18.785 Number theory I — Fall 2016
Lecture #22 — 11/29/2016

22 The main theorems of global class field theory

In this lecture we refine the correspondence between quotients of ray class groups and subfields of ray class fields given by the Artin map so that we can more precisely state the main theorems of global class field theory in their ideal-theoretic form. Let us first recall the notational setup.

We have a number field K and a modulus $\mathfrak{m}\colon M_K \to \mathbb{Z}_{\geq 0}$ that we view as a formal product over the places of K; we may write $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, where $\mathfrak{m}_0 \coloneqq \prod \mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}$ is a product over primes (finite places) of K and $\mathfrak{m}_\infty \coloneqq \prod_{v|\infty} v^{\mathfrak{m}(v)}$ defines a subset of the real places of K (recall that for $v|\infty$ we have $\mathfrak{m}(v) \leq 1$ with $\mathfrak{m}(v) = 0$ if v is complex). We then define

- $\mathcal{I}_K^{\mathfrak{m}} \subseteq \mathcal{I}_K$, the subgroup of fractional ideals prime to $\mathfrak{m}$;
- $K^{\mathfrak{m}} \subseteq K^\times$, the subgroup of $\alpha \in K^\times$ for which $(\alpha) \in \mathcal{I}_K^{\mathfrak{m}}$;
- $K^{\mathfrak{m},1} \subseteq K^{\mathfrak{m}}$, the subgroup of $\alpha \in K^{\mathfrak{m}}$ for which $v_{\mathfrak{p}}(\alpha - 1) \geq v_{\mathfrak{p}}(\mathfrak{m}_0)$ for $\mathfrak{p}|\mathfrak{m}_0$ and $\alpha_v > 0$ for $v|\mathfrak{m}_\infty$ (here $\alpha_v \in \mathbb{R}$ is the image of α under the real-embedding v);
- $\mathcal{R}_K^{\mathfrak{m}} \subseteq \mathcal{I}_K^{\mathfrak{m}}$ the subgroup of ideals $(\alpha) \in \mathcal{I}_K^{\mathfrak{m}}$ with $\alpha \in K^{\mathfrak{m},1}$ (the *ray group*);
- $\mathrm{Cl}_K^{\mathfrak{m}} \coloneqq \mathcal{I}_K^{\mathfrak{m}}/\mathcal{R}_K^{\mathfrak{m}}$ (the *ray class group*);
- $\mathrm{Spl}(L) \coloneqq \mathrm{Spl}(L/K)$, the set of primes of K that split completely in an extension L;
- $\psi_{L/K}^{\mathfrak{m}}\colon \mathcal{I}_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$, the Artin map for an abelian extension L/K.

In the previous lecture we defined the *ray class field* of K for the modulus $\mathfrak{m}$ as a finite abelian extension L/K unramified outside of $\mathfrak{m}$ for which the kernel of the Artin map $\psi_{L/K}^{\mathfrak{m}}$ is equal to the the ray group $\mathcal{R}_K^{\mathfrak{m}}$. A prime $\mathfrak{p} \nmid \mathfrak{m}$ lies in the kernel of $\psi_{L/K}^{\mathfrak{m}}$ if and only if it splits completely in L (for unramified primes $\mathfrak{p}$ in an abelian extension to split completely is to have residue field degree 1, in which case the Frobenius element $\sigma_{\mathfrak{p}}$ is trivial). Thus

$$\{\mathfrak{p} \in \mathcal{R}_K^{\mathfrak{m}}\} \sim \mathrm{Spl}(L)$$

(recall $S \sim T$ means $T - S$ and $S - T$ are finite), and Theorem 21.16 implies that the ray group uniquely determines the ray class field (assuming it exists); we will use $K(\mathfrak{m})$ to denote the ray class field. The Artin map $\psi_{K(\mathfrak{m})/K}^{\mathfrak{m}}$ induces a canonical isomorphism

$$\mathrm{Cl}_K^{\mathfrak{m}} = \mathcal{I}_K^{\mathfrak{m}}/\mathcal{R}_K^{\mathfrak{m}} \simeq \mathrm{Gal}(K(\mathfrak{m})/K)$$

between the ray class group $\mathrm{Cl}_K^{\mathfrak{m}}$ and the Galois group of the ray class field.

More generally, if $L \subseteq K(\mathfrak{m})$ is any subfield of the ray class field, the kernel of the Artin map $\psi_{L/K}^{\mathfrak{m}}$ is a subgroup $\mathcal{C}$ of $\mathcal{I}_K^{\mathfrak{m}}$ that contains the ray group

$$\mathcal{R}_K^{\mathfrak{m}} \subseteq \mathcal{C} \subseteq \mathcal{I}_K^{\mathfrak{m}},$$

and we have an isomorphism

$$\mathcal{I}_K^{\mathfrak{m}}/\mathcal{C} \simeq \mathrm{Cl}_K^{\mathfrak{m}}/\overline{\mathcal{C}} \simeq \mathrm{Gal}(L/K)$$

where $\overline{\mathcal{C}}$ denotes the image of $\mathcal{C}$ in $\mathrm{Cl}_K^{\mathfrak{m}} = \mathcal{I}_K^{\mathfrak{m}}/\mathcal{R}_K^{\mathfrak{m}}$ under the quotient map.

Before proceeding, let us be clear on what we have and have not proved so far. In the previous lecture we proved that the Artin map is surjective (Theorem 21.17), and we *defined* the ray class field $K(\mathfrak{m})$ to be an extension L/K for which $\ker\psi^{\mathfrak{m}}_{L/K} = \mathcal{R}^{\mathfrak{m}}_K$. We have not proved (nor will we prove) that such a field $K(\mathfrak{m})$ exists, but if it does, we know that it is uniquely determined and depends only on the field K and the modulus $\mathfrak{m}$.

Assuming $K(\mathfrak{m})$ exists, if L is a subfield of $K(\mathfrak{m})$ then $\ker\psi^{\mathfrak{m}}_{L/K}$ is a subgroup of $\mathcal{I}^{\mathfrak{m}}_K$ containing $\mathcal{R}^{\mathfrak{m}}_K$ (a *congruence subgroup*, as defined below). To prove that every abelian extension L/K lies in some ray class field $K(\mathfrak{m})$ it is enough to show that $\ker\psi^{\mathfrak{m}}_{L/K}$ contains $\mathcal{R}^{\mathfrak{m}}_K$ for some modulus $\mathfrak{m}$, since then $\operatorname{Spl}(K(\mathfrak{m})) \precsim \operatorname{Spl}(L)$ and therefore $L \subseteq K(\mathfrak{m})$, by Theorem 21.16. This is the other half of *Artin reciprocity* (the hard half), which together with the existence of the ray class fields $K(\mathfrak{m})$ is one of the main theorems of class field theory. In this lecture we want to better understand the structure of congruence subgroups, and to specify a minimal modulus $\mathfrak{m}$ for which we should expect a given finite abelian extension L/K to lie in a subfield of the ray class field $K(\mathfrak{m})$ (the *conductor* of the extension). So far we have not addressed this question even for $K = \mathbb{Q}$ (but see Problem Set 9); our proof of the Kronecker-Weber theorem showed that every abelian extension lies in some cyclotomic field $\mathbb{Q}(\zeta_m)$, but we made no attempt to determine such an integer m (or more precisely, a modulus $\mathfrak{m}$ of the form $\mathfrak{m} = (m)\infty$ or $\mathfrak{m} = (m)$).

22.1 Congruence subgroups

Our presentation here is adapted from [1, §3.3] but our notation differs slightly.

Definition 22.1. Let K be a number field and let $\mathfrak{m}$ be a modulus for K. A *congruence subgroup* (for the modulus $\mathfrak{m}$) is a subgroup $\mathcal{C}$ of $\mathcal{I}^{\mathfrak{m}}_K$ that contains $\mathcal{R}^{\mathfrak{m}}_K$. We write $\overline{\mathcal{C}}$ for the image of $\mathcal{C}$ in $\mathcal{I}^{\mathfrak{m}}_K/\mathcal{R}^{\mathfrak{m}}_K = \operatorname{Cl}^{\mathfrak{m}}_K$ under the quotient map.

As noted above, congruence subgroups are the groups we expect to arise as the kernel of an Artin map $\psi^{\mathfrak{m}}_{L/K}\colon I^{\mathfrak{m}}_K \to \operatorname{Gal}(L/K)$ associated to a finite abelian extension L/K, for a suitable choice of the modulus $\mathfrak{m}$. In general the modulus $\mathfrak{m}$ that we use to define $\psi^{\mathfrak{m}}_{L/K}$ may be any modulus divisible by all the primes of K that ramify in L, and if we have one modulus $\mathfrak{m}$ for which $\mathcal{R}^{\mathfrak{m}}_K \subseteq \ker\psi^{\mathfrak{m}}_{L/K}$ (so $\ker\psi^{\mathfrak{m}}_{L/K}$ is in fact a congruence subgroup), then every modulus divisible by $\mathfrak{m}$ will have the same property (making $\mathfrak{m}$ bigger make $\mathcal{R}^{\mathfrak{m}}_K$ smaller which makes it easier for $\ker^{\mathfrak{m}}_{L/K}$ to contain $\mathcal{R}^{\mathfrak{m}}_K$). For every such $\mathfrak{m}$, if $\mathcal{C} = \ker\psi^{\mathfrak{m}}_{L/K}$ is a congruence subgroup then we have an isomorphism

$$\mathcal{I}^{\mathfrak{m}}_K/\mathcal{C} \simeq \operatorname{Cl}^{\mathfrak{m}}_K/\overline{\mathcal{C}} \simeq \operatorname{Gal}(L/K)$$

that allow us to view L as a subfield of the ray class field $K(\mathfrak{m})$; namely, the unique subfield L of $K(\mathfrak{m})$ for which $\operatorname{Spl}(L) \sim \{\mathfrak{p} : \mathfrak{p} \in \mathcal{C}\}$. There are thus infinitely many congruence subgroups associated to each finite abelian extension L/K; we want to define an equivalence relation on congruence subgroups that will put all the congruence subgroups associated to L/K in a single equivalence class, and to distinguish a unique representative for each class.

We should emphasize that the kernel of the Artin map $\psi^{\mathfrak{m}}_{L/K}$ is not always a congruence subgroup. There are constraints on the modulus $\mathfrak{m}$ that must be satisfied beyond the basic requirement that $\mathfrak{m}$ is divisible by all the primes of K that ramify in L. For example, the cyclic cubic extension $L := \mathbb{Q}[x]/(x^3 - 3x - 1)/\mathbb{Q}$ is ramified only at 3 but clearly does not lie in the cyclotomic field $\mathbb{Q}(\zeta_3)$, so the modulus $\mathfrak{m} = (3)\infty$ does not work, but the modulus $\mathfrak{m} = (9)$ does; in fact L is the ray class field of $\mathbb{Q}$ for this modulus. One of our other goals in this lecture is to associate to each abelian extension L/K a minimal modulus $\mathfrak{c}$, the *conductor* of the extension L/K, with the property that $\psi^{\mathfrak{m}}_{L/K}$ is a congruence subgroup whenever $\mathfrak{m}$ is divisible by $\mathfrak{c}$ and otherwise not.

Definition 22.2. Let K be a number field with moduli $\mathfrak{m}_1$ and $\mathfrak{m}_2$. If $\mathcal{C}_1$ is a congruence subgroup for $\mathfrak{m}_1$ and $\mathcal{C}_2$ is a congruence subgroup for $\mathfrak{m}_2$ then we say that $\mathcal{C}_1$ and $\mathcal{C}_2$ are *equivalent* and write $\mathcal{C}_1 \sim \mathcal{C}_2$ whenever

$$\mathcal{I}_K^{\mathfrak{m}_1} \cap \mathcal{C}_2 = \mathcal{I}_K^{\mathfrak{m}_2} \cap \mathcal{C}_1,$$

as subgroups of $\mathcal{I}_K$. Note that if $\mathfrak{m}_1 = \mathfrak{m}_2$ this reduces to $\mathcal{C}_1 = \mathcal{C}_2$.

Proposition 22.3. *Let K be a number field. The relation $\mathcal{C}_1 \sim \mathcal{C}_2$ is an equivalence relation on the set of congruence subgroups in $\mathcal{I}_K$.*

Proof. The relation $\sim$ is clearly reflexive and symmetric. To show that it is transitive, suppose $\mathcal{C}_1 \sim \mathcal{C}_2$ and $\mathcal{C}_2 \sim \mathcal{C}_3$. Let $\mathfrak{a} \in \mathcal{I}_K^{\mathfrak{m}_3} \cap \mathcal{C}_1$ and pick $\alpha \in K^{\mathfrak{m}_1\mathfrak{m}_3,1}$ so that $\alpha\mathfrak{a} \in \mathcal{I}_K^{\mathfrak{m}_1\mathfrak{m}_2\mathfrak{m}_3}$ (this is possible by Lemma 21.5 and Theorem 8.5). Then $(\alpha) \in \mathcal{R}_K^{\mathfrak{m}_1\mathfrak{m}_3} \subseteq \mathcal{R}_K^{\mathfrak{m}_1} \subseteq \mathcal{C}_1$ and $\mathfrak{a} \subseteq \mathcal{C}_1$, so $\alpha\mathfrak{a} \in \mathcal{C}_1$, and we also have $\alpha\mathfrak{a} \in \mathcal{I}_K^{\mathfrak{m}_1\mathfrak{m}_2\mathfrak{m}_3} \subseteq \mathcal{I}_K^{\mathfrak{m}_2}$, so

$$\alpha\mathfrak{a} \in \mathcal{I}_K^{\mathfrak{m}_2} \cap \mathcal{C}_1 = \mathcal{I}_K^{\mathfrak{m}_1} \cap \mathcal{C}_2 \subseteq \mathcal{C}_2,$$

since $\mathcal{C}_1 \sim \mathcal{C}_2$, and $\alpha\mathfrak{a} \in \mathcal{I}_K^{\mathfrak{m}_1\mathfrak{m}_2\mathfrak{m}_3} \subseteq \mathcal{I}_K^{\mathfrak{m}_3}$, so

$$\alpha\mathfrak{a} \in \mathcal{I}_K^{\mathfrak{m}_3} \cap \mathcal{C}_2 = \mathcal{I}_K^{\mathfrak{m}_2} \cap \mathcal{C}_3 \subseteq \mathcal{C}_3,$$

since $\mathcal{C}_2 \sim \mathcal{C}_3$. We have $(\alpha) \in \mathcal{R}_K^{\mathfrak{m}_1\mathfrak{m}_3} \subseteq \mathcal{R}_K^{\mathfrak{m}_3}$, so $(\alpha) \in \mathcal{C}_3$ and therefore $(\alpha)^{-1} \in \mathcal{C}_3$, since $\mathcal{C}_3$ is a group. Thus $\alpha^{-1}\alpha\mathfrak{a} = \mathfrak{a} \in \mathcal{C}_3$, and we also have $\mathfrak{a} \in \mathcal{C}_1 \subseteq \mathcal{I}_K^{\mathfrak{m}_1}$, so $\mathfrak{a} \in \mathcal{I}_K^{\mathfrak{m}_1} \cap \mathcal{C}_3$. This proves that

$$I_K^{\mathfrak{m}_3} \cap \mathcal{C}_1 \subseteq \mathcal{I}_K^{\mathfrak{m}_1} \cap \mathcal{C}_3$$

and the reverse inclusion follows by symmetry (swap $\mathcal{C}_1$ and $\mathcal{C}_3$). Thus $\mathcal{C}_1 \sim \mathcal{C}_3$, which proves transitivity, and $\sim$ is therefore an equivalence relation. □

Within an equivalence class of congruence subgroups there can be at most one congruence subgroup for each modulus (since $\mathcal{C}_1 \sim \mathcal{C}_2 \Leftrightarrow \mathcal{C}_1 = \mathcal{C}_2$ when $\mathcal{C}_1$ and $\mathcal{C}_2$ have the same modulus), thus the partial ordering of moduli by divisibility (where $\mathfrak{m}_1|\mathfrak{m}_2$ means $\mathfrak{m}_1(v) \le \mathfrak{m}_2(v)$ for all $v \in M_K$) induces a partial ordering of the congruence subgroups within an equivalence class. We now show that each equivalence class of congruence subgroups has a unique minimal element under this partial ordering.

Lemma 22.4. *Let $\mathcal{C}_1$ be a congruence subgroup of modulus $\mathfrak{m}_1$ for a number field K. There exists a congruence subgroup $\mathcal{C}_2$ of modulus $\mathfrak{m}_2|\mathfrak{m}_1$ equivalent to $\mathcal{C}_1$ if and only if*

$$\mathcal{I}_K^{\mathfrak{m}_1} \cap P_K^{\mathfrak{m}_2} \subseteq \mathcal{C}_1,$$

in which case $\mathcal{C}_2 = \mathcal{C}_1\mathcal{R}_K^{\mathfrak{m}_2}$.

Proof. Note that $\mathfrak{m}_2|\mathfrak{m}_1$ implies $\mathcal{I}_K^{\mathfrak{m}_1} \subseteq \mathcal{I}_K^{\mathfrak{m}_2}$, so $\mathcal{C}_1 \subseteq \mathcal{I}_K^{\mathfrak{m}_1} \subseteq \mathcal{I}_K^{\mathfrak{m}_2}$.

Suppose $\mathcal{C}_2 \sim \mathcal{C}_1$ has modulus $\mathfrak{m}_2$. Then $\mathcal{I}_K^{\mathfrak{m}_1} \cap \mathcal{C}_2 = \mathcal{I}_K^{\mathfrak{m}_2} \cap \mathcal{C}_1 = \mathcal{C}_1$, and $\mathcal{R}_K^{\mathfrak{m}_2} \subseteq \mathcal{C}_2$, so $\mathcal{I}_K^{\mathfrak{m}_1} \cap \mathcal{R}_K^{\mathfrak{m}_2} \subseteq \mathcal{C}_1$ as claimed. Now suppose $\mathcal{I}_K^{\mathfrak{m}_1} \cap \mathcal{R}_K^{\mathfrak{m}_2} \subseteq \mathcal{C}_1$, and let $\mathcal{C}_2 := \mathcal{C}_1\mathcal{R}_K^{\mathfrak{m}_2}$. Then $\mathcal{C}_2$ is a congruence subgroup of modulus $\mathfrak{m}_2$ and

$$\mathcal{C}_1(I_K^{\mathfrak{m}_1} \cap \mathcal{R}_K^{\mathfrak{m}_2}) = \mathcal{I}_K^{\mathfrak{m}_1} \cap \mathcal{C}_1\mathcal{R}_K^{\mathfrak{m}_2} = \mathcal{I}_K^{\mathfrak{m}_1} \cap \mathcal{C}_2,$$

and $\mathcal{C}_1(\mathcal{I}_K^{\mathfrak{m}_1} \cap \mathcal{R}_K^{\mathfrak{m}_2}) \subseteq \mathcal{C}_1\mathcal{C}_1 = \mathcal{C}_1$, so $\mathcal{I}_K^{\mathfrak{m}_1} \cap \mathcal{C}_2 \subseteq \mathcal{C}_1$; in fact equality holds since $\mathcal{C}_1 \subseteq \mathcal{I}_K^{\mathfrak{m}_1}$ and $\mathcal{C}_1 \subseteq \mathcal{C}_2$. Thus $\mathcal{I}_K^{\mathfrak{m}_1} \cap \mathcal{C}_2 = \mathcal{C}_1 = \mathcal{I}_K^{\mathfrak{m}_2} \cap \mathcal{C}_1$ and $\mathcal{C}_1 \sim \mathcal{C}_2$.

The equivalence class of $\mathcal{C}_1$ contains at most one congruence subgroup of modulus $\mathfrak{m}_2$, so if one exists it must be $\mathcal{C}_2 = \mathcal{C}_1\mathcal{R}_K^{\mathfrak{m}_2}$. □

Proposition 22.5. *Let $\mathcal{C}_1 \sim \mathcal{C}_2$ be congruence subgroups of modulus $\mathfrak{m}_1$ and $\mathfrak{m}_2$, respectively. There exists a congruence subgroup $\mathcal{C} \sim \mathcal{C}_1 \sim \mathcal{C}_2$ with modulus $\mathfrak{n} := \gcd(\mathfrak{m}_1, \mathfrak{m}_2)$.*

Proof. Put $\mathfrak{m} := \operatorname{lcm}(\mathfrak{m}_1, \mathfrak{m}_2)$ and $\mathcal{D} := \mathcal{I}_K^{\mathfrak{m}_2} \cap \mathcal{C}_1 = \mathcal{I}_K^{\mathfrak{m}_1} \cap \mathcal{C}_2$; then

$$\mathcal{R}_K^{\mathfrak{m}} = \mathcal{R}_K^{\mathfrak{m}_1} \cap \mathcal{R}_K^{\mathfrak{m}_2} \subseteq \mathcal{D} \subseteq \mathcal{I}_K^{\mathfrak{m}},$$

so $\mathcal{D}$ is a congruence subgroup of modulus $\mathfrak{m}$, and we have

$$\mathcal{I}_K^{\mathfrak{m}} \cap \mathcal{R}_K^{\mathfrak{m}_1} \subseteq \mathcal{D} \qquad \text{and} \qquad \mathcal{I}_K^{\mathfrak{m}} \cap \mathcal{R}_K^{\mathfrak{m}_2} \subseteq \mathcal{D},$$

so $\mathcal{D} \sim \mathcal{C}_1 \sim \mathcal{C}_2$, by Lemma 22.4. To prove the existence of an equivalent congruence subgroup $\mathcal{C}$ of modulus $\mathfrak{n}$ it suffices to show $\mathcal{I}_K^{\mathfrak{m}} \cap \mathcal{R}_K^{\mathfrak{n}} \subseteq \mathcal{D}$ (again by Lemma 22.4).

So let $\mathfrak{a} = (\alpha) \in \mathcal{I}_K^{\mathfrak{m}} \cap \mathcal{R}_K^{\mathfrak{n}}$, and choose $\beta \in K^{\mathfrak{m}} \cap K^{\mathfrak{m}_2,1}$ so that $\alpha\beta \in K^{\mathfrak{m}_1,1}$ (this is possible by Theorem 8.5 because $\mathfrak{m} = \operatorname{lcm}(\mathfrak{m}_1, \mathfrak{m}_2)$ and $\mathfrak{n} = \gcd(\mathfrak{m}_1, \mathfrak{m}_2)$). Then $(\beta) \in \mathcal{D}$ and $\beta\mathfrak{a} \in \mathcal{I}_K^{\mathfrak{m}} \cap \mathcal{R}_K^{\mathfrak{m}_1} \subseteq \mathcal{D}$, so $\beta^{-1}\beta\mathfrak{a} = \mathfrak{a} \in \mathcal{D}$. Thus $\mathcal{I}_K^{\mathfrak{m}} \cap P_K^{\mathfrak{n}} \subseteq \mathcal{D}$ and therefore $\mathcal{C} = \mathcal{D}\mathcal{R}_K^{\mathfrak{n}}$ is a congruence subgroup of modulus $\mathfrak{n}$ equivalent to $D \sim \mathcal{C}_1 \sim \mathcal{C}_2$. □

Corollary 22.6. *Let $\mathcal{C}$ be a congruence subgroup of modulus $\mathfrak{m}$ for a number field K. There is a unique congruence subgroup in the equivalence class of $\mathcal{C}$ whose modulus $\mathfrak{c}$ divides the modulus of every congruence subgroup equivalent to $\mathcal{C}$.*

Definition 22.7. Let $\mathcal{C}$ be a congruence subgroup of modulus $\mathfrak{m}$ for a number field K. The unique modulus $\mathfrak{c}$ given by Corollary 22.6 is the *conductor* of $\mathcal{C}$, which we may denote $\mathfrak{c}(\mathcal{C})$. If the conductor of $\mathcal{C}$ is equal to its modulus then we say that $\mathcal{C}$ is *primitive*.

Proposition 22.8. *Let $\mathcal{C}$ be a primitive congruence subgroup of modulus $\mathfrak{m}$ for a number field K. Then $\mathfrak{m}$ is the conductor of every congruence subgroup of modulus $\mathfrak{m}$ contained in $\mathcal{C}$; in particular, $\mathfrak{m}$ is the conductor of $\mathcal{R}_K^{\mathfrak{m}}$.*

Proof. Let $\mathcal{C}_0 \subseteq \mathcal{C}$ be a congruence subgroup of modulus $\mathfrak{m}$ and let $\mathfrak{c}$ be its conductor. Then $\mathfrak{c}|\mathfrak{m}$ and $\mathcal{I}_K^{\mathfrak{m}} \cap \mathcal{R}_K^{\mathfrak{c}} \subseteq \mathcal{C}_0 \subseteq \mathcal{C}$, by Lemma 22.4, and this implies that there is a congruence subgroup of modulus $\mathfrak{c}$ equivalent to $\mathcal{C}$, and therefore $\mathfrak{m}|\mathfrak{c}$, so $\mathfrak{c} = \mathfrak{m}$. □

The proposition implies that a modulus $\mathfrak{m}$ occurs as a conductor if and only if $\mathcal{R}_K^{\mathfrak{m}}$ is primitive; this does not always hold (consider $K = \mathbb{Q}$ and $\mathfrak{m} = (2)$, for example; the conductor of $\mathcal{R}_{\mathbb{Q}}^{(2)} = \mathcal{I}_{\mathbb{Q}}$ is trivial, so (2) is not a conductor).

22.2 Dirichlet's theorem for number fields

We now want to prove a generalization of Dirichlet's theorem on primes in arithmetic progressions. We first need to generalize our notion of a Dirichlet character.

Definition 22.9. Let $\mathfrak{m}$ be a modulus for a number field K. A *character* of $\mathcal{I}_K^{\mathfrak{m}}$ is a group homomorphism $\chi\colon \mathcal{I}_K^{\mathfrak{m}} \to \mathrm{U}(1)$ whose kernel contains $\mathcal{R}_K^{\mathfrak{m}}$. The *modulus* of χ is $\mathfrak{m}$, and the *conductor* of χ is the conductor $\mathfrak{c} = \mathfrak{c}(\chi) :- \mathfrak{c}(\ker \chi)$ of its kernel (as a congruence subgroup of modulus $\mathfrak{m}$); we say that χ is *primitive* if its modulus is equal to its conductor. If $\mathcal{C}$ is a congruence subgroup of modulus $\mathfrak{m}$ we say that χ is a *character for* $\mathcal{C}$ if its kernel contains $\mathcal{C}$, which case χ induces a character of the finite abelian group $\mathcal{I}_K^{\mathfrak{m}}/\mathcal{C} \simeq \mathrm{Cl}_K^{\mathfrak{m}}/\overline{\mathcal{C}}$. The *principal character* χ_0 of modulus $\mathfrak{m}$ is the unique character for $\mathcal{I}_K^{\mathfrak{m}}$; it has trivial conductor.

Each character χ of $\mathcal{I}_K^{\mathfrak{m}}$ induces a character

$$\chi\colon \mathrm{Cl}_K^{\mathfrak{m}} \to \mathrm{U}(1)$$

of the finite abelian group $\mathrm{Cl}_K^{\mathfrak{m}}$. Conversely, each character of $\mathrm{Cl}_K^{\mathfrak{m}}$ induces a character $\chi\colon \mathcal{I}_K^{\mathfrak{m}} \to \mathrm{U}(1)$ whose kernel contains the ray group $\mathcal{R}_K^{\mathfrak{m}}$ (take the value of χ on the image of each $I \in \mathcal{I}_K^{\mathfrak{m}}$ in $\mathrm{Cl}_K^{\mathfrak{m}}$). We thus view χ as a character of both $\mathcal{I}_K^{\mathfrak{m}}$ and $\mathrm{Cl}_K^{\mathfrak{m}}$ and call it a *ray class character*.

Remark 22.10. For $K = \mathbb{Q}$, a ray class character χ of modulus $\mathfrak{m} = (m)\infty$ corresponds to a Dirichlet character of modulus m (see Lecture 17).

Definition 22.11. Let $\mathfrak{m}$ be a modulus for a number field K. The *Weber L-function* of a ray class character χ of modulus $\mathfrak{m}$ is defined by

$$L(s,\chi) := \prod_{\mathfrak{p} \nmid \mathfrak{m}} \bigl(1 - \chi(\mathfrak{p})\mathrm{N}(\mathfrak{p})^{-s}\bigr)^{-1} = \sum_{\mathfrak{a} \perp \mathfrak{m}} \chi(\mathfrak{a})\mathrm{N}(\mathfrak{a})^{-s},$$

where the the product is over prime ideals $\mathfrak{p}$ not dividing $\mathfrak{m}$ and the sum is over $\mathcal{O}_K$-ideals $\mathfrak{a}$ coprime to $\mathfrak{m}$; the product and and sum both converge to a non-vanishing holomorphic function on $\mathrm{Re}(s) > 1$.

Proposition 22.12. *Let χ be a ray class character of modulus $\mathfrak{m}$ for a number field K of degree n. Then $L(s,\chi)$ extends to a meromorphic function on $\mathrm{Re}(s) > 1 - \frac{1}{n}$ that has at most a simple pole at $s = 1$ and is holomorphic if χ is non-principal.*

Proof. Associated to each ray class $\gamma \in \mathrm{Cl}_K^{\mathfrak{m}}$ we have a partial Dedekind zeta function

$$\zeta_{K,\gamma}(s) := \prod_{\mathfrak{p} \in \gamma} (1 - \mathrm{N}(\mathfrak{p})^{-s})^{-1}$$

that is holomorphic on $\mathrm{Re}(s) > 1$. For the trivial modulus $\mathfrak{m}$, our proof of analytic class number formula immediately implies that $\zeta_{K,\gamma}(s)$ has a meromorphic continuation to $1 - \frac{1}{n}$ with a simple pole at $s = 1$ that has the same residue ρ as the Dedekind zeta function $\zeta_K(s)$; recall that in our proof of Theorem 19.12 we treated each $\gamma \in \mathrm{Cl}_K = \mathrm{cl}(\mathcal{O}_K)$ separately and obtained the same value of ρ for each class.

The same proof works for $\mathrm{Cl}_K^{\mathfrak{m}}$, *mutatis mutandi*: replace $\mathrm{covol}(\mathcal{O}_K)$ with $\mathrm{covol}(\mathfrak{m}_0)$, replace the regulator $R_K = \mathrm{covol}(\pi(\mathrm{Log}(\mathcal{O}_K^\times))$ with $R_K^{\mathfrak{m}} := \mathrm{covol}(\pi(\mathrm{Log}(\mathcal{O}_K^\times \cap K^{\mathfrak{m},1}))$, and replace $w_K = \#(\mathcal{O}_K^\times)_{\mathrm{tors}}$ with $w_K^{\mathfrak{m}} = \#(\mathcal{O}_K^\times \cap K^{\mathfrak{m},1})_{\mathrm{tors}}$. The exact value of ρ is not important to us here, the key point is that $\zeta_{K,\gamma}(s)$ has a meromorphic continuation to $\mathrm{Re}(s) > 1 - \frac{1}{n}$ with a simple pole at $s = 1$ whose residue ρ depends only on K and $\mathfrak{m}$ (not γ).

We then have

$$\begin{aligned} L(s,\chi) &= \sum_{\gamma \in \mathrm{Cl}_K^{\mathfrak{m}}} \chi(\gamma)\zeta_{K,\gamma}(s) \\ &= \sum_{\gamma \in \mathrm{Cl}_K^{\mathfrak{m}}} \chi(\gamma)\bigl(\zeta_{K,\gamma}(s) - \rho\,\zeta(s)\bigr) + \sum_{\gamma \in \mathrm{Cl}_K^{\mathfrak{m}}} \chi(\gamma)\rho\,\zeta(s), \end{aligned}$$

The first sum is a finite sum of functions holomorphic on $\mathrm{Re}(s) > 1 - \frac{1}{n}$ (since $\zeta(s)$ has a simple pole at $s = 1$ with residue 1), and the second sum vanishes whenever χ is non-principal (by Corollary 18.11). The proposition follows. □

We now prove an analog of Dirichlet's theorem on primes in arithmetic progressions, subject to the assumption that $L(1,\chi) \neq 0$ for all non-principal χ, which you will recall was the last step in our proof of Dirichlet's theorem.

Remark 22.13. We proved the nonvanishing of Dirichlet L-functions $L(1,\chi)$ for non-principal χ using the analytic class number formula for $\mathbb{Q}(\zeta_m)$, the ray class field $\mathbb{Q}((m)\infty)$, by writing the Dedekind zeta function for $\mathbb{Q}(\zeta_m)$ as a product of Dirichlet L-functions (see Theorem 19.15). A similar approach works for Weber L-functions, given the existence of ray class fields $K(\mathfrak{m})$. Our goal in the remainder of this lecture is to prove as much as we can without assuming the existence of ray class fields, and then show that their existence implies $L(1,\chi) \neq 0$ for all non-principal ray class characters χ.

Theorem 22.14. *Let $\mathcal{C}$ be a congruence subgroup of modulus $\mathfrak{m}$ for a number field K and let $n := [\mathcal{I}_K^{\mathfrak{m}} : \mathcal{C}]$. The set of primes $S := \{\mathfrak{p} \in \mathcal{C}\}$ has Dirichlet density*

$$d(S) = \begin{cases} \frac{1}{n} & \textit{if } L(1,\chi) \neq 0 \textit{ for all characters } \chi \neq \chi_0 \textit{ for } \mathcal{C}, \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. We proceed as we did when proving Dirichlet's theorem (see §18.5). We first construct the indicator function for the set S:

$$\frac{1}{n}\sum_{\chi}\chi(\mathfrak{p}) = \begin{cases} 1 & \text{if } \mathfrak{p} \in \mathcal{C}, \\ 0 & \text{otherwise,} \end{cases}$$

where the sum is over the Dirichlet characters for $\mathcal{C}$; this is equivalent to summing characters of the finite abelian group $G := \mathcal{I}_K^{\mathfrak{m}}/\mathcal{C}$ over the image of $\mathfrak{p}$ in G, so we may apply Corollary 18.11. As $s \to 1^+$ we have

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

and therefore

$$\begin{aligned} \sum_{\chi}\log L(s,\chi) &\sim \sum_{\chi}\sum_{\mathfrak{p}\nmid\mathfrak{m}}\chi(\mathfrak{p})\mathrm{N}(\mathfrak{p})^{-s} \\ &\sim n\sum_{\mathfrak{p}\in\mathcal{C}}\mathrm{N}(\mathfrak{p})^{-s}. \end{aligned}$$

By Proposition 22.12, we may write

$$L(s,\chi) = (s-1)^{m(\chi)}g(s)$$

for some function $g(s)$ that is holomorphic and nonvanishing on a neighborhood of 1, where $m(\chi) := \mathrm{ord}_{s=1}L(s,\chi)$ is -1 when $\chi = \chi_0$ is principal, and $m(\chi) \geq 0$ for $\chi \neq \chi_0$. We have

$$\log\frac{1}{s-1} - \sum_{\chi\neq\chi_0} m(\chi)\log\frac{1}{s-1} \sim n\sum_{\mathfrak{p}\in cC}\mathrm{N}(\mathfrak{p})^{-s}.$$

Dividing both sides by $n\log\frac{1}{s-1}$ yields

$$\frac{1-\sum_{\chi\neq\chi_0}m(\chi)}{n} \sim \frac{\sum_{\mathfrak{p}\in\mathcal{C}}\mathrm{N}(\mathfrak{p})^{-s}}{\log\frac{1}{s-1}} \qquad (\text{as } s \to 1^+),$$

thus

$$d(S) = d(\{\mathfrak{p} \in \mathcal{C}\}) = \lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in\mathcal{C}} \mathrm{N}(\mathfrak{p})^{-s}}{\log \frac{1}{s-1}} = \frac{1 - \sum_{\chi\neq\chi_0} m(\chi)}{n}.$$

The $m(\chi)$ are integers and the Dirichlet density is nonnegative, so either $m(\chi) = 0$ for all $\chi \neq \chi_0$, in which case $L(1,\chi) \neq 0$ for all $\chi \neq 0$ and $d(S) = \frac{1}{n}$, or $m(\chi) = 1$ for exactly one of the $\chi \neq \chi_0$ and $d(S) = 0$. □

Corollary 22.15. *Let $\mathcal{C}$ be a congruence subgroup of modulus $\mathfrak{m}$ for a number field K and let $n := [\mathcal{I}_K^{\mathfrak{m}} : \mathcal{C}]$. For every ideal $\mathfrak{a} \in \mathcal{I}_K^{\mathfrak{m}}$ the set $S := \{\mathfrak{p} \in \mathfrak{a}\mathcal{C}\}$ has Dirichlet density*

$$d(S) = \begin{cases} \frac{1}{n} & \textit{if } L(1,\chi) \neq 0 \textit{ for all characters } \chi \neq \chi_0 \textit{ for } \mathcal{C}, \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. The proof is the same as in Theorem 22.14, except we now use the indicator function

$$\frac{1}{n}\sum_{\chi} \chi(\mathfrak{a})^{-1}\chi(\mathfrak{p}) = \begin{cases} 1 & \text{if } \mathfrak{p} \in \mathfrak{a}\mathcal{C}, \\ 0 & \text{otherwise,} \end{cases}$$

and obtain

$$\sum_{\chi} \chi(\mathfrak{a})^{-1} \log L(s,\chi) \sim \sum_{\chi}\sum_{\mathfrak{p}\nmid\mathfrak{m}} \chi(\mathfrak{a})^{-1}\chi(\mathfrak{p})\mathrm{N}(\mathfrak{p})^{-s} \sim n \sum_{\mathfrak{p}\in\mathfrak{a}\mathcal{C}} \mathrm{N}(\mathfrak{p})^{-s}.$$

The rest of the proof is the same. □

Corollary 22.16. *Let L/K be an abelian extension of number fields and let $\mathcal{C}$ be a congruence subgroup for a modulus $\mathfrak{m}$ of K. If $\mathrm{Spl}(L) \precsim \{\mathfrak{p} : \mathfrak{p} \in \mathcal{C}\}$ then*

$$[\mathcal{I}_K^{\mathfrak{m}} : \mathcal{C}] \leq [L : K]$$

and $L(1,\chi) \neq 0$ for all characters $\chi \neq \chi_0$ for $\mathcal{C}$. If $\mathrm{Spl}(L) \sim \{\mathfrak{p} \in \mathcal{C}\}$ then equality holds.

Proof. We know from Theorem 21.13 that $\mathrm{Spl}(L)$ has polar density $1/[L:K]$, and this is also its Dirichlet density, by Proposition 21.10. The sets $\mathrm{Spl}(L)$ and $\{\mathfrak{p} \in \mathcal{C}\}$ both have Dirichlet densities (by Theorem 22.14) and $\mathrm{Spl}(L) \precsim \{\mathfrak{p} \in \mathcal{C}\}$ (by assumption), so

$$\frac{1}{[L:K]} = d(\mathrm{Spl}(L)) \;\leq\; d(\{\mathfrak{p} \in \mathcal{C}\}),$$

The LHS cannot be zero, so Corollary 22.16 implies that the RHS must be $1/[\mathcal{I}_K^{\mathfrak{m}} : \mathcal{C}]$, and that $L(1,\chi) \neq 0$ for all $\chi \neq \chi_0$. □

Corollary 22.17. *Let $\mathcal{C}$ be a congruence subgroup of modulus $\mathfrak{m}$ for a number field K. If the ray class field $K(\mathfrak{m})$ exists then $L(1,\chi) \neq 0$ for all characters $\chi \neq \chi_0$ of modulus $\mathfrak{m}$.*

Proof. Apply the previous corollary to $L = K(\mathfrak{m})$ and $\mathcal{C} = \ker \psi_{K(\mathfrak{m})/K} = \mathcal{R}_K^{\mathfrak{m}}$. □

22.3 The conductor of an abelian extension

We now introduce another notion of conductor, one attached to an abelian extension of number fields, which is defined as a product of local conductors attached to corresponding abelian extensions of the local field K_v for each place $v \in M_K$.

Definition 22.18. Let L/K be a finite abelian extension of local fields. The *conductor* $\mathfrak{c}(L/K)$ is defined as follows.[1] If K is archimedean then $\mathfrak{c}(L/K) = \infty$ when $K \simeq \mathbb{R}$ and $L \simeq \mathbb{C}$ and $\mathfrak{c}(L/K) = 1$ otherwise. If K is nonarchimedean and $\mathfrak{p}$ is the maximal ideal of its valuation ring $\mathcal{O}_K$, then $\mathfrak{c}(L/K) = \mathfrak{p}^m$, where

$$m := \min\{n : 1 + \mathfrak{p}^n \subseteq \mathrm{N}_{L/K}(L^\times)\}$$

(here $1 + \mathfrak{p}^n$ is a subgroup of $\mathcal{O}_K^\times$, with $1 + \mathfrak{p}^0 := \mathcal{O}_K^\times$). If L/K is a finite abelian extension of global fields then

$$\mathfrak{c}(L/K) := \prod_{v \in M_K} \mathfrak{c}(L_w/K_v),$$

where K_v is the completion of K at v and L_w is the completion of L at a place w above v. (the fact that L/K is Galois ensures that this does not depend on the choice of w).

The product defining $\mathfrak{c}(L/K)$ is finite; it is not hard to show that only ramified primes may divide the conductor. More generally, we have the following.

Proposition 22.19. *Let L/K be a finite abelian extension. For each prime $\mathfrak{p}$ of K we have*

$$v_{\mathfrak{p}}(\mathfrak{c}(L/K)) = \begin{cases} 0 & \textit{if and only if } \mathfrak{p} \textit{ is unramified,} \\ 1 & \textit{if and only if } \mathfrak{p} \textit{ is ramified tamely,} \\ \geq 2 & \textit{if and only if } \mathfrak{p} \textit{ is ramified wildly.} \end{cases}$$

Proof. See Problem Set 11. □

The conductor $\mathfrak{c}(L/K)$ of an abelian extension divides the discriminant ideal $D_{L/K}$ and is divisible by the same set of primes, but the valuation of the conductor at these primes is typically smaller than that of the discriminant. For example, the discriminant of the extension $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is $(p)^{p-2}$, but its conductor is (p).

22.4 Norm groups

We can now identify a candidate for the kernel of the Artin map $\psi_{L/K}^{\mathfrak{m}} \colon \mathcal{I}_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$. Recall from Lecture 6 that the norm map $\mathrm{N}_{L/K} \colon \mathcal{I}_L \to \mathcal{I}_K$ can be defined by

$$\prod_i \mathfrak{q}_i^{n_i} \mapsto \prod_i \mathfrak{p}_i^{n_i f_i},$$

where $f_i := [\mathbb{F}_{\mathfrak{q}_i} : \mathbb{F}_{\mathfrak{p}_i}]$ is the residue field degree.

[1] Many authors use $\mathfrak{f}(L/K)$ rather than $\mathfrak{c}(L/K)$ to denote the conductor, we use $\mathfrak{c}$ to avoid confusion with the residue field degree f.

Definition 22.20. Let L/K be a finite abelian extension of number fields and let $\mathfrak{m}$ be a modulus for K divisible by the conductor of L/K. The *norm group* (or *Takagi group*) associated to $\mathfrak{m}$ is the congruence subgroup

$$T^{\mathfrak{m}}_{L/K} := \mathcal{R}^{\mathfrak{m}}_K \mathrm{N}_{L/K}(\mathcal{I}^{\mathfrak{m}}_L),$$

where $\mathcal{I}^{\mathfrak{m}}_L$ denotes the subgroup of fractional ideals in $\mathcal{I}_L$ that are coprime to $\mathfrak{m}\mathcal{O}_L$.

The norm group $T^{\mathfrak{m}}_{L/K}$ contains every prime $\mathfrak{p}$ of K coprime to $\mathfrak{m}$ that splits completely in L, since these primes all have residue field degree $f_{\mathfrak{p}} = 1$ and therefore lie in the image of the norm map $\mathrm{N}_{L/K}$, since $\mathrm{N}_{L/K}(\mathfrak{q}) = \mathfrak{p}^{f_{\mathfrak{p}}} = \mathfrak{p}$ for every primes $\mathfrak{q}$ of L above $\mathfrak{p}$. These are precisely the primes that in the kernel of the Artin map $\psi^{\mathfrak{m}}_{L/K}$, thus we always have

$$\ker \psi^{\mathfrak{m}}_{L/K} \subseteq T^{\mathfrak{m}}_{L/K}.$$

The proof of Artin reciprocity amounts to proving that the reverse inclusion holds, which implies, in particular, that $\ker \psi^{\mathfrak{m}}_{L/K}$ contains $\mathcal{R}^{\mathfrak{m}}_K \subseteq T^{\mathfrak{m}}_{L/K}$ and is therefore a congruence subgroup. As a first step in this direction we note the following.

Theorem 22.21. *Let L/K be a Galois extension of number fields and let $\mathfrak{m}$ be a modulus for K. Then*

$$[\mathcal{I}^{\mathfrak{m}}_K : T^{\mathfrak{m}}_{L/K}] \le [L : K].$$

Proof. Consider the congruence subgroup $\mathcal{C} = T^{\mathfrak{m}}_{L/K}$. As noted above, $\mathrm{Spl}(L) \precsim T^{\mathfrak{m}}_{L/K}$, so the inequality follows immediately from Corollary 22.16. □

Corollary 22.22. *Let $\chi \ne \chi_0$ be a character for a modulus $\mathfrak{m}$ of a number field K. If there exists an abelian extension L/K for which $T^{\mathfrak{m}}_{L/K} \subseteq \ker \chi$ then $L(1,\chi) \ne 0$.*

Proof. $\mathrm{Spl}(L) \sim \{\mathfrak{p} : \mathfrak{p} \in \ker \psi^{\mathfrak{m}}_{L/K}\}$, so $\ker \psi^{\mathfrak{m}}_{L/K} \subseteq T^{\mathfrak{m}}_{L/K} \subseteq \ker \chi$ implies $\mathrm{Spl}(L) \precsim \ker \chi$, and Corollary 22.16 then implies $L(1,\chi) \ne 0$, since χ is a character for $T^{\mathfrak{m}}_{L/K}$ □

Theorem 22.21 is known as either the "first" or "second" fundamental inequality of class field theory, depending on the author; it was proved first (by Weber) and originally called the first fundamental inequality, but today is often (but not always) called the second fundamental inequality. The reverse inequality is more difficult and is proved by other methods; note that once we establish equality, we can conclude that $\ker \psi^{\mathfrak{m}}_{L/K} = T^{\mathfrak{m}}_{L/K}$, since we have already shown $\ker \psi^{\mathfrak{m}}_{L/K} \subseteq T^{\mathfrak{m}}_{L/K}$.

22.5 The main theorems of class field theory (ideal-theoretic version)

We can give a more precise statement of the main theorems of class field theory. Let $\mathfrak{m}$ be a modulus for a number field K. The three main theorems of class field theory state that:

- **Existence**: The ray class field $K(\mathfrak{m})$ exists.
- **Completeness**: If L/K is finite abelian then $L \subseteq K(\mathfrak{m})$ if and only $\mathfrak{c}(L/K) \mid \mathfrak{m}$. In particular, every finite abelian L/K lies in a ray class field.
- **Artin reciprocity**: For each subextension L/K of $K(\mathfrak{m})$ we have $\ker \psi^{\mathfrak{m}}_{L/K} = T^{\mathfrak{m}}_{L/K}$ with conductor $\mathfrak{c}(L/K)$ and a canonical isomorphism $\mathrm{Cl}^{\mathfrak{m}}_K / T^{\mathfrak{m}}_{L/K} \simeq \mathrm{Gal}(L/K)$.

Artin reciprocity gives us a commutative diagram of canonical bijections:

$$\begin{tikzcd}
\{\text{abelian } L/K \text{ with } \mathfrak{c}(L/K)\,|\,\mathfrak{m}\} \arrow[r, "L\mapsto T_{L/K}^{\mathfrak{m}}"] \arrow[d, "L\mapsto \mathrm{Gal}(L/K)"] & \text{congruence subgroups } \mathcal{C}\subseteq \mathcal{I}_K^{\mathfrak{m}} \arrow[d, "\mathcal{C}\mapsto \mathcal{I}_K^{\mathfrak{m}}/\mathcal{C}"] \\
\{\text{quotients of } \mathrm{Gal}(K(\mathfrak{m})/K)\} & \text{quotients of } \mathrm{Cl}_K^{\mathfrak{m}} \arrow[l, "\psi_{L/K}^{\mathfrak{m}}"']
\end{tikzcd}$$

22.6 The Hilbert class field

For any number field K the ray class field H for the trivial modulus has a special name: it is known as the *Hilbert class field* of K and has several distinguishing properties. First, the Galois group $\mathrm{Gal}(H/K)$ is isomorphic to the ideal class group Cl_K. Second, the extension H/K is unramified, since it necessarily has conductor $\mathfrak{c}(H/K) = (1)$. Moreover, H is the maximal unramified abelian extension of K: every finite unramified abelian extension of K must have trivial conductor, hence lie in H, and if there were an infinite unramified abelian extension L/K it would necessarily contain a finite unramified abelian extension of K that does not lie in H (consider $K(\alpha)$ for any $\alpha \in L$ not in H).

This demonstrates a remarkable fact: the maximal unramified abelian extension of a number field is always a finite extension. Indeed, it is common to simply *define* the Hilbert class field of a number field K as the maximal unramified abelian extension of K, rather than as the ray class field K for the trivial modulus (of course the two coincide). It is not at all obvious *a priori* that the maximal unramified abelian extension should be finite, since many number fields have infinite unramified extensions (which are necessarily nonabelian).

Indeed, one way to construct such an extension is by considering a tower of Hilbert class fields. Starting with a number field $K_0 := K$, for each integer $n \geq 0$ define K_{n+1} to be the be the Hilbert class field of K_n. This yields an infinite tower of finite abelian extensions

$$K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots,$$

and we may then consider the field $L := \bigcup_n K_n$. There are two possibilities: either we eventually reach a field K_n with class number 1, in which case $K_m = K_n$ for all $m \geq n$ and L/K is a finite unramified extension of K, or this does not happen and L/K is an infinite unramified extension of K (which is necessarily nonabelian). It was a longstanding open question as to whether the latter could occur, but in 1964 Golod and Shafarevich proved that indeed it can; in particular, the field

$$K_0 = \mathbb{Q}(\sqrt{-30030}) = \mathbb{Q}(\sqrt{-2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13})$$

is the base of an infinite tower of Hilbert class field extensions.

References

[1] Henri Cohen, *Advanced topics in computational number theory*, Springer, 2000.