inerciales de $\mathfrak{q}_1, \dots, \mathfrak{q}_r$ sobre p .

Luego, la proposición 2.1.2 implica que $2 = \sum_{i=1}^r e_i f_i$, y así se tienen los siguientes 3 casos:

1. $e_1 = 1, e_2 = 1, f_1 = 1, f_2 = 1$ y así $p\mathcal{O}_K = \mathfrak{q}_1 \mathfrak{q}_2$ donde $\|\mathfrak{q}_1\| = \|\mathfrak{q}_2\| = p$ y $\mathfrak{q}_1 \neq \mathfrak{q}_2$.
2. $e_1 = 2, f_1 = 1$ y así $p\mathcal{O}_K = \mathfrak{q}_1^2$ donde $\|\mathfrak{q}_1\| = p$.
3. $e_1 = 1, f_1 = 2$ y así $p\mathcal{O}_K = \mathfrak{q}_1$ donde $\|\mathfrak{q}_1\| = p^2$.

En el caso (1) se dice que p se descompone en K , en el caso (2) se dice que p ramifica en K , y en el caso (3) se dice que p es inerte en K .

Definición 2.2.2. Sean $a \in \mathbb{Z}$ y p primo tales que $a \not\equiv 0 \pmod{p}$, se define el símbolo de Legendre cuadrático como

$$\left(\frac{a}{p} \right) = \begin{cases} 1 & \text{si } x^2 \equiv a \pmod{p} \text{ tiene solución} \\ -1 & \text{si } x^2 \equiv a \pmod{p} \text{ no tiene solución} \end{cases}$$

Si $a \equiv 0 \pmod{p}$, se define como $\left(\frac{a}{p} \right) = 0$.

El siguiente teorema da condiciones para que se tenga cada uno de los tres casos anteriores.

Teorema 2.2.1. Sea K un cuerpo cuadrático, es decir $K = \mathbb{Q}(\sqrt{d})$ para algún $d \in \mathbb{Z}$ libre de cuadrados, y sea \mathcal{O}_K su anillo de enteros algebraicos. Sea $p \in \mathbb{Z}$ un primo impar.

1.

$$\left(\frac{d}{p}\right) = 1 \text{ si y solo si } p\mathcal{O}_K = \mathfrak{q}_1\mathfrak{q}_2,$$

donde $\mathfrak{q}_1, \mathfrak{q}_2$ son ideales primos de \mathcal{O}_K diferentes y $\|\mathfrak{q}_1\| = \|\mathfrak{q}_2\| = p$.

2.

$$\left(\frac{d}{p}\right) = 0 \text{ si y solo si } p\mathcal{O}_K = \mathfrak{q}^2,$$

donde \mathfrak{q} es un ideal primo de \mathcal{O}_K y $\|\mathfrak{q}\| = p$.

3.

$$\left(\frac{d}{p}\right) = -1 \text{ si y solo si } p\mathcal{O}_K = \mathfrak{q},$$

donde \mathfrak{q} es un ideal primo de \mathcal{O}_K y $\|\mathfrak{q}\| = p^2$.

Demostración. 1. Supóngase que $\left(\frac{d}{p}\right) = 1$, entonces existe $a \in \mathbb{Z}$ tal que $a^2 \equiv d \pmod{p}$.

Nótese que $p \nmid a$.

Sean $\mathfrak{q}_1 := p\mathcal{O}_K + (a + \sqrt{d})\mathcal{O}_K$ y $\mathfrak{q}_2 := p\mathcal{O}_K + (a - \sqrt{d})\mathcal{O}_K$ ideales de \mathcal{O}_K , tal que

$$\begin{aligned} \mathfrak{q}_1\mathfrak{q}_2 &= [p\mathcal{O}_K + (a + \sqrt{d})\mathcal{O}_K] [p\mathcal{O}_K + (a - \sqrt{d})\mathcal{O}_K] \\ &= p^2\mathcal{O}_K + p(a + \sqrt{d})\mathcal{O}_K + p(a - \sqrt{d})\mathcal{O}_K + (a^2 - d)\mathcal{O}_K \\ &= p\mathcal{O}_K \left[p\mathcal{O}_K + (a + \sqrt{d})\mathcal{O}_K + (a - \sqrt{d})\mathcal{O}_K + \left(\frac{a^2 - d}{p}\right)\mathcal{O}_K \right] \end{aligned}$$

Llámesse $\mathfrak{i} := p\mathcal{O}_K + (a + \sqrt{d})\mathcal{O}_K + (a - \sqrt{d})\mathcal{O}_K + \left(\frac{a^2 - d}{p}\right)\mathcal{O}_K$ el ideal de \mathcal{O}_K .

Ya que $p \nmid a$ se tiene que $\text{mcd}(p, 2a) = 1$, luego existen $x, y \in \mathbb{Z}$ tal que $1 = xp + 2ay$, esto implica que $1 = px + (a + \sqrt{d})y + (a - \sqrt{d})y \in \mathfrak{i}$, es decir $\mathfrak{i} = \mathcal{O}_K$. Se concluye que $p\mathcal{O}_K = \mathfrak{q}_1\mathfrak{q}_2$.

Nótese que $\mathfrak{q}_1 \neq \mathfrak{q}_2$: Supóngase que $\mathfrak{q}_1 = \mathfrak{q}_2$, como $a + \sqrt{d} \in \mathfrak{q}_2$ y $a - \sqrt{d} \in \mathfrak{q}_2$ se tiene que $2\sqrt{d} \in \mathfrak{q}_2$, ya que $2\sqrt{d} \in \mathcal{O}_K$ entonces $4d \in \mathfrak{q}_2$.

Debido a que $p \nmid d$ y p es impar se tiene que $\text{mcd}(p, 4d) = 1$, por lo tanto $1 \in \mathfrak{q}_2$, esto implica que $\mathfrak{q}_1 = \mathfrak{q}_2 = \mathcal{O}_K$ y así $p\mathcal{O}_K = \mathcal{O}_K$, pero esto es una contradicción ya que $1 \notin p\mathcal{O}_K$.

También se tiene que $\mathfrak{q}_1 \neq \mathcal{O}_K$ y $\mathfrak{q}_2 \neq \mathcal{O}_K$: Supóngase que $\mathfrak{q}_1 = \mathcal{O}_K$, entonces $p\mathcal{O}_K = \mathfrak{q}_2$, esto implica que $a - \sqrt{d} \in p\mathcal{O}_K$ lo cual es una contradicción.

Lo anterior implica que $\|\mathfrak{q}_1\| = p = \|\mathfrak{q}_2\|$, y por lo tanto \mathfrak{q}_1 y \mathfrak{q}_2 son ideales primos de \mathcal{O}_K .

2. Supóngase que $\left(\frac{d}{p}\right) = 0$, entonces $p|d$.

Sea $\mathfrak{q} := p\mathcal{O}_K + \sqrt{d}\mathcal{O}_K$ un ideal de \mathcal{O}_K , tal que

$$\begin{aligned}\mathfrak{q}^2 &= [p\mathcal{O}_K + \sqrt{d}\mathcal{O}_K] [p\mathcal{O}_K + \sqrt{d}\mathcal{O}_K] \\ &= p^2\mathcal{O}_K + p\sqrt{d}\mathcal{O}_K + d\mathcal{O}_K \\ &= p\mathcal{O}_K \left[p\mathcal{O}_K + \sqrt{d}\mathcal{O}_K + \frac{d}{p}\mathcal{O}_K \right]\end{aligned}$$

Llámesese $i := p\mathcal{O}_K + \sqrt{d}\mathcal{O}_K + \frac{d}{p}\mathcal{O}_K$ el ideal de \mathcal{O}_K .

Ya que $\text{mcd}(p, \frac{d}{p}) = 1$ se tiene que $1 \in i$, y por lo tanto $i = \mathcal{O}_K$. Se concluye que $\mathfrak{q}^2 = p\mathcal{O}_K$.

Esto implica que $\|\mathfrak{q}\| = p$, y así \mathfrak{q} es un ideal primo de \mathcal{O}_K .

3. Supóngase que $\left(\frac{d}{p}\right) = -1$, por contradicción supóngase que $p\mathcal{O}_K = \mathfrak{q}_1\mathfrak{q}_2$ ó $p\mathcal{O}_K = \mathfrak{q}_1^2$ con $\mathfrak{q}_1, \mathfrak{q}_2$ ideales primos diferentes de \mathcal{O}_K .

En ambos casos se tiene que $\|\mathfrak{q}_1\| = p = \|\mathfrak{q}_2\|$, esto implica que $[\mathcal{O}_K/\mathfrak{q}_i : \mathbb{Z}/p\mathbb{Z}] = 1$ para $i = 1, 2$, y así, $\mathcal{O}_K/\mathfrak{q}_i \cong \mathbb{Z}/p\mathbb{Z}$ para $i = 1, 2$ como cuerpos y como $\mathbb{Z}/p\mathbb{Z}$ -espacios vectoriales.

Ya que el polinomio $x^2 - d$ tiene una raíz en \mathcal{O}_K , entonces el polinomio $x^2 - \bar{d}$ tiene una raíz en $\mathcal{O}_K/\mathfrak{q}_i$ para $i = 1, 2$.

Si el polinomio $x^2 - \bar{d}$ tiene raíces en $\mathbb{Z}/p\mathbb{Z}$, existe $a \in \mathbb{Z}$ tal que $a^2 \equiv d \pmod{p}$, esto contradice la hipótesis, y por lo tanto $\mathcal{O}_K/\mathfrak{q}_i \not\cong \mathbb{Z}/p\mathbb{Z}$ para $i = 1, 2$.

Por lo tanto se concluye que $p\mathcal{O}_K = \mathfrak{q}$ con \mathfrak{q} un ideal primo de \mathcal{O}_K y $\|\mathfrak{q}\| = p^2$.

Las implicaciones reciprocas se tienen debido a la factorización única en ideales primos en \mathcal{O}_K .

□

Ejemplo 2.2.1. Sea $K = \mathbb{Q}(\sqrt{6})$, puesto que $6 \equiv 2 \pmod{4}$ se obtiene que $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{6}$.

Sea $\mathfrak{a} := 2\mathcal{O}_K + \sqrt{6}\mathcal{O}_K$ un ideal de \mathcal{O}_K , entonces $2\mathcal{O}_K = \mathfrak{a}^2$:

En efecto,

$$\begin{aligned}\mathfrak{a}^2 &= (2\mathcal{O}_K + \sqrt{6}\mathcal{O}_K)(2\mathcal{O}_K + \sqrt{6}\mathcal{O}_K) \\ &= 4\mathcal{O}_K + 2\sqrt{6}\mathcal{O}_K + 6\mathcal{O}_K \\ &= 2\mathcal{O}_K(2\mathcal{O}_K + \sqrt{6}\mathcal{O}_K + 3\mathcal{O}_K),\end{aligned}$$

además $1 = 3 - 2 \in 2\mathcal{O}_K + \sqrt{6}\mathcal{O}_K + 3\mathcal{O}_K$, entonces $2\mathcal{O}_K + \sqrt{6}\mathcal{O}_K + 3\mathcal{O}_K = \mathcal{O}_K$.

Esto implica que $\mathfrak{a}^2 = 2\mathcal{O}_K$.

Por otro lado,

$$\|\mathfrak{a}\|^2 = \|\mathfrak{a}^2\| = \|2\mathcal{O}_K\| = |N_{\mathbb{Q}}^K(2)| = 4,$$

de modo que $\| \mathfrak{a} \| = 2$, por lo tanto $\mathfrak{a} = 2\mathcal{O}_K + \sqrt{6}\mathcal{O}_K$ es un ideal primo de \mathcal{O}_K , y así 2 ramifica en K .

Corolario 2.2.1. *Sea K un cuerpo cuadrático, es decir $K = \mathbb{Q}(\sqrt{d})$ para algún $d \in \mathbb{Z}$ libre de cuadrados, y sea $p \in \mathbb{Z}$ un primo impar.*

Entonces p ramifica en K si y solo si $p|d_K$, donde $d_K := \text{disc}(K)$.

Demostración. Supóngase que p ramifica en K , el teorema anterior implica que $\left(\frac{d}{p}\right) = 0$, y así $p|d$. Por lo tanto $p|d_K$.

Recíprocamente, supóngase que $p|d_K$, si $d \equiv 1 \pmod{4}$ entonces $d_K = d$, y así $\left(\frac{d}{p}\right) = 0$, el teorema anterior implica que p ramifica en K . Ahora si $d \equiv 2, 3 \pmod{4}$ entonces $d_K = 4d$ y así $\left(\frac{d}{p}\right) = 0$, luego el teorema anterior implica que p ramifica en K . \square

2.3. CUERPOS CICLOTÓMICOS

Los cuerpos ciclotómicos son un tipo de cuerpo numérico que fueron estudiados por Gauss, Eisenstein, Kummer y Dirichlet por su gran importancia en el desarrollo del álgebra abstracta y la teoría de números, ya que poseen una estrecha relación con el último teorema de Fermat y con las leyes de reciprocidad.

Dado $n \geq 1$, al conjunto de elementos del cuerpo \mathbb{C} que son raíces del polinomio $x^n - 1$ se les denomina raíces n -ésimas de la unidad. El conjunto de todas estas raíces forma un subgrupo multiplicativo de $\mathbb{C}^* := \mathbb{C} - \{0\}$, dicho subgrupo resulta cíclico de orden n , y a cualquier generador se le denomina raíz primitiva n -ésima de la unidad.

Las n diferentes raíces n -ésimas de la unidad son $e^{2\pi i k/n}$ donde $0 \leq k \leq n-1$, además, se tiene que una raíz de estas es primitiva si $(k, n) = 1$, o equivalentemente, si el orden de esta es n . De este modo se tiene que la cantidad de raíces primitivas n -ésimas de la unidad es $\varphi(n)$ donde φ es la función de Euler.

Sea $\zeta_n := e^{2\pi i/n}$, así ζ_n es una raíz primitiva n -ésima de la unidad y el cuerpo $K := \mathbb{Q}(\zeta_n)$ es el cuerpo de descomposición del polinomio $x^n - 1$.

Definición 2.3.1. Sea $n \geq 1$, se dice que K es un cuerpo ciclotómico si se obtiene de adjuntar una raíz primitiva n -ésima de la unidad a \mathbb{Q} , es decir si $K = \mathbb{Q}(\zeta_n)$.

Definición 2.3.2. Sea $n \geq 1$, el n -ésimo polinomio ciclotómico se define como

$$\Phi_n(x) := \prod_{(a,n)=1} (x - \zeta_n^a),$$

donde $1 \leq a \leq n$. Las raíces de $\Phi_n(x)$ son las raíces primitivas n -ésimas de la unidad, así

$$\text{gr}(\Phi_n(x)) = \varphi(n).$$

El objetivo de esta sección es estudiar algunas propiedades de los cuerpos ciclotómicos y calcular su anillo de enteros algebraicos.

Proposición 2.3.1. *Sea $n \geq 1$, entonces*

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

Demostración. De la definición del n -ésimo polinomio ciclotómico se tiene que

$$x^n - 1 = \prod_{i=0}^{n-1} (x - \zeta_n^i) = \prod_{d|n} \prod_{(i,n)=d} (x - \zeta_n^i).$$

Luego, nótese que

$$\prod_{(i,n)=d} (x - \zeta_n^i) = \prod_{(j,\frac{n}{d})=1} (x - \zeta_{n/d}^j) = \Phi_{n/d}(x).$$

De esto se concluye la proposición. \square

De la proposición anterior se obtiene una manera recursiva de calcular los polinomios ciclotómicos.

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d < n}} \Phi_d(x)}.$$

Corolario 2.3.1. *Para cada $n \geq 1$, el n -ésimo polinomio ciclotómico $\Phi_n(x)$ tiene coeficientes enteros.*

Demostración. La prueba se realiza por inducción sobre n .

Para $n = 1$ se tiene que $\Phi_1(x) = x - 1 \in \mathbb{Z}[x]$.

Sea $n \geq 2$ y supóngase que el resultado es válido para todo número natural menor que n , así

$$p(x) := \prod_{\substack{d|n \\ d < n}} \Phi_d(x) \in \mathbb{Z}[x],$$

luego por el algoritmo de la división existen $q(x), r(x) \in \mathbb{Z}[x]$ tal que

$$x^n - 1 = q(x)p(x) + r(x),$$

donde $r(x) = 0$ o $gr(r(x)) < gr(p(x))$.

De modo que

$$\Phi_n(x)p(x) = q(x)p(x) + r(x),$$

y así, comparando los grados se concluye el resultado. \square

Lema 2.3.1. *Sean $n \geq 1$ y $K := \mathbb{Q}(\zeta_n)$ un cuerpo ciclotómico. Sean $p \in \mathbb{Z}$ un primo tal que $p \nmid n$, y \mathfrak{p} un ideal primo de \mathcal{O}_K que contiene a p . Entonces las clases de $1, \zeta_n, \dots, \zeta_n^{n-1}$ en $\mathcal{O}_K/\mathfrak{p}$ son distintas.*

Demostración. Puesto que

$$1 + x + \cdots + x^{n-1} = \prod_{i=1}^{n-1} (x - \zeta_n^i),$$

se obtiene que

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

$$\bar{n} = \prod_{i=1}^{n-1} (1 - \bar{\zeta}_n^i)$$

en $\mathcal{O}_K/\mathfrak{p}$.

Ya que $\bar{n} \neq \bar{0}$, se concluye que $\bar{\zeta}_n^i \neq \bar{1}$ para todo $1 \leq i \leq n-1$, y así $\bar{\zeta}_n^i \neq \bar{\zeta}_n^j$ para todo $0 \leq i, j \leq n-1$ y $i \neq j$. \square

Con ayuda de la siguiente proposición se obtiene el grado de un cuerpo ciclotómico como extensión de \mathbb{Q} .

Proposición 2.3.2. Sean $n \geq 1$ y $K := \mathbb{Q}(\zeta_n)$ un cuerpo ciclotómico. El n -ésimo polinomio ciclotómico $\Phi_n(x)$ es irreducible sobre \mathbb{Z} , y por lo tanto lo es sobre \mathbb{Q} .

Demostración. Primero, note que $\Phi_1(x) = x - 1$ y $\Phi_2(x) = x + 1$ son irreducibles sobre \mathbb{Z} .

Ahora, sean $n \geq 3$ y $f(x)$ el polinomio mínimo de ζ_n sobre \mathbb{Z} , entonces $f(x) | \Phi_n(x)$, luego, existe $g(x) \in \mathbb{Z}[x]$ tal que $\Phi_n(x) = f(x)g(x)$.

Se quiere probar que $\Phi_n(x) = f(x)$, para esto es suficiente probar que ζ_n^a es una raíz de $f(x)$ para todo $1 \leq a \leq n$ tal que $(a, n) = 1$.

Sea $p \in \mathbb{Z}$ un primo tal que $p \nmid n$, y sea \mathfrak{p} un ideal de \mathcal{O}_K que contiene a p . Puesto que $f(x)$ es el polinomio mínimo de ζ_n , existe $h(x) \in \mathbb{Z}[x]$ tal que $x^n - 1 = f(x)h(x)$. Supóngase que $f(\zeta_n^p) \neq 0$, esto implica que $h(\zeta_n^p) = 0$, y así

$$\bar{0} = \bar{h}(\bar{\zeta}_n^p) = \bar{h}(\bar{\zeta}_n)^p$$

en $\mathcal{O}_K/\mathfrak{p}$.

De esto se obtiene que $\bar{h}(\bar{\zeta}_n) = \bar{0}$ en $\mathcal{O}_K/\mathfrak{p}$, por el lema anterior se tiene que $\bar{f}(\bar{\zeta}_n) \neq \bar{0}$, esto contradice el hecho de que $f(\zeta_n) = 0$. Así, se concluye que $f(\zeta_n^p) = 0$. \square

Corolario 2.3.2. Sean $n \geq 1$ y $\mathbb{Q}(\zeta_n)$ un cuerpo ciclotómico, entonces $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

Demostración. Se sigue directamente de la proposición anterior. \square

El corolario anterior implica que existen $\sigma_1, \dots, \sigma_{\varphi(n)}$ homomorfismos de $K = \mathbb{Q}(\zeta_n)$ en \mathbb{C} que fijan a \mathbb{Q} y están caracterizados por las raíces de $\Phi_n(x)$, es decir, por las raíces primitivas n -ésimas de la unidad.

Por otro lado, puesto que K es el cuerpo de descomposición del polinomio $x^n - 1 \in \mathbb{Q}[x]$, entonces K resulta una extensión de Galois de \mathbb{Q} . El siguiente teorema caracteriza al grupo $\text{Gal}(K/\mathbb{Q})$ para cada $n \geq 2$.

Teorema 2.3.1. Sean $n \geq 2$ y $K := \mathbb{Q}(\zeta_n)$. Si $\sigma \in \text{Gal}(K/\mathbb{Q})$, entonces.

1. $\sigma(\zeta_n) = \zeta_n^a$ donde $1 \leq a < n$ tal que $(a, n) = 1$.
2. El homomorfismo

$$\begin{aligned} \psi : \text{Gal}(K/\mathbb{Q}) &\rightarrow (\mathbb{Z}/n\mathbb{Z})^* \\ \sigma &\mapsto \psi(\sigma) := \bar{a} \end{aligned}$$

es un isomorfismo de grupos.

Demostración. 1. Ya que ζ_n es raíz de $\Phi_n(x) \in \mathbb{Z}[x]$, entonces $\sigma(\zeta_n)$ también es raíz de $\Phi_n(x)$, por lo tanto $\sigma(\zeta_n) = \zeta_n^a$ donde $1 \leq a < n$ y $(a, n) = 1$.

2. Claramente ψ es un homomorfismo de grupos.

ψ es inyectivo: Sea $\sigma \in \text{Gal}(K/\mathbb{Q})$, entonces $\sigma(\zeta_n) = \zeta_n^a$ donde $1 \leq a < n$ y $(a, n) = 1$. Si $\sigma \in \text{Ker}(\psi)$, entonces $\psi(\sigma) = \bar{a} = \bar{1}$, y así $a = 1$, esto implica que $\sigma = i_K$.

ψ es sobreyectivo: Puesto que

$$|\text{Gal}(K/\mathbb{Q})| = \varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|,$$

se concluye que ψ es sobreyectivo. □

Sea $p \in \mathbb{Z}$ primo, entonces el p -ésimo polinomio ciclotómico es

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \dots + x + 1,$$

este es el polinomio mínimo de ζ_p sobre \mathbb{Q} , y puesto que $\text{gr}(\Phi_p(x)) = p - 1$, se concluye que $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$ y $\{1, \zeta_p, \zeta_p^2, \dots, \zeta_p^{p-2}\}$ es una \mathbb{Q} -base para $K := \mathbb{Q}(\zeta_p)$.

Para calcular el anillo de enteros del cuerpo ciclotómico $K := \mathbb{Q}(\zeta_p)$ se hace uso de la traza y la norma.

Lema 2.3.2. Sean $p \in \mathbb{Z}$ primo y $K := \mathbb{Q}(\zeta_p)$ un cuerpo ciclotómico, entonces.

1. $\text{Tr}_{\mathbb{Q}}^K(1) = p - 1$.
2. $\text{Tr}_{\mathbb{Q}}^K(\zeta_p^j) = -1$ para cada $1 \leq j \leq p - 1$.
3. $\text{Tr}_{\mathbb{Q}}^K(1 - \zeta_p^j) = p$ para cada $1 \leq j \leq p - 1$.
4. $N_{\mathbb{Q}}^K(\zeta_p - 1) = (-1)^{p-1} p$.
5. $N_{\mathbb{Q}}^K(1 - \zeta_p) = p$.

Demostración. En este caso, los $p - 1$ homomorfismos de K en \mathbb{C} que dejan fijo a \mathbb{Q} están dados por $\sigma_1(\zeta_p) = \zeta_p, \sigma_2(\zeta_p) = \zeta_p^2, \dots, \sigma_{p-2}(\zeta_p) = \zeta_p^{p-2}, \sigma_{p-1}(\zeta_p) = \zeta_p^{p-1}$.

1.

$$\text{Tr}_{\mathbb{Q}}^K(1) = \sigma_1(1) + \dots + \sigma_{p-1}(1) = p - 1.$$

2. Puesto que ζ_p es raíz de $\Phi_p(x)$, se tiene que $1 + \zeta_p + \dots + \zeta_p^{p-1} = 0$, así

$$\begin{aligned} \text{Tr}_{\mathbb{Q}}^K(\zeta_p) &= \sigma_1(\zeta_p) + \dots + \sigma_{p-1}(\zeta_p) \\ &= \zeta_p + \dots + \zeta_p^{p-1} \\ &= -1. \end{aligned}$$

Luego, nótese que la traza del conjugado de un elemento es igual a la traza del elemento, entonces $\text{Tr}_{\mathbb{Q}}^K(\zeta_p^j) = \text{Tr}_{\mathbb{Q}}^K(\zeta_p) = -1$ para cada $1 \leq j \leq p - 1$.

3. Se obtiene de los dos numerales anteriores, ya que la traza es \mathbb{Q} -lineal, así

$$\text{Tr}_{\mathbb{Q}}^K(1 - \zeta_p^j) = \text{Tr}_{\mathbb{Q}}^K(1) - \text{Tr}_{\mathbb{Q}}^K(\zeta_p^j) = (p - 1) - (-1) = p.$$

4. Ya que $\Phi_p(x) = \frac{x^p - 1}{x - 1}$, entonces

$$g(x) := \Phi_p(x + 1) = \frac{(x + 1)^p - 1}{(x + 1) - 1} = \frac{(x + 1)^p - 1}{x} = x^{p-1} + \sum_{j=1}^{p-2} \binom{p}{j} x^{p-1-j} + p.$$

Y por el criterio de Eisenstein se obtiene que $g(x)$ es el polinomio mínimo de $\zeta_p - 1$ sobre \mathbb{Q} , luego

$$N_{\mathbb{Q}}^K(\zeta_p - 1) = (-1)^{p-1} p.$$

5. Ya que

$$N_{\mathbb{Q}}^K(-1) = (-1)^{p-1},$$

y la norma es multiplicativa, entonces se sigue del numeral anterior que

$$N_{\mathbb{Q}}^K(1 - \zeta_p) = N_{\mathbb{Q}}^K((-1)(\zeta_p - 1)) = N_{\mathbb{Q}}^K(-1) N_{\mathbb{Q}}^K(\zeta_p - 1) = (-1)^{p-1} (-1)^{p-1} p = p.$$

□

Lema 2.3.3. Sean $p \in \mathbb{Z}$ primo y $K = \mathbb{Q}(\zeta_p)$ un cuerpo ciclotómico, entonces.

1. $(1 - \zeta_p)\mathcal{O}_K \cap \mathbb{Z}$ es un ideal de \mathbb{Z} y $(1 - \zeta_p)\mathcal{O}_K \cap \mathbb{Z} = p\mathbb{Z}$.
2. $\text{Tr}_{\mathbb{Q}}^K(\alpha(1 - \zeta_p)) \in p\mathbb{Z}$ para todo $\alpha \in \mathcal{O}_K$.

Demostración. 1. Puesto que $(1 - \zeta_p)\mathcal{O}_K$ es un ideal de \mathcal{O}_K y $\mathbb{Z} \subseteq \mathcal{O}_K$, entonces

$$(1 - \zeta_p)\mathcal{O}_K \cap \mathbb{Z}$$

es un ideal de \mathbb{Z} .

Ya que $\zeta_p \in \mathcal{O}_K$, se sigue que $1 - \zeta_p^j \in \mathcal{O}_K$ para cada $1 \leq j \leq p-1$, entonces

$$p = N_{\mathbb{Q}}^K(1 - \zeta_p) = \prod_{j=1}^{p-1} \sigma_j(1 - \zeta_p) = \prod_{j=1}^{p-1} (1 - \zeta_p^j) = (1 - \zeta_p) \prod_{j=2}^{p-1} (1 - \zeta_p^j) \in (1 - \zeta_p)\mathcal{O}_K,$$

es decir, $p \in (1 - \zeta_p)\mathcal{O}_K \cap \mathbb{Z}$, por lo tanto $p\mathbb{Z} \subseteq (1 - \zeta_p)\mathcal{O}_K \cap \mathbb{Z}$.

Ya que $p\mathbb{Z}$ es un ideal maximal de \mathbb{Z} , luego debe ser que

$$(1 - \zeta_p)\mathcal{O}_K \cap \mathbb{Z} = p\mathbb{Z}.$$

En efecto, supóngase que no, es decir que $(1 - \zeta_p)\mathcal{O}_K \cap \mathbb{Z} = \mathbb{Z}$, entonces

$$1 \in (1 - \zeta_p)\mathcal{O}_K \cap \mathbb{Z},$$

así, existe $\alpha \in \mathcal{O}_K$ tal que $1 = (1 - \zeta_p)\alpha$, esto es, $1 - \zeta_p$ es un invertible en \mathcal{O}_K , luego

$$\begin{aligned} 1 &= N_{\mathbb{Q}}^K(1 - \zeta_p)N_{\mathbb{Q}}^K(\alpha) \\ &= pN_{\mathbb{Q}}^K(\alpha). \end{aligned}$$

Así $p|1$, esto es una contradicción.

2. Sea $\alpha \in \mathcal{O}_K$, se sigue que $\alpha(1 - \zeta_p) \in \mathcal{O}_K$, entonces $Tr_{\mathbb{Q}}^K(\alpha(1 - \zeta_p)) \in \mathbb{Z}$. Por otro lado, para cada $1 \leq j \leq p-1$, tómesese $\alpha_j := \sigma_j(\alpha)$, así $\alpha_j \in \mathcal{O}_K$ para cada $1 \leq j \leq p-1$ puesto que los conjugados de un entero algebraico tienen el mismo polinomio mínimo, por ende

$$Tr_{\mathbb{Q}}^K(\alpha(1 - \zeta_p)) = \sum_{j=1}^{p-1} \sigma_j(\alpha(1 - \zeta_p)) = \sum_{j=1}^{p-1} \alpha_j (1 - \zeta_p^j).$$

Para cada $1 \leq j \leq p-1$, la relación $1 - \zeta_p^j = (1 - \zeta_p) \sum_{l=0}^{j-1} \zeta_p^l$, implica que para cada $1 \leq j \leq p-1$ se tiene que

$$\alpha_j (1 - \zeta_p^j) = (1 - \zeta_p) \alpha_j \sum_{l=0}^{j-1} \zeta_p^l \in (1 - \zeta_p)\mathcal{O}_K,$$

así $Tr_{\mathbb{Q}}^K(\alpha(1 - \zeta_p)) \in (1 - \zeta_p)\mathcal{O}_K$, por lo tanto $Tr_{\mathbb{Q}}^K(\alpha(1 - \zeta_p)) \in (1 - \zeta_p)\mathcal{O}_K \cap \mathbb{Z} = p\mathbb{Z}$. \square

Teorema 2.3.2. Sean $p \in \mathbb{Z}$ un primo y $K = \mathbb{Q}(\zeta_p)$ un cuerpo ciclotómico. Entonces $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$ y $\{1, \zeta_p, \zeta_p^2, \dots, \zeta_p^{p-2}\}$ es una \mathbb{Z} -base de \mathcal{O}_K .

Demostración. Sea $\alpha \in \mathcal{O}_K$, puesto que $\alpha \in K$ y $\{1, \zeta_p, \zeta_p^2, \dots, \zeta_p^{p-2}\}$ es una \mathbb{Q} -base de K , entonces existen $a_0, a_1, \dots, a_{p-2} \in \mathbb{Q}$ tales que $\alpha = \sum_{j=0}^{p-2} a_j \zeta_p^j$, luego

$$\alpha(1 - \zeta_p) = \sum_{j=0}^{p-2} a_j \zeta_p^j (1 - \zeta_p) = \sum_{j=0}^{p-2} a_j (\zeta_p^j - \zeta_p^{j+1}),$$

ya que la traza es \mathbb{Q} -lineal, entonces

$$\begin{aligned} \text{Tr}_{\mathbb{Q}}^K(\alpha(1 - \zeta_p)) &= \text{Tr}_{\mathbb{Q}}^K\left(\sum_{j=0}^{p-2} a_j (\zeta_p^j - \zeta_p^{j+1})\right) \\ &= \sum_{j=0}^{p-2} a_j \text{Tr}_{\mathbb{Q}}^K(\zeta_p^j - \zeta_p^{j+1}) \\ &= a_0 \text{Tr}_{\mathbb{Q}}^K(1 - \zeta_p) + \sum_{j=1}^{p-2} a_j (\text{Tr}_{\mathbb{Q}}^K(\zeta_p^j) - \text{Tr}_{\mathbb{Q}}^K(\zeta_p^{j+1})) \\ &= a_0 \text{Tr}_{\mathbb{Q}}^K(1 - \zeta_p) + \sum_{j=1}^{p-2} a_j ((-1) - (-1)) \\ &= a_0 p \end{aligned}$$

luego $a_0 p = \text{Tr}_{\mathbb{Q}}^K(\alpha(1 - \zeta_p)) \in p\mathbb{Z}$, de donde $a_0 \in \mathbb{Z}$.

De otro lado, $\zeta_p^{-1} = \zeta_p^{p-1} \in \mathcal{O}_K$, entonces $\alpha' := (\alpha - a_0)\zeta_p^{-1} \in \mathcal{O}_K$, así

$$\alpha' = \sum_{j=1}^{p-2} a_j \zeta_p^{j-1},$$

aplicando el razonamiento anterior, resulta que $a_1 p = \text{Tr}_{\mathbb{Q}}^K(\alpha'(1 - \zeta_p)) \in p\mathbb{Z}$, de donde $a_1 \in \mathbb{Z}$.

Aplicando el razonamiento anterior de manera recurrente, se obtiene que $a_j \in \mathbb{Z}$ para cada $0 \leq j \leq p-2$, por lo tanto $a_0, a_1, \dots, a_{p-2} \in \mathbb{Z}$, es decir $\mathcal{O}_K \subseteq \mathbb{Z}[\zeta_p]$, esto implica que $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$ y $\{1, \zeta_p, \zeta_p^2, \dots, \zeta_p^{p-2}\}$ es una \mathbb{Z} -base de \mathcal{O}_K . \square

El teorema anterior también se cumple en general, es decir, sean $n \geq 2$ y $K := \mathbb{Q}(\zeta_n)$ un cuerpo ciclotómico, entonces $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$. Una prueba de este hecho se puede consultar en [21].

Por ultimo, en las siguientes proposiciones se estudia el discriminante de un cuerpo ciclotómico y su relación con los números primos que ramifican en este cuerpo.

Proposición 2.3.3. Sean $p \in \mathbb{Z}$ un primo impar y $K := \mathbb{Q}(\zeta_p)$ un cuerpo ciclotómico. Entonces

$$\text{disc}(K) = (-1)^{\binom{p-1}{2}} p^{p-2}.$$

Demostración. Por el teorema anterior, se tiene que $\{1, \zeta_p, \dots, \zeta_p^{p-2}\}$ es una \mathbb{Z} -base de \mathcal{O}_K , y como $\Phi_p(x) = \frac{x^p-1}{x-1}$ es el polinomio mínimo de ζ_p sobre \mathbb{Q} , se puede usar una de las formulas para el discriminante, y así se obtiene que

$$\text{disc}(K) = \text{disc}(1, \zeta_p, \dots, \zeta_p^{p-2}) = (-1)^{\binom{p-1}{2}} \prod_{k=1}^{p-1} \Phi'_p(\zeta_p^k).$$

Pero

$$\Phi'_p(x) = \frac{px^{p-1} - (1 + x + \dots + x^{p-1})}{x-1},$$

entonces, para cada $1 \leq k \leq p-1$ se tiene que

$$\Phi'_p(\zeta_p^k) = \frac{p\zeta_p^{k(p-1)}}{\zeta_p^k - 1} = \frac{p\zeta_p^{-k}}{\zeta_p^k - 1}.$$

Por lo tanto

$$\begin{aligned} \text{disc}(K) &= (-1)^{\binom{p-1}{2}} \prod_{k=1}^{p-1} \Phi'_p(\zeta_p^k) \\ &= (-1)^{\binom{p-1}{2}} \prod_{k=1}^{p-1} \frac{p\zeta_p^{-k}}{\zeta_p^k - 1} \\ &= (-1)^{\binom{p-1}{2}} p^{p-1} \prod_{k=1}^{p-1} \frac{\zeta_p^{-k}}{\zeta_p^k - 1} \\ &= (-1)^{\binom{p-1}{2}} \frac{p^{p-1}}{N_{\mathbb{Q}}^K(\zeta_p - 1)} \prod_{k=1}^{p-1} \zeta_p^{-k} \\ &= (-1)^{\binom{p-1}{2}} \frac{p^{p-1}}{(-1)^{p-1} p} \frac{1}{(-1)^{p-1}} \\ &= (-1)^{\binom{p-1}{2}} p^{p-2}. \end{aligned}$$

□

Proposición 2.3.4. Sean $p \in \mathbb{Z}$ un primo y $K := \mathbb{Q}(\zeta_p)$ un cuerpo ciclotómico, entonces.

1. Para cada $1 \leq k \leq p-1$ se tiene que

$$1 + \zeta_p + \dots + \zeta_p^{k-1}$$

es invertible en \mathcal{O}_K .

2. Existe u invertible en \mathcal{O}_K tal que $p = (1 - \zeta_p)^{p-1}u$.

Demostración. 1. Para cada $1 \leq k \leq p-1$ defínase

$$z_k := \frac{\zeta_p^k - 1}{\zeta_p - 1} = 1 + \zeta_p + \cdots + \zeta_p^{k-1} \in \mathcal{O}_K,$$

luego, sea $b \in \mathbb{N}$ tal que $kb \equiv 1 \pmod{p}$, entonces $(\zeta_p^k)^b = \zeta_p$, así

$$z_k^{-1} = \frac{\zeta_p - 1}{\zeta_p^k - 1} = \frac{(\zeta_p^k)^b - 1}{\zeta_p^k - 1} = 1 + \zeta_p^k + \cdots + (\zeta_p^k)^{b-1} \in \mathcal{O}_K.$$

Luego, $z_k = 1 + \zeta_p + \cdots + \zeta_p^{k-1}$ es invertible en \mathcal{O}_K .

2. Para cada $1 \leq k \leq p-1$ se tiene que $\zeta_p^k - 1 = (\zeta_p - 1)z_k$ donde z_k es invertible en \mathcal{O}_K . Así,

$$p = N_{\mathbb{Q}}^K(1 - \zeta_p) = \prod_{k=1}^{p-1} (1 - \zeta_p^k) = (1 - \zeta_p)^{p-1} u,$$

donde

$$u := \prod_{k=1}^{p-1} z_k \in \mathcal{O}_K$$

es invertible en \mathcal{O}_K . □

La proposición anterior implica que

$$p\mathcal{O}_K = [(1 - \zeta_p)\mathcal{O}_K]^{p-1},$$

y puesto que

$$\|(1 - \zeta_p)\mathcal{O}_K\| = |N_{\mathbb{Q}}^K(1 - \zeta_p)| = p,$$

entonces $(1 - \zeta_p)\mathcal{O}_K$ es un ideal primo de \mathcal{O}_K .

Luego, si p es impar se tiene que p ramifica en $K = \mathbb{Q}(\zeta_p)$.

2.4. RAMIFICACIÓN EN EXTENSIONES DE GALOIS

Se dice que una extensión es de Galois abeliana, si además de ser extensión de Galois se tiene que el grupo de Galois es un grupo abeliano.

Ahora, se estudiarán algunas propiedades de los ideales mediante automorfismos.

Proposición 2.4.1. Sean $K \subseteq L$ cuerpos numéricos tales que L es una extensión de Galois de K . Sea $\sigma \in \text{Gal}(L/K)$, entonces.

1. $\sigma(\mathcal{O}_L) = \mathcal{O}_L$.
2. Si \mathfrak{A} es un ideal no nulo de \mathcal{O}_L , entonces $\sigma(\mathfrak{A})$ es un ideal no nulo de \mathcal{O}_L .

3. Si \mathfrak{A} es un ideal fraccionario de L , entonces $\sigma(\mathfrak{A})$ es un ideal fraccionario de L .

4. Si \mathfrak{P} es un ideal primo de \mathcal{O}_L , entonces $\sigma(\mathfrak{P})$ es un ideal primo de \mathcal{O}_L .

Demostración. 1. Sea $\alpha \in \sigma(\mathcal{O}_L)$, entonces $\alpha = \sigma(l)$ para algún $l \in \mathcal{O}_L$. Debido a que $\sigma \in \text{Gal}(L/K)$ entonces $\alpha = \sigma(l) \in \mathcal{O}_L$, esto implica que $\sigma(\mathcal{O}_L) \subseteq \mathcal{O}_L$. Por otro lado, sea $\beta \in \sigma^{-1}(\mathcal{O}_L)$, entonces $\beta = \sigma^{-1}(j)$ para algún $j \in \mathcal{O}_L$. Ya que $\sigma^{-1} \in \text{Gal}(L/K)$, entonces

$$\beta = \sigma^{-1}(j) \in \mathcal{O}_L,$$

y así

$$\sigma^{-1}(\mathcal{O}_L) \subseteq \mathcal{O}_L.$$

Luego,

$$\mathcal{O}_L = \sigma(\sigma^{-1}(\mathcal{O}_L)) \subseteq \sigma(\mathcal{O}_L),$$

entonces $\mathcal{O}_L \subseteq \sigma(\mathcal{O}_L)$. Y así, se obtiene la igualdad que se quería probar.

2. Se tiene que $\sigma(\mathfrak{A}) \neq \emptyset$ ya que $\mathfrak{A} \neq \emptyset$, luego, por el item anterior se tiene que

$$\sigma(\mathfrak{A}) \subseteq \mathcal{O}_L.$$

Sean $\alpha, \beta \in \sigma(\mathfrak{A})$, entonces $\alpha = \sigma(a), \beta = \sigma(b)$ para algunos $a, b \in \mathfrak{A}$, y así

$$\alpha + \beta = \sigma(a) + \sigma(b) = \sigma(a + b) \in \sigma(\mathfrak{A})$$

puesto que \mathfrak{A} es un ideal de \mathcal{O}_L .

Por otro lado, sea $y \in \mathcal{O}_L$, luego, existe $x \in \mathcal{O}_L$ tal que $y = \sigma(x)$, entonces

$$\alpha y = \sigma(a)\sigma(x) = \sigma(ax) \in \sigma(\mathfrak{A})$$

ya que \mathfrak{A} es un ideal de \mathcal{O}_L .

Así, se obtiene que $\sigma(\mathfrak{A})$ es un ideal de \mathcal{O}_L .

3. Ya que \mathfrak{A} es un ideal fraccionario de L , entonces $\mathfrak{A} = \alpha\mathfrak{B}$, donde $\alpha \in L$ no nulo y \mathfrak{B} es un ideal de \mathcal{O}_L . Entonces $\sigma(\mathfrak{A}) = \sigma(\alpha)\sigma(\mathfrak{B})$, ya que $\sigma(\alpha) \neq 0$ y $\sigma(\mathfrak{B})$ es un ideal de \mathcal{O}_L , se concluye que $\sigma(\mathfrak{A})$ es un ideal fraccionario de L .

4. Supóngase que $\sigma(\mathfrak{P})$ no es un ideal primo de \mathcal{O}_L , de modo que

$$\sigma(\mathfrak{P}) = \mathfrak{P}_1 \cdots \mathfrak{P}_r$$

donde $r \geq 2$ y $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ son ideales primos de \mathcal{O}_L . Aplicando σ^{-1} se obtiene que

$$\mathfrak{P} = \sigma^{-1}(\mathfrak{P}_1) \cdots \sigma^{-1}(\mathfrak{P}_r).$$

Note que $\sigma^{-1}(\mathfrak{P}_i) \neq \mathcal{O}_L$ para todo $1 \leq i \leq r$, esto implica que \mathfrak{P} no es un ideal primo de \mathcal{O}_L . □

Proposición 2.4.2. Sean $K \subseteq L$ cuerpos numéricos tales que L es una extensión de Galois de K , sea \mathfrak{p} un ideal primo de \mathcal{O}_K y $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ donde $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ son ideales primos de \mathcal{O}_L . Sea $\sigma \in \text{Gal}(L/K)$, entonces para cada $1 \leq i \leq g$ se tiene que $\sigma(\mathfrak{P}_i)$ es un ideal primo de \mathcal{O}_L que contiene a \mathfrak{p} .

Demostración. Ya que $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ donde $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ son ideales primos de \mathcal{O}_L , entonces aplicando σ se obtiene

$$\mathfrak{p}\mathcal{O}_L = \sigma(\mathfrak{P}_1)^{e_1} \cdots \sigma(\mathfrak{P}_g)^{e_g},$$

y además $\sigma(\mathfrak{P}_1), \dots, \sigma(\mathfrak{P}_g)$ son ideales primos de \mathcal{O}_L .

De la igualdad anterior se obtiene que $\sigma(\mathfrak{P}_i) | \mathfrak{p}\mathcal{O}_L$ para cada $1 \leq i \leq g$, de modo que $\sigma(\mathfrak{P}_i)$ contiene a \mathfrak{p} para cada $1 \leq i \leq g$. □

Con ayuda de estos resultados se obtiene una proposición que relaciona la ramificación de un primo en \mathbb{Z} y el discriminante del cuerpo, y también un teorema que relaciona los índices de ramificación, los grados inerciales y el grado de la extensión cuando esta es de Galois.

Proposición 2.4.3. Sea $p \in \mathbb{Z}$ un primo, y sea K un cuerpo numérico tal que $[K : \mathbb{Q}] = n$. Si p ramifica en K entonces $p | \text{disc}(K)$.

Demostración. Sea \mathfrak{p} un ideal primo de \mathcal{O}_K que contiene a p tal que $e := e_{\mathfrak{p}|p} > 1$. Y sea

$$p\mathcal{O}_K = \mathfrak{p}^e \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$$

la factorización de p en ideales primos de \mathcal{O}_K . Defínase $\mathfrak{q} := \mathfrak{p}^{e-1} \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$, de modo que

$$p\mathcal{O}_K = \mathfrak{p}\mathfrak{q}.$$

Nótese que \mathfrak{q} es un ideal de \mathcal{O}_K que tiene en su factorización a todos los ideales primos de \mathcal{O}_K que contienen a p . Además, se tiene que $p\mathcal{O}_K \subsetneq \mathfrak{q}$, de lo contrario

$$\mathfrak{p}\mathfrak{q} = p\mathcal{O}_K = \mathfrak{q},$$

esto implica que $\mathfrak{p} = \mathcal{O}_K$, lo cual es falso.

Sea $\alpha \in \mathfrak{q} - p\mathcal{O}_K$, así, α está contenido en todos los ideales primos de \mathcal{O}_K que contienen a p , pero no está contenido en $p\mathcal{O}_K$.

Sean $n := [K : \mathbb{Q}]$ y $\{\eta_1, \dots, \eta_n\}$ una \mathbb{Z} -base de \mathcal{O}_K , luego, existen $m_1, \dots, m_n \in \mathbb{Z}$ tales que

$$\alpha = m_1\eta_1 + \cdots + m_n\eta_n,$$

puesto que α no está contenido en $p\mathcal{O}_K$ entonces existe $1 \leq i \leq n$ tal que $p \nmid m_i$, sin pérdida de generalidad supóngase que $p \nmid m_1$.

Por otro lado, sean $\sigma_1, \dots, \sigma_n$ los homomorfismos de K en \mathbb{C} que fijan a \mathbb{Q} , usando las propiedades del determinante y

$$\det \begin{bmatrix} m_1\sigma_1(\eta_1) & \sigma_1(\eta_2) & \cdots & \sigma_1(\eta_n) \\ m_1\sigma_2(\eta_1) & \sigma_2(\eta_2) & \cdots & \sigma_2(\eta_n) \\ \vdots & \vdots & \ddots & \vdots \\ m_1\sigma_n(\eta_1) & \sigma_n(\eta_2) & \cdots & \sigma_n(\eta_n) \end{bmatrix} = m_1 \det \begin{bmatrix} \sigma_1(\eta_1) & \sigma_1(\eta_2) & \cdots & \sigma_1(\eta_n) \\ \sigma_2(\eta_1) & \sigma_2(\eta_2) & \cdots & \sigma_2(\eta_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\eta_1) & \sigma_n(\eta_2) & \cdots & \sigma_n(\eta_n) \end{bmatrix}$$

se obtiene que

$$\text{disc}(\alpha, \eta_2, \dots, \eta_n) = m_1^2 \text{disc}(\eta_1, \dots, \eta_n) = m_1^2 \text{disc}(K).$$

La idea es probar que $p \mid \text{disc}(\alpha, \alpha_2, \dots, \alpha_n)$. Para esto, el corolario 1.1.2 implica que existe L un cuerpo numérico que es una extensión finita de K tal que L es una extensión normal de \mathbb{Q} , esto quiere decir que L es una extensión de Galois de \mathbb{Q} .

Ya que α está contenido en todo ideal primo de \mathcal{O}_K que contiene a p , entonces α está contenido en todo ideal primo de \mathcal{O}_L que contiene a p . En efecto, sea \mathfrak{P} un ideal primo de \mathcal{O}_L que contiene a p , y puesto que $\mathfrak{P} \cap \mathcal{O}_K$ es un ideal primo de \mathcal{O}_K que contiene a p , se concluye que $\alpha \in \mathfrak{P} \cap \mathcal{O}_K$, es decir que $\alpha \in \mathfrak{P}$.

Ahora, sean \mathfrak{P} un ideal primo de \mathcal{O}_L que contiene a p y $\sigma \in \text{Gal}(L/\mathbb{Q})$, entonces $\sigma^{-1}(\mathfrak{P})$ es un ideal primo de \mathcal{O}_L tal que $p = \sigma^{-1}(p) \in \sigma^{-1}(\mathfrak{P})$. Lo anterior implica que $\alpha \in \sigma^{-1}(\mathfrak{P})$, y así $\sigma(\alpha) \in \mathfrak{P}$.

Por último, el lema 1.1.1 implica que para cada $1 \leq i \leq n$, el homomorfismo σ_i se extiende a $[L : K]$ homomorfismos de L en \mathbb{C} que fijan a \mathbb{Q} , luego, el teorema 1.1.1 implica que los homomorfismos de L en \mathbb{C} que extienden a cada σ_i son automorfismos de L .

Sea $\gamma_i \in \text{Gal}(L/\mathbb{Q})$ una extensión de σ_i a L para cada $1 \leq i \leq n$, es decir que $\gamma_i|_K = \sigma_i$. Por lo tanto, se tiene que

$$\sigma_i(\alpha) = \gamma_i(\alpha) \in \mathfrak{P}$$

para cada $1 \leq i \leq n$. La definición del determinante implica que

$$\text{disc}(\alpha, \eta_2, \dots, \eta_n) \in \mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}.$$

De modo que

$$p \mid \text{disc}(\alpha, \eta_2, \dots, \eta_n),$$

y como $p \nmid m_1^2$, se concluye que $p \mid \text{disc}(K)$. □

Ejemplo 2.4.1. Sean $p \in \mathbb{Z}$ un primo impar y $K := \mathbb{Q}(\zeta_p)$ un cuerpo ciclotómico. Entonces p es el único primo que ramifica en K .

En efecto, la proposición 2.3.4 implica que p ramifica en K . Ahora, si $q \in \mathbb{Z}$ es otro primo que ramifica en K , la proposición anterior implica que $q \mid \text{disc}(K) = (-1)^{\binom{p-1}{2}} p^{p-2}$, por lo tanto $q = p$, y así, p es el único primo que ramifica en K .

Teorema 2.4.1. Sean $K \subseteq L$ cuerpos numéricos tales que L es una extensión de Galois de K , si \mathfrak{p} es un ideal primo de \mathcal{O}_K , entonces:

1. El grupo de Galois $\text{Gal}(L/K)$ actúa transitivamente sobre los ideales primos de \mathcal{O}_L que contienen a \mathfrak{p} . Esto es, si $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ donde $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ son ideales primos de \mathcal{O}_L , entonces para cada par $\mathfrak{P}_r, \mathfrak{P}_s$ con $1 \leq r, s \leq g$ existe $\sigma \in \text{Gal}(L/K)$ tal que $\sigma(\mathfrak{P}_r) = \mathfrak{P}_s$.
2. Si $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ donde $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ son ideales primos de \mathcal{O}_L , entonces los índices de ramificación son iguales es decir $e_1 = e_2 = \cdots = e_g := e$, y los grados inerciales de \mathfrak{P}_i sobre \mathfrak{p} son iguales es decir $f_1 = f_2 = \cdots = f_g := f$.
Y por lo tanto $[L : K] = efg$.

Demostración. 1. Ya que L es una extensión de Galois de K se tiene que $[L : K] := n < \infty$, y $\text{Gal}(L/K) = \{\sigma_1 = i_L, \sigma_2, \dots, \sigma_n\}$, además se tiene que los n homomorfismos de L en \mathbb{C} que fijan a K son exactamente los elementos de $\text{Gal}(L/K)$.

Sean $\mathfrak{P}_r, \mathfrak{P}_s$ como en la hipótesis. Si $r = s$ entonces se puede tomar $\sigma = i_L$.

Supóngase que $r \neq s$; y sea $\alpha \in \mathfrak{P}_s$, y considere la norma de α en L relativa a K

$$N_K^L(\alpha) = \prod_{i=1}^n \sigma_i(\alpha) = \alpha \prod_{i=2}^n \sigma_i(\alpha).$$

Puesto que $\sigma_i(\alpha) \in \mathcal{O}_L$ para cada $2 \leq i \leq n$, entonces $N_K^L(\alpha) \in \mathfrak{P}_s$.

Ya que $\alpha \in \mathfrak{P}_s \subseteq \mathcal{O}_L$, la propiedad E.1.1 implica que $N_K^L(\alpha) \in \mathcal{O}_K$, de modo que

$$N_K^L(\alpha) \in \mathfrak{P}_s \cap \mathcal{O}_K = \mathfrak{p} \subseteq \mathfrak{P}_r.$$

Como \mathfrak{P}_r es un ideal primo de \mathcal{O}_L , existe $1 \leq i \leq n$ tal que $\sigma_i(\alpha) \in \mathfrak{P}_r$, y sea $1 \leq j \leq n$ tal que $\sigma_j = \sigma_i^{-1}$, aplicando σ_j se obtiene que $\alpha \in \sigma_j(\mathfrak{P}_r)$.

Esto implica que

$$\mathfrak{P}_s \subseteq \bigcup_{i=1}^n \sigma_i(\mathfrak{P}_r).$$

Entonces existe $1 \leq i \leq n$ tal que $\mathfrak{P}_s \subseteq \sigma_i(\mathfrak{P}_r)$, y como \mathfrak{P}_s es un ideal maximal de \mathcal{O}_L se tiene que $\sigma_i(\mathfrak{P}_r) = \mathfrak{P}_s$.

2. Supóngase que $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ donde $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ son ideales primos de \mathcal{O}_L , dados $1 \leq r, s \leq g$ existe $\sigma \in \text{Gal}(L/K)$ tal que $\sigma(\mathfrak{P}_r) = \mathfrak{P}_s$, aplicando σ se obtiene

$$\mathfrak{p}\mathcal{O}_L = \sigma(\mathfrak{P}_1)^{e_1} \cdots \mathfrak{P}_s^{e_r} \cdots \sigma(\mathfrak{P}_g)^{e_g}$$

de modo que por la unicidad de la factorización se concluye que $e_r = e_s$ para todo $1 \leq r, s \leq g$, es decir $e := e_1 = \cdots = e_g$.

Además, se tiene el siguiente isomorfismo de $\mathcal{O}_K/\mathfrak{p}$ -módulos

$$\begin{aligned} \phi : \mathcal{O}_L/\mathfrak{P}_r &\longrightarrow \mathcal{O}_L/\mathfrak{P}_s \\ \bar{x} &\longmapsto \phi(\bar{x}) := \overline{\sigma(x)} \end{aligned}$$

Luego

$$|\mathcal{O}_L/\mathfrak{P}_r| = |\mathcal{O}_L/\mathfrak{P}_s|,$$

esto es

$$|\mathcal{O}_K/\mathfrak{p}|^{f_r} = |\mathcal{O}_K/\mathfrak{p}|^{f_s}$$

y por lo tanto $f_r = f_s$ para cada $1 \leq r, s \leq g$, es decir $f := f_1 = \cdots = f_g$.

La igualdad $[L : K] = efg$ se obtiene como resultado del teorema 2.1.1.

□

El teorema anterior modifica la definición sobre la ramificación en el caso de las extensiones de Galois.

Definición 2.4.1. Sean $K \subseteq L$ cuerpos numéricos tales que L es una extensión de Galois de K , sea \mathfrak{p} un ideal primo de \mathcal{O}_K y $\mathfrak{p}\mathcal{O}_L = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$ donde $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ son ideales primos de \mathcal{O}_L .

Se dice que \mathfrak{p} ramifica en L si $e > 1$, y que \mathfrak{p} no ramifica en L si $e = 1$.

Se dice que \mathfrak{p} se descompone completamente en L si $e = 1 = f$, en este caso \mathfrak{p} no ramifica en L y $[L : K] = g$.

2.4.1. TEOREMA DE KUMMER-DEDEKIND

Dada L una extensión primitiva de cuerpo numérico, su anillo de enteros algebraicos \mathcal{O}_L en general no es la adjunción del elemento primitivo al anillo de enteros algebraicos del cuerpo base, aunque el índice resulta finito. El teorema de Kummer-Dedekind es un criterio para la ramificación de un ideal primo del cuerpo base.

Sean K y L cuerpos numéricos tales que L es una extensión de Galois de K y $[L : K] = n$, el teorema del elemento primitivo implica que $L = K(\alpha)$ para algún $\alpha \in \mathcal{O}_L$.

Nótese que \mathcal{O}_L es un grupo abeliano libre de rango mn donde $m := [K : \mathbb{Q}]$, además, $\mathcal{O}_K[\alpha]$ es un subgrupo aditivo de \mathcal{O}_L también de rango mn , y por lo tanto el índice $[\mathcal{O}_L : \mathcal{O}_K[\alpha]]$ es finito.

Teorema 2.4.2 (Kummer-Dedekind). Sean K y L cuerpos numéricos tales que L es una extensión de Galois de K y $[L : K] = n$, donde $L = K(\alpha)$ para algún $\alpha \in \mathcal{O}_L$.

Sea $f(x) \in K[x]$ el polinomio mínimo de α , así $f(x) \in \mathcal{O}_K[x]$.

Sea \mathfrak{p} un ideal primo de \mathcal{O}_K tal que el único primo racional $p \in \mathbb{Z}$ que existe contenido en \mathfrak{p} no divide a $[\mathcal{O}_L : \mathcal{O}_K[\alpha]]$.

Si $f(x)$ es separable módulo \mathfrak{p} , así $f(x) \equiv f_1(x) \cdots f_g(x) \pmod{\mathfrak{p}}$ donde $f_1(x), \dots, f_g(x) \in \mathcal{O}_K[x]$ son distintos, mónicos e irreducibles módulo \mathfrak{p} . Entonces:

Para cada $1 \leq i \leq g$ se tiene que

$$\mathfrak{P}_i := \mathfrak{p}\mathcal{O}_L + f_i(\alpha)\mathcal{O}_L$$

es un ideal primo de \mathcal{O}_L , y $\mathfrak{P}_i \neq \mathfrak{P}_j$ para $i \neq j$.

Además

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_g,$$

de donde \mathfrak{p} no ramifica en L .

Y por último, $gr(f_i(x)) = f$ para cada $1 \leq i \leq g$, donde $f := f_{\mathfrak{P}_i|\mathfrak{p}}$ es el grado inercial.

Demostración. Nótese que el polinomio mínimo de α sobre K satisface que $f(x) \in \mathcal{O}_K[x]$. En efecto, sean $\alpha_1 := \alpha, \alpha_2, \dots, \alpha_n$ las n raíces de $f(x)$, donde $n = gr(f(x))$.

Sea $z(x) \in \mathbb{Z}[x]$ un polinomio mónico tal que $z(\alpha) = 0$, así $f(x)|z(x)$, y por lo tanto las raíces $\alpha_2, \dots, \alpha_n$ también son enteros algebraicos.

Ahora, escribiendo $f(x)$ en su factorización se obtiene

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

Y calculando los coeficientes de $f(x)$ a partir de esta factorización se obtiene que cada coeficiente es un polinomio simétrico elemental de n variables evaluado en $\alpha_1, \dots, \alpha_n$, esto implica que cada coeficiente de $f(x)$ es un entero algebraico, luego $f(x) \in \mathcal{O}_K[x]$.

Primero se van a demostrar tres afirmaciones, y a partir de ellas se va a concluir el teorema.

Afirmación 1. Para cada $1 \leq i \leq g$, se tiene que $\mathfrak{P}_i = \mathcal{O}_L$ o que $\mathcal{O}_L/\mathfrak{P}_i$ es un cuerpo de tamaño $|\mathcal{O}_K/\mathfrak{p}|^{gr(f_i(x))}$.

En efecto, para cada $1 \leq i \leq g$ sea

$$\begin{aligned} \varphi_i : \mathcal{O}_K[x] &\longrightarrow (\mathcal{O}_K/\mathfrak{p})[x]/\langle \overline{f_i(x)} \rangle \\ k_0 + k_1x + \cdots + k_r x^r &\longmapsto \varphi_i(k_0 + k_1x + \cdots + k_r x^r) := \overline{k_0} + \overline{k_1}x + \cdots + \overline{k_r}x^r + \langle \overline{f_i(x)} \rangle \end{aligned}$$

un homomorfismo de anillos. Además, para cada $1 \leq i \leq g$ se tiene que φ_i es sobreyectivo y $Ker(\varphi_i) = \mathfrak{p}\mathcal{O}_K[x] + f_i(x)\mathcal{O}_K[x]$.

Por lo tanto se obtiene que para cada $1 \leq i \leq g$,

$$\mathcal{O}_K[x]/(\mathfrak{p}\mathcal{O}_K[x] + f_i(x)\mathcal{O}_K[x]) \cong (\mathcal{O}_K/\mathfrak{p})[x]/\langle \overline{f_i(x)} \rangle.$$

Por hipótesis, $\overline{f_i}(x)$ es irreducible en $(\mathcal{O}_K/\mathfrak{p})[x]$ para cada $1 \leq i \leq g$, esto implica que para cada $1 \leq i \leq g$

$$(\mathcal{O}_K/\mathfrak{p})[x]/\langle \overline{f_i}(x) \rangle$$

es un cuerpo, por lo tanto $\mathfrak{p}\mathcal{O}_K[x] + f_i(x)\mathcal{O}_K[x]$ es un ideal maximal de $\mathcal{O}_K[x]$ para cada $1 \leq i \leq g$.

Por otro lado, sea

$$\begin{aligned} \phi : \mathcal{O}_K[x] &\longrightarrow \mathcal{O}_L \\ k_0 + k_1x + \cdots + k_rx^r &\longmapsto \phi(k_0 + k_1x + \cdots + k_rx^r) := k_0 + k_1\alpha + \cdots + k_r\alpha^r \end{aligned}$$

un homomorfismo de anillos. Y para cada $1 \leq i \leq g$ sea

$$\begin{aligned} v_i : \mathcal{O}_L &\longrightarrow \mathcal{O}_L/\mathfrak{P}_i \\ l &\longmapsto v_i(l) := \bar{l} \end{aligned}$$

un homomorfismo de anillos. Luego, para cada $1 \leq i \leq g$ se tiene el homomorfismo de anillos

$$\begin{aligned} v_i \circ \phi : \mathcal{O}_K[x] &\longrightarrow \mathcal{O}_L/\mathfrak{P}_i \\ k_0 + k_1x + \cdots + k_rx^r &\longmapsto v_i \circ \phi(k_0 + k_1x + \cdots + k_rx^r) = \overline{k_0 + k_1\alpha + \cdots + k_r\alpha^r} \end{aligned}$$

Además, se tiene que $\mathfrak{p}\mathcal{O}_K[x] + f_i(x)\mathcal{O}_K[x] \subseteq \text{Ker}(v_i \circ \phi)$ para cada $1 \leq i \leq g$.

Ya que $\mathfrak{p}\mathcal{O}_K[x] + f_i(x)\mathcal{O}_K[x]$ es un ideal maximal de $\mathcal{O}_K[x]$ para cada $1 \leq i \leq g$, entonces

$$\text{Ker}(v_i \circ \phi) = \mathfrak{p}\mathcal{O}_K[x] + f_i(x)\mathcal{O}_K[x] \text{ o } \text{Ker}(v_i \circ \phi) = \mathcal{O}_K[x].$$

Por otro lado, puesto que $\mathcal{O}_K[\alpha] \subseteq \mathcal{O}_K[\alpha] + p\mathcal{O}_L$, entonces

$$(\mathcal{O}_L/\mathcal{O}_K[\alpha])/((\mathcal{O}_K[\alpha] + p\mathcal{O}_L)/\mathcal{O}_K[\alpha]) \cong \mathcal{O}_L/(\mathcal{O}_K[\alpha] + p\mathcal{O}_L),$$

y así $|\mathcal{O}_L/(\mathcal{O}_K[\alpha] + p\mathcal{O}_L)|$ divide a $|\mathcal{O}_L/\mathcal{O}_K[\alpha]|$.

Análogamente, ya que $p\mathcal{O}_L \subseteq \mathcal{O}_K[\alpha] + p\mathcal{O}_L$, entonces

$$(\mathcal{O}_L/p\mathcal{O}_L)/((\mathcal{O}_K[\alpha] + p\mathcal{O}_L)/p\mathcal{O}_L) \cong \mathcal{O}_L/(\mathcal{O}_K[\alpha] + p\mathcal{O}_L),$$

y así $|\mathcal{O}_L/(\mathcal{O}_K[\alpha] + p\mathcal{O}_L)|$ divide a $|\mathcal{O}_L/p\mathcal{O}_L|$.

Ya que

$$|\mathcal{O}_L/p\mathcal{O}_L| = \|p\mathcal{O}_L\| = p^{[L:\mathbb{Q}]},$$

y por hipótesis $p \nmid |\mathcal{O}_L/\mathcal{O}_K[\alpha]|$, entonces

$$|\mathcal{O}_L/(\mathcal{O}_K[\alpha] + p\mathcal{O}_L)| = 1,$$

de donde $\mathcal{O}_L = \mathcal{O}_K[\alpha] + p\mathcal{O}_L$. Ya que $p \in \mathfrak{p} \subseteq \mathfrak{P}_i$ para cada $1 \leq i \leq g$, entonces

$$\mathcal{O}_L = \mathcal{O}_K[\alpha] + p\mathcal{O}_L \subseteq \mathcal{O}_K[\alpha] + \mathfrak{P}_i \subseteq \mathcal{O}_L,$$

es decir que $\mathcal{O}_L = \mathcal{O}_K[\alpha] + \mathfrak{P}_i$ para cada $1 \leq i \leq g$. De esto se concluye que para cada $1 \leq i \leq g$ el homomorfismo $v_i \circ \phi$ es sobreyectivo.

Por lo tanto, se tiene que para cada $1 \leq i \leq g$, $\mathcal{O}_L = \mathfrak{P}_i$ o

$$\mathcal{O}_L/\mathfrak{P}_i \cong \mathcal{O}_K[x]/(\mathfrak{p}\mathcal{O}_K[x] + f_i(x)\mathcal{O}_K[x]),$$

y en este segundo caso se tiene que $\mathcal{O}_L/\mathfrak{P}_i$ es un cuerpo de tamaño $|\mathcal{O}_K/\mathfrak{p}|^{gr(f_i(x))}$.

Afirmación 2. Para todo $1 \leq i, j \leq g$ con $i \neq j$ se tiene que $\mathfrak{P}_i + \mathfrak{P}_j = \mathcal{O}_L$.

En efecto, puesto que $\mathcal{O}_K/\mathfrak{p}$ es un cuerpo, entonces $(\mathcal{O}_K/\mathfrak{p})[x]$ es un DIP.

Y ya que $\bar{f}_i(x) \in (\mathcal{O}_K/\mathfrak{p})[x]$ es irreducible para cada $1 \leq i \leq g$, entonces $\text{mcd}(\bar{f}_i(x), \bar{f}_j(x)) = \bar{1}$ con $i \neq j$. Luego, existen $\bar{h}(x), \bar{l}(x) \in (\mathcal{O}_K/\mathfrak{p})[x]$ tales que

$$\bar{1} = \bar{f}_i(x)\bar{h}(x) + \bar{f}_j(x)\bar{l}(x),$$

de modo que

$$f_i(x)h(x) + f_j(x)l(x) - 1 = w(x) \text{ para algún } w(x) \in \mathfrak{p}[x],$$

y así

$$f_i(\alpha)h(\alpha) + f_j(\alpha)l(\alpha) - 1 = w(\alpha) \in \mathfrak{p}\mathcal{O}_L,$$

y por lo tanto se obtiene que

$$1 = -w(\alpha) + f_i(\alpha)h(\alpha) + f_j(\alpha)l(\alpha) \in \mathfrak{p}\mathcal{O}_L + f_i(\alpha)\mathcal{O}_L + f_j(\alpha)\mathcal{O}_L = \mathfrak{P}_i + \mathfrak{P}_j.$$

Esto implica que $\mathfrak{P}_i + \mathfrak{P}_j = \mathcal{O}_L$ para $i \neq j$.

Afirmación 3. $\mathfrak{p}\mathcal{O}_L | \mathfrak{P}_1 \cdots \mathfrak{P}_g$.

En efecto, ya que

$$f(x) - f_1(x) \cdots f_g(x) \in \mathfrak{p}[x],$$

entonces

$$f_1(\alpha) \cdots f_g(\alpha) \in \mathfrak{p}\mathcal{O}_L,$$

y así, se obtiene que

$$\begin{aligned} \mathfrak{P}_1 \cdots \mathfrak{P}_g &= \prod_{i=1}^g (\mathfrak{p}\mathcal{O}_L + f_i(\alpha)\mathcal{O}_L) \\ &\subseteq \mathfrak{p}\mathcal{O}_L + \prod_{i=1}^g f_i(\alpha)\mathcal{O}_L \\ &\subseteq \mathfrak{p}\mathcal{O}_L. \end{aligned}$$

Por lo tanto, $\mathfrak{p}\mathcal{O}_L | \mathfrak{P}_1 \cdots \mathfrak{P}_g$.

El teorema se concluye de las afirmaciones 1, 2 y 3. En efecto, reorganizando si es necesario, supóngase que $\mathfrak{P}_1, \dots, \mathfrak{P}_s \neq \mathcal{O}_L$ y $\mathfrak{P}_{s+1}, \dots, \mathfrak{P}_g = \mathcal{O}_L$.

La afirmación 1 implica que $\mathfrak{P}_1, \dots, \mathfrak{P}_s$ son los ideales primos de \mathcal{O}_L que contienen a \mathfrak{p} , y puesto que para cada $1 \leq i \leq s$ se tiene que

$$|\mathcal{O}_L/\mathfrak{P}_i| = |\mathcal{O}_K/\mathfrak{p}|^{gr(f_i(x))},$$

y

$$|\mathcal{O}_L/\mathfrak{P}_i| = |\mathcal{O}_K/\mathfrak{p}|^{f_{\mathfrak{P}_i|\mathfrak{p}}},$$

entonces $gr(f_i(x)) = f_{\mathfrak{P}_i|\mathfrak{p}}$ para cada $1 \leq i \leq s$, y ya que la extensión es de Galois, entonces

$$f_{\mathfrak{P}_1|\mathfrak{p}} = \dots = f_{\mathfrak{P}_s|\mathfrak{p}} := f,$$

y así

$$gr(f_1(x)) = \dots = gr(f_s(x)) = f.$$

La afirmación 2 implica que $\mathfrak{P}_i + \mathfrak{P}_j = \mathcal{O}_L$ para cada $1 \leq i, j \leq s$ con $i \neq j$, de modo que $\mathfrak{P}_i \neq \mathfrak{P}_j$ para cada $1 \leq i, j \leq s$ con $i \neq j$.

Por último, la afirmación 3 se convierte en $\mathfrak{p}\mathcal{O}_L|\mathfrak{P}_1 \cdots \mathfrak{P}_s$, pero como $\mathfrak{p} \subseteq \mathfrak{P}_1, \dots, \mathfrak{P}_s$, se concluye que

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_s.$$

El teorema 2.4.1 implica que $n = [L : K] = fs$, por otro lado, y puesto que $n = gr(f(x))$ entonces $n = fg$, de modo que $s = g$.

De esta manera se concluye que para cada $1 \leq i \leq g$ se tiene que

$$\mathfrak{P}_i := \mathfrak{p}\mathcal{O}_L + f_i(\alpha)\mathcal{O}_L$$

es un ideal primo de \mathcal{O}_L , y $\mathfrak{P}_i \neq \mathfrak{P}_j$ para $i \neq j$.

Además

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_g,$$

de donde \mathfrak{p} no ramifica en L .

Y $gr(f_i(x)) = f$ para cada $1 \leq i \leq g$, donde $f := f_{\mathfrak{P}_i|\mathfrak{p}}$ es el grado inercial. \square

Ejemplo 2.4.2. Sean $K := \mathbb{Q}$ y $L := \mathbb{Q}(\zeta_5)$, en la sección 2.3 se probó que L es una extensión de Galois de K . También se probó que $\mathcal{O}_L = \mathbb{Z}[\zeta_5]$, por lo tanto $[\mathcal{O}_L : \mathbb{Z}[\zeta_5]] = 1$, de modo que el teorema de Kummer-Dedekind se puede aplicar en cualquier ideal primo de \mathbb{Z} .

El polinomio $f(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Z}[x]$ es el polinomio mínimo de ζ_5 . Luego, sea $2\mathbb{Z}$ un ideal primo de \mathbb{Z} , en este caso $f(x)$ es irreducible (*mod* 2), y por lo tanto $2\mathbb{Z}[\zeta_5]$ es un ideal primo de $\mathbb{Z}[\zeta_5]$.

Ahora, sea $11\mathbb{Z}$ un ideal primo de \mathbb{Z} , entonces

$$f(x) \equiv (x+2)(x+6)(x+7)(x+8) \pmod{11}.$$

Por el teorema de Kummer-Dedekind se obtiene que

$$11\mathbb{Z}[\zeta_5] = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3\mathfrak{P}_4,$$

donde

$$\mathfrak{P}_1 = 11\mathbb{Z}[\zeta_5] + (\zeta_5 + 2)\mathbb{Z}[\zeta_5],$$

$$\mathfrak{P}_2 = 11\mathbb{Z}[\zeta_5] + (\zeta_5 + 6)\mathbb{Z}[\zeta_5],$$

$$\mathfrak{P}_3 = 11\mathbb{Z}[\zeta_5] + (\zeta_5 + 7)\mathbb{Z}[\zeta_5]$$

y

$$\mathfrak{P}_4 = 11\mathbb{Z}[\zeta_5] + (\zeta_5 + 8)\mathbb{Z}[\zeta_5].$$

Se probó que el ideal $11\mathbb{Z}$ no ramifica en L , y se obtuvo su factorización de ideales primos de $\mathbb{Z}[\zeta_5]$.

2.4.2. SÍMBOLO DE ARTIN

Dados $K \subseteq L$ cuerpos numéricos tales que L es una extensión de Galois de K , y sean \mathfrak{p} un ideal primo de \mathcal{O}_K y \mathfrak{P} un ideal primo de \mathcal{O}_L tales que $\mathfrak{p} \subseteq \mathfrak{P}$, se pueden asociar dos subgrupos de $\text{Gal}(L/K)$ determinados por \mathfrak{P} , estos son, el grupo de descomposición y el grupo de inercia.

El grupo de descomposición surge de manera natural de la acción de $\text{Gal}(L/K)$ sobre los ideales primos de \mathcal{O}_L que contienen a \mathfrak{p} .

Además, se tiene que el grupo de inercia es el núcleo de un homomorfismo sobreyectivo entre el grupo de descomposición y el grupo de Galois $\text{Gal}(\mathcal{O}_L/\mathfrak{P}/\mathcal{O}_K/\mathfrak{p})$. De aquí, se desprende que el cardinal del grupo de descomposición es el producto del índice de ramificación y el grado inercial, para el grupo de inercia se tiene que su cardinal es el índice de ramificación. Estos subgrupos son de gran ayuda para definir el símbolo y el homomorfismo de Artin.

Definición 2.4.2. Sean $K \subseteq L$ cuerpos numéricos tales que L es una extensión de Galois de K , y sean \mathfrak{p} un ideal primo de \mathcal{O}_K y \mathfrak{P} un ideal primo de \mathcal{O}_L tales que $\mathfrak{p} \subseteq \mathfrak{P}$.

Se define

$$D_{\mathfrak{P}} := \{\sigma \in \text{Gal}(L/K) : \sigma(\mathfrak{P}) = \mathfrak{P}\},$$

y se denomina el grupo de descomposición de \mathfrak{P} .

En la notación $D_{\mathfrak{P}}$ no se incluye a \mathfrak{p} , ya que \mathfrak{p} es el único ideal primo de \mathcal{O}_K que está contenido en \mathfrak{P} .

Observación 2.4.1. Sea $\sigma \in D_{\mathfrak{P}}$, entonces $\sigma(\mathfrak{P}) = \mathfrak{P}$, esto significa que σ fija el ideal \mathfrak{P} pero no implica que $\sigma(x) = x$ para todo $x \in \mathfrak{P}$.

Proposición 2.4.4. Sean $K \subseteq L$ cuerpos numéricos tales que L es una extensión de Galois de K , y sean \mathfrak{p} un ideal primo de \mathcal{O}_K y \mathfrak{P} un ideal primo de \mathcal{O}_L tales que $\mathfrak{p} \subseteq \mathfrak{P}$, entonces $D_{\mathfrak{P}}$ es un subgrupo de $\text{Gal}(L/K)$.

Demostración. Note que $D_{\mathfrak{P}} \neq \emptyset$, pues $i_L \in \text{Gal}(L/K)$ y $i_L(\mathfrak{P}) = \mathfrak{P}$, así $i_L \in D_{\mathfrak{P}}$. Ahora, sean $\sigma_1, \sigma_2 \in D_{\mathfrak{P}}$, entonces $\sigma_1(\mathfrak{P}) = \mathfrak{P}$ y $\sigma_2(\mathfrak{P}) = \mathfrak{P}$. De modo que

$$\sigma_1 \circ \sigma_2(\mathfrak{P}) = \sigma_1(\sigma_2(\mathfrak{P})) = \sigma_1(\mathfrak{P}) = \mathfrak{P},$$

y así $\sigma_1 \circ \sigma_2 \in D_{\mathfrak{P}}$.

También se tiene que

$$\sigma_1^{-1}(\sigma_1(\mathfrak{P})) = \sigma_1^{-1}(\mathfrak{P}),$$

esto implica que $\sigma_1^{-1}(\mathfrak{P}) = \mathfrak{P}$, es decir $\sigma_1^{-1} \in D_{\mathfrak{P}}$.

Luego, se concluye que $D_{\mathfrak{P}}$ es un subgrupo de $\text{Gal}(L/K)$. \square

Ahora, con el objetivo de definir otro subgrupo importante del grupo de Galois se tiene la siguiente proposición.

Proposición 2.4.5. Sean $K \subseteq L$ cuerpos numéricos tales que L es una extensión de Galois de K , sean \mathfrak{p} un ideal primo de \mathcal{O}_K y \mathfrak{P} un ideal primo de \mathcal{O}_L tales que $\mathfrak{p} \subseteq \mathfrak{P}$. Si $\sigma \in D_{\mathfrak{P}}$, entonces se induce un automorfismo $\bar{\sigma}$ de $\mathcal{O}_L/\mathfrak{P}$ que deja fijo a $\mathcal{O}_K/\mathfrak{p}$.

Demostración. Defínase

$$\begin{aligned} \bar{\sigma} : \mathcal{O}_L/\mathfrak{P} &\rightarrow \mathcal{O}_L/\mathfrak{P} \\ \bar{x} &\mapsto \bar{\sigma}(\bar{x}) := \overline{\sigma(x)} \end{aligned}$$

Se debe probar que $\bar{\sigma}$ es un homomorfismo de anillos biyectivo:

En efecto, primero note que $\bar{\sigma}$ está bien definido, si $\bar{x} = \bar{y}$ en $\mathcal{O}_L/\mathfrak{P}$, entonces $x - y \in \mathfrak{P}$, y así $\sigma(x) - \sigma(y) \in \sigma(\mathfrak{P}) = \mathfrak{P}$, es decir que $\overline{\sigma(x)} = \overline{\sigma(y)}$.

Además,

$$\bar{\sigma}(\bar{x} + \bar{y}) = \bar{\sigma}(\bar{x}) + \bar{\sigma}(\bar{y}),$$

$$\bar{\sigma}(\bar{x}\bar{y}) = \bar{\sigma}(\bar{x})\bar{\sigma}(\bar{y}),$$

$$\bar{\sigma}(\bar{1}) = \bar{1},$$

para todo $\bar{x}, \bar{y} \in \mathcal{O}_L/\mathfrak{P}$. Esto indica que $\bar{\sigma}$ es un homomorfismo de anillos.

Ahora, supóngase que $\bar{\sigma}(\bar{x}) = \bar{0}$, entonces $\overline{\sigma(x)} = \bar{0}$ y así $\sigma(x) \in \mathfrak{P}$, de modo que $x \in \mathfrak{P}$ ya que $\sigma \in D_{\mathfrak{P}}$, luego $\bar{x} = \bar{0}$ y por lo tanto $\bar{\sigma}$ es inyectivo. Por otro lado sea $\bar{y} \in \mathcal{O}_L/\mathfrak{P}$, existe $x \in \mathcal{O}_L$ tal que $y = \sigma(x)$, esto implica que $\bar{\sigma}(\bar{x}) = \overline{\sigma(x)} = \bar{y}$, y por lo tanto $\bar{\sigma}$ es sobreyectivo.

Por ultimo, $\bar{\sigma}$ deja fijo a $\mathcal{O}_K/\mathfrak{p}$:

Sea $\bar{k} \in \mathcal{O}_K/\mathfrak{p}$, y como $\sigma \in D_{\mathfrak{P}} \subseteq \text{Gal}(L/K)$ se tiene que $\bar{\sigma}(\bar{k}) = \overline{\sigma(k)} = \bar{k}$.

□

De la proposición anterior, se tiene que

$$\bar{\sigma} \in \text{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})).$$

Así, se puede definir el siguiente homomorfismo de grupos

$$\begin{aligned} f : D_{\mathfrak{P}} &\rightarrow \text{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})) \\ \sigma &\mapsto f(\sigma) := \bar{\sigma} \end{aligned} \tag{E.2.1}$$

que satisface $\text{Ker}(f) = I_{\mathfrak{P}}$ donde $I_{\mathfrak{P}} := \{\sigma \in \text{Gal}(L/K) : \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}}, \text{ para todo } \alpha \in \mathcal{O}_L\}$, y por lo tanto $I_{\mathfrak{P}} \trianglelefteq D_{\mathfrak{P}}$.

El grupo $I_{\mathfrak{P}}$ es llamado grupo de inercia de \mathfrak{P} .

Proposición 2.4.6. Sean L y K cuerpos numéricos tales que L es una extensión de Galois de K , sean \mathfrak{p} un ideal primo de \mathcal{O}_K y $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ los ideales primos de \mathcal{O}_L que contienen a \mathfrak{p} . Si se define

$$X := \{\mathfrak{P}_1, \dots, \mathfrak{P}_g\},$$

entonces el grupo $\text{Gal}(L/K)$ actúa sobre X . Además, para cada $\mathfrak{P} \in X$ se tiene que

$$|D_{\mathfrak{P}}| = ef,$$

donde $e = e_{\mathfrak{P}|\mathfrak{p}}$ y $f = f_{\mathfrak{P}|\mathfrak{p}}$.

Demostración. Defínase

$$\begin{aligned} \phi : \text{Gal}(L/K) \times X &\rightarrow X \\ (\sigma, \mathfrak{P}_i) &\mapsto \phi((\sigma, \mathfrak{P}_i)) := \sigma(\mathfrak{P}_i). \end{aligned}$$

Así, ϕ es una acción de $\text{Gal}(L/K)$ sobre X .

Por otro lado, sea $\mathfrak{P} \in X$, el estabilizador de \mathfrak{P} en $\text{Gal}(L/K)$ es

$$D_{\mathfrak{P}} = \{\sigma \in \text{Gal}(L/K) : \sigma(\mathfrak{P}) = \mathfrak{P}\},$$

y la orbita de \mathfrak{P} en $\text{Gal}(L/K)$ es

$$\{\sigma(\mathfrak{P}) : \sigma \in \text{Gal}(L/K)\},$$

puesto que $\text{Gal}(L/K)$ actúa transitivamente sobre los elementos de X , dado \mathfrak{P}_j para algún $1 \leq j \leq g$ existe $\sigma \in \text{Gal}(L/K)$ tal que $\sigma(\mathfrak{P}) = \mathfrak{P}_j$, y así, la orbita de \mathfrak{P} en $\text{Gal}(L/K)$ es X .

Sea $\mathfrak{P} \in X$, el teorema de la orbita y el estabilizador implica que

$$g = |\text{Gal}(L/K) : D_{\mathfrak{P}}|.$$

Ya que $|\text{Gal}(L/K)| = [L : K] = efg$, donde $e = e_{\mathfrak{P}|\mathfrak{p}}$ es el índice de ramificación y $f = f_{\mathfrak{P}|\mathfrak{p}}$ es el grado de inercia, se tiene que

$$|\text{Gal}(L/K) : D_{\mathfrak{P}}| = \frac{|\text{Gal}(L/K)|}{|D_{\mathfrak{P}}|},$$

y de aquí se obtiene que

$$|D_{\mathfrak{P}}| = ef.$$

□

Teorema 2.4.3. Sean $K \subseteq L$ cuerpos numéricos tales que L es una extensión de Galois de K , sean \mathfrak{p} un ideal primo de \mathcal{O}_K y \mathfrak{P} un ideal primo de \mathcal{O}_L tales que $\mathfrak{p} \subseteq \mathfrak{P}$. Y sea f el homomorfismo definido en E.2.1, entonces:

1. El homomorfismo f es sobreyectivo. Por lo tanto

$$D_{\mathfrak{P}}/I_{\mathfrak{P}} \cong \text{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})).$$

2. $|I_{\mathfrak{P}}| = e_{\mathfrak{P}|\mathfrak{p}}$ y $|D_{\mathfrak{P}}| = e_{\mathfrak{P}|\mathfrak{p}}f_{\mathfrak{P}|\mathfrak{p}}$.

Demostración. 1. Sea $L^{D_{\mathfrak{P}}}$ el cuerpo fijo de $D_{\mathfrak{P}}$, es decir

$$L^{D_{\mathfrak{P}}} := \{a \in L : \sigma(a) = a, \text{ para todo } \sigma \in D_{\mathfrak{P}}\},$$

y denótese $M := L^{D_{\mathfrak{P}}}$, de esta manera, $K \subseteq M \subseteq L$.

Sea $\mathcal{O}_M := M \cap \mathcal{O}_L$ el anillo de enteros algebraicos de M , y defínase $\mathfrak{Q}_M := \mathfrak{P} \cap \mathcal{O}_M$ un ideal primo de \mathcal{O}_M .

Se afirma que \mathfrak{P} es el único ideal primo de \mathcal{O}_L que contiene a \mathfrak{Q}_M . En efecto, en primer lugar, nótese que L es una extensión de Galois de M con $\text{Gal}(L/M) = D_{\mathfrak{P}}$. Por otro lado, sea \mathfrak{P}' un ideal primo de \mathcal{O}_L que contiene a \mathfrak{Q}_M , ya que $\text{Gal}(L/M)$ actúa transitivamente sobre los ideales primos de \mathcal{O}_L que contienen a \mathfrak{Q}_M , existe $\sigma \in \text{Gal}(L/M) = D_{\mathfrak{P}}$ tal que $\sigma(\mathfrak{P}) = \mathfrak{P}'$, de esto se concluye que $\mathfrak{P} = \mathfrak{P}'$.

De este modo, $\mathfrak{Q}_M \mathcal{O}_L = \mathfrak{P}^{e'}$ donde $e' := e_{\mathfrak{P}|\mathfrak{Q}_M}$ y $f' := f_{\mathfrak{P}|\mathfrak{Q}_M}$. Se afirma que $e = e'$ y $f = f'$ donde $e := e_{\mathfrak{P}|\mathfrak{p}}$ y $f := f_{\mathfrak{P}|\mathfrak{p}}$, y además, $\mathcal{O}_K/\mathfrak{p} = \mathcal{O}_M/\mathfrak{Q}_M$.

En efecto, puesto que $[L : M] = e'f'$ y $[L : M] = |\text{Gal}(L/M)| = |D_{\mathfrak{P}}|$, se tiene que $ef = e'f'$. Por otro lado

$$[\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}] = [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_M/\mathfrak{Q}_M][\mathcal{O}_M/\mathfrak{Q}_M : \mathcal{O}_K/\mathfrak{p}],$$

y por lo tanto $f \geq f'$.

Por otro lado, se tiene que $\mathfrak{p}\mathcal{O}_M \subseteq \mathfrak{Q}_M$, y así, $(\mathfrak{p}\mathcal{O}_M)\mathcal{O}_L \subseteq \mathfrak{Q}_M\mathcal{O}_L$. Ya que

$$(\mathfrak{p}\mathcal{O}_M)\mathcal{O}_L = \mathfrak{p}\mathcal{O}_L,$$

entonces $\mathfrak{p}\mathcal{O}_L \subseteq \mathfrak{P}^{e'}$. Es decir, $\mathfrak{P}^{e'}$ está en la factorización de $\mathfrak{p}\mathcal{O}_L$, por lo tanto $e \geq e'$. Esto permite concluir que $e = e'$ y $f = f'$. Además, esto implica que

$$[\mathcal{O}_M/\mathfrak{Q}_M : \mathcal{O}_K/\mathfrak{p}] = 1,$$

y así, $\mathcal{O}_K/\mathfrak{p} = \mathcal{O}_M/\mathfrak{Q}_M$.

Por otro lado, puesto que $\mathcal{O}_L/\mathfrak{P}$ es una extensión de $\mathcal{O}_K/\mathfrak{p}$, la proposición 1.2.2 implica que $\mathcal{O}_L/\mathfrak{P}$ es una extensión de Galois de $\mathcal{O}_K/\mathfrak{p}$.

El teorema del elemento primitivo implica que existe $\bar{\alpha} \in \mathcal{O}_L/\mathfrak{P}$ tal que

$$\mathcal{O}_L/\mathfrak{P} = (\mathcal{O}_K/\mathfrak{p})(\bar{\alpha}).$$

Puesto que $\alpha \in \mathcal{O}_L$ es algebraico sobre M , existe $h(x)$ el polinomio mínimo de α sobre M , y sean $\alpha_1 := \alpha, \dots, \alpha_r \in L$ las r raíces diferentes de $h(x)$ donde $r := \text{gr}(h(x))$.

Sea $w(x) \in \mathbb{Z}[x]$ un polinomio mónico tal que $w(\alpha) = 0$, y así $h(x)|w(x)$, y por lo tanto $\alpha_2, \dots, \alpha_r$ también son enteros algebraicos de L . Ahora, escribiendo $h(x)$ en su factorización se obtiene

$$h(x) = (x - \alpha_1) \cdots (x - \alpha_r) \in \mathcal{O}_L[x].$$

Y calculando los coeficientes de $h(x)$ a partir de esta factorización, se obtiene que cada coeficiente es un polinomio simétrico elemental de r variables evaluado en $\alpha_1, \dots, \alpha_r$. Esto implica que cada coeficiente de $h(x)$ es un entero algebraico de L , y puesto que $\mathcal{O}_M = \mathcal{O}_L \cap M$, se obtiene que $h(x) \in \mathcal{O}_M[x]$.

Si se reducen los coeficientes de $h(x)$ módulo \mathfrak{Q}_M , se tiene que

$$\bar{h}(x) \in \mathcal{O}_M/\mathfrak{Q}_M[x],$$

es decir

$$\bar{h}(x) \in \mathcal{O}_K/\mathfrak{p}[x].$$

Por otro lado, sea $\bar{z}(x) \in \mathcal{O}_K/\mathfrak{p}[x]$ el polinomio mínimo de $\bar{\alpha}$ sobre $\mathcal{O}_K/\mathfrak{p}$, y puesto que $h(\alpha) = 0$, se tiene que $\bar{h}(\bar{\alpha}) = 0$, esto implica que $\bar{z}(x) | \bar{h}(x)$.

Por último, sea $\phi \in \text{Gal}(\mathcal{O}_L/\mathfrak{P}/\mathcal{O}_K/\mathfrak{p})$, entonces $\phi(\bar{\alpha})$ también es raíz de $\bar{z}(x)$, y por lo tanto de $\bar{h}(x)$.

Así, existe $1 \leq i \leq r$ tal que

$$\bar{\alpha}_i = \phi(\bar{\alpha}).$$

Ya que α y α_i tienen el mismo polinomio sobre M , existe $\sigma \in \text{Gal}(L/M) = D_{\mathfrak{P}}$ tal que $\sigma(\alpha) = \alpha_i$, por lo tanto

$$\bar{\sigma}(\bar{\alpha}) = \overline{\sigma(\alpha)} = \bar{\alpha}_i = \phi(\bar{\alpha}),$$

puesto que $\bar{\alpha}$ es un elemento primitivo, se obtiene que $\bar{\sigma} = \phi$.

Esto implica que $f(\sigma) = \phi$, donde $\sigma \in D_{\mathfrak{P}}$. Esto es, f es sobreyectivo.

2. La proposición anterior probó que

$$|D_{\mathfrak{P}}| = ef,$$

donde $e := e_{\mathfrak{P}|\mathfrak{p}}$ y $f := f_{\mathfrak{P}|\mathfrak{p}}$.

Por (1) se obtiene que

$$|D_{\mathfrak{P}}/I_{\mathfrak{P}}| = |\text{Gal}(\mathcal{O}_L/\mathfrak{P}/\mathcal{O}_K/\mathfrak{p})|,$$

entonces

$$\frac{|D_{\mathfrak{P}}|}{|I_{\mathfrak{P}}|} = [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}],$$

de esto se concluye que $|I_{\mathfrak{P}}| = e$.

□

Corolario 2.4.1. Sean $K \subseteq L$ cuerpos numéricos tales que L es una extensión de Galois de K , sea \mathfrak{p} un ideal primo de \mathcal{O}_K .

Entonces \mathfrak{p} no ramifica en L si y solo si el grupo de inercia de cada ideal primo de \mathcal{O}_L que contiene a \mathfrak{p} es trivial.

Ahora, se introduce una herramienta muy importante en el estudio de la ley de reciprocidad de Artin, llamado el símbolo de Artin.

Lema 2.4.1. Sean $K \subseteq L$ cuerpos numéricos tales que L es una extensión de Galois de K , sea \mathfrak{p} un ideal primo de \mathcal{O}_K que no ramifica en L . Si \mathfrak{P} es un ideal primo de \mathcal{O}_L que contiene a \mathfrak{p} entonces existe un único $\sigma \in \text{Gal}(L/K)$ tal que

$$\sigma(x) \equiv x^{\|\mathfrak{p}\|} \pmod{\mathfrak{P}}, \text{ para todo } x \in \mathcal{O}_L$$

donde $\|\mathfrak{p}\| = |\mathcal{O}_K/\mathfrak{p}|$.

Demostración. Sea \mathfrak{P} un ideal primo de \mathcal{O}_L que contiene a \mathfrak{p} , ya que el ideal \mathfrak{p} no ramifica en L se tiene que el grupo de inercia $I_{\mathfrak{P}}$ de \mathfrak{P} es trivial, de modo que

$$D_{\mathfrak{P}} \cong \text{Gal}(\mathcal{O}_L/\mathfrak{P}/\mathcal{O}_K/\mathfrak{p})$$

mediante el isomorfismo que asigna $\sigma \mapsto \bar{\sigma}$.

Ahora, ya que $\mathcal{O}_L/\mathfrak{P}$ es una extensión de $\mathcal{O}_K/\mathfrak{p}$ donde ambos son cuerpos finitos, entonces la extensión es de Galois y por lo tanto $\text{Gal}(\mathcal{O}_L/\mathfrak{P}/\mathcal{O}_K/\mathfrak{p})$ es un grupo cíclico generado por una potencia del automorfismo de Frobenius, esta potencia es $[\mathcal{O}_K/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}]$, donde $p \in \mathbb{Z}$ es el único primo que está contenido en \mathfrak{p} , entonces

$$\begin{aligned} \gamma : \mathcal{O}_L/\mathfrak{P} &\rightarrow \mathcal{O}_L/\mathfrak{P} \\ \bar{x} &\mapsto \gamma(\bar{x}) := \bar{x}^p \end{aligned}$$

y así, si se denota por $m := [\mathcal{O}_K/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}]$, se obtiene que

$$\gamma^m(\bar{x}) = (\bar{x}^p)^m = \bar{x}^{\|\mathfrak{p}\|},$$

donde $\|\mathfrak{p}\| = |\mathcal{O}_K/\mathfrak{p}|$.

Luego, existe un único $\sigma \in D_{\mathfrak{P}}$ tal que $\bar{\sigma} = \gamma^m$, es decir, para todo $x \in \mathcal{O}_L$ se tiene que

$$\overline{\sigma(x)} = \gamma^m(\bar{x}),$$

esto implica que

$$\overline{\sigma(x)} = \bar{x}^{\|\mathfrak{p}\|} = \overline{x^{\|\mathfrak{p}\|}}$$

y por lo tanto $\sigma(x) - x^{\|\mathfrak{p}\|} \in \mathfrak{P}$, así, se concluye que

$$\sigma(x) \equiv x^{\|\mathfrak{p}\|} \pmod{\mathfrak{P}}$$

para todo $x \in \mathcal{O}_L$.

Falta ver que σ es único en $\text{Gal}(L/K)$: Sea $\phi \in \text{Gal}(L/K)$ tal que $\phi(x) \equiv x^{\|\mathfrak{p}\|} \pmod{\mathfrak{P}}$ para todo $x \in \mathcal{O}_L$.

Por otro lado, sea $\phi(x) \in \phi(\mathfrak{P})$, entonces

$$\phi(x) - x^{\|\mathfrak{p}\|} = q, \text{ donde } q \in \mathfrak{P},$$

por lo tanto $\phi(x) = x^{\|\mathfrak{p}\|} + q \in \mathfrak{P}$; de modo que $\sigma(\mathfrak{P}) \subseteq \mathfrak{P}$. Ya que $\phi(\mathfrak{P})$ es un ideal maximal de \mathcal{O}_L por ser un ideal primo de \mathcal{O}_L , se concluye que $\phi(\mathfrak{P}) = \mathfrak{P}$, y por lo tanto $\phi \in D_{\mathfrak{P}}$, luego, por la unicidad de σ en $D_{\mathfrak{P}}$ se concluye que $\sigma = \phi$. \square

El único elemento $\sigma \in \text{Gal}(L/K)$ del lema anterior es llamado símbolo de Artin, y se denota por

$$\sigma := \left(\frac{L/K}{\mathfrak{P}} \right)$$

ya que depende del ideal primo \mathfrak{P} .

Usando esta notación se tiene que

$$\left(\frac{L/K}{\mathfrak{P}}\right)(x) \equiv x^{\|\mathfrak{p}\|} \pmod{\mathfrak{P}}, \text{ para todo } x \in \mathcal{O}_L$$

donde $\mathfrak{p} = \mathcal{O}_K \cap \mathfrak{P}$.

Algunas propiedades del símbolo de Artin son estudiadas en las siguientes proposiciones.

Proposición 2.4.7. Sean $K \subseteq L$ cuerpos numéricos tales que L es una extensión de Galois de K , sean \mathfrak{p} un ideal primo de \mathcal{O}_K que no ramifica en L y \mathfrak{P} un ideal primo de \mathcal{O}_L que contiene a \mathfrak{p} .

1. Si $\psi \in \text{Gal}(L/K)$, entonces $\left(\frac{L/K}{\psi(\mathfrak{P})}\right) = \psi \left(\frac{L/K}{\mathfrak{P}}\right) \psi^{-1}$
2. El orden de $\left(\frac{L/K}{\mathfrak{P}}\right)$ es el grado inercial $f := f_{\mathfrak{P}|\mathfrak{p}}$.
3. El ideal \mathfrak{p} se descompone completamente en L si y solo si $\left(\frac{L/K}{\mathfrak{P}}\right) = i_{\text{Gal}(L/K)}$.

Demostración. 1. Ya que $\psi \in \text{Gal}(L/K)$, entonces $\psi^{-1}(\mathcal{O}_L) = \mathcal{O}_L$.

Sea $x \in \mathcal{O}_L$, y así $\psi^{-1}(x) \in \mathcal{O}_L$. Entonces

$$\left(\frac{L/K}{\mathfrak{P}}\right)(\psi^{-1}(x)) \equiv \psi^{-1}(x)^{\|\mathfrak{p}\|} \pmod{\mathfrak{P}},$$

es decir

$$\left(\frac{L/K}{\mathfrak{P}}\right)(\psi^{-1}(x)) - \psi^{-1}(x)^{\|\mathfrak{p}\|} \in \mathfrak{P}.$$

Aplicando ψ , se obtiene

$$\psi \left(\frac{L/K}{\mathfrak{P}}\right) \psi^{-1}(x) - x^{\|\mathfrak{p}\|} \in \psi(\mathfrak{P}),$$

y por lo tanto

$$\psi \left(\frac{L/K}{\mathfrak{P}}\right) \psi^{-1}(x) \equiv x^{\|\mathfrak{p}\|} \pmod{\psi(\mathfrak{P})}.$$

Por otro lado $\left(\frac{L/K}{\psi(\mathfrak{P})}\right)(x) \equiv x^{\|\mathfrak{p}\|} \pmod{\psi(\mathfrak{P})}$, por la unicidad del símbolo de Artin se concluye que

$$\psi \left(\frac{L/K}{\mathfrak{P}}\right) \psi^{-1} = \left(\frac{L/K}{\psi(\mathfrak{P})}\right).$$

2. Por hipótesis, el ideal \mathfrak{p} no ramifica en L , esto implica que $D_{\mathfrak{P}} \cong \text{Gal}(\mathcal{O}_L/\mathfrak{P}/\mathcal{O}_K/\mathfrak{p})$, además

$$|\text{Gal}(\mathcal{O}_L/\mathfrak{P}/\mathcal{O}_K/\mathfrak{p})| = f$$

donde $f = [\mathcal{O}_L/\mathfrak{P}/\mathcal{O}_K/\mathfrak{p}]$.

Puesto que $\left(\frac{L/K}{\mathfrak{P}}\right)$ es el generador del grupo cíclico $\text{Gal}(\mathcal{O}_L/\mathfrak{P}/\mathcal{O}_K/\mathfrak{p})$, se tiene que el orden de $\left(\frac{L/K}{\mathfrak{P}}\right)$ es f .

3. Supóngase que \mathfrak{p} se descompone completamente en L , entonces $e = 1 = f$, y así

$$|D_{\mathfrak{p}}| = ef = 1,$$

esto implica que $D_{\mathfrak{p}} = \{i_{Gal(L/K)}\}$, y por lo tanto $\left(\frac{L/K}{\mathfrak{p}}\right) = i_{Gal(L/K)}$.

Recíprocamente, supóngase que $\left(\frac{L/K}{\mathfrak{p}}\right) = i_{Gal(L/K)}$, por hipótesis \mathfrak{p} no ramifica en L , así $e = 1$.

Ya que el orden de $\left(\frac{L/K}{\mathfrak{p}}\right) = i_{Gal(L/K)}$ es 1, entonces $f = 1$, por lo tanto se concluye que \mathfrak{p} se descompone completamente en L . □

Proposición 2.4.8. Sean $K \subseteq L$ cuerpos numéricos tales que L es una extensión de Galois abeliana de K , sean \mathfrak{p} un ideal primo de \mathcal{O}_K que no ramifica en L y \mathfrak{P} un ideal primo de \mathcal{O}_L que contiene a \mathfrak{p} . Entonces el símbolo de Artin $\left(\frac{L/K}{\mathfrak{P}}\right)$ solo depende de \mathfrak{p} .

En este caso el símbolo de Artin se denota por $\left(\frac{L/K}{\mathfrak{p}}\right)$.

Demostración. Sea \mathfrak{P}' otro ideal primo de \mathcal{O}_L que contiene a \mathfrak{p} , como $Gal(L/K)$ actúa transitivamente existe $\psi \in Gal(L/K)$ tal que $\psi(\mathfrak{P}) = \mathfrak{P}'$, entonces

$$\begin{aligned} \left(\frac{L/K}{\mathfrak{P}'}\right) &= \left(\frac{L/K}{\psi(\mathfrak{P})}\right) \\ &= \psi \left(\frac{L/K}{\mathfrak{P}}\right) \psi^{-1} \\ &= \left(\frac{L/K}{\mathfrak{P}}\right) \end{aligned}$$

donde la última igualdad se tiene por ser $Gal(L/K)$ un grupo abeliano. □

Ahora, para ilustrar un ejemplo acerca del símbolo de Artin, primero se va a calcular el grupo de Galois de un polinomio.

Ejemplo 2.4.3. Sea $p(x) = x^3 - 2 \in \mathbb{Q}[x]$, si se definen

$$\theta := \sqrt[3]{2} \quad \text{y} \quad \alpha := \frac{-1 + \sqrt{-3}}{2}$$

entonces $p(x) = (x - \theta)(x - \theta\alpha)(x - \theta\alpha^2)$, luego, el cuerpo de descomposición de $p(x)$ es $\mathbb{Q}(\alpha, \theta)$. Ya que α es raíz del polinomio ciclotómico $f_3(x) = x^2 + x + 1 \in \mathbb{Q}[x]$, entonces $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$.

Puesto que el polinomio $p(x) = x^3 - 2 \in \mathbb{Q}[x]$ es irreducible y $\text{mcd}(2, 3) = 1$, entonces se tiene que $p(x) = x^3 - 2$ es irreducible sobre $\mathbb{Q}(\alpha)$, pero θ es una raíz de $p(x) = x^3 - 2 \in \mathbb{Q}(\alpha)$, de modo que $[\mathbb{Q}(\alpha, \theta) : \mathbb{Q}(\alpha)] = 3$.

Si se denotan $K = \mathbb{Q}(\sqrt{-3})$ y $L = K(\sqrt[3]{2})$, entonces $[L : K] = 3$, debido a que L es una extensión de Galois de K se tiene que $|Gal(L/K)| = 3$, y por lo tanto $Gal(L/K) \cong \mathbb{Z}/3\mathbb{Z}$.

Observación 2.4.2. Nótese que $K = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}\left(\frac{-1+\sqrt{-3}}{2}\right)$, así, para cada

$$\beta = a + b\frac{-1+\sqrt{-3}}{2} \in \mathbb{Q}\left(\frac{-1+\sqrt{-3}}{2}\right)$$

se tiene que

$$N_{\mathbb{Q}}^K(\beta) = \left(a + b\frac{-1+\sqrt{-3}}{2}\right) \left(a + b\frac{-1-\sqrt{-3}}{2}\right) = a^2 - ab + b^2.$$

Ya que $-3 \equiv 1 \pmod{4}$, se tiene que $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\omega$, donde $\omega = \frac{-1+\sqrt{-3}}{2}$.

En [11] se prueba que, dado π un elemento primo en \mathcal{O}_K tal que $N_{\mathbb{Q}}^K(\pi) \neq 3$, y dado $\gamma \in \mathcal{O}_K$ tal que $\pi \nmid \gamma$, entonces existe un único entero $m \in \{0, 1, 2\}$ tal que

$$\gamma^{(N_{\mathbb{Q}}^K(\pi)-1)/3} \equiv \omega^m \pmod{\pi}.$$

Este hecho permite definir el símbolo de Legendre cúbico como sigue.

Sean π un elemento primo en \mathcal{O}_K tal que $N_{\mathbb{Q}}^K(\pi) \neq 3$ y $\gamma \in \mathcal{O}_K$, el carácter cúbico de $\gamma \pmod{\pi}$ está dado por

1. $\left(\frac{\gamma}{\pi}\right)_3 = 0$ si $\pi \mid \gamma$.
2. $\gamma^{(N_{\mathbb{Q}}^K(\pi)-1)/3} \equiv \left(\frac{\gamma}{\pi}\right)_3 \pmod{\pi}$, donde $\left(\frac{\gamma}{\pi}\right)_3$ es igual a $1, \omega, \omega^2$.

En [11] se pueden consultar mas detalles acerca del símbolo de Legendre cúbico.

En el siguiente ejemplo, el símbolo de Artin generaliza el símbolo de Legendre cúbico.

Ejemplo 2.4.4. Sean $K = \mathbb{Q}(\sqrt{-3})$ y $L = K(\sqrt[3]{2})$, entonces $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\omega$, donde

$$\omega = \frac{-1+\sqrt{-3}}{2}.$$

Además, el anillo \mathcal{O}_K es un *DIP*, luego un ideal primo de \mathcal{O}_K es de la forma $\pi\mathcal{O}_K$, donde π es un elemento primo de \mathcal{O}_K .

Ahora, si $\pi \nmid 6$ se cumple que el polinomio $x^3 - 2$ es separable en $\mathcal{O}_K/\pi\mathcal{O}_K[x]$. En efecto, supóngase que $x^3 - 2$ no es separable en $\mathcal{O}_K/\pi\mathcal{O}_K$, luego existe α una raíz de multiplicidad mayor o igual que 2, y por lo tanto se tiene que α es raíz de la derivada $3x^2$ en $\mathcal{O}_K/\pi\mathcal{O}_K$, es decir $3\alpha^2 \in \pi\mathcal{O}_K$, puesto que $\pi\mathcal{O}_K$ es un ideal primo y $\pi \nmid 6$ se tiene que $\alpha^2 \in \pi\mathcal{O}_K$, de aquí se obtiene que $\alpha \in \pi\mathcal{O}_K$. Luego, $\alpha^3 \in \pi\mathcal{O}_K$, pero $\alpha^3 = 2$ en $\mathcal{O}_K/\pi\mathcal{O}_K$, esto implica que $2 \in \pi\mathcal{O}_K$ pero esta es una contradicción. De modo que el ideal primo $\pi\mathcal{O}_K$ no ramifica en L . El ejemplo anterior implica que

$$\text{Gal}(L/K) \cong \mathbb{Z}/3\mathbb{Z},$$

así, el grupo $Gal(L/K)$ es abeliano, por lo tanto el símbolo de Artin está definido.

Basta evaluar este automorfismo en $\sqrt[3]{2}$, sea \mathfrak{P} un ideal primo de \mathcal{O}_L que contiene a $\pi\mathcal{O}_K$, entonces

$$\begin{aligned} \left(\frac{L/K}{\pi\mathcal{O}_K}\right) (\sqrt[3]{2}) &\equiv \sqrt[3]{2}^{\|\pi\mathcal{O}_K\|} \pmod{\mathfrak{P}} \\ &\equiv 2^{\frac{\|\pi\mathcal{O}_K\|-1}{3}} \sqrt[3]{2} \pmod{\mathfrak{P}} \end{aligned}$$

Luego, $\|\pi\mathcal{O}_K\| = |N_{\mathbb{Q}}^K(\pi)|$, y por definición del símbolo cúbico de Legendre se tiene que

$$2^{\frac{|N_{\mathbb{Q}}^K(\pi)|-1}{3}} \equiv \left(\frac{2}{\pi}\right)_3 \pmod{\pi}.$$

Ya que $\pi \in \pi\mathcal{O}_K \subseteq \mathfrak{P}$, entonces

$$\left(\frac{L/K}{\pi\mathcal{O}_K}\right) (\sqrt[3]{2}) \equiv \left(\frac{2}{\pi}\right)_3 \sqrt[3]{2} \pmod{\mathfrak{P}}.$$

Por ultimo, note que $\left(\frac{L/K}{\pi\mathcal{O}_K}\right) (\sqrt[3]{2})$ es igual a $\sqrt[3]{2}$ veces una raíz cúbica de la unidad. En [11] se prueba que las raíces cúbicas de la unidad son diferentes en $\mathcal{O}_K/\pi\mathcal{O}_K$, esto implica que también lo son en $\mathcal{O}_L/\mathfrak{P}$, esto es consecuencia de que las raíces cúbicas de la unidad están en \mathcal{O}_K y $\mathfrak{P} \cap \mathcal{O}_K = \pi\mathcal{O}_K$. Así, se concluye que

$$\left(\frac{L/K}{\pi\mathcal{O}_K}\right) (\sqrt[3]{2}) = \left(\frac{2}{\pi}\right)_3 \sqrt[3]{2}.$$

De este modo, se dice que el símbolo de Artin generaliza el símbolo de Legendre cúbico.

2.5. LEY DE RECIPROCIDAD CUADRÁTICA

La ley de reciprocidad cuadrática ha sido de gran importancia en las matemáticas de los últimos 300 años, y en particular de la teoría de números. La ley de reciprocidad cuadrática fue formulada por Leonhard Euler en el año 1755, aunque la primera prueba fue dada por Gauss en el año 1796, quien realizó 7 pruebas mas de este teorema usando diferentes herramientas de teoría de números. Después Legendre es quien enuncia la ley de reciprocidad cuadrática usando el símbolo de Legendre, y de esta manera es como se enuncia este teorema en la actualidad.

Definición 2.5.1. Sean $a \in \mathbb{Z}$ y $p \in \mathbb{Z}$ un primo tales que $p \nmid a$.

Si la congruencia $x^2 \equiv a \pmod{p}$ tiene solución, se dice que a es un residuo cuadrático módulo p . En caso contrario se dice que a es un no residuo cuadrático módulo p .

En [11] se prueban algunas propiedades básicas del símbolo cuadrático de Legendre, estas son.

Dados $a, b \in \mathbb{Z}$ y $p \in \mathbb{Z}$ un primo impar tales que $a \not\equiv 0 \pmod{p}$ y $b \not\equiv 0 \pmod{p}$, entonces.

1. Si $a \equiv b \pmod{p}$, entonces $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
2. $\left(\frac{a^2}{p}\right) = 1$.
3. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.
4. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$.
5. Hay tantos residuos cuadráticos como no residuos cuadráticos módulo p , es decir, existen $\frac{p-1}{2}$ residuos cuadráticos módulo p y $\frac{p-1}{2}$ no residuos cuadráticos módulo p .

Corolario 2.5.1. Sea $p \in \mathbb{Z}$ un primo impar, entonces $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Demostración. De la propiedad anterior se tiene que

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p},$$

al ser p impar, entonces $1 \not\equiv -1 \pmod{p}$, y así se obtiene la igualdad. □

Sea \mathbb{A} el anillo de enteros algebraicos de \mathbb{C} , y sean $\omega_1, \omega_2, \gamma \in \mathbb{A}$.

Se dice que $\omega_1 \equiv \omega_2 \pmod{\gamma}$ si y solo si existe $\alpha \in \mathbb{A}$ tal que $\omega_1 - \omega_2 = \gamma\alpha$.

Con esta definición se obtiene un análogo al automorfismo de Frobenius en \mathbb{C} .

Lema 2.5.1. Sean $\omega_1, \omega_2 \in \mathbb{A}$ y $p \in \mathbb{Z}$ un primo, entonces

$$(\omega_1 + \omega_2)^p \equiv \omega_1^p + \omega_2^p \pmod{p}.$$

Demostración. Es consecuencia del hecho que $p \mid \binom{p}{k}$ para todo $1 \leq k \leq p-1$. □

2.5.1. EL CARÁCTER CUADRÁTICO DE 2

El objetivo es describir $\left(\frac{2}{p}\right)$ mediante las condiciones sobre p .

Teorema 2.5.1. Sea $p \in \mathbb{Z}$ un primo impar, entonces

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

Demostración. Sea $\zeta_8 = e^{\frac{2\pi i}{8}}$ una raíz primitiva 8-ésima de la unidad, es decir

$$\zeta_8^8 - 1 = 0 = (\zeta_8^4 - 1)(\zeta_8^4 + 1).$$

Puesto que el orden de ζ_8 es 8, entonces $\zeta_8^4 = -1$, y así $\zeta_8^2 + \zeta_8^{-2} = 0$. Luego $(\zeta_8 + \zeta_8^{-1})^2 = 2$.

Defínase $\tau := \zeta_8 + \zeta_8^{-1}$, entonces

$$\tau^{p-1} = (\tau^2)^{\frac{p-1}{2}} = 2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \pmod{p}.$$

Entonces $\tau^p \equiv \left(\frac{2}{p}\right) \tau \pmod{p}$, el lema anterior implica que

$$\tau^p = (\zeta_8 + \zeta_8^{-1})^p \equiv \zeta_8^p + \zeta_8^{-p} \pmod{p},$$

de modo que

$$\zeta_8^p + \zeta_8^{-p} \equiv \left(\frac{2}{p}\right) \tau \pmod{p}.$$

Por otro lado se tiene que

$$\zeta_8^p + \zeta_8^{-p} = \begin{cases} \tau & \text{si } p \equiv \pm 1 \pmod{8} \\ -\tau & \text{si } p \equiv \pm 3 \pmod{8} \end{cases}$$

Además, se puede observar que de las condiciones sobre p se obtiene la paridad de $\frac{p^2-1}{8}$, es decir

$$\frac{p^2-1}{8} \equiv 0 \pmod{2} \text{ si y solo si } p \equiv \pm 1 \pmod{8},$$

$$\frac{p^2-1}{8} \equiv 1 \pmod{2} \text{ si y solo si } p \equiv \pm 3 \pmod{8}.$$

Esto implica que

$$\zeta_8^p + \zeta_8^{-p} = (-1)^{\frac{p^2-1}{8}} \tau.$$

Reemplazando se obtiene

$$(-1)^{\frac{p^2-1}{8}} \tau \equiv \left(\frac{2}{p}\right) \tau \pmod{p},$$

y así

$$(-1)^{\frac{p^2-1}{8}} 2 \equiv \left(\frac{2}{p}\right) 2 \pmod{p},$$

y ya que $(2, p) = 1$, entonces

$$(-1)^{\frac{p^2-1}{8}} \equiv \left(\frac{2}{p}\right) \pmod{p}.$$

Luego, se concluye que $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. □

2.5.2. PRUEBA DE LA LEY DE RECIPROCIDAD CUADRÁTICA

Debido a la importancia de la ley de reciprocidad cuadrática, varios matemáticos se han dedicado a encontrar diferentes pruebas de este teorema. En [16], Lemmermeyer cita 196 demostraciones diferentes de la ley de reciprocidad cuadrática.

En esta sección se presenta una prueba de la ley de reciprocidad cuadrática, esta prueba no es elemental, pero en ella se hace uso de una parte fundamental de la teoría que se ha desarrollado hasta el momento, por esta razón se presenta esta prueba. Esta prueba se basa en las referencias [23] y [5].

Sean $p \in \mathbb{Z}$ un primo impar y $L := \mathbb{Q}(\zeta_p)$ un cuerpo ciclotómico. Puesto que

$$\text{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^*,$$

se tiene que $\text{Gal}(L/\mathbb{Q})$ es un grupo cíclico de orden $p - 1$. Ya que $p - 1 = 2j$ para algún $j \in \mathbb{Z}^+$, existe un único subgrupo H de $\text{Gal}(L/\mathbb{Q})$ tal que $|H| = j$, y si $\text{Gal}(L/\mathbb{Q}) = \langle \sigma \rangle$, entonces $H = \langle \sigma^2 \rangle$, además

$$|\text{Gal}(L/\mathbb{Q}) : H| = \frac{|\text{Gal}(L/\mathbb{Q})|}{|H|} = \frac{p-1}{j} = 2,$$

es decir que existe un único subgrupo H de $\text{Gal}(L/\mathbb{Q})$ de índice 2, dicho subgrupo H bajo el isomorfismo anterior corresponde a los residuos cuadráticos módulo p .

Ahora, sea K el cuerpo fijo de H , es decir que $\mathbb{Q} \subseteq K \subseteq L$, además

$$[K : \mathbb{Q}] = \frac{|\text{Gal}(L/\mathbb{Q})|}{|\text{Gal}(L/K)|} = \frac{p-1}{|H|} = \frac{p-1}{j} = 2,$$

por lo tanto K es un cuerpo cuadrático.

Puesto que p es el único primo que ramifica en L y

$$p\mathcal{O}_L = [(1 - \zeta_p)\mathcal{O}_L]^{p-1},$$

donde $(1 - \zeta_p)\mathcal{O}_L$ es un ideal primo de \mathcal{O}_L , entonces p es el único primo que ramifica en K : En efecto, supóngase que p no ramifica en K , así, se tienen dos casos.

1. Si $p\mathcal{O}_K = \mathfrak{Q}_1\mathfrak{Q}_2$ donde $\mathfrak{Q}_1, \mathfrak{Q}_2$ son ideales primos diferentes de \mathcal{O}_K , pero

$$\mathfrak{Q}_1\mathcal{O}_L = \mathfrak{P}^{e_1} \quad y \quad \mathfrak{Q}_2\mathcal{O}_L = \mathfrak{P}^{e_2}$$

donde $\mathfrak{P} := (1 - \zeta_p)\mathcal{O}_L$.

La proposición 2.1.1 implica que $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{Q}_1$ y $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{Q}_2$, por lo tanto $\mathfrak{Q}_1 = \mathfrak{Q}_2$.

2. Si $p\mathcal{O}_K = \mathfrak{Q}$ donde \mathfrak{Q} es un ideal primo de \mathcal{O}_K , pero $\mathfrak{Q}\mathcal{O}_L = \mathfrak{P}^e$, así

$$p\mathcal{O}_L = (p\mathcal{O}_K)\mathcal{O}_L = \mathfrak{Q}\mathcal{O}_L = \mathfrak{P}^e.$$

De esto se obtiene que $e = p - 1$, y puesto que $[L : K] = \frac{p-1}{2} = j$, entonces

$$j = ef = (p - 1)f \geq p - 1.$$

Por lo tanto, ninguno de estos dos casos se pueden dar, es decir que p ramifica en K . Ahora, supóngase que $q \in \mathbb{Z}$ es otro primo que ramifica en K , entonces $q\mathcal{O}_K = \mathfrak{Q}^2$ donde \mathfrak{Q} es un ideal primo de \mathcal{O}_K . Y sea $\mathfrak{Q}\mathcal{O}_L = \mathfrak{R}_1^{e'} \cdots \mathfrak{R}_g^{e'}$ la factorización de \mathfrak{Q} en ideales primos de \mathcal{O}_L . Entonces

$$q\mathcal{O}_L = (q\mathcal{O}_K)\mathcal{O}_L = (\mathfrak{Q}\mathcal{O}_L)^2 = \mathfrak{R}_1^{2e'} \cdots \mathfrak{R}_g^{2e'},$$

y como $2e' \geq 2$, entonces q ramifica en L , esto implica que $p = q$.

Lo anterior implica que $K = \mathbb{Q}(\sqrt{p})$ si $p \equiv 1 \pmod{4}$, y $K = \mathbb{Q}(\sqrt{-p})$ si $p \equiv 3 \pmod{4}$: En efecto, como p es el único primo que ramifica en K entonces p es el único primo que divide a $\text{disc}(K)$. De modo que $\text{disc}(K) = \pm p$, pero esto solamente se tiene si $K = \mathbb{Q}(\sqrt{\pm p})$ y $\pm p \equiv 1 \pmod{4}$.

- i) Supóngase que $p \equiv 1 \pmod{4}$ y $K = \mathbb{Q}(\sqrt{-p})$, entonces $-p \equiv 3 \pmod{4}$, de lo que se obtiene que $\text{disc}(K) = -4p$, pero esto es falso. Por lo tanto, si $p \equiv 1 \pmod{4}$ se tiene que $K = \mathbb{Q}(\sqrt{p})$.
- ii) Supóngase que $p \equiv 3 \pmod{4}$ y $K = \mathbb{Q}(\sqrt{p})$, entonces $\text{disc}(K) = 4p$, pero esto es falso. Por lo tanto, si $p \equiv 3 \pmod{4}$ se tiene que $K = \mathbb{Q}(\sqrt{-p})$.

Esto se puede escribir de manera compacta como $K = \mathbb{Q}(\sqrt{p^*})$ donde $p^* = (-1)^{\frac{p-1}{2}} p$.

Lema 2.5.2. Sean $p, q \in \mathbb{Z}$ primos impares distintos y $L := \mathbb{Q}(\zeta_p)$ un cuerpo ciclotómico. Sea $K := \mathbb{Q}(\sqrt{p^*})$ donde $p^* = (-1)^{\frac{p-1}{2}} p$, el único cuerpo cuadrático contenido en L . Los siguientes enunciados son equivalentes.

1. El primo $q \in \mathbb{Z}$ se descompone en K .
2. $\left(\frac{p^*}{q}\right) = 1$.
3. El símbolo de Artin $\left(\frac{L/\mathbb{Q}}{q}\right) \in \text{Gal}(L/\mathbb{Q})$ fija a K .

Demostración. Por el teorema 2.2.1 se tiene que q se descompone en K si y solo si $\left(\frac{p^*}{q}\right) = 1$.

Sea \mathfrak{P} un ideal primo de \mathcal{O}_L que contiene a q , entonces existe un único

$$\left(\frac{L/\mathbb{Q}}{q}\right) \in \text{Gal}(L/\mathbb{Q})$$

tal que

$$\left(\frac{L/\mathbb{Q}}{q}\right)(\alpha) \equiv \alpha^q \pmod{\mathfrak{P}} \text{ para todo } \alpha \in \mathcal{O}_L.$$

Sea $\mathfrak{Q} := \mathfrak{P} \cap \mathcal{O}_K$ un ideal primo de \mathcal{O}_K que contiene a q , y sea $k \in \mathcal{O}_K$, entonces

$$\left(\frac{L/\mathbb{Q}}{q}\right)(k) \equiv k^q \pmod{\mathfrak{P}},$$

de modo que

$$\left(\frac{L/\mathbb{Q}}{q}\right)(k) - k^q \in \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{Q},$$

es decir

$$\left(\frac{L/\mathbb{Q}}{q}\right)(k) \equiv k^q \pmod{\mathfrak{Q}} \text{ para todo } k \in \mathcal{O}_K.$$

Por otro lado, se tiene que existe un único $\left(\frac{K/\mathbb{Q}}{q}\right) \in \text{Gal}(K/\mathbb{Q})$ tal que

$$\left(\frac{K/\mathbb{Q}}{q}\right)(k) \equiv k^q \pmod{\mathfrak{Q}} \text{ para todo } k \in \mathcal{O}_K,$$

de modo que por la unicidad del símbolo de Artin se tiene que la restricción de $\left(\frac{L/\mathbb{Q}}{q}\right)$ a $\text{Gal}(K/\mathbb{Q})$ es igual a $\left(\frac{K/\mathbb{Q}}{q}\right)$.

Luego, por la proposición 2.4.7 se tiene que

$$\begin{aligned} q \text{ se descompone en } K &\Leftrightarrow \left(\frac{K/\mathbb{Q}}{q}\right) = i_{\text{Gal}(K/\mathbb{Q})} \\ &\Leftrightarrow \left(\frac{L/\mathbb{Q}}{q}\right) \text{ fija a } K. \end{aligned}$$

□

Lema 2.5.3. Sean $p, q \in \mathbb{Z}$ primos impares distintos y $L := \mathbb{Q}(\zeta_p)$ un cuerpo ciclotómico. Y sea $K := \mathbb{Q}(\sqrt{p^*})$ donde $p^* = (-1)^{\frac{p-1}{2}} p$, el único cuerpo cuadrático contenido en L . Entonces el símbolo de Artin $\left(\frac{L/\mathbb{Q}}{q}\right)$ fija a K si y solo si $\left(\frac{q}{p}\right) = 1$.

Demostración. Recuérdese que

$$\text{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^*,$$

donde $\sigma \in \text{Gal}(L/\mathbb{Q})$ se identifica con $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^*$ que satisface $\sigma(\zeta_p) = \zeta_p^a$.
 Sea \mathfrak{P} un ideal primo de \mathcal{O}_L que contiene a q , entonces existe un único $\left(\frac{L/\mathbb{Q}}{q}\right) \in \text{Gal}(L/\mathbb{Q})$
 tal que

$$\left(\frac{L/\mathbb{Q}}{q}\right)(\alpha) \equiv \alpha^q \pmod{\mathfrak{P}} \text{ para todo } \alpha \in \mathcal{O}_L.$$

Luego

$$\left(\frac{L/\mathbb{Q}}{q}\right)(\zeta_p) \equiv \zeta_p^q \pmod{\mathfrak{P}},$$

además, se tiene $\bar{q} \in (\mathbb{Z}/p\mathbb{Z})^*$ se identifica con $\varphi \in \text{Gal}(L/\mathbb{Q})$ tal que $\varphi(\zeta_p) = \zeta_p^{\bar{q}}$.
 Puesto que $\zeta_p, \dots, \zeta_p^{p-1}$ son diferentes módulo \mathfrak{P} , entonces

$$\left(\frac{L/\mathbb{Q}}{q}\right)(\zeta_p) = \zeta_p^{\bar{q}},$$

por lo tanto

$$\left(\frac{L/\mathbb{Q}}{q}\right) = \varphi.$$

Así, si $H = \text{Gal}(L/K)$ es el único subgrupo de $\text{Gal}(L/\mathbb{Q})$ de índice 2, entonces

$$\begin{aligned} \left(\frac{L/\mathbb{Q}}{q}\right) \text{ fija a } K &\Leftrightarrow \varphi \in \text{Gal}(L/K) = H \\ &\Leftrightarrow \bar{q} \text{ es un residuo cuadrático } \pmod{p} \\ &\Leftrightarrow \left(\frac{q}{p}\right) = 1. \end{aligned}$$

□

Con ayuda de estos lemas se obtiene una prueba de la ley de reciprocidad cuadrática diferente a las clásicas.

Teorema 2.5.2 (Ley de Reciprocidad Cuadrática). *Sean p y q primos impares diferentes. Entonces*

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

Demostración. Sean $L := \mathbb{Q}(\zeta_p)$ un cuerpo ciclotómico y $K := \mathbb{Q}(\sqrt{p^*})$ el único cuerpo cuadrático contenido en L donde $p^* = (-1)^{\frac{p-1}{2}} p$.

Puesto que $p \neq q$, entonces q no ramifica en K , y así q se descompone o es inerte en K , luego, los lemas anteriores implican que

$$\left(\frac{p^*}{q}\right) = 1 \iff \left(\frac{q}{p}\right) = 1.$$

De aquí, se obtiene

$$\begin{aligned}
 \left(\frac{q}{p}\right) &= \left(\frac{p^*}{q}\right) \\
 &= \left(\frac{(-1)^{\frac{p-1}{2}} p}{q}\right) \\
 &= \left(\frac{-1}{q}\right)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \\
 &= (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{p}{q}\right).
 \end{aligned}$$

Esto concluye la demostración de la ley de reciprocidad cuadrática. \square

2.6. EL CUERPO DE CLASES DE HILBERT Y EL HOMOMORFISMO DE ARTIN

La teoría del cuerpo de clases es una parte fundamental de la teoría algebraica de números, que tiene por estudio la clasificación de las extensiones abelianas de Galois de un cuerpo numérico dado.

Históricamente, en 1829 el matemático noruego Niels Henrik Abel realiza una primera clasificación de las extensiones abelianas del cuerpo $\mathbb{Q}(i)$. Luego, en el año 1853, Kronecker enuncia el teorema de Kronecker-Weber, dicho teorema establece que las extensiones finitas y abelianas de \mathbb{Q} son un subcuerpo de algún cuerpo ciclotómico, es decir, de algún cuerpo de la forma $\mathbb{Q}(\zeta)$ donde ζ es una raíz de la unidad.

Aparte de este teorema, y con ayuda de las ideas planteadas anteriormente por Abel, Kronecker halla la forma de las extensiones finitas abelianas para cualquier cuerpo cuadrático imaginario. Después, en el año 1896, David Hilbert realiza una prueba completa del teorema de Kronecker-Weber, dando paso a su conjetura sobre la existencia y algunas propiedades del llamado cuerpo de clases de Hilbert, la prueba de esta conjetura fue dada en 1907 por el matemático alemán Philipp Furtwängler.

Definición 2.6.1. Considérese $K \subseteq L$ una extensión de Galois abeliana y no ramificada, entonces ya se probó que para cada \mathfrak{p} ideal primo de \mathcal{O}_K está definido el símbolo de Artin

$$\left(\frac{L/K}{\mathfrak{p}}\right).$$

Este símbolo se puede extender de la siguiente manera, sea I_K el conjunto de todos los ideales fraccionarios de K , ya que todo ideal fraccionario de K se puede factorizar de forma única

como producto de ideales primos de \mathcal{O}_K , sea $\mathfrak{b} \in I_K$, entonces

$$\mathfrak{b} = \prod_{i=1}^t \mathfrak{p}_i^{r_i}$$

donde para cada $1 \leq i \leq t$, se tiene que $r_i \in \mathbb{Z}$ y \mathfrak{p}_i es un ideal primo de \mathcal{O}_K , luego se define

$$\begin{aligned} \left(\frac{L/K}{\cdot} \right) : I_K &\rightarrow \text{Gal}(L/K) \\ \mathfrak{b} &\mapsto \left(\frac{L/K}{\mathfrak{b}} \right) := \prod_{i=1}^t \left(\frac{L/K}{\mathfrak{p}_i} \right)^{r_i} \end{aligned}$$

llamado el Homomorfismo de Artin.

El siguiente lema muestra una propiedad importante del homomorfismo de Artin con las extensiones intermedias.

Lema 2.6.1. Sean $K \subseteq M \subseteq L$ cuerpos numéricos tales que L es una extensión de Galois abeliana y no ramificada de K . Y supóngase que M es una extensión normal de K , entonces M es una extensión de Galois abeliana no ramificada de K .

Sean

$$\begin{aligned} \left(\frac{L/K}{\cdot} \right) : I_K &\longrightarrow \text{Gal}(L/K), \\ \left(\frac{M/K}{\cdot} \right) : I_K &\longrightarrow \text{Gal}(M/K) \end{aligned}$$

los respectivos homomorfismos de Artin, y sea

$$r : \text{Gal}(L/K) \longrightarrow \text{Gal}(M/K)$$

el homomorfismo restricción, definido para cada $\sigma \in \text{Gal}(L/M)$ como $r(\sigma)(x) := \sigma(x)$ para todo $x \in M$. Entonces

$$\left(\frac{M/K}{\cdot} \right) = r \circ \left(\frac{L/K}{\cdot} \right).$$

Demostración. Por la definición del homomorfismo de Artin, basta probar la igualdad para un ideal primo de \mathcal{O}_K . Sean \mathfrak{p} un ideal primo de \mathcal{O}_K y \mathfrak{P} un ideal primo de \mathcal{O}_L que contiene a \mathfrak{p} , entonces existe un único $\left(\frac{L/K}{\mathfrak{p}} \right) \in \text{Gal}(L/K)$ tal que

$$\left(\frac{L/K}{\mathfrak{p}} \right) (x) \equiv x^{|\mathfrak{p}|} \pmod{\mathfrak{P}}$$

para todo $x \in \mathcal{O}_L$. En particular, para cada $y \in \mathcal{O}_M$ se tiene que

$$\left(\frac{L/K}{\mathfrak{p}} \right) (y) \equiv y^{|\mathfrak{p}|} \pmod{\mathfrak{P} \cap \mathcal{O}_M}.$$

Luego, sea $\mathfrak{Q} := \mathfrak{P} \cap \mathcal{O}_M$ un ideal primo de \mathcal{O}_M que contiene a \mathfrak{p} , entonces

$$\left(\frac{M/K}{\mathfrak{p}} \right) (y) \equiv y^{\|\mathfrak{p}\|} \pmod{\mathfrak{Q}}$$

para cada $y \in \mathcal{O}_M$. Por último, nótese que

$$r \circ \left(\frac{L/K}{\mathfrak{p}} \right) (y) = \left(\frac{L/K}{\mathfrak{p}} \right) (y)$$

para todo $y \in M$.

Por la unicidad del símbolo de Artin se obtiene que

$$\left(\frac{M/K}{\cdot} \right) = r \circ \left(\frac{L/K}{\cdot} \right).$$

□

Teorema 2.6.1 (El cuerpo de Clases de Hilbert). *Dado K un cuerpo numérico, existe L una extensión de Galois de K , tal que*

1. L es un extensión abeliana y no ramificada de K .
2. Cualquier otra extensión abeliana y no ramificada de K está contenida en L .

El cuerpo L es llamado el cuerpo de clases de Hilbert, esta es la extensión maximal de K que es de Galois, abeliana y no ramificada.

El siguiente teorema es conocido como "La Ley de Reciprocidad de Artin para el cuerpo de clases de Hilbert", que relaciona el grupo de clases de ideales $C(\mathcal{O}_K)$ con el cuerpo de clases de Hilbert mediante el grupo de Galois.

Teorema 2.6.2. *Sea K un cuerpo numérico y L el cuerpo de clases de Hilbert de K , entonces el homomorfismo de Artin*

$$\left(\frac{L/K}{\cdot} \right) : I_K \longrightarrow Gal(L/K)$$

definido como antes, es sobreyectivo, además, el kernel es exactamente el subgrupo P_K de ideales fraccionarios principales de K .

Así, se induce el isomorfismo

$$C(\mathcal{O}_K) \cong Gal(L/K).$$

La aparición del grupo de clases de ideales $C(\mathcal{O}_K)$ en relación con L mediante el teorema anterior explica de cierta manera por qué L es llamado el cuerpo de clases.

Este teorema fue probado inicialmente por Kronecker, aunque este no tenía idea de que tal teorema era un caso particular del teorema que tiempo después enunció Artin como la

ley de reciprocidad de Artin.

Si se considera el cuerpo de clases de Hilbert de un cuerpo numérico K , el siguiente corolario relaciona la ramificación de un ideal primo de \mathcal{O}_K con el grupo de clases de ideales.

Corolario 2.6.1. *Sea L el cuerpo de clases de Hilbert de un cuerpo numérico K , y sea \mathfrak{p} un ideal primo de \mathcal{O}_K . Entonces \mathfrak{p} se descompone completamente en L si y solo si \mathfrak{p} es un ideal principal.*

Demostración. Por ser L el cuerpo de clases de Hilbert de K , el símbolo de Artin $\left(\frac{L/K}{\mathfrak{p}}\right)$ está bien definido.

Luego, por proposición anterior se tiene \mathfrak{p} se descompone completamente en L si y solo si

$$\left(\frac{L/K}{\mathfrak{p}}\right) = i_{Gal(L/K)}.$$

La ley de reciprocidad de Artin para el cuerpo de clases de Hilbert induce el isomorfismo

$$C(\mathcal{O}_K) \cong Gal(L/K),$$

donde este isomorfismo está dado por

$$\overline{\left(\frac{L/K}{\cdot}\right)}(\mathfrak{b}P_K) := \left(\frac{L/K}{\mathfrak{b}}\right),$$

para cada $\mathfrak{b}P_K \in C(\mathcal{O}_K)$.

Así, $\left(\frac{L/K}{\mathfrak{p}}\right) = i_{Gal(L/K)}$ si y solo si la clase lateral de \mathfrak{p} en $C(\mathcal{O}_K)$ es trivial, esto es equivalente a que \mathfrak{p} es un ideal principal de \mathcal{O}_K . \square

Corolario 2.6.2. *Sea K un cuerpo numérico, existe una correspondencia uno a uno entre las extensiones abelianas no ramificadas M de K y los subgrupos H del grupo de clases de ideales $C(\mathcal{O}_K)$.*

Por lo tanto, si la extensión $K \subseteq M$ corresponde al subgrupo $H \subseteq C(\mathcal{O}_K)$, entonces el homomorfismo de Artin induce un isomorfismo

$$C(\mathcal{O}_K)/H \cong Gal(M/K).$$

Demostración. Sea L el cuerpo de clases de Hilbert de K y sea M una extensión abeliana y no ramificada de K , entonces $K \subseteq M \subseteq L$, y así $Gal(L/M)$ es un subgrupo de $Gal(L/K)$. La ley de reciprocidad de Artin para el cuerpo de clases de Hilbert induce el isomorfismo

$$C(\mathcal{O}_K) \cong Gal(L/K)$$

que está dado por $\overline{\left(\frac{L/K}{\cdot}\right)}$.

Sean

$$\mathcal{S} := \{M : M \text{ es una extensión abeliana y no ramificada de } K\}$$

y

$$\mathcal{T} := \{H : H \text{ es un subgrupo de } C(\mathcal{O}_K)\}.$$

Defínase

$$\begin{aligned} \varphi : \mathcal{S} &\rightarrow \mathcal{T} \\ M &\mapsto \varphi(M) := H \end{aligned}$$

donde H es el único subgrupo de $C(\mathcal{O}_K)$ tal que $\overline{\left(\frac{L/K}{\cdot}\right)}(H) = Gal(L/M)$. La función φ está bien definida por la unicidad del subgrupo H .

Por otro lado, dado H un subgrupo de $C(\mathcal{O}_K)$ se tiene que $\overline{\left(\frac{L/K}{\cdot}\right)}(H) := J$ es un subgrupo de $Gal(L/K)$. Por teoría de Galois se tiene que el cuerpo fijo L^J de J satisface $K \subseteq L^J \subseteq L$, el lema 2.1.1 implica que L^J es una extensión no ramificada de K , y además es una extensión abeliana de K pues $Gal(L/L^J)$ es un subgrupo de $Gal(L/K)$, por lo tanto $L^J \in \mathcal{S}$. Defínase

$$\begin{aligned} \phi : \mathcal{T} &\rightarrow \mathcal{S} \\ H &\mapsto \phi(H) := L^J \end{aligned}$$

donde H satisface $\overline{\left(\frac{L/K}{\cdot}\right)}(H) := J$.

La función ϕ está bien definida ya que el subgrupo J es único y la correspondencia del teorema fundamental de Galois es uno a uno.

Ahora, sea H un subgrupo de $C(\mathcal{O}_K)$, entonces

$$(\varphi \circ \phi)(H) = \varphi(\phi(H)) = \varphi(L^J) = H,$$

donde la última igualdad se tiene ya que $\overline{\left(\frac{L/K}{\cdot}\right)}(H) := J$.

Sea M una extensión abeliana y no ramificada de K , entonces

$$(\phi \circ \varphi)(M) = \phi(\varphi(M)) = \phi(H) = L^J = M,$$

donde estas igualdades se tienen debido a que $\overline{\left(\frac{L/K}{\cdot}\right)}(H) = Gal(L/M) := J$.

Lo anterior implica que la correspondencia entre \mathcal{S} y \mathcal{T} es uno a uno.

Para la última afirmación, si la extensión $K \subseteq M$ está en correspondencia con el subgrupo H de $C(\mathcal{O}_K)$ entonces se satisface que

$$\overline{\left(\frac{L/K}{\cdot}\right)}(H) = Gal(L/M).$$

Considérese el homomorfismo restricción

$$r : Gal(L/K) \rightarrow Gal(M/K)$$

definido para cada $\sigma \in Gal(L/K)$ como $r(\sigma)(m) = \sigma(m)$ para todo $m \in M$. Además se tiene que $Ker(r) = Gal(L/M)$.

Defínase

$$\psi := r \circ \overline{\left(\frac{L/K}{\cdot}\right)} : C(\mathcal{O}_K) \rightarrow Gal(M/K).$$

Así definido, ψ es un homomorfismo de grupos tal que $Ker(\psi) = H$, puesto que

$$Ker(\psi) = \overline{\left(\frac{L/K}{\cdot}\right)}^{-1} (ker(r)) = \overline{\left(\frac{L/K}{\cdot}\right)}^{-1} (Gal(L/M)) = H.$$

Esto implica que

$$C(\mathcal{O}_K)/H \cong Im(\psi).$$

Ya que

$$\begin{aligned} |Im(\psi)| &= \frac{|C(\mathcal{O}_K)|}{|H|} \\ &= \frac{|Gal(L/K)|}{|Gal(L/M)|} \\ &= \frac{[L : K]}{[L : M]} \\ &= [M : K] \\ &= |Gal(M/K)|. \end{aligned}$$

Y así $Im(\psi) = Gal(M/K)$, esto concluye que

$$C(\mathcal{O}_K)/H \cong Gal(M/K).$$

□

El corolario anterior clasifica las extensiones abelianas y no ramificadas de un cuerpo numérico en términos de los subgrupos del grupo de clases de ideales, este hecho es importante en la teoría del cuerpo de clases.

CAPÍTULO 3

TEORÍA DEL CUERPO DE CLASES

En este capítulo se introduce el concepto de divisor primo finito e infinito, y con ello, se define un módulo en un cuerpo numérico. Este concepto es fundamental para generalizar el símbolo y el homomorfismo de Artin. El teorema más importante de este capítulo es el Teorema de Artin, de este se deduce la ley de reciprocidad cuadrática, cúbica, y de orden superior.

3.1. UN POCO DE HISTORIA

La geometría algebraica moderna nace con la aparición de Riemann, quien tenía como objetivo el estudio de las integrales abelianas que fueron introducidas por Abel en 1841. Riemann aborda el problema de una manera diferente, su genialidad se basa en el concepto de superficie de Riemann y en el estudio de las funciones algebraicas, gran parte de los resultados obtenidos por Riemann tienen un enfoque analítico y geométrico.

Después de la muerte de Riemann, en 1882 surge una escuela encargada de estudiar los documentos de Riemann desde un enfoque algebraico, por un lado Kronecker y por otro lado Dedekind y Weber. Dedekind y Weber tenían como objetivo obtener los resultados de Riemann solamente mediante álgebra, aunque varios matemáticos de la época no entendían muy bien ese enfoque ya que el álgebra aún se estaba estudiando.

Puesto que la definición de una superficie de Riemann tiene ideas topológicas y analíticas, Dedekind y Weber querían dar una definición netamente algebraica. De este modo, consideran el cuerpo de funciones racionales de una variable sobre \mathbb{C} y sus extensiones algebraicas de grado finito, y definen ciertas funciones desde este cuerpo a los números enteros, estas funciones poseen las propiedades que ahora caracterizan a una valuación.

Una valuación es una función v desde un cuerpo K al anillo de enteros tal que

$$v(xy) = v(x) + v(y) \text{ y } v(x + y) \geq \min \{v(x), v(y)\},$$

para todo $x, y \in K$. Así, Dedekind y Weber definen una superficie de Riemann como el conjunto de todas las valuaciones sobre el cuerpo de funciones racionales, y a partir de esa definición estudiaron sus propiedades.

La herramienta natural para continuar el estudio era la teoría de ideales, pero de este modo no se tiene en cuenta el punto en el infinito, por lo tanto introducen el concepto de divisor. Un divisor asigna a cada valuación un número entero que es cero excepto para un número finito de puntos, por ejemplo un divisor positivo simplemente es un conjunto finito de puntos en la superficie de Riemann. Este concepto nuevo les permitió generalizar ciertos resultados ya obtenidos por Riemann y Gustav Roch.

Por otro lado, Weber publica su libro sobre funciones elípticas y números algebraicos "*Elliptische Funktionen und Algebraische Zahlen*" en el año 1891, donde introduce el término "*Cuerpo de clases*" que inicialmente era una extensión particular de un cuerpo cuadrático imaginario cuyo grupo de Galois es isomorfo al grupo de clases de ideales del cuerpo cuadrático. Ya en el año 1897, Weber extendió el concepto de grupo de clases de ideales mediante el concepto de divisor para poder admitir ideales primos infinitos. Esto lleva al desarrollo de la teoría del cuerpo de clases, donde las extensiones abelianas de un cuerpo numérico son descritas en términos del grupo de clases de ideales generalizado.

3.2. DIVISORES PRIMOS

En esta sección se introducen los divisores primos finitos e infinitos de un cuerpo numérico. En algunas afirmaciones de esta sección no se presentara la prueba ya que son bastante conocidas en la literatura.

Definición 3.2.1. Sea K un cuerpo, una función $|\cdot| : K \rightarrow \mathbb{R}$ se dice que es un valor absoluto sobre K si satisface las siguientes propiedades:

1. $|x| \geq 0$ para todo $x \in K$, y $|x| = 0$ si y solo si $x = 0$.
2. $|xy| = |x||y|$ para todo $x, y \in K$.
3. $|x + y| \leq |x| + |y|$ para todo $x, y \in K$.

Un valor absoluto $|\cdot|$ se dice no arquimediano si satisface

$$|x + y| \leq \max\{|x|, |y|\}, \text{ para todo } x, y \in K.$$

En caso contrario se dice que $|\cdot|$ es arquimediano.

Si $|\cdot|$ es un valor absoluto sobre un cuerpo K , entonces se induce una distancia o métrica dada por

$$d(x, y) := |x - y|, \text{ para todo } x, y \in K.$$

Y con ello se induce una topología sobre K , generada por $\mathcal{B} = \{B_\epsilon(x) : x \in K, \epsilon > 0\}$, donde la bola de radio ϵ y centro en x está definida por

$$B_\epsilon(x) := \{y \in K : d(x, y) < \epsilon\}.$$

Dos valores absolutos sobre K se dicen equivalentes si inducen la misma topología en K .

Ejemplo 3.2.1. Sea K un cuerpo, se define el valor absoluto trivial sobre K para todo $x \in K$ como

$$|x|_0 = \begin{cases} 1 & \text{si } x \neq 0 \\ 0 & \text{si } x = 0. \end{cases}$$

Sean K un cuerpo y $|\cdot|_1, |\cdot|_2$ dos valores absolutos no triviales sobre K . En [19] se prueba que las siguientes afirmaciones son equivalentes.

1. $|\cdot|_1$ y $|\cdot|_2$ son equivalentes.
2. $|x|_1 < 1$ si y solo si $|x|_2 < 1$ para todo $x \in K$.
3. Existe $a > 0$ tal que $|x|_1 = |x|_2^a$ para todo $x \in K$.

El hecho anterior implica que la propiedad de ser equivalente define una relación de equivalencia en el conjunto de valores absolutos sobre K .

Definición 3.2.2. Sea K un cuerpo, una valuación sobre K es una función

$$v : K \rightarrow \mathbb{Z} \cup \{+\infty\}$$

tal que

1. $v(x) = +\infty$ si y solo si $x = 0$.
2. $v(xy) = v(x) + v(y)$ para todo $x, y \in K$.
3. $v(x + y) \geq \min\{v(x), v(y)\}$ para todo $x, y \in K$.

Proposición 3.2.1. Sean K un cuerpo y v una valuación sobre K , entonces se induce un valor absoluto no arquimediano sobre K .

Demostración. Para cada $x \in K$, defínase $|x| := c^{v(x)}$ donde $0 < c < 1$ es fijo.

1. Si $x = 0$, entonces $|x| = c^{v(0)} = c^\infty = 0$. Si $|x| = 0$, entonces $c^{v(x)} = 0$, puesto que $0 < c < 1$, entonces $v(x) = \infty$, y por lo tanto $x = 0$.

- 2.

$$|xy| = c^{v(xy)} = c^{v(x)+v(y)} = c^{v(x)}c^{v(y)} = |x||y|.$$

3. Nótese que la función $f(t) = c^t$ es decreciente ya que $0 < c < 1$. Supóngase que

$$\text{mín} \{v(x), v(y)\} = v(x),$$

entonces

$$|x + y| = c^{v(x+y)} \leq c^{v(x)} \leq c^{v(x)} + c^{v(y)} = |x| + |y|.$$

4. Supóngase que $\text{mín} \{v(x), v(y)\} = v(x)$, entonces $v(x) \leq v(y)$, y así

$$|x| = c^{v(x)} \geq c^{v(y)} = |y|,$$

de modo que $\text{máx} \{|x|, |y|\} = |x|$. Esto implica que

$$|x + y| = c^{v(x+y)} \leq c^{v(x)} = |x| = \text{máx} \{|x|, |y|\}.$$

□

Ejemplo 3.2.2. Sea $p \in \mathbb{Z}$ un primo, y sea $x \in \mathbb{Q}$, entonces

$$x = p^r \frac{a}{b},$$

donde $a, b \in \mathbb{Z}$ no nulos y no divisibles por p . Si $v_p(x) := r$, entonces se induce un valor absoluto no arquimediano sobre \mathbb{Q} dado por

$$|x|_p := c^{v_p(x)}, \text{ donde } 0 < c < 1 \text{ es fijo.}$$

Observación 3.2.1. Nótese que si se escoge otro $e \in (0, 1)$, entonces $e = c^a$ para algún $a > 0$. Esto implica que $|x| := c^{v(x)}$ y $|x|' := e^{v(x)}$ son valores absolutos equivalentes.

Definición 3.2.3. Un cuerpo métrico es un par (K, τ) donde K es un cuerpo y τ es una topología inducida por un valor absoluto sobre K .

Un cuerpo métrico es discreto si todos sus valores absolutos están inducidos por una valuación.

Definición 3.2.4. Sea K un cuerpo, una clase de equivalencia de un valor absoluto no trivial sobre K se llama un divisor primo de K .

Un divisor primo de K es arquimediano o no arquimediano si lo son todos los valores absolutos que lo componen.

Un divisor primo de K es discreto si todos los valores absolutos que lo componen son inducidos por una valuación. Luego, todo divisor primo discreto es no arquimediano.

Por otro lado, sea K un cuerpo numérico y \mathfrak{p} un ideal primo de \mathcal{O}_K , y sea $x \in K$ no nulo, puesto que $x\mathcal{O}_K$ es un ideal fraccionario de K entonces se escribe de forma única como

$$x\mathcal{O}_K = \mathfrak{p}^e \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g},$$

donde $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ son ideales primos de \mathcal{O}_K y $e, e_1, \dots, e_g \in \mathbb{Z}$.

Se define el valor \mathfrak{p} -ádico de x como $v_{\mathfrak{p}}(x) := e$. La función $v_{\mathfrak{p}}$ es una valuación sobre K , y por lo tanto induce un valor absoluto no arquimediano sobre K .

Por ser \mathfrak{p} un ideal primo de \mathcal{O}_K , entonces $\|\mathfrak{p}\| > 1$, luego, tómesese $c := \frac{1}{\|\mathfrak{p}\|}$, por lo tanto el valor absoluto inducido está dado por

$$|x|_{\mathfrak{p}} = \left(\frac{1}{\|\mathfrak{p}\|} \right)^{v_{\mathfrak{p}}(x)}.$$

De esta manera, se tiene que el ideal primo \mathfrak{p} induce una valuación sobre K , y así, un divisor primo no arquimediano de K . Por otro lado, se puede probar que todo divisor primo no arquimediano de K proviene de un ideal primo de \mathcal{O}_K .

Este tipo de divisores primos de K se llaman divisores primos finitos de K .

Nótese que si \mathfrak{p} y \mathfrak{q} son ideales primos de \mathcal{O}_K diferentes, entonces los divisores primos inducidos por estos ideales son diferentes.

En efecto, sean $|\cdot|_{\mathfrak{p}}, |\cdot|_{\mathfrak{q}}$ los valores absolutos inducidos por \mathfrak{p} y \mathfrak{q} respectivamente, y sean $x \in \mathfrak{p} - \mathfrak{q}$ y $y \in \mathfrak{q} - \mathfrak{p}$. Entonces \mathfrak{p} está en la factorización de $x\mathcal{O}_K$ pero \mathfrak{q} no lo está, de modo que $v_{\mathfrak{p}}(x) \geq 1$ y $v_{\mathfrak{q}}(x) = 0$, análogamente se tiene que $v_{\mathfrak{q}}(y) \geq 1$ y $v_{\mathfrak{p}}(y) = 0$. Y por lo tanto

$$|x|_{\mathfrak{p}} = \left(\frac{1}{\|\mathfrak{p}\|} \right)^{v_{\mathfrak{p}}(x)} < 1, \text{ pero } |x|_{\mathfrak{q}} = \left(\frac{1}{\|\mathfrak{q}\|} \right)^{v_{\mathfrak{q}}(x)} = 1.$$

De modo que $|\cdot|_{\mathfrak{p}}$ y $|\cdot|_{\mathfrak{q}}$ no son equivalentes.

Observación 3.2.2. Los valores absolutos usuales sobre \mathbb{R} y sobre \mathbb{C} son arquimedianos, esto implica que estos valores absolutos no son inducidos por un ideal primo.

Sea K un cuerpo numérico y $\sigma : K \rightarrow \mathbb{C}$ uno de los homomorfismos de K en \mathbb{C} que fijan a \mathbb{Q} , entonces se induce un valor absoluto sobre K dado por

$$|x|_{\sigma} = |\sigma(x)|, \text{ para todo } x \in K,$$

donde el valor absoluto del lado derecho de la igualdad es el usual en \mathbb{C} . Este valor absoluto es arquimediano.

En [12] se prueba que para par de homomorfismos $\sigma, \gamma : K \rightarrow \mathbb{C}$ de un cuerpo numérico K en \mathbb{C} que fijan a \mathbb{Q} , se tiene que σ y γ inducen valores absolutos equivalentes sobre K si y solo si $\sigma = \gamma$ o $\sigma = \bar{\gamma}$, donde $\bar{\gamma}$ es la composición de γ con la conjugación compleja.

Ahora, sea K un cuerpo numérico tal que $[K : \mathbb{Q}] = n$, luego existen n homomorfismos de K en \mathbb{C} que fijan a \mathbb{Q} . Sean $\sigma_1, \dots, \sigma_s : K \rightarrow \mathbb{R}$ los s homomorfismos reales, y sean $\sigma_{s+1}, \bar{\sigma}_{s+1}, \dots, \sigma_{s+t}, \bar{\sigma}_{s+t} : K \rightarrow \mathbb{C}$ los $2t$ homomorfismos complejos. De modo que $n = s + 2t$.

Tómese $r := s + t$, el teorema anterior implica que se inducen r valores absolutos arquimedianos no equivalentes dos a dos, y por lo tanto se inducen r divisores primos de K arquimedianos distintos. Este tipo de divisores primos de K se llaman divisores primos infinitos de K , un divisor primo infinito de K se dice real o complejo si está inducido por un homomorfismo real o complejo.

Puesto que se añadieron divisores primos infinitos al conjunto de ideales primos de un cuerpo numérico K , se abusa de la notación para un divisor primo de K ya sea finito o infinito, un divisor primo de K se denota por \mathfrak{p} , y su valor absoluto inducido se denota por $|\cdot|_{\mathfrak{p}}$. Además, a un divisor primo de K también se le llama solamente primo de K .

Ahora, sean K y L cuerpos numéricos tales que $K \subseteq L$, y sean \mathfrak{p} y \mathfrak{P} divisores primos de K y L respectivamente, donde ambos son finitos o ambos son infinitos. Se dice que \mathfrak{P} divide a \mathfrak{p} si $|\cdot|_{\mathfrak{P}}$ al ser restringido a K es equivalente a $|\cdot|_{\mathfrak{p}}$, y se denota por $\mathfrak{P}|\mathfrak{p}$. En otras palabras, si son divisores primos finitos entonces $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$, y si son infinitos entonces el homomorfismo $\sigma : L \rightarrow \mathbb{C}$ que induce al divisor primo \mathfrak{P} es una extensión del homomorfismo que induce al divisor primo \mathfrak{p} .

Por último, en la siguiente definición se estudia la ramificación de los primos infinitos.

Definición 3.2.5. Sean $K \subseteq L$ cuerpos numéricos tales que L es una extensión de Galois de K . Sea \mathfrak{p} un primo infinito de K , y sea $\sigma : K \rightarrow \mathbb{C}$ el homomorfismo asociado a \mathfrak{p} .

Se dice que el primo infinito \mathfrak{p} de K ramifica en L si $\sigma(K) \subseteq \mathbb{R}$ y alguna extensión $\gamma : L \rightarrow \mathbb{C}$ de σ satisface que $\gamma(L) \not\subseteq \mathbb{R}$. Esto es, se dice que \mathfrak{p} ramifica en L si σ es un homomorfismo real pero alguna extensión a L es un homomorfismo complejo.

Ejemplo 3.2.3. Sean $K = \mathbb{Q}$ y $L = \mathbb{Q}(\sqrt{2})$. Así, L es una extensión de Galois abeliana de K puesto que $Gal(L/K) = \{\sigma_1, \sigma_2\}$, donde

$$\sigma_1(a + b\sqrt{2}) = a + b\sqrt{2} \text{ y } \sigma_2(a + b\sqrt{2}) = a - b\sqrt{2},$$

para todo $a, b \in \mathbb{Q}$.

El único primo infinito real de $K = \mathbb{Q}$ es el inducido por el homomorfismo

$$\begin{aligned} \sigma : \mathbb{Q} &\rightarrow \mathbb{R} \\ q &\mapsto \sigma(q) := q. \end{aligned}$$

Y por lo tanto, este primo infinito no ramifica en L pues sus dos extensiones a L son homomorfismos reales.

Ejemplo 3.2.4. Sean $K = \mathbb{Q}$ y $L = \mathbb{Q}(\sqrt{-2})$. Así, L es una extensión de Galois abeliana de K puesto que $Gal(L/K) = \{\sigma_1, \sigma_2\}$, donde

$$\sigma_1(a + b\sqrt{-2}) = a + b\sqrt{-2} \text{ y } \sigma_2(a + b\sqrt{-2}) = a - b\sqrt{-2},$$

para todo $a, b \in \mathbb{Q}$.

El único primo infinito real de $K = \mathbb{Q}$ es el inducido por el homomorfismo

$$\begin{aligned}\sigma : \mathbb{Q} &\rightarrow \mathbb{R} \\ q &\mapsto \sigma(q) := q.\end{aligned}$$

Y por lo tanto, este primo infinito ramifica en L pues sus dos extensiones a L son homomorfismos complejos.

3.3. GRUPO DE CLASES GENERALIZADO

El objetivo de esta sección es generalizar la noción de grupo de clases de ideales, para ello, se introduce el concepto de módulo en un cuerpo, en donde se admiten los primos infinitos.

Definición 3.3.1. Sea K un cuerpo numérico, se define un módulo m en K como un producto formal

$$m = \prod_{\mathfrak{p}} \mathfrak{p}^{m_{\mathfrak{p}}},$$

donde \mathfrak{p} recorre todos los primos de K , y a cada primo \mathfrak{p} de K se le asigna un número natural $m_{\mathfrak{p}}$ tal que:

1. $m_{\mathfrak{p}} = 0$ para todos los primos de K salvo para un número finito de primos de K .
2. $m_{\mathfrak{p}} = 0$ para todo primo infinito complejo de K .
3. $m_{\mathfrak{p}} \leq 1$ para todo primo infinito real de K .

Sean

$$m = \prod_{\mathfrak{p}} \mathfrak{p}^{m_{\mathfrak{p}}} \quad y \quad n = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$$

dos módulos en K , se define el producto de m y n como

$$mn := \prod_{\mathfrak{p}} \mathfrak{p}^{(mn)_{\mathfrak{p}}},$$

donde para cada divisor primo \mathfrak{p} de K se tiene que:

1. $(mn)_{\mathfrak{p}} := m_{\mathfrak{p}} + n_{\mathfrak{p}}$ para todo primo finito de K .
2. $(mn)_{\mathfrak{p}} := \max\{m_{\mathfrak{p}}, n_{\mathfrak{p}}\}$ para todo primo infinito de K .

Nótese que este producto es asociativo y conmutativo, y además, tiene por elemento neutro al módulo

$$1 = \prod_{\mathfrak{p}} \mathfrak{p}^{1_{\mathfrak{p}}},$$

donde $1_p = 0$ para todo primo p de K .

Por otro lado, si

$$\mathfrak{m} = \prod_p \mathfrak{p}^{m_p}$$

es un módulo en K , se destacan dos partes de \mathfrak{m} .

La parte finita de \mathfrak{m} se define como

$$\mathfrak{m}_0 := \prod_p \mathfrak{p}^{m_p},$$

donde el producto es sobre todos los primos p finitos de K , a la parte finita de \mathfrak{m} se le puede considerar como un ideal de \mathcal{O}_K .

La parte infinita de \mathfrak{m} se define como

$$\mathfrak{m}_\infty := \prod_p \mathfrak{p}^{m_p},$$

donde el producto es sobre todos los primos p infinitos de K , y los exponentes m_p son iguales a 1 o 0.

De este modo, se obtiene que $\mathfrak{m} = \mathfrak{m}_0 \mathfrak{m}_\infty$.

Un divisor primo \mathfrak{p} de K se dice que divide al módulo \mathfrak{m} si $m_p \geq 1$, y en este caso, se dice que \mathfrak{m} es divisible por el primo \mathfrak{p} , y se denota por $\mathfrak{p} | \mathfrak{m}$. Ahora, si \mathfrak{m} y \mathfrak{n} son módulos en K , se dice que \mathfrak{m} divide a \mathfrak{n} si $m_p \leq n_p$ para todo primo \mathfrak{p} de K , esto se denota por $\mathfrak{m} | \mathfrak{n}$.

En el caso en que K es un cuerpo numérico totalmente imaginario, es decir que K no puede inyectarse en \mathbb{R} , entonces un módulo en K no tiene parte infinita pues no existen primos infinitos reales, y por lo tanto un módulo en K se puede considerar como un ideal de \mathcal{O}_K .

Definición 3.3.2. Sean K un cuerpo numérico y

$$\mathfrak{m} = \prod_p \mathfrak{p}^{m_p}$$

un módulo en K .

Se define $I_K(\mathfrak{m})$ como el subgrupo del grupo I_K de ideales fraccionarios de K generado por los ideales primos de \mathcal{O}_K asociados a los primos finitos que tienen exponente nulo en \mathfrak{m} , es decir

$$I_K(\mathfrak{m}) := \{ \mathfrak{b} \in I_K : v_p(\mathfrak{b}) = 0 \text{ para todo } \mathfrak{p} \text{ primo finito tal que } m_p \geq 1 \},$$

donde $v_p(\cdot)$ es la valuación correspondiente a \mathfrak{p} .

En el caso en que $\mathfrak{m} = 1$, se denota por $I_K(1) = I_K$.

Nótese que el grupo $I_K(\mathfrak{m})$ solo depende de la parte finita del módulo \mathfrak{m} .

Las siguientes definiciones extienden la noción de congruencia módulo un ideal.

Definición 3.3.3. Sea K un cuerpo numérico y \mathfrak{p} un divisor primo infinito real de K . Sea $\sigma : K \rightarrow \mathbb{R}$ el homomorfismo asociado a \mathfrak{p} . Si $\alpha \in K - \{0\}$, se define

$$\alpha \equiv^* 1 \pmod{\mathfrak{p}} \text{ si y solo si } \sigma(\alpha) > 0,$$

y en tal caso se dice que α y 1 son congruentes módulo \mathfrak{p} .

Ejemplo 3.3.1. Sean $K = \mathbb{Q}$ y \mathfrak{p} el divisor primo real de \mathbb{Q} inducido por el homomorfismo

$$\begin{aligned} \sigma : \mathbb{Q} &\rightarrow \mathbb{R} \\ q &\mapsto \sigma(q) := q. \end{aligned}$$

Sea $\alpha \in \mathbb{Q} - \{0\}$, entonces

$$\alpha \equiv^* 1 \pmod{\mathfrak{p}} \Leftrightarrow \alpha = \sigma(\alpha) > 0.$$

Es decir, α y 1 son congruentes módulo \mathfrak{p} si y solo si $\alpha > 0$.

Definición 3.3.4. Sean K un cuerpo numérico y \mathfrak{p} un ideal primo de \mathcal{O}_K asociado a un primo finito \mathfrak{p} , y sea $n \geq 1$. Si $\alpha \in K - \{0\}$, se define

$$\alpha \equiv^* 1 \pmod{\mathfrak{p}^n}$$

si y solo si α es una unidad en la localización $(\mathcal{O}_K)_{\mathfrak{p}}$ y $v_{\mathfrak{p}(\mathcal{O}_K)_{\mathfrak{p}}}(\alpha - 1) \geq n$, donde $v_{\mathfrak{p}(\mathcal{O}_K)_{\mathfrak{p}}}(\cdot)$ es la valuación correspondiente al ideal $\mathfrak{p}(\mathcal{O}_K)_{\mathfrak{p}}$. Esto es equivalente a es decir que α es una unidad en la localización $(\mathcal{O}_K)_{\mathfrak{p}}$ y

$$\alpha \equiv 1 \pmod{\mathfrak{p}^n(\mathcal{O}_K)_{\mathfrak{p}}},$$

donde esta última congruencia es la congruencia usual en ideales.

Definición 3.3.5. Sean K un cuerpo numérico y

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{m_{\mathfrak{p}}}$$

un módulo en K .

Sea $\alpha \in K - \{0\}$, se dice que

$$\alpha \equiv^* 1 \pmod{\mathfrak{m}}$$

si y solo si

$$\alpha \equiv^* 1 \pmod{\mathfrak{p}}$$

para cada \mathfrak{p} primo infinito real de K tal que $m_{\mathfrak{p}} = 1$, y

$$\alpha \equiv^* 1 \pmod{\mathfrak{p}^{m_{\mathfrak{p}}}}$$

para cada \mathfrak{p} primo finito de K tal que $m_{\mathfrak{p}} \geq 1$.

El asterisco * indica que estas relaciones son compatibles con el producto de $K - \{0\}$.

Definición 3.3.6. Sean K un cuerpo numérico y $\mathfrak{m} = \mathfrak{m}_0 \mathfrak{m}_\infty$ un módulo en K . Se definen los siguientes conjuntos.

$$K_{\mathfrak{m}} := \left\{ \frac{a}{b} : a, b \in \mathcal{O}_K - \{0\} \text{ y } a \mathcal{O}_K, b \mathcal{O}_K \text{ son primos relativos a } \mathfrak{m}_0 \right\}.$$

$$K_{\mathfrak{m},1} := \{ \alpha \in K_{\mathfrak{m}} : \alpha \equiv^* 1 \pmod{\mathfrak{m}} \}.$$

Nótese que $K_{\mathfrak{m}}$ también se puede escribir de la siguiente manera

$$K_{\mathfrak{m}} := \left\{ \frac{a}{b} : a, b \in \mathcal{O}_K - \{0\} \text{ y } v_p(a) = v_p(b) = 0 \text{ para todo } p \text{ primo finito de } K \text{ tal que } \mathfrak{m}_p \geq 1 \right\}.$$

Es facil ver dado K un cuerpo numérico y $\mathfrak{m} = \mathfrak{m}_0 \mathfrak{m}_\infty$ un módulo en K , entonces $K_{\mathfrak{m}}$ y $K_{\mathfrak{m},1}$ son subgrupos multiplicativos de $K - \{0\}$.

Por otro lado, nótese que el grupo $K_{\mathfrak{m}}$ solo depende de los divisores primos finitos que dividen al módulo \mathfrak{m} y no de los exponentes de cada divisor primo finito, mientras que el grupo $K_{\mathfrak{m},1}$ depende de los divisores primos finitos e infinitos que dividen al módulo \mathfrak{m} y también de los exponentes de los divisores primos finitos.

El grupo $K_{\mathfrak{m},1}$ se denomina el rayo $(\text{mod } \mathfrak{m})$.

Ahora, sea

$$\begin{aligned} \iota : K - \{0\} &\rightarrow I_K \\ \alpha &\mapsto \iota(\alpha) := \alpha \mathcal{O}_K. \end{aligned}$$

la inclusión natural de $K - \{0\}$ en I_K , ya que ι es un homomorfismo de grupos multiplicativos entonces la imagen de $K_{\mathfrak{m},1}$ bajo este homomorfismo es un subgrupo de I_K , mas aún, es un subgrupo de $I_K(\mathfrak{m})$. Denótese por $P_{K,1}(\mathfrak{m}) := \iota(K_{\mathfrak{m},1})$.

Ejemplo 3.3.2. Sean $K = \mathbb{Q}$ y $\mathfrak{m} = 5\mathbb{Z}$. Entonces

$$K_{\mathfrak{m}} = \left\{ \frac{a}{b} : a \equiv 1, 2, 3, 4 \pmod{5} \text{ y } b \equiv 1, 2, 3, 4 \pmod{5} \right\},$$

$$K_{\mathfrak{m},1} = \left\{ \frac{a}{b} \in K_{\mathfrak{m}} : a - b \equiv 0 \pmod{5} \right\}$$

y

$$P_{K,1}(\mathfrak{m}) = \left\{ \frac{a}{b} \mathcal{O}_K : \frac{a}{b} \in K_{\mathfrak{m},1} \right\}.$$

Definición 3.3.7. Sean K un cuerpo numérico y \mathfrak{m} un módulo en K , el cociente

$$C_K(\mathfrak{m}) := I_K(\mathfrak{m}) / P_{K,1}(\mathfrak{m})$$

es llamado el grupo de clases de rayos ($\text{mod } \mathfrak{m}$).

Sea H un subgrupo de $I_K(\mathfrak{m})$, se dice que H es un subgrupo de congruencia ($\text{mod } \mathfrak{m}$) si

$$P_{K,1}(\mathfrak{m}) \subseteq H \subseteq I_K(\mathfrak{m}),$$

y el cociente

$$I_K(\mathfrak{m})/H$$

es llamado el grupo de clases de ideales generalizado ($\text{mod } \mathfrak{m}$).

En el caso en que $\mathfrak{m} = 1$, se denota por $P_{K,1}(1) = P_K$, de modo que P_K es un subgrupo de congruencia ($\text{mod } 1$), y así, el grupo de clases de ideales $C(\mathcal{O}_K) = I_K/P_K$ es un grupo de clases de ideales generalizado ($\text{mod } 1$), esto indica que el grupo de clases de ideales generalizado en efecto si es una generalización del grupo de clases de ideales que se definió en el capítulo 1.

En [13] se demuestra un hecho importante del grupo de clases de rayos. Este es, dado K un cuerpo numérico y \mathfrak{m} un módulo en K , entonces el grupo de clases de rayos ($\text{mod } \mathfrak{m}$)

$$C_K(\mathfrak{m}) = I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})$$

es un grupo finito.

El siguiente corolario indica que el grupo de clases de ideales generalizado también resulta ser finito, al igual que el grupo de clases de ideales.

Corolario 3.3.1. Sean K un cuerpo numérico y \mathfrak{m} un módulo en K . Si H es un subgrupo de congruencia ($\text{mod } \mathfrak{m}$), entonces el grupo de clases de ideales generalizado ($\text{mod } \mathfrak{m}$)

$$I_K(\mathfrak{m})/H$$

es finito.

Demostración. Sea

$$\begin{aligned} \phi : I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m}) &\rightarrow I_K(\mathfrak{m})/H \\ \bar{\mathfrak{b}} &\mapsto \phi(\bar{\mathfrak{b}}) := \bar{\mathfrak{b}}. \end{aligned}$$

un homomorfismo de grupos bien definido puesto que $P_{K,1}(\mathfrak{m}) \subseteq H$. Además, ϕ es un homomorfismo sobreyectivo y $\text{Ker}(\phi) = H/P_{K,1}(\mathfrak{m})$. Esto implica que

$$(I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})) / (H/P_{K,1}(\mathfrak{m})) \cong I_K(\mathfrak{m})/H,$$

y puesto que $I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})$ es un grupo finito se obtiene que $I_K(\mathfrak{m})/H$ es un grupo finito. \square

3.4. TEOREMA DE ARTIN

Uno de los teoremas mas importantes de la teoría del cuerpo de clases es el teorema de Artin, este teorema muestra que el grupo de Galois de una extensión abeliana es el grupo de clases de ideales generalizado para algún módulo. Estos dos grupos se relacionan mediante el homomorfismo de Artin.

El homomorfismo de Artin definido en el capítulo 2 está definido para las extensiones abelianas y no ramificadas de un cuerpo numérico dado, la siguiente definición generaliza el homomorfismo de Artin para extensiones abelianas.

Definición 3.4.1. Sean $K \subseteq L$ cuerpos numéricos tales que L es una extensión de Galois abeliana de K . Sea \mathfrak{m} un módulo en K divisible por todos los primos finitos de K que ramifican en L .

Puesto que para cada ideal primo \mathfrak{p} de \mathcal{O}_K asociado a un divisor primo finito de K que no divide a \mathfrak{m} existe un único

$$\left(\frac{L/K}{\mathfrak{p}}\right) \in Gal(L/K),$$

así, dado $\mathfrak{b} \in I_K(\mathfrak{m})$ se tiene que

$$\mathfrak{b} = \prod_{i=1}^t \mathfrak{p}_i^{r_i},$$

donde para cada $1 \leq i \leq t$ se tiene que $r_i \in \mathbb{Z}$ y los \mathfrak{p}_i son ideales primos de \mathcal{O}_K asociados a los primos finitos de K que no dividen a \mathfrak{m} . De este modo se define

$$\begin{aligned} \Phi_{\mathfrak{m}} : I_K(\mathfrak{m}) &\rightarrow Gal(L/K) \\ \mathfrak{b} &\mapsto \Phi_{\mathfrak{m}}(\mathfrak{b}) := \prod_{i=1}^t \left(\frac{L/K}{\mathfrak{p}_i}\right)^{r_i}. \end{aligned}$$

llamado el homomorfismo de Artin para $K \subseteq L$ y \mathfrak{m} . Si se quiere hacer explicita la extensión y el módulo, se denota por $\Phi_{L/K, \mathfrak{m}}$.

Con esta definición es posible enunciar el teorema de Artin, de este teorema se desprenden hechos muy importantes de la teoría del cuerpo de clases.

Teorema 3.4.1 (Teorema de Artin). Sean $K \subseteq L$ cuerpos numéricos tales que L es una extensión de Galois abeliana de K . Sea \mathfrak{m} un módulo divisible por todos los primos (finitos o infinitos) de K que ramifican en L . Entonces:

1. El homomorfismo de Artin $\Phi_{\mathfrak{m}}$ es sobreyectivo.
2. Si los exponentes de los primos finitos de K que dividen a \mathfrak{m} son suficientemente grandes, entonces $Ker(\Phi_{\mathfrak{m}})$ es un subgrupo de congruencia (mod \mathfrak{m}), es decir

$$P_{K,1}(\mathfrak{m}) \subseteq Ker(\Phi_{\mathfrak{m}}) \subseteq I_K(\mathfrak{m}),$$

y por lo tanto

$$I_K(\mathfrak{m})/Ker(\Phi_{\mathfrak{m}}) \cong Gal(L/K).$$

Este isomorfismo muestra que el grupo $Gal(L/K)$ es un grupo de clases de ideales generalizado ($mod \mathfrak{m}$).

Ejemplo 3.4.1. Sea $m \geq 3$, y sea $K = \mathbb{Q}(\zeta_m)$ un cuerpo ciclotómico. Sea $\mathfrak{m} = m\infty$ un módulo en \mathbb{Q} , donde ∞ es el primo real infinito de \mathbb{Q} .

Si $p \in \mathbb{Z}$ es un primo tal que $p \nmid m$, entonces

$$\Phi_m(x) = \prod_{mcd(a,m)=1} (x - \zeta_m^a) \in \mathbb{Z}[x]$$

es separable ($mod p$): En efecto, denótese por $\bar{\Phi}_m(x)$ a la reducción de $\Phi_m(x)$ ($mod p$). Puesto que $\Phi_m(x)$ es mónico, entonces $\bar{\Phi}_m(x)$ también es mónico, esto implica que

$$\varphi(m) = gr(\Phi_m(x)) = gr(\bar{\Phi}_m(x)).$$

Por otro lado, $\Phi_m(\zeta_m^a) = 0$ para cada $1 \leq a < m$ tal que $mcd(a, m) = 1$, entonces

$$\bar{\Phi}_m(\bar{\zeta}_m^a) = \bar{0} \text{ en } \mathcal{O}_K/\mathfrak{p},$$

donde \mathfrak{p} es un ideal de \mathcal{O}_K que contiene a p .

Por lo tanto, $\bar{\zeta}_m^a$ es una raíz de $\bar{\Phi}_m(x)$ en $\mathcal{O}_K/\mathfrak{p}$ para todo $1 \leq a < m$ tal que $mcd(a, m) = 1$.

El lema 2.3.1 implica que

$$\bar{\zeta}_m^i \neq \bar{\zeta}_m^j$$

para todo $1 \leq i, j < m$ tales que $mcd(i, m) = 1$, $mcd(j, m) = 1$ y $i \neq j$.

Por lo tanto, todas las raíces de $\bar{\Phi}_m(x)$ son $\bar{\zeta}_m^a$ para todo $1 \leq a < m$ tal que $mcd(a, m) = 1$, de esto se concluye que $\Phi_m(x)$ es separable en $\mathbb{Z}/p\mathbb{Z}$.

Aplicando el teorema de Kummer-Dedekind se obtiene que el ideal $p\mathbb{Z}$ no ramifica en K . De modo que, el homomorfismo de Artin

$$\Phi_{\mathfrak{m}} : I_{\mathbb{Q}}(\mathfrak{m}) \longrightarrow Gal(K/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$$

está bien definido.

A continuación, se mostrará como está definido el homomorfismo de Artin.

Sea $\frac{a}{b}\mathbb{Z} \in I_{\mathbb{Q}}(\mathfrak{m})$, entonces $\frac{a}{b} \in \mathbb{Q}$ tal que $mcd(a, m) = 1 = mcd(b, m)$, además, se puede suponer que $\frac{a}{b} > 0$ y $mcd(a, b) = 1$. Así

$$\frac{a}{b}\mathbb{Z} = \prod_{i=1}^t (p_i\mathbb{Z})^{r_i},$$

donde $p_i \nmid m$ y $r_i \in \mathbb{Z} - \{0\}$ para cada $1 \leq i \leq t$. De este modo, para cada $1 \leq i \leq t$ se tiene que el ideal $p_i\mathbb{Z}$ no ramifica en K , y ya que

$$\text{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*,$$

se obtiene que el símbolo de Artin está bien definido, y solo depende del ideal $p_i\mathbb{Z}$ para cada $1 \leq i \leq t$, de modo que basta evaluar este automorfismo en ζ_m .

Sea $p \in \{p_1, \dots, p_t\}$, y sea \mathfrak{p} un ideal primo de \mathcal{O}_K que contiene a p , entonces

$$\begin{aligned} \left(\frac{K/\mathbb{Q}}{p\mathbb{Z}} \right) (\zeta_m) &\equiv \zeta_m^{\|p\mathbb{Z}\|} \pmod{\mathfrak{p}} \\ &\equiv \zeta_m^p \pmod{\mathfrak{p}}. \end{aligned}$$

Pero $\left(\frac{K/\mathbb{Q}}{p\mathbb{Z}} \right) (\zeta_m) = \zeta_m^j$, para algún $1 \leq j < m$ tal que $\text{mcd}(j, m) = 1$. Así,

$$\zeta_m^j \equiv \zeta_m^p \pmod{\mathfrak{p}}.$$

Si $1 < p < m$, por el lema 2.3.1 se obtiene que $j = p$, y así, bajo el isomorfismo

$$\text{Gal}(K/\mathbb{Q}) \xrightarrow{\psi} (\mathbb{Z}/m\mathbb{Z})^*,$$

se tiene que

$$\psi \left(\left(\frac{K/\mathbb{Q}}{p\mathbb{Z}} \right) \right) = \bar{p}.$$

En otro caso, supóngase que $p > m$, entonces $\zeta_m^{j-p} \equiv 1 \pmod{\mathfrak{p}}$. Esto implica que

$$j - p \equiv 0 \pmod{m},$$

y así, $j = p + mh$ para algún $h \in \mathbb{Z}$, de modo que, bajo el mismo isomorfismo usado en el caso anterior se tiene que

$$\psi \left(\left(\frac{K/\mathbb{Q}}{p\mathbb{Z}} \right) \right) = \bar{p}.$$

En los dos casos se obtiene que

$$\begin{aligned} \Phi_{\mathfrak{m}} \left(\frac{a}{b}\mathbb{Z} \right) &= \prod_{i=1}^t \left(\frac{K/\mathbb{Q}}{p_i\mathbb{Z}} \right)^{r_i} \\ &= \prod_{i=1}^t \bar{p}_i^{r_i} \\ &= \bar{a}\bar{b}^{-1}. \end{aligned}$$

Por otro lado, nótese que $\text{Ker}(\Phi_{\mathfrak{m}}) = P_{\mathbb{Q},1}(\mathfrak{m})$.

En efecto, sea $\frac{a}{b}\mathbb{Z} \in \text{Ker}(\Phi_{\mathfrak{m}}) \subseteq I_{\mathbb{Q}}(\mathfrak{m})$, entonces

$$\Phi_{\mathfrak{m}} \left(\frac{a}{b}\mathbb{Z} \right) = \bar{a}\bar{b}^{-1} = \bar{1},$$

y así,

$$\bar{a} = \bar{b} \text{ en } \mathbb{Z}/m\mathbb{Z}.$$

Además, puesto que $\frac{a}{b}\mathbb{Z} \in I_{\mathbb{Q}}(\mathfrak{m})$, entonces $\frac{a}{b} \in \mathbb{Q}$ tal que $\text{mcd}(a, m) = 1$ y $\text{mcd}(b, m) = 1$, adicionalmente, se puede suponer que $\frac{a}{b} > 0$ y $\text{mcd}(a, b) = 1$. De modo que

$$\frac{a}{b} \in \mathbb{Q}_m \text{ y } \frac{a}{b} \equiv^* 1 \pmod{\mathfrak{m}},$$

Esto implica que $\frac{a}{b} \in \mathbb{Q}_{m,1}$, y así, $\frac{a}{b}\mathbb{Z} \in P_{\mathbb{Q},1}(\mathfrak{m})$.

Recíprocamente, sea $\frac{a}{b}\mathbb{Z} \in P_{\mathbb{Q},1}(\mathfrak{m}) \subseteq I_{\mathbb{Q}}(\mathfrak{m})$, entonces $\frac{a}{b} \in \mathbb{Q}_{m,1}$, y por lo tanto

$$\frac{a}{b} \in \mathbb{Q}_m \text{ y } \frac{a}{b} \equiv^* 1 \pmod{\mathfrak{m}},$$

si

$$m = \prod_{i=1}^s (q_i\mathbb{Z})^{u_i},$$

donde $q_i \in \mathbb{Z}$ es primo y $u_i \geq 1$ para cada $1 \leq i \leq s$, entonces para cada $1 \leq i \leq s$ se obtiene que

$$\frac{a}{b} \equiv^* 1 \pmod{\mathfrak{q}_i^{m_{q_i}}}$$

para cada $\mathfrak{q}_i := q_i\mathbb{Z}$ ideal primo de \mathbb{Z} y $m_{q_i} := u_i$, de esta manera,

$$\frac{a}{b} \equiv 1 \pmod{\mathfrak{q}_i^{m_{q_i}} \mathbb{Z}_{q_i}}$$

para cada $1 \leq i \leq s$. Por lo tanto

$$a \equiv b \pmod{m},$$

y así $\bar{a} = \bar{b}$ en $\mathbb{Z}/m\mathbb{Z}$, y como $\text{mcd}(b, m) = 1$, entonces

$$\Phi_m\left(\frac{a}{b}\mathbb{Z}\right) = \bar{a}\bar{b}^{-1} = \bar{1},$$

de modo que $\frac{a}{b}\mathbb{Z} \in \text{Ker}(\Phi_m)$.

Por último, el primo ∞ real infinito de \mathbb{Q} ramifica en K , así, aplicando el teorema de Artin se obtiene que Φ_m es sobreyectivo, de esto se concluye que

$$I_{\mathbb{Q}}(\mathfrak{m})/P_{\mathbb{Q},1}(\mathfrak{m}) \cong \text{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*.$$

3.5. HACIA LAS LEYES DE RECIPROCIDAD

En esta sección se presenta el símbolo de Legendre para la n -ésima potencia (este es una generalización del símbolo cuadrático y cúbico de Legendre). También, se demuestra la ley de reciprocidad débil, y usando esto se realiza otra prueba de la ley de reciprocidad cuadrática.

Proposición 3.5.1. *Sea $n \geq 2$, y sea K un cuerpo numérico que contiene a ζ_n . Sean $a \in \mathcal{O}_K$ y \mathfrak{p} un ideal primo de \mathcal{O}_K tales que $na \notin \mathfrak{p}$, entonces.*

1. Las clases de $1, \zeta_n, \dots, \zeta_n^{n-1}$ en $\mathcal{O}_K/\mathfrak{p}$ son distintas.
2. n divide a $\|\mathfrak{p}\| - 1$.
3. $a^{(\|\mathfrak{p}\|-1)/n} \equiv \zeta_n^i \pmod{\mathfrak{p}}$ para un único $0 \leq i \leq n-1$.

Demostración. 1. Puesto que

$$x^n - 1 = \prod_{i=0}^{n-1} (x - \zeta_n^i)$$

y

$$x^n - 1 = (x - 1)(1 + x + \dots + x^{n-1}),$$

entonces

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

Esto implica que

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

por lo tanto

$$\bar{n} = \prod_{i=1}^{n-1} (1 - \bar{\zeta}_n^i) \text{ en } \mathcal{O}_K/\mathfrak{p}.$$

Por otro lado, ya que $na \notin \mathfrak{p}$ y \mathfrak{p} es un ideal primo de \mathcal{O}_K , se obtiene que $n \notin \mathfrak{p}$ y $a \notin \mathfrak{p}$, así, $\bar{n} \neq \bar{0}$ en $\mathcal{O}_K/\mathfrak{p}$. Esto implica que

$$\bar{\zeta}_n^i \neq \bar{1} \text{ para todo } 1 \leq i \leq n-1,$$

y por lo tanto

$$\bar{\zeta}_n^i \neq \bar{\zeta}_n^j \text{ para cada } 1 \leq i, j \leq n-1 \text{ y } i \neq j.$$

2. Puesto que $\mathcal{O}_K/\mathfrak{p}$ es un cuerpo finito y $\|\mathfrak{p}\| = |\mathcal{O}_K/\mathfrak{p}|$, entonces

$$(\mathcal{O}_K/\mathfrak{p})^* = \mathcal{O}_K/\mathfrak{p} - \{0\}$$

es un grupo de tamaño $\|\mathfrak{p}\| - 1$.

Además, el ítem anterior implica que $\bar{\zeta}_n \in (\mathcal{O}_K/\mathfrak{p})^*$, de lo contrario, $\bar{\zeta}_n = \bar{0}$, y así,

$$\bar{\zeta}_n^i = \bar{\zeta}_n^j \text{ para cada } 1 \leq i, j \leq n-1 \text{ y } i \neq j,$$

y de esta manera se contradice el ítem anterior.

Luego, $\langle \bar{\zeta}_n \rangle$ es un subgrupo de $(\mathcal{O}_K/\mathfrak{p})^*$, y por el teorema de Lagrange se tiene que $|\langle \bar{\zeta}_n \rangle|$ divide a $\|\mathfrak{p}\| - 1$.

El ítem anterior implica que $|\langle \bar{\zeta}_n \rangle| = n$, de donde se obtiene que n divide a $\|\mathfrak{p}\| - 1$.

3. Puesto que $\bar{a}^{\|\mathfrak{p}\|-1} = \bar{1}$ en $\mathcal{O}_K/\mathfrak{p}$, se obtiene que

$$\left(\bar{a}^{(\|\mathfrak{p}\|-1)/n}\right)^n = \bar{1} \text{ en } \mathcal{O}_K/\mathfrak{p},$$

entonces

$$\bar{a}^{(\|\mathfrak{p}\|-1)/n} = \bar{\zeta}_n^i \text{ en } \mathcal{O}_K/\mathfrak{p} \text{ para un único } 0 \leq i \leq n-1,$$

y así,

$$a^{(\|\mathfrak{p}\|-1)/n} \equiv \zeta_n^i \pmod{\mathfrak{p}} \text{ para un único } 0 \leq i \leq n-1.$$

□

La proposición anterior permite definir el símbolo de Legendre para la n -ésima potencia.

Definición 3.5.1. Sea $n \geq 2$, y sea K un cuerpo numérico que contiene a ζ_n .

Sean $a \in \mathcal{O}_K$ y \mathfrak{p} un ideal primo de \mathcal{O}_K tales que $na \notin \mathfrak{p}$, se define el símbolo de Legendre para la n -ésima potencia $\left(\frac{a}{\mathfrak{p}}\right)_n$ como la única raíz n -ésima de la unidad que satisface

$$a^{(\|\mathfrak{p}\|-1)/n} \equiv \left(\frac{a}{\mathfrak{p}}\right)_n \pmod{\mathfrak{p}}.$$

Además, sea \mathfrak{a} un ideal de \mathcal{O}_K tal que $na \notin \mathfrak{a}$, y si la factorización de \mathfrak{a} está dada por

$$\mathfrak{a} = \prod_{i=1}^t \mathfrak{p}_i,$$

donde \mathfrak{p}_i es un ideal primo de \mathcal{O}_K para cada $1 \leq i \leq t$, se define el símbolo de Legendre para la n -ésima potencia del ideal \mathfrak{a} como

$$\left(\frac{a}{\mathfrak{a}}\right)_n := \prod_{i=1}^t \left(\frac{a}{\mathfrak{p}_i}\right)_n.$$

Esta definición es una generalización del símbolo de Jacobi, en el caso cuadrático el símbolo de Jacobi se obtiene al generalizar el símbolo de Legendre cuadrático por medio de la multiplicación.

De este modo, el símbolo de Legendre para la n -ésima potencia es una generalización del símbolo de Legendre cuadrático y cúbico. Las dos siguientes proposiciones evidencian este hecho.

Proposición 3.5.2. Sean $n \geq 2$, K un cuerpo numérico que contiene a ζ_n , $a \in \mathcal{O}_K$ y \mathfrak{p} un ideal primo de \mathcal{O}_K tal que $na \notin \mathfrak{p}$.

Entonces $\left(\frac{a}{\mathfrak{p}}\right)_n = 1$ si y solo si la congruencia $x^n \equiv a \pmod{\mathfrak{p}}$ tiene solución.

Demostración. Supóngase que la congruencia $x^n \equiv a \pmod{\mathfrak{p}}$ tiene solución, así, existe $b \in \mathcal{O}_K$ tal que $b^n \equiv a \pmod{\mathfrak{p}}$, entonces

$$(b^n)^{(\|\mathfrak{p}\|-1)/n} \equiv a^{(\|\mathfrak{p}\|-1)/n} \pmod{\mathfrak{p}},$$

esto implica que

$$b^{\|\mathfrak{p}\|-1} \equiv a^{(\|\mathfrak{p}\|-1)/n} \pmod{\mathfrak{p}}.$$

Por otro lado, supóngase que $b \in \mathfrak{p}$, ya que $a - b^n \in \mathfrak{p}$, se obtiene que $a \in \mathfrak{p}$, pero esto contradice la hipótesis, de modo que $b \notin \mathfrak{p}$.

La proposición anterior implica que

$$b^{\|\mathfrak{p}\|-1} \equiv 1 \pmod{\mathfrak{p}},$$

y así,

$$a^{(\|\mathfrak{p}\|-1)/n} \equiv 1 \pmod{\mathfrak{p}}.$$

De esto se concluye que $\left(\frac{a}{\mathfrak{p}}\right)_n = 1$.

Recíprocamente, supóngase que $\left(\frac{a}{\mathfrak{p}}\right)_n = 1$, por definición de tiene que

$$a^{(\|\mathfrak{p}\|-1)/n} \equiv 1 \pmod{\mathfrak{p}},$$

puesto que $\mathcal{O}_K/\mathfrak{p}$ es un cuerpo finito, entonces el grupo $(\mathcal{O}_K/\mathfrak{p})^*$ es cíclico. Sea $\bar{\epsilon}$ un generador de $(\mathcal{O}_K/\mathfrak{p})^*$, entonces existe $r \in \mathbb{Z}$ tal que $\bar{a} = \bar{\epsilon}^r$, y así,

$$\bar{\epsilon}^r \equiv a \pmod{\mathfrak{p}},$$

de modo que

$$1 \equiv a^{(\|\mathfrak{p}\|-1)/n} \equiv \bar{\epsilon}^{r(\|\mathfrak{p}\|-1)/n} \pmod{\mathfrak{p}}.$$

Ya que el orden de $\bar{\epsilon}$ es $\|\mathfrak{p}\| - 1$, entonces $\|\mathfrak{p}\| - 1$ divide a $r \frac{\|\mathfrak{p}\|-1}{n}$, esto implica que

$$r \frac{\|\mathfrak{p}\| - 1}{n} = (\|\mathfrak{p}\| - 1)h \quad \text{para algún } h \in \mathbb{Z},$$

así, $r = nh$, de modo que

$$\begin{aligned} a &\equiv \epsilon^r \pmod{\mathfrak{p}} \\ &\equiv \epsilon^{nh} \pmod{\mathfrak{p}} \\ &\equiv (\epsilon^h)^n \pmod{\mathfrak{p}}. \end{aligned}$$

De esto se concluye que la congruencia $x^n \equiv a \pmod{\mathfrak{p}}$ tiene solución. □

Proposición 3.5.3. Sean $n \geq 2$, K un cuerpo numérico que contiene a ζ_n , $a \in \mathcal{O}_K$ y \mathfrak{p} un ideal primo de \mathcal{O}_K tal que $na \notin \mathfrak{p}$. Si $L = K(\sqrt[n]{a})$, entonces.

1. L es una extensión de Galois abeliana de K .
2. El ideal primo \mathfrak{p} no ramifica en L .
3. $\left(\frac{L/K}{\mathfrak{p}}\right)(\sqrt[n]{a}) = \left(\frac{a}{\mathfrak{p}}\right)_n \sqrt[n]{a}$.

Demostración. 1. Nótese que $x^n - a \in K[x]$, y además

$$x^n - a = \prod_{i=0}^{n-1} (x - \sqrt[n]{a}\zeta_n^i),$$

esta igualdad es consecuencia de que estos dos polinomios coinciden en sus n raíces. De otro lado, $L = K(\sqrt[n]{a})$ es la adjunción a K de todas las raíces del polinomio $x^n - a$, y por lo tanto L es una extensión normal de K , de donde se concluye que L es una extensión de Galois de K .

Por otro lado, dado que $\sigma \in \text{Gal}(L/K)$ está determinado por $\sqrt[n]{a}$, entonces

$$\sigma(\sqrt[n]{a}) = \sqrt[n]{a}\zeta_n^i \text{ para algún } 0 \leq i \leq n-1.$$

Así, defínase el homomorfismo de grupos

$$\begin{aligned} \psi : \text{Gal}(L/K) &\rightarrow \mathbb{Z}/n\mathbb{Z} \\ \sigma &\mapsto \psi(\sigma) := \bar{i}. \end{aligned}$$

Además, ψ es inyectivo. En efecto, sea $\sigma \in \text{Ker}(\psi)$, entonces $\psi(\sigma) = \bar{0}$, pero por definición se tiene que $\psi(\sigma) = \bar{i}$, esto implica que $\bar{i} = \bar{0}$, por la condición de i se tiene que $i = 0$, así, $\sigma(\sqrt[n]{a}) = \sqrt[n]{a}$, por lo tanto $\sigma = i_L$.

De esto se concluye que $\text{Gal}(L/K)$ es un grupo abeliano.

2. Primero, nótese que $\sqrt[n]{a} \in \mathcal{O}_L$.

En efecto, ya que $x^n - a \in \mathcal{O}_K[x]$ y $\mathcal{O}_K \subseteq \mathcal{O}_L$, entonces $x^n - a \in \mathcal{O}_L[x]$. Puesto que $\sqrt[n]{a} \in L$ es raíz de $x^n - a$, entonces $\sqrt[n]{a} \in \mathcal{O}_L$.

Por otro lado, es suficiente ver que $x^n - a$ es separable (mod \mathfrak{p}):

Puesto que

$$x^n - a = \prod_{i=0}^{n-1} (x - \sqrt[n]{a} \zeta_n^i),$$

y si \mathfrak{P} es un ideal primo de \mathcal{O}_L que contiene a \mathfrak{p} , entonces para cada $0 \leq i \leq n-1$ se tiene que $\overline{\sqrt[n]{a} \zeta_n^i} \in \mathcal{O}_L/\mathfrak{P}$ es una raíz de del polinomio $x^n - \bar{a} \in (\mathcal{O}_K/\mathfrak{p})[x]$. Ahora, supóngase que existen $0 \leq i, j \leq n-1$ con $i \neq j$ tales que

$$\overline{\sqrt[n]{a} \zeta_n^i} = \overline{\sqrt[n]{a} \zeta_n^j},$$

entonces

$$\sqrt[n]{a} (\zeta_n^i - \zeta_n^j) \in \mathfrak{P},$$

así, $\sqrt[n]{a} \in \mathfrak{P}$ o $\zeta_n^i - \zeta_n^j \in \mathfrak{P}$.

Si $\zeta_n^i - \zeta_n^j \in \mathfrak{P}$, y ya que $\zeta_n \in K$, entonces $\zeta_n^i - \zeta_n^j \in K$, y por lo tanto

$$\zeta_n^i - \zeta_n^j \in \mathfrak{P} \cap K = \mathfrak{p},$$

lo que es una contradicción.

Si $\sqrt[n]{a} \in \mathfrak{P}$, entonces $\overline{\sqrt[n]{a}} = \bar{0}$ en $\mathcal{O}_L/\mathfrak{P}$. Esto implica que $\bar{0}$ es una raíz de $x^n - \bar{a}$, así, $\bar{a} = \bar{0}$ en $\mathcal{O}_K/\mathfrak{p}$, y por lo tanto $a \in \mathfrak{p}$, lo que es una contradicción.

Así, se concluye que

$$\overline{\sqrt[n]{a} \zeta_n^i} \neq \overline{\sqrt[n]{a} \zeta_n^j},$$

y así, $x^n - a$ es separable (mod \mathfrak{p}). Luego, por el teorema de Kummer-Dedekind se obtiene que \mathfrak{p} no ramifica en L , de donde se tiene que el símbolo de Artin $\left(\frac{L/K}{\mathfrak{p}}\right)$ está bien definido.

3. Basta evaluar el símbolo de Artin en $\sqrt[n]{a}$, entonces

$$\begin{aligned} \left(\frac{L/K}{\mathfrak{p}}\right) (\sqrt[n]{a}) &\equiv \sqrt[n]{a}^{\|\mathfrak{p}\|} \pmod{\mathfrak{P}} \\ &\equiv a^{(\|\mathfrak{p}\|-1)/n} \sqrt[n]{a} \pmod{\mathfrak{P}}. \end{aligned}$$

Por definición del símbolo de Legendre para la n -ésima potencia se tiene que

$$a^{(\|\mathfrak{p}\|-1)/n} \equiv \left(\frac{a}{\mathfrak{p}}\right)_n \pmod{\mathfrak{p}},$$

pero como $\mathfrak{p} \subseteq \mathfrak{P}$, entonces

$$a^{(\|\mathfrak{p}\|-1)/n} \equiv \left(\frac{a}{\mathfrak{p}}\right)_n \pmod{\mathfrak{P}},$$

y así,

$$\left(\frac{L/K}{\mathfrak{p}}\right) (\sqrt[n]{a}) \equiv \left(\frac{a}{\mathfrak{p}}\right)_n \sqrt[n]{a} \pmod{\mathfrak{P}}.$$

Por otro lado, $\left(\frac{L/K}{\mathfrak{p}}\right) (\sqrt[n]{a})$ es igual a $\sqrt[n]{a}$ veces una raíz n -ésima de la unidad, pero las raíces n -ésimas de la unidad son diferentes en $\mathcal{O}_L/\mathfrak{P}$, esto es consecuencia de que las raíces n -ésimas de la unidad están en \mathcal{O}_K y $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$. Luego, se concluye que

$$\left(\frac{L/K}{\mathfrak{p}}\right) (\sqrt[n]{a}) = \left(\frac{a}{\mathfrak{p}}\right)_n \sqrt[n]{a}.$$

□

Observación 3.5.1. Sean $n \geq 2$, K un cuerpo numérico que contiene a ζ_n , y $a \in \mathcal{O}_K$ no nulo. Además, sea \mathfrak{m} un módulo en K divisible por todos los ideales primos de \mathcal{O}_K que contienen a na .

El símbolo de Legendre para la n -ésima potencia induce un el homomorfismo de grupos

$$\begin{aligned} \left(\frac{a}{\cdot}\right)_n : I_K(\mathfrak{m}) &\rightarrow \mu_n \\ \mathfrak{b} &\mapsto \left(\frac{a}{\mathfrak{b}}\right)_n := \left(\frac{a}{\mathfrak{b}}\right)_n \end{aligned}$$

donde $\mu_n \subseteq \mathbb{C}^*$ es el grupo de raíces n -ésimas de la unidad.

Además, si $L = K(\sqrt[n]{a})$, la proposición anterior implica que L es una extensión de Galois de K , y dado que $\sigma \in \text{Gal}(L/K)$ está determinado por $\sqrt[n]{a}$, entonces

$$\sigma(\sqrt[n]{a}) = \sqrt[n]{a} \zeta_n^i \text{ para algún } 0 \leq i \leq n-1.$$

así, defínase el homomorfismo de grupos

$$\begin{aligned} \theta : \text{Gal}(L/K) &\rightarrow \mu_n \\ \sigma &\mapsto \theta(\sigma) := \zeta_n^i. \end{aligned}$$

Además, θ es inyectivo. En efecto, sea $\sigma \in \text{Ker}(\theta)$, entonces $\theta(\sigma) = 1$, pero por definición se tiene que $\theta(\sigma) = \zeta_n^i$, esto implica que $\zeta_n^i = 1$, por la condición de i se tiene que $i = 0$, así, $\sigma(\sqrt[n]{a}) = \sqrt[n]{a}$, por lo tanto $\sigma = i_L$.

El siguiente teorema es llamado Ley de Reciprocidad Débil ya que no brinda una fórmula para calcular el símbolo de Legendre para la n -ésima potencia, pero su importancia radica en el hecho de que este relaciona el homomorfismo de Artin con el símbolo de Legendre, y

por lo tanto, relaciona el teorema de Artin con la ley de reciprocidad.

De modo que, gracias a este teorema, el teorema de Artin es considerado como la ley de reciprocidad mas general.

Teorema 3.5.1 (Ley de Reciprocidad Débil). Sean $n \geq 2$, K un cuerpo numérico que contiene a ζ_n , y $a \in \mathcal{O}_K$ no nulo. Sean $L = K(\sqrt[n]{a})$ y \mathfrak{m} un módulo en K divisible por todos los ideales primos de \mathcal{O}_K que contienen a na .

Si $\text{Ker}(\Phi_{L/K, \mathfrak{m}})$ es un subgrupo de congruencia (mod \mathfrak{m}), entonces el siguiente diagrama

$$\begin{array}{ccc} I_K(\mathfrak{m}) & \xrightarrow{\Phi_{L/K, \mathfrak{m}}} & \text{Gal}(L/K) \\ & \searrow \left(\frac{a}{\cdot}\right)_n & \downarrow \theta \\ & & \mu_n \end{array}$$

es conmutativo. Además, se induce un homomorfismo sobreyectivo

$$\overline{\left(\frac{a}{\cdot}\right)_n} : I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m}) \longrightarrow G$$

donde $G := \theta(\text{Gal}(L/K)) \subseteq \mu_n$.

Demostración. Sea $\mathfrak{b} \in I_K(\mathfrak{m})$, entonces

$$\mathfrak{b} = \prod_{i=1}^t \mathfrak{p}_i^{r_i},$$

donde para cada $1 \leq i \leq t$ se tiene que \mathfrak{p}_i es un ideal primo de \mathcal{O}_K tal que $na \notin \mathfrak{p}_i$ y $r_i \in \mathbb{Z}$ es no nulo.

De modo que

$$\left(\frac{a}{\cdot}\right)_n(\mathfrak{b}) = \left(\frac{a}{\mathfrak{b}}\right)_n = \prod_{i=1}^t \left(\frac{a}{\mathfrak{p}_i}\right)_n^{r_i}.$$

Por otro lado, la proposición anterior implica que para cada $1 \leq i \leq t$ se tiene que

$$\left(\frac{L/K}{\mathfrak{p}_i}\right)(\sqrt[n]{a}) = \left(\frac{a}{\mathfrak{p}_i}\right)_n^{\sqrt[n]{a}},$$

luego,

$$\theta\left(\left(\frac{L/K}{\mathfrak{p}_i}\right)\right) = \left(\frac{a}{\mathfrak{p}_i}\right)_n,$$

así, se obtiene que

$$\begin{aligned}
(\theta \circ \Phi_{L/K, \mathfrak{m}})(\mathfrak{b}) &= (\theta \circ \Phi_{L/K, \mathfrak{m}}) \left(\prod_{i=1}^t \mathfrak{p}_i^{r_i} \right) \\
&= \prod_{i=1}^t (\theta \circ \Phi_{L/K, \mathfrak{m}})(\mathfrak{p}_i)^{r_i} \\
&= \prod_{i=1}^t \theta \left(\left(\frac{L/K}{\mathfrak{p}_i} \right) \right)^{r_i} \\
&= \prod_{i=1}^t \left(\frac{a}{\mathfrak{p}_i} \right)_n^{r_i}.
\end{aligned}$$

Por lo tanto, se concluye que el diagrama es conmutativo.

Para la última parte del teorema, el teorema de Artin implica que el homomorfismo de Artin

$$\Phi_{L/K, \mathfrak{m}} : I_K(\mathfrak{m}) \longrightarrow \text{Gal}(L/K)$$

es sobreyectivo, y puesto que $P_{K,1}(\mathfrak{m}) \subseteq \text{Ker}(\Phi_{L/K, \mathfrak{m}}) \subseteq I_K(\mathfrak{m})$, entonces

$$\begin{aligned}
\overline{\Phi}_{L/K, \mathfrak{m}} : I_K(\mathfrak{m}) / \text{Ker}(\Phi_{L/K, \mathfrak{m}}) &\rightarrow \text{Gal}(L/K) \\
\overline{\mathfrak{b}} &\mapsto \overline{\Phi}_{L/K, \mathfrak{m}}(\overline{\mathfrak{b}}) := \Phi_{L/K, \mathfrak{m}}(\mathfrak{b})
\end{aligned}$$

es un isomorfismo de grupos, además, el homomorfismo

$$\begin{aligned}
\varphi : I_K(\mathfrak{m}) / P_{K,1}(\mathfrak{m}) &\rightarrow I_K(\mathfrak{m}) / \text{Ker}(\Phi_{L/K, \mathfrak{m}}) \\
\overline{\mathfrak{b}} &\mapsto \varphi(\overline{\mathfrak{b}}) := \overline{\mathfrak{b}}
\end{aligned}$$

es sobreyectivo. De modo que, el homomorfismo

$$\begin{aligned}
\theta \circ \overline{\Phi}_{L/K, \mathfrak{m}} \circ \varphi : I_K(\mathfrak{m}) / P_{K,1}(\mathfrak{m}) &\rightarrow G \\
\overline{\mathfrak{b}} &\mapsto (\theta \circ \overline{\Phi}_{L/K, \mathfrak{m}} \circ \varphi)(\overline{\mathfrak{b}}) = (\theta \circ \Phi_{L/K, \mathfrak{m}})(\mathfrak{b})
\end{aligned}$$

es sobreyectivo, usando la conmutatividad del diagrama se obtiene que el homomorfismo

$$\begin{aligned}
\overline{\left(\frac{a}{\cdot} \right)}_n : I_K(\mathfrak{m}) / P_{K,1}(\mathfrak{m}) &\rightarrow G \\
\overline{\mathfrak{b}} &\mapsto \overline{\left(\frac{a}{\cdot} \right)}_n(\overline{\mathfrak{b}}) = \left(\frac{a}{\cdot} \right)_n(\mathfrak{b})
\end{aligned}$$

es sobreyectivo. □

Notación 2. Sea $n = 2$, $a \in \mathbb{Z}$ no nulo y $p\mathbb{Z}$ un ideal primo de \mathbb{Z} donde $p \in \mathbb{Z}$ es primo impar, tal que $2a \notin p\mathbb{Z}$. El símbolo de Legendre cuadrático se va a denotar como en el capítulo anterior, es decir

$$\left(\frac{a}{p}\right) := \left(\frac{a}{p\mathbb{Z}}\right)_2.$$

Lema 3.5.1. *Sea $p \in \mathbb{Z}$ un primo impar fijo, el símbolo de Legendre cuadrático induce un homomorfismo sobreyectivo definido por*

$$\begin{aligned} \left(\frac{\cdot}{p}\right) : (\mathbb{Z}/p\mathbb{Z})^* &\rightarrow \{\pm 1\} \\ \bar{a} &\mapsto \left(\frac{\cdot}{p}\right)(\bar{a}) := \left(\frac{a}{p}\right). \end{aligned}$$

Demostración. La función $\left(\frac{\cdot}{p}\right)$ está bien definida: Supóngase que $\bar{a} = \bar{b}$ en $(\mathbb{Z}/p\mathbb{Z})^*$, entonces $a - b \in p\mathbb{Z}$ y $\text{mcd}(a, p) = 1 = \text{mcd}(b, p)$, de modo que $a \equiv b \pmod{p}$, y así

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

Además, $\left(\frac{\cdot}{p}\right)$ es un homomorfismo de grupos. En efecto, sean $\bar{a}, \bar{b} \in (\mathbb{Z}/p\mathbb{Z})^*$, entonces

$$\left(\frac{\cdot}{p}\right)(\bar{a}\bar{b}) = \left(\frac{\cdot}{p}\right)(\bar{a}\bar{b}) = \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{\cdot}{p}\right)(\bar{a})\left(\frac{\cdot}{p}\right)(\bar{b}).$$

Por último, $\left(\frac{\cdot}{p}\right)$ es sobreyectivo. Esto es consecuencia del hecho que existen $\frac{p-1}{2}$ residuos cuadráticos módulo p y $\frac{p-1}{2}$ no residuos cuadráticos módulo p . \square

A continuación, se presenta una demostración de la ley de reciprocidad cuadrática usando la ley de reciprocidad débil, de esta manera, la ley de reciprocidad cuadrática es una consecuencia del teorema de Artin. Esta demostración se basa en la referencia [7].

Teorema 3.5.2 (Ley de Reciprocidad Cuadrática). *Sean p y q primos impares diferentes. Entonces*

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

Demostración. Sea $L := \mathbb{Q}(\zeta_p)$ un cuerpo ciclotómico, en la primera parte de la sección 2.5.2 se probó que existe un único cuerpo cuadrático $K = \mathbb{Q}(\sqrt{p^*})$ que está contenido en L y en donde $p^* = (-1)^{\frac{p-1}{2}}$. Además, K es una extensión de Galois abeliana de \mathbb{Q} .

Sea $m = p\infty$ un módulo en \mathbb{Q} , donde ∞ es el primo real infinito de \mathbb{Q} . Ya que p es el único primo de \mathbb{Z} que ramifica en K , el homomorfismo de Artin $\Phi_{K/\mathbb{Q}, m}$ está bien definido.

Por otro lado, el ejemplo 3.4.1 implica que $\text{Ker}(\Phi_{L/Q,m}) = P_{Q,1}(\mathfrak{m})$, y se tiene el isomorfismo

$$\bar{\Phi}_{L/Q,m} : I_Q(\mathfrak{m})/P_{Q,1}(\mathfrak{m}) \longrightarrow (\mathbb{Z}/p\mathbb{Z})^*,$$

dado por

$$\bar{\Phi}_{L/Q,m} \left(\overline{\frac{a}{b}\mathbb{Z}} \right) := \bar{a}\bar{b}^{-1}.$$

Por otro lado

$$\begin{aligned} \Theta : (\mathbb{Z}/p\mathbb{Z})^* &\rightarrow I_Q(\mathfrak{m})/P_{Q,1}(\mathfrak{m}) \\ \bar{a} &\mapsto \Theta(\bar{a}) := \bar{a}\mathbb{Z} \end{aligned}$$

resulta ser el homomorfismo inverso de $\bar{\Phi}_{L/Q,m}$.

Primero, Θ es una función bien definida. Supóngase que $\bar{a} = \bar{b}$ en $(\mathbb{Z}/p\mathbb{Z})^*$, entonces $a - b \in p\mathbb{Z}$ y $\text{mcd}(a, p) = 1 = \text{mcd}(b, p)$, así, $\frac{a}{b} \in \mathbb{Q}_m$. También, se puede suponer que $\frac{a}{b} > 0$, y puesto que $a - b \in p\mathbb{Z}$ y $b \notin p\mathbb{Z}$ entonces

$$\frac{a}{b} \equiv^* 1 \pmod{p\mathbb{Z}},$$

esto implica que

$$\frac{a}{b} \equiv^* 1 \pmod{\mathfrak{m}}.$$

Por lo tanto $\frac{a}{b} \in \mathbb{Q}_{m,1}$, y así

$$\frac{a}{b}\mathbb{Z} \in P_{Q,1}(\mathfrak{m}),$$

de esto se concluye que $\bar{a}\mathbb{Z} = \bar{b}\mathbb{Z}$, es decir, $\Theta(\bar{a}) = \Theta(\bar{b})$.

Además,

$$(\bar{\Phi}_{L/Q,m} \circ \Theta)(\bar{a}) = \bar{\Phi}_{L/Q,m}(\bar{a}\mathbb{Z}) = \bar{a} = i_{(\mathbb{Z}/p\mathbb{Z})^*}(\bar{a}),$$

para cada $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^*$, y

$$(\Theta \circ \bar{\Phi}_{L/Q,m}) \left(\overline{\frac{a}{b}\mathbb{Z}} \right) = \Theta(\bar{a}\bar{b}^{-1}) = \frac{a}{b}\mathbb{Z} = i_{I_Q(\mathfrak{m})/P_{Q,1}(\mathfrak{m})} \left(\overline{\frac{a}{b}\mathbb{Z}} \right)$$

para cada $\overline{\frac{a}{b}\mathbb{Z}} \in I_Q(\mathfrak{m})/P_{Q,1}(\mathfrak{m})$. Esto implica que Θ es un isomorfismo de grupos.

De esto resulta que $P_{Q,1}(\mathfrak{m}) \subseteq \text{Ker}(\Phi_{K/Q,m})$.

En efecto, sea $\frac{a}{b}\mathbb{Z} \in P_{Q,1}(\mathfrak{m})$, el lema 2.6.1 implica que

$$\Phi_{K/Q,m} = r \circ \Phi_{L/Q,m},$$

donde

$$r : \text{Gal}(L/Q) \longrightarrow \text{Gal}(K/Q)$$

es el homomorfismo restricción, entonces

$$(r \circ \Phi_{L/\mathbb{Q}, \mathfrak{m}}) \left(\frac{a}{b} \mathbb{Z} \right) = r(i_L) = i_K,$$

así,

$$\frac{a}{b} \mathbb{Z} \in \text{Ker}(\Phi_{K/\mathbb{Q}, \mathfrak{m}}),$$

de esto se concluye que $P_{\mathbb{Q}, 1}(\mathfrak{m}) \subseteq \text{Ker}(\Phi_{K/\mathbb{Q}, \mathfrak{m}})$, esto es, $\text{Ker}(\Phi_{K/\mathbb{Q}, \mathfrak{m}})$ es un subgrupo de congruencia ($\text{mod } \mathfrak{m}$).

Aplicando el teorema de la ley de reciprocidad débil se induce un homomorfismo sobreyectivo

$$\overline{\left(\frac{p^*}{\cdot} \right)} : I_{\mathbb{Q}}(\mathfrak{m}) / P_{\mathbb{Q}, 1}(\mathfrak{m}) \longrightarrow \{\pm 1\}$$

dado por $\overline{\left(\frac{p^*}{\cdot} \right)}(\bar{\mathfrak{b}}) = \left(\frac{p^*}{\cdot} \right)(\mathfrak{b})$.

Luego, la composición

$$\overline{\left(\frac{p^*}{\cdot} \right)} \circ \Theta : (\mathbb{Z}/p\mathbb{Z})^* \longrightarrow \{\pm 1\}$$

es un homomorfismo sobreyectivo.

El lema anterior implica que el homomorfismo

$$\left(\frac{\cdot}{p} \right) : (\mathbb{Z}/p\mathbb{Z})^* \rightarrow \{\pm 1\}$$

$$\bar{a} \mapsto \left(\frac{\cdot}{p} \right)(\bar{a}) := \left(\frac{a}{p} \right).$$

es sobreyectivo.

Puesto que $(\mathbb{Z}/p\mathbb{Z})^*$ es cíclico, solo hay dos homomorfismos de grupos de $(\mathbb{Z}/p\mathbb{Z})^*$ en $\{\pm 1\}$, y solo uno de ellos es sobreyectivo. Esto implica que

$$\left(\frac{\cdot}{p} \right) = \overline{\left(\frac{p^*}{\cdot} \right)} \circ \Theta.$$

De modo que, si $q \in \mathbb{Z}$ es un primo impar distinto de p , entonces $\bar{q} \in (\mathbb{Z}/p\mathbb{Z})^*$, y por lo tanto

$$\left(\frac{\cdot}{p} \right)(\bar{q}) = \left(\overline{\left(\frac{p^*}{\cdot} \right)} \circ \Theta \right)(\bar{q}),$$

así,

$$\begin{aligned}\left(\frac{q}{p}\right) &= \overline{\left(\frac{p^*}{\cdot}\right)}(q\mathbb{Z}) \\ &= \left(\frac{p^*}{\cdot}\right)(q\mathbb{Z}) \\ &= \left(\frac{p^*}{q}\right).\end{aligned}$$

De esto se concluye que

$$\begin{aligned}\left(\frac{q}{p}\right) &= \left(\frac{p^*}{q}\right) \\ &= \left(\frac{(-1)^{\frac{p-1}{2}} p}{q}\right) \\ &= \left(\frac{-1}{q}\right)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \\ &= (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{p}{q}\right).\end{aligned}$$

Esto prueba la ley de reciprocidad cuadrática. \square

En [7] se introduce el símbolo de Hilbert y sus propiedades, y usando la ley de reciprocidad débil se demuestra la ley de reciprocidad fuerte. A partir de esto se prueba la ley de reciprocidad cúbica y bicuadrática.

En este sentido, de la ley de reciprocidad de Artin se deducen las demás leyes de reciprocidad.

BIBLIOGRAFÍA

- [1] S. Alaca and K. S. Williams, *Introductory algebraic number theory*, Cambridge University Press, Cambridge, 2004.
- [2] E. Artin, *Algebra with Galois theory*, reprint of the 1947 original [*Modern higher algebra. Galois theory*, Courant Inst. Math. Sci., New York], Courant Lecture Notes in Mathematics, 15, Courant Institute of Mathematical Sciences, New York, 2007.
- [3] E. Artin and J. Tate, *Class field theory*, AMS Chelsea Publishing, Providence, RI, 2009.
- [4] E. Artin, *Über eine neue Art von L-Reihen*, Abh. Math. Sem. Univ Hamburg. (1923).
- [5] J. Booher, *Reciprocity laws*, <https://www.math.canterbury.ac.nz/j.booyer/expos/reciprocity.pdf>, 2013
- [6] N. Childress, *Class field theory*, Universitext, Springer, New York, 2009.
- [7] D. A. Cox, *Primes of the form $x^2 + ny^2$* , A Wiley-Interscience Publication, John Wiley & Sons, Inc., New York, 1989.
- [8] J. Dieudonné, The historical development of algebraic geometry, Amer. Math. Monthly **79** (1972).
- [9] J. Esmonde and M. Ram Murty, *Problems in algebraic number theory*, Graduate Texts in Mathematics, 190, Springer-Verlag, New York, 1999.
- [10] T. W. Hungerford, *Algebra*, reprint of the 1974 original, Graduate Texts in Mathematics, 73, Springer-Verlag, New York, 1980.
- [11] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, second edition, Graduate Texts in Mathematics, 84, Springer-Verlag, New York, 1990.
- [12] C. Ivorra Castillo, *Teoría de cuerpos de clases*, <https://www.uv.es/ivorra/Libros/Cuerpos.pdf>.
- [13] G. J. Janusz, *Algebraic number fields*, second edition, Graduate Studies in Mathematics, 7, American Mathematical Society, Providence, RI, 1996.

- [14] S. Lang, *Algebra*, revised third edition, Graduate Texts in Mathematics, 211, Springer-Verlag, New York, 2002.
- [15] S. Lang, *Algebraic number theory*, second edition, Graduate Texts in Mathematics, 110, Springer-Verlag, New York, 1994.
- [16] F. Lemmermeyer, *Reciprocity laws*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000.
- [17] D. A. Marcus, *Number fields*, Springer-Verlag, Berlin, Heidelberg, New York, 1977.
- [18] *Mathematical developments arising from Hilbert problems*, Proceedings of Symposia in Pure Mathematics, Vol. XXVIII, American Mathematical Society, Providence, RI, 1976.
- [19] J. S. Milne, *Algebraic Number Theory*, v3.08, <https://www.jmilne.org/math/CourseNotes/ANT.pdf>, 2020.
- [20] J. Neukirch, *Algebraic number theory*, Springer-Verlag, Berlin Heidelberg, 1999.
- [21] P. Ribenboim, *Algebraic numbers*, Wiley-Interscience, New York, 1972.
- [22] P. Ribenboim, *Classical theory of algebraic numbers*, Universitext, Springer-Verlag, New York, 2001.
- [23] P. Samuel, *Algebraic theory of numbers*, Translated from the French by Allan J. Silberger, Houghton Mifflin Co., Boston, MA, 1970.
- [24] N. Snyder, *Artin's L-functions: A Historical Approach*, 2002.
- [25] P. Stevenhagen, The arithmetic of number rings, in *Algorithmic number theory: lattices, number fields, curves and cryptography*, 209–266, Math. Sci. Res. Inst. Publ., 44, Cambridge Univ. Press, Cambridge.
- [26] I. Stewart and D. Tall, *Algebraic number theory and Fermat's last theorem*, third edition, A K Peters, Ltd., Natick, MA, 2002.
- [27] M. Trifković, *Algebraic theory of quadratic numbers*, Universitext, Springer, New York, 2013.
- [28] B. F. Wyman, *What is a reciprocity law?*, Amer. Math. Monthly **79** (1972), 571–586; correction, *ibid.* **80** (1973), 281.