

TEOREMA DE DIRICHLET
TRABAJO FINAL DE TEORÍA DE NÚMEROS ALGEBRAICOS

Ignacio Monteverde

Profesor: Gonzalo Tornaría

Junio de 2007

Universidad de la República

Facultad de Ciencias

Centro de Matemática

Resumen

La idea de este trabajo es demostrar el teorema de Dirichlet, que a grandes rasgos dice que $\forall a, b \in \mathbb{Z} / \text{mcd}(a, b) = 1$ existen infinitos primos de la forma $ax + b$.

Euler fue el primero que conjeturó un resultado de esta forma, diciendo que toda progresión aritmética que empiece en 1 tiene infinitos primos. El teorema tal cual está escrito arriba fue conjeturado por Gauss y probado por Dirichlet en 1835.

La prueba que se presenta en este trabajo es distinta a la original y nos da algo un poco más fuerte. Este trabajo está basado fundamentalmente en un artículo de D.Weissmann (2004) y uno de G.Valiant (2005).

Para entender este trabajo sólo es necesario tener nociones básicas de análisis complejo y de grupos abelianos finitos. En la prueba se utilizan también algunas propiedades de la función ζ de Riemann.

1. Caracteres en grupos abelianos finitos

Definición 1.1. Una representación de un grupo G es un morfismo de grupos $\varphi : G \rightarrow Gl_n(\mathbb{C})$. A n se le llama la dimensión de la representación.

Definición 1.2. Un caracter de un grupo G es una representación unidimensional del grupo. O sea es un morfismo de grupos $\chi : G \rightarrow \mathbb{C}^*$.

Nos concentraremos en el caso en que G es abeliano y finito (que es lo que utilizaremos luego). En este caso la imagen de χ es un subgrupo finito de \mathbb{C}^* . Por tanto $\chi(G)$ es el conjunto de las raíces n -ésimas de la unidad para algún $n \in \mathbb{N}$. Dado que χ es morfismo su núcleo es un subgrupo $H \subset G$ y lleva cada coclase de H a una raíz distinta. Por tanto, cada raíz n -ésima de la unidad tendrá la misma cantidad de preimágenes.

Queremos darle estructura al conjunto de los caracteres de un grupo, que notaremos \widehat{G} . Para ello definimos la multiplicación de caracteres multiplicando elemento a elemento. O sea $(\chi \cdot \chi')(g) = \chi(g) \cdot \chi'(g)$.

Evidentemente, $\chi \cdot \chi'$ así definido es un caracter:

$$(\chi \cdot \chi')(e) = \chi(e) \cdot \chi'(e) = 1$$

$$(\chi \cdot \chi')(gg') = \chi(gg') \cdot \chi'(gg') = \chi(g) \cdot \chi(g') \cdot \chi'(g) \cdot \chi'(g') = (\chi \cdot \chi')(g) \cdot (\chi \cdot \chi')(g')$$

También es claro que el elemento identidad de \widehat{G} es χ_0 , definido como $\chi_0(g) = 1 \forall g \in G$. El inverso de un caracter χ es $\chi^{-1} / \chi^{-1}(g) = 1/\chi(g) = \overline{\chi(g)}$, esta última igualdad se debe a que la imagen de χ está contenida en el círculo unidad y por tanto

inversa y conjugada coinciden. Por tanto, la inversa de χ es $\bar{\chi}$, donde $\bar{\chi}(g) = \overline{\chi(g)}$. $\bar{\chi}$ es claramente un caracter (porque la conjugación respeta la multiplicación). Por tanto \widehat{G} es un grupo.

Lema 1.1. $\widehat{G} \cong G$

Demostración: Dado que G es abeliano y finito, sabemos que $G \cong \mathbb{Z}/d_1 \oplus \dots \oplus \mathbb{Z}/d_k$. Dado un elemento $g \in G$, podemos escribirlo como (a_1, \dots, a_k) , con $a_i \in \mathbb{Z}/d_i$. G esta generado por $\{e_1, \dots, e_k\}$ y cada e_i tiene orden d_i .

Todo caracter χ debe llevar e_i a alguna raíz d_i -ésima de la unidad. O sea, $\chi(e_i) = \zeta_{d_i}^{a_i}$, con $0 \leq a_i < d_i$.

Como $\{e_1, \dots, e_k\}$ es generador de G , cada caracter χ está determinado por lo que vale en cada e_i . Por tanto, podemos saber quién es χ por la k -upla (a_1, \dots, a_k) .

Ahora, dada una k -upla cualquiera (b_1, \dots, b_k) , definimos $\chi(b_1, \dots, b_k) = \prod_{i=1}^k \zeta_{d_i}^{a_i b_i}$. Esto es claramente un caracter cuya k -upla asociada es (a_1, \dots, a_k)

En definitiva, probamos que la función $\varphi : G \rightarrow \widehat{G}$ que a una k -upla (a_1, \dots, a_k) le asocia χ , con $\chi(b_1, \dots, b_k) = \prod_{i=1}^k \zeta_{d_i}^{a_i b_i}$ es biyectivo.

Es claro que este mapa es morfismo. \square

Proposición 1.2. *Los caracteres verifican:*

1. $\sum_{g \in G} \chi(g) = \begin{cases} |G| & \text{si } \chi = \chi_0 \\ 0 & \text{en otro caso} \end{cases}$
2. $\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} |G| & \text{si } g = e \\ 0 & \text{en otro caso} \end{cases}$

Demostración:

1. Previo al lema habíamos observado que χ manda la misma cantidad de elementos a cada raíz n -ésima de la unidad.

Si $\chi \neq \chi_0$, entonces $\sum_{g \in G} \chi(g) = \frac{|G|}{n} \sum_{i=0}^{n-1} \zeta_n^i = 0$, porque $n > 1$ (si no, $\chi = \chi_0$) y por tanto la suma de las raíces n -ésimas de la unidad da 0.

Si $\chi = \chi_0 \Rightarrow \chi(g) = 1 \forall g \Rightarrow \sum_{g \in G} \chi(g) = |G|$

2. Si $g = e \Rightarrow \chi(e) = 1 \forall \chi \Rightarrow \sum_{\chi \in \widehat{G}} \chi(g) = \sum_{\chi \in \widehat{G}} 1 = |\widehat{G}| = |G|$

Si $g \neq e \Rightarrow \exists \chi_1 \in \widehat{G} / \chi_1(g) \neq 1$ (recordemos como es el isomorfismo entre G y \widehat{G}).

$\sum_{\chi \in \widehat{G}} \chi(g) = \sum_{\chi \in \widehat{G}} \chi(g) \chi_1(g) = \chi_1(g) \sum_{\chi \in \widehat{G}} \chi(g)$ (la primer igualdad es porque al ser χ_1 invertible $\chi_1 \chi$ recorre todo \widehat{G} si χ recorre todo \widehat{G})

$\Rightarrow (\chi_1(g) - 1) \sum_{\chi \in \widehat{G}} \chi(g) = 0 \Rightarrow \sum_{\chi \in \widehat{G}} \chi(g) = 0$ \square

2. L-series de Dirichlet

Si $G = (\mathbb{Z}/(b))^\times$, podemos extender un caracter de G a todo \mathbb{Z} como:

$$\chi(n) = \begin{cases} \chi(\bar{n}) & \text{si } \text{mcd}(n, b) = 1 \\ 0 & \text{en otro caso} \end{cases}$$

A este tipo de funciones se les llama caracteres de Dirichlet.

Observemos que χ sigue siendo multiplicativa; y que el producto de dos caracteres de Dirichlet es otro caracter de Dirichlet.

Además, estos caracteres forman un grupo canónicamente isomorfo a \widehat{G} , con identi-

$$\text{dad } \chi_0, \chi_0(n) = \begin{cases} 1 & \text{si } \text{mcd}(n, b) = 1 \\ 0 & \text{en otro caso} \end{cases}.$$

Por esta razón, en adelante nos referiremos a los caracteres de Dirichlet como \widehat{G} .

Para $s \in \mathbb{C}$, $\chi \in \widehat{G}$, la L-serie de Dirichlet se define como:

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

Como $|\chi(n)| = 0$ ó 1 , la serie converge absolutamente para $\text{Re}(s) > 1$.

$\prod_p \text{ primo } (1 - \frac{\chi(p)}{p^s})^{-1} = \prod_p \sum_{h=1}^{\infty} (\frac{\chi(p)}{p^s})^h = \prod_p \sum_{h=1}^{\infty} (\frac{\chi(p^h)}{(p^h)^s}) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ (esta última igualdad se debe a la factorización única en \mathbb{N} , sumado a que χ es multiplicativa).

O sea que $L(s, \chi)$ puede también escribirse como $\prod_p \text{ primo } (1 - \frac{\chi(p)}{p^s})^{-1}$.

Lema 2.1. 1. $L(s, \chi_0)$ tiene extensión analítica a todo el semiplano $\text{Re}(s) > 0$ excepto en $s=1$, donde presenta un polo simple.

2. $L(s, \chi)$ converge para todo $s / \text{Re}(s) > 0$, si $\chi \neq \chi_0$

Demostración:

1. $L(s, \chi_0) = \prod_p \text{ primo } (1 - \frac{\chi_0(p)}{p^s})^{-1} = \prod_{p/\text{mcd}(p,b)=1} (1 - \frac{1}{p^s})^{-1} = \prod_p \text{ primo } (1 - \frac{1}{p^s})^{-1} \prod_{p|b} (1 - \frac{1}{p^s}) = \zeta(s) \prod_{p|b} (1 - \frac{1}{p^s})$. Recordando que $\zeta(s)$ tiene extensión analítica para $\text{Re}(s) > 0$ excepto en $s=1$ (donde presenta un polo simple) y observando que $0 < \prod_{p|b} (1 - \frac{1}{p^s}) < 1$, queda probado.

2. $\sum_{n=N+1}^{N+b} \chi(n) = \sum_{\bar{n} \in G} \chi(\bar{n}) = 0$. Además $\chi(n) = \chi(n+b)$. Entonces las sumas parciales de $\chi(n)$ están acotadas por $\max \{ |\sum_{n=1}^L \chi(n)|, 1 \leq L \leq b \}$.

Además, $\{\frac{1}{n^s}\}$ converge a 0 $\forall s/Re(s) > 0$, por tanto, $|\sum_{n=H}^K \frac{\chi(n)}{n^s}| \leq \frac{1}{|H^s|} |\sum_{n=H}^K \chi(n)| < \epsilon \forall K$ si elijo H suficientemente grande.

□

Teorema 2.2. $L(1, \chi) \neq 0 \forall \chi \neq \chi_0$

Demostración:

(a) Supongamos χ es real, o sea, $\chi : G \rightarrow \{-1, 1\}$.

En este caso, $\chi(n^2) = (\chi(n))^2 = 1 \forall n \in \mathbb{Z}$.

Definimos la siguiente función:

$$f(n) = \sum_{d|n} \chi(d)$$

f es multiplicativa en el sentido que si $mcd(m, n) = 1$, entonces $f(mn) = f(m)f(n)$:

$f(mn) = \sum_{h|mn} \chi(d) = \sum_{d|n, l|m} \chi(dl) = \sum_{d|n, l|m} \chi(d)\chi(l)$ (al ser $mcd(m, n)=1$, la forma de escribir un divisor de mn como un divisor de m por uno de n es única) $= \sum_{d|n} \chi(d) \cdot \sum_{l|m} \chi(l) = f(m)f(n)$.

Al ser f multiplicativa, para conocer su comportamiento nos basta saber cuánto vale en las potencias de primos:

* Si $p|b$, entonces $f(p^m) = 1 \forall m$, dado que el único divisor de p^m en el cual χ no vale 0 es 1.

* Si p no divide a b y m es par, $f(p^m) \geq 1$, porque cada p^k con $0 \leq k \leq m$ par nos aporta un 1, y por lo tanto habrá al menos un divisor más que contribuye con 1 de los que contribuyen con -1.

* Si p no divide a b y m es impar, $f(p^m) \geq 0$, por la misma razón que el caso anterior.

Por las propiedades de arriba, sumado a que f es multiplicativa, tenemos que $f(n) \geq 0 \forall n \in \mathbb{N}$. También podemos afirmar que $f(n^2) \geq 1 \forall n \in \mathbb{N}$, dado que todos los factores primos de n^2 aparecen con exponente par.

Definimos ahora:

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

Tenemos que:

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \geq \sum_{m=1}^{\infty} \frac{f(m^2)}{m^{2s}} \quad (\text{porque } f(n) \geq 0)$$

$$\begin{aligned} &\geq \sum_{m=1}^{\infty} \frac{1}{m^{2s}} (\text{porque } f(m^2) \geq 1) \\ &= \zeta(2s) \end{aligned}$$

Ahora, como $\zeta(2s)$ tiene un polo simple en $s = 1/2$, $F(s)$ presenta una singularidad para $s = 1/2$.

Pero por otra parte $F(s) = L(s, \chi)\zeta(s)$ (al ser f la convolución de χ con 1). Si $L(1, \chi) = 1$, este cero cancelaría el polo de $\zeta(s)$ y por tanto $F(s)$ sería holomorfa en todo $Re(s) > 0$, lo que contradice lo dicho arriba.

(b) Si la imagen de χ no está incluida en los reales, entonces $\chi \neq \bar{\chi}$.

Consideremos $P(s) = \prod_{\chi \in \hat{G}} L(s, \chi)$.

P es producto de funciones analíticas en $Re(s) > 0$, salvo por $L(s, \chi)$ en $s=1$, por lo tanto es analítica, salvo por un posible polo en $s=1$. Comenzaremos asumiendo que ninguna de las L-series que aparecen en este producto es la función idénticamente nula (se prueba al final). Si esto ocurre, podemos encontrar $\forall \delta > 0$ un x con $Re(x) > 1$, $|x - 1| < \delta$ / $L(x, \chi) \neq 0$ (en otro caso, alguna de las $L(s, \chi)$ tendría una sucesión infinita de ceros con 1 como punto de acumulación, y por tanto la función sería la nula). Para estos x tomamos el logaritmo:

$$\begin{aligned} \ln(P(x)) &= \sum_{\chi \in \hat{G}} \ln(L(x, \chi)) = \sum_{\chi \in \hat{G}} \ln \left(\prod_p \left(1 - \frac{\chi(p)}{p^x}\right)^{-1} \right) \\ &= - \sum_{\chi \in \hat{G}} \sum_p \ln \left(1 - \frac{\chi(p)}{p^x}\right) = \sum_{\chi \in \hat{G}} \sum_p \sum_{n=1}^{\infty} \frac{\chi^n(p)}{np^{xn}} = \end{aligned}$$

(podemos cambiar el orden de las sumas porque son absolutamente convergentes al ser $Re(x) > 1$)

$$= \sum_p \sum_{n=1}^{\infty} \frac{1}{np^{xn}} \sum_{\chi \in \hat{G}} \chi(p^n) =$$

(proposición 1.2)

$$= \sum_p \sum_{j/p^j \equiv 1 \pmod{b}} \frac{1}{j p^{js}} \geq 0$$

Tenemos entonces que $\ln(P(x)) \geq 0$ arbitrariamente cerca de 1. Por lo tanto, $P(x) \geq 1$ para una sucesión que acumula en 1.

Si $L(1, \chi) = 0$, entonces también valdría 0 $L(1, \bar{\chi})$ (porque la conjugación

mantiene el producto y la suma). Tendríamos por lo tanto dos L-series distintas que valen 0 en 1. Pero esto implicaría que $P(x)$ vale 0 en 1, porque tengo un polo simple (aportado por $L(s, \chi_0)$) multiplicado por un cero de orden 2 (aportado por $L(s, \chi)L(s, \hat{\chi})$). Esto nos lleva a una contradicción, porque sabíamos que $P(s) \geq 1$ arbitrariamente cerca de 1.

Sólo nos resta probar que ninguna $L(s, \chi)$ es idénticamente nula en $Re(s) > 0$: $L(s, \chi) = 1 + \sum_{n=2}^{\infty} \frac{\chi(n)}{n^s}$. Eligiendo un s con $Re(s)$ suficientemente grande, puedo hacer la suma infinita arbitrariamente pequeña. En particular, tomo s para que la suma sea menor que 1; entonces para ese s , $L(s, \chi) \geq 1 - |\sum_{n=2}^{\infty} \frac{\chi(n)}{n^s}| > 0$ \square

3. Teorema de Dirichlet

Antes de siquiera enunciar el teorema, pasaremos a probar un resultado muy importante para nuestro objetivo:

Proposición 3.1. $\sum_p p^{-s}$ diverge cuando $s \rightarrow 1^+$

Demostración: Para cada primo p , si $s \geq 1$ $|\frac{1}{p^s} + \ln(1-1/p^s)| = |\frac{1}{p^s} - \sum_{n=1}^{\infty} \frac{1}{np^{ns}}| = \sum_{n=2}^{\infty} \frac{1}{np^{ns}} < \frac{1}{2} \sum_{n=2}^{\infty} \frac{1}{p^n} = \frac{1}{2} p^{-2} \frac{1}{1-p^{-1}} = \frac{1}{2p(p-1)} \leq \frac{1}{p^2}$. Dado que $\sum \frac{1}{p^2} < \sum_{n=1}^{\infty} \frac{1}{n^2}$ converge absolutamente, tenemos que $\lim_{s \rightarrow 1^+} \sum_p (\frac{1}{p^s} + \ln(1-1/p^s))$ es finito.

Por tanto, si $\sum_p p^{-s}$ converge cuando $s \rightarrow 1^+$, también lo hace $\sum_p \ln(1-1/p^s)$. Llamemos $L := \lim_{s \rightarrow 1^+} \sum_p \ln(1-1/p^s)$.

Ahora, si hacemos la exponencial de esta última serie, obtenemos:

$$e^{\sum_p \ln(1-1/p^s)} = \prod_p e^{\ln(1-1/p^s)} = \prod_p (1-1/p^s) = (\zeta(s))^{-1}.$$

Pero, por un lado $\lim_{s \rightarrow 1^+} e^{\sum_p \ln(1-1/p^s)} = e^L$, y por otro $\lim_{s \rightarrow 1^+} (\zeta(s))^{-1} = 0$ porque ζ presenta un polo en $s=1$, lo que nos hace concluir que L no es finito. Por tanto, también diverge el $\lim_{s \rightarrow 1^+} \sum_p \frac{1}{p^s}$. \square

Vamos a probar algo más fuerte a lo que dijimos al comienzo del trabajo. Mostraremos que hay "igual cantidad" de primos $p \equiv a \pmod{b} \forall a \in (\mathbb{Z}/(b))^\times$. Para decir esto formalmente, debemos dar la definición de qué significa "igual cantidad".

Definición 3.1. La densidad de Dirichlet de un subconjunto $S \subset \{p/p \text{ primo}\}$ es:

$$\lim_{s \rightarrow 1^+} \frac{\sum_{p \in S} 1/p^s}{\sum_{\text{primos}} 1/p^s}$$

siempre que exista este límite.

Lo que mostraremos es que cada conjunto $S = \{p \text{ primo} / p \equiv a \pmod{b}\}$ tiene densidad $\frac{1}{\phi(b)} \forall a \in (\mathbb{Z}/(b))^*$.

Probaremos en particular que $\lim_{s \rightarrow 1^+} (\sum_{p \equiv a} p^{-s} - \frac{1}{\phi(b)} \sum_{\text{primos}} p^{-s})$ es finito; lo que claramente implica lo anterior.

Sabiendo que la segunda suma en nuestro límite diverge, la única forma de que el límite sea finito es que la primer suma sea infinita, y por lo tanto deben existir infinitos primos de la forma $ax + b$.

Antes de ir al teorema, probaremos un lema que usaremos luego.

Lema 3.2. $\sum_{\text{primos}} \frac{\chi(p)}{p^s}$ converge cuando $s \rightarrow 1^+ \forall \chi \neq \chi_0$

Demostración: Mostraremos que si a esta suma le restamos $\ln(L(s, \chi))$ nos da una función analítica en un entorno de 1. Dado que $\ln(L(s, \chi))$ es una función analítica (porque probamos antes que $L(s, \chi) \neq 0$ si $\chi \neq \chi_0$, esto nos implica que $\sum_{\text{primos}} \frac{\chi(p)}{p^s}$ también lo es en un entorno de 1.

$$\begin{aligned} \ln(L(s, \chi)) - \sum_p \frac{\chi(p)}{p^s} &= \ln \left(\prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} \right) - \sum_p \frac{\chi(p)}{p^s} \\ &= \sum_p \left(-\ln \left(1 - \frac{\chi(p)}{p^s}\right) - \frac{\chi(p)}{p^s} \right) = \sum_p \left(\sum_{n=1}^{\infty} \frac{\chi^n(p)}{np^{ns}} - \frac{\chi(p)}{p^s} \right) = \sum_p \sum_{n=2}^{\infty} \frac{\chi^n(p)}{np^{ns}} \end{aligned}$$

Esta serie es absolutamente convergente en $\{s/Re(s) > 1/2\}$:

$$\begin{aligned} \sum_p \sum_{n=2}^{\infty} \left| \frac{\chi^n(p)}{np^{ns}} \right| &= \sum_p \sum_{n=2}^{\infty} \frac{1}{np^{nRe(s)}} \\ &< \sum_p \sum_{n=2}^{\infty} p^{-nRe(s)} = \frac{1}{2} \sum_p \frac{p^{-2Re(s)}}{1 - p^{-Re(s)}} = \frac{1}{2} \sum_p \frac{1}{p^{Re(s)}(p^{Re(s)} - 1)} \end{aligned}$$

que converge (porque los términos decrecen como $1/p^{2Re(s)}$, y $2Re(s) > 1$). \square

Teorema 3.3.

$$\lim_{s \rightarrow 1^+} \left(\sum_{p \equiv a} p^{-s} - \frac{1}{\phi(b)} \sum_{\text{primos}} p^{-s} \right)$$

es finito si $a \in (\mathbb{Z}/(b))^*$

Demostración:

$$\sum_{\chi \in \hat{G}} \chi(a^{-1}) \sum_p \frac{\chi(p)}{p^s} =$$

(podemos cambiar el orden de la suma porque $\sum_p \frac{\chi(p)}{p^s}$ converge absolutamente si $\operatorname{Re}(s) > 1$)

$$= \sum_p \frac{\sum_{\chi \in \hat{G}} \chi(a^{-1}p)}{p^s} =$$

(por proposición 1.02, sabemos que si $z \neq e \Rightarrow \sum_{\chi \in \hat{G}} \chi(z) = 0$; y si $z = e$, nos da $|G| = |(\mathbb{Z}/(b))^*| = \phi(b)$)

$$= \sum_{p \equiv a \pmod{b}} \frac{\phi(b)}{p^s} = \phi(b) \sum_{p \equiv a \pmod{b}} \frac{1}{p^s}$$

Podemos escribir de otra forma la suma del comienzo, separando el término de χ_0 :

$$\begin{aligned} \sum_{\chi \in \hat{G}} \chi(a^{-1}) \sum_p \frac{\chi(p)}{p^s} &= \chi_0(a^{-1}) \sum_p \frac{\chi_0(p)}{p^s} + \sum_{\chi \neq \chi_0} \chi(a^{-1}) \sum_p \frac{\chi(p)}{p^s} = \\ &= \sum_p \frac{1}{p^s} + \sum_{\chi \neq \chi_0} \chi(a^{-1}) \sum_p \frac{\chi(p)}{p^s} \end{aligned}$$

Juntando las dos igualdades que nos quedaron:

$$\phi(b) \sum_{p \equiv a \pmod{b}} \frac{1}{p^s} = \sum_p \frac{1}{p^s} + \sum_{\chi \neq \chi_0} \chi(a^{-1}) \sum_p \frac{\chi(p)}{p^s}$$

o, lo que es lo mismo:

$$\sum_{p \equiv a \pmod{b}} \frac{1}{p^s} - \frac{1}{\phi(b)} \sum_p \frac{1}{p^s} = \frac{1}{\phi(b)} \sum_{\chi \neq \chi_0} \chi(a^{-1}) \sum_p \frac{\chi(p)}{p^s}$$

Y por el lema anterior, sumado a que \hat{G} es finito, tenemos probado el teorema. \square

4. Teorema de Chebotarev

El teorema de Chebotarev es una generalización del de Dirichlet:

Teorema 4.1. *Sea L una extensión Galois de un cuerpo de números K . Para $\sigma \in \operatorname{Gal}(L/K)$, definimos C_σ como la clase de conjugación de σ . Sea S el conjunto de P ideales primos de K tales que $\forall \mathbf{P}$ primo de L arriba de P , el elemento de Frobenius de \mathbf{P} está en C_σ . Entonces S tiene densidad de Dirichlet $\frac{|C_\sigma|}{|\operatorname{Gal}(L/K)|}$.*

Para ver cómo sigue el teorema de Dirichlet a partir de este, tomemos $K=\mathbb{Q}$, $L=\mathbb{Q}(\zeta_b)$, donde ζ_b es una de las raíces b -ésimas primitivas de 1.

$\mathbb{Q}(\zeta_b)$ es una extensión abeliana de \mathbb{Q} con grupo de Galois $(\mathbb{Z}/(b))^\times$, por lo tanto $C_\sigma = \{\sigma\} \forall \sigma \in Gal(\mathbb{Q}(\zeta_b)/\mathbb{Q})$, y el elemento de Frobenius de \mathbf{P} es el símbolo de Artin $\left(\frac{\mathbb{Q}(\zeta_b)/\mathbb{Q}}{p}\right) = \hat{p} \in (\frac{\mathbb{Z}}{b\mathbb{Z}})^* \forall$ primo \mathbf{P} arriba de p que no divida a b .

Esto nos da una correspondencia biyectiva entre las clases de conjugación (*mod* b) de los primos que no dividen a b y los elementos del grupo de Galois, entonces en el enunciado del teorema nos queda $S_a = \{p \in \mathbb{Z} \text{ primo} / p \equiv a \pmod{b}\}$. Dado que $|C_\sigma| = 1$ y $|Gal(\mathbb{Q}(\zeta_b)/\mathbb{Q})| = \phi(b)$, el teorema nos dice que la densidad de S_a es $\frac{1}{\phi(b)} \forall a \in (\mathbb{Z}/b\mathbb{Z})^*$, lo que dice el teorema de Dirichlet.