CLC_____ Number_____
UDC_____ Available for reference ☐ Yes ☐ No

Senior Thesis

Thesis Title: **Local Class Field Theory for p-adic Fields and Its Applications**

Student Name: **叶靖 Jing YE**

Student ID: **11610328**

Department: **数学系 Department of Mathematics**

Program: **数学与应用数学 Mathematics and Applied Mathematics**

Thesis Advisor: **胡勇 Yong Hu**

Date: 30th April 2020

Local Class Field Theory for p-adic Fields and Its Applications

叶靖 Jing YE

(数学系 Department of Mathematics　Thesis Advisor: 胡勇 Yong HU)

[ABSTRACT]: Class field theory is a crowning achievement of algebraic number theory in the first half of the 20th century. It combines the quadratic and higher reciprocal laws of Gauss, Legendre and others in a unified way and generalizes them widely. This thesis is a note for local class field theory in a special case. In this thesis, we will focus on p-adic fields. We first discuss some basic results of p-adic fields, including the multiplicative structure of the unit group of a p-adic field and its Brauer group. We then establish the fundamental theorem of local class field theory for p-adic fields via cohomological point of view. We will apply this strong result to prove the local Kronecker-Weber theorem as an application.

[Keywords]: p-adic fields; Brauer groups; the reciprocity isomorphisms; the existence theorem; Kronecker-Weber theorem

[摘要]: 类域论是 20 世纪上半叶代数数论的一个重要成果. 它将 Gauss、Legendre 等的二次互反律以及高次互反律统一起来，并得到了广泛的推广. 本论文是对局部类域论的一个读书笔记与总结. 在本文中，我们将关注 p 进域. 我们首先讨论了 p 进域的一些基本结果，包括 p 进域的单位群的乘法结构及其 Brauer 群，然后从上同调的观点建立了 p 进域的局部类域论基本定理. 我们将应用这个强有力的结果来证明局部 Kronecker-Weber 定理.

[关键词]: p 进域; Brauer 群; 互反同构; 存在性定理; Kronecker-Weber 定理

Contents

1 Introduction and Motivation **1**

2 Preliminaries **5**

2.1 p-adic fields 5

2.2 Unramified and totally ramified extensions 6

2.3 Central simple algebras and Brauer groups 9

3 The multiplicative structure of p-adic fields **11**

3.1 The first glance at $F^\times$ 11

3.2 Module structure 13

3.3 Multiplicative structure of $F^\times$ and some applications 15

4 The Brauer group of a p-adic field **17**

4.1 The Hasse invariant 17

4.2 The structure of $\mathrm{Br}(F)$ 21

5 Fundamental theorem of local class field theory **24**

5.1 Reciprocity isomorphisms 24

5.2 The Existence theorem 28

6 A classical application **34**

6.1 The local Kronecker-Weber theorem 34

Reference **38**

Acknowledgement **39**

1 Introduction and Motivation

Before stepping into our main result, we discuss a simple example first. As we know, fintie extensions of a finite field $\mathbb{F}_q$ are of the form $\mathbb{F}_{q^n}$, where q is a prime power. They are all abelian extensions. By Galois theory, we know that, for each $n \geqslant 1$, $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is isomorphic to the cyclic group $\mathbb{Z}/n\mathbb{Z}$. Moreover, $\overline{\mathbb{F}}$ is the maximal abelian extension $\mathbb{F}_q^{\mathrm{ab}}$.

Consider the projection $p_n : \mathrm{Gal}(\mathbb{F}_q^{\mathrm{ab}}/\mathbb{F}_q) \to \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$. We see that $\mathrm{Gal}(\mathbb{F}_q^{\mathrm{ab}}/\mathbb{F}_q) = \varprojlim \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \varprojlim \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}$.

By the infinite Galois theory, we see that there exists a one-to-one correspondence between

$$\{ \text{ finite abelian extensions of } \mathbb{F}_q \}$$

and

$$\{ \text{ open subgroups of } \mathrm{Gal}(\mathbb{F}_q^{\mathrm{ab}}/\mathbb{F}_q) \}.$$

Equivalently, there exists a one-to-one correspondence between

$$\{ \text{ finite abelian extensions of } \mathbb{F}_q \}$$

and

$$\{ \text{ subgroups of } \mathbb{Z} \text{ of finite index} \}.$$

In fact, let $\sigma_q \in \mathrm{Gal}(\mathbb{F}_q^{\mathrm{ab}}/\mathbb{F}_q)$ defiend by $x \mapsto x^q$ and $\rho : \mathbb{Z} \to \mathrm{Gal}(\mathbb{F}_q^{\mathrm{ab}}/\mathbb{F}_q)$ by $r \mapsto \sigma_q^r$. The one-to-one correspondence is given by $U \leftrightarrow \rho^{-1}(U)$, where U is an open subgroup of $\mathrm{Gal}(\mathbb{F}_q^{\mathrm{ab}}/\mathbb{F}_q)$.

Now, we turn to local class field theory, which asserts that a similar phenomenon happens for a local field. Recall the classification theorem of local fields: if K is a local field with a proper absolute value $\| \cdot \|$, then

(1) $K \cong \mathbb{R}$ or $\mathbb{C}$, if $\mathrm{char}(K) = 0$ and $\| \cdot \|$ is archimedean.

(2) K is a finite extension of $\mathbb{Q}_p$ for a prime $p \in \mathbb{Z}$, if $\mathrm{char}(K) = 0$ and $\| \cdot \|$ is non-archimedean.

(3) $K \cong \mathbb{F}_q((T))$, where q is a finite power of p, if $\mathrm{char}(K) = p$ for a prime $p \in \mathbb{Z}$.

The first case is pretty easy and we mainly deal with the second case in this thesis. In this case, the local field K is called a p-adic field. The following is our main result:

Fundamental theorem of local class field theory. *Suppose F is a p-adic field, and $\overline{F}$ is an algebraic closure of F. Let*

$$\mathcal{A} = \left\{ K : F \subseteq K \subseteq \overline{F} \text{ such that } K/F \text{ is finite abelian } \right\}$$

and

$$\mathcal{S} = \left\{ \text{ subgroups of finite index in } F^\times \right\}.$$

Then the map $K \mapsto N_K$ is a one-to-one, order-reversing correspondence between $\mathcal{A}$ and $\mathcal{S}$.

Here, N_K is the so-called "norm subgroup", which has finite index in $F^\times$. We will re-introduce and prove this theorem in chapter 5.

Observe that the bijection is order-reversing, we can deduce some identities immediately from this theorem. Let K_1 and K_2 be two abelian extensions of F. Since the composite K_1K_2 is the smallest abelian extension containing K_1 and K_2, the group $\mathrm{N}_{K_1K_2}$ is then the largest group contained in $\mathrm{N}_{K_1} \cap \mathrm{N}_{K_2}$. So, we must have

$$\mathrm{N}_{K_1K_2} = \mathrm{N}_{K_1} \cap \mathrm{N}_{K_2}\,.$$

In the same manner, we have

$$\mathrm{N}_{K_1 \cap K_2} = \mathrm{N}_{K_1}\,\mathrm{N}_{K_2}\,.$$

Moreover, we have the following result

Theorem 1.0.1. *Suppose K/F is a finite Galois extension of p-adic fields. Then we have an isomorphism of abelian groups*

$$\mathrm{Gal}(K/F)^{\mathrm{ab}} \cong F^\times / \mathrm{N}_{K/F}(K^\times).$$

In particular, if K/F is an abelian extension, we must have $\mathrm{Gal}(K/F) \cong F^\times / \mathrm{N}_K$*, and the index of* N_K *in $F^\times$ is $[K : F]$.*

Now, if we take inverse limit over all finite Galois extension K of F, we have an isomorphism

$$\varprojlim \mathrm{Gal}(K/F)^{\mathrm{ab}} = \mathrm{Gal}(\overline{F}/F)^{\mathrm{ab}} \cong \varprojlim F^\times / \mathrm{N}_{K/F}(K^\times).$$

We then have an injective continuous homomorphism with dense image, the **Artin reciprocity homomorphism**

$$\mathrm{Art}_K : K^\times \to \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}}$$

induced by the canonical map $K^\times \to \varprojlim K^\times / \mathrm{N}_{K/F}(K^\times)$.

Further, the local class field theory can be regarded as the GL_1 case of Langlands Program. We now given an overview of local Langlands correspondence.

Let K be a p-adic field with ring of integers $\mathcal{O}$, unqiue maximal ideal $\mathfrak{p}$ and residue field $\mathbb{K} = \mathcal{O}/\mathfrak{p}$. Let $\mathbb{F}_q$ be the residue field of K, which is a finite extension of $\mathbb{F}_p$, i.e. $q = p^f$.

Definition 1.0.2. *A complex vector space V with an action of $\mathrm{GL}_n(K)$ is said to be a **complex admissible representation** of $\mathrm{GL}_n(K)$. Equivalently, it is a group homomorphism*

$$\varphi : \mathrm{GL}_n(K) \to \mathrm{GL}(V)$$

such that

(***Admissibility***) *If $U \subseteq \mathrm{GL}_n(K)$ is an open subgroup, then V^U is a finite-dimensional vector space.*

(***Smoothness***) *If $v \in V$, then stabilizer of v in $\mathrm{GL}_n(K)$ is open.*

Notation. *Denote by $\mathcal{A}_1(K)$ the set of equivalent classes of irreducible complex admissible representations of $K^\times = GL_1(K)$.*

By Schur's lemma, an irreducible admissible representation φ of $GL_1(K) = K^\times$ is of degree one, i.e. a character

$$\varphi : K^\times \to \mathbb{C}^\times.$$

Thus, $\mathcal{A}_1(K)$ is simply the set of continuous homomorphisms $K^\times \to \mathbb{C}\times$ where $\mathbb{C}^\times$ is endowed with the discrete topology.

Now, given an automorphism $\sigma \in \mathrm{Gal}(\overline{K}/K)$, we have $\sigma(\mathfrak{p}) = \mathfrak{p}$. So we have an induced automorphism $\overline{\sigma} \in \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. Consider the natural map $\pi : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ given by $\sigma \mapsto \overline{\sigma}$. Let I_K be the kernel of this natural map, called **inertia group**. Then we obtain a left exact sequence

$$1 \to I_K \to \mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q).$$

By infinite Galois theory, we have

$$\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \cong \varprojlim \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \varprojlim \mathbb{Z}/n\mathbb{Z} := \hat{\mathbb{Z}}$$

as $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is cyclic of order n generated by the Frobenius map $\sigma_K : x \mapsto x^q$. So it contains the free abelian group $\langle \sigma_K \rangle$ as a subgroup.

Definition 1.0.3. *We define the **Weil group** of K to be the inverse image of $\langle \sigma_K \rangle$ under π, denoted by W_K.*

We then have a commutative diagram with exact rows

$$\begin{array}{ccccccccc}
1 & \longrightarrow & I_K & \longrightarrow & W_K & \longrightarrow & \langle \sigma_K \rangle & \longrightarrow & 1 \\
 & & \| & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & I_K & \longrightarrow & \mathrm{Gal}(\overline{K}/K) & \longrightarrow & \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) & &
\end{array}$$

Let W_K^{ab} be the maximal Hausdorff abelian quotient group of W_K, that is, $W_K^{\text{ab}} = W_K/\overline{W_K'}$, where W_K' is the commutator subgroup and $\overline{W_K'}$ is the closure of W_K'. One can show that the image of $\text{Art}_K : K^\times \to \text{Gal}(\overline{K}/K)^{\text{ab}}$ is W_K^{ab}. Hence, we have an isomorphism

$$\text{Art}_K : K^\times \to W_K^{\text{ab}}.$$

Notation. *Denote by $\mathcal{G}_1(K)$ the set of continuous homomorphisms $W_K \to \mathbb{C}^\times = \text{GL}_1(\mathbb{C})$, where $\mathbb{C}^\times$ is endowed with its usual topology.*

Now, one can check that a homomorphism $W_K \to \mathbb{C}^\times$ with respect to the usual topology on $\mathbb{C}^\times$ if and only if it is continuous with respect to the discrete topology on $\mathbb{C}^\times$.

Now, we see that local class field theory is equivalent to

Theorem 1.0.4 (Local Langlands Correspondence for $\text{GL}_1(K)$). *There is a natural bijection between the sets $\mathcal{A}_1(K)$ and $\mathcal{G}_1(K)$.*

If we let $\mathcal{A}_n(K)$ be the set of equivalent classes of irreducible admissible representations of $\text{GL}_n(K)$ and $\mathcal{G}_n(K)$ be the set of equivalent classes of Frobenius semi-simple complex Weil-Deligne representations of degree n of W_K (for the definition of Frobenius semi-simple Weil-Deligne representation, one can check [6] for more details), the theorem above can be generalized as

Conjecture 1.0.5 (Local Langlands Correspondence for $\text{GL}_n(K)$ over p-adic fields). *There is a unique collection of bijections $\text{Rec}_n : \mathcal{A}_n(K) \to \mathcal{G}_n(K)$.*

In fact, the complete version of this theorem claims further that Rec_n satisfies some nice properties. Unfortunately, these properties involve too many complicated notions and much of them are still open problems so we will not mention them here.

2 Preliminaries

In this chapter, we intend to review some basic definitions and results in local fields. In particular, we will focus on the concepts of p-adic fields, unramified and totally ramified extensions, which will be used later. One can consult [1], [3] and [4] for details.

2.1 p-adic fields

Definition 2.1.1. *Let F be a field. We use $\mu_n(F)$ to denote the group of n-th roots of unity contained in F for each $n \geqslant 1$.*

Remark 2.1.2. *If* $\mathrm{char}(F) = p$ *and* $n = p^\ell m$, *it is clear that* $\mu_n(F) = \mu_m(F)$.

Definition 2.1.3. *Let p be a prime number. A* ***p-adic field*** *is a finite extension K of $\mathbb{Q}_p$.*

Remark 2.1.4. *One should notice that p-adic field is an example of local fields, if the readers are familiar with number theory.*

Theorem 2.1.5. *Let F be a field and v a discrete valuation on F. Suppose F is complete. Let K/F be an extension with $[K : F] = n$. Then there exists a unique discrete valuation v_K on K such that $v_K|_F = v$ and*

$$v_K(\alpha) = \frac{1}{n} v(\mathrm{N}_{K/F}(\alpha)).$$

Moreover, let

$$\min(F, \alpha) = X^d + a_{d-1}X^{d-1} \cdots + a_0,$$

be the minimal polynomial of α, then $v_K(\alpha) = \frac{1}{d} v(a_0)$.

Proof. See [2], Chapter I, Proposition 1.1. ■

Corollary 2.1.6. *Suppose that K/F is finite Galois, $\sigma \in \mathrm{Gal}(K/F)$, and $x \in K$. Then, we have $v_K(\sigma(x)) = v_K(x)$.*

Definition 2.1.7. *Suppose K/F is an extension of p-adic fields. We call*

$$e(K/F) = [v_K(K^\times) : v_F(F^\times)]$$

the ***ramification index****. We denote $e(K/\mathbb{Q}_p)$ by $e(K)$ for convenience.*

We call

$$f(K/F) = [\mathbb{K} : \mathbb{F}]$$

*the **inertia degree** of K/F, where $\mathbb{K}$ and $\mathbb{F}$ are residue fields of K and F respectively. In convention, we set $f(K) = f(K/\mathbb{Q}_p)$.*

From now on, let K/F be an extension of p-adic fields, $\mathcal{O}_K$ and $\mathcal{O}_F$ their rings of integers. We use $\mathfrak{P}$ and $\mathfrak{p}$ to denote the maximal ideals of $\mathcal{O}_K$ and $\mathcal{O}_F$ respectively. Let $\mathbb{K} = \mathcal{O}_K/\mathfrak{P}$ and $\mathbb{F} = \mathcal{O}_F/\mathfrak{p}$ be their residue fields. Let $e = e(K/F)$ and $f = f(K/F)$.

Proposition 2.1.8. (1) $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}^e$.

(2) *The ring $\mathcal{O}_K$ is a free $\mathcal{O}_F$-module of rank $n = [K : F]$.*

Proof. See [1], Chapter 2, Lemma 2.35 and Proposition 2.36. ■

Theorem 2.1.9. *In the notation above, we have $[K : F] = ef$.*

Proof. See [2], Chapter I, Proposition 1.5. ■

2.2 Unramified and totally ramified extensions

Definition 2.2.1. *Suppose we have an extension K/F of p-adic fields. K/F is called **unramified** if the ramification index $e(K/F) = 1$ and **totally ramified** if the inertia degree $f(K/F) = 1$.*

Remark 2.2.2. *K/F is unramified if and only if $\mathfrak{P} = \mathfrak{p}\mathcal{O}_K$ if and only if $v_K(K^\times) = v_F(F^\times)$ if and only if $[K : F] = [\mathbb{K} : \mathbb{F}]$.*

Definition 2.2.3. *The natural map $\mathrm{Gal}(K/F) \to \mathrm{Gal}(\mathbb{K}/\mathbb{F})$ is defined to be $\sigma \mapsto \overline{\sigma}$, where $\overline{\sigma}(\overline{\alpha}) = \overline{\sigma(\alpha)}$ for all $\alpha \in \mathcal{O}_K$.*

*We define the **inertia subgroup** of $\mathrm{Gal}(K/F)$ to be the kernel of $\mathrm{Gal}(K/F) \to \mathrm{Gal}(\mathbb{K}/\mathbb{F})$, denoted by $I(K/F)$.*

Theorem 2.2.4. *Suppose F is a p-adic field. For any $n \geqslant 1$, there exists an unramified extension L/F such that $[L : F] = n$.*

Suppose K/F is an extension such that n divides $[\mathbb{K} : \mathbb{F}]$, there are exactly n distinct embeddings $L \to K$. In particular, the extension L/F is unique up to isomorphism, and is Galois.

The natural map $\mathrm{Gal}(L/F) \to \mathrm{Gal}(\mathbb{L}/\mathbb{F})$ is an isomorphism. Here, $\mathbb{L}$ is the residue field of L.

Proof. See [1], Chapter 2, Theorem 2.40. ■

Corollary 2.2.5. *Let L/F be an unramified extension. Then L/F is Galois and* $\mathrm{Gal}(L/F)$ *is cyclic, generated by a canonical element denoted* $\mathrm{Frob}_{L/F}$ *and said to be the* ***Frobenius element****. We have* $\mathrm{Frob}_{L/F}(x) \equiv x^q \mod \mathfrak{P}$*, for all $x \in \mathcal{O}_L$, where $\mathfrak{P}$ is the maximal ideal of $\mathcal{O}_L$ and $q = |\mathbb{L}|$.*

Corollary 2.2.6. *Suppose F is a p-adic field, and $\overline{F}$ is an algebraic closure of F. Let $\overline{\mathbb{F}}$ be an algebraic closure of the residue field $\mathbb{F}$.*

Let

$$\mathcal{U} = \left\{ K : F \subseteq K \subseteq \overline{F} \text{ such that } K/F \text{ is unramified } \right\}$$

and

$$\mathcal{F} = \left\{ \mathbb{K} : \mathbb{F} \subseteq \mathbb{K} \subseteq \overline{\mathbb{F}} \text{ such that } \mathbb{K}/\mathbb{F} \text{ is finite } \right\}.$$

Then the map $K \mapsto \mathbb{K}$ is a one-to-one, inclusion-preserving and dimension-preserving correspondence between $\mathcal{U}$ and $\mathcal{F}$.

Corollary 2.2.7. *For each integer $n \geqslant 1$, there exists a field $E_n \subseteq \overline{F}$ with E_n/F unramified with $[E_n : F] = n$ and $E_n \subset E_m$ if and only if n divides m. There are no other unramified extension of F in $\overline{F}$.*

Proof. This simply follows from Corollary 2.2.6 and Galois theory of finite fields. ■

Definition 2.2.8. *Suppose K/F is an extension of p-adic fields. We call K_0 an* ***inertia subfield*** *of K/F if $F \subseteq K_0 \subseteq K$ and for any intermediate field L, L/F is unramified if and only if L is a subfield of K_0.*

Remark 2.2.9. *We will see that K_0 exists and is unique in next proposition. The definition means that the inertia subfield K_0 is the maximal unramified extension contained in K.*

Proposition 2.2.10. *Suppose K/F is an extension of p-adic fields. Then there exists a unique inertia subfield K_0 of K/F. We have $[K : K_0] = e(K/F)$. In particular, K/F is unramified if and only if $K = K_0$.*

Proof. First, we may choose an algebraic closure and put all fields in $\overline{F}$. Let $\mathbb{K}$ be the residue field of K, then there exists a unique unramified extension K_0/F such that $K_0 \mapsto \mathbb{K}$. Set $n = [K_0 : F] = [\mathbb{K} : \mathbb{F}]$. We see that K_0 is a subfield of K by Theorem 2.2.4. So, $[K : F] = e(K/F)[\mathbb{K} : \mathbb{F}] = [K_0 : F]$. Thus, $[K : K_0] = e(K/F)$. The fact that K_0 is an

inertia subfield simply follows from Corollary 2.2.6 and the fundamental theorem of Galois theory. ■

Proposition 2.2.11. (1) *Suppose $F \subseteq K \subseteq L$ are extensions of p-adic fields. Then L/F is unramified if and only if K/F and L/K are both unramified.*

(2) *Suppose K/F and L/F are unramified extensions of p-adic fields such that K, L are contained in a common field, then KL/F is also unramified.*

Proof. (1) is clear by Remark 2.2.2. (2) simply follows from that unramified extenisons are contained in the inertia subfield. ■

Proposition 2.2.12. *Suppose K/F is an extenison of p-adic fields. The natural map* $\mathrm{Gal}(K/F) \to \mathrm{Gal}(\mathbb{K}/\mathbb{F})$ *is surjective if K/F is Galois.*

Proof. See [1], Chapter 2, Lemma 2.45. ■

We now list some facts about topological groups, which will be used later. The proofs can be found in [1]

Lemma 2.2.13. *Suppose G is a topological group and H is a group endowed with the discrete topology. Then a homomorphism $\psi : G \to H$ is continuous if and only if* $\ker \psi$ *is open. If H is finite, then* $\ker \psi$ *is open* $\Leftrightarrow \ker \psi$ *is closed.*

Proof. See [1], Chapter 3, Lemma 3.3. ■

Lemma 2.2.14. *Suppose $\{X_i\}$ is a family of discrete topological spaces over a directed set I. Let $X = \varprojlim X_i$ be the inverse limit and $p_i : X \to X_i$ the projection. Let $A, B \subset X$ be subsets of X. If $p_i(A) \subset p_i(B)$ for each $i \in I$, then $A \subset \overline{B}$.*

Proof. See [1], Chapter 3, Lemma 3.12. ■

Definition 2.2.15. *Suppose p is a prime number, and let $r > 0$. We define* ***the open ball of radius*** r ***centered at*** x_0 *to be*

$$B(x_0, r) = \{x \in F : |x - x_0|_p < r\}$$

and ***the closed ball of radius*** r ***centered at*** x_0 *to be*

$$B_c(x_0, r) = \{x \in F : |x - x_0|_p \leqslant r\}.$$

Lemma 2.2.16. *Let p be a prime number, and let $r > 0$. Then*

(1) *If $p^{-(n+1)} < r \leqslant p^{-n}$, then $B(x_0, r) = B_c(x_0, p^{-(n+1)})$. In particular, any open ball is closed.*

(2) *If $p^{-(n+1)} \leqslant r < p^{-n}$, then $B_c(x_0, r) = B(x_0, p^{-n})$. In particular, any closed ball is open.*

(3) *All of the open and closed balls defined above are homeomorphic and compact.*

Proof. See [1], Chapter 3, Lemma 3.26. ■

2.3 Central simple algebras and Brauer groups

In this section, we list some important theorems about central simple algebras and Brauer groups for later use. One can check [1] for details.

Definition 2.3.1. *Let F be a field. A ring A is said to be a central simple F-algebra if its center $\mathcal{Z}(A) \cong F$ and $[A : F] = \dim_F A < \infty$.*

Let F be a field. Suppsoe A, B are two central simple F-algebras. A and B are said to be **Brauer equivalent** if there exists a skewfield K with center F such that $A \cong M_n(K)$ and $B \cong M_m(K)$ for some integers m, n. The isomorphism classes of A are called **Brauer classes** of A, denoted by $[A]$. The set of Brauer classes of all central simple F-algebras are called the **Brauer group** of F, denoted by $\mathrm{Br}(F)$. A basic fact in algebra is that $A \otimes_F B$ is a central simple F-algebra if A, B are simple F-algebras with one of them central and the Brauer class $[A \otimes_F B]$ only depends on $[A]$ and $[B]$. Besides, if K is a skewfield with center F and $[K : F] < \infty$, we have an isomorphism $K \otimes_F K^{\mathrm{op}} \cong M_n(F)$. With these facts, we can define a multiplication on $\mathrm{Br}(F)$ by $[A] \cdot [B] = [A \otimes_F B]$ and endow a group structure on it. We see that $[A]^{-1} = [A^{\mathrm{op}}]$.

Theorem 2.3.2 (the commutant theorem). *Suppose A is a central simple F-algebra and B a simple sub-F-algebra. Let $B' = \mathcal{C}_A(B) = \{a \in A | ab = ba, \forall b \in B\}$. Then*

(1) *B' is simple.*

(2) *$[B : F][B' : F] = [A : F]$.*

(3) *$\mathcal{C}_A(B') = B$, or $B'' = B$.*

Proof. See [1], Chapter 6, Theorem 6.26. ■

Corollary 2.3.3. *Suppose A is a central simple F-algebra and B a simple commutative sub-F-algebra. Let $B' = C_A(B)$. Then $B = Z(B')$ and the following three conditions are equivalent*

(1) *B is a maximal commutative subalgebra of A.*

(2) $B = B'$.

(3) $[A : F] = [B : F]^2$.

Suppsoe A is a central simple F-algebra, and E/F is a field extension. E is said to be a **splitting field** for A if $[A] \in \mathrm{Br}(E/F)$, i.e. $A \otimes_F E$ is Brauer equivalent to E.

Proposition 2.3.4. *Suppose A is a central simple F-algebra. Suppose $E \subset A$ is a maximal commutative subalgebra of A. Then E is a splitting field for A if E is a field.*

Proof. See [1], Chapter 6, Proposition 6.35. ■

Proposition 2.3.5. *Suppose K is a skewfield with $Z(K) = F$ and $[K : F] = n^2$. Then K has a splitting field E with $[E : F] = n$. Moreover, the dimension of any splitting field for K is a multiple of n.*

Proof. See [1], Chapter 6, Corollary 6.39. ■

We now discuss some result related to group extension.

Suppsoe G is a finite cyclic group, M is a G-module. Define

$$M^G = \{m \in M : g \cdot m = m, \forall g \in G\}$$

and a map $N : M \to M$ by $N(m) = \sum_{g \in G} g \cdot m$. We write $N(M) = \mathrm{im}\ N$.

Proposition 2.3.6. *Let $\rho \in G$ be a generator, define $\varphi_\rho : Z^2(G, M) \to M^G$ by*

$$c \mapsto \sum_{\tau \in G} c(\tau, \rho).$$

Then we have an induced isomorphism

$$H^2(G, M) \cong M^G / N(M).$$

Proof. See [1], Chapter 7, Proposition 7.18. ■

Proposition 2.3.7. *The map $\mathrm{H}^2(\mathrm{Gal}(E/F), E^\times) \to \mathrm{Br}(E/F)$ given by $c \mapsto [A_c]$ is a group isomorphism.*

Proof. See [1], Chapter 7, Proposition 7.26. ■

3 The multiplicative structure of p-adic fields

In this chapter, we intend to describe the multiplicative group of a p-adic field, where p is a given prime number.

Conventions for this chapter. Let p be a prime number and F a p-adic field whose residue field will be denoted as $\mathbb{F}$. Set $q = |\mathbb{F}|$ and let $f = f(F)$ be the inertia degree, so we have $q = p^f$. We write v_F or v_p for the valuation on F extending the p-adic valuation v_p on $\mathbb{Q}_p$. The valuation ring of integers will be denoted as $\mathcal{O}_F$. Let $\mathfrak{p} = (\pi)$ be the maximal ideal of $\mathcal{O}_F$ and π a uniformizer. Let $e = e(F)$ be the ramification index, then $v = ev_p$ is the normalized valuation of F. For each $n \geqslant 1$, we write $U_F^{(n)}$, or simply $U^{(n)}$, for the subgroup $1 + \mathfrak{p}^n = \{x \in \mathcal{O}_F : x \equiv 1 \mod \mathfrak{p}^n\}$ of $\mathcal{O}_F^\times$. Let $U^{(0)} = \mathcal{O}_F^\times$.

3.1 The first glance at $F^\times$

First, we shall notice that there exists an isomorphism

$$\mathbb{F} = \mathcal{O}_F/\mathfrak{p} \to \mathfrak{p}^n/\mathfrak{p}^{n+1},$$

for all $n \geqslant 0$. Indeed, we may consider a surjective homomorphism

$$\mathcal{O}_F \to \mathfrak{p}^n/\mathfrak{p}^{n+1}$$

by $x \mapsto \pi^n x + \mathfrak{p}^{n+1}$ whose kernel is simply $\mathfrak{p}$. Consequently, the order of the group $\mathfrak{p}^n/\mathfrak{p}^{n+1}$ is q. By induction on n, we conclude that $|\mathcal{O}_F/\mathfrak{p}^n| = q^n$ once we notice that $\mathcal{O}_F/\mathfrak{p}^n \cong \dfrac{\mathcal{O}_F/\mathfrak{p}^{n+1}}{\mathfrak{p}^n/\mathfrak{p}^{n+1}}$.

Now, we turn to the map

$$\mathcal{O}_F^\times \to (\mathcal{O}_F/\mathfrak{p}^n)^\times,$$

by $x \mapsto x + \mathfrak{p}^n$, whose kernel is nothing but $U^{(n)}$. As a result, we obtain an isomorphism of multiplicative groups $\mathcal{O}_F^\times/U^{(n)} \cong (\mathcal{O}_F/\mathfrak{p}^n)^\times$ once we realize that the map above is surjective. In particular, $\mathcal{O}_F^\times/U^{(1)} \cong \mathbb{F}^\times$.

Proposition 3.1.1. *We have the following topological isomorphisms*

$$\mathcal{O}_F \to \varprojlim \mathcal{O}_F/\mathfrak{p}^n,$$

and

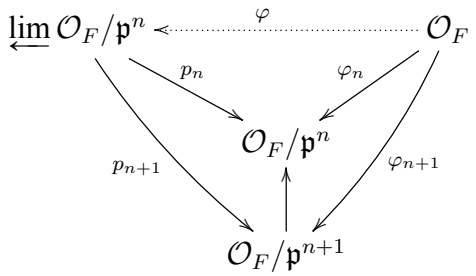
$$\mathcal{O}_F^\times \to \varprojlim \mathcal{O}_F^\times/U^{(n)},$$

as well as

$$U^{(1)} \to \varprojlim U^{(1)}/U^{(n)}.$$

It follows that the three groups $\mathcal{O}_F$, $\mathcal{O}_F^\times$ and $U^{(1)}$ are profinite, and in particular, compact.

Proof. Since $\mathfrak{p}^n = \{x \in \mathcal{O}_F : |x|_p \leqslant p^{-n}\}$ is a closed ball in $\mathcal{O}_F$, it is also a open ball by Lemma 2.2.16. So we know that each homomorphism $\varphi_n : \mathcal{O}_F \to \mathcal{O}_F/\mathfrak{p}^n$ is continuous by Lemma 2.2.13. Consider the following commutative diagram



we have $\varphi_n = p_n \circ \varphi$ for all $n \geqslant 0$. Thus φ is continuous as φ_n is continuous for each n. Now, apply Lemma 2.2.14, we conclude that im φ is dense in $\varprojlim \mathcal{O}_F/\mathfrak{p}^n$. Indeed, set $A = \varprojlim \mathcal{O}_F/\mathfrak{p}^n$, $B =$ im φ as Lemma 2.2.14, then we have $p_n(A) \subseteq \mathcal{O}_F/\mathfrak{p}^n = \varphi_n(\mathcal{O}_F) = p_n(\varphi(\mathcal{O}_F)) = p_n(B)$ for all n. It follows that $\overline{B} \supset A$, i.e. im φ is dense. Furthermore, im φ is compact because $\mathcal{O}_F$ is compact by Lemma 2.2.16 and φ is continuous. So im φ is closed as $\varprojlim \mathcal{O}_F/\mathfrak{p}^n$ is profintie and hence Hausdorff. So far, we conclude that im $\varphi = \varprojlim \mathcal{O}_F/\mathfrak{p}^n$ or φ is surjective. Noting that $\ker\varphi \subseteq \ker\varphi_n = \mathfrak{p}^n$ for each n, we have $\ker\varphi \subseteq \bigcap \mathfrak{p}^n = \{0\}$. The last equality holds because each element in $\bigcap \mathfrak{p}^n$ has infinite valuation. So, φ is bijective. As a consequence, φ is a homeomorphism since it is a continuous bijection from a compact space to a Hausdorff space. By the construction, we have $\left(\varprojlim \mathcal{O}_F/\mathfrak{p}^n\right)^\times \cong \varprojlim (\mathcal{O}_F/\mathfrak{p}^n)^\times$. So $\mathcal{O}_F \to \varprojlim \mathcal{O}_F^\times/U^{(n)}$ as we have shown that $\mathcal{O}_F^\times/U^{(n)} \cong (\mathcal{O}_F/\mathfrak{p}^n)^\times$. The third one is obtained by restriction. ∎

Since each $x \in F^\times$ can be expressed as $x = \pi^n u$ with $n \in \mathbb{Z}$ and $u \in \mathcal{O}_F^\times$ uniquely, we must have $F^\times = \langle\pi\rangle \times \mathcal{O}_F^\times$. For the same reason, each element in $U^{(n)}$ can be expressed as $1 + \pi^n u$ with $u \in \mathcal{O}_F$ uniquely. We may consider the map

$$U^{(n)} \to \mathbb{F} = \mathcal{O}_F/\mathfrak{p}$$

defined by $1 + \pi^n u \mapsto u + \mathfrak{p}$, whose kernel is nothing but $U^{(n+1)}$. As a result, we obtain an isomorphism $U^{(n)}/U^{(n+1)} \cong \mathbb{F}$ as the map above is clearly surjective.

Proposition 3.1.2. *We have a topological isomorphism*

$$F^\times \cong \mathbb{Z} \times \mathbb{Z}/(q-1)\mathbb{Z} \times U^{(1)}.$$

We see that $F^\times$ is locally compact as a topological group.

Proof. Consider the polynomial $f = X^{q-1} - 1 \in \mathcal{O}_F[X]$ and $\overline{f} \in \mathbb{F}[X]$. Since $\mathbb{F}^\times$ is a cyclic group of order $q-1$, we know that $\overline{f}$ splits into distinct linear factors in $\mathbb{F}[X]$. By Hensel's lemma, f splits into distinct linear factors in $\mathcal{O}_F[X]$. Thus, we may identify $\mu_{q-1}(F)$ with $\mathbb{F}^\times$ via an isomorphism $\mathbb{F}^\times \to \mu_{q-1}(F)$. Let $\psi : \mathcal{O}_F^\times \to \mu_{q-1}(F)$ be the map obtained by composing this isomorphism with the quotient map $\mathcal{O}_F \to \mathbb{F}^\times$. We conclude that $\mathcal{O}_F^\times \cong \mu_{q-1}(F) \times U^{(1)}$. Indeed, we have a bijection $\mu_{q-1}(F) \times U^{(1)} \to \mathcal{O}_F^\times$ defined by $(x,u) \mapsto xu$, whose inverse is $\mathcal{O}_F^\times \to \mu_{q-1}(F) \times U^{(1)}$ by $x \mapsto (\psi(x), x\psi(x)^{-1})$. It follows that $\mu_{q-1}(F) \times U^{(1)} \to \mathcal{O}_F^\times$ is a homeomorphism since it is a continuous bijection from a compact space to a Haursdorff space.

As a consequence, $F^\times = \langle \pi \rangle \times \mathcal{O}_F^\times \cong \langle \pi \rangle \times \mu_{q-1}(F) \times U^{(1)} \cong \mathbb{Z} \times \mathbb{Z}/(q-1)\mathbb{Z} \times U^{(1)}$. Moreover, this is a topological isomorphism if $\mathbb{Z}$ is endowed with the discrete topology. Indeed, we may consider the map $f : \mathbb{Z} \times \mu_{q-1}(F) \times U^{(1)} \to F^\times$ given by $(n,x,u) \mapsto \pi^n xu$, which is continuous with the continuous inverse $F^\times \to \mathbb{Z} \times \mathcal{O}_F^\times$ given by $x \mapsto (v(x), \pi^{-v(x)}x)$.

Since $U^{(1)}$ is profinite, $\mathbb{Z}$ and $\mathbb{Z}/(q-1)\mathbb{Z}$ is discrete, each open subset of $\mathbb{Z} \times \mathbb{Z}/(q-1)\mathbb{Z} \times U^{(1)}$ containing the identity $(0,0,1)$ must contain a open subgroup of the form $\{0\} \times \{0\} \times H$, with H open in $U^{(1)}$. Since $U^{(1)}$ is compact and every open subgroup of a topological group is closed, we have that H is compact. So This subgroup is compact and $F^\times$ is locally compact. ■

However, one should notice that $F^\times$ is not compact, since $F^\times$ can be expressed as a union of disjoint open subsets $F_n^\times = \{x \in F^\times : v(x) = n\}$. Also, $F^\times$ is not complete since $\pi^n \to 0$ as $n \to \infty$ but $0 \notin F^\times$.

3.2 Module structure

Now, it remains to describe the structure of $U^{(1)}$. Before we do this, we first review some basic facts about formal power series.

Suppose $f, g \in \mathbb{Q}[[X]]$, we may talk about the composition $f(g(X))$ if the constant term

of g is 0. In detail, if $f(X) = \sum a_n X^n$, we may define a family of power series

$$h_N = \sum_{n=0}^{N} a_n g(X)^n,$$

for each $N \geqslant 0$. One can easily verify that all of these h_N have the same k-th coefficient if $N > k$. Thus, we may define it to be the k-th coefficient of $f(g(X))$.

We now define the exponential and logarithm to be the formal power series

$$\exp(X) = \sum_{n \geqslant 0} \frac{X^n}{n!}$$

and

$$\log(1+X) = \sum_{n \geqslant 1} (-1)^{n-1} \frac{X^n}{n}$$

respectively. One may readily check that $\exp(\log(1+X)) = 1+X$ in $\mathbb{Q}[[X]]$ by using some basic facts in calculus. Moreover, we have

$$\log((1+X)(1+Y)) = \log(1+X) + \log(1+Y),$$

and

$$\exp(X+Y) = \exp(X)\exp(Y).$$

Proposition 3.2.1. *For each $x \in \mathfrak{p}$, the power series $\log(1+X)$ converges at $X = x$. We have a continuous homomorphism*

$$\log : U^{(1)} \to F.$$

Further, $\log(U^{(n)}) \subset \mathfrak{p}^n$.

For all $n > \frac{e}{p-1}$ and any $x \in \mathfrak{p}^n$, the power series $\exp(X)$ converges at $X = x$, to an element of $U^{(n)}$. There is a continuous map

$$\exp : \mathfrak{p}^n \to U^{(n)}.$$

Proof. See [4], chapter II, section 5, proposition 5.4 and 5.5. ∎

We now want to endow $U^{(n)}$ a $\mathbb{Z}_p$-module structure. We will do this with $U^{(1)}$ first. Let A be an abelian group, in which we write the operation multiplicatively. If there exists a positive integer N such that $a^N = 1$ for all $a \in A$, then we may define a^λ for all $\lambda \in \mathbb{Z}/N\mathbb{Z}$.

This makes A into a $\mathbb{Z}/N\mathbb{Z}$-module. Since we have shown that $U^{(n)}/U^{(n+1)} \cong \mathbb{F}$, the order of $U^{(n)}/U^{(n+1)}$ is thus q. By some simple induction on n, we have that $U^{(1)}/U^{(n+1)}$ has order q^n once we notice that $U^{(1)}/U^{(n)} \cong \dfrac{U^{(1)}/U^{(n+1)}}{U^{(n)}/U^{(n+1)}}$. Consequently, $U^{(1)}/U^{(n+1)}$ is a $\mathbb{Z}/q^n\mathbb{Z}$-module. Since $U^{(1)} = \varprojlim U^{(1)}/U^{(n+1)}$ by Proposition 3.1.1, and $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \varprojlim \mathbb{Z}/q^n\mathbb{Z}$, we may define $x^\lambda = (x_n^{\lambda_n})_{n\geqslant 1}$, where $x = (x_n)_{n\geqslant 1} \in U^{(1)}$ and $\lambda = (\lambda_n)_{n\geqslant 1} \in \mathbb{Z}_p$. So $U^{(1)}$ has a $\mathbb{Z}_p$-module structure and each subgroup $U^{(n)}$ is a $\mathbb{Z}_p$-submodule of $U^{(1)}$. Noting that $\left|U^{(1)}/U^{(n+1)}\right| = q^n$, we have $x^\lambda \in U^{(n+1)}$, which is an open subset, for any $x \in U^{(1)}$ and $\lambda \in q^n\mathbb{Z}_p$. So, $\lambda \mapsto x^\lambda$ is a continuous map for any fixed $x \in U^{(1)}$. It follows that the continuous map $\log : U^{(n)} \to \mathfrak{p}^n$ is $\mathbb{Z}_p$-linear as $\mathbb{Z}$ is dense in $\mathbb{Z}_p$.

By Proposition 3.2.1, we know that there exists a topological isomorphism $\mathfrak{p}^n \cong U^{(n)}$ as $\mathbb{Z}_p$-moduels for $n > \dfrac{e}{p-1}$. Further, for all n, $\mathcal{O}_F \to \mathfrak{p}^n$ by $x \to \pi^n x$ is a topological isomorphism of topological groups since multiplication is continuous. We must have a topological isomorphism $U^{(n)} \cong \mathcal{O}_F \cong \mathbb{Z}_p^d$, where $d = [F : \mathbb{Q}_p]$, as $\mathbb{Z}_p$-modules for all $n > \dfrac{e}{p-1}$ by Proposition 2.1.8.

Proposition 3.2.2. *The group $U^{(1)}$ is topologically isomorphic to $\mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}_p^d$ for some $a \geqslant 0$, where $d = [F : \mathbb{Q}_p]$.*

Proof. Since $U^{(1)}/U^{(n+1)}$ is of order q^n, it is torsion. As we mentioned above, $U^{(n+1)} \cong \mathbb{Z}_p^d$ for $n > \dfrac{e}{p-1}$, so $U^{(1)}$ is a finitely generated module over $\mathbb{Z}_p$, which is a PID. Thus, $U^{(1)} \cong \mathbb{Z}_p^d \times U_{tor}^{(1)}$, where $U_{tor}^{(1)}$ is the torsion in $U^{(1)}$. From the structure theorem of finitely generated modules over a PID, we know that $U_{tor}^{(1)}$ is finite. So the elements in $U_{tor}^{(1)}$ are roots of unity contained in $U^{(1)} \subset F^\times$. This implies that $U_{tor}^{(1)}$ is a finite cyclic group, whose order is a power of p as the order of $U^{(1)}/U^{(n+1)}$ is. Thus $U^{(1)}$ is topologically isomorphic to $\mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}_p^d$ for some $a \geqslant 0$. ∎

3.3 Multiplicative structure of $F^\times$ and some applications

According to what we have discussed above, we have the following theorem.

Theorem 3.3.1. *Suppose $F^\times$ is the topological group endowed with topology induced from the valuation on the p-adic field F. Then $F^\times$ is topologically isomorphic to*

$$\mathbb{Z} \times \mathbb{Z}/(q-1)\mathbb{Z} \times \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}_p^d,$$

where $d = [F : \mathbb{Q}_p]$, $q = |\mathbb{F}|$ and $a \geqslant 0$ is an integer.

Further, under this identification,

• *the map $F^\times \to \mathbb{Z}$ corresponding to the projection to the first factor is v, the normalized valuation;*

• *the subgroup $\{0\} \times \mathbb{Z}/(q-1)\mathbb{Z} \times \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}_p^d$ corresponds to $\mathcal{O}_F^\times$;*

• *the subgroup $\{0\} \times \{0\} \times \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}_p^d$ corresponds to $U^{(1)}$;*

• *the subgroup $\{0\} \times \mathbb{Z}/(q-1)\mathbb{Z} \times \mathbb{Z}/p^a\mathbb{Z} \times \{0\}$ corresponds to the roots of unity contained in $F^\times$.*

Proposition 3.3.2. *Suppose F is a p-adic field, then any subgroup of finite index in $F^\times$ is closed.*

Proof. Let H be a subgroup of $G = F^\times$ and suppose that $[G : H] = n$. Set $A = G^n$, then $A \subseteq H$. Indeed, take $x \in A$, then $x = g^n$ for some $g \in G$. So, $xH = g^nH = (gH)^n = 1$ since $|G/H| = n$. It follows that $x \in H$. We now claim that $[G : G^n] < +\infty$. By Theorem 3.3.1, we see that the subgroup $\{0\} \times \mathbb{Z}/(q-1)\mathbb{Z} \times \mathbb{Z}/p^a\mathbb{Z} \times \{0\}$ corresponds to the roots of unity contained in $F^\times$. We denote μ_F the group of all roots of unity contained in $F^\times$, then we have $G \cong \mathbb{Z} \times \mu_F \times \mathbb{Z}_p^d$. Write $n = p^k m$ with $(p, m) = 1$. Recall that an element of $\mathbb{Z}_p$ has an inverse if and only if it is not in $p\mathbb{Z}_p$, we see that $m\mathbb{Z}_p = \mathbb{Z}_p$. It follows that $n\mathbb{Z}_p = p^k\mathbb{Z}_p$. So, $[\mathbb{Z}_p^d : n\mathbb{Z}_p^d] = p^{kd}$. Note that the index of μ_F^n in μ_F is nothing but $|\mu_n(F)|$ and the index of $n\mathbb{Z}$ in $\mathbb{Z}$ is n. We see that $[G : G^n] = n \cdot |\mu_n(F)| \cdot p^{kd} < +\infty$. Again, by Theorem 3.3.1, we see that the map $x \mapsto x^n$ is closed since its restriction on each component, i.e. $\mathbb{Z}$, $\mathbb{Z}/(q-1)\mathbb{Z}$, $\mathbb{Z}/p^a\mathbb{Z}$ and $\mathbb{Z}_p$ is closed. Indeed, $\mathbb{Z}$, $\mathbb{Z}/(q-1)\mathbb{Z}$, $\mathbb{Z}/p^a\mathbb{Z}$ are discrete and $\mathbb{Z}_p$ is compact Hausdorff. Thus, A is a closed subgroup of G. Thus, H contains a closed subgroup of finite index, which implies that H is also closed. Indeed, A is a subgroup of finite index of H and it follows that H is a finite union of cosets of A. ■

4 The Brauer group of a p-adic field

4.1 The Hasse invariant

Lemma 4.1.1. *Suppose $F \subseteq \mathcal{Z}(K)$ and K is not commutative. Then there exists an unramified field extension E/F such that $F \subsetneq E \subseteq K$.*

Proof. Assume this lemma fails. Then for any $x \in K$, we consider the field $E = F(x)$. Its inertia subfield $E_0 = F$, so E/F is totally ramified. Hence, they have the same residue field. Thus, if $x \in \mathcal{O}_K$, there exists $a_0 \in \mathcal{O}_F$ such that $a_0 + \mathfrak{P} = x + \mathfrak{P}$, i.e. $x - a_0 \in \mathfrak{P}$. Apply this to the element $(x - a_0)\Pi^{-1} \in \mathcal{O}_K$, we may find $a_1 \in \mathcal{O}_F$ such that $(x - a_0)\Pi^{-1} - a_1 \in \mathfrak{P}$. Thus, $x - a_0 - a_1\Pi \in \mathfrak{P}^2$. Therefore, we may find $a_n \in \mathcal{O}_F$ such that $x - a_0 - a_1\Pi - a_2\Pi^2 - \cdots - a_n\Pi^n \in \mathfrak{P}^{n+1}$ for each $n \geqslant 1$, i.e.

$$x \equiv a_0 + a_1\Pi + a_2\Pi^2 + \cdots + a_n\Pi^n \mod \mathfrak{P}^{n+1}.$$

So we conclude that $F(\Pi)$ is dense in K and then K must be commutative as $F(\Pi)$ is, A contradiction. ■

Corollary 4.1.2. *Assume $\mathcal{Z}(K) = F$. There exists a maximal unramified extension field E of F contained in K. It follows that $[K] \in \mathrm{Br}(E/F)$.*

Proof. If K is commutative, we must have $K = F$ as $\mathcal{Z}(K) = F$ and we're done. Thus, we may assume that K is not commutative.

By induction on $n = [K : F]$. If $n = 1$, there nothing to prove. We assume the result holds for $[K : F] < n$. By Lemma 4.1.1, there exists a field $F \subsetneq E_0 \subset K$ such that E_0/F is unramified. Let $E_0' = \mathcal{Z}_K(E_0)$, then by Corollary 2.3.3, we have that E_0 is the center of E_0', i.e. $E_0 = \mathcal{Z}(E_0')$. Since $[E_0' : E_0] < n$, by our induction hypothesis, there exists a field E with $E_0 \subset E \subset E_0$ which is maximal and E/E_0 is unramified. So E/F is unramified. Again by Corollary 2.3.3, $[E_0' : E_0] = [E : E_0]^2$. Since $[K : F] = [E_0 : F][E_0' : F]$ by Theorem 2.3.2, we have $[E : F]^2 = [E : E_0]^2[E_0 : F]^2 = [E_0' : E_0][E_0 : F]^2 = [E_0' : F][E_0 : F] = [K : F]$. We conclude that E is maximal by Corollary 2.3.3 again.

$[K] \in \mathrm{Br}(E/F)$ simply follows from Proposition 2.3.4. ■

Corollary 4.1.3. *The group $\mathrm{Br}(F)$ is the union of the groups $\mathrm{Br}(E/F)$ where E runs through the fields $F \subset E \subset \overline{F}$, with E/F unramified. The cohomological Brauer group is the colimit of the groups $\mathrm{H}^2(\mathrm{Gal}(E/F), E^\times)$ for the same E.*

Lemma 4.1.4. *Let E/F be an unramified extension of p-adic fields, and let $\mathcal{O}_E$ and $\mathcal{O}_F$ be the valuation rings of E and F respectively. Then* $\mathrm{Tr}_{E/F}(\mathcal{O}_E) = \mathcal{O}_F$.

Proof. Recall that $\mathrm{Tr}_{E/F}(a) = \sum_{\sigma \in \mathrm{Gal}(E/F)} \sigma(a)$. By Corollary 2.1.6, we have that $v_E(\mathrm{Tr}_{E/F}(a)) \geqslant 0$ if $a \in \mathcal{O}_E$. Since $\mathrm{Tr}_{E/F}(a) \in F$, we know that $v_F(\mathrm{Tr}_{E/F}(a)) = v_E(\mathrm{Tr}_{E/F}(a)) \geqslant 0$. Thus, we must have $\mathrm{Tr}_{E/F}(\mathcal{O}_E) \subseteq \mathcal{O}_F$. This is an ideal of $\mathcal{O}_F$ as $\mathrm{Tr}_{E/F}$ is a $\mathcal{O}_F$-linear map. If $\mathrm{Tr}_{E/F}(\mathcal{O}_E) \neq \mathcal{O}_F$, then $\mathrm{Tr}_{E/F}(\mathcal{O}_E) \subseteq \mathfrak{p}$, where $\mathfrak{p}$ is the maximal ideal of the ring $\mathcal{O}_F$. Note that $\mathrm{Tr}_{\mathbb{E}/\mathbb{F}}(\overline{a}) = \sum_{\overline{\sigma} \in \mathrm{Gal}(\mathbb{E}/\mathbb{F})} \overline{\sigma}(\overline{a}) = \sum_{\sigma \in \mathrm{Gal}(E/F)} \overline{\sigma(a)} = \overline{\sum_{\sigma \in \mathrm{Gal}(E/F)} \sigma(a)} = \overline{\mathrm{Tr}_{E/F}(a)} = 0$ for $\overline{a} \in \mathbb{E}$. Thus, $\mathrm{Tr}_{\mathbb{E}/\mathbb{F}} = 0$, which implies that $\{\sigma\}_{\sigma \in \mathrm{Gal}(\mathbb{E}/\mathbb{F})}$ is linearly dependent. This is a contradiction by Dedekind's lemma. ∎

Lemma 4.1.5. *Let E/F be an unramified extension of p-adic fields, and let $\mathcal{O}_E$ and $\mathcal{O}_F$ denote the respective valuation rings. Suppose $[E : F] = n$. Then for any $f \in \mathcal{O}_F^\times$, there exists $z \in E$ such that* $\mathrm{N}_{E/F}(z) = f$.

Proof. Let $\mathfrak{p} = (\pi)$ and $\mathfrak{P} = \mathfrak{p}\mathcal{O}_E$ be the maximal ideals of $\mathcal{O}_F$ and $\mathcal{O}_E$ respectively.

We can find a sequence $(z_k)_{k \geqslant 1}$ of elements of E with

$$\mathrm{N}_{E/F}(z_k) \equiv f \mod \mathfrak{p}^k \qquad \text{and} \qquad z_k \equiv z_{k-1} \mod \mathfrak{P}^{k-1}$$

by induction.

For the case $k = 1$. Let $|\mathbb{F}| = q$ and then $|\mathbb{E}| = q^n$. So for each $x \in \mathbb{E}^\times$, we have $\mathrm{N}_{\mathbb{E}/\mathbb{F}}(x) = x x^q x^{q^2} \cdots x^{q^{n-1}} = x^{\frac{q^n-1}{q-1}}$ as $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ is generated by the map $x \mapsto x^q$. Since $\mathbb{E}^\times$ is a cyclic group of order $q^n - 1$ and $\mathbb{F}^\times$ is a cyclic group of order $q - 1$, we know that $\mathrm{N}_{\mathbb{E}/\mathbb{F}} : \mathbb{E} \to \mathbb{F}$ is surjective. So there exists $z_1 \in E$ such that $\mathrm{N}_{\mathbb{E}/\mathbb{F}}(\overline{z_1}) = \overline{f}$. However, $\mathrm{N}_{\mathbb{E}/\mathbb{F}}(\overline{z_1}) = \prod_{\overline{\sigma} \in \mathrm{Gal}(\mathbb{E}/\mathbb{F})} \overline{\sigma}(\overline{z_1}) = \prod_{\sigma \in \mathrm{Gal}(E/F)} \overline{\sigma(z_1)} = \overline{\prod_{\sigma \in \mathrm{Gal}(E/F)} \sigma(z_1)} = \overline{\mathrm{N}_{E/F}(z_1)}$, we conclude that $\mathrm{N}_{E/F}(z_1) \equiv f \mod \mathfrak{p}$. Now, suppose we have $\mathrm{N}_{E/F}(z_{k-1}) \equiv f \mod \mathfrak{p}^{k-1}$ and $z_{k-1} \equiv z_{k-2} \mod \mathfrak{P}^{k-2}$, then $f\,\mathrm{N}_{E/F}(z_{k-1})^{-1} = 1 + x\pi^{k-1}$ with $x \in \mathcal{O}_F$. By Lemma 4.1.4, there exists $y \in \mathcal{O}_E$ such that $\mathrm{Tr}_{E/F}(y) = x$. Let $z_k = z_{k-1}(1 + y\pi^{k-1})$. So $\mathrm{N}_{E/F}(1 + y\pi^{k-1}) \equiv 1 + \mathrm{Tr}_{E/F}(y\pi^{k-1}) = 1 + x\pi^{k-1} \mod \mathfrak{p}^k$ if $k \geqslant 2$. Hence, we have $\mathrm{N}_{E/F}(z_k) \equiv f \mod \mathfrak{p}^k$. Since $z_k \equiv z_{k-1} \mod \mathfrak{P}^{k-1}$, $(z_k)_{k \geqslant 1}$ is a Cauchy sequence, which converges to some $z \in E$ as E is complete, i.e. there exists $z \in E$ such that $z \equiv z_k \mod \mathfrak{P}^k$. Then $\mathrm{N}_{E/F}(z) \equiv \mathrm{N}_{E/F}(z_k) \equiv f \mod \mathfrak{p}^k$ for all k. Thus, $\mathrm{N}_{E/F}(z) = f$ as desired. ∎

Proposition 4.1.6. *Let E_n be the unramified extension of F with degree $[E_n : F] = n$. Then*

$$\mathrm{N}_{E_n/F}(E_n^\times) = \{f \in F^\times : n \text{ divides } v(f)\}.$$

Proof. Let v be the normalized valuation on F and w the valuation on E_n extending v. Then we must have $v(F^\times) = \mathbb{Z}$ and $v(\mathrm{N}_{E_n/F}(x)) = nw(x)$ by Theorem 2.1.5. Since E_n/F is unramified, $w(E_n^\times) = ev(F^\times) = \mathbb{Z}$. So $v(\mathrm{N}_{E_n/F}(E_n^\times)) = n\mathbb{Z}$. This implies that

$$\mathrm{N}_{E_n/F}(E_n^\times) \subseteq \{f \in F^\times : n \text{ divides } v(f)\}.$$

Conversely, if n divides $v(f)$, then $v(f) \in n\mathbb{Z} = v(\mathrm{N}_{E_n/F}(E_n^\times))$. Thus there exists $g \in \mathrm{N}_{E_n/F}(E_n^\times)$ such that $v(f) = v(g)$, i.e. $v(f/g) = 0$. Thus there exists some $z \in E_n^\times$ such that $\mathrm{N}_{E_n/F}(z) = f/g$ by Lemma 4.1.5. So $f = g\,\mathrm{N}_{E_n/F}(z) \in \mathrm{N}_{E_n/F}(E_n^\times)$. Hence, we have

$$\mathrm{N}_{E_n/F}(E_n^\times) = \{f \in F^\times : n \text{ divides } v(f)\}.$$

■

Corollary 4.1.7. *The group* $\mathrm{Br}(E_n/F)$ *is cyclic of order* n.

Proof. Consider the map $\varphi : F^\times \to \mathbb{Z}/n\mathbb{Z}$ obtained by composing $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ with $v : F^\times \to \mathbb{Z}$. Its kernel is simply $\{f \in F^\times : n \text{ divides } v(f)\} = \mathrm{N}_{E_n/F}(E_n^\times)$. So

$$\mathrm{Br}(E_n/F) \cong F^\times/\,\mathrm{N}_{E_n/F}(E_n^\times) \cong \mathbb{Z}/n\mathbb{Z}.$$

■

Lemma 4.1.8. *Let* F *ba a* p*-adic field.*

(1) *Let* K *be a skewfield with* $\mathcal{Z}(K) = F$. *Then the degree of* K *is the smallest integer* n *such that* $[K] \in \mathrm{Br}(E_n/F)$. *If* $[K] \in \mathrm{Br}(E_m/F)$, *we have* $n|m$.

(2) *The number of skewfields* K, *up to isomorphism, with* $\mathcal{Z}(K) = F$ *of degree dividing* n *is* n.

(3) *The number of skewfields* K, *up to isomorphism, with* $\mathcal{Z}(K) = F$ *of degree* n *is* $\varphi(n)$.

Proof. (1) Let n be the degree of K, consider $F \subset E_n \subset K$, we must have that $[E_n : F] = n$. By Corollay 2.3.3 and Proposition 2.3.4, we know that E_n is a splitting field for K. If $[K] \in \mathrm{Br}(E_m/F)$, then E_m is a splitting field for K. By Proposition 2.3.5, we conclude that $n|m$. Thus, the degree of K is the smallest integer n such that $[K] \in \mathrm{Br}(E_n/F)$.

(2) Let K be a skew field with center F and degree m. If $[K] \in \mathrm{Br}(E_n/F)$, then m must divide n by (1). If $m|n$, we must have $[K] \in \mathrm{Br}(E_m/F) \subseteq \mathrm{Br}(E_n/F)$. The number of skewfields K, up to isomorphism, with $\mathcal{Z}(K) = F$ of degree dividing n is $|\,\mathrm{Br}(E_n/F)| = n$.

(3) Let K be a skew field with center F and degree n. Then $[K]$ does not belong to any proper subgroup of $\mathrm{Br}(E_n/F)$ by (1). Thus, $[K]$ is a generator of $\mathrm{Br}(E_n/F)$. So the number of such K is precisely $\varphi(n)$. ■

Suppose K is a skewfield with center F. Then there exists a field E with $F \subset E \subset K$ which is maximal and E/F unramified. Let $\mathfrak{P}$ be the maxiamal ideal of E. Let σ be the Frobenius element of the group $\mathrm{Gal}(E/F)$, i.e. $\sigma(x) \equiv x^q \mod \mathfrak{P}$ for all $x \in \mathcal{O}_E$, where q is the size of the residue field of E. By Skolem-Noether theorem, there exists $a \in K$ such that $axa^{-1} = \sigma(x)$ for $x \in E$. Finally, recall that there is a unique extension w to K of the valuation v defined on F. The number $w(a)$ is an element of $\mathbb{Q}$. We let $\mathrm{Inv}(K, E, a)$ denote the class of $w(a)$ in $\mathbb{Q}/\mathbb{Z}$.

Lemma 4.1.9. *The element* $\mathrm{Inv}(K, E, a)$ *only depends on* K *up to isomorphism of* F*-algebras. It gives a map*

$$\mathrm{Inv} : \mathrm{Br}(F) \to \mathbb{Q}/\mathbb{Z}.$$

Proof. We first show that $\mathrm{Inv}(K, E, a)$ does not depend on a. Let b be another element such that $\sigma(x) = bxb^{-1}$ for all $x \in E$. Then $a^{-1}b \in \mathcal{Z}_K(E)^\times = E^\times$ by Corollary 2.3.3. So $b = ea$ for some $e \in E^\times$. Since E/F is unramified, $w(E^\times) = v(F^\times) = \mathbb{Z}$. So $w(ea) = w(e) + w(a) \equiv w(a) \mod \mathbb{Z}$.

Let $\psi : K \to L$ be an isomorphism of F-algebras. By Theorem 2.1.5, we have $w_K(a) = w_L(\psi(a))$ for all $a \in K$. Then $\mathcal{O}_{\psi(E)}$ is the valuation ring of $\psi(E)$ with the maximal ideal $\psi(\mathfrak{P})$. Since $axa^{-1} \equiv x^q \mod \mathfrak{P}$, we must have $\psi(a)\psi(x)\psi(a)^{-1} \equiv \psi(x)^q \mod \psi(\mathfrak{P})$. So $\psi(a)$ defines the Frobenius element of the group $\mathrm{Gal}(\psi(E)/F)$. Thus, $\mathrm{Inv}(L, \psi(E), \psi(a))$ is well-defined and $\mathrm{Inv}(L, \psi(E), \psi(a)) = \mathrm{Inv}(K, E, a)$.

Suppose that E' is another field with $F \subset E' \subset K$ which is maximal and E'/F unramified. Then we have $[E' : F] = [E : F]$by Corollary 2.3.3. By Theorem 2.2.4, we know that $E' \cong E$. So there exists an inner automorphism ψ of K with $\psi(E) = E'$ by Skolem-Noether theorem. By the discussion above, we must have $\mathrm{Inv}(K, E, a) = \mathrm{Inv}(\psi(K), \psi(E), \psi(a)) = \mathrm{Inv}(K, E', \psi(a))$.

Thus, $\mathrm{Inv}(K, E, a)$ only depends on $[K]$. This gives a well-defiend map

$$\mathrm{Inv} : \mathrm{Br}(F) \to \mathbb{Q}/\mathbb{Z}$$

by $[K] \mapsto \mathrm{Inv}(K, E, a)$. ■

Definition 4.1.10. *The element* $\mathrm{Inv}(K)$ *in* $\mathbb{Q}/\mathbb{Z}$ *is called the* ***Hasse invariant*** *of a skew field* K.

4.2 The structure of $\mathrm{Br}(F)$

Lemma 4.2.1. *The invariant*

$$\mathrm{Inv} : \mathrm{Br}(F) \to \mathbb{Q}/\mathbb{Z}$$

induces an isomorphism

$$\mathrm{Inv}(n) : \mathrm{Br}(E_n/F) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

Proof. Let $n \geqslant 1$ and K a skewfield with $[K] \in \mathrm{Br}(E_n/F)$. Suppose $[K] \notin \mathrm{Br}(E_d/F)$ for all proper divisor d of n. By Lemma 4.1.8(1), we have $[K : F] = n^2$. We may choose E such that $F \subset E \subset K$ with E/F unramified and E is maximal in K. Then $[E : F] = n$ by Corollary 2.3.3. Since $K \cong A_c$ for some $c \in \mathscr{Z}^2(\mathrm{Gal}(E/F), E^\times)$, where A_c is the crossed product algebra associated to c. Clearly we have $E \cong E_n$ by Theorem 2.2.4. By Lemma 4.1.9, we know that $\mathrm{Inv}(K)$ only depends on $[K]$, thus we may assume that $K = A_c$ and $E = E_n$.

Let $e_1, e_2, \cdots, e_n$ be a basis of E_n over F and assume that $\mathrm{Gal}(E_n/F) = \langle\rho\rangle$, where ρ is the Frobenius element. Then by the construction of A_c, we know that $\{e_i a_{\rho^j}\}_{i,j}$ is a basis of K over F. So $e_i a_{\rho^j} a_\rho = c(\rho^j, \rho) e_i a_{\rho^{j+1}}$. Thus, we conclude that $\mathrm{N}_{K/F}(a_\rho) = (\pm 1)\left(\prod_{0\leqslant i<n} c(\rho^i, \rho)\right)^n$.

Define

$$\varphi_\rho : \mathscr{Z}^2(\mathrm{Gal}(E_n/F), E_n^\times) \to F^\times$$

by $c \mapsto \prod_{0\leqslant i<n} c(\rho^i, \rho)$. Then $\mathrm{N}_{K/F}(a_\rho) = \pm\varphi_\rho(c)^n$. So we conclude that $w(a_\rho) = \frac{1}{n} v(\varphi_\rho(c))$ by Theorem 2.1.5. By Proposition 2.3.6, we know that φ_ρ induces an isomorphism

$$\widetilde{\varphi_\rho} : \mathrm{H}^2(\mathrm{Gal}(E_n/F), E_n^\times) \to F^\times / \mathrm{N}_{E_n/F}(E_n^\times).$$

By Proposition 4.1.6, $\frac{1}{n}v$ induces an isomorphism $F^\times/\mathrm{N}_{E_n/F}(E_n^\times) \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z}$. Since $\gamma_n : \mathrm{Br}(E_n/F) \to \mathrm{H}^2(\mathrm{Gal}(E_n/F), E_n^\times)$ given by $[A_c] \mapsto c$ is an isomorphism by Proposition 2.3.7. We know that $I_n := \frac{1}{n}v \circ \widetilde{\varphi_\rho} \circ \gamma_n$ is an isomorphism between $\mathrm{Br}(E_n/F)$ and $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$. Since

$$\mathrm{Inv}(K) = w(a_\rho) \mod \mathbb{Z} = \frac{1}{n} v(\varphi_\rho(c)) \mod \mathbb{Z} = \frac{1}{n} v(\widetilde{\varphi_\rho}(\gamma_n([A_c]))) \mod \mathbb{Z} = I_n([K]),$$

it follows that

$$\text{Inv}(n) : \text{Br}(E_n/F) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}$$

is an isomorphism induced by $\text{Inv} : \text{Br}(F) \to \mathbb{Q}/\mathbb{Z}$.

Now, consider the following commutative diagram

$$\begin{array}{ccccccc}
\text{Br}(E_n/F) & \xrightarrow{\gamma_n} & \text{H}^2(\text{Gal}(E_n/F), E_n^\times) & \xrightarrow{\varphi_\rho} & F^\times/\,\text{N}_{E_n/F}(E_n^\times) & \xrightarrow{\frac{1}{n}v} & \frac{1}{n}\mathbb{Z}/\mathbb{Z} \\
\downarrow{\scriptstyle \subset} & & \downarrow{\scriptstyle \inf} & & \downarrow{\scriptstyle f\mapsto f^{m/n}} & & \downarrow{\scriptstyle \subset} \\
\text{Br}(E_m/F) & \xrightarrow{\gamma_m} & \text{H}^2(\text{Gal}(E_m/F), E_m^\times) & \xrightarrow{\varphi_\rho} & F^\times/\,\text{N}_{E_m/F}(E_m^\times) & \xrightarrow{\frac{1}{m}v} & \frac{1}{m}\mathbb{Z}/\mathbb{Z}
\end{array},$$

where $n|m$. We conclude that for any m, $I_m([K]) = I_n([K]) = \text{Inv}(K)$. This implies that for each n, we must have

$$\text{Inv}(n) : \text{Br}(E_n/F) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}$$

is an isomorphism induced by $\text{Inv} : \text{Br}(F) \to \mathbb{Q}/\mathbb{Z}$. ■

Theorem 4.2.2. *The invariant*

$$\text{Inv} : \text{Br}(F) \to \mathbb{Q}/\mathbb{Z}$$

is an isomorphism of groups.

Proof. Since $\mathbb{Q}/\mathbb{Z} = \bigcup_n \frac{1}{n}\mathbb{Z}/\mathbb{Z}$, we know that the map $\text{Inv} : \text{Br}(F) \to \mathbb{Q}/\mathbb{Z}$ is surjective by Lemma 4.2.1. Inv is clearly injective as $\text{Inv}(n)$ is injective for each n. Thus, the invariant

$$\text{Inv} : \text{Br}(F) \to \mathbb{Q}/\mathbb{Z}$$

is an isomorphism of groups. ■

We now state a theorem about naturality without proof. One can consult [1] for details.

Theorem 4.2.3. *Suppose K/F is an extension of p-adic fields and $[K : F] = n < \infty$. Then the following diagram commutes*

$$\begin{array}{ccc}
\text{Br}(F) & \xrightarrow{\text{Inv}} & \mathbb{Q}/\mathbb{Z} \\
\downarrow & & \downarrow{\scriptstyle x\mapsto nx} \\
\text{Br}(K) & \xrightarrow{\text{Inv}} & \mathbb{Q}/\mathbb{Z}
\end{array}$$

Proof. See [1], Chapter 8, Theorem 8.10. ■

Corollary 4.2.4. *In the notation above,* $\mathrm{Br}(K/F)$ *is cyclic of order* n*.*

Proof. By definition, the relative Brauer group $\mathrm{Br}(K/F)$ is the kernel of $\mathrm{Br}(F) \to \mathrm{Br}(K)$, which can be identified with the kernel of $\mathbb{Q}/\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ given by $x \mapsto nx$ according to Theorem 4.2.3. Thus, $\mathrm{Br}(K/F) = \frac{1}{n}\mathbb{Z}/\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$. ■

5 Fundamental theorem of local class field theory

5.1 Reciprocity isomorphisms

In this section, we will prove the theorem of reciprocity isomorphisms based on an powerful result of group cohomology, known as Tate's theorem. So, we assume that the readers are familiar with homological algebra.

Definition 5.1.1. *Suppose G is a group and M is a G-module, we define the **Tate cohomology groups** of G with coefficients in M to be*

$$\widehat{\mathrm{H}^n} = \begin{cases} \mathrm{H}^n(G, M), & n \geqslant 1, \\ M^G/\mathrm{N}(M), & n = 0, \\ {}_N M/M', & n = -1, \\ \mathrm{H}_{-(n+1)}(G, M), & n \leqslant -2, \end{cases}$$

where $\mathrm{N}(M) = \{\sum_{\sigma\in G} \sigma \cdot m : m \in M\}$, $M^G = \{m \in M : \sigma \cdot m = m, \forall \sigma \in G\}$ and $M' = \{m - \sigma \cdot m : m \in M, \sigma \in G\}$.

Theorem 5.1.2 (Tate). *Suppose G is a finite group and A is a G-module. If $\mathrm{H}^2(H, A)$ is cyclic of order $|H|$ for every subgroup $H \leqslant G$ and $\mathrm{H}^1(H, A) = 0$, then for any $n \in \mathbb{Z}$ and any subgroup $H \leqslant G$, we have an isomorphism $\psi_{H,n} : \widehat{\mathrm{H}}^{n-2}(H, \mathbb{Z}) \to \widehat{\mathrm{H}}^n(H, A)$. Moreover, we have a commutative diagram*

$$\begin{array}{ccc} \widehat{\mathrm{H}}^{n-2}(H', \mathbb{Z}) & \xrightarrow{\psi_{H',n}} & \widehat{\mathrm{H}}^n(H', A) \\ \Big\downarrow{\scriptstyle \mathrm{Cor}} & & \Big\downarrow{\scriptstyle \mathrm{Cor}} \\ \widehat{\mathrm{H}}^{n-2}(H, \mathbb{Z}) & \xrightarrow{\psi_{H,n}} & \widehat{\mathrm{H}}^n(H, A), \end{array}$$

where Cor *is the corestriction map induced by the inclusion $H' \hookrightarrow H$.*

Proof. See [1], Chapter 13, Theorem 13.11. ■

Theorem 5.1.3. *Suppose K/F is a finite Galois extension of p-adic fields. Then we have an isomorphism of abelian groups*

$$\mathrm{Gal}(K/F)^{\mathrm{ab}} \cong F^\times/\mathrm{N}_{K/F}(K^\times).$$

In particular, if K/F is an abelian extension, we must have $\mathrm{Gal}(K/F) \cong F^\times/\mathrm{N}_K$*, and the index of* N_K *in* $F^\times$ *is* $[K:F]$

Proof. This theorem simply follows from Tate's theorem. Indeed, we set $G = \mathrm{Gal}(K/F)$. Then any subgroup of G is of the form $\mathrm{Gal}(K/L)$, and we have $\mathrm{H}^1(\mathrm{Gal}(K/L), K^\times) = 0$ by Hilbert 90. We have already known that $\mathrm{H}^2(\mathrm{Gal}(K/L), K^\times) \cong \mathrm{Br}(K/L) \cong \mathbb{Z}/n\mathbb{Z}$, where $n = [K:L] = |\mathrm{Gal}(K/L)|$. So by Tate's theorem, $\widehat{\mathrm{H}}^{n-2}(H, \mathbb{Z}) \cong \widehat{\mathrm{H}}^{n}(H, K^\times)$ for any subgroup H of G and any $n \in \mathbb{Z}$. Take $H = G$ and $n = 0$, we have $\widehat{\mathrm{H}}^{-2}(\mathrm{Gal}(K/F), \mathbb{Z}) \cong \widehat{\mathrm{H}}^{0}(\mathrm{Gal}(K/F), K^\times)$. By now, by definition, we have

$$\widehat{\mathrm{H}}^{0}(\mathrm{Gal}(K/F), K^\times) = F^\times/\mathrm{N}_{K/F}(K^\times)$$

and

$$\widehat{\mathrm{H}}^{-2}(\mathrm{Gal}(K/F), \mathbb{Z}) = \mathrm{H}_1(\mathrm{Gal}(K/F), \mathbb{Z}) \cong \mathrm{Gal}(K/F)^{\mathrm{ab}}.$$

It follows that

$$\mathrm{Gal}(K/F)^{\mathrm{ab}} \cong F^\times/\mathrm{N}_{K/F}(K^\times).$$

■

Similarly, we have $\mathrm{Gal}(K/L)^{\mathrm{ab}} \cong L^\times/\mathrm{N}_{K/L}(K^\times)$ for any intermedia fields L. Consider the composition maps $L^\times \to L^\times/\mathrm{N}_{K/L}(K^\times) \to \mathrm{Gal}(K/L)^{\mathrm{ab}}$, we may use $x \mapsto (x, K/L)$ to denote these map for convenience.

Definition 5.1.4. *The map $x \mapsto (x, K/L)$ defined above via composition is called* ***local norm residue map*** *and the element $(x, K/L)$ is called* ***Artin symbol*** *or* ***local norm residue symbol*** *of x.*

Lemma 5.1.5. *Let $F \subset L \subset K$ such that K/F is finite and Galois. Then we have a commutative diagram*

$$\begin{array}{ccc} L^\times & \xrightarrow{x\mapsto(x,K/L)} & \mathrm{Gal}(K/L)^{\mathrm{ab}} \\ \Big\downarrow{\scriptstyle \mathrm{N}_{L/F}} & & \Big\downarrow{\scriptstyle i^{\mathrm{ab}}} \\ F^\times & \xrightarrow{x\mapsto(x,K/F)} & \mathrm{Gal}(K/F)^{\mathrm{ab}}, \end{array}$$

where i^{ab} is induced by the inclusion map $i : \mathrm{Gal}(K/L) \hookrightarrow \mathrm{Gal}(K/F)$.

Proof. This lemma simply follows from Tate's theorem and the following commuatative diagram

$$\begin{array}{ccc} L^\times & \xrightarrow{x\mapsto\overline{x}} & L^\times/\,\mathrm{N}_{K/L}(K^\times) \\ \Big\downarrow{\scriptstyle \mathrm{N}_{L/F}} & & \Big\downarrow \\ F^\times & \xrightarrow{x\mapsto\overline{x}} & F^\times/\,\mathrm{N}_{K/F}(K^\times). \end{array}$$

■

Lemma 5.1.6. *Let $F \subset L \subset K$ such that K/F, L/F are Galois and K/F is finite. Consider the following diagram*

$$\begin{array}{ccc} F^\times & \xrightarrow{f_K : x\mapsto (x,K/F)} & \mathrm{Gal}(K/F)^{\mathrm{ab}} \\ \| & & \Big\downarrow{\scriptstyle r^{\mathrm{ab}}} \\ F^\times & \xrightarrow{f_L : x\mapsto (x,L/F)} & \mathrm{Gal}(L/F)^{\mathrm{ab}}, \end{array}$$

where r^{ab} is induced by the restriction map $r : \mathrm{Gal}(K/F) \to \mathrm{Gal}(L/F)$. Then $\ker(r^{\mathrm{ab}} \circ f_K) = \ker(f_L)$.

Proof. By the definition, we know that both f_K and f_L are surjective. Moreover $\ker(f_K) = N_{K/F}(K^\times)$ and $\ker(f_L) = N_{L/F}(L^\times)$. So, we see that $\ker(f_L) \subseteq \ker(f_K) \subseteq \ker(r^{\mathrm{ab}} \circ f_K)$. By counting the indices, we have $|\ker(f_L)| = |\ker(r^{\mathrm{ab}} \circ f_K)|$. So we conclude that $\ker(f_L) = \ker(r^{\mathrm{ab}} \circ f_K)$ as desired. ■

Definition 5.1.7. *Suppose that F is a p-adic field. A subgroup of the form $N_K = \mathrm{N}_{K/F}(K^\times)$ for some finite Galois extension K/F is called a* ***norm subgroup*** *of $F^\times$.*

Lemma 5.1.8. *Suppose K/F is finite and Galois. Let K^{ab}/F be the largest abelian extension contained in K. Then $N_K = N_{K^{\mathrm{ab}}}$.*

Proof. First note that $\mathrm{Gal}(K^{\mathrm{ab}}/F) = \mathrm{Gal}(K/F)^{\mathrm{ab}}$ by definition. Indeed, set $G = \mathrm{Gal}(K/F)$. Since $\mathrm{Gal}(K^{\mathrm{ab}}/F) \cong \mathrm{Gal}(K/F)/\,\mathrm{Gal}(K/K^{\mathrm{ab}})$ is abelian, we know that $\mathrm{Gal}(K/K^{\mathrm{ab}}) \supseteq G'$. By Galois theory, $G' = \mathrm{Gal}(K/E)$ for some extension E/F, so $K^{\mathrm{ab}} \subseteq E$. Then $\mathrm{Gal}(E/F) \cong G/G' = G^{\mathrm{ab}}$ is abelian, which tells us that E/F is abelian. However, by the definition of K^{ab}, we know that $K^{\mathrm{ab}} = E$. In Lemma 5.1.6, if we take $L = K^{\mathrm{ab}}$, we then have $N_{K^{\mathrm{ab}}} = \ker f_{K^{\mathrm{ab}}} = \ker(r^{\mathrm{ab}} \circ f_K)$. The above argument tells us r^{ab} is an isomorphism, which implies that $N_k = N_{K^{\mathrm{ab}}}$. ■

Lemma 5.1.9. *Suppose K_1 and K_2 are finite abelian extensions of F such that $K_i \subseteq \overline{F}$ for $i = 1, 2$. Then, we have $N_{K_1K_2} = N_{K_1} \cap N_{K_2}$.*

Proof. By the property of norm map, we see that

$$N_{K_1K_2} = \mathrm{N}_{K_1K_2/F}((K_1K_2)^\times) = \mathrm{N}_{K_1/F} \circ \mathrm{N}_{K_1K_2/K_1}((K_1K_2)^\times) \subseteq \mathrm{N}_{K_1/F}(K_1^\times) = N_{K_1}.$$

So $N_{K_1K_2} \subseteq N_{K_1} \cap N_{K_2}$ is rather trivial. It remains to prove $N_{K_1K_2} \supseteq N_{K_1} \cap N_{K_2}$. Take $x \in N_{K_1} \cap N_{K_2}$. Let $K = K_1K_2$ and $L = K_i$, $i = 1, 2$. By Lemma 5.1.6 and the fact that K_1K_2/F, K_i/F are abelian, we know that $r((x, K_1K_2/F)) = 0$, where $r : \mathrm{Gal}(K_1K_2/F) \to \mathrm{Gal}(K_i/F)$ is the restriction map. Thus, $(x, K_1K_2/F) = 0$ because an element of $\mathrm{Gal}(K_1K_2/F)$ is completely determined by the action on K_1 and K_2. Recall the definition of Artin symbol, we conclude that $x \in N_{K_1K_2}$. It follows that $N_{K_1} \cap N_{K_2} \subseteq N_{K_1K_2}$. ■

Proposition 5.1.10. *Suppose F is a p-adic field. Let*

$$\mathcal{A} = \left\{ K : F \subseteq K \subseteq \overline{F} \text{ such that } K/F \text{ is finite abelian } \right\}$$

and

$$\mathcal{N} = \left\{ \text{ norm subgroups of } F^\times \right\}.$$

Then the map $K \mapsto N_K$ is a one-to-one, order-reversing correspondence between $\mathcal{A}$ and $\mathcal{N}$.

Proof. We here use $f : \mathcal{A} \to \mathcal{N}$ to denote the given map, i.e. $f(K) = N_K$. By Lemma 5.1.8, we see that f is surjective. Now, we prove that $K \subset L$ if and only if $N_L \subset N_K$. If $K \subset L$, then $N_L = \mathrm{N}_{L/F}(L^\times) = \mathrm{N}_{K/F} \circ \mathrm{N}_{L/K}(L^\times) \subseteq \mathrm{N}_{K/F}(K^\times) = N_K$. Conversely, suppose $N_L \subset N_K$. We have $N_{KL} = N_K \cap N_L = N_L$ by Lemma 5.1.9. Consequently, $x \mapsto (x, KL/F)$ and $x \mapsto (x, L/F)$ have the same kernel. Now, by Lemma 5.1.6, we conclude that the restriction map $r : \mathrm{Gal}(KL/F) \to \mathrm{Gal}(L/F)$ is injective. Thus, $\ker r = \mathrm{Gal}(KL/L) = 0$. So $KL = L$ and it follows that $K \subset L$. As a result, $N_K = N_L$ implies that $K = L$, i.e. f is injective. ■

Corollary 5.1.11. *Let N be a subgroup of $F^\times$. If N contains a norm subgroup N_L, then N is also a norm subgroup.*

Proof. Without lose of generality, we may assume that L/F is finite abelian, by Proposition 5.1.10. Then we have $F^\times/N_L \cong \mathrm{Gal}(L/F)^{\mathrm{ab}} = \mathrm{Gal}(L/F)$ by Theorem 5.1.3. Since a group containing N_L is $1-1$ corresponds to a subgroup of $F^\times/N_L$, we may identify N with a subgroup of $\mathrm{Gal}(L/F)$. By the fundamental theorem of Galois theory, N corresponds to a finite abelian extension K/F with $K \subset L$. As a result, $N = N_K$. ■

5.2 The Existence theorem

We will use some simple notions of Hilbert symbol in this section, so we shall spend some time to review the basic definition and some properties of it before we step into our main theorem.

Given $\chi \in \mathrm{H}^1(F, \mathbb{Q}/\mathbb{Z})$, i.e. χ is a continuous homomorphism $\mathrm{Gal}(\overline{F}/F) \to \mathbb{Q}/\mathbb{Z}$. We have already known that the kernel of χ is open, so it is closed. Thus, $\ker \chi = \mathrm{Gal}(\overline{F}/E)$ for some finite Galois extension E/F by the fundamental theorem of Galois theory. Now, by first isomorphism theorem, $|\chi(G)| = |\mathrm{Gal}(E/F)| = [E : F]$ is of finite order, say $n = [E : F]$. Then, $\chi(G) = \frac{1}{n}\mathbb{Z}/\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$. Let σ be a generator of $\mathrm{Gal}(E/F)$, i.e. σ is an element such that $\chi(\sigma) = \frac{1}{n}$. By some basic facts of homological algebra, we have an isomorphism

$$\varphi_\sigma : \mathrm{H}^2(\mathrm{Gal}(E/F), E^\times) \to F^\times / \mathrm{N}_{E/F}(E^\times).$$

We denote the element of $\mathrm{H}^2(\mathrm{Gal}(E/F), E^\times)$ which maps to $[b] \in F^\times / \mathrm{N}_{E/F}(E^\times)$ via φ_σ by (χ, b). Further, we can view (χ, b) as an element of $\mathrm{H}^2(F, \overline{F}^\times)$ since $\mathrm{H}^2(\mathrm{Gal}(E/F), E^\times)$ can be viewed as a subgroup of $\mathrm{H}^2(F, \overline{F}^\times)$. A well-known fact is that (χ, b) is bilinear.

Now, we fix an integer $n \geqslant 1$ and assume that F contains a primitive n-th root of unity. We have an isomorphism $F^\times/F^{\times n} \cong \mathrm{Hom}(G, \mathbb{Z}/n\mathbb{Z})$, where $G = \mathrm{Gal}(\overline{F}/F)$. It tells us that every $\chi : G \to \frac{1}{n}\mathbb{Z}/\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$ corresponds to an element $[a]$ of $F^\times/F^{\times n}$. We write it as χ_a. For each $a, b \in F^\times$, (χ_a, b) has the following properties

- $\mathrm{Inv}(\ker \chi_a) = F[\sqrt[n]{a}]$ and $(\chi_a, b) = 0$ if and only if $b \in \mathrm{N}_{F[\sqrt[n]{a}]/F}(F[\sqrt[n]{a}])$.
- $(\chi_a, b) \in \mathrm{H}^2(F, \overline{F}^\times)$ is n-torsion.
- (χ_a, b) only depends on $[a]$ and $[b]$ in $F^\times/F^{\times n}$.

We will not provide the proof for these statements. The intersted readers may consult Chapter 11 of [1] for details.

Recall that by Kummer theory, we have $\mathrm{H}^2(F, \mu_n(F)) \cong \mathrm{H}^2(F, \mathbb{Z}/n\mathbb{Z})$ is the n-torsion in $\mathrm{H}^2(F, \overline{F}^\times)$. The **Hilbert symbol** of a and b is just defined to be the element of $\mathrm{H}^2(F, \mathbb{Z}/n\mathbb{Z})$ corresponding to (χ_a, b), denoted by (a, b) or $(a, b)_F$.

We have a basic result for this notion:

Proposition 5.2.1. *Let F be a field with a primitive n-th root of unity.*

(1) *Suppose $x, a \in F$ such that $a \neq 0$ and $x^n - a \neq 0$. Then $(a, x^n - a) = 0$. In particular, $(a, -a) = 0$ and $(a, 1 - a) = 0$.*

(2) $(b, a) = -(a, b)$.

Proof. See [5], chapter XIV, section 2, proposition 4. ■

Lemma 5.2.2. *If $(\chi, b) = 0$ for all $b \in F^\times$, then $\chi = 0$.*

Proof. From the discussion above, we see that the kernel of $b \mapsto (\chi, b)$ is $N_E = \mathrm{N}_{E/F}(E^\times)$, where E is the field such that $\ker \chi = \mathrm{Gal}(\overline{F}/E)$. So, $N_E = F^\times = N_F$. By Proposition 5.1.10, we conclude that $E = F$. Hence, $\ker \chi = \mathrm{Gal}(\overline{F}/F)$, which means that $\chi = 0$. ■

Let F be a p-adic field that contains a primitive q-th root of unity, where q is a prime number. Suppose $\chi_a : \mathrm{Gal}(\overline{F}/F) \to \mathbb{Z}/q\mathbb{Z} \cong \frac{1}{q}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$ is a continuous homomorphism associated to $a \in F^\times$, we may view it as an element in $\mathrm{H}^1(F, \mathbb{F}_q)$ by identifying $\mathbb{Z}/q\mathbb{Z}$ and $\frac{1}{q}\mathbb{Z}/\mathbb{Z}$ with $\mathbb{F}_q$. By Kummer theory, we have $\mathrm{H}^1(F, \mu_q(F)) \cong \mathrm{H}^1(F, \mathbb{Z}/q\mathbb{Z}) \cong F^\times/F^{\times q}$. Using this identification, we have a bilinear form

$$\mathrm{H}^1(F, \mathbb{F}_q) \times \mathrm{H}^1(F, \mathbb{F}_q) \to \mathbb{F}_q$$

given by $([a], [b]) \mapsto (a, b)$.

Theorem 5.2.3. *Let F be a p-adic field that contains a primitive q-th root of unity, where q is a prime number. Then the bilinear form*

$$\mathrm{H}^1(F, \mathbb{F}_q) \times \mathrm{H}^1(F, \mathbb{F}_q) \to \mathbb{F}_q$$

is nondegenerate.

Proof. By Lemma 5.2.2, if $[a] \in \mathrm{H}^1(F, \mathbb{F}_q)$ nonzero, then there exists $[b] \in \mathrm{H}^1(F, \mathbb{F}_q)$ such that $(a, b) \neq 0$. Now, by Proposition 5.2.1, $(b, a) = -(a, b)$. Thus, if $[b] \in \mathrm{H}^1(F, \mathbb{F}_q)$ nonzero, then there exists $[a] \in \mathrm{H}^1(F, \mathbb{F}_q)$ such that $(a, b) \neq 0$. This means that the bilinear form is nondegenerate. ■

Corollary 5.2.4. *Suppose $(a, b) = 0$ for all $a \in F^\times$, then b has a q-th root in F.*

Proof. The nondegenerate property tells us that $[b] = 0$ in $F^\times/F^{\times q} \cong \mathrm{H}^1(F, \mathbb{F}_q)$, i.e. $b \in F^{\times q}$. So, b has a q-th root in F. We're done. ■

Definition 5.2.5. *Let F be a p-adic field. The intersection of all the norm subgroups N_K of $F^\times$ with K/F finite is called the **group of universal norms**, denoted by D_F.*

Definition 5.2.6. *A continuous map $f : X \to Y$ is said to be **proper** if $f^{-1}(K)$ is compact for any compact subset $K \subseteq Y$.*

Lemma 5.2.7. *Let E/F and L/E be finite extesions. Let $y \in D_F$ and $K(L) = \mathrm{N}_{L/E}(L^\times) \cap \mathrm{N}_{E/F}^{-1}(y)$. Then,*

(1) $\mathrm{N}_{E/F} : E^\times \to F^\times$ *is proper.*

(2) $\bigcap_{L/E} K(L) \neq \varnothing$, *where L runs through all finite extension L/E.*

Proof. (1) Note that the norm map $\mathrm{N}_{E/F} : E^\times \to F^\times$ is continuous. Indeed, $v_E(\sigma(x)) = v_E(x)$, where $\sigma \in \mathrm{Gal}(E/F)$, for any $x \in E^\times$. Thus, $v(\mathrm{N}_{E/F}(x)) = cv(x)$ for some constant c since $\mathrm{N}_{E/F}(x) = \left(\prod_{\sigma \in \mathrm{Gal}(E/F)} \sigma(x) \right)^{[E:F]_i}$. This implies that $\mathrm{N}_{E/F}$ is continuous.

Now, for any integer $n \in \mathbb{Z}$, we define the set $\mathrm{val}(n) \subseteq F^\times$ to be $\{x \in F^\times : v(x) = n\}$. Then, we see that $\{\mathrm{val}(n)\}_n$ is an open covering for $F^\times$. Moreover, if $f_n \in \mathrm{val}(n)$, then $\mathrm{val}(n) = f_n \,\mathrm{val}(0) = f_n \mathcal{O}_F^\times$. We have already known that $\mathcal{O}_F^\times$ is compact by Proposition 3.1.1. Thus, $\mathrm{val}(n)$ is compact. Similarly, $\mathrm{N}_{E/F}^{-1}(\mathrm{val}(n))$ is also compact by the compactness of $\mathcal{O}_E^\times$.

Now, let K be a compact subset of $F^\times$ (so it is closed), then there exist a finite subset $J \subseteq \mathbb{Z}$ such that $K \subseteq \bigcup_{n \in J} \mathrm{val}(n)$. So $\mathrm{N}_{E/F}^{-1}(K) \subseteq \bigcup_{n \in J} \mathrm{N}_{E/F}^{-1}(\mathrm{val}(n))$. Since $\mathrm{N}_{E/F}^{-1}(K)$ is closed by the continuity of $\mathrm{N}_{E/F}$, we see that $\mathrm{N}_{E/F}^{-1}(K)$ is compact. Thus, $\mathrm{N}_{E/F}$ is proper.

(2) By (1), we know that $\mathrm{N}_{E/F}^{-1}(\{y\})$ is compact. We claim that $\mathrm{N}_{L/E}(L^\times)$ is closed in $E^\times$, which implies that $K(L)$ is compact immediately. Let $b \in E^\times$ be a limit point of $\mathrm{N}_{L/E}(L^\times)$, then there exists $\{\mathrm{N}_{L/E}(a_k)\}_{k \geqslant 0}$ with $a_k \in L^\times$ such that $\mathrm{N}_{L/E}(a_k)$ converges to b. Now, let $K = \{x \in E^\times : x = \mathrm{N}_{L/E}(a_k) \text{ or } x = b\}$. We see that K is compact since it is sequentially compact in the metric space $E^\times$. Thus, $\mathrm{N}_{L/E}^{-1}(K)$ is also compact as $\mathrm{N}_{L/E}$ is proper. Then, $\{a_k\}_k$ has a converging subsequence, which we still denote by $\{a_k\}_k$. Let a be the limit of $\{a_k\}_k$, then we see that $b = \mathrm{N}_{L/E}(a) \in \mathrm{N}_{L/E}(L^\times)$. Thus, $\mathrm{N}_{L/E}(L^\times)$ is closed in $E^\times$. So, $K(L)$ is closed in $\mathrm{N}_{E/F}^{-1}(y)$ and it follows that $K(L)$ is compact and closed because $E^\times$ is Hausdorff.

Now, we assume that $\bigcap_{L/E} K(L) = \varnothing$. Now, $T(L) := K(E) \cap K(L)$ is closed in $K(E)$, so $T(L)$ is a compact subset of $K(E)$ and $\bigcap_{L/E} T(L) = \varnothing$. This reduces to the case $E^\times$ is compact. Then, there exists $L_1, \cdots, L_m$ such that $K(L_1) \cap K(L_2) \cap \cdots \cap K(L_m) = \varnothing$. Now, we can choose a field L containing all L_i, so $K(L) \subseteq K(L_i)$ for all i by the transitivity of norm maps. Thus, $K(L) = \varnothing$.

However, $K(L) \neq \varnothing$ for any L/E finite. Indeed, for any L/E finite, we have $y \in N_L$, so $y = \mathrm{N}_{L/F}(x) = \mathrm{N}_{E/F}(\mathrm{N}_{L/E}(x))$ for some $x \in L^\times$. Thus, $\mathrm{N}_{L/E}(x) \in \mathrm{N}_{L/F}^{-1}(y) \cap \mathrm{N}_{L/E}(L^\times) = K(L)$.

We conclude that $\bigcap_{L/E} K(L) \neq \varnothing$ as desired. ■

Proposition 5.2.8. *Suppose E/F is finite, then $\mathrm{N}_{E/F}(D_E) = D_F$.*

Proof. We first prove that $\mathrm{N}_{E/F}(D_E) \subseteq D_F$. Let $y \in \mathrm{N}_{E/F}(D_E)$, then $y = \mathrm{N}_{E/F}(x)$ for some $x \in D_E$. For any finite extension L/F, we may consider the composite $K = EL$. By definiton of D_E, we see that $x \in \mathrm{N}_{K/E}(K^\times)$. Thus, $y \in \mathrm{N}_{E/F}(\mathrm{N}_{K/E}(K^\times)) = \mathrm{N}_{K/F}(K^\times) = \mathrm{N}_{L/F}(\mathrm{N}_{K/L}(K^\times)) \subseteq \mathrm{N}_{L/F}(L^\times) = N_L$. Thus, $y \in D_F$.

Conversely, for any $y \in D_F$, there exists $x \in \bigcap_{L/E} K(L) = D_E \cap \mathrm{N}_{E/F}^{-1}(y)$. Thus, $y = \mathrm{N}_{E/F}(x) \in \mathrm{N}_{E/F}(D_E)$. ■

Definition 5.2.9. *A group G is said to be **divisible** if for any $g \in G$ and $n \geqslant 1$, there exists $h \in G$ such that $h^n = g$.*

Example 5.2.10. *If G is cyclic and divisible, then $G = 1$. This is trivial.*

Example 5.2.11. *If G is a divisible subgroup of $\mathbb{Z}_p$, then $G = 1$. Indeed, take $g_0 \in G$, then g_0 is divisible by p, i.e. there exists $g_1 \in G$ such that $pg_1 = g_0$. However, g_1 is also divisible by p, so we can repeat this procedure indefinitely, which implies that $v_p(g_0) = +\infty$. So $g_0 = 0$.*

Lemma 5.2.12. *If $G \subseteq F^\times$ is a divisible subgroup, then G is trivial.*

Proof. By Theorem 3.3.1, $F^\times \cong \mathbb{Z} \times \mathbb{Z}/(q-1)\mathbb{Z} \times \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}_p^d$. From Example 5.2.10 and 5.2.11, we see that $G = 1$. ■

Proposition 5.2.13. *For any p-adic field F, the group D_F is trivial.*

Proof. Suppose q is a prime number and $F_q = F(\mu_q)$, where $\mu_q = \mu_q(F)$ is the set of q-th roots of unity. Let L/F be a finite extension. Let E be a field containing F_q and L. Now, take $y \in D_F$, then there exists $x \in D_E$ such that $y = \mathrm{N}_{E/F}(x)$ by Proposition 5.2.8. Recall that the kernel of the map $\varphi : E^\times \to \mathrm{H}^2(E, \overline{E}^\times)$ given by $f \mapsto (\chi, f)$ is a norm subgroup, so we see that $x \in \ker\varphi$. Thus, $(a, x) = 0$ for all $a \in E^\times$. By Corollary 5.2.4, we see that $x = e^q$ for some $e \in E^\times$. Let $f = \mathrm{N}_{E/F}(e)$, then $y = f^q$.

Set $K(L) = \{g \in F^\times : g^q = y\} \cap N_L$, we see that $K(E)$ is nonempty as $f \in K(E)$. Thus, we see that $K(L)$ is nonempty for all L/F finite as $L \subseteq E$ implies that $K(E) \subseteq K(L)$. Moreover, $K(L)$ is finite. So, by using a similar argument as in the proof of last lemma, we see that $\bigcap_L K(L) \neq \varnothing$. Thus, there exists $g \in \bigcap_L K(L)$, i.e. $g \in D_F$ with $g^q = y$. We conclude that D_F is a divisible subgroup of $F^\times$. By Lemma 5.2.12, we see that D_F is trivial.
■

Lemma 5.2.14. *Let H be a subgroup of finite index in $F^\times$, then there exists a norm subgroup N such that $N \cap \mathcal{O}_F^\times \subseteq H$.*

Proof. Note that $\bigcap_N N \cap \mathcal{O}_F^\times \subseteq D_F = \{1\}$, we have $\bigcap_N N \cap \mathcal{O}_F^\times = \{1\}$, where N runs through all norm subgroup of $F^\times$. By Proposition 3.3.2, we know that any norm subgroup of $F^\times$ is closed and so open. For the same reason, H is also open and closed. Then it complement H^c is closed in $F^\times$. Now, consider the closed subsets $H^c \cap N \cap \mathcal{O}_F^\times$ in the compact space $\mathcal{O}_F^\times$. We know that $H^c \cap N \cap \mathcal{O}_F^\times$ is compact. Observe that $\bigcap_N (H^c \cap N \cap \mathcal{O}_F^\times) \subseteq D_F = \{1\}$ and $1 \notin H^c$. We conclude that $\bigcap_N (H^c \cap N \cap \mathcal{O}_F^\times) = \varnothing$. Thus, there exists finitely many norm subgroups $N_1, \cdots, N_r$ such that $\bigcap_{i=1}^r (H^c \cap N_i \cap \mathcal{O}_F^\times) = \varnothing$, i.e. $H^c \cap (N_1 \cap N_2 \cap \cdots \cap N_r) \cap \mathcal{O}_F^\times = \varnothing$. Let $N = N_1 \cap N_2 \cap \cdots \cap N_r$, we see that $N \cap \mathcal{O}_F^\times \subseteq H$. By Lemma 5.1.8 and 5.1.9, we see that N is a norm subgroup. ∎

Theorem 5.2.15 (the Existence theorem). *Let H be a subgroup of finite index in $F^\times$, then there exists an abelian extension K/F such that $H = N_K$.*

Proof. Let N be a norm subgroup of $F^\times$, then N has finite index. So, $H \cap N$ also has finite index in $F^\times$ by the relation $[H : H \cap N] = [HN : N]$. Set $H_N = (H \cap N)\mathcal{O}_F^\times$, which is of finite index in $F^\times$ because it contains $H \cap N$. Note that H_N contains $\mathcal{O}_F^\times$, the kernel of $v : F^\times \to \mathbb{Z}$. Then $v(H_N) = n\mathbb{Z}$ for some $n \geqslant 1$. So by Proposition 4.1.6, we conclude that $H_N = \mathrm{N}_{E_n/F}(E_n^\times) = N_{E_n}$ for some unramified extension E_n/F of degree n. So, H_N is a norm subgroup. Consequently, $N \cap H_N$ is also a norm subgroup by Lemma 5.1.8 and 5.1.9.

By Lemma 5.2.14, there exists a norm subgroup N such that $N \cap \mathcal{O}_F^\times \subseteq H$. Take $a \in N \cap H_N \subseteq H_N = (H \cap N)\mathcal{O}_F^\times$, then $a = bc$ for some $b \in H \cap N$ and $c \in \mathcal{O}_F^\times$. So, $c = ab^{-1} \in N$ as $a, b \in N$. We see that $c \in N \cap \mathcal{O}_F^\times \subseteq H$. So, $a = bc \in H$. It follows that $N \cap H_N \subseteq H$. Thus, we conclude that H is a norm subgroup as it contains one by Corollary 5.1.11. Again, by Lemma 5.1.8, we're done. ∎

We now can summarize what we discussed previously into a strong result:

Theorem 5.2.16 (Fundamental theorem of local class field theory). *Suppose F is a p-adic field, and $\overline{F}$ is an algebraic closure of F. Let*

$$\mathcal{A} = \left\{ K : F \subseteq K \subseteq \overline{F} \text{ such that } K/F \text{ is finite abelian } \right\}$$

and

$$\mathcal{S} = \left\{ \text{ subgroups of finite index in } F^\times \right\}.$$

Then the map $K \mapsto N_K$ is a one-to-one, order-reversing correspondence between $\mathcal{A}$ and $\mathcal{S}$.

Usually, if H is a subgroup of finite index in $F^\times$, then the unique field K such that $N_K = H$ is called the **class field** of H.

6 A classical application

In this chapter, we intend to discuss a classical application of local class field theory we developed in last chapter.

6.1 The local Kronecker-Weber theorem

Local class field theory mainly study the classification of abelian extensions of a local field K, although we only deal with p-adic fields in this thesis. An interesting case is that $K = \mathbb{Q}_p$. We will study the abelian extension of $\mathbb{Q}_p$ in this section. By the fundamental theorem of local class field theory, the first step is investigating the norm subgroups N_K for each finite abelian extension $K/\mathbb{Q}_p$.

Lemma 6.1.1. *If $p = 2$, then the subgroup of squares in $U^{(2)}$ is $U^{(3)}$ and $[U^{(2)} : U^{(3)}] = 2$.*

Proof. From the discussion in §3.1, we have $U^{(n)}/U^{(n+1)} \cong \mathbb{Z}_2$. Thus, $|U^{(n)}/U^{(n+1)}| = |\mathbb{Z}/2\mathbb{Z}| = 2$, for all $n \geqslant 1$. In particular, we see that $[U^{(2)} : U^{(3)}] = 2$.

By Proposition 3.2.1, we see that $U^{(n)} \cong \mathfrak{p}^n \cong \mathbb{Z}_2$ for all $n > 1$. Thus, $U^{(2)} \cong \mathbb{Z}_2$. Note that $\mathbb{Z}_2$ has a unique subgroup of index 2, which is $2\mathbb{Z}_2$. Using the isomorphism, we see that the unique subgroup of $U^{(2)}$ having index 2 is the subgroup of squares. Since $[U^{(2)} : U^{(3)}] = 2$, we see that $U^{(3)}$ is precisely the subgroup of squares in $U^{(2)}$. ■

Lemma 6.1.2. *Let ζ be a primitive p^n-th root of unity for some $n \geqslant 1$. Suppose $K = \mathbb{Q}_p(\zeta)$. Then*

(1) *$K/\mathbb{Q}_p$ is Galois and* $\mathrm{Gal}(K/\mathbb{Q}_p) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$.

(2) $\mathrm{N}_{K/\mathbb{Q}_p}(1 - \zeta) = p$.

(3) *the corresponding norm subgroup is $N_K = \langle p \rangle \times U^{(n)}$.*

Proof. (1) By definition, we see that K is the splitting field of $x^{p^n} - 1 \in \mathbb{Q}_p[x]$, which is a separable polynomial. Thus, $K/\mathbb{Q}_p$ is Galois. Since ζ is a primitive p^n-th root, we have an isomorphism $\mathbb{Z}/p^n\mathbb{Z} \to \mu_{p^n}$ given by $k \mapsto \zeta^k$. We can define a homomorphism $i : \mathrm{Gal}(K/\mathbb{Q}_p) \to (\mathbb{Z}/p^n\mathbb{Z})^\times$ by $\sigma \mapsto i(\sigma)$, where $i(\sigma)$ is the element in $(\mathbb{Z}/p^n\mathbb{Z})^\times$ such that $\sigma(\zeta) = \zeta^{i(\sigma)}$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q}_p)$. First, i is injective; let $i(\sigma) = 1$, then $\sigma(\zeta) = \zeta$. Thus, $\sigma = 1$.

Let $\psi(X) = 1 + X^{p^{n-1}} + X^{2p^{n-1}} + \cdots + X^{(p-1)p^{n-1}} \in \mathbb{Q}_p[X]$. We must have $\psi(\zeta) = 0$. Indeed, set $y = \zeta^{p^{n-1}}$. Then $y^p = 1$ and this implies that $1 + y + y^2 + \cdots + y^{p-1} = 0$. We

claim that ψ irreducible. It suffices to prove that $\phi(X) = \psi(X+1)$ is irreducible. Indeed, $\phi(X) = \frac{(X+1)^{p^n}-1}{(X+1)^{p^{n-1}}-1} \equiv \frac{X^{p^n}+1-1}{X^{p^{n-1}}+1-1} \equiv X^{(p-1)p^{n-1}} \mod p$. Since $\phi(0) = p$, we see that $p^2 \nmid p$. Thus, $\phi(X)$ is irreducible by Eisenstein's criterion. Thus, $\psi(X)$ is irreducible. This implies that ψ is the minimal polynomial of ζ. Thus, $[K : \mathbb{Q}_p] = (p-1)p^{n-1}$. It follows that $\mathrm{Gal}(K/\mathbb{Q}_p) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$ by counting the order.

(2) Since $\psi(\zeta) = 0$ and ζ is an arbitrary primitive p^n-th root, we see that

$$\psi(X) = \prod_{\xi}(X - \xi) = \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q}_p)} (X - \sigma(\zeta)),$$

where ξ runs through all primitive p^n-th roots. Thus, $p = \psi(1) = \prod_{\sigma\in\mathrm{Gal}(K/\mathbb{Q}_p)}(1-\sigma(\zeta)) = \mathrm{N}_{K/\mathbb{Q}_p}(1-\zeta)$.

(3) We first prove that $U^{(n)} \subseteq \mathrm{N}_K$.

Case 1: p is an odd prime. By Proposition 3.2.1, we see that $\mathfrak{p}^m = (p^m) = U^{(m)}$ for all $m \geqslant 1$, where $\mathfrak{p} = (p)$ is the maximal ideal of $\mathbb{Z}_p$. Since $p-1$ is invertible in $\mathbb{Z}_p$, we see that the multiplication by $p-1$ gives an isomorphism between (p^m) and itself. So, $[p^{n-1}(p-1)]\mathfrak{p} = p^{n-1}(p) = (p^n) = \mathfrak{p}^n$. Thus, $(U^{(1)})^{p^{n-1}(p-1)} = U^{(n)}$. However, for any $a \in \mathbb{Q}_p$, $\mathrm{N}_{K/\mathbb{Q}_p}(a) = \prod_{\sigma\in\mathrm{Gal}(K/\mathbb{Q}_p)} \sigma(a) = \prod_{\sigma\in\mathrm{Gal}(K/\mathbb{Q}_p)} a = a^{p^{n-1}(p-1)}$ since $|\mathrm{Gal}(K/\mathbb{Q}_p)| = p^{n-1}(p-1)$. It follows that $U^{(n)} \subseteq \mathrm{N}_{K/\mathbb{Q}_p}(U^{(1)}) \subseteq \mathrm{N}_K$.

Case 2: $p = 2$. If $n = 1$, using a similar argument as above, we have $(U^{(1)})^{p-1} = U^{(1)}$. Moreover, $|\mathrm{Gal}(K/\mathbb{Q}_p)| = p-1$. Thus, we conclude that $U^{(1)} \subseteq \mathrm{N}_K$.

Now, suppose $n \geqslant 2$. Then, we have $U^{(m)} = (2^m)$ for all $m \geqslant 2$ and $(U^{(2)})^{2^{n-2}} = U^{(n)}$. We have $\mathrm{N}_{K/\mathbb{Q}_p}(a) = a^{2^{n-1}}$ for all $a \in \mathbb{Q}_p$ since $|\mathrm{Gal}(K/\mathbb{Q}_p)| = 2^{n-1}$ now. Let $y \in U^{(n)}$, then there exists $x \in U^{(2)}$ such that $x^{2^{n-2}} = y$. So, if $x = a^2$ for some $a \in K^\times$, we are done.

By Lemma 6.1.1, $U^{(3)}$ is the subgroup of squares in $U^{(2)}$. Since $5 \notin U^{(3)}$, we see that $5 \in U^{(2)}$ is not a square. Since $[U^{(2)} : U^{(3)}] = 2$, we see that $U^{(2)} = U^{(3)} \cup 5U^{(3)}$. Thus, if x is not a square, then we may write $x = 5z^2$ for some z. So, $y = 5^{2^{n-2}}z^{2^{n-1}}$. Since -1 is not a square in $\mathbb{Q}_2$ as $-1 \notin U^{(3)}$, let $i = \sqrt{-1}$, then $i^4 = 1$ and $[\mathbb{Q}_2(i) : \mathbb{Q}_2] = 2$. So, $i \in K$ and $|\mathrm{Gal}(K/\mathbb{Q}_2(i))| = [K : \mathbb{Q}_2(i)] = 2^{n-2}$. We see that $\mathrm{N}_{K/\mathbb{Q}_2}(2+i) = \mathrm{N}_{\mathbb{Q}_2(i)/\mathbb{Q}_2}(\mathrm{N}_{K/\mathbb{Q}_2}(2+i)) = \mathrm{N}_{\mathbb{Q}_2(i)/\mathbb{Q}_2}((2+i)^{2^{n-2}}) = \mathrm{N}_{\mathbb{Q}_2(i)/\mathbb{Q}_2}(2+i)^{2^{n-2}} = [(2+i)(2-i)]^{2^{n-2}} = 5^{2^{n-2}}$. Thus, $y = \mathrm{N}_{K/\mathbb{Q}_2}((2+i)z) \in \mathrm{N}_K$.

Now, we intend to investigate N_K. By (2), we see that $p \in \mathrm{N}_K$. Thus, we have $\langle p\rangle \times U^{(n)} \subseteq \mathrm{N}_K$. By Theorem 5.1.3, we see that $[\mathbb{Q}_p^\times : \mathrm{N}_K] = |\mathrm{Gal}(K/\mathbb{Q}_p)| = (p-1)p^{n-1}$. Recall that $\mathbb{Q}_p^\times = \mathbb{Z} \times \mathbb{Z}/(|\mathbb{F}_p|-1)\mathbb{Z} \times U^{(1)}$ and $|U^{(1)}/U^{(n)}| = |\mathbb{F}_p|^{n-1} = p^{n-1}$. It follows that $[\mathbb{Q}_p^\times : \langle p\rangle \times U^{(n)}] = (p-1)p^{n-1}$. We conclude that $N_K = \langle p\rangle \times U^{(n)}$. ■

Remark 6.1.3. *In this case, $K/\mathbb{Q}_p$ is totally ramified.*

Lemma 6.1.4. *Suppose ℓ is an integer prime to p. Let ζ be a primitive ℓ-th root of unity. Suppose $K = \mathbb{Q}_p(\zeta)$ and m is the smallest integer such that $p^m \equiv 1 \mod \ell$. Then*

(1) *$K/\mathbb{Q}_p$ is unramified of degree m.*

(2) *the corresponding norm subgroup is $N_K = \langle p^m \rangle \times \mathbb{Z}_p^\times$.*

Proof. (1) We first prove that K/F is unramified. Let $\psi(X) = \min(\mathbb{Q}_p, \zeta) \in \mathbb{Z}_p[X]$. Then $\psi(X)|X^\ell - 1$. Let $\overline{\psi}$ the image of ψ in $\mathbb{F}_p[X]$. We must have $\overline{\psi}(X)|X^\ell - 1$. Note that $\overline{\psi}$ does not have repeated roots since $\gcd(\ell, p) = 1$. Now, by Hensel's lemma, we see that the polynomial $\overline{\psi}$ is irreducible. Note that $\overline{\psi}(\overline{\zeta}) = 0$ and $\overline{\zeta} \in \mathbb{K}$. It follows that $[\mathbb{K} : \mathbb{F}_p] \geqslant \deg(\overline{\psi}) = \deg(\psi) = [K : \mathbb{Q}_p] = e[\mathbb{K} : \mathbb{F}_p]$. Thus, $e = 1$. This means that $K/\mathbb{Q}_p$ is unramified. Thus, $\mathbb{K} = \mathbb{Q}_p(\overline{\zeta})$.

Note that $\zeta^\ell = 1$ implies that $v_K(\zeta) = 0$. We have $\zeta \in \mathcal{O}_K$. So, we see that the roots of $X^\ell - 1 \in \mathbb{Z}_p[X]$ are all in $\mathcal{O}_K$. It follows that $X^\ell - 1$ is a product of linear factors in $\mathcal{O}_K[X]$ and thus in $\mathbb{K}[X]$. We conclude that $\mathbb{K}/\mathbb{Q}_p$ is cyclotomic and $\overline{\zeta}$ is primitive. Since $\ell | p^m - 1$, we see that $|\mathbb{K}^\times| = p^m - 1$. Thus, $|\mathbb{K}| = p^m$, i.e. $[\mathbb{K} : \mathbb{F}_p] = m$.

(2) By Proposition 4.1.6, we see that $\mathrm{N}_K = v_p^{-1}(m\mathbb{Z}) = \langle p^m \rangle \times \mathbb{Z}_p^\times$. ∎

Lemma 6.1.5. *Any subgroup of finite index in $\mathbb{Q}_p^\times$ contains a subgroup of the form $\langle p^m \rangle \times U^{(n)}$ for some $n, m \in \mathbb{N}$.*

Proof. Let G be a subgroup of finite index in $\mathbb{Q}_p^\times$. First, observe that the valuation group $v_p(G) = s\mathbb{Z}$ for some $s > 0$. Then G contains some element $p^s u$ with $u \in \mathbb{Z}_p^\times = U^{(0)}$ a unit.

We claim that G contains a subgroup of the form $U^{(n)}$ for some n. Suppose that we have established the claim. Recall that $[U^{(0)} : U^{(n)}] = (p-1)p^{n-1}$. Let $t = (p-1)p^{n-1}$, then $u^t \in U^{(n)}$ and $p^{st}u^t = (p^s u)^t \in G$. Let $m = st$, then we see that $p^m \in G$. It follows that G contains $\langle p^m \rangle$ and $U^{(n)}$, i.e. $\langle p^m \rangle \times U^{(n)} \subseteq G$.

Now, it remains to prove the claim. By Proposition 3.3.2, we see that G is closed and hence open. By Proposition 3.1.2, we may assume that $G \subseteq U^{(1)}$. Let $\mathfrak{p} = (p)$, then we have $\mathfrak{p}^{n+m} = p^m \mathfrak{p}^n$ for all m, n. By Proposition 3.2.1, we see that $U^{(m+n)} = (U^{(n)})^{p^m}$ for any $n \geqslant 2$. So, for any given $k \geqslant 0$, $U^{(m+n)} \subseteq (U^{(n)})^{p^k} \subseteq (U^{(1)})^{p^k}$ for all $m \geqslant k$ and $n \geqslant 2$. Hence, for any given $k \geqslant 0$, there exist some n such that $U^{(n)} \subseteq (U^{(1)})^{p^k}$.

Recall that $U^{(1)} \cong \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}_p^d$, so we need to investigate $\mathbb{Z}_p$. Any neighborhood of 0 in $\mathbb{Z}_p$ contains an ideal of the form (p^k) for some k. Thus, any open set in $\mathbb{Z}_p^d$ containing 0 must

contain a submodule of the form $p^k\mathbb{Z}_p^d$. Thus, G contains a subgroup of the form $(U^{(1)})^{p^k}$ for some k. Hence, we are done. ■

Theorem 6.1.6 (Kronecker-Weber). *Suppose p is a prime number and $K/\mathbb{Q}_p$ is a finite abelian extension. Then K is contained in a cyclotomic extension of $\mathbb{Q}_p$.*

Proof. By Lemma 6.1.5, we see that N_K contains a subgroup of the form $\langle p^m\rangle \times U^{(n)}$ for some m, n. Let ξ be a primitive (p^m-1)-th root and ζ a primitive p^n-th root. Let $K_1 = \mathbb{Q}_p(\xi)$ and $K_2 = \mathbb{Q}_p(\zeta)$. Then, K_1 is the unramified extension of degree m and $N_{K_1} = \langle p^m\rangle \times \mathbb{Z}_p^\times$ by Lemma 6.1.4. By Lemma 6.1.2, we see that $N_{K_2} = \langle p\rangle \times U^{(n)}$. Thus, $\langle p^m\rangle \times U^{(n)} = \left(\langle p^m\rangle \times \mathbb{Z}_p^\times\right) \cap \left(\langle p\rangle \times U^{(n)}\right) = N_{K_1} \cap \mathrm{N}_{K_2}$. Note that $\mathrm{Gal}(K_1/\mathbb{Q}_p) \cong \mathrm{Gal}(\mathbb{K}_1/\mathbb{F}_p)$ is cyclic and $\mathrm{Gal}(\mathbb{K}_2/\mathbb{F}_p) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$, where $\mathbb{K}_i$ is the residue field of K_i with $i = 1, 2$. We see that $K_1/\mathbb{Q}_p$ and $K_2/\mathbb{Q}_p$ are both abelian extensions. By Lemma 5.1.9, $N_{K_1K_2} = N_{K_1} \cap N_{K_2}$. Clearly, $\xi\zeta$ is a primitive $p^n(p^m-1)$-th root. So, K_1K_2/F is a cyclotomic extenison. By the fundamental theorem of local class field theory, we see that $K \subseteq K_1K_2$. ■

Reference

[1] Pierre Guillot. *A Gentle Course in Local Class Field Theory*. Cambridge University Press, Cambridge, 2018.

[2] Kenkichi Iwasawa. *Local Class Field Theory*. Oxford University Press, New York, 1986.

[3] Patrick Morandi. *Field and Galois Theory, Graduate Texts in Mathematics, Volume 167*. Springer, New York, 1996.

[4] J. Neukirch. *Algebraic Number Theory*. Springer-Verlag, Berlin, 1999.

[5] J.-P. Serre. *Local fields, Graduate Texts in Mathematics, Volume 67*. Springer, New York, 1979.

[6] T. Wedhorn. *Local Langlands Correspondence for GL(n) over p-adic Fields*. Lectures given at the School on Automorphic Forms on GL(n), Trieste, 2000.

Acknowledgement

First of all, I would like to thank my undergraduate thesis advisor, Prof. Yong Hu. This thesis is written and revised under the guidance of Prof. Hu. Therefore, I would like to express my sincere thanks to him for his careful help and guidance. I would also like to thank Prof. Caiheng Li and Prof. Zhan Li for their help in my studies and their guidance in my Ph.D. application process and fortunately, I got Ph.D. offers from some U.S. universies this year with their help. In this period of time, not only have I learned a lot of professional knowledge from them, but also felt that they were hardworking, friendly and approachable. In addition, their rigorous attitude and selfless spirit are worth learning.

I would like to express my gratitude to the Department of Mathematics of Southern University of Science and Technology that provided me with a good environment for studying and scientific research so that I can concentrate on studying and discover the beauty of modern mathematics. I would like to thank all professors who prepared online courses for us carefully due to the impact of COVID-19. I would also like to thank all the like-minded friends I have met in the Department of Mathematics in the past few years for their help in learning seminars. Thank you everyone who supported and helped me in the past 22 years.

Jing Ye
April, 2020