THE CHEBOTAREV DENSITY THEOREM

NICHOLAS GEORGE TRIANTAFILLOU

Abstract. The Chebotarev density theorem states that for a finite Galois extension of number fields L/K and a conjugacy class $\mathcal{C} \subset \mathrm{Gal}(L/K)$, if δ denotes the density of primes $\mathfrak{p}$ of K such that the Artin symbol satisfies $\left[\frac{L/K}{\mathfrak{p}}\right] = \mathcal{C}$ then δ exists and is equal to $\#\mathcal{C}/\#\,\mathrm{Gal}(L/K)$. This result (and its proof) has played an important role in the development of modern number theory, inspiring Artin's proof of class field theory and several important results in modern arithmetic geometry. We give two proofs of the Chebotarev density theorem: Chebotarev's original proof [Tsc26], which predates class field theory, and a more recent proof due to Lagarias and Odlyzko [LO77] and refined by Serre [Ser81] which gives an "effective" error term. We also give several applications of the Chebotarev density theorem and discuss its connection with Dirichlet's theorem on primes in arithmetic progressions.

This work was completed while supported by an NSF Graduate Fellowship.

Contents

1. Introduction

This paper is an expository paper on the Chebotarev density theorem and some applications written as a final project for Math 229X - Introduction to Analytic Number Theory as taught by Noam Elkies at Harvard in the Fall of 2015. We make an effort to keep this paper mostly self-contained, but in the interest of brevity, assume some standard definitions from analytic number theory.

The notation used in the paper should be mostly self-explanatory. We include a brief appendix on notation, just in case.

Before we can discuss the Chebotarev density theorem, we need a definition.

Definition 1.1 (The Artin Symbol)**.** Let L/K be a finite Galois extension of number fields. For any prime $\mathfrak{p}$ of $\mathcal{O}_K$ and any prime $\mathfrak{P}$ of L lying over $\mathfrak{p}$, the *Artin symbol* $\left[\frac{L/K}{\mathfrak{P}}\right]$ is the unique element $\sigma \in \mathrm{Gal}(L/K)$ such that

$$\sigma(\alpha) = \alpha^{\mathrm{Nm}(\mathfrak{p})} \pmod{\mathfrak{P}} \text{ for all } \alpha \in L. \tag{1.1}$$

For any $\mathfrak{p}$, all of the primes $\mathfrak{P}$ lying over $\mathfrak{p}$ are isomorphic via elements of $\mathrm{Gal}(L/K)$. Hence, the values of $\left[\frac{L/K}{\mathfrak{P}}\right]$ lying over $\mathfrak{p}$ are all conjugate in $\mathrm{Gal}(L/K)$. We denote by $\left[\frac{L/K}{\mathfrak{p}}\right]$ the conjugacy class of $\left[\frac{L/K}{\mathfrak{P}}\right]$ in $\mathrm{Gal}(L/K)$ for any $\mathfrak{P}$ lying over $\mathfrak{p}$. In the case that $\mathrm{Gal}(L/K)$ is abelian, we abuse notation and use $\left[\frac{L/K}{\mathfrak{p}}\right]$ to refer to the single element of the conjugacy class.

Informally, the Chebotarev density theorem says that for any finite Galois extension of number fields L/K and any conjugacy class $\mathcal{C} \subset \mathrm{Gal}(L/K)$, the number of primes $\mathfrak{p}$ of $\mathcal{O}_K$ such that $\left[\frac{L/K}{\mathfrak{p}}\right] = \mathcal{C}$ is proportional to the size of $\mathcal{C}$. This can be thought of as an equidistribution result on primes. Although it is not obvious at first, we shall see throughout this paper (and particularly in Section 3) that the Chebotarev density theorem is a generalization of and is intimately related to Dirichlet's theorem on the infinitude of primes in arithmetic progressions.

It would be difficult to overstate the importance of the Chebotarev density theorem to modern number theory. Since its proof, it has been one of the most important tools for proving that various interesting subsets of primes are infinite. In the past 40 years, since the development of "effective" versions, the Chebotarev density has also been applied to the study of coefficients of modular forms, ℓ-adic representations of infinite Galois groups, and many other subjects at the forefront of modern number theory and arithmetic geometry. Serre developed several of these applications in [Ser81]. These applications are beyond the scope of this report, so we content ourselves to very briefly describe the general flavor of these results in Section 7.

The Chebotarev density theorem (or at least its original proof) had another extremely important consequence for modern number theory. While it might not be obvious from most modern treatments, which present the density theorem as a consequence of class field theory, the proof of the Chebotarev density theorem predated and inspired Artin's original proof of class field theory. For more details on the historical context of the Chebotarev density theorem in number theory (as well as an engaging account of the life and other work of Nikolai Chebotarev), see [SL96].

1.1. **Outline.** The remainder of the paper begins with three sections of setup and general discussion, followed by two sections proving two different "strengths" of the Chebotarev density theorem by two different methods, and finishing with a section presenting some applications.

More precisely, in Section 2, we give three different statements of the Chebotarev density theorem: Chebotarev's original statement without an error term and two "effective" versions due to Lagarias and Odlyzko [LO77] with a refinement by Serre [Ser81] that specify the error term of the Chebotarev density theorem for L/K in terms of d_L

(the absolute value of the the discriminant of L) and n_L (the index of L over $\mathbb{Q}$). After giving these precise statements of the Chebotarev density theorem, we demonstrate the relationship between Chebotarev's density theorem and Dirichlet's theorem on primes in arithmetic progressions in Section 3. In Section 4 we introduce and briefly compare Artin L-functions and Dirichlet-Hecke L-functions, the central analytic objects needed for our proofs.

Sections 5 and 6 contain most of the heavy analytic number theory. In Section 5, we present a proof of the Chebotarev density theorem for Dirichlet density without error term. We roughly follow the treatment of Chebotarev's original proof as described in [FJ08]. In particular, we do not assume knowledge of class field theory with the exception of one statement the special case of cyclotomic extensions.

Section 6 is an exposition of Lagarias and Odlyzko's "effective" version of the Chebotarev density theorem, based on their proof in [LO77]. We attempt to capture the heart of the argument, which is remarkably similar to the proof of Dirichlet's theorem in [Dav00]. We fill in a few details omitted in [LO77], while omitting other details covered in depth in the original paper. [LO77] is an excellent resource for the reader interested in an extremely clear treatment of the details we omit.

Finally, we close the paper by discussing several different problems to which the Chebotarev density and its effective versions can be applied. We present four different types of applications, including proving the infinitude of a subset of primes, improving upper bounds on the size of zero density sets of primes, computing Galois groups, and proving that different collections of data about field extensions are equivalent. Besides giving a bit more information on each of these applications in Section 7, we work out two simple applications in detail.

2. Statement of Main Results

In order to state our main results precisely, we need to recall the following definitions.

Definition 2.1 (Dirichlet and Natural Density for Number Fields)**.** Let K be a number field, and let $Q(K)$ be some set of prime ideals of $\mathcal{O}_K$. The quantity

$$\lim_{s\to 1^+} \left(\sum_{\mathfrak{p}\in Q(K)} \frac{1}{(\operatorname{Nm}\mathfrak{p})^s} \right) / \left(\sum_{\mathfrak{p}\in P(K)} \frac{1}{(\operatorname{Nm}\mathfrak{p})^s} \right) \tag{2.1}$$

is called the Dirichlet density of $Q(K)$ if the limit exists. The quantity

$$\lim_{x\to\infty} \#\{\mathfrak{p}\in Q(K) : \operatorname{Nm}\mathfrak{p}\le x\}/\#\{\mathfrak{p}\in P(K) : \operatorname{Nm}\mathfrak{p}\le x\} \tag{2.2}$$

is called the natural density of $Q(K)$ if the limit exists.

We can now state the main results of this paper. (The statements are quoted from [FJ08] for Theorem 2.2, [Ser81] for Theorem 2.3, and [LO77] for Theorem 2.4.)

Theorem 2.2. *Let L/K be a finite Galois extension of number fields and let $\mathcal{C}$ be a conjugacy class of* $\operatorname{Gal}(L/K)$*. Let*

$$P_{\mathcal{C}} := \left\{ \mathfrak{p}\in P(K) : \mathfrak{p} \text{ is unramified in } L,\ \left[\frac{L/K}{\mathfrak{p}}\right] = \mathcal{C} \right\}.$$

Then, the Dirichlet (resp. natural) density of $P_{\mathcal{C}}$ in $\{\mathfrak{p} \in P(K) : \mathfrak{p}$ is unramified in $L\}$ exists and is equal to $\frac{\#\mathcal{C}}{\#\operatorname{Gal}(L/K)}$.

Theorem 2.2 (for Dirichlet density) is essentially the original statement of the Chebotarev density theorem, as proved in [Tsc26] in 1926.

Set

$$\pi_{\mathcal{C}}(x, L/K) = \{\#\mathfrak{p} \in P_{\mathcal{C}} : \operatorname{Nm}\mathfrak{p} \leq x\}. \tag{2.3}$$

After a short computation, the natural density version of Theorem 2.2 can be rephrased as

$$\pi_{\mathcal{C}}(x, L/K) \sim \frac{\#\mathcal{C}}{\#\operatorname{Gal}(L/K)} \int_2^x \frac{dt}{\log t} \sim \frac{\#\mathcal{C}}{\#\operatorname{Gal}(L/K)} \frac{x}{\log x} \text{ as } x \to \infty. \tag{2.4}$$

While this is certainly a powerful statement, early proofs of Theorem 2.2 and (2.4) either gave no information about the error terms or gave estimates including constants depending in an unpredictable way on the fields L and K. In their 1977 paper [LO77], Lagarias and Odlyzko made progress towards resolving this deficiency in the understanding of the subject by proving the following "effective" versions of the Chebotarev density theorem. We first give a statement conditional on GRH as refined by Serre in [Ser81].

Theorem 2.3 (Theorem 1.1. of [LO77] refined as in [Ser81])**.** *Let L/K be a Galois extension of number fields. Assume the generalized Riemann hypothesis for the Dedekind zeta function $\zeta_L(s)$. Then, there is an effectively computable positive absolute constant c such that for every $x > 2$,*

$$\left|\pi_{\mathcal{C}}(x, L/K) - \frac{\#\mathcal{C}}{\#\operatorname{Gal}(L/K)} \int_2^x \frac{dt}{\log t}\right| \leq c \left(\frac{\#\mathcal{C}}{\#\operatorname{Gal}(L/K)} x^{1/2} \log(d_L x^{n_L})\right). \tag{2.5}$$

Lagarias and Odlyzko also proved an unconditional version of their "effective" Chebotarev density theorem, with the remaining ineffectivity quantified in terms of the location of a possible Siegel zero. The shape of their result is reminiscent of the quantitative versions of Dirichlet's theorem on primes in arithmetic progressions. The result is

Theorem 2.4 (Theorem 1.3. of [LO77])**.** *If $n_L > 1$, then $\zeta_L(s)$ has at most one zero in the region defined by $s = \sigma + it$ with*

$$1 - (4 \log d_L)^{-1} \leq \sigma \leq 1, \quad |t| \leq (4 \log d_L)^{-1}. \tag{2.6}$$

If such a zero exists, it must be real and simple. Call it β_0.
Then, there exist effectively computable absolute constants c_1 and c_2 such that if

$$x \geq \exp(10 n_L (\log d_L)^2), \tag{2.7}$$

then

(2.8)

$$\left|\pi_{\mathcal{C}}(x, L/K) - \frac{\#\mathcal{C}}{\#\operatorname{Gal}(L/K)} \int_2^x \frac{dt}{\log t}\right| \leq \frac{\#\mathcal{C}}{\#\operatorname{Gal}(L/K)} \int_2^{x^{\beta_0}} \frac{dt}{\log t} + c_1 x \exp\left(-c_2 n_L^{-1/2} (\log x)^{1/2}\right),$$

where the β_0 term is present only when β_0 exists. If $\mathcal{C}$ is replaced by a union of conjugacy classes, the same estimate holds after multiplying the last error term by the number of conjugacy classes in $\mathcal{C}$.

Theorems 2.3 and 2.4 lead immediately to upper bounds on the lowest norm of a prime with $\left[\frac{L/K}{\mathfrak{p}}\right] = \mathcal{C}$, although better results along these lines can be achieved via more specialized methods, as in [LMO79].

While there are several other statements of the Chebotarev density theorem, including a version for function fields (see for example [FJ08]), such further statements are beyond the scope of this paper.

3. The Connection to Dirichlet's Theorem on Primes in Arithmetic Progressions

While on the surface the Chebotarev density theorem is a statement about how prime ideals behave under field extensions, the Chebotarev density theorem is also a generalization of Dirichlet's Theorem on primes in arithmetic progressions. Indeed, Dirichlet's theorem (modulo n) is the special case of the Chebotarev density theorem when $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_n)$, where ζ_n is a primitive nth root of unity.

Corollary 3.1 (Dirichlet's Theorem on Primes in Arithmetic Progressions)**.** *Let $a, n \geq 1$ be positive integers with $(a, n) = 1$. Then, the natural (resp. Dirichlet) density of primes p such that $p \equiv a \pmod{n}$ in the set of all primes of $\mathbb{Z}$ is $\frac{1}{\phi(n)}$.*

Proof. Let $\zeta_n \in \overline{\mathbb{Q}}$ be a primitive nth root of unity, $K = \mathbb{Q}$, and $L = \mathbb{Q}(\zeta_n)$. By the theory of cyclotomic extensions, L/K is Galois with $\mathrm{Gal}(L/K) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. This isomorphism is given explicitly by identifying an element $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ with the unique automorphism of L/K that maps ζ_n^k to ζ_n^{ak} for all k.

Now, for a prime number $p \in \mathbb{Z}$, $\mathrm{Nm}(p\mathbb{Z}) = p$. If $\mathfrak{P}$ is a prime of $\mathcal{O}_L$ lying over p such that $\sigma \in \mathrm{Gal}(L/K)$ satisfies $\sigma(\alpha) = \alpha^{\mathrm{Nm}(p\mathbb{Z})} \mod \mathfrak{P}$, we must have that $\sigma(\zeta_n^k) = \zeta_n^{pk} \mod \mathfrak{P}$ for all k. So long as $p \nmid n$, the ideal $p\mathbb{Z}$ does not ramify in L, so $\left[\frac{L/K}{p\mathbb{Z}}\right] = \overline{p} \in \mathrm{Gal}(L/K)$, where $\overline{p}$ is the class of p modulo n. Thus, $\left[\frac{L/K}{p\mathbb{Z}}\right] = a$ if and only if $p \equiv a \mod n$.

In our setting, Theorem 2.2 states that the natural (resp. Dirichlet) density of primes ideals $p\mathbb{Z}$ of $\mathbb{Q}$ such that $\left[\frac{L/K}{p\mathbb{Z}}\right] = a$ is $\frac{1}{\#\,\mathrm{Gal}(L/K)} = \frac{1}{\phi(n)}$. In other words, the natural (resp. Dirichlet) density of primes p such that $p \equiv a \mod n$ is $\frac{1}{\phi(n)}$. □

We have seen that Dirichlet's theorem is a special case of Chebotarev's density theorem. In some sense, Dirichlet's theorem is much more than a special case. For instance, the main analytic step in the proof of the Chebotarev density theorem is used to prove the theorem in the case where L/K is a cyclotomic extension (or an abelian extension if class field theory is assumed). The strategy for proving Chebotarev in this special case is very similar to the proof of Dirichlet's theorem, with Dirichlet L-functions replaced by a suitable generalization defined in terms of prime ideals of $\mathcal{O}_K$ and the extension

L. The full power of Chebotarev, first for abelian extensions and then for general extensions, follows by some clever applications of Galois theory. Even when controlling the error term, the strategy of proof is exactly the same as with Dirichlet's theorem, but with more complicated book-keeping. Modern proofs taking into account the error term tend to closely mirror the proof of Dirichlet's theorem with error term.

4. Dirichlet-Hecke L-Functions and Artin L-Functions

Having seen that the Chebotarev density theorem is a generalization of Dirichlet's theorem, we would like to mimic the proof. Before we have any hope of carrying out the proof, we need to answer the question: What is the right generalization of Dirichlet L-functions?

For our purposes, there are two answers: Dirichlet-Hecke L-functions and Artin L-functions. In the remainder of this section, we define both types of L-functions and discuss how they are related.

First, we define Dirichlet-Hecke L-functions. These L-functions generalize Dirichlet L-functions to base fields other than $\mathbb{Q}$. We first need to set up some notation as in section VI of [Lan86].

Definition 4.1. Let K be a number field with ring of integers $\mathcal{O}_K$. Let $\mathfrak{c} = \prod_{\mathfrak{p}} \mathfrak{p}^{m(\mathfrak{p})}$ be an ideal of $\mathcal{O}_K$ with its factorization into primes. Denote the localization of $\mathcal{O}_K$ at $\mathfrak{p}$ by $\mathcal{O}_{\mathfrak{p}}$ with maximal ideal $\mathfrak{m}_{\mathfrak{p}}$. Set

$$I(\mathfrak{c}) := \{\mathfrak{a} \text{ fractional ideals of } K : \mathfrak{a} \text{ and } \mathfrak{c} \text{ are relatively prime.}\}, \tag{4.1}$$

with the natural group structure and let

$$P(\mathfrak{c}) := \{\text{principal fractional ideals } x\mathcal{O}_K \text{ of } K \text{ satisfying (1) and (2).}\} \tag{4.2}$$

(1) If $m(\mathfrak{p}) > 0$, i.e. $\mathfrak{p}|\mathfrak{c}$, then $x \in \mathcal{O}_{\mathfrak{p}}$ and moreover $x \equiv 1 \mod \mathfrak{m}_{\mathfrak{p}}^{m(\mathfrak{p})}$.
(2) For each real embedding $\sigma : K \to \mathbb{R}$, $\sigma(x) > 0$, i.e. x is a *totally positive* element of K.

The quotient $G(\mathfrak{c}) = I(\mathfrak{c})/P(\mathfrak{c})$ is called the $\mathfrak{c}$-*ideal class group* of $\mathfrak{c}$.

Remark 4.2. To be precise, we are really defining the ideal class group of the $\mathfrak{c}$ together with *all* of the real places. The condition on the real embeddings can be relaxed to get an ideal class group which only takes into account some of the real places.

As with the usual ideal class group, the $\mathfrak{c}$-ideal class group is also finite. Theorem 1 of chapter VI of [Lan86] provides an explicit formula for the cardinality.

The finite abelian group $G(\mathfrak{c})$ will play the role in the construction of Dirichlet-Hecke L-functions that the group $(\mathbb{Z}/n\mathbb{Z})^\times$ plays in the construction of Dirichlet L-functions. Indeed, $G(\mathfrak{c})$ is a generalization of $(\mathbb{Z}/n\mathbb{Z})^\times$ to ideals of number fields. If $K = \mathbb{Z}$ and $\mathfrak{c} = n\mathbb{Z}$, then $I(n\mathbb{Z}) = \{a\mathbb{Z} : a \in \mathbb{Z}, (a, n) = 1\}$ and $P(n\mathbb{Z}) = \{a\mathbb{Z} : a \in \mathbb{Z}, a \equiv 1 \pmod{n}\}$, so $G(n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})^\times$.

Let $\widehat{G(\mathfrak{c})}$ denote the group of characters of $G(\mathfrak{c})$. We are now ready to define the Dirichlet-Hecke L-function associated to $\chi \in \widehat{G(\mathfrak{c})}$.

Definition 4.3. Let $\mathfrak{c}$ be an ideal of $\mathcal{O}_K$ and let $\chi \in \widehat{G(\mathfrak{c})}$. The Dirichlet-Hecke L-function associated to $\mathfrak{c}$ and χ is the analytic function

$$L_{\mathfrak{c}}(s,\chi) := \sum_{(\mathfrak{a},\mathfrak{c})=1} \frac{\chi(\mathfrak{a})}{(\operatorname{Nm}\mathfrak{a})^s} = \prod_{(\mathfrak{p},\mathfrak{c})=1} \left(1 - \frac{\chi(\mathfrak{p})}{(N\mathfrak{p})^s}\right)^{-1}, \tag{4.3}$$

defined on the half-plane $\operatorname{Re}(s) > 1$, where the sum is over all ideals $\mathfrak{a} \subset \mathcal{O}_K$ relatively prime to $\mathfrak{c}$ and the product is over all *prime* ideals $\mathfrak{p} \subset \mathcal{O}_K$ relatively prime to $\mathfrak{c}$. Note that the Euler product and L-series are equal because $\chi(\mathfrak{a}) \cdot \chi(\mathfrak{b}) = \chi(\mathfrak{a} \cdot \mathfrak{b})$.

Next, we define Artin L-functions, our second generalization of Dirichlet L-functions. Artin L-functions are defined as an Euler product involving representations of $\operatorname{Gal}(L/K)$ for a finite Galois extension L/K of number fields.

Definition 4.4. Let L/K be a Galois extension of number fields with Galois group $\operatorname{Gal}(L/K)$. Let $\rho : \operatorname{Gal}(L/K) \to V$ be a finite dimensional complex representation. For each prime $\mathfrak{p}$ of $\mathcal{O}_K$, choose a prime $\mathfrak{P}$ of $\mathcal{O}_L$ lying over $\mathfrak{p}$. Then, the Artin L-function associated to L/K and ρ is

$$L_{L/K}(s,\rho) := \prod_{\mathfrak{p} \subset \mathcal{O}_K} \det\left(1 - (\operatorname{Nm}\mathfrak{p})^{-s} \rho\left(\left[\frac{L/K}{\mathfrak{P}}\right]\right)\right)^{-1}, \tag{4.4}$$

on $\operatorname{Re}(s) > 1$, where we restrict to the subspace of V of elements fixed by the inertia group at $\mathfrak{P}$ before taking the determinant if $\mathfrak{p}$ ramifies in L. Note that the local factors are well-defined irrespective of the choice of $\mathfrak{P}$ over $\mathfrak{p}$ since making a different choice of $\mathfrak{P}$ corresponds to conjugating the matrix $\left(1 - (\operatorname{Nm}\mathfrak{p})^{-s} \rho\left(\left[\frac{L/K}{\mathfrak{P}}\right]\right)\right)$ by some $\rho(\sigma)$ and the determinant is conjugation-invariant.

In the special case where $L = \mathbb{Q}(\zeta_n)$ and $K = \mathbb{Q}$, we can identify elements of $\operatorname{Gal}(L/K)$ with characters of $(\mathbb{Z}/n\mathbb{Z})^\times$. In this case, the local factors at the unramified primes are $(1 - \chi(p)p^{-s})$, and (at least for primes not dividing n) we recover the Dirichlet L-functions modulo n.

Remark 4.5. Throughout the remainder of this paper, we will typically ignore the ramified primes when discussing Artin L-functions, although we will point out/bound their contribution when necessary. While this may seem cavalier, very little will be lost for our purposes since we are interested in density statements. Only finitely many primes ramify in a finite extension of number fields and the possible primes are well-controlled by invariants of the field, so ramification won't interfere too badly with our estimates.

Although Artin L-functions cannot typically be expressed as L-series when $\operatorname{Gal}(L/K)$ is non-abelian, the logarithm and logarithmic derivatives of Artin L-functions still have nice expressions. (See Section 2.1.4 of [Sny02] for full details.) Since $L_{L/K}(s,\rho)$ is defined as an Euler product, $\log L_{L/K}(s,\rho)$ is a sum over local factors. At a prime $\mathfrak{p}$ which does not ramify in L, the factor is $-\log\det\left(1 - (\operatorname{Nm}\mathfrak{p})^{-s}\rho\left(\left[\frac{L/K}{\mathfrak{P}}\right]\right)\right)$. Diagonalizing $\rho\left(\left[\frac{L/K}{\mathfrak{P}}\right]\right)$ turns the determinant into a product. Taking Taylor expansions of

each term, the factor at $\mathfrak{p}$ is $\sum_{m=1}^{\infty} \frac{1}{m} \operatorname{Tr} \rho \left(\left[\frac{L/K}{\mathfrak{P}} \right]^m \right) (\operatorname{Nm} \mathfrak{p})^{-sm}$. The ramified primes require a bit more attention since the local factors are more complicated. The result is as follows:

First, if $\phi = \operatorname{Tr}(\rho) : \operatorname{Gal}(L/K) \to \mathbb{C}$ is the character associated to the representation $\rho : \operatorname{Gal}(L/K) \to V$, $\mathfrak{P}$ is any ideal of $\mathcal{O}_L$ lying over the ideal $\mathfrak{p}$ of $\mathcal{O}_K$, and $I_{\mathfrak{P}}$ is the inertia group at $\mathfrak{P}$, write

$$\phi_K(\mathfrak{p}^m) := \frac{1}{\# I_{\mathfrak{P}}} \sum_{\alpha \in I_{\mathfrak{P}}} \phi \left(\left[\frac{L/K}{\mathfrak{P}} \right]^m \alpha \right). \tag{4.5}$$

This is well-defined since $\left[\frac{L/K}{\sigma(\mathfrak{P})} \right]^m = \sigma \circ \left[\frac{L/K}{\mathfrak{P}} \right]^m \circ \sigma^{-1}$, $I_{\sigma(\mathfrak{P})} = \sigma I_{\mathfrak{P}} \sigma^{-1}$ and ϕ is a class function. In this notation,

$$\log L_{L/K}(s, \phi) = \sum_{\mathfrak{p} \subset \mathcal{O}_K} \sum_{m=1}^{\infty} \frac{1}{m} \phi_K(\mathfrak{p}^m) (\operatorname{Nm} \mathfrak{p})^{-ms}, \tag{4.6}$$

$$-\frac{L'_{L/K}}{L_{L/K}}(s, \phi) = \sum_{\mathfrak{p} \subset \mathcal{O}_K} \sum_{m=1}^{\infty} \phi_K(\mathfrak{p}^m) \log(\operatorname{Nm} \mathfrak{p}) (\operatorname{Nm} \mathfrak{p})^{-ms}. \tag{4.7}$$

Warning: the functions ϕ_K are in general non-linear. In particular, we cannot take the exponent outside of the ϕ_K.

Dirichlet-Hecke L-functions and Artin L-functions each have their own advantages and disadvantages, particularly in the context of the Chebotarev density theorem. Artin L-functions clearly involve the Artin symbol – the function we are studying. The downside is that Artin L-functions use non-linear characters of the Galois group. As a result, we no longer have an L-series representation and therefore are deprived of several standard tools. For instance, the proof of analyticity for Dirichlet L-functions does not hold for general Artin L-functions. When working with Dirichlet-Hecke L-functions, the toolbox is full, but it is less clear how characters of a $\mathfrak{c}$-ideal class group relate to the Artin character.

Fortunately, class field theory implies that when L/K is an abelian extension, Artin L-functions are the same as Dirichlet-Hecke L-functions for appropriately chosen $\mathfrak{c}$ (up to modification at the ramified places). The general case of the Chebotarev density theorem follows from the case of abelian (in fact, cyclic) Galois group, using only a bit of field theory and representation theory of finite groups. Hence, we may assume that the extensions we are dealing with are abelian, in which case, we have the best of both worlds.

At this point, we recall that although this view may suggest that the Chebotarev density theorem is a consequence of class field theory, Chebotarev did not have access to the full statements of class field theory when he wrote his paper [Tsc26] in 1926. Indeed, the Chebotarev density theorem led to the first full proofs of class field theory.

5. The Chebotarev Density Theorem for Dirichlet Density

In this section, we prove Theorem 2.2, the original statement of the Chebotarev density theorem for Dirichlet density, following Chebotarev's original strategy [Tsc26].

Our treatment is inspired by [FJ08], although our notation is slightly different. The proof starts with the case that L/K is cyclotomic. This case goes as follows:

(1) Compute the volume of a fundamental domain of a certain lattice to bound the number of representatives of a class in $G(\mathfrak{c})$ with small norm. Use this to meromorphically continue $L_{\mathfrak{c}}(s,\chi)$ to a function on $\mathrm{Re}(s) > 1 - \frac{1}{n_K}$ which is analytic, except for a possible pole at 1 which exists if and only if χ is trivial.
(2) Prove a result from class field theory for cyclotomic extensions to see that the Dirichlet-Hecke L-functions are Artin L-functions.
(3) Use class field theory for cyclotomic extensions and the behavior at $s = 1$ of the zeta function $L_{\mathfrak{c}\mathcal{O}_L}(s,\chi_0)$ to conclude that $L_{\mathfrak{c}}(s,\chi) \neq 0$ for $\chi \neq \chi_0$.
(4) Take an appropriate character-weighted linear combination of the $L_{\mathfrak{c}}(s,\chi)$.

Note that steps (1), (3), and (4) are analogous to steps in the proof of Dirichlet's theorem without error term.

The case that L/K is abelian follows from the cyclotomic case by Chebotarev's "field crossing" argument. The general case can be reduced to the cyclic (and therefore abelian) case using a bit of representation theory.

Proof of Theorem 2.2 for Cyclotomic Extensions. We first recall that the abscissa of convergence of an L-series is controlled by its coefficients. Specifically,

Proposition 5.1 ([Lan86], Chp. VIII Theorem 4)**.** *Let $\{a_n\}$ be a sequence of complex numbers, with partial sums A_n. Let $0 \leq \sigma_0 < 1$ and suppose that for some $\rho \in \mathbb{C}$, $A_n = n\rho + O(n^{\sigma_0})$. Then, $f(s) = \sum a_n/n^s$ has an analytic continuation to $\mathrm{Re}(s) > \sigma_0$, except for a simple pole with residue ρ at $s = 1$ when ρ is non-zero.*

Proof. If ρ is non-zero, let $b_n = a_n - \rho$, let B_n be the partial sums of b_n, and let $g(s) = \sum b_n/n^s$. Then, $f(s) = g(s) + \rho\zeta(s)$. Write $s = \sigma + it$. If $\sigma > \sigma_0$, by summation-by-parts,

$$\sum_{n=M+1}^{N} \frac{b_n}{n^s} = \int_{M+1/2}^{N+1/2} \frac{1}{x^s} dB(x) = B_N \frac{1}{(N+1/2)^s} + s\int_{M+1/2}^{N+1/2} \frac{B(x)}{x^{s+1}} dx$$
$$\ll N^{\sigma-\sigma_0} + |s| \int_{M+1/2}^{N+1/2} \frac{1}{x^{\sigma+1-\sigma_0}} dx \ll \frac{1}{N^{\sigma-\sigma_0}} + \frac{|s|}{(\sigma-\sigma_0)(M+1/2)^{\sigma-\sigma_0}},$$

so the series clearly converges at s. □

To take advantage of this proposition, we rewrite the $L_{\mathfrak{c}}(s,\chi)$ as a sum over classes in $G(\mathfrak{c})$. We use the following proposition, which appears as Theorem 3 of Chapter VI of [Lan86].

Proposition 5.2. *Let $\mathfrak{c}$ be an ideal of $\mathcal{O}_K$ and $\mathscr{A}$ be a class in $G(\mathfrak{c})$. There is a constant $\rho_{\mathfrak{c}}$ depending only on $\mathfrak{c}$ such that the number of ideals $\mathfrak{a}$ of $\mathcal{O}_K$ such that $\mathfrak{a} \in \mathscr{A}$ and $\mathrm{Nm}\,\mathfrak{a} \leq n$ is $\rho_{\mathfrak{c}} n + O(N^{1-n_K^{-1}})$.*

We omit the proof, which involves computing the volume of the fundamental domain of a lattice.

Since $\rho_{\mathfrak{c}}$ is independent of the class $\mathscr{A} \in G(C)$, breaking up the sum of the coefficients $\chi(\mathfrak{a})$ of $L_{\mathfrak{c}}$ by class shows that as $n \to \infty$,

$$\sum_{(\mathfrak{a},\mathfrak{c})=1, \operatorname{Nm}\mathfrak{a} \leq n} \chi(\mathfrak{a}) = \begin{cases} \#G(\mathfrak{c}) \cdot \rho_{\mathfrak{c}} n + O(n^{1-n_K^{-1}}), & \chi = \chi_0 \\ O(n^{1-n_K^{-1}}), & \chi \neq \chi_0. \end{cases} \tag{5.1}$$

Applying Proposition 5.1 proves

Lemma 5.3. *$L_{\mathfrak{c}}(s,\chi)$ extends to a meromorphic function on $\operatorname{Re}(s) > 1 - n_K^{-1}$ which is analytic except for a simple pole of residue $\#G(\mathfrak{c})\rho_{\mathfrak{c}}$ at 1 when $\chi = \chi_0$.*

Now that we have proved an analytic continuation, we wish to move toward the world of Artin L-functions. We could do this for all abelian extensions by citing an appropriate theorem of class field theory. However, in the cyclotomic case, the proof has an interesting analytic step, so we present it below.

Suppose for now that L/K is an abelian extension, and let $\mathfrak{c}$ be a prime such that $\mathfrak{p}|\mathfrak{c}$ for all primes $\mathfrak{p}$ of K that ramify in L. Then, the Artin symbol extends by multiplication to a homomorphism $I(\mathfrak{c}) \to \operatorname{Gal}(L/K)$, which we denote $\left[\frac{L/K}{\cdot}\right]_{\mathfrak{c}}$. Restricting further to the case where L/K is cyclotomic, we have:

Lemma 5.4 (Lemma 6.5.3. of [FJ08])**.** *Let ζ_m be a primitive mth root of 1, let L/K be a Galois extension of number fields such that $L \subset K(\zeta_m)$ and let $\mathfrak{c}$ be an $\mathcal{O}_K$-ideal such that $m|\mathfrak{c}$. Then, $P(\mathfrak{c}) \subseteq \ker \left[\frac{L/K}{\cdot}\right]_{\mathfrak{c}}$.*

The proof is not hard but is completely algebraic, so we omit it. See [FJ08] for details.

Lemma 5.4 implies that $\left[\frac{L/K}{\cdot}\right]_{\mathfrak{c}}$ descends to a map $\overline{\left[\frac{L/K}{\cdot}\right]_{\mathfrak{c}}} : G(\mathfrak{c}) \to \operatorname{Gal}(L/K)$. Let $G := \operatorname{image} \overline{\left[\frac{L/K}{\cdot}\right]_{\mathfrak{c}}} \subset \operatorname{Gal}(L/K)$. Given a character $\chi \in \widehat{G}$, the composition $\chi \circ \overline{\left[\frac{L/K}{\cdot}\right]_{\mathfrak{c}}}$ is a character of $G(\mathfrak{c})$. This allows us to write $L_{\mathfrak{c}\mathcal{O}_L}(s,\chi_0)$ in terms of the $L_{\mathfrak{c}}\left(s, \chi \circ \overline{\left[\frac{L/K}{\cdot}\right]_{\mathfrak{c}}}\right)$. Working at the level of local factors, for $\mathfrak{p} \nmid \mathfrak{c}$, the order of $\left[\frac{L/K}{\mathfrak{p}}\right]$ is equal to the inertial degree f. Since $\mathfrak{p}$ does not ramify in L, there are $\frac{\#\operatorname{Gal}(L/K)}{f}$ primes lying over $\mathfrak{p}$. Hence,

$$\prod_{\mathfrak{P} \text{ lying over } \mathfrak{p}} \frac{1}{1-(\operatorname{Nm}\mathfrak{P})^{-s}} = \left(\frac{1}{1-(\operatorname{Nm}\mathfrak{p})^{-sf}}\right)^{\frac{\#\operatorname{Gal}(L/K)}{f}} = \prod_{\chi \in \widehat{G}} \left(\frac{1}{1-\chi\left(\left[\frac{L/K}{\mathfrak{p}}\right]\right)(\operatorname{Nm}\mathfrak{p})^{-sf}}\right)^{\frac{\#\operatorname{Gal}(L/K)}{\#G}}, \tag{5.2}$$

where the second equality is a standard statement about characters. Taking the product of both sides over all $\mathfrak{p}$ prime to $\mathfrak{c}$, gives the formula

$$L_{\mathfrak{c}\mathcal{O}_L}(s,\chi_0) = \prod_{\chi \in \widehat{G}} L_{\mathfrak{c}}\left(s, \chi \circ \overline{\left[\frac{L/K}{\cdot}\right]_{\mathfrak{c}}}\right)^{\frac{\#\operatorname{Gal}(L/K)}{\#G}}. \tag{5.3}$$

Using this formula, we see

Theorem 5.5. *Let $\zeta_m \in \overline{\mathbb{Q}}$ be a primitive mth root of 1, let L/K be a Galois extension of number fields satisfying $K \subset L \subset K(\zeta_m)$ and let $\mathfrak{c} \subset K$ be an ideal divisible by m. Then, the map $\overline{\left[\frac{L/K}{\cdot}\right]}_{\mathfrak{c}} : G(\mathfrak{c}) \to \mathrm{Gal}(L/K)$ is surjective.*

Moreover, if χ is a nontrivial character of $\mathrm{Gal}(L/K)$, $L_{\mathfrak{c}}\left(1, \chi \circ \overline{\left[\frac{L/K}{\cdot}\right]}_{\mathfrak{c}}\right) \neq 0$.

Proof. For any character $\chi \in \widehat{G}$, Lemma 5.3, implies that

$$\mathrm{ord}_{s=1} L_{\mathfrak{c}}\left(1, \chi \circ \overline{\left[\frac{L/K}{\cdot}\right]}_{\mathfrak{c}}\right) = \begin{cases} a_\chi, & \chi \neq \chi_0 \\ -1, & \chi = \chi_0, \end{cases} \tag{5.4}$$

for some constants $a_\chi \in \mathbb{Z}_{\geq 0}$.

Applying (5.4) to (5.3) yields

$$-1 = \frac{\#\,\mathrm{Gal}(L/K)}{\#G}\left(-1 + \sum_{\chi \in \widehat{G}} a_\chi\right). \tag{5.5}$$

Then, $\frac{\#\,\mathrm{Gal}(L/K)}{\#G}$ divides 1, so $G = \mathrm{Gal}(L/K)$. Since $a_\chi \geq 0$ for $\chi \neq \chi_0$, we must have $a_\chi = 0$ for $\chi \neq \chi_0$. □

The statement $\mathrm{Gal}(L/K) = G$ means that the Galois characters all induce characters of $G(\mathfrak{c})$, so the Artin L-functions for L/K are all Dirichlet-Hecke L-functions for $\mathfrak{c}$.

Having proved the special case of class field theory that we needed, we are ready to begin our final attack on the Chebotarev density theorem for cyclotomic extensions.

Recall that to apply Dirichlet L-functions to compute the density of primes in $\mathbb{Q}$ congruent to $a \mod n$, one first shows that the contribution of higher powers in the double summation expression for $\log L(s, \chi)$ is $O(1)$ as $s \to 1$ from above and then takes a linear combination of the $\log L(s, \chi)$ weighted by appropriate characters. We do the same here.

Lemma 5.6. *Let $\zeta_m \in \overline{\mathbb{Q}}$ be a primitive mth root of unity, let L/K be a Galois extension of number fields such that $K \subset L \subset K(\zeta_m)$, and let χ be a character of $\mathrm{Gal}(L/K)$. Then, as $s \to 1^+$,*

$$\log L_{L/K}(s, \chi) = \sum_{\mathfrak{p} \subset \mathcal{O}_K} \frac{\chi\left(\left[\frac{L/K}{\mathfrak{p}}\right]\right)}{(\mathrm{Nm}\,\mathfrak{p})^s} + O(1). \tag{5.6}$$

Proof. From the Euler product and the Taylor series for log, we know that

$$\log L_{L/K}(s, \chi) = \sum_{\mathfrak{p} \subset \mathcal{O}_K} \sum_{k=1}^{\infty} \frac{\chi\left(\left[\frac{L/K}{\mathfrak{p}}\right]^k\right)}{k(\mathrm{Nm}\,\mathfrak{p})^{sk}} + O(1), \tag{5.7}$$

where the $O(1)$ term accounts for the finitely many ramified primes. There are at most n_K primes of $\mathcal{O}_K$ lying above any prime $p\mathbb{Z} \subset \mathbb{Z}$ and each has norm at least p. Hence, the total contribution from the $k > 1$ is bounded in magnitude by

$$n_K \sum_{k=2}^{\infty} \frac{1}{p^{k\sigma}} \ll O(1), \tag{5.8}$$

which proves the lemma. □

Since the ramified places affect only the residue of the pole of $L_{L/K}(s, \chi)$ at 1 and not its order, given any $\sigma \in \mathrm{Gal}(L/K)$, Lemma 5.3 implies that as $s \to 1^+$,

$$\log L_{L/K}(s, \chi_0) = -\log(s-1) + O(1), \quad \text{and} \tag{5.9}$$

$$\sum_{\chi \in \widehat{\mathrm{Gal}(L/K)}} \frac{1}{\#\,\mathrm{Gal}(L/K)} \chi(\sigma^{-1}) \log L_{L/K}(s, \chi) = -\frac{1}{\#\,\mathrm{Gal}(L/K) \cdot \log(s-1)}. \tag{5.10}$$

On the other hand, by the orthogonality of characters and Lemma 5.6,

$$\log L_{L/K}(s, \chi_0) = \sum_{\mathfrak{p} \subset \mathcal{O}_K} \frac{1}{(\mathrm{Nm}\,\mathfrak{p})^s} + O(1), \quad \text{and} \tag{5.11}$$

$$\sum_{\chi \in \widehat{\mathrm{Gal}(L/K)}} \frac{1}{\#\,\mathrm{Gal}(L/K)} \chi(\sigma^{-1}) \log L_{L/K}(s, \chi) = \sum_{\mathfrak{p} \subset \mathcal{O}_K : \left[\frac{L/K}{\mathfrak{p}}\right] = \sigma} \frac{1}{(\mathrm{Nm}\,\mathfrak{p})^s} + O(1). \tag{5.12}$$

Putting these together, we see that $\lim_{s \to 1^+} \dfrac{\sum_{\mathfrak{p} \subset \mathcal{O}_K : \left[\frac{L/K}{\mathfrak{p}}\right] = \sigma} \frac{1}{(\mathrm{Nm}\,\mathfrak{p})^s}}{\sum_{\mathfrak{p} \subset \mathcal{O}_K} \frac{1}{(\mathrm{Nm}\,\mathfrak{p})^s}} = \dfrac{1}{[L:K]}$, completing the proof of the Chebotarev density theorem for cyclotomic extensions. □

Proof of Theorem 2.2 for Abelian Extensions. To extend from the cyclotomic case to the general abelian case, we have two options. One option is to cite the appropriate theorems of class field theory to show that for any L/K abelian, we can still choose an ideal $\mathfrak{c} \subset \mathcal{O}_K$ such that the map $G(\mathfrak{c}) \to \mathrm{Gal}(L/K)$ is surjective. The remainder of the proof from the cyclotomic case then goes through for the abelian case nearly unchanged. Instead, we present a "field crossing" argument similar to that of Chebotarev's original proof. Related ideas are often used as a preliminary step in proofs of class field theory, including Artin's original proof.

We start by outlining the proof, generally following the approach of [FJ08]. Given L/K an abelian Galois extension of number fields and $\sigma \in \mathrm{Gal}(L/K)$, the first step is to construct an auxiliary cyclotomic extension of number fields F/E of degree $k \cdot \mathrm{order}(\sigma)$ for $k \in \mathbb{Z}$ such that $L \subset F$, $K \subset E$, and F/K is Galois. The contribution of primes of E which are not split in E/K can be ignored, since there are finitely many ramified primes and the rest have large norm. This allows us to compute the densities for many subsets of elements of $\mathrm{Gal}(F/K)$ which restrict to σ on L. The sum of these densities gives a lower bound for the density of the primes mapping to the conjugacy class $\mathcal{C} \subset \mathrm{Gal}(L/K)$ of σ. Taking an appropriate sequence of fields gives the correct lower bound. Observing that all of the densities sum to 1 completes the proof.

We now give the argument in full detail.

We wish to compute the density of primes $\mathfrak{p}$ such that $\left[\frac{L/K}{\mathfrak{p}}\right] = \sigma$. To start, we bring in an auxiliary cyclotomic field extension. Choose a cyclotomic extension M/K such that M/K has an element τ with $\operatorname{ord}\sigma | \operatorname{ord}\tau$ and $M \cap L = K$. Then, the compositum $F = LM$ is Galois over K with $\operatorname{Gal}(F/K) \cong \operatorname{Gal}(L/K) \times \operatorname{Gal}(M/K)$. Let $\rho = (\sigma, \tau) \in \operatorname{Gal}(F/K)$. Note that $\operatorname{ord}\rho = \operatorname{ord}\tau$ by our choice of τ. Let $E = F^\rho$ be the fixed field of ρ. Then, $E \cap M = M^\tau$. Thus, $[M : E \cap M] = \operatorname{ord}\tau = \operatorname{ord}\rho = [F : E]$ and so $F = EM$. Thus, F is a cyclotomic extension of E.

By the Chebotarev density theorem for cyclotomic extensions, the set $Q_1(\rho)$ of primes $\mathfrak{q} \subset \mathcal{O}_E$ such that $\left[\frac{F/E}{\mathfrak{q}}\right] = \rho$ has density $\frac{1}{[F:E]}$. Denote by $Q_2(\rho)$ the set of primes $\mathfrak{q} \subset \mathcal{O}_E$ such that $\left[\frac{F/E}{\mathfrak{q}}\right] = \rho$ and $\mathfrak{q}$ has degree 1 above $\mathfrak{p} = \mathfrak{q} \cap K$. Since the sum $\sum \frac{1}{\operatorname{Nm}\mathfrak{q}}$ over all primes of E which do not have degree 1 above $\mathfrak{p}$ is bounded by $\sum_{\mathfrak{q} \text{ ramified}} \frac{1}{\operatorname{Nm}\mathfrak{q}} + [E : K] \sum_p \frac{1}{p^2}$, the density of Q_2 and Q_1 are equal.

Also, if $\mathfrak{q} \in Q_2(\rho)$ and $\mathfrak{p} = \mathfrak{q} \cap K$, then $\operatorname{Nm}\mathfrak{q} = \operatorname{Nm}\mathfrak{p}$. It follows immediately that $\rho = \left[\frac{F/E}{\mathfrak{q}}\right] = \left[\frac{F/K}{\mathfrak{p}}\right]$. Moreover, any prime $\mathfrak{p}$ lying under some element of $Q_2(\rho)$ must have exactly $[E : K]$ primes in $Q_2(\rho)$ lying over it by the definition of $Q_2(\rho)$. Since elements $\mathfrak{q} \in Q_2(\rho)$ satisfy $\operatorname{Nm}_L \mathfrak{q} = \operatorname{Nm}_K(K \cap \mathfrak{q})$, this implies that the set P_ρ of primes $\mathfrak{p} \subset \mathcal{O}_K$ such that $\left[\frac{F/K}{\mathfrak{p}}\right] = \rho$ has density at least $\frac{1}{[E:K]} \cdot \frac{1}{[F:E]} = \frac{1}{[F:K]}$.

Now, if $\mathfrak{p} \in P_\rho$, $\rho(\alpha) = \alpha^{\operatorname{Nm}\mathfrak{p}} \mod \mathfrak{P}$ for all $\alpha \in F$ for any $\mathfrak{P} \subset \mathcal{O}_F$ lying over $\mathfrak{p}$, so $\rho(\alpha) = \alpha^{\operatorname{Nm}\mathfrak{p}} \mod \mathfrak{P} \cap L$ for all $\alpha \in L$, which implies that the density of $P_\sigma = \{\mathfrak{p} \subset \mathcal{O}_K : \left[\frac{L/K}{\mathfrak{p}}\right] = \sigma\}$ has density at least $\frac{1}{[F:K]} = \frac{1}{[L:K]\cdot[M:K]}$.

We have already shown that P_σ has positive density. To go further, note that we were free to choose any $\tau \in \operatorname{Gal}(M/K)$ so long as $\operatorname{ord}(\sigma) | \operatorname{ord}(\tau)$. For different choices of τ, the sets $P_1((\sigma, \tau))$ will be disjoint, so the sums of their densities will also be a lower bound on the density of P_σ. Now, if $\operatorname{ord}\sigma = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ and $\operatorname{Gal}(M/K)$ is cyclic of order $p_1^{\beta_1} \cdots p_\ell^{\beta_\ell}$, the number of elements of of $\operatorname{Gal}(M/K)$ of order a multiple of $\operatorname{order}(\sigma)$ is

$$(p_1^{\beta_1} - p_1^{\alpha_1 - 1}) \cdots (p_k^{\beta_k} - p_k^{\alpha_k - 1}) p_{k+1}^{\beta_{k+1}} \cdots p_\ell^{\beta_\ell} = [M : K] \cdot \prod_{j=1}^{k} (1 - p_j^{\alpha_j - 1 - \beta_j}). \tag{5.13}$$

Assuming we can construct such an M, the density of P_σ is at least

$$\frac{1}{[L : K]} \cdot \prod_{j=1}^{k} (1 - p_j^{\alpha_j - 1 - \beta_j}). \tag{5.14}$$

Of course, by Dirichlet's theorem on primes in arithmetic progressions, i.e. the special case of the Chebotarev density theorem for the cyclotomic extension $\mathbb{Q}(\zeta_m)/\mathbb{Q}$, there are infinitely many primes p such that $p \equiv 1 \pmod{m}$ for any $m = \prod_j p_j^{\beta_j}$. For any sufficiently large such p, $K(\zeta_p) \cap L = K$ and $\operatorname{Gal}(K(\zeta_p)/K) \cong (\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$. Thus, we can choose a sequence of such fields $M = K(\zeta_p)$ so that the β_j get arbitrarily large. Thus, the Dirichlet density of P_σ is at least $\frac{1}{[L:K]}$. This argument applies to all

$\sigma \in \mathrm{Gal}(L/K)$, the P_σ are disjoint, and the total Dirichlet density is 1, so in fact, the Dirichlet density of P_σ is exactly $\frac{1}{[L:K]}$. $\square$

Proof of Theorem 2.2 for Finite Galois Extensions. For this section, we depart from [FJ08], which gives a more combinatorial argument reducing the proof to the case of cyclic extensions in favor of the representation theory based argument in Section 4 of [LO77]. The general case follows from the cyclic case by the representation theory of finite groups. Given a finite Galois extension $\mathrm{Gal}(L/K)$ and a conjugacy class $\mathcal{C} \subset \mathrm{Gal}(L/K)$, pick some $\sigma \in \mathcal{C}$ and let $E = L^\sigma$ be the fixed field of σ. Then, $\mathrm{Gal}(L/E) = \langle \sigma \rangle$ is the cyclic subgroup of $\mathrm{Gal}(L/K)$ generated by σ. Orthogonality of characters implies that for $\tau \in \mathrm{Gal}(L/K)$,

(5.15)
$$\sum_{\phi, \text{ char. of } \mathrm{Gal}(L/K)} \overline{\phi(\sigma)}\phi(\tau) = \sum_{\chi \in \widehat{\mathrm{Gal}(L/E)}} \overline{\chi(\sigma)} \operatorname{Tr} \operatorname{Ind}_{\langle\sigma\rangle}^{\mathrm{Gal}(L/K)} \chi(\tau) = \begin{cases} \frac{\#\mathrm{Gal}(L/K)}{\#\mathcal{C}}, & \tau \in \mathcal{C}, \\ 0, & \tau \notin \mathcal{C}. \end{cases}$$

By (4.6), absorbing the finitely many ramified primes and the contribution from $m \geq 2$ into an $O(1)$ term as before, we have that for any $\sigma \in \mathcal{C}$,

$$\begin{aligned} \sum_{\mathfrak{p} \subset \mathcal{O}_K : \left[\frac{L/K}{\mathfrak{p}}\right] = \mathcal{C}} (\mathrm{Nm}\,\mathfrak{p})^{-s} + O(1) &= -\frac{\#\mathcal{C}}{\#\mathrm{Gal}(L/K)} \sum_{\phi, \text{ char. of } \mathrm{Gal}(L/K)} \overline{\phi(\sigma)} \log L_{L/K}(s, \phi) \\ &= -\frac{\#\mathcal{C}}{\#\mathrm{Gal}(L/K)} \sum_{\chi \in \widehat{\mathrm{Gal}(L/E)}} \overline{\chi(\sigma)} \log L_{L/K}(s, \operatorname{Tr} \operatorname{Ind}_{\mathrm{Gal}(L/E)}^{\mathrm{Gal}(L/K)} \chi). \end{aligned} \tag{5.16}$$

Now, it is not hard to check by Mackey's Theorem in the unramified case and an explicit computation in the case of ramification that $L_{L/K}(s, \mathrm{Ind}_{\mathrm{Gal}(L/E)}^{\mathrm{Gal}(L/K)} \chi) = L_{L/E}(s, \chi)$, (see, for example Section 2.5.7. of [Sny02]). Continuing from (5.16),

$$\begin{aligned} \sum_{\mathfrak{p} \subset \mathcal{O}_K : \left[\frac{L/K}{\mathfrak{p}}\right] = \mathcal{C}} (\mathrm{Nm}\,\mathfrak{p})^{-s} + O(1) &= -\frac{\#\mathcal{C}}{\#\mathrm{Gal}(L/K)} \sum_{\chi \in \widehat{\mathrm{Gal}(L/E)}} \overline{\chi(\sigma)} \log L_{L/E}(s, \chi) \\ &= \frac{\#\mathcal{C} \cdot \#\mathrm{Gal}(L/E)}{\#\mathrm{Gal}(L/K)} \sum_{\mathfrak{q} \subset \mathcal{O}_E : \left[\frac{L/E}{\mathfrak{q}}\right] = \sigma} (\mathrm{Nm}\,\mathfrak{q})^{-s} + O(1), \end{aligned} \tag{5.17}$$

as $s \to 1^+$. Since the class $\{\sigma\}$ has density $\frac{1}{\#\mathrm{Gal}(L/E)}$ in P_E and also,

$$\sum_{\mathfrak{p} \subset \mathcal{O}_K} (\mathrm{Nm}\,\mathfrak{p})^{-s} = \sum_{\mathfrak{q} \subset \mathcal{O}_E} (\mathrm{Nm}\,\mathfrak{q})^{-s} + O(1) \to \infty, \tag{5.18}$$

as $s \to 1^+$, we see that the Dirichlet density of primes $\mathfrak{p} \subset \mathcal{O}_K$ with $\left[\frac{L/K}{\mathfrak{p}}\right] = \mathcal{C}$ is $\frac{\#\mathcal{C} \cdot \#\mathrm{Gal}(L/E)}{\#\mathrm{Gal}(L/K)} \cdot \frac{1}{\#\mathrm{Gal}(L/E)} = \frac{\#\mathcal{C}}{\#\mathrm{Gal}(L/K)}$, which completes the proof of the Chebotarev density theorem for Dirichlet density. $\square$

6. "Effective" Chebotarev for Natural Density

For many applications of the Chebotarev density theorem, Theorem 2.2 is sufficient. In particular, if the end-user's goal is simply to prove the infinitude of some set of primes, there is no need to cite a full-strength Chebotarev. However, if one requires a prime (or many primes) of relatively low norm in some ideal class, error bounds given in terms of numerical invariants of the fields are very useful. This is exactly what Theorems 2.3 and 2.4, proved by Lagarias and Odlyzko in [LO77] and refined by Serre in [Ser81], provide. While these theorems did not give the world record bound on the lowest norm prime in an ideal class, (the record at the time still belonging to Lagarias and Odlyzko with the addition of Montgomery [LMO79]), they were still the first example of a proof of the Cebotarev density theorem with an explicit, effectively computable error term. We follow Lagarias and Odlyzko's extremely clear presentation of the proof from their original paper [LO77], omitting all but a select few particularly instructive details.

The outline of the proof could almost be read out of Davenport's "Multiplicative Number Theory" [Dav00], although there are a few additional wrinkles. (In particular, there will be some inputs from class field theory and representation theory. The error terms will also be more complicated). The general argument goes as follows:

(1) Compare $\psi_{\mathcal{C}}(x, L/K) := \sum_{\substack{\operatorname{Nm}\mathfrak{p}^m \leq x, \left[\frac{L/K}{\mathfrak{p}}\right]^m = \mathcal{C} \\ \mathfrak{p} \text{ unramified}}} \log(\operatorname{Nm}\mathfrak{p})$ to a truncated inverse Mellin tranform of a character-weighted linear combination of the logarithms of Artin L-functions.
(2) Use an argument as in the proof of Theorem 2.2 for finite Galois extensions at the end of Section 5 to replace the Artin L-functions associated to L/K with Artin L-functions associated to a cyclic extension L/E (which are then Dirichlet-Hecke L-functions by class field theory).
(3) Use the functional equation and Hadamard product formula of the L-functions in question and the inequality $3 + 4\cos\theta + \cos 2\theta \geq 0$ to prove a zero-free (or nearly zero-free) region for $\zeta_L(s) := \prod_\chi L_{L/E}(s, \chi)$. Alternately, assume the generalized Riemann hypothesis for ζ_L.
(4) Use the functional equation and Hadamard product to bound the number of non-trivial zeros of the L-functions with imaginary part between $t-1$ and $t+1$.
(5) Shift the line of integration from the truncated inverse Mellin transform to the left to get an explicit formula for $\psi_{\mathcal{C}}(x, L/K)$ with main term $x \cdot \#C/\#\operatorname{Gal}(L/K)$ and with the error term depending on a sum over zeros of L-functions.
(6) Put everything together and choose an appropriate value of T (the value at which the Mellin transform was truncated) to balance error terms. The result is an estimate for $\psi_{\mathcal{C}}(x, L/K)$ with effective error terms.
(7) Use summation by parts to prove the corresponding result for $\pi_{\mathcal{C}}(x, L/K)$.

We now give a more detailed outline, filling in some details that Lagarias and Odlyzko leave unproven and including most of the key equations. We move quickly through the first couple of steps.

Orthogonality of characters and (4.7) imply (3.5) and (3.6) of [LO77], which state that for any $\tau \in \mathcal{C}$,

(6.1)
$$F_{\mathcal{C}}(s) := -\frac{\#\mathcal{C}}{\#\operatorname{Gal}(L/K)} \sum_{\phi \text{ char. of } \operatorname{Gal}(L/K)} \overline{\phi(\tau)} \frac{L'_{L/K}}{L_{L/K}}(s,\phi) = \sum_{\mathfrak{p}\subset\mathcal{O}_K} \sum_{m=1}^{\infty} \theta(\mathfrak{p}^m) \log(\operatorname{Nm}\mathfrak{p})(\operatorname{Nm}\mathfrak{p})^{-ms},$$

where $\theta(\mathfrak{p}^m)$ is an indicator function for $\left[\frac{L/K}{\mathfrak{p}}\right]^m = \mathcal{C}$ if $\mathfrak{p}$ does not ramify in L and takes values in $[0,1]$ if $\mathfrak{p}$ ramifies in L.

Let $\sigma_0 = 1 + 1/\log x$ and let

$$I_{\mathcal{C}}(x,T) := \frac{1}{2\pi i} \int_{\sigma_0 - iT}^{\sigma_0 + iT} F_{\mathcal{C}}(s) \frac{x^s}{s} ds \tag{6.2}$$

be the truncated inverse Mellin transform of $F_{\mathcal{C}}(s)$. $\psi_{\mathcal{C}}(x)$ is the sum up to norm x of the coefficients of $F_{\mathcal{C}}(s)$, with the ramified primes omitted. Serre shows in Sections 1.3. and 2.4. of [Ser81] that

(6.3)
$$\sum_{\substack{\mathfrak{p}\subset\mathcal{O}_K, m:(\operatorname{Nm}\mathfrak{p})^m \le x \\ \mathfrak{p} \text{ ramified in } L/K}} \log \operatorname{Nm}\mathfrak{p} \le 2\log x \sum_{\substack{\mathfrak{p}\subset\mathcal{O}_K \\ \mathfrak{p} \text{ ramified in } L/K}} \log \operatorname{Nm}\mathfrak{p} \le \frac{4}{\#\operatorname{Gal}(L/K)} \log x \log d_L,$$

which gives an upper bound on the error term resulting from the unramified primes. Applying the same strategy for bounding the error term from the Mellin transform as in [Dav00]'s proof of Dirichlet's theorem yields the improved version of (3.10) and (3.18) of [LO77],

$$|\psi_{\mathcal{C}}(x) - I_{\mathcal{C}}(x,T)| \ll \frac{\log x \log d_L}{\#\operatorname{Gal}(L/K)} + n_K \log x + n_K \frac{x}{T} (\log x)^2. \tag{6.4}$$

Now, the same argument as in the reduction of Theorem 2.2 to the case of cyclic extensions shows that we may replace the sum $\sum_{\phi \text{ char. of } \operatorname{Gal}(L/K)} \overline{\phi(\tau)} \frac{L'_{L/K}}{L_{L/K}}(s,\phi)$ in the definition of $F_{\mathcal{C}}(s)$ with $\sum_{\chi \in \widehat{\operatorname{Gal}(L/E)}} \overline{\chi(\tau)} \frac{L'_{L/E}}{L_{L/E}}(s,\chi)$, where E is the fixed field of τ.

We now "recall" some facts about the $L_{L/E}(s,\chi)$. The L-functions $L_{L/E}(s,\chi)$ have a completed L-function $\xi_{L/E}(s,\chi)$. $\xi_{L/E}$ has a functional equation $\xi_{L/E}(1-s,\overline{\chi}) = W(\chi)\xi_{L/E}(s,\chi)$. Also, $\xi_{L/E}$, is entire of order 1. If $\xi_{L/E}$ is non-vanishing in $s \ge 1$, then $\xi_{L/E}$ has a Hadamard product. Indeed, this is the case:

Proposition 6.1. *$L_{L/E}(s,\chi)$ has no zeros in $\sigma \ge 1$. Hence the zeros of $\xi_{L/E}(s,\chi)$ lie in the critical strip $\{0 < \operatorname{Re}(s) < 1\}$.*

Proof. To show the result for $L_{L/E}(s,\chi)$, it suffices to prove the proposition for $\zeta_L(s)$, where

$$\zeta_L(s) := \prod_{\chi \in \widehat{\operatorname{Gal}(L/E)}} L_{L/E}(s,\chi) = \prod_{\mathfrak{P}\subset\mathcal{O}_L} \frac{1}{1-(\operatorname{Nm}\mathfrak{P})^{-s}} = \sum_{0\neq\mathfrak{A}\subset\mathcal{O}_L} (\operatorname{Nm}\mathfrak{a})^{-s}. \tag{6.5}$$

From the last expression, $\zeta_L(s)$ is clearly positive for all $s \in \mathbb{R}$ with $s > 1$ and has a simple pole with residue 1 at $s = 1$. Then, since $3 + 4\cos\theta + \cos 2\theta \geq 0$, for any $\sigma > 1, t \in \mathbb{R}$, taking the Taylor expansion of $-\log(1 - \operatorname{Nm}\mathfrak{P})$ for each $\mathfrak{P} \subset \mathcal{O}_L$,

$$\operatorname{Re}\left[3\log\zeta_L(\sigma) + 4\log\zeta_L(\sigma + it) + \log\zeta_L(\sigma + 2it)\right] \geq 0, \tag{6.6}$$

and so $|\zeta_L(\sigma)^3\zeta_L(\sigma+it)^4\zeta_L(\sigma+2it)| \geq 1$. Now, for $\sigma = 1, t = 0$, $\zeta_L(\sigma+it)$ has a pole and so is clearly non-zero. For $t \neq 0$, if $\zeta_L(1 + it) = 0$, then $\lim_{\sigma\to 1^+}\zeta_L(\sigma)^3\zeta_L(\sigma + it)^4 = 0$. Also, $\zeta_L(\sigma + 2it)$ does not have a pole, so the whole product tends to zero. But this contradicts that the product has magnitude at least 1, so $\zeta_L(\sigma + it)$ cannot have a zero with $\sigma \geq 1$.

The statement about $\xi_{L/E}(s\chi)$ follows immediately from the functional equation. □

The logarithmic derivative of the Hadamard product for $\xi_{L/E}$ yields

$$\frac{L'_{L/E}}{L_{L/E}}(s,\chi) = B(\chi) + \sum_{\rho : L_{L/E}(\rho,\chi)=0}\left(\frac{1}{s-\rho} + \frac{1}{\rho}\right) - \frac{1}{2}\log A(\chi) - \delta_{\chi_0}(\chi)\left(\frac{1}{s} + \frac{1}{s-1}\right) - \frac{\gamma'_\chi}{\gamma_\chi}(s), \tag{6.7}$$

where $A(\chi)$ is the product of d_E with the norm of the conductor of χ, $B(\chi)$ is some constant depending on χ, and γ_χ is a certain product of powers of π and Gamma functions coming from the infinite places.

We can now improve the zero-free region from Proposition 6.1 by observing that the functional equation of $\xi_{L/E}(s,\chi)$ implies

$$\sum_\rho\left(\frac{1}{s-\rho} + \frac{1}{s-\overline{\rho}}\right) = \log A(\chi) + 2\delta_{\chi_0}(\chi)\left(\frac{1}{s} + \frac{1}{s-1}\right) + 2\frac{\gamma'_\chi}{\gamma_\chi}(s) - \frac{L'_{L/E}}{L_{L/E}}(s,\chi) - \frac{L'_{L/E}}{L_{L/E}}(s,\overline{\chi}). \tag{6.8}$$

Summing over all $\chi \in \widehat{\operatorname{Gal}(L/E)}$ and applying a refined version of the argument in Proposition 6.1 with $\frac{\zeta'_L}{\zeta_L}$ in place of $\log\zeta_L$, gives the following zero-free and "almost" zero-free regions, which we state without proof.

Lemma 6.2 (Lemma 8.1. of [LO77])**.** *There is an effectively computable positive absolute constant c such that $\zeta_L(s)$ has no zeros ρ in the region*

$$|\operatorname{Im}(\rho)| \geq \frac{1}{1 + 4\log d_L}, \quad |\operatorname{Re}(\rho)| \geq 1 - \frac{c}{\log d_L + n_L\log(|\operatorname{Im}(\rho)| + 2)}. \tag{6.9}$$

Lemma 6.3 (Lemma 8.2. of [LO77])**.** *If $n_L > 1$, $\zeta_L(s)$ has at most one zero ρ in the region*

$$|\operatorname{Im}(\rho)| \geq \frac{1}{4\log d_L}, \quad |\operatorname{Re}(\rho)| \geq 1 - \frac{1}{4\log d_L}. \tag{6.10}$$

If such a zero exists, it is real, simple, and comes from $L_{L/E}(s,\chi)$ for a real character χ.

Another important consequence of (6.8) and the functional equation of $\xi_{L/E}(s,\chi)$ is Lemma 6.4, which bounds the number of zeros in a thin strip.

Lemma 6.4 (Lemma 5.4. of [LO77])**.** *Let $n_\chi(t)$ be the number of zeros of $L_{L/E}(s,\chi)$ with imaginary part in the interval $[t-1,t+1]$ and real part in $(0,1)$. For all t, $n_\chi(t) \ll \log A(\chi) + n_E \log(|t|+2)$.*

Proof. At $s = 2+it$, $\left|\frac{\gamma_\chi'}{\gamma_\chi}(s)\right| \ll n_E \log(|t|+2)$, $\left|\frac{L_{L/E}'}{L_{L/E}}(s,\chi)\right| \leq -\frac{\zeta_E'}{\zeta_E}(2) \ll n_E$, and $\frac{1}{s}$ and $\frac{1}{s-1}$ are both $O(1)$. Taking the real part of both sides of (6.8) yields

$$\sum_\rho \operatorname{Re}\left(\frac{1}{2+it-\rho} + \frac{1}{2+it-\overline{\rho}}\right) \ll \log A(\chi) + n_E \log(|t|+2), \tag{6.11}$$

where we omit the absolute value on the left-hand side since every term is positive. Now, if $|\operatorname{Im}(\rho) - t| < 1$ and $0 < \operatorname{Re}(\rho) < 1$, $\operatorname{Re}\left(\frac{1}{2+it-\rho} + \frac{1}{2+it-\overline{\rho}}\right) \geq \frac{1}{5}$, so the left hand side of (6.11) is $\gg n_\chi(t)$. □

This has the important consequence that the mysterious constant $B(\chi)$ satisfies

$$B(\chi) + \sum_{\rho:|\rho|<1/2} \frac{1}{\rho} \ll \log A(\chi) + n_E. \tag{6.12}$$

See Lemma 5.5. of [LO77] for a slightly more general statement and proof.

The next step is to use these bounds to show that if $U > 1$ is a positive half-integer and $\Pi(U,T)$ is the path given by concatenating the straight lines from σ_0+iT to $-U+iT$ to $-U-iT$ to σ_0-iT, then

$$\frac{1}{2\pi i}\int_{\Pi(U,T)} \frac{x^s}{s}\frac{L_{L/E}'}{L_{L/E}}(s,\chi) \ll \frac{x\log x}{T}(\log A(\chi) + n_E \log T) + \frac{Tx^{-U}}{U}(\log A(\chi) + n_E \log(T+U)). \tag{6.13}$$

The first term comes from the horizontal integrals and the second term comes from the vertical integrals. The only difficulty is bounding the contribution of the horizontal integrals near the critical strip. For this, it is helpful to compare the values of $\frac{L_{L/E}'}{L_{L/E}}(\sigma+it,\chi)$ and $\frac{L_{L/E}'}{L_{L/E}}(3+it,\chi)$ to estimate $\frac{L_{L/E}'}{L_{L/E}}(s,\chi)$ by $\sum_{\rho:|\operatorname{Im}(s-\rho)<1|}\frac{1}{s-\rho}$ within a $\log(A(\chi))+n_E\log(|t|+2)$ error term.

Now, the Cauchy integral formula and (6.13) imply that

$$\frac{1}{2\pi i}\int_{\sigma_0-iT}^{\sigma_0+iT} \frac{x^s}{s}\frac{L_{L/E}'}{L_{L/E}}(s,\chi) = \sum_{\substack{\nu \text{ poles of } \frac{x^s}{s}\cdot\frac{L_{L/E}'}{L_{L/E}}(s,\chi) \\ \nu\in[-U,\sigma_0]+i[-T,T],}} \operatorname{res}_\nu\left(\frac{x^s}{s}\frac{L_{L/E}'}{L_{L/E}}(s,\chi)\right) + \mathcal{E}, \tag{6.14}$$

with error term $\mathcal{E}$ as in (6.13). There are four sources for poles of $\frac{x^s}{s}\frac{L_{L/E}'}{L_{L/E}}(s,\chi)$:

(1) The non-trivial zeros of $L_{L/E}(s,\chi)$. Each contributes a residue $\frac{x^\rho}{\rho}$ (counting zeros with multiplicity).
(2) The trivial zeros of $L_{L/E}(s,\chi)$ at negative integers $> U$. The residue at $-k$ is $-a_{k \pmod 2}(\chi)\frac{x^{-k}}{k}$, where $a_{k \pmod 2}(\chi)$ depends only on the parity of k and $\gamma_E(\chi)$.

(3) The possible pole of $\frac{L'_{L/E}}{L_{L/E}}(s,\chi)$ at 1 which contributes the residue $-\delta_{\chi_0}(\chi)x$.

(4) The pole of $\frac{x^s}{s}$ and possible pole of $\frac{L'_{L/E}}{L_{L/E}}(s,\chi)$ at 0. The residue here is some $R(\chi)$, which can be shown to satisfy

$$\left| R(\chi) - \sum_{\rho:|\rho|<\frac{1}{2}} \frac{1}{\rho} \right| \ll \log A(\chi) + n_E \log(x), \tag{6.15}$$

by applying (6.12) and easy estimates on the size of $\frac{L'_{L/E}}{L_{L/E}}(s,\chi)$ and $\frac{\gamma'_E}{\gamma_E}(s,\chi)$. (Note that our notation departs a bit from [LO77] here. In particular, [LO77] breaks this term down further before deriving the bound.)

Taking the limit as $U \to \infty$, summing these terms over $\chi \in \widehat{\mathrm{Gal}(L/E)}$, (weighted by $\overline{\chi(\tau)}$ of course), and applying the identity $n_L = [L:E] \cdot n_E$ and the conductor-discriminant formula $\sum_\chi \log A(\chi) = \log d_L$, we arrive at Theorem 6.5.

Theorem 6.5 (Theorem 7.1 of [LO77])**.** *Suppose $x \geq 2$ and $T \geq 2$. Define*

$$S(x,T) = \frac{\#\mathcal{C}}{\#\operatorname{Gal}(L/K)} \sum_{\chi \in \widehat{\mathrm{Gal}(L/E)}} \overline{\chi(\tau)} \left(\sum_{\rho:|\operatorname{Im}(\rho)|<T} \frac{x^\rho}{\rho} - \sum_{\rho:|\rho|<\frac{1}{2}} \frac{1}{\rho} \right), \tag{6.16}$$

where the sums are over zeros of $\zeta_L(s)$. Then,

$$\begin{aligned} \left| \psi_{\mathcal{C}}(x, L/K) - \frac{\#\mathcal{C}}{\#\operatorname{Gal}(L/K)} x \right| &\ll |S(x,T)| + \frac{\log x \log d_L}{\#\operatorname{Gal}(L/K)} + \frac{n_L}{\#\operatorname{Gal}(L/K)} \frac{x(\log x)^2}{T} \\ &\quad + \frac{\#\mathcal{C}}{\#\operatorname{Gal}(L/K)} \left(\frac{x \log x + T}{T} \log d_L + n_L \log x + \frac{n_L x \log x \log T}{T} \right) \end{aligned} \tag{6.17}$$

We are now ready to prove Theorem 2.3.

Proof of Theorem 2.3. . Under GRH for $\zeta_L(s)$,

$$\begin{aligned} \left| \sum_{\rho:|\operatorname{Im}(\rho)|<T} \frac{x^\rho}{\rho} - \sum_{\rho:|\rho|<\frac{1}{2}} \frac{1}{\rho} \right| &= \left| \sum_{\rho:|\operatorname{Im}(\rho)|<T} \frac{x^\rho}{\rho} \right| \leq x^{1/2} \sum_{\rho:|\operatorname{Im}(\rho)|<T} \frac{1}{|\rho|} \\ &\ll x^{1/2} \sum_{t=1}^{T} \frac{\sum_{\chi \in \widehat{\mathrm{Gal}(L/E)}} n_\chi(t)}{t} \ll x^{1/2} \log T \left(\log d_L + n_L \log T \right). \end{aligned} \tag{6.18}$$

Taking $T \sim x^{1/2}$ to balance the error terms in (6.17) yields

$$\left| \psi_{\mathcal{C}}(x, L/K) - \frac{\#\mathcal{C}}{\#\operatorname{Gal}(L/K)} x \right| \ll \frac{\#\mathcal{C}}{\#\operatorname{Gal}(L/K)} x^{1/2} \log(d_L x^{n_L})(\log x). \tag{6.19}$$

Removing the terms for $\left[\frac{L/K}{\mathfrak{p}}\right]^m = \mathcal{C}$ for $m \geq 2$ from $\psi_{\mathcal{C}}(x, L/K)$ introduces an error term of at most $n_K x^{1/2}$ since

$$\sum_{\mathfrak{p}, m \geq 2 : \mathrm{Nm}_{K/\mathbb{Q}}(\mathfrak{p})^m \leq x} \log \mathrm{Nm}_{K/\mathbb{Q}} \mathfrak{p} \leq n_K \sum_{p, m : p^m \leq x} \log p \ll n_K x^{1/2}. \tag{6.20}$$

In particular, if we write $\psi'_{\mathcal{C}}(x, L/K)$ for the sum $\psi_{\mathcal{C}}(x, L/K)$ with the $m \geq 2$ terms removed, then (6.19) also holds for $\psi'_{\mathcal{C}}(x, L/K)$. Denoting the error term by $R(x)$, and integrating by parts,

$$\begin{aligned}
\pi_{\mathcal{C}}(x, L/K) &= \int_2^x \frac{d\psi'_{\mathcal{C}}(n, L/K)}{\log n} \\
&= \frac{\#\mathcal{C}}{\#\operatorname{Gal}(L/K)} \frac{x}{\log x} + \frac{R(x)}{\log x} - \frac{\#\mathcal{C}}{\#\operatorname{Gal}(L/K)} \int_2^x \frac{dn}{\log^2 n} - \int_2^x \frac{R(n) dn}{n \log^2 n} \\
&= \frac{\#\mathcal{C}}{\#\operatorname{Gal}(L/K)} \int_2^x \frac{dt}{\log t} + O\left(\frac{\#\mathcal{C}}{\#\operatorname{Gal}(L/K)} x^{1/2} \log(d_L x^{n_L}) \right) - \int_2^x \frac{R(n) dn}{n \log^2 n}. \qquad (6.21)
\end{aligned}$$

Since $\int_2^x \frac{(\log d_L n^{n_L})}{n^{1/2} \log n} = O\left(\frac{\#\mathcal{C}}{\#\operatorname{Gal}(L/K)} x^{1/2} \log(d_L x^{n_L}) \right)$, (6.21) implies Theorem 2.3. □

A similar argument (dealing with the more complicated zero-free region) can be used to prove 2.4.

7. Applications of the Chebotarev Density Theorem

To conclude, we give several interesting applications of the Chebotarev density theorem, chosen to highlight some of the different ways this theorem can be used.

Our first example demonstrates perhaps the most obvious application of Chebotarev – showing that a certain set of primes is infinite. This example, described by Serre in [Ser03] uses Chebotarev to translate a group-theoretic theorem of Jordan into a number theory statement.

Theorem 7.1. *Let f be an irreducible degree $n \geq 2$ polynomial with coefficients in $\mathbb{Z}$. Let $P_0(f)$ be the set of primes such that f has no zeros in the finite field $\mathbb{F}_p$. $P_0(f)$ has positive density $\geq \frac{1}{n}$ with strict inequality when n is not a prime power.*

Proof. We require some group theoretic input, which we state without proof.

Theorem 7.2 (Jordan [Jor72], Cameron and Cohen [CC92])**.** *Let G be a group acting transitively on a set X with $n \geq 2$ elements. Let $G_0 = \{g \in G : g \cdot x \neq x \forall x \in X\}$. Then, $G_0 \neq \emptyset$. More precisely, $\frac{\#G_0}{\#G} \geq \frac{1}{n}$, with equality possible only when $\#G$ is a power of a prime.*

Let $L = \mathbb{Q}[\alpha_1, \ldots, \alpha_n]$, where $\alpha_1, \ldots, \alpha_n$ are the roots of $f \in \overline{Q}$. L is Galois over $\mathbb{Q}$. Our strategy is to apply this result and Chebotarev with $G = \operatorname{Gal}(L/\mathbb{Q})$ and for $\mathcal{C}$ ranging over all conjugacy classes contained in G_0.

Note that $\operatorname{Gal}(L/\mathbb{Q})$ acts transitively on the n-element set of roots of f in L. For any prime p which is unramified in L and does not divide the leading coefficient of f, the degrees of the polynomials in the factorization of f over $\mathbb{F}_p$ give the cycle type of

$\sigma = \left[\frac{L/\mathbb{Q}}{p}\right]$ viewed as an element of S_n via the action on the n roots. Since the number of fixed points of a permutation is invariant under conjugation, the set $G_0 \subset \mathrm{Gal}(L/\mathbb{Q})$ of fixed-point free permutations is a (disjoint) union of conjugacy classes in $\mathrm{Gal}(L/\mathbb{Q})$. So,

$$P_0(f) \doteq \left\{p : \left[\frac{L/\mathbb{Q}}{p}\right] \in G_0\right\}, \quad \text{up to a finite set of primes.} \tag{7.1}$$

Applying the Chebotarev density theorem to the conjugacy classes $\mathcal{C} \subset G_0$, together with Cameron and Cohen's refinement of Jordan's theorem, we see that $P_0(f)$ has density $\geq 1/n$ (with strict inequality if n is not a power of p). □

We briefly remark that this application did not actually require the full power of the Chebotarev density theorem, but follows from an easier theorem of Frobenius dating back to 1880. In our notation above, Frobenius's theorem states that the density of primes p for which f factors as a product of degree $d_1, d_2, \ldots, d_t$ polynomials is proportional to the number of elements of $\mathrm{Gal}(L/\mathbb{Q})$ which at on $\{\alpha_1, \ldots, \alpha_n\}$ with cycle type $d_1, d_2, \ldots, d_t$. See [SL96] for a historical context and numerical examples exhibiting Frobenius's theorem.

Another application of this flavor shows that the set of primes (in $\mathbb{Z}$) represented by the primitive positive definite quadratic form $ax^2 + bxy + cy^2$ is positive and can be computed in terms of the discriminant and symmetries of the form. The proof applies the Chebotarev density theorem for a certain dihedral Galois extension depending on the quadratic form. For details, see Theorem 9.12. of [Cox89].

The Chebotarev density theorem can also help to prove the infinitude of some set of primes even when the set of primes cannot be shown to have positive density. As one step in Elkies's proof that every elliptic curve over $\mathbb{Q}$ has infinitely many supersingular primes [Elk87], Elkies used Dirichlet's theorem to find an additional supersingular prime outside of any finite set of supersingular primes. It seems possible that a similar argument using the full power of Chebotarev could prove the infinitude of some other set of primes.

As our next application, we show how the Chebotarev density theorem can be used to show that two pieces of data determine each other. The idea is to use Chebotarev to produce an infinite set of primes and then to use a local-to-global theorem to say that the behavior of some data at an infinite set of primes determines the data globally. The prototypical example of such a result is the fact that $x \in \mathbb{Q}$ satisfies $x = 0$ if and only if $x \equiv 0 \pmod{p}$ for infinitely many primes p. We closely follow the treatment in [Cox89], although we strengthen the statement of the theorem. The result, which says that a Galois extension is determined by the primes that split completely, is important for the study of ray class fields.

Theorem 7.3 (8.19 of [Cox89])**.** *Let K be a number field and let L and M be Galois extensions of K. Let*

$$\mathcal{P}_{L/K} := \{\mathfrak{p} \subset \mathcal{O}_K \text{ prime} : \mathfrak{p} \text{ splits completely in } L\}.$$

Then, $L = M$ if and only if there exist density zero sets of primes Σ_1 and Σ_2 such that $\mathcal{P}_{L/K} \cup \Sigma_1 = \mathcal{P} \cup \Sigma_2$.

Proof. By interchanging the roles of L and M, it suffices to prove $L \subset M$ if and only if there exists a density zero Σ such that $\mathcal{P}_{M/K} \subset \mathcal{P}_{L/K} \cup \Sigma$. If $L \subset M$, this is clear. Suppose $\mathcal{P}_{M/K} \subset \mathcal{P}_{L/K} \cup \Sigma$. Let N be the normal closure of $L \cdot M$ over K, so N/K is Galois and contains L and M. Galois theory says that it is enough to show that any $\sigma \in \mathrm{Gal}(N/M)$ fixes L.

Given $\sigma \in \mathrm{Gal}(N/M) \subset \mathrm{Gal}(N/K)$, by the Chebotarev density theorem there are infinitely many primes $\mathfrak{p}$ of K with $\sigma \in \left[\frac{N/K}{\mathfrak{p}}\right]$. Since σ fixes M, $\left[\frac{M/K}{\mathfrak{P}\cap M}\right] = 1$, whence $\mathfrak{P} \cap M$ splits completely over $\mathfrak{p}$. In particular, $\mathfrak{p} \in \mathcal{P}_{M/K}$. Then, for infinitely many primes, $\mathfrak{p} \in \mathcal{P}_{L/K}$. Now, $\alpha^{\mathrm{Nm}\,\mathfrak{p}} \cong \sigma(\alpha) \pmod{\mathfrak{P}}$ for all $\alpha \in N$ implies that $\alpha^{\mathrm{Nm}\,\mathfrak{p}} \cong \sigma|_L(\alpha) \pmod{\mathfrak{P} \cap L}$ for all $\alpha \in L$, so $\sigma|_L = \left[\frac{N/K}{\mathfrak{P}}\right]|_L = \left[\frac{L/K}{\mathfrak{P}\cap L}\right] = 1_L$ since $\mathfrak{p} \in \mathcal{P}_{L/K}$.

We could increase the density hypothesis to a small positive number given a bound on the degree over K of the Galois closure of the compositum of L and M in terms of the extensions L/K and M/K. For instance, the result still holds if we replace the hypothesis that Σ_1 and Σ_2 have density zero by the hypothesis that Σ_1 and Σ_2 have density strictly less than $\frac{1}{([L:K]\cdot[M:K])!}$ since the relative degree of the compositum is at most the product of the relative degrees of the base fields and the relative degree of the Galois closure is at most the factorial of the relative degree of the original extension. □

Our third application relates to the computational problem of determining the Galois group of L/K, or at least its cycle structure. By computing the Artin symbol at various primes, the Chebotarev density theorem says that we will eventually find an element of every conjugacy class. The "effective" versions of the Chebotarev density theorem give a bound which provides a guarantee that we will find a representative of each class after some finite computation of known length. Moreover, the effective bounds, together with a bound of the size of the Galois group can allow us to exactly determine the size of the group and the conjugacy classes. This still isn't enough to pin down the group, but is a good place to start. See the introduction to [LO77] for a bit more discussion.

Serre provided another important class of applications of the Chebotarev density theorem in [Ser81]. Even though the Chebotarev density theorem gives a result that certain sets of primes have positive density, it can be used to give better upper bounds on the sizes of certain sets of density zero primes, particularly when dealing with infinite Galois groups. Assuming I understand the French correctly, in section 4 of [Ser81], for $\mathcal{G}$ a compact ℓ-adic Lie group of M-dimension $N \geq 1$, $\mathcal{C}$ a closed subset of $\mathcal{G}$ with M-dimension $\leq d$ that is stable under conjugation, and a representation $\rho : \mathrm{Gal}(E/K) \to \mathcal{G}$ of an infinite Galois extension, Serre defines the counting function $\pi_{\mathcal{C}}(x)$ to be the number of prime ideals $\mathfrak{p} \subset \mathcal{O}_K$ of norm less than or equal to x such that $\mathfrak{p}$ is unramified in E and $\rho\left(\left[\frac{E/K}{\mathfrak{p}}\right]\right)$ (once it is appropriately defined for an infinite Galois extension) lies in $\mathcal{C}$. Serre shows that $\pi_{\mathcal{C}}(x)$ satisfies

$$\pi_{\mathcal{C}}(x) = O\left(\varepsilon(x)^{\frac{d}{N}-1} \int_2^x \frac{dx}{\log x}\right), \quad \text{as } x \to \infty, \text{ where we can take} \tag{7.2}$$

$$\varepsilon(x) = \begin{cases} \log x (\log\log x)^{-2} (\log\log\log x)^{-1}, & \text{for } x > 16 \text{ unconditionally,} \\ x^{1/2}(\log x)^{-2}, & \text{under GRH.} \end{cases} \tag{7.3}$$

The Chebotarev density theorem comes into the proof via the finite Galois groups G_n and conjugacy classes $\mathcal{C}_n$ involved in the definition of $\mathrm{Gal}(E/K)$ and $\mathcal{C}$ as a projective limit. Later on, Serre improves these bounds, and proves another application – that asymptotic formulas on the number of zeros of multiplicative functions (of ideals) along the primes can be used to give asymptotic formulas of the number of non-zero values along all ideals. Serre also uses these methods to prove upper bounds on the asymptotic number of coefficients of primes in modular forms equal to an arbitrary polynomial and to prove the surjectivity of $\mathbb{Z}_\ell$-valued representations of infinite Galois groups on the ℓ-adic Tate module of an elliptic curve for ℓ exceeding some effectively computable bound. Similar results (with the base field equal to $\mathbb{Q}$) played an important role in Mazur's theorem giving the possible degrees of isogenies over $\mathbb{Q}$. These results are all well outside the scope of this report. Still, they clearly demonstrate that the Chebotarev density theorem is not just interesting in its own right, but also has a wealth of interesting and important consequences in number theory and arithmetic geometry.

Appendix A. Notation

- Throughout this paper, K refers to a number field with ring of integers $\mathcal{O}_K$, absolute value of the discriminant d_K, and $n_K = [K : \mathbb{Q}]$ and similarly for L and E. We try our best to reserve $\mathfrak{P}$ for primes of $\mathcal{O}_L$, $\mathfrak{q}$ for primes of E, and $\mathfrak{p}$ for primes of K.
- $\mathrm{Nm}\,\mathfrak{p}$ without a subscript always refers to the absolute norm.
- χ_0 is always the trivial character of the group in question.
- $\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$ is the totient function.
- ζ_m is a primitive mth root of unity (usually in $\overline{\mathbb{Q}}$).
- $\mathrm{ord}_{s=x}\, f(s)$ denotes the order of vanishing (negative at poles) of f at the point x.
- $\mathrm{res}_\nu\, f(s)$ denotes the residue of f at ν.
- The Dedekind zeta function is $\zeta_L(s) := \sum_{\mathfrak{P}\subset\mathcal{O}_L} (\mathrm{Nm}\,\mathfrak{p})^{-s}$.
- $\left[\frac{L/K}{\mathfrak{p}}\right]$ and $\left[\frac{L/K}{\mathfrak{P}}\right]$ refer to the Artin symbol, defined in Definition 1.1.
- $\delta_{\chi_0}(\chi) = \begin{cases} 1, & \chi = \chi_0, \\ 0, & \chi \neq \chi_0, \end{cases}$ denotes the indicator function of $\{\chi_0\}$.
- $n_\chi(t)$ denotes the number of zeros ρ of $L_{L/E}(s,\chi)$ with $0 < \mathrm{Re}(\rho) < 1$ and $|\,\mathrm{Im}(\rho) - t| < 1$.

References

[CC92] Peter J. Cameron and Arjeh M. Cohen. On the number of fixed point free elements in a permutation group. *Discrete Mathematics*, 106/107:135–138, 1992.

[Cox89] David A. Cox. *Primes of the Form x + ny: Fermat, Class Field Theory, and Complex Multiplication (Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts)*. Wiley-Interscience, 1989.

[Dav00] Harold Davenport. *Multiplicative Number Theory (Graduate Texts in Mathematics) (v. 74)*. Springer, 2000.

[Elk87] N.D. Elkies. The existence of infinitely many supersingular primes for every elliptic curve over q. *Inventiones mathematicae*, 89:561–568, 1987.

[FJ08] Michael D. Fried and Moshe Jarden. The chebotarev density theorem. In *Field Arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics*, pages 107–131. Springer Berlin Heidelberg, 2008.

[Jor72] Camille Jordan. Recherches sur les substitutions. *Journal de Mathématiques Pures et Appliquées*, 17:351–367, 1872.

[Lan86] Serge Lang. *Algebraic Number Theory (Graduate Texts in Mathematics)*. Springer New York, 1986.

[LMO79] J.C. Lagarias, H.L. Montgomery, and A.M. Odlyzko. A bound for the least prime ideal in the chebotarev density theorem. *Inventiones mathematicae*, 54(3):271–296, 1979.

[LO77] J.C. Lagarias and A.M. Odlyzdo. Effective versions of the chebotarev density theorem. In A. Frohlich, editor, *Algebraic Number Fields, L-Functions and Galois Properties"*, pages 409–464. Academic Press, New York, London, 1977.

[Ser81] Jean-Pierre Serre. Quelques applications du thorme de densit de chebotarev. *Publications Mathmatiques de l'Institut des Hautes tudes Scientifiques*, 54(1):123–201, 1981.

[Ser03] Jean-Pierre Serre. On a theorem of jordan. *Bulletin (New Series) of the American Mathematical Society*, 40:429–440, 2003.

[SL96] P. Stevenhagen and H.W. Lenstra. Chebotarv and his density theorem. *The Mathematical Intelligencer*, 18(2):26–37, 1996.

[Sny02] Noah Snyder. Artin's l-functions: A historical approach. `http://math.columbia.edu/~nsnyder/thesismain.pdf`, 2002.

[Tsc26] N. Tschebotareff. Die bestimmung der dichtigkeit einer menge von primzahlen, welche zu einer gegebenen substitutionsklasse gehren. *Mathematische Annalen*, 95(1):191–228, 1926.

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, Massachusetts, 02139

E-mail address: `ngtriant@mit.edu`