TEORÍA ALGEBRAICA DE NÚMEROS

Universidad de Oviedo

Facultad de Ciencias

Daira Pinto Prieto

Tutora

Consuelo Martínez López

2016 - 2017

TEORÍA ALGEBRAICA DE NÚMEROS

HACIA UNA LEY DE RECIPROCIDAD GENERAL

Trabajo de fin de grado

Matemáticas

Agradecimientos

En primer lugar, quiero expresar mi agradecimiento a la Profesora Dra. Consuelo Martínez López por su paciencia y disposición, así como por sus orientaciones y consejos ya que han sido una guía inestimable durante todo el proyecto.

También quiero agradecer al Dr. Lucio Guerberoff, al Profesor Dr. Juan Ramón Delgado Pérez y al Profesor Dr. Carlos Ivorra Castillo la ayuda que tan amablemente me han brindado.

Por otro lado, me gustaría hacer una mención especial al Departamento de Matemáticas de la Universidad de León, al que agradezco profundamente el que haya puesto su biblioteca a mi plena disposición.

Por último, quiero dar las gracias a mi familia, amigos y amigas por todo el apoyo y cariño que me han demostrado a lo largo de la elaboración de este trabajo.

A todos, muchas gracias.

Índice general

Introducción I

1 Marco teórico 1
- 1.1 Estructuras algebraicas . . . 1
- 1.2 Localización . . . 4
- 1.3 Enteros algebraicos . . . 7
- 1.4 Norma de una extensión de cuerpos . . . 8
- 1.5 Anillos de Dedekind . . . 9
- 1.6 Grupo de clases . . . 18
- 1.7 Valoraciones . . . 19
- 1.8 Grupo de descomposición y grupo de inercia . . . 26
- 1.9 Grupo radial . . . 27

2 Motivación e Historia 31
- 2.1 La ley de reciprocidad cuadrática . . . 32
- 2.2 Otras leyes de reciprocidad . . . 36
- 2.3 Emil Artin . . . 41

3 La ley de reciprocidad de Artin 47
- 3.1 Teoría de cuerpos de clases . . . 47
  - 3.1.1 Historia . . . 48
  - 3.1.2 Teoremas principales . . . 53
- 3.2 Teorema de Artin . . . 58
  - 3.2.1 Una ley de reciprocidad general . . . 63
- 3.3 Aplicaciones . . . 65

Conclusiones 67

Índice alfabético 68

Bibliografía 71

Introducción

La teoría algebraica de números es, según la *Encyclopedia of Mathematics*, una «rama de la teoría de números cuyo principal objetivo es estudiar las propiedades de los enteros algebraicos de un cuerpo de números». En un primer curso de esta disciplina o en cualquier libro introductorio a la misma, se suele empezar estudiando los anillos de enteros, los anillos de Dedekind, el concepto de ramificación y de inercia, y el teorema de Kronecker-Weber, entre otras cosas. Además, es bastante común dedicar cierto tiempo a la conocida como «ley de reciprocidad cuadrática», una ley que establece, a grandes rasgos, una relación recíproca entre dos primos. Llegados a este punto de la asignatura, es fácil que se haga referencia al libro de Lemmermeyer «Leyes de reciprocidad: Desde Euler hasta Eisenstein», en el cual el autor hace un exhaustivo estudio de las leyes de reciprocidad publicadas entre 1741 y 1850. Sin embargo, una de las cosas que más llama la atención en un primer momento no se encuentra en el cuerpo del libro sino en sus apéndices: aparte de una lista de problemas abiertos y un *dramatis personae*, en uno de estos apéndices aparece una lista de 196 demostraciones de la ley de reciprocidad cuadrática, que van desde una prueba (incompleta) de Legendre en 1788 hasta una prueba del propio Lemmermeyer del año 2000.

Es comprensible que una lista como esta provoque cierto efecto llamada, de forma que llegue un momento en que la motivación para buscar una prueba alternativa de la ley de reciprocidad cuadrática sea justamente formar parte de dicha lista (en `https://www.rzuser.uni-heidelberg.de/~hb3/rchrono.html`, en mayo de 2017, hemos encontrado una lista de 246 pruebas, la última del año 2013). Pero, en un principio,

¿por qué invertir el tiempo en demostrar algo que ya se sabe que es cierto?

No es difícil encontrar la respuesta a esta pregunta: la ley de reciprocidad cuadrática es un resultado de gran utilidad, por lo que tener una ley de reciprocidad general, es decir, de la que la ley de reciprocidad cuadrática, cúbica, bicuadrática o de cualquier orden que queramos sean casos particulares, permitiría avanzar a pasos agigantados en ciertas direcciones de la teoría. Por lo menos, eso era lo que esperaban aquellos que aparecen en las primeras entradas de la lista de Lemmermeyer, y por este motivo trataban de encontrar una demostración de la ley de reciprocidad cuadrática fácilmente generalizable.

La pregunta que sigue a esta explicación no puede ser otra sino si, finalmente, encontraron esa ley de reciprocidad que tanto buscaban.

¿Existe entonces una ley de reciprocidad general?

El objetivo de este trabajo es precisamente dar repuesta a esta pregunta; o más que dar respuesta, que ya adelantamos que es afirmativa, nuestro objetivo va a ser comprender la magnitud del problema y aproximarnos tanto como sea posible a dicha ley.

Decimos «aproximarnos» porque el enunciado explícito de esa ley de reciprocidad general surge de combinar diferentes teorías sobre cuerpos de funciones, curvas elípticas o multiplicación compleja en las que no podemos profundizar en este trabajo. No obstante, sí que podemos enunciar el teorema del que se deduce dicha ley y el que históricamente puso punto final a la búsqueda de leyes de reciprocidad. Se trata del teorema de Artin, un teorema enmarcado en la teoría de cuerpos de clases que establece un isomorfismo entre cierto grupo cociente de clases de ideales de una extensión de un cuerpo de números y su grupo de Galois.

Además, aunque nosotros hayamos llegado a este resultado buscando una ley de reciprocidad general, lo cierto es que el teorema de Artin es uno de los pilares de la teoría de cuerpos de clases por lo que nos hemos detenido brevemente a esbozar las bases de su demostración y a conocer las aplicaciones que se le pueden dar fuera y dentro de las matemáticas. En definitiva, en este trabajo vamos a desarrollar fundamentalmente tres puntos: la base teórica que nos va a permitir plantear y responder si existe o no una ley de reciprocidad general, la motivación histórica que justifica la trascendencia de esta pregunta y la presentación del resultado teórico del que se desprende su respuesta.

En el **primer capítulo** daremos las definiciones y resultados necesarios para seguir el progreso del trabajo. En él haremos especial hincapié en las ventajas que supone en este contexto trabajar con anillos de Dedekind y extensiones de Galois.

En el **segundo capítulo** hacemos un breve recorrido histórico desde Gauss, primera persona conocida que se preocupó por la generalización de las leyes de reciprocidad, hasta Artin, matemático que enunciaría y demostraría el teorema que permite dicha generalización. De hecho, reservamos una sección a su biografía.

Por último, en el **tercer capítulo** contextualizaremos y enunciaremos el teorema de Artin. Las últimas secciones de este capítulo están dedicadas, como ya hemos mencionado, a discutir su demostración y a recopilar algunas de sus aplicaciones.

Capítulo 1

Marco teórico

Uno de los principales objetivos del presente trabajo es mostrar el camino recorrido por la comunidad matemática para demostrar y generalizar las conocidas como « leyes de reciprocidad». Es por ello, que a lo largo de su desarrollo se ha dado prioridad a la exposición y explicación de los resultados, dejando indicado dónde se pueden encontrar las demostraciones. Sin embargo, en este primer capítulo hacemos una excepción. Para poder valorar ampliamente la trascendencia de la ley de reciprocidad de Artin, conviene tener en cuenta los pilares teóricos en los que se sustenta. Este planteamiento es el que nos lleva a dedicar el capítulo 1 a su recopilación, y a detenernos en la demostración de los resultados especialmente fundamentales.

1.1. Estructuras algebraicas

En primer lugar, vamos a recorrer brevemente las distintas estructuras algebraicas que necesitaremos para introducir el lenguaje de la teoría algebraica de números. En general, las consideraremos conocidas y por tanto no nos detendremos en su estudio.

Decimos que A es un **anillo** si es un conjunto con dos operaciones internas $+, \cdot$ tales que $(A, +)$ es un grupo abeliano y la operación $\cdot$ cumple la propiedad asociativa y distributiva respecto a $+$ a derecha e izquierda. Si además $\cdot$ es conmutativa o tiene elemento neutro se tiene un **anillo conmutativo** o un **anillo unitario** respectivamente. Recordemos también que un **cuerpo** es un anillo $(K, +, \cdot)$ tal que $(K, +)$ y $(K\backslash\{0\}, \cdot)$ son grupos abelianos.

Definición 1.1.1. *Dado $(A, +, \cdot)$ un anillo y $0 \neq a \in A$, se dice que a es* ***divisor de 0 a izquierda (respectivamente a derecha)*** *si existe un $0 \neq b \in A$ tal que $a \cdot b = 0$ (respectivamente $b \cdot a = 0$). Si $(A, +, \cdot)$ es un anillo conmutativo, con identidad y sin divisores de cero, se llama* ***dominio de integridad*** *. El* ***cuerpo de fracciones*** *de un dominio de integridad A dado es el menor cuerpo que contiene a A.*

A partir de ahora todos los anillos que se consideren serán anillos conmutativos con identidad.

Definición 1.1.2. *Sea $(A,+,\cdot)$ un anillo, y $(\mathfrak{i},+,\cdot)$ un subanillo de A. El subanillo $\mathfrak{i}$ es un* ***ideal*** *de A si $xy \in \mathfrak{i}\ \forall x \in A,\ y \in \mathfrak{i}$. Si $\mathfrak{i}$ es un ideal generado por un único elemento, se dice* ***ideal principal****. Se llama* ***dominio de ideales principales*** *a un dominio de integridad donde todo ideal es principal. Se dice que $\mathfrak{m}$ es un* ***ideal maximal*** *si para todo $\mathfrak{i}$ ideal de A que contiene a $\mathfrak{m}$ se cumple que $\mathfrak{i} = A$ o $\mathfrak{i} = \mathfrak{m}$ y se llama* ***ideal primo*** *a un ideal $\mathfrak{p}$ tal que dados $x, y \in A$ se cumple que $x \cdot y \in \mathfrak{p} \ \Rightarrow\ x \in \mathfrak{p}$ o $y \in \mathfrak{p}$. Por último, el conjunto*

$$U(A) := \{x \ \in \ A \mid \exists\ x^{-1} :\ xx^{-1} = x^{-1}x = 1_A\}.$$

es un subgrupo de A y recibe el nombre de ***grupo de unidades*** *de A.*

Además, conviene recordar el siguiente resultado sobre anillos con identidad:

Teorema 1.1.1. ***Teorema chino de los restos.*** *Sea B un anillo con identidad y $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ un conjunto de ideales de B tales que $B = \mathfrak{q}_i + \mathfrak{q}_j$ para $i \neq j$. Entonces*

$$\frac{B}{\mathfrak{i}} \ \cong\ \frac{B}{\mathfrak{q}_1} \oplus \cdots \oplus \frac{B}{\mathfrak{q}_n}$$

con $\mathfrak{i} = \bigcap_i \mathfrak{q}_i$ bajo el isomorfismo que lleva cada $b + \mathfrak{i} \in \frac{B}{\mathfrak{i}}$ a $(b + \mathfrak{q}_1, \ldots, b + \mathfrak{q}_n)$.

Por otra parte, dado un anillo A y un grupo abeliano M se dice que $(M,+)$ es un **A-módulo** si existe una operación externa de $A \times M$ en M, que denotaremos por yuxtaposición, tal que dados $m, n \in M$ se verifique que

- $(a+b)m = am + bm\ \forall\ a,\ b\ \in\ A$,
- $a(m+n) = am + an\ \forall\ a\ \in\ A$,
- $(ab)m = a(bm)\ \forall\ a,\ b\ \in\ A$.

Si además A es un anillo con identidad 1_A entonces se llamará **A-módulo unitario** a un A-módulo M tal que $1_A \cdot m = m$ para todo $m \in M$. Dado un anillo con identidad A y un A-módulo unitario se dice que $S \subseteq M$ es un **sistema generador** de M si $A\langle S\rangle = M$, es decir, si para todo $m \in M$ existen $s_1, \ldots, s_n \in S$ y $r_1, \ldots, r_n \in A$ tales que $m = r_1 s_1 + \cdots + r_n s_n$. En las mismas condiciones, el conjunto S se dirá **A-libre** si $r_1 s_1 + \cdots + r_n s_n = 0$ implica que $r_1 = \cdots = r_n = 0$ para $r_i \in A$, $s_i \in S$. Por último, se llama **base** de un A-módulo a un conjunto S que sea sistema generador de dicho módulo y A-libre, y se dice **módulo libre** a un A-módulo unitario que admita una base.

Extensiones de Galois

Definición 1.1.3. *Dada una extensión de cuerpos L/K llamaremos* ***grupo de Galois*** *de L/K al conjunto de K-automorfismos de L. Lo denotaremos por $Gal(L/K)$. Para cada cuerpo intermedio F, $Gal(L/F) := \{\sigma \in Gal(L/K) \mid \sigma(x) = x,\ \forall x \in F\}$ es un subgrupo*

de $Gal(L/K)$ y para cada subgrupo H de $Gal(L/K)$, $H^* := \{x \in L \mid \sigma(x) = x,\ \forall \sigma \in H\}$ es un subcuerpo de L que contiene a K. A H^* se le llamará ***cuerpo fijo de*** *H. Una extensión L/K se dirá* ***extensión de Galois*** *si $Gal(L/K)^* = K$, y se dirá* ***extensión abeliana*** *si es de Galois y $Gal(L/K)$ es un grupo abeliano.*

Antes de recordar dos caracterizaciones muy útiles de ciertas extensiones de Galois, vamos a recopilar algunos conceptos referentes a una extensión de cuerpos L/K dada:

- Diremos que es una **extensión finita** si la dimensión de L sobre K, o grado de la extensión, es finita.
- Se considerará una **extensión simple** si existe algún elemento $\alpha \in L$ tal que L es un cuerpo generado por K y α, es decir, $L = K(\alpha)$.
- Un elemento α de L se dirá **algebraico sobre** K si existe un polinomio no nulo $p \in K[X]$ tal que $p(\alpha) = 0$. En caso contrario, se dirá que α es un **elemento trascendente** . Llamaremos **polinomio mínimo de α sobre** K al polinomio mónico de menor grado del que α es raíz. Por su parte, la extensión L/K se dirá **algebraica** si todo elemento $\alpha \in L$ es algebraico sobre K.
- Dado un cuerpo K, diremos que un polinomio $p \in K[X]$ se **escinde** en K si existen $\lambda, \alpha_1, \alpha_n \in K$ tales que
$$p = \lambda(X - \alpha_1) \cdots (X - \alpha_n).$$
Diremos que L es el **cuerpo de escisión** de un polinomio $p \in K[X]$ si es el menor cuerpo en el que p se escinde. En cuanto a la extensión, diremos que es **normal** si todo polinomio $p \in K[X]$ irreducible que tenga una raíz en L se escinde en L.
- Dado un cuerpo K y un polinomio irreducible $p \in K[X]$ decimos que dicho p es **separable sobre** K si no tiene raíces múltiples en ninguna extensión de K en la que se escinda. Dado un elemento α de L algebraico sobre K, diremos que α es **separable sobre** K si su polinomio mínimo sobre K es separable sobre K. A su vez, diremos que la extensión L/K es **separable** si todo elemento de L es separable sobre K.

Conviene recordar también el conocido como *teorema del elemento primitivo* sobre extensiones de cuerpos ya que juega un relevante papel en la teoría de Galois.

Teorema 1.1.2. ***Teorema del elemento primitivo.*** *Toda extensión de cuerpos finita y separable es simple.*

Con todo ello, estamos en condiciones de comprender las siguientes caracterizaciones, que debemos tener presentes a lo largo del trabajo.

Proposición 1.1.1. *Una extensión finita de cuerpos L/K es de Galois si y solo si es normal y separable.*

Proposición 1.1.2. *Una extensión finita de cuerpos L/K es de Galois si y solo si* $[L : K] =| Gal(L/K) |$.

En particular, si L/K es una extensión finita de Galois entonces, por el teorema del elemento primitivo, es una extensión simple, es decir, existe un elemento $\alpha \in L$ tal que $L = K(\alpha)$.

Évariste Galois fue un matemático francés que vivió entre los años 1811 y 1832 y da nombre a la teoría que acabamos de introducir. En los cinco años en los que pudo dedicarse a las matemáticas, hizo estudios sobre fracciones continuas, funciones elípticas e integrales abelianas, aunque destacó por su estudio sobre la resolución de ecuaciones. No fue hasta después de su muerte cuando estos manuscritos salieron a la luz de la mano de Joseph Liouville $(1809 - 1882)$ que dijo haber encontrado en ellos una solución « tan correcta como profunda de este entrañable problema: Dada una ecuación irreducible de grado primo, determinar si es o no resoluble por radicales.» [a]
Para nosotros, la teoría que se desarrolló a partir de las ideas de este joven matemático va a cobrar especial importancia, ya que la ley de reciprocidad de Artin está contextualizada en el estudio de extensiones finitas y abelianas de cuerpos. De hecho, las condiciones de normalidad y separabilidad de las extensiones que consideremos a lo largo del trabajo serán claves para poder obtener los resultados finales.

Figura 1.1: Dibujo de 1848 en memoria de E. Galois hecho por su hermano.

[a] `http://www-history.mcs.st-andrews.ac.uk/Biographies/Galois.html` Fecha de acceso: 21/02/2017.

1.2. Localización

Dados un dominio de integridad A y $S \subseteq A$, decimos que S es un **subconjunto multiplicativo de** A si no contiene al cero y es un conjunto cerrado para el producto. En este apartado consideraremos siempre $(A, +, \cdot)$ dominio de integridad y S un subconjunto multiplicativo de A.

Definición 1.2.1. *Sea la relación de equivalencia $\sim$ en $A \times S$ dado por $(a, s) \sim (b, t) \iff at = bs$. Entonces, llamamos* ***anillo de fracciones de*** *A* ***respecto a*** *S al conjunto*

cociente

$$A_S := \frac{A \times S}{\sim} = \{[(a,s)] : a \in A, s \in S\}.$$

El anillo A_S no solo tiene la estructura de dominio de integridad sino que además es el anillo más pequeño que contiene a A y a los inversos respecto al producto de todos los elementos de S.

Dados dos elementos de A_S, $[(a,s)]$ y $[(b,t)]$ (que denotaremos en adelante por $\frac{a}{s}$ y $\frac{b}{t}$ para simplificar la notación), definimos su suma como

$$\frac{a}{s} +^s \frac{b}{t} = \frac{(at+bs)}{st}$$

y su producto como

$$\frac{a}{s} \cdot^s \frac{b}{t} = \frac{a \cdot b}{s \cdot t}$$

Estas dos operaciones están bien definidas; son internas; $(A_S, +^s)$ es un grupo abeliano con elemento neutro $\frac{0}{s}$ para cualquier $s \in S$ y elemento inverso de $\frac{a}{s} = \frac{-a}{s}$; y $\frac{s}{s}$ es la identidad respecto al producto $\cdot^s$ para cualquier $s \in S$. Teniendo en cuenta las propiedades que se derivan del hecho de que A sea dominio de integridad, concluimos que A_S posee también dicha estructura respecto a las operaciones definidas. Por comodidad haremos un abuso de notación escribiendo $+^s$ y $\cdot^s$ como $+$ y $\cdot$ respectivamente.

Sea la aplicación

$$\begin{aligned} \varphi_s : A &\to A_S \\ a &\mapsto \frac{as}{s} \end{aligned}$$

Esta aplicación es un monomorfismo de anillos, con lo cual $A \subseteq A_S$. Además, A_S contiene el inverso respecto al producto de todos los elementos de S ya que dado $s \in S$, $s \cdot \frac{1}{s} = \frac{s}{1} \cdot \frac{1}{s} = \frac{s}{s}$.

Por último, tomemos B un dominio de integridad tal que $A \subseteq B$ y $\{s^{-1} | s \in S\} \subseteq B$, y ϕ un homomorfismo de anillos definido como

$$\begin{aligned} \phi_s : A_S &\to B \\ \frac{a}{s} &\mapsto a \cdot s^{-1} \end{aligned}$$

ϕ es un homomorfismo inyectivo ya que si $\phi\left(\frac{a}{s}\right) = \phi\left(\frac{b}{t}\right)$ implica que $a \cdot s^{-1} = b \cdot t^{-1}$ y por B anillo conmutativo $a \cdot t = c \cdot s$ y por lo tanto $\frac{a}{s} = \frac{b}{t}$. Con lo cual, B contiene a A_S y podemos concluir que A_S es el menor anillo que contiene a A y a los inversos de los elementos de S, es decir, A_S es el anillo generado por por A y $\{s^{-1} | s \in S\}$.

Proposición 1.2.1. *Sea A un dominio de integridad y S un subconjunto multiplicativo de A. Existe una correspondencia unívoca entre los ideales primos de A que tienen intersección*

vacía con S y los ideales primos de la localización A_S.

Así, un ideal primo $\mathfrak{p}$ de A se corresponde con el ideal primo $\mathfrak{p}A_S$.

Demostración:

Sea $\mathfrak{q}$ un ideal primo de A_S. Veamos que es de la forma $\mathfrak{p}A_S$ para cierto $\mathfrak{p}$ ideal primo de A tal que $\mathfrak{p} \cap S = \emptyset$.

Sea $\mathfrak{p} = \mathfrak{q} \cap A$. Este conjunto es un ideal de A ya que dado $a \in A$, $a\mathfrak{p} = a(\mathfrak{q} \cap A) = \mathfrak{q} \cap A$ por $\mathfrak{q}$ ideal. Además, $\mathfrak{p}$ es primo ya que si $ab \in \mathfrak{p}$ con $a, b \in A$, entonces $ab \in \mathfrak{q} \cap A$ y por tanto $ab \in \mathfrak{q}$ y $ab \in A$. Como $\mathfrak{q}$ es primo, $a \in \mathfrak{q}$ o $b \in \mathfrak{q}$, con lo cual $a \in \mathfrak{q} \cap A$ o $b \in \mathfrak{q} \cap A$ y en consecuencia $\mathfrak{p}$ es ideal primo.

Veamos entonces que $\mathfrak{q} = \mathfrak{p}A_S$. Por un lado, si $x \in \mathfrak{p}A_S$, existen $a \in (\mathfrak{q} \cap A)$ y $\frac{b}{s} \in A_S$ tales que $x = a \cdot \frac{b}{s}$ y como a en particular pertenece al ideal $\mathfrak{q}$, $x \in \mathfrak{q}$. Por otro, si tomamos un elemento $x \in \mathfrak{q}$, dicho elemento será de la forma $x = \frac{a}{s}$ con $a \in A$ y $s \in S$. Pero a pertenece al ideal $\mathfrak{q}$ por $a = x \cdot s$ y por lo tanto $x = a \cdot \frac{1}{s}$ pertenece a $(\mathfrak{q} \cap A)A_S$.

Para terminar con esta primera parte de la demostración solo nos falta probar que $\mathfrak{p} \cap S = \emptyset$. Efectivamente, si $s \in S$ pertenece a $\mathfrak{p}$, quiere decir que $s \in \mathfrak{q} \cap A$, en particular, $s \in \mathfrak{q}$ y por lo tanto $\frac{1}{s} \cdot s = \frac{s}{s} \in \mathfrak{q}$, lo cual contradice que $\mathfrak{q}$ sea ideal primo de A_S.

Además, dado un ideal primo $\mathfrak{p} \subset A$ con $\mathfrak{p} \cap S = \emptyset$, se cumple que $\mathfrak{p} = \mathfrak{q} \cap A$ donde $\mathfrak{q} = \mathfrak{p}A_S$ es un ideal primo de A_S.

En efecto, $\mathfrak{q} = \mathfrak{p}A_S$ es un ideal de A_S ya que dado $\frac{a}{s} \in A_S$, $\frac{a}{s}\mathfrak{q} = \frac{a}{s}\mathfrak{p}A_S = \mathfrak{p}\frac{1}{s}A_S = \mathfrak{p}A_S = \mathfrak{q}$. Por otro lado, es primo ya que si $xy \in \mathfrak{q}$ entonces existen $p \in \mathfrak{p}$ y $\frac{a}{s} \in A_S$ tales que $xy = p \cdot \frac{a}{s}$, por lo tanto $s(xy) = pa \in \mathfrak{p}$ y como $\mathfrak{p}$ primo $xy \in \mathfrak{p}$ ya que $\mathfrak{p} \cap S = \emptyset$. En consecuencia, ó $x \in \mathfrak{p}$ ó $y \in \mathfrak{p}$, con lo cual, ó $x \in \mathfrak{p}A_S = \mathfrak{q}$ ó $y \in \mathfrak{p}A_S = \mathfrak{q}$.

Por último podemos concluir que $\mathfrak{p} = \mathfrak{q} \cap A$ por doble contenido: si $x \in \mathfrak{q} \cap A$, entonces $x \in \mathfrak{p}A_S \cap A = \mathfrak{p}\langle A, S^{-1}\rangle \cap A = \mathfrak{p}$. El otro contenido es inmediato.

Q.E.D.

La proposición anterior nos va a permitir trabajar con ideales primos de la localización A_S para sacar conclusiones sobre los ideales primos de A.

Hay una localización especialmente interesante en el contexto de este trabajo, la localización de un ideal primo. Dado un ideal primo $\mathfrak{p}$ de A, el conjunto $S = A \backslash \mathfrak{p}$ es un conjunto multiplicativo a partir del cual podemos tomar la localización A_S, que denotaremos por $A_\mathfrak{p}$ y que llamaremos **localización de un ideal primo**. Nótese que

$$A_\mathfrak{p} = \{\frac{a}{b} \mid b \notin \mathfrak{p}\}$$

.

Si $\mathfrak{p}$ es un ideal primo de un dominio de integridad A, entonces $\mathfrak{p}A_S$ es el único ideal maximal de la localización $A_{\mathfrak{p}}$, es decir, $A_{\mathfrak{p}}$ es un anillo local ([J], pg. 3).

1.3. Enteros algebraicos

Dado A un dominio de integridad y B un subanillo de A con $1_A = 1_B$, diremos que $a \in A$ es **entero sobre** B si existe un polinomio mónico $f(x) \in B[X]$ no nulo tal que $f(a) = 0$. Claramente, los elementos de A son enteros sobre A. Además diremos que $f(x)$ es una **ecuación de dependencia entera** para a.

Teorema 1.3.1. *([J], pg. 5) Dado B un subanillo de un dominio de integridad A, el conjunto de elementos de A enteros sobre B es un subanillo de A que contiene a B.*

A lo largo de este trabajo vamos a considerar un dominio de integridad A contenido en su cuerpo de fracciones K. En este caso, el conjunto de elementos de K enteros sobre A recibe el nombre de **clausura entera de** A y lo denotaremos por $\bar{A}$. Además, si $A = \bar{A}$ diremos que A es **íntegramente cerrado**.

Proposición 1.3.1. *([J], pg. 5) Sean $C \subseteq B \subseteq A$ tres dominios de integridad tales que todos los elementos de B son enteros sobre C y todos los elementos de A son enteros sobre B. Entonces, todos los elementos de A son enteros sobre C.*

Esta proposición nos va a permitir construir anillos íntegramente cerrados a partir de un dominio de integridad A dado, ya que bastaría considerarlo contenido en su cuerpo de fracciones y calcular su clausura entera. Si $\bar{A}$ no fuese íntegramente cerrado, querría decir que existe un anillo D tal que $\bar{A} \subset D \subseteq K$ cuyos elementos son enteros sobre $\bar{A}$. Pero por la proposición anterior, tendríamos que todos los elementos de D son enteros sobre A, lo cual contradice que $\bar{A} \subset D$.

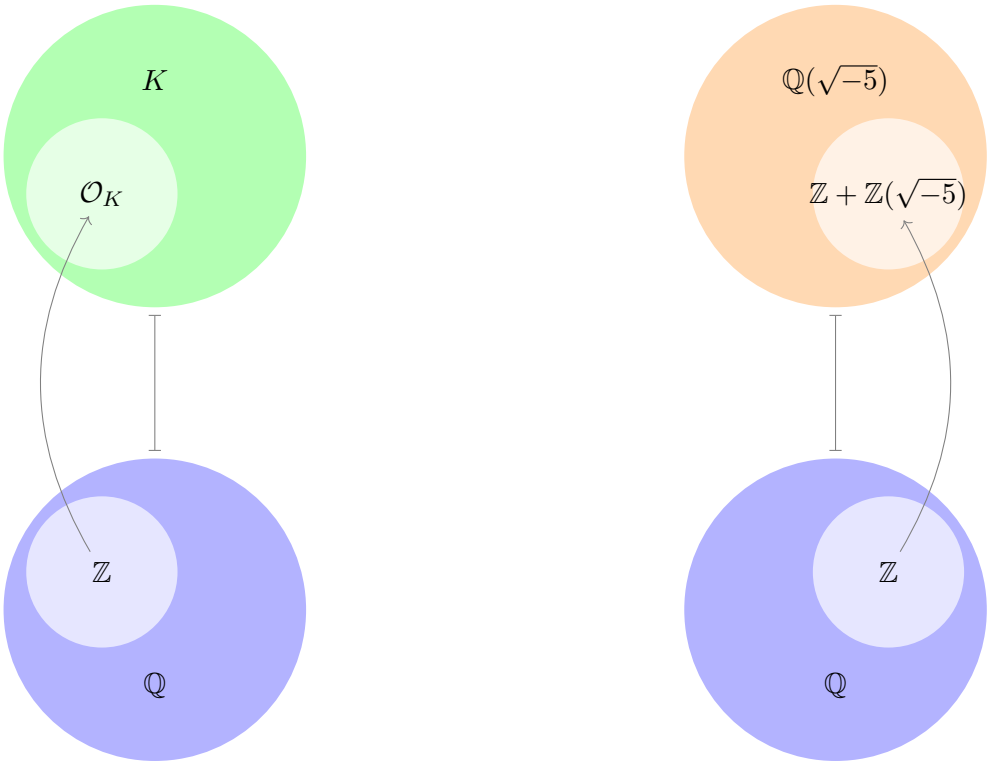
Por ejemplo, si A es un anillo íntegramente cerrado y S un subconjunto multiplicativo de A, entonces la localización A_S también es íntegramente cerrada, ya que si tomamos un elemento u del cuerpo de fracciones de A_S algebraico sobre A_S, existe un polinomio mónico $X^n + \frac{a}{s_{n-1}}X^{n-1} + \frac{b}{s_{n-2}}X^{n-2} + \cdots + \frac{c}{s_2}X^2 + \frac{d}{s_1}X + \frac{e}{s_0}$ con coeficientes en A_S del que u es raíz. Si tomamos $s \in S$ el común denominador de los coeficientes, tenemos que u es raíz del polinomio $sX^n + a'X^{n-1} + b'X^{n-2} + \cdots + c'X^2 + d'X + e'$ para ciertos $a', b', c', d', e' \in A$ y por tanto su es raíz del polinomio mónico $X^n + a'X^{n-1} + sb'X^{n-2} + \cdots + s^{n-3}c'X^2 + s^{n-2}d'X + s^{n-1}e'$. Con lo cual, el elemento su pertenece a A por ser este íntegramente cerrado, y como $s \in S$, $\frac{su}{u}$ pertenece a S, es decir, $u \in A_S$ y por lo tanto A_S es íntegramente cerrado.

Dentro de los enteros de un dominio de integridad sobre otro, nosotros vamos a estar interesados especialmente en los enteros de un cuerpo de números.

Definición 1.3.1. *Decimos que K es un **cuerpo de números (algebraicos)** si es una extensión finita algebraica del cuerpo de los números racionales $\mathbb{Q}$. Y un elemento u de un cuerpo de números K es un **entero (algebraico)** del cuerpo si es entero sobre $\mathbb{Z}$.*

Es decir, por ser K una extensión algebraica de $\mathbb{Q}$, dado $u \in K$ sabemos que existe un polinomio mónico no nulo $f(x)$ con coeficientes en $\mathbb{Q}$ tal que $f(u) = 0$, pero si además existe un polinomio en las mismas condiciones que tiene a u como raíz y coeficientes en $\mathbb{Z}$ dicho u no será solo un número algebraico sino que será un entero algebraico del cuerpo de acuerdo con la definición.

El conjunto de los elementos enteros de un cuerpo de números K, es decir, la clausura de $\mathbb{Z}$ sobre K, forma un anillo que llamaremos el **anillo de enteros de** K y que denotaremos por $\mathcal{O}_K$.



1.4. Norma de una extensión de cuerpos

Definición 1.4.1. *Sea K un cuerpo y L una extensión finita de K. Para cada elemento x de L se puede definir una función*

$$\begin{aligned} r_x : L &\longrightarrow L \\ y &\longmapsto xy \end{aligned}$$

Si consideramos L como espacio vectorial finito dimensional sobre K, r_x es una aplicación lineal y para $\{u_1, \ldots, u_n\}$ K-base vectorial de L, r_x tiene una matriz coordenada $[a_{ij}]$ tal que $r_x(u_i) = xu_i = \sum_j u_j a_{ij}$. Se llama ***norma de*** *L* ***sobre*** *K a la función $N_{L/K}(x) = det(r_x)$. Esta definición es independiente de la base escogida, es decir, solo depende de la extensión L/K.*

Los cuerpos de números surgen como generalización de $\mathbb{Q}$ como cuerpo de fracciones de $\mathbb{Z}$. Sin embargo, al dar este salto se pierden algunas propiedades importantes que sí que cumple el anillo de enteros de $\mathbb{Q}$, como por ejemplo el hecho de que sea un dominio de factorización única (DFU). Es decir, en $\mathbb{Z}$, todo elemento puede escribirse como producto de elementos irreducibles, mientras que dado un cuerpo de números cualquiera no puede concluirse lo mismo sobre su anillo de enteros en general. De hecho, si consideramos $\mathbb{Z}+\mathbb{Z}(\sqrt{-5})$ vemos que

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

Fue Ernest Kummer $(1810 - 1893)$ quien se dio cuenta de este obstáculo, lo cual tuvo profundas consecuencias en el desarrollo de la teoría de números. Por ejemplo, en muchas de las demostraciones publicadas anteriormente sobre el conocido como «último teorema de Fermat», sus autores daban por hecho que trabajaban en dominios de factorización única, a pesar de trabajar en anillos con números complejos que muchas veces no lo eran [F]. Afortunadamente, no tardaron en encontrar una alternativa a la exigencia de trabajar con dominios de factorización única, como veremos en próximas secciones.

A continuación recogemos algunas propiedades de esta función.

Propiedad 1.4.1. *([J], pgs. 20 y 25) Dados L una extensión finita del cuerpo K y $x,\ y \in L$ y $a \in K$, se cumple:*

- $N_{L/K}(xy) = N_{L/K}(x)N_{L/K}(y)$.
- $N_{L/K}(ax) = a^n N_{L/K}(x)$ *donde* $n = [L : K]$.

Teorema 1.4.1. *([J], pgs. $24 - 25$) Sea $K \subseteq L \subseteq F$ una cadena de extensiones separables con F/K extensión de Galois y $G = Gal(F/K)$ y $H = Gal(F/L)$. Sean $\sigma_1, \ldots, \sigma_n$ los distintos K-monomorfismos de L en N con N/K una extensión normal y $n = [L : K]$. Entonces, para todo $x \in L$:*

$$N_{L/K}(x) = \sigma_1(x) \cdots \sigma_n(x).$$

De este teorema se desprende un corolario importante:

Corolario 1.4.1. *([J], pg. 25) Si $K \subseteq E \subseteq L$ con extensiones separables de dimensión finita de K, entonces se cumple que para todo $x \in L$*

$$N_{L/K} = N_{E/K}(N_{L/E}(x)).$$

1.5. Anillos de Dedekind

Definición 1.5.1. *Sea A un anillo y M un A-módulo. El A-**módulo** M se dice **Noetheriano** si satisface alguna de estas condiciones equivalentes:*

- *Toda familia no vacía de submódulos de M posee un elemento maximal.*
- *Toda serie creciente de submódulos de M es estacionaria.*
- *Todo submódulo de M es de tipo finito.*

*Un **anillo** A se dice **Noetheriano** si, considerado como A-módulo es noetheriano.*

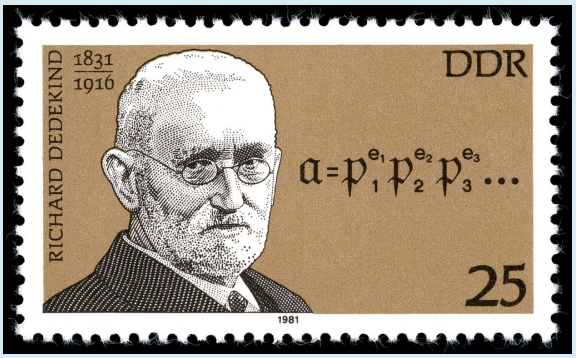


Figura 1.2: Sello de Alemania del Este de 1981 en memoria de Richard Dedekind.

Julius Wilhelm Richard Dedekind fue un matemático alemán que vivió entre los años 1831 y 1916. Fue discípulo de C.F. Gauss ($1777-1855$), quien dirigió su tesis doctoral y P.G.L. Dirichlet ($1805-1859$) entre otros. Pasó a la Historia de las matemáticas gracias a su definición de los números irracionales a través de los llamados «cortes de Dedekind» y de introducir el concepto de «ideal» en la teoría algebraica de números. Como diría H. M. Edwards (1936–), « El legado de Dedekind [...] no solo consiste en importantes teoremas, ejemplos, y conceptos, sino un estilo matemático que ha servido de inspiración a todas las generaciones siguientes.»[a]
Trabajar con dominios de Dedekind fue lo que permitió que la teoría de números avanzara a pesar de que el anillo de enteros de un cuerpo de números cualquiera no sea, en general, un dominio de factorización única. Como hemos visto, dado un cuerpo de números K, no podemos asegurar que un elemento de $\mathcal{O}_K$ cualquiera se pueda expresar de forma única como producto de elementos primos; sin embargo, sí que podemos afirmar la sentencia anterior en términos de ideales. Uno de los motivos que hace tan interesante el estudio de los dominios de factorización única es que todo dominio de ideales principales es a su vez un dominio de factorización única; de ahí que se considere a los anillos de Dedekind como una generalización de los dominios de ideales principales.

[a] `http://www-gap.dcs.st-and.ac.uk/~history/Biographies/Dedekind.html` Fecha de acceso: 26/02/2017.

Definición 1.5.2. *Un anillo A es un **anillo de Dedekind** si es un dominio de integridad tal que:*

- *es un anillo Noetheriano,*
- *es íntegramente cerrado y*

- *todo ideal primo no nulo de A es maximal.*

También podemos definir **anillo de Dedekind** como un anillo A que sea un dominio de integridad Noetheriano tal que la localización $A_{\mathfrak{p}}$ sea un DIP con un único ideal maximal para todos los ideales primos no nulos $\mathfrak{p}$ de A. A los dominios de ideales principales con esta característica se les conoce como **anillos de valoración discreta** (AVD).

Esta definición equivalente de anillo de Dedekind nos va a permitir trabajar con anillos locales ($A_{\mathfrak{p}}$) que cumplen ciertas propiedades interesantes:

Propiedad 1.5.1. *([J], pg. 7) Dado A un anillo de valoración discreta (AVD) y π un elemento de A tal que (π) sea el único ideal maximal de A, se cumple que:*

a) A es un anillo Noetheriano.

b) Si A no es un cuerpo, todo elemento x no nulo de A es de la forma $x = u\pi^n$ para cierta unidad $u \in A$ y cierto entero $n \geq 0$.

c) Todo ideal no nulo de A es de la forma (π^n) para cierto entero $n \geq 0$.

d) A es íntegramente cerrado.

e) Si A no es un cuerpo, entonces el ideal (π) es el único ideal primo no nulo de A.

Nuestro objetivo en esta sección va a ser demostrar que en un anillo de Dedekind un ideal se puede factorizar de forma única como producto de ideales primos.

Para ello necesitaremos varios resultados previos.

Propiedad 1.5.2. *Sea A un anillo de Dedekind. Entonces,*

a) Todo ideal primo no nulo de A es un ideal maximal.

b) Dado S un subconjunto multiplicativo de A se verifica que A_S es a su vez un anillo de Dedekind.

Demostración:

a) Sea $\mathfrak{p}$ un ideal primo no nulo de A y supongamos que existe un ideal maximal $\mathfrak{m} \subset A$ tal que $\mathfrak{p} \subset \mathfrak{m}$. Como todo ideal maximal es primo, por la proposición (1.2.1) $\mathfrak{p}A_{\mathfrak{m}}$ y $\mathfrak{m}A_{\mathfrak{m}}$ son dos ideales primos de $A_{\mathfrak{m}}$ tales que $\mathfrak{p}A_{\mathfrak{m}} \subset \mathfrak{m}A_{\mathfrak{m}}$, es decir, $A_{\mathfrak{m}}$ tiene al menos dos ideales primos distintos. Como A es un anillo de Dedekind, $A_{\mathfrak{m}}$ es un AVD y por la propiedad (1.5.1) solo tiene un ideal primo no nulo, con lo cual, no existe un ideal $\mathfrak{m}$ que cumpla las condiciones supuestas.

b) Sea $\mathfrak{p}_S$ un ideal primo no nulo de A_S cualquiera. Veamos que $(A_S)_{\mathfrak{p}_S}$ es un AVD:

Como $\mathfrak{p}_S$ es un ideal primo de A_S, es de la forma $\mathfrak{p}_S = \mathfrak{p}A_S$ para cierto $\mathfrak{p}$ ideal primo de A tal que $\mathfrak{p} \cap S = \emptyset$. Basta ver que

$$A_{\mathfrak{p}} = (A_S)_{\mathfrak{p}A_S}$$

para obtener el resultado.

Efectivamente, $(A_S)_{\mathfrak{p}A_S}$ es el anillo generado por A_S y los elementos inversos, considerados en el cuerpo de fracciones de A_S, del complementario de $\mathfrak{p}A_S$, pero por cómo está definido el producto en A_S,

$$(A_S)_{\mathfrak{p}A_S} = \langle A_S, \left((\mathfrak{p}A_S)^c\right)^{-1}\rangle = \langle A_S, (\mathfrak{p}^c)^{-1}\rangle = \langle A, S^{-1}, (\mathfrak{p}^c)^{-1}\rangle$$

y teniendo en cuenta que $S \subseteq \mathfrak{p}^c$ por $\mathfrak{p} \cap S = \emptyset$,

$$(A_S)_{\mathfrak{p}A_S} = \langle A, (\mathfrak{p}^c)^{-1}\rangle = A_{\mathfrak{p}}.$$

Como A es anillo de Dedekind, $A_{\mathfrak{p}}$ es AVD y por lo tanto $(A_S)_{\mathfrak{p}A_S}$ también.

Q.E.D.

Además, como consecuencia del teorema chino de los restos se cumple la siguiente proposición:

Proposición 1.5.1. *Sean B un anillo con identidad y $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ un conjunto de ideales de B tales que $B = \mathfrak{q}_i + \mathfrak{q}_j$ para $i \neq j$. Entonces*

$$\mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n = \mathfrak{q}_1 \cdots \mathfrak{q}_n$$

.

A partir de ahora consideremos A un anillo de Dedekind, $\mathfrak{a}$ un ideal de A no nulo y K el cuerpo de fracciones de A.

Lema 1.5.1. *Todo ideal de $A/\mathfrak{a}$ contiene un producto de ideales primos. En particular, existen n ideales primos de $A/\mathfrak{a}$ distintos $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ y n enteros positivos a_i tales que*

$$\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_n^{a_n} = \big(0\big).$$

Demostración:

Supongamos que no todo ideal de $B = A/\mathfrak{a}$ contiene un producto de ideales primos. Entonces, puedo tomar un maximal $\mathfrak{m}$ del conjunto $\{\mathfrak{i}$ ideal de $B \mid \mathfrak{i}$ no contiene un producto de ideales primos$\}$. En particular $\mathfrak{m}$ no es primo, con lo cual $\exists x, y \in \mathfrak{m}$ tales que $xy \in \mathfrak{m}$ pero $y \notin \mathfrak{m}$ y $x \notin \mathfrak{m}$.

Sean $\mathfrak{u} = xB + \mathfrak{m}$ y $\mathfrak{b} = yB + \mathfrak{m}$. Estos dos ideales contienen estrictamente a $\mathfrak{m}$ y por lo tanto contienen un producto de ideales primos. Sin embargo, $\mathfrak{ub} = xyB + xB\mathfrak{m} + yB\mathfrak{m} + \mathfrak{mm} \subseteq \mathfrak{m}$ por lo que $\mathfrak{m}$ contiene el producto de los productos de ideales primos contenidos en $\mathfrak{u}$ y $\mathfrak{b}$, lo cual contradice la hipótesis inicial.

Si aplicamos lo anterior al ideal $\big(0\big)$ tenemos que existen $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ ideales primos de $A/\mathfrak{a}$ y $a_1, \ldots, a_n$ enteros positivos tales que $\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_n^{a_n} \subseteq \big(0\big)$. El otro contenido se cumple por $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ ideales y por lo tanto $\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_n^{a_n} = \big(0\big)$. Q.E.D.

Lema 1.5.2. *Si $\mathfrak{p}_1$ y $\mathfrak{p}_2$ son dos ideales maximales distintos de $B = A/\mathfrak{a}$ entonces para a, b enteros cualesquiera estrictamente positivos se cumple que*

$$\mathfrak{p}_1^a + \mathfrak{p}_2^b = B$$

.

Demostración:

Sea a un número entero. El ideal $\mathfrak{p}_1^a$ no está contenido en $\mathfrak{p}_2$ por ser $\mathfrak{p}_2$ primo. Como $\mathfrak{p}_1^a \not\subseteq \mathfrak{p}_2$ y $\mathfrak{p}_2$ es ideal maximal, se cumple que $\mathfrak{p}_1^a + \mathfrak{p}_2 = B$.

Supongamos ahora que para cierto entero $c \geq 1$ se cumple que $\mathfrak{p}_1^a + \mathfrak{p}_2^c = B$. Entonces, $\mathfrak{p}_2^c = \mathfrak{p}_2^c B = \mathfrak{p}_2^c\left(\mathfrak{p}_1^a + \mathfrak{p}_2\right) \subseteq \mathfrak{p}_1^a + \mathfrak{p}_2^{c+1}$. En consecuencia, por un lado tenemos que $B = \mathfrak{p}_1^a + \mathfrak{p}_2^c \subseteq \mathfrak{p}_1^a + \left(\mathfrak{p}_1^a + \mathfrak{p}_2^{c+1}\right) = \mathfrak{p}_1^a + \mathfrak{p}_2^{c+1}$ y por otro, como $\mathfrak{p}_1$ y $\mathfrak{p}_2 \subseteq B$ tenemos el contenido inverso. Como hemos probado al principio que para $c = 1$ se cumple el resultado, se cumple para cualquier entero b.

Q.E.D.

Lema 1.5.3. *Sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ los ideales primos de $B = A/\mathfrak{a}$ tales que $\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_n^{a_n} = \left(0\right)$. Entonces,*

$$B \cong \frac{B}{\mathfrak{p}_1} \oplus \ldots \oplus \frac{B}{\mathfrak{p}_n}.$$

Demostración:

Por el lema (1.5.1) $B = \mathfrak{p}_i^{a_i} + \mathfrak{p}_j^{a_j}$ para todo $i \neq j$ con $i, j \in \{1, \ldots, n\}$, y por tanto podemos aplicar el teorema chino de los restos que asegura que

$$\frac{B}{\mathfrak{i}} \cong \frac{B}{\mathfrak{p}_1^{a_1}} \oplus \cdots \oplus \frac{B}{\mathfrak{p}_n^{a_n}}$$

con $\mathfrak{i} = \bigcap_i \mathfrak{p}_i^{a_i}$. Pero por la proposición (1.5.1), $\bigcap_i \mathfrak{p}_i^{a_i} = \prod_i \mathfrak{p}_i^{a_i}$ que por hipótesis es igual a $\left(0\right)$, luego $\bigcap_i \mathfrak{p}_i^{a_i} = \left(0\right)$ y

$$B \cong \frac{B}{\mathfrak{p}_1} \oplus \cdots \oplus \frac{B}{\mathfrak{p}_n}.$$

Q.E.D.

Corolario 1.5.1. *Los ideales $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ del lema anterior son todos los ideales primos de $B = A/\mathfrak{a}$.*

Demostración:

Por el lema (1.5.3) si conocemos todos los ideales primos de $\frac{B}{\mathfrak{p}_1} \oplus \cdots \oplus \frac{B}{\mathfrak{p}_n}$ conoceremos todos los ideales primos de B. Sea $B_i = B/\mathfrak{p}_i^{a_i}$ para todo i. Los únicos ideales primos en una suma directa $B_1 \oplus \cdots \oplus B_n$ son la suma directa $I_1 \oplus \cdots \oplus I_n$ de ideales I_i de B_i. Sabemos que $I_1 \oplus \cdots \oplus I_n$ es primo si y solo si

$$B_1/I_1 \oplus \cdots \oplus B_n/I_n$$

es un dominio de integridad. Bajo esta condición obtenemos que los distintos primos de $\frac{B}{\mathfrak{p}_1} \oplus \cdots \oplus \frac{B}{\mathfrak{p}_n}$ son los de la forma

$$\frac{B_1}{\mathfrak{p}_1^{a_1}} \oplus \cdots \oplus \frac{B_{i-1}}{\mathfrak{p}_{i-1}^{a_{i-1}}} \oplus \mathfrak{p}_i \oplus \frac{B_{i+1}}{\mathfrak{p}_{i+1}^{a_{i+1}}} \oplus \cdots \oplus \frac{B_n}{\mathfrak{p}_n^{a_n}}$$

para cada i, y por isomorfía todos los ideales primos de B son justamente $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$.

Q.E.D.

Lema 1.5.4. *Sea A un anillo de Dedekind, K su cuerpo de fracciones, $\mathfrak{p}$ un ideal primo de A y a un entero positivo. Entonces la aplicación natural de A sobre $A_\mathfrak{p}$ induce un isomorfismo de $\frac{A}{\mathfrak{p}^a}$ a $\frac{A_\mathfrak{p}}{\mathfrak{p}^a A_\mathfrak{p}}$. Es decir,*

$$\frac{A}{\mathfrak{p}^a} \cong \frac{A_\mathfrak{p}}{\mathfrak{p}^a A_\mathfrak{p}}.$$

Demostración:

Veamos que el homomorfismo $f : A/\mathfrak{p}^a \longrightarrow A_\mathfrak{p}/\mathfrak{p}^a A_\mathfrak{p}$ tal que $f(r + \mathfrak{p}^a) = r + \mathfrak{p}^a A_\mathfrak{p}$ es biyectivo. La inyectividad está clara por definición, luego solo queda probar la suprayectividad. Sea $\frac{r}{s} \in A_\mathfrak{p}$. Por A anillo de Dedekind y $\mathfrak{p}$ ideal primo, $\mathfrak{p}$ es un ideal maximal de A y por lo tanto $(s) + \mathfrak{p} = A$. Entonces, $(s) + \mathfrak{p}^a = A$, ya que si tomamos la hipótesis de inducción $(s) + \mathfrak{p}^{a-1} = A^{a-1}$, entonces $A^a = A \cdot A^{a-1} = ((s) + \mathfrak{p})((s) + \mathfrak{p}^{a-1}) = (s) + (s)\mathfrak{p}^{a-1} + \mathfrak{p}(s) + \mathfrak{p}^a = (s) + \mathfrak{p}^a$ y $A^a = A$. Por lo tanto $\exists c \in A$ y $q \in \mathfrak{p}^a$ tales que $sc + q = 1$. Esto implica que $f(rc + \mathfrak{p}^a) = rc + \mathfrak{p}^a A_\mathfrak{p} = r(1/s - q/s) + \mathfrak{p}^a A_\mathfrak{p} = r/s + \mathfrak{p}^a A_\mathfrak{p}$ y por consiguiente f es suprayectiva.

Q.E.D.

Corolario 1.5.2. *Dado $\mathfrak{p}$ un ideal primo de un anillo de Dedeking A, todo ideal de $A/\mathfrak{p}^a$ es una potencia de $\mathfrak{p}/\mathfrak{p}^a$ para cualquier entero positivo a. Además, $\mathfrak{p}/\mathfrak{p}^a$ es un ideal principal de $A/\mathfrak{p}^a$.*

Demostración:

En primer lugar, como A es un anillo de Dedeking, $\mathfrak{p}$ es un ideal maximal por ser ideal primo, y por lo tanto podemos aplicar el lema anterior. Con lo cual, para ver que todo ideal de $A/\mathfrak{p}^a$ es de la forma $\left(\mathfrak{p}/\mathfrak{p}^a\right)^n$ para cierto n, basta ver que todo ideal de $\frac{A_\mathfrak{p}}{\mathfrak{p}^a A_\mathfrak{p}}$ es una potencia de $\mathfrak{p}A_\mathfrak{p}/\mathfrak{p}^a A_\mathfrak{p}$. Como A es un anillo de Dedekind, $A_\mathfrak{p}$ es un AVD y por lo tanto es un dominio de ideales principales con un único ideal maximal. Además, por la propiedad (1.5.2), $A_\mathfrak{p}$ es a su vez anillo de Dedeking y en consecuencia, un ideal primo será también maximal. Por la proposición (1.2.1) $\mathfrak{p}A_\mathfrak{p}$ es ideal primo de $A_\mathfrak{p}$ y por tanto es el único ideal maximal de $A_\mathfrak{p}$. Teniendo en cuenta la propiedad (1.5.1) podemos concluir que todo ideal no nulo de $A_\mathfrak{p}$ es de la forma $\left(\mathfrak{p}A_\mathfrak{p}\right)^n$ para cierto entero positivo n. Esto implica que todo ideal no nulo de $\frac{A_\mathfrak{p}}{\mathfrak{p}^a A_\mathfrak{p}}$ es de la forma $\left(\mathfrak{p}A_\mathfrak{p}/\mathfrak{p}^a A_\mathfrak{p}\right)^n$, lo cual demuestra el enunciado.

Q.E.D.

Proposición 1.5.2. *([J], pg. 12) Sea $\mathfrak{a}$ un ideal no nulo de A y $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ todos los ideales primos que contienen a $\mathfrak{a}$. Entonces, $\mathfrak{a} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_n^{a_n}$ para ciertos enteros a_i.*

Ahora sí, podemos enunciar y demostrar fácilmente el objetivo principal de esta sección:

Teorema 1.5.1. *Sea A un anillo de Dedekind y $\mathfrak{a}$ un ideal no nulo de A. Entonces $\mathfrak{a} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_n^{a_n}$ para $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ ideales primos, distintos dos a dos, determinados de forma única por $\mathfrak{a}$ y a_i enteros positivos también determinados de forma única por $\mathfrak{a}$.*

Demostración:

Sabemos que $\mathfrak{a} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_n^{a_n}$ por la proposición (1.5.2). Falta ver que $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ y $a_1, \ldots, a_n$ están determinados de forma única. Por un lado, $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ están determinados de forma única por ser todos los primos que contienen a $\mathfrak{a}$. De la misma manera, cada a_i es el mínimo entero que cumple que el ideal maximal de $A_{\mathfrak{p}_i}/\mathfrak{a}A_{\mathfrak{p}_i}$ elevado a dicho entero es el ideal 0, es decir, cada a_i es el mínimo entero positivo tal que $\mathfrak{a}A_{\mathfrak{p}_i} = \mathfrak{p}_i^{a_i} A_{\mathfrak{p}_i}$ por lo que quedan determinados de forma única.

Q.E.D.

Tal y como adelantábamos, el teorema anterior muestra una de las propiedades más interesantes de los anillos de Dedekind: todo ideal de un anillo de Dedekind se factoriza de forma única como producto de ideales primos.

Además, se cumple que el anillo de enteros algebraicos de un cuerpo de números es un anillo de Dedekind.

Teorema 1.5.2. *([N], pgs. $12-17$) El anillo de los enteros algebraicos de un cuerpo de números K, $\mathcal{O}_K$, es un anillo de Dedekind.*

A continuación, vamos a introducir algunos conceptos, amén de propiedades y otros resultados sobre ellos, que intervendrán en el desarrollo de la ley de reciprocidad de Artin.

Definición 1.5.3. *Dados $A \subseteq B$ dos anillos de Dedekind y $\mathfrak{P}$ un ideal primo no nulo de B, llamamos **índice de ramificación** de $\mathfrak{P}$ sobre A a la potencia a la que aparece elevado $\mathfrak{P}$ en la factorización del ideal $\mathfrak{p}B$, donde $\mathfrak{p}$ es $A \cap \mathfrak{P}$. Se denotará por $e(\mathfrak{P}/A)$ o por $e(\mathfrak{P}/\mathfrak{p})$.*

Definición 1.5.4. *Sean $A \subseteq B$ dos anillos de Dedekind, $\mathfrak{P}$ un ideal primo no nulo de B y $\mathfrak{p} = \mathfrak{P} \cap A$. El índice $f = [B/\mathfrak{P} : A/\mathfrak{p}]$ se llama **grado relativo de $\mathfrak{P}$ sobre $\mathfrak{p}$**. Se denotará por $f(\mathfrak{P}/A)$ o $f(\mathfrak{P}/\mathfrak{p})$.*

El siguiente lema nos asegura que el grado relativo de un ideal que cumpla las condiciones de la definición anterior está bien definido y es finito.

Lema 1.5.5. *([J], pgs. $29-30$) Sean $A \subseteq B$ dos anillos de Dedekind con $K \subseteq L$ sus cuerpos de fracciones respectivamente y $\mathfrak{b}$ un ideal de B tal que $\mathfrak{b} \cap A = \mathfrak{p}$ es un ideal primo no nulo de A. Entonces $B/\mathfrak{b}$ es un espacio vectorial sobre $A/\mathfrak{p}$ y su dimensión satisface la desigualdad*

$$[B/\mathfrak{b} : A/\mathfrak{p}] \leq [L : K].$$

Tanto las definiciones como el resultado anterior se han dado para dos anillos de Dedekind cualesquiera $A \subseteq B$ con cuerpos de fracciones K y L respectivamente. A nosotros nos va a interesar el caso particular en el que B es la clausura entera de A.

El siguiente teorema establece una relación fundamental entre el índice de ramificación, el grado relativo y la dimensión de una extensión del cuerpo de fracciones de un anillo de Dedekind dado.

Teorema 1.5.3. *([J], pgs. 30−32) Sean A un anillo de Dedekind, K su cuerpo de fracciones y L una extensión finita y separable de K. Entonces, considerando B la clausura entera de A en L y $\mathfrak{p}$ un ideal primo no nulo de A, se cumple que*

$$\sum_{i=1}^{t} e_i f_i = [L : K]$$

donde e_i y f_i denotan el índice de ramificación y el grado relativo respectivamente de los ideales primos de B que aparecen en la factorización de $\mathfrak{p}B$ y t es el número de ideales primos que aparece en dicha factorización.

Gracias al siguiente teorema vamos a poder hablar del **grado relativo de $\mathfrak{p}$** y del **índice de ramificación de $\mathfrak{p}$** en el caso de trabajar con extensiones finitas de Galois.

Teorema 1.5.4. *([J], pgs. $32-33$)Sea A un anillo de Dedekind con cuerpo de fracciones K y sea B la clausura entera de A en una extensión finita de Galois L de K con grupo de Galois G. Entonces, para un ideal primo $\mathfrak{p}$ de A dado se cumple que:*

a) El ideal $\mathfrak{p}B$ se factoriza como

$$\mathfrak{p}B = (\mathfrak{P}_1 \cdots \mathfrak{P}_t)^e$$

con $\mathfrak{P}_i$ ideales primos distintos de B.

b) Todos los grados relativos $f(\mathfrak{P}_i/\mathfrak{p})$ son iguales.

c) G actúa transitivamente sobre los ideales primos $\mathfrak{P}_i$ de B que contienen a $\mathfrak{p}$.

Además,

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

Definición 1.5.5. *Sea A un anillo de Dedekind, K su cuerpo de fracciones, L una extensión finita separable del cuerpo K y B la clausura entera de A en L. Sea $\mathfrak{P}$ un ideal primo no nulo de B y $\mathfrak{p} = A \cap \mathfrak{P}$. Se dice que $\mathfrak{P}$ es **ramificado sobre** A si su índice de ramificación $e(\mathfrak{P}/\mathfrak{p})$ es mayor que 1.*

*Por otra aparte, se dice que $\mathfrak{p}$ es **ramificado en** B si el ideal $\mathfrak{p}B$ es divisible por algún ideal primo ramificado de B, y es **completamente ramificado en** B si $\mathfrak{p}B = \mathfrak{P}^e$, con $e > 1$, y su grado relativo $f(\mathfrak{P}/\mathfrak{p})$ es uno.*

Además, diremos que la ***extensión*** L/K *es* ***ramificada*** *o completamente ramificada si todo ideal primo* $\mathfrak{p}$ *de* A *es ramificado o completamente ramificado respectivamente en* B*.*

Por último, diremos que $\mathfrak{p}$ *se* ***escinde completamente*** *en la extensión si es divisible por algún ideal primo de* B *con grado relativo e índice de ramificación igual a uno.*

En una extensión de Galois L/K diremos que $\mathfrak{p}$ **se ramifica completamente en** L si su grado relativo f y t valen uno; y que **se escinde completamente en** L si su grado relativo f es uno y su índice de ramificación e también.

Dado un anillo de Dedekind A con K su cuerpo de fracciones y B la clausura entera de A en una extensión finita y separable L del cuerpo K, vamos a poder definir la norma de un ideal dado de B. Esta norma va a ser una aplicación que nos va a permitir relacionar ideales de B con ideales de A y además vamos a poder determinarla a partir del grado relativo del ideal de B.

Definición 1.5.6. *En las condiciones anteriores, se define como* ***norma del ideal*** $\mathfrak{b}$ *de* B *al ideal de* A *generado por todos los elementos* $N_{L/K}(b)$ *con* $b \in \mathfrak{b}$*, y se denota por* $N_{L/K}(\mathfrak{b})$*.*

Basta recordar cómo está definida la norma $N_{L/K}(\ )$ de un elemento de B para ver que $N_{L/K}(b) \in A$ para $b \in B$ y que por tanto la aplicación

$$\begin{aligned} B &\to A \\ b &\mapsto N_{L/K}(b) \end{aligned}$$

está bien definida.

La siguiente proposición nos dice cómo se puede calcular la norma de un ideal a partir de su grado relativo.

Proposición 1.5.3. *([J], pgs.* $43-44$*) Sea* $\mathfrak{P}$ *un ideal primo no nulo de* B *y* $\mathfrak{p} = A \cap \mathfrak{P}$*. Entonces,*

$$N(\mathfrak{P}) = \mathfrak{p}^f$$

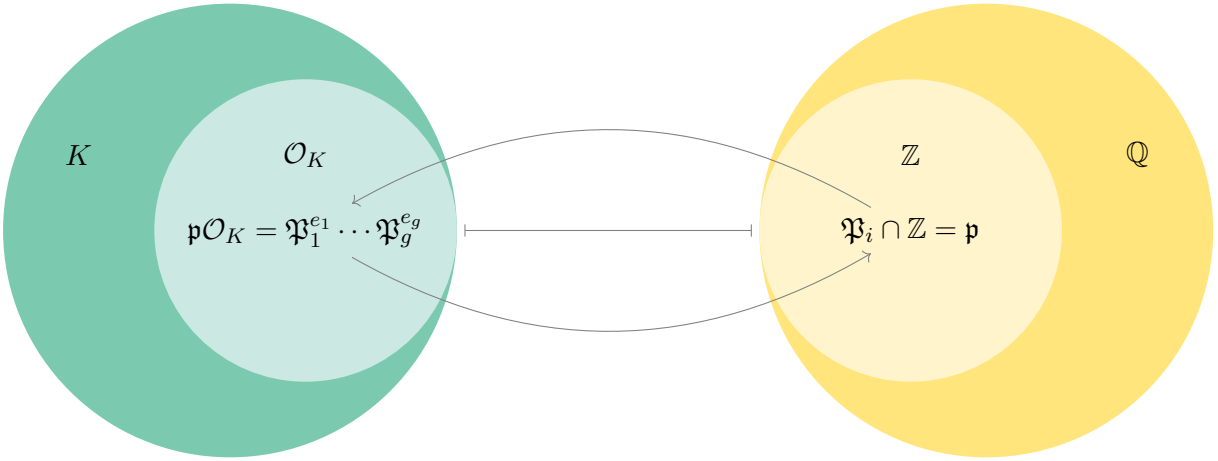
con $f = f(\mathfrak{P}/A) = [B/\mathfrak{P} : A/\mathfrak{p}]$*.*

Además, si $\mathfrak{b} = \prod \mathfrak{P}_i^{e_i}$ *es un ideal* B *con* $\mathfrak{P}_i$ *ideal primo de* B *para todo* i*,* $\mathfrak{p}_i = \mathfrak{P}_i \cap A$ *y* $f_i = f(\mathfrak{P}_i/A)$*, entonces*

$$N(\mathfrak{a}) = \prod \mathfrak{p}_i^{e_i f_i}.$$

En particular, si $K = \mathbb{Q}$, $A = \mathbb{Z}$, L es una extensión finita de $\mathbb{Q}$ y B es el anillo de enteros algebraicos de L, la norma $N_{L/\mathbb{Q}}(\mathfrak{a})$ para $\mathfrak{a}$ ideal de B es un ideal principal $m\mathbb{Z} = (m)$ para cierto m. Si imponemos que este m sea mayor o igual que cero queda únicamente determinado y es el número de elementos del anillo $B/\mathfrak{a}$. A dicho m se le suele denotar por $\mathcal{N}(\mathfrak{a})$ y recibe el nombre de **norma absoluta de** $\mathfrak{a}$ ([J], pg. 45).

Esta norma puede decirnos si un ideal $\mathfrak{a}$ de B es primo ya que si $\mathcal{N}(\mathfrak{a}) = p$ primo, entonces $B/\mathfrak{a}$ tiene p elementos y por tanto $\mathfrak{a}$ es un ideal primo y $f(\mathfrak{a}/\mathbb{Z}) = 1$. En particular, si $x \in B$ y $N_{L/K}(x) = \pm p$ entonces $\mathfrak{a} = xB$ es un ideal primo con grado relativo 1 sobre $\mathbb{Z}$.



1.6. Grupo de clases

A lo largo de esta sección A denota un anillo de Dedekind y K su cuerpo de fracciones.

Definición 1.6.1. *Se llama* ***ideal fraccionario*** *de A a un A-submódulo de K $\mathfrak{a}$ finitamente generado no nulo.*

Un ideal fraccionario de A no es un ideal de A a menos que esté contenido en A. Sin embargo, todos los ideales de un anillo Noetheriano son ideales fraccionarios ya que están finitamente generados. Para evitar posibles confusiones, llamaremos a los ideales de A **ideales enteros** y denotaremos por I_A al conjunto de ideales fraccionarios de A.

Definimos el producto entre dos ideales fraccionarios $\mathfrak{a}$ y $\mathfrak{b}$ como el conjunto de todas las sumas $\sum a_i b_i$ con $a_i \in \mathfrak{a}$ y $b_i \in \mathfrak{b}$. Si $\{x_j\}$ e $\{y_k\}$ son dos conjuntos finitos de generadores de $\mathfrak{a}$ y $\mathfrak{b}$ respectivamente, entonces $\{x_j y_k\}$ es a su vez un conjunto finito generador de $\mathfrak{ab}$, y por tanto, el producto de ideales fraccionarios así definido es a su vez un ideal fraccionario.

El conjunto de ideales fraccionarios de un anillo de Dedekind A con el producto definido en el párrafo anterior tiene estructura de grupo, siendo el propio A la identidad y el inverso de un ideal fraccionario $\mathfrak{a}$ es el conjunto $\{x \in K \mid x\mathfrak{a} \subseteq A\}$. Este conjunto es a su vez un ideal fraccionario de A: por definición, $\mathfrak{a}^{-1}$ es un A-submódulo de K. Además, tomando cualquier $a \in \mathfrak{a}$ no nulo, $\mathfrak{a}^{-1}a \subseteq A$, luego $\mathfrak{a}^{-1} \subseteq Aa^{-1}$. Como Aa^{-1} es un A-módulo finitamente generado y A es un anillo Noetheriano, el submódulo $\mathfrak{a}^{-1}$ es también finitamente generado y por tanto ideal fraccionario.

Cuando $\mathfrak{a}$ es un ideal fraccionario de A y n es un entero positivo, denotaremos por $\mathfrak{a}^{-n}$ a $(\mathfrak{a}^{-1})^n$.

Análogamente al caso de los ideales de un anillo de Dedekind A, un ideal fraccionario de dicho anillo también puede expresarse de forma única como producto de potencias de ideales primos, como recoge el siguiente teorema.

Teorema 1.6.1. *([J], pg. 18) Cualquier ideal fraccionario $\mathfrak{a}$ de un anillo de Dedeking A puede expresarse de forma única como un producto*

$$\mathfrak{a} = \mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2}\cdots\mathfrak{p}_n^{a_n}$$

con $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ ideales primos y $a_1, a_2, \ldots, a_n$ enteros positivos o negativos.

Definición 1.6.2. *Se llama **grupo de ideales de** A al conjunto de ideales fraccionarios de A con el producto definido por $\mathfrak{ab} = \{\sum a_i b_i \mid a_i \in \mathfrak{a},\ b_i \in \mathfrak{b}\}$. Se denota por I_A.*

*El conjunto de todos los ideales fraccionarios principales $P_A := \{\ xA \mid x \in K\ \}$ es un subgrupo de I_A y su cociente se conoce como el **grupo de clases de** A y se denota por C_A.*

$$C_A = \frac{I_A}{P_A}$$

Si el anillo A es un dominio de ideales principales, $I_A = P_A$ y C_A es el grupo trivial. C_A puede considerarse, entre comillas, una medida de cómo de cerca está el anillo A de ser un dominio de ideales principales. Dado K un cuerpo de números también puede hablarse del **grupo de ideales de** K y del **grupo de clases de** K considerando $A = \mathcal{O}_K$ y los denotaremos por I_K y C_K respectivamente. Al orden del grupo de clases de K se le llamará **número de clases de** K.

Además, el grupo de clases de un cuerpo de números K es un grupo finito, como recoge el siguiente resultado.

Teorema 1.6.2. *([J], pg. 72) Dado K un cuerpo de números y A su anillo de enteros algebraicos, se cumple que $C(A)$ es un grupo finito.*

Aunque nosotros estamos interesados en el estudio de cuerpos de números y por tanto en el de sus anillos de enteros, cabe destacar que este teorema no se cumple en general para un anillo de Dedekind arbitrario. Es decir, dado un anillo de Dedekind A, el grupo C_A no tiene por qué ser finito *a priori*.

1.7. Valoraciones

El objetivo de esta sección es definir una métrica para un cuerpo dado que nos permita tomar otro cuerpo que contenga al primero y sea completo respecto a dicha métrica. Lo que buscamos con esto no es otra cosa que una generalización de $\mathbb{R}$ como compleción de $\mathbb{Q}$ respecto al valor absoluto.

Definición 1.7.1. *Sea K un cuerpo y $|\ |\colon x \mapsto |\ x\ |$ una función de K en $\mathbb{R}$. La función $|\ |$ es un **valor absoluto** si:*

- $\mid x \mid \geq 0$ *para todo* $x \in K$ $y \mid x \mid = 0$ *si y solo si* $x = 0$,
- $\mid x \mid\mid y \mid = \mid xy \mid$ *para todo* $x, y \in K$,
- *existe una constante positiva* C *tal que* $\mid x + y \mid \leq C \cdot máx\{\mid x \mid, \mid y \mid\}$ *para todo* $x, y \in K$.

A partir de ahora vamos a considerar valores absolutos $\mid\ \mid$, para los cuales existe algún $x \in K$ tales que $\mid x \mid \neq 1$.

Definición 1.7.2. *Dados dos valores absolutos* $\mid\ \mid_1$, $\mid\ \mid_2$ *definidos del cuerpo* K *en* $\mathbb{R}$, *diremos que son* ***equivalentes*** *si se cumple que para cualquier* $x \in K$,

$$\mid x \mid_1 < 1 \iff \mid x \mid_2 < 1.$$

Proposición 1.7.1. *Dados dos valores absolutos equivalentes* $\mid\ \mid_1$, $\mid\ \mid_2$ *definidos sobre el cuerpo* K, *existe un número real* a *tal que*

$$\mid x \mid_1^a = \mid x \mid_2 \quad \forall x \in K.$$

Dentro de los valores absolutos, vamos a centrarnos en aquellos $\mid\ \mid$ que verifican la desigualdad triangular, es decir, que

$$\mid x + y \mid \leq \mid x \mid + \mid y \mid, \ \forall x, y \in K.$$

A estos valores absolutos, para los cuales la constante mencionada en la definición (1.7.1) puede tomarse como $C = 2$ ya que $\mid x \mid + \mid y \mid \leq 2 \cdot máx\{\mid x \mid, \mid y \mid\}$, los llamaremos **valoraciones**.

Va a haber dos valoraciones de especial interés en el estudio de los cuerpos de números algebraicos: aquellas para las que se pueda tomar $C = 1$, donde C es la constante definida en (1.7.1), que llamaremos **valoraciones no arquimedianas**, y aquellas que no sean equivalentes a ninguna valoración no arquimediana, que llamaremos **valoraciones arquimedianas**.

Nótese que dada una valoración no arquimediana $\mid\ \mid$ se cumple que

$$\mid x + y \mid \leq máx\{\mid x \mid, \mid y \mid\}.$$

Definición 1.7.3. *Sea* A *un anillo de Dedekind y* K *su cuerpo de fracciones. Dada una función* v_1 *definida de* $K\backslash\{0\}$ *en* $\mathbb{R}$ *que verifica*

a) $v_1(x)$ *es un número entero para todo* $x \in K\backslash\{0\}$

b) $v_1(xy) = v_1(x) + v_1(y)$ *para todo* $x, y \in K\backslash\{0\}$

c) $v_1(x + y) \geq mín\{v_1(x), v_1(y)\}$ *para todo* $x, y \in K\backslash\{0\}$

llamamos ***valoración exponencial*** *de* K *a la función*

$$v : K \to \mathbb{R} \cup \{\infty\}$$
$$0 \neq x \mapsto v_1(x)$$
$$0 \mapsto \infty$$

A partir de una valoración exponencial cualquiera de K podemos definir una valoración no arquimediana de K tomando un número real c entre 0 y 1 y definiendo dicha valoración como

$$| \ x \ |_v = c^{v(x)}.$$

Efectivamente, $| \ |_v$ es una valoración ya que $| \ x \ |_v = c^{v(x)} \geq 0$ para todo $x \in K$; $| \ x \ |_v | \ y \ |_v = c^{v(x)}c^{v(y)} = c^{v(x)+v(y)} = | \ x + y \ |_v$ para todo $x, y \in K$; y, tomando $v(x) = mín\{v(x), v(y)\}$, $| \ x + y \ |_v = c^{v(x+y)} \leq c^{v(x)} \leq c^{v(x)} + c^{v(y)} = | \ x \ |_v + | \ y \ |_v$. Y es no arquimediana ya que considerando de nuevo $v(x) = mín\{v(x), v(y)\}$, tenemos que $| \ x \ |_v = máx\{| \ x \ |_v, \ | \ y \ |_v\}$ por $0 < c < 1$ y por tanto,

$$| \ x + y \ |_v = c^{v(x+y)} \leq c^{v(x)} = | \ x \ |_v = máx\{| \ x \ |_v, \ | \ y \ |_v\}.$$

Nótese que la elección de la constante c no es un problema ya que si tomamos otra constante c' entre 0 y 1 tendríamos una valoración equivalente a la anterior ya que $c' = c^a$ para cierto a.

En este trabajo nos va a interesar una valoración exponencial particular. Dado un cuerpo de números algebraicos K y A su anillo de enteros algebraicos, como A es un anillo de Dedekind, xA es un ideal fraccionario para cualquier $x \in K\backslash\{0\}$ y por tanto,

$$xA = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(x)}.$$

La aplicación $v_{\mathfrak{p}}(x)$ que lleva a cada $x \in K\backslash\{0\}$ al entero al que aparece elevado el ideal primo $\mathfrak{p}$ en la factorización de xA, es una valoración exponencial ([J], pg. 85) y se conoce como **valoración $\mathfrak{p}$-ádica** de K. Además, todas las valoraciones no arquimedianas de un cuerpo de enteros algebraicos se definen a partir de una valoración $\mathfrak{p}$-ádica de dicho cuerpo a través del procedimiento descrito anteriormente.

Trabajar con valoraciones va a tener distintas ventajas, por ejemplo, a partir de una valoración no arquimediana $| \ |$ de un cuerpo de números K vamos a poder definir un anillo local con un único ideal maximal. A este anillo se le conoce como **anillo de valoración** asociado a $| \ |$ y es el conjunto

$$A = \{x \in K :| \ x \ | \leq 1\},$$

su ideal maximal es

$$\mathfrak{p} = \{x \in K :| x |< 1\}$$

y K su cuerpo de fracciones. Una propiedad especialmente interesante de este tipo de anillos es que son un AVD si y solo si el conjunto de valores no nulos $\{| x |: x \in K, x \neq 0\}$ es un subgrupo multiplicativo de los números reales isomorfo al grupo aditivo de los enteros ([J], pgs. $86 - 87$).

También va a ser importante saber si, dada una valoración, esta es arquimediana o no. Para ello podemos apoyarnos en que una valoración $|\ |$ de un cuerpo K es arquimediana si y solo si los valores $| n1_K |$, con 1_K la identidad del cuerpo K, están acotados a medida que n recorre los números enteros; y que un cuerpo de característica no nula tiene únicamente valoraciones no arquimedianas ([J], pg. 87). En particular, si estamos trabajando con el cuerpo de los números racionales, cabe destacar la siguiente proposición:

Proposición 1.7.2. *([J], pgs. $88 - 89$) Toda valoración no arquimediana de $\mathbb{Q}$ es equivalente a una valoración p-ádica para cierto entero primo p. Por otra parte, toda valoración arquimediana de $\mathbb{Q}$ es equivalente al valor absoluto usual de los números reales restringido a $\mathbb{Q}$.*

Definición 1.7.4. *Llamaremos **primo de un cuerpo** K a una clase de equivalencia de valoraciones en dicho cuerpo. Si la clase de equivalencia contiene valoraciones arquimedianas es llamada **primo infinito de** K, y si por el contrario contiene valoraciones no arquimedianas, será un **primo finito del cuerpo** K. Utilizaremos las letras $\mathfrak{P}$ o $\mathfrak{p}$ para referirnos a primos de un cuerpo, y para referirnos a una valoración de dicho primo escribiremos $|\ |_{\mathfrak{P}}$ o $|\ |_{\mathfrak{p}}$.*

Una vez identificadas las valoraciones de $\mathbb{Q}$, veamos cómo podemos extenderlas a cuerpos que lo contengan.

Definición 1.7.5. *Sea $\{a_n\}$ una sucesión de elementos del cuerpo K y $|\ |$ una valoración sobre K. La **sucesión** $\{a_n\}$ es **de Cauchy** si*

$$\forall\ 0 < \epsilon \in \mathbb{R},\ \exists 0 < N \in \mathbb{N}\ tal\ que\ \ | a_m - a_n |< \epsilon,\ \forall m, n > N.$$

*La **sucesión** $\{a_n\}$ **converge a** $a \in K$ si*

$$\forall\ 0 < \epsilon \in \mathbb{R},\ \exists 0 < N \in \mathbb{N}\ tal\ que\ \ | a - a_n |< \epsilon,\ \forall n > N.$$

*Un cuerpo K es **completo** respecto a una valoración si toda sucesión de Cauchy de elementos de K converge a un elemento del cuerpo.*

Si consideramos $\mathfrak{C}$ el conjunto de todas las sucesiones de Cauchy de elementos de K y $\mathfrak{N}$ el subconjunto de todas las sucesiones convergentes a cero, resulta que $\mathfrak{C}$ forma un anillo

conmutativo con las operaciones adición y multiplicación definidas como

$$\{a_n\} + \{b_n\} = \{a_n + b_n\}$$

$$\{a_n\} \cdot \{b_n\} = \{a_n b_n\}$$

y con identidad $1_{\mathfrak{C}} = \{1\}$; y $\mathfrak{N}$ es un ideal maximal suyo ([J], pg. 91).

Teorema 1.7.1. ***Teorema de compleción.*** *([J], pgs. 91 − 93) Sea K un cuerpo con valoración $|\ |$. Entonces, el cuerpo $\hat{K} = \mathfrak{C}/\mathfrak{N}$ contiene una copia isomorfa de K y es completo respecto a la norma que extiende $|\ |$ a $\hat{K}$ definida por*

$$|\ \{x_n\} + \mathfrak{N}\ |_0 = \lim_{n\to\infty} |\ x_n\ |\ .$$

Diremos que $(\hat{K}, |\ |_0)$ es una **compleción** de $(K, |\ |)$. Además, esta compleción es única salvo isomorfismo ([J], pg. 94).

Denotaremos por $\mathbb{Q}_\infty$ a la compleción de $(\mathbb{Q}, |\ |_\infty)$, que es isomorfa al cuerpo de los números reales. Análogamente, denotaremos por $\mathbb{Q}_p$ a la compleción de $(\mathbb{Q}, |\ |_p)$ con $|\ |_p$ una valoración p-ádica. A esta compleción $\mathbb{Q}_p$ se la conoce como **cuerpo p-ádico**.

En la siguientes proposiciones, veremos que a partir de un anillo de valoración discreta podemos obtener un cuerpo completo respecto a una valoración no arquimediana y cómo se relacionan su anillo de valoración y el anillo de valoración discreta dado.

Proposición 1.7.3. *([J], pg. 94) Si $|\ |$ es una valoración no arquimediana en el cuerpo K cuyo anillo de valoración A es un AVD, entonces, el anillo de valoración $\hat{A}$ de la compleción $(K_{\mathfrak{p}}, |\ |)$ de $(K, |\ |)$ es también un AVD. Además, los ideales maximales de A y $\hat{A}$ son generados por el mismo elemento.*

En particular, dado un anillo de valoración discreta A con ideal maximal $\mathfrak{p} = \pi A$ y cuerpo de fracciones K; si consideramos la valoración $\mathfrak{p}$-ádica $|\ |$ sobre K tal que

$$|\ a\pi^k\ | = c^k$$

para $a \in A$ y $a \notin \mathfrak{p}$, k un entero y $c = |\ \pi\ |$ menor que uno. El anillo de valoración de la compleción $(K_{\mathfrak{p}}, |\ |)$ será un AVD y está definido por

$$\hat{A} = \{x\ \in\ K_{\mathfrak{p}} :|\ x\ | \leq 1\}$$

y su ideal maximal

$$\hat{\mathfrak{p}} = \{x\ \in\ K_{\mathfrak{p}} :|\ x\ | < 1\}.$$

Corolario 1.7.1. *([J], pg. 95) Dadas las mismas condiciones que en la proposición anterior, todo elemento α de $K_{\mathfrak{p}}$ es el límite de una sucesión $\{a_n\}$ de elementos de K donde $|\ a_n\ |$ es constante. Además, las unidades del anillo de valoración de $K_{\mathfrak{p}}$, $\hat{R}$, son los límites de las sucesiones de Cauchy $\{a_n\}$ de elementos de K tales que $|\ a_n\ | = 1$ para todo n.*

Proposición 1.7.4. *([J], pg. 95) Dado cualquier entero positivo n, la inclusión de A en $\hat{A}$ induce un isomorfismo*

$$A/\mathfrak{p}^n \cong \hat{A}/\hat{\mathfrak{p}}^n.$$

Dado un cuerpo K con una valoración no arquimediana $|\ |_\mathfrak{p}$, A su anillo de valoración, que asumiremos AVD, y $\mathfrak{p} = \pi A$ su ideal maximal, vamos a dar varios resultados que nos permitirán determinar valoraciones en una extensión L finita y separable de K tales que al restringirlas a K coinciden exactamente con $|\ |_\mathfrak{p}$. Veremos también que si K además es completo no solo se puede extender $|\ |_\mathfrak{p}$ a L si no que además esta extensión está determinada de forma única.

Teorema 1.7.2. *([J], pg. 101) Sea A un AVD con $\mathfrak{p}$ su ideal maximal y K su cuerpo de fracciones. Sea además B la clausura entera de A en una extensión finita separable L de K y $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ la factorización de $\mathfrak{p}B$ en ideales primos de B. Entonces, las valoraciones $\mathfrak{P}_i$-ádicas de L, con $1 \leq i \leq g$, restringidas a K son valoraciones equivalentes a la valoración $\mathfrak{p}$-ádica de K. Recíprocamente, cualquier valoración de L que extienda la valoración $\mathfrak{p}$-ádica de K es equivalente a una de las $\mathfrak{P}_i$-ádicas valoraciones de L. Las valoraciones exponenciales asociadas a dichas valoraciones se relacionan de la siguiente manera:*

$$v_{\mathfrak{P}_i}(x) = e_i v_\mathfrak{p}(x)$$

para todo $x \in K$ y e_i el índice de ramificación de $\mathfrak{P}_i$ sobre A.

Este teorema reduce el problema de determinar las valoraciones no arquimedianas de un cuerpo de números algebraicos a determinar la factorización de la extensión de un ideal primo de $\mathbb{Z}$ a la clausura algebraica de $\mathbb{Z}$ en el cuerpo de números.

Teorema 1.7.3. *([J], pgs. 103 – 104) Sea K un cuerpo completo respecto a una valoración no arquimediana $|\ |_\mathfrak{p}$ cuyo anillo de valoración A sea un AVD. Sea también una extensión finita y separable L de K de dimensión $[L : K] = n$. Entonces, la clausura entera de A en L es a su vez un AVD y L es completo respecto a la única extensión de $|\ |_\mathfrak{p}$ en L. Si denotamos por $|\ |$ a dicha extensión, se cumple que*

$$|\ y\ | = |\ N_{L/K}(y)\ |_\mathfrak{p}^{1/n}\ .$$

Es decir, si partimos de un cuerpo completo respecto una valoración $\mathfrak{p}$-ádica, $\mathfrak{p}B$ es una potencia de un ideal primo $\mathfrak{P}$ de B.

El siguiente teorema relaciona los índices de ramificación de los ideales primos de una extensión de un cuerpo algebraico de números y los índices de ramificación de dichos ideales en la compleción del cuerpo.

Teorema 1.7.4. *([J], pg. 106) Sea K un cuerpo de números algebraico que sea el cuerpo de fracciones de un AVD A con ideal maximal $\mathfrak{p}$. Sea además L una extensión finita de K con B la clausura entera de A en L y $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ la factorización de $\mathfrak{p}B$ en ideales*

primos de B. Entonces, dado $\mathfrak{P} = \mathfrak{P}_i$ para cierto i, $|\ |_{\mathfrak{p}}$ la valoración $\mathfrak{p}$-ádica de K y $|\ |_{\mathfrak{P}}$ la valoración $\mathfrak{P}$-ádica de L, se cumple:

- $\hat{\mathfrak{p}} = \mathfrak{p}\hat{A}$ *y* $\hat{\mathfrak{P}} = \mathfrak{P}\hat{B}$
- $e(\hat{\mathfrak{P}}/\hat{\mathfrak{p}}) = e(\mathfrak{P}/\mathfrak{p}) = e$
- $f(\hat{\mathfrak{P}}/\hat{\mathfrak{p}}) = f(\mathfrak{P}/\mathfrak{p}) = f$
- $[L_{\mathfrak{P}} : K_{\mathfrak{p}}] = ef$

donde $K_{\mathfrak{p}}$ y $L_{\mathfrak{P}}$ denotan la compleción de K y L respecto a las valoraciones $\mathfrak{p}$, $\mathfrak{P}$-ádicas respectivamente; $\hat{A}$ y $\hat{B}$ sus anillos de valoración y $\hat{\mathfrak{p}}$ y $\hat{\mathfrak{P}}$ los ideales maximales de estos.

Si además consideramos que la extensión es finita y no ramificada y que el cuerpo base es una compleción respecto a una valoración no arquimediana, vamos a poder encontrar un elemento primitivo que genere la extensión, como afirma el siguiente teorema:

Teorema 1.7.5. *([J], pg.* 107*) Sean K un cuerpo de números y L una extensión de dimensión finita de la compleción $K_{\mathfrak{p}}$ tal que $\mathfrak{p}$ sea no ramificado en ella. Entonces,*

$$L = K_{\mathfrak{p}}(\beta)$$

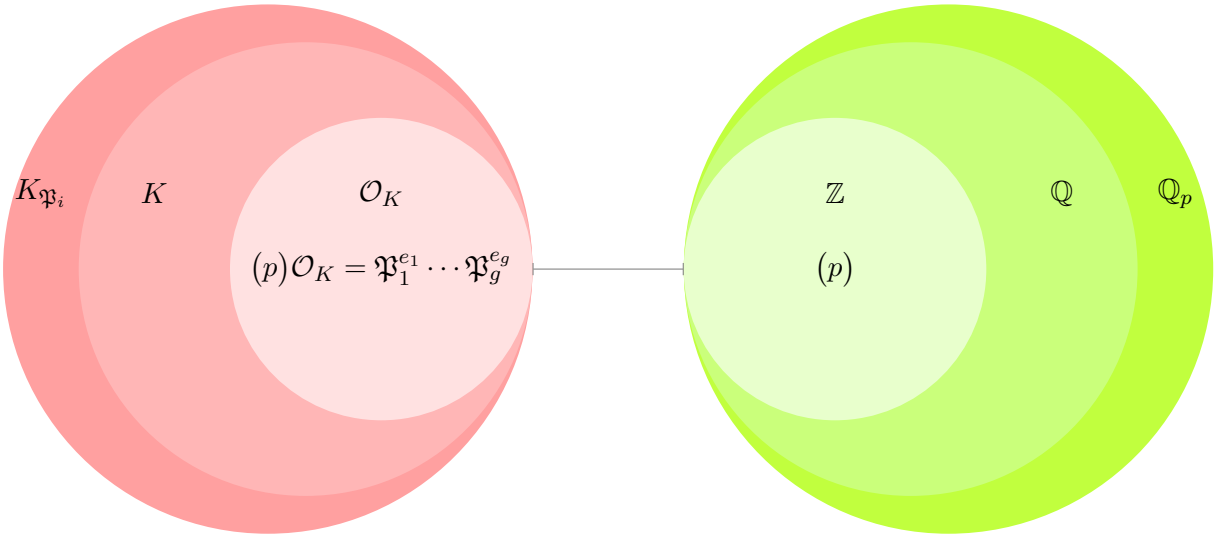
con β una raíz primitiva de la unidad de orden $f = [L : K_{\mathfrak{p}}]$. Además, para cualquier entero positivo f dado, dada una raíz primitiva f-ésima de la unidad β, la extensión $K_{\mathfrak{p}}(\beta)/K_{\mathfrak{p}}$ es no ramificada y tiene grado f.

El siguiente teorema nos va a permitir describir las valoraciones arquimedianas de un cuerpo de números algebraico.

Teorema 1.7.6. ***Teorema de Ostroski.*** *([J], pg.* 108*) Sea K un cuerpo completo respecto a una valoración arquimediana $|\ |$. Entonces, el cuerpo K es isomorfo al cuerpo de los números reales o al cuerpo de los números complejos y dicha valoración es equivalente al valor absoluto usual.*

Con lo cual, dado un cuerpo algebraico de números y una valoración arquimediana $|\ |_1$ en él, su compleción $\hat{K}$ es isomorfa a $\mathbb{R}$ o a $\mathbb{C}$. Además, si denotamos por ϕ a ese isomorfismo, se cumple que $|\ x\ |_1 = |\ \phi(x)\ |$ para todo $x \in K$ donde $|\ |$ denota el valor absoluto usual en $\mathbb{R}$ o en $\mathbb{C}$ ([J], pg. 109).

Con esta información podemos extender el concepto de primo infinito de un cuerpo. Decíamos que una clase de valoraciones equivalentes de un cuerpo K se llamaba primo infinito de dicho cuerpo si contenía una valoración arquimediana. Si la compleción del cuerpo con una valoración arquimediana dada es isomorfa al cuerpo de los números reales, diremos que la clase de equivalencia que contiene esa valoración es un **primo real** de K, y si por el contrario es isomorfa al cuerpo de los complejos diremos que la clase de equivalencia a la que pertenece la valoración es un **primo complejo** de K.



1.8. Grupo de descomposición y grupo de inercia

En esta sección vamos a considerar que K es un cuerpo de números algebraico y L una extensión finita de Galois del mismo, cuyo grupo de Galois lo denotaremos por G. Presentaremos resultados que relacionan lo números de ramificación y grados relativos de los primos de K con los subgrupos de G. Aunque la mayoría de resultados se cumplen tanto para primos finitos como infinitos, nosotros vamos a estar interesados especialmente en los primeros.

Definición 1.8.1. *Sea K un cuerpo de números algebraicos, $\mathfrak{p}$ un primo de K y L una extensión finita y de Galois de K. Sean $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ los primos de L tales que $\mathfrak{p} = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$ con $e = e(\mathfrak{P}_i/\mathfrak{p})$ su índice de ramificación. Se llama* ***grupo de descomposición de*** *$\mathfrak{P}$ para $\mathfrak{P} \in \{\mathfrak{P}_1, \ldots, \mathfrak{P}_g\}$ a*

$$G(\mathfrak{P}) = \{\sigma \in Gal(L/K) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

En el caso de que $\mathfrak{p}$ sea un primo de K finito, podemos identificar cada $\mathfrak{P}_i$ con un ideal del anillo de enteros algebraicos en L y $\sigma(\mathfrak{P}_i)$ será simplemente el ideal obtenido al aplicar σ a cada uno de los elementos de $\mathfrak{P}_i$. Si por el contrario, alguno de los $\mathfrak{P}_i$ que intervienen en la factorización de $\mathfrak{p}$ es un primo infinito de L, podemos identificar $\mathfrak{P}_i$ con un homomorfismo de anillos τ_i de L en $\mathbb{R}$ o $\mathbb{C}$ y $\sigma(\mathfrak{P}_i)$ será el primo infinito de L que se identifica con el homomorfismo $\tau_i\sigma^{-1}$.

Teorema 1.8.1. *([J], pgs. $122 - 123$) Sea $\mathfrak{P}_i$ una extensión en L del primo $\mathfrak{p}$ de K y sea $G(\mathfrak{P})$ el grupo de descomposición de $\mathfrak{P}$ en el grupo de Galois G de la extensión L/K. Entonces, $L_{\mathfrak{P}}$ es una extensión de Galois de $K_{\mathfrak{p}}$ con grupo de Galois $G(\mathfrak{P})$, y*

$$\mid G(\mathfrak{P}) \mid = e(\mathfrak{P}/\mathfrak{p}) f(\mathfrak{P}/\mathfrak{p}).$$

Definición 1.8.2. *Sea $\mathfrak{p}$ un primo finito de K. Sea A el anillo de valoraciones correspondiente a $\mathfrak{p}$, por tanto con $\mathfrak{p}$ ideal maximal, y sea B la clausura entera de A en L. Sea $\mathfrak{P}$ un ideal primo de B que contenga a $\mathfrak{p}$. Como dado $\sigma \in G(\mathfrak{P})$ se cumple que $\sigma(\mathfrak{P}) = \mathfrak{P}$, σ induce un automorfismo $\hat{\sigma}$ en el anillo $\hat{B} = B/\mathfrak{P}$ definido por*

$$\hat{\sigma}(x + \mathfrak{P}) = \sigma(x) + \mathfrak{P},\ x \in B.$$

Si consideramos $\hat{A} = A/\mathfrak{p}$, el automorfismo $\hat{\sigma}$ es un elemento del grupo de Galois de $\hat{B}$ sobre $\hat{A}$. La correspondencia $\sigma \mapsto \hat{\sigma}$ es un homomorfismo de $G(\mathfrak{P})$ a $Gal(\hat{B}/\hat{A})$. Llamamos ***grupo de inercia de*** *$\mathfrak{P}$ al núcleo de dicho homomorfismo y lo denotamos por $T(\mathfrak{P})$.*

Propiedad 1.8.1. *([J], pg. 96) Bajo las condiciones de la definición anterior se verifica:*

- *El homomorfismo de $G(\mathfrak{P})$ a $Gal(\hat{B}/\hat{A})$ dado por $\sigma \mapsto \hat{\sigma}$ es suprayectivo.*
- $\mid T(\mathfrak{P}) \mid = e(\mathfrak{P}/\mathfrak{p}) = e$.

1.9. Grupo radial

En esta sección vamos a ampliar el concepto de grupo de clases teniendo en cuenta las compleciones de un cuerpo de números.

Sean K un cuerpo algebraico de números, A su anillo de enteros algebraicos, $\mathfrak{p}$ un primo de K (finito o infinito) y $K_{\mathfrak{p}}$ la compleción de K respecto a una valoración contenida en ese primo.

Consideremos la aplicación

$$\begin{aligned} \iota : K^* &\to I_K \\ \alpha &\mapsto (\alpha) = \alpha A \end{aligned}$$

donde $K^* = K \backslash \{0\}$ e I_K denota el grupo de los A-ideales fraccionarios de K.

El núcleo de esta aplicación es el grupo U_K de las unidades de A y su co-núcleo, $I_K/\iota(K^*)$, es el grupo de clases de K, es decir, C_K. Estos grupos forman una cadena exacta

$$1 \to U_K \to K^* \xrightarrow{\iota} I_K \to C_K \to 1$$

La teoría de cuerpos de clases busca estudiar los términos de esta cadena y sus componentes y cómo se relacionan entre ellos con el objetivo de describir todas las extensiones abelianas de K.

Con este fin, aparece el concepto de módulo que definimos a continuación.

Definición 1.9.1. *Un **módulo** de K se define como producto formal*

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}$$

sobre todos los primos, finitos e infinitos, de K donde cada exponente $n(\mathfrak{p})$ es un entero no negativo y $n(\mathfrak{p}) > 0$ solo para un número finito de primos. Además, si $\mathfrak{p}$ es un primo real infinito entonces $n(\mathfrak{p}) = 0$ o 1 y $n(\mathfrak{p}) = 0$ si es un primo complejo infinito. Un módulo $\mathfrak{m}$ puede ser considerado como un producto $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ con

$$\mathfrak{m}_0 = \prod_{\mathfrak{p}\ finito} \mathfrak{p}^{n(\mathfrak{p})}, \quad \mathfrak{m}_\infty = \prod_{\mathfrak{p}\ real} \mathfrak{p}^{n(\mathfrak{p})}.$$

*Este $\mathfrak{m}_0$ es un ideal de A y $\mathfrak{m}_\infty$ es un producto de algún subconjunto de los primos infinitos reales de K. Nos referiremos a $\mathfrak{m}_0$ como **parte finita** de $\mathfrak{m}$ y a $\mathfrak{m}_\infty$ como **parte infinita**.*

Vamos a extender la noción de congruencia entre dos elementos de A módulo un ideal, a la noción de congruencia entre dos elementos de K^* módulo un módulo. La llamaremos **congruencia multiplicativa**.

Sea $\mathfrak{p}$ un primo real de K y sea $x \to x_\mathfrak{p}$ la inclusión de x en la compleción $K_\mathfrak{p} \cong \mathbb{R}$. Para $\alpha, \beta \in K^*$ escribimos

$$\alpha \equiv^* \beta \ mod\ \mathfrak{p}$$

para expresar que $\alpha_\mathfrak{p}$ y $\beta_\mathfrak{p}$ tienen el mismo signo, es decir, $(\alpha/\beta)_\mathfrak{p} > 0$.

Ahora consideremos $\mathfrak{p}$ un primo finito de K y n un entero positivo. Dados dos elementos $\alpha, \beta \in K^*$ escribimos

$$\alpha \ \equiv \ \beta \ mod^*\ \mathfrak{p}^n$$

si α pertenece a $\beta(1 + \mathfrak{p}^n A_\mathfrak{p})$. Equivalentemente, podríamos decir que $\alpha \ \equiv^* \ \beta \ mod\ \mathfrak{p}^n$ si y solo si α/β es una unidad de la localización $A_\mathfrak{p}$ y

$$v_\mathfrak{p}\Big(\frac{\alpha}{\beta} - 1\Big) \geq n$$

donde $v_\mathfrak{p}$ denota la valoración exponencial $\mathfrak{p}$.

Tomemos entonces un módulo $\mathfrak{m}$ como los definidos anteriormente. Para dos elementos $\alpha, \beta \in K^*$ escribiremos

$$\alpha \ \equiv^* \ \beta \ mod\ \mathfrak{m}$$

si

$$\alpha \ \equiv^* \ \beta \ mod\ \mathfrak{p}^{n(\mathfrak{p})}$$

para todos los primos $\mathfrak{p}$ de K con $n(\mathfrak{p}) > 0$ en $\mathfrak{m}$.

De forma inmediata tenemos que si $\alpha \equiv^* \beta \ mod\ \mathfrak{m}$ y $\alpha_1 \equiv^* \beta_1 \ mod\ \mathfrak{m}$ entonces

$$\alpha\alpha_1 \equiv^* \beta\beta_1 \ mod\ \mathfrak{m}.$$

La suma sin embargo no va a preservar la congruencia dado que no es una operación interna en K^*.

Dado un módulo de K $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ con $\mathfrak{m}_0$ parte finita y $\mathfrak{m}_\infty$ parte infinita, nos van a interesar especialmente dos subgrupos de K^* asociados a él:

$$K_\mathfrak{m} = \{a/b : a, b \in A \text{ y } aA,\ bA \textit{ primos respecto a } \mathfrak{m}_0\} \text{ y}$$

$$K_{\mathfrak{m},1} = \{\alpha \ \in \ K_\mathfrak{m} : \alpha \ \equiv^* \ 1 \ mod \ \mathfrak{m}\}.$$

Nótese que $K_\mathfrak{m}$ depende solo de los primos finitos que dividen $\mathfrak{m}$ y no de sus exponentes. El grupo $K_{\mathfrak{m},1}$ depende tanto de los primos finitos como los infinitos y también de sus exponentes.

Definición 1.9.2. *Sea $I^\mathfrak{m}$ el grupo generado por los ideales primos de A que no dividen a $\mathfrak{m}_0$. Se llama* ***grupo radial módulo*** $\mathfrak{m}$ *al cociente*

$$I^\mathfrak{m}/\iota(K_{\mathfrak{m},1}).$$

Las clases de este cociente se conocen como ***clases radiales módulo*** $\mathfrak{m}$.

Cabe destacar que $I^\mathfrak{m}$ depende de los primos finitos que dividen a $\mathfrak{m}$ pero no de sus exponentes. Además, el grupo radial de clases es un grupo finito para cualquier módulo dado ([J], pg. 141).

Las nociones que hemos introducido en esta sección van a ser piezas centrales en el desarrollo de la teoría de cuerpos de clases, que, como hemos adelantado anteriormente, busca clasificar las extensiones abelianas de un cuerpo de números dado.

Capítulo 2

Motivación e Historia

A lo largo de la historia de las matemáticas se han publicado libros que han marcado un antes y un después. Un ejemplo indiscutible son los «Elementos» de Euclides (*aprox.* 325 *a.C.* − *aprox.* 265 *a.C.*), un tratado de trece libros que recoge el saber matemático conocido hasta la época del sabio griego. En estos libros aparece por primera vez un sistema axiomático del que se deben derivar el resto de afirmaciones y desde entonces hasta nuestros días, el estudio de las matemáticas se sustenta en sistemas axiomáticos.

De la misma forma que los «Elementos» establecieron una nueva línea de trabajo en el desarrollo de la geometría, la publicación de «*Disquisitiones Arithmeticae*» de Johann Carl Friedrich Gauss (1777−1855) inauguró una nueva era en la teoría de números. En este libro Gauss recopiló, corrigió, amplió y conectó entre sí los resultados sobre aritmética y teoría de números que existían, dando lugar a más de trescientos cincuenta artículos breves sobre la materia. Sin embargo, este gran matemático destacó un resultado por encima de todos los demás, al que se referiría como *Theorema Aureum* y al que dedicó muchos desvelos a lo largo de toda su carrera profesional. Se trata, concretamente, de la «ley de reciprocidad cuadrática».

En realidad, la ley de reciprocidad cuadrática ya había sido enunciada por Leonhard Euler (1707 − 1783), pero fue Gauss quien la probó por primera vez. Enfatizamos «por primera vez» porque a esta prueba le siguieron otras cinco distintas del mismo autor, cinco de Eisenstein, otra de Dirichlet, otra de Kummer, otra de Lebesgue, otra de Kroneker ... y podríamos seguir así hasta las 196 demostraciones que recoge Franz Lemmermeyer en [L].

¿Qué establece esta ley que la hace tan única y relevante? ¿Por qué obsesionó a tantas generaciones de matemáticos? A lo largo de este capítulo daremos respuesta a ambas preguntas.

2.1. La ley de reciprocidad cuadrática

Si buscamos en cualquier libro de introducción a la teoría algebraica de números, veremos que esta rama se dedica principalmente al estudio de los cuerpos algebraicos de números y sus propiedades. Sin embargo, esta concepción de la disciplina surge a partir del ya mencionado «*Disquisitiones Arithmeticae*» de J. C. F. Gauss. Anteriormente, la teoría de números era, más que una teoría, un conjunto de resultados desconexos entre sí, referentes en muchos de los casos, a la resolución de ecuaciones diofánticas. Una **ecuación diofántica** es una ecuación en varias variables cuya solución o soluciones son números enteros o racionales. El apelativo «diofánticas» se debe a Diofanto de Alejandría $(200-284)$ quien recopiló en trece libros 130 problemas que se reducen a una ecuación de estas características. Por ejemplo, uno de los más famosos es el problema 8 del libro II, titulado «descomponer un cuadrado en dos cuadrados». En él, Diofanto busca una solución para la ecuación

$$x^2 + y^2 = 16 \text{ } con \text{ } x, y \in \mathbb{Q}.$$

Como se puede ver, se trata de un enunciado aparentemente sencillo y fácil de comprender. Todos los problemas de esta índole comparten dicha característica, si bien por norma general, la complejidad de su resolución es inversamente proporcional a la de su planteamiento. Tanto es así que, en pos de dar solución a muchos de ellos, se han desarrollado a lo largo de la historia gran parte de las fórmulas, leyes y teoremas que dan forma a la teoría de números. La ley que aquí nos compete es una de ellas, pero vamos a indagar un poco más en el contexto en el que surge para convencernos de su relevancia.

Una vez hemos visto cómo descomponer un cuadrado en la suma de dos cuadrados, podemos plantearnos otras preguntas semejantes como ¿puedo descomponer un número cualquiera como suma de dos cuadrados? ¿y como suma de dos números enteros al cuadrado? Vamos a ser «menos» ambiciosos, y vamos a quedarnos en los números primos,

$$\textit{Dado } p \textit{ un número primo, ¿existen } x, y \in \mathbb{Z} \textit{ tales que } p = x^2 + y^2 \textit{?}$$

Lo primero que haríamos después de plantearnos esta pregunta sería ir tanteando con algunos números primos. Por ejemplo, si el primo dado es 17, 29 o 53 la respuesta sería afirmativa ya que $4^2+1^2 = 17$, $5^2+2^2 = 29$ y $7^2+2^2 = 53$. De hecho, para cualquier primo suficientemente pequeño podríamos dirimir la cuestión probando con todos los enteros que *a priori* podrían ser solución. Pero, ¿qué pasa si nos dan un primo de más de veintidós millones de cifras? En este caso, el método del tanteo parece completamente ineficiente, incluso seguramente inviable con los medios que tenemos a mano. Ante esta situación, podríamos pensar en buscar una condición que (creamos que) cumplan aquellos primos para los cuales sí exista solución de la ecuación y a continuación probar o refutar la conjetura formulada.

Por ejemplo, sabemos que 17, 29 y 53 verifican la ecuación y todos ellos cumplen que $p+1$

es un múltiplo de 3 (es decir, $p \equiv 2\ mod(3)$) para $p \in \{17, 29, 53\}$. Proponemos por tanto la siguiente conjetura:

Conjetura 2.1.1. *Sea p un número primo impar. Entonces, existen dos números enteros x e y tales que*

$$p \equiv 2\ mod(3) \Leftrightarrow p = x^2 + y^2$$

Rápidamente encontramos un contraejemplo ya que, por un lado, 11 es un número primo tal que $11 + 1 = 12 = 4 \cdot 3$ pero $11 \neq x^2 + y^2$ para ningún entero x, y. Y, por otro, el número primo $37 = 1^2 + 6^2$ y sin embargo, $37 + 1 = 38$ no es múltiplo de 3.

Parece ser que, al fin y al cabo, la pregunta propuesta no es tan inocente. Afortunadamente, Pierre de Fermat $(1601 - 1665)$ ya se peleó con el problema hace casi cuatrocientos años y formuló una conjetura que aparentemente funcionaba:

Conjetura 2.1.2. ***Pierre de Fermat*** *(1640). Sea p un número primo impar. Entonces, existen dos enteros x e y tales que*

$$p = x^2 + y^2 \Leftrightarrow p \equiv 1\ mod(4)$$

Ver que $p = x^2 + y^2 \Rightarrow p \equiv 1\ mod(4)$ es inmediato: si x es congruente con 0 o 2 módulo 4, entonces x^2 es múltiplo de 4[1]; y si es congruente con 1 o 3 módulo 4, entonces su cuadrado es congruente con 1 módulo 4. Por lo tanto, $x^2 + y^2$ solo puede ser congruente con 0, 1 o 2 módulo 4. Si $x^2 + y^2 \equiv 0\ mod(4)$, entonces 4 dividiría a $x^2 + y^2$, pero estamos suponiendo que dicha suma es un número primo, por lo que llegamos a una contradicción. Si $x^2 + y^2 \equiv 2\ mod(4)$, entonces $x^2 + y^2 = p$ es par, con lo que llegamos de nuevo a una contradicción.

La otra implicación, como decíamos, aparentemente es cierta ya que si tomamos los primos del 1 al 100 congruentes con 1 módulo 4 podemos escribirlos como suma de cuadrados,pero ¿qué pasa con los primos mayores que cien? ¿Y con los primos mayores que el mayor primo conocido?

Para poder estar seguros de que esta caracterización es cierta deberíamos probar la implicación necesaria en general o, en este caso, consultar la demostración que dio Leonhard Paul Euler $(1707 - 1783)$ en 1749 de la misma. El hecho de que entre que se planteó la conjetura y su demostración mediasen cien años puede verse como un indicativo de que no se trataba de un problema baladí. Sin embargo, no es su complejidad lo que hace de este un resultado destacable, sino el hecho de que en su demostración se utilizó por primera vez, aunque de forma indirecta, la hoy conocida como ley de reciprocidad cuadrática.

La demostración que dio L. P. Euler del teorema consistía en dos pasos:

1− Primero, probó que si $p \mid a^2 + b^2$, con $a, b \in \mathbb{Z}$ y $mcd(a, b) = 1$, entonces p se puede expresar como suma de cuadrados.

[1] Si $a_1 \equiv b_1\ mod(n)$ y $a_2 \equiv b_2\ mod(n)$ entonces $a_1 + a_2 \equiv b_1 + b_2\ mod(n)$ y $a_1 a_2 \equiv b_1 b_2\ mod(n)$.

2− Después probó que si $p \equiv 1 \ mod \ 4$ entonces existen $a, b \in \mathbb{Z}$ con $mcd(a, b) = 1$ tales que $p \mid a^2 + b^2$.

$5 = 1^2 + 2^2$
$13 = 2^2 + 3^2$
$17 = 1^2 + 4^2$
$29 = 2^2 + 5^2$
$37 = 1^2 + 6^2$
$41 = 4^2 + 5^2$
$53 = 2^2 + 7^2$
$61 = 5^2 + 6^2$
$73 = 3^2 + 8^2$
$89 = 5^2 + 8^2$
$97 = 4^2 + 9^2$

Fue este segundo paso el que le llevó a enunciar la ley de reciprocidad cuadrática años más tarde, la cual le permitiría resolver fácilmente esta y otras ecuaciones similares. Por comodidad, nosotros la enunciaremos usando la notación introducida por Adrien-Marie Legendre en 1798 en «*Essai sur la Théorie de nombres*»:

Definición 2.1.1. *Dado un primo impar p y un entero a no divisible entre p, definimos el* ***símbolo de Legendre*** *como*

$$\left(\frac{a}{p}\right) := \begin{cases} 1, \ \textit{si existe } x \textit{ tal que } x^2 \equiv a \ mod \ p \\ -1, \ \textit{en otro caso} \end{cases} \tag{2.1}$$

Además, si $\left(\frac{a}{p}\right) = 1$ decimos que a es un resto cuadrático de p.

Teorema 2.1.1. ***Ley de reciprocidad cuadrática.*** *Dados p y q dos primos impares distintos entre sí, se cumple que*

$$\left(\frac{p}{q}\right) = (-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)}\left(\frac{q}{p}\right) \tag{2.2}$$

Esta ley establece una reciprocidad entre dos primos impares, ya que según su enunciado, un primo impar p es un resto cuadrático de otro primo impar q si y solo si q también lo es de p, salvo que p y q sean congruentes con 3 módulo 4, en cuyo caso solo uno de los primos es resto cuadrático del otro.

Esta implicación se deduce fácilmente de la fórmula (2.2) ya que si $p \equiv q \equiv 3 \ mod \ 4$, entonces $\frac{(p-1)(q-1)}{4} \equiv 1 \ mod \ 4$ y por tanto,

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

En caso contrario, al menos uno de ellos (s.p.g. podemos considerar p) tiene que ser congruente con 1 módulo 4, con lo cual $\frac{(p-1)}{2} \equiv 0 \ mod \ 4$ y $\frac{1}{2}(p-1)\frac{1}{2}(q-1)$ es un número par.

Es decir,

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right).$$

Además, de esta ley se deducen otras dos leyes muy útiles a la hora de resolver ecuaciones diofánticas:

Teorema 2.1.2. ***Leyes complementarias.*** *Sea p un primo impar. Se cumple que*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)} \tag{2.3}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)} \tag{2.4}$$

Para ilustrar un claro ejemplo de ello, vamos a cerrar la sección demostrando que $p \equiv 1 \ mod \ 4 \Rightarrow p = x^2 + y^2$, siguiendo el esquema de L. P. Euler.

Para ver que si p divide una suma de cuadrados él se puede expresar a su vez como una suma de cuadrados vamos a aplicar un razonamiento que se conoce como **descenso infinito**. Vamos a ver que si $p \mid a^2+b^2$ y no existen $a', b' \in \mathbb{Z}$ tales que $p = a'^2+b'^2$ entonces existe un primo estrictamente más pequeño que p que divide una suma de cuadrados y tampoco se puede escribir como suma de cuadrados. De esta forma podríamos obtener primos cada vez más pequeños que cumplen dichas condiciones *ad infinitum* lo que contradice el principio de buena ordenación de los números naturales.

Antes de empezar, vamos a dar un lema que nos facilitará la demostración:

Lema 2.1.1. *Sean $N = a^2+b^2$ con $a, b \in \mathbb{Z}$ primos entre sí y $q = c^2+d^2$ un divisor primo de N. Entonces, N/q es a su vez una suma de dos enteros al cuadrado primos entre sí.*

Demostración:

Como q es divisor de N, en particular divide a $c^2N - a^2q$ que es igual a $c^2N - a^2q = c^2a^2 + c^2b^2 - a^2c^2 - a^2d^2 = c^2b^2 - a^2d^2 = (cb-ad)(cb+ad)$, así que $q \mid cb-ad$ o $q|cb+ad$. Sin pérdida de generalidad podemos suponer que $p|cb-ad$ y por tanto existe un $n \in \mathbb{Z}$ tal que

$$cb - ad = qn.$$

Además, c divide a $(a+nd)d$ ya que

$$(a+nd)d = c(b-cn).$$

Pero c y d son primos entre sí, así que c divide a $a+nd$, es decir,

$$a + nd = cm.$$

Despejando tenemos por tanto que $cmd = (a+nd)d = c(b-cn)$, es decir, $b = dm+cn$ y $a = cm-dn$, luego $N = a^2+b^2 = (dm+cn)^2+(cm-dn)^2 = (c^2+d^2)(n^2+m^2) =$

$q(n^2+m^2)$ y

$$\frac{N}{q} = n^2 + m^2.$$

Q.E.D.

Sea entonces un número primo p tal que existen $a, b \in \mathbb{Z}$ primos entre sí tales que $p \mid a^2+b^2$. Sin pérdida de generalidad podemos suponer que $|a|$ y $|b|$ son menores o iguales que $\frac{p}{2}$, ya que si $|a| > \frac{p}{2}$ y/o $|b| > \frac{p}{2}$ basta considerar $a_1 = p - a$ y/o $b_1 = p - b$ para que se cumplan las hipótesis.

Supongamos ahora que p no se puede expresar como suma de cuadrados. En particular, $p \neq a^2 + b^2$ y por tanto existe un entero $d \neq 0$ tal que $pd = a^2 + b^2$. Como $|a|$ y $|b|$ son menores o iguales que $\frac{p}{2}$ tenemos que $pd \leq \frac{p^2}{4}$ y por tanto $d < p$. Con lo cual, existe un primo q estrictamente menor que p que divide a $a^2 + b^2$. Además, q no se puede escribir como suma de cuadrados: si $q = c^2 + d^2$ con $c, d \in \mathbb{Z}$ entonces, por el lema (2.1.1), $\frac{a^2+b^2}{q}$ también es suma de cuadrados y p es divisor de dicha suma. Con un razonamiento análogo al anterior vemos que podemos construir una sucesión de primos estrictamente decreciente, con lo cual concluímos que no existen $c, d \in \mathbb{Z}$ tales que $q = c^2 + d^2$.

Considerando q en el papel de p del razonamiento previo, vemos que existe un primo estrictamente menor que q que también divide una suma de cuadrados pero no lo es, a partir del cuál podríamos obtener otro primo estrictamente menor a los tres anteriores que cumple las mismas condiciones y así sucesivamente. Como el conjunto de los números primos es subconjunto de los números naturales tiene que tener mínimo, así que hemos llegado de nuevo a una contradicción. Es decir, podemos concluir que existen $x, y \in \mathbb{Z}$ tales que $p = x^2 + y^2$.

Quedaría probar que si $p \equiv 1 \ mod \ 4$ entonces existen $a, b \in \mathbb{Z}$ con $mcd(a, b) = 1$ tales que $p \mid a^2 + b^2$. Como ya hemos mencionado, en tiempos de L. P. Euler probar este resultado suponía todo un reto, sin embargo, con la ley de reciprocidad cuadrática y sus leyes suplementarias a nuestra disposición, es inmediato: si $p \equiv 1 \ mod \ 4$, entonces $p = 4n+1$ y por (2.3) -1 es un resto cuadrático de p, es decir, existe $a \in \mathbb{Z}$ tal que $p \mid a^2 + 1$.

2.2. Otras leyes de reciprocidad

El estudio de Gauss sobre la reciprocidad entre primos no se limitó a los restos cuadráticos. En 1828 y 1832 publicó dos memorias sobre restos bicuadráticos (cuárticos) en los que enunciaba la ley de reciprocidad cúbica y bicuadrática. Al igual que la ley de reciprocidad cuadrática estas leyes permitían resolver fácilmente ciertas ecuaciones diofánticas, amén de otras aplicaciones dentro de la teoría de números; aunque para entonces, el estudio de las leyes de reciprocidad había adquirido identidad propia.

Una de las novedades que aparece con estas dos leyes es el hecho de que para poder definirlas hay que salirse de $\mathbb{Z}$. En el caso de la ley de reciprocidad cúbica necesitamos considerar el

Johann Carl Friedrich Gauss (1777 – 1855) es considerado uno de los mejores matemáticos de la historia, hasta el punto de ser reconocido por el título oficioso de «príncipe de las matemáticas». Este matemático alemán se dedicó a gran variedad de áreas tanto de física como de matemáticas y en todas ellas alcanzó logros destacables. Uno de los resultados de los que se sintió más orgulloso en vida fue resolver el problema de construir un polígono regular de 17 lados utilizando únicamente regla y compás. No obstante, lo que le daría fama internacional más allá de los círculos matemáticos, fue la predicción correcta de la órbita de Ceres. [a]

A pesar de que J. C. F. Gauss hizo avanzar la teoría de números a pasos agigantados, en este trabajo no ocupa un lugar destacado por su obra sino por los interrogantes que dejó abiertos, ya que fue el primero en plantear la pregunta a la que queremos dar respuesta:

¿existe una ley de reciprocidad general?

[a] `http://www-history.mcs.st-andrews.ac.uk/Biographies/Gauss.html` Fecha de acceso: 04/04/2017.

Figura 2.1: J. C. F. Gauss con 26 años, dos años después de que se publicase por primera vez «*Disquisitiones arithmeticae*».

anillo de enteros de Eisenstein $\mathbb{Z}[\omega] = \{a + b\omega : a,\ b \in \mathbb{Z}\}$ con $\omega = (-1 + i\sqrt{3})/2$[2]. Este anillo es un dominio euclídeo y por tanto de factorización única. Sus unidades son los enteros de Eisenstein $\pm 1,\ \pm\omega,\ \pm\omega^2$ y sus primos son, salvo unidades, de uno de estos tres tipos:

i) $1 - \omega$.

ii) Un entero de Eisenstein $a + b\omega$ ó $a + b\omega^2$ tal que $(a + b\omega)(a + b\omega^2)$ es un primo entero congruente con 1 módulo 3.

iii) Un entero de Eisenstein $a + b\omega$ con $b = 0$ y a un primo entero congruente con 2 módulo 3.

En este contexto podemos extender la definición del símbolo de Legendre como sigue:

Definición 2.2.1. *Dados un primo $\pi \in \mathbb{Z}[\omega]$ que no divida a 3 en el anillo de Eisenstein, y α un entero de Eisenstein no divisible por π, definimos el* ***símbolo de Legendre*** $(\frac{\alpha}{\pi})_3$

[2] Nótese que dado $\alpha = a + b\omega \in \mathbb{Z}[\omega] \subset \mathbb{C}$, su conjugado $\bar{\alpha} = a + b\omega^2$.

como

$$\left(\frac{\alpha}{\pi}\right)_3 := \begin{cases} 1 \ si \ \alpha^{(N(\pi)-1)/3} \equiv 1 \ mod \ \pi \\ \omega \ si \ \alpha^{(N(\pi)-1)/3} \equiv \omega \ mod \ \pi \\ \omega^2 \ si \ \alpha^{(N(\pi)-1)/3} \equiv \omega^2 \ mod \ \pi \end{cases} \tag{2.5}$$

donde $N(\pi) = \pi\bar{\pi}$.

Bajo esta notación, se cumple que α es resto cúbico de π en $\mathbb{Z}[\omega]$ si y solo si $(\frac{\alpha}{\pi})_3 = 1$; y podemos establecer una reciprocidad entre los primos de este anillo atendiendo a su condición de resto cúbico.

Teorema 2.2.1. ***Ley de reciprocidad cúbica.*** *Si π y θ son primos de $\mathbb{Z}[\omega]$ tales que $\pi \equiv \theta \equiv \pm 1 \ mod \ 3$ y $N(\pi) \neq N(\theta)$, entonces*

$$(\frac{\theta}{\pi})_3 = (\frac{\pi}{\theta})_3.$$

Para enunciar la ley de reciprocidad bicuadrática también hay que situarse en una extensión de $\mathbb{Z}$, concretamente, en el **anillo de enteros de Gauss** $\mathbb{Z}[i] = \{a + bi : a, \ b \in \mathbb{Z}\}$ con $i = \sqrt{-1}$. Este anillo también es un dominio euclídeo y en consecuencia dominio de factorización única. En este caso, las unidades del anillo son ± 1, $\pm i$ y sus primos son, salvo unidades, de uno de estos tres tipos:

i) $1 + i$.

ii) Un entero de Gauss $a+bi$ ó $a-bi$ tal que $(a+bi)(a-bi)$ es un primo entero congruente con 1 módulo 4.

iii) Un entero de Gauss $a+bi$ con $b = 0$ y a un primo entero congruente con 3 módulo 4.

Para elementos de este anillo, se define el símbolo de Legendre de la siguiente manera:

Definición 2.2.2. *Dados un primo $\pi \in \mathbb{Z}[i]$ que no divida a 2 en el anillo de Gauss, y α un entero de Gauss no divisible por π, definimos el* ***símbolo de Legendre*** $(\frac{\alpha}{\pi})_4$ *como*

$$\left(\frac{\alpha}{\pi}\right)_4 := \begin{cases} 1 \ si \ \alpha^{(N(\pi)-1)/4} \equiv 1 \ mod \ \pi \\ -1 \ si \ \alpha^{(N(\pi)-1)/4} \equiv -1 \ mod \ \pi \\ i \ si \ \alpha^{(N(\pi)-1)/4} \equiv i \ mod \ \pi \\ -i \ si \ \alpha^{(N(\pi)-1)/4} \equiv -i \ mod \ \pi \end{cases} \tag{2.6}$$

donde $N(\pi) = \pi\bar{\pi}$.

Al igual que en el caso anterior, se cumple que α es resto bicuadrático de π en $\mathbb{Z}[i]$ si y solo si $(\frac{\alpha}{\pi})_4 = 1$; y podemos establecer una reciprocidad entre los primos de este anillo atendiendo a su condición de resto bicuadrático.

Teorema 2.2.2. ***Ley de reciprocidad bicuadrática.*** *Si π y θ son primos de $\mathbb{Z}[i]$ tales que $\pi \equiv \theta \equiv 1$ mod $2+2i$, entonces*

$$(\frac{\theta}{\pi})_4 = (\frac{\pi}{\theta})_4 (-1)^{(N(\theta)-1)(N(\pi)-1)/16}.$$

Ambas leyes fueron probadas de forma completa por Ferdinand Gotthold Max Eisenstein $(1823-1852)$ en 1844, aunque muchos años antes habían permitido a Gauss demostrar algunos de los resultados que darían lugar a sus memorias sobre restos bicuadráticos. A modo de ejemplo, veamos cómo la ley de reciprocidad cúbica permite probar el siguiente teorema:

Teorema 2.2.3. *Sea p un primo entero. Entonces, $p = x^2 + 27y^2$ si y solo si $p \equiv 1$ mod 3 y 2 es un resto cúbico de p.*

Este teorema fue conjeturado por Euler alrededor de 1750 y probado por Gauss entre 1805 y 1814. Nosotros vamos a probarlo apoyándonos en el siguiente lema:

Lema 2.2.1. *([X], pgs. 77 y 80) Dado un primo entero p se cumple que:*

i) Si $p = 3$ o $p \equiv 2$ mod 3, todo número entero es resto cúbico de p.

ii) Si $p \equiv 1$ mod 3 entonces existe un primo de $\mathbb{Z}[\omega]$ π tal que $p = \pi\bar{\pi}$ y un entero a es resto cúbico de p si y solo si dicho a es resto cúbico de π.

Supongamos entonces que $p = x^2 + 27y^2$. Considerando las posibles congruencias de $x^2 + 27y^2$ módulo 3 en función de x, vemos que ó $p \equiv 1\ mod(3)$ ó $p = 3$. Como $3 \neq x^2+27y^2$ para cualquier $x, y \in \mathbb{Z}$, tenemos la primera parte del resultado. Ahora, tomemos $\pi = x + 3y + 6y\omega \in \mathbb{Z}[\omega]$. π es un primo de Eisenstein ya que $(x+3y+6y\omega)(x+3y+6y\omega^2) = x^2+27y^2 = p$, que es congruente con 1 módulo p. Como además $(x + 3y + 6y\omega)(x + 3y + 6y\omega^2) = \pi\bar{\pi}$, π es justamente el primo de $\mathbb{Z}[\omega]$ que aparece en el lema (2.2.1). En consecuencia, 2 será resto cúbico de p si y solo si 2 es resto cúbico de π. Veamos por tanto que $(\frac{2}{\pi})_3 = 1$.

Como tanto π como 2 son primos de $\mathbb{Z}[\omega]$ congruentes con 2 módulo 3, podemos aplicar la ley de reciprocidad cúbica, que nos dice que

$$(\frac{2}{\pi})_3 = 1 \iff (\frac{\pi}{2})_3 = 1.$$

Dado que $\pi^{(N(2)-1)/3} = \pi = x+3y+6y\omega \equiv x+y\ mod\ 2$, basta ver que x e y tienen paridad contraria para obtener el resultado. Efectivamente, si $x = 2n$ e $y = 2m$ o $x = 2r + 1$ e $y = 2s + 1$, $p = x^2 + 27y^2$ sería múltiplo de dos, lo cual lleva a una contradicción.

Veamos qué pasa con la implicación contraria: si $p \equiv 1 \ mod\ 3$, por el lema (2.2.1) existe un primo $\pi \in \mathbb{Z}[\omega]$ tal que $p = \pi\bar{\pi}$ y por tanto dicho π es congruente con 1 módulo 3. Es decir, $\pi = 3(a + b\omega) + 1 = c + 3b\omega$ para ciertos $a, b, c \in \mathbb{Z}$. En consecuencia tenemos que

$$4p = 4\pi\bar{\pi} = 4(c + 3b\omega)(c + 3b\omega^2) = c^2 + c3b\omega^2 + 3b\omega c + 9b^2\omega^3 =$$
$$c^2 + \frac{-3cb - 3cbi\sqrt{3}}{2} + \frac{-3cb + 3cbi\sqrt{3}}{2} + 9b^2 = 4(c^2 - 3cb + 9b^2) =$$
$$4c^2 - 12cb + 36b^2 = 27b^2 + (9b^2 - 12cb + 4c^2) = 27b^2 + (3b - 2c)^2$$

Es decir, $p = \frac{27b^2}{4} + \frac{(3b-2c)^2}{4}$ y si b es par, *i.e.*, $b = 2d$, entonces

$$p = \frac{27 \cdot 4d}{4} + \frac{4(3d - c)^2}{4} = 27d^2 + (3d - c)^2 = 27y^2 + x^2.$$

Con lo cual, basta comprobar que b es un entero par. Por hipótesis, sabemos que 2 es un resto cúbico de p. Por el lema (2.2.1) 2 es por tanto resto cúbico de π, y por la ley de reciprocidad cúbica, π es a su vez resto cúbico de 2, es decir, $\pi \equiv 1 \ mod\ 2$. Como $\pi = c + 3b\omega$ con $c, b \in \mathbb{Z}$, la única posibilidad de que se cumpla la congruencia es que c sea impar y b par.

En vista de esta y muchas otras aplicaciones que pudieron darse a las leyes de reciprocidad cuadrática, cúbica y bicuadrática, parecía que disponer de leyes de reciprocidad de diferentes órdenes podía dar luz a algunos problemas abiertos de teoría de números. Sin embargo, tener que dar una ley de reciprocidad particular para cada orden resultaba poco práctico, por lo que ya Gauss se preguntó si se podría establecer una ley de reciprocidad de n-ésimo grado, es decir, una ley de reciprocidad general. Con este objetivo en mente, Carl Gustav Jacob Jacobi $(1804 - 1851)$, Ferdinand Gotthold Max Eisenstein $(1823 - 1852)$ y Ernst Eduard Kummer $(1810 - 1893)$ entre otros, trabajaron en una ley de reciprocidad de orden n-ésimo, aunque solo pudieron darla para cuerpos ciclotómicos. La siguiente generación de matemáticos, entre los que cabe destacar a David Hilbert $(1862 - 1943)$, Teiji Takagi $(1875 - 1960)$, Helmut Hasse $(1898 - 1979)$ y Emil Artin $(1898 - 1962)$, recogió el testigo de las leyes de reciprocidad y fueron un paso más allá: dar una ley de reciprocidad de orden n-ésimo definida sobre cualquier extensión de un cuerpo de números dado y de la que las leyes de reciprocidad ya conocidas fuesen casos particulares.

Hoy en día este problema se considera resuelto gracias al conocido como «teorema de Artin». Dicho teorema fue demostrado por Emil Artin en 1927 y de él se desprende una ley de reciprocidad general sobre extensiones abelianas de un cuerpo de números. El objetivo de este trabajo es justamente presentar dicho resultado.

En el Congreso Internacional de Matemáticas de París (1900), David Hilbert (1862 – 1943) empezaba su discurso inaugural con las siguientes palabras:
«¿Quién de nosotros no quisiera levantar el velo tras el cual yace escondido el futuro, y asomarse, aunque fuera por un instante, a los próximos avances de nuestra ciencia y a los secretos de su desarrollo ulterior en los siglos futuros? ¿Cuáles serán las metas particulares que tratarán de alcanzar los líderes del pensamiento matemático de las generaciones futuras? ¿Qué nuevos métodos y nuevos hechos nos depararán los siglos por venir en el ancho y rico campo del pensamiento matemático?
La historia nos enseña la continuidad del desarrollo de la ciencia. Sabemos que cada época tiene sus propios problemas, y dependerá de la próxima generación, ya sea, resolverlos o bien, desecharlos por considerarlos improductivos y remplazarlos por nuevos problemas. Si queremos darnos una idea del desarrollo probable del conocimiento matemático en el futuro inmediato, debemos plantear a nuestras mentes aquellas cuestiones dudosas al observar los problemas que la ciencia de hoy nos propone y cuya solución la esperamos del futuro. El momento presente, marcado por el encuentro de dos siglos, me parece una buena ocasión para presentar una revisión de estos problemas. Porque el cierre de una gran época no solo nos invita a mirar al pasado, sino que también dirige nuestros pensamientos hacia el futuro.»[O]

Figura 2.2: David Hilbert en 1900.

Tras estas palabras hace un breve recorrido por los grandes problemas matemáticos de todos los tiempos y expone lo que, a su parecer, debería ser un problema matemático y cuándo la comunidad matemática se debería dar por satisfecha. También analiza dónde y cuándo surgen estos grandes problemas y finalmente propone 23 problemas que marcarían la investigación matemática del siglo XX. Aquí vamos a hacer hincapié en el noveno:
«Para cualquier cuerpo de números debe probarse una ley de reciprocidad que funcione tanto para restos cuadráticos como para restos de orden primo impar o restos de orden potencia de primos.»
Lo que el matemático alemán proponía con este problema no era otra cosa que establecer una ley de reciprocidad general, aplicable a restos de distinto orden y que englobase las leyes anteriores. Veintisiete años más tarde, Emil Artin lo resolvería definitivamente.

2.3. Emil Artin

Antes de introducirnos en la teoría de cuerpos de clases y enunciar el teorema que motiva este trabajo, vamos a dedicar esta sección a conocer a su autor: Emil Artin.

Emil Artin nació un 3 de marzo de 1898 en Viena. Los años de su juventud los pasó en

Europa Central aunque acabó emigrando a los Estados Unidos donde ganó el prestigio, tanto como matemático como profesor, que le acompañaría durante el resto de su vida. Afortunadamente, se conservan testimonios de algunos de sus compañeros y alumnos [B][A] de los que podemos sacar información de primera mano. De estos testimonios se desprende un profundo respeto y afecto, pero no fueron solo las personas de su entorno quienes reconocieron su valía: en 1952 le nombraron miembro de honor de la institución *London Mathematical Society* y recibió el título de doctor honorario de la Universidad de Clermont-Ferrant en 1962. Murió el 20 de diciembre de 1962.

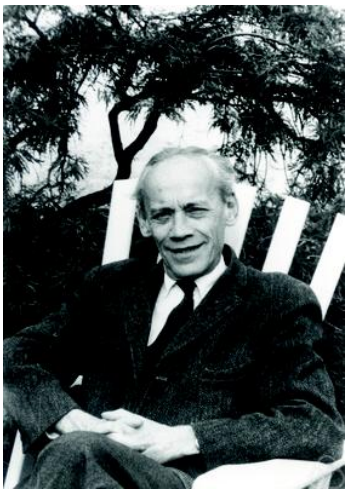


Figura 2.3: Emil Artin. Oberwolfach Photo Collection.

Artin pasó la mayor parte de su infancia y adolescencia en Liberec (Alemania) donde realizó sus estudios obligatorios e hizo el examen de acceso a la universidad. Hasta los 16 años nunca había mostrado interés por las matemáticas y su intención al hacer el examen de acceso era convertirse en estudiante de química. Desgraciadamente, la I Guerra Mundial se interpuso en su camino y hasta el fin de esta no pudo retomar sus estudios. Por aquel entonces ya había despertado en él la curiosidad por las matemáticas y se matriculó de esta disciplina en la Universidad de Leipzig. En 1929 se casó con Natascha Jasng $(1909-2003)$, matemática y fotográfa, con la que tuvo tres hijos: Karin Artin (1933−), Michael Artin (1934−) y Tom Artin (1938−).

En los años treinta Adolf Hitler y el partido Nazi habían adquirido mucho poder en Alemania y Emil Artin tuvo que abandonar su condición de profesor debido a la ascendencia judía de su mujer. La presión política llegó hasta el punto de obligarle a firmar en 1934 un documento oficial en el que corroboraba que Natascha Artin no era de «raza aria». Finalmente, él y su familia emigraron a los Estados Unidos de America en 1937 donde conseguiría el puesto de profesor de una de las universidades más prestigiosas del país. Diecinueve años más tarde volvería de nuevo a Hamburg donde se asentaría el resto de su vida.

En cuanto a sus gustos y personalidad cabe destacar las palabras de Richard Brauer [B]

quien sostiene que «la simbiosis entre el científico y el artista en Artin era única», lo cual explica su gusto por la música, la historia de la música, la bioquímica y la astronomía, materias aparentemente tan dispares. Tanto Brauer como Hans Zassenhaus [A] solo tiene buenas palabras para él: le describen como una excelente persona, empático, divertido, curioso y amante de las conversaciones enriquecedoras.

En su esfera profesional, su alumno Zassenhaus le resenta como «un auténtico científico-filósofo del siglo $XVII$ como Blais Pascal, René Descartes, Newton y Leibniz». Su carrera académica, tal y como hemos mencionado anteriormente, comenzó en la Universidad de Leipzig donde obtuvo el doctorado en 1921. No tardó en medrar dentro de la universidad ya que si en 1923 fue contratado como profesor adjunto en la Universidad de Hamburg, tres años después ya era profesor titular en dicha universidad. Durante los once años siguientes dirigió junto a Erich Hecke $(1887-1947)$ y Wilhelm Blaschke $(1885-1962)$ las actividades del Seminario de Matemáticas de la Universidad de Hamburg. Además, fueron sus años más fructíferos como matemático.

Durante sus años de estudiante aparecieron las publicaciones de Teiji Takagi $(1875-1960)$ que recopilaban todos los avances en la teoría de cuerpos de clases. Esta rama de la teoría algebraica de números cautivó al joven Artin que dedicaría sus primeros años como investigador a seguir los pasos del matemático japonés. En 1923 enunció, sin demostración, la ley de reciprocidad general (posteriormente conocida como el teorema de Artin) la cual era clave en sus trabajos sobre teoría de cuerpos de clases que publicó durante la década de los veinte. Por aquel entonces Helmut Hasse $(1898-1979)$ estaba escribiendo la primera parte de su *Class Field Report*, sin embargo, rehusó incluir los resultados de Artin en la edición de 1925 ya que se apoyaban en una ley que aún no había conseguido probar. Ese mismo año Artin le escribía a Hasse en una carta fechada el 10 de febrero el siguiente párrafo:

«[...] no he podido estudiar en profundidad el artículo de Chebotarëv publicado en el volumen 95 de los *Annalen*, pero si sus conclusiones resultan ser correctas creo que podría probar la ley de reciprocidad general. »

Solo dos años más tarde Hasse recibe una nueva carta fechada el 17 de julio en la que Artin incluye esta información:

«Este semestre he dado un curso de cuerpos de clases y en esta ocasión he podido probar la ley de reciprocidad general tal y como la había enunciado.»

Ese mismo año la demostración fue publicada y Hasse no dudó en reescribir su *Class Field Report* incluyendo los trabajos de Artin. El teorema de Artin pasaría a convertirse en uno de los resultados centrales de la teoría. De hecho, en la revisión del trabajo que contenía la demostración Takagi, calificaba a esta ley como «uno de los resultados más bellos de la teoría algebraica de números actual». Durante estos años Emil Artin también publicó tres artículos $(1929-1931)$ que serían claves para la resolución del décimoséptimo problema

de Hilbert (descomposición de una función definida positiva en sumas de cuadrados de funciones racionales) y otros trabajos sobre números hipercomplejos (1928).

Figura 2.4: Emil Artin (izda.) y Helmut Hasse (dcha.). Oberwolfach Photo Collection.

Tras su traslado a los Estados Unidos, fue profesor en la Universidad de Notre Dame y en la Universidad de Indiana antes de asentarse como profesor en la Universidad de Princeton en 1946. Durante su estancia en Princeton destacaron sus investigaciones sobre grupos finitos simples (1955) y sobre la teoría de grupos de trenzas, que inauguraría él mismo en 1955. En 1956 aceptó la invitación de la Universidad de Göttingen (Alemania) para hacer una estancia anual como *Gauss Pofessor*. Durante este año «sabático» también ejerció en su antigua universidad, la Universidad de Hamburg, y aunque volviese a Princeton al año siguiente ya había decidido volver definitivamente a su país de origen, donde se asentaría en 1958 como profesor de la Universidad de Hamburg.

Si algo destacan las personas que conocieron a Emil Artin en el ámbito académico es su entusiasmo por la enseñanza de matemáticas. Sus alumnos recuerdan que su frase favorita era «*This is enormously simple*» lo cual significaba que había conseguido dividir un proceso extremadamente complejo en una serie de pasos muy sencillos. Todos ellos le describen como un gran comunicador, paciente y claro. Concretamente, Hans Zassenhaus recuerda cómo Artin repetía en todas sus exposiciones «*I want you to see this concept in your mind in full clarity*» y cómo a base de explicar, gesticular, poner ejemplos, especular o invitar a la audiencia a participar acababa lográndolo. Zassenhaus añade una pequeña experiencia personal en la que afirma que el curso de introducción al análisis que recibió de Emil Artin a los 17 años hizo que su carrera para convertirse en físico teórico se desviase hacia las matemáticas.

Figura 2.5: De izquierda a derecha: Hans Petersson, Robert Furch, Emil Artin, Gustav Herglotz, Kurt Reidemeister, Karl Brauner, Wolfgang Haack, Guido Slotnik Hoheisel, Karl Reinhardt, Otto Schreier, Wilhelm Blaschke, Heinrich Behnke, Hendrick Kloosterman y Bartel L. van der Waerden en 1927. Oberwolfach Photo Collection.

Aunque es cierto que Artin creaba sus propios círculos de discusión matemática allá donde iba, fue en Princeton donde su actividad pedagógica fue más productiva. Allí tuvo alumnos de la altura de John Tate (Premio Abel 2010) y Serge Lang (*Leroy P. Steele Prize* de 1999 y *Frank Nelson Cole Prize in Algebra* en 1960), quienes al ser preguntados sobre su director de tesis ambos coincidían en que «Es algo que solo te ocurre una vez en la vida. No todos los matemáticos tienen tanta suerte». Su didáctica de las matemáticas no solo influyó en la generación de matemáticos que pasó por sus clases, muchos libros clásicos en la enseñanza de las matemáticas actuales tienen como referencia los libros y apuntes de este matemático.

Como conclusión, reproducimos las palabras con las que su amigo y compañero Richard Brauer cierra su artículo [B]:

«Para Artin, ser un matemático significaba participar en un esfuerzo colectivo por continuar el trabajo empezado hace miles de años, arrojar luces nuevas a los viejos descubrimientos y abrir nuevos caminos para los descubrimientos del futuro. Sea como sea, no hay duda de que él fue un gran matemático».

Figura 2.6: De izquierda a derecha: Ernst Witt, Paul Bernays, Helene Weyl, Hermann Weyl, Joachim Weyl, Emil Artin, Emmy Noether, Ernst Knauf, Chiungtze Tsen, Erna Bannow y otro en 1933. Oberwolfach Photo Collection.

Capítulo 3

La ley de reciprocidad de Artin

Desde que se enunció la primera ley de reciprocidad hasta que se publicó una ley de reciprocidad general pasaron casi doscientos años. Durante este periodo de tiempo la teoría algebraica de números creció exponencialmente, por lo que no es de extrañar que, aparentemente, dichas leyes solo tengan el nombre en común. Tanto es así, que mientras que la primera se reduce a una fórmula sobre los números enteros, la segunda se desprende de un teorema sobre extensiones abelianas de un cuerpo de números que se enmarca en una teoría conocida como «teoría de cuerpos de clases».

Con este capítulo daremos fin a nuestro recorrido hacia la ley de reciprocidad general. Para ello, nos introduciremos brevemente en la teoría de cuerpos de clases con el objetivo de enunciar y discutir el teorema de Artin. Por último, veremos algunas aplicaciones de este resultado.

3.1. Teoría de cuerpos de clases

La teoría de cuerpos de clases surge a finales del siglo XIX a partir de la teoría de números. Concretamente, a partir de tres líneas de investigación: el estudio de las extensiones de un cuerpo de números en función de su grupo de clases; la búsqueda de teoremas de densidad para ideales primos del anillo de enteros de un cuerpo de números; y la búsqueda de leyes de reciprocidad. El nombre de «cuerpos de clases» hace referencia a extensiones de cuerpos de números L/K que cumplen ciertas propiedades relacionadas con el grupo de clases del cuerpo K.

A grandes rasgos, podemos decir que el objetivo de esta teoría es clasificar las extensiones de Galois de un cuerpo de números a través de los cuerpos de clases. En esta sección veremos cómo surge la teoría y presentaremos tres de sus resultados más relevantes.

3.1.1. Historia

El nacimiento de la teoría se suele fijar en 1853, año en el que Leopold Kronecker (1823 – 1891) anunció un teorema que relacionaba las extensiones finitas abelianas de $\mathbb{Q}$ y los cuerpos ciclotómicos. El teorema en cuestión afirma lo siguiente:

Teorema 3.1.1. ***Kronecker-Weber.*** *Sea $L/\mathbb{Q}$ una extensión abeliana finita. Entonces, existe una raíz de la unidad ζ tal que L es un subcuerpo del cuerpo $\mathbb{Q}(\zeta)$.*

Históricamente, se le atribuye la demostración de este teorema a Heinrich Weber (1842 – 1913). Sin embargo, la prueba que publicó este matemático en 1886 contenía un error, y fue David Hilbert (1862 – 1943) el que finalmente daría una demostración correcta diez años más tarde. Para llevar a cabo dicha demostración, D. Hilbert utilizó los resultados que había obtenido al desarrollar su «teoría de ramificación», teoría que a partir de entonces se convertiría en una herramienta muy presente en el desarrollo de la teoría de cuerpos de clases.

Aparte del teorema que lleva su nombre, L. Kronecker ayudó a sentar las bases de la incipiente teoría gracias a numerosos ejemplos y conjeturas. Por ejemplo, basándose en los trabajos de Niels Henrik Abel (1802 – 1829) sobre las extensiones abelianas de $\mathbb{Q}(i)$, halló la forma de obtener extensiones abelianas de cualquier cuerpo cuadrático imaginario y, de hecho, esperaba demostrar que todas las extensiones abelianas finitas de un cuerpo cuadrático imaginario eran como las que él había definido. Trabajando en esta dirección, probó que cierta extensión L de un cuerpo de números K cualquiera era de Galois y su grupo de Galois era isomorfo al grupo de clases de K. Este ejemplo fue, sin conocimiento del autor, el primer caso particular del teorema de isomorfía que se enunciaría años más tarde y que constituye uno de los pilares de la teoría. También contrastó que estas extensiones de cuerpos L/K cuyo grupo de Galois era isomorfo al grupo de clases del cuerpo K, a las que llamaría «especies de K», también cumplían que eran extensiones no ramificadas y que todo ideal de $\mathcal{O}_K$, el anillo de enteros algebraicos de K, se convertía en ideal principal en $\mathcal{O}_L$, la clausura entera de $\mathcal{O}_K$. Sin saberlo, L. Kronecker había definido a través de estas «especies» el antecedente de los cuerpos de clases tal y como se entienden hoy en día y que veremos más adelante.

Otro tema en el que este matemático hizo interesantes aportaciones fue en el de la densidad de ideales primos. En sus publicaciones de 1880 estableció que, dada una extensión de Galois $L/\mathbb{Q}$, el conjunto de primos que se escinden completamente en L tiene densidad $1/[L:\mathbb{Q}]$. Este resultado era fácilmente extrapolable para cualquier cuerpo de números y, gracias a él, M. Bauer demostró un teorema conjeturado por L. Kronecker en sus publicaciones de 1880 para $K = \mathbb{Q}$.

Teorema 3.1.2. ***M. Bauer.*** *Sean L_1 y L_2 dos extensiones de Galois finitas de un cuerpo de números K. Entonces $L_1 = L_2$ si y solo si el conjunto de ideales primos de $\mathcal{O}_K$ que se escinden completamente en L_1 es el mismo que el conjunto de ideales primos de $\mathcal{O}_K$ que se escinden completamente en L_2.*

Este teorema supone un avance considerable en la teoría ya que afirma que toda extensión de Galois L/K de un cuerpo de números queda determinada por ciertos ideales primos de $\mathcal{O}_K$. No obstante, por aquel entonces no se supo dar una regla que permitiese calcular o caracterizar dichos ideales.

Hubo que esperar a 1908 a que apareciese una definición rigurosa de «cuerpo de clases». Esta definición vendría de la mano de H. Weber, que ya había utilizado este nombre para denotar las especies de Kronecker en un libro de teoría de números en 1891. Sin embargo, estas especies o cuerpos de clases, le parecían casos muy particulares por lo que pensó en ampliar el concepto. Para ello, introdujo algunas definiciones:

Definición 3.1.1. *Llamamos* ***subgrupo de congruencia*** *a un subgrupo H de I_K para el cual existe un módulo $\mathfrak{m}$ de K tal que*

$$\iota(K_{\mathfrak{m},1}) \subseteq H \subseteq I_K^{\mathfrak{m}}$$

En este contexto diremos que H ***está definido módulo*** *$\mathfrak{m}$.*

Entre los subgrupos de congruencia de I_K podemos definir una relación de equivalencia de la siguiente manera:

Dados dos subgrupos de congruencia H_1 y H_2,

$$H_1 \sim H_2 \text{ si y solo si existe un módulo de } K \text{ tal que } H_1 \cap I_K^{\mathfrak{m}} = H_2 \cap I_K^{\mathfrak{m}}.$$

Una clase de equivalencia obtenida a través de esta relación se llama ***grupo de ideales****. Dados un grupo de ideales E y un módulo $\mathfrak{m}$, si hay algún subgrupo de congruencia definido módulo $\mathfrak{m}$ que pertenezca a E es único y diremos que E es un* ***grupo de ideales módulo*** *$\mathfrak{m}$. Al subgrupo de congruencia en cuestión lo denotaremos $H^{\mathfrak{m}}$.*

Además, en este contexto se cumple que existe un único módulo $\mathfrak{f}$ tal que si $H_1^{\mathfrak{f}} \in E$ y $H_2^{\mathfrak{m}} \in E$ entonces $\mathfrak{f} \mid \mathfrak{m}$. Es decir, existe un módulo $\mathfrak{f}$ que es el máximo común divisor de todos los módulos $\mathfrak{m}$ para los cuales E contiene un subgrupo de congruencia módulo $\mathfrak{m}$. A dicho módulo se le denomina ***módulo director de*** *E.*

Considerando estos elementos, H. Weber definió «cuerpo de clases» como una extensión de Galois L/K tal que, dados un módulo de K $\mathfrak{m}$, un subgrupo de congruencia H definido módulo $\mathfrak{m}$ y un ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$ que no divida a $\mathfrak{m}$, dicho ideal primo se escinde completamente en la extensión si y solo si pertenece a H.

Una de las consecuencias de tomar esta definición de cuerpo de clases era que, si existía un cuerpo de clases para un subgrupo de congruencias H, este era único. De esta manera, entró en juego la cuestión de la existencia de los cuerpos de clases. H. Weber pudo probar su existencia para cierto subgrupo de congruencias H y K un cuerpo cuadrático imaginario, sin embargo, la existencia de cuerpos de clases, en el sentido de Weber, para cualquier H y cualquier K era todavía una conjetura.

Hasta ahora hemos visto cómo, poco a poco y con gran influencia de los teoremas de densidad, se fue forjando el concepto de cuerpo de clases y con él el conocimiento sobre las extensiones abelianas de un cuerpo de números. En este punto, cobró importancia la figura de David Hilbert, quien no solo dio un empujón a la clasificación de las extensiones abelianas si no que además lo hizo a raíz de su estudio sobre las leyes de reciprocidad, introduciendo así el tercer ingrediente clave en el desarrollo de la teoría de cuerpos de clases.

D. Hilbert se involucró en el estudio de las extensiones abelianas de cuerpos de números a partir de sus trabajos sobre extensiones cuadráticas y cuerpos ciclotómicos. Uno de sus objetivos en este contexto era dar una ley de reciprocidad que valiese para cualquier cuerpo de números y publicó su propuesta en 1897. Esta ley parecía ir bien encaminada, ya que era equivalente a la ley de reciprocidad cuadrática y además no exigía que los elementos sobre los que se aplicase fuesen exclusivamente primos e impares. Sin embargo, a la hora de demostrarla, se encontró con serios problemas al considerar las extensiones de cuerpos cuadráticos no ramificadas. Entre la prueba del teorema de Kronecker y esto, D. Hilbert empezó a sentir curiosidad por las extensiones abelianas no ramificadas, lo cual le llevó a formular la siguiente conjetura:

Conjetura 3.1.1. *Dado un cuerpo de números K existe una única extensión finita L/K tal que*

1.- *L/K es una extensión de Galois y su grupo de Galois es isomorfo al grupo de clases de K.*

2.- *L/K es una extensión no ramificada y toda extensión abeliana de K con esta propiedad es un subcuerpo de L.*

3.- *El grado relativo de un ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$ es el orden de la clase de $\mathfrak{p}$ en el grupo de clases de K.*

4.- *La extensión en L de todo ideal fraccionario de $\mathcal{O}_K$ es un ideal fraccionario principal de la clausura entera de $\mathcal{O}_K$ en L.*

Esta conjetura se convirtió en teorema de la mano de Philipp Furtwängler $(1869 - 1940)$, quien probó las dos primeras partes en 1907, la tercera en 1911 y la cuarta en 1930.

Como podemos observar, el cuerpo L descrito en ella cumple las propiedades que L. Kronecker había atribuído a sus especies anteriormente. Además, entra dentro de la definición de cuerpo de clases dada por H. Weber para $\mathfrak{m} = (1)$ y H el grupo de ideales fraccionarios principales de $\mathcal{O}_K$. De hecho, a la extensión L/K se la conoce a día de hoy como «el cuerpo de clases de Hilbert».

Otro matemático que ocupó un lugar destacado en la teoría fue Teiji Takagi $(1875 - 1960)$ que, influenciado por los trabajos de D. Hilbert y P. Furtwängler se lanzó a resolver el

problema de la existencia de cuerpos de clases para cualquier cuerpo de números dado. Para ello, lo primero que hizo fue dar una nueva definición de cuerpos de clases.

Definición 3.1.2. ***Takagi.*** *Se llama* ***cuerpo de clase*** *a una extensión de Galois L/K de un cuerpo de números para la cual existe un módulo $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ tal que*

$$[I^{\mathfrak{m}} : \iota(K_{\mathfrak{m},1})N_{L/K}(I_L^{\mathfrak{m}})] = [L : K]$$

donde $N_{L/K}(I_L^{\mathfrak{m}})$ es el conjunto formado por los ideales de $\mathcal{O}_K$ que coinciden con la norma de algún ideal fraccionario de la clausura entera de $\mathcal{O}_K$ en L, que denotaremos por $\mathcal{O}_L$, y que no dividen a $\mathfrak{m}_0$. A cualquier módulo $\mathfrak{m}$ para el cuál se cumpla la condición anterior se le llama ***módulo admisible*** *para L/K y al menor módulo admisible se le llama* ***módulo director*** *de L/K.*

La principal diferencia entre la definición de T. Takagi y H. Weber radica en que la del primero se apoya en la norma de ciertos ideales, mientras que la del segundo depende de los ideales primos que se escinden completamente en la extensión. No obstante, ambas ideas están relacionadas entre sí ya que, dada una extensión de Galois L/K y un ideal primo $\mathfrak{p} \in \mathcal{O}_K$ no ramificado en L, $\mathfrak{p}$ se escinde completamente en L si y solo si $\mathfrak{p}$ es la norma de algún ideal de $\mathcal{O}_L$.

Otra diferencia notable entre ambas definiciones es que, mientras que H. Weber toma un grupo de ideales a partir del cuál construir un cuerpo de clases, lo cual implica tener que probar su existencia; T. Takagi plantea hacer justo lo contrario, tomar una extensión abeliana y comprobar si es un cuerpo de clases o no.

El legado de T. Takagi referente a la teoría de cuerpos de clases queda recogido en el teorema que publicó en 1920, el cual engloba los principales resultados obtenidos hasta ese momento.

Teorema 3.1.3. ***Takagi.*** *Sea K un cuerpo de números.*

1.- *(Existencia) Para todo grupo de ideales E existe un cuerpo de clases sobre K.*

2.- *(Isomorfismo) Si E es un grupo de ideales con módulo $\mathfrak{m}$ y $\mathfrak{m}$ es un módulo admisible para una extensión L/K, entonces $Gal(L/K) \cong I^{\mathfrak{m}}/E$.*

3.- *(Completitud) Cualquier extensión finita y abeliana de K es un cuerpo de clases.*

4.- *(Comparación) Si E_1 y E_2 son dos grupos de ideales con módulo $\mathfrak{m}$ y $\mathfrak{m}$ es un módulo admisible para cierta extensión L_1/K tal que $E_1 \subset L_1$ y cierta extensión L_2/K tal que $E_2 \subset L_2$, entonces $L_1 \subset L_2 \Leftrightarrow E_2 \subset E_1$.*

5.- *(Director) Dada una extensión abeliana y finita L/K, los primos que tienen exponente no nulo en el módulo director de la extensión son todos los primos ramificados de L/K.*

El programa de Langlands

La clasificación de las extensiones abelianas de un cuerpo de números quedó definitivamente resuelta en el siglo XX. El siguiente paso natural era preguntarse qué ocurre con las extensiones de un cuerpo de números que son de Galois pero no abelianas .
Dar respuesta a esta pregunta es uno de los objetivos del programa de Langlands, unas recopilación de conjeturas que relacionan áreas de las matemáticas aparentemente independientes. La versión más clásica del programa es la que envió Robert Phelan Langlands (1936−) en una carta al matemático André Weil (1906 − 1998) en 1967 y partía justamente del teorema de Artin para extensiones abelianas.
Actualmente, el problema de resolver las conjeturas del programa de Langlands se encuentra en la primera línea de investigación en matemáticas y ha llevado a personajes como Laurent Lafforgue y Ngô Bào Châu a ganar la medalla Fields en 2002 y en 2010 respectivamente. En los último años cabe destacar el trabajo de Peter Scholzen sobre algunas de estas conjeturas, gracias al cual ha sido merecedor del premio SASTRA Ramanujan en 2013, el premio Ostrowski en 2015 y el premio Leibniz en 2016 entre otros.

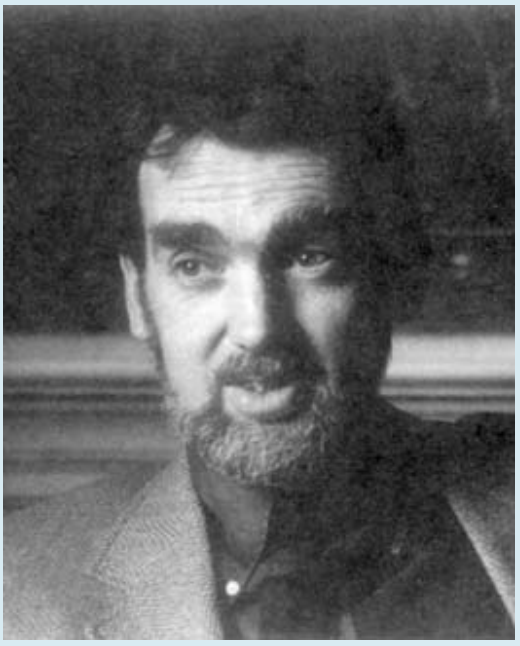


Figura 3.1: Robert Phelan Langlands.

6.- *(Descomposición) Si E es un grupo de ideales con módulo $\mathfrak{m}$ y $\mathfrak{m}$ es un módulo admisible para una extensión L/K, entonces todo primo $\mathfrak{p}$ que tenga exponente nulo en el módulo $\mathfrak{m}$ es no ramificado en L/K y el grado relativo de dicho primo coincide con el orden de la clase de $I^{\mathfrak{m}}/E$ a la que pertenece.*

De los puntos de *isomorfismo* y *completitud* del teorema de T. Takagi se desprende que los cuerpos de clases de un cuerpo de números dados son justamente sus extensiones abelianas finitas, quedando resuelto el problema de clasificar las extensiones de Galois de un cuerpo de números en el caso abeliano. El propio Takagi dudaba de esta afirmación, dado que él solo había podido demostrar la existencia del isomorfismo que presenta el teorema de forma indirecta. Fue Emil Artin el que puso el broche de oro a esta parte de la teoría en 1927 dando un isomorfismo explícito entre estos dos grupos. Dicho isomorfismo se recoge en el «teorema de Artin» el cual, además de ser una piedra angular en la clasificación de las extensiones abelianas de un cuerpo de números, justifica la existencia de una reciprocidad entre primos

de cualquier cuerpo de números, poniendo punto y final al problema de generalizar las leyes de reciprocidad.

3.1.2. Teoremas principales

Dentro de la teoría de cuerpos de clases global hay tres resultados especialmente destacados: el teorema de Artin, el teorema de existencia y el teorema del módulo director. En esencia, lo que aseguran estos teoremas es que a partir de un cuerpo de números dado, existe un módulo respecto al cual podemos construir un cuerpo de clases único y cuyo grupo de clases es isomorfo al grupo de Galois de la extensión, lo cual establece una correspondencia biyectiva entre las extensiones abelianas y los cuerpos de clases de un cuerpo de números. En realidad, esto ya quedaba recogido en el teorema (3.1.3) de T. Takagi; sin embargo, el isomorfismo definido en el teorema de Artin permite enunciar los otros dos teoremas de forma que, no solo anuncien la existencia de cierta estructura, sino que determinen cuál es.

Para dar estos enunciados necesitamos definir el símbolo de Artin, para lo cual partiremos del símbolo o automorfismo de Frobenius.

Definición 3.1.3. *Sean K un cuerpo de números, L/K una extensión de Galois, $\mathfrak{p}$ un primo del cuerpo K y $\mathfrak{P}$ un primo de L tal que $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$ no sea ramificado en L. Entonces, definimos el* ***automorfismo de Frobenius de*** *$\mathfrak{P}$ como el único elemento σ del grupo de descomposición de $\mathfrak{P}$ tal que*

$$\sigma(x) \equiv x^q \ mod\ \mathfrak{P},\ x \in \mathcal{O}_L$$

donde $\mathcal{O}_L$ denota la clausura entera de $\mathcal{O}_K$ en L y q es el número de elementos del cuerpo finito $\mathcal{O}_K/\mathfrak{p}$. Lo denotaremos por

$$\sigma = \left[\frac{L/K}{\mathfrak{P}}\right].$$

Este automorfismo cumple una serie de propiedades de las que caben destacar las siguientes ([J], pgs. $126 - 128$):

1.- **Primos conjugados:** Dado $\tau \in Gal(L/K)$,

$$\left[\frac{L/K}{\tau(\mathfrak{P})}\right] = \tau\left[\frac{L/K}{\mathfrak{P}}\right]\tau^{-1}.$$

2.- **Cambio de extensión:** Dado un que cuerpo E tal que $K \subseteq E \subseteq L$ y $\mathfrak{p}_0 = \mathfrak{P} \cap E$ se cumple que

$$\left[\frac{L/K}{\mathfrak{P}}\right]^{f(\mathfrak{p}_o/\mathfrak{p})} = \left[\frac{L/E}{\mathfrak{P}}\right]$$

y que

$$\left[\frac{E/K}{\mathfrak{p}_0}\right] = \left[\frac{L/K}{\mathfrak{P}}\right]_{|_E}. \tag{3.1}$$

3.- **Composición:** Dados E y F cuerpos tales que $K \subseteq E$, $F \subset L$, E y F extensiones de Galois sobre K y $L = EF$ entonces

$$\left[\frac{EF}{\mathfrak{P}}\right]_{|_E} = \left[\frac{E/K}{\mathfrak{p}_E}\right]$$

y

$$\left[\frac{EF/K}{\mathfrak{P}}\right]_{|_F} = \left[\frac{F/K}{\mathfrak{p}_F}\right]$$

donde $\mathfrak{p}_E = \mathfrak{P} \cap E$ y $\mathfrak{p}_F = \mathfrak{P} \cap F$.

Además, a partir de este símbolo de Frobenius, se puede caracterizar fácilmente la condición en la que se basaba H. Weber para definir los cuerpos de clases:

Proposición 3.1.1. *([J], pg. 128) En las condiciones anteriores, $\mathfrak{p}$ se escinde completamente en L si y solo si*

$$\left[\frac{L/K}{\mathfrak{P}}\right] = 1.$$

Es decir, que un primo del cuerpo K se escinda completamente en L es equivalente a que el automorfismo de Frobenius de la extensión de dicho primo en L sea la identidad.

Hasta ahora hemos trabajado con una extensión de un cuerpo de números de Galois, sin importar que fuese abeliana o no. Añadiendo esta condición, es decir, considerando L/K una extensión abeliana, resulta que el automorfismo de Frobenius se puede definir para $\mathfrak{p}$ un primo de K no ramificado ya que por la propiedad *primos conjugados* vista anteriormente, los automorfismos de Frobenius de cualquiera de los primos de L que aparecen en la factorización de $\mathfrak{p}\mathcal{O}_L$ son iguales. En este contexto, hablaremos por tanto del **automorfismo de Frobenius de $\mathfrak{p}$** que denotaremos por $[L/K, \mathfrak{p}]$ y que establece una correspondencia entre los ideales primos de $\mathcal{O}_K$ y los elementos del grupo $Gal(L/K)$. Teniendo esto en cuenta, definimos el símbolo de Artin como sigue:

Definición 3.1.4. *Sea L/K una extensión de un cuerpo de números abeliana y S un conjunto finito de ideales primos de $\mathcal{O}_K$ que contenga todos los que sean primos ramificados en L. Llamamos **símbolo u homomorfismo de Artin** a la aplicación*

$$\varphi_{L/K} : I_K^S \longrightarrow Gal(L/K)$$

dada por

$$\varphi_{L/K}\Big(\prod_{\substack{\mathfrak{p}\ primo \\ \mathfrak{p}\notin S}} \mathfrak{p}^{a(\mathfrak{p})}\Big) = \prod_{\substack{\mathfrak{p}\ primo, \\ \mathfrak{p}\notin S}} [L/K, \mathfrak{p}]^{a(\mathfrak{p})}$$

donde I_K^S es el subgrupo del grupo de ideales de $\mathcal{O}_K$ generado por los ideales primos no nulos de $\mathcal{O}_K$ que no se encuentran en S.

Nótese que $\varphi_{L/K}(\mathfrak{p})$ con $\mathfrak{p}$ primo no ramificado de K es justamente el automorfismo de Frobenius de $\mathfrak{p}$ y que el símbolo de Artin solo está definido para ideales cuya factorización involucre primos no ramificados.

Entre todas las propiedades que verifica el homomorfismo de Artin, a nosotros nos va a interesar especialmente una que nos ofrece información sobre el núcleo de esta aplicación.

Proposición 3.1.2. *Sean E/K una extensión finita de un cuerpo de números dado, L/K una extensión abeliana con L el cuerpo de escisión de cierto polinomio $p \in K[X]$ y S un conjunto finito de primos de K que contenga a todos los primos de K ramificados en L. El cuerpo de escisión del polinomio p sobre E es EL/E y el grupo de Galois de dicha extensión, si lo restringimos a L, es un subgrupo de $Gal(L/K)$. Entonces, considerando la restricción de $Gal(EL/E)$ en L se cumple que*

$$\varphi_{EL/E_{|_L}} = \varphi_{L/K} N_{E/K} \text{ sobre } I_E^{S(E)}$$

donde $S(E)$ es un conjunto finito formado por los primos de E que dividen a alguno de los primos contenidos en S, en el cual se encuentran en particular todos los primos de E ramificados en EL.

Demostración:

Sea $\mathfrak{P}_E$ un primo de E tal que $\mathfrak{P}_E \notin S(E)$, y veamos que

$$\varphi_{EL/E_{|_L}}(\mathfrak{P}_E) = \varphi_{L/K} N_{E/K}(\mathfrak{P}_E).$$

Sea $\mathfrak{P}_{EL}$ un primo de EL tal que $\mathfrak{P}_{EL} \cap E = \mathfrak{P}_E$ y tomemos $\mathfrak{P}_L = L \cap \mathfrak{P}_{EL}$ y $\mathfrak{p}_K = K \cap \mathfrak{P}_{EL}$. Como $\mathfrak{P}_E$ no pertenece a $S(E)$ se trata de un primo de E no ramificado en EL y por lo tanto $\varphi_{EL/E}(\mathfrak{P}_E)$ coincide con el automorfismo de Frobenius $[EL/E, \mathfrak{P}_E]$. Dicho automorfismo es un elemento de $Gal(EL/E)$ σ tal que $\sigma(x) \equiv x^m \ mod\ \mathfrak{P}_{EL}$ para todo x perteneciente a la clausura entera de $\mathcal{O}_E$ sobre EL, que denotaremos $\mathcal{O}_{EL}$. El exponente m es el número de elementos del cuerpo $\mathcal{O}_E/\mathfrak{P}_E$, que por las propiedades de la norma de una extensión y la norma de ideales sabemos que es

$$\mathcal{N}(\mathfrak{P}_E) = N_{E/\mathbb{Q}}(\mathfrak{P}_E) = N_{K/\mathbb{Q}}\big(N_{E/K}(\mathfrak{P}_E)\big) = N_{K/\mathbb{Q}}(\mathfrak{p}_K^f) = \mathcal{N}(\mathfrak{p})^f = q^f$$

para cierto q y $f = f(\mathfrak{P}_E/\mathfrak{p}_K)$. Es decir, $\varphi_{EL/E}(\mathfrak{P}_E) = \sigma \in Gal(EL/L)$ tal que

$$\sigma(x) \equiv x^{q^f} \ mod\ \mathfrak{P}_{EL},\ x \in \mathcal{O}_{EL}.$$

En particular, para un elemento x de la clausura entera de EL sobre E tal que $x \in L$, se cumple que

$$\sigma(x) \equiv x^{q^f} \ mod\ \mathfrak{P}_L.$$

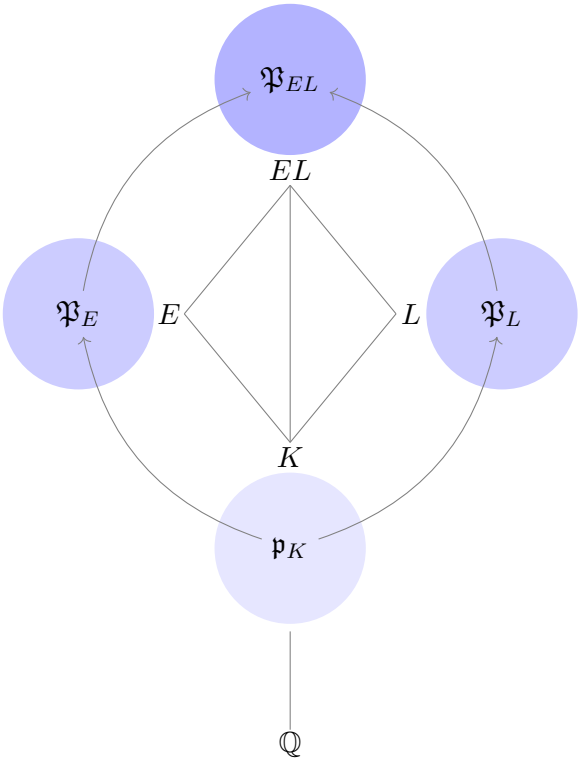
Consideremos ahora $\tau = \varphi_{L/K}(\mathfrak{p}_K)$. El primo $\mathfrak{p}_K$ es no ramificado sobre L ya que si lo fuese, pertenecería a S y como $\mathfrak{P}_E$ lo divide, $\mathfrak{P}_E$ pertenecería a $S(E)$. Por ser $\mathfrak{p}_K$ no ramificado, τ es el automorfismo de Frobenius $[L/K, \mathfrak{p}_K]$, y por tanto $\tau(x) \equiv x^q \ mod \ \mathfrak{P}_L$ para x perteneciente a la clausura entera de $\mathcal{O}_K$ en L. En consecuencia,

$$\tau^f(x) \equiv x^{q^f} \ mod \, \mathfrak{P}_L, \ x \in \mathcal{O}_L.$$

Por la unicidad en el grupo de Galois, tenemos que $\tau^f = \sigma_{|_L}$, es decir,

$$\varphi_{EL/E}(\mathfrak{P}_E)_{|_L} = \varphi_{L/K}(\mathfrak{p}_K)^f = \varphi_{L/K}(N_{E/K}(\mathfrak{P}_E)).$$

Q.E.D.



Un corolario inmediato de este resultado es que

$$N_{L/K}\big(I_L^{S(L)}\big) \subseteq ker \ \varphi_{L/K}$$

ya que para $E = L$, $\varphi_{L/K} N_{L/K} = \varphi_{L/L} = 1$. Esta información es muy relevante, ya que conocer la imagen y el núcleo de $\varphi_{L/K}$ va a ser clave para probar el teorema de Artin, el cual dice así:

Teorema 3.1.4. ***Teorema de Artin.*** *Sea L una extensión abeliana de un cuerpo de números K y sea $\mathfrak{m}$ un módulo de K tal que*

- *sea divisible por todos los primos de K ramificados en L,*

- *y cuyos primos finitos tengan un exponente suficientemente grande*[1].

Entonces, el homomorfismo de Artin $\varphi_{L/K} : I_K^{\mathfrak{m}} \longrightarrow Gal(L/K)$ *es suprayectivo y su núcleo es* $\iota(K_{\mathfrak{m},1})N_{L/K}(I_L^{\mathfrak{m}})$.

Hemos repetido varias veces a lo largo de la exposición que las extensiones abelianas de un cuerpo de números son justamente sus cuerpos de clases. Con este teorema podemos entender mejor dicha afirmación ya que, para cualquier extensión abeliana L sobre K, por el primer teorema de isomorfía y el teorema de Artin tenemos que

$$\frac{I_K^{\mathfrak{m}}}{\iota(K_{\mathfrak{m},1})N_{L/K}(I_L^{\mathfrak{m}})} \cong Gal(L/K)$$

para cierto $\mathfrak{m}$ y por tanto el cuerpo L es un cuerpo de clases en el sentido de Takagi ya que

$$[I_K^{\mathfrak{m}} : \iota(K_{\mathfrak{m},1})N_{L/K}(I_L^{\mathfrak{m}})] = \mid Gal(L/K) \mid = [L : K].$$

Ahora bien, dada una extensión abeliana ¿existe siempre un módulo de K que cumpla las condiciones del teorema? La respuesta a esta pregunta es afirmativa y, de hecho, si existe un módulo que las cumpla, todos los módulos divisibles por él también lo hacen. En vista de esto, sería interesante poder hablar del *mínimo* módulo que se ajusta al enunciado de Artin. La segunda condición no va a suponer ningún problema ya que si tenemos un módulo que verifica solo la primera, siempre podremos tomar otro con exponentes más altos al que divida. La primera condición en cambio no es tan inmediata dado que para hablar del máximo común divisor de un conjunto de módulos lo que tenemos que hacer es considerar un grupo de ideales que contenga subgrupos de congruencias para estos módulos y tomar el módulo director de dicho grupo de ideales; pero ¿podemos asegurar que ese módulo director va a ser a su vez divisible por todos los primos ramificados de la extensión? El siguiente teorema de la sección resuelve justamente esta cuestión:

Teorema 3.1.5. ***Teorema del módulo director.*** *Sea* L/K *una extensión abeliana. Entonces, existe un módulo* $\mathfrak{f}$ *de* K *tal que*

- *Un primo de* K *es ramificado en* L *si y solo si divide a* $\mathfrak{f}$.
- *Dado un módulo* $\mathfrak{m}$ *de* K *divisible por todos los primos ramificados en* L*, el núcleo del homomorfismo de Artin es un subgrupo de congruencia módulo* $\mathfrak{m}$ *si y solo si* $\mathfrak{f} \mid \mathfrak{m}$.

Con el problema del módulo resuelto, podemos dar una definición de «cuerpo de clases de K» basada en el símbolo de Artin:

Definición 3.1.5. *Sea* L *una extensión finita y abeliana de un cuerpo de números* K*. Al grupo de ideales* E *que contiene todos los subgrupos de congruencia* $H := ker\varphi_{L/K}$*,*

[1] En esta condición «suficientemente grande» se refiere a que los exponentes de los primos finitos que aparecen en $\mathfrak{m}$ sean mayores que $v_{\mathfrak{p}}(d) + v_{\mathfrak{p}}(p)/(p-1)$ donde $v_{\mathfrak{p}}$ es la valoración $\mathfrak{p}$-ádica de K, $d = [L_{\mathfrak{P}} : K_{\mathfrak{p}}]$ y p es el primo entero perteneciente a $\mathfrak{p}$.

con $\varphi_{L/K}$ definido sobre $I_K^{\mathfrak{m}}$ para los distintos módulos $\mathfrak{m}$ que cumplen las condiciones del teorema de Artin, le llamaremos ***grupo de clases de la extensión*** *L/K y L será el* ***cuerpo de clases del grupo de ideales*** *E. Además, al módulo director de E se le llamará* ***módulo director de la extensión*** *y se le denotará por $\mathfrak{f}(L/K)$.*

Bajo esta definición de cuerpo de clases, lo que se desprende del teorema de Artin es que toda extensión abeliana de un cuerpo de números K es un cuerpo de clases cuyo grupo de clases es cierto grupo de ideales de K. Cabe preguntarse si ocurre lo mismo al revés, si dado un grupo de ideales de K existe una extensión abeliana cuyo grupo de clases sea justamente dicho grupo de ideales. De nuevo, podemos responder afirmativamente a nuestra pregunta:

Teorema 3.1.6. ***Teorema de existencia K.*** *Sean K un cuerpo de números, $\mathfrak{m}$ un módulo de K y H un subgrupo de congruencia módulo $\mathfrak{m}$. Entonces, existe una única extensión abeliana L/K para la cual*

$$ker\varphi_{L/K} = H$$

con $\varphi_{L/K}$ definido sobre $I_K^{\mathfrak{m}}$.

A raíz de estos tres teoremas, se puede establecer una correspondencia unívoca salvo isomorfismo entre los grupos de ideales de un cuerpo de números K y las extensiones finitas abelianas de dicho cuerpo, es decir, se puede dar una clasificación de todas las extensiones finitas abelianas de K a partir de objetos intrínsecos a K.

3.2. Teorema de Artin

A lo largo de este trabajo hemos visto cómo las llamadas «leyes de reciprocidad» han sido de gran utilidad en el desarrollo de la teoría algebraica de números, hasta el punto de convertirse ellas mismas en relevantes objetos de estudio. Desde el siglo $XVIII$ se han propuesto leyes de reciprocidad de diferente orden y sobre diferentes cuerpos, pero la ley de reciprocidad por antonomasia es la que se desprende del teorema de Artin ya que establece una reciprocidad entre los primos de cualquier extensión abeliana de un cuerpo de números respecto a su condición como resto n-ésimo, es decir, establece una ley de reciprocidad general.

Este teorema fue aplaudido en su entorno no solo por resolver el noveno problema de Hilbert sino por las consecuencias que tendría en la teoría de cuerpos de clases. Sin embargo, dicho teorema fue durante varios años una conjetura debido a la dificultad de su demostración, la cual fue publicada finalmente en 1927. En esta sección presentaremos los puntos clave de dicha demostración y discutiremos la relación entre el teorema y las leyes de reciprocidad.

Durante el resto de la sección asumiremos que K es un cuerpo de números; L/K una extensión finita y abeliana; I_K el grupo de ideales de $\mathcal{O}_K$; $\mathfrak{m}$ un módulo de K en las condiciones del teorema de Artin; $I_K^{\mathfrak{m}}$ el subgrupo de I_K generado por los ideales primos de $\mathcal{O}_K$ que no dividen a $\mathfrak{m}$; $\iota(K_{\mathfrak{m},1})$ el grupo formado por los ideales fraccionarios principales

generados por los elementos de $K_{\mathfrak{m},1} = \{\frac{a}{b} : (a),(b) \nmid \mathfrak{m} \ y \ \frac{a}{b} \equiv^* 1 \ mod \ \mathfrak{m}\}$; y $\varphi_{L/K}$ el símbolo de Artin definido sobre $I_K^{\mathfrak{m}}$. Conviene recordar también que $N_{L/K}(I_L^{\mathfrak{m}})$ es el conjunto formado por la norma de los $\mathcal{O}_L$-ideales fraccionarios pertenecientes al grupo generado por los primos $\mathfrak{P} \in L$ tales que $\mathfrak{P} \cap K \in I_K^{\mathfrak{m}}$, donde $\mathcal{O}_L$ denota la clausura entera de $\mathcal{O}_K$ en L. Por último, recordemos que un elemento de $I_K^{\mathfrak{m}}$ es de la forma

$$\mathfrak{a} = \prod_{\substack{\mathfrak{p} \ primo \\ \mathfrak{p} \nmid \mathfrak{m}}} \mathfrak{p}^{a(\mathfrak{p})}$$

y que en este contexto nos referiremos al símbolo de Artin como un homomorfismo de grupos definido de $I_K^{\mathfrak{m}}$ en $Gal(L/K)$ tal que

$$\varphi_{L/K}(\mathfrak{a}) = \prod_{\substack{\mathfrak{p} \ primo, \\ \mathfrak{p} \nmid \mathfrak{m}}} [L/K, \mathfrak{p}]^{a(\mathfrak{p})}$$

con $[L/K, \mathfrak{p}]$ el automorfismo de Frobenius de $\mathfrak{p}$.

Teniendo en cuenta esta notación, el teorema de Artin se limita a afirmar que la aplicación $\varphi_{L/K}$ es suprayectiva y que su núcleo es el grupo de ideales fraccionarios $\iota(K_{\mathfrak{m},1})N_{L/K}(I_L^{\mathfrak{m}})$. La estrategia de Artin para probarlo constaba de dos partes:

1. En primer lugar, había que ver que efectivamente $ker(\varphi_{L/K}) = \iota(K_{\mathfrak{m},1})N_{L/K}(I_L^{\mathfrak{m}})$, lo cual suponía a su vez dos pasos:

   1.1. Ver que se verifica la llamada «primera desigualdad fundamental»:

   $$[I_K^{\mathfrak{m}} : \iota(K_{\mathfrak{m},1})N_{L/K}(I_L^{\mathfrak{m}})] \ \leq \ [L : K],$$

   1.2. y ver que $\iota(K_{\mathfrak{m},1})N_{L/K}(I_L^{\mathfrak{m}}) \subseteq \ ker(\varphi_{L/K})$.

2. A continuación, había que comprobar que la imagen de $\varphi_{L/K}$ era todo $Gal(L/K)$.

En [J] podemos encontrar una demostración completamente detallada del teorema; aquí, en cambio, nos limitaremos a dar un esquema de la misma dado que gran parte de los resultados en los que apoya se escapan del alcance de este trabajo.

Demostrar la primera desigualdad fundamental, es decir, que

$$[I_K^{\mathfrak{m}} : \iota(K_{\mathfrak{m},1})N_{L/K}(I_L^{\mathfrak{m}})] \leq [L : K],$$

fue la parte que le dio más problemas a Emil Artin. Después de trabajar varios años sobre este punto consiguió demostrarla, pero no con métodos y herramientas de la teoría algebraica de números, sino desde la teoría analítica de números. La idea, *grosso modo*, consistía en estudiar la distribución de los ideales primos en la extensión L/K.

Figura 3.2: Helmut Hasse.

La teoría de cuerpos de clases tal y como la estamos presentando en este trabajo se corresponde en realidad con la teoría de cuerpos de clases *global*. Históricamente hablando, esta es la primera teoría que se formuló, y a partir de ella se desarrolló una teoría de cuerpos de clases equivalente para cuerpo locales.
Sin embargo, algunos matemáticos como Helmut Hasse (1898−1979) veían varias pegas en este desarrollo de la teoría. Por un lado, consideraban más natural el paso de una teoría local a una teoría global que al contrario. Por otro, el hecho de que un resultado puramente algebraico, como era el teorema de Artin, tuviera que apoyarse en el análisis matemático para ser demostrado les provocaba cierto recelo.
Estos fueron los principales motivos por los que se siguió trabajando en la teoría a pesar de haber obtenido ya una clasificación de las extensiones abelianas de un cuerpo de números. Los resultados no se hicieron de rogar ya que en 1936 Claude Chevalley (1909 − 1984) introdujo el término *idèle* que permitía reescribir la teoría y suplir ambos inconvenientes. En la actualidad la teoría de cuerpos de clases se suele abordar desde el punto de vista defendido por H. Hasse y C. Chevalley. En este trabajo, por el contrario, hemos optado por mantener el punto de vista clásico ya que, además de ser notablemente más accesible, muestra cómo se pueden llegar a complementar el álgebra y el análisis.

Definición 3.2.1. *Sea S un conjunto de ideales primos de $\mathcal{O}_K$ y s una variable compleja. Si existe un número real δ tal que*

$$lim_{s\to 1} - \delta log(s-1) - \sum_{\mathfrak{p}\in S} \frac{1}{\mathcal{N}(\mathfrak{p})^s} \text{ es finito}$$

decimos que S tiene ***densidad de Dirichlet*** *δ y lo denotamos por $\delta(S) = \delta$.*

Considerando esta definición y aplicando el teorema de densidad de Frobenius es fácil probar la primera desigualdad.

Teorema 3.2.1. ***Teorema de densidad de Frobenius.*** *([J], pgs. 162 − 164) Sea $\sigma \in Gal(L/K)$ un elemento de orden n y sea S el conjunto de primos de K que son divisibles*

por un primo de L cuyo automorfismo de Frobenius pertenezca al conjunto D formado por los elementos de G que son el conjugado de algún σ^m con m primo respecto a n. Entonces S tiene densidad de Dirichlet $\delta(S) = t/ \mid Gal(L/K) \mid$ donde t es el número de elementos de D.

Teorema 3.2.2. *([J], pg. 161) Sea $\mathfrak{m}$ un módulo de K y H un subgrupo de congruencia módulo $\mathfrak{m}$. Entonces, dado S un conjunto de ideales primos contenido en H, se cumple que*

$$\delta(S) \leq \frac{1}{[I_K^{\mathfrak{m}} : H]}$$

.

Teorema 3.2.3. ***Primera desigualdad fundamental.*** *Dado $\mathfrak{m}$ un módulo de K se cumple que*

$$[I_K^{\mathfrak{m}} : \iota(K_{\mathfrak{m},1})N_{L/K}(I_L^{\mathfrak{m}})] \leq [L : K] \tag{3.2}$$

Aplicando el teorema (3.2.1) al conjunto $\iota(K_{\mathfrak{m},1})N_{L/K}(I_L^{\mathfrak{m}})$ se tiene que su densidad de Dirichlet es justamente $1/[L : K]$, así que por el teorema (3.2.2) se cumple que

$$\frac{1}{[L : K]} \leq \frac{1}{[I_K^{\mathfrak{m}} : \iota(K_{\mathfrak{m},1})N_{L/K}(I_L^{\mathfrak{m}})]}$$

y despejando, tenemos el resultado.

Sin embargo, si queremos obtener la desigualdad contraria tendremos que ser menos exigentes y considerar L/K una extensión cíclica, es decir, una extensión de Galois cuyo grupo de Galois es cíclico.

Resulta, que

$$[I_K^{\mathfrak{m}} : \iota(K_{\mathfrak{m},1})N_{L/K}(I_L^{\mathfrak{m}})] = a(\mathfrak{m})n(\mathfrak{m})q(H)$$

donde $a(\mathfrak{m})$ y $n(\mathfrak{m})$ son el orden ciertos grupos cociente dependientes de $\mathfrak{m}$; H es el conjunto de los elementos α de L^* tales que $\iota(\alpha)$ es divisible únicamente por primos que aparezcan en $\mathfrak{m}$; y $q(H)$ el conocido como «cociente de Herbrand» de H que, a grandes rasgos, podemos considerar como el cociente de los órdenes de los grupos de cohomología de H, cuya definición y propiedades podemos encontrar detalladas en ([J], pgs. $170 - 171$). En nuestro caso, nos basta con saber que $a(\mathfrak{m})$ y $q(H)$ están relacionados con los índices de ramificación y grados relativos de los primos divisores de $\mathfrak{m}$, concretamente

$$a(\mathfrak{m}) = \prod_{\mathfrak{p}|\mathfrak{m}} e_{\mathfrak{p}} f_{\mathfrak{p}}$$

y

$$q(H) = \frac{[L : K]}{\prod_{\mathfrak{p}|\mathfrak{m}} e_{\mathfrak{p}} f_{\mathfrak{p}}}.$$

Es decir,

$$[I_K^{\mathfrak{m}} : \iota(K_{\mathfrak{m},1})N_{L/K}(I_L^{\mathfrak{m}})] = [L : K]n(\mathfrak{m}).$$

Como la desigualdad (3.2) se verifica para cualquier extensión abeliana en particular se cumple para L/K por ser cíclica, con lo cual, tenemos que por un lado $[I_K^{\mathfrak{m}} : \iota(K_{\mathfrak{m},1})N_{L/K}(I_L^{\mathfrak{m}})]$ es igual a un múltiplo de $[L : K]$ y por otro $[I_K^{\mathfrak{m}} : \iota(K_{\mathfrak{m},1})N_{L/K}(I_L^{\mathfrak{m}})] \leq [L : K]$. En consecuencia, tenemos que en extensiones cíclicas se da la igualdad fundamental.

Si seguimos restringiéndonos a extensiones cíclicas, el teorema de Artin es inmediato si nos apoyamos en el siguiente teorema:

Teorema 3.2.4. *([J], pgs. 195 – 197) Dada L/K una extensión cíclica, si se verifica la igualdad $[I_K^{\mathfrak{m}} : \iota(K_{\mathfrak{m},1})N_{L/K}(I_L^{\mathfrak{m}})] = [L : K]$, entonces $ker\varphi_{L/K}$ es un subgrupo de congruencia módulo $\mathfrak{m}$, es decir,*

$$\iota(K_{\mathfrak{m},1}) \subseteq ker\varphi_{L/K} \subseteq I_K^{\mathfrak{m}}.$$

No obstante, nosotros vamos a utilizarlo directamente para extender el resultado a extensiones abelianas en general:

Si consideramos de nuevo que L/K es una extensión finita abeliana, tenemos que el grupo $Gal(L/K)$ es a su vez un grupo abeliano finito, y por el primer teorema de estructura de este tipo de grupos, se puede expresar como un producto finito de grupos cíclicos, es decir,

$$Gal(L/K) = C_1 \times \cdots \times C_s.$$

Además, si definimos H_j como el producto directo de los C_i con $i \neq j$, tenemos que $Gal(L/K) = C_j \times H_j$. Consideremos entonces E_j el cuerpo fijo de H_j. El grupo de Galois de la extensión E_j/K es C_j y por tanto dicha extensión es cíclica. Por el teorema (3.2.4) tenemos que para cierto módulo $\mathfrak{m}_j$ de K se verifica que $\iota(K_{\mathfrak{m}_j,1}) \subseteq ker\varphi_{E_j/K}$ y como todo primo ramificado en E_j es a su vez ramificado en L, si tomamos $\mathfrak{m}_j$ de forma que solo sea divisible por los primos de K ramificados en E_j, se tiene que $\mathfrak{m}_j \mid \mathfrak{m}$. Por la definición de $K_{\mathfrak{m}_j,1}$ se tiene que entonces $\iota(K_{\mathfrak{m},1}) \subseteq ker\varphi_{E_j/K}$ para todo E_j y por lo tanto

$$\iota(K_{\mathfrak{m},1}) \subseteq \bigcap_j ker\varphi_{E_j/K}.$$

Aparte, la ecuación (3.1) nos dice que para cualquier ideal $\mathfrak{a}$ de $I_K^{\mathfrak{m}}$ se cumple que

$$\varphi_{L/K_{|_{E_j}}}(\mathfrak{a}) = \varphi_{E_j/K}(\mathfrak{a}),$$

así que para $\mathfrak{a} \in \iota(K_{\mathfrak{m},1})$,

$$\varphi_{L/K_{|_{E_j}}} = 1, \ \forall E_j$$

por $\iota(K_{\mathfrak{m},1})$ contenido en el núcleo de $\varphi_{E_j/K}$. Pero como $L = E_1 \dots E_s$,

$$\varphi_{L/K} = 1$$

y por tanto $\iota(K_{\mathfrak{m},1})$ está contenido en el núcleo del homomorfismo de Artin.

Para poder continuar el cálculo del núcleo de $\varphi_{L/K}$ hay que resolver el tema de la suprayectividad de $\varphi_{L/K}$. Al igual que ocurría con la primera desigualdad, este resultado se obtiene de forma independiente aplicando el teorema de densidad de Frobenius, como podemos comprobar en ([J], pg. 164); por lo que vamos a asumir que $Im\varphi_{L/K} = Gal(L/K)$.

Para terminar, recordemos que en la proposición (3.1.2) habíamos visto que $N_{L/K}(I_L^{\mathfrak{m}})$ estaba contenida en el núcleo de $\varphi_{L/K}$. Combinando este resultado con el que acabamos de obtener, tenemos que

$$\iota(K_{\mathfrak{m},1})N_{L/K}(I_L^{\mathfrak{m}}) \subseteq ker\varphi_{L/K}.$$

Aplicando el primer teorema de isomorfía, sabemos que el índice $[I_K^{\mathfrak{m}} : ker\varphi_{L/K}]$ es igual al orden del grupo de Galois de L/K, que por ser una extensión de Galois coincide a su vez con el índice de la extensión. Es decir,

$$[I_K^{\mathfrak{m}} : ker\varphi_{L/K}] = [L : K].$$

Pero por la primera desigualdad sabemos que

$$[I_K^{\mathfrak{m}} : \iota(K_{\mathfrak{m},1})N_{L/K}(I_L^{\mathfrak{m}})] \leq [I_K^{\mathfrak{m}} : ker\varphi_{L/K}]$$

con lo cual, ambos subgrupos tienen que ser necesariamente iguales, es decir,

$$ker\varphi_{L/K} = \iota(K_{\mathfrak{m},1})N_{L/K}(I_L^{\mathfrak{m}}).$$

Cabe destacar que la única parte de la demostración que se podría extender para extensiones de cuerpos de números no abelianas es la primera desigualdad fundamental, ya que el resto se apoya directamente en caracterizaciones de las extensiones abelianas.

3.2.1. Una ley de reciprocidad general

Hace doscientos años Carl Fiedrich Gauss se enfrentaba por primera vez a un problema que desafiaría a la comunidad matemática hasta mediados del siglo pasado: generalizar la ley de reciprocidad cuadrática.

A lo largo de este trabajo hemos ido profundizando en dicho problema hasta llegar a uno de los teoremas centrales de la teoría de cuerpos de clases: el teorema de Artin.

Para ver cómo se relaciona este resultado sobre extensiones abelianas de un cuerpo de números con las leyes de reciprocidad, veamos en primer lugar cómo se generaliza el símbolo de Legendre:

Definición 3.2.2. *Dados un cuerpo de números K que contenga una raíz primitiva n-ésima de la unidad, $\mathfrak{p}$ un ideal primo de $\mathcal{O}_K$ y $\alpha \in \mathcal{O}_K$, definimos el* ***símbolo de Legendre*** $\left(\frac{\alpha}{\mathfrak{p}}\right)_n$

como la única raíz n-ésima ζ_n de la unidad que satisface

$$\alpha^{(\mathcal{N}(\mathfrak{p})-1)/n} \equiv \zeta_n \ mod\ \mathfrak{p}.$$

Además, este símbolo se puede generalizar para cualquier ideal $\mathfrak{a}$ de $\mathcal{O}_K$ de la siguiente manera:

$$\left(\frac{\alpha}{\mathfrak{a}}\right)_n = \prod_{i=1}^{r} \left(\frac{\alpha}{\mathfrak{p}_i}\right)_n,$$

donde $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ es la factorización prima del ideal $\mathfrak{a}$.

El siguiente resultado, en ocasiones citado como «ley de reciprocidad de Artin», recoge el nexo entre el símbolo de Artin y el símbolo de Legendre generalizado que buscábamos.

Teorema 3.2.5. ***Teorema débil de reciprocidad.*** *([X], pg. 166) Sean K un cuerpo de números que contenga una raíz primitiva n-ésima de la unidad, sea $L = K(\sqrt[n]{\alpha})$ donde $\alpha \in \mathcal{O}_K \backslash \{0\}$ y μ_n el conjunto de las raíces primitivas n-ésimas de la unidad. Entonces, dado un módulo de K divisible por todos los primos de K ramificados en L y cuyos primos finitos tengan exponente suficientemente grande, el siguiente diagrama es conmutativo:*

$$\begin{array}{ccc} I_K^{\mathfrak{m}} & \xrightarrow{\varphi_{L/K}} & Gal(L/K) \\ & \searrow^{(\alpha/\cdot)_n} & \downarrow i \\ & & \mu_n \end{array}$$

donde la aplicación i es un monomorfismo de grupos que hace $i(\sigma) = \zeta$ con $\zeta \in \mu_n$ tal que $\sigma(\sqrt[n]{\alpha}) = \zeta \sqrt[n]{\alpha}$.

El apelativo de «débil» se debe a que no da una fórmula que permita computar $(\alpha/\mathfrak{a})_n$. No obstante, sigue siendo un resultado extremadamente relevante, ya que permite ver al símbolo de Legendre de orden n como un epimorfismo entre $I_K^{\mathfrak{m}}/ker\varphi_{L/K}$ y un subgrupo de μ_n. En ([X], pgs. $166 - 167$) podemos ver una demostración de la ley de reciprocidad cuadrática a partir del teorema 3.2.5.

La historia de las leyes de reciprocidad termina, finalmente, con la teoría local de cuerpos de clases, en cuyo contexto se puede definir el símbolo de Hilbert a partir del símbolo de Artin y dar una fórmula explícita para calcular

$$\left(\frac{\alpha}{\beta}\right)_n \left(\frac{\beta}{\alpha}\right)_n^{-1}.$$

Dicha fórmula se recoge en el conocido como «teorema fuerte de reciprocidad», que podemos encontrar en ([X], pg. 167).

3.3. Aplicaciones

Hemos dedicado gran parte de este capítulo a comprender el teorema de Artin, por lo que no podíamos terminarlo de otra manera que no fuese exponiendo brevemente las repercusiones que ha tenido.

Desde el punto de vista del presente trabajo, la principal aplicación del teorema de Artin es justamente dar lugar a una ley de reciprocidad general. Ya hemos visto que esto es en sí mismo un logro ya que cerró uno de los problemas de Hilbert; sin embargo, también tiene consecuencias mucho más prácticas dado que, al igual que la ley de reciprocidad cuadrática permitía caracterizar los primos de la forma x^2+y^2 o la ley de reciprocidad cúbica permitía caracterizar los del tipo x^2+27y^2, disponer de una ley de reciprocidad general va a permitir caracterizar los primos

$$p = x^2 + ny^2$$

para cualquier $n \in \mathbb{N}$ dado [X]. En general, con esta ley podemos resolver ciertas ecuaciones diofánticas lo cual es de gran utilidad en criptografía de clave pública. Además, las leyes de reciprocidad también permiten elaborar tests de primalidad.

No obstante, no podemos olvidarnos de que el teorema de Artin es uno de los pilares de la teoría de cuerpos de clases, y en este contexto también tiene importantes aplicaciones. Debemos tener en cuenta que, el gran avance que produjo este teorema no fue tanto el allanar el terreno hacia la clasificación definitiva de las extensiones abelianas de cuerpos de números sino dar un homomorfismo explícito a partir del cual se pudo formular la computación de las mismas. Así, llegamos a la primera consecuencia del teorema de Artin como resultado teórico: proporcionó la forma de crear algoritmos que calculasen el grupo radial, los subgrupos de congruencias o el módulo director de una extensión abeliana sobre un cuerpo de números dada. Esto ha permitido que se elabore *sofware* diseñado para resolver específicamente problemas de álgebra o de teoría de números, como puede ser MAGMA (1993). Este tipo de *sofware* facilita la tarea de evidenciar conjeturas en estas ramas de las matemáticas y permite construir tablas de cuerpos de números.

Por último, no sería descabellado considerar que en cierta medida las aplicaciones que se le dan a día de hoy a la teoría de cuerpos de clases están ligadas al teorema de Artin ya que sin él la teoría no habría avanzado al mismo ritmo. Concretamente, la teoría de cuerpos de clases, en especial si consideramos cuerpos de funciones en lugar de cuerpos de números, se está utilizando en el desarrollo de códigos correctores de errores y en el estudio teórico de los sistemas de comunicación *wireless*.


¿Existe una ley de reciprocidad general?
Sí, se desprende del TEOREMA DE ARTIN
dentro de la TEORÍA DE CUERPOS DE CLASES aplicable a
Desarrollo de sofware algebraico
Elaboración de tablas de cuerpos de números
Códigos correctores de errores
Comunicación *wireless*
Resolución de ecuaciones diofánticas
Primalidad
Criptografía

Conclusiones

La teoría algebraica de números es un campo de estudio especialmente amplio y ramificado dentro de las matemáticas. En este trabajo nos hemos introducido en él con un objetivo concreto en mente: dirimir la posibilidad de generalizar las leyes de reciprocidad.

Como muchos antes que nosotros, hemos podido comprobar que estas leyes enunciadas de forma aislada han facilitado la resolución de ciertos tipos de ecuaciones y de algunos problemas clásicos de la teoría algebraica de números. Por ello, parecía natural suponer que el disponer de una ley de reciprocidad general aumentaría estos beneficios.

En nuestro recorrido hacia dicha generalización hemos seguido dos caminos paralelos. Por un lado, hemos seleccionado los resultados teóricos que nos permitirían acercarnos fácilmente al problema, entre los que cabe destacar el hecho de que el anillo de enteros de un cuerpo de números no es un dominio de factorización única, pero sí un anillo de Dedekind y por tanto, existe una factorización única de sus ideales como producto de ideales primos. Por otro, hemos ido reconstruyendo el contexto del problema, dando pinceladas del momento histórico en el que surge y se desarrolla y las personas que contribuyeron a su resolución. Gracias a ello hemos podido ir más allá del habitual esquema problema-solución y mostrar la evolución de un enunciado clásico a lo largo de los años.

Una de las consecuencias más llamativas que ha generado nuestra discusión ha sido que, a raíz de una fórmula sobre primos enteros, hemos acabado en una parte de la teoría de números que a día de hoy tiene nombre propio: la teoría de cuerpos de clases. La propiedad de que el anillo de enteros de un cuerpo de números sea un anillo de Dedekind ha permitido que se construyesen elementos como los módulos o los primos de un cuerpo, que a su vez darían la terminología necesaria para generar esta nueva teoría. Bajo este marco teórico cada vez más sofisticado, se pudo definir cierto grupo cociente de ideales del cuerpo base de una extensión abeliana que resultaría ser isomorfo al grupo de Galois de la misma.

Esta afirmación constituye la tesis del teorema de Artin del cual se desprende la ley general que se buscaba y que representa el punto de culminación de nuestro trabajo. No obstante, nos hemos detenido en el problema un poco más y hemos expuesto el esqueleto de su demostración más clásica, dada en su día por el propio Emil Artin, ya que, aparte de evidenciar la dificultad de extender el resultado a extensiones de cuerpos de números más generales, aporta un buen ejemplo de cómo ramas *a priori* tan dispares como el análisis y el álgebra finalmente se complementan.

Por último, hemos visto que, tal y como se intuía en un principio, disponer de una ley de reciprocidad general ha dado un impulso no solo a la teoría algebraica de números sino también a la teoría de cuerpos de clases y, de hecho, se espera que aporte una contribución notable a campos como la criptografía y la comunicación sin cable.

Índice alfabético

Anillo, 1
Anillo conmutativo, 1
Anillo de Dedekind, 10
Anillo de enteros, 8
Anillo de fracciones, 4
Anillo de valoración, 21
Anillo de valoración discreta, 11
Anillo Noetheriano, 10
Anillo unitario, 1
Automorfismo de Frobenius, 53, 54

Base, 2

Clausura entera, 7
Completamente ramificado, 17
Cuerpo, 1
Cuerpo de escisión, 3
Cuerpo de fracciones, 1
Cuerpo de números, 7
Cuerpo fijo, 3

Densidad de Dirichlet, 60
Divisor de cero, 1
Dominio de ideales principales, 2
Dominio de integridad, 1

Ecuación diofántica, 32
Elemento algebraico, 3
Elemento trascendente, 3
Entero algebraico, 7
Entero sobre un anillo, 7
Enteros de Eisenstein, 37
Enteros de Gauss, 38
Escinde completamente, 17
Extensión simple, 3
Extensión abeliana, 3
Extensión algebraica, 3
Extensión de Galois, 3
Extensión finita, 3
Extensión normal, 3
Extensión ramificada, 17
Extensión separable, 3

Grado relativo, 15, 16
Grupo de clases, 19, 58
Grupo de descomposición, 26
Grupo de Galois, 2
Grupo de ideales, 19, 49
Grupo de inercia, 27
Grupo de unidades, 2
Grupo radial, 29

Ideal, 2
Ideal entero, 18
Ideal fraccionario, 18
Ideal maximal, 2
Ideal primo, 2
Ideal principal, 2
Índice de ramificación, 15, 16
Íntegramente cerrado, 7

Localización, 6

Módulo, 2
Módulo de un cuerpo, 28
Módulo director, 49, 58
Módulo libre, 2
Módulo unitario, 2

Número de clases, 19
Norma , 8
Norma absoluta, 17

Norma de un ideal, 17

Polinomio mínimo, 3
Primera desigualdad, 61
Primo complejo, 25
Primo de un cuerpo, 22
Primo real, 25

Ramificado, 16

Símbolo de Artin, 54
Sistema generador, 2
Sistema libre, 2
Subconjunto multiplicativo, 4
Subgrupo de congruencia, 49
Sucesión convergente, 22

Valoración $\mathfrak{p}$-ádica, 21
Valoración arquimediana, 20
Valoración exponencial, 21
Valoración no arquimediana, 20
Valoraciones, 20

Bibliografía

[B] Brauer, Richard. Emil Artin. *Bulletin-American Mathematical Society*, 1967, vol. 73, no. 1, 27 – 43.

[C] Conrad, Keith. History of class field theory. *Disponible en* `http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/cfthistory.pdf`, 2001.

[F] Oré, Fabio Abraham Contreras. El último teorema de Fermat-Wiles. *Horizonte de la Ciencia*, 2015, vol. 5, no 9, p. 211 – 218.

[X] Cox, David A. Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication. 1989. ISBN: 0-471-50654-0.

[H] Hilbert, David. Mathematical problems. *Bulletin-American Mathematical Society*, 2000, vol. 37, no 4, p. 407 – 436.

[J] Janusz, Gerald J. Algebraic number fields. Second edition. Graduate Studies in Mathematics, 7. *American Mathematical Society*, *Providence*, RI, 1996. $x + 276$ pp. ISBN: 0-8218-0429-4.

[L] Lemmermeyer, Franz. Reciprocity Laws: From Euler to Eisenstein. Springer Science & Business Media, 2000. ISBN: 3-540-66957-4.

[G] Cardenal, Edwin León. La Gema de la Reina: Una breve revisión histórica de la ley de reciprocidad cuadrática. *Lecturas Matemáticas*, 2009, vol. 30, p. 17 – 27.

[M] Milne, James S. Class field theory. *Disponible en* `http://www.jmilne.org/math/CourseNotes/CFT.pdf`, 1997.

[N] Neukirch, Jürgen. Algebraic number theory. Springer, 1999. ISBN: 3-540-65399-6.

[O] Hilbert, David. Los problemas futuros de la matemática. JR Ortiz, trad, 1994, vol. 9. *Disponible en* `http://casanchi.com/ref/hilbert.pdf`

[R] Roquette, Peter. On the history of Artin's L-functions and conductors. Seven letters from Artin to Hasse in the year 1930. *Mitteilungen der Mathematischen Gesellschaft in Hamburg*, 2000, vol. 19, no 5 – 50, p. 97.

[T] Rufián Lizana, Antonio. Una revolución en teoría de números. Gauss. RBA, 2012. ISBN: 978-84-473-8831-8.

[K] Travesa, Artur. El teorema de Kronecker-Weber. *Disponible en* `https://atlas.mat.ub.edu/personals/travesa/Kr-W.pdf`, *CSIC*, 2008.

[A] Zassenhaus, Hans. Emil Artin, his life and his work. *Notre Dame Journal of formal logic*, 1964, vol. 5, no 1, p. $1 - 9$.