26 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. As proved on Problem Set 7, every such field is one of the following:

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

An equivalent characterization of a global function field is that it is the function field of a smooth projective geometrically integral curve over a finite field.

In Lecture 23 we defined the *adele ring* $\mathbb{A}_K$ of a global field K as the restricted product

$$\mathbb{A}_K := \prod\nolimits_v (K_v, \mathcal{O}_v) = \big\{(a_v) \in \prod K_v : a_v \in \mathcal{O}_v \text{ for almost all } v\big\},$$

where v ranges over the places of K (equivalence classes of absolute values), K_v denotes the completion of K at v (a local field), and $\mathcal{O}_v$ is the valuation ring of K_v if v is nonarchimedean, and $\mathcal{O}_v := K_v$ otherwise. As a topological ring, $\mathbb{A}_K$ is locally compact and Hausdorff. The field K is canonically embedded in $\mathbb{A}_K$ via the diagonal map $x \mapsto (x, x, x, \ldots)$ whose image is discrete, closed, and cocompact; see Theorem 23.12.

In Lecture 24 we defined the *idele group*

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

which coincides with the unit group of $\mathbb{A}_K$ as a set 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.

26.1 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

$$\begin{aligned} \varphi\colon \mathbb{I}_K &\to \mathcal{I}_K \\ a &\mapsto \prod \mathfrak{p}^{v_\mathfrak{p}(a)}, \end{aligned}$$

where $v_\mathfrak{p}(a)$ is the $\mathfrak{p}$-adic valuation of the component $a_v \in K_v^\times$ of $a = (a_v) \in \mathbb{I}_K$ at the place v corresponding to the absolute value $\|x\|_v = \mathrm{N}(\mathfrak{p})^{-v_\mathfrak{p}(x)}$ induced by the discrete valuation $v_\mathfrak{p}\colon K_v \to \mathbb{Z}$; here $\mathrm{N}(\mathfrak{p}) := \mathcal{O}_K/\mathfrak{p}$ is the absolute norm of $\mathfrak{p}$. We have the following commutative diagram of exact sequences:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K^\times & \longrightarrow & \mathbb{I}_K & \longrightarrow & C_k & \longrightarrow & 1 \\ & & \big\downarrow{\scriptstyle x\mapsto(x)} & & \big\downarrow{\scriptstyle \varphi} & & \big\downarrow & & \\ 1 & \longrightarrow & \mathcal{P}_K & \longrightarrow & \mathcal{I}_K & \longrightarrow & \mathrm{Cl}_k & \longrightarrow & 1 \end{array}$$

where $\mathcal{P}_K$ is the subgroup of principal ideals and $\mathrm{Cl}_K := \mathcal{I}_K / \mathcal{P}_K$ is the ideal class group.

Definition 26.1. Let L/K is a finite separable extension of global fields. The *idele norm* $\mathrm{N}_{L/K}\colon \mathbb{I}_L \to \mathbb{I}_K$ is defined by $\mathrm{N}_{L/K}(b_w) = (a_v)$, where each

$$a_v := \prod_{w|v} \mathrm{N}_{L_w/K_v}(b_w)$$

is a product over places w of L that extend the place v of K and $\mathrm{N}_{L_w/K_v}\colon L_w \to K_v$ is the field norm of the corresponding finite separable extension of local fields L_w/K_v.

It follows from Corollary 11.21 and Remark 11.22 that the idele norm $\mathrm{N}_{L/K}\colon \mathbb{I}_L \to \mathbb{I}_K$ agrees with the field norm $\mathrm{N}_{L/K}\colon L^\times \to K^\times$ on the subgroup of principal ideles $L^\times \subseteq \mathbb{I}_L$. The field norm is also compatible with the ideal norm $\mathrm{N}_{L/K}\colon \mathcal{I}_L \to \mathcal{I}_K$ (see Proposition 6.5), and we thus obtain the following commutative diagram

$$\begin{array}{ccccc} L^\times & \longrightarrow & \mathbb{I}_L & \longrightarrow & \mathcal{I}_L \\ \downarrow{\scriptstyle \mathrm{N}_{L/K}} & & \downarrow{\scriptstyle \mathrm{N}_{L/K}} & & \downarrow{\scriptstyle \mathrm{N}_{L/K}} \\ K^\times & \longrightarrow & \mathbb{I}_K & \longrightarrow & \mathcal{I}_K \end{array}$$

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 $\mathrm{N}_{L/K}$, and we obtain the commutative diagram:

$$\begin{array}{ccc} C_L & \twoheadrightarrow & \mathrm{Cl}_L \\ \downarrow{\scriptstyle \mathrm{N}_{L/K}} & & \downarrow{\scriptstyle \mathrm{N}_{L/K}} \\ C_K & \twoheadrightarrow & \mathrm{Cl}_K \end{array}$$

26.2 The Artin homomorphism

We now want to use the local Artin homomorphisms we defined in the previous lecture to construct a global Artin homomorphism. Let us first fix once and for all a separable closure K^{sep} of our global field K, and for each place v of K, a separable closure K_v^{sep} of the local field K_v. Let K^{ab} and K_v^{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 25.2, each local field K_v is equipped with a local Artin homomorphism

$$\theta_{K_v}\colon K_v^\times \to \mathrm{Gal}(K_v^{\mathrm{ab}}/K_v),$$

and for each finite abelian L_w/K_v the map θ_{K_v} induces (via restriction) a surjective homomorphism

$$\theta_{L_w/K_v}\colon K_v^\times \to \mathrm{Gal}(L_w/K_v)$$

with kernel $\mathrm{N}_{L_w/K_v}(L_w^\times)$. When K_v is nonarchimedean and L_w/K_v is unramified we also have $\theta_{L_w/K_v}(\pi) = \mathrm{Frob}_{L_w/K_v}$ for every uniformizer π of $\mathcal{O}_v$.

By Corollary 11.17, we may view L_w as the completion of a finite abelian extension L/K at a place w extending v (recall that we write $w|v$ to indicate this). If v corresponds to a prime $\mathfrak{p}$ of K, then w corresponds to a prime $\mathfrak{q}$ for which $\mathrm{Gal}(L_w/K_v) \simeq D_{\mathfrak{q}}$, where

$D_{\mathfrak{q}} \subseteq \mathrm{Gal}(L/K)$ is the decomposition group of $\mathfrak{q}$ (the subgroup of $\mathrm{Gal}(L/K)$ fixing $\mathfrak{q}$), by Theorem 11.20. This allows us to define an embedding

$$\mathrm{Gal}(L_w/K_v) \hookrightarrow \mathrm{Gal}(L/K)$$

as follows:

- if v is archimedean then either $L_w \simeq K_v$ and we identify $\mathrm{Gal}(L_w/K_v)$ with the trivial subgroup of $\mathrm{Gal}(L/K)$, or $L_w/K_v \simeq \mathbb{C}/\mathbb{R}$ and we identify $\mathrm{Gal}(L_w/K_v)$ with the subgroup of $\mathrm{Gal}(L/K)$ generated by complex conjugation (which must be nontrivial).
- if v is nonarchimedean, let $\mathfrak{q}$ be the prime of L corresponding to the place w and identify $\mathrm{Gal}(L_w/K_v)$ with the decomposition group $D_{\mathfrak{q}} \subseteq \mathrm{Gal}(L/K)$ via the isomorphism given by part (6) of Theorem 11.20.

Notice that the embedding $\mathrm{Gal}(L_w/K_v) \hookrightarrow \mathrm{Gal}(L/K)$ is the same for every $w|v$: this is obvious in the archimedean case, and in the nonarchimedean case the decomposition groups $D_{\mathfrak{q}}$ are necessarily conjugate in $\mathrm{Gal}(L/K)$, hence equal, since $\mathrm{Gal}(L/K)$ is abelian.

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

$$\begin{aligned} K_v^\times &\hookrightarrow \mathbb{I}_K \\ \alpha &\mapsto (1, 1, \dots, 1, \alpha, 1, 1, \dots), \end{aligned}$$

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

$$\begin{array}{ccc} L_w^\times & \xrightarrow{\mathrm{N}_{L_w/K_v}} & K_v^\times \\ \downarrow & & \downarrow \\ \mathbb{I}_L & \xrightarrow{\mathrm{N}_{L/K}} & \mathbb{I}_K \end{array}$$

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

$$\begin{aligned} \theta_{L/K} \colon \mathbb{I}_K &\to \mathrm{Gal}(L/K) \\ (a_v) &\mapsto \prod_v \theta_{L_w/K_v}(a_v), \end{aligned}$$

where the product takes place in $\mathrm{Gal}(L/K)$ via the embeddings $\mathrm{Gal}(L_w/K_v) \hookrightarrow \mathrm{Gal}(L/K)$ defined above. The value of $\theta_{L_w/K_v}(a_v)$ is independent of our choice of w because the embeddings are the same for every $w|v$, 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 $\mathrm{Gal}_{L_w/K_v} \simeq \langle \mathrm{Frob}_{L_w/K_v} \rangle$ and therefore

$$\theta_{L_w/K_v}(a_v) = \mathrm{Frob}_{L_w/K_v}^{v(a_v)} = 1,$$

since $\theta_{L_w/K_v}(\pi) = \mathrm{Frob}_{L_w/K_v}$ for any uniformizer π of $\mathcal{O}_v$. It is clear that $\theta_{L/K}$ is a homomorphism, since each θ_{L_w/K_v} is, and $\theta_{L/K}$ is continuous because its kernel is a basic open set $\prod_{v|\,\mathrm{disc}_{L/K}} U_v \times \prod_{v\nmid \mathrm{disc}_{L/K}} \mathcal{O}_v^\times$ of $\mathbb{I}_K$.

If $L_1 \subseteq L_2$ are two finite abelian extensions of K, then then $\theta_{L_2/K}(x)_{|_{L_1}} = \theta_{L_1/K}(x)$ for all $x \in \mathbb{I}_K$. The $\theta_{L/K}$ form a compatible system of homomorphisms from $\mathbb{I}_K$ to the inverse

limit $\varprojlim_L \mathrm{Gal}(L/K) \simeq \mathrm{Gal}(K^{\mathrm{ab}}/K)$, 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 26.2. Let K be a global field. The *global Artin homomorphism* is the continuous homomorphism

$$\theta_K \colon \mathbb{I}_K \to \varprojlim_{\substack{L \subseteq K^{\mathrm{ab}} \\ L/K \text{finite}}} \mathrm{Gal}(L/K) \simeq \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

defined by the compatible system of homomorphisms $\theta_{L/K} \colon \mathbb{I}_K \to \mathrm{Gal}(L/K)$.

The isomorphism $\mathrm{Gal}(K^{\mathrm{ab}}/K) \simeq \varprojlim \mathrm{Gal}(L/K)$ is the natural isomorphism between a Galois group and its profinite completion with respect to the Krull topology (Theorem 24.21) and is thus canonical, as is the global Artin homomorphism $\theta_K \colon \mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$.

Proposition 26.3. *Let K be global field. The global Artin homomorphism θ_K is the unique continuous homomorphism $\mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ 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*

$$\begin{array}{ccc} K_v^\times & \xrightarrow{\theta_{L_w/K_v}} & \mathrm{Gal}(L_w/K_v) \\ \downarrow & & \downarrow \\ \mathbb{I}_K & \xrightarrow{\theta_{L/K}} & \mathrm{Gal}(L/K) \end{array}$$

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

Proof. That θ_K has this property follows directly from its construction. Now suppose $\theta'_K \colon \mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ has the same property. The idele group $\mathbb{I}_K$ is generated by the images of the embeddings $K_v^\times$, so if θ_K and θ'_K are not identical, then they disagree at a point $a := (1, 1, \dots, 1, a_v, 1, 1, \dots)$ in the image of one the embeddings $K_v \hookrightarrow \mathbb{I}_K$. We must have $\theta_{L/K}(a) = \theta_{L_w/K_v}(a_v) = \theta'_{L/K}(a)$ for every finite abelian extension L/K in K^{ab} and every place w of L extending v. This implies that $\theta_K(a) = \theta'_K(a)$, since the image of a under any homomorphism to $\mathrm{Gal}(K^{\mathrm{ab}}/K) \simeq \varprojlim \mathrm{Gal}(L/K)$ is determined by its images in the $\mathrm{Gal}(L/K)$, by Theorem 24.21 and the universal property of the profinite completion. □

26.3 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 $K_v^\times$ plays in local Artin reciprocity (Theorem 25.2).

Theorem 26.4 (Global Artin Reciprocity)**.** *Let K be a global field. The kernel of the global Artin homomorphism θ_K contains $K^\times$, and we thus have a continuous homomorphism*

$$\theta_K \colon C_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K),$$

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

$$\theta_{L/K} \colon C_K \to \mathrm{Gal}(L/K)$$

obtained by composing θ_K with the quotient map $\mathrm{Gal}(K^{\mathrm{ab}}/K) \to \mathrm{Gal}(L/K)$ is surjective with kernel $\mathrm{N}_{L/K}(C_L)$. and thus induces an isomorphism $C_K/\mathrm{N}_{L/K}(C_L) \simeq \mathrm{Gal}(L/K)$.

Remark 26.5. When K is a number field, θ_K is surjective but not injective; its kernel is the connected component of the identity in C_K. When K is a global function field, θ_K is injective but not surjective; its image is consists of automorphisms $\sigma \in \mathrm{Gal}(K^{\mathrm{ab}}/K)$ corresponding to integer powers of the Frobenius automorphism of $\mathrm{Gal}(k^{\mathrm{sep}}/k)$, where k is the constant field of K (this is precisely the dense image of $\mathbb{Z}$ in $\widehat{\mathbb{Z}} \simeq \mathrm{Gal}(k^{\mathrm{sep}}/k)$).

We also have a global existence theorem.

Theorem 26.6 (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 inside K^{ab} for which $\mathrm{N}_{L/K}(C_L) = H$.*

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 26.7 (Main theorem of global class field theory)**.** *Let K be a global field. The global Artin homomorphism θ_K induces a canonical isomorphism*

$$\widehat{\theta}_K \colon \widehat{C_K} \xrightarrow{\sim} \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

of profinite groups.

We have an inclusion reversing bijection

$$\begin{aligned} \{ \text{ finite index open subgroups } H \text{ of } C_K \} &\longleftrightarrow \{ \text{ finite abelian extensions } L/K \text{ in } K^{\mathrm{ab}} \} \\ H &\mapsto (K^{\mathrm{ab}})^{\theta_K(H)} \\ \theta_K^{-1}(\mathrm{Gal}(K^{\mathrm{ab}}/L)) &\hookleftarrow L \end{aligned}$$

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

Theorem 26.8 (Functoriality)**.** *Let K be a global field and let L/K be any finite separable extension (not necessarily abelian). Then the following diagram commutes*

$$\begin{array}{ccc} C_L & \xrightarrow{\theta_L} & \mathrm{Gal}(L^{\mathrm{ab}}/L) \\ \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle \mathrm{res}} \\ C_K & \xrightarrow{\theta_K} & \mathrm{Gal}(K^{\mathrm{ab}}/K). \end{array}$$

26.4 Relation to ideal-theoretic version of global class field theory

Let K be a global field and let $\mathfrak{m} \colon M_K \to \mathbb{Z}_{\geq 0}$ be a modulus for K, which we view as a formal product $\mathfrak{m} = \prod_v v^{e_v}$ 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 21.1). For each place v we define the open subgroup

$$U_K^{\mathfrak{m}}(v) := \begin{cases} \mathcal{O}_v^\times & \text{if } v \nmid \mathfrak{m}, \text{ where } \mathcal{O}_v^\times := K_v^\times \text{ when } v \text{ is infinite}), \\ \mathbb{R}_{>0} & \text{if } v|\mathfrak{m} \text{ is real, where } \mathbb{R}_{>0} \subseteq \mathbb{R}^\times \simeq \mathcal{O}_v^\times := K_v^\times, \\ 1 + \mathfrak{p}^{e_v} & \text{if } v|\mathfrak{m} \text{ is finite, where } \mathfrak{p} = \{x \in \mathcal{O}_v : |x|_v < 1\}, \end{cases}$$

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

$$C_K^{\mathfrak{m}} := \mathbb{I}_K/(U_K^{\mathfrak{m}} \cdot K^\times) = C_K/\overline{U}_K^{\mathfrak{m}},$$

and we have isomorphisms

$$C_K^{\mathfrak{m}} \simeq \mathrm{Cl}_K^{\mathfrak{m}} \simeq \mathrm{Gal}(K(\mathfrak{m})/K),$$

where $\mathrm{Cl}_K^{\mathfrak{m}}$ is the ray class group for the modulus $\mathfrak{m}$ (see Definition 21.2), and $K(\mathfrak{m})$ is the corresponding *ray class field*, which we can now define as the finite abelian extension L/K for which $\mathrm{N}_{L/K}(C_L) = \overline{U}_K^{\mathfrak{m}}$, whose existence is guaranteed by Theorem 26.6.

If L/K is any finite abelian extension, then $\mathrm{N}_{L/K}(C_L)$ contains $\overline{U}_L^{\mathfrak{m}}$ for some modulus $\mathfrak{m}$; this follows from the fact that the groups $\overline{U}_L^{\mathfrak{m}}$ form a fundamental system of open neighborhoods of the identity. Indeed, the conductor of the extension L/K (see Definition 22.18) is precisely the minimal modulus $\mathfrak{m}$ for which this is true. It follows that every finite abelian extension L/K lies in a ray class field $K(\mathfrak{m})$ with $\mathrm{Gal}(L/K)$ isomorphic to a quotient of a ray class group $C_K^{\mathfrak{m}}$.

26.5 The Chebotarev density theorem

We now give a proof of the Chebotarev density theorem, a generalization of the Frobenius density theorem you proved on Problem Set 10. Recall from Lecture 17 (and Problem Set 9) that if S is a set of primes of a global field K, the *Dirichlet density* of S is defined by

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

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). A subset C of a group is said to be *stable under conjugation* if $\sigma\tau\sigma^{-1} \in C$ for all $\sigma \in G$ and $\tau \in C$.

Theorem 26.9 (Chebotarev density theorem)**.** *Let L/K be a finite Galois extension of number fields with Galois group $G := \mathrm{Gal}(L/K)$. Let $C \subseteq G$ be stable under conjugation, and let S be the set of primes $\mathfrak{p}$ of K unramified in L with $\mathrm{Frob}_{\mathfrak{p}} \subseteq C$. Then $d(S) = \#C/\#G$.*

Note that G is not assumed to be abelian, so $\mathrm{Frob}_{\mathfrak{p}}$ is a conjugacy class. However, the main difficulty in proving the Chebotarev density theorem (and the only place where class field theory is actually needed) occurs when G is abelian in which case $\mathrm{Frob}_{\mathfrak{p}}$ contains a single element. The main result we need is the generalization of Dirichlet's theorem on primes in arithmetic progressions to number fields, which we proved in Lecture 22, subject to the existence of ray class fields, which for convenience we now assume.[1]

Proposition 26.10. *Let $\mathfrak{m}$ be a modulus for a number field K and let $\mathrm{Cl}_K^{\mathfrak{m}}$ be the corresponding ray class group. For every ray class $c \in \mathrm{Cl}_K^{\mathfrak{m}}$ the Dirichlet density of the set of primes $\mathfrak{p}$ of K that lie in c is $1/\#\mathrm{Cl}_K^{\mathfrak{m}}$.*

[1] 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 ζ is a primitive root of unity, which removes the need to assume the existence of ray class fields; see [4] for details.

Proof. This follows from Theorem 26.6, which guarantees that the ray class field $K(\mathfrak{m})$ exists, and Theorem 22.14, Corollary 22.15, and Corollary 22.17, from Lecture 22. □

Corollary 26.11. *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 unramified primes $\mathfrak{p}$ of K for which $\mathrm{Frob}_\mathfrak{p} = \{\sigma\}$ is $1/\#G$.*

Proof. Let $\mathfrak{m} = \mathrm{cond}(L/K)$ be the conductor of the extension L/K; then L is a subfield of the ray class field $K(\mathfrak{m})$ and $\mathrm{Gal}(L/K) \simeq \mathrm{Cl}_K^\mathfrak{m}/H$ for some subgroup H of the ray class group. For each unramified prime $\mathfrak{p}$ of K we have $\mathrm{Frob}_\mathfrak{p} = \{\sigma\}$ if and only if $\mathfrak{p}$ lies in one of the ray classes contained in the coset of H in $\mathrm{Cl}_K^\mathfrak{m}/H$ corresponding to σ. The Dirichlet density of the set of primes in each ray class is $1/\#\mathrm{Cl}_K^\mathfrak{m}$, by Proposition 26.10, and there are $\#H$ ray classes in each coset of H; thus $d(S) = \#H/\#\mathrm{Cl}_K^\mathfrak{m} = 1/\#G$. □

Proof of the Chebotarev density theorem. It suffices to prove the case where C is a single conjugacy class, since we can reduce to this case by partitioning C into conjugacy classes and summing Dirichlet densities (as proved on Problem Set 9). If L/K is abelian then $\#C = 1$ and the theorem follows from Corollary 26.11.

For the general case, let σ be a representative of the conjugacy class C, let $H = \langle\sigma\rangle$ be the subgroup of G it generates, and let $F = L^H$ be the corresponding fixed field. Let T be the set of primes $\mathfrak{q}$ of F that are unramified in L for which the Frobenius class $\mathrm{Frob}_\mathfrak{q} = \{\sigma\}$ (where $\mathrm{Frob}_\mathfrak{q} \subseteq \mathrm{Gal}(L/F) \subseteq \mathrm{Gal}(L/K)$). The extension L/F is abelian with Galois group H, so $d(T) = 1/\#H$, by Corollary 26.11. 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 by their subsets of degree-1 primes.

Claim: For each prime $\mathfrak{p} \in S$ exactly $\#G/(\#H\#C)$ primes $\mathfrak{q} \in T$ lie above $\mathfrak{p}$.

Assuming the claim, we have

$$\sum_{\mathfrak{p}\in S} \mathrm{N}(\mathfrak{p})^{-s} = \frac{\#H\#C}{\#G} \sum_{\mathfrak{q}\in T} \mathrm{N}(\mathfrak{q})^{-s},$$

since $\mathrm{N}(\mathfrak{q}) = \mathrm{N}(\mathfrak{p})$ for each degree-1 prime $\mathfrak{q}$ lying above a degree-1 prime $\mathfrak{p}$, and therefore

$$d(S) = \frac{\#H\#C}{\#G} d(T) = \frac{\#C}{\#G}$$

as desired.

Proof of claim: Let U be the set of primes $\mathfrak{r}$ of L for which $\mathfrak{r} \cap K = \mathfrak{p} \in S$ and $\mathrm{Frob}_{\mathfrak{r}/\mathfrak{p}} = \sigma$. For each $\mathfrak{r} \in U$, if we put $\mathfrak{q} := \mathfrak{r} \cap F$ then $\mathrm{Frob}_\mathfrak{q} = \{\sigma\}$, and since σ fixes F it acts trivially on $\mathbb{F}_\mathfrak{q} := \mathcal{O}_F/\mathfrak{q}$, so the residue field extension $\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p}$ is trivial and $\mathfrak{q} \in T$. On the other hand, $\mathrm{Gal}(L/F) = \langle\sigma\rangle = H$, so the residue field extension $\mathbb{F}_\mathfrak{r}/\mathbb{F}_\mathfrak{q}$ has degree $\#H$, and this implies that $\mathfrak{r}$ is the only prime of L above $\mathfrak{q}$. Conversely, for each $\mathfrak{q} \in T$, every prime $\mathfrak{r}$ of L above $\mathfrak{q}$ must have $\mathrm{Frob}_r = \sigma$, hence lie in U, and have residue degree $[\mathbb{F}_\mathfrak{r} : \mathbb{F}_\mathfrak{q}] = \#H$, hence be the unique prime of L above $\mathfrak{q}$.

The sets U and T are thus in bijection, so to count the primes $\mathfrak{q} \in T$ that lie above some prime $\mathfrak{p} \in S$ it suffices to count the primes $\mathfrak{r} \in U$ that lie above $\mathfrak{p}$. The set X of primes $\mathfrak{r}$ of L that lie above $\mathfrak{p}$ has cardinality $\#G/\#H$, since the primes $\#r$ are all unramified and have residue degree $\#H$. The transitive action of G on X partitions it into $\#C$ orbits corresponding to the conjugates of σ, each of which has size $\#G/(\#H\#C)$. Each orbit corresponds to a possible value of $\mathrm{Frob}_\mathfrak{r}$, all of which are conjugate to σ, exactly one of

which is equal to σ; this orbit is the set of primes $\mathfrak{r}$ of L above $\mathfrak{p}$ that lie in U and has cardinality $\#G/(\#H\#C)$, which proves the claim and completes the proof. □

Remark 26.12. 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 (element of the ray class group) have a natural density.

References

[1] Erich Hecke, *Über die L-Funktionen und den Dirichletschen Primzahlsatz für einen beliebigen Zahlkörper*, Nachrichten von der Königlichen Gesellschaft der Wissenschaften zu Göttingen, Mathematisch–Physikalische Klasse (1917) 299–318.

[2] Michiel Kosters, *A short proof of a Chebotarev density theorem for function fields*, arXiv:1404.6345.

[3] Hans Reichardt, *Der Primdivisorsatz für algebraische Funktionenkörper über einem endlichen Konstantenkörper*, Mathematische Zeitschrift **40** (1936) 713–719.

[4] Peter Stevenhagen and H.W. Lenstra Jr., *Chebotarev and his density theorem*, Math. Intelligencer **18** (1996), 26–37.

18.785 Number Theory I
Fall 2016