ON THE DENSITY THEOREM OF ČEBOTAREV

Shaunak Bhandarkar
Euler Circle
Palo Alto CA 94303, USA
shaunak@gmail.com

June 6, 2019

ABSTRACT

In this paper, we do exactly what the title implies: prove the Čebotarev Density Theorem. This is an extremely valuable theorem because it is a vast generalization of Dirichlet's Theorem on primes in an arithmetic progression, which states that for any $a, n \in \mathbb{Z}_+$ relatively prime, there are infinitely many primes that are $\equiv a \pmod{n}$. Our theorem goes even further to the case of other number fields; we will show that the prime ideals in an imaginary quadratic field K are virtually equidistributed among the conjugacy classes of Artin symbols in the Galois group of a Galois extension L over K. Note that L need not be abelian over K.

We start by introducing the L-functions. This will familiarize us with the most basic definitions as well as important functions. Then, we talk about convergence of L-functions, which will be especially important in later sections.

Next, we briefly visit some character theory. Specifically, the study of Dirichlet characters will help us prove important statements regarding partial zeta functions that will aid us in our journey to the Density Theorem. We then return to our study of L-functions and incorporate some of the theory that we have built up to this point. In particular, we derive an important theorem regarding where an L-function is analytic.

At this point, we introduce the notion of density. Starting with polar density, we explore various density-related properties and go on to prove some powerful results, such as the Artin map being surjective.

Then, we move on to Dirichlet density (and briefly introduce natural density). We prove that if polar density exists, then so does Dirichlet density, and that the two are equal. This nicely connects these two forms of density. We also explore some properties of Dirichlet density.

In the next section, we deepen our treatment of L-functions. We introduce several of the concepts in class field theory that allow us to derive preliminary density results. Most importantly, we prove that for a nontrivial Dirichlet character of the ray class group, the corresponding L-function does not vanish at $s = 1$.

By generalizing our arguments in the study of L-functions, we establish the theory needed to prove the main theorem in the case of an abelian extension $L \supset K$. At this point, we finally arrive at the main theorem, and prove it in the case of non-abelian extensions by cleverly connecting it to the abelian case.

Finally, we come to what is arguably the most important section: applications of the Čebotarev Density Theorem. This theorem has prolific applications, ranging from the theory of binary quadratic forms to the first main theorem of complex multiplication, although we just list a few. We then part with some concluding remarks.

Keywords Class Field Theory · Čebotarev Density Theorem · Analytic Number Theory · Algebraic Number Theory

1 A Review of L-Series

We start this paper by introducing basic notions needed to prove the main theorem. The first big topic is L-Series. These sums carry valuable information pertaining to prime density, which we will see later on. We assume basic knowledge of number fields and algebraic number theory. For a refresher of some of the assumed knowledge, check out Bhandarkar [8].

Definition 1.1. A Dirichlet series is a sum of the form

$$f(n) = \sum_{n \geq 1} \frac{a(n)}{n^s}$$

where $a(n) \in \mathbb{C}$ and $s = \sigma + it \in \mathbb{C}$. An Euler product belonging to a number field K is a product of the form

$$g(n) = \prod_{\mathfrak{p}} \frac{1}{(1 - \theta_1(\mathfrak{p}) N\mathfrak{p}^{-s}) \cdots (1 - \theta_d(\mathfrak{p}) N\mathfrak{p}^{-s})}$$

where $\theta_i(\mathfrak{p}) \in \mathbb{C}$, $s \in \mathbb{C}$, and $\mathfrak{p}$ runs over all but finitely many prime ideals of the ring of integers, $\mathcal{O}_K$. Also, N over here denotes the norm function.

Let us look at two important examples of Dirichlet series.

1. The Riemann zeta function is
$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_{p} \frac{1}{1 - p^{-s}}$$
Notice that the sum is equal to the product because of unique factorization in $\mathbb{Z}$.
2. More importantly, we will explore the Dedekind zeta function,
$$\zeta_K(s) = \sum_{\mathfrak{a} \geq 0} \frac{1}{N\mathfrak{a}^s} = \prod_{\mathfrak{p}} \frac{1}{1 - N\mathfrak{p}^{-s}}$$
The sum is over the integral ideals of $\mathcal{O}_K$ while the product is over the prime ideals of $\mathcal{O}_K$. Furthermore, the sum above is equal to the product because of unique factorization of ideals into prime ideals in the ring of integers $\mathcal{O}_K$ (because it is a Dedekind domain).

Definition 1.2. Let $I_K^{\mathfrak{m}}$ denote the set of fractional ideals in $\mathcal{O}_K$ that are coprime to the modulus $\mathfrak{m}$. Define a Dirichlet character χ to be a homomorphism

$$\chi : I_K^{\mathfrak{m}} \longrightarrow \mathbb{C}^{\times}$$

that is trivial over the principal class $P_{K,1}$ of the ray class group $C_{\mathfrak{m}} = I_K^{\mathfrak{m}} / P_{K,1}$. In other words, χ is a character over the ray class group.

Notice that χ somewhat resembles the Artin map (which we will explicitly characterize in Theorem 6.4), though it is not quite the same. Still, characters are especially useful when dealing with L-functions.

Definition 1.3. A Dirichlet L-series for a given character χ is

$$L(s, \chi) = \sum_{\mathfrak{a} \subset \mathcal{O}_K, (\mathfrak{a}, \mathfrak{m}) = 1} \frac{\chi(\mathfrak{a})}{N\mathfrak{a}^s} = \prod_{(\mathfrak{p}, \mathfrak{m}) = 1} \frac{1}{1 - \chi(\mathfrak{p}) N\mathfrak{p}^{-s}}$$

Once again, we can turn the sum into the product because of unique factorization of ideals in $\mathcal{O}_K$.

2 Convergence of L-series

In this section, we list some analytic statements regarding the convergence of Dirichlet series. We omit the proof of most theorems in this section; they generally reduce to extensive computation. Still, they make good exercises for the reader.

Proposition 2.1. *Let*

$$f(n) = \sum_{n \geq 1} \frac{a(n)}{n^s}$$

be a Dirichlet series and let $S(x) = \sum_{n \leq x} a(n)$, and suppose there exist constants a and b such that $|S(x)| \leq ax^b$ for all large x. Then, $f(s)$ converges uniformly for s in

$$D(b, \delta, \epsilon) = \{\Re(s) \geq b + \delta, \arg(s - b) \leq \pi/2 - \epsilon\}$$

for all $\delta, \epsilon \geq 0$, and it converges to an analytic function on the half plane $\Re(s) > b$. (Note that $\Re(s)$ denotes the real part of s.)

Lemma 2.2. *The Riemann zeta function $\zeta(s)$ has a meromorphic continuation to the half plane $\Re(s) > 0$ with a simple pole at $s = 1$.*

Lemma 2.3. *For s real and $s > 1$,*

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

Hence, $\zeta(s)$ has a simple pole at $s = 1$ and

$$\zeta(s) = \frac{1}{s-1} + \textit{function holomorphic near } 1$$

Proof. This is left as an exercise to the reader. (Hint: Look at the graph of $y = x^{-s}$ and relate $\zeta(s)$ to the area under the curve.) ■

Armed with this fact, we can look at other interesting Dirichlet series.

Proposition 2.4. *Let $f(n)$ be a Dirichlet series for which there exists constants C, a, and $b < 1$ such that $|S(n) - an| \leq Cx^b$. Then, f extends to a meromorphic function on $\Re(s) > b$ with a simple pole at $s = 1$ with residue a.*

Proof. For the Dirichlet series $f(s) - a\zeta(s)$, $|S(n)| \leq Cx^b$, so by Proposition 2.1, this series converges for $\Re(s) > b$. The result readily follows. ■

Before we move on, we encounter one last lemma that will prove to be useful soon.

Lemma 2.5. *Let $u_1, u_2, \cdots$ be a sequence of real numbers ≥ 2 for which*

$$f(s) = \prod_{j=1}^{\infty} \frac{1}{1 - u_j^{-s}}$$

is uniformly convergent on each region $D(1, \delta, \epsilon)$ (with $\delta, \epsilon > 0$). Then,

$$\log f(s) \sim \sum \frac{1}{u_j^s}$$

as $s \to 1^+$ (i.e., from the right side of the plane).

Proof. This is a simple exercise in manipulating sums. (Hint: use the Maclaurin series for $\log(1 - x)$ and then break the double sum apart.) ■

3 Characters and Partial Zeta Functions

Now, we introduce some basic character theory. In particular, knowing certain statements about characters - namely, the orthogonality relations - will aid us in our study of L-functions.

Definition 3.1. A one-dimensional representation of a group G, i.e. $\chi : G \longrightarrow \mathbb{C}^\times$ is a character of G. Note that this map is a homomorphism.

Proposition 3.2. *For a character χ of G, we have that* $\sum_{a \in G} \chi(a) = \begin{cases} |G| & \text{if } \chi = \chi_0 \text{ (the trivial character)} \\ 0 & \text{otherwise} \end{cases}$

Proof. The first part is obvious. If we have a nontrivial character χ, then for some $g \in G$, $\chi(g) \neq 1$. Then,

$$\chi(g) \sum_{a \in G} \chi(a) = \sum_{a \in G} \chi(ga) = \sum_{a \in G} \chi(a),$$

meaning $\sum_{a \in G} \chi(a) = 0$, as desired. ■

Proposition 3.3. *Suppose the group G is abelian. Fix some $a \in G$. Then,*

$$\sum_{\chi \in \hat{G}} \chi(a) = \begin{cases} |G| & \text{if } a = 1 \\ 0 & \text{otherwise} \end{cases}$$

Here, $\hat{G} = \mathrm{Hom}(G, C^\times)$ is the character group of G.

Proof. Using the fact that G is noncanonically isomorphic to $\hat{G}$, this proof becomes identical to that of the previous proposition. ■

Before we introduce some new tools, let us provide some motivation to our treatment of L-functions. Let K be a number field and $\mathfrak{m}$ be some modulus. Begin with the Dedekind zeta function, $\zeta_K(s)$. For some class $\mathfrak{t} \in C_\mathfrak{m}$ (i.e., the class group), define the partial zeta function to be

$$\zeta(s, \mathfrak{t}) = \sum_{\mathfrak{a} \geq 0, \mathfrak{a} \in \mathfrak{t}} \frac{1}{N\mathfrak{a}^s}$$

Note that for every character χ of the class group,

$$\zeta_K(s) = \sum_{\mathfrak{t} \in C_\mathfrak{m}} \zeta(s, \mathfrak{t}) \text{ and}$$

$$L(s, \chi) = \sum_{\mathfrak{t} \in C_\mathfrak{m}} \chi(\mathfrak{t}) \zeta(s, \mathfrak{t})$$

In other words, knowing about $\zeta(s, \mathfrak{t})$ can tell us about the Dedekind zeta function as well as the corresponding L-function.

Theorem 3.4. *The partial zeta function $\zeta(s, \mathfrak{t})$ is analytic for $\Re(s) > 1 - \frac{1}{[K:\mathbb{Q}]}$ except for a simple pole at $s = 1$. If we let $g_\mathfrak{m}$ denote the residue at $s = 1$, then $g_\mathfrak{m}$ is independent of $\mathfrak{t}$.*

Proof. We omit the proof of this theorem, mainly because it relies on the famous class number formula. It allows us to determine exactly what $g_\mathfrak{m}$ is. ■

Corollary 3.5. *If χ is not the trivial character, the L-function $L(s, \chi)$ is analytic for $\Re(s) > 1 - \frac{1}{[K:\mathbb{Q}]}$.*

Proof. Near $s = 1$,

$$L(s, \chi) = \sum_{\mathfrak{t} \in C_\mathfrak{m}} \chi(\mathfrak{t}) \zeta(s, \mathfrak{t}) = \frac{\sum_{\mathfrak{t} \in C_\mathfrak{m}} \chi(\mathfrak{t}) g_\mathfrak{m}}{s - 1} + \text{ holomorphic function}$$

and Proposition 3.2 shows us that the numerator of the first term is 0. ■

4 Polar Density

At last, we come across one type of density. For a set T of prime ideals of K, we define $\zeta_{K,T}(s) = \prod_{\mathfrak{p} \in T} \frac{1}{1 - N\mathfrak{p}^{-s}}$.

Definition 4.1. If some positive integral power $\zeta_{K,T}(s)^n$ of $\zeta_{K,T}(s)$ extends to a meromorphic function on a neighborhood of 1 having a pole of order m at 1, we say that T has polar density $\delta(T) = \frac{m}{n}$.

Proposition 4.2 (Properties of Polar Density)**.** *We have the following assertions:*

1. *The set of all prime ideals of K has polar density 1.*
2. *The polar density of every set is nonnegative.*
3. *If T is the disjoint union of T_1 and T_2, and two of the three polar densities exist, then so does the third, and we have $\delta(T) = \delta(T_1) + \delta(T_2)$.*
4. *If $T \subset T'$, then $\delta(T) \leq \delta(T')$.*
5. *A finite set has density zero.*

Proof.

1. We know that $\zeta_{K,T}(s)$ extends to a neighborhood of 1, where it has a simple pole. Thus $\frac{m}{n} = 1$, as desired.
2. Having a negative polar density means $m < 0$, i.e., $\zeta_{K,T}(s)$ is holomorphic in a neighborhood of $s = 1$ and zero there. However, $\zeta_{K,T}(1) = \prod_{\mathfrak{p} \in T} \frac{1}{1 - N\mathfrak{p}^{-1}} > 0$, meaning polar density is nonnegative.
3. Observe that $\zeta_{K,T}(s) = \zeta_{K,T_1}(s) \cdot \zeta_{K,T_2}(s)$. Suppose $\zeta_{K,T}(s)^n$ and $\zeta_{K,T_1}(s)^{n_1}$ extend to meromorphic functions with poles of order m and m_1, respectively; the other two cases are identical. Then
$$\zeta_{K,T_2}(s)^{nn_1} = \frac{\zeta_{K,T}(s)^{nn_1}}{\zeta_{K,T_1}(s)^{nn_1}}$$
extends to a meromorphic function in a neighborhood of $s = 1$ and has a pole there of order $mn_1 - m_1 n$. Thus, $\delta(T_2) = \frac{mn_1 - m_1 n}{nn_1} = \frac{m}{n} - \frac{m_1}{n_1} = \delta(T) - \delta(T_1)$, as desired.
4. This follows readily from 3.
5. This is obvious; $m = 0$ because $\zeta_{K,T}(s)$ is finite and positive. Moreover, there is no pole at $s = 1$.

■

Proposition 4.3. *If T contains no primes $\mathfrak{p}$ for which $N\mathfrak{p}$ is prime (in $\mathbb{Z}$), then $\delta(T) = 0$.*

Proof. Let $\mathfrak{p}$ be a prime in T. Since $N\mathfrak{p} = p^f$ (where p lies under $\mathfrak{p}$ in $\mathbb{Z}$ and f denotes the inertial degree of $\mathfrak{p}$), we must have $f \geq 2$; if $f = 1$, $N\mathfrak{p}$ would be prime. Moreover, for any given prime $p \in \mathbb{Z}$, there are at most $[K : \mathbb{Q}]$ primes of K lying over p. Thus, $\zeta_{K,T}(s)$ can be decomposed into a product $\prod_{1 \leq i \leq [K:\mathbb{Q}]} g_i(s)$ of d infinite products over the prime numbers, with each factor of g_i being either a 1 or a $\frac{1}{1-p^{-fs}}$ (for every prime p). Thus, for any i, $g_i(1) \leq \prod_p \frac{1}{1-p^{-f_p}} \leq \prod_p \frac{1}{1-p^{-2}} = \zeta(2) = \frac{\pi^2}{6}$. Thus, $g_i(s)$ is holomorphic at $s = 1$, meaning that the order of the pole there must be 0 (recall that polar density cannot be negative). We conclude that $\delta(T) = 0$. ■

Corollary 4.4. *Let T_1 and T_2 be sets of prime ideals in K. If the sets differ only by primes $\mathfrak{p}$ for which $N\mathfrak{p}$ is not prime and one of the two sets has polar density, then so does the other, and the densities are equal.*

At last, the time has come to exploit the power of polar density. It turns out we can derive some important analytic results.

Theorem 4.5. *Let $L \supset K$ be a field extension of finite degree and let M be its Galois closure. Then the set of prime ideals of K that split completely in L has density $\frac{1}{[M:K]}$.*

Proof. The first thing to notice is that a prime ideal $\mathfrak{p}$ of K splits completely in L if and only if it splits completely in M. One direction is easy: if it splits completely in M, it must split completely in the subfield L. If it splits completely in L, then it also splits completely in every conjugate field L'. All of these conjugate fields must lie under the decomposition field (the fixed field of the decomposition group of $\mathrm{Gal}(M/K)$), and so their compositum is a field lying under the decomposition field as well. This field is just M! $\mathfrak{p}$ splits completely only up to and including the decomposition field, so we conclude that it splits completely in M as well.

Thus, it suffices to prove this theorem with the assumption that L is Galois over K. Let S be the set of prime ideals of K that split completely in L and let T be the primes of L lying over a prime ideal in S. For each $\mathfrak{p} \in S$, there are exactly $[L : K]$ prime ideals $\mathfrak{P} \in T$, and for each of them, $N_K^L(\mathfrak{P}) = \mathfrak{p}$ (where N_K^L denotes norm). Thus, $N\mathfrak{P} = N\mathfrak{p}$ (where N denotes norm over $\mathbb{Q}$). This tells us that $\zeta_{L,T}(s) = \zeta_{K,S}(s)^{[L:K]}$. Also, T contains every prime ideal of L that is unramified over K and for which $N\mathfrak{P}$ is prime (in $\mathbb{Z}$). Thus, T differs from the set of all prime ideals in L by a set of polar density 0 (using Corollary 4.4), and so T has density 1. Moreover, this shows that $\zeta_{K,S}$ has the property signifying that S is a set of polar density $\frac{1}{[L:K]}$, as desired. ■

Corollary 4.6. *If $f(x) \in K[x]$ splits into linear factors modulo $\mathfrak{p}$ for all but finitely many prime ideals $\mathfrak{p}$ of K, then f splits into linear factors in K.*

Proof. If L is the splitting field of f, then L is Galois over K. Now, use Theorem 4.5 on L/K. For more interesting details, see Bhandarkar [8], Section 4. ■

Corollary 4.7. *For every abelian extension L/K and every finite set S of primes of K including those that ramify in L, let I_K^S denote the fractional ideals that are prime to all ideals in S. Then, the Artin map*

$$\left(\frac{L/K}{\cdot}\right) : I_K^S \longrightarrow \mathrm{Gal}(L/K)$$

is surjective.

Proof. Let H be the image of the Artin map; it is some subgroup of $\mathrm{Gal}(L/K)$. If its fixed field is L^H, then we see that $H = \mathrm{Gal}(L/L^H)$ is the image. For all $\mathfrak{p} \notin S$, $\left(\frac{L^H/K}{\mathfrak{p}}\right) = \left(\frac{L/K}{\mathfrak{p}}\right)|_{L^H} = 1$, which implies that $\mathfrak{p}$ splits completely in L^H. Thus, all but finitely many prime ideals of $\mathcal{O}_K$ split completely in L^H, so Theorem 4.5 tells us that $[L^H : K] = 1$; in other words, the Artin map is surjective. ■

5 Dirichlet Density

Define two functions $f(s)$ and $g(s)$ for $s > 1$ and real. We write $f(s) \sim g(s)$ as $s \to 1^+$ if $\lim_{s\to 1^+} \frac{f(s)}{g(s)} = 1$. Then, $f(s) \sim \delta \log \frac{1}{s-1}$ as $s \to 1^+$ means

$$\lim_{s\to 1^+} \frac{f(s)}{\log \frac{1}{s-1}} = \delta.$$

When f and g are holomorphic in a neighborhood of $s = 1$ except for possibly poles at $s = 1$, then $f \sim g$ if and only if f and g differ by a function that is holomorphic in a neighborhood of $s = 1$.

Definition 5.1. Let T be a set of primes of K. If there exists a δ such that

$$\sum_{\mathfrak{p}\in T} \frac{1}{N\mathfrak{p}^s} \sim \delta \log \frac{1}{s-1} \text{ as } s \to 1^+$$

then we say that T has Dirichlet density δ.

Definition 5.2. If the limit

$$\lim_{x\to\infty} \frac{\text{number of } \mathfrak{p} \in T \text{ with } N\mathfrak{p} \le x}{\text{number of } \mathfrak{p} \text{ with } N\mathfrak{p} \le x}$$

exists, then we call it the natural density of T.

Natural density is much more intuitive than the other types of density, and one might wonder if at all natural density is ever equal to Dirichlet density or polar density. The answer, though reassuring, is somewhat surprising:

Proposition 5.3.

1. *If polar density exists, then so does Dirichlet density, and the two are equal.*
2. *If natural density exists, then so does Dirichlet density, and the two are equal.*

Proof. We only prove the first part. If T has polar density $\frac{m}{n}$, then

$$\zeta_{K,T}(s)^n = \frac{a}{(s-1)^m} + \frac{g(s)}{(s-1)^{m-1}}$$

where g is holomorphic near $s = 1$. Furthermore, $a > 0$ because $\zeta_{K,T}(s) > 0$ for $s > 1$ and real. Taking logs and applying Lemma 2.5 gives us

$$n \sum_{\mathfrak{p}\in T} \frac{1}{N\mathfrak{p}^s} = m \log \frac{1}{s-1}$$

In other words, T has Dirichlet density $\frac{m}{n}$, as desired. ■

Remark 5.4. A set can have a Dirichlet density without having a natural density. For example, let T be the set of prime numbers with leading digit 1. Then, T does not have a natural density, but it has a Dirichlet density, namely $\log_{10} 2$. Thus, it is a stronger statement to say that a set has natural density.

Also, notice that polar densities are rational numbers. Thus, every set having a natural density that is irrational will not have a polar density!

Now, we shall see that Dirichlet density has similar properties to those of polar density:

Proposition 5.5 (Properties of Dirichlet Density)**.**

1. *The set of all prime ideals of K has Dirichlet density* 1.
2. *The Dirichlet density of any set is nonnegative.*
3. *If T is the disjoint union of T_1 and T_2, and two of the three Dirichlet densities exist, then so does the third, and $\delta(T) = \delta(T_1) + \delta(T_2)$.*
4. *If $T \subset T'$, then $\delta(T) \leq \delta(T')$.*
5. *If T is finite, then $\delta(T) = 0$.*

Proof.

1. The set of prime ideals of K even has polar density 1, which is stronger.
2. For $s > 0$ and real, $\frac{1}{N\mathfrak{p}^s} > 0$ and for $s \to 1^+$, $\log \frac{1}{s-1} > 0$, so Dirichlet density must be nonnegative.
3. Clearly,
$$\sum_{\mathfrak{p} \in T} \frac{1}{N\mathfrak{p}^s} = \sum_{\mathfrak{p} \in T_1} \frac{1}{N\mathfrak{p}^s} + \sum_{\mathfrak{p} \in T_2} \frac{1}{N\mathfrak{p}^s}$$
so long as $\Re(s) > 1$. Thus, if
$$\sum_{\mathfrak{p} \in T_1} \frac{1}{N\mathfrak{p}^s} \sim \delta_1 \log \frac{1}{s-1} \text{ and } \sum_{\mathfrak{p} \in T_2} \frac{1}{N\mathfrak{p}^s} \sim \delta_2 \log \frac{1}{s-1}$$
then
$$\sum_{\mathfrak{p} \in T} \frac{1}{N\mathfrak{p}^s} \sim (\delta_1 + \delta_2) \log \frac{1}{s-1}$$
The other two cases are virtually identical to this one.
4. This readily follows from 3.
5. When T is finite, $\sum_{\mathfrak{p} \in T} \frac{1}{N\mathfrak{p}^s}$ is holomorphic for all s and thus bounded near any point. In particular, as $s \to 1^+$, the Dirichlet density must go to 0.

■

Proposition 5.6. *Let T be the set of prime ideals of K having degree 1 over $\mathbb{Q}$, i.e., for which the inertial degree $f(\mathfrak{p}/p) = 1$. Then, $\delta(T) = 1$.*

Proof. Proposition 4.3 tells us that the complement of T has polar density equal to 0, and thus, Dirichlet density equal to 0 as well. ■

Corollary 5.7. *Let T be as in the proposition. Then, for every set S of primes in K having Dirichlet density,*
$$\delta(T \cap S) = \delta(S)$$

Proof. The complement T' of T has Dirichlet density 0, so $\delta(S) = \delta(S \cap T) + \delta(S \cap T') = \delta(S \cap T)$, since $\delta(S \cap T') \leq \delta(T') = 0$. ■

6 Making Magic out of L-functions

At last, it is time to put together some of our basic results. We can do this by playing around with L-functions. The value of L-functions, especially as $s \to 1^+$ is crucial to our discussion surrounding the Čebotarev Density Theorem.

Definition 6.1. Recall that for a number field K and a modulus $\mathfrak{m}$, we say that a subgroup $H \subset I_K^{\mathfrak{m}}$ is a congruence subgroup for $\mathfrak{m}$ if it satisfies $P_{K,1} \subset H \subset I_K^{\mathfrak{m}}$. In this case, the quotient $I_K^{\mathfrak{m}}/H$ is called a generalized ideal class group for $\mathfrak{m}$.

Proposition 6.2. *Let $\mathfrak{m}$ be a modulus for K and let H be a congruence subgroup for $\mathfrak{m}$:*

$$P_{K,1} \subset H \subset I_K^{\mathfrak{m}}$$

Then, if $L(1,\chi)$ is nonzero for all nontrivial characters χ of the ray class group $I_K^{\mathfrak{m}}/H$, $\delta(\{\mathfrak{p} \in H\}) = \frac{1}{(I_K^{\mathfrak{m}}:H)}$; otherwise, it is 0.

Proof. Let $h = (I_K^{\mathfrak{m}} : H)$ and χ be a character of $I_K^{\mathfrak{m}}$ trivial on H, and as usual, let

$$L(s,\chi) = \prod_{\mathfrak{p} \nmid \mathfrak{m}} \frac{1}{1 - \chi(\mathfrak{p}) N\mathfrak{p}^{-s}}$$

Lemma 2.5 tells us that

$$\log L(s,\chi) \sim \sum_{\mathfrak{p} \nmid \mathfrak{m}} \frac{\chi(\mathfrak{p})}{N\mathfrak{p}^s} \text{ as } s \to 1^+$$

But Proposition 3.3 (note that $I_K^{\mathfrak{m}}/H$ is abelian) gives us

$$\sum_{\chi} \chi(\mathfrak{p}) = \begin{cases} h \text{ if } \mathfrak{p} \in H \\ 0 \text{ if } \mathfrak{p} \notin H \end{cases}$$

Thus, summing over all χ, we get

$$\sum_{\chi} \log L(s,\chi) \sim h \sum_{\mathfrak{p} \in H} \frac{1}{N\mathfrak{p}^s} \text{ as } s \to 1^+$$

Now, if $\chi \neq \chi_0$, then $L(s,\chi)$ is holomorphic near $s = 1$, ie. $L(s,\chi) = (s-1)^{m(\chi)}(g(s))$, where $m(\chi) \geq 0$ and $g(1) \neq 0$. Thus, $\log L(s,\chi) \sim m(\chi) \log(s-1) = -m(\chi) \log \frac{1}{s-1}$. If $\chi = \chi_0$, then

$$L(s,\chi) = \frac{\zeta_K(s)}{\prod_{\mathfrak{p}|\mathfrak{m}} \frac{1}{1 - N\mathfrak{p}^{-s}}}$$

which means that

$$\log L(s,\chi_0) \sim \log \zeta_K(s) \sim \log \frac{1}{s-1}$$

Thus, we find that

$$h \sum_{\mathfrak{p} \in H} \frac{1}{N\mathfrak{p}^s} \sim (1 - \sum_{\chi \neq \chi_0} m(\chi)) \log \frac{1}{s-1}$$

and hence

$$\delta(\{\mathfrak{p} \in H\}) = \frac{1 - \sum_{\chi \neq \chi_0} m(\chi)}{h}$$

This shows that $\delta(\{\mathfrak{p} \in H\}) = \frac{1}{h}$ if $L(1,\chi) \neq 0$ for every $\chi \neq \chi_0$; otherwise, the density must be 0 (i.e. exactly one of the $m(\chi)$ must be equal to 1, meaning at most one $L(s,\chi)$ can have a zero at $s = 1$ since Dirichlet density is nonnegative, and it must be a simple zero). ■

Now, we visit an inequality that will give us useful information about L-functions:

Theorem 6.3 (The Second Inequality)**.** *For every Galois extension L of K and modulus $\mathfrak{m}$ of K,*

$$(I_K^{\mathfrak{m}} : P_{K,1} \cdot N_K^L(I_L^{\mathfrak{m}})) \leq [L : K]$$

Note that here, $I_L^{\mathfrak{m}}$ denotes the set of fractional ideals of L (lying above ideals of $I_K^{\mathfrak{m}}$) prime to $\mathfrak{m}$.

Proof. Let $H = P_{K,1} \cdot N_K^L(I_L^{\mathfrak{m}})$. If $\mathfrak{p}$ splits in L, then $f(\mathfrak{P}/\mathfrak{p}) = 1$ for all $\mathfrak{P} \subset \mathcal{O}_L$ lying over $\mathfrak{p} \subset \mathcal{O}_K$, in which case $\mathfrak{p}$ is the norm of any prime ideal of $\mathcal{O}_L$ lying over it. Thus, $\{\mathfrak{p} \in H\}$ contains the set of prime ideals splitting completely in L. Then, Theorem 4.5 tells us that

$$\delta(\{\mathfrak{p} \in H\}) \geq [L : K]^{-1} > 0$$

Moreover, Proposition 6.2 tells us that if $\delta(\{\mathfrak{p} \in H\}) > 0$, it must be equal to $(I_K^{\mathfrak{m}} : H)^{-1}$. This only occurs if for all nontrivial characters χ of $I_K^{\mathfrak{m}}/H$, $L(1, \chi) \neq 0$. Finally, we have

$$(I_K^{\mathfrak{m}} : H) = \delta(\{\mathfrak{p} \in H\})^{-1} \leq [L : K]$$

■

This theorem is particularly important because it tells us that if H is of the form as in Proposition 6.2, then $L(1, \chi) \neq 0$ for all nontrivial characters χ of $I_K^{\mathfrak{m}}/H$. But when we are given a Galois extension $L \supset K$, how do we know this hypothesis is satisfied? Lucky for us, Artin Reciprocity comes to the rescue!

Theorem 6.4 (Reciprocity Law)**.** *Let L be a finite Abelian extension of K, and let S be the set of primes of K ramifying in L. Then, the Artin map*

$$\left(\frac{L/K}{\cdot}\right) : I_K^S \longrightarrow \mathrm{Gal}(L/K)$$

admits a modulus $\mathfrak{m}$ such that a prime of K (finite or infinite) ramifies if and only if it divides $\mathfrak{m}$ and induces the isomorphism

$$I_K^{\mathfrak{m}}/(P_{K,1} \cdot N_K^L(I_L^{\mathfrak{m}})) \xrightarrow{\sim} \mathrm{Gal}(L/K)$$

This theorem is literally the very foundation of class field theory. To use this theorem, we also introduce another important theorem of class field theory: the Existence Theorem.

Theorem 6.5 (Existence Theorem)**.** *For every congruence subgroup H modulo $\mathfrak{m}$, there exists a finite Abelian extension L/K such that $H = P_{K,1} \cdot N_K^L(I_L^{\mathfrak{m}})$.*

This theorem is nice because it complements Artin Reciprocity in a way that allows us to construct an important bijection. Notice that for H and L as in the theorem, Artin Reciprocity allows us to construct the isomorphism

$$I_K^{\mathfrak{m}}/H \xrightarrow{\sim} \mathrm{Gal}(L/K)$$

In particular, there is a field $L_{\mathfrak{m}}$ known as the ray class field modulo $\mathfrak{m}$ for which the Artin map defines an isomorphism

$$C_{\mathfrak{m}} = I_K^{\mathfrak{m}}/(P_{K,1} \cdot N_K^L(I_L^{\mathfrak{m}})) \xrightarrow{\sim} \mathrm{Gal}(L_{\mathfrak{m}}/K)$$

For a field $L \subset L_{\mathfrak{m}}$, set

$$N_K^L(C_{\mathfrak{m},L}) = (P_{K,1} \cdot N_K^L(I_L^{\mathfrak{m}}) \pmod{P_{K,1}}$$

Thus, the Existence Theorem provides the following beautiful corollary:

Corollary 6.6. *For a modulus $\mathfrak{m}$, the map $L \mapsto N_K^L(C_{\mathfrak{m},L})$ is a bijection from the set of Abelian extensions of K contained in $L_{\mathfrak{m}}$ to the set of subgroups of $C_{\mathfrak{m}}$.*

Proof. This is a rather neat result of applying the Galois correspondence. ■

Thus, class field theory shows us that the hypothesis of Proposition 6.2 is satisfied: every congruence subgroup H is of the form $P_{K,1} \cdot N_K^L(I_L^{\mathfrak{m}})$ for a unique Abelian extension $L \supset K$. For our particular discussion, we obtain the following corollary:

Corollary 6.7. *For any modulus $\mathfrak{m}$ of K and any nontrivial Dirichlet character $\chi : C_{\mathfrak{m}} \longrightarrow \mathbb{C}^{\times}$, $L(1, \chi) \neq 0$.*

7 Proof of the Čebotarev Density Theorem

At last, we have the tools necessary to prove our main theorem. We will start by handling the abelian case and cleverly use that to tackle the nonabelian case.

Theorem 7.1. *Let $\mathfrak{m}$ be a modulus for K, and let H be a congruence subgroup for $\mathfrak{m}$. For any class $\mathfrak{t} \in I_K^{\mathfrak{m}}/H$, the set of prime ideals in $\mathfrak{t}$ has Dirichlet density $\frac{1}{(I_K^{\mathfrak{m}} : H)}$.*

Proof. It suffices to prove a more general version of Proposition 6.2. Consider some class $\mathfrak{t} \in I_K^{\mathfrak{m}}/H$ and let $\mathfrak{a}$ be a coset representative of this class. Also, let $h = (I_K^{\mathfrak{m}} : H)$. Much like we considered the sum $\sum_\chi \log L(s,\chi)$, we now consider the sum

$$\sum_\chi \chi(\mathfrak{a})^{-1} \log L(s,\chi) \sim \sum_\chi \chi(\mathfrak{a})^{-1} \sum_{\mathfrak{p} \nmid \mathfrak{m}} \frac{\chi(\mathfrak{p})}{N\mathfrak{p}^s} = \sum_{\mathfrak{p} \nmid \mathfrak{m}} \sum_\chi \frac{\chi(\mathfrak{a}^{-1}\mathfrak{p})}{N\mathfrak{p}^s} = h \sum_{\mathfrak{p} \in \mathfrak{t}} \frac{1}{N\mathfrak{p}^s}$$

where we obtain the last equality by applying our character orthogonality relations.

Now, Corollary 6.7 shows us that $L(1,\chi) \neq 0$ for any nontrivial χ. Thus, using the terminology of Proposition 6.2, we see that if $L(s,\chi) = (s-1)^{m(\chi)} g(s)$ near $s = 1$, then in fact $m(\chi) = 0$. Thus, density-wise, $\log L(s,\chi) \sim -m(\chi) \log \frac{1}{s-1} = 0$ as $s \to 1^+$, so $L(s,\chi)$ for nontrivial characters χ do not contribute to the Dirichlet density.

However, if $\chi = \chi_0$, then as we found before, $\log L(s,\chi_0) \sim \log \frac{1}{s-1}$. Thus, by summing $\log L(s,\chi)$ across all χ in the character group, we see that

$$h \sum_{\mathfrak{p} \in \mathfrak{t}} \frac{1}{N\mathfrak{p}^s} \sim \log \frac{1}{s-1} \text{ or } \delta(\{\mathfrak{p} \in \mathfrak{t}\}) = \frac{\sum_{\mathfrak{p} \in \mathfrak{t}} \frac{1}{N\mathfrak{p}^s}}{\log \frac{1}{s-1}} = \frac{1}{h}$$

as desired. ■

Corollary 7.2. *Let $L \supset K$ be a finite Abelian extension and let $\sigma \in \mathrm{Gal}(L/K)$. Then, the set of prime ideals $\mathfrak{p}$ of K that are unramified in L and for which $\left(\frac{L/K}{\mathfrak{p}}\right) = \sigma$ has Dirichlet density $\frac{1}{[L:K]}$.*

Proof. Artin Reciprocity gives us the isomorphism $I_K^{\mathfrak{m}}/H \xrightarrow{\sim} \mathrm{Gal}(L/K)$ for some modulus $\mathfrak{m}$ and congruence subgroup H. Thus, the inverse image of σ is one entire class $\mathfrak{t}$ of $I_K^{\mathfrak{m}}/H$. At this point, we may apply Theorem 7.1 to obtain the result. ■

Voilà! We have just proven the Čebotarev Density Theorem for Abelian extensions $L \supset K$! At this point, we may extend to the general (not necessarily abelian) case:

Theorem 7.3 (Čebotarev)**.** *Let L be a finite Galois extension of the field K and suppose $\sigma \in \mathrm{Gal}(L/K)$. Moreover, denote C by the conjugacy class of σ in $\mathrm{Gal}(L/K)$. Then, the set*

$$T = \{\mathfrak{p} \text{ a prime ideal in } \mathcal{O}_K \mid \mathfrak{p} \text{ unramified in } L, \left(\frac{L/K}{\mathfrak{p}}\right) = \sigma\}$$

has Dirichlet density

$$\delta(T) = \frac{|C|}{|\mathrm{Gal}(L/K)|} = \frac{|C|}{[L:K]}$$

.

Proof. Since $\mathrm{Gal}(L/K)$ is not necessarily abelian, we try to cleverly reduce to this case. Let $\sigma \in \mathrm{Gal}(L/K)$ have order f and let $M = L^{\langle\sigma\rangle}$ be the fixed field of the set of automorphisms $\langle\sigma\rangle$ (subgroup of automorphisms generated by σ). Then, L is a cyclic extension of M of degree f, and the Artin map gives us an isomorphism

$$C_{\mathfrak{m}}/H \xrightarrow{\sim} \langle\sigma\rangle$$

for some modulus $\mathfrak{m}$ of M and $H = P_{M,1} \cdot N_M^L(I_L^{\mathfrak{m}})$.

Now, let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$, $\mathfrak{q}$ be prime lying above $\mathfrak{p}$ in $\mathcal{O}_M$, and $\mathfrak{P}$ be a prime lying above $\mathfrak{q}$ in $\mathcal{O}_L$. If we let $c = |C|$ and $d = [L:K]$, we must show that $\delta(T) = \frac{c}{d}$. Also, we must note that in this proof, we ignore the finitely many primes that are not prime to $\mathfrak{m}$ (i.e. primes that ramify).

Let

$$T_{M,\sigma} = \{\mathfrak{q} \subset \mathcal{O}_M \mid \left(\frac{L/M}{\mathfrak{q}}\right) = \sigma, f(\mathfrak{q},\mathfrak{p}) = 1\}$$

By Corollary 7.2, we know that the set of primes satisfying the first condition (i.e. $\left(\frac{L/M}{\mathfrak{q}}\right) = \sigma$) of $T_{M,\sigma}$ has density $\frac{1}{f}$, and thus, $T_{M,\sigma}$ has density $\frac{1}{f}$ (using Corollary 5.7).

Now, let

$$T_{L,\sigma} = \{\mathfrak{P} \subset \mathcal{O}_L \mid \left(\frac{L/K}{\mathfrak{P}}\right) = \sigma\}$$

We aim to relate $T_{M,\sigma}$ and $T_{L,\sigma}$.

Lemma 7.4. *We have the following two assertions:*

1. *The map $\mathfrak{P} \mapsto \mathfrak{q} = \mathfrak{P} \cap \mathcal{O}_M$ defines a bijection $T_{L,\sigma} \to T_{M,\sigma}$.*
2. *The map $\mathfrak{P} \mapsto \mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K : T_{L,\sigma} \to T$ sends exactly $\frac{d}{cf}$ primes of $T_{L,\sigma}$ to each prime of T.*

Proof.

1. Take some $\mathfrak{P} \in T_{L,\sigma}$ and let $\mathfrak{q} = \mathfrak{P} \cap \mathcal{O}_M$ and $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. Then, the Decomposition Group $D(\mathfrak{P} \mid \mathfrak{p}) \cong \mathrm{Gal}(\mathcal{O}_L/\mathfrak{P} \,/\, \mathcal{O}_K/\mathfrak{p})$ is generated by σ but σ fixes the residue field $\mathcal{O}_M/\mathfrak{q}$ (because it fixes M). Thus, $\mathcal{O}_M/\mathfrak{q} = \mathcal{O}_K/\mathfrak{p}$, meaning that $f(\mathfrak{q}/\mathfrak{p}) = 1$. This means that $\mathfrak{q} \in T_{M,\sigma}$, so we have a map
$$\mathfrak{P} \mapsto \mathfrak{q} = \mathfrak{P} \cap \mathcal{O}_M : T_{L,\sigma} \to T_{M,\sigma}$$
This map is injective because $f(\mathfrak{P}/\mathfrak{q}) = f(\mathfrak{q}/\mathfrak{p})^{-1} f(\mathfrak{P}/\mathfrak{p}) = 1 \cdot f = f$, so $\mathfrak{P}$ is the only prime of $\mathcal{O}_L$ lying over $\mathfrak{q}$. Moreover, this map is surjective because for any prime $\mathfrak{P}$ lying over $\mathfrak{q} \in T_{M,\sigma}$,
$$\left(\frac{L/K}{\mathfrak{P}}\right) = \left(\frac{L/K}{\mathfrak{P}}\right)^{f(\mathfrak{q}/\mathfrak{p})} = \left(\frac{L/M}{\mathfrak{q}}\right) = \sigma$$
and so $\mathfrak{P}$ lies in $T_{L,\sigma}$. Thus, our map is a bijection.

2. Fix a $\mathfrak{p}_0 \in T$ and let $\mathfrak{P}_0 \in T_{L,\sigma}$ lie over $\mathfrak{p}_0$. Then, for $\tau \in \mathrm{Gal}(L/K)$,
$$\left(\frac{L/K}{\tau\mathfrak{P}_0}\right) = \tau \left(\frac{L/K}{\mathfrak{P}_0}\right) \tau^{-1}$$
and so
$$\tau \left(\frac{L/K}{\mathfrak{P}_0}\right) \tau^{-1} = \sigma \iff \tau \in C_G(\sigma)$$
where $C_G(\sigma)$ denotes the centralizer of σ in $\mathrm{Gal}(L/K)$. Therefore, the map $\tau \mapsto \tau\mathfrak{P}_0$ gives us a bijection
$$C(\sigma)/D(\mathfrak{P}_0/\mathfrak{p}_0) \longrightarrow \{\mathfrak{P}_0 \in T_{L,\sigma} \mid \mathfrak{P}_0 \cap \mathcal{O}_K = \mathfrak{p}_0\}$$
where $D(\mathfrak{P}_0/\mathfrak{p}_0)$ denotes decomposition group. The decomposition group is $\langle\sigma\rangle$, which has order f and $C_G(\sigma)$ has order $\frac{d}{c}$ because there is a bijection
$$\tau \mapsto \tau\sigma\tau^{-1} : \mathrm{Gal}(L/K)/C_G(\sigma) \to C$$
Therefore, $(C_G(\sigma) : D(\mathfrak{P}_0/\mathfrak{p}_0)) = \frac{d}{cf}$. Thus, we have shown that for each $\mathfrak{p} \in T$, there are exactly $\frac{d}{cf}$ primes $\mathfrak{P} \in T_{L,\sigma}$ lying over $\mathfrak{p}$. This completes part 2.

■

Returning to our proof, we can combine statements 1 and 2 to obtain the map
$$\mathfrak{q} \mapsto \mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$$
which is a $\frac{d}{cf} : 1$ map $T_{M,\sigma} \to T$. For such a $\mathfrak{q}$, $N_K^M(\mathfrak{q}) = \mathfrak{p}$, so $N\mathfrak{q} = N\mathfrak{p}$. Hence
$$\sum_{\mathfrak{p} \in T} \frac{1}{N\mathfrak{p}^s} = \frac{cf}{d} \sum_{\mathfrak{q} \in T_{M,\sigma}} \frac{1}{N\mathfrak{q}^s} \sim \frac{cf}{d} \cdot \frac{1}{d} \log \frac{1}{s-1} = \frac{c}{d} \log \frac{1}{s-1}$$
which completes the proof of the Čebotarev Density Theorem. ■

Remark 7.5. Interestingly enough, the prime number theorem generalizes nicely to general number fields; it is called the Landau Prime Ideal Theorem. Using this theorem and keeping the notation we used above, if we set
$$\pi_C(x) = \{\mathfrak{p} \text{ is a finite, unramified prime ideal of } \mathcal{O}_K \mid \left(\frac{L/K}{\mathfrak{p}}\right) = C, N\mathfrak{p} \leq x\}$$
then we can obtain the following effective form of the Density Theorem:
$$\pi_C(x) \sim \frac{c}{d} \frac{x}{\log x}.$$

8 Applications of the Density Theorem

The Density Theorem has many applications throughout number theory. By no means do we provide a full treatment of its applications; rather, we focus on a few rather elegant examples. We start by pointing out a simple yet special case: Dirichlet's Theorem on Primes in Arithmetic Progression.

Corollary 8.1 (Dirichlet)**.** *For any positive integers a and m, with $\gcd(a, m) = 1$, there are infinitely many primes p for which $p \equiv a \pmod{m}$.*

Proof. Using the Čebotarev Density Theorem, we will prove an even stronger result: that the set of primes $\equiv a \pmod{m}$ has Dirichlet density $\frac{1}{\phi(m)}$ in the set of primes (of $\mathbb{Z}$), where ϕ denotes the totient function.

Now, let ζ_m be an m^{th} root of unity. Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_m)$ be a cyclotomic extension. We know that L/K is Galois and that $\mathrm{Gal}(L/K) \cong (\mathbb{Z}/m\mathbb{Z})^\times$. This isomorphism can be made explicit by taking some $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ and mapping it to the unique automorphism that takes ζ_m^k to ζ_m^{ak}.

For a prime number $p \in \mathbb{Z}$, $N(p\mathbb{Z}) = p$. If $\mathfrak{P} \subset \mathcal{O}_L$ is a prime lying over p such that $\sigma \in \mathrm{Gal}(L/K)$ satisfies $\sigma(\alpha) \equiv \alpha^{N(p\mathbb{Z})} \pmod{\mathfrak{P}}$, we must have $\sigma(\zeta_m^k) = \zeta_m^{pk}$ for all k. As long as $p \nmid m$, $p\mathbb{Z}$ does not ramify in L, in which case $\left(\frac{L/K}{p\mathbb{Z}}\right) = \bar{p} \in \mathrm{Gal}(L/K)$, where $\bar{p}$ is the class of p modulo m. Thus, $\left(\frac{L/K}{p\mathbb{Z}}\right) = a$ if and only if $p \equiv a \pmod{m}$. At this point, the Density Theorem states that the density of primes $p\mathbb{Z}$ of $\mathbb{Q}$ such that $\left(\frac{L/K}{p\mathbb{Z}}\right) = a$ is $\frac{1}{|\mathrm{Gal}(L/K)|} = \frac{1}{\phi(m)}$, as desired. ∎

So being able to prove Dirichlet's theorem with a snap of our fingers is a sign of just how powerful the Čebotarev Density Theorem is! Now, we move on to another interesting application, which explores primes that split completely in number fields. In particular, these primes can characterize a given extension $L \supset K$. First, we introduce some terminology.

Definition 8.2. Given two sets $\mathcal{S}$ and $\mathcal{T}$, we say $\mathcal{S} \dot{\subset} \mathcal{T}$ if $\mathcal{S} \subset \mathcal{T}$ up to a finite set of elements. We also say $\mathcal{S} \doteq \mathcal{T}$ if $\mathcal{S} \dot{\subset} \mathcal{T}$ and $\mathcal{T} \dot{\subset} \mathcal{S}$.

Definition 8.3. Given an extension $L \supset K$, we set

$$\mathcal{S}_{L/K} = \{\mathfrak{p} \text{ is a finite prime ideal of } K \mid \mathfrak{p} \text{ splits completely in } L\}$$

.

Also, let

$$\tilde{\mathcal{S}}_{L/K} = \{\mathfrak{p} \text{ is a finite prime ideal of } \mathcal{O}_K \mid \mathfrak{p} \text{ unramified in } L, f(\mathfrak{P} \mid \mathfrak{p}) = 1 \text{ for some prime } \mathfrak{P} \text{ of } L \text{ lying over } \mathfrak{p}\}$$

Using this terminology, we can effectively state the following powerful theorem:

Theorem 8.4. *Let L and M be finite extensions of K. Then:*

1. *If M is Galois over K, then $L \subset M \iff \mathcal{S}_{M/K} \dot{\subset} \mathcal{S}_{L/K}$.*
2. *If L is Galois over K, then $L \subset M \iff \tilde{\mathcal{S}}_{M/K} \dot{\subset} \mathcal{S}_{L/K}$*

Proof. We begin with the proof of 2. When $L \subset M$, we easily have $\tilde{\mathcal{S}}_{M/K} \dot{\subset} \mathcal{S}_{L/K}$; indeed, for $\mathfrak{p} \in \tilde{\mathcal{S}}_{M/K}$, $f(\mathfrak{P} \mid \mathfrak{p}) = 1$ for some $\mathfrak{P}$ lying over $\mathfrak{p}$ in $\mathcal{O}_M$. Thus, if $\mathfrak{q}$ is a prime of $\mathcal{O}_L$ lying over $\mathfrak{p}$ and under $\mathfrak{P}$, then we must have $f(\mathfrak{q} \mid \mathfrak{p}) = 1$. But since inertial degrees of all conjugates of a prime ideal are the same in a Galois extension, we conclude that $\mathfrak{p}$ has inertial degree $f = 1$ in L. Moreover, since it is unramified, we conclude that $\mathfrak{p}$ splits completely in L, and thus $\mathfrak{p} \in \mathcal{S}_{L/K}$ as well.

Conversely, suppose that $\tilde{\mathcal{S}}_{M/K} \dot{\subset} \mathcal{S}_{L/K}$, and let N be a Galois extension of K containing both L and M; it suffices to show that $\mathrm{Gal}(N/M) \subset \mathrm{Gal}(N/L)$. Thus, given $\sigma \in Gal(N/M)$, we need to prove that $\sigma \mid_L = 1$. By the Čebotarev Density Theorem, there is a prime $\mathfrak{p}$ in K, unramified in N such that $\left(\frac{N/K}{\mathfrak{p}}\right)$ is the conjugacy class of σ. Thus, there is some prime $\mathfrak{P}$ of N for which $\left(\frac{N/K}{\mathfrak{P}}\right) = \sigma$. We claim that $\mathfrak{p} \in \tilde{\mathcal{S}}_{M/K}$. To see this, let $\mathfrak{P}' = \mathfrak{P} \cap \mathcal{O}_M$. Then, for $\alpha \in \mathcal{O}_M$,

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

where the first congruence follows from $\sigma \mid_M = 1$ and the second from the definition of the Artin symbol. Thus, the Artin symbol is trivial, meaning that $f(\mathfrak{P}' \mid \mathfrak{p}) = 1$ (since f is the order of the decomposition group generated by the Artin symbol, which is trivial). This means $\mathfrak{p} \in \tilde{\mathcal{S}}_{M/K}$, as desired. The Density Theorem implies that there are infinitely many such $\mathfrak{p}$'s. Thus, $\tilde{\mathcal{S}}_{M/K} \dot{\subset} \mathcal{S}_{L/K}$ tells us that $\mathfrak{p} \in \mathcal{S}_{L/K}$, i.e., $\left(\frac{L/K}{\mathfrak{p}}\right) = 1$, meaning that $\sigma \mid_L = \left(\frac{N/K}{\mathfrak{P}}\right) \mid_L = \left(\frac{L/K}{\mathfrak{p}}\right) = 1$, as desired.

Now, to prove 1, note that $L \subset M$ easily implies $\mathcal{S}_{M/K} \dot{\subset} \mathcal{S}_{L/K}$ using the exact same reasoning as in the proof of part 2 above. To show the other direction, let L' be the Galois closure of L over K. Using the reasoning from Theorem 4.5, we see that a prime of K splits completely in L if and only if it splits completely in L'. Thus, $\mathcal{S}_{L/K} = \mathcal{S}_{L'/K}$. Thus, our hypothesis $\mathcal{S}_{M/K} \dot{\subset} \mathcal{S}_{L/K}$ may be rephrased as $\mathcal{S}_{M/K} \dot{\subset} \mathcal{S}_{L'/K}$. By part 2, we obtain $L' \subset M$, so $L \subset M$, and we are done. ■

Why did we bother to prove all of that? For one, it tells us about the relationship between field extension and the prime ideals contained in them. Moreover, it allows us to formulate the following corollary:

Corollary 8.5. *Let L and M be Galois extensions of K. Then:*

1. $L \subset M \iff \mathcal{S}_{M/K} \dot{\subset} \mathcal{S}_{L/K}$.
2. $L = M \iff \mathcal{S}_{M/K} \doteq \mathcal{S}_{L/K}$.

Proof. Notice first that 1 immediately implies 2, so it suffices to prove just 1. Now, observe that if M is Galois over K, then $\tilde{\mathcal{S}}_{M/K}$ reduces to $\mathcal{S}_{M/K}$, so applying Theorem 8.4 immediately proves part 1 of this corollary. ■

Now, we introduce one last application, which is to the theory of binary quadratic forms. Although we do not prove it here, it points out a beautiful interplay between binary quadratic forms and ideals in number fields.

Theorem 8.6. *Let $f(x, y) = ax^2 + bxy + cy^2$ be a primitive positive definite binary quadratic form of discriminant $D < 0$. Moreover, let $\mathcal{S}$ be the set of primes represented by f. Then, the Dirichlet density $\delta(\mathcal{S})$ exists and is equal to*

$$\delta(\mathcal{S}) = \begin{cases} \frac{1}{2h(D)} \text{ if } f \text{ is properly equivalent to its opposite} \\ \frac{1}{h(D)} \text{ otherwise} \end{cases}$$

where $h(D)$ is the famous class number. In particular, f represents infinitely many prime numbers!

Proof. We omit the proof because it relies on developing a theory of ideals in orders of imaginary quadratic fields. Still, we refer the reader to Cox [1]. ■

9 Some Parting Remarks

The Čebotarev Density Theorem is elegant and powerful. It is at a crossroads between algebraic and analytic number theory, and has various applications across number theory. We sincerely hope the reader has taken away something useful from this paper and is inclined to learn more about related topics.

References

[1] Cox, D.: Primes of the Form $x^2 + ny^2$. 2nd edn. Wiley-Interscience (1997)

[2] Marcus, D.: Number Fields. 2nd edn. Springer International Publishing (2018)

[3] Serre, Jean-Perre.: Linear Representations of Finite Groups. 1st edn. Springer-Verlag New York (1977)

[4] Artin, Michael.: Algebra. 2nd edn. Pearson (2010)

[5] Janusz, Gerald . 2nd edn. American Mathematical Society (2005)

[6] Milne, James. Class Field Theory. Retrieved from http://www.jmilne.org/math/CourseNotes/CFT.pdf. Version 4.02. 2013.

[7] Triantafillou, Nicholas. The Chebotarev Density Theorem. Retreived from https://math.mit.edu/ ngtriant/notes/chebotarev.pdf (2015)

[8] Bhandarkar, Shaunak. From Hilbert Class Field Theorey to Complex Multiplication. Retreived from https://drive.google.com/file/d/1SE1GEhtP-UWMUOTcWtJOPLuPOkYjiRw3/view (2018)

[9] Yott, Dylan.: Frobenius Elements, the Chebotarev Density Theorem, and Reciprocity. Retreived from https://math.berkeley.edu/ dyott/Frobenius%20elements.pdf (2014)

[10] Lenstra, Henrik. and Stevenhagen, Peter.: Chebotarëv and his Density Theorem. Retreived from http://websites.math.leidenuniv.nl/algebra/chebotarev.pdf (2002)

[11] Conrad, Brian.: Dirichlet Density for Global Fields. Retreived from http://math.stanford.edu/ conrad/676Page/handouts/dirdensity.pdf (2004)