The Chebotarev Density Theorem
Joel Clingempeel

The primary source used to create these notes was *L-functions and Densities of Primes* by Anatoly Preygel.

1 Review of Class Field Theory

Let K be a number field.

Definition 1.1 *By a modulus* $\mathfrak{m}$, *we mean a finite formal product of primes of* K *raised to non-negative powers.*

We shall write $x \equiv 1 \pmod{\mathfrak{m}}$ to mean that $\text{ord}(x-1)_{\mathfrak{p}} \geq m$ where $\mathfrak{p}^m \,||\, \mathfrak{m}$ for $\mathfrak{p}$ non-archimedean and $\nu(x) > 0$ for ν real archimedean.

We have a natural map $\iota : K^\times \to I_K$ defined by $\iota(a) = a\mathcal{O}_k$. Set $I_K^{\mathfrak{m}} = I_K^{S_{\mathfrak{m}}}$ where $S_{\mathfrak{m}} = \{\mathfrak{p} \text{ finite} : \mathfrak{p} \,|\, \mathfrak{m}\}$ and $K^{\mathfrak{m}} = \iota^{-1}(I_K^{\mathfrak{m}})$. Now denote $K_1^{\mathfrak{m}} = \{x \in K^{\mathfrak{m}} : x \equiv 1 \pmod{\mathfrak{m}}\}$ and $P_K^{\mathfrak{m}} = \iota(K_1^{\mathfrak{m}})$.

Definition 1.2 *The Ray class group is defined to be* $Cl_K^{\mathfrak{m}} = I_K^{\mathfrak{m}}/P_K^{\mathfrak{m}}$.

We may neglect the K subscript when no ambiguity can arise.

Definition 1.3 *A congruence subgroup* $H^{\mathfrak{m}}$ *is any subgroup of* $I^{\mathfrak{m}}$ *containing* $P^{\mathfrak{m}}$. *A (generalized) class group is the corresponding quotient* $I^{\mathfrak{m}}/H^m$.

Proposition 1.1 *If* $\mathfrak{m} \,|\, \mathfrak{n}$, *then* $I^{\mathfrak{n}} \subset I^{\mathfrak{m}}$. *Then given a congruence subgroup* $H^{\mathfrak{m}} \subset I^{\mathfrak{m}}$, *if we set* $H^{\mathfrak{n}} = H^{\mathfrak{m}} \cap I^{\mathfrak{n}}$, *then* $H^{\mathfrak{n}}$ *is a congruence subgroup with* $H^{\mathfrak{m}} = H^{\mathfrak{n}} P^{\mathfrak{m}}$. *Moreover, the inclusion* $I^{\mathfrak{n}} \hookrightarrow I^{\mathfrak{m}}$ *induces an isomorphism* $I^{\mathfrak{n}}/H^{\mathfrak{n}} \cong I^{\mathfrak{m}}/H^{\mathfrak{m}}$.

From this we see that if a class group is defined mod $\mathfrak{m}$, then it is defined mod all multiples of $\mathfrak{m}$. For any class group, there is a unique minimal m called the conductor and denoted by †.

One can show that these generalized class groups are indeed finite as is the case with the standard ideal class group.

Now given a finite Galois extension L/K of number fields and a prime $\mathfrak{p}$ of K, the Galois group $\text{Gal}(L/K)$ acts transitively on the set of primes P_i lying above $\mathfrak{p}$. For each P_i, set $D_{\mathfrak{b}_i} = \{\sigma \in \text{Gal}(L/K) : \sigma(P_i) = P_i\}$. If we let l and k denote the residue fields of L and K respectively, then there is a natural surjective homomorphism $\text{Gal}(L/K) \to \text{Gal}(l/k)$, and we define the kernel to be I_{P_i}. If P_i is unramified, then I_{P_i} is trivial, and so we have an isomorphism. We define $(\frac{L/K}{P_i})$ to be the inverse image of the Frobenius element of $\text{Gal}(l/k)$. If P_i, is ramified, we may still apply this construction, but the result is only well-defined up to conjugation. If this case, we write $\{(\frac{L/K}{P_i})\}$ for the corresponding conjugacy class. Note that applying $\sigma \in \text{Gal}(L/K)$ to P_i has the effect of

conjugating $(\frac{L/K}{P_i})$ by σ. Therefore if L/K is an abelian extension, then $(\frac{L/K}{P_i})$ only depends on $\mathfrak{p}$. In this case, we denote it by $(\frac{L/K}{\mathfrak{p}})$.

Theorem 1.1 (Artin Reciprocity) *Given an abelian extension L/K of number fields, there exists a modulus m divisible by all primes that ramify in L and a congruence subgroup $H^{\mathfrak{m}} \subset I^{\mathfrak{m}}$ such that the map*

$$(\frac{L/K}{\cdot}) : I^{\mathfrak{m}}/H^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$$

defined by sending $\mathfrak{p}$ to $(\frac{L/K}{\mathfrak{p}})$ for $\mathfrak{p}$ prime and extending multiplicatively. Furthermore, every generalized class group arises in such a manner.

2 Class Field Theory and L-functions

Given $\chi \in \mathrm{Hom}(Cl^{\mathfrak{m}}, S^1)$, we may regard it as a character on $I^{\mathfrak{m}}$ in a natural way. We may then extend it to all ideals by defining it to be zero on ideals dividing $\mathfrak{m}$.

Definition 2.1 *Given $\chi \in \mathrm{Hom}(Cl^{\mathfrak{m}}, S^1)$, we define the Dirichlet-Hecke L-series by*

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

Definition 2.2 *Given $\mathfrak{c} \in Cl^{\mathfrak{m}}$, we define the ideal class zeta function by*

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

Note that this enables us to write

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

Proposition 2.1 *Let $\chi \in \mathrm{Hom}(Cl^{\mathfrak{m}}, S^1)$. Then $L(\mathfrak{m}, s, \chi)$ converges absolutely for $\Re(s) > 1$ and uniformly for $\Re(s) > 1 + \delta$ for any $\delta > 0$. Moreover, for $\Re(s) > 1$, we have the Euler product factorization*

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

Definition 2.3 *Given a modulus $\mathfrak{m}$ and a character $\chi \in \mathrm{Hom}(Cl^{\mathfrak{m}}, S^1)$, we define the conductor of χ, denoted $\dagger_\chi$, to be the conductor of $I^{\mathfrak{m}}/\ker(\chi)$.*

Proposition 2.2 *Given the above set-up, $\dagger_\chi$ is the smallest modulus $\mathfrak{n}$ for which χ factors through $Cl^{\mathfrak{n}}$. Furthermore, there exists a unique $\tilde{\chi} \in \mathrm{Hom}(Cl^{\dagger_\chi}, S^1)$ so that χ factors through $\tilde{\chi}$.*

Definition 2.4 *Let L/K be a Galois extension of number fields with Galois group G, and let $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ be an irreducible representation of G. Given a finite prime $\mathfrak{p}$ in K and a prime P lying over $\mathfrak{p}$ in L, $(\frac{L/K}{P})$ is a coset in G of I_P. But $\rho(\frac{L/K}{\mathfrak{p}})|_{I_P}$ is independent of the choice of representative for the coset and moreover remains invariant if one replaces P by a different prime lying over $\mathfrak{p}$. Therefore the quantity $\det(\mathrm{id} - \rho(\frac{L/K}{\mathfrak{p}})|_{I_P})$ is well-defined. We then define the Artin L-function attached to ρ by*

$$L(L/K, s, \rho) = \prod_{\mathfrak{p}} \det(\mathrm{id} - \rho(\frac{L/K}{\mathfrak{p}})|_{I_P})^{-1}.$$

For our purposes, it shall suffice to consider the case when L/K is abelian, and ρ is one-dimensional, i.e. a character on G. In this case, we will see that the L-function agrees with a Dirichlet-Hecke L-function and thus inherits all the corresponding properties.

Theorem 2.1 *Let L/K be an abelian extension of number fields with Galois group G, and let ρ be a character on G. Let F be the subfield of L fixed by $\ker \rho$. By class field theory, ρ corresponds to some $\chi \in \mathrm{Hom}(Cl^{\mathfrak{m}}, S^1)$. Let $\dagger$ be the conductor, and let $\tilde{\chi}$ be the induced character. Then*

$$L(L/K, s, \rho) = L(\mathfrak{m}, s, \tilde{\chi}).$$

Proposition 2.3 *Let L/K be an abelian extension of number fields. Then on their common domain of definition, we have*

$$\zeta_L(s) = \prod_{\rho} L(L/K, s, \rho) = \zeta_K(s) \prod_{\chi \neq \chi_0} L(\dagger_\chi, s, \tilde{\chi}).$$

Comparing vanishing orders at $s = 1$ yields the following.

Proposition 2.4 *Given the above set-up, $L(\mathfrak{m}, 1, \chi) \neq 0$ for $\chi \neq \chi_0$.*

3 The Chebotarev Density Theorem

Definition 3.1 *If S is a set of finite primes of K, then we define the density of S by*

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

Note that $0 \leq \delta(S) \leq 1$.

The first step in proving the Chebotarev Density Theorem is to establish the following key technical result.

Proposition 3.1 *Let K be a number field, $\mathfrak{m}$ a modulus, and $H^{\mathfrak{m}}$ a congruence subgroup. Given $\mathfrak{c} \in I^{\mathfrak{m}}/H^{\mathfrak{m}}$, if we let $S(\mathfrak{c})$ denote the set of prime ideals representing $\mathfrak{c}$, then*

$$\delta(S(\mathfrak{c})) = \frac{1}{[I^{\mathfrak{m}} : H^{\mathfrak{m}}]}.$$

Combining this with class field theory and using the fact that we can neglect a finite set of primes yields the following

Theorem 3.1 (Chebotarev Density Theorem - Abelian Case) *Let L/K be an abelian extension of number fields with Galois group G, and let $\sigma \in G$. Set*

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

Then

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

Now let L/K be an arbitrary Galois extension of number fields with Galois group G. Fix $\sigma \in G$, and write c_σ for the corresponding conjugacy class. Set

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

Then

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

Let $H =< \sigma >$, and set $S' = \{\mathfrak{p} \in S : \mathfrak{p} \text{ unramified in } L/K\}$, $T = \{P \text{ prime of } L^H \text{ over } \mathfrak{p} \in S' : (\frac{L/L^H}{P}) = \sigma, f_{L^H/K}(P) = e_{L^H/K}(P) = 1\}$, and $U = \{\mathfrak{P} \text{ prime of } L \text{ over } \mathfrak{p} \in S' : (\frac{L/K}{\mathfrak{P}}) = \sigma\}$. Then one can show that the map $U \to T$ defined by $\mathfrak{P} \mapsto \mathfrak{P} \cap \mathcal{O}_{L^H}$ is a bijection, and the map $U \to S'$ defined by $\mathfrak{P} \mapsto \mathfrak{P} \cap \mathcal{O}_K$ is $\frac{|Z_H|}{|H|}$ to one. Then the abelian case gives us $\delta(T) = \frac{1}{|T|}$ so

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

But S and S' only differ by a finite set so they must have the same density. We have thus shown the following.

Theorem 3.2 (Chebotarev Density Theorem) *Given the above set-up, we have*

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