The roots of unity in $K$, then by (2.8.8), by the above, they all have the same norm in $\tilde{G}$ consists of $\mathbf{z} \in (\mathbb{R}^s \times \mathbb{C}^t)^*$ such that $N(\mathbf{z}) \leq 1$. 

$\lambda(\mathbf{z}) = \sum_{k=1}^{s+t} \xi_k l_k$.

Restriction of automorphisms gives rise to $\text{Gal}(L/\mathbb{Q}[k]) \cong \text{Gal}(C/\mathbb{Q}[k])$. 

$\mathbb{C} \cong K = k$.
Class Field Theory

Travis Dirle

December 4, 2016
## Contents

1 Global Class Field Theory 1
1.1 Ray Class Groups ......................................... 1
1.2 The Idèlic Theory .......................................... 5
1.3 Artin Reciprocity ........................................... 10
1.4 The Existence Theorem and its Consequences ............. 13

2 Local Class Field Theory 19
2.1 Preliminaries on Local Fields .............................. 19
2.2 A Fundamental Exact Sequence ............................ 20
2.3 Local Units Modulo Norms ................................. 21
2.4 Lubin-Tate Extensions ..................................... 22
2.5 The Local Artin Map ...................................... 24
Chapter 1

Global Class Field Theory

1.1 Ray Class Groups

Definition 1.1.1. If \( S \) is a set of prime ideals of \( \mathcal{O}_F \), and

\[
\lim_{s \to 1^+} \sum_{p \in S} Np^{-1} \log \left( \frac{1}{s-1} \right) = \delta \text{ exists},
\]

then we say that \( S \) has **Dirichlet density** \( \delta = \delta_F(S) \).

Corollary 1.1.2. Let \( K/F \) be Galois, and let

\[ S_{K/F} = \{ p \in \mathcal{O}_F : p \text{ splits completely in } K/F \}. \]

Then \( \delta_F(S_{K/F}) = \frac{1}{[K : F]} \).

Definition 1.1.3. Let \( S, T \) be sets of primes in \( \mathcal{O}_F \), where \( F \) is a number field. We define the following notation.

Write \( S \prec T \) to mean \( \delta_F(S \setminus T) = 0 \).

Write \( S \approx T \) if \( S \prec T \prec S \).

Theorem 1.1.4. Let \( E \) and \( K \) be number fields, each of which is Galois over \( \mathbb{Q} \). Then \( S_K \prec S_E \) if and only if \( E \subset K \).

Theorem 1.1.5. (Approximation Theorem) Let \( | \cdot |_1, \ldots, | \cdot |_n \) be non-trivial pairwise inequivalent absolute values on a number field \( F \), and let \( \beta_1, \ldots, \beta_n \) be non-zero elements of \( F \). For any \( \epsilon > 0 \), there is an element \( \alpha \in F \) such that \( |\alpha - \beta_j|_j < \epsilon \), for each \( j = 1, \ldots, n \).
CHAPTER 1. GLOBAL CLASS FIELD THEORY

Note that when \( p \) is a prime ideal of \( O_F \) and \( c = |\pi|_p \) for \( \pi \in p - p^2 \), the statement \( \alpha \beta \neq 0 \) and \( |\alpha - \beta|_p < \epsilon \) gives \( \text{ord}_p(\alpha / \beta - 1) > n \), where \( n \) is given by \( \epsilon | \beta |_p < c^n \). If \( \alpha \) and \( \beta \) are \( p \)-adic units, then this just means \( \alpha \equiv \beta \mod p^n \).

Note also that when \( |\cdot|_j = |\cdot|_\sigma \), where \( \sigma : F \hookrightarrow \mathbb{R} \), the statement \( \alpha \beta \neq 0 \) and \( |\alpha - \beta|_\sigma < \epsilon \) for small \( \epsilon \) means that \( \sigma(\alpha / \beta) > 0 \).

In the \( p \)-adic situation, we were able to write \( \alpha \equiv \beta \mod p^n \). We can write something similar in the case of real embeddings \( \sigma \) of \( F \) if we make the following convention.

**Definition 1.1.6.** When \( \sigma : F \hookrightarrow \mathbb{R} \), we associate to \( \sigma \) a formal object that we call an infinite real prime, which we denote by \( p_\sigma \). We may then define

\[ \alpha \equiv \beta \mod p_\sigma \text{ if and only if } \sigma(\alpha / \beta) > 0. \]

We may also define infinite imaginary primes: We associate an object \( p_\sigma \) to each conjugate pair \( \sigma, \overline{\sigma} : F \hookrightarrow \mathbb{C} \). We dont use the congruence notation with infinite imaginary primes however.

**Definition 1.1.7.** Other language used for prime ideals can be adapted to infinite primes as well. If \( K/F \) is an extension of number fields, we say that an infinite prime \( p_\sigma \) ramifies in \( K/F \) if and only if \( \sigma(F) \subset \mathbb{R} \), but for some extension of \( \sigma \) to \( K \) we have \( \sigma(K) \not\subset \mathbb{R} \).

**Definition 1.1.8.** Using the infinite real primes (and the usual primes), we may also define a divisor or modulus for \( F \) as a formal product \( \prod p^{t(p)} \), where \( t(p) \in \mathbb{N} \) is non-zero for only finitely many \( p \), and can only take a value of 0 or 1 when \( p \) is an infinite real prime. (We may consider the notion of an infinite imaginary prime, but if we do, we must take \( t(p) = 0 \) for all infinite imaginary primes \( p \)) Specifically, we shall denote the product of all the infinite real primes by \( m_\infty = \prod_{\sigma \text{ real}} p_\sigma \).

**Definition 1.1.9.** If an element \( \alpha \in F \) satisfies \( \sigma(\alpha) > 0 \) for every real embedding \( \sigma \) of \( F \), we say that \( \alpha \) is totally positive, and write \( \alpha \gg 0 \).

**Definition 1.1.10.** Let \( m \) be a non-zero integral ideal of \( O_F \). Define \( \mathcal{P}^+_F(m) \) to be the subgroup of \( \mathcal{P}_F \), which is

\[ \{ \langle \alpha \rangle : \alpha \in O_F, \alpha \equiv 1 \mod m, \text{ and } \alpha \gg 0 \} \text{ or also, } \]

\[ \{ \frac{\alpha}{\beta} : \alpha \gg 0; \alpha, \beta \in O_F \text{ prime to } m; \alpha \equiv \beta \mod m \} \]

**Definition 1.1.11.** Let \( \mathcal{I}_F(m) \) be the group of fractional ideals of \( F \) whose factorizations do not contain a non-trivial power of any prime ideal dividing \( m \):

\[ \mathcal{I}_F(m) = \{ a \in \mathcal{I}_F : \text{ord}_p a = 0 \text{ for all } p | m \}. \]
Definition 1.1.12. The strict (narrow) ray class group or generalized ideal class group of $F$ for $m$, is

$$\mathcal{R}_{F,m}^+ = \mathcal{I}_F(m)/\mathcal{P}_{F,m}^+.$$ 

We write $\alpha \equiv 1 \mod m$ when $\alpha \equiv 1 \mod \text{ord}_p(m)$ in the completion $F_p$ for every $p | m$. When writing congruences modulo powers of $p$ in the completion, we really mean congruences modulo the unique maximal ideal in the ring of integers of $F_p$.

Definition 1.1.13. For a non-zero integral ideal $m$ of $\mathcal{O}_F$ we define the ray modulo $m$ as

$$\mathcal{P}_{F,m} = \{\langle \alpha \rangle : \alpha \equiv 1 \mod m\}.$$ 

Definition 1.1.14. The ray class group of $F$ for $m$ is

$$\mathcal{R}_{F,m} = \mathcal{I}_F(m)/\mathcal{P}_{F,m}.$$ 

The strict ray class group $\mathcal{R}_{F,m}^+$ may also be viewed as a ray class group in the above sense if one views $\mathcal{P}_{F,m}^+$ as a ray modulo the divisor $mm_\infty$.

When $m = \mathcal{O}_F$, we have

$$\mathcal{R}_{F,m} = \mathcal{I}_F/\mathcal{P}_F = \mathcal{C}_F,$$ the ordinary ideal class group

$$\mathcal{R}_{F,m}^+ = \mathcal{I}_F/\mathcal{P}_F^+,$$ the strict (narrow) ideal class group.

Definition 1.1.15. A generalized Dirichlet character or Weber character of modulus $m$ is a homomorphism of groups $\chi : \mathcal{R}_{F,m}^+ \to \mathbb{C}^\times$.

Proposition 1.1.16. $\mathcal{R}_{F,m}^+$ is a finite group, with

$$\#\mathcal{R}_{F,m}^+ = \frac{h_F 2^{r_1} \phi(m)}{[\mathcal{U}_F : \mathcal{U}_{F,m}^+]}$$

where

$$h_F = \#\mathcal{C}_F$$

$$r_1 = \# \text{ of real embeddings of } F$$

$$\phi(m) = \#(\mathcal{O}_F/m)^\times = \Pi_{p|\text{ord}_p(m)} (Np - 1),$$ where $m = \Pi_{p|m} p^{e_p}$

$\mathcal{U}_F = \mathcal{O}_F^\times$ the units of $\mathcal{O}_F$

$\mathcal{U}_{F,m}^+ = \{\epsilon \in \mathcal{U}_F : \epsilon \gg 0, \epsilon \equiv 1 \mod m\}$
CHAPTER 1. GLOBAL CLASS FIELD THEORY

Definition 1.1.17. \( R_{F,m}^+ \) is called the strict ray class number modulo \( m \) or the ray class number modulo \( mm_\infty \).

Definition 1.1.18. Let \( K/F \) be Galois, and let \( m \) be an integral ideal of \( \mathcal{O}_F \). We say that \( K \) is the class field over \( F \) of \( \mathcal{P}_{F,m}^+ \) if
\[
S_{K/F} = \{ \text{primes } p \text{ of } \mathcal{O}_F : p \text{ splits completely in } K/F \}
\]
\[
\approx \{ \text{primes } p \text{ of } \mathcal{O}_F : p \in \mathcal{P}_{F,m}^+ \}.
\]

Recall, that \( S \approx T \) if and only if they differ by a set with Dirichlet density zero.

Definition 1.1.19. More generally, we may define the notion of class field for subgroups of \( \mathcal{I}_F(m) \) that contain \( \mathcal{P}_{F,m}^+ \). If \( m \) is a non-zero integral ideal of \( \mathcal{O}_F \), and \( H \) satisfies
\[
\mathcal{P}_{F,m}^+ < H < \mathcal{I}_F(m),
\]
then we say \( K \) is the class field over \( F \) of \( H \) if \( K/F \) is Galois and
\[
S_{K/F} \approx \{ \text{primes } p \text{ of } \mathcal{O}_F : p \in H \}.
\]

Theorem 1.1.20. If the class field \( K \) of \( H \) exists, then it is unique.

Definition 1.1.21. For \( a \in \mathcal{I}_F(m) \) we may define
\[
S_{a,m} = \{ \text{primes } p \text{ of } \mathcal{O}_F : p \equiv a \text{ in } \mathcal{R}_{F,m}^+ \} = \{ \text{primes } p \in a\mathcal{P}_{F,m}^+ \}.
\]

Proposition 1.1.22. Let \( a \in \mathcal{I}_F(m) \). Suppose \( \mathcal{P}_{F,m}^+ < H < \mathcal{I}_F(m) \). If for all characters \( \chi \neq \chi_0 \) of \( \mathcal{I}_F(m) \) that are trivial on \( H \), we have \( L_m(1, \chi) \neq 0 \), then
\[
\delta_F(\{ \text{primes } p \text{ of } \mathcal{O}_F : p \in aH \}) = \frac{1}{[\mathcal{I}_F(m) : H]}.
\]

Theorem 1.1.23. Suppose \( K/F \) is Galois, and \( \mathcal{P}_{F,m}^+ < H < \mathcal{I}_F(m) \). Suppose there is some set of primes \( J \subset H \) with \( S_{K/F} \approx J \). Then
\[
[\mathcal{I}_F(m) : H] \leq [K : F],
\]
and \( L_m(1, \chi) \neq 0 \) whenever \( \chi \neq \chi_0 \) and \( \chi \) is trivial on \( H \).

Corollary 1.1.24. If \( K/F \) is Galois and \( K \) is the class field for \( H \) where \( \mathcal{P}_{F,m}^+ < H < \mathcal{I}_F(m) \), then
\[
[\mathcal{I}_F(m) : H] = [K : F].
\]

Theorem 1.1.25. (Universal Norm Index Inequality) Let \( K/F \) be a Galois extension of number fields and let \( H = \mathcal{P}_{F,m}^+ N_{K/F}(m) \) where
\[
N_{K/F}(m) = \{ a \in \mathcal{I}_F(m) : a = N_{K/F}(\mathfrak{A}) \text{ for some } \mathfrak{A} \text{ in } \mathcal{I}_K \}.
\]
(Note that the factorization of the fractional ideal \( \mathfrak{A} \) of \( K \) cannot contain a non-trivial power of any prime ideal that divides \( m\mathcal{O}_K \), i.e., \( \mathfrak{A} \in \mathcal{I}_K(m\mathcal{O}_K) \).) Then
\[
[\mathcal{I}_F(m) : H] \leq [K : F].
\]
It is possible to rephrase what we have done in terms of divisors. For a divisor \( m = \prod_p p^{a(p)} \) of \( F \), we shall write \( m_0 = \prod_{\text{finite}} p^{a(p)} \) and \( m_{\text{re}} = \prod_{\text{real}} p^{a(p)} \). Of course, if \( p \) is real, then \( a(p) \) is either 0 or 1, and in general, we have \( a(p) = 0 \) for all but finitely many \( p \).

Given a divisor \( m \) of \( F \), we write \( \alpha \equiv 1 \mod m \) to denote \( \alpha \equiv 1 \mod m_0 \) (i.e., \( \text{ord}_p(\alpha - 1) \geq \text{ord}_p(m_0) \) for all \( p \) dividing \( m_0 \)), and that \( \sigma(\alpha) > 0 \) whenever \( \sigma \) is a real embedding with \( p_\sigma \) dividing \( m_{\text{re}} \).

**Definition 1.1.26.** Remembering that \( m \) is a divisor of \( F \) (and not necessarily an ideal), we let \( \mathcal{P}_{F,m} \) denote the set of principal fractional ideals of \( F \) that have a generator \( \alpha \) with \( \alpha \equiv 1 \mod m \). (\( \mathcal{P}_{F,m} \) is sometimes called the ray modulo the divisor \( m \)). Also, set \( \mathcal{I}_F(m) = \mathcal{I}_F(m_0) \). We call \( \mathcal{R}_{F,m} = \mathcal{I}_F(m)/\mathcal{P}_{F,m} \) the ray class group modulo the divisor \( m \).

### 1.2 THE İĐËLIC THEORY

**Definition 1.2.1.** We say that two absolute values are **equivalent** if they induce the same topology.

**Definition 1.2.2.** A **place** of \( F \) is an equivalence class of non-trivial absolute values on \( F \). Denote the set of places of \( F \) by \( V_F \).

**Theorem 1.2.3.** Each of the places of \( F \) falls into one of the following three categories:

i) Places that contain one of the \( p \)-adic absolute values given by \( \|\alpha\|_p = N_p^{-\text{ord}_p(\alpha)} \) for a non-zero prime ideal \( p \) of \( \mathcal{O}_F \). These are the finite/non-Archimedean/discrete places of \( F \).

ii) Places that contain one of the absolute values \( \|\alpha\|_\sigma = |\sigma(\alpha)|_\mathbb{R} \), for some real embedding \( \sigma : F \hookrightarrow \mathbb{R} \) of \( F \). These are the infinite/real-Archimedean places of \( F \).

iii) Places that contain one of the absolute values \( \|\alpha\|_\sigma = |\sigma(\alpha)|_\mathbb{C} \), for some \( \sigma : F \hookrightarrow \mathbb{C} \), an imaginary embedding of \( F \). These are the infinite imaginary/imaginary-Archimedean places of \( F \).

Note that two distinct non-zero prime ideals of \( \mathcal{O}_F \) cannot produce absolute values that are equivalent, so there is a distinct finite place for each non-zero
prime ideal of $\mathcal{O}_F$. Similarly, distinct real embeddings produce inequivalent absolute values. For the imaginary embeddings, each place contains the two (equivalent) absolute values corresponding to a conjugate pair of embeddings. But, if two imaginary embeddings of $F$ are not conjugate, then they give rise to inequivalent absolute values. Thus, there is a single place for each conjugate pair of imaginary embeddings of $F$.

For a number field $F$, there are a finite number of infinite places. Also, given $x \in F^\times$, there can be only finitely many prime ideals $p$ of $\mathcal{O}_F$ for which $\|x\|_p \neq 1$. For a non-zero prime ideal $p$ of $\mathcal{O}_F$, we let $v_p$ denote the place containing $\|\cdot\|_p$. For an embedding $\sigma : F \hookrightarrow \mathbb{C}$, we let $v_\sigma$ denote the place containing $\|\cdot\|_\sigma$. Conversely, for a finite place $v \in V_F$, we let $p_v$ denote the associated prime ideal of $\mathcal{O}_F$. To simplify notation, we write $\text{ord}_v$ instead of $\text{ord}_p$.

For $v \in V_F$, we may complete $F$ with respect to $v$. Denote the completion by $F_v$. Note that if $v$ is a finite place, then $F_v = F_p$ for some $p$ of $\mathcal{O}_F$. If $v$ is an infinite real place, then $F_v \cong \mathbb{R}$, while if $v$ is an infinite imaginary place, then $F_v \cong \mathbb{C}$.

**Definition 1.2.4.** An idèle of a number field $F$ is an ‘infinite vector’ $\alpha = (\ldots, a_v, \ldots)_{v \in V_F}$ where each $a_v$ is an element of its corresponding $F_v^\times$, and where $a_v \in U_v$ for all but finitely many $v$.

**Definition 1.2.5.** The idèles of $F$ form a multiplicative group, denoted $J_F = \prod_v F_v^\times$, being a ‘restricted topological product’. We let $\mathcal{E}_F = \prod_{v \in V_F} U_v$, which is a subgroup of $J_F$. We may give $\mathcal{E}_F$ the product topology, where each $U_v$ has its metric topology.

**Definition 1.2.6.** A topological group is a group $G$ that is also a topological space, for which multiplication and inversion are continuous.

**Proposition 1.2.7.** $J_F$ is a locally compact topological group.

**Proposition 1.2.8.** The quotient group $J_F / \mathcal{E}_F$ is isomorphic to $\mathcal{I}_F$, the group of fractional ideals of $F$.

**Definition 1.2.9.** We may view $\alpha \in F^\times$ as an idèle $(\ldots, \iota_v(\alpha), \ldots)$, where $\iota_v : F \hookrightarrow F_v$ is an embedding of $F$ into its completion at $v$. This gives an embedding, called the diagonal embedding,

$$\iota : F^\times \hookrightarrow J_F, \text{ where } \iota(\alpha) = (\ldots, \iota_v(\alpha), \ldots).$$

Usually it will do no harm to identify $\alpha$ and $\iota(\alpha)$, and we shall often write $F^\times$ when we really mean $\iota(F^\times)$. If we define a map $\eta : J_F \to \mathcal{I}_F$ by $a = (\ldots, a_v, \ldots) \mapsto \langle a \rangle = \Pi_v \text{ finite } p_v^{\text{ord}_v(a_v)}$, we find that $\eta(\alpha) = \Pi_v \text{ finite } p_v^{\text{ord}_v(\iota_v(\alpha))} = \alpha \mathcal{O}_F$ and $\eta(F^\times) = \mathcal{P}_F$. 


Proposition 1.2.10. For a number field $F$, we have

$$J_F/F^\times \mathcal{E}_F \cong \mathcal{C}_F = I_F/P_F.$$ 

A given place $v$ of $F$ will lie above either the infinite real place $\infty$ of $\mathbb{Q}$ or above a finite place of $\mathbb{Q}$ corresponding to a prime $p$ of $\mathbb{Z}$. Above the place $\infty$, we choose the $\iota_v$ from the set of embeddings $F \hookrightarrow F_v \subset \mathbb{C}$, so that each infinite place of $F$ is represented exactly once. Similarly, for the finite places $v$ above $p$, we want to choose the $\iota_v$ from the embeddings $F \hookrightarrow F_v \subset \mathbb{C}_p$ so that each place of $F$ above $p$ is represented exactly once.

Let $|\cdot|$ denote the usual absolute value on $\mathbb{C}$. For the infinite places and their embeddings, we have $\|x\|_v = |\iota_v(x)|^d$ (where $d = 1$ if $v$ is real and $d = 2$ if $v$ is imaginary, i.e., $d = [F_v : \mathbb{R}]$). For a finite place $v = v_p$, where $p$ lies above $p$, the embedding $\iota_v : F \hookrightarrow F_v \subset \mathbb{C}_p$ satisfies $\|x\|_v = |\iota_v(x)|_p^d$, where $d = [F_v : \mathbb{Q}_p]$ and $|\cdot|_p$ is the $p$-adic absolute value of $\mathbb{C}_p$, normalized so that $|p|_p = 1/p$.

Proposition 1.2.11. Let $m$ be a non-zero integral ideal of $\mathcal{O}_F$, and define

$$J_{F,m}^+ = \{a \in J_F : a_v > 0 \text{ for all real } v, \text{ and } a_v \equiv 1 \mod p_v^{\text{ord}_v(m)} \text{ for all } p_v \mid m\};$$

$$\mathcal{E}_{F,m}^+ = J_{F,m}^+ \cap \mathcal{E}_F.$$ 

Then

$$J_F/F^\times \mathcal{E}_{F,m}^+ \cong \mathcal{R}_{F,m}^+.$$ 

Corollary 1.2.12. The set of subgroups $\mathcal{H}$ of $J_F$, with $\mathcal{H} \supset F^\times \mathcal{E}_{F,m}^+$ for some $m$, corresponds to the set of open subgroups of $J_F$ that contain $F^\times$.

Definition 1.2.13. Let $K/F$ be an extension of number fields. Define $N_{K/F} : J_K \to J_F$ as follows. Let $(\ldots, a_w, \ldots) = a \in J_K$, where the $w$ are places of $K$. For a fixed $v \in V_F$, the set $\{w \in V_K : w \mid v\}$ is finite. We construct the norm of $a$ as an idèle of $F$ by computing each $v$-component in terms of the corresponding set $\{w \in V_K : w \mid v\}$. Specifically, we let $b_v = \Pi_{w|v} N_{K_w/F_v}(a_w)$ and define $N_{K/F}(a) = (\ldots, b_v, \ldots) \in J_F$.

Recall that if $\alpha \in K$, then for any fixed $v \in V_F$

$$N_{K/F}(\alpha) = \Pi_{w|v} N_{K_w/F_v}(\iota_w(\alpha)).$$

Hence if $\alpha \in K^\times$ is viewed as an idèle in $J_K$, then $N_{K/F}(\alpha)$ is the idèle in $J_F$ arising from the usual norm of the element $\alpha$.

Proposition 1.2.14. Let $K/F$ be abelian Galois, and let

$$\mathcal{H} = F^\times N_{K/F} J_K$$

(so $F^\times \subset \mathcal{H} \subset J_F$). Then $\mathcal{H}$ is an open subgroup in $J_F$. Moreover, if $m$ is chosen so that

$$\mathcal{E}_{F,m}^+ \subset \mathcal{H}.$$
then the image of $\mathcal{H}$ under the isomorphism

$$J_F/F^\times \cong T_\mathcal{F}(m)/P_\mathcal{F}^m$$

is precisely $P_\mathcal{F}^m N_{K/F}(m)/P_\mathcal{F}^m$. We have $[J_F : \mathcal{H}] = [T_\mathcal{F}(m) : P_\mathcal{F}^m N_{K/F}(m)] \leq [K : F]$.

**Definition 1.2.15.** Let $K/F$ be a (not necessarily abelian) Galois extension of number fields. We define an action of $\text{Gal}(K/F)$ on $J_K$. Let $G = \text{Gal}(K/F)$ and let $p = (\ldots, a_w, \ldots) \in J_K$. Let $\sigma \in G$. For a place $w$ of $K$, define the place $\sigma w$ by

$$\|\alpha\|_{\sigma w} = \|\sigma^{-1}(\alpha)\|_w \text{ or also } \|\sigma(\alpha)\|_{\sigma w} = \|\alpha\|_w.$$ 

It is clear that $G$ transitively permutes the places of $K$. $\sigma$ induces an isomorphism between the completion that we also denote by $\sigma : K_w \to K_{\sigma w}$. We may now define for each $v \in V_F$

$$\sigma(\ldots, a_w, \ldots)_{\sigma w} = (\ldots, b_w, \ldots)_{\sigma w},$$

where $b_{\sigma w} = \sigma(a_w)$, i.e., $b_w = \sigma(a_{\sigma^{-1}w})$ This gives an action of $\sigma$ on $J_K$.

Since $\Pi_{v|w} N_{K_w/F_v}(a_w)$ is the $v^{th}$ coordinate of $N_{K/F}(a)$, if we embed $J_F \to J_K$ as before, we have

$$\Pi_{\sigma \in G} \sigma(a) = N_{K/F}(a).$$

**Lemma 1.2.16.** Let $C_K = J_K/K^\times$ be the group of idèle classes of $K$, and similarly let $C_F = J_F/F^\times$. The embedding $J_F \hookrightarrow J_K$ induces an embedding $C_F \hookrightarrow C_K$. Furthermore, $C_K^G = C_F$.

**Lemma 1.2.17.** Let $k_2/k_1$ be an extension of local fields, (for some $p, k_j/Q_p$ is a finite extension), with $\text{Gal}(k_2/k_1) = G$, a cyclic group. Let $\mathcal{U}_j$ denote the units of $k_j$, i.e., the elements of absolute value 1. Then $\mathcal{Q}_G(\mathcal{U}_2) = 1$, and

$$[\mathcal{U}_2^G : s(G)\mathcal{U}_2] = [\mathcal{U}_1 : N_{k_2/k_1}\mathcal{U}_2] = e(k_2/k_1)$$

(whence also $[\text{ker } s(G) : (\sigma - 1)\mathcal{U}_2] = e(k_2/k_1)$).

**Lemma 1.2.18.** Let $k_2/k_1$ be an extension of local fields and suppose we have subgroups $B < A < \mathcal{U}_2$, with $[A : B] = d$. Then $N_{k_2/k_1}B \subset N_{k_2/k_1}A$ are subgroups of $\mathcal{U}_1$ and $[N_{k_2/k_1}A : N_{k_2/k_1}B]$ divides $d$.

**Corollary 1.2.19.** If $k_2/k_1$ is an abelian extension of local fields, then

$$[\mathcal{U}_1 : N_{k_2/k_1}\mathcal{U}_2] \leq e(k_2/k_1).$$
CHAPTER 1. GLOBAL CLASS FIELD THEORY

**Proposition 1.2.20.** For an abelian extension \( K/F \) of number fields with group \( G \), let \( \mathcal{H} = F^\times N_{K/F} J_K \). Then

i) \( \mathcal{H} \) is open in \( J_F \), so \( \mathcal{H} \supset \mathcal{E}_{F,m}^+ \) for some \( m \).

ii) the image of \( \mathcal{H} \) under the isomorphism

\[ J_F/F^\times \mathcal{E}_{F,m}^+ \cong \mathcal{I}_F(m)/\mathcal{P}_{F,m}^+ \]

is precisely

\[ \mathcal{P}_{F,m}^+ N_{K/F}(m)/\mathcal{P}_{F,m}^+. \]

**Proposition 1.2.21.** Let \( K/F \) be a Galois extension of number fields, with cyclic Galois group \( G = \langle \sigma \rangle \). Let \( v \) be a place of \( F \) and let \( w \) be a place of \( K \) above \( v \).

i) \( Q_G(U_w) = 1 \) if \( w \) is finite, if \( w \) is real, or if \( v \) is imaginary.

ii) \( Q_G(U_w) = 2 \) if \( w \) is imaginary but \( v \) is real.

iii) \( Q_G(\Pi_{v\in S} \Pi_{w|v} U_w) = 1 \), where \( S = \{ v \in V_F : v \) is infinite, or \( v \) ramifies in \( K/F \}. \)

**Lemma 1.2.22.** Let \( S \) be a finite set and let \( V = \bigoplus_{w \in S} \mathbb{R} X_w \) be a real vector space. For an element \( \sum_{w \in S} a_w X_w \) of \( V \), define

\[ \| \sum_{w \in S} a_w X_w \|_0 = \max_{w \in S} \{|a_w| : w \in S\}, \]

(the sup-norm on \( V \)). If \( \{ X'_w : w \in S \} \) is given so that \( \| X'_w - X_w \|_0 < \frac{1}{\dim_{\mathbb{R}} V} \) for each \( w \), then \( \{ X'_w : w \in S \} \) is also a basis for \( V \).

**Lemma 1.2.23.** Let \( G \) be a finite group acting on a finite set \( S \). Let \( V = \bigoplus_{w \in S} \mathbb{R} X_w \) be a vector space. Then \( G \) acts on \( V \) via

\[ \sigma \left( \sum_{w \in S} a_w X_w \right) = \sum_{w \in S} a_w X_{\sigma w}. \]

Note that the action of \( G \) preserves sup-norms: \( \| \sigma(X) \|_0 = \| X \|_0 \) for all \( X \in V \). Let \( L \subset V \) be a lattice preserved by \( G \). Then there is a basis \( \{ Y_w \}_{w \in S} \) of \( V \) contained in \( L \) such that \( \sigma(Y_w) = Y_{\sigma w} \) for all \( \sigma \in G \) and for all \( w \in S \).

**Proposition 1.2.24.** Let \( K/F \) be a Galois extension of number fields, with cyclic Galois group \( G = \langle \sigma \rangle \). Then

\[ Q_G(U_K) = \frac{2^a}{[K : F]} \]

where \( a = \# \{ v \in V_F : v \) is real on \( F \), but extends to imaginary places on \( K \}. \)

**Corollary 1.2.25.** \( Q_G(\mathcal{C}_K) = [K : F] \).
\textbf{Theorem 1.2.26. (Global Cyclic Norm Index Inequality)} If \( K/F \) is a cyclic extension of number fields and \( m \) is an integral ideal of \( \mathcal{O}_F \) that is divisible by a sufficiently high power of every ramified prime in \( K/F \), then

\[ [\mathcal{I}_F(m) : \mathcal{P}_{F,m}^+ \mathcal{N}_{K/F}(m)] = [K : F]. \]

\section*{1.3 Artin Reciprocity}

Recall that for an ideal \( m \) of \( \mathcal{O}_F \), we set

\begin{align*}
J_{F,m}^+ &= \{ a \in J_F : a_v > 0 \text{ all real } v, a_v \equiv 1 \mod p_v^{ord_v(m)} \text{ all finite } v\}, \\
\mathcal{E}_{F,m}^+ &= J_{F,m}^+ \cap \mathcal{E}_F \\
F_{m}^+ &= J_{F,m}^+ \cap F^\times \\
\mathcal{I}_F(m) &= \{ a \in \mathcal{I}_F : ord_p a = 0 \text{ for all } p | m \} \\
\mathcal{P}_{F,m}^+ &= \{ \langle \alpha \rangle \in \mathcal{P}_F : \alpha \gg 0, \alpha \equiv 1 \mod m \} \\
\mathcal{N}_{K/F}(m) &= \{ a \in \mathcal{I}_F(m) : a = \mathcal{N}_{K/F}(A) \text{ for some } A \in \mathcal{I}_K \}
\end{align*}

and showed

\[ J_F/F^\times \mathcal{E}_{F,m}^+ \cong J_{F,m}^+ / \mathcal{E}_{F,m}^+ F_m^+ \cong \mathcal{I}_F(m) / \mathcal{P}_{F,m}^+ \]

via the homomorphism \( \eta_m : J_{F,m}^+ \rightarrow \mathcal{I}_F(m) \) given by

\[ a = (\ldots, a_v, \ldots) \mapsto \langle a \rangle = \prod_{v \text{ finite}} p_v^{ord_v(a_v)} \]

\textbf{Definition 1.3.1.} There is a minimal ideal \( \mathfrak{f} \) of \( \mathcal{O}_F \) such that \( \mathcal{E}_{F,\mathfrak{f}}^+ \subset \mathcal{H} \). This ideal \( \mathfrak{f} \) is called the conductor of \( \mathcal{H} \) (or of \( K/F \)), denoted \( \mathfrak{f} = \mathfrak{f}(K/F) \). By minimality here, we mean that if \( \mathcal{E}_{F,m}^+ \subset \mathcal{H} \) then \( \mathfrak{f} | m \).

By the minimality of \( \mathfrak{f} \) we have that if \( p_v \) is unramified then \( p_v \nmid \mathfrak{f} \). The conductor cannot be divisible by any unramified prime.

\textbf{Definition 1.3.2.} Let \( K/F \) be a Galois extension of number fields with abelian Galois group \( G \), and \( p \) a prime ideal of \( \mathcal{O}_F \) that is unramified in \( K/F \). Then the decomposition group \( G_p = \mathcal{Z}(p) \) must be cyclic (inertia is trivial) with a canonical generator \( \sigma_p = \left( \frac{p}{K/F} \right) \), the Artin automorphism.
Let \( m \) be an ideal of \( \mathcal{O}_F \) that is divisible by all the primes that ramify in the extension \( K/F \) and no others. The map \( p \mapsto \sigma_p \) induces a homomorphism \( \mathcal{A} = \mathcal{A}_{K/F}: \mathcal{I}_F(m) \to G \) given by \( a \mapsto \sigma_a = \left( \frac{a}{K/F} \right) \) where, for \( a = \prod_p p^{n_p} \in \mathcal{I}_F(m) \), we set

\[
\sigma_a = \prod_p \sigma_p^{n_p} = \left( \frac{a}{K/F} \right).
\]

(\( \sigma_a \) does not depend on the choice of \( m \)). The map \( \mathcal{A} \) is called the Artin map and \( \left( \frac{a}{K/F} \right) \) is the Artin symbol. Note that since \( m \) is divisible by all the ramifying primes, \( \sigma_p \) is defined for all \( p \nmid m \).

**Proposition 1.3.3.** Let \( F \subset L \subset K, F \subset E \subset K \) be number fields and suppose \( K/F \) is abelian. Let \( \mathfrak{p} \) be a prime ideal of \( \mathcal{O}_F \) that is unramified in \( K/F \) and let \( \mathfrak{P}_K \) be a prime ideal of \( \mathcal{O}_K \) that divides \( \mathfrak{p} \). Let \( \mathfrak{P}_L = \mathfrak{P}_K \cap L, \mathfrak{P}_E = \mathfrak{P}_K \cap E \) (prime ideals of \( \mathcal{O}_E, \mathcal{O}_L \), respectively, that divide \( \mathfrak{p} \)). Then

\[
\left( \frac{\mathfrak{P}_E}{K/E} \right) \big|_L = \left( \frac{\mathfrak{p}}{L/F} \right)^f
\]

where \( f = f(\mathfrak{P}_E/\mathfrak{p}) \) is the residue field degree.

**Corollary 1.3.4.** Let \( F \subset L \subset K \) be number fields, where \( K/F \) is abelian Galois. Let \( \mathfrak{p} \) be a prime ideal of \( \mathcal{O}_F \) that is unramified in \( K/F \). Then

\[
\left( \frac{\mathfrak{p}}{K/F} \right) \big|_L = \left( \frac{\mathfrak{p}}{L/F} \right).
\]

**Corollary 1.3.5.** Let \( F \subset E \subset K \) be number fields, where \( K/F \) is abelian Galois. Let \( \mathfrak{p} \) be a prime ideal of \( \mathcal{O}_F \) that is unramified in \( K/F \) and let \( \mathfrak{P}_E \) be a prime of \( \mathcal{O}_E \) above \( \mathfrak{p} \). Then

\[
\left( \frac{\mathfrak{P}_E}{K/E} \right) = \left( \frac{N_{E/F} \mathfrak{P}_E}{K/F} \right).
\]

**Corollary 1.3.6.** Let \( K/F \) be an abelian Galois extension of number fields. Let \( m \) be an ideal of \( \mathcal{O}_F \) that is divisible by all the primes that ramify in \( K/F \). Then

\[
N_{K/F}(m) \subset \ker(\mathcal{A}: \mathcal{I}_F(m) \to G).
\]

**Theorem 1.3.7.** (Artin Reciprocity) Let \( K/F \) be an abelian extension of number fields, and assume \( m \) is an ideal of \( \mathcal{O}_F \), divisible by all the ramifying primes. Let \( G = \text{Gal}(K/F) \). Then

i) \( \mathcal{A}: \mathcal{I}_F(m) \to G \) is surjective,

ii) the ideal \( m \) of \( \mathcal{O}_F \) can be chosen so that it is divisible only by the ramified primes and satisfies \( \mathcal{P}_{F,m}^+ \subset \ker(\mathcal{A}); \) thus we have an epimorphism \( \mathcal{I}_F(m)/\mathcal{P}_{F,m}^+ \to G \).

iii) \( N_{K/F}(m) \subset \ker(\mathcal{A}) \).
Choosing \( m \) as in ii, we have a well defined homomorphism

\[ \mathcal{I}_F(m)/\mathcal{P}_{F,m}^+N_{K/F}(m) \to G \]

Since the cardinality of the LHS is \( \leq [K : F] = \#G \) by the Universal Norm Index Inequality, we have

\[ \mathcal{I}_F(m)/\mathcal{P}_{F,m}^+N_{K/F}(m) \cong G. \]

Note that this isomorphism is given by the Artin map.

**Proposition 1.3.8.** If \( K/F \) is a cyclic extension of number fields with Galois group \( G \), and \( m \) is an ideal of \( \mathcal{O}_F \) sufficiently large so that it is divisible by all the ramifying primes in \( K/F \) and so that \( \mathcal{E}_{F,m}^+ \subset F^\times N_{K/F}J_K \), then the kernel of the Artin map satisfies \( \ker(A) \subset \mathcal{P}_{F,m}^+N_{K/F}(m) \).

**Lemma 1.3.9.** Let \( r > 1, a > 1 \) be integers, and let \( q \) be a prime number. There is a prime number \( p \) such that the order of \( a \mod p \) in \( (\mathbb{Z}/p\mathbb{Z})^\times \) is \( q^r \).

**Corollary 1.3.10.** Let \( a > 1 \) be an integer. Given \( q^r \) as before, there are infinitely many primes \( p \) such that \( q^r \) divides the order of \( a \mod p \) in \( (\mathbb{Z}/p\mathbb{Z})^\times \).

**Lemma 1.3.11.** Let \( S \) be a finite set of primes, and let \( a > 1, n > 1 \) be integers. There is an integer \( d \), prime to all the elements of \( S \), such that \( n \) divides the order of \( a \mod d \) in \( (\mathbb{Z}/d\mathbb{Z})^\times \).

**Lemma 1.3.12.** Given integers \( n > 1, a > 1 \), and a finite set \( S \) of primes, there is a positive integer \( m \) such that

i) \( m \) is prime to all the elements of \( S \)

ii) \( n \) divides the order of \( a \mod m \) in \( (\mathbb{Z}/m\mathbb{Z})^\times \)

iii) there exists \( b \in \mathbb{Z} \) such that \( n \) divides the order of \( b \mod m \) in \( (\mathbb{Z}/m\mathbb{Z})^\times \) but \( a \) and \( b \) are independent \( \mod m \) (i.e., \( \langle a \mod m \rangle \cap \langle b \mod m \rangle = 1 \)).

**Lemma 1.3.13.** Let \( F \) be a number field, \( S \) a finite set of primes in \( \mathbb{Z} \), \( \mathfrak{p} \) a prime of \( \mathcal{O}_F \). Then for any integer \( n > 1 \), there exists \( m \in \mathbb{Z} \), prime to \( S \) and to \( \mathfrak{p} \), such that if \( \zeta_m \) is a primitive \( m^{th} \) root of unity, then

i) \( \text{Gal}(F(\zeta_m)/F) \cong (\mathbb{Z}/m\mathbb{Z})^\times \).

ii) \( \left( \frac{p}{F(\zeta_m)/F} \right) \) has order divisible by \( n \) in \( \text{Gal}(F(\zeta_m)/F) \).

iii) there is some \( \tau \in \text{Gal}(F(\zeta_m)/F) \) of order divisible by \( n \), such that \( \tau \) is independent to \( \left( \frac{p}{F(\zeta_m)/F} \right) \). Note: independence implies \( \langle \tau \rangle \cap Z(\mathfrak{p}) = 1 \), since \( \left( \frac{p}{F(\zeta_m)/F} \right) \) generates the decomposition group \( Z(\mathfrak{p}) \).

**Lemma 1.3.14.** (Artin’s Lemma) Let \( K/F \) be a cyclic extension of number fields of degree \( n \), \( S \) a finite set of primes of \( \mathbb{Z} \), \( \mathfrak{p} \) a prime of \( \mathcal{O}_F \). Then there is some \( m \in \mathbb{Z}_+ \), prime to the elements of \( S \) and to \( \mathfrak{p} \), and an extension \( E/F \) such that

i) \( K \cap E = F \)
ii) \( K(\zeta_m) = E(\zeta_m) \), i.e., \( KE \subset K(\zeta_m) = E(\zeta_m) \)

iii) \( K \cap F(\zeta_m) = F \)

iv) \( \mathfrak{p} \) splits completely in \( E/F \).

Suppose \( m \) satisfies Artin reciprocity and let

\[
S_{K/F} = \{ \text{prime ideals } \mathfrak{p} \text{ of } O_F : \mathfrak{p} \text{ splits completely in } K/F \}
\]

\[
J_{K/F} = \{ \text{prime ideals } \mathfrak{p} \text{ of } O_F : \mathfrak{p} \in \mathcal{P}_{F,m}^{+}N_{K/F}(m) \}.
\]

**Corollary 1.3.15.** Let \( K/F \) be an abelian extension of number fields, say with \([K : F] = n\), and let \( \mathfrak{p} \) be a prime of \( O_F \), unramified in \( K/F \). Suppose \( m \) is divisible by all the ramified primes and no others, and suppose \( m \) satisfies Artin Reciprocity. Let \( f \) be the smallest positive integer such that \( \mathfrak{p}^f \in \mathcal{P}_{F,m}^{+}N_{K/F}(m) \). Then, in \( O_L \), we have a factorization \( \mathfrak{p}O_L = \mathfrak{P}_1 \cdots \mathfrak{P}_g \), where each \( \mathfrak{P}_i \) is a prime of \( O_L \) with residue degree \( f \) over \( \mathfrak{p} \), and where \( g = n/f \). In particular, \( S_{K/F} = J_{K/F} \).

The statement of Artin Reciprocity reformulated in terms of idèles goes as follows. If \( m \) is chosen so that \( \mathcal{E}_{F,m}^{+} \subset F^{\times}N_{K/F}J_K \) then we have

\[
J_F \to J_F/F^{\times}N_{K/F}J_K \to \mathcal{I}_F(m)/\mathcal{P}_{F,m}^{+}N_{K/F}(m) \to \text{Gal}(K/F)
\]

**Definition 1.3.16.** Let \( \rho_{K/F} : J_F \to \text{Gal}(K/F) \) be the composition. It is a surjective homomorphism of groups with kernel \( F^{\times}N_{K/F}J_K \). We say \( K \) is the class field over \( F \) of \( F^{\times}N_{K/F}J_K \) and we call \( \rho_{K/F} \) the idelic Artin map. For \( a \in J_F \), we sometimes denote

\[
\rho_{K/F}(a) = \left( \frac{a}{K/F} \right).
\]

### 1.4 The Existence Theorem and its Consequences
Theorem 1.4.1. (The Existence Theorem) Every open subgroup $\mathcal{H} \subset J_F$ with $\mathcal{H} \supset F^\times$ is of the form $\mathcal{H} = F^\times N_{K/F} J_K$ for some (unique) finite abelian extension $K/F$.

Theorem 1.4.2. (The Existence Theorem) For any $\mathcal{H}$, with $\mathcal{P}_{F,m}^{+} < \mathcal{H} < \mathcal{I}_F(m)$, there is a class field $K/F$ associated to $\mathcal{H}$.

Theorem 1.4.3. (The Completeness Theorem) For any abelian extension $K/F$, there is some $m$ and some $\mathcal{H}$ with $\mathcal{P}_{F,m}^{+} < \mathcal{H} < \mathcal{I}_F(m)$ such that $K$ is the class field over $F$ of $\mathcal{H}$.

Theorem 1.4.4. (The Isomorphy Theorem) When $\mathcal{P}_{F,m}^{+} < \mathcal{H} < \mathcal{I}_F(m)$, and $K$ is the class field over $F$ of $\mathcal{H}$, we have $\text{Gal}(K/F) \cong \mathcal{I}_F(m)/\mathcal{H}$ with the isomorphism being induced by the Artin map.

Proposition 1.4.5. Let

$$\Phi : \{\text{finite abelian extensions } K \text{ of } F\} \rightarrow \{\text{open subgroups } \mathcal{H} \text{ of } J_F \text{ that contain } F^\times\}$$

be given by $\Phi(K) = F^\times N_{K/F} J_K$. Then:

i) $K \subset K'$ if and only if $\Phi(K') \subset \Phi(K)$, the Ordering Theorem,

ii) $\Phi(KK') = \Phi(K) \cap \Phi(K')$,

iii) $\Phi(K \cap K') = \Phi(K) \Phi(K')$,

iv) If $\mathcal{H} = \Phi(E) = F^\times N_{E/F} J_E$ and $K \supset E$, then $E$ is the fixed field of $\rho_K/F(\mathcal{H})$.

Corollary 1.4.6. Suppose $K$ is the class field to the open subgroup $\mathcal{H}$ of $J_F$, where $\mathcal{H}$ contains $F^\times$, and let $\mathcal{H}' \supset \mathcal{H}$ be an open subgroup of $J_F$. Then $\mathcal{H}'$ has a class field over $F$.

Proposition 1.4.7. (Reduction Lemma) Let $K/F$ be a cyclic extension of number fields and suppose $\mathcal{H}$ is an open subgroup of $J_F$ that contains $F^\times$. Let $\mathcal{H}_K = \{x \in J_K : N_{K/F}(x) \in \mathcal{H}\} = N_{K/F}^{-1}(\mathcal{H})$. If $\mathcal{H}_K$ has a class field over $K$, then $\mathcal{H}$ has a class field over $F$.

Definition 1.4.8. An abelian extension $K/F$ is said to have exponent $n$ if the abelian group $\text{Gal}(K/F)$ has exponent $n$.

Definition 1.4.9. A finite abelian extension $K/F$ is called a Kummer $n$-extension if $\text{Gal}(K/F)$ is a group with exponent $n$ and $F$ contains all the $n^{th}$ roots of unity.

Theorem 1.4.10. Let $F$ be a number field containing all the $n^{th}$ roots of unity. There is a bijective correspondence between the finite Kummer $n$-extensions $K$ of $F$ and the subgroups $W$ of $F^\times$ with $(F^\times)^n \subset W$ and $W/(F^\times)^n$ finite. The correspondence associates $W$ to the field $K = F(W^{1/n})$, for which we have $\text{Gal}(K/F) \cong W/(F^\times)^n$. 

14
Let $F$ be a number field. Let $S$ be a finite set of places of $F$ and assume $S \supseteq S_{\infty} = \{\text{infinite places of } F\}$. Define

$$J_{F,S} = \prod_{v \in S} F_v^\times \times \prod_{v \notin S} \mathcal{U}_v$$

an open subgroup of $J_F$.

$$F_S = J_{F,S} \cap F^\times$$

the S-units of $F$, a discrete subgroup of $J_{F,S}$.

Note that $F_S$ also may be defined without using idèles:

$$F_S = \{\alpha \in F^\times : \text{the factorization of } \langle \alpha \rangle \text{ involves no prime } p_v \text{ with } v \notin S\}.$$

**Lemma 1.4.11.** There is a finite set of places $S \supseteq S_{\infty}$ such that $J_F = F^\times J_{F,S}$.

**Theorem 1.4.12.** Let $S$ be a finite set of places of $F$, with $S_{\infty} \subset S$. Then $F_S$ is the direct product of the (finite cyclic) group of roots of unity in $F$, and a free abelian group of rank $\#S - 1$. That is

$$F_S \cong \mathcal{W}_F \times \mathbb{Z}^{#S-1}.$$

**Corollary 1.4.13.** If $F$ contains the $n$th roots of unity and $S \supseteq S_{\infty}$ is a finite set of places of $F$, then

$$[F_S : F^u_S] = n^{#S}.$$

**Lemma 1.4.14.** Let $v$ be a finite place of $F$, and let $n \in \mathbb{Z}_+$. If $\mu_n$ denotes the set of all $n$th roots of unity, then

i) $[\mathcal{U}_v : \mathcal{U}_v^n] = \frac{1}{\|n\|_v} (F_v \cap \mu_n)$.

ii) $[F_v^\times : (F_v^\times)^n] = \frac{n}{\|n\|_v} (F_v \cap \mu_n)$.

**Theorem 1.4.15.** Let $F$ be a number field that contains all the $n$th roots of unity. Let $S$ be a finite set of places of $F$ containing $S_{\infty}$, the places $v$ such that $p_v | n$ and sufficiently many finite places so that $J_F = F^\times J_{F,S}$. Let

$$B = \prod_{v \in S} (F_v^\times)^n \times \prod_{v \notin S} \mathcal{U}_v.$$

Then $F^\times B$ has class field $F(F_S^{1/n})$ over $F$.

**Theorem 1.4.16.** (The Existence Theorem) Let $F$ be a number field. Let $\mathcal{H}$ be an open subgroup of $J_F$ with $F^\times \subset \mathcal{H}$. Then $\mathcal{H}$ has a class field over $F$, i.e., there is a finite abelian extension $K$ of $F$ such that $\mathcal{H} = F^\times N_K/F J_K$.

**Theorem 1.4.17.** Let $\mathcal{H}$ be an open subgroup of $J_F$ that contains $F^\times$ and let $K$ be the class field of $\mathcal{H}$ over $F$. Let $v$ be a place of $F$. If $p_v$ splits completely in $K/F$, then $\phi_v(F_v^\times) \subset \mathcal{H}$, where $\phi$ is the embedding $\phi_v : F_v^\times \hookrightarrow J_F$.

**Theorem 1.4.18.** Let $\mathcal{H}$ be an open subgroup of $J_F$ that contains $F^\times$ and let $K$ be the class field over $F$ of $\mathcal{H}$. Suppose $J_F/\mathcal{H}$ has exponent $n$ and that $F$ contains the $n$th roots of unity. Let $v_0$ be a place of $F$ with $\phi_{v_0}(F_v^\times) \subset \mathcal{H}$. Then $p_{v_0}$ splits completely in $K/F$. 

15
Theorem 1.4.19. Let $K/F$ be an abelian extension of number fields, and let $v$ be a finite place of $F$. The Artin map $\rho_{K/F}$ satisfies $\rho_{K/F}(\phi_v(F_v^\times)) = \mathbb{Z}(p_v)$, the decomposition group.

Theorem 1.4.20. (Complete Splitting Theorem) Let $\mathcal{H}$ be an open subgroup $J_F$ with $F^\times \subset \mathcal{H}$, and let $K$ be the class field of $\mathcal{H}$ over $F$. Let $v$ be a finite place of $F$. Then $p_v$ splits completely in $K/F$ if and only if $\phi_v(F_v^\times) \subset \mathcal{H}$.

Corollary 1.4.21. Let $\mathcal{H}$ be an open subgroup of $J_K$ with $F^\times \subset \mathcal{H}$ and let $K$ be the class field of $\mathcal{H}$ over $F$. Then

$$\phi_v(F_v^\times) \cap \mathcal{H} = \phi_v(N_{K_w/F_w}K_w^\times)$$
$$\phi_v(U_v) \cap \mathcal{H} = \phi_v(N_{K_w/F_w}U_w).$$

Theorem 1.4.22. Let $K/F$ be an abelian extension of number fields, and let $\mathcal{H} = F^\times N_{K/F}J_K$. Let $v$ be a finite place of $F$. Then $\rho_{K/F}(\phi_v(U_v)) = T(p_v)$, the inertia subgroup in $\text{Gal}(K/F)$.

Corollary 1.4.23. If $\mathcal{H}$ is an open subgroup of $J_F$ with $F^\times \subset \mathcal{H}$, and $K$ is the class field to $\mathcal{H}$ over $F$, then for any finite place $v$ of $F$, the class field to $\mathcal{H}\phi_v(U_v)$ is the maximal subfield of $K$ in which $p_v$ is unramified, hence it is the field $K_T$, (the fixed field of $T(p_v)$).

Corollary 1.4.24. Let $K/F$ be an abelian extension of number fields, $v$ a finite place of $F$, and $w$ a place of $K$ above $v$. Then

$$U_v/N_{K_w/F_w}U_w \cong T(p_v).$$

Theorem 1.4.25. If $K/F$ is an abelian extension of number fields, then $\mathfrak{f}(K/F)$ is divisible by all the ramified primes, and no others.

Theorem 1.4.26. (Kronecker, Weber) Every finite abelian extension $F$ of $\mathbb{Q}$ satisfies $F \subset \mathbb{Q}(\zeta)$ for some root of unity $\zeta$.

Proposition 1.4.27. Let $F$ be a number field and let $\mathcal{H}$ be an open subgroup of $J_F$ that contains $F^\times$. Then $\mathcal{H} \supset F^\times \mathcal{E}_F$ if and only if the class field to $\mathcal{H}$ over $F$ is an abelian extension of $F$ that is everywhere unramified.

Definition 1.4.28. Taking $\mathcal{H} = F^\times \mathcal{E}_F$ and applying previous proposition, we find that the extension $F_1/F$ (where $F_1$ is the class field of $\mathcal{H}$) is abelian and everywhere unramified; it is necessarily the maximal unramified abelian extension of $F$. $F_1$ is called the Hilbert class field of $F$.

Theorem 1.4.29. (Principal Ideal Theorem) Every fractional ideal $\alpha$ of a number field $F$ becomes principal in $F_1$, i.e., $\alpha \mathcal{O}_{F_1}$ is principal.

Theorem 1.4.30. Let $K/F$ be an extension of number fields and suppose $K \cap F_1 = F$. Then

i) $h_F | h_K$.
ii) the map $N_{K/F} : C_K \to C_F$ is surjective.
Proposition 1.4.31. If $K/F$ is an extension of number fields, and there is some prime $p$ of $O_F$ that is totally ramified in $K/F$, then $h_F \mid h_K$.

Theorem 1.4.32. Let $E/F$ be an extension of number fields and let $\mathcal{H} = F^\times N_{E/F} J_E$, an open subgroup of $J_F$ that contains $F^\times$. Let $K$ be the class field of $\mathcal{H}$ over $F$. Then $K/F$ is the maximal abelian subextension of $E/F$.

Let $E/F$ be an arbitrary (not necessarily Galois) extension of number fields and put

$$S_{E/F}^1 = \{ \text{unramified primes } p \text{ of } O_F : f(\mathfrak{P}/p) = 1 \text{ for some prime } \mathfrak{P} | pO_E \}.$$

Theorem 1.4.33. Suppose $K/F$ is a Galois extension of number fields and $L/F$ is any finite extension. Then $S_{L/F}^1 \prec S_{K/F}$ if and only if $K \subset L$.

Corollary 1.4.34. A Galois extension of number fields $K/F$ is uniquely determined by the set $S_{K/F}$ of primes that split completely.

Definition 1.4.35. Let $M/F$ be a (possibly infinite) Galois extension with Galois group $G$. For each $\sigma \in G$, we take the cosets

$$\{ \sigma \text{Gal}(M/K) : K/F \text{ is a finite subextension of } M/F \}$$

as a basis of open neighborhoods of $\sigma$. The resulting topology is called the Krull topology on $G$.

Theorem 1.4.36. (Main Theorem of Galois Theory - General Case) Let $M/F$ be a Galois extension with Galois group $G$. The map $L \mapsto \text{Gal}(M/L)$ is a bijective correspondence between the subextension $L/F$ of $M/F$ and the closed subgroups of $\text{Gal}(M/F)$. Moreover, in this correspondence the open subgroups of $\text{Gal}(M/F)$ are paired with the finite subextensions of $M/F$.

Theorem 1.4.37. Let $p > 2$ be a prime, let $E = \mathbb{Q}(\zeta_p)$ have class number $h$, and let $E^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ have class number $h^+$. Let $h^- = h/h^+$. Then

$$h^- = 2p \Pi_{\chi \text{ odd}, f_\chi = p} \frac{1}{2} L(0, \chi)$$

$$h^+ = [\mathcal{U}_E : \mathcal{Y}_E]$$

where $\mathcal{Y}_E$ is the group of cyclotomic units of $E$, i.e.,

$$\mathcal{Y}_E = \left\{ \frac{1 - \zeta_p^a}{1 - \zeta_p^b} : a, b \not\equiv 0 \mod p \right\}.$$

Theorem 1.4.38. Let $p > 2$ be a prime, let $E = \mathbb{Q}(\zeta_p)$, and let $E^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ as before. The map $\mathcal{C}_{E^+} \to \mathcal{C}_E$ given by $[a]_{E^+} \mapsto [aO_E]_E$ is injective.
CHAPTER 1. GLOBAL CLASS FIELD THEORY

Theorem 1.4.39. Let $E = \mathbb{Q}(\zeta_p)$ and let $B_n$ denote the $n^{th}$ Bernoulli number, i.e.,
$$
\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}.
$$
Then $p \mid h_E$ if and only if $p$ divides the numerator of some $B_{2k}$, where $1 \leq k < \frac{p-1}{2}$.

Theorem 1.4.40. If $p > 2$ is prime and $p \nmid h_E$, where $E = \mathbb{Q}(\zeta_p)$, then
$$
x^p + y^p = z^p, \quad (xyz, p) = 1
$$
has no non-trivial solution in integers.

Lemma 1.4.41. If $K/E$ is everywhere unramified and Galois with $\text{Gal}(K/E) = G$, then $\mathcal{I}_K^G = \mathcal{I}_E$.

Theorem 1.4.42. (Kummer) Let $E = \mathbb{Q}(\zeta_p)$ where $p > 2$ is prime. If $p \mid h^+$, then $p \mid h^-$.

Proposition 1.4.43. Suppose $K/F$ is a $\mathbb{Z}_p$-extension, where $F$ is a number field. Let $\mathfrak{q}$ be a prime of $F$ that does not divide $p\mathcal{O}_F$. Then $K/F$ is unramified at $\mathfrak{q}$.

Proposition 1.4.44. Let $K/F$ be a $\mathbb{Z}_p$-extension, where $F$ is a number field. Some prime of $\mathcal{O}_F$ ramifies in $K/F$ and moreover there is some level $m$ such that every prime that ramifies in $K/K^{(m)}$ is totally ramified.
Chapter 2

Local Class Field Theory

2.1 Preliminaries on Local Fields

Here we let $K$ be a field that is complete with respect to a normalized discrete valuation $v_K : K^\times \to \mathbb{Z}$. We could just assume that $K$ is an extension field of $\mathbb{Q}_p$ (of possibly infinite degree). Let

- $\mathcal{O}_K = \{ x \in K : v_K(x) \geq 0 \}$
- $\mathcal{U}_K = \{ x \in K : v_K(x) = 0 \}$
- $\pi_K$, a uniformizer in $K$, so $v_K(\pi_K) = 1$
- $\mathcal{P}_K = \{ x \in K : v_K(x) > 0 \} = \pi_K \mathcal{O}_K$
- $\mathcal{U}_K^{\text{un}} = \{ x \in \mathcal{U}_K : x \equiv 1 \ \text{mod} \ \mathcal{P}_K^{\text{un}} \}$
- $\mathbb{F}_K = \mathcal{O}_K / \mathcal{P}_K$, the residue field of $K$

We also denote the following

- $K_{ur}$ a maximal unramified extension of $K$
- $\widehat{K}_{ur}$ the completeion of $K_{ur}$
- $\widehat{\mathbb{F}}_{ur}$ the residue field of $\widehat{K}_{ur}$
- $\Omega$ a complete, algebraically closed extension of $\widehat{K}_{ur}$

Consider the case when $K$ is local. Let $K_{(t)}$ denote the unramified extension of $K$ of degree $t$, i.e., the splitting field over $K$ of the polynomial $X^{q^t} - X$, where $q = \#\mathbb{F}_K$. Clearly $K_{(t)} \subset K_{(n)}$ if and only if $t \mid n$. The field $K_{ur}$ is simply the union $\bigcup K_{(t)}$. 

19
**Proposition 2.1.1.** Let $K$ be a local field. The field $\mathbb{F}_{ur}$ is an algebraic closure of $\mathbb{F}_K$. Moreover, there is a natural isomorphism $\text{Gal}(K_{ur}/K) \cong \text{Gal}(\mathbb{F}_{K_{ur}}/\mathbb{F}_K)$.

**Definition 2.1.2.** The Frobenius automorphism is just the lift to $\text{Gal}(L/K)$ of the map $x \mapsto x^q$ from $\text{Gal}(\mathbb{F}_L/\mathbb{F}_K)$, where $q$ is the cardinality of the residue field of $K$. But the map $x \mapsto x^q$ also can be viewed as belonging to $\text{Gal}(\mathbb{F}_{K_{ur}}/\mathbb{F}_K)$; its life to $\text{Gal}(K_{ur}/K)$ will be called the Frobenius automorphism of $K$, denoted $\phi$.

**Proposition 2.1.3.** Let $K$ be a local field and suppose $L/K$ is Galois with $K_{ur} \subset L$. Let $\sigma \in \text{Gal}(L/K)$ be such that $\sigma|_{K_{ur}} = \phi$. Let $F$ be the fixed field of $\sigma$ in $L$. Then $FK_{ur} = L$ and $F \cap K_{ur} = K$, so $\text{Gal}(L/F) \cong \text{Gal}(K_{ur}/K)$. Note this implies $F/K$ is totally ramified.

**Theorem 2.1.4.** (Decomposition Theorem) Let $L/K$ be a finite Galois extension, and suppose $\mathbb{F}_K$ is a finite field. There is a totally ramified extension $L'/K$ such that $L'_{ur} = L'K_{ur} = LK_{ur} = L_{ur}$. Moreover, if $\text{Gal}(L/K)_{\text{ram}}$ is central in $\text{Gal}(L/K)$, then we can take $L'/K$ to be abelian.

### 2.2 A Fundamental Exact Sequence

**Lemma 2.2.1.** Let $G$ be a finite abelian group and let $g \in G$. Then $G$ contains a subgroup $H$ such that $G/H$ is cyclic and the order of $gH$ in $G/H$ is the same as the order of $g$ in $G$.

Throughout this section, we suppose $K$ is complete with respect to a discrete valuation and $\mathbb{F}_K$ is algebraically closed. For the extension $L/K$, we put

$$V(L/K) = \langle \frac{\sigma(u)}{u} : u \in U_L, \sigma \in \text{Gal}(L/K) \rangle,$$

a subgroup of $U_L$.

**Proposition 2.2.2.** Let $L/K$ be a finite abelian extension. The group homomorphism

$$i : \text{Gal}(L/K) \to U_L/V(L/K) \text{ given by } i(\sigma) = \frac{\sigma(\pi_L)}{\pi_L}V(L/K)$$

is injective.

**Theorem 2.2.3.** Suppose $\mathbb{F}_K$ is algebraically closed, and $L/K$ is a finite cyclic extension. Let $N : U_L/V(L/K) \to U_K$ be the map that sends the coset $uV(L/K)$
to \( N_{L/K}(u) \). Since elements of \( \mathcal{V}(L/K) \) have norm 1, this is a well-defined homomorphism. The sequence

\[
1 \to \text{Gal}(L/K) \xrightarrow{i} \mathcal{U}_L/\mathcal{V}(L/K) \xrightarrow{N} \mathcal{U}_K \to 1
\]

is exact.

**Lemma 2.2.4.** Let \( L/K \) be a finite Galois extension, and let \( K \subset E \subset L \), where \( E/K \) is Galois. Then \( N_{L/E} \mathcal{V}(L/K) = \mathcal{V}(E/K) \).

**Lemma 2.2.5.** Let \( L/K \) be a finite abelian extension, let \( E \) be an intermediate field such that \( L/E \) is cyclic. Then

\[
1 \to \text{Gal}(L/E) \xrightarrow{i} \mathcal{U}_L/\mathcal{V}(L/K) \xrightarrow{\tilde{N}} \mathcal{U}_E/\mathcal{V}(E/K) \to 1
\]

is exact, where the map \( \tilde{N} \) is induced by \( N_{L/E} \).

**Theorem 2.2.6.** If \( \mathbb{F}_K \) is algebraically closed and \( L/K \) is a finite abelian extension, then

\[
1 \to \text{Gal}(L/K) \xrightarrow{i} \mathcal{U}_L/\mathcal{V}(L/K) \xrightarrow{N} \mathcal{U}_K \to 1
\]

is an exact sequence.

### 2.3 Local Units Modulo Norms

Throughout this section, we suppose \( K \) is a local field (so \( \mathbb{F}_K \) is finite). Let \( L/K \) be a finite abelian extension that is totally ramified. Then the extension \( \tilde{L}_{ur}/\tilde{K}_{ur} \) is abelian and totally ramified with \( \text{Gal}(\tilde{L}_{ur}/\tilde{K}_{ur}) \cong \text{Gal}(L/K) \). Recall we let \( \mathbb{F}_ur \) denote the residue field of \( \tilde{K}_{ur} \) (and of \( K_{ur} \)), so that \( \mathbb{F}_ur \) is an algebraic closure of \( \mathbb{F}_K \). We use \( \phi \) to denote the Frobenius automorphism in \( \text{Gal}(\mathbb{F}_ur/\mathbb{F}_K) \); also we continue to use \( \phi \) to denote its lifts in \( \text{Gal}(K_{ur}/K) \) and \( \text{Gal}(L_{ur}/L) \), and their extensions to \( \tilde{K}_{ur} \) and \( \tilde{L}_{ur} \). We have a homomorphism

\[
\phi - 1 : \mathcal{U}_{\tilde{K}_{ur}} \to \mathcal{U}_{\tilde{K}_{ur}}
\]

given by \( u \mapsto \phi(u)u^{-1} \).

**Lemma 2.3.1.** We have the following:

1. \( \phi - 1 : \mathcal{U}_{K_{ur}} \to \mathcal{U}_{K_{ur}} \) is surjective, as is \( \phi - 1 : \mathcal{O}_{K_{ur}} \to \mathcal{O}_{K_{ur}} \).
2. \( \phi - 1 : \mathcal{V}(L_{ur}/\tilde{K}_{ur}) \to \mathcal{V}(L_{ur}/\tilde{K}_{ur}) \) is surjective,
3. \( \ker(\phi - 1 : \mathcal{U}_{\tilde{K}_{ur}} \to \mathcal{U}_{\tilde{K}_{ur}}) = \mathcal{U}_K \).
Proposition 2.3.2. Define a map $\theta_{L/K} : \mathcal{U}_K \to \text{Gal}(L/K)$ for abelian extensions $L/K$ that are totally ramified. Then

1) $\theta_{L/K}$ is surjective
2) $\ker \theta_{L/K} = N_{L/K} \mathcal{U}_L$.

Theorem 2.3.3. For any finite totally ramified abelian extension $L/K$, there is an isomorphism

$\tilde{\theta}_{L/K} : \mathcal{U}_K/N_{L/K} \mathcal{U}_L \to \text{Gal}(L/K)$.

Theorem 2.3.4. If $L/K$ is a finite abelian extension, then there is a canonical isomorphism $\tilde{\theta}_{L/K} : \mathcal{U}_K/N_{L/K} \mathcal{U}_L \to \text{Gal}(L/K)_{\text{ram}}$.

### 2.4 Lubin-Tate Extensions

Definition 2.4.1. For two formal power series $F, G$ we write $F \equiv G \mod \deg d$ to mean that $F$ and $G$ coincide in terms of degree less than $d$.

Definition 2.4.2. A one-dimensional formal group law over $R$ is a power series, $F \in R[[X,Y]]$ such that

1) $F(X,0) = X$, $F(0,Y) = Y$, and
2) $F(X,F(Y,Z)) = F(F(X,Y),Z)$.

If we also have $F(X,Y) = F(Y,X)$, then $F$ is said to be a commutative formal group law.

Definition 2.4.3. Suppose $F$ and $G$ are one-dimensional formal group laws over $R$. A power series $\theta \in R[[X]]$ that satisfies

1) $\theta(X) \equiv 0 \mod \deg 1$, and
2) $\theta(F(X,Y)) = G(\theta(X),\theta(Y))$

is called an $R$-homomorphism from $F$ to $G$. Denote the set of all $R$-homomorphisms from $F$ to $G$ by $\text{Hom}_R(F,G)$.

Let $K$ be a local field. For each uniformizer $\pi$ of $K$, let

$\mathcal{F}_\pi = \{f(X) \in \mathcal{O}_K[[X]] : f(X) \equiv \pi X \mod \deg 2 \text{ and } f(X) \equiv X^q \mod \mathcal{P}_K\}$

Theorem 2.4.4. (Lubin, Tate) Let $\pi$ be a uniformizer in a local field $K$, and let $F_K$ have order $q$. Suppose $f, g \in \mathcal{F}_\pi$ and let $\ell(X_1, \ldots, X_m) = a_1X_1 + \cdots +$
Lemma 2.4.11. Suppose \( a_{m}X_{m} \) be a linear form (with \( a_{i} \in \mathcal{O}_{K} \)). Then there is a unique power series \( F \in \mathcal{O}_{K}[[X_{1}, \ldots, X_{m}]] \) such that

\[
F(X_{1}, \ldots, X_{m}) \equiv f(X_{1}, \ldots, X_{m}) \mod \deg 2
\]

\[
f(F(X_{1}, \ldots, X_{m})) = F(g(X_{1}), \ldots, g(X_{m})).
\]

**Definition 2.4.5.** For \( f \in \mathcal{F}_{\pi} \), let \( F_{f}(X, Y) \) be the unique power series in \( \mathcal{O}_{K}[[X, Y]] \) that satisfies

\[
F_{f}(X, Y) \equiv X + Y \mod \deg 2,
\]

\[
f(F_{f}(X, Y)) = f(f(X), f(Y)).
\]

The formal group laws \( F_{f} \) for \( f \in \mathcal{F}_{\pi_{K}} \) are called the **Lubin-Tate formal group laws** for \( \pi_{K} \).

**Lemma 2.4.6.** (Lubin, Tate) Suppose \( K \) is a local field, with residue field \( \mathbb{F}_{K} \) of order \( q \). Let \( \pi \) be a uniformizer in \( K \), and let \( f(X), g(X) \in \mathcal{F}_{\pi} \). Then for any \( a \in \mathcal{O}_{K} \) there is a unique power series \( [a]_{f, g}(X) \in \mathcal{O}_{K}[[X]] \) such that

\[
f([a]_{f, g}(X)) = [a]_{f, g}(g(X))
\]

\[
[a]_{f, g}(X) \equiv aX \mod X^{2}
\]

**Corollary 2.4.7.** (Lubin, Tate) Let \( K \) be a local field and let \( \pi \) be a uniformizer in \( K \). Suppose \( f(X), g(X), h(X) \in \mathcal{F}_{\pi} \) and \( a, b \in \mathcal{O}_{K} \). As is customary, we put \( [a]_{f} = [a]_{f, f} \).

i) \([\pi]_{f}(X) = f(X)\)

ii) \([a]_{f, g}([b]_{g, h}(X)) = [ab]_{f, h}(X) \) for any \( a, b \in \mathcal{O}_{K} \)

iii) \([1]_{f, g}([1]_{g, f}(X)) = X\)

iv) \([a]_{f, g}(F_{g}(X, Y)) = F_{f}([a]_{f, g}(X), [a]_{f, g}(Y))\)

v) \([a + b]_{f, g}(X) = F_{f}([a]_{f, g}(X), [b]_{f, g}(X))\).

**Lemma 2.4.8.** Let \( k \) be any field, and let \( g(X) = X^{n} + a_{n-1}X^{n-1} + \cdots + a_{0} \in k[X] \) where either \( \text{char } k = 0 \) or \( n \) is prime to \( \text{char } k \). Then we may find a positive integer \( r \) and a polynomial \( \tilde{g}(X) \in k[X] \) of degree less than \( r \), such that the polynomial \( h(X) = X^{r}g(X) + \tilde{g}(X) \) has only simple zeros.

**Proposition 2.4.9.** Let \( K \) be a local field and fix a polynomial \( f(X) \in \mathcal{F}_{\pi_{K}} \). For \( m \in \mathbb{Z}_{+} \), let \( L_{m} \) be the field associated to \( f(X) \). Then

\[
N_{L_{m}/K}\mathcal{U}_{L_{m}} \subset \mathcal{U}_{K}^{m}.
\]

**Lemma 2.4.10.** Let \( f(X) \in \mathcal{O}_{K}[[X]] \), and suppose \( L/K \) is a finite extension. If there is some \( \lambda \in L \) with \( v_{L}(\lambda) > 0 \) and \( f(\lambda) = 0 \), then there is a power series \( h(X) \in \mathcal{O}_{K}[[X]] \) with \( f(X) = (X - \lambda)h(X) \).

**Lemma 2.4.11.** Suppose \( u, u' \in \mathcal{U}_{K} \) and let \( f(X) \in \mathcal{F}_{\pi_{K}} \) be a polynomial of degree \( q \). If \( [u]_{f}(\lambda_{m}) = [u']_{f}(\lambda_{m}) \) then \( u\mathcal{U}_{K}^{m} = u'\mathcal{U}_{K}^{m} \).
CHAPTER 2. LOCAL CLASS FIELD THEORY

Theorem 2.4.12. Let $K$ be a local field and let $L_m$ be as above, for some polynomial $f(X) \in \mathcal{F}_{\pi_K}$ of degree $q$. Then $L_m/K$ is Galois, and $\text{Gal}(L_m/K) \cong \mathcal{U}_K/\mathcal{U}_m^K$.

Corollary 2.4.13. The extensions $L_m/K$ depend only on the choice of uniformizer $\pi_K$; they do not depend on the choice of polynomial $f(X) \in \mathcal{F}_{\pi_K}$.

Definition 2.4.14. The field $L_m$ is called the $m$th Lubin-Tate extension of $K$ associated to the uniformizer $\pi_K$.

Corollary 2.4.15. Let $L_m$ be the $m$th Lubin-Tate extension of a local field $K$. Then $N_{L_m/K} \mathcal{U}_{L_m} = \mathcal{U}_m^K$.

Theorem 2.4.16. Let $K$ be a local field. There are isomorphisms $\text{Gal}(K_{ab}/K)_{\text{ram}} \cong \mathcal{U}_K$ and $\text{Gal}(K_{ab}/K) \cong \mathcal{U}_K \times \hat{\mathbb{Z}}$.

Corollary 2.4.17. Let $K$ be a local field with uniformizer $\pi_K$. Put $L_{\pi_K} = \bigcup L_m$ where the $L_m$ are the Lubin-Tate extensions of $K$ associated to the uniformizer $\pi_K$. Then $K_{ab} = L_{\pi_K} K_{ur}$.

2.5 The Local Artin Map

Lemma 2.5.1. If $L/K$ is a finite abelian extension, then $[K^\times : N_{L/K}L^\times] = [L : K]$.

Let $\rho_{LK(t)/K} : K^\times \to \text{Gal}(LK(t)/K)$ be the unique homomorphism that satisfies

$$\rho_{LK(t)/K}(u) = \theta_{L/K}(u^{-1}) \text{ for } u \in \mathcal{U}_K$$

$$\rho_{LK(t)/K}(\pi_K) = \phi \text{ Frobenius in } \text{Gal}(LK(t)/L).$$

Lemma 2.5.2. Let $K(t)/K$ be a finite unramified extension of $K$ of degree $t$. Let $L/K$ and $E/K$ be finite totally ramified abelian extension of $K$ such that $LK(t) = ED(t)$. Consider the composition

$$K^\times \xrightarrow{\rho_{LK(t)/K}} \text{Gal}(LK(t)/K) \xrightarrow{\text{nat}} \text{Gal}(E/K).$$

The kernel of this composition is $N_{E/K}E^\times$. 

24
Definition 2.5.3. Choose a uniformizer $\pi_K$ of $K$, and use the union $L_{\pi_K}$ of the Lubin-Tate extensions of $K$, recalling that $K_{ab} = L_{\pi_K} K_{ur}$, and we may identify $\text{Gal}(K_{ab}/K_{ur}) = \text{Gal}(L_{\pi_K}/K)$. Define $\rho_K : K^\times \to \text{Gal}(K_{ab}/K)$ to be the unique homomorphism that satisfies

$$\rho_K(u) = \theta_{K_{ab}/K}(u^{-1}) \in \text{Gal}(L_{\pi_K}/K) \text{ for } u \in U_K$$

$$\rho_K(\pi_K) = \phi \text{ Frobenius in } \text{Gal}(K_{ab}/L_{\pi_K}).$$

Since $\pi_K \in N_{L_m/K} L_m^\times$ for all the Lubin-Tate extensions $L_m/K$, it follows that $\rho_K$ agrees with $\rho_{L_m,K_{(i)}/K}$. $\rho_K$ is called the local Artin map or the local norm residue map.

Theorem 2.5.4. Let $L/K$ be a finite abelian extension. Consider the composition

$$K^\times \overset{\rho_K}{\to} \text{Gal}(K_{ab}/K) \overset{\text{rest}}{\to} \text{Gal}(L/K).$$

The kernel of this composition is $N_{L/K} L^\times$.

Corollary 2.5.5. The open subgroups of finite index in $K^\times$ are precisely the subgroups of the form $N_{L/K} L^\times$, for $L/K$ finite abelian. Indeed, any open subgroup of finite index in $K^\times$ is the kernel of the composition

$$K^\times \overset{\rho_K}{\to} \text{Gal}(K_{ab}/K) \overset{\text{nat}}{\to} \text{Gal}(L/K)$$

for some finite abelian extension $L/K$.

Lemma 2.5.6. Let $\pi$ and $\pi'$ be uniformizers in a local field $K$, say with $\pi' = u \pi$, where $u \in U_K$. Let $q = \# F_K$ and suppose $f(X), g(X)$ are polynomials of degree $q$ such that $f(X) \in F_\pi$ and $g(X) \in F_{\pi'}$. We use $\phi$ to denote the Frobenius automorphism in $\text{Gal}(K_{ur}/K)$ and also its extension to $\hat{K}_{ur}$.

Theorem 2.5.7. Define the homomorphism $\gamma_\pi : K^\times \to \text{Gal}(L_\pi K_{ur}/K)$, with

$$\gamma_\pi(u) = \sigma_u^{-1} \in \text{Gal}(L_\pi K_{ur}/K_{ur}) \cong \text{Gal}(L_\pi/K),$$

$$\gamma_\pi(\pi) = \phi \text{ Frobenius in } \text{Gal}(L_\pi K_{ur}/L_\pi).$$

$\gamma_\pi$ does not depend on the choice of uniformizer $\pi$. Moreover, $\gamma_\pi$ is the local Artin map, i.e., $\gamma_\pi = \rho_K$. 

25