28 Global class field theory, the Chebotarev density theorem

Recall that a global field is a field with a product formula whose completions at nontrivial absolute values are local fields. By the Artin-Whaples theorem (see Problem Set 7), every such field is either

- a number field: finite extension of \( \mathbb{Q} \) (characteristic zero);
- a global function field: finite extension of \( \mathbb{F}_q(t) \) (positive characteristic).

In Lecture 25 we defined the adele ring \( \mathcal{A}_K \) of a global field \( K \) as the restricted product

\[
\mathcal{A}_K := \prod_v (K_v, \mathcal{O}_v) = \{ (a_v) \in \prod_v K_v : a_v \in \mathcal{O}_v \text{ for almost all } v \},
\]

where \( v \) ranges over the places of \( K \) (equivalence classes of absolute values), \( K_v \) denotes the completion of \( K \) at \( v \), and \( \mathcal{O}_v \) is the valuation ring of \( K_v \) if \( v \) is nonarchimedean, and equal to \( K_v \) otherwise. As a topological ring, \( \mathcal{A}_K \) is locally compact and Hausdorff. The field \( K \) is canonically embedded in \( \mathcal{A}_K \) via the diagonal map \( x \mapsto (x, x, x, \ldots) \) whose image is discrete, closed, and cocompact; see Theorem 25.12.

In Lecture 26 we defined the idele group

\[
\mathbb{I}_K := \prod_v (K_v^\times, \mathcal{O}_v^\times) = \{ (a_v) \in \prod_v K_v^\times : a_v \in \mathcal{O}_v^\times \text{ for almost all } v \},
\]

which coincides with the unit group of \( \mathcal{A}_K \) but has a finer topology (using the restricted product topology ensures that \( a \mapsto a^{-1} \) is continuous, which is not true of the subspace topology). As a topological group, \( \mathbb{I}_K \) is locally compact and Hausdorff. The multiplicative group \( K^\times \) is canonically embedded as a discrete subgroup of \( \mathbb{I}_K \) via the diagonal map \( x \mapsto (x, x, x, \ldots) \), and the idele class group is the quotient \( C_K := \mathbb{I}_K / K^\times \), which is locally compact but not compact.

28.1 The idele norm

The idele group \( \mathbb{I}_K \) surjects onto the ideal group \( \mathcal{I}_K \) of invertible fractional ideals of \( \mathcal{O}_K \) via the surjective homomorphism

\[
\varphi: \mathbb{I}_K \to \mathcal{I}_K
\]

\[
a \mapsto \prod p^{v_p(a)},
\]

where \( v_p(a) \) is the \( p \)-adic valuation of the component \( a_v \in K_v^\times \) of \( a = (a_v) \in \mathbb{I}_K \) at the finite place \( v \) corresponding to the absolute value \( \| \|_p \). We have the following commutative diagram of exact sequences:

\[
1 \longrightarrow K^\times \longrightarrow \mathbb{I}_K \longrightarrow C_K \longrightarrow 1
\]

\[
\downarrow \quad \quad \downarrow \quad \quad \downarrow
\]

\[
1 \longrightarrow P_K \longrightarrow \mathcal{I}_K \longrightarrow \mathcal{C}_K \longrightarrow 1
\]

where \( P_K \) is the subgroup of principal ideals and \( \mathcal{C}_K := \mathcal{I}_K / P_K \) is the ideal class group.

Andrew V. Sutherland
Definition 28.1. Let \( L/K \) is a finite separable extension of global fields. The idele norm \( N_{L/K} : \mathbb{I}_L \to \mathbb{I}_K \) is defined by \( N_{L/K}(b_w) = (a_v) \), where each

\[
a_v := \prod_{w \mid v} N_{L_w/K_v}(b_w)
\]

is a product over places \( w \) of \( L \) that extend the place \( v \) of \( K \) and \( N_{L_w/K_v} : L_w \to K_v \) is the field norm of the corresponding finite separable extension of local fields \( L_w/K_v \).

It follows from Corollary 11.24 and Remark 11.25 that the idele norm \( N_{L/K} : \mathbb{I}_L \to \mathbb{I}_K \) agrees with the field norm \( N_{L/K} : L^\times \to K^\times \) on the subgroup of principal ideles \( L^\times \subseteq \mathbb{I}_L \). The field norm is also compatible with the ideal norm \( N_{L/K} : \mathbb{I}_L \to \mathbb{I}_K \) (see Proposition 6.6), and we have the following commutative diagram:

\[
\begin{array}{ccc}
L^\times & \longrightarrow & \mathbb{I}_L \\
\downarrow{N_{L/K}} & & \downarrow{N_{L/K}} \\
K^\times & \longrightarrow & \mathbb{I}_K \\
\end{array}
\]

The image of \( L^\times \) in \( \mathbb{I}_L \) under the composition of the maps on the top row is precisely the group \( \mathcal{P}_L \) of principal ideals, and the image of \( K^\times \) in \( \mathbb{I}_K \) is similarly \( \mathcal{P}_K \). Taking quotients yields induced norm maps on the idele and ideal class groups, both of which we also denote \( N_{L/K} \), and we have a commutative square

\[
\begin{array}{ccc}
C_L & \longrightarrow & \text{Cl}_L \\
\downarrow{N_{L/K}} & & \downarrow{N_{L/K}} \\
C_K & \longrightarrow & \text{Cl}_K \\
\end{array}
\]

28.2 The Artin homomorphism

We now construct the global Artin homomorphism using the local Artin homomorphisms we defined in the previous lecture. Let us first fix once and for all a separable closure \( K^{\text{sep}} \) of our global field \( K \), and for each place \( v \) of \( K \), a separable closure \( K_v^{\text{sep}} \) of the local field \( K_v \). Let \( K^{\text{ab}} \) and \( K_v^{\text{ab}} \) denote maximal abelian extensions within these separable closures; henceforth all abelian extensions of \( K \) and the \( K_v \) are assumed to lie in these maximal abelian extensions.

By Theorem 27.2, each local field \( K_v \) is equipped with a local Artin homomorphism

\[
\theta_{K_v} : K_v^\times \to \text{Gal}(K_v^{\text{ab}}/K_v).
\]

For each finite abelian extension \( L/K \) and each place \( w|v \) of \( L \), composing \( \theta_{K_v} \) with the natural map \( \text{Gal}(K_v^{\text{ab}}/K_v) \to \text{Gal}(L_w/K_v) \) yields a surjective homomorphism

\[
\theta_{L_w/K_v} : K_v^\times \to \text{Gal}(L_w/K_v)
\]

with kernel \( N_{L_w/K_v}(L_w^\times) \). When \( K_v \) is nonarchimedean and \( L_w/K_v \) is unramified we have \( \theta_{L_w/K_v}(\pi_v) = \text{Frob}_{L_w/K_v} \) for all uniformizers \( \pi_v \) of \( K_v \). Note that by Theorem 11.20, every finite separable extension of \( K_v \) is of the form \( L_w \) for some place \( w|v \).
We now define an embedding of Galois groups

$$\varphi_w : \text{Gal}(L_w/K_v) \hookrightarrow \text{Gal}(L/K)$$

$$\sigma \mapsto \sigma|_L$$

The map $\varphi_w$ is well defined and injective because every element of $L_w$ can be written as $\ell x$ for some $\ell \in L$ and $x \in K_v$ (any $K$-basis for $L$ spans $L_w$ as a $K_v$ vector space), so each $\sigma \in \text{Gal}(L_w/K_v)$ is uniquely determined by its action on $L$, which fixes $K \subseteq K_v$. If $v$ is archimedean then $\varphi_w(\text{Gal}(L_w/K_v))$ is either trivial or generated by the involution corresponding to complex conjugation in $L_w \cong \mathbb{C}$. If $v$ is a finite place and $q$ is the prime of $L$ corresponding to $w|v$, then $\varphi_w(\text{Gal}(L_w/K_v))$ is the decomposition group $D_q \subseteq \text{Gal}(L/K)$; this follows from parts (5) and (6) of Theorem 11.23.

More generally, for any place $v$ of $K$, the Galois group $\text{Gal}(L/K)$ acts on the set $\{w|v\}$, via $|w|_v(\sigma) := |\sigma|_w$, and $\varphi_w(\text{Gal}(L_w/K_v))$ is the stabilizer of $w$ under this action. It thus makes sense to call $\varphi_w(\text{Gal}(L_w/K_v))$ the decomposition group of the place $w$. For $w|v$ the groups $\varphi_w(\text{Gal}(L_w/K_v))$ are necessarily conjugate, and in our abelian setting, equal.

Moreover, the composition $\varphi_w \circ \theta_{L_w/K_v}$ defines a map $K_v^\times \to \text{Gal}(L/K)$ that is independent of the choice of $w|v$: this is easy to see when $v$ is an unramified nonarchimedean place, since then $\varphi_w(\theta_{L_w/K_v}(\pi_v)) = \text{Frob}_v$ for every uniformizer $\pi_v$ of $K_v$, and this determines $\varphi_w \circ \theta_{L_w/K_v}$ since the $\pi_v$ generate $K_v^\times$.

For each place $v$ of $K$ we now embed $K_v^\times$ into the idele group $\mathbb{I}_K$ via the map

$$\iota_v : K_v^\times \hookrightarrow \mathbb{I}_K$$

$$\alpha \mapsto (1, 1, \ldots, 1, \alpha, 1, 1, \ldots),$$

whose image intersects $K^\times \subseteq \mathbb{I}_K$ trivially. This embedding is compatible with the idele norm in the following sense: if $L/K$ is any finite separable extension and $w$ is a place of $L$ that extends the place $v$ of $K$ then the diagram

$$\begin{array}{ccc}
L_w^\times & \xrightarrow{N_{L_w/K_v}} & K_v^\times \\
\downarrow \iota_w & & \downarrow \iota_v \\
\mathbb{I}_L & \xrightarrow{N_{L/K_v}} & \mathbb{I}_K
\end{array}$$

commutes.

Now let $L/K$ be a finite abelian extension. For each place $v$ of $K$, let us pick a place $w$ of $L$ extending $v$ and define

$$\theta_{L/K} : \mathbb{I}_K \to \text{Gal}(L/K)$$

$$(a_v) \mapsto \prod_v \varphi_w(\theta_{L_w/K_v}(a_v)),$$

where the product takes place in $\text{Gal}(L/K)$. The value of $\varphi_w(\theta_{L_w/K_v}(a_v))$ is independent of our choice of $w|v$, as noted above. The product is well defined because $a_v \in \mathcal{O}_v^\times$ and $v$ is unramified in $L$ for almost all $v$, in which case

$$\varphi_w(\theta_{L_w/K_v}(a_v)) = \text{Frob}_v^{v(a_v)} = 1,$$

It is clear that $\theta_{L/K}$ is a homomorphism, since each $\varphi_w \circ \theta_{L_w/K_v}$ is, and $\theta_{L/K}$ is continuous because its kernel is a union of open sets: each $a := (a_v) \in \text{ker} \theta_{L/K}$ lies in an open set.
\[ U_a := U_S \times \prod_{v \notin S} O_v^\times \subseteq \ker \theta_{L/K}, \] where \( S \) contains all ramified \( v \) and all \( v \) for which \( a_v \notin O_v^\times \), and \( U_S \) is the kernel of \((a_v)_{v \in S} \mapsto \prod_{v \in S} \varphi_w(\theta_{Lw/Kw}(a_v))\), which is open in \( \prod_{v \in S} K_v^\times \).

If \( L_1 \subseteq L_2 \) are two finite abelian extensions of \( K \), then \( \theta_{L_1/K}(a) = \theta_{L_2/K}(a) |_{L_1} \) for all \( a \in I_K \). The \( \theta_{L/K} \) form a compatible system of homomorphisms from \( I_K \) to the inverse limit \( \varprojlim_L \text{Gal}(L/K) \simeq \text{Gal}(K^{ab}/K) \), where \( L \) ranges over finite abelian extensions of \( K \) in \( K^{ab} \) ordered by inclusion. By the universal property of the profinite completion, they uniquely determine a continuous homomorphism.

**Definition 28.2.** Let \( K \) be a global field. The **global Artin homomorphism** is the continuous homomorphism

\[ \theta_K : I_K \to \varprojlim_L \text{Gal}(L/K) \simeq \text{Gal}(K^{ab}/K) \]

defined by the compatible system of homomorphisms \( \theta_{L/K} : I_K \to \text{Gal}(L/K) \), where \( L \) ranges over finite abelian extensions of \( K \) in \( K^{ab} \).

The isomorphism \( \text{Gal}(K^{ab}/K) \simeq \varprojlim_L \text{Gal}(L/K) \) is the natural isomorphism between a Galois group and its profinite completion with respect to the Krull topology (Theorem 26.22) and is thus canonical, as is the global Artin homomorphism \( \theta_K : I_K \to \text{Gal}(K^{ab}/K) \).

**Proposition 28.3.** Let \( K \) be global field. The global Artin homomorphism \( \theta_K \) is the unique continuous homomorphism \( I_K \to \text{Gal}(K^{ab}/K) \) with the property that for every finite abelian extension \( L/K \) in \( K^{ab} \) and every place \( w \) of \( L \) lying over a place \( v \) of \( K \) the diagram

\[
\begin{array}{ccc}
K_v^\times & \xrightarrow{\theta_{Lw/Kw}} & \text{Gal}(L_w/K_v) \\
\downarrow{\iota_v} & & \downarrow{\varphi_w} \\
I_K & \xrightarrow{\theta_{L/K}} & \text{Gal}(L/K)
\end{array}
\]

commutes, where the homomorphism \( \theta_{L/K} \) is defined by \( \theta_{L/K}(a) := \theta_K(a)|_L \).

**Proof.** That \( \theta_K \) has this property follows from its construction. Now suppose that there is another continuous homomorphism \( \theta'_{L/K} : I_K \to \text{Gal}(K^{ab}/K) \) with the same property. We may view elements of \( \text{Gal}(K^{ab}/K) \simeq \varprojlim_L \text{Gal}(L/K) \) as elements of \( \prod_{L/K} \text{Gal}(L/K) \), where \( L \) varies over finite abelian extensions of \( K \) in \( K^{ab} \). If \( \theta_K \) and \( \theta'_{L/K} \) are not identical, then there must be an \( a \in I_K \) and a finite abelian extension \( L/K \) for which \( \theta_{L/K}(a) \neq \theta'_{L/K}(a) \).

Let \( S \) be a finite set of places of \( K \) that includes all places \( v \) for which \( a_v \notin O_v^\times \) and all ramified places of \( L/K \). Define \( b \in I_K \) by \( b_v := 1 \) for \( v \in S \) and \( b_v := a_v \) for \( v \notin S \), so that \( a = b \prod_v \iota_v(a_v) \). Then \( \theta_{Lw/Kw}(b_v) = 1 \) for all places \( v \), so we must have \( \theta_{L/K}(b) = 1 = \theta'_{L/K}(b) \), and for \( v \in S \) we have

\[ \theta_{L/K}(\iota_v(a_v)) = \varphi_w(\theta_{Lw/Kw}(a_v)) = \theta'_{L/K}(\iota_v(a_v)), \]

by the commutativity of the diagram in the proposition. But then

\[ \theta_{L/K}(a) = \theta_{L/K}(b) \prod_{v \in S} \theta_{L/K}(\iota_v(a_v)) = \theta'_{L/K}(b) \prod_{v \in S} \theta'_{L/K}(\iota_v(a_v)) = \theta'_{L/K}(a), \]

which is a contradiction. So \( \theta'_{L/K} = \theta_K \) as claimed. \( \square \)
28.3 The main theorems of global class field theory

In the global version of Artin reciprocity, the idele class group $C_K := \mathbb{I}_K/K^\times$ plays the role that the multiplicative group $K_1^\times$ plays in local Artin reciprocity (Theorem 27.2).

**Theorem 28.4 (Global Artin Reciprocity).** Let $K$ be a global field. The kernel of the global Artin homomorphism $\theta_K$ contains $K^\times$, and we thus have a continuous homomorphism

$$\theta_K : C_K \to \text{Gal}(K^{ab}/K),$$

with the property that for every finite abelian extension $L/K$ in $K^{ab}$ the homomorphism

$$\theta_{L/K} : C_K \to \text{Gal}(L/K)$$

obtained by composing $\theta_K$ with the natural map $\text{Gal}(K^{ab}) \to \text{Gal}(L/K)$ is surjective with kernel $N_{L/K}(C_L)$, inducing an isomorphism $C_K/N_{L/K}(C_L) \simeq \text{Gal}(L/K)$.

**Remark 28.5.** When $K$ is a number field, $\theta_K$ is surjective but not injective; its kernel is the connected component of the identity, including the image of $\prod_{v|\infty} \mathbb{R}_{>0} \times \prod_{v<\infty} 1 \subseteq \mathbb{I}_K$, which injects into $C_K$. When $K$ is a global function field, $\theta_K$ is injective but not surjective; its image is dense in $\text{Gal}(K^{ab}/K)$.

We also have a global existence theorem.

**Theorem 28.6 (Global Existence Theorem).** Let $K$ be a global field. For every finite index open subgroup $H$ of $C_K$ there is a unique finite abelian extension $L/K$ in $K^{ab}$ for which $N_{L/K}(C_L) = H$.

As with the local Artin homomorphism, taking profinite completions yields an isomorphism that allows us to summarize global class field theory in one statement.

**Theorem 28.7 (Main theorem of global class field theory).** Let $K$ be a global field. The global Artin homomorphism $\theta_K$ induces a canonical isomorphism

$$\hat{\theta}_K : \hat{C}_K \simeq \text{Gal}(K^{ab}/K)$$

of profinite groups.

We then have an inclusion reversing bijection

$$\{\text{finite index open subgroups } H \text{ of } C_K\} \leftrightarrow \{\text{finite abelian extensions } L/K \text{ in } K^{ab}\}$$

$$H \mapsto (K^{ab})^{\theta_K(H)}$$

$$N_{L/K}(C_L) \leftrightarrow L$$

and corresponding isomorphisms $C_K/H \simeq \text{Gal}(L/K)$, where $H = N_{L/K}(C_L)$. We also note that the global Artin homomorphism is functorial in the following sense.

**Theorem 28.8 (Functoriality).** Let $K$ be a global field and let $L/K$ be any finite separable extension (not necessarily abelian). Then the following diagram commutes

$$C_L \xrightarrow{\theta_L} \text{Gal}(L^{ab}/L) \xrightarrow{\text{res}} \text{Gal}(K^{ab}/K).$$
28.4 Relation to ideal-theoretic version of global class field theory

Let $K$ be a number field and let $m: M_K \to \mathbb{Z}_{\geq 0}$ be a modulus for $K$, which we view as a formal product $m = \prod_v v^{e_v}$ over the places $v$ of $K$ with $e_v \leq 1$ when $v$ is archimedean and $e_v = 0$ when $v$ is complex (see Definition 21.2). For each place $v$ we define the open subgroup

$$U^m_K(v) := \begin{cases} \mathcal{O}_v^\times & \text{if } v \not| m, \text{ where } \mathcal{O}_v^\times := K_v^\times \text{ when } v \text{ is infinite}, \\ \mathbb{R}_{>0} & \text{if } v|m \text{ is real, where } \mathbb{R}_{>0} \subseteq \mathbb{R}^\times \simeq \mathcal{O}_v^\times := K_v^\times, \\ 1 + p^e_v & \text{if } v|m \text{ is finite, where } p = \{ x \in \mathcal{O}_v : |x|_v < 1 \}, \end{cases}$$

and let $U^m_K := \prod_v U^m_K(v) \subseteq \mathbb{I}_K$ denote the corresponding open subgroup of $\mathbb{I}_K$. The image $\mathcal{U}^m_K$ of $U^m_K$ in the idele class group $\mathcal{C}_K = \mathbb{I}_K/K^\times$ is a finite index open subgroup. The idelic version of a ray class group is the quotient

$$C^m_K := \mathbb{I}_K/(U^m_K K^\times) = C_K/\mathcal{U}^m_K,$$

and we have isomorphisms

$$C^m_K \simeq \text{Cl}^m_K \simeq \text{Gal}(K(m)/K),$$

where $\text{Cl}^m_K$ is the ray class group for the modulus $m$ (see Definition 21.3), and $K(m)$ is the corresponding ray class field, which we can now define as the finite abelian extension $L/K$ for which $N_{L/K}(C_L) = \mathcal{U}^m_K$, whose existence is guaranteed by Theorem 28.6.

If $L/K$ is any finite abelian extension, then $N_{L/K}(C_L)$ contains $\mathcal{U}^m_K$ for some modulus $m$; this follows from the fact that the groups $\mathcal{U}^m_K$ form a fundamental system of open neighborhoods of the identity. Indeed, the conductor of the extension $L/K$ (see Definition 22.24) is precisely the minimal modulus $m$ for which this is true. It follows that every finite abelian extension $L/K$ lies in a ray class field $K(m)$, with $\text{Gal}(L/K)$ isomorphic to a quotient of a ray class group $C^m_K$.

28.5 The Chebotarev density theorem

We conclude this lecture with a proof of the Chebotarev density theorem, a generalization of the Frobenius density theorem you proved on Problem Set 10. Recall from Lecture 18 and Problem Set 9 that if $S$ is a set of primes of a number field $K$, the Dirichlet density of $S$ is defined by

$$d(S) := \lim_{s \to 1^+} \frac{\sum_{p \in S} N(p)^{-s}}{\sum_p N(p)^{-s}} = \lim_{s \to 1^+} \frac{\sum_{p \in S} N(p)^{-s}}{\log \frac{1}{s-1}},$$

whenever this limit exists. As you proved on Problem Set 9, if $S$ has a natural density then it has a Dirichlet density and the two coincide (and similarly for polar density).

In order to state Chebotarev’s density theorem we need one more definition: a subset $C$ of a group $G$ is said to be stable under conjugation if $\sigma \tau \sigma^{-1} \in C$ for all $\sigma \in G$ and $\tau \in C$. Equivalently, $C$ is a union of conjugacy classes of $G$.

Theorem 28.9 (Chebotarev Density Theorem). Let $L/K$ be a finite Galois extension of number fields with Galois group $G := \text{Gal}(L/K)$. Let $C \subseteq G$ be stable under conjugation, and let $S$ be the set of primes $p$ of $K$ unramified in $L$ with $\text{Frob}_p \subseteq C$. Then $d(S) = \#C/\#G$. 

18.785 Fall 2021, Lecture #28, Page 6
Note that $G$ is not assumed to be abelian, so $\text{Frob}_p$ is a conjugacy class, not an element. However, the main difficulty in proving the Chebotarev density theorem (and the only place where class field theory is used) occurs when $G$ is abelian, in which case $\text{Frob}_p$ contains a single element. The main result we need is a corollary of the generalization of Dirichlet’s theorem on primes in arithmetic progressions to number fields that we proved in Lecture 22, a special case of which we record below.

**Proposition 28.10.** Let $m$ be a modulus for a number field $K$ and let $\text{Cl}_K^m$ be the corresponding ray class group. For every ray class $c \in \text{Cl}_K^m$ the Dirichlet density of the set of primes $p$ of $K$ that lie in $c$ is $1/\#\text{Cl}_K^m$.

**Proof.** Apply Corollary 22.22 to the congruence subgroup $C = \mathcal{R}_K^m$. \hfill \Box

The Chebotarev density theorem for abelian extensions follows from Proposition 28.10 and the existence of ray class fields, which we now assume.\footnote{This assumption is not necessary; indeed Chebotarev proved his density theorem in 1923 without it. With slightly more work one can derive the general case from the cyclotomic case $L = K(\zeta)$, where $\zeta$ is a primitive root of unity, which removes the need to assume the existence of ray class fields; see [4] for details.}

**Corollary 28.11.** Let $L/K$ be a finite abelian extension of number fields with Galois group $G$. For every $\sigma \in G$ the Dirichlet density of the set $S$ of primes $p$ of $K$ unramified in $L$ for which $\text{Frob}_p = \{\sigma\}$ is $1/\#G$.

**Proof.** Let $m = \text{cond}(L/K)$ be the conductor of the extension $L/K$; then $L$ is a subfield of the ray class field $K(m)$ and $\text{Gal}(L/K) \cong \text{Cl}_K^m/H$ for some subgroup $H$ of the ray class group. For each unramified prime $p$ of $K$ we have $\text{Frob}_p = \{\sigma\}$ if and only if $p$ lies in one of the ray classes contained in the coset of $H$ in $\text{Cl}_K^m/H$ corresponding to $\sigma$. The Dirichlet density of the set of primes in each ray class is $1/\#\text{Cl}_K^m$, by Proposition 28.10, and there are $\#H$ ray classes in each coset of $H$; thus $d(S) = \#H/\#\text{Cl}_K^m = 1/\#G$. \hfill \Box

We now derive the general case from the abelian case.

**Proof of the Chebotarev density theorem.** It suffices to consider the case where $C$ is a single conjugacy class, which we now assume; we can reduce to this case by partitioning $C$ into conjugacy classes and summing Dirichlet densities (as proved on Problem Set 9). Let $S$ be the set of primes $p$ of $K$ unramified in $L$ for which $\text{Frob}_p$ is the conjugacy class $C$.

Let $\sigma \in G$ be a representative of the conjugacy class $C$, let $H_\sigma := \langle \sigma \rangle \subseteq G$ be the subgroup it generates, and let $F_\sigma := L^{H_\sigma}$ be the corresponding fixed field. Let $T_\sigma$ be the set of primes $q$ of $F_\sigma$ unramified in $L$ for which $\text{Frob}_q = \{\sigma\} \subseteq \text{Gal}(L/F_\sigma) \subseteq \text{Gal}(L/K)$ (note that the Frobenius class $\text{Frob}_q$ is a singleton because $\text{Gal}(L/F_\sigma) = H_\sigma$ is abelian). We have $d(T_\sigma) = 1/\#H_\sigma$, since $L/F_\sigma$ is abelian, by Corollary 28.11.\footnote{Note that the integers $\#H_\sigma$ and $[G : H_\sigma]$ do not depend on the choice of $\sigma$ (the $H_\sigma$ are all conjugate).}

As you proved on Problem Set 9, restricting to degree-1 primes (primes whose residue field has prime order) does not change Dirichlet densities, so let us replace $S$ and $T_\sigma$ by their subsets of degree-1 primes, and define $T_\sigma(p) := \{q \in T_\sigma : q|p\}$ for each $p \in S$.

**Claim:** For each prime $p \in S$ we have $\#T_\sigma(p) = [G : H_\sigma]$.

**Proof of claim:** Let $r$ be a prime of $L$ lying above $q \in T_\sigma(p)$. Such an $r$ is unramified, since $p$ is, and we have $\text{Frob}_r = \sigma$, since $\text{Frob}_q = \{\sigma\}$. It follows that $\text{Gal}(\mathbb{F}_r/\mathbb{F}_q) = \langle \sigma \rangle \cong H_\sigma$. Therefore, $\#T_\sigma(p) = [G : H_\sigma]$. \hfill \Box

18.785 Fall 2021, Lecture #28, Page 7
Therefore \( f_{\ell/q} = \#H_\sigma \) and \( \#\{r|q\} = 1 \), since \( \#H_\sigma = [L: F_\sigma] = \sum_{e_{\ell/q}f_{\ell/q}} \). We have 
\( f_{\ell/p} = f_{\ell/q}q_{\ell/p} = f_{\ell/q} = \#H_\sigma \), since \( f_{q/p} = 1 \) for degree-1 primes \( q|p \), and \( e_{\ell/p} = 1 \), thus
\[
\#G = [L:K] = \sum_{e_{\ell/p}f_{\ell/p}} \] = \#\{r|p\}\#H_\sigma = \#T_\sigma(p)\#H_\sigma,
\]
so \( \#T_\sigma(p) = \#G/\#H_\sigma = [G:H_\sigma] \) as claimed. We now observe that
\[
\sum_{p \in S} N(p)^{-s} = \sum_{\sigma \in G/H_{\sigma}} \frac{1}{[G:H_{\sigma}]} \sum_{q \in T_\sigma(p)} N(q)^{-s} = \frac{\#C}{[G:H_{\sigma}]} \sum_{q \in T_\sigma} N(q)^{-s}
\]
since \( N(q) = N(p) \) for each degree-1 prime \( q \) lying above a degree-1 prime \( p \), and therefore
\[
d(S) = \frac{\#C}{[G:H_{\sigma}]}d(T_\sigma) = \frac{\#C}{[G:H_{\sigma}]\#H_{\sigma}} = \frac{\#C}{\#G}.
\]

**Remark 28.12.** The Chebotarev density theorem holds for any global field; the generalization to function fields was originally proved by Reichardt [3]; see [2] for a modern proof (and in fact a stronger result). In the case of number fields (but not function fields!) Chebotarev’s theorem also holds for natural density. This follows from results of Hecke [1] that actually predate Chebotarev’s work; Hecke showed that the primes lying in any particular ray class have a natural density.

**References**


