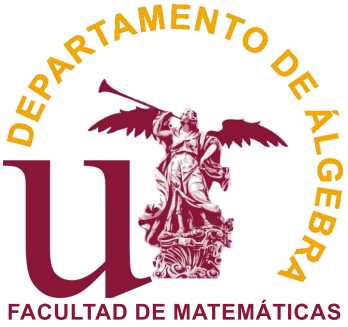
Teorema de Dirichlet para Progresiones Aritméticas

Garrido López, Verónica



Teorema de Dirichlet para Progresiones Aritméticas

Memoria presentada como parte de los requisitos para la obtención del título de Máster Universitario en Matemáticas por la Universidad de Sevilla.

Realizada por
Garrido López, Verónica

Tutorizada por
Rojas León, Antonio

Índice general

Sumario

English Abstract

Prime numbers aroused the curiosity of many for centuries, and they keep answering many questions that come up currently.

Euclid carried out the first prove about the infinitude of prime numbers in his time. What we now call Euclid's Theorem drove numerous proves of itself.

In the XVIII century, Euler achieved the connection of the study of prime numbers with the Riemann Zeta function with the help of the Euler product

$$\zeta(s) = \sum_{n\in\mathbb{N}} \frac{1}{n^s} = \prod_{p\ Primo} \frac{1}{1-p^{-s}}$$

proving the Euclid's theorem with this new tool.

Our aim is to generalise this result to the arithmetic sequences

$$\{a + mk \mid a, m \in \mathbb{N} \text{ fixed},\ \gcd(a, m) = 1, k \in \mathbb{N}_0\}$$

This is the Dirichlet's Theorem on arithmetic progressions, which states the existence of infinite prime numbers in each of this sets.

We will give a classical prove making use of some results on Analytic Number Theory regarding the Riemann Zeta function and its derivatives applied to some Algebraic Number Theory issues on cyclotomic extensions, guiding ourselves primarily by Ribenboim's book[7].

We will start going over extensions in algebraic number fields and Dedekind domains, which we can find in the Neukirch book[5], followed by a brief introduction to ideal clases and the group of units of a number field.

Understanding this concepts and applying them on cyclotomic fields is key to show the relationship between prime ideals and Dirichlet's theorem, the goal of this dissertation.

Once we are finish with the main issue we can proceed with some extra results on the density of this families of prime numbers, which is related to the Euler's totient function, as well as getting closer with more general results like Chevotarev's density making the same observations over any number field,

Resumen

Los números primos han suscitado la curiosidad de muchos durante siglos, y siguen dando respuesta a muchas de las preguntas que surgen en la actualidad.

Euclides desarrollo en su época la primera prueba sobre la infinitud de los números primos. Lo que hoy llamamos Teorema de Euclides impulsó numerosas pruebas del mismo.

En el siglo XVIII, Euler consiguió relacionar el estudio de los números primos con la función Zeta de Riemann con lo que llamamos producto de Euler

$$\zeta(s) = \sum_{n\in\mathbb{N}} \frac{1}{n^s} = \prod_{p\ Primo} \frac{1}{1-p^{-s}}$$

llegando a probar el Teorema de Euclides con su nueva herramienta de estudio.

Nuestro objetivo es generalizar este resultado a series aritméticas de la forma

$$\{a+mk \mid a, m \in \mathbb{N} \text{ fijados},\ \gcd(a,m) = 1, k \in \mathbb{N}_0\}$$

Se trata del teorema de Dirichlet para progresiones aritméticas, el cual dice que existen infinitos primos en cada uno de estos conjuntos.

Daremos una demostración clásica usando algunos resultados sobre Teoría Analítica de Números respecto a la función Zeta de Riemann y sus derivados aplicados a resultados algebraicos sobre extensiones ciclotómicas guiándonos principalmente por el libro de Ribenboim[7].

Empezaremos haciendo un repaso sobre las extensiones de cuerpos de números algebraicos y dominios de Dedekind con resultados que podremos encontrar en el libro

de Neukirch[5], seguido del desarrollo breve de las clases de ideales o el grupo de unidades de un cuerpo de números.

Entender estos conceptos y aplicarlos correctamente a extensiones ciclotómicas será la clave para ver la relación entre los ideales primos en ellas y el teorema de Dirichlet, objetivo de nuestro trabajo.

Una vez finalizado el tema principal podremos dar algún resultado extra sobre la densidad de familias de números primos, que tendrá que ver con la función indicatriz de Euler, además de aproximarnos ligeramente a resultados más generales como el densidad de Chevotarev que hace estas mismas observaciones sobre un cuerpo de números cualquiera.

1 Conocimientos Introductorios

Como bien sabemos, un dominio de ideales principales tiene propiedades muy únicas como es que sus ideales estén generados por un sólo elemento o la factorización única de sus elementos. Resultaría de gran ayuda poder heredar dichas propiedades en el estudio de extensiones de cuerpo algebraicas, sin embargo se trata de un caso especial.

No obstante podemos estudiar dichas propiedades de forma análoga en los dominios de Dedekind haciendo uso de los ideales, veremos en los siguientes apartados cómo podemos conseguir una factorización única de ideales alzados al cuerpo extendido como descomposición en ideales primos.

También observaremos lo que se llama el número de clase de un cuerpo de números algebraico, que será un invariante del cuerpo que se corresponde con la cantidad de clases de ideales que existen en el cuerpo y nos indicará cuánto dista un cierto ideal de ser principal según la clase a la que pertenezca. Estas clases se comportarán como un grupo finito y serán necesarias a la hora de definir la llamada función Zeta de Dedekind.

Por último revisaremos el grupo de las unidades del anillo de enteros de un cuerpo de números algebraico. Las unidades son lo que diferencian los distintos elementos asociados de un anillo y evidentemente dos elementos asociados generan el mismo ideal. Nos interesa conocer cual se su estructura en nuestro estudio, y gracias a ella podremos definir otro invariante más del cuerpo que es el regulador.

1.1 Dominios de Dedekind y Ramificación

Dominios de Dedekind

Comenzaremos por unas definiciones básicas que necesitaremos como son la norma y la traza y su relación con el discriminante de un cuerpo de números.

Definición 1.1.1.1 (Traza y Norma). *Sea L/K una extensión de cuerpos finita, la traza y la norma de un elemento $x \in L$ se definen respectivamente como la traza y el determinante del endomorfismo:*

$$T_x : L \to L, \quad T_x(a) = xa$$

$$\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}(T_x), \qquad \mathrm{N}_{L/K}(x) = \det(T_x)$$

Observación 1.1.1.2. Sea $n = [L : K]$. Si tomamos el polinomio característico de T_x como $f_x(t) = \prod_\sigma (t - \sigma x)$ donde σ varía por los distintos $K-$embeddings de L, podemos reconocer la traza y la norma como los coeficientes de los términos de grado $n-1$ y 0 respectivamente.

$$Tr_{L/K}(x) = \sum_\sigma \sigma x, \quad N_{L/K}(x) = \prod_\sigma \sigma x$$

Algo importante de la traza y la norma es que aplicadas a elementos de $\mathcal{O}_L$ su valor permanece en $\mathcal{O}_K$, de esta manera se convierten en fáciles de identificar.

Definición 1.1.1.3 (Discriminante). *Sea $\{\alpha_1, \dots, \alpha_n\}$ una base de una extensión separable L/K y sean σ_i los distintos $K-$embeddings de L, se define el discriminante asociado a la base como*

$$\mathrm{d}(\alpha_1, \dots, \alpha_n) = det((\sigma_i \alpha_j))^2 = \det\left(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)\right)$$

Dos bases íntegras, con elementos en $\mathcal{O}_L$, tienen el mismo discriminante asociado, ya que la matriz de cambio es invertible y de coeficientes enteros, es decir, con determinante ± 1. De este modo el discriminante asociado a una base íntegra es un invariante llamado el discriminante del cuerpo L.

Definición 1.1.1.4 (Dominio de Dedekind). *Un dominio de Dedekind es un dominio de integridad que satisface la siguientes propiedades:*

1. *Todo ideal es finitamente generado.*
2. *Todo ideal primo no trivial es maximal.*
3. *Es íntegramente cerrado en su cuerpo de fracciones.*

Lema 1.1.1.5. Sea K un cuerpo, y α un elemento íntegro sobre K. La extensión finita $K(\alpha) \supset K$ de grado n, formada al añadir el elemento α, es cuerpo.

Demostración. Sea α un elemento íntegro sobre K entonces existe un polinomio mónico $f(x) \in K[x]$ de grado $n \geq 1$ tal que $f(\alpha) = 0$. Tomemos f de grado mínimo y supongamos que es reducible. En este caso existen $g(x), h(x) \in K[x]$ no unidades tales que $f(x) = g(x)h(x)$. Esto implica que $f(\alpha) = g(\alpha)h(\alpha) = 0$ y por tanto $g(\alpha) = 0$ o $h(\alpha) = 0$, pero no es posible ya que $f(x)$ es de grado mínimo, es decir, $g(x)$ o $h(x)$ es una unidad. De aquí $f(x)$ es irreducible y $\langle f(x)\rangle$ es maximal en $K[x]$, por ende $K[X]/\langle f\rangle = K(\alpha)$ es cuerpo. ∎

Proposición 1.1.1.6. Sea K un cuerpo de números algebraicos. Si $\mathcal{O}_K$ el anillo de enteros de K entonces $\mathcal{O}_K$ es un dominio de Dedekind.

Demostración. Por la propia definición de anillo de enteros $\mathcal{O}_K$ es íntegramente cerrado y también es un $\mathbb{Z}-$módulo finitamente generado. Por lo que $\mathcal{O}_K$ es Noetheriano.

Sea un ideal primo $\mathfrak{p} \in \mathcal{O}_K$, $\mathfrak{p} \neq 0$, y consideremos $(p) = \mathfrak{p} \cap \mathbb{Z}$ que es un ideal primo en $\mathbb{Z}$. Sea $x \in \mathfrak{p}$, $x \neq 0$, se tiene el polinomio

$$x^n + a_{n-1}x^{n-1} + \cdots + xa_1 + a_0 = 0,\ a_i \in \mathbb{Z}\ 1 \leq i \leq n-1,\ a_0 \in \mathfrak{p} \cap \mathbb{Z},\ a_0 \neq 0$$

Con esto se prueba que $(p) \neq 0$. Entonces el dominio de integridad $\overline{\mathcal{O}} = \mathcal{O}_K/\mathfrak{p}$ se levanta desde $\mathbb{Z}p$ añadiendo elementos algebraicos, por lo que es un cuerpo por el lema anterior, y de aquí $\mathfrak{p}$ es ideal maximal. ∎

Los ideales de un Dominio de Dedekind tienen asociadas operaciones parecidas a los enteros y podemos definir la divisibilidad como la contención, $I|J$ si y sólo si $J \subset I$, y a raíz de ésto $\operatorname{lcm}(I, J) = I + J$, y $\gcd(I, J) = IJ$.

Proposición 1.1.1.7. En un dominio Noetheriano todo ideal no trivial contiene un producto de ideales primos.

Demostración. Sea D un dominio Noetheriano que contiene al menos un ideal no trivial que no contiene un producto de ideales primos. Llamemos S al conjunto de estos ideales, $S \neq \emptyset$, como D es Noetheriano cumple la condición maximal, es decir, $\exists I \in S$ maximal con respecto a dicha propiedad.

Puesto que I no es primo $\exists a_1, a_2 \notin I$ tales que $a_1a_2 \in I$. Sean $J_1 = \langle a_1\rangle + I$ y $J_2 = \langle a_2\rangle + I$, se tiene que $I \subsetneq J_1, J_2$ por lo que no están en S. Esto significa que ambos contienen un producto de ideales primos. Ahora bien

$$J_1J_2 = (\langle a_1\rangle + I)(\langle a_2\rangle + I) \subset I$$

y por lo tanto existe un producto de ideales primo contenido en I, lo que contradice que $I \in S$. ∎

Lema 1.1.1.8. Sea $\mathcal{O}_K$ un dominio de Dedekind, y $\mathfrak{p} \subset \mathcal{O}_K$ es un ideal primo. Definamos

$$\mathfrak{p}^{-1} = \{x \in K | x\mathfrak{p} \subseteq \mathcal{O}_K\}$$

Entonces, $\forall I \subset \mathcal{O}_K$ ideal no trivial, se tiene que

$$I\mathfrak{p}^{-1} = \left\{ \sum_i a_i x_i \mid a_i \in I,\ x_i \in \mathfrak{p}^{-1} \right\} \neq I$$

Ahora vamos a ver uno de los resultados más importantes, que es la factorización única de ideales del anillo de enteros, una vez visto esto vamos a ver propiedades ligadas a los propios ideales primos que aparezcan en la descomposición.

Teorema 1.1.1.9 (Factorización Ideales). *Todo ideal $I \subset \mathcal{O}_K$ distinto de $\langle 0 \rangle$ y $\langle 1 \rangle$ admite una factorización $I = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ en ideales primos $\mathfrak{p}_i$ de $\mathcal{O}_K$ que es única salvo por el orden de los factores.*

Demostración. Comenzamos probando la existencia de la descomposición. Sea S el conjunto de todos los ideales distintos de $\langle 0 \rangle$ y $\langle 1 \rangle$ que no admiten descomposición en ideales primos. Si S no es vacío, por el razonamiento de la proposición anterior debe existir un elemento maximal I en S. Éste está contenido en un ideal maximal $\mathfrak{p}$, así que

$$I \subseteq I\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}_K$$

Por el lema se tiene que $I \subsetneq I\mathfrak{p}^{-1}$ y $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}_K$. Al set $\mathfrak{p}$ ideal maximal sigue que $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_K$. En vista a la maximalidad de I en S, $I \neq \mathfrak{p}$ y $I\mathfrak{p}^{-1} \neq \mathcal{O}_K$. Entonces el ideal $I\mathfrak{p}^{-1}$ admite una descomposición en ideales primos $I\mathfrak{p}^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, y también lo hace $I = I\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}_1 \cdots \mathfrak{p}_r\mathfrak{p}$, en contradicción ya que $I \in S$.

Sea I un ideal tal que tiene dos factorizaciones distintas en ideales primos

$$I = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_s$$

Entonces $\mathfrak{p}_1$ divide algún factor $\mathfrak{q}_i$, digamos $\mathfrak{q}_1$, y siendo maximales $\mathfrak{p}_1 = \mathfrak{q}_1$. Multiplicamos por $\mathfrak{p}_1^{-1}$ y obtenemos

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s$$

Continuando este proceso llegamos a que $r = s$ y que $\mathfrak{p}_i = \mathfrak{q}_i \forall 1 \leq i \leq r$, concluyendo la unicidad de la descomposición. ∎

Teorema 1.1.1.10 (Teorema Chino del Resto). *Sean $I_1, \ldots, I_n$ ideales en un dominio de Dedekind $\mathcal{O}$ tales que $I_i + I_j = \mathcal{O}$ para todo $i \neq j$. Entonces, si $I = \bigcap_{i=1}^{n} I_i$, se*

tiene

$$\mathcal{O}/I \cong \bigoplus_{i=1}^{n} \mathcal{O}/I_i$$

Demostración. El homomorfismo canónico

$$\mathcal{O} \to \bigoplus_{i=1}^{n} \mathcal{O}/I_i, \quad a \to \bigoplus_{i=1}^{n} a \bmod I_i$$

tiene núcleo $I = \bigcap_{i=1}^{n}$, lo que nos da inyectividad, luego nos basta probar la sobreyectividad. Sean $x_i \bmod I_i \in \mathcal{O}/I_i$ dados para $1 \leq i \leq n$. Si $n = 2$ podemos escribir $1 = a_1 + a_2$, $a_i \in I_i$, y tomando $x = x_1 a_2 + x_2 a_1$ tenemos que $x \equiv x_i \bmod I_i$, $i = 1, 2$.

Si $n > 2$, podemos encontrar elementos $y_1, y_2, \ldots, y_n$ tales que

$$y_i \equiv 1 \bmod I_i, \quad y_i \equiv 0 \bmod \bigcap_{j \neq i} I_j$$

Tomando $x = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n$ nos encontramos con que $x \equiv x_i \bmod I_i$, $1 \leq i \leq n$. De aquí sacamos la sobreyectividad. ∎

Definición 1.1.1.11 (Ideal Fraccionario). *Sea D un dominio de integridad con cuerpo de fracciones K. Un subconjunto I no vacío de K se llama $D-$ideal fraccionario si satisface las siguientes propiedades:*

1. *Si $a, b \in I$, entonces $a + b \in I$*
2. *Si $a \in I$ y $d \in D$, entonces $ad \in I$*
3. *Existe $\gamma \in D$ tal que $\gamma I \subseteq D$*

Observación 1.1.1.12. Sea K un cuerpo de números, los $\mathcal{O}_K-$ideales fraccionarios de K forman un grupo abeliano. La identidad es $\mathcal{O}_K$ y el inverso de un ideal I es

$$I^{-1} = \{x \in K \mid xI \subseteq \mathcal{O}_K\}$$

Ramificación de Ideales

Aunque durante el resto del trabajo trataremos con extensiones $K\backslash\mathbb{Q}$, vamos a generalizar a extensiones L/K con anillos de enteros $o = \mathcal{O}_K$ y $\mathcal{O} = \mathcal{O}_L$ para definir conceptos relativos a la descomposición de ideales en ideales primos .

Definición 1.1.2.1 (Índice de Ramificación y Grado de Inercia). *Sea $\mathfrak{p}$ un ideal primo de $\mathcal{o}$ y $\mathfrak{P}$ un ideal primo de $\mathcal{O}$ en la descomposición de $\mathfrak{p}$. Llamamos índice de ramificación de $\mathfrak{P}$ al exponente e con el que aparece y el grado de la extensión $f = [\mathcal{O}/\mathfrak{P} : \mathcal{o}/\mathfrak{p}]$ se llama grado de inercia de $\mathfrak{P}$ sobre $\mathfrak{p}$.*

Proposición 1.1.2.2. Sea L/K una extensión separable de grado n y la descomposición $\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ del ideal primo $\mathfrak{p}$ en $\mathcal{O}$. Entonces se tiene la identidad fundamental

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

Demostración. Para realizar la prueba vamos a utilizar el Teorema Chino del Resto

$$\mathcal{O}/\mathfrak{p}\mathcal{O} \cong \bigoplus_{i=1}^{r} \mathcal{O}/\mathfrak{P}_i^{e_i}$$

Sean $b_1, \dots, b_m \in \mathcal{O}$ representantes de una base $\overline{b}_1, \dots, \overline{b}_m$ de $\mathcal{O}/\mathfrak{p}\mathcal{O}$ sobre $k = \mathcal{o}/\mathfrak{p}$, nos basta con probar que $b_1, \dots, b_m$ es una base de L/K. Supongamos que $b_1, \dots, b_m$ son linealmente dependientes sobre K, y por tanto también sobre $\mathcal{o}$. Entonces existen elementos $a_1, \dots, a_m \in \mathcal{o}$ no todos nulos tales que

$$a_1 b_1 + \cdots a_m b_m = 0$$

Consideremos el ideal $J = \langle a_1, \dots, a_m \rangle$ de $\mathcal{o}$ y un elemento $a \in J^{-1}$ tal que $a \notin J^{-1}\mathfrak{p}$, así $aJ \not\subseteq \mathfrak{p}$. Entonces los elementos $aa_1, \dots, aa_m$ están en $\mathcal{o}$ pero no todos en $\mathfrak{p}$ llegando a la congruencia

$$aa_1 b_i + \cdots + aa_m b_m \equiv 0 \bmod \mathfrak{p}$$

que resulta en la dependencia lineal de $\overline{b}_1, \dots, \overline{b}_m$ en k, que es una contradicción. Por lo que $b_1, \dots, b_m$ son linealmente independientes sobre K.

Para ver que los b_i forman una base de L/K consideramos los $\mathcal{o}-$módulos $M = \mathcal{o}b_1 + \cdots + \mathcal{o}b_m$ y $N = \mathcal{O}/M$. Dado que $\mathcal{O} = M + \mathfrak{p}\mathcal{O}$, tenemos que $N = \mathfrak{p}N$, y como L/K es separable, $\mathcal{O}$ y N son $\mathcal{o}-$módulos finitamente generados. Si $c_1, \dots, c_s$ es un sistema de generadores de N, entonces

$$c_i = \sum_{j=1}^{s} a_{ij} c_j, \quad a_{ij} \in \mathfrak{p}$$

Sea A la matriz $(a_{ij} - I)$, y sea B la matriz adjunta de A. Entonces se da que $A(c_1, \dots, c_n)^t = 0$ y $BA = dI$, donde $d = det(A)$. Por consiguiente

$$0 = BA(c_1, \dots, c_n)^t = (dc_1, \dots, dc_n)^t$$

y por tanto $dN = 0$, es decir, $d\mathcal{O} \subseteq M = \mathfrak{o}b_1 + \cdots + \mathfrak{o}b_m$. Nos encontramos con que $d = (-1)^s \bmod \mathfrak{p}$ ya que $a_{ij} \in \mathfrak{p}$. Se sigue que $L = dL = Kb_1 + \cdots + kb_m$ y de aquí, $b_1, \ldots, b_m$ es una base de L/K. Deducimos pues que

$$\dim_{\mathfrak{o}/\mathfrak{p}}(\mathcal{O}/\mathfrak{p}\mathcal{O}) = n$$

A continuación consideremos la cadena descendiente de $k-$espacios vectoriales

$$\mathcal{O}/\mathfrak{P}_i^{e_i} \supseteq \mathfrak{P}_i/\mathfrak{P}_i^{e_i} \supseteq \cdots \supseteq \mathfrak{P}_i^{e_i-1}/\mathfrak{P}_i^{e_i} \supseteq \langle 0 \rangle$$

Los cocientes sucesivos tomados como $\mathfrak{P}_i^v/\mathfrak{P}_i^{v+1}$ en esta cadena son todos isomorfos a $\mathcal{O}\mathfrak{P}_i$, ya que para $b \in \mathfrak{P}_i^v \backslash \mathfrak{P}_i^{v+1}$ podemos definir el homomorfismo

$$\mathcal{O} \to \mathfrak{P}_i^v/\mathfrak{P}_i^{v+1}, \quad a \to ab,$$

con kernel $\mathfrak{P}_i$. Es sobreyectivo ya que $\mathfrak{P}_i^v$ es el máximo común divisor entre $\mathfrak{P}_i^{v+1}$ y $\langle b \rangle = b\mathcal{O}$ por tanto $\mathfrak{P}_i^v = b\mathcal{O} + \mathfrak{P}_i^{v+1}$. Al ser $f_i = [\mathcal{O}/\mathfrak{P}_i : k]$, obtenemos que $\dim_k(\mathfrak{P}_i^v/\mathfrak{P}_i^{v+1}) = f_i$ y de aquí

$$\dim_k(\mathcal{O}/\mathfrak{P}_i^{e_i}) = \sum_{v=0}^{e_i-1} \dim_k(\mathfrak{P}_i^v/\mathfrak{P}_i^{v+1}) = e_i f_i$$

Definición 1.1.2.3. *Sea un ideal primo en $\mathfrak{o}$, este se dice que descompone completamente en L si en su descomposición $\mathfrak{p}\mathcal{O} = \mathfrak{P}_i^{e_1} \cdots \mathfrak{P}_r^{e_r}$ se tiene que $r = n = [L : K]$, de forma que $f_i = e_i = 1$.*

Del mismo modo, se dice que que el ideal no descompone si $r = 1$, y además si .

Definición 1.1.2.4. *Sea $\mathfrak{P}_i$ un ideal que aparece en la descomposición $\mathfrak{p}\mathcal{O}$. Se dice que no ramifica en $\mathfrak{o}$ si $e_i = 1$ y si la extensión residual de cuerpo $(\mathcal{O}/\mathfrak{P}_i)/(\mathfrak{o}/\mathfrak{p})$ es separable. Si no, se dice que es ramificado, si además se tiene que $f_i = 1$ es completamente ramificado.*

Si ninguno los $\mathfrak{P}_i$ es ramificado, entonces se dice que $\mathfrak{p}$ no es ramificado. De otro modo es ramificado.

La extensión L/K se dice no ramificada si ninguno de los ideales primos de K es ramificado en L.

Hay un caso muy concreto en el que podemos estudiar la ramificación de ideales, y es cuando la extensión L/K es de Galois. Nos interesa especialmente porque nos centraremos en las extensiones ciclotómicas, las cuales están estrechamente ligadas a las progresiones aritméticas que queremos estudiar.

Proposición 1.1.2.5. Sea L/K una extensión de Galois y G su grupo de Galois. Entonces G actúa transitivamente en el conjunto de todos los primos $\mathfrak{P}$ de $\mathcal{O}$ que se levantan sobre $\mathfrak{p}$.

Demostración. Sean $\mathfrak{P}$ y $\mathfrak{P}'$ dos ideales primos sobre $\mathfrak{p}$. Supongamos que $\mathfrak{P}' \neq \sigma\mathfrak{P}$ para todo $\sigma \in G$. Por el teorema Chino del Resto existe $x \in \mathcal{O}$ tal que

$$x \equiv 0 \bmod \mathfrak{P}' \quad \text{y} \quad x \equiv 1 \bmod \sigma\mathfrak{P}\ \forall \sigma \in G$$

Entonces la norma $\mathrm{N}_{L/K}(x) = \prod_{\sigma\in G} \sigma x \in \mathfrak{P}' \cap o = \mathfrak{p}$. Por otro lado $x \notin \sigma\mathfrak{P}$ para ningún $\sigma \in G$, así que $\sigma x \notin \mathfrak{P}$ para ningún $\sigma \in G$. Consecuentemente $\prod_{\sigma\in G} \sigma x \notin \mathfrak{P} \cap o = \mathfrak{p}$, con lo que llegamos a contradicción. ∎

Corolario 1.1.2.6. En una extensión de Galois los grados de inercia $f_1, \ldots, f_r$ y los índices de ramificación $e_1, \ldots, e_r$ de la descomposición en primos no dependen del subíndice ya que son iguales.

1.2 Clases de ideales

Norma de un Ideal

El anillo de enteros de un cuerpo de números algebraico K es un dominio de Dedekind, aunque no tiene por qué ser un dominio de ideales principales. Vamos a estudiar un invariante de K, el número de clases de ideales, que nos dirá cómo de lejos está de ser DIP.

Para ello antes vamos a ver lo que es la norma de in ideal, herramienta que recordaremos hacia el final de éste trabajo, que nos servirá para determinar el número de elementos en el cociente $\mathcal{O}_K/\mathfrak{p}$. Puesto que $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, entonces este número ha de ser una potencia de p.

Proposición 1.2.1.1. Sean $\mathfrak{p}$ un ideal primo de $\mathcal{O}_K$ y $e \geq 1$, entonces $\#(\mathcal{O}_K/\mathfrak{p}^e) = \#(\mathcal{O}_K/\mathfrak{p})^e$.

Demostración. Procedemos a la prueba por inducción, para $e = 1$ está claro que se tiene el resultado, así que supongamos $e \geq 2$ y que se cumple para $e - 1$. Por el tercer teorema de isomorfía

$$(\mathcal{O}_K/\mathfrak{p}^e)/(\mathfrak{p}^{e-1}/\mathfrak{p}^e) \cong \mathcal{O}_K/\mathfrak{p}^{e-1}$$

por lo que se deduce que $\#(\mathcal{O}_K/\mathfrak{p}^e) = \#(\mathcal{O}_K/\mathfrak{p}^{e-1})\#(\mathfrak{p}^{e-1}/\mathfrak{p}^e)$. Por la hipótesis de inducción nos basta comprobar que $\#(\mathfrak{p}^{e-1}/\mathfrak{p}^e) = \#(\mathcal{O}_K/\mathfrak{p})$.

Sea $b \in \mathfrak{p}^{e-1}/\mathfrak{p}^e$ formemos el homomorfismo de anillos

$$f : \mathcal{O}_K \to \mathfrak{p}^{e-1}/\mathfrak{p}^e : a \mapsto ab$$

El kernel de esta aplicación es evidentemente $\mathfrak{p}$, luego $\mathcal{O}_K/\mathfrak{p} \cong \mathfrak{p}^{e-1}/\mathfrak{p}^e$. ∎

Corolario 1.2.1.2. Sea $J \subset \mathcal{O}_K$ cuya descomposición en ideales primos es $J = \prod \mathfrak{p}_i^{e_i}$, entonces

$$\#(\mathcal{O}_K/J) = \prod \#(\mathcal{O}_K/\mathfrak{p}_i)^{e_i}$$

Demostración. Por la versión del Teorema Chino del Resto para ideales sabemos que

$$\mathcal{O}_K/J \cong \bigoplus \mathcal{O}_K/\mathfrak{p}_i^{e_i}$$

por lo que es directo, añadiendo la proposición anterior, que la proposición anterior que

$$\#(\mathcal{O}_K/J) = \prod \#(\mathcal{O}_K/\mathfrak{p}_i^{e_i}) = \prod \#(\mathcal{O}_K/\mathfrak{p}_i)^{e_i}$$

∎

Definición 1.2.1.3 (Norma de un Ideal). *La norma de un ideal $J \subset \mathcal{O}_K$ en un cuerpo de números algebraico K se define como el entero positivo $\mathrm{N}_{K/\mathbb{Q}}J = \#(\mathcal{O}_K/J)$ y es una función multiplicativa.*

Proposición 1.2.1.4. Sea J un ideal íntegro con base $y_1, \ldots, y_n$, y sea d el discriminante del cuerpo K. Entonces

$$(\mathrm{N}_{K/\mathbb{Q}}J)^2 = \frac{\mathrm{d}(y_1, \ldots, y_n)}{d}$$

Demostración. Sea $\alpha_1, \ldots, \alpha_n$ una base de $\mathcal{O}_K$, se tiene que $\mathcal{O}_K = \bigoplus \alpha_i\mathbb{Z}$. En vista de [7](6.L), sean $r_1, \ldots, r_n$ enteros tales que $r_1\alpha_1, \ldots, r_n\alpha_n$ formen una base de $J = \bigoplus r_i\alpha_i\mathbb{Z}$. Entonces se tiene el siguiente isomorfismo

$$\mathcal{O}_K/J \cong \prod \mathbb{Z}r_i$$

por lo que $\mathrm{N}_{K/\mathbb{Q}}J = \prod |r_i|$. Y puesto que

$$\mathrm{d}(r_1\alpha_1, \dots, r_n\alpha_n) = d\prod |r_i|^2$$

obtenemos el resultado que queríamos siendo $y_i = r_i\alpha_i$.

Corolario 1.2.1.5. Para todo $y \in \mathcal{O}_K$ no nulo, consideramos el ideal principal $y\mathcal{O}_K$, entonces se tiene que

$$\mathrm{N}_{K/\mathbb{Q}}(y\mathcal{O}_K) = |\mathrm{N}_{K/\mathbb{Q}}(y)|$$

Demostración. Sea $\alpha_1, \dots, \alpha_n$ una base de $\mathcal{O}_K$, $y\alpha_1, \dots, y\alpha_n$ la forma del ideal $y\mathcal{O}_K$. Si calculamos el discriminante de la base de $y\mathcal{O}_K$

$$\mathrm{d}(y\alpha_1, \dots, y\alpha_n) = \det(\sigma_i(yx_j))^2 = \det(\sigma_i(x_j))^2 \det(\sigma_i(yI))^2 = d\mathrm{N}_{K/\mathbb{Q}}(y)^2$$

Proposición 1.2.1.6. Sea J un ideal integral no trivial de $\mathcal{O}_K$ con norma m, entonces J divide al ideal principal $m\mathcal{O}_K$. Para cada entero $m > 0$ existe una cantidad finita de ideales con norma m.

Demostración. Puesto que $\#(\mathcal{O}_K/J) = \mathrm{N}_{K/\mathbb{Q}}J = m$, el orden de los elementos del grupo cociente $\mathcal{O}_K/J$ divide a m, por lo tanto, si $x \in \mathcal{O}_K$ entonces $mx \in J$, en particular $m = 1 \cdot m \in J$, así que $m\mathcal{O}_K \subset J$.

Ahora, ya que $m\mathcal{O}_K$ tiene una cantidad finita de divisores, existe una cantidad finita de ideales J con norma m.

Proposición 1.2.1.7. Sea $m > 2$ y sea ζ una raíz $m-$ésima primitiva de la unidad, consideramos $K = \mathbb{Q}(\zeta)$ y un primo p, entonces p descompone completamente en $\varphi(m)$ ideales de norma p si y sólo si $p \equiv 1 \bmod m$.

Demostración. Supongamos que p descompone completamente, esto es que

$$p\mathcal{O}_K = \prod_{i=1}^{\varphi(m)} \mathfrak{p}_i$$

con $e = 1$, $f = 1$ y $r = \varphi(m)$. Sea $\mathfrak{p}$ en la descomposición de p y $G \cong (\mathbb{Z}m)^\times$ el grupo de Galois, formamos el grupo $G_\mathfrak{p} = \{\sigma \in G | \sigma\mathfrak{p} = \mathfrak{p}\}$, se tiene que $r = \#(G/G_\mathfrak{p})$, luego $G_\mathfrak{p} = \{id\}$.

Ahora tomemos el homomorfismo sobreyectivo $G_\mathfrak{p} \to \mathrm{Gal}((\mathcal{O}_K/\mathfrak{p})\backslash\mathbb{Z}p)$, como $1 \geq \#\mathrm{Gal}((\mathcal{O}_K/\mathfrak{p})\backslash\mathbb{Z}p) \leq [\mathcal{O}_K/\mathfrak{p} : \mathbb{Z}p] = 1$, su grupo se compone también de la identidad.

De aquí $\mathrm{Frob}_p(x) = x$ y el frobrnius es la identidad, un elemento de orden 1 en G, que se corresponde con $\bar{1} \in (\mathbb{Z}m)^\times$, luego $p \equiv 1 \bmod m$.

El resultado se puede generalizar a elementos de otros ordenes como se puede ver en [7](11.O) relacionado con los grupos de descomposición y de inercia que están mejor definidos en [2](§1.2.3).

Por el otro lado, supongamos por reducción al absurdo que p no descompone completamente, es decir,

$$p\mathcal{O}_K = \prod_{i=1}^{r} \mathfrak{p}_i^e$$

con $f = 1$ al ser el orden de p módulo m. De aquí $\varphi(m) = er$, pero e no puede ser 1, ya que entonces p descompondría totalmente, pero tampoco puede ser mayor, ya que entonces implicaría que p divide a m, un divisor del discriminante de K. Por último, la norma $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}) = p^f$ para cualquier $\mathfrak{p}$ en la descomposición de p por la propia definición de f.

Proposición 1.2.1.8. Sea K un cuerpo de números y sea $x_1, \dots, x_n$ una base de $\mathcal{O}_K$ y σ_j cada una de las inmersiones, si notamos $\sigma_j x_i = x_i^{(j)}$ definimos

$$\mu = \prod_{j=1}^{n} \sum_{i=1}^{n} |x_i^{(j)}|$$

Entonces para cada ideal íntegro de $\mathcal{O}_K$ existe un $a \in J$ no nulo tal que

$$|\mathrm{N}_{K/\mathbb{Q}}(a)| \leq \mathrm{N}_{K/\mathbb{Q}}(J) \cdot \mu$$

Demostración. Sea k un número natural tal que $k^n \leq \mathrm{N}_{K/\mathbb{Q}}(J) < (k+1)^n$. Consideremos el conjunto S de todos los elementos $\sum_{i=1}^{n} d_i x_i$ con $0 \leq d_i \leq k$. Como $\#S = (K+1)^n > \#(\mathcal{O}_K/J)$ deben existir $b, c \in S$ tales que

$$a = b - c = \sum_{i=1}^{n} (b_i - c_i) x_i \in J, \quad |a_i| \leq k$$

Entonces

$$|\mathrm{N}_{K/\mathbb{Q}}(a)| = \left| \prod_{j=1}^{n} \sum_{i=1}^{n} a_i x_i^{(j)} \right| \leq \prod_{j=1}^{n} k \sum_{i=1}^{n} |x_i^{(j)}| = k^n \mu \leq \mathrm{N}_{K/\mathbb{Q}}(J) \cdot \mu$$

Clases de Ideales

Con anterioridad definimos lo que son los $\mathcal{O}_K-$ideales fraccionarios y que se comportan como un grupo abeliano. Vamos a notar dicho grupo como $\mathcal{F} = \mathcal{F}(K)$ y considerando el subgrupo de los ideales principales $\mathcal{P}r = \mathcal{P}r(K)$ tomaremos el grupo cociente $C(K) = \mathcal{F}/\mathcal{P}r$.

Este último grupo se llama el grupo de las clases de ideales de K y vamos a estudiar su finitud a la vez que intentaremos generalizarlo ligeramente cuando esté sujeto a un ideal no nulo J.

Teorema 1.2.2.1. *El número de clases de ideales de un cuerpo de números algebraico es finito.*

Demostración. Ya hemos visto que existe una cantidad finita de ideales íntegros con norma menor que un cierto entero dado. Sea μ tal y como se ha definido antes, entonces existirá una cantidad finita de ideales $J_1, \dots, J_h$ tales que su norma es menor o igual a μ.

Sea $I \subset \mathcal{O}_K$ un ideal cualquiera, consideramos el ideal fraccionario I^{-1} y un elemento $c \in \mathcal{O}_K$ tal que cI^{-1} sea ideal íntegro.

Por la proposición 1.2.1.8 debe existir un $b \in cI^{-1}$ tal que $\mathrm{N}_{k/\mathbb{Q}}(b\mathcal{O}_K) \leq \mathrm{N}_{K/\mathbb{Q}}(cI^{-1})\mu$. Multiplicando por la norma de I

$$\begin{aligned}\mathrm{N}_{K/\mathbb{Q}}(c^{-1}bI)\mathrm{N}_{K/\mathbb{Q}}(c\mathcal{O}_K) =& \mathrm{N}_{K/\mathbb{Q}}(bI) = \mathrm{N}_{K/\mathbb{Q}}(b\mathcal{O}_K)\mathrm{N}_{K/\mathbb{Q}}(I) \\ \leq& \mathrm{N}_{K/\mathbb{Q}}(cI^{-1})\mu\mathrm{N}_{K/\mathbb{Q}}(I) = \mathrm{N}_{K/\mathbb{Q}}(c\mathcal{O}_K)\mu\end{aligned}$$

por lo que $I(c^{-1}b\mathcal{O}_K) = c^{-1}bI = J_i$ para algún i. ∎

Definición 1.2.2.2 (Número de clase). *Sea K un cuerpo de números, definimos como el número de clase h a la cantidad de clases de ideales existentes en K.*

Si $J \in \mathcal{F}$, resulta directo ver que al ser h el orden de C, entonces J^h es un ideal fraccionario principal de $\mathcal{O}_K$.

Observación 1.2.2.3. Aunque no es nuestro objetivo, cabe remarcar que por el Teorema de Estructuras podemos separar C como producto de grupos cíclicos C_i de orden h_i, por lo que los ideales que generen cumplirán que $J_i h_i$ es un ideal principal $a_i\mathcal{O}_K$. Este detalle puede usarse para construir una extensión de K de grado h a lo sumo en el que los ideales de K son principales.

Por último, sea J un ideal íntegro no trivial, vamos a considerar los grupos que definimos al principio, pero asociados a este J. Ajustamos dichos grupos del siguiente modo

$$\begin{aligned}\mathcal{F}_J &= \{I/I' \mid \gcd(I,J) = \gcd(I',J) = \mathcal{O}_K\} \\ \mathcal{P}r_J &= \{x\mathcal{O}_K \mid x \in K, x \equiv 1 \bmod J\}\end{aligned}$$

donde queda claro que son subgrupos de los primeros y que por tanto $\mathcal{C}_J = \mathcal{F}_J/\mathcal{P}r_J$ es un grupo finito y tiene su número de clase asociado h_J, además tenemos que $\mathcal{F}_{\mathcal{O}_K} = \mathcal{F}$, $\mathcal{P}r_{\mathcal{O}_K} = \mathcal{P}r$ y $\mathcal{C}_{\mathcal{O}_K} = \mathcal{C}$.

A partir de ellos podemos definir unos últimos grupos, $\mathcal{P}r_{J+}$ y $\mathcal{C}_{J+}$ de forma que x es totalmente positivo, es decir, que sus conjugados reales sean positivos.

Proposición 1.2.2.4. Para todo ideal íntegro $J \neq 0$, el grupo $\mathcal{C}_{J+}$ es finito.

Demostración. Por el Tercer Teorema de Isomorfía se tiene que $\mathcal{C}_J \cong (\mathcal{F}_J/\mathcal{P}r_{J+})/(\mathcal{P}r_J/\mathcal{P}r_{J+})$ y sabemos que $\mathcal{C}_J$ es un conjunto finito. Nos centraremos en ver que $\mathcal{P}r_J/\mathcal{P}r_{J+}$ es finito y eso será suficiente.

Sea $r_1 \geq 0$ el número de embeddings reales, definimos la aplicación

$$\Sigma : \mathcal{P}r_J/\mathcal{P}r_{J+} \longrightarrow (A/J)^\times \times \{1,-1\}^{r_1}$$

$$C \to (x \bmod J, \operatorname{signo}(x))$$

donde $C = x\mathcal{O}_K\mathcal{P}r_{J+}$ y $\operatorname{signo}(x) = (\operatorname{signo}(x^{(1)}), \ldots, \operatorname{signo}(x^{(r_1)})$. Tomemos $C \neq C'$, entonces se tiene que $x \equiv x' \equiv 1 \bmod J$ pero $\operatorname{signo}(x) \neq \operatorname{signo}(x')$. Si ocurriese lo contrario x/x' sería totalmente positivo y $x\mathcal{O}_K = (x/x')\mathcal{O}_K x'\mathcal{O}_K \in x'\mathcal{O}_K\mathcal{P}r_{J+}$. Como la aplicación es inyectiva y los conjuntos a derecha son finitos, $\mathcal{P}r_J/\mathcal{P}r_{J+}$ es finito. ∎

1.3 El Grupo de Unidades

Unidades de un Cuerpo

Dos elementos de un anillo pueden generar el mismo ideal, en este caso se dice que son asociados, es decir, que se diferencian por la multiplicación de una unidad. Vamos a ver propiedades del grupo de las unidades de un cuerpo de números algebraico K de modo que podremos describir su estructura.

Proposición 1.3.1.1. Sea $c > 0$ y K un cuerpo de números algebraico. Entonces existen finitos $x \in \mathcal{O}_K$ tales que $|x^{(i)}| \leq c$ para todo i.

Demostración. Sea $n = [K : \mathbb{Q}]$ y $s_1, \dots s_n$ los polinomios simétricos elementales. Tomamos

$$c' = \text{máx}\left\{nc, \binom{n}{2}c^2, \dots, \binom{n}{n-1}c^{n-1}, c^n\right\}$$

Sea F el conjunto de polinomios mónicos de grado, a lo sumo, n con coeficientes enteros $|a| \leq c'$, F es un conjunto finito. Sea S e conjunto de las raíces de los polinomios de F, consideremos $x \in \mathcal{O}_K$ tal que $|x^{(i)}| \leq c$ para todo i. Entonces $|s_k(x^{(1)}, \dots, x^{(n)})| \leq c'$ para todo k. Como $s_k(x^{(1)}, \dots, x^{(n)}) \in \mathbb{Z}$, el polinomio $\prod(X - x^{(i)})$ está en F, luego $x \in S$.

Proposición 1.3.1.2. Sea $x \in \mathcal{O}_K$. x es una raíz de la unidad si y sólo si $|x^{(i)}| = 1$ para todo i.

Demostración. Si x es una raíz de la unidad, existe m tal que $x^m = 1$

$$|x^m| = 1 \Rightarrow |x|^m = 1 \Rightarrow |x^{(i)}|^m = 1 \ \forall i$$

Ahora, por la proposición anterior sabemos que existe un número finito de elementos $x \in \mathcal{O}_K$ tales que $|x^{(i)}| = 1$ para todo i.

Toda potencia de x cumple dicha propiedad, por lo que deben existir r, s tales que $x^r = x^s$. Como $x^{r-s} = 1$, x es una raíz de la unidad.

Notaremos como W al conjunto de unidades que son raíces de la unidad. Si h es el mayor de los ordenes de los elementos de W, el orden de cualquier elemento divide a h. Como el grupo de las raíces $h-$ésimas de la unidad es un grupo cíclico multiplicativo, W que es un subgrupo también lo es.

Sea $n = [K : \mathbb{Q}]$ de forma que $n = r_1 + 2r_2$ siendo r_1 el número de embeddings reales y r_2 las parejas de embeddings complejos, tomaremos $r = r_1 + r_2 - 1$. Sea U el grupo de las unidades de K, consideramos la aplicación

$$\lambda : U \to \mathbb{R}^r : u \to (\log|u^{(1)}|, \dots, \log|u^{(r)}|)$$

Proposición 1.3.1.3. Sea u una unidad. Entonces u es una raíz de la unidad si y sólo si $\lambda(u) = 0$

Demostración. Si $u \in W$, $|u^{(i)}| = 1$ para todo i, por lo que $\lambda(u) = 0$.

Por otro lado, sea $u \in U$ tal que $|u^{(i)}| = 1$ para $1 \leq i \leq r$. Como $\mathrm{N}_{K/\mathbb{Q}}(u) = 1$, $\sum_{i=1}^{n} \log|u^{(i)}| = 0$. Ahora, al ser $|u^{(r_1+i)}| = |u^{(r_1+r_2+i)}|$, del resto de relaciones obtenemos que $|u^{(i)}| = 1$ para todo $1 \leq i \leq n$, por lo que es una raíz de la unidad.

Tomemos $u_1, \dots, u_q \in U$ tales que $\lambda(u_1), \dots, \lambda(u_q)$ sean linealmente independientes en $\mathbb{R}^r$. Sea el grupo aditivo

$$G = \left\{ (a_1, \dots, a_q) \in \mathbb{R}^q | v \in U, \lambda(v) = \sum a_i \log |u_i| \right\}$$

Se tiene que $\mathbb{Z}^q \subset G$ y cada clase de G respecto a $\mathbb{Z}^q$ es un elemento de

$$G_1 = \left\{ (a_1, \dots, a_q) \in G | 0 \leq a_i < 1, v \in U, \lambda(v) = \sum a_i \log |u_i| \right\}$$

Proposición 1.3.1.4. El grupo $G/\mathbb{Z}^q$ es finito.

Demostración. Denotemos como $U_1 = \{v \in U | (a_1, \dots a_q) \in G_1)\}$. Sea $v \in U_1$ y dos elementos distintos de G_1 tales que

$$\lambda(v) = \sum a_i \log |u_i| = \sum b_i \log |u_i|$$

entonces

$$\sum (a_i - b_i) \log |u_i| = 0$$

por lo que la aplicación $U_1 \to G_1$ es inyectiva. Sea $v \in U_1$, entonces

$$|\log(v^{(i)})| = \left| \sum a_j \log |u_j^{(i)}| \right| \leq \sum |\log |u_j^{(i)}||$$

para todo $1 \leq i \leq r$. Sea $\alpha_i = \sum_j \log |u_j^{(i)}|$ y α su máximo, se tiene que $e^{-\alpha} \leq e^{-\alpha_i} \leq |v^{(i)}| \leq e^{\alpha_i} \leq \alpha$ para $1 \leq i \leq r$.

Como $1 = \mathrm{N}_{K/\mathbb{Q}}(v) = \prod |v^{(i)}|$ para todo $1 \leq i \leq n$ y además $|v^{(r_1+r_2)}|^2 = \left(\prod_{\substack{i \neq r_1+r_2, \\ i \neq r_1+2r_2}} |v^{(i)}| \right)^{-1}$,

existe $\beta > 0$ tal que $|v^{(i)}| < \beta$ para todo i. Por la proposición 1.3.1.1, U_1 es finito. ∎

Definición 1.3.1.5. *Sean $u_1 \dots, u_k$ unidades de $\mathcal{O}_K$, diremos que son independientes cuando para enteros m_i, la relación*

$$u_1^{m_1} \cdots u_k^{m_k} = 1$$

se cumple únicamente cuando todo $m_i = 0$.

Proposición 1.3.1.6. Sean $u_1 \dots u_k$ unidades en $\mathcal{O}_K$. Son equivalentes

(a) $u_1 \dots u_k$ son unidades independientes.

(b) $\lambda(u_1) \dots \lambda(u_k)$ son linealmente independientes sobre $\mathbb{Q}$.

(c) $\lambda(u_1) \dots \lambda(u_k)$ son linealmente independientes sobre $\mathbb{R}$

Demostración. • **(a)⇒ (b)**

Supongamos que $\lambda(u_1) \dots \lambda(u_k)$ son linealmente dependientes sobre $\mathbb{Q}$, entonces existen $n_j \in \mathbb{Z}$ tales que $\sum n_j \lambda(u_j) = 0$, por lo que $\prod u_j^{n_j}$ es una raíz de la unidad, por lo que existe $h \geq 1$ tal que $\prod u_j^{hn_j} = 1$, lo cual contradice **(a)**.

- **(b)⇒ (c)**

  Supongamos que $\lambda(u_1) \dots \lambda(u_k)$ son linealmente dependientes sobre $\mathbb{R}$. Sean los primeros q independientes, para $q < s \leq k$ tenemos que $\lambda(u_s) = \sum_{j=1}^{q} a_j \lambda(u_j)$. Por la proposición anterior, si $h = \#(G/\mathbb{Z}^q)$, $ha_j \in \mathbb{Z}$, por lo que $a_j \in \mathbb{Q}$, y llegamos a contradicción con **(b)**.

- **(c)⇒ (a)**

  Supongamos que $u_1 \dots u_k$ son linealmente dependientes, entonces existen enteros m_j, no todos nulos, tales que

  $$u_1^{m_1} \cdots u_k^{m_k} = 1$$

  Pero esto implicaría una contradicción con **(c)**.

Estructura del Grupo de Unidades

A continuación vamos a ver cual es la estructura del grupo de unidades y a definir otro de los invariantes del cuerpo de números K, el regulador. Demostraremos el Teorema de Dirichelt sobre la estructura del grupo de unidades en tres partes

Teorema 1.3.2.1 (Teorema de Dirichlet). *El grupo U de las unidades de un cuerpo de números algebraico K tiene la siguiente estructura*

$$U \cong W \times C_1 \times \cdots \times C_r$$

donde W es el grupo cíclico de las raíces de la unidad, y cada C_i es un grupo multiplicativo infinito. Entonces, si ξ es un generador de W y u_i un generador de C_i, un elemento $v \in U$ se puede expresar como $v = \xi^m u_1^{m_1} \cdots u_r^{m_r}$.

Demostración. Primero distinguiremos el caso trivial $r = 0$. Como $r = r_1 + r_2 - 1$, tenemos como posibilidades, $K = \mathbb{Q}$ si $r_1 = 1$ o $K = \mathbb{Q}(\sqrt{d})$ con $d < 0$ libre de cuadrados si $r_2 = 1$. Distinguimos dos casos.

Si $d \equiv 2, 3 \bmod 4$, su enteros son de la forma $x = a + b\sqrt{d}$. Si es una unidad, $\mathrm{N}_{K/\mathbb{Q}}(x) = |x|^2 = a^2 - b^2 d = 1$, cuyas soluciones son $a = \pm 1$, $b = 0$, y si $d = -1$ añadimos $a = 0$, $b = \pm 1$.

Si $d \equiv 1 \bmod 4$, sus enteros son de la forma $x = (a + b\sqrt{d})/2$. Una unidad de norma 1 cumple que $a^2 - b^2 d = 4$, lo cual es posible cuando $a = \pm 2$, $b = 0$, y en el caso en que $d = -3$, existen además las soluciones $a = \pm 1$, $b = \pm 1$.

En cualquier caso, el grupo de unidades es $U = W$.

- Parte 1: $U \cong W \times C_1 \times \cdots \times C_k$; $0 \leq k \leq r$

  Probaremos que U/W es un grupo libre multiplicativo de rango k. Si $U = W$, $k = 0$ tal y como hemos visto antes. En caso contrario existe $u \in U \setminus W$ y se pueden tomar $u_1, \ldots, u_k$ linealmente independientes y que sea conjunto maximal, con $1 \leq k \leq r$.

  Sea $G = \left\{(a_1, \ldots, a_k) \in \mathbb{R}^k | v \in U, \lambda(v) = \sum a_i \log |u_i|\right\}$, el cociente $G/\mathbb{Z}^k$ es un grupo finito por la proposición 1.3.1.4. Sea $h = \#(G/\mathbb{Z}^k)$. Sea F el subgrupo generado por $u_1, \ldots, u_k$ en U. F es un grupo abeliano libre sin torsión de rango k, sea $u \in U$, y se tiene que $u^h = \xi v$, donde $\xi \in W$ y $v \in F$.

  Veamos la afirmación anterior, si $u \in F$, $u^h = 1 \cdot u$. Si $u \notin F$, entonces $\{u, u_1, \ldots, u_k\}$ es linealmente dependiente, por lo que

  $$\lambda(u) = \sum_{i=1}^{k} b_i \lambda(u_i), \quad b_i \in \mathbb{Q}$$

  Sea $d > 1$ el menos entero tal que $d b_i \in \mathbb{Z}$ para todo i

  $$\lambda(u^d) = \sum_{i=1}^{k} d b_i \lambda(u_i), \quad d b_i \in \mathbb{Z}$$

  Por lo que d divide a h. Sea $v = \prod u_i^{h b_i}$, $\lambda(u^h) = \lambda(v)$, por tanto hay una raíz de la unidad en W tal que $u^h = \xi v$.

  Sea ξ_1 raíz del polinomio $X^h - \xi$, ξ_1^{wh} donde $w = \#W$. Sea t_i una raíz de $X^h - u_i$. Se tiene que $u^h = (\xi_1 \prod t_i^{h b_i})^h$, por lo que $u = \xi_2 \xi_1 \prod t_i^{h b_i}$ con $\xi_2^h = 1$.

Sea ξ_3 una raíz $hw-$ésima primitiva de la unidad. Sea U' generado por $\xi_3, t_1, \dots, t_k$, y W' generado por ξ_3.

$$W = W \cap U', \quad U/W = U/(W \cap U') \subset U'/W'$$

Como U'/W' es isomorfo al grupo libre generado por $\{t_i, \dots, t_k\}$, U/W tiene a lo sumo rango k, pero al ser linealmente independiente, su rango es exactamente k.

- Parte 2: Existencia de suficientes unidades

  Veremos que si $c_1, \dots, c_r$ son reales no todos nulos, entonces existe una unidad $u \in U$ tal que $\sum c_i \log |u^{(i)}| \neq 0$. Sea $\{\alpha_1, \dots, \alpha_n\}$ una base de K y $d^2 = d(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}$, se tiene que $1 < |d|$. Sea $\beta > 0$ suficientemente grande, por ejemplo, $\beta = \sum |c_i| \log |d| + 1$. Consideremos las siguientes n formas lineales

  $$L_i = \sum_{j=1}^{n} \alpha_j^{(i)} X_j$$

  Sean $\tau_1, \dots, \tau_n$ números reales tales que $\tau_{r_1+j} = \tau_{r_1+r_2+j}$, $1 \leq j \leq r_2$ y $\prod \tau_j = |d|$. Debe existir $y \in \mathcal{O}_K$ tal que $y^{(i)} = L_i(x_1, \dots, x_n) = \sum \alpha_j^{(i)} x_j$ tal que $|y^{(i)}| \leq \tau_i$ y se tiene que

  $$\frac{\tau_i}{|d|} \leq \frac{1}{\prod_{j \neq 1} \tau_j} \leq \frac{1}{\prod_{j \neq 1} \leq y^{(j)}} \leq |y^{(i)} \leq \tau_i \leq \tau_i |d|$$

  Si $F(y) = \sum c_i \log |y^{(i)}|$ deducimos que

  $$\left| F(y) - \sum c_i \log \tau_i \right| = \left| \sum c_i \log \frac{|y^{(i)}|}{\tau_i} \right| \leq \sum |c_i| \, |\log |d|| < \beta$$

  Consideremos a continuación para cada $h = 1, 2, \dots$ los números τ_{hi} del mismo modo que antes, y añadiendo la condición

  $$\sum c_i \log \tau_{hi} = 2\beta h$$

  Sean $y_h \in \mathcal{O}_K$ obtenidos del mismo modo por los τ_{hi},

  $$|F(y_h) - 2\beta h| = \left| F(y_h) - \sum c_i \log \tau_{hi} \right| < \beta \Rightarrow \beta(2h-1) < F(y_h) < \beta(2h+1)$$

  De donde $F(y_1) < F(y_2) < \cdots$. Como $\mathrm{N}_{K/\mathbb{Q}}(y_h) \leq |d|$, deben existir dos índices distintos $h \neq h'$ tales que $y_h \mathcal{O}_K = y_{h'} \mathcal{O}_K$, por lo tanto $u = y_{h'}/y_h$ es una unidad de K y se tiene que

  $$\sum c_i \log |u^{(i)}| = F(u) = F(y_{h'}) - F(y_h) \neq 0$$

- Parte 3: Construcción

  Tomemos $c_=1$ y el resto $c_j = 0$, entonces existe $u_1 \in U$ con $\log|u_1^{(1)}| \neq 0$. Sean ahora $c_1 = -\log|u_1^{(2)}|$, $c_2 = \log|u_1^{(1)}|$ y el resto $c_j = 0$, $\exists u_2 \in U$ tal que $c_1 \log|u_2^{(1)}| + c_2 \log|u_2^{(2)}| \neq 0$, es decir,

$$\begin{vmatrix} \log|u_1^{(1)}| & \log|u_2^{(1)}| \\ \log|u_1^{(2)}| & \log|u_2^{(2)}| \end{vmatrix} \neq 0$$

  Repitiendo el argumento con

$$c_1 = \begin{vmatrix} \log|u_1^{(2)}| & \log|u_2^{(2)}| \\ \log|u_1^{(3)}| & \log|u_2^{(3)}| \end{vmatrix}, \qquad c_2 = -\begin{vmatrix} \log|u_1^{(1)}| & \log|u_2^{(1)}| \\ \log|u_1^{(3)}| & \log|u_2^{(3)}| \end{vmatrix}$$

$$c_3 = \begin{vmatrix} \log|u_1^{(1)}| & \log|u_2^{(1)}| \\ \log|u_1^{(2)}| & \log|u_2^{(2)}| \end{vmatrix}$$

  Existe $u_3 \in U$ tal que $c_1 \log|u_3^{(1)}| + c_2 \log|u_3^{(2)}| + c_3 \log|u_3^{(3)}| \neq 0$, es decir,

$$\begin{vmatrix} \log|u_1^{(1)}| & \log|u_2^{(1)}| & \log|u_3^{(1)}| \\ \log|u_1^{(2)}| & \log|u_2^{(2)}| & \log|u_3^{(2)}| \\ \log|u_1^{(3)}| & \log|u_2^{(3)}| & \log|u_3^{(3)}| \end{vmatrix} \neq 0$$

  Podemos así determinar r unidades distintas en U, y como el determinante $\det(\log|u_j^{(i)}|) \neq 0$ se trata de un conjunto linealmente independiente, por lo que concluimos que $k = r$.

Definición 1.3.2.2 (Sistema Fundamental de Unidades). *Un conjunto $\{u_1, \dots, u_r\}$ de K se dice que es un sistema fundamental de unidades de K si cualquier unidad $u \in U$ se expresa de forma única como*

$$u = \xi^m u_1^{m_1} \cdots u_r^{m_r}$$

donde ξ es un generador de W, $1 \leq m \leq w$, $m_i \in \mathbb{Z}$.

Proposición 1.3.2.3. Sean $\{u_1, \dots, u_r\}$ y $\{v_1, \dots, v_r\}$ sistemas fundamentales de unidades, entonces

$$|\det(\log|u_j^{(i)}|)| = |\det(\log|v_j^{(i)}|)|$$

Demostración. Al ser ambos sistemas fundamentales podemos expresar para todo j

$$v_j = \xi^{a_j} u_1^{a_{1j}} \cdots u_r^{a_{rj}}; \quad u_j = \xi^{a'_j} v_1^{a'_{1j}} \cdots v_r^{a'_{rj}}$$

Por la unicidad de representación (a_{ij}) y (a'_{ij}) son inversas de coeficientes enteros, como $\det(a_{ij})\det(a'_{ij}) = 1$, se tiene que $|\det(a_{ij})|, |\det(a'_{ij})| = 1$. Como $\log|v_j| = \sum a_{ij} \log|u_j^{(i)}|$

$$|\det(\log|v_j^{(i)}|)| = |\det(a_{ij})||\det(\log|u_j^{(i)}|)| = |\det(\log|u_j^{(i)}|)|$$

Definición 1.3.2.4 (Regulador). *Sean $\{u_1, \dots, u_r\}$ un sistema fundamental de unidades de K, definimos el regulador como el invariante*

$$R = |\det(\log|u_j^{(i)}|)|$$

2 | Caracteres y Funciones Zeta

2.1 Caracteres y sumas gaussianas

En una extensión cuadrática, el símbolo de Legendre visualiza cuando un elemento es residuo cuadrático. Los caracteres cumplen esta función a la hora de observar los residuos de una cierta potencia, para lo que estudiaremos el caso concreto de los caracteres modulares. Necesitaremos familiarizarnos con las propiedades de los caracteres para ser capaces de operar con ellos.

Veremos que son elementos de la base de un espacio vectorial de funciones complejas y cómo se comportan respecto a la suma, ya que nos interesa saber lo que sucederá al considerar las series infinitas para el estudio posterior de L-series.

Grupos de Caracteres

Definición 2.1.1.1 (Carácter asociado a un grupo). *Sea G un grupo abeliano finito, un homomorfismo $\chi : (G, *) \to (\mathbb{C}^\times, \cdot)$ se llama un carácter de G.*

Puesto que es un homomorfismo podemos deducir que $\chi(a) \neq 0 \, \forall a \in G$, y $\chi(a * b) = \chi(a) \cdot \chi(b)$. De aquí se obtiene directamente, si $|G| = n$, que $\chi(G)$ es un subgrupo de las raíces n-ésimas de la unidad. Si e es el elemento neutro en G,

$$a^n = e \to (\chi(a))^n = \chi(a^n) = \chi(e) = 1$$

Notaremos $\widehat{G}$ al conjunto de los caracteres de G y definimos la operación multiplicativa entre sus elementos: $(\chi \cdot \chi')(a) = \chi(a) \cdot \chi'(a)$. Llamaremos carácter trivial a $\chi_0(a) = 1 \, \forall a \in G$.

Proposición 2.1.1.2. El conjunto $\widehat{G}$ de los caracteres de G es un grupo multiplicativo.

Demostración. Se puede comprobar sencillamente que la operación es interna y asociativa, además el grupo cuenta con un elemento neutro, el que hemos llamado carácter trivial χ_0. Nos falta la existencia de un elemento inverso único. Sean $a \in G$ y $\chi \in \widehat{G}$,

$$\chi(a)\chi^{-1}(a) = 1 = \chi(a)\overline{\chi(a)} \to \chi^{-1}(a) = \overline{\chi(a)}\ \forall a \in G$$

A este elemento inverso le llamaremos más normalmente como el carácter conjugado de χ, y lo notaremos $\overline{\chi}$.

Definición 2.1.1.3. *Sean G, H grupos abelianos finitos, y $\varphi : G \to H$ un homomorfismo. Definimos el homomorfismo entre grupos de caracteres, $\widehat{\varphi} : \widehat{H} \to \widehat{G}$, como $\widehat{\varphi}(\chi) = \chi \circ \varphi$.*

Como vemos, un homomorfismo entre grupos induce un homomorfismo entre los grupos de caracteres. Nos interesaría si un isomorfismo induce otro o la relación que tendría un grupo con sus subgrupos, ya que tenemos la siguiente sucesión exacta si $H \leq G$, i es la inclusión y q la aplicación cociente

$$1 \longrightarrow H \overset{i}{\hookrightarrow} G \overset{q}{\longrightarrow} G/H \longrightarrow 1$$

Esto induce los siguientes homomorfismos en los grupos de caracteres

$$\widehat{q} : \widehat{G/H} \to \widehat{G}, \quad \widehat{i} : \widehat{G} \to \widehat{H}$$

Si observamos el homomorfismo $\widehat{i}$, se trata de una restricción de los caracteres al subgrupo H, y su núcleo consiste de los caracteres que coinciden para las distintas clases de H, es decir, si $\chi \in \widehat{G}$ y $aH = bH$, entonces $\chi(a) = \chi(b)$.

Si pasamos al homomorfismo $\widehat{q}$ inducido por el cociente, éste es inyectivo, pues si $\widehat{q}(\tilde{\chi}) = \chi_0$, entonces $1 = \chi_0(a) = \widehat{q}(\tilde{\chi})(aH)$ para cualquier clase. Con ello se aprecia que $\widehat{q}(\widehat{G/H}) = \ker \widehat{i}$, y por tanto

$$\widehat{G}/\widehat{q}(\widehat{G/H}) = \widehat{G}/\ker \widehat{i} \cong \widehat{i}(\widehat{G}) \subset \widehat{H}$$

En los siguientes resultados podremos ver que la ultima inclusión es en verdad una igualdad y la relación entre un grupo y su grupo de caracteres.

Proposición 2.1.1.4. Sea G un grupo cíclico de orden n con generador a, y sea ζ una raíz $n-$ésima primitiva de la unidad. Entonces los caracteres en $\widehat{G}$ son $\chi_0, \dots, \chi_{n-1}$ donde

$$\chi_r(a^s) = \zeta^{rs}, \quad s = 1, \dots n\ r = 0, \dots n-1.$$

Es más $G \cong \widehat{G}$.

Demostración. Por un lado, cada una de las aplicaciones χ_r es un carácter en $\widehat{G}$ por su propia definición, y para $r \neq t$ se tiene que $\chi_r \neq \chi_t$ al ser ζ una raíz primitiva.

Por otro, sea $\chi \in \widehat{G}$, entonces $(\chi(a))^n = \chi(a^n) = 1$, por lo que $\chi(a) = \zeta^r$ para algún $r = 0, \dots, n-1$. Entonces $\chi(a^s) = (\chi(a))^s = \zeta^{rs} = \chi_r(a^s)$ para $s = 1, \dots, n$, con lo que vemos que $\chi = \chi_r$.

Como se puede observar, para cada generador $a \in G$ existe un isomorfismo $\psi_a : G \to \widehat{G}$ tal que $\psi_a(a^s) = \chi_s$. ∎

No todos los grupos abelianos son cíclicos, pero como es sabido, cualquier grupo abeliano puede expresarse como producto de grupos cíclicos.

Proposición 2.1.1.5. Si $\varphi : G \to \prod_{i=1}^r G_i$ es un isomorfismo de grupos, entonces este induce el isomorfismo entre los grupos de caracteres

$$\widehat{\varphi} : \widehat{G} \to \prod_{i=1}^r \widehat{G}_i$$

Demostración. Sean $\nu_i : G_i \to G$ definidas como $\nu_i(x_i) = \varphi^{-1}(1, \dots, x_i, \dots, 1)$, cada una es un isomorfismo a un subgrupo de G de la forma habitual.

Si $\chi \in \widehat{G}$ y llamamos $\chi_i = \widehat{\nu_i}(\chi)$ de forma que $\chi_i \in \widehat{G}_i$. Entonces podemos definir el homomorfismo

$$\widehat{\varphi} : \widehat{G} \to \prod_{i=1}^r \widehat{G}_i$$

tal que $\widehat{\varphi}(\chi) = (\chi_1, \dots, \chi_r)$. Éste es inyectivo, ya que si cada χ_i resulta ser el carácter trivial

$$\chi(x) = \chi\left(\prod_{i=1}^r \nu_i\big(\pi_i(\varphi(x))\big)\right) = \prod_{i=1}^r \chi_i\big(\pi_i(\varphi(x))\big) = 1, \ \forall x \in G.$$

Si tomamos ahora caracteres $\chi_i \in \widehat{G}_i$ y definimos $\chi(x) = \prod_{i=1}^r \chi_{(i)}\big(\pi_i(\varphi(x))\big)$ para cada $x \in G$. Entonces $\chi \in \widehat{G}$ y

$$\begin{aligned} \nu_i(\chi)(x_i) &= \prod_{j=1}^r \chi_{(j)}\big(\pi_j(\varphi \circ \nu_i(x_i))\big) \\ &= \prod_{j=1}^r \chi_{(j)}\big(\pi_j(1, \dots, x_i, \dots, 1)\big) = \chi_i(x_i), \ \forall x_i \in G_i. \end{aligned}$$

De este modo $\widehat{\varphi}(\chi) = (\chi_{(1)}, \dots, \chi_{(r)})$, lo que concluye que $\widehat{\varphi}$ es un isomorfismo de grupos.

Corolario 2.1.1.6. Sean G un grupo y $\widehat{G}$ su grupo de caracteres asociado, son isomorfos.

Demostración. Sea G un grupo tal que $G \cong \prod_{i=1}^{r} G_i$ sea una de sus descomposiciones en grupos cíclicos, entonces por las proposiciones 2.1.1.4 y 2.1.1.5 se tiene

$$\widehat{G} \cong \prod_{i=1}^{r} \widehat{G}_i \cong \prod_{i=1}^{r} G_i \cong G$$

Observación 2.1.1.7. Gracias a este último corolario podremos estudiar más fácilmente los caracteres modulares definidos a partir de un $\mathbb{Z}m$ y la descomposición canónica dada por el Teorema Fundamental de grupos abelianos finitos.

Corolario 2.1.1.8. Sea G un grupo de orden n y $H \leq G$ un subgrupo de orden m, entonces todo carácter $\chi' \in \widehat{H}$ admite n/m extensiones a caracteres de $\widehat{G}$.

Demostración. Tal y como teníamos al principio, sean $i : H \hookrightarrow G$ la inclusión y $q : G \to G/H$ la aplicación cociente. Hemos visto que $\widehat{i} : \widehat{G} \to \widehat{H}$ induce un isomorfismo $\widehat{G}/\widehat{q}(\widehat{G/H}) \cong \widehat{i}(\widehat{G}) \subset \widehat{H}$.

De lo ésto se deduce que

$$\frac{\#\widehat{G}}{\#\widehat{q}(\widehat{G/H})} = \#\widehat{i}(\widehat{G}) \leq \#\widehat{H},$$

pero por el corolario 2.1.1.6

$$\#\widehat{q}(\widehat{G/H}) \leq \#\widehat{G/H} = \#G/H = \frac{\#G}{\#H},$$

es decir,

$$\#H \leq \frac{\#\widehat{G}}{\#\widehat{q}(\widehat{G/H})} \leq \#\widehat{H} = \#H$$

Se puede ver entonces que $\widehat{i}(\widehat{G}) \cong \widehat{G}/\widehat{q}(\widehat{G/H}) \cong \widehat{H}$, por lo que todo carácter en $\widehat{H}$ es una restricción de un carácter en $\widehat{G}$ y, puesto que el núcleo de $\widehat{i}$ es $\widehat{q}(\widehat{G/H})$ con orden n/m, todo carácter de $\widehat{H}$ admite n/m extensiones hacia caracteres de $\widehat{G}$.

Si juntamos todo hasta ahora obtenemos que si

$$1 \longrightarrow H \overset{i}{\hookrightarrow} G \overset{q}{\longrightarrow} G/H \longrightarrow 1$$

es una sucesión exacta entonces

$$1 \to \widehat{G/H} \xrightarrow{\hat{q}} \widehat{G} \xrightarrow{\hat{i}} \widehat{H} \to 1$$

es también una sucesión exacta.

Para poder operar más adelante con los caracteres asociados a un grupo tanto en sumas finitas como en series vamos a ver cuál seria un sistema de generadores de $\widehat{G}$ y que se comportará como base del $\mathbb{C}-$espacio vectorial V de dimensión n donde definiremos el producto interno usual con su norma asociada.

De esta forma podremos resolver sistemas de ecuaciones lineales con caracteres de forma mucho más sencilla.

Lema 2.1.1.9. La evaluación en elementos de G, $\gamma : G \to \widehat{\widehat{G}}$ es un isomorfismo.

Demostración. Resulta de la aplicación directa del corolario 2.1.1.6. ∎

Observación 2.1.1.10. Puesto que la evaluación es un isomorfismo, podemos deducir que el grupo de caracteres asociados separa correctamente los elementos del grupo.

Proposición 2.1.1.11. Un elemento $a \in G$ es una potencia $k-$ésima si y sólo si $\chi(a) = 1$ para todo carácter cuyo orden divida a k.

Demostración. Sea $a = b^k$, si $\chi^k = \chi_0$ entonces

$$\chi(a) = \chi(b^k) = (\chi(b))^k = \chi^k(b) = \chi_0(b) = 1$$

Por otro lado, si consideramos el homomorfismo $q : G \to G/G^k$ y tomamos un carácter $\chi' \in \widehat{G/G^k}$, éste tiene orden k, ya que

$$(\hat{q}(\chi'))^k(x) = ((\chi' \circ q)(x))^k = (\chi'(xG^k))^k = \chi'(x^k G^k) = 1, \ \forall x \in G$$

Puesto que suponemos que $\hat{q}(\chi')(a) = 1$, se tiene $\chi'(aG^k) = 1$, lo que implica que $a \in G^k$. ∎

Proposición 2.1.1.12. El conjunto $\{\chi_1, \dots, \chi_s\}$ es un sistema generador de $\widehat{G}$ si y sólo si $\chi_i(a) = 1$ $\forall i$ implica que $a = e$.

Demostración. Si suponemos que $\{\chi_1, \dots, \chi_s\}$ es sistema generador y que $\chi_i(a) = 1$ para todo i entonces podemos escribir $\chi \in \widehat{G}$ como $\chi = \prod_{i=1}^{s} \chi_i^{t_i}$, y se tendrá que $\chi(a) = 1$ para todo χ. Puesto que, por el corolario 2.1.1.9, la evaluación es un isomorfismo, se deduce que $a = e$.

Pongamos ahora que $\widehat{H} \leq \widehat{G}$ es el subgrupo generado por $\{\chi_1, \dots, \chi_s\}$. Si consideramos el homomorfismo $q : \widehat{G} \to \widehat{G}/\widehat{H}$ y un carácter $\chi' \in \widehat{\widehat{G}/\widehat{H}}$ entonces $\chi' \circ q \in \widehat{\widehat{G}}$, y debe existir un elemento, por el mismo corolario, tal que $\gamma(a) = \gamma_a = \chi' \circ q$.

Puesto que $q(\chi_i) = \chi_i \widehat{H} = H$, entonces $\chi_i(a) = \gamma_a(\chi_i) = \chi' \circ q(\chi_i) = 1$ para todo i, esto implica que $a = e$, y por tanto que $\chi' \circ q(\chi) = 1$ para cualquier $\chi \in \widehat{G}$.

Como resultado, $\chi' = \chi_0$, y al tener $\widehat{\widehat{G}/\widehat{H}}$ un único elemento $\widehat{H} = \widehat{G}$. ∎

Los caracteres asociados a un grupo G de orden n conforman la base del espacio vectorial V de funciones complejas definidas en G y de dimensión n. En V podemos definir el siguiente producto interno

$$\langle f, g \rangle = \frac{1}{n} \sum_{a \in G} f(a)\overline{g(a)}$$

Proposición 2.1.1.13. Se tienen las siguientes propiedades:

(a) $\|\chi_i\| = 1$ y $\langle \chi_i, \chi_j \rangle = 0$ si $i \neq j$.

(b) $\langle \sum_{i=0}^{n-1} \alpha_i \chi_i, \chi_j \rangle = \alpha_j$ para $j = 1, \dots, n-1$ y $\alpha_i \in \mathbb{C}$.

(c) $\{\chi_0, \dots, \chi_{n-1}\}$ es una base de V.

Demostración. **(a)** Sea $\alpha = \langle \chi_i, \chi_0 \rangle$, entonces si $i = 0$

$$\alpha = \frac{1}{n} \sum_{a \in G} \chi_0(a) = 1,$$

si $i \neq 0$ entonces existe $b \in G$ tal que $\chi_i(b) \neq 0$, y se tiene

$$\alpha \chi_i(b) = \frac{1}{n} \sum_{a \in G} \chi_i(a)\chi_i(b) = \frac{1}{n} \sum_{a \in G} \chi_i(ab) = \alpha,$$

por tanto $\alpha = 0$. Si aplicamos ahora ésto a nuestro caso,

$$\langle \chi_i, \chi_j \rangle = \frac{1}{n} \sum_{a \in G} \chi_i(a)\overline{\chi_j(a)} = \langle \chi_i \chi_j^{-1}, \chi_0 \rangle$$

Entonces si $i = j$, $\|\chi_i\|^2 = \langle \chi_i, \chi_i \rangle = 1$, y si $i \neq j$ $\langle \chi_i, \chi_j \rangle = 0$.

(b) Por simple linealidad, y por el apartado anterior, se tiene que

$$\left\langle \sum_{i=0}^{n-1} \alpha_i \chi_i, \chi_j \right\rangle = \sum_{i=0}^{n-1} \alpha_i \langle \chi_i, \chi_j \rangle = \alpha_j$$

(c) Sea la combinación lineal $\sum_{i_0}^{n-1} \alpha_i \chi_i = 0$, entonces para cada $j = 0, \dots, n-1$ se tiene $\alpha_j = \left\langle \sum_{i_0}^{n-1} \alpha_i \chi_i, \chi_j \right\rangle = 0$. Ésto quiere decir que $\chi_0, \dots, \chi_{n-1}$ son linealmente independientes, y como el espacio V tiene dimensión n se trata de una base.

Corolario 2.1.1.14. Se tienen las siguientes propiedades de ortogonalidad:

(a) $$\sum_{a \in G} \chi_i(a) = \begin{cases} n, \text{ si, } i = 0, \\ 0, \text{ si, } i \neq 0 \end{cases}$$

(b) $$\sum_{a \in G} \chi_i(a)\overline{\chi_j}(a) = \begin{cases} n, \text{ si, } i = j, \\ 0, \text{ si, } i \neq j \end{cases}$$

(c) $$\sum_{i=0}^{n-1} \chi_i(a) = \begin{cases} n, \text{ si, } a = e, \\ 0, \text{ si, } a \neq e \end{cases}$$

(d) $$\sum_{i=0}^{n-1} \chi_i(a)\overline{\chi_i}(b) = \begin{cases} n, \text{ si, } a = b, \\ 0, \text{ si, } a \neq b \end{cases}$$

El siguiente resultado nos hará falta para probar el Teorema de Dirichlet, ya que necesitaremos separar los primos en sus distintas clases residuales primas.

Proposición 2.1.1.15. Sean $G = \{a_0, \dots, a_{n-1}\}$ y $\widehat{G} = \{\chi_0, \dots, \chi_{n-1}\}$, donde a_0 y χ_0 son las unidades de cada grupo. El sistema lineal de n ecuaciones

$$\frac{1}{n} \sum_{j=0}^{n-1} \chi_i(a_j) X_j = \beta_i, \quad \beta_i \in \mathbb{C}, \ i = 0, \dots, n-1$$

tiene solución única

$$x_j = \frac{1}{n} \sum_{i=0}^{n-1} \overline{\chi}_i(a_j)\beta_i, \quad j = 0, \dots, n-1$$

Demostración. Definamos la matriz $A = \left(\chi_i(a_j)\right)_{ij}$. Por las reglas de ortogonalidad se tiene que $A \cdot A^* = nI$, es decir, $\operatorname{rg}(A) = n$, por lo que tiene que tener solución única.

La inversa de la matriz $(1/\sqrt{n})A$ es $(1/\sqrt{n})A^*$. Sea $(x_0, \dots, x_{n-1})$ la solución, ha de cumplir la ecuación

$$\sum_{j=0}^{n-1} \frac{1}{\sqrt{n}} \chi_i(a_j) x_j = \frac{1}{\sqrt{n}} \beta_i, \quad i = 0, \dots, n-1$$

Si multiplicamos por la inversa

$$x_j = \sum_{i=0}^{n-1} \frac{1}{\sqrt{n}} \overline{\chi_i}(a_j) \frac{1}{\sqrt{n}} \beta_i = \frac{1}{n} \sum_{i=0}^{n-1} \overline{\chi_i}(a_j) \beta_i, \quad j = 0, \dots, n-1$$

Por último vamos definir el operador *shifting*, S_a, para cada $a \in G$ para elementos de V, tal que $S_a(f)(b) = f(ab)$. Es fácil ver que los autovectores de S_a son los caracteres χ de G con autovalor $\chi(a)$.

Ahora, para cada cualquier elemento de V podemos construir un nuevo operador

$$S_f := \sum_{a \in G} f(a) S_a,$$

de forma que tiene, de nuevo, autovectores $\chi \in \widehat{G}$

$$S_f(\chi)(b) = \sum_{a \in G} f(a) S_a(\chi)(b) = \left(\sum_{a \in G} f(a)\chi(a) \right) \chi(b),$$

con autovalores, en su caso, $\sum_{a \in G} f(a)\chi(a)$. Con esto podemos probar a continuación la siguiente relación

Proposición 2.1.1.16. Sea $f \in V$ entonces la norma del operador S_f es

$$\prod_{\chi \in \widehat{G}} \left(\sum_{a \in G} f(a)\chi(a) \right) = \det \left[\left(f(ba^{-1}) \right)_{a,b} \right]$$

Demostración. La norma de un operador lineal en un espacio de dimensión finita viene dada por su determinante, que es igual al producto de sus autovalores. Si $\{\chi_0, \dots, \chi_{n-1}\}$ es una base de V, entonces la norma de S_f es

$$\prod_{i=0}^{n-1} \left(\sum_{a \in G} f(a)\chi_i(a) \right)$$

Si realizamos el cambio a la base canónica (h_a) de V, donde

$$h_a(b) = \begin{cases} 1, & \text{si } b = a \\ 0, & \text{si } b \neq a \end{cases}$$

Entonces

$$\begin{aligned} S_f(h_b)(c) &= \sum_{a\in G} f(a)S_a(h_b)(c) = \sum_{a\in G} f(a)h_b(ac) \\ &= f(bc^{-1}) = \sum_{a\in G} f(ba^{-1})h_a(c) \end{aligned}$$

Vemos pues que $S_f(h_b) = \sum_{a\in G} f(ba^{-1})h_a$, así que la matriz respecto de la base canónica es $\left(f(ba^{-1})\right)_{a,b}$. Por tanto

$$\det\left[\left(f(ba^{-1})\right)_{a,b}\right] = \prod_{i=0}^{n-1}\left(\sum_{a\in G} f(a)\chi_i(a)\right)$$

Caracteres Modulares

Definición 2.1.2.1 (Carácter modular). *Sea $m > 1$ un entero. La aplicación$\chi : \mathbb{Z} \to \mathbb{C}$ se llama un carácter modular con módulo m si satisface*

(a) $\chi(a) = o$ *si y sólo si* $\gcd(a, m) \neq 1$

(b) *Si* $a \equiv b \bmod m$ *entonces* $\chi(a) = \chi(b)$

(c) $\chi(ab) = \chi(a)\chi(b)$

Proposición 2.1.2.2. Sea $m > 1$. Hay una correspondencia biyectiva entre caracteres modulares con módulo m y los caracteres del grupo multiplicativo $(\mathbb{Z}m)^\times$.

Demostración. Sea χ un carácter módulo m. Definimos $\tilde{\chi} : (\mathbb{Z}m)^\times \to \mathbb{C}$ como $\tilde{\chi}(\bar{a}) = \chi(a)$. $\tilde{\chi}$ es un carácter de $(\mathbb{Z}m)^\times$ bien definido.

Y si si partimos un carácter ρ de $(\mathbb{Z}m)^\times$, y definimos $\chi : \mathbb{Z} \to \mathbb{C}$ como

$$\chi(a) = \begin{cases} \rho(a), \text{ si, } \gcd(a, m) = 1 \\ 0, \text{ si, } \gcd(a, m) \neq 1 \end{cases}$$

esto concluye la prueba, ya que $\tilde{\chi} = \rho$.

Definición 2.1.2.3 (Conductor). *Sea $m > 1$ un entero, y sea χ un carácter módulo m. Consideramos el conjunto M_χ de enteros $m' \geq 1$ que cumplen que, si* $\gcd(a, m) = \gcd(b, m) = 1$ *y* $a \equiv b \bmod m'$, *entonces $\chi(a) = \chi(b)$. Cada elemento de M_χ se dice que es un módulo distintivo de χ, y al más pequeño se le llama conductor, notado f_χ.*

Proposición 2.1.2.4. El conjunto M_χ está formado por los múltiplos positivos del conductor de χ.

Demostración. Sea χ un carácter módulo m, y sean $m_1, m_2 \in M_\chi$ con $d = \gcd(m_1, m_2)$. Sean a, b tales que $\gcd(a, m) = \gcd(b, m)$ y $a \equiv b \bmod d$, llamemos m' al producto de todos los primos que aparecen en la descomposición de m pero no dividen a m_2, de manera que $\gcd(m'm_1, m_2) = d$, entonces el siguiente sistema tiene solución

$$\begin{cases} x \equiv a \bmod m'm_1 \\ x \equiv b \bmod m_2 \end{cases}$$

y cumple que $\gcd(x, m) = 1$, ya que de otro modo existiría un primo p que divida a x y a m, pero no a m_2 por ser $\gcd(b, m) = 1$. Entonces p dividiría a $m'm_1$, y por tanto a a, pero $\gcd(a, m) = 1$. Además se tiene que $\chi(a) = \chi(x) = \chi(b)$ por $m'm_1, m_2 \in M_\chi$. Con esto d cumple la definición de módulo distintivo de χ. Esto implica que M_χ está formado por múltiplos del conductor f_χ, ya que $\gcd(f_\chi, m) \in M_{chi} \forall m \in M_\chi$.

Corolario 2.1.2.5. El conductor de un carácter modular no puede ser 2.

Demostración. El resultado es sencillo, ya que en dicho caso debe tratarse del carácter modular trivial con conductor 1.

Definición 2.1.2.6 (Carácter primitivo). *Un carácter modular cuyo módulo coincide con su conductor recibe el nombre de carácter primitivo.*

Proposición 2.1.2.7. Sea χ un carácter módulo m con conductor f, existe un único carácter φ módulo f tal que si $\gcd(a, m) = 1$ entonces $\varphi = \chi$.

Demostración. Vamos a construir este carácter módulo f siguiendo la idea de la demostración 2.1.2.4.

Sea a tal que $\gcd(a, m) = 1$. Llamamos m' al producto de los primos que aparecen en m y no en f, de modo que podemos encontrar

$$\begin{cases} a' \equiv a \bmod f \\ a' \equiv 1 \bmod m' \end{cases}$$

Entonces, si $\gcd(b, m) = 1$ y $b \equiv a \bmod f$, $\chi(a') = \chi(b)$.

Definimos pues $\varphi(a) = \chi(a')$ cuando $\gcd(a, f) = 1$ y $\varphi(a) = 0$ en caso contrario, φ es un carácter módulo f bien definido y de conductor f.

Supongamos ahora que existe otro carácter φ' módulo f tal que si $\gcd(a', m) = 1$ se tiene que $\varphi'(a) = \chi(a')$, pero entonces es inmediato que $\varphi'(a) = \chi(a') = \varphi(a)$.

Proposición 2.1.2.8. χ es un carácter primitivo con conductor f si y sólo si para todo divisor $1 < d < f$, existe un entero tal que $\gcd(a, f) = 1$, $a \equiv 1 \bmod d$, y $\chi(a) \neq 1$.

Demostración. Supongamos que existe un carácter φ módulo d. Si $\gcd(a, f) = 1$ entonces $\varphi(a) = \chi(a)$, y si además $a \equiv 1 \bmod d$, $\chi(a) = \varphi(a) = \varphi(1) = 1$.

Por otro lado, asumamos que existe un divisor d de f tal que si $\gcd(a, f) = 1$ y $a \equiv 1 \bmod d$ entonces $\chi(a) = 1$, y definimos el carácter φ módulo d como $\varphi(b) = \chi(b)$, si $\gcd(b, f) = 1$.

Como hemos visto en la prueba de la proposición 2.1.2.7, si b es coprimo con d entonces podemos encontrar b' coprimo con f tal que $b' \equiv b \bmod d$. Definimos pues $\varphi(b) = \chi(b')$, ya que, si b', b'' son coprimos con f y $b', b'' \equiv b \bmod d$ existe $a \in \mathbb{Z}$ tal que $ab' \equiv b'' \bmod f$. De aquí $a \equiv 1 \bmod d$ y $\gcd(a, m) = 1$, y por hipótesis

$$\chi(b'') = \chi(ab') = \chi(a)\chi(b') = \chi(b)$$

Obtenemos de esto que φ es un carácter módulo d, y si $\gcd(b, f) = 1$ entonces $\chi(b) = \varphi(b)$, por lo que χ no sería un carácter primitivo módulo f. ∎

Proposición 2.1.2.9. Sea $m = m_1 \cdots m_r$, donde los m_i son coprimos dos a dos. Si χ es un carácter módulo m, entonces puede escribirse de la forma $\chi = \chi_1 \cdots \chi_r$, donde cada χ_i es un carácter módulo m_i. Además tenemos la relación $f = f_1 \cdots f_r$ para los conductores, y si χ es primitivo entones cada χ_i también lo es.

Demostración. Sea a tal que $\gcd(a, m) = 1$, podemos plantear el sistema

$$\begin{cases} a_i \equiv a \bmod m_i \\ a_1 \equiv 1 \bmod m_j, \ j \neq i \end{cases}$$

de forma que $\gcd(a_i, m) = 1$. Definimos el carácter módulo m_i como $\chi_i(a) = \chi(a_i)$ si $\gcd(a_i, m_i)$, y 0 en caso contrario. Así se cumple que, como $a = a_1 \cdots a_r$,

$$\chi(a) = \chi(a_1) \cdots \chi(a_r) = \chi_1(a) \cdots \chi_r(a)$$

Veamos que esta descomposición es única. Supongamos que $\chi = \chi_1' \cdots \chi_r'$ es otra forma de escribir el carácter y fijémonos en uno de los a_i calculados anteriormente, entonces

$$\chi_i'(a) = \chi_i'(a_i) = \chi_1(a_i) \cdots \chi_i'(a_i) \cdots \chi_r'(a_i) = \chi(a_i)\chi_i(a)$$

Para la segunda parte del enunciado, supongamos que d_i es un módulo distintivo de χ_i, y tomemos $d = d_1 \cdots d_r$. Sean a, b tales que $\gcd(a, m) = \gcd(b, m) = 1$ y $a \equiv b \bmod d$,

entonces se tiene que $a \equiv b \bmod d_i$ para todo i, por lo que $\chi_i(a) = \chi_i(b)$. Ésto implica que $\chi(a) = \chi(b)$.

Sea ahora d un módulo distintivo de χ que divida a m, llamemos $d_i = \gcd(d, m_i)$. Entonces $d = d_1 \cdots d_r$ y, si $\gcd(a, m) = \gcd(b, m) = 1$ y $a \equiv b \bmod d_i$, tomamos a_i, b_i como en las ecuaciones anteriores de forma que $a_i \equiv b_i \bmod d$, por lo que $\chi_i(a) = \chi(a_i) = \chi(b_i) = \chi_i(b)$.

Por último, si f_i es el conductor del carácter módulo m_i, resulta directo que $f = f_i \cdots f_r$ es el conductor de χ.

Sumas Gaussianas

Definición 2.1.3.1 (Suma Gaussiana). *Sea χ un carácter módulo m y sea $\zeta = e^{2\pi i/m}$ la raíz $m-$ésima de la unidad, definimos como*

$$\tau_k(\chi) = \sum_{a \in (\mathbb{Z}m)^\times} \chi(a)\zeta^{ak}$$

a la $k-$ésima suma Gaussiana asociada a χ.

Cuando $k = 1$ se dice que es la suma Gaussiana principal.

La suma principal es importante, ya que podemos expresar el resto en función de ésta.

Proposición 2.1.3.2. Sea χ un carácter módulo m y $1 \leq k < m$. Si $\gcd(k, m) = 1$ entonces

$$\tau_k(\chi) = \frac{1}{\chi(k)}\tau_1(\chi)$$

Además, cuando χ es un carácter primitivo y $\gcd(k, m) \neq 1$ se tiene $\tau_k(\chi) = 0$.

Demostración. Si $\gcd(k, m) = 1$ se tiene que $\chi(k) \neq 0$, y

$$\chi(k)\tau_k(\chi) = \sum_{a \in (\mathbb{Z}m)^\times} \chi(k)\chi(a)\zeta^{ak} = \sum_{b \in (\mathbb{Z}m)^\times} \chi(b)\zeta^{b} = \tau_1(\chi)$$

Sea ahora χ un carácter primitivo y sea $d = \gcd(k, m) > 1$ de forma que $m = dm'$, existe $b \in \mathbb{Z}$ tal que $\gcd(b, m) = 1$, $b \equiv 1 \bmod m'$ y $\chi(b) \neq 1$, por tanto $\zeta^{bk} = \zeta^k$, y nos queda

$$\tau_k(\chi) = \sum_{a \in (\mathbb{Z}m)^\times} \chi(a)\zeta^{ak} = \tau_k(\chi) = \sum_{a \in (\mathbb{Z}m)^\times} \chi(ab)\zeta^{abk} =$$
$$= \chi(b) \sum_{a \in (\mathbb{Z}m)^\times} \chi(a)\zeta^{ak} = \chi(b)\tau_k(\chi)$$

Siguiendo con las relaciones, vamos a implementar lo visto en la proposición 2.1.2.9 para descomponer las sumas Gaussianas.

Proposición 2.1.3.3. Sea $m = m_1 \cdots m_r$ donde los m_i son coprimos dos a dos. Sea χ un carácter módulo m y χ_i los caracteres módulo m_i que aparecen en su descomposición. Si notamos $m_i' = m/m_i$, y $\zeta_i = \zeta^{m_i'} = e^{2\pi i/m_i}$ entonces

$$\tau_1(\chi) = \prod_{i=1}^{r} \chi_i(m_i')\tau_i(\chi_i)$$

Demostración. Sea a con $\gcd(a, m) = 1$, planteamos el sistema

$$\begin{cases} a_i \equiv a \bmod m_i \\ a_1 \equiv 1 \bmod m_j, \ j \neq i \end{cases}$$

de forma que obtenemos la descomposición habitual $\chi(a) = \chi_1(a_1) \cdots \chi_r(a_r)$. Por otro lado, ya que $\gcd(m_i, m_i') = 1$ podemos encontrar b_i tal que $b_i m_i' \equiv 1 \bmod m_i$, entonces $a = \sum_{i=1}^{r} b_i m_i' a_i$, por tanto

$$\tau_1(\chi) = \sum_{a \in (\mathbb{Z}m)^\times} \chi(a)\zeta^a = \prod_{i=1}^{r} \left(\sum_{a_i \in (\mathbb{Z}m_i)^\times} \chi_i(a_i)\zeta_i^{b_i a_i} \right)$$

Si desarrollamos el paréntesis

$$\sum_{a_i \in (\mathbb{Z}m_i)^\times} \chi_i(a_i)\zeta_i^{b_i a_i} = \chi_i(b_i m_i') \sum_{a_i \in (\mathbb{Z}m_i)^\times} \chi_i(a_i)\zeta_i^{b_i a_i} =$$
$$\chi_i(m_i') \sum_{a_i \in (\mathbb{Z}m_i)^\times} \chi_i(b_i a_i)\zeta_i^{b_i a_i} = \chi_i(m_i')\tau_i(\chi_i)$$

de donde deducimos que

$$\tau_1(\chi) = \prod_{i=1}^{r} \left(\sum_{a_i \in (\mathbb{Z}m_i)^\times} \chi_i(a_i)\zeta_i^{b_i a_i} \right) = \prod_{i=1}^{r} \chi_i(m_i')\tau_i(\chi_i)$$

∎

Proposición 2.1.3.4. Sea χ un carácter primitivo con conductor p^v, entonces se tiene que $|\tau_1(\chi)|^2 = p^v$.

Demostración. Si desarrollamos el primer miembro nos queda

$$\overline{\tau_1(\chi)}\tau_1(\chi) = \left(\sum_{a \in (\mathbb{Z}p^v)^\times} \overline{\chi(a)}\zeta^{-a} \right) \left(\sum_{b \in (\mathbb{Z}p^v)^\times} \chi(b)\zeta^b \right) = \sum_{a \in (\mathbb{Z}p^v)^\times} \sum_{b \in (\mathbb{Z}p^v)^\times} \overline{\chi(a)}\chi(b)\zeta^{b-a}$$

Puesto que $a, b \in (\mathbb{Z}p^v)^\times$ podemos encontrar t tal que $b \equiv at \bmod p^v$

$$\overline{\tau_1(\chi)}\tau_1(\chi) = \sum_{t\in(\mathbb{Z}p^v)^\times}\sum_{a\in(\mathbb{Z}p^v)^\times}\chi(t)\zeta^{a(t-1)} = \sum_{t\in(\mathbb{Z}p^v)^\times}\chi(t)\left(\sum_{a\in(\mathbb{Z}p^v)^\times}\zeta^{a(t-1)}\right)$$
$$= \sum_{t\in(\mathbb{Z}p^v)^\times}\chi(t)\left(\sum_{a=1}^{p^v}\zeta^{a(t-1)} - \sum_{c=1}^{p^{v-1}}\zeta^{pc(t-1)}\right)$$

Por inducción en v es fácil probar que

$$\sum_{a=1}^{p^v}\zeta^{a(t-1)}\begin{cases}p^v, \text{ si } t=1\\ 0, \text{ en otro caso}\end{cases} \qquad \sum_{c=1}^{p^{v-1}}\zeta^{pc(t-1)}\begin{cases}p^{v-1}, \text{ si } t\equiv 1 \bmod p^{v-1}\\ 0, \text{ en otro caso}\end{cases}$$

Hemos de distinguir casos según cual sea el conductor del carácter χ, en ambos haremos uso de la proposición 2.1.1.4 para expresarlos. Notemos $\zeta_r^s = e^{2\pi is/r}$.

Cuando $p = 2$ y $v \geq 2$, el grupo de unidades puede expresarse como $\{1,-1\}\times\mathbb{Z}2^{v-2}$. Aquí podemos expresar $t \equiv (-1)^\alpha 5^\beta \bmod 2^v$, donde $\alpha = 0, 1$ y $0 \leq \beta < 2^{v-2}$. Como ha de cumplirse que $t \equiv 1 \bmod 2^{v-1}$, sólo hay dos soluciones. Si $v = 2$, $t = 1, 3$, y si $v > 2$, $\alpha = 0$ y $\beta = 0, 2^{v-3}$

$$\sum_{t\in(\mathbb{Z}2^v)^\times}\chi(t)\sum_{c=1}^{2^{v-1}}\zeta^{2c(t-1)} = 2^{v-1}\sum_{\substack{t\in(\mathbb{Z}2^v)^\times\\ t\equiv 1 \bmod 2^{v-1}}}\chi(t) = \begin{cases}\text{si } v=2,\ 2^{v-1}(1-1)=0\\ \text{si } v\neq 2,\ 2^{v-1}(1+\zeta_{2^{v-2}}^{2^{v-3}})=0\end{cases}$$

Ahora si $p > 2$, el grupo de unidades se comporta como $\mathbb{Z}(p-1)\times\mathbb{Z}p^{v-1}$ y podemos representar $t \equiv b^\alpha(1+p)^\beta$ con $1 \leq \alpha < p$, $1 \leq \beta < p^{v-1}$. Aquí la congruencia que debemos resolver nos da p soluciones cuando $\alpha = 0$ y $\beta = kp^{v-2}$, $0 \leq k < p$

$$\sum_{t\in(\mathbb{Z}p^v)^\times}\chi(t)\sum_{c=1}^{p^{v-1}}\zeta^{pc(t-1)} = p^{v-1}\sum_{\substack{t\in(\mathbb{Z}p^v)^\times\\ t\equiv 1 \bmod p^{v-1}}}\chi(t) = p^{v-1}\sum_{k=0}^{p-1}\zeta_{p^{v-1}}^{kp^{v-2}} = 0$$

Por lo que en cualquier caso nos quedamos con que

$$|\tau_1(\chi)|^2 = \sum_{t\in(\mathbb{Z}p^v)^\times}\chi(t)\sum_{a=1}^{p^v}\zeta^{a(t-1)} = p^e$$

Visto ésto podemos dar el siguiente resultado.

Corolario 2.1.3.5. Sea χ un carácter primitivo con conductor f entonces tenemos $|\tau_1(\chi)|^2 = f$.

Demostración. El conductor f lo podemos descomponer en su producto de primos, siendo $f = p_1^{v_1} \cdots p_r^{v_r}$, lo que nos da la expresión $\chi = \chi_1 \cdots \chi_r$, donde cada χ_i es un carácter primitivo con conductor $p_i^{v_i}$. Haciendo uso de las proposiciones 2.1.3.3 y 2.1.3.4

$$|\tau_1(\chi)|^2 = \left|\prod \tau_i(\chi)\right|^2 = \prod p_i^{v_i} = f$$

2.2 Funciones Zeta y $L-$Series

Series de Dirichlet

Un resultado bien conocido en teoría de números es la prueba de Euler para la existencia de infinitos primos en la que expresó la suma asociada a la función Zeta de Riemann evaluada en 1 como un producto

$$\sum_{n=1}^{\infty} \frac{1}{n} = \prod_{p \in P} \frac{1}{1 - 1/p}$$

Entonces, por reducción al absurdo, si se supone que existen finitos primos, el miembro derecho sería acotado, pero a la izquierda tenemos la serie armónica.

Con el estudio de las funciones multiplicativas conseguimos expresar también la función Zeta como producto de Euler. A nosotros nos interesa en este trabajo saber cómo afecta cambiar la sucesión constantemente 1 en el numerador por otra cualquiera, $\{a_n\}$, de números complejos.

Definición 2.2.1.1 (Serie de Dirichlet). *Sea $s > 0$ y $\{a_n\}$ una sucesión de números complejos, definimos la serie de Dirichlet asociada como*

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

Al igual que conocemos el dominio de convergencia para la función Zeta, deberemos conocer qué valores de s son válidos para estas series, nos restringiremos en todo caso a valores reales.

Proposición 2.2.1.2. Sea $\{a_n\}$ una sucesión de números primos y $S(m) = a_1 + \cdots + a_m$ sus sumas parciales. Si existe $s_0 > 0$ y un número real $\alpha > 0$ tales que

$$\left|\frac{S(m)}{m^{s_0}}\right| < \alpha, \quad \forall m \geq 1$$

entonces para todo $\delta > 0$, la serie de Dirichlet asociada a $\{a_n\}$ converge uniformemente en el intervalo $[s_0 + \delta, +\infty)$ y define una función continua en $(s_0, +\infty)$.

Demostración. Tomemos $s \geq s_0 + \delta$, entonces

$$\begin{aligned}
\left|\sum_{n=m}^{m+h} \frac{a_n}{n^s}\right| &= \left|\sum_{n=m}^{m+h} \frac{S(n) - S(n-1)}{n^s}\right| \\
&= \left|\frac{S(m+h)}{(m+h)^s} - \frac{S(m-1)}{m^s} + \sum_{n=m}^{m+h-1} S(n)\left(\frac{1}{n^s} - \frac{1}{(n-1)^s}\right)\right| \\
&\leq \left|\frac{S(m+h)}{(m+h)^s}\right| + \left|\frac{S(m-1)}{m^s}\right| + \sum_{n=m}^{m+h-1} |S(n)|\left(\frac{1}{n^s} - \frac{1}{(n-1)^s}\right) \\
&\leq \frac{\alpha(m+h)^{s_0}}{(m+h)^s} + \frac{\alpha(m-1)^{s_0}}{m^s} + \alpha s \sum_{n=m}^{m+h-1} n^{s_0} \int_n^{n+1} \frac{dx}{x^{s+1}} \\
&\leq \frac{2\alpha}{m^{s-s_0}} + \alpha s \int_m^{\infty} \frac{dx}{x^{s-s_0+1}} = \frac{2\alpha}{m^{s-s_0}} + \frac{\alpha s}{s - s_0}\frac{1}{m^{s-s_0}}
\end{aligned}$$

y puesto que la función $s/(s - s_0)$ es decreciente, nos queda que

$$\left|\sum_{n=m}^{m+h} \frac{a_n}{n^s}\right| \leq \frac{2\alpha}{m^{\delta}} + \frac{\alpha(s_0 + \delta)}{\delta}\frac{1}{m^{\delta}}$$

Como esta acotación es independiente de s y al incrementar m tiende a 0, el resto de la serie también lo hace, es decir, que la serie de Dirichlet converge uniformemente en $[s_0 + \delta, +\infty)$, lo que implica que la serie define una función continua en $(s_0, +\infty)$. ∎

El siguiente lema es un resultado conocido sobre la función Zeta de Riemann que nos ayudará a acotar también las series de Dirichlet.

Lema 2.2.1.3. Cuando $s \to 1^+$ se tiene que

$$\lim_{s \to 1^+} (s-1)\zeta(s) = 1$$

Demostración. Para $1 < s$ tenemos las desigualdades

$$\int_n^{n+1} \frac{dx}{x^s} \leq \frac{1}{n^s} \leq \int_{n-1}^{n} \frac{dx}{x^s}$$

Si aplicamos el sumatorio desde $n = 1$, teniendo cuidado en el último miembro en el que sumamos desde $n = 2$ y añadimos el valor equivalente en el miembro central

$$\int_1^{\infty} \frac{dx}{x^s} < \sum_{n=1}^{\infty} \frac{1}{n^s} < 1 + \int_1^{\infty} \frac{dx}{x^s}$$

$$\frac{1}{s-1} < \zeta(s) < \frac{s}{s-1}$$

$$1 < (s-1)\zeta(s) < s$$

de dónde se deduce claramente el resultado al hacer tender s hacia 1^+. ∎

Observación 2.2.1.4. En este caso hemos comparado el comportamiento asintótico de las dos funciones. Si el límite anterior entre ellas es finito, entonces podemos usar la notación de Landau cuando $s \to 1^+$ para decir que son aproximadas una de la otra

$$f(x) = O(g(x)) \Leftrightarrow f(x) \approx Cg(x)$$

De esta última forma es como lo expresaremos.

Proposición 2.2.1.5. Sea $\{a_n\}$ una sucesión de números complejos y $S(m)$ sus sumas parciales. Si se tiene que

$$\lim_{m\to\infty} \frac{S(m)}{m} = c$$

Entonces la serie de Dirichlet es convergente para $s > 1$ y, además

$$\lim_{s\to 1^+} (s-1) \sum_{n=1}^{\infty} \frac{a_n}{n^s} = c$$

Demostración. Que la serie sea convergente lo tenemos por la proposición anterior directamente cuando $s_0 = 1$. Ahora, como $\lim_{m\to\infty} \frac{S(m)}{m} = c$ podemos escribir $S(m) = cm + v(m)m$, donde $\lim_{m\to\infty} v(m) = 0$.

Consideramos $s > 1$ y tomamos $S(0) = 0$. Podemos desarrollar la siguiente diferencia

$$\begin{aligned}\left|\sum_{n=1}^{\infty}\frac{a_n - c}{n^s}\right| &= \left|\sum_{n=1}^{\infty}\frac{S(n)-S(n-1)}{n^s} - c\sum_{n=1}^{\infty}\frac{n-(n-1)}{n^s}\right| \\ &= \left|\sum_{n=1}^{\infty} S(n)\left(\frac{1}{n^s}-\frac{1}{(n+1)^s}\right) - c\sum_{n=1}^{\infty} n\left(\frac{1}{n^s}-\frac{1}{(n+1)^s}\right)\right| \\ &= \left|\sum_{n=1}^{\infty} v(n)n\left(\frac{1}{n^s}-\frac{1}{(n+1)^s}\right)\right| = \left|s\sum_{n=1}^{\infty} v(n)n\int_n^{n+1}\frac{dx}{x^{s+1}}\right| \\ &\leq s\sum_{n=1}^{\infty}|v(n)|\int_n^{n+1}\frac{dx}{x^{s+1}}\end{aligned}$$

Ahora bien, como $\lim_{n\to\infty} v(n) = 0$, existe $\beta > 0$ tal que $|v(n)| \leq \beta$ para todo n, entonces

$$\begin{aligned}\left|(s-1)\sum_{n=1}^{\infty}\frac{a_n - c}{n^s}\right| &\leq s(s-1)\sum_{n=1}^{\infty}|v(n)|\int_n^{n+1}\frac{dx}{x^{s+1}} \\ &\leq \beta(s-1)\int_1^{\infty}\frac{s\,dx}{x^{s+1}} = \beta(s-1)\end{aligned}$$

evidentemente al hacer tender $s \to 1^+$ vemos que la diferencia se hace cero, por lo que usando el lema anterior

$$\lim_{s\to 1^+}(s-1)\sum_{n=1}^{\infty}\frac{a_n}{n^s} = \lim_{s\to 1^+}(s-1)c\sum_{n=1}^{\infty}\frac{1}{n^s} = c$$

Proposición 2.2.1.6. Sea f una función multiplicativa. Si la serie $\sum_{n=1}^{\infty} f(n)$ es absolutamente convergente, entonces podemos expresarla como producto de Euler y éste es también absolutamente convergente

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

Demostración. Puesto que la serie es absolutamente convergente, entonces otra con menos términos también lo será $\sum_{p\in P}|f(p)| \leq \sum_{n=1}^{\infty}|f(n)|$ Esta condición es necesaria y suficiente para que el producto sea absolutamente convergente

$$\prod_{p\in P}(1-f(p)) = \alpha \neq 0$$

por lo que directamente

$$\prod_{p\in P}\frac{1}{1-f(p)}$$

es absolutamente convergente.

Vamos a llamar P_m a los primos menores a m, y $\mathbb{N}_m$ a los números naturales resultantes de multiplicar los elementos de P_m. Para cada primo se tiene que

$$\sum_{n=1}^{\infty} f(n) \geq \sum_{k=0}^{\infty} f(p^k) = \sum_{k=0}^{\infty} f(p)^k = \frac{1}{1-f(p)}$$

entonces

$$\prod_{p\in P_m}\frac{1}{1-f(p)} = \prod_{p\in P_m}\sum_{k=0}^{\infty} f(p^k) = \sum_{n\in\mathbb{N}_m} f(n)$$

Tomando límite cuando m tiende a infinito obtenemos el resultado que queríamos. ▮

L-Series

Ahora que hemos visto el funcionamiento de las series de Dirichlet nos vamos a centrar en el caso particular de las $L-$series en las que la sucesión que acompañaba a la Zeta de Riemann ahora serán los caracteres modulares que hemos estudiado en la sección anterior. Con ésto conseguiremos una base teórica que querremos expandir a dominios de Dedekind.

Definición 2.2.2.1 ($L-$Serie de un carácter). *Sea χ un carácter modular, definimos la $L-$serie asociada a χ para $s>1$ como la función*

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

Como los términos conforman una función multiplicativa también tenemos la expresión

$$L(s|\chi) = \prod_{p\in P}\frac{1}{1-\chi(p)/p^s}$$

Proposición 2.2.2.2. Si χ es un carácter módulo m no trivial, entonces $L(s|\chi)$ es una función continua para $s>0$.

Demostración. Tomemos la sucesión $a_n=\chi(n)$. Sea $R=km+r$, entonces

$$\left|\sum_{n=1}^{R}\chi(n)\right| = \left|\sum_{n=1}^{r}\chi(n)\right| \leq \sum_{n=1}^{r}|\chi(n)| = \varphi(m)$$

es decir, que la serie está uniformemente acotada. Si llamamos $f_n(s) = n^{-s}$, nos encontramos con una sucesión de funciones monótona decreciente y uniformemente convergente a 0 en $(0, +\infty)$. Por el test de convergencia de Abel podemos decir que $L(s|\chi)$ converge uniformemente en el intervalo $(0, +\infty)$ y es una función continua.

Por la expresión como producto de Euler, tomando el carácter trivial χ_0 se tiene que

$$L(s|\chi_0) = \prod_{p\in P} \frac{1}{1-\chi_0(p)/p^s} = \zeta(s) \prod_{p|m} 1 - 1/p^s$$

Proposición 2.2.2.3. Sea χ un carácter módulo m. Entonces para $s \to 1^+$

$$\log L(s|\chi) \approx \sum_{p\in P} \frac{\chi(p)}{p^s}$$

Demostración. Para $s > 1$ se tiene que

$$L(s|\chi) = \prod_{p\in P} \frac{1}{1-\chi(p)/p^s}$$

Tomando logaritmos

$$\log L(s|\chi) = \log \prod_{p\in P} \frac{1}{1-\chi(p)/p^s} = \sum_{p\in P} \log \frac{1}{1-\chi(p)/p^s}$$

Cuando $|x| < 1$ tenemos la siguiente expresión para el logaritmo

$$\log \frac{1}{1-x} = \sum_{n=1}^{\infty} \frac{x^n}{n}$$

aplicado ésto a nuestro caso

$$\log L(s|\chi) = \sum_{p\in P} \log \frac{1}{1-\chi(p)/p^s} = \sum_{p\in P} \sum_{v=1}^{\infty} \frac{1}{v} \frac{\chi(p^v)}{p^{vs}} = \sum_{p\in P} \frac{\chi(p)}{p^s} + \sum_{p\in P} \sum_{v=2}^{\infty} \frac{1}{v} \frac{\chi(p^v)}{p^{vs}}$$

Trabajaremos con este segundo término cuando s tiende a 1 por la derecha

$$\begin{aligned}\left|\sum_{p\in P} \sum_{v=2}^{\infty} \frac{1}{v} \frac{\chi(p^v)}{p^{vs}}\right| &\leq \frac{1}{2} \sum_{p\in P} \sum_{v=2}^{\infty} \frac{1}{p^{vs}} = \frac{1}{2} \sum_{p\in P} \frac{1/p^{2s}}{1-1/p^s} \\ &< \sum_{p\in P} \frac{1}{p^{2s}} \leq \sum_{p\in P} \frac{1}{p^2} < \zeta(2)\end{aligned}$$

de dónde vemos que

$$\left|\log L(s|\chi) - \sum_{p\in P}\frac{\chi(p)}{p^s}\right| = \left|\sum_{p\in P}\sum_{v=2}^{\infty}\frac{1}{v}\frac{\chi(p^v)}{p^{vs}}\right| < \zeta(2)$$

Al mantenerse acotada la diferencia entre ambas para todo $s > 1$, se deduce el resultado.

Proposición 2.2.2.4. Si χ no es el carácter trivial entonces

$$L(s|\chi) = \frac{1}{m}\sum_{k=0}^{m-1}\tau_k(\chi)\sum_{n=1}^{\infty}\frac{\zeta^{-nk}}{n^s}$$

Demostración. Por simple definición se tiene que para $s > 0$

$$L(s|\chi) = \sum_{n=1}^{\infty}\frac{\chi(n)}{n^s} = \sum_{a\in(\mathbb{Z}p)^\times}\chi(a)\sum_{n\equiv a \bmod m}\frac{1}{n^s}$$

Tomando $b_n = 1$ si $n \equiv a \bmod m$ y 0 en caso contrario, y conociendo que

$$\sum_{k=0}^{m-1}\zeta^{(n-a)k} = \begin{cases} m, \text{ cuando } n \equiv a \bmod m \\ 0, \text{ en otro caso} \end{cases}$$

podemos escribir que

$$b_n = \frac{1}{m}\sum_{k=0}^{m-1}\zeta^{(n-a)k}$$

por lo que

$$\begin{aligned} L(s|\chi) &= \sum_{a\in(\mathbb{Z}m)^\times}\chi(a)\sum_{n=1}^{\infty}\frac{b_n}{n^s} = \sum_{a\in(\mathbb{Z}m^\times}\chi(a)\sum_{n=1}^{\infty}\frac{1}{m}\sum_{k=0}^{m-1}\frac{\zeta^{(a-n)k}}{n^s} \\ &= \frac{1}{m}\sum_{k=0}^{m-1}\sum_{a\in(\mathbb{Z}m)^\times}\chi(a)\zeta^{ak}\sum_{n=1}^{\infty}\frac{\zeta^{-nk}}{n^s} = \frac{1}{m}\sum_{k=0}^{m-1}\tau_k(\chi)\sum_{n=1}^{\infty}\frac{\zeta^{-nk}}{n^s} \end{aligned}$$

Función Zeta de Dedekind

Vamos a dar el último paso antes de llegar al objetivo de este trabajo, necesitamos generalizar los resultados anteriores en un cuerpo de números K. Para ello vamos a expresarlo en función de ideales en el anillo de enteros de K usando la norma definida en 1.2.1.3 y veremos que todo coincide en el caso $K = \mathbb{Q}$.

Desarrollaremos de forma análoga las funciones Zeta de Dedekind y los caracteres de Hecke con su $L-$serie asociada, y la parte más esencial será trasladar la proposición 2.2.1.5.

Definición 2.2.3.1 (Serie Zeta de Dedeiknd). *Sea K un cuerpo de números algebraico, definimos su serie Zeta de Dedekind como*

$$\sum_{m=1}^{\infty} \frac{\nu(m)}{m^s}$$

donde $s > 1$ y $\nu(m) = \#\{I \in \mathcal{O}_K | \mathrm{N}_{K/\mathbb{Q}}(I) = m\}$.

Para ver la convergencia de esta serie y que define una función continua en $(1, +\infty)$ vamos a estudiar un poco la serie

$$\sigma(t) = \sum_{m=1}^{\lfloor t \rfloor} \nu(m)$$

Esta suma podemos restringirla a una de las clases de ideales en K, y la pregunta que nos hacemos es si el límite $\sigma(t, C_i)/t$ es independiente de la clase C_i escogida.

Sea $n = r_1 + 2r_2$ el grado de extensión de K, recordemos que r_1 son los $K^{(j)}$ cuerpos reales conjugados a $K = K^{(1)}$ y los siguientes $2r_2$ son los conjugados complejos. Sea $x \in K$ y $\{\alpha_1, \dots, \alpha_n\}$ una base de K, podemos expresar los conjugados de x

$$x^{(j)} = \sum_{k=1}^{n} y_k \alpha_k^{(j)}$$

para y_k números reales fijos. Si $\{u_1, \dots, u_r\}$ es un sistema fundamental de las unidades de $\mathcal{O}_K$, $l_i = 1$ si $1 \leq i \leq r_1$ y $l_i = 2$ cuando $r_1 < i \leq r_1 + r_2$, y sea el regulador $R = |\det(l_i \log |u_j^{(i)}|)_{ij}| \neq 0$, entonces los exponentes a_k de x cumplen las relaciones

$$\log \left| \frac{x^{(j)}}{|x^{(1)} \cdots x^{(n)}|} \right| = \sum_{k=1}^{r=r_1+r_2-1} a_k \log |u_k^{(j)}|$$

En el caso en que ξ sea una unidad se tiene que $\xi = \zeta u_1^{m_1} \cdots u_r^{m_r}$ con ζ una raíz de la unidad y los m_k enteros.

Con ésto podemos plantear el siguiente resultado.

Proposición 2.2.3.2. Sea K un cuerpo de números algebraico. Para toda clase de ideales C se tiene

$$\lim_{t\to\infty} \frac{\sigma(t, C)}{t} = L < +\infty$$

Demostración. Sea J un ideal íntegro de la clase C^{-1}, para todo $t \geq 1$ tenemos una correspondencia entre los conjuntos

$$\begin{cases} \varepsilon_t = \{I \in C | I \text{ es íntegral}, \mathrm{N}_{K/\mathbb{Q}}(I) \leq t\} \\ \varepsilon'_t = \{x\mathcal{O}_K | 0 \neq x\mathcal{O}_K \subset J, |\mathrm{N}_{K/\mathbb{Q}}(x)| \leq \mathrm{N}_{K/\mathbb{Q}}(J)\, t\} \end{cases}$$

Dado $I \in C$, un ideal íntegro con $\mathrm{N}_{K/\mathbb{Q}}(I) \leq t$. $IJ \in CC^{-1}$ que es la clase de los ideales principales, por lo que $IJ = x\mathcal{O}_K$ con $x \in IJ \subset J$, además

$$|\mathrm{N}_{K/\mathbb{Q}}(x)| = \mathrm{N}_{K/\mathbb{Q}}(x\mathcal{O}_K) = \mathrm{N}_{K/\mathbb{Q}}(I)\mathrm{N}_{K/\mathbb{Q}}(J) \leq \mathrm{N}_{K/\mathbb{Q}}(J)\, t$$

y si tenemos I, I' distintos, entonces $IJ = x\mathcal{O}_K$ e $IJ = x'\mathcal{O}_K$ son distintos.

Por el otro lado, sea $x\mathcal{O}_K \subset J$ no trivial tal que $\mathrm{N}_{K/\mathbb{Q}}(x\mathcal{O}_K) \leq \mathrm{N}_{K/\mathbb{Q}}(J)\, t$. Tomemos $I = J^{-1}(x\mathcal{O}_K)$. Entonces $I \in C$ es un ideal íntegro tal que $\mathrm{N}_{K/\mathbb{Q}}(I) \leq t$.

Puesto que $\sigma(t, C) = \#\varepsilon_t$, nos basta con contar los elementos de ε'_t, para lo que tomamos un sistema fundamental de unidades $U = \{u_1, \ldots, u_r\}$ de orden infinito en $\mathcal{O}_K$ y asociamos el conjunto ε'_t con

$$\varepsilon''_t = \{x \in J | 0 < |\mathrm{N}_{K/\mathbb{Q}}(x)| \leq \mathrm{N}_{K/\mathbb{Q}}(J)t,\ 0 \leq \alpha_k < 1 \text{ respecto a } U\}$$

Para ver la relación entre ε'_t y ε''_t. Sean $x, y \in \varepsilon''_t$ tales que $x\mathcal{O}_K = y\mathcal{O}_K$, entonces $x = \xi y$ dónde ξ es una unidad. Considerando los exponentes α_k, m_k y β_k respectivos tenemos que $\alpha_k = m_k + \beta_k$, donde $0 \leq \alpha_k, \beta_k < 1$ y los m_k son enteros. Se deduce que $m_k = 0$ para todo k, y $\xi = \zeta$ una raíz de la unidad, sea $w = \#W$ el cardinal del subgrupo de unidades formado por las raíces de la unidad, y por tanto $\#\varepsilon''_t = w\, \#\varepsilon'_t$.

A continuación vamos a definir el dominio $D_t \subset \mathbb{R}^n$ en relación con ε''_t. Sea $\{\alpha_1, \ldots, \alpha_n\}$ una base del grupo abeliano libre J, para cada $n-$tupla $(y_1, \ldots, y_n) \in \mathbb{R}^n$, sea

$$x^{(j)} = \sum_{k=1}^{n} y_k \alpha_k^{(j)}, \quad \text{para } 1 \leq j \leq n$$

Sea E_t el conjunto en $\mathbb{R}^n$ tales que las $n-$tuplas cumplen que

$$0 < \left|\prod x^{(j)}\right| \leq \mathrm{N}_{K/\mathbb{Q}}(J)\, t$$

y que los exponentes a_k de los $x^{(j)}$ están en $[0, 1)$. Puesto que $\mathrm{d}(\alpha_1 \cdots \alpha_n) = \left|\det(\alpha_k^{(j)})\right|^2 \neq 0$, la transformación lineal $(y_1, \cdots y_n) \mapsto (x^{(1)}, \ldots, x^{(n)})$ es invertible y

$$|x^{(j)}| = \left|\prod_{i=1}^{n} x^{(i)}\right| \exp\left(\sum_{k=1}^{r} a_k \log|u_k^{(j)}|\right) \leq (\mathrm{N}_{K/\mathbb{Q}}(J)\, t)^{1/n} \exp(rM_u)$$

el conjunto E_t es acotado por ser la imagen inversa de un acotado. Para conseguir el conjunto cerrado D_t nos falta definir E_t' de los puntos en $\mathbb{R}^n$ tales que para algún i

$$x^{(i)} = \sum_{k=1}^{n} y_k \alpha_k^{(i)} = 0$$

Sea $D_t = E_t \cup E_t'$. Entonces D_t es un conjunto compacto de $\mathbb{R}^n$. Sea $x \in \varepsilon_t''$, entonces las coordenadas de x son enteras, entonces $x \mapsto (m_1, \ldots, m_n) \in E_t$ no todos nulos, y cualquier punto de coordenadas enteras proviene de $x \in \varepsilon_t''$, por lo que hay una correspondencia biyectiva entre ε_t'' y los puntos enteros de E_t. Si $x \in \varepsilon_t''$ tal que su imagen está en E_t', entonces $x = 0$, lo que obliga a E_t' a estar compuesto únicamente por el origen.

El total de puntos con coordenadas enteras de D_t es igual a $1 + \#\varepsilon_t''$, si intentamos calcular el límite obtenemos que

$$\lim_{t\to\infty} \frac{w\sigma(t, C)}{t} = \lim_{t\to\infty} \frac{1 + w\sigma(t, C)}{t} = \lim_{t\to\infty} \frac{1 + \#\varepsilon_t''}{t} = \lim_{t\to\infty} \frac{\#D_t}{t}$$

Si ahora transformamos linealmente $z_k = \theta(y_k) = y_k t^{-1/n}$, se tiene $\theta(D_t) = D_1$, y los hipercubos de centro los puntos de coordenadas enteras y lado uno se transforman en hipercubos de centro $\theta(m_1, \ldots, m_n)$ y lado $t^{-1/n}$, cada uno con medida $1/t$, por lo que nuestro límite es una aproximación de la medida de D_1

$$\lim_{t\to\infty} \frac{w\sigma(t, C)}{t} = \lim_{t\to\infty} \frac{\#D_t}{t} = \mu(D_1) < +\infty$$

Por lo que

$$\lim_{t\to\infty} \frac{\sigma(t, C)}{t} = w\mu(D_1) = L$$

es una expresión completamente independiente de la clase de ideales elegida.

Observación 2.2.3.3. Aunque no es necesario para nuestro objetivo, el lector puede sentir curiosidad por el valor del límite anterior. Éste puede calcularse realizando una serie de cambios de variable sobre la medida de D_1 y resulta

$$\lim_{t\to\infty} \frac{w\sigma(t,C)}{t} = \mu(D_1) = \frac{2^{r_1+r_2}\pi^{r_2}R}{d}$$

Como ayuda a las mentes inquietas, es necesario cambiar primeramente a coordenadas polares dadas por la expresión en los cuerpos conjugados complejos, luego usamos la definición del conjunto E_t, y por último consideramos la propiedad logarítmica de los exponentes.

Corolario 2.2.3.4.

$$\lim_{t\to\infty} \frac{\sigma(t)}{t} = hL < +\infty$$

Demostración. Recordamos que h es el número de clase de K, un invariante que determina la cantidad de clases de ideales hay en K, por lo que

$$\lim_{t\to\infty} \frac{\sigma(t)}{t} = \sum_{i=1}^{h} \lim_{t\to\infty} \frac{\sigma(t,C_i)}{t} = hL < +\infty$$

Proposición 2.2.3.5. La serie de Dedekind del cuerpo de números K converge uniformemente en $(1,+\infty)$ y define una función continua, la función Zeta de Dedekind $\zeta_K(s)$, en dicho intervalo, y además

$$\lim_{s\to 1^+}(s-1)\zeta_K = hL$$

Demostración. Con el resultado del corolario anterior nos ponemos en la hipótesis de la proposición 2.2.1.5

A continuación veremos la expresión como producto sobre ideales primos de la función Zeta de Dedekind. Sea $\mathcal{J}$ un conjunto de ideales no triviales en K, y sea

$$\mathcal{J}_m = \{J \in \mathcal{J} | \mathrm{N}_{K/\mathbb{Q}}(J) \leq m\}, \quad \nu_{\mathcal{J}}(m) = \#\{J \in \mathcal{J} | \mathrm{N}_{K/\mathbb{Q}}(J) = m\}$$

podemos definir

$$\#\mathcal{J}_m = \sum_{k=1}^{m} \nu_{\mathcal{J}}(k), \quad S_m(\mathcal{J}) = \sum_{k=1}^{m} \frac{\nu_{\mathcal{J}}}{k^s} = \sum_{J\in\mathcal{J}_m} \frac{1}{(\mathrm{N}_{K/\mathbb{Q}}J)^s}$$

y por tanto también

$$T_m(\mathcal{J}) = \prod_{k=1}^{m} \left(\frac{1}{1-1/k^s} \right)^{\nu_{\mathcal{J}(k)}} = \prod_{J \in \mathcal{J}_m} \left(\frac{1}{1-(\mathrm{N}_{K/\mathbb{Q}} J)^{-s}} \right)$$

Proposición 2.2.3.6. Sea $\mathcal{J}$ el conjunto de los ideales íntegros no triviales de K, y sea $\mathcal{P}$ el conjunto de los ideales primos en K, entonces

$$\prod_{\mathfrak{p} \in \mathcal{P}} \frac{1}{1-(\mathrm{N}_{K/\mathbb{Q}} \mathfrak{p})^{-s}}$$

es absolutamente convergente para $s > 1$ y

$$\prod_{\mathfrak{p} \in \mathcal{P}} \frac{1}{1-(\mathrm{N}_{K/\mathbb{Q}} \mathfrak{p})^{-s}} = \sum_{J \in \mathcal{J}} \frac{1}{(\mathrm{N}_{K/\mathbb{Q}} J)^s}$$

Demostración. Análogamente a la prueba para la función Zeta de Riemann, miramos si la serie es convergente, lo cual implicará la convergencia absoluta del producto

$$\begin{aligned} \sum_{\mathfrak{p} \in \mathcal{P}} \frac{1}{(\mathrm{N}_{K/\mathbb{Q}} \mathfrak{p})^s} &= \lim_{m \to \infty} \sum_{\mathfrak{p} \in \mathcal{P}_m} \frac{1}{(\mathrm{N}_{K/\mathbb{Q}} \mathfrak{p})^s} = \lim_{m \to \infty} \sum_{k=1}^{m} \frac{\nu_{\mathcal{P}}}{k^s} \\ &\leq \lim_{m \to \infty} \sum_{k=1}^{m} \frac{\nu_{\mathcal{J}}}{k^s} \leq \sum_{k=1}^{\infty} \frac{\nu(k)}{k^s} \end{aligned}$$

Dada la convergencia, que los ideales considerados están en $\mathcal{O}_K$, por lo que se descomponen en multiplicación de ideales primos, y que la norma es una función multiplicativa, tenemos también que

$$\prod_{\mathfrak{p} \in \mathcal{P}} \frac{1}{1-(\mathrm{N}_{K/\mathbb{Q}} \mathfrak{p})^{-s}} = \sum_{J \in \mathcal{J}} \frac{1}{(\mathrm{N}_{K/\mathbb{Q}} J)^s}$$

Observación 2.2.3.7. Cuando $\mathcal{P}$ es el conjunto de todos los ideales primos en K

$$\zeta_K(s) = \prod_{\mathfrak{p} \in \mathcal{P}} \frac{1}{1-(\mathrm{N}_{K/\mathbb{Q}} \mathfrak{p})^{-s}}$$

Y en el caso particular en que $K = \mathbb{Q}$ volvemos a tener la expresión que ya conocemos

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

Para continuar con la réplica de los resultados de la sección anterior vamos a ver una acotación para la función Zeta. En una extensión recordamos que el grado de inercia de un ideal primo, $f = [\mathcal{O}/\mathfrak{P} : o/\mathfrak{p}]$, es el grado de extensión entre los cuerpos residuales con los anillos de enteros al levantarse, que también podemos ver como su dimensión como espacio vectorial de cuerpo $o/\mathfrak{p}$.

Proposición 2.2.3.8. Sea $\mathcal{P}_f$ el conjunto de ideales primos en K con grado de inercia f. Para $f \geq 1$ y $s > 1$, se tiene que

$$1 \leq \prod_{\mathfrak{p}\in\mathcal{P}_f} \frac{1}{1-(\mathrm{N}_{K/\mathbb{Q}}\mathfrak{p})^{-s}} \leq |\zeta_K(fs)|^n$$

y si $f \geq 2$

$$1 \leq \prod_{\mathfrak{p}\in\mathcal{P}_f} \frac{1}{1-(\mathrm{N}_{K/\mathbb{Q}}\mathfrak{p})^{-s}} \leq |\zeta_K(f)|^n$$

Demostración. Para $f \geq 1$ y $s > 1$, al existir a lo sumo n ideales primos dada una norma

$$1 \leq \prod_{\mathfrak{p}\in\mathcal{P}_f} \frac{1}{1-(\mathrm{N}_{K/\mathbb{Q}}\mathfrak{p})^{-s}} \leq \left(\prod_{\mathfrak{p}\in\mathcal{P}} \frac{1}{1-(\mathrm{N}_{K/\mathbb{Q}}\mathfrak{p})^{-fs}}\right)^n = |\zeta_K(fs)|^n$$

y si notamos que $|\zeta_K(f)| > |\zeta_K(fs)|$ cuando $f \geq 2$ obtenemos la segunda desigualdad. ∎

Proposición 2.2.3.9. Sea $\mathcal{J}$ el conjunto de todos los ideales íntegros de K, cuando $s \to 1^+$

$$\log \sum_{J\in\mathcal{J}} \frac{1}{(\mathrm{N}_{K/\mathbb{Q}}J)^s} \approx \sum_{\mathfrak{p}\in\mathcal{P}_1} \frac{1}{(\mathrm{N}_{K/\mathbb{Q}}\mathfrak{p})^s}$$

Demostración. Tenemos que

$$\sum_{J\in\mathcal{J}} \frac{1}{(\mathrm{N}_{K/\mathbb{Q}}J)^s} = \prod_{\mathfrak{p}\in\mathcal{P}} \frac{1}{1-(\mathrm{N}_{K/\mathbb{Q}}\mathfrak{p})^{-s}} = \prod_{f=1}^{n} \prod_{\mathfrak{p}\in\mathcal{P}_f} \frac{1}{1-(\mathrm{N}_{K/\mathbb{Q}}\mathfrak{p})^{-s}}$$

que al tomar logaritmo queda

$$\begin{aligned} log \sum_{J\in\mathcal{J}} \frac{1}{(\mathrm{N}_{K/\mathbb{Q}}J)^s} &= \sum_{f=1}^{n} \log \prod_{\mathfrak{p}\in\mathcal{P}_f} \frac{1}{1-(\mathrm{N}_{K/\mathbb{Q}}\mathfrak{p})^{-s}} \\ &\leq \log \prod_{\mathfrak{p}\in\mathcal{P}_1} \frac{1}{1-(\mathrm{N}_{K/\mathbb{Q}}\mathfrak{p})^{-s}} + (n-1)\log|\zeta_K(2)|^n \end{aligned}$$

Ahora hemos de obtener la suma y acotar el término extra que obtendremos

$$\log \prod_{\mathfrak{p}\in\mathcal{P}_1} \frac{1}{1-(\mathrm{N}_{K/\mathbb{Q}}\mathfrak{p})^{-s}} = \sum_{\mathfrak{p}\in\mathcal{P}_1} \log \frac{1}{1-(\mathrm{N}_{K/\mathbb{Q}}\mathfrak{p})^{-s}} = \sum_{\mathfrak{p}\in\mathcal{P}_1}\sum_{v=1}^{\infty} \frac{1}{v}\frac{1}{(\mathrm{N}_{K/\mathbb{Q}}\mathfrak{p})^{vs}}$$
$$= \sum_{\mathfrak{p}\in\mathcal{P}_1} \frac{1}{(\mathrm{N}_{K/\mathbb{Q}}\mathfrak{p})^{s}} + \sum_{\mathfrak{p}\in\mathcal{P}_1}\sum_{v=2}^{\infty} \frac{1}{v}\frac{1}{(\mathrm{N}_{K/\mathbb{Q}}\mathfrak{p})^{vs}}$$

y éste último

$$\sum_{v=2}^{\infty}\sum_{\mathfrak{p}\in\mathcal{P}_1} \frac{1}{v}\frac{1}{(\mathrm{N}_{K/\mathbb{Q}}\mathfrak{p})^{vs}} \leq \sum_{\mathfrak{p}\in\mathcal{P}_1} \frac{1}{2}\sum_{v=2}^{\infty} \frac{1}{(\mathrm{N}_{K/\mathbb{Q}}\mathfrak{p})^{vs}} = \sum_{\mathfrak{p}\in\mathcal{P}_1} \frac{1}{2}\frac{(\mathrm{N}_{K/\mathbb{Q}}\mathfrak{p})^{2s}}{1-(\mathrm{N}_{K/\mathbb{Q}}\mathfrak{p})^{-s}}$$
$$\leq \sum_{\mathfrak{p}\in\mathcal{P}_1} \frac{1}{(\mathrm{N}_{K/\mathbb{Q}}\mathfrak{p})^{2s}} \leq n\sum_{p\in P}\frac{1}{p^{2s}} \leq n\zeta(2s)$$

Por lo que concluimos que cuando $s \to 1^+$

$$\log \sum_{J\in\mathcal{J}} \frac{1}{(\mathrm{N}_{K/\mathbb{Q}}J)^s} \approx \sum_{\mathfrak{p}\in\mathcal{P}_1} \frac{1}{(\mathrm{N}_{K/\mathbb{Q}}\mathfrak{p})^s}$$

Por último vamos a ver las $L-$series de Hecke, que generalizan las $L-$series a ideales íntegros de K en el grupo $C_{J+} = \mathcal{F}_j/\mathcal{P}r_{J+}$ visto en la introducción. Empezamos definiendo un nuevo carácter con el que desarrollar el resto de conceptos

Definición 2.2.3.10 (Carácter de Hecke). *Sea K un cuerpo de números algebraico, y sea $J \subset K$ un ideal íntegro no trivial. Sea$C_{J+} = \mathcal{F}_J/\mathcal{P}r_{J+}$ el grupo de las clases de ideales módulo J definimos el carácter modular*

$$\chi(I) = \begin{cases} \tilde{\chi}(\tilde{I}), \text{ cuando } I \in \mathcal{F}_J \\ 0 \text{ en otro caso} \end{cases}$$

siendo $\tilde{\chi}$ un carácter del grupo C_{J+}, y $\tilde{I}$ la imagen de I en C_{J+}.

Definición 2.2.3.11 ($L-$serie de Hecke). *Sea K un cuerpo de números algebraico, sea $J \subset K$ un ideal íntegro no trivial y χ un carácter de Hecke asociado a J, definimos*

$$L(s|\chi) = \sum_{I\in\mathcal{I}} \frac{\chi(I)}{(\mathrm{N}_{K/\mathbb{Q}}I)^s}$$

como la $L-$serie de Hecke asociada a χ, y ésta recorre los ideales íntegros no triviales de K.

Puesto que hemos definido un carácter podemos usar los resultados para sumas gausiannas y $L-$series que hemos visto con anterioridad, lo único que cambiamos, con en el resto de esta subsección, son los subíndices. Vamos a enumerar las propiedades de las $L-$series de Hecke:

- Para cada carácter de Hecke χ, la $L-$serie asociada converge uniformemente en $(1, +\infty)$ y define una función continua en dicho intervalo.
- Si χ es un carácter de Hecke distinto del trivial, entonces la $L-$serie de Hecke converge uniformemente en $(0, +\infty)$ y define ahí una función continua.
- Para $s > 1$ tenemos la expresión como producto de Euler

$$\sum_{I \in \mathcal{I}} \frac{\chi(I)}{(\mathrm{N}_{K/\mathbb{Q}} I)^s} = \prod_{\mathfrak{p} \in \mathcal{P}_J} \frac{1}{1 - \chi(\mathfrak{p})(\mathrm{N}_{K/\mathbb{Q}} \mathfrak{p})^{-s}}$$

  siendo $\mathcal{P}_J$ son los ideales primos que no dividen a J.
- Para χ_0 se tiene que

$$L(s|\chi_0) = \zeta_K(s) \prod_{\mathfrak{p}|J} \left(1 - \frac{1}{(\mathrm{N}_{K/\mathbb{Q}} \mathfrak{p})^s}\right)$$

- Para cualquier carácter de Hecke χ y $s \to 1^+$,

$$\log L(s|\chi_0) \approx \sum_{\mathfrak{p} \in \mathcal{P}} \frac{\chi(\mathfrak{p})}{(\mathrm{N}_{K/\mathbb{Q}} \mathfrak{p})^s}$$

3 Teorema de Dirichelt para Series Aritméticas

3.1 Teorema de Dirichlet para Series Aritméticas

Demostración

Antes de dedicarnos al teorema de Dirichlet, vamos a pararnos en el caso particular que pudo comprobar Euler varios años antes, la prueba de este teorema nos da una idea para la construcción del tema principal

Proposición 3.1.1.1. Sea m un número natural fijo, entonces existen infinitos primos en conjunto $C_m = \{1 + mk \mid k \in \mathbb{N}_0\}$, y se tiene que

$$\varphi(m) \sum_{p \in C_m} \frac{1}{p^s} \approx \log \frac{1}{s-1} \qquad \text{para } s \to 1^+$$

Demostración. Sea ξ una raíz $m-$ésima primitiva de la unidad, consideramos el cuerpo $K = \mathbb{Q}(\xi)$ de forma que el grado de extensión es $\varphi(m)$.

En nuestro caso, como $p \equiv 1 \bmod m$, p descompone completamente en un total de $\varphi(m)$ ideales $\mathfrak{p} \subset K$ con norma $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}) = p$ al no ser ramificado, entonces

$$\varphi(m) \sum_{p \in C_m} \frac{1}{p^s} = \sum_{\mathfrak{p} \in \mathcal{P}_1} \frac{1}{\left(\mathrm{N}_{K/Q}\mathfrak{p}\right)^s}$$

Como ya hemos visto, para $s \to 1^+$

$$\sum_{\mathfrak{p} \in \mathcal{P}_1} \frac{1}{\left(\mathrm{N}_{K/Q}\mathfrak{p}\right)^s} \approx \log \zeta_K(s),$$

y además $\lim_{s\to 1^+}(s-1)\log\zeta_K(s) = c \neq 0$.

Tomando pues, ε con $0 < \varepsilon < c$, existe $\delta > 0$ tal que si $1 < s < 1+\delta$, entonces $|(s-1)\log\zeta_K(s) - c| < \varepsilon$. Podemos ver que este valor está acotado y además no se acerca a cero. Si tomamos logaritmo y hacemos tender $s \to 1^+$ obtenemos

$$\log\zeta_K(s) \approx \log\frac{1}{s-1}.$$

Uniendo este último resultado al anterior

$$\varphi(m)\sum_{p\in C_m}\frac{1}{p^s} \approx \log\frac{1}{s-1}, \quad \text{para } s \to 1^+.$$

Esto implica que la serie es divergente, por lo que existe una infinitud de números primos en el conjunto C_m.

Teorema 3.1.1.2 (Teorema de Dirichlet para Series Aritméticas). *Sean* $1 \leq a \leq m$ *naturales tales que* $\gcd(a,m) = 1$, *entonces la progresión aritmética*

$$C_{a,m} = \{a + mk | k \in \mathbb{N}_0\}$$

contiene una cantidad infinita de primos.

Demostración. Para esta prueba haremos uso de los caracteres módulo m para distinguir entre las distintas progresiones según a, entonces para los distintos caracteres modulares χ_i planteamos el sistema de ecuaciones

$$\sum_{p\in P}\frac{\chi_i(p)}{p^s} = \sum_{a\in(\mathbb{Z}m)^\times}\chi_i(a)\left(\sum_{p\equiv a \bmod m}\frac{1}{p^s}\right)$$

que por la proposición 2.1.1.15 tiene como soluciones para cada $a \in (\mathbb{Z}m)^\times$

$$\sum_{p\equiv a \bmod m}\frac{1}{p^s} = \frac{1}{\varphi(m)}\sum_{i=0}^{\varphi(m)-1}\overline{\chi_i}(a)\left(\sum_{p\in P}\frac{\chi_i(p)}{p^s}\right)$$

Usando la aproximación de la proposición 2.2.2.3, cuando $s \to 1^+$ obtenemos

$$\sum_{p\equiv a \bmod m}\frac{1}{p^s} \approx \frac{1}{\varphi(m)}\sum_{i=0}^{\varphi(m)-1}\overline{\chi_i}(a)\log L(s|\chi_i)$$

Para $i = 0$ se deduce fácilmente que con $s \to 1^+$

$$\log L(s\chi_0) \approx \log\frac{1}{s-1}$$

luego el primer término no está acotado, vamos a ver que el resto sí y que además cada $L(1|\chi_i) \neq 0$, bien definidos por ser funciones continuas en $(0, +\infty)$. Tomando $a \equiv 1 \bmod m$

$$\sum_{p \equiv 1 \bmod m} \frac{1}{p^s} \approx \frac{1}{\varphi(m)} \sum_{i=0}^{\varphi(m)-1} \log L(s|\chi_i)$$

por la proposición anterior, cuando $s \to 1^+$,

$$\frac{1}{\varphi(m)} \sum_{i=0}^{\varphi(m)-1} \log L(s|\chi_i) \approx \log \frac{1}{s-1} \approx \log L(s\chi_0)$$

por lo que el resto de la suma debe permanecer acotada. Si llamamos

$$H(s) = \sum_{\chi_i \neq \chi_0} \log L(s|\chi_i)$$

ésta está acotada cuando $s \to 1^+$ y además

$$\prod_{\chi_i \neq \chi_0} L(1|\chi_i) = \lim_{s \to 1^+} \prod_{\chi_i \neq \chi_0} L(s|\chi_i) = \lim_{s \to 1^+} e^{H(s)} \neq 0$$

de este modo $L(s|\chi_i) \neq 0$ si $\chi_i \neq \chi_0$

Definición 3.1.1.3 (Densidad de Dirichlet). *Sea $A \subset \mathcal{P}$ un subconjunto, supongamos que existe el límite*

$$\delta(A) := \lim_{s \to 1^+} \frac{\sum_{p \in A} \frac{1}{p^s}}{\sum_{p \in \mathcal{P}} \frac{1}{p^s}}$$

Entonces se llama $\delta(A)$ a la densidad de Dirichlet de A.

Corolario 3.1.1.4. Sean a, m números naturales $1 \leq a \leq m$ tales que $\gcd(a, m)$, entonces el conjunto de números primos en la progresión aritmética $C_{a,j}$ tiene densidad de Dirichlet igual a $\varphi(m)^{-1}$.

Demostración. Acabamos de ver que cuando $s \to 1^+$

$$\sum_{p \equiv a \bmod m} \frac{1}{p^s} \approx \frac{1}{\varphi(m)} \log \frac{1}{s-1}$$

Puesto que

$$\sum_{p \in P} \frac{1}{p^s} \approx \log \frac{1}{s-1}$$

su división ha de ser

$$\lim_{s\to 1^+}\left(\sum_{p\in P}\frac{1}{p^s}\right)\Big/\left(\log\frac{1}{s-1}\right)=1$$

Entonces

$$\delta(C_{a,j})=\lim_{s\to 1^+}\left(\sum_{p\equiv a \bmod m}\frac{1}{p^s}\right)\Big/\left(\log\frac{1}{s-1}\right)=\frac{1}{\varphi(m)}$$

Haciendo los cambios oportunos y usando los caracteres de Hecke, somos capaces de generalizar el Teorema de Dirichlet que acabamos de ver con una prueba muy similar e intuitiva, aunque no entraremos en detalles ya que se escapa de los objetivos de este trabajo, pero podemos enunciar el siguiente teorema.

Teorema 3.1.1.5. *Cada clase en C_{J+}(o C_J) contiene una cantidad infinita de ideales primos, y además, para cada clase $\tilde{I}\in C_J$, $\tilde{I}_+\in C_{J+}$ tenemos las densidades de Dirichlet*

$$\lim_{s\to 1^+}\left(\sum_{\mathfrak{p}\in\tilde{I}}\frac{1}{(\mathrm{N}_{K/\mathbb{Q}}\mathfrak{p})^s}\right)\Big/\left(\log\frac{1}{s-1}\right)=\frac{1}{h_J}$$

$$\lim_{s\to 1^+}\left(\sum_{\mathfrak{p}\in\tilde{I}_+}\frac{1}{(\mathrm{N}_{K/\mathbb{Q}}\mathfrak{p})^s}\right)\Big/\left(\log\frac{1}{s-1}\right)=\frac{1}{h_J+}$$

3.2 Generalizaciones del Teorema

Cosas que comentar por encima

Teorema de Densidad de Chevotarev

Tal y como expresamos al principio, las extensiones de Galois pueden resultar un tanto especiales en cuanto a la simplificación de los problemas de ramificación. Nos podemos preguntar ahora que hemos visto la densidad de Dirichlet aplicada a los conjuntos formados por las progresiones aritméticas como cambia al considerar otros conjuntos, como por ejemplo los primos no ramificados que tengan asociada la misma clase de conjugación por el frobenius Frob_p

Teorema 3.2.1.1 (Teorema de Densidad de Tchevotarev). *Sea L/K una extensión finita de cuerpos con grupo de Galois $G = \mathrm{Gal}(L/K)$. Sea C una de las clases de conjugación de G. Entonces*

$$\delta(\{p \in \mathcal{P} : p \text{ no ramificado}, Frob_p = C\}) = \frac{|C|}{|G|}$$

Aunque es un resultado bastante intuitivo, la prueba puede ser laboriosa. Una ligera idea sobre ella es llegar a probar que la densidad de Dirichlet para uno de los embeddings es $1/|G|$ y a la hora de sumar en cada clase se obtiene el resultado $|C|/|G|$.

Conjetura de Dickson

Consideremos un sistema lineal de k ecuaciones $\{a_k + b_k n\}$, la conjetura de Dickson dice que existen infinitos naturales n tales que todas las ecuaciones son números primos excluyendo el caso en el que para algún p primo, alguna de las ecuaciones es múltiplo de p para todo n.

El caso de $k = 1$ lo hemos visto como el Teorema de Dirichlet. Cuando $k = 2$ existen conjeturas más conocidas, como los primos gemelos $\{n, n+2\}$ o los primos de Germain $\{n, 1 + 2n\}$.

Teorema de Green-Tao

El Teorema de Green-Tao formula que para todo natural k, existe una progresión aritmética de primos con k términos. Mas formalmente

Teorema 3.2.3.1 (Teorema de Green-Tao). *Sea $\pi(N)$ el número de primos menores o iguales a N. Si A es un subconjunto de los números primos tal que su densidad es positiva*

$$\limsup_{N\to\infty} \frac{|A \cap [1, \dots, N]|}{\pi(N)} > 0$$

Entonces para todo natural k, el conjunto A contiene infinitas progresiones aritméticas de longitud k.

Es una derivación del Teorema de Szemerédi que dice que si la densidad anterior es positiva para un conjunto A, entonces existen progresiones de longitud k.

Bibliografía

[1] S. Alaca and K. S. Williams, *Introductory algebraic number theory.*, Cambridge University Press, 2004.

[2] V. Garrido López, *Cálculo explícito de elementos de frobenius en grupos de galois*, 2019. https://idus.us.es/handle/11441/90011.

[3] B. Green and T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Annals of Mathematics, 167 (2008), p. 481–547.

[4] R. A. Mollin, *Algebraic number theory*, Chapman and Hall/CRC, 2011.

[5] J. Neukirch, *Algebraic number theory*, vol. 322, Springer Science & Business Media, 2013.

[6] S. W. PARK, *Existence of the frobenius element and its applications*, 2015. http://math.uchicago.edu/~may/REU2015/REUPapers/Park.pdf.

[7] P. Ribenboim, *Classical theory of algebraic numbers*, Springer Science & Business Media, 2013.

[8] J.-P. Serre, *Topics in galois theory, volume 1 of research notes in mathematics. ak peters ltd., wellesley, ma, 2008*, With notes by Henri Darmon, 4.

[9] R. van Bommel, *Using the chebotarev density theorem to calculate the size of galois groups*, (2012). https://www.raymondvanbommel.nl/Bachelor.pdf.