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* $\mathbb{A}_K$ of a global field K as the restricted product

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

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, $\mathbb{A}_K$ 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 25.12.

In Lecture 26 we defined the *idele group*

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

which coincides with the unit group of $\mathbb{A}_K$ 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

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

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 finite place v corresponding to the absolute value $\|\ \|_\mathfrak{p}$. We have the following commutative diagram of exact sequences:

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

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.

Lecture by Andrew V. Sutherland

Definition 28.1. 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 11.24 and Remark 11.25 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 6.6), and we have 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 have a commutative square

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

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^{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 27.2, each local field K_v is equipped with a local Artin homomorphism

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

For each finite abelian extension L/K and each place $w|v$ of L, composing θ_{K_v} with the natural map $\mathrm{Gal}(K_v^{\mathrm{ab}}/K_v) \to \mathrm{Gal}(L_w/K_v)$ yields 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 have $\theta_{L_w/K_v}(\pi_v) = \mathrm{Frob}_{L_w/K_v}$ for all uniformizers π_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

$$\begin{aligned}\varphi_w\colon \mathrm{Gal}(L_w/K_v) &\hookrightarrow \mathrm{Gal}(L/K)\\ \sigma &\mapsto \sigma_{|L}\end{aligned}$$

The map φ_w is well defined and injective because every element of L_w can be written as ℓx 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 $\sigma \in \mathrm{Gal}(L_w/K_v)$ is uniquely determined by its action on L, which fixes $K \subseteq K_v$. If v is archimedean then $\varphi_w(\mathrm{Gal}(L_w/K_v))$ is either trivial or generated by the involution corresponding to complex conjugation in $L_w \simeq \mathbb{C}$. If v is a finite place and $\mathfrak{q}$ is the prime of L corresponding to $w|v$, then $\varphi_w(\mathrm{Gal}(L_w/K_v))$ is the decomposition group $D_{\mathfrak{q}} \subseteq \mathrm{Gal}(L/K)$; this follows from parts (5) and (6) of Theorem 11.23.

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

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

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

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

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

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

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

where the product takes place in $\mathrm{Gal}(L/K)$. 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

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

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 $a := (a_v) \in \ker \theta_{L/K}$ lies in an open set

$U_a := U_S \times \prod_{v \notin S} \mathcal{O}_v^\times \subseteq \ker \theta_{L/K}$, where S contains all ramified v and all v for which $a_v \notin \mathcal{O}_v^\times$, and U_S is the kernel of $(a_v)_{v \in S} \mapsto \prod_{v \in S} \varphi_w(\theta_{L_w/K_v}(a_v)))$, 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 $a \in \mathbb{I}_K$. 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 28.2. Let K be a global field. The *global Artin homomorphism* is the continuous homomorphism

$$\theta_K \colon \mathbb{I}_K \to \varprojlim_L \mathrm{Gal}(L/K) \simeq \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

defined by the compatible system of homomorphisms $\theta_{L/K} \colon \mathbb{I}_K \to \mathrm{Gal}(L/K)$, where L ranges over finite abelian extensions of K in K^{ab}.

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 26.23) and is thus canonical, as is the global Artin homomorphism $\theta_K \colon \mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$.

Proposition 28.3. *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*

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

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

Proof. That θ_K has this property follows from its construction. Now suppose that there is another continuous homomorphism $\theta'_K \colon \mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ with the same property. We may view elements of $\mathrm{Gal}(K^{\mathrm{ab}}/K) \simeq \varprojlim \mathrm{Gal}(L/K)$ as elements of $\prod_{L/K} \mathrm{Gal}(L/K)$, where L varies over finite abelian extensions of K in K^{ab}. If θ_K and θ'_K are not identical, then there must be an $a \in \mathbb{I}_K$ 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 $a_v \notin \mathcal{O}_v^\times$ and all ramified places of L/K. Define $b \in \mathbb{I}_K$ by $b_v := 1$ for $v \in S$ and $b_v := a_v$ for $v \notin S$, so that $a = b \prod_{v \in S} \iota_v(a_v)$. Then $\theta_{L_w/K_v}(b_v) = 1$ for all places v, so we must have $\theta_{L/K}(b) = 1 = \theta'_{L/K}(b)$, and for $v \in S$ we have

$$\theta_{L/K}(\iota_v(a_v)) = \varphi_w(\theta_{L_w/K_v}(a_v)) = \theta'_{L/K}(\iota_v(a_v)),$$

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 $\theta'_K = \theta_K$ 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 $K_v^\times$ 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 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 natural map $\mathrm{Gal}(K^{\mathrm{ab}}/K) \twoheadrightarrow \mathrm{Gal}(L/K)$ is surjective with kernel $\mathrm{N}_{L/K}(C_L)$, inducing an isomorphism $C_K/\mathrm{N}_{L/K}(C_L) \simeq \mathrm{Gal}(L/K)$.

Remark 28.5. When K is a number field, θ_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, θ_K is injective but not surjective; its image is dense in $\mathrm{Gal}(K^{\mathrm{ab}}/K)$.

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 $\mathrm{N}_{L/K}(C_L) = H$.*

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 28.7 (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 then have an inclusion reversing bijection

$$\{\,\text{finite index open subgroups } H \text{ of } C_K\,\} \longleftrightarrow \{\,\text{finite abelian extensions } L/K \text{ in } K^{\mathrm{ab}}\,\}$$
$$H \mapsto (K^{\mathrm{ab}})^{\theta_K(H)}$$
$$\mathrm{N}_{L/K}(C_L) \mapsfrom L$$

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 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*

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

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

Let K be a number field and let $\mathfrak{m}\colon M_K \to \mathbb{Z}_{\ge 0}$ 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 $e_v \le 1$ 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

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

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

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

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 21.3), 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 28.6.

If L/K is any finite abelian extension, then $\mathrm{N}_{L/K}(C_L)$ contains $\overline{U}_K^{\mathfrak{m}}$ for some modulus $\mathfrak{m}$; this follows from the fact that the groups $\overline{U}_K^{\mathfrak{m}}$ 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 $\mathfrak{m}$ 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 $C_K^{\mathfrak{m}}$.

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

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

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).

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 $G := \mathrm{Gal}(L/K)$. 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, 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 $\mathrm{Frob}_{\mathfrak{p}}$ 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 $\mathfrak{m}$ 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 $1/\#\mathrm{Cl}_K^{\mathfrak{m}}$.*

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

The Chebotarev density theorem for abelian extensions follows from Proposition 28.10 and the existence of ray class fields, which we now assume.[1]

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 $\mathfrak{p}$ of K unramified in L 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 28.10, and there are $\#H$ ray classes in each coset of H; thus $d(S) = \#H/\#\mathrm{Cl}_K^{\mathfrak{m}} = 1/\#G$. □

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 $\mathfrak{p}$ of K unramified in L for which $\mathrm{Frob}_{\mathfrak{p}}$ 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_σ be the set of primes $\mathfrak{q}$ of F_σ unramified in L for which $\mathrm{Frob}_{\mathfrak{q}} = \{\sigma\} \subseteq \mathrm{Gal}(L/F_\sigma) \subseteq \mathrm{Gal}(L/K)$ (note that the Frobenius class $\mathrm{Frob}_{\mathfrak{q}}$ is a singleton because $\mathrm{Gal}(L/F_\sigma) = H_\sigma$ is abelian). We have $d(T_\sigma) = 1/\#H_\sigma$, since L/F_σ is abelian, by Corollary 28.11.[2]

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_σ by their subsets of degree-1 primes, and define $T_\sigma(\mathfrak{p}) \coloneqq \{\mathfrak{q} \in T_\sigma : \mathfrak{q}|\mathfrak{p}\}$ for each $\mathfrak{p} \in S$.

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

Proof of claim: Let $\mathfrak{r}$ be a prime of L lying above $\mathfrak{q} \in T_\sigma(\mathfrak{p})$. Such an $\mathfrak{r}$ is unramified, since $\mathfrak{p}$ is, and we have $\mathrm{Frob}_{\mathfrak{r}} = \sigma$, since $\mathrm{Frob}_{\mathfrak{q}} = \{\sigma\}$. It follows that $\mathrm{Gal}(\mathbb{F}_{\mathfrak{r}}/\mathbb{F}_{\mathfrak{q}}) = \langle\bar\sigma\rangle \simeq H_\sigma$.

[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.

[2] Note that the integers $\#H_\sigma$ and $[G : H_\sigma]$ do not depend on the choice of σ (the H_σ are all conjugate).

Therefore $f_{\mathfrak{r}/\mathfrak{q}} = \#H_\sigma$ and $\#\{\mathfrak{r}|\mathfrak{q}\} = 1$, since $\#H_\sigma = [L : F_\sigma] = \sum_{\mathfrak{r}|\mathfrak{q}} e_{\mathfrak{r}/\mathfrak{q}} f_{\mathfrak{r}/\mathfrak{q}}$. We have $f_{\mathfrak{r}/\mathfrak{p}} = f_{\mathfrak{r}/\mathfrak{q}} f_{\mathfrak{q}/\mathfrak{p}} = f_{\mathfrak{r}/\mathfrak{q}} = \#H_\sigma$, since $f_{\mathfrak{q}/\mathfrak{p}} = 1$ for degree-1 primes $\mathfrak{q}|\mathfrak{p}$, and $e_{\mathfrak{r}/\mathfrak{p}} = 1$, thus

$$\#G = [L : K] = \sum_{\mathfrak{r}|\mathfrak{p}} e_{\mathfrak{r}/\mathfrak{p}} f_{\mathfrak{r}/\mathfrak{p}} = \#\{\mathfrak{r}|\mathfrak{p}\}\#H_\sigma = \#T_\sigma(\mathfrak{p})\#H_\sigma,$$

so $\#T_\sigma(\mathfrak{p}) = \#G/\#H_\sigma = [G : H_\sigma]$ as claimed.

We now observe that

$$\sum_{\mathfrak{p}\in S} \mathrm{N}(\mathfrak{p})^{-s} = \sum_{\sigma\in C} \sum_{\mathfrak{p}\in S} \frac{1}{[G : H_\sigma]} \sum_{\mathfrak{q}\in T_\sigma(\mathfrak{p})} \mathrm{N}(\mathfrak{q})^{-s} = \frac{\#C}{[G : H_\sigma]} \sum_{\mathfrak{q}\in T_\sigma} \mathrm{N}(\mathfrak{q})^{-s}$$

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

$$d(S) = \frac{\#C}{[G : H_\sigma]} d(T_\sigma) = \frac{\#C}{[G : H_\sigma]\#H_\sigma} = \frac{\#C}{\#G}. \qquad \square$$

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

[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 2021