L-FUNCTIONS AND THE DENSITIES OF PRIMES

ANATOLY PREYGEL

ABSTRACT. We present some of the easier to prove analytic properties of Dirichlet-Hecke L-functions, including the Dedekind zeta functions. We use Artin reciprocity to show that abelian Artin L-functions are Dirichlet-Hecke L-functions, and thus share these properties. We proceed to show a decomposition formula for the Dedekind zeta function, use this to show non-vanishing at $s = 1$ of L-series for non-principal ideal class characters, and to prove the Chebotarev Density Theorem.

1. INTRODUCTION

1.1. **Elementary Motivation.** We begin with an elementary proof, the extension of which may be viewed as a driving force for this expository paper:

Proposition 1.1.1 (Special Case of Dirichlet's Theorem on Primes)**.** *For each fixed positive integer n, there are infinitely many primes p satisfying $p \equiv 1 \pmod{n}$.*

Proof. Assume the contrary, and say that $p_1, \ldots, p_r$ is the complete list of such primes for our fixed n.

Let Φ_k be the k^{th} cyclotomic polynomial. That is:

$$\Phi_k \stackrel{\text{def}}{=} \prod_{d|k} (1 - x^{k/d})^{\mu(d)},$$

where $\mu(d)$ is $0, 1, -1$ according to whether d is divisible by a square, is the product of an even number of primes, or of an odd number of primes, respectively.

Say q is a prime such that $(k, q) = 1$. Let K denote the splitting field of $f = x^k - 1$ over $\mathbb{F}_q$. Note that $f' = kx^{k-1}$ is non-zero for $q \nmid k$, and then f and f' have no common roots. Then for $d|k$, $(x^d - 1, x^k - 1) = (x^d - 1)$, and as $f = x^k - 1$ has distinct roots, $x^d - 1 \parallel x^k - 1$. Then, counting multiplicities in the definition of Φ_k shows us that the roots of Φ_k are precisely the elements of order exactly k.

So, if Φ_k has a root over $\mathbb{F}_p$ for $p \nmid k$, then this root is an element of order k. By Lagrange's Theorem, this implies that $k \left| \left| \mathbb{F}_p^\times \right| \right. = p - 1$. So, $p \equiv 1 \pmod{k}$.

Now, let $N = n \prod p_i$. As Φ_N has only finitely many roots, we may take $k \in \mathbb{Z}_{>0}$ such that $\Phi_N(kN) \neq 0$. Then, $\Phi_N(kN)$ has prime factors, and we may let q be any prime dividing it. Note that $\Phi_N(0) = 1$, so $\Phi_N(kN) \equiv 1 \pmod{k}N$, and q is co-prime to kN and so to N. So, $q \nmid N$ and kN is a root in $\mathbb{F}_q$ of Φ_N. Thus, $q \equiv 1 \pmod{N}$ and so $q \equiv 1 \pmod{}$, but q is not one of the p_i. This yields a contradiction, establishing our result. □

We offer an alternative interpretation of the idea of the above proof, using some standard results of algebraic number theory. Let $K = \mathbb{Q}(\zeta_n)$ be the n^{th} cyclotomic field. Then, $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$, and the primes which ramify in K all divide n. For p an unramified prime of K, the map $\{\zeta_n \mapsto \zeta_n^p\}$ is the Frobenius of p. Now, the reduction of Φ_n in $\mathbb{F}_p[x]$ factors as

$\prod_{i=1}^{g} f_i^e$, where $e = 1$ (recall unramified) and $\deg f_i = f$ is the order of the Frobenius. So, Φ_n splits into linear factors if and only if the Frobenius is trivial. This occurs if and only if $\zeta_n^{p-1} = 1$, which occurs if and only if $p \equiv 1 \pmod{n}$. So, our problem is equivalent to finding many primes with trivial Frobenius. It turns out that the question of the distribution of primes with a specified Frobenius is a fruitful generalization, and the goal of this paper will be to develop the techniques to prove the Chebotarev Density Theorem.

The above proof is entirely algebraic, and is relatively elementary. However, it seems that such algebraic methods only get us so far. Indeed, in 1837 Dirichlet brought in analytic methods to prove the following result generalizing our above proposition:

Theorem 1.1.1 (Dirichlet's Theorem on Primes in an Arithmetic Progression)**.** *Let $a, b \in \mathbb{N}$ be such that $(a, b) = 1$. Then, there are infinitely many primes p satisfying $p \equiv a \pmod{b}$.*

To this day, results of this nature are handled with analytic machinery. We will begin by developing sufficient tools to sketch a proof of this result, before extending them to allow us to prove our desired generalization.

1.2. **Characters and L-functions.** In proving his theorem, Dirichlet introduced a class of analytic objects tied to the rational number field: the Dirichlet L-series.

We assume the reader is familiar with basic representation theory of finite groups. Throughout this paper, all representations will be over $\mathbb{C}$. For an abelian group G, we will use the word *character* to refer to a (continuous) homomorphism $G \to S^1 \subseteq \mathbb{C}^\times$ [note that for G finite, these characters are precisely the one-dimensional representations under the identification $\mathrm{GL}_1(\mathbb{C}) \leftrightarrow \mathbb{C}^\times$, for the image must be a torsion element]. We let $\mathrm{Hom}(G, S^1)$ denote the group of characters of G; we will denote the identity in $\mathrm{Hom}(G, S^1)$ by χ_0 which we will call the *principal character*. We will prove some of the basic properties of this construction:

Proposition 1.2.1. *For G a finite abelian group (written multiplicatively here). Then:*

(a) $G \simeq \mathrm{Hom}(G, S^1)$*;*

(b) $G \cong \mathrm{Hom}(\mathrm{Hom}(G, S^1), S^1)$ *by the evaluation map;*

(c) $\sum_{g \in G} \chi(g) = \begin{cases} |G| & \chi = \chi_0 \\ 0 & \text{otherwise} \end{cases}$*;*

(d) $\sum_{\chi \in \mathrm{Hom}(G, S^1)} \chi(g) = \begin{cases} |G| & g = 1 \\ 0 & \text{otherwise} \end{cases}$*.*

(e) *For any $g \in G$, we have*

$$\prod_{\chi \in \mathrm{Hom}(G, S^1)} (1 - \chi(g)t) = \left(1 - t^{\operatorname{ord} g}\right)^{\frac{|G|}{\operatorname{ord} g}}.$$

Proof. By the structure theorem for finite abelian groups, we may decompose G into cyclic factors

$$G \xrightarrow[\gamma]{\sim} \bigoplus_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z}$$

with $1 < n_i || G|$.

Let ζ_i be a primitive n_i^{th} root of unity, and consider the map:

$$G \longrightarrow \operatorname{Hom}(G, S^1)$$

$$g \longmapsto \chi^g(a) = \prod_i \zeta_i^{\gamma(a)_i \gamma(g)_i}$$

We readily check that each χ^g is indeed a homomorphism $G \to S^1$ (for it maps the generator of the i^{th} cyclic summand to $\zeta_i^{\gamma(g)_i}$). Furthermore, every such homomorphism is of this form, for it must map this generator to an element of order dividing n_i, so to a power of ζ_i. So, this map is surjective onto $\operatorname{Hom}(G, S^1)$. We may explicitly check that it is a homomorphism. Now, it suffices to prove injectivity. But indeed, $\chi^g = \chi_0$ implies that χ^g is 1 on the generators of the cyclic summands, which in turn implies $\zeta_i(\gamma(g)_i) = 1$, whence $\gamma(g)_i = 0$, for each i, and thus $g = 1$. This proves (a).

For (b), note that the evaluation map

$$G \ni g \mapsto \widehat{\widehat{g}} \text{ s.t. } \widehat{\widehat{g}}(\chi) = \chi(g)$$

is a homomorphism $G \to \operatorname{Hom}(\operatorname{Hom}(G, S^1), S^1)$. For each $g \in G$ distinct from id, there will be some character with non-trivial value on G by the above characterization of $\operatorname{Hom}(G, S^1)$, so this map is an injection. By (a), we have that $|G| = |\operatorname{Hom}(\operatorname{Hom}(G, S^1), S^1)|$, so this map must be an isomorphism.

For (c), note that the claim is trivial for $\chi = \chi_0$. Then, if $\chi \neq \chi_0$, then there exists a $g' \in G$ such that $\chi(g') \neq 1$. Then

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

which implies our desired result.

Then, (d) follows from (b) and (c).

Now, let $H = \langle g \rangle$. We may take H to be one of our cyclic factors for G. Take it to be our first cyclic factor, and then $n_1 = \operatorname{ord} g$. Then, by the above characterization, we see that:

$$\begin{aligned}
\prod_{\chi \in \operatorname{Hom}(G, S^1)} (1 - \chi(g)t) &= \prod_{a_1=1}^{n_1} \prod_{a_2=1}^{n_2} \cdots \prod_{a_r=1}^{n_r} \left(1 - \zeta_{n_1}^{a_1} t\right) \\
&= \left(\prod_{a_1=1}^{n_1} \left(1 - \zeta_{n_1}^{a_1} t\right) \right)^{n_2 \cdots n_r} \\
&= \left(1 - t^{n_1}\right)^{n_2 \cdots n_r} \\
&= \left(1 - t^{\operatorname{ord} g}\right)^{\frac{|G|}{\operatorname{ord} g}}.
\end{aligned}$$

This shows (e). We could also have established this by noting that $G \cong H \oplus G/H$ so $\operatorname{Hom}(G, S^1) \cong \operatorname{Hom}(H, S^1) \oplus \operatorname{Hom}(G/H, S^1)$, and a similar product identity. □

Now, we will introduce Dirichlet's L-series.

Definition. Let $N > 1$ be an integer. Let χ be a character of $(\mathbb{Z}/N\mathbb{Z})^\times$. We may extend χ to a multiplicative function, which we also call χ, on $\mathbb{Z}$ by:

$$\chi(k) = \begin{cases} \chi(\bar{k}) & (k, N) = 1, \bar{k} = \text{image of } k \text{ in } (\mathbb{Z}/N\mathbb{Z})^\times \\ 0 & \text{otherwise} \end{cases}$$

We refer to both of these meanings of χ as the *Dirichlet character*. There shall be no ambiguity, for it will always suffice to expand to a function on $\mathbb{Z}$.

Then, the *Dirichlet L-series* for the Dirichlet character χ is:

$$\mathrm{L}(s, \chi) \stackrel{\text{def}}{=} \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \sum_{(n,N)=1} \frac{\chi(n)}{n^s}$$

Remark. Not worrying about convergence, the quick reader may immediately notice that the multiplicative property of χ lets us write the above in a product form:

$$\prod_{p \text{ prime}} \left(1 - \chi(p)p^{-s}\right)^{-1}.$$

Indeed, a Dirichlet series expansion and an Euler product expansion are two of the properties, along with a functional equation, defining L-series.

1.3. **Convergence properties of Dirichlet series.** We wish to prove some convergence properties of the $\mathrm{L}(s, \chi)$. We will consider a more general class of objects, in order to get results that we can re-use later.

Definition. A *Dirichlet series* is a series of the form

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

with the a_n complex numbers and s a complex variable.

Lemma 1.3.1. *If the Dirichlet series $\sum_n \frac{a_n}{n^s}$ converges for some $s = s_0$, then it converges for any s with $\mathrm{Re}(s) > \mathrm{Re}(s_0)$, and converges uniformly on any compact subset of this region (so, the series represents an analytic function on that half plane).*

Moreover, if there exist constants $C, \sigma > 0$ such that $|a_1 + \ldots + a_k| \leq Ck^\sigma$ for each $k \geq 1$, then the series converges for $\mathrm{Re}(s) > \sigma$.

Proof. Let $P_n(s) = \sum_{i=0}^{n} a_i i^{-s}$.

For $\delta > 0$, $\mathrm{Re}(s) \geq \mathrm{Re}(s_0) + \delta$, $i > 0$ note that we have:

$$\left|\frac{1}{i^{s-s_0}} - \frac{1}{(i+1)^{s-s-0}}\right| = \left|(s - s_0)\int_i^{i+1} \frac{dx}{x^{s-s_0+1}}\right| \leq |s - s_0| \frac{1}{i^{\mathrm{Re}(s)-\mathrm{Re}(s_0)+1}} \leq \frac{|s - s_0|}{i^{1+\delta}}$$

Then, for $m < n$ we have

$$\begin{aligned} |P_n(s) - P_m(s)| &= \left|\sum_{i=m+1}^{n} \frac{a_i}{i^{s_0} i^{s-s_0}}\right| \\ &= \left|\frac{P_n(s_0)}{n^{s-s_0}} - \frac{P_m(s_0)}{(m+1)^{s-s_0}} + \sum_{i=m+1}^{n-1} P_i(s_0)\left[\frac{1}{i^{s-s_0}} - \frac{1}{(i+1)^{s-s_0}}\right]\right| \end{aligned}$$

and by the above:

$$\leq \left|\frac{1}{(m+1)^{s-s_0}}\right| \left|P_m(s_0) - P_n(s_0)\left(\frac{m+1}{n}\right)^{s-s_0}\right| + \sum_{i=m+1}^{n-1} |P_i(s_0)| \frac{|s-s_0|}{i^{1+\delta}}$$

Now, as $P_n(s_0)$ converges, we may take M s.t. $M \geq |P_n(s_0|$ for all n. Then:

$$\leq 2M \left|\frac{1}{(m+1)^{\delta}}\right| + M|s-s_0| \sum_{i=m+1}^{\infty} \frac{1}{i^{1+\delta}}$$

Now, on any compact set, $|s-s_0|$ is bounded, and the last sum is convergent by the integral test, so taking m sufficiently large we see that the P_n converge uniformly on compact subsets of $\mathrm{Re}(s) \geq 1+\delta$. Recall that the uniform-on-compacts limit of holomorphic functions on a domain is holomorphic. Applying this to the partial sums of the Dirichlet series, this completes the first part of the result. This afford us the freedom to be sloppy in declaring that convergent Dirichlet series give analytic functions.

Now, let $S_n = a_1 + \ldots + a_n$. Then, for $n > m$, $\delta > 0$ and $\mathrm{Re}(s) \geq \sigma + \delta$:

$$\begin{aligned} |P_n(s) - P_m(s)| &= \left|\frac{A_n}{n^s} - \frac{A_m}{(m+1)^s} + \sum_{i=m+1}^{n-1} A_k \left[\frac{1}{i^s} - \frac{1}{(i+1)^s}\right]\right| \\ &\leq \frac{C}{n^{\mathrm{Re}(\sigma)-s}} + \frac{C}{(m+1)^{\mathrm{Re}(\sigma)-s}} + \sum_{i=m+1}^{n-1} C\left[\frac{1}{i^{s-\sigma}} - \frac{1}{(i+1)^{s-\sigma}}\right] \end{aligned}$$

and by the above:

$$\leq \frac{C}{n^{\delta}} + \frac{C}{(m+1)^{\delta}} + C\,|s-\sigma| \sum_{i=m+1}^{n-1} \frac{1}{i^{1+\delta}}$$

This proves our result. □

1.4. **Sketch of Proof of Theorem 1.1.1.** We will use the following analytic results in this proof:

(a) Convergence of $\mathrm{L}(s,\chi)$ and ζ_K (Dedekind zeta) for $\mathrm{Re}(s) > 1$, and for $\mathrm{Re}(s) > 0$ for $\chi \neq \chi_0$.
(b) Existence and convergence of Euler product for $\mathrm{L}(s,\chi)$ and ζ_K for $\mathrm{Re}(s) > 1$.
(c) For $\chi \neq \chi_0$, $\mathrm{L}(s,\chi)$ is analytic at $s = 1$. $\mathrm{L}(s,\chi_0)$ and ζ_K all have simple poles at $s = 1$.

We prove the first of these here. We prove more general version of the later two in the sequel.

Let $G = (\mathbb{Z}/b\mathbb{Z})^{\times}$. Then, for $\chi \in \mathrm{Hom}(G, S^1)$ not the principal character, we note that by Prop. 1.2.1 the sums $\sum_{n=1}^{k} a_n = \sum_{n=1}^{k} \chi(k)$ are cyclic and so bounded. So, we may apply Lemma 1.3.1 to $\mathrm{L}(s,\chi)$ with $\sigma = 0$, to get that $\mathrm{L}(s,\chi)$ is analytic for $\mathrm{Re}(s) > 0$ and so at $s = 1$. Applying Lemma 1.3.1 to $\mathrm{L}(s,\chi_0)$ with $\sigma = 1$ yields that it is analytic for $\mathrm{Re}(s) > 1$.

Also, using multiplicativity of χ and the Fundamental Theorem of Arithmetic, we may prove the Euler product expansion for $\mathrm{L}(s,\chi)$:

$$\mathrm{L}(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p \text{ prime}} \left(1 - \chi(p)p^{-s}\right)^{-1}.$$

For $p \nmid b$, let $f(p)$ denote the order of the image of p in G. Then, by Prop. 1.2.1 we have

$$\prod_{\chi \in \mathrm{Hom}(G,S^1)} \mathrm{L}(s,\chi) = \prod_{p \nmid b} \left(1 - p^{-sf(p)}\right)^{-\phi(b)/f(p)}.$$

Let $K = \mathbb{Q}(\zeta_b)$. Define $\zeta_K = \prod_{\mathfrak{p}} \left(1 - \mathrm{Norm}(\mathfrak{p})\right)^{-1}$, where the product is over finite primes of K.

Now, note that the only rational primes ramified in $K/\mathbb{Q}$ are those dividing b, by a discriminant argument. So, we may show that

$$\zeta_K(s) = \prod_{p} \left(1 - p^{-sf(p)}\right)^{-\phi(b)/f(p)} = \prod_{\chi \in \mathrm{Hom}(G,S^1)} \mathrm{L}(s,\chi) \prod_{p \mid b} \left(1 - p^{-sf(p)}\right)^{-\phi(b)/f(p)}.$$

The last factors are analytic at $s = 1$, ζ_K and $\mathrm{L}(s,\chi_0)$ have simple poles at $s = 1$, and the other factors are analytic there. So, the equality implies that these analytic factors are non-zero. That is, $\mathrm{L}(1,\chi) \neq 0$ for $\chi \neq \chi_0$.

Then, letting a^{-1} be the inverse of a in G, note that by Prop. 1.2.1 we have

$$\sum_{p \equiv a \pmod{b}} p^{-s} = \frac{1}{|G|} \sum_{\chi \in \mathrm{Hom}(G,S^1)} \sum_{p} \chi(p)\chi(a^{-1})p^{-s}$$

Now, for functions f, g, we write $f \sim g$ if $f - g$ may be analytically continued on some neighborhood of $s = 1$.

Taking logarithms in the Euler product for $\mathrm{L}(s,\chi)$ we get

$$\log \mathrm{L}(s,\chi) = \sum_{p} \chi(p)p^{-s} + \sum_{p} \sum_{m \geq 2} \frac{1}{m} \chi(p^m)p^{-sm}$$

This last term is absolutely convergent in a neighborhood of $s = 1$ by comparison to $\zeta(2s)$, which is analytic on $\mathrm{Re}(s) > \frac{1}{2}$. So,

$$\sum_{p \equiv a \pmod{b}} p^{-s} \sim \frac{1}{|G|} \sum_{\chi \in \mathrm{Hom}(G,S^1)} \chi(a^{-1}) \log \mathrm{L}(s,\chi)$$

We have that $(s-1)\mathrm{L}(s,\chi_0)$ is analytic and non-vanishing at $s = 1$ (we just kill the simple pole), so $\log \mathrm{L}(s,\chi_0) \sim \log \frac{1}{s-1}$. Also, for $\chi \neq \chi_0$ we have that $\mathrm{L}(s,\chi)$ is analytic at $s = 1$. Then

$$\sum_{p \equiv a \pmod{b}} p^{-s} \sim \frac{1}{|G|} \chi_0(a^{-1}) \log \frac{1}{s-1} = \frac{1}{|G|} \log \frac{1}{s-1}.$$

If there were finitely many primes $p \equiv a \pmod{b}$, then this sum would be bounded as $s \to 1^+$, but $\log \frac{1}{s-1}$ is not. This yields our desired result.

Remark. There are other ways to establish the crucial fact that $\mathrm{L}(1,\chi) \neq 0$. The above method closely mirrors the proof that we will follow below. Another common approach is to split into the case of complex characters (that is, $\chi^2 \neq \chi_0$) and real characters (that is, $\chi^2 = \chi_0$). Such an approach may in fact be used to prove the general case that we wish to use here; see for instance [Hei67].

1.5. **Prerequisites and references.** We assume that the reader has a reasonable familiarity with basic complex analysis, the splitting of primes in number fields, basic commutative algebra (incl. localization), and valuations. In addition, we will state and then use without proof the fundamental results of class field theory. In addition, we will occasionally make remarks hinting at the more general theory, specifically Großencharakters, analytic continuation, and Artin L-series.

There are many excellent references on this material and the topics surrounding it. For a historical account of class field theory see [Coh85]; for the modern cohomological treatment see one of [Lan94], [Jan96] (lacks the idèlic formulation, the closest to the exposition of class field theory given here), [Lan94] (no proofs for global theory), [SD01] (concise!), [Neu86] (s slightly unusual cohomological treatment, without the Brauer group!), [Neu99] (as the previous). For an analytic view on class field theory, including all the theory of L-functions discussed herein and more, see [Gol71].

A full treatment of Dirichlet-Hecke L-functions (including a proper treatment of Großencharakters) may be found in [Gol71], [SD01] (concise!), or [Tat67] (the original source for many of the arguments given in the preceding two). These sources also address the question of analytic continuation of these L-functions to all of $\mathbb{C}$, as does [Neu99] (with a different approach, using theta functions, from Hecke). The exposition of the analytic theory in [Neu86] is simple, and is the closest to the exposition given here.

1.6. **Notation.** Unless otherwise stated, we will use the following notation throughout the remainder of this document:

K will denote a number field.

By a prime of K we will mean either a non-zero prime ideal of $\mathcal{O}_K$ (a "finite prime"), or a real embedding $K \hookrightarrow \mathbb{R}$ (a "real infinite prime"), or a conjugate pair of complex embeddings $K \hookrightarrow \mathbb{C}$ (a "complex infinite prime"). Equivalently, we may regard these as the equivalence classes of valuations on K. We will use ν to denote a (not necessarily finite) prime of K, and K_ν will denote the completion of K with respect to the topology induced by the valuation (along with the canonical inclusion $K \hookrightarrow K_\nu$ written $x \mapsto x_\nu$).

For an extension L/K of number fields, $\mathfrak{p}$ a finite prime of K and $\mathfrak{P}$ a prime lying above it, we will denote by $D_{\mathfrak{P}}, I_{\mathfrak{P}}$ the decomposition and inertia groups of $\mathfrak{P}$ (if our extension is abelian, we may write $\mathfrak{p}$ in place of $\mathfrak{P}$). For $\mathfrak{p}$ unramified, we will denote by $\left[\frac{L/K}{\mathfrak{P}}\right]$ the Frobenius corresponding to $\mathfrak{P}$ and by $\left(\frac{L/K}{\mathfrak{p}}\right)$ the Artin map of $\mathfrak{p}$, that is the conjugacy class $\{\left[\frac{L/K}{\mathfrak{P}}\right] : \mathfrak{P}|\mathfrak{p}\}$ (which we will regard as just an element for L/K abelian). If $\mathfrak{p}$ is ramified, we modify each of these to be $I_{\mathfrak{P}}$-cosets. We define the Artin map on arbitrary ideals by unique factorization into primes.

For functions f, g, we write $f \sim g$ if $f - g$ may be analytically continued on some neighborhood of $s = 1$.

2. Congruence subgroups, class groups, and reciprocity

In order to generalize the notion of a Dirichlet character and series, we must have an appropriate generalization of the group $(\mathbb{Z}/n\mathbb{Z})^\times$. In the context of our proof-sketch above, the field $K = \mathbb{Q}(\zeta_n)$ was introduced. Indeed, the $(\mathbb{Z}/n\mathbb{Z})^\times$ may be viewed as the Galois group $\mathrm{Gal}(K/\mathbb{Q})$.

Let us consider the phrasing of our goal in terms of Frobenius elements of Galois extensions. Observe that for $L/F/K$ a tower of Galois extensions, the restriction map induces a surjection of decomposition groups $D_{\mathfrak{P}} \to D_{\mathfrak{p}}$, for $\mathfrak{P}$ a prime of L and $\mathfrak{p} = \mathcal{O}_F \cap \mathfrak{p}$. So, to understand the Frobenius elements of F we may look at the Frobenius elements of L. When our base field is $\mathbb{Q}$, the Kronecker-Weber theorem assures us that every abelian extension $K/\mathbb{Q}$ is contained in some cyclotomic extension. Now, our characterization of the Frobenius in cyclotomic extensions lets us reduce this study to the study of certain congruences defining the relevant subgroup of the Galois group of this cyclotomic field.

Example. The above discussion is almost in reverse of how we got to the Frobenius statement in the first place. Let us bring things back to that context for a quick example. Say we wanted to look for primes p satisfying $p \equiv \pm 1 \pmod 7$. Note that $\{\pm 1\} \subset (\mathbb{Z}/7\mathbb{Z})^\times$ is a subgroup. Now, we may realize the latter as $\mathrm{Gal}(K/\mathbb{Q})$ for $K = \mathbb{Q}(\zeta_7)$. Then, let H be the subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ corresponding to $\{\pm 1\}$, and set $L = K^H = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$. Then, for p not ramified in K (that is, not 7), we have that $\left(\frac{K/\mathbb{Q}}{p}\right) = \{\zeta_7 \mapsto \zeta_7^p\}$, and $p \equiv \pm 1 \pmod 7 \Leftrightarrow \left(\frac{K/\mathbb{Q}}{p}\right) \in H \Leftrightarrow \left(\frac{L/\mathbb{Q}}{p}\right) = \mathrm{id}$. From this, $p \equiv \pm 1 \pmod 7 \Leftrightarrow p$ splits completely in $L/\mathbb{Q}$. Finding the minimal polynomial for a primitive element of L, and showing that the ring of integers is monogenic, we can relate this to polynomials: $p \equiv \pm 1 \pmod 7 \Leftrightarrow x^3 + x^2 - 2x - 1$ splits in $\mathbb{F}_p[x]$, a "reciprocity law!"

This picture over $\mathbb{Q}$ is the prototype for what follows.

2.1. **Notation.** Let $\mathbf{I}_K$ denote the free abelian group generated by the finite primes of K. For a set S of primes of K, let $\mathbf{I}_K^S$ denote the free abelian group generated by the finite primes of K excluding the elements of S. We let $\iota : K^\times \to \mathbf{I}_K$ be the map given by $a \mapsto a\mathcal{O}_K = \prod_i \mathfrak{p}_i^{e_i} \in \mathbf{I}_K$.

Define an *modulus* as a formal product of primes of K. We write $x \equiv 1 \pmod{\mathfrak{m}}$ to mean that:

- For each finite prime $\mathfrak{p} \mid \mathfrak{m}$ we have $\mathrm{ord}_{\mathfrak{p}}(x-1) \geq m$ for $m > 0$ such that $\mathfrak{p}^m \parallel \mathfrak{m}$;
- For each real infinite prime $\nu \mid \mathfrak{m}$ we have $x_\nu > 0$.

Denote $\mathbf{I}_K^{\mathfrak{m}} \stackrel{\text{def}}{=} \mathbf{I}_K^S$ where $S = \{\mathfrak{p} \text{ finite prime} : \mathfrak{p} \mid \mathfrak{m}\}$.

Denote

$$K^{\mathfrak{m}} \stackrel{\text{def}}{=} \iota^{-1}(\mathbf{I}_K^{\mathfrak{m}}) = \left\{ \frac{a}{b} : a, b \in \mathcal{O}_K, \text{for each prime } \mathfrak{p} \in S \ \mathrm{ord}_{\mathfrak{p}} a = \mathrm{ord}_{\mathfrak{p}} b = 0 \right\}$$

and

$$K_1^{\mathfrak{m}} \stackrel{\text{def}}{=} \{x \in K^{\mathfrak{m}} : x \equiv 1 \pmod{\mathfrak{m}}\}.$$

Finally, denote:

$$\mathbf{P}_K^{\mathfrak{m}} \stackrel{\text{def}}{=} \iota(K_1^{\mathfrak{m}}) \subseteq \mathbf{I}_K^{\mathfrak{m}} \qquad \text{and} \qquad \mathrm{Cl}_K^{\mathfrak{m}} \stackrel{\text{def}}{=} \mathbf{I}_K^{\mathfrak{m}} / \mathbf{P}_K^{\mathfrak{m}}.$$

We call $\mathrm{Cl}_K^{\mathfrak{m}}$ the *ray class group of* $\mathfrak{m}$. We will often drop the subscript K from $\mathbf{I}_K^{\mathfrak{m}}, \mathbf{P}_K^{\mathfrak{m}}, \mathrm{Cl}_K^{\mathfrak{m}}$. If we drop the $\mathfrak{m}$, then it is assumed that $\mathfrak{m} = 1$.

2.2. **Congruence subgroups.** A *congruence subgroup* (defined mod. $\mathfrak{m}$) is a subgroup $H^{\mathfrak{m}}$ of $\mathbf{I}_K^{\mathfrak{m}}$ containing $\mathbf{P}_K^{\mathfrak{m}}$. Whenever we write a superscript modulus on a group, we take that to mean that it is a congruence subgroup defined mod. $\mathfrak{m}$.

Proposition 2.2.1. *Say* $\mathfrak{m}|\mathfrak{n}$*, then* $\mathbf{I}^{\mathfrak{m}} \supseteq \mathbf{I}^{\mathfrak{n}}$*. Define* $H^{\mathfrak{n}} = H^{\mathfrak{m}} \cap \mathbf{I}^{\mathfrak{n}}$*. Then,* $H^{\mathfrak{n}}$ *is a congruence subgroup (defined mod.* $\mathfrak{n}$*) and:*

(a) $H^{\mathfrak{m}} = H^{\mathfrak{n}}\mathbf{P}^{\mathfrak{m}}$*;*
(b) *the inclusion* $\mathbf{I}^{\mathfrak{n}} \hookrightarrow \mathbf{I}^{\mathfrak{m}}$ *induces* $\mathbf{I}^{\mathfrak{n}}/H^{\mathfrak{n}} \cong \mathbf{I}^{\mathfrak{m}}/H^{\mathfrak{m}}$*.*

Proof. [Jan96, Ch. V, §6] The general idea of the proof is to use the Chinese Remainder Theorem to show that we may avoid given ideals in a suitable sense. □

So, if a congruence subgroup is defined mod. $\mathfrak{m}$, it is uniquely defined mod. all multiples of $\mathfrak{m}$. Then, we may define an equivalence relation on congruence subgroups, with $H_1^{\mathfrak{m}_1} \sim H_2^{\mathfrak{m}_2}$ if there is some common multiple $\mathfrak{m}$ of $\mathfrak{m}_1, \mathfrak{m}_2$ such that they have common restriction to $\mathbf{I}^{\mathfrak{m}}$ (that is, if $H_1^{\mathfrak{m}_1} \cap \mathbf{I}^{\mathfrak{m}} = H_2^{\mathfrak{m}_2} \cap \mathbf{I}^{\mathfrak{m}}$). Call such an equivalence class of congruence subgroups an *ideal group* or by abuse of terminology a *congruence subgroup*. We will write H for an ideal group, and then $H^{\mathfrak{m}}$ for its realization mod. $\mathfrak{m}$.

By the above, the quotients $\mathbf{I}^{\mathfrak{m}_i}/H_i^{\mathfrak{m}_i}$ for $i = 1, 2$ will be isomorphic. So, to each ideal group we may associate an equivalence class of such quotients, which we will call the *congruence class group*. We will sometimes write this as just $\mathbf{I}/H$.

Proposition 2.2.2. *Say* $H_1^{\mathfrak{m}_1} \sim H_2^{\mathfrak{m}_2}$*. Let* $\mathfrak{m}$ *be the greatest common divisor of* $\mathfrak{m}_1$ *and* $\mathfrak{m}_2$*. Then, there is a congruence subgroup* $H^{\mathfrak{m}}$ *such that* $H^{\mathfrak{m}} \cap \mathbf{I}^{\mathfrak{m}_i} = H_i^{\mathfrak{m}_i}$ *for* $i = 1, 2$*.*

Proof. [Jan96, Ch. V, §6] □

Combining Prop. 2.2.1 and Prop. 2.2.2, we see that for any ideal group H there is a minimal modulus (with respect to divisibility) $\mathfrak{f}$ such that H may be realized mod. $\mathfrak{f}$. We call this the *conductor* of H. Similarly, we have the notion of conductor of a congruence class group I/H, defined as the conductor of H.

2.3. **Finiteness of congruence class groups.** Now, we claim that each congruence class group is finite. If we have $\mathbf{P}^{\mathfrak{m}} \subseteq H^{\mathfrak{m}} \subseteq \mathbf{I}^{\mathfrak{m}}$, then we may regard $\mathbf{I}^{\mathfrak{m}}/H^{\mathfrak{m}}$ as a subgroup of $\mathbf{I}^{\mathfrak{m}}/\mathbf{P}^{\mathfrak{m}} = \mathrm{Cl}^{\mathfrak{m}}$. So, it suffices to show that the ray class groups are finite:

Proposition 2.3.1. $\mathrm{Cl}^{\mathfrak{m}}$ *is finite*

Proof. Note that

$$[\mathbf{I}^{\mathfrak{m}} : \mathbf{P}_K^{\mathfrak{m}}] = [\mathbf{I}^{\mathfrak{m}} : \iota(K_1^{\mathfrak{m}})] = [\mathbf{I}^{m} : \iota(K^{\mathfrak{m}})][\iota(K^{\mathfrak{m}}) : \iota(K_1^{\mathfrak{m}})].$$

Note that $\iota(K^{\mathfrak{m}}) = \mathbf{I}^{\mathfrak{m}} \cap \mathbf{P}^1$. So, by the above, $I^{\mathfrak{m}}/\iota(K^{\mathfrak{m}}) \cong \mathbf{I}^1 \cap \mathbf{P}^1 = \mathrm{Cl}_K$. So, the first term is just the class number, which is finite.

The second factor is a divisor of $[K^{\mathfrak{m}} : K_1^{\mathfrak{m}}]$, so it suffices to show that this quantity is finite. Say $\mathfrak{m} = \prod_{i=1}^r \mathfrak{m}_i$ where $\mathfrak{m}_i = \nu_i^{n_i}$ with the ν_i distinct. Then, consider the reduction map

$$\frac{K^{\mathfrak{m}}}{K_1^{\mathfrak{m}}} \longrightarrow \prod_{i=1}^{r} \frac{K^{\mathfrak{m}_i}}{K_1^{\mathfrak{m}_i}}.$$

Note that the kernel of this map is the set of elements in each $K_1^{\mathfrak{m}_i}$, which is precisely $K_1^{\mathfrak{m}}$ for the constraints imposed by each $\mathfrak{m}_i$ are independent and in total are precisely the constraints imposed by $\mathfrak{m}$. So, the map is injective.

By writing out the conditions for something to map to a prescribed element of the codomain and applying the Weak Approximation Theorem (a weak form of the equivalent of the Chinese Remainder Theorem for valuations), we see that the map is surjective.

So, it suffices to prove that each term in the product is finite. If $\mathfrak{m}$ is a complex place, the quotient is trivial; if it a real place, the quotient has order 2.

If $\mathfrak{m} = \mathfrak{p}^n$ is a finite place, then

$$K^{\mathfrak{m}} = \left\{ \frac{a}{b} : a, b \in \mathcal{O}_K, \mathfrak{p} \nmid a, b \right\} = (\mathcal{O}_K)_{\mathfrak{p}}^{\times},$$

where the subscript denotes localization.

Then, $K_1^{\mathfrak{m}} = 1 + \mathfrak{p}^n(\mathcal{O}_K)_{\mathfrak{p}}$.

So, the quotient is

$$\frac{(\mathcal{O}_K)_{\mathfrak{p}}^{\times}}{1 + \mathfrak{p}^n(\mathcal{O}_K)_{\mathfrak{p}}} \cong \left(\frac{(\mathcal{O}_K)_{\mathfrak{p}}}{\mathfrak{p}^n(\mathcal{O}_K)_{\mathfrak{p}}} \right)^{\times} \cong \left(\frac{\mathcal{O}_K}{\mathfrak{p}^n} \right)_{\mathfrak{p}}^{\times}$$

Now, $\frac{\mathcal{O}_K}{\mathfrak{p}^n}$ is finite, so this last group is finite. This proves our claim. □

2.4. **Artin reciprocity.** In the following sections we will want to invoke class field theory. So, we will briefly review a statement of the important results, without proof.

Theorem 2.4.1 (Artin Reciprocity Theorem)**.** *For L/K an abelian extension of number fields, there is a modulus $\mathfrak{m}$ divisible by all the ramified primes of L/K and a congruence subgroup $H^{\mathfrak{m}}$ such that the following is an exact sequence*

$$1 \longrightarrow H^{\mathfrak{m}} \hookrightarrow \mathbf{I}_K^{\mathfrak{m}} \xrightarrow{\left(\frac{L/K}{\cdot}\right)} \mathrm{Gal}(L/K) \longrightarrow 1.$$

Explicitly, we have $H^{\mathfrak{m}} = \mathbf{P}_K^{\mathfrak{m}} \cdot \mathrm{Norm}_{L/K}(\mathbf{I}_L^{\mathfrak{m}})$.

When the conditions of the previous theorem hold, we say that L is the *class field* for K of the congruence class group $\mathbf{I}_K^{\mathfrak{m}}/H^{\mathfrak{m}}$. Furthermore, we say that $\mathfrak{m}$ is an admissible modulus for L/K and for the corresponding congruence class group $\mathbf{I}/H$. We define the *conductor* of L/K to be the minimal (with respect to divisibility) modulus $\mathfrak{f}$ such that $\mathfrak{f}$ is an admissible modulus for L/K (equivalently, the conductor of $\mathbf{I}/H$). We have the following result:

Proposition 2.4.1. *Let $\mathfrak{f}$ be the conductor of L/K. Then, the primes dividing $\mathfrak{f}$ are precisely the ramified primes of L/K.*

In addition to the reciprocity theorem, there is also a correspondence going the other way:

Theorem 2.4.2 (Existence Theorem)**.** *For any congruence subgroup $\mathbf{P}_K^{\mathfrak{m}} \subseteq H^{\mathfrak{m}} \subseteq \mathbf{I}_K^{\mathfrak{m}}$, there is a unique abelian extension L/K such that L is the class field for K of the congruence class group $\mathbf{I}_K^{\mathfrak{m}}/H^{\mathfrak{m}}$. [Equivalently, such that $H^{\mathfrak{m}} = \mathbf{P}_K^{\mathfrak{m}} \cdot \mathrm{Norm}_{L/K}(\mathbf{I}_L^{\mathfrak{m}})$.]*

These two theorems provide a correspondence between objects outside of K, specifically the abelian extensions, and objects inside K, specifically the congruence subgroups.

Remark. Let us look at the situation over $\mathbb{Q}$ in this context. The abelian extensions over $\mathbb{Q}$ correspond to congruence subgroups, which in turn correspond to subgroups of the ray class groups, here $(\mathbb{Z}/m\mathbb{Z})^\times$. Call the class field corresponding to a ray class group a *ray class field*. Then, for any abelian extension $K/\mathbb{Q}$, we have the conductor $\mathfrak{m}$. We may assume that $\infty \mid \mathfrak{m}$ and $\mathfrak{m} = m\infty$, in which case we get that the ray class field for $\mathfrak{m}$ is $\mathbb{Q}(\zeta_m)$. So, the notion of admissible modulus and conductor correspond in this setting to finding a cyclotomic extension containing K (almost: the case where $\infty \nmid \mathfrak{m}$ leads to the ray class field being the maximal totally real subfield of the cyclotomic extension, to keep the real infinite prime of $\mathbb{Q}$ from splitting).

3. Dirichlet-Hecke L-functions

3.1. **Definitions.** Now, we may consider the group of characters of $\mathrm{Cl}_K^{\mathfrak{m}}$, which is a finite abelian group by Prop. 2.3.1.

For $\chi \in \mathrm{Hom}(\mathrm{Cl}_K^{\mathfrak{m}}, S^1)$ we may view χ as a function on $\mathbf{I}_K^{\mathfrak{m}}$ whose kernel contains $\mathbf{P}_K^{\mathfrak{m}}$, and then as a multiplicative function on $\mathbf{I}_K$ by setting it to 0 on the ideals not coprime to $\mathfrak{m}$. We will also denote this map $\mathbf{I}_K \to \mathbb{C}$ by χ. As before, we denote the identity element by χ_0 and call it the principal character. We call these the *generalized Dirichlet characters* or *ideal class characters*, and we may define the corresponding *Dirichlet-Hecke L-series*:

$$\mathrm{L}(\mathfrak{m}, s, \chi) = \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{\mathrm{Norm}(\mathfrak{a})^{-s}},$$

where the sum is over all integral ideals of $\mathcal{O}_K$ (or equivalently, over those ideals coprime to $\mathfrak{m}$).

Note that we do not indicate an order for the summation. For now, whenever we give a sum over primes we assume it is taken as a Dirichlet series, that is that the sum if to be taken over ideals in order of increasing norm (as we write out in 3.2.1). Later we will prove absolute convergence results and this will become largely irrelevant.

Example. Set $K = \mathbb{Q}$, $\mathfrak{m} = m\infty$. Note that $\mathcal{O}_K = \mathbb{Z}$ is a PID. Then, each ideal $(a) \subseteq \mathbf{I}^{\mathfrak{m}}$ has two generators, $\pm a$. Mapping the positive generator (note $\infty|\mathfrak{m}$) to its image in $(\mathbb{Z}/m\mathbb{Z})^\times$ we get a surjective homomorphism, with kernel equal to the set of things congruent to 1 (mod m), which is precisely the set of things congruent to 1 (mod p^ℓ) for $p^\ell \parallel \mathfrak{m}$.

So, $\mathrm{Cl}_K^{\mathfrak{m}} \cong (\mathbb{Z}/m\mathbb{Z})^\times$. So, we get the classical Dirichlet characters and their Dirichlet L-series as special cases.

Example. Let $\mathfrak{m} = 1$ and $\chi = \chi_0$ be the principal character. Then,

$$\mathrm{L}(\mathfrak{m}, s, \chi_0) = \sum_{\mathfrak{a}} \mathrm{Norm}(\mathfrak{a})^{-s} \stackrel{\mathrm{def}}{=} \zeta_K(s)$$

This is the so-called *Dedekind zeta function.*

For a modulus $\mathfrak{m}$ let us define *ideal class zeta functions*:

$$\zeta(s, \mathfrak{c}) = \sum_{\mathfrak{a} \in \mathfrak{c}} \mathrm{Norm}(\mathfrak{a})^{-s},$$

where $\mathfrak{c} \in \mathrm{Cl}_K^{\mathfrak{m}}$ is an ideal class (viewed as a coset of $\mathbf{P}_K^{\mathfrak{m}}$ in $\mathbf{I}_K^{\mathfrak{m}}$).

Note that for an ideal class character χ of modulus $\mathfrak{m}$

$$\mathrm{L}(\mathfrak{m}, s, \chi) = \sum_{\mathfrak{c} \in \mathrm{Cl}^{\mathfrak{m}}} \chi(\mathfrak{c}) \zeta(s, \mathfrak{c})$$

as formal series (and on their common domain of convergence — which will be the intersections of the domains of convergence of the ideal class zeta functions).

Remark. The characters and L-series introduced in this section are generally called generalized Dirichlet characters and L-series. There is a wider class of characters and L-series, the Hecke Großencharakters and their L-series, which maintain all of the interesting properties of the class described here. They may be thought of as characters of the idèle class group, or alternatively as generalized Dirichlet characters with an "infinite part." There is a discussion of the relationship between these two classes of characters in [Neu99] and [Hei67].

3.2. **Convergence properties.** Now, we look at the convergence properties of these L-series.

Proposition 3.2.1. *Let χ be an ideal class character for the modulus $\mathfrak{m}$ of the field K. Then:*

(a) $\mathrm{L}(\mathfrak{m}, s, \chi)$ *converges absolutely on* $\mathrm{Re}(s) > 1$*, and uniformly on* $\mathrm{Re}(s) > 1 + \delta$ *for any* $\delta > 0$*;*

(b) *For* $\mathrm{Re}(s) > 1$ *we have the convergent Euler product identity:*

$$\mathrm{L}(\mathfrak{m}, s, \chi) = \prod_{\mathfrak{p} \nmid \mathfrak{m}} \left(1 - \mathrm{Norm}(\mathfrak{p})^{-s} \chi(\mathfrak{p})\right)^{-1}$$

Noting that we set $\chi(\mathfrak{p}) = 0$ if $\mathfrak{p}$ is not coprime to $\mathfrak{m}$, we may take the product over only those ideals that are.

Proof. We write $\mathrm{L}(\mathfrak{m}, s, \chi)$ as a Dirichlet series:

$$\mathrm{L}(\mathfrak{m}, s, \chi) = \sum_{n=1}^{\infty} a_n n^{-s} \qquad \text{where} \qquad a_n = \sum_{\mathrm{Norm}(\mathfrak{a}) = n} \chi(\mathfrak{a})$$

Now, we claim that each ideal class of Cl_K can contain at most one ideal of a given norm. Indeed, say I, J are in the same ideal class. Then, $I = \alpha J$ for some $\alpha \in K^\times$. Then, $\mathrm{Norm}(I) = |\mathrm{Norm}(\alpha)| \mathrm{Norm}(J)$, so $\mathrm{Norm}(I) = \mathrm{Norm}(J)$ implies that $|\mathrm{Norm}(\alpha)| = 1$. Then, α is a unit in $\mathcal{O}_K$, so $I = J$. This proves our claim.

Then, $|a_n| \leq |\{\mathfrak{a} : \mathrm{Norm}(\mathfrak{a}) = n\}| \leq |\mathrm{Cl}_K|$.

So, for $\delta > 0$ and $\mathrm{Re}(s) > 1 + \delta$ we have:

$$\left|a_n n^{-s}\right| = |a_n| n^{-\mathrm{Re}(s)} \leq \mathrm{Cl}_K \, n^{-(1+\delta)}$$

Then, $\mathrm{L}(\mathfrak{m}, s, \chi)$ converges uniformly and absolutely on $\mathrm{Re}(s) > 1 + \delta$ by comparison to $\mathrm{Cl}_K \sum_n n^{-(1+\delta)}$ (which converges by the integral test). This proves (i).

Now, note that for $s > 1$ we have the absolutely convergent expansion:

$$\left(1 - p^{-s}\right)^{-1} = \sum_{m=0}^{\infty} p^{-sm}$$

Then, say $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ are the prime ideals satisfying $\mathrm{Norm}(\mathfrak{p}) \leq N$. By unique factorization of ideals and multiplicativity of χ we have

$$\prod_{\mathrm{Norm}(\mathfrak{p})\leq N} \left(1 - \mathrm{Norm}(\mathfrak{p})^{-s}\chi(\mathfrak{p})\right)^{-1} = \sum_{\mathfrak{a}=\mathfrak{p}_1^{k_1}\cdots\mathfrak{p}_r^{k_r}} \chi(\mathfrak{a})\,\mathrm{Norm}(\mathfrak{a})^{-s}$$
$$= \sum_{\mathrm{Norm}(\mathfrak{a})\leq N} \chi(\mathfrak{a})\,\mathrm{Norm}(\mathfrak{a})^{-s} + \sum_{\substack{\mathrm{Norm}(\mathfrak{a})>N \\ \mathfrak{a}=\mathfrak{p}_1^{k_1}\cdots\mathfrak{p}_r^{k_r}}} \chi(\mathfrak{a})\,\mathrm{Norm}(\mathfrak{a})^{-s}.$$

So,

$$\left|\prod_{\mathrm{Norm}(\mathfrak{p})\leq N} \left(1 - \mathrm{Norm}(\mathfrak{p})^{-s}\chi(\mathfrak{p})\right)^{-1} - \mathrm{L}(\mathfrak{m}, s, \chi)\right| \leq \sum_{\mathrm{Norm}(\mathfrak{a})>N} \left|\chi(a)\,\mathrm{Norm}(\mathfrak{a})^{-s}\right|$$

The absolute convergence of $\mathrm{L}(\mathfrak{m}, s, \chi)$ on the region in (i) thus imply thus the equality in (ii).

Finally, we'll check that the Euler product converges as a product (that is, its logarithm converges as a sum): Note that

$$-\sum_p p \log\left(1 - \mathrm{Norm}(\mathfrak{p})^{-s}\chi(\mathfrak{p})\right) = \sum_{\mathfrak{p}} \sum_{m\geq 1} \frac{1}{m}\,\mathrm{Norm}(\mathfrak{p})^{-ms}\chi(\mathfrak{p}^m).$$

This converges absolutely on $\mathrm{Re}(s) > 1$ by comparison to $\mathrm{L}(\mathfrak{m}, s, \chi)$. Exponentiating, we get that Euler product converges as an infinite product (that is, has an *non-zero* limit) on $\mathrm{Re}(s) > 1$. □

Now, we look at some (simple) analytic continuation properties.

Proposition 3.2.2. *Let $\zeta = \zeta_{\mathbb{Q}}$ be the Riemann zeta function. Then, ζ may be analytically continued to $\mathrm{Re}(s) > 0$, except for a simple pole at $s = 1$ with residue 1.*

Proof. Let

$$\psi_r(n) = \begin{cases} 1 - r & r|n \\ 1 & \text{otherwise} \end{cases}$$

Then, define

$$\zeta_r(s) \stackrel{\text{def}}{=} \sum_n \psi_r(n) n^{-s}.$$

Now, ζ_r is a Dirichlet series, with partial sums bounded by $r - 1$, so by Lemma 1.3.1 it has abscissa of convergence at most 0 and so it is analytic on $\mathrm{Re}(s) > 0$.

Now, note that we have the equality of formal series:

$$\zeta(s) = \zeta_r(s) + \frac{r}{r^s}\zeta s$$

So, we may continue ζ to $\mathrm{Re}(s) > 0$ by setting:

$$\zeta(s) = \frac{\zeta_r(s)}{1 - r^{1-s}}$$

The numerator is analytic on $\mathrm{Re}(s) > 0$ for each r, and the denominator vanishes only when $1 = r^{1-s}$. By the uniqueness of meromorphic continuation, the continuations for different r must agree. So, for s to be a pole, we must have $1 = r^{1-s}$ for each $r = 2, 3, \dots$.

This implies $s = 1$. This gives our desired continuation. Note that $\zeta_2(1) = \ln 2$, so the order of the pole at $s = 1$ is the order of vanishing of the denominator. Expanding out the Taylor series, we see that it is of order 1.

So, $(s-1)\zeta(s)$ is analytic at $s = 1$, and to compute $\operatorname{res}_{s=1} \zeta(s) = \lim_{s\to 1}(s-1)\zeta(s)$ we can compute the limit for $s \to 1^+$ real.

But, for $s > 1$ a positive real:

$$\frac{1}{s-1} = \int_1^\infty \frac{dt}{t^s} \le \zeta(s) \le 1 + \int_1^\infty \frac{dt}{t^s} = 1 + \frac{1}{s-1}$$

So, the residue is indeed 1. □

Remark. We do not need, thus do not prove, the following functional equation for ζ:

$$\zeta(1-s) = 2(2\pi)^{-s}\cos(\frac{1}{2}s\pi)\Gamma(s)\zeta(s)$$

Along with the above, this lets us analytically continue ζ to the whole complex plane except for the pole at $s = 1$.

In the preceding we used only the finiteness of the class group. We can get better convergence results by using the above and looking at the ideal class zeta functions by estimating the distribution of norms in the ideal classes.

We state without proof a result of this nature:

Proposition 3.2.3. *Let $\mathfrak{c} \in \mathrm{Cl}_K^{\mathfrak{m}}$ be an ideal class. Let*

$$S(\mathfrak{c}, n) = |\{\mathfrak{a} \in \mathfrak{c} :| : \mathrm{Norm}(\mathfrak{a}) \le n\}.$$

Then, $S(\mathfrak{c}, n) = \kappa_{\mathfrak{m}} n + O(n^{1-\frac{1}{N}})$ where $N = [K : \mathbb{Q}]$ and

$$\kappa_{\mathfrak{m}} = \frac{2^{r+s}\,\mathrm{reg}(\mathfrak{m})\pi^s}{\omega_{\mathfrak{m}}\,\mathrm{Norm}(\mathfrak{m})\,|\Delta_K|^{\frac{1}{2}}}$$

where r, s are the number of real and complex primes of K, $\omega_{\mathfrak{m}}$ the number of roots of unity in $\mathcal{O}_K^\times \cap K_1^{\mathfrak{m}}$, $\mathrm{reg}(\mathfrak{m})$ the regulator of $\mathfrak{m}$, Δ_K the discriminant of $\mathcal{O}_K$.

Proof. See [Jan96, Ch. IV, §2] or [Lan94, Ch. VI, §3]. □

This allows us to get:

Proposition 3.2.4. *Let $K, \mathfrak{m}, \chi$ be as in Prop. 3.2.1, $\mathfrak{c}, \kappa_{\mathfrak{m}}$ be as in Prop. 3.2.3, and let $N = [K : \mathbb{Q}]$. Then:*

(a) *$\zeta(s, \mathfrak{c})$ may be analytically continued to the region $\mathrm{Re}(s) > 1 - \frac{1}{N}$ except for the simple pole at $s = 1$ with residue $\kappa_{\mathfrak{m}}$.*
(b) *If $\chi = \chi_0$, then $\mathrm{L}(\mathfrak{m}, s, \chi)$ may be analytically continued to the region $\mathrm{Re}(s) > 1 - \frac{1}{N}$ except for the simple pole at $s = 1$ with residue $|\mathrm{Cl}_K^{\mathfrak{m}}|\,\kappa_{\mathfrak{m}}$.*
(c) *$\zeta_K(s)$ may be analytically continued to the region $\mathrm{Re}(s) > 1 - \frac{1}{N}$ except for the simple pole at $s = 1$ with residue $|\mathrm{Cl}_K|\,\kappa_1$*
(d) *If $\chi \ne \chi_0$, then $\mathrm{L}(\mathfrak{m}, s, \chi)$ converges on $\mathrm{Re}(s) > 1 - \frac{1}{N}$, and is analytic in that half plane.*

Proof. Let $f(s) = \zeta(s, \mathfrak{c}) - \kappa_{\mathfrak{m}}\zeta_{\mathbb{Q}}(s)$ be an equality of Dirichlet series. Then, f is given by a Dirichlet series with coefficients a_i such that

$$\left|\sum_{i=1}^{k} a_i\right| = |S(\mathfrak{c}, k) - \kappa_{\mathfrak{m}} k|,$$

which by Prop. 3.2.3 is $O(k^{1-\frac{1}{N}})$.

By Lemma 1.3.1, f is analytic on $\mathrm{Re}(s) > 1 - \frac{1}{N}$. By Prop. 3.2.2, $\zeta_{\mathbb{Q}}$ may be analytically continued to $\mathrm{Re}(s) > 0$ except for a simple pole at $s = 1$ with residue 1. So, setting $\zeta(s, \mathfrak{c}) = f(s) + \kappa_{\mathfrak{m}}\zeta_{\mathbb{Q}}(s)$ gives a continuation of $\zeta(s, \mathfrak{c})$ to $\mathrm{Re}(s) > 1 - \frac{1}{N}$. Furthermore,

$$\mathrm{res}_{s=1}\, \zeta(s, \mathfrak{c}) = \mathrm{res}_{s=1}\, f(s) + \kappa_{\mathfrak{m}} \mathrm{res}_{s=1}\, \zeta_{\mathbb{Q}}(s) = \kappa_{\mathfrak{m}}$$

This proves (a).

Now, note that

$$\mathrm{L}(\mathfrak{m}, s, \chi_0) = \sum_{\mathfrak{c} \in \mathrm{Cl}^{\mathfrak{m}}} \zeta(s, \mathfrak{c}).$$

With (a), this gives the desired continuation. Also, the residue is just the sum of the residues, which is $|\mathrm{Cl}_K^{\mathfrak{m}}|\, \kappa_{\mathfrak{m}}$.

Setting $\mathfrak{m} = 1$ we get $\mathrm{L}(\mathfrak{m}, s, \chi_0) = \zeta_K(s)$, giving us (c).

Now, recall that we have

$$\mathrm{L}(\mathfrak{m}, s, \chi) = \sum_{\mathfrak{c} \in \mathrm{Cl}_K^{\mathfrak{m}}} \chi(\mathfrak{c})\zeta(s, \mathfrak{c})$$

This is a Dirichlet series with coefficients a_i such that

$$\begin{aligned}
\sum_{i=1}^{k} a_i &= \sum_{\mathfrak{c} \in \mathrm{Cl}^{\mathfrak{m}}} \chi(\mathfrak{c}) S(\mathfrak{c}, k) \\
&= \sum_{\mathfrak{c} \in \mathrm{Cl}^{\mathfrak{m}}} \chi(\mathfrak{c}) \left(\kappa_{\mathfrak{m}} k + O(k^{1-\frac{1}{1-N}})\right) \\
&= O(k^{1-\frac{1}{1-N}} + k\kappa_{\mathfrak{m}} \sum_{\mathfrak{c} \in \mathrm{Cl}^{\mathfrak{m}}} \chi(\mathfrak{c})
\end{aligned}$$

for $\chi \neq \chi_0$, we may use Prop. 1.2.1 to write this as:

$$= O(k^{1-\frac{1}{1-N}})$$

So, Lemma 1.3.1 implies (d). □

4. L-series and Galois groups

4.1. **Conductors of characters.** For a modulus $\mathfrak{m}$ and a character $\chi \in \mathrm{Hom}(\mathrm{Cl}_K^{\mathfrak{m}}, S^1)$, let the *conductor* $\mathfrak{f}_\chi$ of χ be the conductor of $\ker \chi$ viewed as a subgroup of $\mathbf{I}_K^{\mathfrak{m}}$ containing $\mathbf{P}_K^{\mathfrak{m}}$, or equivalently the conductor of $\mathbf{I}_K^{\mathfrak{m}}/\ker \chi$.

Proposition 4.1.1. *Let $\mathfrak{m}, \chi, \mathfrak{f}_\chi$ be as above. Then, $\mathfrak{f}_\chi$ is equal to the least modulus $\mathfrak{n}$ such that χ factors through $\mathrm{Cl}_K^{\mathfrak{n}}$. Also, there is a unique $\widetilde{\chi} \in \mathrm{Hom}(\mathrm{Cl}_K^{\mathfrak{f}_\chi}, S^1)$ such that χ factors through $\widetilde{\chi}$.*

Proof. Let $H^{\mathfrak{m}} = \ker \chi \subseteq \mathbf{I}_K^{\mathfrak{m}}$; note that it is a congruence subgroup. As $\mathbf{P}_K^{\mathfrak{f}_\chi} \subseteq H^{\mathfrak{f}_\chi}$ and by Prop. 2.2.1 we have the maps

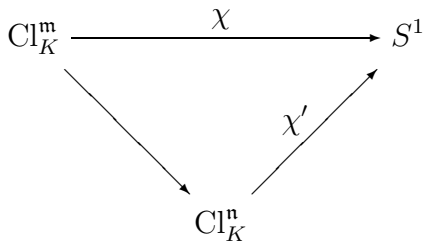
$$\mathbf{I}_K^{\mathfrak{f}_\chi}/\mathbf{P}_K^{\mathfrak{f}_\chi} \longrightarrow \mathbf{I}_K^{\mathfrak{f}_\chi}/H^{\mathfrak{f}_\chi} \longrightarrow \mathbf{I}_K^{\mathfrak{m}}/H^{\mathfrak{m}}$$

which induce

$$\mathrm{Hom}(\mathrm{Cl}_K^{\mathfrak{f}_\chi}, S^1) \longleftarrow \mathrm{Hom}(\mathbf{I}_K^{\mathfrak{f}_\chi}/H^{\mathfrak{f}_\chi}, S^1) \longleftarrow \mathrm{Hom}(\mathbf{I}_K^{\mathfrak{m}}/H^{\mathfrak{m}}, S^1).$$

Now, χ factors through $\mathbf{I}_K^{\mathfrak{m}}/H^{\mathfrak{m}}$, and so under this map it factors through $\mathrm{Cl}_K^{\mathfrak{f}_\chi}$. Furthermore, $\widetilde{\chi}$ is defined by this, giving uniqueness.

Say χ factors through $\mathrm{Cl}_K^{\mathfrak{n}}$ for some $\mathfrak{n} \mid \mathfrak{m}$:



Then, $\ker \chi = \mathbf{I}_K^{\mathfrak{n}} \cap \ker \chi'$. Set $H^{\mathfrak{n}} = \ker \chi'$, we see that $H^{\mathfrak{n}}$ realizes $\ker \chi$ mod. $\mathfrak{n}$, and so $\mathfrak{f}_\chi \mid \mathfrak{n}$ by the minimality of the conductor and Prop. 2.2.2. So, $\mathfrak{f}_\chi$ is minimal with this property. □

We say that a character $\chi \in \mathrm{Hom}(\mathrm{Cl}^{\mathfrak{m}}, S^1)$ is *primitive* if $\mathfrak{m} = \mathfrak{f}_\chi$. To every character χ there corresponds a unique primitive character, the $\widetilde{\chi}$ of Prop. 4.1.1; we will continue to use $\widetilde{\chi}$ to refer to the primitive character corresponding to χ.

Example. For any modulus $\mathfrak{m}$ and $\chi_0 \in \mathrm{Hom}(\mathrm{Cl}_K^{\mathfrak{m}}, S^1)$ the principal character, we have $\mathfrak{f}_{\chi_0} = 1$ and $\widetilde{\chi_0}$ is the principal character in $\mathrm{Hom}(\mathrm{Cl}_K, S^1)$.

Let us compare the Dirichlet-Hecke series of χ and $\widetilde{\chi}$.

Proposition 4.1.2. *Say $\chi \in \mathrm{Hom}(\mathrm{Cl}^{\mathfrak{m}}, S^1)$ with conductor $\mathfrak{f}$. Let F be the fixed field in L of $\left(\frac{L/K}{\ker \chi}\right)$ (that is, the image of $\ker \chi$ under the Artin map). Then, for $\mathrm{Re}(s) > 1$:*

$$\begin{aligned} \mathrm{L}(\mathfrak{f}, s, \widetilde{\chi}) &= \mathrm{L}(\mathfrak{m}, s, \chi) \prod_{\substack{\mathfrak{p} \mid \mathfrak{m} \\ \mathfrak{p} \nmid \mathfrak{f}}} \left(1 - \widetilde{\chi}(\mathfrak{p}) \operatorname{Norm}(\mathfrak{p})^{-s}\right)^{-1} \\ &= \prod_{\substack{\mathfrak{p} \text{ unr.} \\ \text{in } F/K}} \left(1 - \widetilde{\chi}(\mathfrak{p}) \operatorname{Norm}(\mathfrak{p})^{-s}\right)^{-1} \end{aligned}$$

Proof. The first equality follows at once from writing out the Euler products on both sides.

Let L/K be the class field of $\mathrm{Cl}^{\mathfrak{m}}$. By Prop. 4.1.1 the conductor of χ is equal to the conductor of $\mathbf{I}^{\mathfrak{m}}/\ker \chi$, so by Prop. 2.4.1 the primes dividing $\mathfrak{f}_\chi$ are precisely the ramified primes of the class field of $\mathbf{I}^{\mathfrak{m}}/\ker \chi$. Artin Reciprocity together with the Galois correspondence imply that F is the class field of $\mathbf{I}^{\mathfrak{m}}/\ker \chi$. So, the primes dividing $\mathfrak{f}_\chi$ are precisely the ramified primes of F. The second equality follows. □

Using Artin Reciprocity, we may treat a generalized Dirichlet character as a character on a certain abelian Galois group and vice versa. The class of Artin characters and L-functions further generalizes this notion.

4.2. **Artin L-functions.** Let L/K be a Galois extension of number fields, with Galois group $G = \mathrm{Gal}(L/K)$. Then, we may consider an irreducible finite dimension complex representation of G, $\rho : G \to \mathrm{Aut}(V)$.

Let $\mathfrak{p}$ be a finite prime of L/K. Then, for a prime $\mathfrak{P}$ lying over $\mathfrak{p}$, $\left[\frac{L/K}{\mathfrak{P}}\right]$ gives a coset in G of the inertia group $I_{\mathfrak{P}}$. Then, $\rho\left[\frac{L/K}{\mathfrak{P}}\right]$ is a linear map on $V^{I_{\mathfrak{P}}}$. Note that the characteristic polynomial of this map is unchanged by conjugation, and so is unchanged by replacing $\mathfrak{P}$ with any other prime $\tau\mathfrak{P}\tau^{-1}$ lying over $\mathfrak{p}$. Then, the quantity

$$\det\left(\mathrm{id} - \rho\left[\frac{L/K}{\mathfrak{P}}\right]\Big|_{V^{I_{\mathfrak{P}}}}\right)$$

is also independent of the choice of prime $\mathfrak{P}$ lying over $\mathfrak{p}$.

So, we may define the Artin L-function for ρ by the Euler product:

$$\mathrm{L}(L/K, s, \rho) = \prod_{\mathfrak{p}} \det\left(\mathrm{id} - \rho\left[\frac{L/K}{\mathfrak{P}}\right]\Big|_{V^{I_{\mathfrak{P}}}}\right)^{-1}$$

As $\rho\left[\frac{L/K}{\mathfrak{P}}\right]$ has finite order we may conclude that it is diagonalizable, with root of unity eigenvalues. Taking logarithms, and writing this in terms of the eigenvalues, we may explicitly establish convergence properties. We will not do this, because the only class which we are interested in will be shown in Corollary 4.2.1 to be equivalent to certain Dirichlet-Hecke L-functions, whose convergence properties we have already considered.

Note that sometimes the Artin L-functions are defined without the factors for the ramified primes (e.g. in [Hei67]). However, it seems better to include these factors. Various functorial properties of these L-functions with respect to change of representation are true in this form, for example how the L-function behaves under induction of characters. Also, this form allows the Artin L-functions to actually generalize the Dirichlet L-functions, as we shall see:

Proposition 4.2.1. *Let L/K be an abelian extension of number fields, and ρ an irreducible, so one dimensional, representation of $G = \mathrm{Gal}(L/K)$. As ρ is one dimensional, view it as an element of $\mathrm{Hom}(G, S^1)$ under the identification $S^1 \subset \mathbb{C}^\times \leftrightarrow \mathrm{GL}_1(\mathbb{C})$. Let F be the fixed field in L of $\ker\rho$. Then:*

$$\mathrm{L}(L/K, s, \rho) = \prod_{\substack{\mathfrak{p} \text{ unr.} \\ \text{in } F/K}} \left(1 - \rho\left(\frac{L/K}{\mathfrak{p}}\right)\right)^{-1}$$

(That each term in the product is well defined is part of the conclusion.)

Proof. Galois theory gives us the short exact sequence

$$1 \longrightarrow \mathrm{Gal}(L/F) \hookrightarrow \mathrm{Gal}(L/K) \xrightarrow{\mathrm{res}} \mathrm{Gal}(F/K).$$

So, for $F = L^{\ker\rho}$ we have that ρ factors through $\mathrm{Gal}(F/K)$.

Note that $V = \mathbb{C}$ for our representation, so for a prime $\mathfrak{P}$ of L lying over $\mathfrak{p}$ we have

$$V^{\mathbf{I}_{\mathfrak{P}}} = \begin{cases} \mathbb{C} & \rho(\mathbf{I}_{\mathfrak{P}}) = \{\mathrm{id}\} \\ 0 & \text{otherwise} \end{cases}$$

Then, we may write

$$\det\left(\mathrm{id} - \rho\left[\frac{L/K}{\mathfrak{P}}\right]\Big|_{V^{I_\mathfrak{P}}}\right) = \begin{cases} 1-\rho\left(\frac{L/K}{\mathfrak{p}}\right) & \mathbf{I}_\mathfrak{P} \subseteq \ker\rho \\ 1 & \text{otherwise} \end{cases}$$

Note that the $\mathbf{I}_\mathfrak{P}$ are conjugate, and $\ker\rho$ is a normal subgroup. So, this quantity is indeed well defined with respect to different choices of primes lying over $\mathfrak{p}$. (In fact, we knew this a priori, for the LHS is well defined with respect to different choices of primes lying over $\mathfrak{p}$.)

Also, we have

$$\begin{aligned} I_\mathfrak{P} \subseteq \ker\rho &\Leftrightarrow F = L^{\ker\rho} \subseteq L^{I_\mathfrak{P}} \\ &\Leftrightarrow \mathfrak{p} \text{ unr. in } F/K. \end{aligned}$$

This proves our result. □

Corollary 4.2.1. *Let $L/K, \rho, F$ be as in Prop. 4.2.1. Under the Artin map, ρ induces a character $\chi \in \mathrm{Hom}(\mathrm{Cl}_K^\mathfrak{m}, S^1)$ for some $\mathfrak{m}$. Let $\mathfrak{f}_\chi$ be the conductor of χ, and $\widetilde{\chi}$ the corresponding primitive character. Then:*

$$\mathrm{L}(L/K, s, \rho) = \mathrm{L}(\mathfrak{f}_\chi, s, \widetilde{\chi})$$

Proof. By Theorem 2.4.1 the Artin map induces $\mathrm{Gal}(L/K) \cong \mathbf{I}_K^\mathfrak{m}/H^\mathfrak{m}$ for some $\mathfrak{m}$ and congruence subgroup $H^\mathfrak{m}$. So, under the Artin map ρ induces a character $\chi \in \mathrm{Hom}(\mathrm{Cl}_K^\mathfrak{m}, S^1)$. Then, by Prop. 4.1.2, noting that the F there matches the F here, we have that

$$\mathrm{L}(\mathfrak{f}_\chi, s, \widetilde{\chi}) = \prod_{\substack{\mathfrak{p} \text{ unr.} \\ \text{in } F/K}} \left(1 - \widetilde{\chi}(\mathfrak{p})\right)^{-1}.$$

By Prop. 4.2.1 we have that

$$\mathrm{L}(L/K, s, \chi) = \prod_{\substack{\mathfrak{p} \text{ unr.} \\ \text{in } F/K}} \left(1 - \rho\left(\frac{L/K}{\mathfrak{p}}\right)\right)^{-1}.$$

Note that $\ker\rho \supseteq \mathrm{Gal}(L/F)$ by construction so we may define $\rho' \in \mathrm{Hom}(\mathrm{Gal}(F/K), S^1)$ such that ρ' restricts to ρ on $\mathrm{Gal}(L/K)$. Now, note that under the Artin map ρ' induces $\chi' \in \mathrm{Hom}(\mathrm{Cl}_K^{\mathfrak{f}_\chi}, S^1)$ (for $\mathfrak{f}_\chi$ is the conductor of L/F by comments in the proof of Prop. 4.1.2). Note that χ' is defined by

$$\chi'(\mathfrak{p}) = \rho'\left(\frac{F/K}{\mathfrak{p}}\right) = \rho\left(\frac{L/K}{\mathfrak{p}}\right).$$

Then, by the uniqueness claim from Prop. 4.1.1 we must have $\widetilde{\chi} = \chi'$. This proves our result. □

4.3. **Extension of zeta functions, non-vanishing of L-functions.** We are now ready to move forward towards the crucial part of our proof, showing how zeta functions extend under extension of field and using this to show the non-vanishing of the L-series corresponding to non-principal characters at $s = 1$.

Proposition 4.3.1. *Let L/K be an abelian extension of number fields. Then on their common domain of definition*

$$\begin{aligned}\zeta_L(s) &= \prod_{\rho} \mathrm{L}(L/K, s, \rho) \\ &= \prod_{\chi} \mathrm{L}(\mathfrak{f}_\chi, s, \widetilde{\chi}) \\ &= \zeta_K(s) \prod_{\chi \neq \chi_0} \mathrm{L}(\mathfrak{f}_\chi, s, \widetilde{\chi})\end{aligned}$$

where the first product is over all irreducible representations (equivalently characters) of $G = \mathrm{Gal}(L/K)$, the second is over the corresponding (in the sense of Corollary 4.2.1) Dirichlet characters χ, and the final is over all such characters which are not the the principal character (equivalently, which do not come from the trivial representation).

Proof. Let $\mathfrak{p}, \mathfrak{P}$ denote primes of K, L respectively. Let $e(\mathfrak{p}), f(\mathfrak{p}), g(\mathfrak{p})$ be such that $\mathfrak{p} = \left(\mathfrak{P}_1 \cdots \mathfrak{P}_{g(\mathfrak{p})}\right)^{e(\mathfrak{p})}$ (so then, $f(\mathfrak{p})$ is the inertial degree of any $\mathfrak{P}_i$ over $\mathfrak{p}$), and note that their product is $N = [L : K]$. Then:

$$\begin{aligned}\zeta_L(s) &= \prod_{\mathfrak{P}} \left(1 - \mathrm{Norm}(\mathfrak{P})^{-s}\right)^{-1} \\ &= \prod_{\mathfrak{p}} \left(1 - \mathrm{Norm}(\mathfrak{p})^{-sf(\mathfrak{p})}\right)^{-g(\mathfrak{p})}\end{aligned}$$

Now, by Prop. 4.2.1 we have

$$\begin{aligned}\prod_{\rho} \mathrm{L}(L/K, s, \rho) &= \prod_{\rho} \prod_{\substack{\mathfrak{p} \text{ unr.} \\ \text{in } L^{\ker \rho}/K}} \left(1 - \rho\left(\frac{L/K}{\mathfrak{p}}\right) \mathrm{Norm}(\mathfrak{p})^{-s}\right)^{-1} \\ &= \prod_{\mathfrak{p}} \prod_{\rho(I_{\mathfrak{P}})=0} \left(1 - \rho\left(\frac{L/K}{\mathfrak{p}}\right) \mathrm{Norm}(\mathfrak{p})^{-s}\right)^{-1}\end{aligned}$$

Now, we note that the irreducible representations of G are one dimensional, and are thus just the characters on G. Furthermore, the characters satisfying $\chi(I_{\mathfrak{P}}) = 0$ correspond exactly to characters of $G/I_{\mathfrak{P}}$. The image of $\left(\frac{L/K}{\mathfrak{p}}\right)$ in this quotient will have order equal to the order of the Frobenius in the residue field extension, that is $f(\mathfrak{p})$. Noting that $|G/I_{\mathfrak{P}}| = f(\mathfrak{p})g(\mathfrak{p})$, and applying Prop. 1.2.1 we get that our previous product is equal to

$$= \prod_{\mathfrak{p}} \left(1 - \mathrm{Norm}(\mathfrak{p})^{-sf(\mathfrak{p})}\right)^{-g(\mathfrak{p})}.$$

This proves the first equality in the statement. The second equality follows by Corollary 4.2.1. The final equality follows by noting that for χ equal to the principal character, we have $\mathfrak{f}_\chi = 1$, and $\mathrm{L}(\mathfrak{f}_\chi, s, \widetilde{\chi}) = \zeta_K(s)$. □

Proposition 4.3.2. *Let $K, \mathfrak{m}$ be as above. Then $\mathrm{L}(\mathfrak{m}, 1, \chi) \neq 0$ for $\chi \neq \chi_0$.*

Proof. Let L/K be the ray class field mod. $\mathfrak{m}$. Then, by Prop. 4.3.1

$$\zeta_L(s) = \zeta_K(s) \prod_{\chi \neq \chi_0} \mathrm{L}(\mathfrak{f}_\chi, s, \widetilde{\chi}).$$

By Prop. 3.2.4, all quantities may be continued to a neighborhood of $s = 1$, so this equality must hold there.

Also, by Prop. 3.2.4, ζ_L and ζ_K have simple poles at $s = 1$, so the product must have neither a pole nor a zero at $s = 1$. But, by Prop. 3.2.4 the $\mathrm{L}(\mathfrak{f}_\chi, s, \widetilde{\chi})$ are analytic there. So, no terms of the product have a pole there and so none can vanish there. □

Remark. Note that we could have developed all of the results we need without introducing Artin L-functions, sticking to Dirichlet-Hecke L-functions arising from primitive characters. Class field theory would still be crucial to the argument, arising in Prop. 4.1.2.

The advantage lies in exposing ties to more general theory. From Corollary 4.2.1 we get that all abelian Artin L-functions are Dirichlet-Hecke L-functions, and so share their analytical properties. Hecke and Tate showed that these extend analytically to all of $\mathbb{C}$, except for a pole at $s = 1$ for the principal character (which corresponds to the trivial representation). Then, we may develop a general theory for the functorial properties of Artin L-functions under change of representation, such as direct sum and inducing a representation from a subgroup (which would yield Prop. 4.3.1 by letting the subgroup be $\{\mathrm{id}\} \subseteq \mathrm{Gal}(L/K)$). Then, a result of Brauer shows that the character of any Galois representation is a $\mathbb{Z}$-linear combination of the characters of abelian characters, giving an arbitrary L-function as a quotient of products of abelian L-series, which implies that it can be meromorphically extended to $\mathbb{C}$. Of course, Artin's Conjecture, that they may in fact be analytically extended (except for $s = 1$ if it contains the trivial representation), remains quite open.

5. Dirichlet density and the Chebotarev Density Theorem

5.1. **Density.**

Definition. Let $S \subseteq \mathrm{mSpec}(\mathcal{O}_K)$ be a set of finite primes of K. Then, the *Dirichlet density* of S is given by

$$\delta(S) \stackrel{\mathrm{def}}{=} \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in S} \mathrm{Norm}(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}} \mathrm{Norm}(\mathfrak{p})^{-s}},$$

where the sum in the denominator is taken over all of $\mathrm{mSpec}(\mathcal{O}_K)$.

We note that the denominator is just $\zeta_K(s)$, which converges for $\mathrm{Re}(s) > 1$ by Prop. 3.2.1, and the numerator converges by comparison to it. So, our limit has a chance of being meaningful. Note that we take the limit as $s \to 1^+$ to avoid having to worry about continuation to to the left of $\mathrm{Re}(s) = 1$ (although by Prop. 3.2.4 we can do this for the denominator).

We can in fact say more:

Proposition 5.1.1. *For S any set of finite primes of K, if $\delta(S)$ exists then:*

(a) $0 \leq \delta(S) \leq 1$;

(b)

$$\delta(S) = \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in S} \mathrm{Norm}(\mathfrak{p})^{-s}}{-\log(s-1)};$$

Proof. Note that the fraction in our limit is always non-negative and is bounded above by 1. This yields (a).

Using the Euler product for ζ_K, we have that for $\mathrm{Re}(s) > 1$:

$$\log \zeta_K(s) = \sum_{\mathfrak{p}} -\log(1 - \mathrm{Norm}(\mathfrak{p})^{-s})$$

Expanding this latter in a power series, and re-grouping terms:

$$= \sum_{\mathfrak{p}} \mathrm{Norm}(\mathfrak{p})^{-s} + \sum_{\mathfrak{p}} \sum_{m \geq 2} \frac{1}{m} \mathrm{Norm}(\mathfrak{p})^{-sm}.$$

Now, we may bound $\frac{1}{m}$ by $\frac{1}{2}$, sum the result geometric series, and bounding the Norm from below by 2 to get

$$\sum_{\mathfrak{p}} \sum_{m \geq 2} \left| \frac{1}{m} \mathrm{Norm}(\mathfrak{p})^{-sm} \right| \leq \sum_{\mathfrak{p}} \frac{1}{2} 2 \, \mathrm{Norm}(\mathfrak{p})^{-2\,\mathrm{Re}(s)} \leq \zeta_K(2\,\mathrm{Re}(s)).$$

Then, as $\zeta_K(s)$ converges for $\mathrm{Re}(s) \geq 1$, we have that our left hand term does so for $\mathrm{Re}(s) > 1/2$. Viewing it as a Dirichlet series, we see that it gives an analytic function there, and in particular in a neighborhood around $s = 1$. So,

$$\sum_{\mathfrak{p}} \mathrm{Norm}(\mathfrak{p})^{-s} \sim \log \zeta_K(s) \sim \log \frac{1}{s-1}.$$

The last relation follows for $\zeta_K(s)$ has a simple pole at $s - 1$, so $(s-1)\zeta_K(s)$ is analytic and non-zero around $s = 1$. Then, $\log(s-1)\zeta_K(s) = \log(s-1) + \log \zeta_K(s)$ is analytic at $s = 1$, and thus bounded near there.

Noting that

$$\lim_{s \to 1^+} \log \frac{1}{s-1} = +\infty \qquad \text{so} \qquad \lim_{s \to 1^+} \frac{\log \frac{1}{s-1}}{\sum_{\mathfrak{p}} \mathrm{Norm}(\mathfrak{p})^{-s}} = 1$$

we get (b):

$$\delta(S) = \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in S} \mathrm{Norm}(\mathfrak{p})^{-s}}{-\log(s-1)}.$$ □

Now, as the denominator gets arbitrary large as $s \to 1^+$, changing S in ways which changes the numerator by a bounded amount does not affect $\delta(S)$. More precisely:

Proposition 5.1.2. *Let S, S' be two sets of (finite) primes of K. Say*

$$\Delta(S, S', s) = \sum_{\mathfrak{p} \in S} \mathrm{Norm}(\mathfrak{p})^{-s} - \sum_{\mathfrak{p} \in S'} \mathrm{Norm}(\mathfrak{p})^{-s}$$

is bounded for $s \in (1, 1+\epsilon)$ for some $\epsilon > 0$. Then, $\delta(S) = \delta(S')$.

This is true, in particular in the following cases:

(a) *If S and S' differ by a finite number of elements;*
(b) *If S and $S = S' \cap A$, where A is the set of primes having (inertial) degree 1.*

Proof. The first statement follows by the comments before the statement of this proposition.

Now, if S and S' differ by a finite number of elements, then

$$\Delta(S, S', s) = \sum_{\mathfrak{p} \in S \setminus S'} \mathrm{Norm}(\mathfrak{p})^{-s} - \sum_{\mathfrak{p} \in S' \setminus S} \mathrm{Norm}(\mathfrak{p})^{-s}$$

has only finite many terms and so is analytic at $s = 1$ and bounded there, so we may apply the first part of our claim.

Also,

$$|\Delta(S, S', s)| \leq \sum_{\mathfrak{p} \notin A} \mathrm{Norm}(\mathfrak{p})^{-s}.$$

Now, for each rational prime p, there are at most $[K : \mathbb{Q}]$ primes lying over it and so at most that many of them not in A. Furthermore, each of those that are not in A have norm at least p^2, so:

$$\sum_{\mathfrak{p} \notin A} \mathrm{Norm}(\mathfrak{p})^{-s} \leq [K : \mathbb{Q}] \sum_{p} p^{-2s} \leq [K : \mathbb{Q}] \zeta(2s)$$

Now, $\zeta(2s)$ is analytic on $\mathrm{Re}(s) > 1/2$ and in particular at $s = 1$, and so bounded in a neighborhood around 1. So, we may apply the first part of our claim. □

5.2. **Comparison to natural density.** Now, we called the above concept a density. However, there is a more intuitive notion of density:

Definition. Let S be as above. For a set T of primes of K, define

$$\pi_K(T, n) \stackrel{\mathrm{def}}{=} \#\{\mathfrak{p} \in T : \mathrm{Norm}(\mathfrak{p}) \leq n\}.$$

If T is omitted, then we assume $T = \mathrm{mSpec}(\mathcal{O}_K)$. Then, the *natural density* of S is given by

$$\delta_{\mathrm{nat}}(S) \stackrel{\mathrm{def}}{=} \lim_{n \to \infty} \frac{\pi_K(S, n)}{\pi_K(n)}.$$

While we will not need to use any of this, it is worthwhile to consider the relationship between these two notions of density.

The following justifies calling the $\delta(S)$ a "density":

Proposition 5.2.1. *Let S be as above. If $\delta_{nat}(S)$ exists, then $\delta(S)$ exists and the two are equal.*

Proof. See [Gol71, §14-1]. □

Note that the other direction is *not* true. Let $K = \mathbb{Q}$ and

$$S = \{p \text{ prime} : p \text{ has leading decimal digit } 1\}.$$

Then, using the Prime Number Theorem, it is possible to show that $\delta(S) = \log_{10} 2$ while $\delta_{\mathrm{nat}}(S)$ fails to exist (as mentioned in [Ser73]).

Remark. Note that all the results which we prove below for Dirichlet density *are* also true for natural density. The proofs require sharper analytic information and generalize the prime number theorem. See [Gol71].

5.3. **Density of Frobenius in abelian extensions.** We proceed to prove a generalized version of the argument we gave for Theorem 1.1.1, with the crucial ingredient of the non-vanishing of $\mathrm{L}(1,\chi)$ for $\chi \neq \chi_0$ provided by Prop. 4.3.2.

Proposition 5.3.1. *Let K be a number field, $\mathfrak{m}$ a modulus, and $H^{\mathfrak{m}}$ a congruence subgroup group. If $\mathfrak{c}$ is a coset of $\mathbf{I}^{\mathfrak{m}}/H^{\mathfrak{m}}$, then the set $S(\mathfrak{c})$ of prime ideals in $\mathfrak{c}$ has density $\delta(S(\mathfrak{c})) = \frac{1}{[\mathbf{I}^{\mathfrak{m}}:H^{\mathfrak{m}}]}$.*

Proof. Let $G = \mathbf{I}^{\mathfrak{m}}/H^{\mathfrak{m}}$.

Note that by Prop. 1.2.1

$$\begin{aligned}\sum_{\mathfrak{p}\in\mathfrak{c}} \mathrm{Norm}(\mathfrak{p})^{-s} &= \frac{1}{|G|}\sum_{\mathfrak{p}}\sum_{\chi\in\mathrm{Hom}(G,S^1)} \chi(\mathfrak{p})\chi(\mathfrak{c}^{-1})\,\mathrm{Norm}(\mathfrak{p})^{-s} \\ &= \frac{1}{|G|}\sum_{\chi\in\mathrm{Hom}(G,S^1)} \chi(\mathfrak{c}^{-1})\sum_{\mathfrak{p}}\chi(\mathfrak{p})\,\mathrm{Norm}(\mathfrak{p})^{-s}.\end{aligned}$$

Then, taking logarithms in the Euler product formula of Prop. 3.2.1, and expanding the power series for $\log\frac{1}{1-t}$, we have, for $\mathrm{Re}(s) > 1$:

$$\log \mathrm{L}(\mathfrak{m}, s, \chi) = \sum_{\mathfrak{p}} \chi(\mathfrak{p})\,\mathrm{Norm}(\mathfrak{p})^{-s} + \sum_{\mathfrak{p}}\sum_{\mathfrak{m}\geq 2}\frac{1}{m}\chi(\mathfrak{p}^m)\,\mathrm{Norm}(\mathfrak{p})^{-sm}.$$

We have that

$$\sum_{\mathfrak{p}}\sum_{\mathfrak{m}\geq 2}\left|\frac{1}{m}\chi(\mathfrak{p}^m)\,\mathrm{Norm}(\mathfrak{p})^{-sm}\right| \leq \sum_{\mathfrak{p}}\sum_{\mathfrak{m}\geq 2}\frac{1}{m}\,\mathrm{Norm}(\mathfrak{p})^{-\,\mathrm{Re}(s)m} \leq [K:\mathbb{Q}]\zeta_{\mathbb{Q}}(2\,\mathrm{Re}(s))$$

and as $\zeta_{\mathbb{Q}}(2s)$ converges on $\mathrm{Re}(s) > 1/2 + \delta$, our LHS does as well and so defines an analytic function there. So:

$$\log \mathrm{L}(\mathfrak{m}, s, \chi) \sim \sum_{\mathfrak{p}} \chi(\mathfrak{p})\,\mathrm{Norm}(\mathfrak{p})^{-s}.$$

Then, we note that for $\chi \neq \chi_0$ we have that $\mathrm{L}(\mathfrak{m}, s, \chi)$ is analytic at $s = 1$ and $\mathrm{L}(\mathfrak{m}, 1, \chi) \neq 0$ (Prop. 3.2.4, Prop. 4.3.2), so $\log \mathrm{L}(\mathfrak{m}, s, \chi)$ is analytic in a neighborhood of $s = 1$. So,

$$\sum_{\mathfrak{p}\in\mathfrak{c}} \mathrm{Norm}(\mathfrak{p})^{-s} \sim \frac{1}{|G|}\sum_{\chi\in\mathrm{Hom}(G,S^1)} \chi(\mathfrak{c}^{-1})\log \mathrm{L}(\mathfrak{m}, s, \chi) \sim \frac{1}{|G|}\mathrm{L}(\mathfrak{m}, s, \chi_0).$$

Now, we note that $\mathrm{L}(\mathfrak{m}, s, \chi_0)$ has a simple pole at $s = 1$ (Prop. 3.2.4), and so

$$\log \mathrm{L}(\mathfrak{m}, s, \chi_0) \sim \log\frac{1}{s-1}.$$

Then, we have

$$\sum_{\mathfrak{p}\in\mathfrak{c}} \mathrm{Norm}(\mathfrak{p})^{-s} = -\frac{\log(s-1)}{|G|} + g(s)$$

for g bounded in a neighborhood of $s = 1$.

Then,

$$\delta(S) = \lim_{s\to 1^+}\frac{\sum_{\mathfrak{p}\in\mathfrak{c}}\mathrm{Norm}(\mathfrak{p})^{-s}}{-\log(s-1)} = \lim_{s\to 1^+}\left(\frac{1}{|G|} - \frac{g(s)}{\log(s-1)}\right) = \frac{1}{|G|},$$

where the last equality follows as g is analytic at $s = 1$ thus bounded in a neighborhood of it, while $-\log(s-1)$ gets arbitrarily large. □

Corollary 5.3.1. *Let L/K be an abelian extension of number fields, with Galois group $G = \mathrm{Gal}(L/K)$. Let $\sigma \in G$. Let*

$$S = \{\mathfrak{p} \text{ unramified finite prime of } K : \left(\frac{L/K}{\mathfrak{p}}\right) = \sigma\}.$$

Then, $\delta(S) = \frac{1}{|G|}$.

Proof. We know that L/K is the class field for some congruence divisor class group $I/H \cong G$ with conductor $\mathfrak{f}$.

Then, Theorem 2.4.1 and Prop. 2.4.1 tells us that S is the set of primes in some coset $\mathfrak{c} \in \mathbf{I}^{\mathfrak{f}}/H^{\mathfrak{f}}$, up to a finite number of primes dividing $\mathfrak{f}$.

Then, by Prop. 5.3.1 we have that

$$\delta(S) = \frac{1}{[\mathbf{I}^{\mathfrak{f}} : H^{\mathfrak{f}}]} = \frac{1}{|I/H|} = \frac{1}{|G|}.$$ □

5.4. **Reduction of Chebotarev Density Theorem.** Now, we may reduce the Chebotarev Density Theorem to the abelian case. In conjunction with the previous section, this will prove it.

We follow a proof essentially from [Mac68] though now widespread (e.g. in [Gol71, Neu86, Jan96, Neu99]).

Theorem 5.4.1 (Chebotarev Density Theorem)**.** *Let L/K be a Galois extension of number fields, with Galois group $G = \mathrm{Gal}(L/K)$. Let $\sigma \in G$, and c_σ be the conjugacy class of σ. Let*

$$S = \{\mathfrak{p} \text{ finite prime of } K : \left(\frac{L/K}{\mathfrak{p}}\right) = c_\sigma\}.$$

Then, $\delta(S) = \frac{|c_\sigma|}{|G|}$.

Proof. Now, let $H = \langle\sigma\rangle$. Let L^H be the fixed field of H.

Let $S' = \{\mathfrak{p} \in S : \mathfrak{p} \text{ unramified in } L/K\}$.

Let $T = \{P \text{ prime of } L^H \text{ over } \mathfrak{p} \in S' : \left(\frac{L/L^H}{\mathbf{P}}\right) = \sigma, f_{L^H/K}(P) = e_{L^H/K}(P) = 1\}$ (L/L^H is abelian, so the Artin map will indeed yield a single element).

Let $U = \{\mathfrak{P} \text{ prime of } L \text{ over } \mathfrak{p} \in S' : \left[\frac{L/K}{\mathfrak{P}}\right] = \sigma\}$.

Consider the map $U \to T$ given by $\mathfrak{P} \mapsto \mathfrak{P} \cap \mathcal{O}_{L^H}$. We readily see that its image does lie in T. for $\mathfrak{P}$ must be unramified and the inertial degrees for $\mathfrak{P}$ and $\mathfrak{P} \cap \mathcal{O}_{L^H}$ will both be $|H|$. Furthermore, as H is the decomposition group of $\mathfrak{P}$, we have no splitting from L^H to L, so it is injective. Finally, we note that it is surjective, for given a prime P of L^H, there will be a prime $\mathfrak{P}$ of L lying over it; the only things that could prevent $\mathfrak{P}$ from being in U are ramification from K to L^H, or change of Frobenius – the first is prevented by requiring $e_{L^H/K}(P) = 1$, the second is prevented by requiring $f_{L^H/K}(P) = 1$.

Then, by Prop. 5.1.2 we may ignore the finitely many ramified primes and the primes of degree > 1 (over $\mathbb{Q}$, so certainly over K), Prop. 5.3.1 gives us that $\delta(T) = \frac{1}{|H|}$.

Now, consider the map $U \to S'$ given by $\mathfrak{P} \mapsto \mathfrak{P} \cap \mathcal{O}_K$. It is of course surjective. Now, how many elements map to the same $\mathfrak{p} \in S'$? Say $\mathfrak{P}$ is one pre-image, then $\tau\mathfrak{P}$ maps to

it as well if and only if $\tau\sigma\tau^{-1} = \sigma \Leftrightarrow \tau \in Z_H$, and this counts each pre-image $|D_{\mathfrak{P}}| = |H|$ times. So, there are $|Z_H|/|H|$ such pre-images. Furthermore, note that by basic group theory $|Z_H| = \frac{|G|}{|c_\sigma|}$. So:

$$\delta(S) = \delta(S') = \delta(T)\frac{|H|}{|Z_H|} = \frac{1}{|H|}\frac{|H|}{|Z_H|} = \frac{|c_\sigma|}{|G|} \qquad \square$$

Remark. We may now recover Dirichlet's Theorem as a corollary. Simply let $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta_n)$, and use the standard isomorphism $\mathrm{Gal}(L/K) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. Then, for an unramified prime p, $\left[\frac{L/K}{p}\right]$ corresponds to p in $(\mathbb{Z}/n\mathbb{Z})^\times$, so letting σ correspond to $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, we get infinitely many primes p with $p \equiv a \pmod{n}$.

Remark. For a Galois extension L/K, we say that a finite prime $\mathfrak{p}$ of K splits completely if it does not ramify and the primes lying over it have inertial degree 1, so those unramified primes with Artin symbol equal to identity. By the above, we have that the density of those primes which split completely is $1/[L : K]$.

The elementary proof opening this paper was a special case of this, corresponding to $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_n)$.

References

[Coh85] Harvey Cohn, *Introduction to the construction of class fields*, Cambridge Studies in Advanced Mathematics, vol. 6, Cambridge University Press, Cambridge, 1985.

[Gol71] Larry Joel Goldstein, *Analytic number theory*, Prentice-Hall Inc., Englewood Cliffs, N.J., 1971.

[Hei67] H. Heilbronn, *Zeta-functions and L-functions*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965) (J.W.S. Cassels and A. Fröhlich, eds.), Thompson, Washington, D.C., 1967, pp. 204–230.

[Jan96] Gerald J. Janusz, *Algebraic number fields*, second ed., Graduate Studies in Mathematics, vol. 7, American Mathematical Society, Providence, RI, 1996.

[Lan94] Serge Lang, *Algebraic number theory*, second ed., Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994.

[Mac68] C.R. MacCluer, *A reduction of the Čebotarev density theorem to the cyclic case*, Acta Arith. **15** (1968), 45–47.

[Neu86] Jürgen Neukirch, *Class field theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 280, Springer-Verlag, Berlin, 1986.

[Neu99] ———, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[SD01] H. P. F. Swinnerton-Dyer, *A brief guide to algebraic number theory*, London Mathematical Society Student Texts, vol. 50, Cambridge University Press, Cambridge, 2001.

[Ser73] J.-P. Serre, *A course in arithmetic*, Springer-Verlag, New York, 1973, Translated from the French, Graduate Texts in Mathematics, No. 7.

[Tat67] J. T. Tate, *Fourier analysis in number fields, and Hecke's zeta-functions*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965) (J.W.S. Cassels and A. Fröhlich, eds.), Thompson, Washington, D.C., 1967, pp. 305–347.