**18.785 Number theory I** **Fall 2016**
**Lecture #21** **11/22/2016**

# 21 Class field theory: ray class groups and ray class fields

In the Lecture 20 we proved the Kronecker-Weber theorem: every abelian extension $L$ of $\mathbb{Q}$ lies in a cyclotomic extension $\mathbb{Q}(\zeta_m)/\mathbb{Q}$. The isomorphism $\operatorname{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$ allows us to view $\operatorname{Gal}(L/\mathbb{Q})$ as a quotient of $(\mathbb{Z}/m\mathbb{Z})^\times$. Conversely, for each quotient $H$ of $(\mathbb{Z}/m\mathbb{Z})^\times$, there is a subfield $L$ of $\mathbb{Q}(\zeta_m)$ for which $H \simeq \operatorname{Gal}(L/\mathbb{Q})$. We would like to make the correspondence between $H$ and $L$ explicit, and then generalize this setup to base fields $K$ other than $\mathbb{Q}$. To do so we need the Artin map, which we briefly recall.

## 21.1 The Artin map

Let $L/K$ be a finite Galois extension of global fields. For each prime $\mathfrak{p}$ of $K$, the Galois group $\operatorname{Gal}(L/K)$ acts on the set $\{\mathfrak{q}|\mathfrak{p}\}$ of primes lying above $\mathfrak{p}$. For each $\mathfrak{q}|\mathfrak{p}$ the stabilizer of $\mathfrak{q}$ under this action is the decomposition group $D_\mathfrak{q} \subseteq \operatorname{Gal}(L/K)$, and there is a natural surjective homomorphism

$$\begin{aligned}\pi_\mathfrak{q}\colon D_\mathfrak{q} &\to \operatorname{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})\\ \sigma &\mapsto \overline{\sigma} := (\overline{a} \mapsto \overline{\sigma(a)})\end{aligned}$$

where $a \in \mathcal{O}_L$ is any lift of $\overline{a} \in \mathbb{F}_\mathfrak{q} := \mathcal{O}_L/\mathfrak{q}$ to $\mathcal{O}_L$ and $\overline{\sigma(a)}$ is the reduction of $\sigma(a) \in \mathcal{O}_L$ modulo $\mathfrak{q}$; the automorphism $\overline{\sigma} \in \operatorname{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$ is well-defined because $\sigma \in D_\mathfrak{q}$ stablizes $\mathfrak{q}$). When $\mathfrak{q}$ is unramified the inertia group $I_\mathfrak{q} := \ker \pi_\mathfrak{q}$ is trivial and the map $\pi_\mathfrak{q}$ is an isomorphism. The *Artin symbol* (Definition 7.17) is defined by

$$\left(\frac{L/K}{\mathfrak{q}}\right) := \sigma_\mathfrak{q} := \pi_\mathfrak{q}^{-1}(x \mapsto x^{\#\mathbb{F}_\mathfrak{p}}),$$

where $(x \mapsto x^{\#\mathbb{F}_\mathfrak{p}}) \in \operatorname{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$ is the Frobenius atomorphism, a canonical generator for the cyclic group $\operatorname{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$. Equivalently, $\sigma_\mathfrak{q}$ is the unique element of $\operatorname{Gal}(L/K)$ for which

$$\sigma_\mathfrak{q}(x) \equiv x^{\#\mathbb{F}_\mathfrak{p}} \bmod \mathfrak{q}$$

for all $x \in \mathcal{O}_L$. The *Frobenius elements* $\sigma_\mathfrak{q}$ for $\mathfrak{q}|\mathfrak{p}$ are all conjugate (they form the *Frobenius class* $\operatorname{Frob}_\mathfrak{p}$), and when $L/K$ is abelian they coincide, in which case we may write $\sigma_\mathfrak{p}$ instead of $\sigma_\mathfrak{q}$ and we have (or use $\operatorname{Frob}_\mathfrak{p} = \{\sigma_\mathfrak{p}\}$ to denote $\sigma_\mathfrak{p}$), and write the Artin symbol as

$$\left(\frac{L/K}{\mathfrak{p}}\right) := \sigma_\mathfrak{p}.$$

Now assume $L/K$ is abelian, let $\mathfrak{m}$ be an $\mathcal{O}_K$-ideal divisible by every ramified prime of $K$, and let $\mathcal{I}_K^\mathfrak{m}$ denote the subgroup of fractional ideals $I$ for which $v_\mathfrak{p}(I) = 0$ for all $\mathfrak{p}|\mathfrak{m}$. The *Artin map* (Definition 7.20) is the homomorphism

$$\begin{aligned}\psi_{L/K}^\mathfrak{m}\colon \mathcal{I}_K^\mathfrak{m} &\to \operatorname{Gal}(L/K)\\ \prod_{\mathfrak{p}\nmid\mathfrak{m}} \mathfrak{p}^{n_\mathfrak{p}} &\mapsto \prod_{\mathfrak{p}\nmid\mathfrak{m}} \left(\frac{L/K}{\mathfrak{p}}\right)^{n_\mathfrak{p}}.\end{aligned}$$

One of the main theorems of class field theory (which we will prove in this lecture) is that the Artin map $\psi_{L/K}^\mathfrak{m}$ is surjective. We can then identify $\operatorname{Gal}(L/K)$ with a quotient of $\mathcal{I}_K^\mathfrak{m}$, allowing us to characterize all abelian extensions $L/K$ in terms of quotients of $\mathcal{I}_K^\mathfrak{m}$. This is remarkable because the ideal $\mathfrak{m} \subseteq \mathcal{O}_K$ and the ideal group $\mathcal{I}_K^\mathfrak{m}$ depend only on $K$, yet they completely determine the possibilities for $L$.

*Lecture by Andrew Sutherland*

## 21.2 Class field theory for $\mathbb{Q}$

We now specialize to $K = \mathbb{Q}$, in which case the Kronecker-Weber theorem tells us that every abelian extension $L/K$ lies in a cyclotomic field $\mathbb{Q}(\zeta_m)$. Each $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ is determined by its action on $\zeta_m$, and we have an isomorphism

$$\omega\colon \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/m\mathbb{Z})^\times$$

defined by $\sigma(\zeta_m) = \zeta_m^{\omega(\sigma)}$. The primes $p$ that ramify in $\mathbb{Q}(\zeta_m)$ are precisely those that divide $m$ (by Corollary 10.21). For each prime $p \nmid m$ the Frobenius element $\sigma_p$ is the unique $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ for which $\sigma(x) \equiv x^p \bmod \mathfrak{q}$ for any (equivalently, all) $\mathfrak{q}|(p)$. Thus $\omega(\sigma_p) = p \bmod m$, and it follows that the Artin map induces an inverse isomorphism $(\mathbb{Z}/m\mathbb{Z})^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$: for every integer $a$ coprime to $m$ we have $(a) \in \mathcal{I}_{\mathbb{Q}}^m$ and

$$\omega^{-1}(\bar{a}) = \left(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{(a)}\right),$$

where $\bar{a} = a \bmod m$. Notice that (as you showed on Problem Set 4), the surjectivity of the Artin map follows immediately, since $a$ ranges over all integers coprime to $m$.[1]

Now let $K$ be a subfield of $\mathbb{Q}(\zeta_m)$. We cannot directly apply $\omega$ to $\mathrm{Gal}(L/\mathbb{Q})$, since $\mathrm{Gal}(L/\mathbb{Q})$ is a quotient of $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ (not a subgroup!), but we still have the Artin map $\mathcal{I}_{\mathbb{Q}}^m \to \mathrm{Gal}(L/\mathbb{Q})$ available; notice that the modulus $m$ works for $L$ as well as $\mathbb{Q}(\zeta_m)$, since any primes that ramify in $L$ also ramify in $\mathbb{Q}(\zeta_m)$ and therefore divide $m$. The Artin map factors through the quotient map $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \to \mathrm{Gal}(L/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})/\mathrm{Gal}(\mathbb{Q}(\zeta_m)/L)$ induced by restriction (send each $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ to $\sigma_{|L} \in \mathrm{Gal}(L/\mathbb{Q})$). That is, for any $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ we have

$$\left(\frac{L/\mathbb{Q}}{(a)}\right) = \left(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{(a)}\right)_{|L}.$$

To see this, write $L = \mathbb{Q}(\alpha)$ with $\alpha \in \mathcal{O}_L$; then $\alpha \in \mathcal{O}_{\mathbb{Q}(\zeta_m)} = \mathbb{Z}[\zeta_m]$, so $\alpha = f(\zeta_m)$ for some $f \in \mathbb{Z}[x]$. For any prime $p \nmid m$, if we put $\sigma := \left(\frac{L/\mathbb{Q}}{(p)}\right)$ and $\tau := \left(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{(p)}\right)$, then

$$\sigma(\alpha) = \sigma(f(\zeta_m)) \equiv_{\mathfrak{q}} f(\zeta_m)^p = f(\zeta_m^p) \equiv_{\mathfrak{q}} f(\tau(\zeta_m)) = \tau(f(\zeta_m)),$$

where the equivalences are modulo any prime $\mathfrak{q}|p$ of $L$ (note that $f(\tau(\zeta_m)) = \tau(f(\zeta_m))$ is conjugate to $\alpha = f(\zeta_m)$ and therefore lies in $\mathcal{O}_L$ so this makes sense).

To sum up, we can now say the following about abelian extensions of $\mathbb{Q}$:

- **Existence**: for every modulus $m$ we have a *ray class field*: an abelian extension ramified only at primes $p|m$ with Galois group isomorphic to $(\mathbb{Z}/m\mathbb{Z})^\times$ (take $\mathbb{Q}(\zeta_m)$).
- **Completeness**: every abelian extension lies in a ray class field (Kronecker-Weber).
- **Reciprocity**: for each abelian extension $L$ of $\mathbb{Q}$ contained in the ray class field of modulus $m$ the Artin map induces a surjective homomorphism $(\mathbb{Z}/m\mathbb{Z})^\times \to \mathrm{Gal}(L/\mathbb{Q})$.

All of these statements can be made more precise; in particular, we can refine the first two statements so that the fields are uniquely determined up to isomorphism, and we will give an explicit description of the kernel of the Artin map that allows us to identify $\mathrm{Gal}(L/K)$ with a quotient of $(\mathbb{Z}/m\mathbb{Z})^\times$. We will address these details in the next lecture. Let us first consider how to generalize these statements to base fields $K$ other than $\mathbb{Q}$; in particular, we want to define the *ray class groups* that will play the role of $(\mathbb{Z}/m\mathbb{Z})^\times$.

[1] In particular, there is no need to invoke Dirichlet's theorem on primes in arithmetic progressions.

## 21.3 Moduli and ray class groups

Recall that for a global field $K$ we use $M_K$ to denote its set of places (equivalence classes of absolute values). We generically denote places by the symbol $v$, but for finite places, those arising from a discrete valuation associated to a prime $\mathfrak{p}$ of $K$ (by which we mean a nonzero prime ideal of $\mathcal{O}_K$), we may write $\mathfrak{p}$ in place of $v$. We write $v|\infty$ to indicate that $v$ is an infinite place (one not arising from a prime of $K$); when $K$ is a number field infinite places are archimedean and may be real ($K_v \simeq \mathbb{R}$) or complex ($K_v \simeq \mathbb{C}$).

**Definition 21.1.** Let $K$ be a global field. A *modulus* (or *cycle*) $\mathfrak{m}$ for $K$ is a function $M_K \to \mathbb{Z}_{\geq 0}$ with finite support such that for $v|\infty$ we have $\mathfrak{m}(v) \leq 1$ with $\mathfrak{m}(v) = 0$ unless $v$ is a real place. We view $\mathfrak{m}$ as a formal product $\prod v^{\mathfrak{m}(v)}$ over $M_K$, which we may factor as

$$\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty, \qquad \mathfrak{m}_0 := \prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}, \qquad \mathfrak{m}_\infty := \prod_{v|\infty} v^{\mathfrak{m}(v)},$$

where $\mathfrak{m}_0$ corresponds to an $\mathcal{O}_K$-ideal and $\mathfrak{m}_\infty$ represents a subset of the real places of $K$; we use $\#\mathfrak{m}_\infty$ to denote the number of real places in the support of $\mathfrak{m}$. If $\mathfrak{m}$ and $\mathfrak{n}$ are two moduli for $K$ we say that $\mathfrak{m}$ divides $\mathfrak{n}$ if $\mathfrak{m}(v) \leq \mathfrak{n}(v)$ for all $v \in M_K$ and define $\gcd(\mathfrak{m}, \mathfrak{n})$ and $\operatorname{lcm}(\mathfrak{m}, \mathfrak{n})$ in the obvious way. We use 1 to denote the trivial modulus (the zero function).

We use $\mathcal{I}_K$ to denote the ideal class group of $\mathcal{O}_K$ and define the following notation:[2]

- a fractional ideal $\mathfrak{a} \in \mathcal{I}_K$ is *coprime to* $\mathfrak{m}$ (or *prime to* $\mathfrak{m}$) if $v_\mathfrak{p}(\mathfrak{a}) = 0$ for all $\mathfrak{p}|\mathfrak{m}_0$.
- $\mathcal{I}_K^\mathfrak{m} \subseteq \mathcal{I}_K$ is the subgroup of fractional ideals coprime to $\mathfrak{m}$.
- $K^\mathfrak{m} \subseteq K^\times$ is the subgroup of elements $\alpha \in K^\times$ for which $(\alpha) \in \mathcal{I}_K^\mathfrak{m}$.
- $K^{\mathfrak{m},1} \subseteq K^\mathfrak{m}$ is the subgroup of elements $\alpha \in K^\mathfrak{m}$ 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 $\alpha_v \in K_v \simeq \mathbb{R}$ is the image of $\alpha$ under $K \hookrightarrow K_v$).
- $\mathcal{R}_K^\mathfrak{m} \subseteq \mathcal{I}_K^\mathfrak{m}$ is the subgroup of principal fractional ideals $(\alpha) \in \mathcal{I}_K^\mathfrak{m}$ with $\alpha \in K^{\mathfrak{m},1}$.

The groups $\mathcal{R}_K^\mathfrak{m}$ are called *rays* or *ray groups.*

**Definition 21.2.** The *ray class group* of $K$ for the modulus $\mathfrak{m}$ is the quotient

$$\operatorname{Cl}_K^\mathfrak{m} := \mathcal{I}_K^\mathfrak{m}/\mathcal{R}_K^\mathfrak{m}.$$

When $\mathfrak{m}$ is the trivial modulus, this is just the usual class group $\operatorname{Cl}_K := \operatorname{cl}(\mathcal{O}_K)$; in general the class group $\operatorname{Cl}_K$ is a quotient of the ray class group $\operatorname{Cl}_K^\mathfrak{m}$.

**Remark 21.3.** If $\mathfrak{m}(v) = 1$ for every real place $v \in M_K$ then $\operatorname{Cl}_K^\mathfrak{m}$ is called a *narrow ray class group.* The narrow ray class group with $\mathfrak{m}_0 = (1)$ is also called the *narrow class group* and the usual class group $\operatorname{Cl}_K = \operatorname{cl}\mathcal{O}_K$ is then sometimes called the *wide class group* to better distinguish the two. But note that the wide class group is a **quotient** of the narrow class group, so in general it is **smaller**, despite what the terminology might suggest (yes this is confusing, but it appears throughout the literature so we are stuck with it).

**Example 21.4.** For $K = \mathbb{Q}$ and $\mathfrak{m} = (5)$ we have we have $K^\mathfrak{m} = \{a/b : a, b \not\equiv 0 \bmod 5\}$, $K^{\mathfrak{m},1} = \{a/b : a \equiv b \not\equiv 0 \bmod 5\}$. Thus

[2] This notation varies from author to author; there is unfortunately no universally accepted notation for these objects (in particular, many authors put some but not all of the $\mathfrak{m}$'s in subscripts). Things will improve when we come to the adelic/idelic formulation of class field theory where there is more consistency.

- $\mathcal{I}_K^{\mathfrak{m}} = \{(1), (1/2), (2), (1/3), (2/3), (3/2), (3), (1/4), (3/4), (4/3), (4), (1/6), (6), \ldots\}$.
- $\mathcal{R}_K^{\mathfrak{m}} = \{(1), (2/3), (3/2), (1/4), (4), (6), (1/6), (2/7), (7/2), \ldots\}$.

You might not have expected $(2/3) \in \mathcal{R}_K^{\mathfrak{m}}$, but note that $-2/3 \in K^{\mathfrak{m},1}$ and $(-2/3) = (2/3)$. The ray class group $\mathrm{Cl}_K^{\mathfrak{m}} = \mathcal{I}_K^{\mathfrak{m}}/\mathcal{R}_K^{\mathfrak{m}} = \{[(1)], [(2)]\} \simeq (\mathbb{Z}/5\mathbb{Z})^\times/\{\pm 1\}$. But for the modulus $\mathfrak{m} = (5)\infty$ we have $\mathcal{R}_K^{\mathfrak{m}} = \{(1), (6), (1/6), (2/7), (7/2), \ldots\}$ and $\mathrm{Cl}_K^{\mathfrak{m}} \simeq (\mathbb{Z}/5\mathbb{Z})^\times$.

**Lemma 21.5.** *Let $A$ be a Dedekind domain and let $\mathfrak{a}$ be an $A$-ideal. Every ideal class in* $\mathrm{cl}(A)$ *can be represented by an ideal coprime to $\mathfrak{a}$.*

*Proof.* Let $I = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$ be the unique factorization of some nonzero fractional ideal $I$ of $A$. We may write $I = I_1 I_2$ with $I_1 := \prod_{\mathfrak{p}\nmid\mathfrak{a}} \mathfrak{p}^{n_{\mathfrak{p}}}$ and $I_2 := \prod_{\mathfrak{p}|\mathfrak{a}} \mathfrak{p}^{n_{\mathfrak{p}}}$ coprime. Choose a uniformizer $\pi_{\mathfrak{p}}$ for each $\mathfrak{p}|\mathfrak{a}$ and put $\alpha := \prod_{\mathfrak{p}|\mathfrak{a}} \pi_{\mathfrak{p}}^{-n_{\mathfrak{p}}}$. Then $[\alpha I] = [I]$ and $\alpha I$ is coprime to $\mathfrak{a}$. □

**Theorem 21.6.** *Let $\mathfrak{m}$ be a modulus for a global field $K$. We have an exact sequence*

$$1 \longrightarrow \mathcal{O}_K^\times \cap K^{\mathfrak{m},1} \longrightarrow \mathcal{O}_K^\times \longrightarrow K^{\mathfrak{m}}/K^{\mathfrak{m},1} \longrightarrow \mathrm{Cl}_K^{\mathfrak{m}} \longrightarrow \mathrm{Cl}_K \longrightarrow 1$$

*and a canonical isomorphism*

$$K^{\mathfrak{m}}/K^{\mathfrak{m},1} \simeq \{\pm 1\}^{\#\mathfrak{m}_\infty} \times (\mathcal{O}_K/\mathfrak{m}_0)^\times.$$

*Proof.* Let us consider the composition of the maps $K^{\mathfrak{m},1} \subseteq K^{\mathfrak{m}}$ and $\alpha \mapsto (\alpha)$:

$$K^{\mathfrak{m},1} \xrightarrow{f} K^{\mathfrak{m}} \xrightarrow{g} \mathcal{I}_K^{\mathfrak{m}}.$$

The kernel of $f$ is trivial, the kernel of $g \circ f$ is $\mathcal{O}_K^\times \cap K^{\mathfrak{m},1}$ (since $(\alpha) = (1) \iff \alpha \in \mathcal{O}_K^\times$), the kernel of $g$ is $\mathcal{O}_K^\times$, the cokernel of $f$ is $K^{\mathfrak{m}}/K^{\mathfrak{m},1}$, the cokernel of $g \circ f$ is $\mathrm{Cl}_K^{\mathfrak{m}} = \mathcal{I}_K^{\mathfrak{m}}/\mathcal{R}_K^{\mathfrak{m}}$ (by definition), and the cokernel of $g$ is $\mathrm{Cl}_K$ (by Lemma 21.5). Applying the snake lemma (see [2, Lemma 5.13], for example) to the commutative diagram with exact rows

$$\begin{tikzcd}
1 \arrow[r] & K^{\mathfrak{m},1} \arrow[r, hook, "f"] \arrow[d, "g\circ f"] & K^{\mathfrak{m}} \arrow[r] \arrow[d, "g"] & K^{\mathfrak{m}}/K^{\mathfrak{m},1} \arrow[r] \arrow[d, "\pi"] & 1 \\
1 \arrow[r] & \mathcal{I}_K^{\mathfrak{m}} \arrow[r, "\sim"] & \mathcal{I}_K^{\mathfrak{m}} \arrow[r] & 1 &
\end{tikzcd}$$

yields the exact sequence $\ker g\circ f \to \ker g \to \ker \pi \to \operatorname{coker} g \circ f \to \operatorname{coker} g \to \operatorname{coker} \pi$:

$$1 \longrightarrow \mathcal{O}_K^\times \cap K^{\mathfrak{m},1} \longrightarrow \mathcal{O}_K^\times \longrightarrow K^{\mathfrak{m}}/K^{\mathfrak{m},1} \longrightarrow \mathrm{Cl}_K^{\mathfrak{m}} \longrightarrow \mathrm{Cl}_K \longrightarrow 1,$$

where the initial 1 follows from the fact that $f$ is injective (and $\ker \pi = \operatorname{coker} f$).

We can write each $\alpha \in K^{\mathfrak{m}}$ as $\alpha = a/b$ with $a, b \in \mathcal{O}_K$ such that $(a)$ and $(b)$ are coprime to $\mathfrak{m}_0$ and to each other. The ideals $(a)$ and $(b)$ are uniquely determined by $\alpha$ (even though $a$ and $b$ are not), since $a/b = a'/b' \Rightarrow ab' = a'b \Rightarrow (a)(b') = (a')(b)$, and since $(a)$ and $(b)$ are coprime we must have $(a) = (a')$ and $(b) = (b')$ (by unique factorization of ideals).

We now define the homomorphism

$$\begin{aligned}
\varphi\colon K^{\mathfrak{m}} &\to \left(\prod_{v|\mathfrak{m}_\infty} \{\pm 1\}\right) \times (\mathcal{O}_K/\mathfrak{m}_0)^\times \\
\alpha &\mapsto \left(\prod_{v|\mathfrak{m}_\infty} \mathrm{sgn}(\alpha_v)\right) \times (\bar{\alpha}),
\end{aligned}$$

where $\bar{\alpha} = \bar{a}\bar{b}^{-1} \in (\mathcal{O}_K/\mathfrak{m}_0)^\times$ (here $\bar{a}, \bar{b}$ are the images of $a, b \in \mathcal{O}_K$ in $\mathcal{O}_K/\mathfrak{m}_0$, and they both lie in $(\mathcal{O}_K/\mathfrak{m}_0)^\times$ because $(a)$ and $(b)$ are coprime to $\mathfrak{m}_0$). The ring $(\mathcal{O}_K/\mathfrak{m}_0)^\times$ is isomorphic to $\prod_{\mathfrak{p}|\mathfrak{m}_0}(\mathcal{O}_K/\mathfrak{p}^{\mathfrak{m}(\mathfrak{p})})^\times$, by the Chinese remainder theorem, and weak approximation (Theorem 8.5) implies that $\varphi$ is surjective. The kernel of $\varphi$ is clearly $K^{\mathfrak{m},1}$, thus $\varphi$ induces an isomorphism $K^{\mathfrak{m}}/K^{\mathfrak{m},1} \simeq \{\pm\}^{\#\mathfrak{m}_\infty} \times (\mathcal{O}_K/\mathfrak{m}_0)^\times$. This isomorphism is canonical, because $\bar{\alpha}$ depends only on the uniquely determined ideals $(a)$ and $(b)$ (if we replace $a$ with $a' = au$ for some $u \in \mathcal{O}_K^\times$ we must replace $b$ with $b' = bu$). □

**Corollary 21.7.** *Let $K$ be a number field and let $\mathfrak{m}$ be a modulus for $K$. The ray class group $\mathrm{Cl}_K^{\mathfrak{m}}$ is a finite abelian group whose cardinality $h_K^{\mathfrak{m}} := \#\mathrm{Cl}_K^{\mathfrak{m}}$ is given by*

$$h_K^{\mathfrak{m}} = \frac{\phi(\mathfrak{m})h_K}{[\mathcal{O}_K^\times : \mathcal{O}_K^\times \cap K^{\mathfrak{m},1}]},$$

*where $h_K := \#\mathrm{Cl}_K$ and $\phi(\mathfrak{m}) := \#(K^{\mathfrak{m}}/K^{\mathfrak{m},1}) = \phi(\mathfrak{m}_\infty)\phi(\mathfrak{m}_0)$, with*

$$\phi(\mathfrak{m}_\infty) = 2^{\#\mathfrak{m}_\infty}, \qquad \phi(\mathfrak{m}_0) = \#(\mathcal{O}_K/\mathfrak{m}_0)^\times = \mathrm{N}(\mathfrak{m}_0)\prod_{\mathfrak{p}|\mathfrak{m}_0}(1 - \mathrm{N}(\mathfrak{p})^{-1}).$$

*In particular, $h_K | h_K^{\mathfrak{m}}$ and $h_K^{\mathfrak{m}} | (h_K\phi(\mathfrak{m}))$.*

Explicitly computing the integer $h_K^{\mathfrak{m}}$ is not a trivial problem, but there are algorithms for doing so; see [1], which considers this problem in detail.

## 21.4 Polar density

We now want to prove the surjectivity of the Artin map for finite abelian extensions $L/K$ of number fields; as explained in §21.2, we already know this for $K = \mathbb{Q}$. In order to do so we first introduce a new way to measure the density of a set of primes that is defined in terms of a generalization of the Dedekind zeta function.

**Definition 21.8.** Let $K$ be a number field and let $S$ be a set of primes of $K$. The *partial Dedekind zeta function* associated to $S$ is the complex function

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

which converges to a holomorphic function on $\mathrm{Re}(s) > 1$ (by the same argument we used for $\zeta_K(s)$ in Lecture 18).

If $S$ is finite then $\zeta_{K,S}(s)$ is certainly holomorphic (and nonzero) on a neighborhood of 1. If $S$ contains all but finitely many primes of $K$ then it differs from $\zeta_K(s)$ by a holomorphic factor and therefore extends to a meromorphic function with a simple pole at $s = 1$, by Theorem 19.12.

Between these two extremes the function $\zeta_{K,S}(s)$ may or may not extend to a function that is meromorphic on a neighborhood of 1, but if it does, or more generally, if some power of it does, then we can use the order of the pole at 1 (or the absence of a pole) to measure the density of $S$.

**Definition 21.9.** If for some integer $n \geq 1$ the function $\zeta_{K,S}^n$ extends to a meromorphic function on a neighborhood of 1, the *polar density* of $S$ is defined by

$$\rho(S) := \frac{m}{n}, \qquad m = -\mathrm{ord}_{s=1}\zeta_{K,S}^n(s)$$

(so $m$ is the order of the pole at $s = 1$, if one is present). Note that if $\zeta_{K,S}^{n_1}$ and $\zeta_{K,s}^{n_2}$ both extend to a meromorphic function on a neighborhood of 1 then we necessarily have

$$n_2\mathrm{ord}_{s=1}\zeta_{K,S}^{n_1}(s) = \mathrm{ord}_{s=1}\zeta_{K,S}^{n_1 n_2} = n_1\mathrm{ord}_{s=1}\zeta_{K,S}^{n_2},$$

which implies that $\rho(S)$ does not depend on the choice of $n$.

In Lecture 17 we encountered two other notions of density, the *Dirichlet density*

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

(the equality of the two expressions for $d(S)$ follows from the fact that $\zeta_K(s)$ has a simple pole at $s = 1$, see Problem Set 9), and the *natural density*

$$\delta(S) := \lim_{x\to\infty} \frac{\#\{\mathfrak{p} \in S : \mathrm{N}(\mathfrak{p}) \leq x\}}{\#\{\mathfrak{p} : \mathrm{N}(\mathfrak{p}) \leq x\}}.$$

On Problem Set 9 you proved that if $S$ has a natural density then it has a Dirichlet density and the two coincide. We now show that the same is true of the polar density.

**Proposition 21.10.** *Let $S$ be a set of primes of a number field $K$. If $S$ has a polar density then it has a Dirichlet density and the two are equal.*

*Proof.* Suppose $S$ has polar density $\rho(S) = m/n$. By taking the Laurent series expansion of $\zeta_{K,S}^n(s)$ as $s = 1$ and factoring out the leading nonzero term we can write

$$\zeta_{K,S}(s)^n = \frac{a}{(s-1)^m}\left(1 + \sum_{n>1} a_n(s-1)^n\right),$$

for some $a \in \mathbb{C}^\times$. We must have $a \in \mathbb{R}_{>0}$, since $\zeta_{K,S}(s) \in \mathbb{R}_{>0}$ for $s \in \mathbb{R}_{>1}$ and therefore $\lim_{s\to 1}(s-1)^m\zeta_{K,S}(s)^n$ is a positive real number. Taking logs of both sides yields

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

which implies that $S$ has Dirichlet density $d(S) = m/n$. □

**Corollary 21.11.** *Let $S$ be a set of primes of a number field $K$. If $S$ has both a polar density and a natural density then the two coincide.*

We should note that not every set of primes with a natural density has a polar density, since the later is always a rational number while the former need not be.

Recall that a degree-1 prime in a number field $K$ is a prime with residue field degree 1 over $\mathbb{Q}$, equivalently, a prime $\mathfrak{p}$ whose absolute norm $\mathrm{N}(\mathfrak{p}) = [\mathcal{O}_K : \mathfrak{p}]$ is prime.

**Proposition 21.12.** *Let $S$ and $T$ denote sets of primes in a number field $K$ and let $\mathcal{P}$ be the set of all primes of $K$.*

(a) *If $S$ is finite then $\rho(S) = 0$; if $\mathcal{P} - S$ is finite then $\rho(S) = 1$.*

(b) *If $S \subseteq T$ both have polar densities, then $\rho(S) \leq \rho(T)$.*

(c) *If two sets $S$ and $T$ have finite intersection and any two of the sets $S$, $T$, and $S \cup T$ have polar densities then so does the third and $\rho(S \cup T) = \rho(S) + \rho(T)$.*

(d) *The polar density of all degree-1 primes is 1 and the polar density of any set of primes is determined by its subset of degree-1 primes.*

*Proof.* We first note that for any finite set $S$, the function $\zeta_{K,S}(s)$ is a finite product of nonvanishing entire functions and therefore holomorphic and nonzero everywhere (including at $s = 1$). If the symmetric difference of $S$ and $T$ is finite, then $\zeta_{K,S}(s)f(s) = \zeta_{K,T}(s)g(s)$ for some nonvanishing functions $f(s)$ and $g(s)$ holomorphic on $\mathbb{C}$. Thus if $S$ and $T$ differ by a finite set, then $\rho(S) = \rho(T)$ whenever either set has a polar density

Part (a) follows, since $\rho(\emptyset) = 0$ and $\rho(\mathcal{P}) = 1$ (note that $\zeta_{K,\mathcal{P}}(s) = \zeta_K(s)$, and $\operatorname{ord}_{s=1}\zeta_K(s) = -1$, by Theorem 19.12).

Part (b) follows from the analogous statement for Dirichlet density proved on Problem Set 9.

For (c) we may assume $S$ and $T$ are disjoint (by the argument above), in which case $\zeta_{K,S\cup T}(s)^n = \zeta_{K,S}(s)^n\zeta_{K,T}(s)^n$ for all $n \geq 1$, and the claim follows.

For (d), let $S_1$ be the set of all degree-1 primes and let $S_2 = \mathcal{P} - S$, so that $\mathcal{P} = S_1 \sqcup S_2$. For each rational prime $p$ there are at most $n := [K : \mathbb{Q}]$ (in fact $n/2$) primes $\mathfrak{p}|p$ in $S_2$, each of which has absolute norm $\mathrm{N}(\mathfrak{p}) \geq p^2$. It follows by comparison with $\zeta(2s)^n$ that the product defining $\zeta_{K,S_2}(s)$ converges absolutely to a holomorphic function on $\mathrm{Re}(s) > 1/2$ and is therefore holomorphic (and nonvanishing) on a neighborhood of 1; thus $\rho(S_2) = 0$ and $\rho(S_1) = 1$. For any set of primes $S$ we have $\rho(S\cap S_2) = 0$, so $\rho(S) = \rho(S\cap S_1)$ whenever $\rho(S \cap S_1)$ exists, by (c). □

For a finite Galois extension of number fields $L/K$, let $\mathrm{Spl}(L/K)$ denote the set of primes of $K$ that split completely in $L$. When $K$ is clear from context we may just write $\mathrm{Spl}(L)$.

**Theorem 21.13.** *Let $L/K$ be a Galois extension of number fields of degree $n$. Then*

$$\rho(\mathrm{Spl}(L)) = 1/n.$$

*Proof.* Let $S$ be the set of degree-1 primes that split completely in $L$; by Proposition 21.12, it suffices to show $\rho(S) = 1/n$. Recall that $\mathfrak{p}$ splits completely in $L$ if and only if both the ramification index $e_\mathfrak{p}$ and residue field degree $f_\mathfrak{p}$ are equal to 1. Let $T$ be the set of primes $\mathfrak{q}$ of $L$ that lie above some $\mathfrak{p} \in S$. For each $\mathfrak{q} \in T$ lying above $\mathfrak{p} \in S$ we have $\mathrm{N}_{L/K}(\mathfrak{q}) = \mathfrak{p}^{f_\mathfrak{p}} = \mathfrak{p}$, so $\mathrm{N}(\mathfrak{q}) = \mathrm{N}(\mathrm{N}_{L/K}(\mathfrak{q})) = \mathrm{N}(\mathfrak{p})$, thus $\mathfrak{q}$ is a degree-1 prime, since $\mathfrak{p}$ is.

On the other hand, if $\mathfrak{q}$ is any unramified degree-1 prime of $L$ and $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$, then $N(\mathfrak{q}) = \mathrm{N}(\mathrm{N}_{L/K}(\mathfrak{q})) = \mathrm{N}(\mathfrak{p}^{f_\mathfrak{p}})$ is prime, so we must have $f_\mathfrak{p} = 1$, and $e_\mathfrak{p} = 1$ since $\mathfrak{q}$ is unramified, so $\mathfrak{p}$ splits completely in $L$. Only finitely many primes ramify, so all but finitely many of the degree-1 primes in $L$ lie in $T$ and therefore $\rho(T) = 1$, by Proposition 21.12. Each $\mathfrak{p} \in S$ has exactly $n$ primes $\mathfrak{q} \in T$ lying above it (since $\mathfrak{p}$ splits completely), thus

$$\zeta_{L,T}(s) = \prod_{\mathfrak{q}\in T}(1 - \mathrm{N}(\mathfrak{q})^{-s})^{-1} = \prod_{\mathfrak{q}\in T}(1 - \mathrm{N}(\mathrm{N}_{L/K}(\mathfrak{q}))^{-s})^{-1} = \prod_{\mathfrak{p}\in S}(1 - \mathrm{N}(\mathfrak{p})^{-s})^{-n} = \zeta_{K,S}(s)^n.$$

Therefore $\rho(S) = \frac{1}{n}\rho(T) = \frac{1}{n}$ as desired. □

**Corollary 21.14.** *If $L/K$ is a finite extension of number fields with Galois closure $M/K$ of degree $n$, then $\rho(\operatorname{Spl}(L)) = \rho(\operatorname{Spl}(M)) = 1/n$*

*Proof.* A prime $\mathfrak{p}$ of $K$ splits completely in $L$ if and only if it splits completely in all the conjugates of $L$ in $M$; the Galois closure $M$ is the compositum of the conjugates of $L$, so $\mathfrak{p}$ splits completely in $L$ if and only if it splits completely in $M$. □

**Corollary 21.15.** *Let $L/K$ be a finite Galois extension of number fields with Galois group $G := \operatorname{Gal}(L/K)$ and let $H$ be a normal subgroup of $G$. The set $S$ of primes for which $\operatorname{Frob}_{\mathfrak{p}} \subseteq H$ has polar density $\rho(S) = \#H/\#G$.*

*Proof.* Let $F = L^H$; then $F/K$ is Galois (since $H$ is normal) and $\operatorname{Gal}(F/K) \simeq G/H$. For each unramified prime $\mathfrak{p}$ of $K$, the Frobenius class $\operatorname{Frob}_{\mathfrak{p}}$ lies in $H$ if and only if every $\sigma_{\mathfrak{q}} \in \operatorname{Frob}_{\mathfrak{p}}$ acts trivially on $L^H = F$, which occurs if and only if $\mathfrak{p}$ splits completely in $F$. By Theorem 21.13, the density of this set of primes is $1/[F : K] = \#H/\#G$. □

If $S$ and $T$ are sets of primes whose symmetric difference is finite, then either $\rho(S) = \rho(T)$ or neither set has a polar density. Let us write $S \sim T$ to indicate that two sets of primes have finite symmetric difference (this is clearly an equivalence relation), and partially order sets of primes by defining $S \precsim T \Leftrightarrow S \sim S \cap T$ (all but finitely many of the primes in $S$ lie in $T$). If $S$ and $T$ have polar densities, then $S \precsim T$ implies $\rho(S) \leq \rho(T)$.

**Theorem 21.16.** *If $L/K$ and $M/K$ are two finite Galois extensions of number fields then*

$$\begin{aligned} L \subseteq M &\Longleftrightarrow \operatorname{Spl}(M) \precsim \operatorname{Spl}(L) \Longleftrightarrow \operatorname{Spl}(M) \subseteq \operatorname{Spl}(L), \\ L = M &\Longleftrightarrow \operatorname{Spl}(M) \sim \operatorname{Spl}(L) \Longleftrightarrow \operatorname{Spl}(M) = \operatorname{Spl}(L), \end{aligned}$$

*and the map $L \mapsto \operatorname{Spl}(L)$ is an injection from the set of finite Galois extensions of $K$ (inside some fixed $\overline{K}$) to sets of primes of $K$ that have a positive polar density.*

*Proof.* The implications $L \subseteq M \Rightarrow \operatorname{Spl}(M) \subseteq \operatorname{Spl}(L) \Rightarrow \operatorname{Spl}(M) \precsim \operatorname{Spl}(L)$ are clear, so it suffices to show if $\operatorname{Spl}(M) \precsim \operatorname{Spl}(L) \Rightarrow L \subseteq M$.

A prime $\mathfrak{p}$ of $K$ splits completely in the compositum $LM$ if and only if it splits completely in both $L$ and $M$: the forward implication is clear and for the reverse we first note that if $\mathfrak{p}$ splits completely in both $L$ and $M$ then it certainly splits completely in $L \cap M$, so we may assume $K = L \cap M$; we then have $\operatorname{Gal}(LM/K) \simeq \operatorname{Gal}(L/K) \times \operatorname{Gal}(M/K)$, and if the decomposition subgroups of all primes above $\mathfrak{p}$ are trivial in both $\operatorname{Gal}(L/K)$ and $\operatorname{Gal}(M/K)$ then the same applies in $\operatorname{Gal}(LM/K)$. Thus $\operatorname{Spl}(LM) = \operatorname{Spl}(L) \cap \operatorname{Spl}(M)$.

It follows that $\operatorname{Spl}(M) \precsim \operatorname{Spl}(L) \Rightarrow \operatorname{Spl}(LM) \sim \operatorname{Spl}(M)$. By Theorem 21.13, we have $\rho(\operatorname{Spl}(M)) = 1/[M : K]$ and $\rho(\operatorname{Spl}(LM) = 1/[LM : K]$, thus $\operatorname{Spl}(LM) \sim \operatorname{Spl}(M)$ implies

$$[LM : K] = \rho(\operatorname{Spl}(LM)) = \rho(\operatorname{Spl}(M)) = [M : K],$$

in which case $LM = M$ and $L \subseteq M$. This proves $\operatorname{Spl}(M) \precsim \operatorname{Spl}(L) \Rightarrow L \subseteq M$, so the three conditions in the first line of biconditionals are all equivalent, and this immediately implies the second line of biconditionals. The last statement of the theorem is clear, since $\operatorname{Spl}(L)$ has positive polar density, by Theorem 21.13. □

### 21.5 Ray class fields and Artin reciprocity

As a special case of Corollary 21.14, if $F/K$ is a finite extension of number fields in which all but finitely many primes split completely, then $[F:K]=1$ and therefore $F=K$. This implies that the Artin map is surjective.

**Theorem 21.17.** *Let $L/K$ be a finite abelian extension of number fields and let $\mathfrak{m}$ be a modulus for $K$ divisible by all ramified primes. The Artin map $\psi_{L/K}^{\mathfrak{m}}\colon \mathcal{I}_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ is surjective.*

*Proof.* Let $H \subseteq \mathrm{Gal}(L/K)$ be the image of $\psi_{L/K}^{\mathfrak{m}}$ and let $F = L^H$ be its fixed field. For each prime $\mathfrak{p} \in \mathcal{I}_K^{\mathfrak{m}}$ the automorphism $\psi_{L/K}^{\mathfrak{m}}(\mathfrak{p})$ acts trivially on $F$, which implies that $\psi_{F/K}^{\mathfrak{m}}(\mathfrak{p}) = 1$ and therefore $\mathfrak{p}$ splits completely in $F$. The group $\mathcal{I}_K^{\mathfrak{m}}$ contains all but finitely many primes $\mathfrak{p}$ of $K$, so the polar density of the set of primes of $K$ that split completely in $F$ is 1, therefore $[F:K]=1$ and $H = \mathrm{Gal}(L/K)$. □

The theorem implies that we have an exact sequence

$$1 \to \ker \psi_{L/K}^{\mathfrak{m}} \to \mathcal{I}_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K) \to 1.$$

One of the key results of class field theory is that for a suitable choice of the modulus $\mathfrak{m}$, we have $\mathcal{R}_K^{\mathfrak{m}} \subseteq \ker \psi_{L/K}^{\mathfrak{m}}$. This implies that the Artin map induces an isomorphism between $\mathrm{Gal}(L/K)$ and a quotient of the ray class group $\mathrm{Cl}_K^{\mathfrak{m}} = \mathcal{I}_K^{\mathfrak{m}}/\mathcal{R}_K^{\mathfrak{m}}$.

If $\mathcal{R}_K^{\mathfrak{m}} = \ker \psi_{L/K}^{\mathfrak{m}}$, then we have an isomorphism $\mathrm{Gal}(L/K) \simeq \mathrm{Cl}_K^{\mathfrak{m}}$. Such a field $L$ is called the *ray class field* of $K$ for the modulus $\mathfrak{m}$. When $K=\mathbb{Q}$ the ray class group for $\mathfrak{m} = (m)\infty$ is the cyclotomic field $\mathbb{Q}(\zeta_m)$. For $K \neq \mathbb{Q}$ it is far from obvious that ray class fields exist, but this is indeed the case; this is one of the main theorems of class field theory. Once we have a ray class field $L/K$ for the modulus $\mathfrak{m}$, the Artin map allows us to relate subfields of $L$ to quotients of the ray class group $\mathrm{Cl}_K^{\mathfrak{m}} \simeq \mathrm{Gal}(L/K)$ in a way that we will make more precise in the next lecture; this is known as *Artin reciprocity.*

The ray class field for the trivial modulus $\mathfrak{m}=1$ has a special name; it is called the *Hilbert class field* of $K$. As we will prove in the next lecture, it is the maximal unramified abelian extension of $K$ (which is the usual way to define the Hilbert class field), and it is unique up to isomorphism. The Hilbert class field $L$ of $K$ has the remarkable property that $\mathrm{Gal}(L/K) \simeq \mathrm{Cl}_K$; it is a Galois extension of $K$ whose Galois group is canonically isomorphic to the class group of $K$. Every ray class field of $K$ necessarily contains the Hilbert class field. For $K=\mathbb{Q}$ the Hilbert class field is trivial, but in general a ray class field should really be viewed as a tower of two abelian extensions of $K$, the first of which is independent of the modulus $\mathfrak{m}$.

## References

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

[2] Allen Altman and Steven Kleiman, *A term of commutative algebra*, Worldwide Center of Mathematics, 2013.

18.785 Number Theory I
Fall 2016