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 (for number fields) 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 $\mathfrak{m}_0 := \prod \mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}$ is a product over primes (finite places) of K and $\mathfrak{m}_\infty := \prod_{v|\infty} v^{\mathfrak{m}(v)}$ 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 not real). The moduli for K are partially ordered by the divisibility relation $\mathfrak{m}|\mathfrak{n}$, which holds if and only if $\mathfrak{m}(v) \leq \mathfrak{n}(v)$ for all $v \in M_K$. We then define

- $\mathcal{I}_K^{\mathfrak{m}} \subseteq \mathcal{I}_K$, the subgroup of fractional ideals prime to $\mathfrak{m}$ (equivalently, $\mathfrak{m}_0$);
- $K^{\mathfrak{m}} \subseteq K^\times$, 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* for $\mathfrak{m}$);
- $\mathrm{Cl}_K^{\mathfrak{m}} := \mathcal{I}_K^{\mathfrak{m}}/\mathcal{R}_K^{\mathfrak{m}}$ (the *ray class group* for $\mathfrak{m}$);
- $\mathrm{Spl}(L) := \mathrm{Spl}(L/K)$, the set of primes of K that split completely in an extension L;
- $\psi_{L/K}^{\mathfrak{m}}\colon \mathcal{I}_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$, Artin map of an abelian extension L/K unramified at $\mathfrak{p} \nmid \mathfrak{m}$.

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 at all $\mathfrak{p} \nmid \mathfrak{m}$ such that the kernel of the Artin map $\psi_{L/K}^{\mathfrak{m}}$ is equal to the the ray group $\mathcal{R}_K^{\mathfrak{m}}$. We did not prove that such fields exist, but we did prove that there is at most one of them; see Theorem 21.20. Let $K(\mathfrak{m})$ denote this field.

Assuming the ray class field $K(\mathfrak{m})$ exists, it follows from the surjectivity of the Artin map $\psi_{K(\mathfrak{m})/K}^{\mathfrak{m}}\colon \mathcal{I}_K^{\mathfrak{m}} \to \mathrm{Gal}(K(\mathfrak{m})/K)$ proved in Theorem 21.19 that we have 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 and the Galois group of the ray class field. More generally, if L is any intermediate field between K and $K(\mathfrak{m})$, the kernel of the Artin map is a subgroup $\mathcal{C} \subseteq \mathcal{I}_K^{\mathfrak{m}}$ 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.

Thus 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 $\mathcal{R}_K^{\mathfrak{m}}$ (a *congruence subgroup*, as defined below). To prove that a given abelian extension L/K lies in a ray class field, it is enough to show that there exists a modulus $\mathfrak{m}$ for K such that $\mathcal{R}_K^{\mathfrak{m}} \subseteq \ker \psi_{L/K}^{\mathfrak{m}}$, since we then have $\mathrm{Spl}(K(\mathfrak{m})) \precsim \mathrm{Spl}(L)$ and $L \subseteq K(\mathfrak{m})$, by Theorem 21.18.

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 $K(\mathfrak{m})$; this minimal modulus is known as the *conductor* of the extension. So far we have not addressed this question even for $K = \mathbb{Q}$ (but see Problem Set 10); 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 of congruence subgroups in this section follows [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 $\mathcal{I}_K^{\mathfrak{m}}$ that contains $\mathcal{R}_K^{\mathfrak{m}}$. We use $\overline{\mathcal{C}}$ to denote the image of $\mathcal{C}$ in $\mathcal{I}_K^{\mathfrak{m}}/\mathcal{R}_K^{\mathfrak{m}} = \mathrm{Cl}_K^{\mathfrak{m}}$ under the quotient map.

As explained above, congruence subgroups are precisely the groups we expect to arise as the kernel of an Artin map $\psi_{L/K}^{\mathfrak{m}} \colon \mathcal{I}_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ associated to a finite abelian extension L/K, for a suitable choice of modulus $\mathfrak{m}$. The choice of $\mathfrak{m}$ is critical; as can be seen in Example 22.2 below, $\ker \psi_{L/K}^{\mathfrak{m}}$ need not be a congruence subgroup for the modulus $\mathfrak{m}$; there are constraints on the modulus $\mathfrak{m}$ that must be satisfied beyond the basic requirement that $\mathfrak{m}$ must be divisible by all the primes of K that ramify in L (so that $\psi_{L/K}^{\mathfrak{m}}$ is defined).

Example 22.2. Let $K = \mathbb{Q}$, and consider the cyclic cubic extension $L := \mathbb{Q}[x]/(x^3 - 3x - 1)$, which is ramified only at 3. The Artin map $\psi_{L/K}^{\mathfrak{m}}$ is well-defined for any modulus $\mathfrak{m}$ divisible by (3). The ray class field for $\mathfrak{m} = (3)$ is $\mathbb{Q}(\zeta_3)^+ = \mathbb{Q}$, and the ray class field for $\mathfrak{m} = (3)\infty$ is $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$, neither of which contains L, so $\ker \psi_{L/K}^{\mathfrak{m}}$ does not contain $\mathcal{R}_K^{\mathfrak{m}}$ for either of these moduli and is not a congruence subgroup. On the other hand, L is equal to $\mathbb{Q}(\zeta_9)^+$, the ray class field for $\mathfrak{m} = (9)$, so $\ker \psi_{L/K}^{\mathfrak{m}}$ contains (and is equal to) $\mathcal{R}_K^{\mathfrak{m}}$, and is thus a congruence subgroup for the modulus $\mathfrak{m} = (9)$.

If $\ker \psi_{L/K}^{\mathfrak{m}}$ is a congruence subgroup for the modulus $\mathfrak{m}$, then $\ker \psi_{L/K}^{\mathfrak{n}}$ is a congruence subgroup for each modulus $\mathfrak{n}$ divisible by $\mathfrak{m}$. If $\mathfrak{m}$ divides $\mathfrak{n}$ then $\mathcal{R}_K^{\mathfrak{n}} \subseteq \mathcal{R}_K^{\mathfrak{m}}$ and $\psi_{L/K}^{\mathfrak{n}}$ is the restriction of $\psi_{L/K}^{\mathfrak{m}}$ to $\mathcal{I}_K^{\mathfrak{n}}$, which contains $\mathcal{R}_K^{\mathfrak{n}}$. If $\mathfrak{m}$ and $\mathfrak{n}$ are supported on the same primes, then $\mathcal{I}_K^{\mathfrak{m}} = \mathcal{I}_K^{\mathfrak{n}}$ and $\psi_{L/K}^{\mathfrak{m}} = \psi_{L/K}^{\mathfrak{n}}$, but the ray groups $\mathcal{R}_K^{\mathfrak{m}}$ and $\mathcal{R}_K^{\mathfrak{n}}$ may differ.

To deal with these complications, we define an equivalence relation on congruence subgroups and show that each equivalence class has a canonical representative whose modulus divides the modulus of every equivalent congruence subgroup.

Definition 22.3. 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 $(\mathcal{C}_1, \mathfrak{m}_1)$ and $(\mathcal{C}_2, \mathfrak{m}_2)$ are *equivalent* and write $(\mathcal{C}_1, \mathfrak{m}_1) \sim (\mathcal{C}_2, \mathfrak{m}_2)$ whenever

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

Note that when $\mathfrak{m}_1 = \mathfrak{m}_2$ this reduces to $\mathcal{C}_1 = \mathcal{C}_2$.

Proposition 22.4. *Let K be a number field. The relation $(\mathcal{C}_1, \mathfrak{m}_1) \sim (\mathcal{C}_2, \mathfrak{m}_2)$ is an equivalence relation. If $(\mathcal{C}_1, \mathfrak{m}_1) \sim (\mathcal{C}_2, \mathfrak{m}_2)$ then $\mathcal{I}_K^{\mathfrak{m}_1}/\mathcal{C}_1 \simeq \mathcal{I}_K^{\mathfrak{m}_2}/\mathcal{C}_2$ are related by a canonical isomorphism that preserves cosets of fractional ideals prime to both $\mathfrak{m}_1$ and $\mathfrak{m}_2$.*

Proof. The relation $\sim$ is clearly symmetric, and reflexive. To show that it is transitive, let $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ be congruence subgroups for moduli $\mathfrak{m}_1, \mathfrak{m}_2, \mathfrak{m}_3$ and suppose $(\mathcal{C}_1, \mathfrak{m}_1) \sim (\mathcal{C}_2, \mathfrak{m}_2)$ and $(\mathcal{C}_2, \mathfrak{m}_2) \sim (\mathcal{C}_3, \mathfrak{m}_3)$. Let $I \in \mathcal{I}_K^{\mathfrak{m}_3} \cap \mathcal{C}_1$ and pick $\alpha \in K^{\mathfrak{m}_1\mathfrak{m}_3,1}$ so that $\alpha I \in \mathcal{I}_K^{\mathfrak{m}_1\mathfrak{m}_2\mathfrak{m}_3}$ (this is possible by Lemma 21.7 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 $I \subseteq \mathcal{C}_1$, so $\alpha I \in \mathcal{C}_1$, and we also have $\alpha I \in \mathcal{I}_K^{\mathfrak{m}_1\mathfrak{m}_2\mathfrak{m}_3} \subseteq \mathcal{I}_K^{\mathfrak{m}_2}$, so

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

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

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

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 $\alpha^{-1}\alpha I = I \in \mathcal{C}_3$, and we also have $I \in \mathcal{C}_1 \subseteq \mathcal{I}_K^{\mathfrak{m}_1}$, so $I \in \mathcal{I}_K^{\mathfrak{m}_1} \cap \mathcal{C}_3$. Since $I \in \mathcal{I}_K^{\mathfrak{m}_3} \cap \mathcal{C}_1$ was chosen arbitrarily, this proves that

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

The reverse inclusion follows by symmetry, so $(\mathcal{C}_1, \mathfrak{m}_1) \sim (\mathcal{C}_3, \mathfrak{m}_3)$ as desired.

For the last statement, for any fractional ideal $I \in \mathcal{I}_K^{\mathfrak{m}_1}$ we can pick $\alpha \in K^{\mathfrak{m}_1,1}$ so that $\alpha I \in \mathcal{I}_K^{\mathfrak{m}_2}$ (via Lemma 21.7 and Theorem 8.5). The image of αI in $\mathcal{I}_K^{\mathfrak{m}_2}/\mathcal{C}_2$ does not depend on the choice of α, since for any $\alpha' \in K^{\mathfrak{m}_1,1}$ with $\alpha' I \in \mathcal{I}_K^{\mathfrak{m}_2}$ we have $(\alpha I)/(\alpha' I) = (\alpha/\alpha') \in \mathcal{I}_K^{\mathfrak{m}_2}$ and $(\alpha/\alpha') \in \mathcal{R}_K^{\mathfrak{m}_1}$, so $(\alpha/\alpha') \in \mathcal{I}_K^{\mathfrak{m}_2} \cap \mathcal{R}_K^{\mathfrak{m}_1} = \mathcal{I}_K^{\mathfrak{m}_1} \cap \mathcal{R}_K^{\mathfrak{m}_2} \subseteq \mathcal{R}_K^{\mathfrak{m}_2}$. This defines a group homomorphism $\varphi\colon \mathcal{I}_K^{\mathfrak{m}_1} \to \mathcal{I}_K^{\mathfrak{m}_2}/\mathcal{C}_2$. For $I \in \mathcal{C}_1$, we have $\alpha I \in \mathcal{I}_K^{\mathfrak{m}_2} \cap \mathcal{C}_1 = \mathcal{I}_K^{\mathfrak{m}_1} \cap \mathcal{C}_2 \subseteq \mathcal{C}_2$, but for $I \in \mathcal{I}_K^{\mathfrak{m}_1} - \mathcal{C}_1$ we have $\alpha I \in \mathcal{I}_K^{\mathfrak{m}_2} - \mathcal{C}_1$ and therefore $\alpha I \notin \mathcal{C}_2$, so $\ker\varphi = \mathcal{C}_1$. It follows that φ induces an injective homomorphism $\mathcal{I}_K^{\mathfrak{m}_1}/\mathcal{C}_1 \to \mathcal{I}_K^{\mathfrak{m}_2}/\mathcal{C}_2$, and by symmetry we have an injective homomorphism in the opposite direction, so $\mathcal{I}_K^{\mathfrak{m}_1}/\mathcal{C}_1 \simeq \mathcal{I}_K^{\mathfrak{m}_2}/\mathcal{C}_2$ as claimed.

This isomorphism is independent of the choice of α used to define it (hence canonical), and for fractional ideals I coprime to both $\mathfrak{m}_1$ and $\mathfrak{m}_2$ we can choose $\alpha = 1$, in which case the coset of I in $\mathcal{I}_K^{\mathfrak{m}_1}/\mathcal{C}_1$ will be identified with the coset of I in $\mathcal{I}_K^{\mathfrak{m}_2}/\mathcal{C}_2$. □

We now observe that if $\mathcal{C}$ is a congruence subgroup for two moduli $\mathfrak{m}_1$ and $\mathfrak{m}_2$, then $(\mathcal{C}, \mathfrak{m}_1) \sim (\mathcal{C}, \mathfrak{m}_2)$. In particular, each subgroup of $\mathcal{I}_K$ lies in at most one equivalence class of congruence subgroups. We can thus view the equivalence relation $(\mathcal{C}_1, \mathfrak{m}_1) \sim (\mathcal{C}_2, \mathfrak{m}_2)$ as an equivalence relation on the congruence subgroups of $\mathcal{I}_K$ and write $\mathcal{C}_1 \sim \mathcal{C}_2$ without ambiguity. It follows from Proposition 22.4 that each equivalence class of congruence subgroups uniquely determines a finite abelian group that is the quotient of a ray class group.

Within an equivalence class of congruence subgroups there can be at most one congruence subgroup for each modulus (since $\mathcal{C}_1 \sim \mathcal{C}_2 \Leftrightarrow \mathcal{C}_1 = \mathcal{C}_2$ whenever $\mathcal{C}_1$ and $\mathcal{C}_2$ are congruence subgroups for the same modulus). The following lemma gives a criterion for determining when there exists a congruence subgroup of a given modulus within a given equivalence class.

Lemma 22.5. *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*

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

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 we have

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

so $\mathcal{C}_1 \sim \mathcal{C}_2$. 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 22.6. *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 22.5. 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 22.5).

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 $\mathcal{I}_K^{\mathfrak{m}} \cap \mathcal{R}_K^{\mathfrak{n}} \subseteq \mathcal{D}$ 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 22.7. *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 22.8. Let $\mathcal{C}$ be a congruence subgroup for a number field K. The unique modulus $\mathfrak{c} := \mathfrak{c}(\mathcal{C})$ given by Corollary 22.7 is the *conductor* of $\mathcal{C}$, and we say that $\mathcal{C}$ is *primitive* if $\mathcal{C} = \mathcal{C}\mathcal{R}_K^{\mathfrak{c}}$ (the unique congruence subgroup of modulus $\mathfrak{c}$ equivalent to $\mathcal{C}$).

Proposition 22.9. *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 22.5, 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 $\mathcal{R}_{\mathbb{Q}}^{(2)} = \mathcal{I}_{\mathbb{Q}}^{(2)}$ is (1), since $\mathcal{R}_{\mathbb{Q}}^{(2)} \cap \mathcal{I}_{\mathbb{Q}}^{(1)} = \mathcal{I}_{\mathbb{Q}}^{(1)} \cap \mathcal{I}_{\mathbb{Q}}^{(2)}$ implies $\mathcal{R}_{\mathbb{Q}}^{(2)} \sim \mathcal{I}_{\mathbb{Q}}^{(1)}$. Thus (2) is not the conductor of any congruence subgroup for $\mathbb{Q}$.

22.2 Ray class characters

We now want to prove a generalization of Dirichlet's theorem on primes in arithmetic progressions. Given a congruence subgroup $\mathcal{C}$ for a modulus $\mathfrak{m}$ we would like to compute the Dirichlet density $d(\mathcal{C}) := d(\{\mathfrak{p} \in \mathcal{C}\})$ of the set of prime ideals $\mathfrak{p} \in \mathcal{I}_K^{\mathfrak{m}}$ that lie in $\mathcal{C}$. We first need to generalize our notion of a Dirichlet character.

Definition 22.10. Let K be a number field and let $\chi\colon \mathcal{I}_K \to \mathbb{C}$ be a totally multiplicative function with finite image; so $\chi(\mathcal{O}_K) = 1$, $\chi(IJ) = \chi(I)\chi(J)$ for all $I, J \in \mathcal{I}_K$, and χ restricts to a homomorphism from a subgroup of $\mathcal{I}_K$ to a finite subgroup of $\mathrm{U}(1)$ whose kernel we denote $\ker\chi$. If $\mathfrak{m}$ is a modulus for K such that $\chi^{-1}(\mathrm{U}(1)) = \mathcal{I}_K^{\mathfrak{m}}$ and $\mathcal{R}_K^{\mathfrak{m}} \subseteq \ker\chi$, then χ is a *ray class character of modulus* $\mathfrak{m}$ and its kernel is a congruence subgroup of modulus $\mathfrak{m}$. Equivalently, χ is the *extension by zero* of a character of the finite abelian group $\mathrm{Cl}_K^{\mathfrak{m}} = \mathcal{I}_K^{\mathfrak{m}}/\mathcal{R}_K^{\mathfrak{m}}$ defined by setting $\chi(I) = 0$ for $I \notin \mathcal{I}_K^{\mathfrak{m}}$.

Example 22.11. For $K = \mathbb{Q}$ there is a one-to-one correspondence between Dirichlet characters $\chi\colon \mathbb{Z} \to \mathbb{C}$ and ray class characters $\chi'\colon \mathcal{I}_{\mathbb{Q}} \to \mathbb{C}$ with $\chi(a) = \chi'((a))$ for all $a \in \mathbb{Z}_{\geq 1}$. Each Dirichlet character χ of modulus m corresponds to a ray class character of modulus $\mathfrak{m} = (m)\infty$ whose conductor divides (m) if and only if χ is an *even* Dirichlet character, meaning that $\chi(-1) = 1$.

Definition 22.12. Let χ_1, χ_2 be ray class characters of moduli $\mathfrak{m}_1, \mathfrak{m}_2$ of a number field K, with $\mathfrak{m}_1 | \mathfrak{m}_2$. If $\chi_2(I) = \chi_1(I)$ for all $I \in \mathcal{I}_K^{\mathfrak{m}_2}$, then χ_2 is *induced* by χ_1. A ray class character is *primitive* if it is not induced by any ray class character other than itself.

Definition 22.13. The *conductor* of a ray class character χ is the conductor $\mathfrak{c}(\chi) := \mathfrak{c}(\ker\chi)$ of its kernel (as a congruence subgroup).

Theorem 22.14. *A ray class character is primitive if and only if its kernel is primitive. Every ray class character χ is induced by a unique primitive ray class character $\widetilde{\chi}$.*

Proof. Let χ be a ray class character of modulus $\mathfrak{m}$, let $\kappa\colon \mathcal{I}_K^{\mathfrak{m}}/(\ker\chi) \to \mathrm{U}(1)$ be the group character induced by χ, and let $\mathcal{C}$ be the primitive congruence subgroup equivalent to $\ker\chi$ with modulus $\mathfrak{c} = \mathfrak{c}(\chi)$ dividing $\mathfrak{m}$ given by Corollary 22.7. By Proposition 22.4, we have a canonical isomorphism $\varphi\colon \mathcal{I}_K^{\mathfrak{c}}/\mathcal{C} \xrightarrow{\sim} \mathcal{I}_K^{\mathfrak{m}}/(\ker\chi)$ that we can use to define a ray class character $\widetilde{\chi}$ of modulus $\mathfrak{c}$ as the extension by zero of the character $\kappa \circ \varphi$ of $\mathcal{I}_K^{\mathfrak{c}}/\mathcal{C}$. The isomorphism φ preserves cosets of fractional ideals in $\mathcal{I}_K^{\mathfrak{m}} \subseteq \mathcal{I}_K^{\mathfrak{c}}$, so $\widetilde{\chi}(I) = \chi(I)$ for all $I \in \mathcal{I}_K^{\mathfrak{m}}$ and χ is induced by $\widetilde{\chi}$.

If χ_2 is a ray class character of conductor $\mathfrak{m}_2$ induced by a ray class character χ_1 of conductor $\mathfrak{m}_1$, then $\ker\chi_1 \cap \mathcal{I}_K^{\mathfrak{m}_2} = \ker\chi_2 = \ker\chi_2 \cap \mathcal{I}_K^{\mathfrak{m}_1}$ and $\ker\chi_1 \sim \ker\chi_2$, and we also note that if $\chi_1 \neq \chi_2$ then $\mathcal{I}_K^{\mathfrak{m}_1} \neq \mathcal{I}_K^{\mathfrak{m}_2}$ and $\mathfrak{m}_1 \neq \mathfrak{m}_2$. It follows that $\widetilde{\chi}$ is primitive, it is the unique primitive ray class character that induces χ. Thus χ is primitive if and only if it is equal to $\widetilde{\chi}$, which holds if and only if $\ker\chi = \ker\widetilde{\chi}$ is primitive. □

Theorem 22.14 is a direct generalization of Theorem 18.13 for Dirichlet characters. For a modulus $\mathfrak{m}$ of K we use $X(\mathfrak{m})$ to denote the set of primitive ray class characters of conductor dividing $\mathfrak{m}$, which we note is in bijection with the character group of $\mathrm{Cl}_K^{\mathfrak{m}}$, and thus has a group structure given by $\widetilde{\chi_1}\widetilde{\chi_2} = \widetilde{\chi_1\chi_2}$. Indeed, for each character of $\mathrm{Cl}_K^{\mathfrak{m}}$, its extension by zero is a ray class character χ of modulus $\mathfrak{m}$ induced by a primitive ray class character $\widetilde{\chi}$ whose conductor divides $\mathfrak{m}$, and each primitive ray class character $\widetilde{\chi}$ of conductor dividing $\mathfrak{m}$ induces a ray class character χ of modulus $\mathfrak{m}$ that determines a character of $\mathrm{Cl}_K^{\mathfrak{m}}$; these two maps are inverses, hence bijections. This generalizes Corollary 18.16.

Definition 22.15. A ray class character χ is *principal* if $\ker \chi = \chi^{-1}(\mathrm{U}(1))$. We use $\mathbb{1}$ to denote the unique primitive principal ray class character.

Remark 22.16. For Dirichlet characters, $\mathbb{1}$ is the unique Dirichlet character of conductor 1, but for ray class characters this holds only when the class group Cl_K is trivial (as when $K = \mathbb{Q}$). In general, the extension by zero of any character of Cl_K is a ray class character of conductor (1) and need not be principal (but is necessarily primitive).

Like Dirichlet characters, each ray class character has an associated L-function.

Definition 22.17. The *Weber L-function* $L(s,\chi)$ of a ray class character χ for a number field K is the complex function

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

where the the product is over prime ideals of $\mathcal{O}_K$ and the sum is over nonzero $\mathcal{O}_K$-ideals; the product and sum both converge to a non-vanishing holomorphic function on $\mathrm{Re}(s) > 1$ (this follows from comparison with the Dedekind zeta function $\zeta_K(s)$, since $|\chi(\mathfrak{a})| \le 1$).

Example 22.18. For $K = \mathbb{Q}$, Weber L-functions are Dirichlet L-functions. For any number field K, the Weber L-function for $\mathbb{1}$ is the Dedekind zeta function: $L(s,\mathbb{1}) = \zeta_K(s)$.

More generally, we have the following theorem, which is analogous to Theorem 19.15 but avoids the need to assume the existence of a ray class field.

Proposition 22.19. *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 Dirichlet series

$$\zeta_{K,\gamma}(s) := \sum_{\mathfrak{a}\in\gamma} \mathrm{N}(\mathfrak{a})^{-s}$$

that is holomorphic on $\mathrm{Re}(s) > 1$. For the trivial modulus $\mathfrak{m}$, our proof of analytic class number formula (Theorem 19.12) implies that $\zeta_{K,\gamma}(s)$ has a meromorphic continuation to $1 - \frac{1}{n}$ with a simple pole at $s = 1$ and residue $\rho = 2^r(2\pi)^2 R_K/(\omega_K|D_K|^{1/2})$, independent of γ. Recall that in our proof of Theorem 19.8 we treated each $\gamma \in \mathrm{Cl}_K = \mathrm{cl}(\mathcal{O}_K)$ separately and obtained the same value of ρ for each γ, leading to the residue $\rho_K = h_K\rho$ that appears in Theorem 19.12.

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 $w_K = \#\mu_K$ with $w_K^{\mathfrak{m}} := \#(\mu_K \cap K^{\mathfrak{m},1})$. 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

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

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 18.37). The proposition follows. □

We now prove a generalization of Dirichlet's theorem on primes on arithmetic progressions for arbitrary number fields. 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, assuming the existence of ray class fields $K(\mathfrak{m})$: the Dedekind zeta function of $K(\mathfrak{m})$ is equal to the product of the Weber L-functions for $\chi \in X(\mathfrak{m})$. But we will prove the non-vanishing of $L(1,\chi)$ for non-principal χ without assuming the existence of ray class fields.

For a congruence subgroup $\mathcal{C}$, let $X(\mathcal{C})$ denote the set of primitive ray class characters whose kernels contain $\mathcal{C}$. If $\mathcal{C}$ is a congruence subgroup of modulus $\mathfrak{m}$ then $X(\mathcal{C})$ is a subgroup of $X(\mathfrak{m})$ isomorphic to the character group of $\mathcal{I}_K^{\mathfrak{m}}/\mathcal{C}$ and we may view $X(\mathcal{C})$ as the the character group of $\mathcal{I}_K^{\mathfrak{m}}/\mathcal{C}$.

Theorem 22.20. *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 $\{\mathfrak{p} \in \mathcal{C}\}$ has Dirichlet density*

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

In fact $d(\mathcal{C}) = \frac{1}{n}$ always holds, as we will prove in Corollary 22.22 below, but it is easier to prove the theorem as stated and then use this to derive the corollary.

Proof. We proceed as in the proof of Dirichlet's theorem on primes in arithmetic progressions (see §18.4). We first construct the indicator function for the set $\{\mathfrak{p} \in \mathcal{C}\}$:

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

Note that summing over $\chi \in X(\mathcal{C})$ is equivalent to summing over the character group of $\mathcal{I}_K^{\mathfrak{m}}/\mathcal{C}$, so Corollary 18.37 applies: therefore $\sum \chi(\mathfrak{p}) = 0$ unless the image of $\mathfrak{p}$ in $I_K^{\mathfrak{m}}/\mathcal{C}$ is the identity, meaning that $\mathfrak{p} \in \mathcal{C}$, in which case $\sum \chi(\mathfrak{p}) = \#X(\mathcal{C}) = n$.

As $s \to 1^+$ we have

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

and therefore

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

By Proposition 22.19, we may write

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

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

$$\log \frac{1}{s-1} - \sum_{\chi \neq \mathbb{1}} e(\chi) \log \frac{1}{s-1} \sim n \sum_{\mathfrak{p} \in \mathcal{C}} \mathrm{N}(\mathfrak{p})^{-s}.$$

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

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

thus

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

The $e(\chi)$ are integers and the Dirichlet density is nonnegative, so either $e(\chi) = 0$ for all $\chi \neq \mathbb{1}$, in which case $L(1,\chi) \neq 0$ for all $\chi \neq \mathbb{1}$ and $d(\mathcal{C}) = \frac{1}{n}$, or $e(\chi) = 1$ for exactly one of the $\chi \neq \mathbb{1}$ and $d(\mathcal{C}) = 0$. (in fact this never happens, as noted above). □

Proposition 22.21. *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 $I \in \mathcal{I}_K^{\mathfrak{m}}$ the set $\{\mathfrak{p} \in I\mathcal{C}\}$ has Dirichlet density*

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

Proof. The proof is the same as in Theorem 22.20, except we now use the indicator function

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

and obtain

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

The rest of the proof is the same. □

Corollary 22.22. *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 $I \in \mathcal{I}_K^{\mathfrak{m}}$ the set $\{\mathfrak{p} \in I\mathcal{C}\}$ has Dirichlet density $1/n$, and for every $\chi \neq \mathbb{1}$ in $X(\mathcal{C})$ we have $L(1,\chi) \neq 0$.*

Proof. Let $I_1, \dots, I_n \in \mathcal{I}_K^{\mathfrak{m}}$ be a complete set of coset representatives for $\mathcal{C} \subseteq \mathcal{I}_K^{\mathfrak{m}}$. All but finitely many primes $\mathfrak{p}$ of K lie in $\mathcal{I}_K^{\mathfrak{m}}$, hence in one of the cosets $I_j\mathcal{C}$ partitioning $\mathcal{I}_K^{\mathfrak{m}}$, therefore

$$d(I_1\mathcal{C}) + \cdots + d(I_n\mathcal{C}) = 1.$$

By Proposition 22.21, every term in this sum is either 0 or $1/n$, and the equality implies they must all be equal to $1/n$, which then implies $L(1,\chi) \neq 0$ for all $\chi \neq \mathbb{1}$ in $X(\mathcal{C})$. □

Corollary 22.23. *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 $\mathrm{Spl}(L) \precsim \{\mathfrak{p} \in \mathcal{C}\}$ then*

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

with equality whenever $\mathrm{Spl}(L) \sim \{\mathfrak{p} \in \mathcal{C}\}$.

Proof. We know from Theorem 21.15 that $\mathrm{Spl}(L)$ has polar density $1/[L:K]$, and this is also its Dirichlet density, by Proposition 21.12. The set $\{\mathfrak{p} \in \mathcal{C}\}$ has Dirichlet density $1/[\mathcal{I}_K^{\mathfrak{m}} : \mathcal{C}]$, by Theorem 22.22, and $\mathrm{Spl}(L) \precsim \{\mathfrak{p} \in \mathcal{C}\}$ (by assumption), so

$$\frac{1}{[L:K]} = d(\mathrm{Spl}(L)) \;\le\; d(\mathcal{C}) = \frac{1}{[\mathcal{I}_K^{\mathfrak{m}} : \mathcal{C}]}.$$ □

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 22.24. 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 $\mathfrak{c}(L/K) = 1$ when $K \simeq \mathbb{R}$ and $L \simeq \mathbb{C}$ and $\mathfrak{c}(L/K) = 0$ otherwise. If K is nonarchimedean and $\mathfrak{p}$ is the maximal ideal of its valuation ring $\mathcal{O}_K$, then

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

(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 its conductor is the modulus

$$\begin{aligned} \mathfrak{c}(L/K) : M_K &\to \mathbb{Z} \\ v &\mapsto \mathfrak{c}(L_w/K_v) \end{aligned}$$

where K_v is the completion of K at v and L_w is the completion of L at a place $w|v$. (the fact that L/K is Galois ensures that $\mathfrak{c}(L_w/K_v)$ is the same for every $w|v$). As with any modulus, we may view the finite part of $\mathfrak{c}(L/K)$ as an $\mathcal{O}_K$-ideal and the infinite part as a subset of ramified infinite places.

It is not hard to show that conductor is supported on ramified places (in particular, it has finite support, as required for a modulus). More generally, we have the following.

Proposition 22.25. *Let L/K be a finite abelian extension of local or global fields. For each prime $\mathfrak{p}$ of K we have*

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

Proof. See Problem Set 11. □

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

The finite part of the conductor of an abelian extension divides the discriminant ideal 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 $(p)\infty$.

Lemma 22.26. *Let L_1/K and L_2/K be two finite abelian extensions of a local or global field K. If $L_1 \subseteq L_2$ then $\mathfrak{c}(L_1/K)$ divides $\mathfrak{c}(L_2/K)$.*

Proof. If $K \simeq \mathbb{R}, \mathbb{C}$ the result is clear, and for nonarchimedean local K we may apply $N_{L_2/K}(L_2^\times) = N_{L_1/K}(N_{L_2/L_1}(L_2^\times)) \subseteq N_{L_1/K}(L_1^\times)$. The global case follows. □

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 $N_{L/K} \colon \mathcal{I}_L \to \mathcal{I}_K$ can be defined by

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

where $\mathfrak{p}_i \coloneqq \mathfrak{q}_i \cap \mathcal{O}_K$ and $f_i := [\mathbb{F}_{\mathfrak{q}_i} : \mathbb{F}_{\mathfrak{p}_i}]$ is the residue field degree.

Definition 22.27. 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

$$T_{L/K}^{\mathfrak{m}} := \mathcal{R}_K^{\mathfrak{m}} N_{L/K}(\mathcal{I}_L^{\mathfrak{m}}),$$

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

Proposition 22.28. *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. Then $\ker \psi_{L/K}^{\mathfrak{m}} \subseteq T_{L/K}^{\mathfrak{m}}$.*

Proof. Let $\mathfrak{p}$ be a prime of K that lies in $\ker \psi_{L/K}^{\mathfrak{m}}$. Then $\mathfrak{p}$ is coprime to $\mathfrak{m}$ and splits completely in L, so $e_{\mathfrak{p}} = f_{\mathfrak{p}} = 1$. There is at least one prime $\mathfrak{q}$ of L above $\mathfrak{p}$, and for this prime we have $N_{L/K}(\mathfrak{q}) = \mathfrak{p}^{f_{\mathfrak{p}}} = \mathfrak{p}$ (by Theorem 6.10), so $\mathfrak{p} \in N_{L/K}(\mathcal{I}_L^{\mathfrak{m}}) \subseteq T_{L/K}^{\mathfrak{m}}$. □

To prove Artin reciprocity we need to establish the reverse inclusion, which requires a different approach (we will prove it for the trivial modulus $\mathfrak{m}$ over the next two lectures). But we can record the following theorem, historically known as the "first" fundamental inequality of class field theory (in modern terminology it is typically known as the second, even though it was proved first, by Weber).

Theorem 22.29. *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. Then*

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

Proof. Proposition 22.28 implies $[\mathcal{I}_K^{\mathfrak{m}} : T_{L/K}^{\mathfrak{m}}] \le [\mathcal{I}_K^{\mathfrak{m}} : \ker \psi_{L/K}^{\mathfrak{m}}] = [L : K]$, where the equality follows from the surjectivity of the Artin map (Theorem 21.19). □

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 $\mathfrak{c}(L/K)|\mathfrak{m}$ and a canonical isomorphism $\mathcal{I}^{\mathfrak{m}}_K/T^{\mathfrak{m}}_{L/K} \simeq \mathrm{Gal}(L/K)$.

Artin reciprocity gives us a commutative diagram of canonical bijections:

$$\begin{array}{ccc} \{\text{abelian } L/K \text{ with } \mathfrak{c}(L/K) \mid \mathfrak{m}\} & \xrightarrow{L \mapsto T^{\mathfrak{m}}_{L/K}} & \{\text{congruence subgroups } \mathcal{C} \subseteq \mathcal{I}^{\mathfrak{m}}_K\} \\ \Big\downarrow{\scriptstyle L \mapsto \mathrm{Gal}(L/K)} & & \Big\downarrow{\scriptstyle \mathcal{C} \mapsto \mathcal{I}^{\mathfrak{m}}_K/\mathcal{C}} \\ \{\text{quotients of } \mathrm{Gal}(K(\mathfrak{m})/K)\} & \xleftarrow[\psi^{\mathfrak{m}}_{L/K}]{} & \{\text{ quotients of } \mathrm{Cl}^{\mathfrak{m}}_K\} \end{array}$$

22.6 The Hilbert class field

Definition 22.30. Let K be global field. The *Hilbert class field* of K is the maximal unramified abelian extension of K (the compositum of all finite unramified abelian extensions of K inside a fixed separable closure of K).

While it is not obvious from the definition, it follows from the completeness theorem of class field theory that the Hilbert class field must be the ray class field for the trivial modulus, and in particular, that it is a finite extension of K. This is a remarkable result (which we will prove in a later lecture), since infinite unramified extensions of number fields do exist (they 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. One might ask whether one can use an imaginary quadratic field of smaller discriminant than this. It is known that no imaginary quadratic field of discriminant $|D| \leq 420$ has an infinite Hilbert class field tower [3]; they all stabilize at either K_2 or K_3.

Extensions arising from Hilbert class field towers are necessarily solvable, since they are towers of finite abelian extensions. One might ask whether infinite nonsolvable unramified extensions exist. As shown by Maire [2], they do, and this can happen even when the base field has class number one and the Hilbert class field tower is trivial. Indeed, the biquadratic extension

$$\mathbb{Q}(\sqrt{17601097}, \sqrt{17380678572169893})$$

has class number one and its maximal unramified extension is an infinite extension.

References

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

[2] Christian Maire, *On infinite unramfieid extensions*, Pacific J. Math. **192** (2000), 135–142.

[3] Ken Yamamura, *Maximal unramified extensions of imaginary quadratic number fields of small conductors*, Journal de Théorie des Nombres de Bordeaux **9** (1997) 405–448.

18.785 Number Theory I
Fall 2019