USC UNIVERSIDADE DE SANTIAGO DE COMPOSTELA
FACULTADE DE MATEMÁTICAS

Trabajo Fin de Grado

El teorema de densidad de Chebotarev

Gabriel Fernández Lago

Curso 2024/2025

UNIVERSIDAD DE SANTIAGO DE COMPOSTELA

GRADO DE MATEMÁTICAS

Trabajo Fin de Grado

El teorema de densidad de Chebotarev

Gabriel Fernández Lago

Junio, 2025

UNIVERSIDAD DE SANTIAGO DE COMPOSTELA

Trabajo propuesto

Área de Coñecemento: Álxebra
Título: O teorema de densidade de Chebotarev
Breve descrición do contido
O obxectivo deste TFG é o estudo do teorema de densidade de Chebotarev traballando algunhas das súas aplicacións, especialmente a factorización de polinomios módulo p. Na primeira parte, realizaremos unha primeira aproximación á conexión entre a teoría de Galois e a factorización de polinomios módulo p, traballando a relación con outros resultados como a lei de reciprocidade cuadrática. A continuación, explicaremos o papel que desempeña o teorema de densidade de Chebotarev e discutiremos outras aplicacións.
Recomendacións
Outras observacións

Índice

Resumen

El objetivo de este TFG es el estudio del teorema de densidad de Chebotarev, trabajando algunas de sus aplicaciones, especialmente la factorización de polinomios módulo p. En la primera parte, realizaremos una primera aproximación a la conexión entre la teoría de Galois y la factorización de polinomios módulo p, trabajando la relación con otros resultados como la ley de reciprocidad cuadrática. A continuación, explicaremos el papel que desempeña el teorema de densidad de Chebotarev y discutiremos otras aplicaciones del mismo.

Abstract

The aim of this Bachelor's Thesis is to study Chebotarev's density theorem, exploring some of its applications, especially the factorization of polynomials modulo p. In the first part, we will present an initial approach to the connection between Galois theory and the factorization of polynomials modulo p, examining its relationship with other results such as the law of quadratic reciprocity. We will then explain the role played by Chebotarev's density theorem and discuss further applications.

Introducción

El objetivo de este trabajo es motivar el teorema de densidad de Chebotarev e introducir algunas de las herramientas necesarias para su demostración. A pesar de su enunciado más o menos abstracto, a lo largo de los primeros capítulos vamos a presentar tres problemas matemáticos que se pueden ver como casos particulares del mismo.

(A) Un problema clásico de la teoría de números es determinar qué primos se pueden expresar como suma de dos cuadrados, es decir, cuándo existen enteros x, y de manera que

$$p = x^2 + y^2.$$

La respuesta, que usa la aritmética de los enteros gaussianos, es que es posible si y solamente si $p = 2$ o $p \equiv 1$ (mód 4). Una pregunta análoga es determinar qué primos se pueden expresar como $x^2 + 2y^2$, con $x, y \in \mathbb{Z}$. En este caso, el teorema de Chebotarev afirmará que la *mitad* de los primos se pueden expresar como suma de dos cuadrados (donde el uso del término *mitad* requiere introducir una noción de densidad que presentaremos a lo largo del trabajo). Una cuestión análoga que admite el mismo tratamiento es determinar qué primos se pueden escribir como $p = x^2 + 2y^2$, con $x, y \in \mathbb{Z}$. Aunque no trabajaremos este último problema explícitamente a lo largo del TFG, es una muestra más de cómo el resultado aparece en cuestiones diversas de la teoría de números.

(B) Otro resultado muy conocido es el *teorema de la progresión aritmética de Dirichlet*, que afirma que, si a y b son enteros positivos con $\gcd(a, b) = 1$, entonces existen infinitos números primos de la forma $an + b$, con n un entero positivo. Por ejemplo, existen infinitos números primos de la forma $7n+4$. El teorema de Chebotarev permite deducir este resultado como un corolario suyo, afirmando además que la *densidad* de primos de la forma $an + b$ es $1/\varphi(n)$. Por ejemplo, como $\varphi(7) = 6$, tenemos que $1/6$ de los primos son congruentes con 4 módulo 7.

(C) El tercer resultado que queremos ilustrar en esta introducción tiene que ver con la factorización de polinomios módulo p. Consideremos los polinomios $q_1(X) = X^4 + 4X^2 + 2$ y $q_2(X) = X^4 + X + 1$. En el caso de $q_1(X)$, al factorizar módulo p, si p es suficientemente

grande, nos podemos encontrar con tres situaciones: o es irreducible; o factoriza como producto de dos factores de grado dos; o descompone totalmente en cuatro factores de grado uno. En cambio, la situación para $q_2(X)$ es distinta, ya que también se da el caso en el que factoriza como un factor de grado tres y otro de grado uno o como uno de grado dos y dos de grado uno. Además, la frecuencia de cada tipo de factorización varía en cada una de las situaciones. El teorema de Chebotarev nos dará un resultado preciso sobre los patrones de factorización que pueden aparecer y la densidad de cada uno de ellos.

En cuanto a la estructura de la memoria, primero presentaremos los símbolos de Legendre y la ley de reciprocidad cuadrática, conceptos importantes los cuales aplicaremos para la factorización de polinomios de grado 2 módulo p. También discutiremos la factorización de algunos ejemplos de polinomios de grado 3 e 4 y la relacionaremos con el grupo de Galois de esos polinomios. En ese sentido, hemos realizado diferentes experimentos numéricos con SageMath de cara a ilustrar los patrones de factorización de los polinomios módulo p. Se ha incluido el código que hemos desarrollado como anexo a este trabajo.

A partir de la segunda parte del trabajo adoptamos un enfoque más teórico, introduciendo algunos conceptos importantes para la demostración del teorema de Chebotarev. Esto incluye, en particular, los índices de ramificación, el grado de inercia o el elemento de Frobenius, además de algunos resultados útiles sobre ellos, en torno a los cuales pivota el capítulo 2.

A continuación, y como paso previo a la presentación del teorema de Chebotarev, en el tercer capítulo se discute el teorema de Dirichlet de la progresión aritmética, que es un caso particular del teorema de Chebotarev cuando se considera la extensión ciclotómica. Esto sirve, a su vez, para presentar diferentes herramientas de análisis complejo relativas a la convergencia de las llamadas *series* L, y que luego desempeñan un papel relevante en el estudio del resultado principal de la memoria.

Finalmente, en el cuarto capítulo enunciamos el teorema de Chebotarev y lo relacionamos con los conceptos previos, recuperando los tres resultados que hemos discutido en esta introducción. El último capítulo sirve para introducir algunas de las ideas que intervienen en la demostración. Grosso modo, podríamos decir que son precisos dos tipos de ingredientes principales: (i) los de tipo algebraico, relativos principalmente a la llamada teoría de cuerpos de clase; y (ii) los de tipo analítico, relativos a generalizaciones de las funciones L de Dirichlet cuyas propiedades analíticas permiten demostrar el resultado.

Capítulo 1

Factorización de polinomios módulo p

En nuestro camino hacia la presentación del teorema de densidad de Chebotarev, resulta interesante comenzar analizando el comportamiento de la factorización de polinomios de bajo grado (dos, tres y cuatro) módulo p. Más adelante en la memoria, podremos comprobar cómo estos resultados encajan con el teorema principal del trabajo. Con este objetivo, retomamos algunos teoremas clásicos, como la ley de reciprocidad cuadrática, y realizamos diversos experimentos numéricos con SageMath.

1.1. La ley de reciprocidad cuadrática

Para poder analizar el comportamiento de los polinomios de grado dos vamos a introducir algunos conceptos que nos serán de utilidad para ver la factorización módulo un primo p. Vamos a comenzar presentando la ley de reciprocidad cuadrática, que se puede encontrar en cualquier libro introductorio a la teoría de números, aunque hemos usado principalmente el texto de Ireland y Rosen [6], que también muestra cómo extenderla a casos como la reciprocidad cúbica o bicuadrática.

Definición 1.1. Sea a un entero y p un primo. Diremos que a es *residuo cuadrático módulo p* si existe solución para la siguiente congruencia:

$$x^2 \equiv a \qquad (\text{mód } p).$$

En caso contrario, decimos que a no es residuo cuadrático.

Si a es múltiplo de p, la congruencia $x^2 \equiv a \pmod{p}$ tiene exactamente una solución módulo p. En caso contrario, si tiene solución, tiene exactamente dos soluciones. Sabiendo esto, podemos definir lo que se llama *símbolo de Legendre*.

Definición 1.2. Dado a un entero y p un primo, se define el *símbolo de Legendre* como:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } p \text{ es divisor de } a, \\ 1 & \text{si } p \text{ no es divisor de } a \text{ y } a \text{ es residuo cuadrático} \pmod p, \\ -1 & \text{si } p \text{ no es divisor de } a \text{ y } a \text{ no es residuo cuadrático} \pmod p. \end{cases}$$

Observación 1.3. Para $a = 2$ y para $a = -1$ el símbolo de Legendre viene dado por las siguientes expresiones:

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \text{ o } 7 \pmod 8 \\ -1 & \text{si } p \equiv 3 \text{ o } 5 \pmod 8. \end{cases}$$

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \pmod 4 \\ -1 & \text{si } p \equiv 3 \pmod 4. \end{cases}$$

Observación 1.4. El símbolo de Legendre tiene la siguiente propiedad multiplicativa: sean a y b dos enteros y p un primo; entonces,

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right).$$

Estas observaciones las podemos encontrar en el texto *A Course in Arithmetic* de Jean-Pierre Serre [11], uno de los textos de referencia para este trabajo.

Ejemplo 1.5. Para ilustrar los resultados anteriores, tomemos $p = 5$ y veamos cuál es el símbolo de Legendre de 18 sobre 5 usando la propiedad multiplicativa.

$$\left(\frac{18}{5}\right) = \left(\frac{9}{5}\right) \cdot \left(\frac{2}{5}\right) = \left(\frac{3}{5}\right)^2 \cdot \left(\frac{2}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

En la penúltima igualdad hemos usado que el cuadrado de un símbolo de Legendre es 1 (si el número de arriba no divide al de abajo) y que 2 no es residuo cuadrático módulo 5. Llegamos por lo tanto a la conclusión de que 18 no es residuo cuadrático módulo 5.

Esto es consistente con el hecho de que el símbolo de Legendre solo depende de la clase módulo p, por lo que directamente podríamos haber observado que

$$\left(\frac{18}{5}\right) = \left(\frac{3}{5}\right) = -1,$$

ya que los únicos residuos cuadráticos no nulos módulo 5 son 1 y 4.

Gracias a haber introducido el símbolo de Legendre, podemos formular la ley de reciprocidad cuadrática, que es uno de los resultados más clásicos y conocidos de la teoría de números.

Teorema 1.6 (**Ley de reciprocidad cuadrática**). *Sean p e q dos primos impares distintos. Entonces se cumple que*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)\cdot(q-1)}{4}}.$$

Hay muchas demostraciones en la literatura de este hecho, que generalmente se atribuye a Gauss, que presentó siete diferentes. Dado que no es el objetivo central de este trabajo, omitimos la prueba que, en su versión más elemental, pasa por aplicar el teorema chino del resto de forma adecuada. En un lenguaje informal, este resultado afirma que si al menos uno de los primos es congruente con 1 módulo 4, entonces p es residuo cuadrático módulo q si y solamente si q es residuo cuadrático módulo p, mientras que si ambos son congruentes con 3 módulo 4, p es residuo cuadrático módulo q si y solamente si q no es residuo cuadrático módulo p.

1.2. Factorización de polinomios de grado 2

En esta sección vamos a ver cómo pueden factorizar los polinomios de grado dos módulo un primo p. Para eso, recordamos que estos polinomios pueden factorizar de tres formas: puede ser irreducible (factorizar como un polinomio de grado dos), puede factorizar como la multiplicación de dos polinomios de grado uno distintos o puede factorizar como un polinomio de grado uno al cuadrado.

Vamos a suponer siempre que p es un primo impar, es decir, vamos a omitir el caso en el que $p = 2$, lo cual simplificará algunos razonamientos.

Supongamos que $f(x) = x^2 + ax + b$. Entonces, si multiplicamos por 4, no cambia nada su factorización módulo p. Por lo tanto, consideremos nuestro nuevo polinomio

$$4 \cdot f(x) = g(x) = 4x^2 + 4ax + 4b = (2x + a)^2 + 4b - a^2.$$

Podemos hacer el cambio de variable $y = 2x + a$ y $c = 4b - a^2$, con lo que acabamos teniendo un polinomio $g(y) = y^2 + c$. Por lo tanto, si entendemos el comportamiento de los polinomios de la forma $f(x) = x^2 + a$ vamos a comprender el de los polinomios con término lineal mediante este cambio de variable.

Veamos a continuación cuándo se dan los distintos casos relativos a la factorización de estos polinomios.

Sea $f(x) = x^2 + a$ un polinomio con $a \in \mathbb{Z}$. Veamos cuándo este polinomio puede factorizarse como un polinomio de grado uno al cuadrado. Sea p un primo impar cualquiera, entonces:

$$\left\{ \begin{array}{ll} x^2 + a \equiv (x + c)^2 & (\text{mód } p) \\ (x + c)^2 = x^2 + c^2 + 2 \cdot c \cdot x & \end{array} \right\} \quad \Leftrightarrow \quad \left\{ \begin{array}{ll} 2 \cdot c \equiv 0 & (\text{mód } p) \\ c^2 \equiv a & (\text{mód } p) \end{array} \right\},$$

y podemos razonar lo siguiente:

$$p \mid 2 \cdot c \;\Leftrightarrow\; p \mid c \;\Leftrightarrow\; c \equiv 0 \pmod{p} \;\Leftrightarrow\; c^2 \equiv a \equiv 0 \pmod{p}$$

Por lo tanto, si $f(x) = x^2+a$ factoriza como un polinomio de grado uno al cuadrado, entonces es de la forma $f(x) \equiv x^2 \pmod{p}$ y esto pasa si y solamente si $p \mid a$. En conclusión, dado un polinomio fijo, este polinomio solo factoriza un número finito de veces en un polinomio de grado uno al cuadrado módulo p (pues los factores en la factorización en primos de a son finitos).

Para analizar el resto dos casos, comencemos viendo qué pasa si $f(x) = x^2 + q$ con q primo distinto de p. Notamos que en este caso solo tenemos dos opciones: que sea irreducible en módulo p o que factorice en dos polinomios distintos de grado uno módulo p. También notamos que el polinomio no será irreducible módulo p si tiene alguna solución, es decir, $x^2 + q$ no es irreducible módulo p si $-q$ es residuo cuadrático $\pmod{p}$. Veamos esto último con un ejemplo.

Ejemplo 1.7. Dado $f(x) = x^2 + 2$ estudiemos cómo factoriza módulo los distintos primos.

Sea p un primo impar. El polinomio $f(x)$ será irreducible o no dependiendo de si -2 es residuo cuadrático módulo p o no, lo cual podemos ver usando el símbolo de Legendre: si $\left(\frac{-2}{p}\right) = 1$, el polinomio $f(x)$ factoriza en dos de grado uno, y si $\left(\frac{-2}{p}\right) = -1$, el polinomio es irreducible. Además, sabemos lo siguiente:

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{2}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \pmod{p} \\ 1 & \text{si } p \equiv 3 \pmod{p} \\ -1 & \text{si } p \equiv 5 \pmod{p} \\ -1 & \text{si } p \equiv 7 \pmod{p} \end{cases}$$

Por lo tanto, si $p \equiv 1, 3 \pmod{8}$, $f(x)$ factoriza en dos polinomios distintos de grado uno. En cambio, si $p \equiv 5, 7 \pmod{8}$, $f(x)$ es irreducible.

Ya visto el caso de $q = 2$ en el ejemplo anterior pasemos al caso general, fijando un primo impar cualquiera q y veamos cómo factoriza $f(x) = x^2 + q$ módulo los primos impares. Si $p = q$ entonces $x^2 + q \equiv x^2$, que va a ser el único caso donde nuestro polinomio factorice como uno de grado uno al cuadrado. Como mostramos en el ejemplo, $x^2 + q$ factoriza en dos polinomios distintos de grado 1 módulo p si $x^2 + q$ tiene soluciones módulo p, es decir, si $-q$ es residuo cuadrático módulo p. Para ver esto, usaremos la ley de reciprocidad cuadrática vista antes:

$$\left(\frac{-q}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{q}{p}\right) = \left(\frac{-1}{p}\right) \cdot (-1)^{\frac{(p-1)\cdot(q-1)}{4}} \cdot \left(\frac{p}{q}\right)$$

En la ecuación anterior hemos usado la propiedad multiplicativa del símbolo de Legendre en la primera igualdad y la ley de reciprocidad cuadrática en la segunda.

Como $\left(\frac{-1}{p}\right)$ solo depende de cuánto es p módulo 4, $\left(\frac{p}{q}\right)$ depende de p módulo q y $(-1)^{\frac{(p-1)\cdot(q-1)}{4}}$ depende de p módulo 4, entonces con saber el valor de p módulo $4 \cdot q$ podremos saber como factoriza el polinomio módulo p.

Ejemplo 1.8. Tomemos $f(x) = x^2 + 3$, es decir, $q = 3$. Como vimos antes, $p = 3$ es el único caso donde $f(x) \equiv x^2 \pmod{p}$. Ahora, dado p un primo mayor que 3 bastaría saber cuánto es p módulo $4 \cdot 3 = 12$ para saber como factoriza, pues si $\left(\frac{-3}{p}\right) = 1$ entonces el polinomio factoriza como dos de grado uno módulo p, y si $\left(\frac{-3}{p}\right) = -1$ entonces el polinomio es irreducible módulo p.

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{3}{p}\right) = \left(\frac{-1}{p}\right) \cdot (-1)^{\frac{(p-1)\cdot(3-1)}{4}} \cdot \left(\frac{p}{3}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{p}{3}\right) \cdot (-1)^{\frac{(p-1)}{2}}.$$

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \pmod 4, \\ -1 & \text{si } p \equiv 3 \pmod 4. \end{cases}$$

$$\left(\frac{p}{3}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \pmod 3, \\ -1 & \text{si } p \equiv 2 \pmod 3. \end{cases}$$

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{si } p \equiv 1 \pmod 4, \\ -1 & \text{si } p \equiv 3 \pmod 4. \end{cases}$$

Con todo esto, vemos que

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \text{ o } 7 \pmod{12}, \\ -1 & \text{si } p \equiv 5 \text{ o } 11 \pmod{12}. \end{cases}$$

Por tanto, $f(x)$ factoriza como el producto de dos polinomios de grado uno si $p \equiv 1$ o $7 \pmod{12}$ y es irreducible si $p \equiv 5$ o $11 \pmod{12}$.

Para el caso general de un polinomio de la forma $f(x) = x^2 + a$, con $a \in \mathbb{Z}$ arbitrario, se hace de una forma similar. Primero, descomponemos a en factores primos:

$$a = \pm 1 \cdot p_1^{n_1} \cdot p_2^{n_2} \cdots p_m^{n_m}.$$

Queremos mirar la factorización del polinomio módulo p, siendo p un primo impar que no divide a a, pues, de ser el caso, el polinomio factoriza como uno de grado uno al cuadrado como ya vimos antes. Para analizar cual será la factorización módulo p, usaremos como antes la ley de reciprocidad cuadrática y las propiedades de los símbolos de Legendre, sabiendo que el polinomio tendrá raíces si $-a$ es residuo cuadrático módulo p; de tener raíces factorizará en dos polinomios distintos de grado uno. En caso de no tener raíces, es decir, si $-a$ no es residuo cuadrático módulo p, será irreducible:

$$\left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{a}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{p_1}{p}\right)^{n_1} \cdot \left(\frac{p_2}{p}\right)^{n_2} \cdot \ldots \cdot \left(\frac{p_m}{p}\right)^{n_m}.$$

Notamos que si el exponente n_i es par, el símbolo de Legendre elevado a ese número será uno (recordemos que estamos tomando p un primo impar que no divide a a). Si a es un entero negativo, podemos usar la propiedad multiplicativa del símbolo de Legendre con $a = (-1) \cdot (-a)$ y nos queda un caso simplificado pues en la expresión de arriba habría menos factores ya que aparece $\left(\frac{-1}{p}\right)^2$, que es uno. Tomando entonces a entero positivo tendremos la siguiente expresión:

$$\left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right) \cdot \prod_{i \in I_p} \left(\frac{p_i}{p}\right) = \left(\frac{-1}{p}\right) \cdot \prod_{i \in I_p} (-1)^{\frac{(p-1)\cdot(p_i-1)}{4}} \cdot \left(\frac{p}{p_i}\right),$$

siendo I_p el conjunto de los índices i tales que n_i es impar.

Por lo tanto, por el mismo razonamiento que antes, podríamos saber la factorización del polinomio $f(x) = x^2 + a$ tan solo sabiendo cómo es p módulo $(4 \cdot \prod_{i \in I_p} p_i)$

Ejemplo 1.9. Queremos saber cómo factoriza $f(x) = x^2 + 60$ módulo p. Supongamos que $p \nmid 60$, entonces sabemos que factorizará como multiplicación de dos polinomios distintos de primer grado o será irreducible. Veamos si -60 es residuo cuadrático módulo p

$$\begin{aligned}\left(\frac{-60}{p}\right) &= \left(\frac{-1}{p}\right) \cdot \left(\frac{2}{p}\right)^2 \cdot \left(\frac{3}{p}\right) \cdot \left(\frac{5}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{3}{p}\right) \cdot \left(\frac{5}{p}\right) \\ &= \left(\frac{-1}{p}\right) \cdot (-1)^{\frac{(p-1)\cdot(3-1)}{4}} \cdot \left(\frac{p}{3}\right) \cdot (-1)^{\frac{(p-1)\cdot(5-1)}{4}} \cdot \left(\frac{p}{5}\right) \\ &= \left(\frac{-1}{p}\right) \cdot (-1)^{\frac{(p-1)}{2}} \cdot \left(\frac{p}{3}\right) \cdot \left(\frac{p}{5}\right).\end{aligned}$$

Por lo tanto, con saber cuánto es p módulo 60 podríamos determinar el valor del símbolo de Legendre correspondiente, ya que $\left(\frac{-1}{p}\right)$ depende del resto de p módulo 4 (y los otros elementos que intervienen dependen de los restos módulo 3 o módulo 5).

1.3. Factorización de polinomios de grado 3 e 4

En esta sección discutiremos sobre la factorización de algunos polinomios tanto de grado 3 como de grado 4 módulo los distintos primos.

En los polinomios de grado 3 no vamos a tener en cuenta las factorizaciones de la forma grado uno al cubo y grado uno al cuadrado por otro de grado uno ya que a lo largo de los números primos solo apareceran un número finito de veces, igual que pasaba en la anterior sección con los de grado 1 al cuadrado.

1.3.1. Polinomios de grado 3

Comenzaremos discutiendo sobre la factorización del polinomio $f(x) = x^3 + 2$ módulo los primos impares. Diferenciaremos entre los primos $p \equiv 1 \pmod 3$ y $p \equiv 2 \pmod 3$. Primero, veamos como factoriza módulo p siendo $p \equiv 2 \pmod 3$. Para empezar, definamos la seguinte aplicación:

$$\phi\colon (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times; \quad x \mapsto x^3.$$

Antes de seguir, es necesario recordar lo que es una raíz primitiva módulo n. Sea $n \in \mathbb{N}$, diremos que a es una raíz primitiva módulo n si genera al grupo multiplicativo $(\mathbb{Z}/n\mathbb{Z})^\times$. Además, si n es un primo impar, entonces existe una raíz primitiva módulo n. Por ejemplo, para $n = 5$ se podría tomar $g = 3$ o $g = 2$ como raiz primitiva módulo 5.

Sea g una raíz primitiva módulo p. Por tratarse de un grupo cíclico con respecto a la multiplicación, se pueden ver los elementos de $(\mathbb{Z}/p\mathbb{Z})^\times$ como $\{1, g, g^2, g^3, ..., g^{p-2}\}$. Esto quiere decir que la aplicación ϕ definida antes se puede interpretar como la aplicación $g^i \mapsto g^{3\cdot i}$.

Definimos por lo tanto la siguiente aplicación:

$$\psi\colon \mathbb{Z}/(p-1)\mathbb{Z} \longrightarrow \mathbb{Z}/(p-1)\mathbb{Z}; \quad i \mapsto 3 \cdot i.$$

Como el 3 es una unidad módulo $p-1$ (ya que estamos en el caso $p \equiv 2 \pmod 3$), la aplicación ψ es biyectiva, por lo que se puede ver que ϕ es un isomorfismo de grupos. En otras palabras, dado cualquier elemento $y \in (Z/p\mathbb{Z})^\times$ existe un único elemento x en $(\mathbb{Z}/p\mathbb{Z})^\times$ de forma que $x^3 = y$.

Con lo cual, la equivalencia $x^3 \equiv -2 \pmod p$ tiene una única solución, por lo que, si $p = 3k + 2$, el polinomio $f(x) = x^3 + 2$ factoriza como la multiplicacion de un polinomio de grado uno por un polinomio de grado dos. (ya que no puede ser irreducible al existir solución a la equivalencia y no puede ser la multiplicación de tres polinomios de grado uno ya que solo existe una única solución).

Ahora veamos qué pasa en el caso en el que $p \equiv 1 \pmod 3$. La aplicación ψ correspondiente no es sobreyectiva ya que el 3 no es una unidad módulo $p - 1$, y solo 1/3 de los elementos tienen preimagen (los multiplos de 3 en $\mathbb{Z}/(p-1)\mathbb{Z}$). Además $|\ker\psi| = 3$ ya que $\ker(\psi) = \{0, \frac{p-1}{3}, \frac{2\cdot(p-1)}{3}\}$. También notamos que si un elemento de $\mathbb{Z}/(p-1)\mathbb{Z}$ tiene preimagen por ψ, entonces tiene exactamente 3 (si a es la preimagen de un elemento, entonces $a + \frac{p-1}{3}$ y $a + \frac{2\cdot(p-1)}{3}$ son preimágenes del mismo elemento). Todo esto implica que 1/3 de los elementos de $(\mathbb{Z}/p\mathbb{Z})^\times$ tienen preimagen por ϕ, y, si un elemento tiene preimagen, entonces tiene 3.

Volvamos al caso particular de nuestro polinomio. Si $f(x) = x^3 + 2$ tiene algunha solución módulo p, entonces eso significa que -2 tiene preimagen por ϕ. Como vimos antes, si tiene

una entonces va a tener tres distintas, por lo que si $f(x)$ tiene una solución, va a tener tres, y factorizará como la multiplicación de tres polinomios de grado 1 módulo p. En el caso de no tener soluciones, el polinomio será irreducible.

Controlando ya los dos casos que se pueden dar de primos módulo 3, vamos a ver la proporción de veces que nuestro polinomio factoriza en las distintas formas.

La proporción o el porcentaje del que vamos a hablar va a ser un concepto que veamos con más profundidad en próximas secciones, pero vamos a introducir una noción aproximada de lo que significa para poder entender bien lo que vamos a hablar.

Sea P el conjunto de los números primos y A un subconjunto de P. Sea P_n el conjunto de los n primeros números primos, y $A_n = P_n \cap A$ el conjunto de los números primos de A que están entre los n primeros primos. Vamos a llamar densidad de A en P al valor del siguiente límite (en caso de que exista):

$$\delta(A) := \lim_{n\to\infty} \frac{|A_n|}{|P_n|}$$

Por ejemplo, sea A el subconjunto de P de los primos p de la forma $p \equiv 2 \pmod 3$, sucede que la densidad de A en P es de $1/2$, es decir, que a medida que vayamos recorriendo todos los números primos, la mitad de los que aparezcan serán de esa forma. Lo mismo ocurre con los primos de la forma $p \equiv 1 \pmod 3$.

Por otra parte, conviene aclarar que cuando digamos que un polinomio factoriza de una forma con una determinado proporción, nos referiremos a que ese polinomio factoriza de esa misma forma en los primos del subconjunto $A \subset P$ y que A tiene esa proporción en P.

Para facilitar la escritura, diremos que un polinomio factoriza como $(a_1)(a_2)...(a_n)$ con $a_1 \geq a_2 \geq ... \geq a_n$ si en su descomposición en producto de primos se descompone como un factor de grado a_1, otro de a_2 y así hasta a_n.

Como dijimos antes, la proporción de veces que aparecen primos de la forma $p \equiv 2 \pmod 3$ es de $1/2$, por lo que $f(x)$ factoriza como $(2)(1)$ con una proporción de $1/2$.

Por otro lado, cuando $p \equiv 1 \mod 3$, como $1/3$ de los elementos tienen preimagen por ϕ, entonces:

$$f(x) = x^3 + 2 \text{ factoriza como } (1)(1)(1) \text{ con proporción } \frac{1}{2}\cdot\frac{1}{3} = \frac{1}{6},$$
$$f(x) = x^3 + 2 \text{ factoriza como } (3) \text{ con proporción } \frac{1}{2}\cdot\frac{2}{3} = \frac{1}{3}.$$

Otro ejemplo de polinomio de grado 3 que podemos ver como factoriza es el polinomio $g(x) = x^3 - 3x - 1$. Cuando este polinomio tiene una solución, va a tener otras dos y las tres son

distintas entre si. Además, la proporción en la que factoriza este polinomio es de 1/3 en forma (1)(1)(1) y de 2/3 en forma (3).

Tomando como ejemplo los dos polinomios anteriores, podemos ver cómo se relaciona el grupo de Galois de cada polinomio con su factorización módulo los distintos primos. En nuestro caso, los grupos de Galois de $f(x) = x^3 + 2$ y $g(x) = x^3 - 3x - 1$ (que son los polinomios usados antes) son el grupo simétrico S_3 y el grupo alternado A_3 respectivamente, que son los siguientes grupos:

$$S_3 = \{\mathrm{Id}, (2,3), (1,3), (1,2), (1,2,3), (1,3,2)\},$$
$$A_3 = \{\mathrm{Id}, (1,2,3), (1,3,2)\}.$$

Vemos que en ambos casos la proporción de veces que aparecen las distintas formas en el grupo de Galois corresponden con la proporcion de veces que factoriza de esa misma forma el polinomio correspondente módulo los primos.

Por ejemplo, dijimos que el polinomio con grupo de Galois asociado S_3 factoriza como producto de uno de grado dos y otro de grado uno con una proporcion de 1/2, y viendo el grupo de Galois S_3 que tiene seis elementos, tres de ellos son transposiciones. Es decir, 1/2 de los elementos de S_3 son transposiciones, que podemos asociar con la proporción de veces que factoriza el polinomio de la forma descrita antes.

En efecto, el grupo de Galois nos permitirá conocer los diferentes patrones que pueden aparecer en la factorización de estos polinomios módulo p. Para facilitar la comprensión de esta idea cuando el grado del polinomio es mayor, vamos a realizar en primer lugar ciertos experimentos computacionales.

1.3.2. Polinomios de grado 4 y 5

En las siguientes tablas vamos a ver algunos ejemplos de factorización de polinomios de grado cuatro y cinco con distintos grupos de Galois asociados en los primeros mil primos. Veremos el número esperado de veces que factoriza cada polinomio seguún su grupo de Galois, el número de veces que realmente factoriza de cada forma conseguido con SageMath y valoraremos los resultados. El código usado se puede consultar en el apéndice de este trabajo. Por otro lado, hemos considerado un polinomio para cada posible grupo de Galois; para ello, conviene recordar que el grupo de Galois de un polinomio de Galois irreducible sobre $\mathbb{Q}$ es un subgrupo transitivo de S_n, por lo que hay cinco posibilidades tanto en grado 4 como en grado 5.

Cuadro 1.1: Factorización módulo los primeros mil primos (valor esperado grado 4)

Polinomio	Grupo de Galois	(4)	(3)(1)	(2)(2)	(2)(1)(1)	(1)(1)(1)(1)
x^4+x+1	S_4	250	333	125	250	42
x^4+8x^2+8x+4	A_4	0	666	250	0	83
x^4-2	D_8	250	0	375	250	125
x^4+4x^2+2	$\frac{\mathbb{Z}}{4\mathbb{Z}}$	500	0	250	0	250
x^4-x^2+1	$\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$	0	0	750	0	250

Cuadro 1.2: Factorización módulo los primeros mil primos (valor real grado 4)

Polinomio	Grupo de Galois	(4)	(3)(1)	(2)(2)	(2)(1)(1)	(1)(1)(1)(1)
x^4+x+1	S_4	258	334	123	250	34
x^4+8x^2+8x+4	A_4	0	667	254	0	77
x^4-2	D_8	254	0	376	252	117
x^4+4x^2+2	$\frac{\mathbb{Z}}{4\mathbb{Z}}$	506	0	248	0	245
x^4-x^2+1	$\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$	0	0	757	0	241

Cuadro 1.3: Factorización módulo los primeros mil primos (valor esperado grado 5)

Polinomio	Grupo de Galois	(5)	(4)(1)	(3)(1)(1)	(3)(2)	(2)(2)(1)	(2)(1)(1)(1)	(1)(1)(1)(1)(1)
x^5-x-1	S_5	200	250	167	167	125	83	8
$x^5+20x+16$	A_5	400	0	334	0	250	0	16
$x^5+11x+44$	D_{10}	400	0	0	0	500	0	100
$x^5+x^4-4x^3-3x^2+3x+1$	Aff(5)	200	500	0	0	250	0	50
x^5-2	$\frac{\mathbb{Z}}{5\mathbb{Z}}$	800	0	0	0	0	0	200

Cuadro 1.4: Factorización módulo los primeros mil primos (valor real grado 5)

Polinomio	Grupo de Galois	(5)	(4)(1)	(3)(1)(1)	(3)(2)	(2)(2)(1)	(2)(1)(1)(1)	(1)(1)(1)(1)(1)
x^5-x-1	S_5	198	245	170	167	125	89	4
$x^5+20x+16$	A_5	389	0	358	0	239	0	12
$x^5+11x+44$	D_{10}	401	0	0	0	505	0	91
$x^5+x^4-4x^3-3x^2+3x+1$	Aff(5)	198	507	0	0	246	0	47
x^5-2	$\frac{\mathbb{Z}}{5\mathbb{Z}}$	799	0	0	0	0	0	200

Tras ver las tablas, podemos ver que el grupo de Galois asociado al polinomio tiene un papel importante en la densidad de factorizacion de los polinomios módulo los distintos primos, pues el valor esperado de cada polinomio se parece mucho al valor real obtenido con SageMath factorizando módulo los cien primeros primos.

Vamos a ilustrarlo a través de algún ejemplo. En el caso del polinomio $x^4 - 2$, su grupo de Galois es el grupo diedral de 8 elementos, D_8, que se puede identificar con las simetrías del cuadrado. Entendido como subgrupo de S_4, sus elementos son los siguientes:

- la identidad;
- los dos 4-ciclos $(1,2,3,4)$ y $(1,4,3,2)$;
- los tres productos de transposiciones $(1,2)(3,4)$, $(1,3)(2,4)$ y $(1,4)(2,3)$;
- las dos transposiciones $(1,3)$ y $(2,4)$.

Al primer tipo pertenecen 1/8 de los elementos, por lo que el número esperado de primos es $\frac{1}{8} \cdot 1000 = 125$; para el segundo, $\frac{2}{8} \cdot 1000 = 250$; para el tercero, $\frac{3}{8} \cdot 1000 = 375$; y, para el último, $\frac{2}{8} \cdot 1000 = 250$.

Como vemos en la segunda tabla, los resultados están muy cerca de parecerse a los que esperabamos con el grupo de Galois, pues tenemos:

- El polinomio factoriza 117 veces de la forma $(1)(1)(1)(1)$. Esta factorización es la que asociamos con la identidad cuyo numero esperado de primos era 125.
- Factoriza 252 veces de la forma $(2)(1)(1)$. Esta factorización es la que asociamos con las transposiciones que nos daban un valor esperado de 250.
- Factoriza 376 veces de la forma $(2)(2)$, que asociamos con el producto de dos transposiciones con valor esperado de 375.
- Factoriza 274 veces de la forma (4) que asociamos con el numero de 4-ciclos. Estos tienen un valor esperado de 250.

Notar que en los valores reales la suma de todos no da 1000, esto es porque no se esta contando con las veces que algun factor está repetido, que como explicamos anteriormente, pasa un número finito de ocasiones.

Vamos a discutir ahora el caso del grupo afín de 20 elementos, $\mathrm{Aff}(5)$, que es el grupo de Galois del polinomio $x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$. Sus elementos se pueden identificar con pares (α, β), donde $\alpha \in (\mathbb{Z}/5\mathbb{Z})^\times$ y $\beta \in \mathbb{Z}/5\mathbb{Z}$. $(\mathrm{Aff}(5), \cdot)$ es un grupo donde la operación esta definida de la siguiente forma: dados $(\alpha, \beta), (\gamma, \delta) \in \mathrm{Aff}(5)$, entonces $(\alpha, \beta) \cdot (\gamma, \delta) = (\alpha\gamma, \alpha\delta + \beta)$ (todo en módulo 5).

Antes de continuar, vamos a brevemente motivar la construcción de este grupo. Recordemos que las afinidades biyectivas para la recta real afín son de la forma $x \mapsto ax + b$ con $x, b \in \mathbb{R}$ y

$a \in \mathbb{R} \setminus \{0\}$. Una afinidad de este tipo se puede representar en forma matricial de la siguiente forma:

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} ax+b \\ 1 \end{pmatrix}.$$

Esta afinidad se puede hacer también para cuerpos finitos (en particular, para el cuerpo finito de cinco elementos), por lo que en este caso $a \in (\mathbb{Z}/5\mathbb{Z})^\times$ y $b \in \mathbb{Z}/5\mathbb{Z}$. Por tanto, los elementos de $\mathrm{Aff}(5)$ son todas las posibles afinidades biyectivas en un cuerpo finito de orden 5, y la operación no es más que la multiplicación de las matrices que las representan (que sería la matriz que representa la composición de afinidades):

$$\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \gamma & \delta \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \alpha\gamma & \alpha\delta+\beta \\ 0 & 1 \end{pmatrix}.$$

Por tanto, para ver el orden de los elementos de $\mathrm{Aff}(5)$, tenemos que tener en cuenta que (α, β) es la identidad si $\alpha x + \beta = x$, es decir,

$$\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} x \\ 1 \end{pmatrix}.$$

Por tanto, $(1, 0)$ es la identidad de $\mathrm{Aff}(5)$ y podemos analizar los distintos casos:

- si $\alpha = 1$ y $\beta = 0$, tenemos la identidad, por lo que el número esperado de primos con la descomposición $(1)(1)(1)(1)(1)$ es $\frac{1}{20} \cdot 1000 = 50$;
- si $\alpha = 1$ y $\beta \neq 0$, tenemos un 5-ciclo, por lo que el número esperado de primos con descomposición (5) es $\frac{4}{20} \cdot 1000 = 1000 = 200$;
- si $\alpha = -1$, hay exactamente un punto fijo y, como el elemento tiene orden dos, tenemos una descomposición de la forma $(2)(2)(1)$, por lo que el número esperado de primos en esta categoría es $\frac{5}{20} \cdot 1000 = 250$;
- si $\alpha = \pm 2$, hay exactamente un punto fijo y el elemento tiene orden cuatro; esto indica que el número esperado de primos con la descomposición $(4)(1)$ es $\frac{10}{20} \cdot 1000 = 500$.

Vamos a comparar estos resultados esperados con los resultados reales:

- El polinomio factoriza 47 veces de la forma $(1)(1)(1)(1)(1)$, y esperabamos que lo hiciera 50 veces.

- Factoriza 246 veces de la forma (2)(2)(1), y lo esperado era 250.
- Factoriza 507 veces de la forma (4)(1), y el valor esperado era 500.
- Es irreducible en 198 ocasiones, y lo esperado era que lo fuera en 200.

Viendo estos ejemplos de polinomios de grado 4 y grado 5 con distintos grupos de Galois, vemos que los valores obtenidos y los esperados analizando su grupo de Galois son muy parecidos, lo que nos confirma la relación del grupo de Galois del polinomio con su factorización módulo los distintos primos.

Capítulo 2

Factorización de primos en extensiones

En esta sección vamos a presentar conceptos esenciales para enunciar y poder demostrar el teorema de densidad de Chebotarev (y, más en general, para discutir diferentes resultados de teoría algebraica de números que se necesitan a lo largo de la memoria). Entre estos conceptos está el anillo de enteros de un cuerpo, los índices de ramificación, grado de inercia y el elemento de Frobenius. Para este capítulo, las referencias principales que se han usado son [8], [9] y [10], aunque también hemos usado [7], que proporciona un acercamiento adecuado a los temas de teoría de cuerpos de clase que se introducirán en capítulos posteriores.

2.1. Factorización en extensiones

Para comenzar, denotaremos por K a un subcuerpo de $\mathbb{C}$ y $[K:\mathbb{Q}]$ al grado de la extensión de K sobre $\mathbb{Q}$, que supondremos finita. Decimos entonces que K es un *cuerpo de números*. Definamos en primer lugar el anillo de enteros de K.

Definición 2.1. Sea K un cuerpo sobre $\mathbb{Q}$, el *anillo de enteros de* K, denotado como $\mathcal{O}_K$, será el conjunto de los $\alpha \in K$ que son ceros de algún polinomio mónico con coeficientes enteros.

$$\begin{array}{ccc} K & \text{——} & \mathcal{O}_K \\ | & & | \\ \mathbb{Q} & \text{——} & \mathbb{Z} \end{array}$$

Nótese que el anillo de enteros de $\mathbb{Q}$ es el propio $\mathbb{Z}$. Se tiene además que $\mathcal{O}_K$, como su nombre sugiere, es un anillo, aunque no es completamente evidente que sea cerrado para la suma y la multiplicación. Por ejemplo, el anillo de enteros de $K = \mathbb{Q}(\sqrt{-3})$ es $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ y el de $K = \mathbb{Q}(i)$ es $\mathcal{O}_K = \mathbb{Z}[i]$.

Ya definidos los anillos de enteros de un cuerpo K, tenemos estos dos resultados importantes sobre ellos.

Teorema 2.2. *Sea $\mathcal{O}_K$ el anillo de enteros del cuerpo K. Entonces, $\mathcal{O}_K$ es un dominio de Dedekind, es decir:*

1. *$\mathcal{O}_K$ es íntegramente cerrado en K, es decir, si $\alpha \in K$ es cero de un polinomio mónico con coeficientes en $\mathcal{O}_K$, entonces $\alpha \in \mathcal{O}_K$.*
2. *$\mathcal{O}_K$ es noetheriano, es decir, dada cualquier cadena de ideales $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset ...$, existe un entero n tal que $\mathfrak{a}_n = \mathfrak{a}_{n+1} = ...$*
3. *Todo ideal primo distinto de cero de $\mathcal{O}_K$ es maximal.*

El motivo principal por el que nos interesa realizar esta definición es que los dominios de Dedekind satisfacen un resultado de factorización única. Es decir, no es cierto que sean dominios de factorización única, pero sí hay un resultado análogo cuando tomamos productos de ideales primos.

Teorema 2.3. *Sea K cuerpo de números. Todo ideal distinto de cero de $\mathcal{O}_K$ se puede escribir como producto de ideales primos*

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$$

y esta descomposición es única para cada ideal $\mathfrak{a}$. Además, esos $\mathfrak{p}_i$ son exactamente los ideales primos de $\mathcal{O}_K$ que contienen a $\mathfrak{a}$.

Durante este capítulo vamos a considerar la extensión de cuerpos de números L/K finita y separable. Antes de continuar vamos a mencionar algunos conceptos importantes sobre estas extensiones:

Definición 2.4. Sea L/K una extensión de cuerpos de números finita y separable y sea $\mathcal{O}_K$ el anillo de enteros de K. Decimos que $\alpha \in L$ es *entero sobre* $\mathcal{O}_K$ si es raíz de algún polinomio mónico con coeficientes en $\mathcal{O}_K$. El conjunto de elementos de L que son enteros sobre $\mathcal{O}_K$ es un anillo que llamaremos *clausura íntegra de $\mathcal{O}_K$ en L* y la denotaremos por $\mathcal{O}_L$.

Notamos que el anillo de enteros de K es la clausura íntegra de $\mathbb{Z}$ sobre K considerando la extensión $K/\mathbb{Q}$.

Observación 2.5. Aunque estemos llamando $\mathcal{O}_K$ al anillo de enteros de K y $\mathcal{O}_L$ a la clausura íntegra de $\mathcal{O}_K$ sobre L, hay que notar que $\mathcal{O}_L$ no es el anillo de enteros de L, pues dado un elemento de $\mathcal{O}_L$, este elemento es raíz de un polinomio mónico con coeficientes en $\mathcal{O}_K$, pero no

tiene que ser raíz de un polinomio mónico con coeficientes enteros. A pesar de ello, se tiene que $\mathcal{O}_K \subseteq \mathcal{O}_L$ es una extensión de anillos.

$$\begin{array}{ccc} L & \text{——} & \mathcal{O}_L \\ | & & | \\ K & \text{——} & \mathcal{O}_K \end{array}$$

Proposición 2.6. *Sea L/K una extensión finita y separable de cuerpos de números. Sea $\mathcal{O}_K$ el anillo de enteros de K y sea $\mathcal{O}_L$ la clausura íntegra de $\mathcal{O}_K$ sobre L. Entonces se tiene que $\mathcal{O}_L$ es un dominio de Dedekind.*

Este resultado nos va a permitir trabajar sobre extensiones de cuerpos de números arbitrarias, pues la factorización de los ideales primos en $\mathcal{O}_L$ va a seguir siendo única ya que sigue siendo un dominio de Dedekind.

Como ya mostramos en el capítulo anterior, uno de los objetivos principales es entender cómo es la factorización en producto de primos en extensiones de $\mathbb{Q}$. Para ello, definamos los índices de ramificación y el grado de inercia:

Definición 2.7. Sea K un cuerpo de números, y sea L una extesión finita de K. Si $\mathfrak{p}$ es un ideal primo de $\mathcal{O}_K$, entonces $\mathfrak{p}\mathcal{O}_L$ es un ideal de $\mathcal{O}_L$ (el ideal de $\mathcal{O}_L$ generado por $\mathfrak{p}$) y su factorización en primos será:

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

donde los $\mathfrak{P}_i$ son los distintos primos de L que contienen a $\mathfrak{p}$.

- Llamaremos *índices de ramificación* a los enteros que denotamos antes como e_i.
- Diremos también que $\mathfrak{P}_i$ es *no ramificado sobre* $\mathfrak{p}$ si $e_i = 1$.
- Si $\mathfrak{P}_i$ es no ramificado para $i = 1, ..., g$ diremos que $\mathfrak{p}$ es *no ramificado en* $\mathcal{O}_L$.
- Por otra parte, si algún índice de ramificación e_i es mayor que uno, decimos que $\mathfrak{p}$ *ramifica en* L y se puede probar que solo un número finito de primos de K ramifican en L.

Supongamos que en la descomposición anterior el primo no está ramificado. Si $g > 1$ decimos que $\mathfrak{p}$ *se descompone en* $\mathcal{O}_L$, pero si $g = 1$, entonces $\mathfrak{p}\mathcal{O}_L$ es primo de $\mathcal{O}_L$ y decimos que $\mathfrak{p}$ es *inerte*.

Observación 2.8. Para la anterior factorización del ideal $\mathfrak{p}\mathcal{O}_L$, a los ideales primos $\mathfrak{P}_i$ los llamaremos ideales primos de $\mathcal{O}_L$ que contienen a $\mathfrak{p}$ o que dividen a $\mathfrak{p}$.

Cada primo $\mathfrak{P}_i$ escrito antes también define una extensión de cuerpos finitos

$$\mathcal{O}_K/\mathfrak{p} \subset \mathcal{O}_L/\mathfrak{P}_i$$

ya que, como estamos en un dominio de Dedekind, todo ideal primo será maximal; por lo tanto, el cociente del anillo y el ideal será un cuerpo. Gracias a esta extensión podemos definir el grado de inercia.

Definición 2.9. Definimos el *grado de inercia* o *grado residual* del primo $\mathfrak{p}$ en $\mathfrak{P}_i$ como el grado de la extensión $[\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}] = f_i$.

Uno de los resultados por los que estos índices son importantes es el siguiente.

Teorema 2.10. *Sea $K \subset L$ una extensión de cuerpos, y $\mathfrak{p}$ un primo de K. Si e_i e f_i son los índices de ramificación y los grados de inercia respectivamente definidos arriba, entonces*

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

Como la mayoría de extensiones $K \subset L$ con las que trabajaremos son extensiones de Galois, existe una simplificación del teorema anterior para este tipo de extensiones:

Teorema 2.11. *Sea $K \subset L$ una extensión de Galois y $\mathfrak{p}$ un primo de K. Sean $\mathfrak{P}_1, ..., \mathfrak{P}_g$ los primos de L que contienen a $\mathfrak{p}$. Entonces todos estos primos tienen los mismos índices de ramificación y los mismos grados de inercia, lo que simplifica la fórmula anterior de la siguiente forma:*

$$efg = [L : K],$$

siendo e el índice de ramificación común, f el grado de inercia común y g el número de primos de L que contienen a $\mathfrak{p}$.

En este caso, si $K \subset L$ es una extensión de Galois, diremos que el primo $\mathfrak{p}$ de K ramifica si $e > 1$ y no ramifica si $e = 1$.

2.2. El elemento de Frobenius

En este apartado trataremos de definir lo que es el elemento de Frobenius. Para ello necesitamos introducir el grupo de descomposición y el grupo de inercia. Antes de eso, veamos la siguiente proposición importante sobre el grupo de Galois de una extensión de cuerpos:

Proposición 2.12. *Sea L/K una extensión de cuerpos y G su grupo de Galois. Entonces:*

- *G actúa sobre $\mathcal{O}_L$, es decir, $\sigma(\mathcal{O}_L) \subseteq \mathcal{O}_L$ $\forall \sigma \in \mathrm{Gal}(L/K)$.*
- *Si $\mathfrak{p}$ es un ideal primo no nulo de $\mathcal{O}_K$ y $\mathfrak{P}$ es un ideal primo de $\mathcal{O}_L$ que contiene a $\mathfrak{p}$, entonces $\sigma(\mathfrak{P})$ es un ideal primo de $\mathcal{O}_L$ que contiene a $\mathfrak{p}$.*
- *Sea $\mathfrak{p}$ un ideal primo no nulo de $\mathcal{O}_K$. La acción de G sobre el conjunto de ideales primos de $\mathcal{O}_L$ que contienen a $\mathfrak{p}$ es transitiva, es decir, si $\mathfrak{P}_1$ y $\mathfrak{P}_2$ son ideales primos de $\mathcal{O}_L$ que contienen a $\mathfrak{p}$, entonces existe $\sigma \in \mathrm{Gal}(L/K)$ tal que $\sigma(\mathfrak{P}_1) = \mathfrak{P}_2$.*

El resultado que acabamos de ver va a ser importante tenerlo en cuenta para algunas proposiciones durante el trabajo. Con esto en mente, definamos los conceptos hablados antes:

Definición 2.13. Sea L/K una extensión de cuerpos con grupo de Galois G. Sea también $\mathfrak{p}$ un ideal primo no nulo de $\mathcal{O}_K$ y $\mathfrak{P}$ uno de los ideales primos de $\mathcal{O}_L$ que contiene a $\mathfrak{p}$. Entonces, el conjunto:

$$D(\mathfrak{P} \mid \mathfrak{p}) = \{\sigma \in G : \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

es un subgrupo del grupo de Galois llamado *grupo de descomposición de $\mathfrak{P}$ sobre $\mathfrak{p}$*. Si la extensión es de Galois, entonces $|D(\mathfrak{P} \mid \mathfrak{p})| = e \cdot f$ siendo e y f el índice de ramificación y el grado de inercia respectivamente.

Para definir el grupo de inercia, antes tenemos que considerar la siguiente aplicación.

Proposición 2.14. *Dado σ un automorfismo del cuerpo L, $\mathfrak{P}$ un ideal primo no nulo de $\mathcal{O}_L$ y $\mathfrak{P}' = \sigma(\mathfrak{P})$. Entonces existe una única aplicación $\overline{\sigma} : \mathcal{O}_L/\mathfrak{P} \to \mathcal{O}_L/\mathfrak{P}'$ que satisface que*

$$\overline{\sigma}(\alpha + \mathfrak{P}) = \sigma(\alpha) + \mathfrak{P}' \quad \forall \alpha \in \mathcal{O}_L,$$

y es un isomorfismo de anillos. Además, si σ deja fijo un subcuerpo $K \subset L$ y si $\mathfrak{p}$ es un ideal primo de $\mathcal{O}_K$ contenido en $\mathfrak{P}$, entonces $\overline{\sigma}$ deja fijo $\mathcal{O}_K/\mathfrak{p}$. Vamos a denotar por $\psi_{\mathfrak{P}}$ a la aplicación que lleva $\sigma \mapsto \overline{\sigma}$ y por $\psi_{\mathfrak{P}}|_{\mathfrak{p}}$ a la restricción de esta aplicación a $D(\mathfrak{P} \mid \mathfrak{p})$. La imagen de esta última aplicación está contenida en $\mathrm{Gal}(\frac{\mathcal{O}_L}{\mathfrak{P}}/\frac{\mathcal{O}_K}{\mathfrak{p}})$.

Definición 2.15. Sea L/K una extensión de cuerpos con grupo de Galois G, y sea $\mathfrak{P}$ un ideal primo de $\mathcal{O}_L$ que contiene a $\mathfrak{p}$, ideal primo no nulo de $\mathcal{O}_K$. Entonces la aplicación

$$\psi_{\mathfrak{P}}|_{\mathfrak{p}} : D(\mathfrak{P} \mid \mathfrak{p}) \to \mathrm{Gal}(\frac{\mathcal{O}_L}{\mathfrak{P}}/\frac{\mathcal{O}_K}{\mathfrak{p}})$$

es un homomorfismo de grupos sobreyectivo cuyo núcleo es

$$I(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in G : \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}} \text{ para todo } \alpha \in \mathcal{O}_L\}$$

y a $I(\mathfrak{P}/\mathfrak{p})$ le llamamos *grupo de inercia de $\mathfrak{P}$ sobre $\mathfrak{p}$*. Si la extensión es de Galois, entonces $|I(\mathfrak{P}/\mathfrak{p})| = e$ por lo que, para los primos no ramificados, el grupo de inercia es trivial.

Y con todo esto, podemos definir el elemento de Frobenius.

Definición 2.16. Sea L/K una extensión de Galois con grupo de Galois G. Sea $\mathfrak{p}$ un ideal primo no nulo de $\mathcal{O}_K$ que no ramifica en $\mathcal{O}_L$ y sea $\mathfrak{P}$ uno de los ideales primos de $\mathcal{O}_L$ que contiene a $\mathfrak{p}$. Entonces se define el elemento de Frobenius de $\mathfrak{P}$ como el elemento de $D(\mathfrak{P} \mid \mathfrak{p})$ cuya imagen por la aplicación $\psi_{\mathfrak{P}}|_{\mathfrak{p}}$ es el automorfismo de Frobenius $(x \to x^{N(\mathfrak{p})})$ de $\mathrm{Gal}(\frac{\mathcal{O}_L}{\mathfrak{P}}/\frac{\mathcal{O}_K}{\mathfrak{p}})$. El elemento de Frobenius será denotado indistintamente por el símbolo de Frobenius $\left[\frac{L/K}{\mathfrak{P}}\right]$ o $\sigma_{\mathfrak{P}}$.

Observación 2.17. Estamos llamando $N(\mathfrak{p})$ a la norma absoluta del ideal $\mathfrak{p}$, la cual se define como

$$N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|.$$

En la definición anterior, tiene sentido hablar del elemento de Frobenius puesto que, al estar en el caso de $\mathfrak{p}$ no ramificado en $\mathcal{O}_L$ el grupo de inercia es trivial y por lo tanto $\psi_{\mathfrak{P}}|_{\mathfrak{p}}$ es un isomorfismo. Al ser un isomorfismo, podemos tomar el automorfismo de Frobenius y mirarlo dentro del grupo de descomposición mediante el isomorfismo.

Proposición 2.18. *En el mismo contexto que la anterior definición, el elemento de Frobenius es el único elemento del grupo de Galois $\sigma \in G$ que cumple la siguiente congruencia:*

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{P}} \quad \forall \alpha \in \mathcal{O}_L.$$

Demostración. Como $\psi_{\mathfrak{P}}|_{\mathfrak{p}}\left(\left[\frac{L/K}{\mathfrak{P}}\right]\right)$ es el automorfismo de Frobenius, esta claro que cumple la congruencia.

Supongamos que $\sigma \in G$ también la cumple y veamos que entonces $\sigma = \left[\frac{L/K}{\mathfrak{P}}\right]$. Sea $\alpha \in \mathfrak{P}$, entonces

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \equiv 0 \pmod{\mathfrak{P}}.$$

Por lo anterior sabemos entonces que $\sigma(\mathfrak{P}) \subseteq \mathfrak{P}$. Por la proposición 2.12 sabemos que $\sigma(\mathfrak{P})$ es un ideal primo de $\mathcal{O}_L$, por lo que $\sigma(\mathfrak{P}) = \mathfrak{P}$. Como σ satisface la congruencia del enunciado de la proposición, tenemos que

$$\psi_{\mathfrak{P}}|_{\mathfrak{p}}(\sigma)(x) = x^{N(\mathfrak{p})} \quad \forall x \in \frac{\mathcal{O}_L}{\mathfrak{P}}.$$

Con lo cual $\psi_{\mathfrak{P}}|_{\mathfrak{p}}(\sigma)$ es el automorfismo de Frobenius de $\mathrm{Gal}(\frac{\mathcal{O}_L}{\mathfrak{P}}/\frac{\mathcal{O}_K}{\mathfrak{p}})$, pero como $\psi_{\mathfrak{P}}|_{\mathfrak{p}}$ es inyectiva y $\psi_{\mathfrak{P}}|_{\mathfrak{p}}(\left[\frac{L/K}{\mathfrak{P}}\right])$ es también el automorfismo de Frobenius, entonces $\sigma = \left[\frac{L/K}{\mathfrak{P}}\right]$. □

Proposición 2.19. *En el mismo contexto que antes, para cada $\sigma \in G$ tenemos:*

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

Demostración. Sea $\sigma \in G$ y sea $\alpha \in \mathcal{O}_L$. Por la proposición 2.12 sabemos que $\sigma^{-1}(\alpha) \in \mathcal{O}_L$, entonces:

$$\left[\frac{L/K}{\mathfrak{P}}\right](\sigma^{-1}(\alpha)) \equiv (\sigma^{-1}(\alpha))^{N(\mathfrak{p})} \pmod{\mathfrak{P}} \iff \left[\frac{L/K}{\mathfrak{P}}\right](\sigma^{-1}(\alpha)) - (\sigma^{-1}(\alpha))^{N(\mathfrak{p})} \in \mathfrak{P}$$

Aplicando ahora el isomorfismo σ llegamos a lo siguiente:

$$\begin{aligned}\sigma\left(\left[\frac{L/K}{\mathfrak{P}}\right](\sigma^{-1}(\alpha)) - (\sigma^{-1}(\alpha))^{N(\mathfrak{p})}\right) &= \sigma\left(\left[\frac{L/K}{\mathfrak{P}}\right](\sigma^{-1}(\alpha))\right) - (\sigma(\sigma^{-1}(\alpha)))^{N(\mathfrak{p})} = \\ &= \left(\sigma\left[\frac{L/K}{\mathfrak{P}}\right]\sigma^{-1}\right)(\alpha) - \alpha^{N(\mathfrak{p})}.\end{aligned}$$

Con lo que llegamos a que

$$\left(\sigma\left[\frac{L/K}{\mathfrak{P}}\right]\sigma^{-1}\right)(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\sigma(\mathfrak{P})}.$$

Como esto se tiene para todo elemento α de $\mathcal{O}_L$ y teniendo en cuenta la unicidad de la proposición 2.18 se tiene el resultado. □

Definición 2.20. Sea L/K una extensión de cuerpos de números de Galois, y sea $\mathfrak{p}$ un ideal primo de $\mathcal{O}_K$ que es no ramificado en $\mathcal{O}_L$. Sea P el conjunto de todos los ideales primos de $\mathcal{O}_L$ que contienen a $\mathfrak{p}$. El conjunto formado por los elementos de Frobenius de todos los primos de P se llama *clase de Frobenius* y se identifica con el símbolo de Artin:

$$\left(\frac{L/K}{\mathfrak{p}}\right) = \left\{\left[\frac{L/K}{\mathfrak{P}}\right] : \mathfrak{P} \in P\right\}.$$

Ejemplo 2.21. Consideremos la extensión de cuerpos de números $\mathbb{Q}(\sqrt{-2})/\mathbb{Q}$. Sea $B = \mathcal{O}_{\mathbb{Q}(\sqrt{-2})} = \mathbb{Z}[\sqrt{-2}]$ el anillo de enteros de $\mathbb{Q}(\sqrt{-2})$. El grupo de Galois de esta extensión es S_2. Tomemos el ideal primo (3) de $\mathbb{Z}$. Sabemos que 3 descompone en B (ya que $3 = (1+\sqrt{-2})\cdot(1-\sqrt{-2})$). Por la proposición 2.12 sabemos que existe $\sigma \in G$ tal que $\sigma((1+\sqrt{-2})) = (1-\sqrt{-2})$, por lo que σ será el elemento distinto de la identidad de G.

Ahora bien, el Frobenius de q_1 es un elemento de el grupo de descomposición $D((1+\sqrt{-2})|(3))$, y este grupo esta formado solo por la identidad, entonces:

$$\left[\frac{\mathbb{Q}(\sqrt{-2})/\mathbb{Q}}{(1+\sqrt{-2})}\right] = \left[\frac{\mathbb{Q}(\sqrt{-2})/\mathbb{Q}}{(1-\sqrt{-2})}\right] = \mathrm{Id},$$

y por tanto

$$\left(\frac{\mathbb{Q}(\sqrt{-2})/\mathbb{Q}}{(3)}\right) = \left\{\left[\frac{\mathbb{Q}(\sqrt{-2})/\mathbb{Q}}{(1+\sqrt{-2})}\right]\right\} = \{\mathrm{Id}\}.$$

Antes de introducir alguna proposición importante, vamos a definir lo que es una clase de conjugación de un grupo.

Definición 2.22. Sea G un grupo, y sean $\sigma_1, \sigma_2 \in G$. Decimos que σ_1 y σ_2 estan en la misma *clase de conjugación* si existe $\tau \in G$ de manera que $\tau \cdot \sigma_1 \cdot \tau^{-1} = \sigma_2$.

Proposición 2.23. *En el mismo contexto que la definición 2.20, para cada $\mathfrak{P} \in P$ la clase de Frobenius $\left(\frac{L/K}{\mathfrak{p}}\right)$ es la clase de conjugación de $\left[\frac{L/K}{\mathfrak{P}}\right]$ en G.*

Demostración. La demostración de esto se sigue inmediatamente de la definición de clase de Frobenius y de la proposición 2.19. □

Un resultado elemental sobre el grupo simétrico es que dos elementos son conjugados si, y solamente si, tienen el mismo patrón en su descomposición en ciclos disjuntos. Por ejemplo, en S_9 tenemos que

$$\sigma_1 = (1,2,3,4)(5,6,7)(8,9) \quad \text{y} \quad \sigma_2 = (1,5,9,8)(2,7,6)(3,4)$$

son conjugados. Del mismo modo, podemos decir que dos subgrupos son conjugados si se cumple la propiedad análoga.

Definición 2.24. Sea G un grupo, y sean H_1 y H_2 dos subgrupos de G. Decimos que H_1 y H_2 son dos *subgrupos conjugados* si para cualquier $\sigma_1 \in H_1$ y $\sigma_2 \in H_2$ existe $\tau \in G$ de manera que $\tau \cdot \sigma_1 \cdot \tau^{-1} = \sigma_2$.

Por ejemplo, en S_4, el subgrupo H_1 de orden 4 generado por el ciclo $(1,2,3,4)$ es conjugado al subgrupo H_2 generado por el ciclo $(1,3,2,4)$.

Capítulo 3

Funciones de densidad y el teorema de la progresión aritmética

El objetivo de este capítulo es presentar el teorema de Dirichlet sobre primos en progresiones aritméticas, que es un caso particular del teorema de densidad de Chebotarev cuando se considera la extensión ciclotómica. Para ello vamos a introducir los caracteres de Dirichlet y sus funciones L, cuyas propiedades serán importantes para demostrar el teorema, e introduciremos el concepto de densidad del que ya hemos hablado brevemente en el primer capítulo. Las principales referencias para el estudio de las funciones L y los aspectos analíticos de la teoría de números han sido [1] and [11]. Para la demostración del teorema de la progresión aritmética, otra referencia que se ha usado es [12, Cap. 8].

3.1. Caracteres de Dirichlet y funciones L

Durante todo este capítulo vamos a tomar $n \in \mathbb{N}$ un número natural cualquiera y denotar por $(\mathbb{Z}/n\mathbb{Z})^\times$ y $\mathbb{C}^\times$ a los grupos multiplicativos formados por las unidades de $\mathbb{Z}/n\mathbb{Z}$ y $\mathbb{C}$ respectivamente.

Definición 3.1. Un *carácter de Dirichlet* de $(\mathbb{Z}/n\mathbb{Z})^\times$ es un homomorfismo de grupos de la forma

$$\chi : (\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times.$$

El carácter de Dirichlet va a ser importante a la hora de demostrar el teorema de las progresiones aritméticas que veremos mas adelante.

Proposición 3.2. *Sea χ un carácter de Dirichlet no trivial ($\chi \neq 1$) de $G = (\mathbb{Z}/n\mathbb{Z})^\times$, entonces*

se cumple que

$$\sum_{x \in G} \chi(x) = 0.$$

Demostración. Tomemos $y \in (\mathbb{Z}/n\mathbb{Z})^\times$ un elemento del grupo multiplicativo tal que $\chi(y) \neq 1$, que sabemos que existe por la hipotesis de que χ es un carácter de Dirichlet no trivial. Se tiene entonces:

$$\chi(y) \cdot \sum_{x \in G} \chi(x) = \sum_{x \in G} \chi(y)\chi(x) = \sum_{x \in G} \chi(xy) = \sum_{x \in G} \chi(x).$$

Por tanto, llegamos a lo siguiente:

$$(\chi(y) - 1) \cdot \sum_{x \in G} \chi(x) = 0.$$

Como $\chi(y) \neq 1$, entonces tenemos la igualdad buscada. □

Corolario 3.3. *Dado $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ un elemento distinto del neutro y denotemos por H_n el conjunto de los caracteres de Dirichlet de $(\mathbb{Z}/n\mathbb{Z})^\times$. Se tiene que*

$$\sum_{\chi \in H_n} \chi(x) = 0.$$

Ejemplo 3.4. Tomemos $(\mathbb{Z}/5\mathbb{Z})^\times$ y tomemos el siguiente carácter de Dirichlet:

$$\chi : (\mathbb{Z}/5\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times; \quad 1 \mapsto 1; \quad 2 \mapsto i; \quad 3 \mapsto -i; \quad 4 \mapsto -1.$$

Se tiene:

$$\chi(1) + \chi(2) + \chi(3) + \chi(4) = 1 + i - i - 1 = 0$$

y vemos que, como χ es un carácter de Dirichlet no trivial, se cumple el teorema. Para ver el corolario, tomemos $2 \in (\mathbb{Z}/5\mathbb{Z})^\times$. Para ver cómo son los caracteres de Dirichlet de $(\mathbb{Z}/5\mathbb{Z})^\times$ tenemos que tener en cuenta las siguientes cosas:

- el $1 \in (\mathbb{Z}/5\mathbb{Z})^\times$ siempre debe ir al $1 \in \mathbb{C}^\times$;
- los elementos de $(\mathbb{Z}/5\mathbb{Z})^\times$ deben ir al grupo multiplicativo formado por las raices cuartas de la unidad;
- como el 2 es una raiz primitiva módulo n, la imagen del 2 determinará la imagen del resto de elementos.

Como las raices cuartas de la unidad son $\{1, i, -1, -i\} \subset \mathbb{C}^\times$, los distintos caracteres de Dirichlet serían:

$$\begin{array}{llll} \chi_1(1) = 1; & \chi_1(2) = 1; & \chi_1(3) = 1; & \chi_1(4) = 1. \\ \chi_2(1) = 1; & \chi_2(2) = -1; & \chi_2(3) = -1; & \chi_2(4) = 1. \\ \chi_3(1) = 1; & \chi_3(2) = i; & \chi_3(3) = -i; & \chi_3(4) = -1. \\ \chi_4(1) = 1; & \chi_4(2) = -i; & \chi_4(3) = i; & \chi_4(4) = -1. \end{array}$$

Por tanto, viendo esto tenemos que se cumple el corolario, pues:

$$\sum_{\chi \in H_5} \chi(2) = 1 - 1 + i - i = 0$$

donde H_5 es el conjunto formado por los caracteres de Dirichlet de $(\mathbb{Z}/n\mathbb{Z})^\times$.

Observación 3.5. Cualquier carácter de Dirichlet χ de $(\mathbb{Z}/n\mathbb{Z})^\times$ se puede extender a una aplicación $\chi : \mathbb{Z} \longrightarrow \mathbb{C}$ definiendo $\chi(x) = 0$ si $(x, m) > 1$ y $\chi(n) = \chi(\overline{n})$ siendo $\overline{n}$ la clase de n en $(\mathbb{Z}/n\mathbb{Z})^\times$. Esta aplicación es multiplicativa ($\chi(nm) = \chi(n)\chi(m)$ si $(n, m) = 1$) y acotada. Notar que χ es una función multiplicativa en el sentido estricto, es decir, $\chi(mn) = \chi(m)\chi(n)\ \ \forall m, n \in \mathbb{Z}$.

A partir de ahora cuando nos refiramos a un carácter de Dirichlet módulo m trabajaremos con esta extensión.

Para continuar, debemos recordar la función zeta de Riemann, que se definía de la siguiente manera:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in P} \frac{1}{1 - \frac{1}{p^s}},$$

donde P es el conjunto de todos los primos (la expresión tiene sentido para $Re(s) > 1$).

Ahora, podemos definir lo que son las funciones L. Por comodidad en la notación, a un carácter de Dirichlet de $(\mathbb{Z}/m\mathbb{Z})^\times$ lo llamaremos carácter de Dirichlet módulo m.

Definición 3.6. Sea $m \geq 1$ y sea χ un carácter de Dirichlet módulo m, se define su *función L* como

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$

donde estamos usando la extensión a $\mathbb{Z}$ del carácter de Dirichlet módulo m.

De la definición podemos notar que los únicos enteros n que contribuyen en la suma son los enteros coprimos con m.

3.2. Propiedades analíticas de las series L

En esta sección introduciremos algunas propiedades de las funciones zeta y L necesarias para luego la demostracion del teorema de la progresión aritmética.

Proposición 3.7. *La función zeta de Riemann es holomorfa distinta de cero en el semiplano* $Re(s) > 1$. *Además, se tiene que*

$$\zeta(s) = \frac{1}{s-1} + \phi(s)$$

donde $\phi(s)$ *es una función holomorfa para* $Re(s) > 1$.

Demostración. Vamos a ver una idea de la demostración. La demostración completa la podemos ver en [11, Cap. VI, §3] el Serre (capítulo VI apartado 3). Básicamente hay que ver que

$$\frac{1}{s-1} = \int_1^\infty t^{-s}dt = \sum_{n=1}^{\infty} \int_n^{n+1} t^{-s}dt.$$

Con esto podemos poner lo siguiente

$$\zeta(s) = \frac{1}{s-1} + \sum_{n=1}^{\infty} \left(\frac{1}{n^s} - \int_n^{n+1} t^{-s}dt \right)$$

donde tenemos que la función zeta es de la forma dada por la proposición. Únicamente habría que demostrar que $\phi(s)$ esta definida y es holomorfa en el semiplano $Re(s) > 1$. □

A modo de notación, si $f(s)$ y $g(s)$ son dos funciones de variable compleja definidas para $Re(s) > 1$, pondremos que $f(s) \sim g(s)$ cuando $s \to 1$ si

$$\lim_{s \to 1} \frac{f(s)}{g(s)} = 1,$$

entendiendo que el límite se considera únicamente en el semiplano dado por $Re(s) > 1$.

Proposición 3.8. *Se tiene que* $\sum_{p \in P} p^{-s} \sim \log \frac{1}{s-1}$ *(donde* P *es el conjunto de todos los primos) y* $\sum_{p,k \geq 2} \frac{1}{p^{ks}}$ *se mantiene acotado.*

Demostración. La demostración la podemos ver en [11, Cap. VI, §3] el Serre (capítulo VI apartado 3). Es sencilla tomando el logaritmo de la función zeta:

$$\log(\zeta(s)) = \log \prod_{p \in P} \frac{1}{1 - \frac{1}{p^s}} = \sum_{p \in P} \log \frac{1}{1 - \frac{1}{p^s}} = \sum_{p \in P} -\log(1 - p^{-s}) = \sum_{p \in P} \sum_{k=1}^{\infty} \frac{1}{k p^{sk}},$$

donde la última igualdad se sigue de la serie de potencias:

$$-\log(1-p) = \sum_{i=1}^{\infty} \frac{p^k}{k}.$$

Ahora, continuando con la expresión anterior, nos queda que

$$\sum_{p\in P}\sum_{k=1}^{\infty}\frac{1}{kp^{sk}} = \sum_{p\in P}\frac{1}{p^s} + \sum_{p\in P}\sum_{k\geq 2}\frac{1}{kp^{sk}}.$$

La serie de la segunda igualdad está mayorada, como podemos comprobar, de la siguiente forma:

$$\sum_{p\in P,\ k\geq 2}\frac{1}{kp^{ks}} \leq \sum_{p\in P,\ k\geq 2}\frac{1}{p^{ks}} = \sum_{p\in P}\frac{1}{p^s(p^s-1)} \leq \sum_{p\in P}\frac{1}{p(p-1)} \leq \sum_{n=2}^{\infty}\frac{1}{n(n-1)} = 1.$$

Por tanto esa serie está acotada, y como por la proposición 3.7 sabemos que $\log(\zeta(s)) \sim \log(\frac{1}{s-1})$, demostrando así el corolario. □

Vamos ahora a enunciar el principal resultado sobre convergencia de funciones L, y que desempeña un papel crucial en la demostración del teorema de Dirichlet de las progresiones aritméticas.

Proposición 3.9. *Sea χ un carácter de Dirichlet no trivial, se tiene entonces que $L(s,\chi)$ converge absolutamente para $Re(s) > 1$. Además,*

$$L(s,\chi) = \prod_{p\in P}\frac{1}{1-\frac{\chi(p)}{p^s}} \text{ para } Re(s) > 1.$$

Demostración. Es fácil de ver que converge absolutamente para $Re(s) > 1$. Dado χ un carácter de Dirichlet no trivial, se definía $L(s,\chi)$ como

$$L(s,\chi) = \sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}.$$

Como χ está acotado, por la convergencia absoluta de la serie $\sum_{n=1}^{\infty} 1/n^{\alpha}$ con $\alpha > 1$, tenemos que $L(s,\chi)$ converge absolutamente para $Re(s) > 1$.

Para ver que la función L es igual a ese producto, hay que hacer el mismo razonamiento que para demostrar que la función ζ se puede poner como un producto sobre todos los primos. El razonamiento es el siguiente:

Recordemos que todo entero positivo se puede expresar de forma única como producto de primos elevados cada uno a un cierto exponente. Con esto en mente, dado p un primo, vamos a considerar la siguiente serie geométrica que converge para $Re(s) > 1$:

$$\sum_{n=0}^{\infty}\frac{\chi(p^n)}{p^{ns}} = \sum_{n=0}^{\infty}\frac{\chi(p)^n}{p^{ns}} = \sum_{n=0}^{\infty}\left(\frac{\chi(p)}{p^s}\right)^n = \frac{1}{1-\frac{\chi(p)}{p^s}},$$

donde en la primera igualdad hemos usado que χ es una función multiplicativa en el sentido estricto ($\chi(nm) = \chi(n)\chi(m) \ \ \forall n, m \in \mathbb{Z}$).

Ahora, tomando el producto sobre todos los primos de esta suma sobre se da que

$$\prod_{p \in P} \left(\sum_{n=0}^{\infty} \frac{\chi(p^n)}{p^{ns}} \right) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = L(s, \chi),$$

y se obtiene el resultado.

□

Observación 3.10. Al igual que la función zeta de Riemann, se puede extender analíticamente la función $L(\chi, s)$ a todo el plano complejo.

Teorema 3.11. *Para todo $\chi \neq 1$ se tiene que $L(1, \chi) \neq 0$.*

3.3. El teorema de la progresión aritmética

Antes de ver el teorema de la progresión aritmética, debemos introducir el concepto de densidad de Dirichlet.

Definición 3.12. Sea $A \subseteq P$, decimos que A tiene *densidad de Dirichlet* k en el conjunto de los primos P si

$$\lim_{s \to 1} \frac{\sum_{p \in A} \frac{1}{p^s}}{\log\left(\frac{1}{s-1}\right)} = k$$

Antes de formular el teorema importante, debemos enunciar unos lemas previos que luego usaremos en la demostración de dicho teorema.

Sea χ un carácter de Dirichlet de $(\mathbb{Z}/n\mathbb{Z})^{\times}$. Llamaremos f_χ a la función compleja definida como

$$f_\chi(s) = \sum_{p \nmid m} \frac{\chi(p)}{p^s},$$

y esta serie es convergente para $s > 1$.

Lema 3.13. *Si $\chi = 1$ entonces $f_\chi \sim log\left(\frac{1}{1-s}\right)$ cuando $s \to 1$*

Demostración. La demostración de este lema es inmediata al razonar que f_1 se diferencia de la serie $\sum_{p \in P} \frac{1}{p^s}$ en un numero finito de elementos, y viendo la proposición 3.8. □

Lema 3.14. *Si $\chi \neq 1$, entonces f_χ esta acotado cuando $s \to 1$*

Ahora si, vamos a definir el teorema de la progresión aritmética:

Teorema 3.15 (**Teorema de la progresion aritmética**). *Sea $m \geq 1$ un entero, y sea a otro entero tal que $(m, a) = 1$. Sea también P_a el conjunto formado por los numeros primos p que cumplen que $p \equiv a \mod m$. Entonces el conjunto P_a tiene densidad $\frac{1}{\varphi(m)}$*

Demostración. Para la demostración del teorema, vamos a tener que estudiar el comportamiento de la función compleja

$$g_a(s) = \sum_{p \in P_a} \frac{1}{p^s}$$

cuando $s \to 1$. Veamos que

$$g_a(s) = \frac{1}{\phi(m)} \sum_{\chi} \chi(a)^{-1} f_\chi(s),$$

donde esa suma es la suma sobre todos los caracteres de Dirichlet de $\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^\times$ Usando la definición de $f_\chi(s)$, se tiene que

$$\sum_{\chi} \chi(a)^{-1} f_\chi(s) = \sum_{p \nmid m} \frac{\sum_\chi \chi(a^{-1})\chi(p)}{p^s}.$$

Además $\chi(a^{-1})\chi(p) = \chi(a^{-1}p)$. Usando el corolario 3.3 tenemos que:

$$\sum_{\chi} \chi(a^{-1}p) = \phi(m) \text{ si } a^{-1}p \equiv 1 \mod m,$$
$$\sum_{\chi} \chi(a^{-1}p) = 0 \text{ en otro caso.}$$

y por tanto

$$\sum_{\chi} \chi(a)^{-1} f_\chi(s) = \sum_{p \in P_a} \frac{\phi(m)}{p^s} = \phi(m) g_a(s).$$

Por el lema 3.13 sabemos que $f_\chi(s) \sim \log \frac{1}{s-1}$ para $\chi = 1$ y por el lema 3.14 sabemos que el resto de f_χ se mantienen acotadas. Como antes hemos demostrado que $g_a(s) = \frac{1}{\phi(m)} \sum_\chi \chi(a)^{-1} f_\chi(s)$, entonces $g_a(s) \sim \frac{1}{\phi(m)} log \frac{1}{s-1}$ y esto implica que la densidad de P_a es $\frac{1}{\phi(m)}$. □

Capítulo 4

El teorema de densidad de Chebotarev: enunciado y ejemplos

Todos los resultados hasta ahora han sido vistos con el objetivo de poder enunciar y demostrar el teorema de Chebotarev. En este capítulo vamos a enunciar el teorema principal del trabajo, así como ver su aplicación a casos particulares como el caso cuadrático y el caso ciclotómico; y por último veremos la relación entre el teorema y la factorización de los polinomios módulo p que vimos en el primer capítulo que vimos de manera computacional. Las referencias principales que seguimos son [3] y [4], aunque para una visión ligeramente distinta puede consultarse también [5, Cap. 7].

4.1. Enunciado del teorema

Veamos pues el enunciado del **teorema de densidad de Chebotarev**:

Teorema 4.1 (**Teorema de densidad de Chebotarev**)**.** *Sea L/K una extension de cuerpos de números, con grupo de Galois $G = \mathrm{Gal}(L/K)$. Sea C una clase de conjugación de G y sea P el conjunto de los ideales primos no nulos $\mathfrak{p} \subset \mathcal{O}_K$ que son no ramificados en $\mathcal{O}_L$ que cumplen que $\left(\frac{L/K}{\mathfrak{p}}\right) \in C$. Entonces la densidad de Dirichlet $\delta(P)$ de P existe y cumple que $\delta(P) = \frac{|C|}{|G|}$.*

Observación 4.2. Como hemos comentado en los primeros capítulos, si $G = S_n$, dos elementos están en la misma clase de conjugación si y solamente si tienen la misma descomposición en ciclos.

En el caso de que el grupo de Galois sea abeliano, cada clase de conjugación consta exactamente de un elemento, por lo que el teorema simplemente dice que la densidad de Dirichlet de

los primos cuyo Frobenius es un elemento fijado es $\frac{1}{|G|}$. Es lo que sucede por ejemplo con el caso cuadrático y el caso ciclotómico, que comentaremos con más detalle en la próxima sección.

Vamos a comentar algun corolario del teorema de Chebotarev, si bien las aplicaciones más destacadas son las que ya hemos discutido y sobre las que ahondaremos en las siguientes secciones. Para ello, dados dos conjuntos S y T, ponemos $S \dot{\subset} T$ si $S \subset T \cup \Sigma$, siendo Σ un conjunto finito. Por otro lado, dada una extensión de cuerpos de números $K \subset L$, ponemos $S_{L/K}$ para el conjunto de primos de K que descomponen completamente en L.

Corolario 4.3. *Sean L y M dos extensiones de Galois de K.*

(a) $L \subset M$ si y solamente si $S_{M/K} \dot{\subset} S_{L/K}$.

(b) $L = M$ si y solamente si $S_{M/K} \dot{=} S_{L/K}$.

Demostración. Véase [3, Teo. 8.19]. □

La importancia del teorema anterior radica en que establece que dar los primos que descomponen en una extensión (es decir, aquellos para los cuales el elemento de Frobenius es la identidad) la determina completamente. Por ejemplo, en una extensión cuadrática *la mitad* de los primos descomponen totalmente, pero ese conjunto nunca va a coincidir para dos extensiones diferentes.

4.2. El caso cuadrático y el caso ciclotómico

En esta sección, vamos a explicar cómo en el caso de extensiones cuadráticas y extensiones ciclotómicas se recuperan resultados que ya se han trabajado en capítulos anteriores.

4.2.1. Caso cuadrático

Sea $m \in \mathbb{Z}$ un entero libre de cuadrados, vamos a considerar la extensión de cuerpos de números $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$. Esta es una extensión de Galois y $[\mathbb{Q}(\sqrt{m})/\mathbb{Q}] = 2$ pues

$$\mathrm{Irr}(\sqrt{m}, \mathbb{Q}; x) = x^2 - m,$$

donde $\mathrm{Irr}(\alpha, \mathbb{Q}; x)$ denota, como es habitual, el polinomio irreducible con coeficientes racionales del elemento $\alpha \in K$. Sea G el grupo de Galois de esta extensión, que será el grupo simétrico de dos elementos S_2, y que también se puede identificar con $\mathbb{Z}/2\mathbb{Z}$. Vamos a denotar por B al anillo de enteros de $\mathbb{Q}(\sqrt{m})$ sobre $\mathbb{Z}$.

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{m}) & \text{——} & B \\ | & & | \\ \mathbb{Q} & \text{————} & \mathbb{Z} \end{array}$$

Sea $p \in \mathbb{Z}$ un primo que no ramifica en B. Tenemos dos posibilidades:

- $pB = q_1 \cdot q_2$ con q_1, q_2 ideales primos distintos de B, es decir, p descompone.
- $pB = p$, es decir, p es inerte (el ideal de B generado por p es un ideal primo de B).

Como $G = S_2$ es un grupo abeliano, las clases de conjugación de G constan de un único elemento. En este caso, G tiene dos elementos y cada uno forma una clase de conjugación diferente.

Sea $\left(\frac{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}{p}\right)$ el elemento de Frobenius de p. Tenemos dos posibilidades, dependiendo de si p es inerte o se descompone en B:

1. Si p se descompone en B, es decir, $pB = q_1 \cdot q_2$, entonces $\left(\frac{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}{p}\right) = \{\mathrm{Id}\}$. Esto se puede explicar de la siguiente manera: sabemos que la acción de G es transitiva sobre el conjunto de ideales primos de B que contienen a p por la proposición 2.12 de la sección 2. Sabemos también que G tiene dos elementos y uno de ellos es la identidad, por tanto, si $\sigma \in G$ es el elemento de G distinto de la identidad, se cumple que $\sigma(q_1) = q_2$. Por consiguiente, el grupo de descomposición de q_1 está formado por la identidad. Por la definición 2.16, el Frobenius de q_1 tiene que estar en el grupo de descomposición, por lo que tiene que ser la identidad.

2. Si p es inerte en B entonces el grupo de descomposición tiene cardinal dos, y recordando las identificaciones en torno a la definición 2.16 de elemento de Frobenius, tenemos que $\mathrm{Gal}(\frac{B}{pB}/\frac{\mathbb{Z}}{p\mathbb{Z}})$ es un grupo de dos elementos. Ahora, teniendo en cuenta que el automorfismo de Frobenius es un generador del grupo de Galois de cualquier extensión de cuerpos finitos, entonces el automorfismo de Frobenius de $\mathrm{Gal}(\frac{B}{pB}/\frac{\mathbb{Z}}{p\mathbb{Z}})$ es el elemento no trivial del grupo, por lo que la preimagen del automorfismo de Frobenius en el grupo de descomposición es el elemento no trivial de G, es decir, $\left(\frac{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}{p}\right) = \{(1,2)\}$.

Sea P_1 el conjunto de todos los primos de $\mathbb{Z}$ no ramificados que descomponen en B, es decir, aquellos primos p para los que $\left(\frac{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}{p}\right) = \{\mathrm{Id}\}$. Por tanto, usando el teorema de densidad de Chebotarev, tenemos que

$$\delta(P_1) = \frac{|\{\mathrm{Id}\}|}{|G|} = \frac{1}{2}.$$

Haciendo el mismo razonamiento para P_2 el conjunto de los primos que no ramifican y son inertes en B, llegamos a que $\delta(P_2) = 1/2$.

Por tanto, como la cantidad de primos de $\mathbb{Z}$ que ramifican en B son finitos, tenemos que $1/2$ de los primos de $\mathbb{Z}$ se descomponen en B y $1/2$ son inertes.

Ejemplo 4.4. Tomemos $m = -1$. Sea entonces $\mathbb{Q}(i)/\mathbb{Q}$ y $B = \mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$ la clausura íntegra de $\mathbb{Z}$ en $\mathbb{Q}(i)$. Sea también $G = \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$. En este caso, el primo 2 es el único que ramifica en $\mathbb{Q}(i)$ pues $2 = (1 + \sqrt{-1}) \cdot (1 - \sqrt{-1}) = (1 - \sqrt{-1})^2 \cdot \sqrt{-1}$ siendo $\sqrt{-1}$ es una unidad en B. Por lo tanto, tenemos que los primos que descomponen totalmente, es decir, los primos cuya clase de Frobenius es la identidad, son los de la forma $4k + 1$. Veamos porqué esto es así

Como la extensión es de grado 2 y $[\mathbb{Q}(i) : \mathbb{Q}] = efg$, entonces tenemos que el grado residual $f = 1$, en otras palabras, $\mathbb{Z}[i]/q_1$ tiene el mismo orden que $\mathbb{Z}/p\mathbb{Z}$. Esto implica que la característica del cuerpo $\mathbb{Z}[i]/q_1$ es p. Por otra parte, el Frobenius de q_1 es la identidad, por lo que, dado $\alpha \in \mathbb{Z}[i]$ se cumple lo siguiente:

$$(\alpha + q_1)^p = \alpha + q_1 \iff (a + bi + q_1)^p \equiv a^p + b^p i^p + q_1^p \equiv a + bi \pmod{q_1},$$

siendo a, b enteros. Como $a^p \equiv a \pmod{q_1}$ y $b^p \equiv b \pmod{q_1}$, entonces la cadena de congruencias es cierta si $i^p \equiv i \pmod{q_1}$, con lo cual $p = 4k + 1$. La densidad de estos primos, aplicando el teorema de Chebotarev, es de $1/2$.

De igual modo, los primos inertes son los primos de la forma $4k + 3$ y tienen densidad $1/2$ sobre el conjunto de todos los primos.

4.2.2. Caso ciclotómico

Consideremos ahora $n \in \mathbb{N}$ y sea ζ_n una raíz primitiva n-ésima de la unidad. Vamos a analizar en este apartado cómo se aplica el teorema de densidad de Chebotarev a extensiones ciclotómicas de la forma $\mathbb{Q}(\zeta_n)/\mathbb{Q}$.

$$\begin{array}{ccc} \mathbb{Q}(\zeta_n) & \text{——} & B \\ | & & | \\ \mathbb{Q} & \text{———} & \mathbb{Z} \end{array}$$

Primero, notar que estamos en el contexto de una extensión de Galois y que $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$. Por tanto,

$$|\,\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = \varphi(n).$$

Además, $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ es un grupo conmutativo, por lo que sus clases de conjugación están bien definidas pues cada elemento de G forma una clase de conjugación distinta.

Sea p un primo de $\mathbb{Z}$ coprimo con n. El Frobenius de p se va a corresponder con la aplicación $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ tal que $\sigma(\zeta_n) = (\zeta_n)^a$ con $a \equiv p \pmod{n}$.

Por tanto, usando el teorema de densidad de Chebotarev para P el conjunto de los números primos no ramificados tales que son congruentes con a módulo p (notar que $(a, n) = 1$) tenemos que:

$$\delta(P) = \frac{1}{\varphi(n)}.$$

Ejemplo 4.5. Tomemos $n = 5$. Sea ζ_5 una raíz primitiva quinta de la unidad, vamos a considerar la extensión $\mathbb{Q}(\zeta_5)/\mathbb{Q}$. El grupo de Galois está formado por $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ donde $\sigma_i(\zeta_5) = (\zeta_5)^i \ \ \forall i \in \{0, 1, 2, 3, 4\}$.

Como ya dijimos, cada elemento forma una clase de conjugación. Sea P el conjunto de los primos de $\mathbb{Z}$ que son congruentes con k módulo 5. Para cada $p \in P$, el Frobenius de p será:

$$\left(\frac{\mathbb{Q}(\zeta_5)/\mathbb{Q}}{p}\right) = \sigma_k,$$

Por el teorema de densidad de Chebotarev, la densidad de P es $1/5$. Como este razonamiento es igual para cualquier $k \in \{1, 2, 3, 4\}$, entonces tenemos que la proporción de primos congruentes con k módulo 5 es $1/5$ para todo k.

4.3. Factorización de polinomios módulo p

Por último, explicamos la relación entre el teorema de Chebotarev y la factorización de polinomios módulo p estudiada computacionalmente en el primer capítulo. Para ello, comenzamos enunciado una propiedad del elemento de Frobenius que será se utilidad.

Vamos a empezar con una cuestión relativa a los elementos de Frobenius cuando consideramos una torre de extensiones de la forma $L/E/K$. En ese caso, podemos considerar el Frobenius relativo a la extensión L/K y relacionarlo con los Frobenius de las dos subextensiones. Vamos a utilizar aquí la notación $\sigma_{\mathfrak{p}}$ para denotar el Frobenius, dado que en estos casos la extensión a la que nos referimos estará clara por el contexto.

Proposición 4.6. *Sean $K \subseteq E \subseteq L$ extensiones finitas de cuerpos de números, con E/K y L/E extensiones de Galois. Sea $\mathfrak{P}$ un ideal primo de $\mathcal{O}_L$ que no es ramificado en L/K, y sean $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_E$ y $\mathfrak{p}_K = \mathfrak{P} \cap \mathcal{O}_K$. Entonces, el elemento de Frobenius*

$$\sigma_{\mathfrak{P}} \in \mathrm{Gal}(L/K)$$

proyecta sobre el elemento de Frobenius

$$\sigma_{\mathfrak{p}} \in \mathrm{Gal}(E/K)$$

bajo el morfismo natural de grupos de Galois inducido por la inclusión $E \subseteq L$:

$$\mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(E/K).$$

Demostración. Como L/K es una extensión de Galois, toda la torre $K \subseteq E \subseteq L$ está dentro de un contexto en el que los grupos de Galois están bien definidos y las proyecciones son naturales. En particular, el grupo $\mathrm{Gal}(L/K)$ actúa sobre L, y la restricción de automorfismos a E define un homomorfismo de grupos:

$$\mathrm{res} : \mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K), \quad \sigma \mapsto \sigma|_E.$$

Como $\mathfrak{P}$ no está ramificado en L/K, el automorfismo de Frobenius $\sigma_{\mathfrak{P}}$ está bien definido como el generador del grupo de descomposición. Recordemos que, a nivel de cuerpos finitos, la acción de $\sigma_{\mathfrak{P}}$ sobre un elemento x está dada por:

$$\sigma_{\mathfrak{P}}(x) \equiv x^{N(\mathfrak{p})} \mod \mathfrak{P},$$

donde $N(\mathfrak{p})$ es el número de elementos del cuerpo residual.

La proyección $\mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K)$ lleva $\sigma_{\mathfrak{P}}$ a un automorfismo $\tau \in \mathrm{Gal}(E/K)$ que, al actuar sobre el cuerpo residual, induce:

$$\tau(x) \equiv x^{N(\mathfrak{p})} \mod \mathfrak{p}.$$

Pero esto es precisamente la definición del automorfismo de Frobenius $\sigma_{\mathfrak{p}} \in \mathrm{Gal}(E/K)$. Por tanto:

$$\mathrm{res}(\sigma_{\mathfrak{P}}) = \sigma_{\mathfrak{p}}.$$

Esto concluye la demostración. □

Vamos a considerar ahora la situación en la que L/K es una extensión de Galois, pero E/K no lo es necesariamente. La situación típica en la que hemos de pensar es aquella en la que $K = \mathbb{Q}$, $E = \mathbb{Q}(\alpha)$, siendo α la raíz de un polinomio irreducible en $\mathbb{Q}[X]$, y L el cuerpo de escisión del polinomio $f(X)$. Si $\mathfrak{p}$ es un primo de K que no ramifica en E, podemos poner $\mathfrak{p}\mathcal{O}_E = \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}$. Como el primo no ramifica, el patrón de descomposición de $\mathfrak{p}$ queda bien definido a partir de la sucesión de índices de inercia $f(\mathfrak{q}/\mathfrak{p})$. Escribimos $\sigma_{\mathfrak{p}}$ para un elemento de Frobenius en la extensión L/K; esto dependerá de la elección del primo de L que divide a $\mathfrak{p}$.

Proposición 4.7. *Sea L/K una extensión de Galois de cuerpos de números, con grupo de Galois $G = \mathrm{Gal}(L/K)$, y sea $H \subseteq G$ un subgrupo. Sea $E = L^H$ el subcuerpo fijo por H. Sea $\mathfrak{p}$ un primo no ramificado de $\mathcal{O}_K$ y sea $\sigma_{\mathfrak{p}} \in G$ un elemento de Frobenius asociado.*

Entonces, la descomposición del ideal primo $\mathfrak{p}\mathcal{O}_E$ en primos de $\mathcal{O}_E$ coincide con la descomposición en ciclos de la acción de $\sigma_{\mathfrak{p}}$ sobre el conjunto de clases laterales G/H.

Demostración. Sea $\mathfrak{P}$ un ideal primo de $\mathcal{O}_L$ que divide a $\mathfrak{p}$ y sea $\sigma_{\mathfrak{P}} \in G$ el elemento de Frobenius asociado a $\mathfrak{P}$. Dado que L/K es Galois y $\mathfrak{p}$ no ramifica en L, el grupo de descomposición de $\mathfrak{P}$ está generado por $\sigma_{\mathfrak{P}}$, y los primos de L sobre $\mathfrak{p}$ están en correspondencia con la órbita de G sobre $\mathfrak{P}$ ya que la acción de Galois es transitiva.

Ahora consideremos el conjunto G/H, sobre el cual G actúa por traslación izquierda:

$$g \cdot xH = gxH.$$

Esta acción es transitiva, y los puntos fijos de un elemento $\tau \in G$ corresponden a las clases laterales gH tales que $\tau \in gHg^{-1}$. La acción de $\sigma_{\mathfrak{P}}$ en G/H permuta los elementos de G/H en ciclos, y cada ciclo representa un ideal primo de $\mathcal{O}_E$ sobre $\mathfrak{p}$.

La clave para este hecho está en que los ciclos de esta acción describen las *órbitas de la acción de Frobenius*, y cada órbita corresponde a un ideal primo de $\mathcal{O}_E$ sobre $\mathfrak{p}$. La longitud de cada ciclo es el grado de inercia de ese primo, es decir, el grado f del cuerpo residual.

En resumen, los primos de $\mathcal{O}_E$ sobre $\mathfrak{p}$ están en correspondencia con los ciclos de la acción de $\sigma_{\mathfrak{P}}$ en G/H, y el grado de inercia de cada uno es la longitud del correspondiente ciclo. Por tanto, la factorización de $\mathfrak{p}\mathcal{O}_E$ viene dada por:

$$\mathfrak{p}\mathcal{O}_E = \mathfrak{q}_1 \cdots \mathfrak{q}_r, \quad \text{con } \deg \mathfrak{q}_i = \text{longitud del } i\text{-ésimo ciclo.}$$

Esto demuestra la proposición. □

Volvamos ahora a la situación de partida. Sea L/K una extensión de cuerpos de números, con L generado por una raíz α de un polinomio irreducible $f(X) \in \mathcal{O}_K[X]$. Supongamos que f es el polinomio mínimo de α y que $L = K(\alpha)$. Denotamos por $G = \mathrm{Gal}(L/K)$ y por H el subgrupo de G que fija α, de modo que $E = L^H = K(\alpha)$.

Sea $\mathfrak{p}$ un ideal primo de $\mathcal{O}_K$ que no divide el discriminante de f, de modo que f es separable módulo $\mathfrak{p}$ y su reducción $\overline{f}$ en $(\mathcal{O}_K/\mathfrak{p})[X]$ se puede factorizar como producto de polinomios irreducibles distintos:

$$\overline{f}(X) = \prod_{i=1}^{r} \overline{f_i}(X),$$

donde los $\overline{f_i}$ son irreducibles de grado d_i sobre $\mathcal{O}_K/\mathfrak{p}$.

Este patrón de factorización está directamente relacionado con la acción del elemento de Frobenius $\sigma_{\mathfrak{P}} \in \mathrm{Gal}(L/K)$ asociado a un ideal primo $\mathfrak{P}$ de $\mathcal{O}_L$ que divide $\mathfrak{p}$. En efecto, como se ha demostrado anteriormente, el patrón de descomposición de $\mathfrak{p}$ en $\mathcal{O}_E$ coincide con la descomposición en ciclos de $\sigma_{\mathfrak{P}}$ actuando en el conjunto de raíces del polinomio f, es decir, sobre los conjugados de α en L.

Más formalmente, notamos que el conjunto de raíces de f en L es precisamente la órbita de α bajo la acción de G sobre L, es decir,

$$\{\sigma(\alpha) \mid \sigma \in G\} \cong G/H.$$

La acción de $\sigma_{\mathfrak{p}}$ sobre las raíces de f induce una permutación de este conjunto, cuya descomposición en ciclos tiene la siguiente interpretación aritmética:

(-) Cada ciclo de longitud d_i corresponde a un factor irreducible $\overline{f_i}$ de $\overline{f}$ de grado d_i.

(-) Por tanto, el patrón de factorización de f mód $\mathfrak{p}$ viene dado por la descomposición en ciclos de $\sigma_{\mathfrak{P}}$ actuando sobre G/H.

Desde esta perspectiva, el comportamiento de f mód $\mathfrak{p}$ no es otra cosa que la manera en la que el automorfismo de Frobenius reordena las raíces de f en L. Este hecho permite vincular el estudio de la factorización módulo p con la teoría de Galois: el grupo de Galois de f determina todas las posibles factorizaciones que puede adoptar f al reducirlo módulo diferentes primos, y el teorema de Chebotarev garantiza que cada clase de conjugación en $\mathrm{Gal}(L/K)$ (es decir, cada patrón de factorización posible) aparece con una densidad proporcional al tamaño de la clase.

Este resultado justifica desde un punto de vista teórico los cálculos que habíamos realizado al final del primer capítulo. Es decir, el grupo de Galois de un polinomio $f(X)$ determina los posibles patrones de factorización de f módulo p, y viceversa, mediante la observación de dichos patrones (en un número suficientemente grande de primos) es posible recuperar información sobre la estructura del grupo de Galois.

Capítulo 5

El teorema de densidad de Chebotarev: idea de la demostración

En este capítulo vamos a extender las ideas relativas a la demostración del teorema de la progresión aritmética de Dirichlet para abordar el teorema de Chebotarev. En general, dado que se usan muchas herramientas técnicas, nos vamos a limitar a dar una idea general, enfatizando el papel de dos de los ingredientes centrales como son los *modulus* y las funciones L de Weber. Para el estudio de los modulus y, más en general, de la teoría de cuerpos de clase, hemos seguido principalmente [3] y [4], y también la referencia [2], de tipo más bien histórico.

5.1. La noción de modulus

Durante esta sección, vamos a denotar por K a un cuerpo de números y $\mathcal{O}_K$ su anillo de enteros. Para empezar, debemos definir lo que son los ideales fraccionales de K así como algunas de sus propiedades más importantes que nos permitirán definir con propiedad lo que es un modulus posteriormente.

Definición 5.1. Un *ideal fraccional de* K, $\mathfrak{a}$, es un $\mathcal{O}_K$-submódulo de K. Estos ideales son conjuntos de la forma αI donde $\alpha \in K$ e I es un ideal de $\mathcal{O}_K$. Notar que los ideales de $\mathcal{O}_K$ son, en particular, ideales fraccionales de K (basta tomar $\alpha = 1$).

Proposición 5.2. *Sea* $\mathfrak{a}$ *un ideal fraccional de* K*. Entonces:*

- $\mathfrak{a}$ *es invertible, es decir, existe* $\mathfrak{b}$ *ideal fraccional de* K *tal que* $\mathfrak{ab} = \mathcal{O}_K$*, donde el producto de ideales fraccionales se define igual que el producto de ideales en un anillo. El ideal* $\mathfrak{b}$ *se denotará por* $\mathfrak{a}^{-1}$*.*

- $\mathfrak{a}$ *se puede descomponer de forma única como el producto* $\prod_{i=1}^{s} \mathfrak{p}_i^{r_i}$ *donde* $r_i \in \mathbb{Z}$ *y los* $\mathfrak{p}_i$ *son ideales primos distintos de* $\mathcal{O}_K$.

Observación 5.3. Dado $\mathfrak{a}$ ideal fraccional de K, el inverso $\mathfrak{a}^{-1}$ es el siguiente ideal:

$$\mathfrak{a}^{-1} = \{\alpha \in K : \alpha\mathfrak{a} \subset \mathcal{O}_K\}.$$

Vamos a denotar por $\mathcal{I}_K$ al conjunto de los ideales fraccionales de K. $\mathcal{I}_K$ es cerrado con la multiplicación definida en la proposición anterior, y como vimos antes que cada elemento tiene inversa, entonces sabemos que $\mathcal{I}_K$ es un grupo. Además, $\mathcal{I}_K$ es un grupo libre generado por los ideales primos de $\mathcal{O}_K$.

El subgrupo más importante de $\mathcal{I}_K$ es el subgrupo de ideales principales fraccionales $\mathcal{P}_K$, que está formado por los elementos de $\mathcal{I}_K$ de la forma $\alpha\mathcal{O}_K$ con $\alpha \in K^\times$. El subgrupo $\mathcal{P}_K$ es un subgrupo normal de $\mathcal{I}_K$, por lo que el grupo cociente $\mathcal{I}_K/\mathcal{P}_K$ está bien definido. Este grupo cociente es finito, se llama *grupo de clases de ideales* y lo denotaremos por Cl_K.

Coloquialmente, el grupo de clases de ideales de K nos está diciendo cómo de cerca está $\mathcal{O}_K$ de ser un dominio de ideales principales, pues de serlo, Cl_K sería el grupo trivial.

Observación 5.4. Recordemos que un embebimiento es un homomorfismo de anillos inyectivo. El cuerpo de números K tiene exactamente $[K : \mathbb{Q}] = n$ embebimientos en $\mathbb{C}$. Si σ es un embebimiento de K en $\mathbb{C}$, entonces su conjugado complejo $\overline{\sigma}$ también lo es ($\overline{\sigma}(\alpha) = \overline{\sigma(\alpha)}$). Se tiene que $n = r + 2s$ donde r es el número de embebimientos reales de K (embebimientos de K en $\mathbb{C}$ cuya imagen está contenida en los reales) y s el número de embebimientos complejos (embebimientos de K en $\mathbb{C}$ que no son embebimientos reales).

Con esto, podemos definir el concepto de modulus:

Definición 5.5 (*Modulus*)**.** Un *modulus* $\mathfrak{m}$ de K consiste en el producto formal de $\mathfrak{m}_0 \cdot \mathfrak{m}_\infty$ donde $\mathfrak{m}_0$ es un ideal no nulo de $\mathcal{O}_K$ y $\mathfrak{m}_\infty$ es un subconjunto de embebimientos reales de K.

Observación 5.6. Si $\mathfrak{m}_\infty$ es el conjunto de todos los embebimientos reales, entonces se denota por ∞, es decir, $\mathfrak{m} = \mathfrak{m}_0 \cdot \mathfrak{m}_\infty = \mathfrak{m}_0 \cdot \infty$. Estos son los que más nos importan pues son los que se usan en la prueba del teorema de Chebotarev.

Definición 5.7. Sea K un cuerpo de números, y sea $\mathfrak{m}$ un modulus de K. Definimos:

- $\mathcal{I}_K^{\mathfrak{m}}$ es el subgrupo de $\mathcal{I}_K$ generado por los ideales no nulos coprimos con $\mathfrak{m}_0$ (es decir, los ideales de $\mathcal{O}_K$ cuya factorización en primos no comparte factores comunes con los de la factorización en primos de $\mathfrak{m}_0$).
- $\mathcal{O}_K^{\mathfrak{m}} = \{\alpha \in \mathcal{O}_K \setminus \{0\} : \alpha \equiv 1 \pmod{\mathfrak{m}_0} \text{ y } \sigma(\alpha) > 0 \ \ \forall \sigma \in \mathfrak{m}_\infty\} \subseteq K^\times$.

- $K^{\mathfrak{m}}$ es el subgrupo de $K^\times$ generado por el conjunto $\mathcal{O}_K^{\mathfrak{m}}$ (donde $K^\times$ es un grupo con la multiplicación).
- $\mathcal{P}_K^{\mathfrak{m}} = \{\mathfrak{a} \in \mathcal{I}_K^{\mathfrak{m}} : \mathfrak{a} = \alpha\mathcal{O}_K \text{ para algún } \alpha \in K^{\mathfrak{m}}\}$ es el subgrupo normal de $\mathcal{I}_K^{\mathfrak{m}}$ de ideales principales generados por un elemento $\alpha \in K^{\mathfrak{m}}$.

Con esto, podemos definir el grupo de clases de radicales.

Definición 5.8. En el contexto de la definición anterior, vamos a definir el *grupo de clases de radicales de K para el modulus* $\mathfrak{m}$ como el siguiente grupo cociente:

$$\mathrm{Cl}_K^{\mathfrak{m}} = \mathcal{I}_K^{\mathfrak{m}}/\mathcal{P}_K^{\mathfrak{m}}.$$

Este grupo $\mathrm{Cl}_K^{\mathfrak{m}}$ es un grupo finito, como se establece en [8, Cap. 6].

Observación 5.9. Si $\mathfrak{m}_\infty = \emptyset$ y $\mathfrak{m}_0 = \mathcal{O}_K$ entonces $\mathrm{Cl}_K^{\mathfrak{m}} = \mathrm{Cl}_K$.

Ejemplo 5.10. Si $K = \mathbb{Q}$ y $\mathfrak{m} = (m) \cdot \infty$, siendo m un entero, entonces $\mathrm{Cl}_{\mathbb{Q}}^{\mathfrak{m}}$ es isomorfo a $(\mathbb{Z}/m\mathbb{Z})^\times$.

En efecto, fijado m un entero, entonces el conjunto $\mathcal{I}_{\mathbb{Q}}^{\mathfrak{m}}$ es el conjunto de ideales coprimos con (m). Entonces, podemos definir la aplicación de $\mathcal{I}_{\mathbb{Q}}^{\mathfrak{m}}$ a $(\mathbb{Z}/m\mathbb{Z})^\times$ donde enviamos cada ideal coprimo con (m) a su imagen módulo m. El núcleo de esta aplicación es $\mathcal{P}_{\mathbb{Q}}^{\mathfrak{m}}$, es decir, los ideales de $\mathcal{I}_{\mathbb{Q}}^{\mathfrak{m}}$ congruentes con 1 módulo m. Por tanto, usando el primer teorema de isomorfía y recordando que $\mathrm{Cl}_{\mathbb{Q}}^{\mathfrak{m}} = \mathcal{I}_{\mathbb{Q}}^{\mathfrak{m}}/\mathcal{P}_{\mathbb{Q}}^{\mathfrak{m}}$ vemos que ambos conjuntos son isomorfos.

5.2. Funciones L de Weber

En esta sección vamos a tratar de introducir las funciones L de Weber, que trataran de generalizar el concepto de funciones L definidas en el capítulo 3. Será preciso entonces tener en cuenta la definición 3.6 y la proposición 3.9.

Observación 5.11. Aunque en el capítulo 3 hemos definido los caracteres de Dirichlet en el contexto de cuerpos de la forma $(\mathbb{Z}/n\mathbb{Z})^\times$, estos se pueden definir para grupos abelianos finitos de la misma forma: sea G un grupo abeliano finito arbitrario, un carácter de Dirichlet de G es un homomorfismo de grupos de G a $\mathbb{C}^\times$ el grupo multiplicativo complejo.

Con esto en mente, vamos a definir las funciones L de Weber.

Definición 5.12. Sea K un cuerpo de números y sea $\mathfrak{m} = \mathfrak{m}_0 \cdot \mathfrak{m}_\infty$ un modulus de K. Sea también χ un carácter de Dirichlet del grupo $\mathrm{Cl}_K^{\mathfrak{m}}$. La *función L de Weber*, $L_K^{\mathfrak{m}}(s, \chi)$ se define como

$$L_K^{\mathfrak{m}}(s,\chi) = \prod_{\mathfrak{p}\nmid\mathfrak{m}_0} \left(1 - \frac{\chi(\tilde{\mathfrak{p}})}{N(\mathfrak{p})^s}\right)^{-1} = \sum_{\gcd(\mathfrak{a},\mathfrak{m}_\circ)=1} \frac{\chi(\tilde{\mathfrak{a}})}{N(\mathfrak{a})^s},$$

donde el producto es sobre los infinitos ideales primos no nulos de $\mathcal{O}_K$ que no contienen al ideal $\mathfrak{m}_0$ y la suma es sobre todos los ideales de $\mathcal{O}_K$ cuya factorización en ideales primos no nulos no tenga ningún factor común con la factorización en ideales primos del ideal $\mathfrak{m}_0$. Además, $\tilde{\mathfrak{p}}$ y $\tilde{\mathfrak{a}}$ son las clases en $\mathrm{Cl}_K^{\mathfrak{m}}$ de $\mathfrak{p}$ y $\mathfrak{a}$ respectivamente.

Este producto y esta suma convergen absolutamente y son iguales para todo $s \in \mathbb{C}$ que cumpla que $Re(s) > 1$.

Mientras que las funciones L de Dirichlet vistas en el capítulo 3 nos permitían demostrar el teorema de la progresión aritmética, estas funciones L de Weber nos permitirán salirnos del caso de extensiones ciclotómicas, lo cual será más útil a la hora de demostrar el teorema de Chebotarev. Además, estas funciones tienen propiedades analíticas muy similares a las que tenían las funciones vistas en el capítulo 3.

Antes de pasar con una de las propiedades más interesantes de las funciones L de Weber, vamos a denotar por $H(n)$ al conjunto

$$H(n) = \{s \in \mathbb{C} : Re(s) > n\}.$$

Con esto en mente, veamos la siguiente proposición:

Proposición 5.13. *Sea K un cuerpo de números y sea $\mathfrak{m}$ un modulus de K. Sea χ un carácter de Dirichlet de $Cl_K^{\mathfrak{m}}$. Entonces la función $L_K^{\mathfrak{m}}(s, \chi)$ es una función holomorfa en $H(1)$. Además, se cumple lo siguiente:*

- *Si χ es el carácter trivial, entonces la función $L_K^{\mathfrak{m}}(s, \chi)$ tiene una extensión meromorfa al semiplano $H\left(1 - \frac{1}{[K:\mathbb{Q}]}\right)$ que es holomorfa menos en el punto $s = 1$ donde tiene un polo simple.*
- *Si χ no es el carácter trivial, entonces la función $L_K^{\mathfrak{m}}(s, \chi)$ tiene una extensión analítica al semiplano $H\left(1 - \frac{1}{[K:\mathbb{Q}]}\right)$.*

Demostración. Se puede ver en la sección 4.3 de [4]. □

En este sentido, las funciones L de Weber son mas restrictivas que las vistas en el capítulo 3, pues recordemos que las funciones L vistas anteriormente podían extenderse de forma analítica a todo el plano complejo. A pesar de esta restricción, esta propiedad es útil para poder probar el teorema de Chebotarev.

5.3. Esquema de la demostración

En esta sección intentaremos dar unas pequeñas pinceladas sobre la idea principal de la demostración del teorema de Chebotarev. Grosso modo, hay tres aspectos que conviene considerar.

(a) Demostrar el teorema para extensiones contenidas en una extensión ciclotómica, variando ligeramente el acercamiento que se usó para probar el teorema de la progresión aritmética de Dirichlet. En particular, eso requiere utilizar las funciones L de Weber que se introdujeron en la sección anterior.

(b) A partir de lo anterior, Chebotarev consigue extender el resultado a cualquier extensión con grupo de Galois abeliano, empleando de nuevo propiedades de los modulus y las funciones L de Weber.

(c) Finalmente, un argumento de Deuring (a veces llamado *argumento de conteo de Deuring*) nos permite concluir el caso general del teorema empleando el teorema para las extensiones abelianas de cuerpos de números.

Vamos a explicar brevemente el paso (a); para los otros dos, referimos a los últimos capítulos de [4].

Como acabamos de decir, el primer paso para la demostración es demostrar que el teorema de Chebotarev se cumple para las extensiones contenidas en una extensión ciclotómica, es decir, que se cumple el siguiente teorema:

Teorema 5.14 (**Teorema de Chebotarev para extensiones ciclotómicas**). *Sea $K \subseteq L \subset K(\zeta_m)$ una torre de cuerpos de números, donde ζ_m es una raíz primitiva m-ésima de la unidad (para un cierto $m \in \mathbb{Z}$). Sea también $G = \mathrm{Gal}(L/K)$ el grupo de Galois de la extensión intermedia y sea $\tau \in G$ un elemento del grupo de Galois. Por último, definamos por P al siguiente conjunto:*

$$P = \left\{ \mathfrak{p} \in P(K) : \mathfrak{p} \text{ no ramifica en } L, \left(\frac{L/K}{\mathfrak{p}} \right) = \{\tau\} \right\},$$

siendo $P(K)$ el conjunto de ideales primos no nulos de $\mathcal{O}_K$. Entonces:

$$\delta(P) = \frac{1}{|G|}.$$

donde $\delta(P)$ es la densidad de Dirichlet del conjunto P en $P(K)$.

Como vemos, el teorema que acabamos de enunciar no es más que un caso particular del teorema de Chebotarev enunciado en el capítulo 4, pues, al ser la torre de cuerpos de números $K \subseteq L \subseteq K(\zeta_m)$, entonces el grupo de Galois de la extensión L/K es abeliano y las clases de conjugación de ese grupo están formadas por un único elemento.

Para la demostración de este teorema, que se puede ver en [4, §4.5], se utilizan los conceptos ya vistos de modulus y función L de Weber. Vamos a presentar algunos de los resultados importantes para la demostración del teorema.

Definición 5.15. Sea K un cuerpo de números, $\mathfrak{m} = \mathfrak{m}_0 \cdot \mathfrak{m}_\infty$ un modulus de K, χ un carácter de Dirichlet del grupo $\mathrm{Cl}_K^{\mathfrak{m}}$ y $s \in H(1)$. Entonces definimos

$$\ell_K^{\mathfrak{m}}(s,\chi) = -\sum_{\mathfrak{p}\nmid\mathfrak{m}_\circ} \log\left(1 - \frac{\chi(\tilde{\mathfrak{p}})}{N(\mathfrak{p})^s}\right),$$

que es una serie que converge absolutamente y satisface que

$$L_K^{\mathfrak{m}}(s,\chi) = e^{\ell_K^{\mathfrak{m}}(s,\chi)}.$$

Proposición 5.16. *La función $\ell_K^{\mathfrak{m}}(s,\chi)$ es una función holomorfa sobre s en $H(1)$.*

Proposición 5.17. *En el mismo contexto que antes, se tiene que*

$$\ell_K^{\mathfrak{m}}(s,\chi) = \sum_{\mathfrak{p}\nmid\mathfrak{m}_0} \frac{\chi(\tilde{\mathfrak{p}})}{N(\mathfrak{p})^s} + O(1) \quad si \quad s \to 1^+.$$

Proposición 5.18. *Sea $A \subseteq P(K)$, entonces*

$$\delta(A) = \lim_{\sigma\to 1^+} \frac{\sum_{\mathfrak{p}\in A} N(\mathfrak{p})^{-\sigma}}{-\log(\sigma-1)}.$$

Esto último nos dice que la densidad de Dirichlet de A sobre $P(K)$ existe si y solamente si el límite lateral existe, y en ese caso, los valores coinciden.

Estos son los resultados principales (entre otros) que se usan para la demostración del teorema.

Tras esto, para la demostración del teorema de densidad de Chebotarev se sigue el esquema que pusimos al principio de la sección: primero podemos conseguir extender el resultado que acabamos de ver para cualquier tipo de extensión con grupo de Galois abeliano.

Por último, gracias al argumento de conteo de Deuring se puede demostrar el caso general, concluyendo así con toda la demostración del **teorema de densidad de Chebotarev**.

Anexo I

Código de SageMath para factorizar polinomios módulo p

A continuación, mostramos el código utilizado en el primer capítulo para estudiar los patrones de factorización de polinomios irreducibles módulo p. En el código que se muestra, se hace para el polinomio $x^5 + 11x + 44$ en concreto y en los experimentos numéricos que se han realizado se ha ido variando el polinomio elegido (la tercera línea) y haciendo los ajustes necesarios al código para que funcione correctamente.

```
R.<x> = ZZ[];
p = Primes();
poly = x^5+11*x+44
repeatedFactors = 0;
n = 1000;
factor5 = 0;
factor41 = 0;
factor32 = 0;
factor311 = 0;
factor221 = 0;
factor2111 = 0;
factor11111 = 0;

print("Number of primes :")
print(n);
print("Polynomial :")
print(poly);

for j in range(0, n):
    prime = p.unrank(j);
```

```
    factor = poly.factor_mod(prime);
    thisRepeated = 0;
    for i in range(0, len(factor)):
        if thisRepeated == 0 and factor[i][1] > 1:
            thisRepeated = 1;
            repeatedFactors = repeatedFactors + 1;

    if thisRepeated == 0:
        if len(factor) == 1:
            factor5 = factor5 + 1;
        elif len(factor) == 2:
            if (factor[0][0].degree() == 4 or
                factor[1][0].degree() == 4):
                factor41 = factor41 + 1;
            else:
                factor32 = factor32 + 1;
        elif len(factor) == 3:
            if (factor[0][0].degree() == 2 or
            factor[1][0].degree() == 2 or
            factor[2][0].degree() == 2):
                factor221 = factor221 + 1;
            else:
                factor311 = factor311 + 1;
        elif len(factor) == 4:
            factor2111 = factor2111 + 1;
        elif len(factor) == 5:
            factor11111 = factor11111 + 1;
    else:
        print("REPEATED FACTORS FOUND AT PRIME "),
        print(prime);

print("Primes with repeated factors found: "),
print(repeatedFactors);

print("Factorizations of the form (5) :"),
print(factor5),
print(", percentage "),
print(factor5/(n - repeatedFactors));

print("Factorizations of the form (4,1) :"),
print(factor41),
print(", percentage "),
print(factor41/(n - repeatedFactors));
```

```
print("Factorizations of the form (3,2) :"),
print(factor32),
print(", percentage "),
print(factor32/(n - repeatedFactors));

print("Factorizations of the form (3,1,1) :"),
print(factor311),
print(", percentage "),
print(factor311/(n - repeatedFactors));

print("Factorizations of the form (2,2,1) :"),
print(factor221),
print(", percentage "),
print(factor221/(n - repeatedFactors));

print("Factorizations of the form (2,1,1,1) :"),
print(factor2111),
print(", percentage "),
print(factor2111/(n - repeatedFactors));

print("Factorizations of the form (1,1,1,1,1) :"),
print(factor11111),
print(", percentage "),
print(factor11111/(n - repeatedFactors));
```

Bibliografía

[1] Apostol, T. M. (1976). *Introduction to Analytic Number Theory*, Undergraduate Texts in Mathematics, Springer, New York.

[2] Conrad, K. (2025). *History of Class Field Theory*, online notes.

[3] Cox, D. A. (1989). *Primes of the Form $x^2 + ny^2$*, Wiley.

[4] Di Meglio, M. (2019). *Chebotarev's Density Theorem*, School of Mathematics and Statistics, UNSW Sydney.

[5] Fried, M. D. y Jarden, M. (2023). *Field Arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics, Springer, Cham.

[6] Ireland, K. y Rosen, M. (1990). *A Classical Introduction to Modern Number Theory*, 2nd ed., Graduate Texts in Mathematics, Springer-Verlag, New York.

[7] Janusz, G. J. (1996). *Algebraic Number Fields*, 2nd ed., Graduate Studies in Mathematics, American Mathematical Society.

[8] Marcus, D. A. (2018). *Number Fields*, 2nd ed., Universitext, Springer, Cham.

[9] Milne, J. S. (2017). *Algebraic Number Theory (v3.07)*, online notes.

[10] Neukirch, J. (1999). *Algebraic Number Theory*, Grundlehren der mathematischen Wissenschaften, Springer, Berlin–Heidelberg.

[11] Serre, J.-P. (1973). *A Course in Arithmetic*, Graduate Texts in Mathematics, Springer-Verlag, New York.

[12] Stein, E. M. y Shakarchi, R. (2003). *Fourier Analysis: An Introduction*, Princeton Lectures in Analysis, vol. 1, Princeton University Press, Princeton.