21 Statement of the 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. Let us first recall the notational setup.

We have a number field K and a modulus $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ that we view as a formal product over the places of K; the product over finite places $\mathfrak{m}_0$ can be any $\mathcal{O}_K$-ideal (so primes $\mathfrak{p}|\mathfrak{m}_0$ may occur with multiplicity), and the product over infinite places $\mathfrak{m}_\infty$ is a product of real places (with no multiplicity, so $\mathfrak{m}_\infty$ can be viewed as a set). 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 elements $\alpha \in \mathcal{K}^\times$ for which $(\alpha) \in \mathcal{I}_K^{\mathfrak{m}}$;
- $K^{\mathfrak{m},1} \subseteq K^{\mathfrak{m}}$, the subgroup of elements $\alpha \in K^{\mathfrak{m}}$ such that $v_{\mathfrak{p}}(\alpha - 1) \geq v_{\mathfrak{p}}(\mathfrak{m}_0)$ 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);
- $\mathcal{P}_K^{\mathfrak{m}} \subseteq \mathcal{I}_K^{\mathfrak{m}}$ the subgroup of principal fractional ideals $(\alpha) \in \mathcal{I}_K^{\mathfrak{m}}$ with $\alpha \in K^{\mathfrak{m},1}$;
- $\mathrm{Spl}(L)$, the set of primes of K that split completely in an extension L/K.

The *ray class group* $\mathrm{Cl}_K^{\mathfrak{m}}$ is the quotient $\mathcal{I}_K^{\mathfrak{m}}/\mathcal{P}_K^{\mathfrak{m}}$. The corresponding *ray class field* is a finite abelian extension L/K for which the kernel of the Artin map

$$\psi_{L/K}^{\mathfrak{m}} \colon \mathcal{I}_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$$

is equal to $\mathcal{P}_K^{\mathfrak{m}}$; equivalently, $\{\mathfrak{p} \in \mathcal{P}_K^{\mathfrak{m}}\} \sim \mathrm{Spl}(L)$ (recall $S \sim T$ means $T - S$ and $S - T$ are finite). The ray class field is denoted $K(\mathfrak{m})$, and $\psi_{K(\mathfrak{m})/K}^{\mathfrak{m}}$ induces an isomorphism

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

between the Galois group of the ray class field $K(\mathfrak{m})$ and the ray class group $\mathrm{Cl}_K^{\mathfrak{m}}$. 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 *congruence subgroup* $\mathcal{C}$, a group of fractional ideals prime to $\mathfrak{m}$ for which

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

and $\psi_{L/K}^{\mathfrak{m}}$ induces an isomorphism

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

where $\overline{\mathcal{C}}$ is the image of $\mathcal{C}$ in $\mathrm{Cl}_K^{\mathfrak{m}}$.

Before we proceed, let us be clear on what we have and have not proved so far. We have proved that the Artin map is surjective (see Theorem 20.15), and we *defined* the ray class field $K(\mathfrak{m})$ to be an extension L/K for which $\ker \psi_{L/K}^{\mathfrak{m}} = \mathcal{P}_K^{\mathfrak{m}}$. We have not proved that such a field $K(\mathfrak{m})$ exists, but we do know that if it does, it is uniquely determined by $\ker \psi_{K(\mathfrak{m})/K} = \mathcal{P}_K^{\mathfrak{m}}$, which depends only on the modulus $\mathfrak{m}$, since $\{\mathfrak{p} \in \mathcal{P}_K^{\mathfrak{m}}\} \sim \mathrm{Spl}(K(\mathfrak{m}))$ uniquely determines $K(\mathfrak{m})$, by Theorem 20.14.

Assuming $K(\mathfrak{m})$ exists, if L is a subfield of $K(\mathfrak{m})$ then $\ker \psi_{L/K}^{\mathfrak{m}}$ is a subgroup of $\mathcal{I}_K^{\mathfrak{m}}$ containing $\mathcal{P}_K^{\mathfrak{m}}$ (a congruence subgroup). To prove that every abelian extension L/K lies in some ray class field $K(\mathfrak{m})$ it is enough to show that $\ker \psi_{L/K}^{\mathfrak{m}}$ contains $\mathcal{P}_K^{\mathfrak{m}}$ for some modulus $\mathfrak{m}$, since then $\mathrm{Spl}(K(\mathfrak{m})) \precsim \mathrm{Spl}(L)$ and therefore $L \subseteq K(\mathfrak{m})$, by Theorem 20.14.

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 congruence subgroups that we will eventually show arise as kernels of Artin maps, 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 $\mathfrak{m} = (m)$).

21.1 Congruence subgroups

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

Definition 21.1. 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 $\mathcal{I}_K^{\mathfrak{m}}$ that contains $\mathcal{P}_K^{\mathfrak{m}}$. We write $\overline{\mathcal{C}}$ for the image of $\mathcal{C}$ in $\mathcal{I}_K^{\mathfrak{m}}/\mathcal{P}_K^{\mathfrak{m}} = \mathrm{Cl}_K^{\mathfrak{m}}$.

As noted above, congruence subgroups are the groups we expect to arise as the kernel of an Artin map $\psi_{L/K}^{\mathfrak{m}} \colon I_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ 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 $\psi_{L/K}^{\mathfrak{m}}$ 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 $\mathcal{P}_K^{\mathfrak{m}} \subseteq \ker \psi_{L/K}^{\mathfrak{m}}$ (so $\ker \psi_{L/K}^{\mathfrak{m}}$ is in fact a congruence subgroup), then every modulus divisible by $\mathfrak{m}$ will have the same property (making $\mathfrak{m}$ bigger only makes it easier for $\ker_{L/K}^{\mathfrak{m}}$ to contain $\mathcal{P}_K^{\mathfrak{m}}$). For every such $\mathfrak{m}$, if $\mathcal{C} = \ker \psi_{L/K}^{\mathfrak{m}}$ is a congruence subgroup with image $\overline{\mathcal{C}}$ in $\mathcal{I}_K^{\mathfrak{m}}/\mathcal{P}_K^{\mathfrak{m}} = \mathrm{Cl}_K^{\mathfrak{m}}$, we will have isomorphisms

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

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 $\mathrm{Spl}(L) \sim \{\mathfrak{p} : \mathfrak{p} \in \mathcal{C}\}$ (recall that $S \sim T$ means the symmetric difference of the sets S and T is finite). There are thus infinitely many congruence subgroups associated to each finite abelian extension L/K; we now wish 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 $\psi_{L/K}^{\mathfrak{m}}$ 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 $\mathfrak{m} = (3)\infty$ will not work (but the modulus $\mathfrak{m} = (9)$ does, in fact L is the ray class group 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 $\psi_{L/K}^{\mathfrak{m}}$ is a congruence subgroup whenever $\mathfrak{m}$ is divisible by $\mathfrak{c}$ and otherwise not.

Definition 21.2. 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 21.3. *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 $\mathcal{I}_K$. Moreover, $\mathcal{C}_1 \sim \mathcal{C}_2$ if and only if $\mathcal{I}_K^{\mathfrak{m}_1}/\mathcal{C}_1 \simeq \mathcal{I}_K^{\mathfrak{m}_2}/\mathcal{C}_2$, equivalently, $\mathrm{Cl}_K^{\mathfrak{m}_1}/\overline{\mathcal{C}}_1 \simeq \mathrm{Cl}_K^{\mathfrak{m}_2}/\overline{\mathcal{C}}_2$, where $\mathfrak{m}_1$ and $\mathfrak{m}_2$ are the moduli of $\mathcal{C}_1$ and $\mathcal{C}_2$ respectively.*

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 $\alpha \in K^{\mathfrak{m}_1\mathfrak{m}_2\mathfrak{m}_3,1}$ so that $\alpha\mathfrak{a} \in \mathcal{I}_K^{\mathfrak{m}_1\mathfrak{m}_2\mathfrak{m}_3}$ (this is possible by Lemma 20.4 and Theorem 3.26). Then $(\alpha) \in \mathcal{P}_K^{\mathfrak{m}_1\mathfrak{m}_2\mathfrak{m}_3} \subseteq \mathcal{P}_K^{\mathfrak{m}_1} \subseteq \mathcal{C}_1$ and $\mathfrak{a} \subseteq \mathcal{C}_1$, so $\alpha\mathfrak{a} \in \mathcal{C}_1$, and we also have $\alpha\mathfrak{a} \in \mathcal{I}_K^{\mathfrak{m}_2}$, 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 $\alpha\mathfrak{a} \in \mathcal{I}_K^{\mathfrak{m}_3}$, 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 $(\alpha) \in \mathcal{P}_K^{\mathfrak{m}_1\mathfrak{m}_2\mathfrak{m}_3} \subseteq \mathcal{P}_K^{\mathfrak{m}_3}$, 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.

To prove the second claim, for any $\mathfrak{a} \in \mathcal{I}_K^{\mathfrak{m}_1}$ we can pick $\alpha \in K^{\mathfrak{m}_1\mathfrak{m}_2,1}$ such that $\alpha\mathfrak{a} \in \mathcal{I}_K^{\mathfrak{m}_2}$ as above, and the image of $(\alpha)\mathfrak{a}$ in $\mathcal{I}_K^{\mathfrak{m}_2}/\mathcal{C}_2$ does not depend on the choice of α, since for any other $\alpha' \in K^{\mathfrak{m}_1\mathfrak{m}_2,1}$ we have $\alpha/\alpha' \in K^{\mathfrak{m}_1\mathfrak{m}_2,1}$ and $(\alpha/\alpha') \in \mathcal{P}_K^{\mathfrak{m}_1\mathfrak{m}_2} \subseteq \mathcal{P}_K^{\mathfrak{m}_2} \subseteq \mathcal{C}_2$, so $\alpha\mathfrak{a} \equiv \alpha'\mathfrak{a} \bmod \mathcal{C}_2$. We thus have a well-defined group homomorphism $\mathcal{I}_K^{\mathfrak{m}_1}/\mathcal{C}_1 \to \mathcal{I}_K^{\mathfrak{m}_2}/\mathcal{C}_2$, that is invertible (via multiplication by α^{-1}), hence injective. By symmetry, we also have an injective homomorphism in the reverse direction, and therefore an isomorphism, because the groups are finite (they are both subgroups of ray class groups). This proves the forward implication. For the reverse implication, assume $\mathcal{I}_K^{\mathfrak{m}_1}/\mathcal{C}_1 \simeq \mathcal{I}_K^{\mathfrak{m}_2}/\mathcal{C}_2$ and let $\mathfrak{a} \in \mathcal{I}_K^{\mathfrak{m}_2} \cap \mathcal{C}_1$. Then $\mathfrak{a} \in \mathcal{C}_1 \subseteq \mathcal{I}_K^{\mathfrak{m}_1}$ has trivial image in $\mathcal{I}_K^{\mathfrak{m}_1}$ and therefore must also have trivial image in $\mathcal{I}_K^{\mathfrak{m}_2}/\mathcal{C}_2$ and lie in $\mathcal{C}_2$. Thus $\mathfrak{a} \in \mathcal{I}_K^{\mathfrak{m}_1} \cap \mathcal{C}_2$, and therefore $\mathcal{I}_K^{\mathfrak{m}_2} \cap \mathcal{C}_1 \subseteq \mathcal{I}_K^{\mathfrak{m}_1} \cap \mathcal{C}_2$; the reverse inclusion follows by symmetry and therefore $\mathcal{I}_K^{\mathfrak{m}_2} \cap \mathcal{C}_1 = \mathcal{I}_K^{\mathfrak{m}_1} \cap \mathcal{C}_2$ and $\mathcal{C}_1 \sim \mathcal{C}_2$. □

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 induces a partial ordering of the congruence subgroups within an equivalence class. We now show that in fact this partial order has a unique minimal element.

Lemma 21.4. *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 $\mathcal{C}_2 = \mathcal{C}_1\mathcal{P}_K^{\mathfrak{m}_2}$.

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

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

and $\mathcal{C}_1(\mathcal{I}_K^{\mathfrak{m}_1} \cap \mathcal{P}_K^{\mathfrak{m}_2}) \subseteq \mathcal{C}_1\mathcal{C}_1 = \mathcal{C}_1$, 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 $\mathcal{C}_2 = \mathcal{C}_1\mathcal{P}_K^{\mathfrak{m}_2}$. □

Proposition 21.5. *Let $\mathcal{C}_1 \sim \mathcal{C}_2$ be subgroups of modulus $\mathfrak{m}_1$ and $\mathfrak{m}_2$, respectively. There exists a congruence subgroup $\mathcal{C}$ equivalent to $\mathcal{C}_1$ and $\mathcal{C}_2$ 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

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

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

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

so $\mathcal{D} \sim \mathcal{C}_1 \sim \mathcal{C}_2$, by Lemma 21.4. To prove the existence of an equivalent congruence subgroup $\mathcal{C}$ of modulus $\mathfrak{n}$ it suffices to show $\mathcal{I}_K^{\mathfrak{m}} \cap \mathcal{P}_K^{\mathfrak{n}} \subseteq \mathcal{D}$ (again by Lemma 21.4).

So let $\mathfrak{a} = (\alpha) \in \mathcal{I}_K^{\mathfrak{m}} \cap \mathcal{P}_K^{\mathfrak{n}}$, 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 3.26 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 $\beta\mathfrak{a} \in \mathcal{I}_K^{\mathfrak{m}} \cap \mathcal{P}_K^{\mathfrak{m}_1} \subseteq \mathcal{D}$, 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 $\mathcal{C} = \mathcal{D}\mathcal{P}_K^{\mathfrak{n}}$ is a congruence subgroup of modulus $\mathfrak{n}$ equivalent to $D \sim \mathcal{C}_1 \sim \mathcal{C}_2$. □

Corollary 21.6. *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 21.7. Let $\mathcal{C}$ be a congruence subgroup of modulus $\mathfrak{m}$ for a number field K. The unique modulus given by Corollary 21.6 is the *conductor* of $\mathcal{C}$, denoted $\mathfrak{c}(\mathcal{C})$. If the conductor of $\mathcal{C}$ is equal to its modulus then we say that $\mathcal{C}$ is *primitive*.

Proposition 21.8. *Let $\mathcal{C}$ be a primitive congruence subgroup of modulus $\mathfrak{m} = \mathfrak{c}(\mathcal{C})$ 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 $\mathcal{P}_K^{\mathfrak{m}}$.*

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 $\mathcal{I}_K^{\mathfrak{m}} \cap \mathcal{P}_K^{\mathfrak{c}} \subseteq \mathcal{C}_0 \subseteq \mathcal{C}$, by Lemma 21.4, 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 $\mathcal{P}_K^{\mathfrak{m}}$ is primitive; this does not always hold (consider $K = \mathbb{Q}$ and $\mathfrak{m} = (2)$, for example; the conductor of $\mathcal{P}_{\mathbb{Q}}^{(2)}$ is trivial).

21.2 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 21.9. Let $\mathfrak{m}$ be a modulus for a number field K. A *character* χ of modulus $\mathfrak{m}$ is a group homomorphism $\mathcal{I}_K^{\mathfrak{m}} \to \mathbb{C}^\times$ whose kernel contains $\mathcal{P}_K^{\mathfrak{m}}$. The *conductor* $\mathfrak{c}(\chi)$ of χ is the conductor of its kernel (which we note is a congruence subgroup of modulus $\mathfrak{m}$), and 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 $\mathcal{C}$. The *principal character* χ_0 is the unique character for $\mathcal{I}_K^{\mathfrak{m}}$; it has trivial conductor.

Each character χ of modulus $\mathfrak{m}$ induces a character of the finite abelian group $\mathrm{Cl}_K^{\mathfrak{m}}$ and conversely; in particular, there are exactly $h_{\mathfrak{m}} := \#\mathrm{Cl}_K^{\mathfrak{m}}$ distinct characters of modulus $\mathfrak{m}$. For $K = \mathbb{Q}$ a character χ of modulus $\mathfrak{m} = (m)\infty$ is the same thing as a Dirichlet character of modulus m (see Lecture 17), and the notions of conductor and primitive character coincide.

For each character χ of modulus $\mathfrak{m}$ we have an associated *Weber L-series*

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

where the sum is over $\mathcal{O}_K$-ideals $\mathfrak{a}$ prime to $\mathfrak{m}$; the sum and product both converge (and are nonzero) on $\mathrm{Re}(s) > 1$.

Proposition 21.10. *Let χ be a 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 is holomorphic if $\chi \neq \chi_0$ and for $\chi = \chi_0$ has only a simple pole at $s = 1$.*

Proof. Let $\delta = \frac{1}{n}$. For the principal character $\chi = \chi_0$ we have

$$L(s,\chi_0) = \zeta_K(s) \prod_{\mathfrak{p}\mid\mathfrak{m}} (1 - \mathrm{N}(\mathfrak{p})^{-s}),$$

where the finite product is entire and nonvanishing; thus, like $\zeta_K(s)$, the L-series $L(s,\chi_0)$ extends to a meromorphic function on $\mathrm{Re}(s) > 1 - \delta$ with a simple pole at $s = 1$, by Theorem 18.13 (the analytic class number formula).

For $\chi \neq \chi_0$ the function $L(s,\chi)$ is holomorphic on $\mathrm{Re}(s) > 1 - \delta$. To see this, first note that, as in the analytic class number formula, there is a real $\rho > 0$ (depending on K and $\mathfrak{m}$) for which we have

$$\#\{\mathfrak{a} \in \mathcal{I}_K^{\mathfrak{m}} : \mathfrak{a} \subseteq \mathcal{O}_K,\ \mathrm{N}(\mathfrak{a}) \le t\} = \rho t + O\big(t^{1-\delta}\big) \qquad (\text{as } t \to \infty).$$

Moreover, exactly as in the proof of the analytic class number formula, this also holds if we restrict to the set S_c of $\mathcal{O}_K$-ideals $\mathfrak{a} \perp \mathfrak{m}$ that lie in any particular ideal class $c \in \mathrm{Cl}_K^{\mathfrak{m}}$, provided we replace ρ with $\rho := \rho/\#\mathrm{Cl}_K^{\mathfrak{m}}$ (the constant is the same for every class; we don't care about its actual value). We then have

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

where ζ_{K,S_c} is the partial Dedekind zeta function (Definition 20.7). For $\chi \neq \chi_0$ the second sum vanishes (by Corollary 17.10), and Lemmas 18.10 and 18.12 imply that the first sum is holomorphic on $\mathrm{Re}(s) > 1 - \frac{1}{n}$. □

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 $\chi \neq \chi_0$. Recall that the nonvanishing of $L(1,\chi)$ was key to our proof of Dirichlet's theorem, and we used the analytic class number formula for $\mathbb{Q}(\zeta_m)$ (the ray class field $\mathbb{Q}((m)\infty)$), to prove it. The same approach will work in our more general setting, provided we assume the ray class field $K(\mathfrak{m})$ exists.

Theorem 21.11. *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*

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

Proof. We proceed as we did when proving Dirichlet's theorem (see §17.6). 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 $\mathcal{C}$; note that this is equivalent to summing characters of the finite abelian group $G := \mathcal{I}_K^{\mathfrak{m}}/\mathcal{C}$ on the image of $\mathfrak{p}$ in G, so we may apply (Corollary 17.10). 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 21.10, 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, with $m(\chi) := \mathrm{ord}_{s=1} L(s,\chi)$ equal to -1 when $\chi = \chi_0$ and nonnegative otherwise. We thus 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 21.12. *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*

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

Proof. The proof is the same as in Theorem 21.11, 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 21.13. *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 $\mathrm{Spl}(L) \precsim \mathcal{C}$ 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 $\mathcal{C}$; moreover, if $\mathrm{Spl}(L) \sim \{\mathfrak{p} \in \mathcal{C}\}$, then equality holds.

Proof. We know from Theorem 20.11 that $\mathrm{Spl}(L)$ has polar density $1/[L : K]$, and this is also its Dirichlet density, by Proposition 20.9. Since the sets $\mathrm{Spl}(L)$ and $\{\mathfrak{p} \in \mathcal{C}\}$ both have Dirichlet densities (by Theorem 21.11) and $\mathrm{Spl}(L) \precsim \{\mathfrak{p} \in \mathcal{C}\}$ (by assumption), we must have

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

since the RHS cannot be zero, in which case $L(1,\chi) \neq 0$ for all characters $\chi \neq \chi_0$ for $\mathcal{C}$ and $[\mathcal{I}_K^{\mathfrak{m}} : \mathcal{C}] \leq [L : K]$ as claimed, and the last statement follows. □

Corollary 21.14. *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 $\mathcal{C} = \ker \psi_{K(\mathfrak{m})/K} = \mathcal{P}_K^{\mathfrak{m}}$. □

21.3 The conductor of an abelian extension

We now introduce another notion of conductor attached to an abelian extension of number fields. Note that a modulus $\mathfrak{m}$ for a number field K is a product over places $v \in M_K$, each of which corresponds to a local field K_v, the completion of K at v. It thus makes sense to view a modulus (and in particular, a conductor) as a product of local moduli, each of which is a power of the place v of the local field K_v (if $K_v \simeq \mathbb{C}$ this power must be $v^0 = 1$ and if $K_v \simeq \mathbb{R}$ it can be $v^0 = 1$ or $v^1 = v$).

Definition 21.15. 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 $\mathfrak{c}(L/K) = \infty$ if $K \simeq \mathbb{R}$ and $L \simeq \mathbb{C}$ and $\mathfrak{c}(L/K) = 1$ otherwise. If K is nonarchimedean with maximal ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ then $\mathfrak{c}(L/K) = \mathfrak{p}^f$, where

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

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

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

Proof. See Problem Set 11. □

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

21.4 Norm groups

We can now identify a candidate for the kernel of the Artin map $\psi_{L/K}^{\mathfrak{m}}$. Recall from Lecture 6 that the ideal 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.

Definition 21.17. 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 (and let $\mathfrak{m}$ also denote the modulus $\mathfrak{m}\mathcal{O}_L$ for L). The *norm group* (or *Takagi group*) associated to $\mathfrak{m}$ is the congruence subgroup

$$T_{L/K}^{\mathfrak{m}} := \mathcal{P}_K^{\mathfrak{m}} \mathrm{N}_{L/K}(\mathcal{I}_L^{\mathfrak{m}}).$$

We now observe that $T_{L/K}^{\mathfrak{m}}$ contains every prime $\mathfrak{p}$ of K coprime to $\mathfrak{m}$ that splits completely in L, since these primes all have residue field degree 1 and therefore lie in the image of the ideal norm map $\mathrm{N}_{L/K}$. These are precisely the primes that lie in the kernel of the Artin map $\psi_{L/K}^{\mathfrak{m}}$, thus

$$\ker \psi_{L/K}^{\mathfrak{m}} \subseteq T_{L/K}^{\mathfrak{m}}.$$

[1] Many authors use $\mathfrak{f}(L/K)$ rather than $\mathfrak{c}(L/K)$ to denote the conductor.

The proof of Artin reciprocity essentially boils down to proving that the reverse inclusion holds (and in particular, that $\ker \psi^{\mathfrak{m}}_{L/K}$ is a congruence subgroup). As a first step in this direction we note the following.

Theorem 21.18. *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 21.13. □

Corollary 21.19. *Let $\chi \neq \chi_0$ be a character for a modulus $\mathfrak{m}$ of a number field K. If there exists a Galois extension L/K for which $T^{\mathfrak{m}}_{L/K} \subseteq \ker \chi$ then $L(1,\chi) \neq 0$.*

Theorem 21.18 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 $\ker \psi^{\mathfrak{m}}_{L/K} \subseteq T^{\mathfrak{m}}_{L/K}$.

21.5 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 K be a number field and let $\mathfrak{m}$ be a modulus for K.

- **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 $K(\mathfrak{m})/K$, the Artin map induces a canonical isomorphism between $\mathrm{Gal}(L/K)$ and $\mathrm{Cl}^{\mathfrak{m}}_K/\overline{\mathcal{C}}$, where $\mathcal{C} = T^{\mathfrak{m}}_{L/K} = \ker \psi^{\mathfrak{m}}_{L/K}$.

We can say a bit more about Artin reciprocity. The conductor of $\mathcal{C} = T^{\mathfrak{m}}_{L/K} = \ker \psi^{\mathfrak{m}}_{L/K}$ is equal to the conductor of L/K and the Artin map gives an order preserving bijection

$$\{\text{abelian extension } L/K \text{ with } \mathfrak{c}(L/K) \mid \mathfrak{m}\} \longleftrightarrow \{\text{congruence subgroups } \mathcal{C} \text{ for } \mathfrak{m}\}$$

compatible with the Galois correspondence between quotients of $\mathrm{Cl}^{\mathfrak{m}}_K$ and subfields of $K(\mathfrak{m})$.

21.6 The Hilbert class field

Let K be a number field. The ray class field $K(1)$ for the trivial modulus is known as the *Hilbert class field*, which has a number of distinguishing properties. First, the Galois group $\mathrm{Gal}(K(1)/K)$ is isomorphic to the class group Cl_K. Second, the extension $K(1)/K$ is unramified, since it follows from the completeness theorem that it has conductor 1. Moreover, $K(1)$ is the maximal unramified abelian extension of K; every finite unramified abelian extension of K must have trivial conductor, hence lie in $K(1)$, 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 $K(1)$ (consider $K(\alpha)$ for any $\alpha \in L$ not in $K(1)$).

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 $K(1)$ (of course the two coincide). It is not at all obvious that the maximal unramified abelian extension should be finite, in fact many number fields do have infinite unramified extensions (that are nonabelian).

Indeed, one way to construct such an extension is by considering a tower of Hilbert class fields. Starting with a number field $K_0 := K$, we $K_1 = K_0(1)$ be its Hilbert class field. We then define $K_2 := K_1(1)$ as the Hilbert class field of K_1, and continue in this fashion to obtain an infinite tower of finite abelian extensions:

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

and consider the extension of K given by the union of all these fields $L := \bigcup K_n$. 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 happen, but in 1964 Golod and Shafarevich proved that indeed it can; in particular, this occurs for the field

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

References

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

18.785 Number Theory I
Fall 2015