# Notes on Class Field Theory

Alexandre Daoud
alex.daoud@mac.com

May 7, 2017

We first give an exposition of the classical approach to Class Field Theory via ideals. In Section 2, we introduce idèles and look at Class Field Theory in that setting, making sure to link back to the ideas in Section 1 heavily. We assume the content covered in what is typically a standard first two courses in Algebraic Number Theory. Likely sufficient is a first course in Algebraic Number Theory together with a first course in Local Fields.

## Contents

# 1 Ideal Approach to Global Class Field Theory

Throughout this section, $L/K$ shall be a finite extension of number fields. By $\mathcal{O}_K$ and $\mathcal{O}_L$ we shall mean the ring of integers of $K$ and $L$ respectively. Recall that $\mathcal{O}_K$ and $\mathcal{O}_L$ are Dedekind domains and so ideals of these rings admit a unique factorisation into prime ideals.

Let $K$ be a number field. By a **prime** $\mathfrak{p}$ of $K$, we mean an equivalence class of absolute values on $K$. Recall that by Ostrowski's Theorem, every absolute value $|\cdot|_\mathfrak{p}$ on $K$ is either a non-archimedean $\mathfrak{p}$-adic absolute value or an archimedean absolute value. We may thus identify the primes of $K$ with prime ideals (henceforth the **finite primes**) of $\mathcal{O}_K$ and the field embeddings $K \hookrightarrow \mathbb{C}$ (henceforth the **infinite primes**). Given a prime $\mathfrak{p}$ of $K$, we shall write $K_\mathfrak{p}$ for its completion with respect to $\mathfrak{p}$ (a **local field**). If $\mathfrak{p}$ is finite ($\mathfrak{p} \nmid \infty$) then we shall write $\mathcal{O}_{\mathfrak{p},K}$ for its ring of integers. If $\mathfrak{p}$ is infinite ($\mathfrak{p} \mid \infty$) and corresponds to a real embedding we shall say that $\mathfrak{p}$ is **real**; if it corresponds to a complex embedding we shall say that $\mathfrak{p}$ is **complex**.

**Definition 1.1.** Let $\mathfrak{p} \triangleleft \mathcal{O}_K$ be a finite prime and suppose we have the factorisation

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}$$

where $\mathfrak{P}_i \triangleleft \mathcal{O}_L$ are distinct prime ideals and $g, e_i$ are positive integers. We say that each $\mathfrak{P}_i$ **lies over** $\mathfrak{p}$ and write $\mathfrak{P}_i/\mathfrak{p}$. We make the following definitions:

1. We say that $g$ is the **decomposition number** of $\mathfrak{p}$ in $L/K$.
2. We say that $e_i$ is the **ramification index** of $\mathfrak{P}_i$ in $L/K$.
3. We say that $\mathfrak{P}_i$ is **unramified** in $L/K$ if $e_i = 1$.
4. We say that $\mathfrak{p}$ is **unramified** in $L/K$ if $e_i = 1$ for all $1 \leq i \leq g$.
5. We say that $\mathfrak{p}$ is **totally ramified** in $L/K$ if there exists a unique prime $\mathfrak{q}$ of $L$ lying over $\mathfrak{p}$ and its ramification index is equal to $[L : K]$.
6. We define the **inertial degree** of $\mathfrak{P}_i$ in $L/K$, denoted $f_i$, to be $f_i = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$.
7. We say that $\mathfrak{p}$ **splits completely** if $e_i = f_i = 1$ for all $1 \leq i \leq g$.

**Definition 1.2.** Let $\mathfrak{p}$ be an infinite prime of $K$ and let $\mathfrak{P}$ be any infinite prime of $L$ extending $\mathfrak{p}$, denoted $\mathfrak{P}/\mathfrak{p}$. We define the **ramification index** to be $e(\mathfrak{P}/\mathfrak{p}) = [L_\mathfrak{P} : K_\mathfrak{p}]$. If $e(\mathfrak{P}/\mathfrak{p}) = 1$ we say that $\mathfrak{P}/\mathfrak{p}$ is **unramified**. If $e(\mathfrak{P}/\mathfrak{p}) = 2$ we say that $\mathfrak{P}/\mathfrak{p}$ is **ramified**. For notational conveniences, we shall always set $f(\mathfrak{P}/\mathfrak{p}) = 1$.

**Proposition 1.3.** *Suppose that $L/K$ is Galois and $\mathfrak{p}$ is a finite prime of $K$ admitting a factorisation*

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}$$

*in $\mathcal{O}_L$. Then $\mathrm{Gal}(L/K)$ acts via transitive permutation on the $\mathfrak{P}_i$.*

*Proof.* Fix $\sigma \in \mathrm{Gal}(L/K)$ and $1 \leq i \leq g$. We first claim that $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$ for some $1 \leq i \leq g$. Indeed, $\sigma$ restricts to a ring automorphism of $\mathcal{O}_L$ and so we can write $\sigma(\mathfrak{P}_i) = (\sigma^{-1})^{-1}(\mathfrak{P}_i)$. Since the inverse image of a prime ideal is again a prime ideal, we see that $\sigma(\mathfrak{P}_i)$ is some prime ideal of $\mathcal{O}_L$. But $\sigma$ fixes $\mathcal{O}_K$ and, in particular, $\mathfrak{p}$ and so $\mathfrak{p} \subseteq \sigma(\mathfrak{P}_i)$. Hence $\sigma(\mathfrak{P}_i)$ is a

prime of $\mathcal{O}_L$ lying over $\mathfrak{p}$. The only such primes are the ones that appear in the factorisation of $\mathfrak{p}\mathcal{O}_L$ and so $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$ for some $1 \leq j \leq g$ and so $\sigma$ permutes the $\mathfrak{P}_j$.

Fix $1 \leq i, j \leq g$. We need to show that there exists $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$. By the Chinese Remainder Theorem, we have that

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathcal{O}_L/\mathfrak{P}_i^{e_i}$$

and so we can always choose $x \in \mathcal{O}_L$ such that $x \in \mathfrak{P}_i$ but $x \notin \mathfrak{P}_n$ for $i \neq n$. Note that

$$\mathrm{N}_{L/K}(x) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x) \in \mathcal{O}_K \cap \mathfrak{P}_i = \mathfrak{p} \subseteq \mathfrak{P}_j$$

Now, $\mathfrak{P}_j$ is a prime ideal and so $\sigma(x) \in \mathfrak{P}_j$ for some $\sigma \in \mathrm{Gal}(L/K)$. But, by construction, $\sigma(\mathfrak{P}_i)$ is the only prime ideal satisfying $\sigma(x) \in \sigma(\mathfrak{P}_i)$ so we must have that $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$ as desired. □

**Corollary 1.4.** *Suppose that $L/K$ is Galois and $\mathfrak{p}$ is a finite prime of $K$ admitting a factorisation*

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}$$

*in $\mathcal{O}_L$. Then $e_1 = \dots = e_g$, $f_1 = \dots = f_g$ and $efg = [L : K]$.*

*Proof.* Since the action of $\mathrm{Gal}(L/K)$ on the $\mathfrak{P}_i$ is transitive, it follows immediately that $e_i = e_j$ for all $1 \leq i, j \leq g$. Furthermore, we must have that $\mathcal{O}_L/\mathfrak{P}_i \cong \mathcal{O}_L/\mathfrak{P}_j$ and so $f_i = f_j$ for all $1 \leq i, j \leq g$. The last formula follows from the fact that $[L : K] = e_i f_i$ which itself is a consequence of the multiplicativity of the norm map. □

**Remark.** From now on, when $L/K$ is Galois, we shall write $e_\mathfrak{p}$ and $f_\mathfrak{p}$ for the common ramification indices and inertial degrees of $\mathfrak{p}$ and $g_\mathfrak{p}$ for the decomposition number.

**Definition 1.5.** Suppose that $L/K$ is Galois, $\mathfrak{p}$ a finite prime of $K$ and $\mathfrak{P}$ a prime of $L$ lying over $\mathfrak{p}$. We define the **decomposition group relative to $\mathfrak{P}$** to be

$$\mathrm{Gal}(L/K)_\mathfrak{P} = \{\, \sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathfrak{P}) = \mathfrak{P} \,\}$$

**Lemma 1.6.** *Suppose that $L/K$ is Galois, $\mathfrak{p}$ be a finite prime of $K$ and $\mathfrak{P}_i$ the primes of of $L$ lying over $\mathfrak{p}$. Then $|\mathrm{Gal}(L/K)_\mathfrak{P}| = e_\mathfrak{p} f_\mathfrak{p}$.*

*Proof.* Since $\mathrm{Gal}(L/K)$ acts transitively on the $\mathfrak{P}_i$, it follows that the index of $\mathrm{Gal}(L/K)_\mathfrak{P}$ in $\mathrm{Gal}(L/K)$ is $g_\mathfrak{p}$. But $|\mathrm{Gal}(L/K)| = [L : K] = g_\mathfrak{p} e_\mathfrak{p} f_\mathfrak{p}$. The Lemma then follows upon appealing to Lagrange's Theorem. □

**Lemma 1.7.** *Suppose that $L/K$ is Galois, $\mathfrak{p}$ a finite prime of $K$ and $\mathfrak{P}$ a prime of $L$ lying over $\mathfrak{p}$. Then $[L_\mathfrak{P} : K_\mathfrak{p}] = e_\mathfrak{p} f_\mathfrak{p}$.*

*Proof.* Recall that $\mathcal{O}_{\mathfrak{p},K}$ and $\mathcal{O}_{\mathfrak{P},L}$ are discrete valuation rings so they both each have a unique maximal ideal. We shall refer to these ideals by $\widehat{\mathfrak{p}}$ and $\widehat{\mathfrak{P}}$ respectively. Furthermore, $\mathcal{O}_{\mathfrak{p},K}$ and $\mathcal{O}_{\mathfrak{P},L}$ are both Dedekind domains so we have the factorisation

$$\widehat{\mathfrak{p}}\mathcal{O}_{\mathfrak{P},L} = \widehat{\mathfrak{P}}^e$$

for some integer $e > 0$. Let $f$ be the inertial degree of $\widehat{\mathfrak{P}}$ in $L_{\mathfrak{P}}/K_{\mathfrak{p}}$. Then $[L_{\mathfrak{P}} : K_{\mathfrak{p}}] = ef$. We first claim that $f = f_{\mathfrak{p}}$. Indeed, recall that $[\mathcal{O}_{\mathfrak{P},L} : \mathcal{O}_{\mathfrak{p},K}] = [\mathcal{O}_L : \mathcal{O}_K]$ whence the claim follows.

Now let $\mathfrak{P}_1, \ldots, \mathfrak{P}_j$ be the other primes of $L$ lying over $\mathfrak{p}$. Then

$$\widehat{\mathfrak{p}}\mathcal{O}_{\mathfrak{P},L} = (\mathfrak{p}\mathcal{O}_{\mathfrak{p},K})\mathcal{O}_{\mathfrak{P},L} = (\mathfrak{p}\mathcal{O}_L)\mathcal{O}_{\mathfrak{P},L} = \mathfrak{P}^{e_{\mathfrak{p}}} \left( \prod_{i=1}^{n} \mathfrak{P}_i^{e_{\mathfrak{p}}} \right) \mathcal{O}_{\mathfrak{P},L} = \mathfrak{P}^{e_{\mathfrak{p}}}\mathcal{O}_{\mathfrak{P},L} = \widehat{\mathfrak{P}}^{e_{\mathfrak{p}}}$$

and so $e = e_{\mathfrak{p}}$ as desired. □

**Proposition 1.8.** *Suppose that $L/K$ is Galois, $\mathfrak{p}$ a finite prime of $K$ and $\mathfrak{P}$ a prime of $L$ lying over $\mathfrak{p}$. Then $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is Galois and*

$$\mathrm{Gal}(L/K)_{\mathfrak{P}} \cong \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$$

*Proof.* Let $\sigma \in \mathrm{Gal}(L/K)_{\mathfrak{P}}$. Then $\sigma$ acts as an isometry of the absolute value $|\cdot|_{\mathfrak{P}}$ of L and, in particular, it preserves Cauchy sequences in $L$. Thus $\sigma$ extends to a $K_{\mathfrak{p}}$-automorphism of $L_{\mathfrak{P}}$. This induces an injection $\mathrm{Gal}(L/K)_{\mathfrak{P}} \hookrightarrow \mathrm{Aut}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$.

Conversely, fix $\sigma \in \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$. Then $\sigma|_L$ is clearly a $K$-automorphism of $L$. Furthermore, this restriction mapping is injective since $K$ is dense in $K_{\mathfrak{p}}$ and $L$ is dense in $L_{\mathfrak{P}}$. Since $\sigma$ fixes $|\cdot|_{\mathfrak{P}}$, it follows that $\sigma_L(\mathfrak{P}) = \mathfrak{P}$ and so we get an injection $\mathrm{Aut}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$. This easily yields an isomorphism $\mathrm{Gal}(L/K)_{\mathfrak{P}} \cong \mathrm{Aut}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$.

The Lemmata 1.6 and 1.7 then imply that $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is Galois and so $\mathrm{Gal}(L/K)_{\mathfrak{P}} \cong \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$. □

Given a finite prime $\mathfrak{p}$ of $K$ and $\mathfrak{P}$ a prime of $L$ lying over $\mathfrak{p}$. Let $\mathbb{F}_{\mathfrak{P}} = \mathcal{O}_{\mathfrak{P},L}/\mathfrak{P}$ and $\mathbb{F}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p},K}/\mathfrak{p}$. Then $\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ surjects onto $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$.

**Definition 1.9.** Suppose that $L/K$ is Galois, $\mathfrak{p}$ a finite prime of $K$ and $\mathfrak{P}$ a prime of $L$ lying over $\mathfrak{p}$. We define the **inertial group relative to $\mathfrak{P}$**, denoted, $I_{\mathfrak{P}}$, to be the subgroup of elements of $\mathrm{Gal}(L/K)_{\mathfrak{P}}$ that become trivial in $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$.

**Definition 1.10.** Suppose that $L/K$ is Galois, $\mathfrak{p}$ a finite unramified prime of $K$ and $\mathfrak{P}$ a prime of $L$ lying over $\mathfrak{p}$. We define the **Frobenius element** of $\mathrm{Gal}(L/K)_{\mathfrak{P}}$ to be the unique element of $\mathrm{Gal}(L/K)_{\mathfrak{P}}$ that acts as Frobenius on $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$ and is denoted by

$$\left( \frac{L/K}{\mathfrak{P}} \right)$$

In other words, it is the unique element of $\mathrm{Gal}(L/K)_{\mathfrak{P}}$ that maps to the Frobenius automorphism $(x \mapsto x^{|\mathbb{F}_{\mathfrak{p}}|})$.

**Proposition 1.11.** *Suppose that $L/K$ is Galois, $\mathfrak{p}$ a finite prime of $K$ and $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ the primes of $L$ lying over $\mathfrak{p}$. Let $i \neq j$ and $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$. Then*

$$\mathrm{Gal}(L/K)_{\mathfrak{P}_j} = \sigma \,\mathrm{Gal}(L/K)_{\mathfrak{P}_i} \sigma^{-1}$$

*If furthermore $\mathfrak{p}$ is unramified then*

$$\left( \frac{L/K}{\mathfrak{P}_j} \right) = \sigma \left( \frac{L/K}{\mathfrak{P}_i} \right) \sigma^{-1}$$

*Proof.* First let $x \in \sigma \operatorname{Gal}(L/K)_{\mathfrak{P}_i}\sigma^{-1}$ so that $x = \sigma\tau\sigma^{-1}$ for some $\tau \in \operatorname{Gal}(L/K)_{\mathfrak{P}_i}$. Then

$$x(\mathfrak{P}_j) = \sigma\tau\sigma^{-1}(\mathfrak{P}_j) = \sigma\tau(\mathfrak{P}_i) = \sigma(\mathfrak{P}_j) = \mathfrak{P}_j$$

so $x \in \operatorname{Gal}(L/K)_{\mathfrak{P}_j}$. The converse follows via symmetry.

Now, let $\tau \in \operatorname{Gal}(L/K)_{\mathfrak{P}_i}$ be the Frobenius element relative to $\mathfrak{P}_i$ and $q = |\mathbb{F}_\mathfrak{p}|$. Then for all $x \in \mathcal{O}_L$ we have $\tau(x) \equiv x^q \pmod{\mathfrak{P}_i}$. In particular, we have $\tau(\sigma^{-1}(x)) \equiv \sigma^{-1}(x)^q \pmod{\mathfrak{P}_i}$. Left-composing by $\sigma$ yields $\sigma\tau\sigma^{-1}(x) \equiv x^q \pmod{\mathfrak{P}_j}$ as desired. □

**Corollary 1.12.** *Suppose that $L/K$ is abelian, $\mathfrak{p}$ a finite unramified prime of $K$ and $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ the primes of $L$ lying over $\mathfrak{p}$. Then*

$$\left(\frac{L/K}{\mathfrak{P}_i}\right) = \left(\frac{L/K}{\mathfrak{P}_j}\right)$$

*for all $i \neq j$.*

**Definition 1.13.** Suppose that $L/K$ is abelian and $\mathfrak{p}$ a finite unramified prime of $K$ and $\mathfrak{P}$ a prime of $L$ lying over $\mathfrak{p}$. Then we define the **Frobenius element** (or **Artin symbol**) relative to $\mathfrak{p}$ to be the Frobenius element relative to $\mathfrak{P}$ and denote it

$$\left(\frac{L/K}{\mathfrak{p}}\right)$$

**Proposition 1.14.** *Suppose that $L/K$ is abelian and $\mathfrak{p}$ a finite prime of $K$ and $\mathfrak{P}$ a prime of $L$ lying over $\mathfrak{p}$. Then $((L/K)/\mathfrak{p}) = 1$ if and only if $\mathfrak{p}$ splits completely in $L$.*

Let $M_K$ be the set of all primes of $K$, $M_K^\infty$ the subset of infinite primes

*Proof.* We have that

$$\begin{aligned}
\left(\frac{L/K}{\mathfrak{p}}\right) = 1 &\iff \text{the identity is the unique element of } \operatorname{Gal}(L/K)_\mathfrak{p} \\
&\qquad \text{acting as Frobenius on } \mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p} \\
&\iff [\mathbb{F}_\mathfrak{P} : \mathbb{F}_\mathfrak{p}] = 1 \\
&\iff f_\mathfrak{p} = 1 \\
&\iff \mathfrak{p} \text{ splits completely in } L
\end{aligned}$$

□

**Definition 1.15.** Suppose that $L/K$ is abelian and let $S$ be the collection of all infinite primes of $K$ and the finite primes of $K$ that ramify in $L$. Let $I_K^S$ be the subgroup of all fractional ideals of $K$ that do not contain a prime of $S$ in their factorisation. We define the **Artin map** to be the unique homomorphism $\varphi_{L/K}^S : I_K^S \to \operatorname{Gal}(L/K)$ that extends the Artin symbol. In other words, let $\mathfrak{a} = \prod_{i=1}^n \mathfrak{p}_i^{a_i}$ for some finite unramified primes $\mathfrak{p}_i$ of $K$ and integers $a_i$. Then the Artin map is given by

$$\begin{aligned}
\left(\frac{L/K}{\cdot}\right) : I_K^S &\to \operatorname{Gal}(L/K) \\
\mathfrak{a} &\mapsto \prod_{i=1}^n \left(\frac{L/K}{\mathfrak{p}_i}\right)^{a_i}
\end{aligned}$$

**Remark.** Note that the Artin map is well-defined as $L/K$ is abelian. Furthermore, $S$ is finite since there are only finite many primes of $K$ that ramify in $L$. This follows from the fact that the primes of $K$ that ramify in $L$ are exactly those that divide the relative discriminant of $L/K$. For a proof of this in the case of $K/\mathbb{Q}$, see

**Definition 1.16.** We define the **relative norm map** from $L$ to $K$ to be the unique homomorphism

$$\mathrm{N}_{L/K}(\cdot) : I_L \to I_K$$

satisfying $\mathrm{N}_{L/K}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})}$ where $\mathfrak{P}$ is a finite prime of $L$ lying over the finite prime $\mathfrak{p}$ of $K$ which is then extended multiplicatively.

**Proposition 1.17.** *Suppose that $L/K$ is abelian and $K'$ is an intermediate extension of $L/K$. Let $S$ be a set of the finite primes of $K$ containing all those that ramify in $L$ and also those of $K'$ lying over the former primes. Then the diagram*

$$\begin{array}{ccc} I_{K'}^S & \xrightarrow{\varphi_{L/K'}^S} & \mathrm{Gal}(L/K') \\ \downarrow{\scriptstyle \mathrm{N}_{K'/K}(\cdot)} & & \downarrow \\ I_K^S & \xrightarrow{\varphi_{L/K}^S} & \mathrm{Gal}(L/K) \end{array}$$

*commutes.*

*Proof.* By multiplicativity, it suffices to prove the Proposition for prime ideals in $I_K'^S$. Fix a finite prime $\mathfrak{p}'$ of $K'$ lying over a prime $\mathfrak{p}$ of $K$ not in $S$. Then $\mathrm{N}_{K'/K}(\mathfrak{p}') = \mathfrak{p}^{f(\mathfrak{p}'/\mathfrak{p})}$. We thus need to show that

$$\varphi_{L/K'}^S(\mathfrak{p}') = \varphi_{L/K}^S(\mathfrak{p}^{f(\mathfrak{p}'/\mathfrak{p})})$$

In other words, we need to show that

$$\left(\frac{L/K'}{\mathfrak{P}}\right) = \left(\frac{L/K}{\mathfrak{P}}\right)^{f(\mathfrak{p}'/\mathfrak{p})}$$

for all primes $\mathfrak{P}$ lying over $\mathfrak{p}$. But this follows immediately from the fact that the Frobenius element in $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}'})$ is the $f(\mathfrak{p}'/\mathfrak{p})$-power of the Frobenius element in $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$. □

**Corollary 1.18.** *Suppose that $L/K$ is abelian and $S$ a collection of finite primes of $K$ containing those that ramify in $L$. Then*

$$\mathrm{N}_{L/K}(I_L^S) \subseteq \ker(\varphi_{L/K}^S)$$

*Proof.* The Corollary follows immediately upon taking $K' = L$ in the commutative diagram in Proposition 1.17. □

**Definition 1.19.** Let $S$ be the set of all primes of $K$. We define a **modulus** of $K$ to be a function $\mathfrak{m} : S \to \mathbb{Z}$ such that

1. $\mathfrak{m}(\mathfrak{p}) \geq 0$ for all $\mathfrak{p} \in S$ and $\mathfrak{m}(\mathfrak{p}) = 0$ for all but finitely many finite $\mathfrak{p}$.
2. $\mathfrak{m}(\mathfrak{p}) = 0$ or 1 for all real primes $\mathfrak{p}$.
3. $\mathfrak{m}(\mathfrak{p}) = 0$ for all complex primes $\mathfrak{p}$.

We shall write such a modulus as a formal product

$$\mathfrak{m} = \prod_{\mathfrak{p} \in S} \mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}$$

Moreover, we can write $\mathfrak{m} = \mathfrak{m}_\infty \mathfrak{m}_0$ where $\mathfrak{m}_\infty$ is the real infinite part of $\mathfrak{m}$ and $\mathfrak{m}_0$ is the finite part of $\mathfrak{m}$ which can be identified with an integral ideal of $\mathcal{O}_K$.

Given two moduli $\mathfrak{m}$ and $\mathfrak{n}$, we say that $\mathfrak{m}$ **divides** $\mathfrak{n}$ if $\mathfrak{m}(\mathfrak{p}) \leq \mathfrak{n}(\mathfrak{p})$ for all $\mathfrak{p} \in S$.

**Definition 1.20.** Let $\mathfrak{m}$ be a modulus of $K$ and $\alpha \in K^\times$. We say that $\alpha$ is **multiplicatively congruent** to 1 modulo $\mathfrak{m}$, denoted $\alpha \equiv 1 \pmod^\times \mathfrak{m}$, if

1. $\alpha \in 1 + \mathfrak{p}^{\mathfrak{m}(\mathfrak{p})} \mathcal{O}_{\mathfrak{p},K}$ for all finite primes $\mathfrak{p}$ such that $\mathfrak{m}(\mathfrak{p}) > 0$.
2. $|\alpha|_\mathfrak{p} > 0$ for all real primes $\mathfrak{p}$ such that $\mathfrak{m}(\mathfrak{p}) > 0$.

**Definition 1.21.** Let $\mathfrak{m}$ be a modulus of $K$. Let $I_K^\mathfrak{m}$ be the collection of fractional ideals of $K$ prime to $\mathfrak{m}$, $P_K^\mathfrak{m}$ the subgroup of $I_K^\mathfrak{m}$ consisting of principal ideals and define

$$P_K^{\mathfrak{m},1} = \{ (\alpha) \in P_K^\mathfrak{m} \mid \alpha \equiv 1 \pmod^\times \mathfrak{m} \}$$

We define the **ray class group modulo** $\mathfrak{m}$ to be the quotient $C_K^\mathfrak{m} = I_K^\mathfrak{m} / P_K^{\mathfrak{m},1}$.

**Theorem 1.22** (Weak Approximation Theorem)**.** *Let $K$ be a valued field and $|\cdot|_1, \ldots, |\cdot|_n$ a family of pair-wise non-equivalent, non-trivial absolute values on $K$. Given any $a_1, \ldots, a_1 \in K$ and $\varepsilon > 0$, there exists $b \in K$ such that $|a_i - b|_i < \varepsilon$ for all $1 \leq i \leq n$.*

*Proof.* See appendix of [4]. □

**Lemma 1.23.** *Let $\mathfrak{m}$ be a modulus of $K$ and $C_K$ the ideal class group of $K$. Then any ideal class in $C_K$ admits a representative that is prime to $\mathfrak{m}$.*

*Proof.* Fix an ideal class $[I] \in C_K$ and let its unique factorisation be $I = \prod_\mathfrak{p} \mathfrak{p}^{e_\mathfrak{p}}$. If $I$ is prime to $\mathfrak{m}$ then we are done. If not then we can write $I = \mathfrak{a}\mathfrak{a}'$ with $\mathfrak{a}$ prime to $\mathfrak{a}' = \prod_{\mathfrak{p}|\mathfrak{m}} \mathfrak{p}^{e_\mathfrak{p}}$. Choosing a uniformiser $\pi_\mathfrak{p}$ for each such prime, denote $\alpha = \prod_{\mathfrak{p}|\mathfrak{m}} \pi_\mathfrak{p}^{-e_\mathfrak{p}}$. Then $[\alpha\mathfrak{a}] = [\mathfrak{a}]$ and $(\alpha\mathfrak{a}, \mathfrak{a}) = 1$. □

**Theorem 1.24.** *Let $\mathfrak{m}$ be a modulus of $K$ and $C_K$ the ideal class group of $K$. Let $K^\mathfrak{m} = \{ \alpha \in K^\times \mid (\alpha) \in P_K^\mathfrak{m} \}$ and similarly for $K^{\mathfrak{m},1}$. Then we have an exact sequence*

$$1 \longrightarrow \mathcal{O}_K^\times / (\mathcal{O}_K^\times \cap K^{\mathfrak{m},1}) \longrightarrow K^\mathfrak{m} / K^{\mathfrak{m},1} \longrightarrow C_K^\mathfrak{m} \longrightarrow C_K \longrightarrow 1$$

*Furthermore, $K^\mathfrak{m} / K^{\mathfrak{m},1} \cong \{ \pm 1 \}^{|\mathfrak{m}_\infty|} \times (\mathcal{O}_K / \mathfrak{m}_0)^\times$. In particular, $C_K^\mathfrak{m}$ is finite.*

*Proof.* Denote by $\iota$ the inclusion $K^{\mathfrak{m},1} \hookrightarrow K^\mathfrak{m}$ and $\phi : K^\mathfrak{m} \to I_K^\mathfrak{m}$ the map given by $\alpha \mapsto (\alpha)$. Then we have a commutative diagram

$$\begin{array}{ccccccc} & & K^{\mathfrak{m},1} & \xrightarrow{\iota} & K^\mathfrak{m} & \longrightarrow & K^\mathfrak{m}/K^{\mathfrak{m},1} \longrightarrow 1 \\ & & \downarrow{\scriptstyle \phi\circ\iota} & & \downarrow{\scriptstyle \phi} & & \downarrow \\ 1 & \longrightarrow & I_K^\mathfrak{m} & \longrightarrow & I_K^\mathfrak{m} & \longrightarrow & 1 \end{array}$$

to which we would like to apply the Snake Lemma. Firstly, it is clear that $\ker(\iota) = 1$. We then have that $\ker(\phi \circ f) = \mathcal{O}_K^\times \cap K^{\mathfrak{m},1}$. Furthermore, $\ker(\phi) = \mathcal{O}_K^\times$. Now, $\operatorname{coker}(f) = K^\mathfrak{m}/K^{\mathfrak{m},1}$ from which we see that $\operatorname{coker}(\phi \circ f) = C_K^\mathfrak{m}$. Finally, $\operatorname{coker}(\phi) = C_K$ by Lemma 1.23. Thus the Snake Lemma implies that we have an exact sequence

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

The exact sequence in the Theorem then follows immediately.

To prove the isomorphism, note that, by the Chinese Remainder Theorem, it suffices to show that

$$K^{\mathfrak{m}}/K^{\mathfrak{m},1} \cong \{\pm 1\}^{|\mathfrak{m}_\infty|} \times \prod_{\mathfrak{p}|\mathfrak{m}_0} (\mathcal{O}_K/\mathfrak{p}^{\mathfrak{m}(\mathfrak{p})})^\times$$

We define a homomorphism

$$\psi : K^{\mathfrak{m}} \to \{\pm 1\}^{|\mathfrak{m}_\infty|} \times \prod_{\mathfrak{p}|\mathfrak{m}_0} (\mathcal{O}_K/\mathfrak{p}^{\mathfrak{m}(\mathfrak{p})})^\times$$

where $\alpha \in K^{\mathfrak{m}}$ is mapped to $\alpha/|\alpha|_{\mathfrak{p}}$ for real primes $\mathfrak{p}$ and to the quotient $\mathcal{O}_K/\mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}$ for the finite primes $\mathfrak{p}$. The latter is clearly well-defined since we can always choose $a, b \in \mathcal{O}_K$ such that $\alpha = a/b$ and both $(a)$ and $(b)$ prime to $\mathfrak{m}$ and to each other. Moreover, the image of $\alpha$ is contained in the unit group since $(\alpha)$ is coprime to $\mathfrak{m}$. The surjectivity of $\psi$ follows immediately by weak approximation. Now $\psi(\alpha) = 1$ if and only if $\alpha \equiv 1 \pmod^\times \mathfrak{m}$ if and only if $\alpha \in K^{\mathfrak{m},1}$ and so $\ker(\psi) = K^{\mathfrak{m},1}$ whence the Theorem follows. □

**Definition 1.25.** Let $\mathfrak{m}$ be a modulus for $K$. A **congruence subgroup** for $\mathfrak{m}$ is a subgroup $\mathcal{C}$ of $I_K^{\mathfrak{m}}$ that contains $P_K^{\mathfrak{m}}$.

**Definition 1.26.** Let $L/K$ be a finite abelian extension of local fields. We define the **conductor** of $L/K$, denoted $\mathfrak{f}(L/K)$ in the following way: If $K \cong \mathbb{R}$ and $L \cong \mathbb{C}$ then we write $\mathfrak{f}(L/K) = \infty$, else we write $\mathfrak{f}(L/K) = 1$. If $K$ is non-archimedean with unique maximal ideal $\mathfrak{p} \lhd \mathcal{O}_{\mathfrak{p},K}$ then we write $\mathfrak{f}(L/K) = \mathfrak{p}^f$ where $f = \min\{n \mid 1 + \mathfrak{p}^n \subseteq \mathrm{N}_{L/K}(L^\times)\}$.

If $L/K$ is a finite abelian extension of number fields then we define

$$\mathfrak{f}(L/K) = \prod_{\mathfrak{p}} \mathfrak{f}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$$

where $\mathfrak{P}$ is any prime of $L$ lying above $\mathfrak{p}$.

**Proposition 1.27.** *Suppose that $L/K$ is abelian. Then $\mathfrak{f}(L/K)$ is divisible by exactly the primes of $K$ that ramify in $L$.*

*Proof.* See Propositions 11.10 and 11.11 in [10]. □

**Theorem 1.28** (Class Field Theory)**.** *Let $\mathfrak{m}$ be a modulus for $K$. Then*

1. *(Existence) There exists an abelian extension of $K$, denoted $K(\mathfrak{m})$ and called the **ray class field** of $K$ modulo $\mathfrak{m}$, such that $C_K^{\mathfrak{m}} \cong \mathrm{Gal}(K(\mathfrak{m})/K)$ via the Artin map.*

2. *(Completeness) Given a finite abelian extension $L/K$, we have $L \subseteq K(\mathfrak{m})$ if and only if $\mathfrak{f}(L/K)$ divides $\mathfrak{m}$. In particular, every finite abelian extension of $K$ is contained in a ray class field of $K$ for some modulus $\mathfrak{m}$.*

3. *(Artin Recpirocity) For every intermediate field $L$ of $K(\mathfrak{m})/K$, the Artin map induces an isomorphism*

$$\varphi_{L/K}^{\mathfrak{m}} : \frac{I_K^{\mathfrak{m}}}{P_K^{\mathfrak{m},1}\,\mathrm{N}_{L/K}(I_L^{\mathfrak{m}})} \to \mathrm{Gal}(L/K)$$

*Moreover, the Artin map induces an order-preserving one-to-one correspondence between the abelian extensions $L/K$ with $\mathfrak{f}(L/K)$ dividing $\mathfrak{m}$ and the congruence subgroups for $\mathfrak{m}$.*

*Proof.* See [9]. □

**Example 1.29.** Let $K$ be a number field and $C_K$ its class group. Consider the trivial modulus 1 of $K$. Then $K(1)$ is referred to as the **Hilbert class field** of $K$ and satisfies $\mathrm{Gal}(L/K) \cong C_K$. Furthermore, it is an unramified extension since completeness implies that $\mathfrak{f}(K(1)/K)$ is trivial. Completeness also implies that every finite unramified abelian extension must be contained in $K(1)$; indeed, the conductor of any such extension must be trivial and thus divides the trivial modulus 1.

Were there to exist an infinite unramified abelian extension of $K$, it would necessarily contain a finite unramified abelian extension of $K$ not contained in $K(1)$ which is a contradiction. $K(1)$ is thus the maximal unramified abelian extension of $K$.

# 2 Idèlic Approach to Global Class Field Theory

We continue using the notation established from the previous section. We shall assume that $L/K$ is an arbitrary extension of number fields. Furthermore, write $M_K$ for the collection of all primes of a number field $K$.

Recall that a **profinite group** is a topological group that is obtained as the inverse limit of a collection of finite groups, each of which is given the discrete topology. Given an arbitrary group $G$, we can form its **profinite completion** $\widehat{G}$ by taking the inverse limit of the inverse system given by the groups $G/H$ where $H$ is a finite-index open subgroup of $G$ and the connection homomorphisms are given by the natural maps induced by the inclusions of the subgroups. $\widehat{G}$ is uniquely characteristed by the following universal property: if $H$ is any profinite group and $\phi : G \to H$ is a homomorphism then $\phi$ factors uniquely through the natural map $G \to \widehat{G}$. Moreover, the latter map sends $G$ to a dense subspace of $\widehat{G}$. This mapping is injective precisely when the intersection of all finite-index normal subgroups of $G$ is trivial.

**Definition 2.1.** Suppose that $L/K$ is an infinite Galois extension. We define the **Galois group** of $L/K$ to be

$$\mathrm{Gal}(L/K) = \varprojlim_{K'/K \text{ finite Galois}} \mathrm{Gal}(K'/K)$$

The topology on $\mathrm{Gal}(L/K)$ is called the **Krull topology** and has a basis consisting of the finite-index normal subgroups.

**Theorem 2.2** (Galois Theory)**.** *Suppose that $L/K$ is a Galois extension. Given a closed normal subgroup $H \subseteq \mathrm{Gal}(L/K)$, let $L^H$ represent the fixed field of $H$. Let $K'$ be an intermediate field of $L/K$. Then the maps $K' \to \mathrm{Gal}(L/K')$ and $H \to L^H$ are mutually-inverse, inclusion-reversing bijections.*

*Proof.* See [3]. □

**Theorem 2.3** (Product Formula)**.** *Let $x \in K^\times$. Then*

$$\prod_{\mathfrak{p} \in M_K} |x|_\mathfrak{p} = 1$$

*Proof.* Let $x\mathcal{O}_K = \prod_{\mathfrak{p} \in M_K} \mathfrak{p}^{e_\mathfrak{p}}$ be the prime factorisation of the ideal $x\mathcal{O}_K$. Since only finitely many of the $e_\mathfrak{p}$ are non-zero, it follows that only finitely many terms of the product are not equal to 1. In particular, the product taken over the finite primes is equal to $N(\mathfrak{p})^{-e_\mathfrak{p}} = N(x\mathcal{O}_K)^{-1} = |\,\mathrm{N}_{K/\mathbb{Q}}(x\mathcal{O}_K)|^{-1}$. On the other hand, the product taken over the infinite primes is equal to $|\,\mathrm{N}_{K/\mathbb{Q}}(x\mathcal{O}_K)|$ whence the Theorem follows. □

**Definition 2.4.** Let $\{ G_i \}_{i \in I}$ a family of locally compact groups and $K_i \subseteq G_i$ an open compact subgroup for each $i \in S$ where $S \subseteq I$ is finite. We define the **restricted product** of the $G_i$ with respect to the $K_i$ to be

$$\prod_{i \in I \setminus S}^{K_i} G_i = \left\{ (g_i) \in \prod_{i \in I} G_i \;\middle|\; g_i \in K_i \text{ for all but finitely many } i \in I \setminus S \right\}$$

We equip the restricted product with the topology generated by the basis of open sets

$$\left\{ \prod_{i \in I} A_i \;\middle|\; A_i \text{ is open in } G_i \text{ and } A_i = K_i \text{ for all but finitely many } i \in I \right\}$$

**Proposition 2.5.** *Let $\{ G_i \}_{i \in I}$ a family of locally compact groups and $K_i \subseteq G_i$ an open compact subgroup for each $i \in S$ where $S \subseteq I$ is finite. Then the restricted product of the $G_i$ with respect to the $K_i$ is locally compact.*

*Proof.* Let $S'$ be any set containing $S$. Consider the open set

$$G_{S'} = \prod_{i \in S'} G_i \times \prod_{i \notin S'} K_i$$

Then $G_{S'}$ is locally compact in the product topology. Indeed, the $S'$-part of the product is locally compact since it is the product of finitely many locally compact spaces. Furthermore, the second part of the product is compact by Tychonoff's Theorem and so, in particular, it is also locally compact. But the restricted product topology on $G_{S'}$ is the same as the one induced by the product topology and so $G_{S'}$ is locally compact in the restricted product topology. Now, for all $x$ in the restricted product, there exists an $S'$ such that $x \in G_{S'}$ and so the restricted product is locally compact. □

**Definition 2.6.** Let $S \subseteq M_K$ be the set of all infinite primes of $K$. We define the **idèle group** of $K$ to be

$$\mathbb{I}_K = \prod_{\mathfrak{p} \in M_K \setminus S}^{\mathcal{O}_{\mathfrak{p},K}^\times} K_\mathfrak{p}^\times$$

Moreover, we define the **1-idèles** to be the subgroup

$$\mathbb{I}_K^1 = \prod_{\mathfrak{p} \nmid \infty} \mathcal{O}_{\mathfrak{p},K}^\times \times \prod_{\mathfrak{p} \mid \infty} K_\mathfrak{p}^\times$$

**Proposition 2.7.** *$K^\times$ embeds as a discrete subgroup of $\mathbb{I}_K$.*

*Proof.* $K^\times$ is clearly a subgroup of $\mathbb{I}_K$ so it suffices show that $K^\times$ inherits the discrete topology from $\mathbb{I}_K$. Now, multiplication is a homeomorphism of $\mathbb{I}_K$ so it suffices to show that there exists a neighbourhood of 1 containing no other element of $K^\times$. Consider the neighbourhood of 1

$$U = \prod_{\mathfrak{p} \nmid \infty} \mathcal{O}_{\mathfrak{p},K}^\times \times \prod_{\mathfrak{p} \mid \infty} \{ x \in K_\mathfrak{p} \mid |x - 1|_\mathfrak{p} < 1 \}$$

Now suppose that $1 \neq \alpha \in K^\times \cap U$. Then $\alpha \in \mathcal{O}_K$ which clearly implies that $0 \neq \alpha - 1 \in \mathcal{O}_K$. Then $|\alpha - 1|_\mathfrak{p} < 1$ for all $\mathfrak{p} | \infty$. But this contradicts the product formula so we must have that $\alpha = 1$. □

**Definition 2.8.** We define the **idèle class group** of $K$ to be the quotient

$$\mathcal{C}_K = \mathbb{I}_K / K^\times$$

**Remark.** $\mathcal{C}_K$ is not compact. Indeed, consider the so-called volume function $V(x) : \mathbb{I}_K \to \mathbb{R}$ given by $(x) \mapsto \prod_{\mathfrak{p} \in M_K} |x_\mathfrak{p}|_\mathfrak{p}$. This is trivial on $K^\times$ by the product formula and so induces a continuous function on the idèle class group. But this induced function is clearly unbounded and so $\mathcal{C}_K$ cannot be compact.

**Definition 2.9.** Let $(a) \in \mathbb{I}_K$ be an idèle. We define the **ideal associated to** $(a)$ to be

$$\mathfrak{a} = \prod_{\mathfrak{p} \nmid \infty} \mathfrak{p}^{v_\mathfrak{p}(a_\mathfrak{p})}$$

If we equip $I_K$ with the discrete topology then this assignment gives a continuous surjective homomorphism $\mathfrak{I} : \mathbb{I}_K \to I_K$, referred to as the idealifier, with kernel exactly the 1-idèles.

**Proposition 2.10.** *Let $C_K$ be the ideal class group of $K$. Then*

$$\mathcal{C}_K / \mathbb{I}_K^1 \cong C_K$$

*Proof.* Let $\mathfrak{I} : \mathbb{I}_K \to I_K$ be the idealifier and $g : I_K \to C_K$ the homomorphism sending each ideal of $I_K$ to its ideal class in $C_K$. Then $g \circ \mathfrak{I}$ maps $\mathbb{I}_K$ onto $C_K$ and its kernel is given by

$$\begin{aligned} \{\, (x) \in \mathbb{I}_K \mid \mathfrak{I}((x)) \text{ is principal} \,\} &= \{\, (x) \in \mathbb{I}_K \mid \mathfrak{I}((x)) \in \mathfrak{I}(K^\times) \,\} \\ &= \{\, (x) \in \mathbb{I}_K \mid (x) \in K^\times \ker(\mathfrak{I}) \,\} \\ &= K^\times \mathbb{I}_K^1 \end{aligned}$$

whence the Proposition follows. □

**Corollary 2.11.** *Every open subgroup of $C_K$ has finite index.*

*Proof.* Fix an open subgroup $H$ of $C_K$ and let $G$ be the subgroup of $\mathbb{I}_K$ that is mapped to $H$ under the canonical surjection $\pi : \mathbb{I}_K \to C_K$. Then $G$ is open by definition and contains an open neighbourhood of 1 of the form

$$U_\varepsilon = \prod_{\mathfrak{p} \nmid \infty} \mathcal{O}_{\mathfrak{p},K}^\times \times \prod_{\mathfrak{p} \mid \infty} \{\, x_\mathfrak{p} \mid |x_\mathfrak{p} - 1|_\mathfrak{p} < \varepsilon \,\}$$

But then $G$ also contains the subgroup generated by $U_\varepsilon$ which is exactly the group of 1-idèles $\mathbb{I}_K^1$. Hence $C_K / H = \mathbb{I}_K / G K^\times \subseteq \mathbb{I}_K / \mathbb{I}_K^1 K^\times = \mathcal{C}_K$. The Corollary then follows by the finiteness of the class number. □

**Proposition 2.12.** *Let $\mathfrak{m}$ be a modulus for $K$ and define the sets*

$$U_K^{\mathfrak{m}(\mathfrak{p})} = \begin{cases} \mathcal{O}_{\mathfrak{p},K}^\times & \text{if } \mathfrak{p} \nmid \infty, \mathfrak{m}(\mathfrak{p}) = 0 \\ 1 + \mathfrak{p}^{\mathfrak{m}(\mathfrak{p})} \mathcal{O}_{\mathfrak{p},K} & \text{if } \mathfrak{p} \nmid \infty, \mathfrak{m}(\mathfrak{p}) > 0 \\ K_\mathfrak{p}^\times & \text{if } \mathfrak{p} \mid \infty, \mathfrak{m}(\mathfrak{p}) = 0 \\ \mathbb{R}_{>0}^\times & \text{if } \mathfrak{p} \text{ is real}, \mathfrak{m}(\mathfrak{p}) > 0 \end{cases}$$

*Denote $U_K^\mathfrak{m} = \prod_{\mathfrak{p} \in M_K} U_K^{\mathfrak{m}(\mathfrak{p})}$. Then*

1. *$U_K^\mathfrak{m}$ is an open subgroup of $\mathbb{I}_K$.*

2. *Every open subgroup of $\mathbb{I}_K$ contains $U_K^{\mathfrak{m}}$ for some modulus $\mathfrak{m}$.*

3. $C_K/U_K^{\mathfrak{m}} \cong C_K^{\mathfrak{m}}$.

*Proof.* The first two parts are immediate from the definition of the topology on $\mathbb{I}_K$. In particular, $U_K^{\mathfrak{m}}$ is an element of the basis.

To prove the third part, first define

$$\mathbb{I}_K^{\mathfrak{m}} = \{\, (x) \in \mathbb{I}_K \mid x_{\mathfrak{p}} \in U_K^{\mathfrak{m}(\mathfrak{p})} \text{ for all } \mathfrak{p} \nmid \infty \text{ such that } \mathfrak{p} | \mathfrak{m} \,\}$$

Note that $U_K^{\mathfrak{m}}$ is actually a subgroup of $\mathbb{I}_K^{\mathfrak{m}}$. We first observe that $K^{\mathfrak{m},1} = K^\times \cap \mathbb{I}_K^{\mathfrak{m}}$. We next observe that $\mathfrak{I}|_{\mathbb{I}_K^{\mathfrak{m}}}$ surjects onto $I_K^{\mathfrak{m}}$. We now would like to apply the Kernel-Cokernel Lemma (see Appendix) to the pair of homomorphisms $K^{\mathfrak{m},1} \overset{\iota}{\hookrightarrow} \mathbb{I}_K^{\mathfrak{m}} \overset{\mathfrak{I}}{\to} I_K^{\mathfrak{m}}$. We note that $\ker(\mathfrak{I}) = U_K^{\mathfrak{m}}, \operatorname{coker}(\iota) = \mathbb{I}_K^{\mathfrak{m}}/K^{\mathfrak{m},1}, \operatorname{coker}(\mathfrak{I} \circ \iota) = I_K^{\mathfrak{m}}/P_K^{\mathfrak{m},1} = C_K^{\mathfrak{m}}$ and $\operatorname{coker}(\mathfrak{I}) = 1$ so we have an exact sequence

$$U_K^{\mathfrak{m}} \longrightarrow \mathbb{I}_K^{\mathfrak{m}}/K^{\mathfrak{m},1} \longrightarrow C_K^{\mathfrak{m}} \longrightarrow 1$$

From which we may read off the isomorphism $\mathbb{I}_K^{\mathfrak{m}}/(U_K^{\mathfrak{m}} K^{\mathfrak{m},1}) \cong C_K^{\mathfrak{m}}$. The Proposition will follow upon showing that $\mathbb{I}_K^{\mathfrak{m}}/K^{\mathfrak{m},1} \cong \mathbb{I}_K/K^\times$. Consider the canonical mapping $\mathbb{I}_K^{\mathfrak{m}} \to \mathbb{I}_K/K^\times$. The kernel of this mapping is $\mathbb{I}_K^{\mathfrak{m}} \cap K^\times = K^{\mathfrak{m},1}$ and so we get an injection $\mathbb{I}_K^{\mathfrak{m}}/K^{\mathfrak{m},1} \hookrightarrow \mathbb{I}_K/K^\times$. The surjectivity of this map follows immediately from weak approximation. □

**Definition 2.13.** We define the **idèle norm** $\mathrm{N}_{L/K}(\cdot)$ to be the map

$$\mathrm{N}_{L/K}(\cdot) : \mathbb{I}_L \to \mathbb{I}_K$$

that sends an idèle $(x) \in \mathbb{I}_L$ to the idèle $(y) \in \mathbb{I}_K$ whose $\mathfrak{p}^{th}$ component is $\prod_{\mathfrak{P}/\mathfrak{p}} \mathrm{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(x_{\mathfrak{P}})$.

**Proposition 2.14.** *We have a commutative diagram*

$$\begin{array}{ccccc} L^\times & \longrightarrow & \mathbb{I}_L & \xrightarrow{\mathfrak{I}} & I_L \\ \downarrow{\scriptstyle \mathrm{N}_{L/K}(\cdot)} & & \downarrow{\scriptstyle \mathrm{N}_{L/K}(\cdot)} & & \downarrow{\scriptstyle \mathrm{N}_{L/K}(\cdot)} \\ K^\times & \longrightarrow & \mathbb{I}_K & \xrightarrow{\mathfrak{I}} & I_K \end{array}$$

*Furthermore, $\mathrm{N}_{L/K}(\cdot)$ descends to a homomorphism on $C_L$ and we have a commutative diagram*

$$\begin{array}{ccc} C_L & \longrightarrow & \mathcal{C}_L \\ \downarrow{\scriptstyle \mathrm{N}_{L/K}(\cdot)} & & \downarrow{\scriptstyle \mathrm{N}_{L/K}(\cdot)} \\ C_K & \longrightarrow & \mathcal{C}_L \end{array}$$

*Proof.* Recall, from the elementary theory of local fields [5], that we have a canonical isomorphism

$$L \otimes_K K_{\mathfrak{p}} = \prod_{\mathfrak{P}/\mathfrak{p}} L_{\mathfrak{P}}$$

for any prime $\mathfrak{p}$ of $K$. But the norm map is invariant under tensors so we have that $\mathrm{N}_{L/K}(\alpha) = \prod_{\mathfrak{P}/\mathfrak{p}} \mathrm{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\alpha)$ for all $\alpha \in L$. We thus have the commutativity of the left-hand square of the first diagram and the right-hand square follows easily. The fact that $\mathrm{N}_{L/K}(\cdot)$ descends to a homomorphism on $C_L$ follows immediately from a standard quotient group argument. The second commutative diagram now follows easily via quotienting out by the image of $L^\times$ on every object in the first diagram. □

**Theorem 2.15** (Class Field Theory)**.** *Let $K^{\mathrm{ab}}$ be the maximal abelian extension of $K$. Then there is a continuous surjective homomorphism called the* ***Artin map***

$$[\cdot, K^{\mathrm{ab}}/K] : \mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

*For an intermediate abelian field $L$ of $K^{\mathrm{ab}}/K$ write $[\cdot, L/K] = [\cdot, K^{\mathrm{ab}}/K]|_L$. The Artin map satisfies the following properties:*

1. *(Artin Reciprocity) $[K^\times, K^{\mathrm{ab}}/K] = 1$ and so the Artin map descends to a homomorphism $C_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ which induces an isomorphism*

   $$[\cdot, K^{\mathrm{ab}}/K] : \widehat{C_K} \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

   *Furthermore, for every finite abelian extension $L/K$, we have an isomorphism*

   $$[\cdot, L/K] : C_K/\,\mathrm{N}_{L/K}(C_L) \to \mathrm{Gal}(L/K)$$

2. *(Existence) For every finite-index open subgroup $N$ of $C_K$, there exists a unique abelian extension $L/K$ such that $N = \mathrm{N}_{L/K}(C_L)$. In particular, for every modulus $\mathfrak{m}$ of $K$, the ray class field $K(\mathfrak{m})$ is the unique abelian extension such that $\mathrm{N}_{K(\mathfrak{m})/K}(C_{K(\mathfrak{m})}) = U_K^{\mathfrak{m}}$.*

3. *(Compatibility) Let $L/K$ be a finite abelian extension and $x \in \mathbb{I}_K$ be an idèle such that $\mathfrak{J}(x)$ is prime to all finite primes of $K$ that ramify in $L$. Then*

   $$[x, L/K] = \left(\frac{L/K}{\mathfrak{J}(x)}\right)$$

4. *(Norm Restriction) Let $L/K$ be an extension of number fields. Then*

   $$[x, L^{\mathrm{ab}}/L] = [\mathrm{N}_{L/K}(x), K^{\mathrm{ab}}/K]$$

*Proof.* See [7]. □

**Corollary 2.16.** *There exists a one-to-one inclusion reversing correspondence between the finite abelian extension of $K$ and the finite-index open subgroups of $C_K$. Furthermore, given finite abelian extensions $L_1$ and $L_2$ of $K$, this bijection satisfies*

1. $\mathrm{N}_{L_1L_2/K}(C_{L_1L_2}) = \mathrm{N}_{L_1/K}(C_{L_1}) \cap \mathrm{N}_{L_2/K}(C_{L_2})$
2. $\mathrm{N}_{(L_1\cap L_2)/K}(C_{L_1\cap L_2}) = \mathrm{N}_{L_1/K}(C_{L_1}) \cdot \mathrm{N}_{L_2/K}(C_{L_2})$

**Remark.** The homomorphism $C_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ is almost an isomorphism of topological groups in the following sense: it is a topological homeomorphism but not necessarily a group isomorphism. It cannot be a group isomorphism as $\mathrm{Gal}(K^{\mathrm{ab}/K})$ is profinite whereas $C_K$ is not. Indeed, recall that a topological group is profinite if and only if it is compact, Hausdorff and totally disconnected. But by an earlier remark, $C_K$ is not compact. Hence this homomorphism only becomes an isomorphism once we pass to the profinite completion of $C_K$.

**Definition 2.17.** We define a **Hecke character** of $C_K$ to be a continuous homomorphism

$$\psi : C_K \to \mathbb{C}^\times$$

We say that a Hecke character is of **finite order** if $\psi^m = 1$ for some positive integer $m$. Furthermore, we define a **1-dimensional Galois representation** of $K$ to be a continuous homomorphism

$$\chi : \mathrm{Gal}(K^{\mathrm{ab}}/K) \to \mathbb{C}^\times$$

**Theorem 2.18.** *There is a one-to-one correspondence between Hecke characters of $C_K$ of finite order and 1-dimensional Galois representations of $K$.*

*Proof.* Fix a 1-dimensional Galois representation $\chi$ and let $\varphi_K$ be the idèlic Artin map. We observe that $\chi \circ \varphi_K$ defines a Hecke character of $C_K$.

We first claim that $\chi$ has finite image. Indeed. let $U \subseteq \mathbb{C}^\times$ be an open neighbourhood containing no non-trivial subgroup of $\mathbb{C}^\times$. By continuity, $\chi^{-1}(U)$ is open and contains the identity automorphism and therefore contains an open subgroup $H$ of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ since the latter is profinite. Pulling $H$ forward along $\chi$, we get an open subgroup of $U$ which, by construction, must be trivial. $\chi$ is thus trivial on $H$ and so descends to a continuous homomorphism $\chi : \mathrm{Gal}(K^{\mathrm{ab}}/K)/H \to \mathbb{C}^\times$ whose image coincides with the image of $\chi$. Now, $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ is compact since it is profinite and open subgroups of compact groups have finite index and so the image of $\chi$ must be finite.

From the claim it follows that $\chi$ factors through the Galois group of a finite abelian extension $L/K$ so we may assume that $\chi$ is a continuous homomorphism $\chi : \mathrm{Gal}(L/K) \to \mathbb{C}^\times$. By Class Field Theory, $\chi \circ \varphi_K$ then factors through $G = C_K/\,\mathrm{N}_{L/K}(C_L)$ which is a Hecke character of finite order. We thus have an injection of the character group of $\mathrm{Gal}(L/K)$ into the character group of $G$. Recall that the character group of a finite abelian group $H$ is isomorphic to $H$. This, combined with the fact that $G \cong \mathrm{Gal}(L/K)$ establishes that this injection is in fact a bijection as required. □

# 3 Appendix

**Lemma 3.1** (Kernel-Cokernel Lemma)**.** *Let $A, B$ and $C$ be abelian groups and $f : A \to B$ and $g : B \to C$ homomorphisms. Then we have an exact sequence*

$$0 \longrightarrow \ker(f) \longrightarrow \ker(g \circ f) \xrightarrow{f} \ker(g) \longrightarrow \mathrm{coker}(f) \longrightarrow \mathrm{coker}(g \circ f) \longrightarrow \mathrm{coker}(g) \longrightarrow 0$$

*Proof.* This follows immediately upon applying the Snake Lemma to the following diagram with exact rows

$$\begin{array}{ccccccc} & & A & \xrightarrow{f} & B & \longrightarrow & \mathrm{coker}(f) \longrightarrow 0 \\ & & \downarrow{\scriptstyle g\circ f} & & \downarrow{\scriptstyle g} & & \downarrow \\ 0 & \longrightarrow & C & \xrightarrow{id} & C & \longrightarrow & 0 \end{array}$$

□

# References


[1] Andrew Sutherland, *Number Theory*, http://math.mit.edu/classes/18.785/2015fa/ [Accessed 28/03/17]

[2] Bjorn Poonen, *A Brief Summary of the Statements of Class Field Theory*, http://www-math.mit.edu/~poonen/papers/cft.pdf [Accessed 28/03/17]

[3] Brian Osserman, *Number Theory*, https://www.math.ucdavis.edu/~osserman/classes/254A/ [Accessed 28/03/17]

[4] J.S Milne, *Class Field Theory*, http://www.jmilne.org/math/CourseNotes/CFT310.pdf [Accessed 28/03/17]

[5] J.S Milne, *Algebraic Number Theory*, http://www.jmilne.org/math/CourseNotes/ANT.pdf [Acessed 31/01/17]

[6] Alexandre Daoud, *Algebraic Number Theory*, http://www.p-adic.com/AlgebraicNumberTheory.pdf [Accessed 28/03/17]

[7] Matthias Flach, *Global Class Field Theory*, http://www.math.caltech.edu/~2015-16/3term/ma160c/ [Accessed 31/03/17]

[8] Joseph H. Silverman, *Advanced Topics in the Arithmetic of Elliptic curves*, Springer

[9] Nancy Childress, *Class Field Theory*, Springer

[10] Gerald Janusz, *Algebraic Number Fields*, American Mathematical Society