Local Class Field Theory

KENKICHI IWASAWA
Princeton University
Local class field theory is a theory of abelian extensions of so-called local fields, typical examples of which are the $p$-adic number fields. This book is an introduction to that theory.

Historically, local class field theory branched off from global, or classical, class field theory, which studies abelian extensions of global fields—that is, algebraic number fields and algebraic function fields with finite fields of constants. So, in earlier days, some of the main results of local class field theory were derived from those of the global theory. Soon after, however, in the 1930s, F. K. Schmidt and Chevalley discovered that local class field theory can be constructed independently of the global theory; in fact, the former provides us essential devices for the proofs in the latter. Around 1950, Hochschild and Nakayama brought much generality and clarity into local class field theory by introducing the cohomology theory of groups. Classical books such as Artin [1] and Serre [21] follow this cohomological method. Later, different approaches were proposed by others—for example, the method of Hazewinkel [11], which forgoes cohomology groups, and that of Kato [14], based on algebraic $K$-theory. More recently, Neukirch also introduced a new idea to local class field theory, which applies as well to global fields.

Meanwhile, motivated by the analogy with the theory of complex multiplication on elliptic curves, Lubin and Tate showed in their paper [19] of 1965 how formal groups over local fields can be applied to deduce important results in local class field theory. In recent years, this idea has been further pursued by several mathematicians, in particular by Coleman. Following this trend, we shall try in this book to build up local class field theory entirely by means of the theory of formal groups. This approach, though not the shortest, seems particularly well suited to prove some deeper theorems on local fields.

In Chapters I and II, we discuss in the standard manner some basic definitions and properties of local fields. In Chapter III, we consider certain infinite extensions of local fields and study formal power series with coefficients in the valuation rings of those fields. These results are used in Chapters IV and V, where we introduce a generalization of Lubin–Tate formal groups and construct similarly as in [19] abelian extensions of local fields by means of division points of such formal groups. In Chapter VI, the main theorems of local classfield theory are proved: we first show that the abelian extensions constructed in Chapter V in fact give us all abelian extensions of local fields, and then define the so-called norm residue maps and prove important functorial properties of such maps. In Chapter VII, the classical results on finite abelian extensions of local fields are deduced from the main theorems of Chapter VI. In the last chapter, an explicit reciprocity theorem of Wiles [25] is proved, which generalizes a beautiful formula of Artin–Hasse [2] on norm residue symbols.
The book is almost self-contained and the author tried to make the exposition as readable as possible, requiring only some basic background in algebra and topological groups on the part of the reader. The contents of this book are essentially the same as the lectures given by the author at Princeton University in the Spring term of 1983. However, the original exposition in the lectures has been much improved at places, thanks to the idea of de Shalit [6].

In 1980, the author published a book [13] on local class field theory in Japanese from Iwanami-Shoten, Tokyo, which mainly followed the idea of Hazewinkel [11]. When the matter of translating this text into English arose, the author decided to rewrite the whole book in the manner just described. In order to give the reader some idea of other approaches in local class field theory, a brief account of cohomological method and Hazewinkel’s method are included in an Appendix. At the end of the book, a short list of references is attached, containing only those items in the literature mentioned in the text; for a more complete bibliography on local fields and local class field theory, the reader is referred to Serre [21]. An index and a table of notations are also appended for the convenience of the reader.

The author expresses here his hearty gratitude to D. Dummit and E. Friedman who carefully read the book in manuscript and offered many valuable suggestions for its improvement. He also thanks D. W. Degenhardt of Oxford University Press for his help in publishing this book.

Princeton
September 1985

K.I.
Contents

Chapter I. Valuations 3
   1.1. Some Basic Definitions 3
   1.2. Complete Fields 7
   1.3. Finite Extensions of Complete Fields 12

Chapter II. Local Fields 18
   2.1. General Properties 18
   2.2. The Multiplicative Group $k^\times$ 22
   2.3. Finite Extensions 25
   2.4. The Different and the Discriminant 29
   2.5. Finite Galois Extensions 32

Chapter III. Infinite Extensions of Local Fields 35
   3.1. Algebraic Extensions and Their Completions 35
   3.2. Unramified Extensions and Totally Ramified Extensions 36
   3.3. The Norm Groups 40
   3.4. Formal Power Series 43
   3.5. Power Series over $\mathfrak{o}_K$ 45

Chapter IV. Formal Groups $F_f(X, Y)$ 50
   4.1. Formal Groups in General 50
   4.2. Formal Groups $F_f(X, Y)$ 53
   4.3. The $\mathfrak{o}$-Modules $W^n_f$ 57
   4.4. Extensions $\tilde{L}^n/\tilde{K}$ 61

Chapter V. Abelian Extensions Defined by Formal Groups 65
   5.1. Abelian Extensions $L^n$ and $k^{m,n}_\pi$ 65
   5.2. The Norm Operator of Coleman 69
   5.3. Abelian Extensions $L$ and $k_\pi$ 75

Chapter VI. Fundamental Theorems 80
   6.1. The Homomorphism $\rho_k$ 80
   6.2. Proof of $L_k = k_{ab}$ 84
   6.3. The Norm Residue Map 88
LOCAL CLASS FIELD THEORY
Chapter I

Valuations

In this chapter, we shall briefly discuss some basic facts on valuations of fields which will be used throughout the subsequent chapters. We shall follow the classical approach in the theory of valuations, but omit the proofs of some elementary results in Section 1.1, which can be found in many standard textbooks on algebra.† For further results on valuations, we refer the reader to Artin [1] and Serre [21].

1.1. Some Basic Definitions

Let \( k \) be a field. A function \( v(x) \) on \( k, x \in k \), is called a valuation of \( k \) if it satisfies the following conditions:

(i) \( v(x) \) is a real number for \( x \neq 0 \); and \( v(0) = +\infty \).

(ii) For any \( x, y \) in \( k \),

\[
\min(v(x), v(y)) \leq v(x + y).
\]

(iii) Similarly,

\[
v(x) + v(y) = v(xy).
\]

**Example 1.** Let

\[
v_0(0) = +\infty, \quad v_0(x) = 0 \quad \text{for all } x \neq 0 \text{ in } k.
\]

Then \( v_0 \) is a valuation of \( k \). It is called the trivial valuation of \( k \).

**Example 2.** Let \( p \) be a prime number. Each non-zero rational number \( x \) can be uniquely written in the form \( x = p^e y \), where \( e \) is an integer and \( y \) is a rational number whose numerator and denominator are not divisible by \( p \). We define a function \( v_p \) on the rational field \( \mathbb{Q} \) by

\[
v_p(0) = +\infty; \quad v_p(x) = e, \quad \text{if } x \neq 0 \text{ and } x = p^e y \text{ as above}.
\]

Then \( v_p \) is a valuation of \( \mathbb{Q} \); it is the well-known \( p \)-adic valuation of the rational field. \( v_p \) is the unique valuation \( v \) on \( \mathbb{Q} \) satisfying \( v(p) = 1 \).††

**Example 3.** Let \( F \) be a field and let \( F(T) \) denote the field of all rational functions in an indeterminate \( T \) with coefficients in \( F \). Then each \( x \neq 0 \) in \( F(T) \) can be uniquely written in the form \( x = T^e y \), where \( e \) is an integer and \( y \) is a quotient of polynomials in \( F[T] \), not divisible by \( T \). Putting \( v(0) = +\infty \) and \( v(x) = e \) for \( x \neq 0 \) as above, we obtain a valuation \( v \) of the field \( k = F(T) \) such that \( v(T) = 1 \). Instead of \( T \), we can choose any irreducible

† See, for example, Lang [16] and van der Waerden [23].

†† Compare van der Waerden [23].
polynomial \( f(T) \) in \( F(T) \) and define similarly a valuation \( v \) on \( k = F(T) \) with \( v(f) = 1 \).

Let \( v \) be a valuation of a field \( k \). Then it follows immediately from the definition that

\[
v(\pm 1) = 0, \quad v(-x) = v(x), \quad v(x) < v(y) \implies v(x + y) = v(x).
\]

Here 1 (= 1\(_k\)) denotes the identity element of the field \( k \). Let

\[
\mathfrak{o} = \{ x \mid x \in k, \quad v(x) \geq 0 \},
\]

\[
\mathfrak{p} = \{ x \mid x \in k, \quad v(x) > 0 \}.
\]

Then \( \mathfrak{o} \) is a subring of \( k \) continuing 1 and \( \mathfrak{p} \) is a maximal ideal of \( \mathfrak{o} \) so that

\[
\mathfrak{f} = \mathfrak{o}/\mathfrak{p}
\]

is a field. \( \mathfrak{o} \), \( \mathfrak{p} \), and \( \mathfrak{f} \) are called the valuation ring, the maximal ideal, and the residue field of \( v \), respectively. By (iii) above, the valuation \( v \) defines a homomorphism

\[
v : k^\times \to \mathbb{R}^+
\]

from the multiplicative group \( k^\times \) of the field \( k \) into the additive group \( \mathbb{R}^+ \) of real numbers. Hence the image \( v(k^\times) \) is a subgroup of \( \mathbb{R}^+ \), and we have

\[
k^\times/U \cong v(k^\times)
\]

where

\[
U = \text{Ker}(v) = \{ x \mid x \in k^\times, \quad v(x) = 0 \}.
\]

\( U \) is called the unit group of the valuation \( v \).

Let \( v \) be a valuation of \( k \). For any real number \( \alpha > 0 \), define a function \( \mu(x) \) on \( k \) by

\[
\mu(x) = \alpha v(x), \quad \text{for all } x \in k.
\]

Then \( \mu \) is again a valuation of \( k \). When two valuations \( v \) and \( \mu \) on \( k \) are related in this way—namely, when one is a positive real number times the other—we write

\[
v \sim \mu
\]

and say that \( v \) and \( \mu \) are equivalent valuations of \( k \). Equivalent valuations have the same valuation ring, the same maximal ideal, the same residue field, the same unit group, and they share many other important properties.

Let \( v \) be a valuation of a field \( k \). For each \( x \in k \) and \( \alpha \in \mathbb{R} \), let

\[
N(x, \alpha) = \{ y \mid y \in k, \quad v(y - x) > \alpha \}.
\]

This is a subset of \( k \) containing \( x \). Taking the family of subsets \( N(x, \alpha) \) for all \( \alpha \in \mathbb{R} \) as a base of neighbourhoods of \( x \) in \( k \), we can define a Hausdorff topology on \( k \), which we call the \( v \)-topology of \( k \). \( k \) is then a topological field in that topology; the valuation ring \( \mathfrak{o} \) is closed in \( k \) and the maximal ideal \( \mathfrak{p} \) is open in \( k \). A sequence of points, \( x_1, x_2, x_3, \ldots \), in \( k \) converges to
$x \in k$ in the $v$-topology—that is,

$$\lim_{n \to \infty} x_n = x,$$

if and only if

$$\lim_{n \to \infty} v(x_n - x) = +\infty.$$

When this is so, then

$$\lim_{n \to \infty} v(x_n) = v(x).$$

In fact, if $x \neq 0$, then $v(x_n) = v(x)$ for all sufficiently large $n$. A sequence $x_1, x_2, x_3, \ldots$ in $k$ is called a Cauchy sequence in the $v$-topology when

$$v(x_m - x_n) \to +\infty, \text{ as } m, n \to +\infty.$$

A convergent sequence is of course a Cauchy sequence, but the converse is not necessarily true. The valuation $v$ is called complete if every Cauchy sequence in the $v$-topology converges to a point in $k$. If $v$ is complete then the infinite sum

$$\sum_{n=1}^{\infty} x_n = \lim_{i \to \infty} \sum_{n=1}^{i} x_n$$

converges in $k$ if and only if

$$v(x_n) \to +\infty, \text{ as } n \to +\infty.$$

A valuation $v$ of $k$ is called discrete if $v(k^\times)$ is a discrete subgroup of $\mathbb{R}^+$—that is, if

$$v(k^\times) = \mathbb{Z}\beta = \{n\beta \mid n = 0, \pm 1, \pm 2, \ldots\}$$

for some real number $\beta \geq 0$. If $\beta = 0$, then $v$ is the trivial valuation $v_0$ in Example 1. When $\beta = 1$—that is, when

$$v(k^\times) = \mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\},$$

$v$ is called a normalized, or normal, valuation of $k$. It is clear that a valuation $v$ of $k$ is discrete but non-trivial if and only if $v$ is equivalent to a normalized valuation of $k$.

Let $k'$ be an extension field of $k$, and $v'$ a valuation of $k'$. Let $v' \mid k$ denote the function on $k$, obtained from $v'$ by restricting its domain to the subfield $k$. Then $v' \mid k$ is a valuation of $k$, and we call it the restriction of $v'$ to the subfield $k$. On the other hand, if $v$ is a valuation of $k$, any valuation $v'$ on $k'$ such that

$$v' \mid k = v$$

is called an extension of $v$ to $k'$. When $v'$ on $k'$ is given, its restriction $v' \mid k$ is always a well-determined valuation of $k$. However, given a valuation $v$ on $k$, it is not known a priori whether $v$ can be extended to a valuation $v'$ of $k'$. The study of such extensions is one of the main topics in the theory of valuations.
Let $v' \mid k = v$ as stated above. Then the $v'$-topology on $k'$ induces the $v$-topology on the subfield $k$ so that $k$ is a topological subfield of $k'$. Let $\mathfrak{o}'$, $\mathfrak{p}'$, and $f'$ denote the valuation ring, the maximal ideal, and the quotient field of $v'$, respectively:

\[
\begin{align*}
\mathfrak{o}' &= \{ x' \in k' \mid v'(x') \geq 0 \}, \\
\mathfrak{p}' &= \{ x' \in k' \mid v'(x') > 0 \}, \\
f' &= \mathfrak{o}'/\mathfrak{p}'.
\end{align*}
\]

Then

\[
\mathfrak{o} = \mathfrak{o}' \cap k, \quad \mathfrak{p} = \mathfrak{p}' \cap k = \mathfrak{p}' \cap \mathfrak{o}
\]

so that

\[
f = \mathfrak{o}/\mathfrak{p} = \mathfrak{o}/(\mathfrak{p}' \cap \mathfrak{o}) = (\mathfrak{o} + \mathfrak{p}')/\mathfrak{p}' \subseteq \mathfrak{o}'/\mathfrak{p}' = f'.
\]

Thus the residue field $f$ of $v$ is naturally imbedded in the residue field $f'$ of $v'$. On the other hand, $v' \mid k = v$ also implies

\[
v(k^\times) \subseteq v'(k'^\times) \subseteq \mathbb{R}^+.
\]

Let

\[
e = e(v'/v) = [v'(k'^\times):v(k^\times)], \quad f = f(v'/v) = [f':f],
\]

where $[v'(k'^\times):v(k^\times)]$ is the group index and $[f':f]$ is the degree of the extension $f'/f$. $e$ and $f$ are called the ramification index and the residue degree of $v'/v$, respectively. They are either natural numbers $1, 2, 3, \ldots$, or $+\infty$.

The following proposition is a fundamental result on the extension of valuations.

**Proposition 1.1.** Let $v$ be a complete valuation of $k$ and let $k'$ be an algebraic extension of $k$. Then $v$ can be uniquely extended to a valuation $v'$ of $k'$: $v' \mid k = v$. If, in particular, $k'/k$ is a finite extension, then $v'$ is also complete, and

\[
v'(x') = \frac{1}{n} \cdot v(N_{k'/k}(x')) \quad \text{for all } x' \in k',
\]

where $n = [k':k]$ is the degree and $N_{k'/k}$ is the norm of the extension $k'/k$.

**Proof.** We refer the reader to van der Waerden [23].

**Corollary.** Let $k'/k$, $v$, and $v'$ be as stated above and let $\sigma$ be an automorphism of $k'$ over $k$. Then $v' \circ \sigma = v'$—that is,

\[
v'(\sigma(x')) = v'(x'), \quad \text{for all } x' \in k',
\]

so that

\[
v(\mathfrak{o}') = \mathfrak{o}', \quad \sigma(\mathfrak{p}') = \mathfrak{p}'.
\]

Hence $\sigma$ is a topological automorphism of $k'$ in the $v'$-topology, and it induces an automorphism $\sigma'$ of $f'$ over $f$:

\[
\sigma':f' \supseteq f'.
\]

**Proof.** The proof can easily be reduced to the special case where $k'/k$ is
Let \( v \) be a valuation of \( k \), not necessarily complete. It is well known that there exists an extension field \( k' \) of \( k \) and an extension \( v' \) of \( v \) on \( k' \) such that \( v' \) is complete and \( k \) is dense in \( k' \) in the \( v' \)-topology of \( k' \). Such a field \( k' \) is called a completion of \( k \) with respect to the valuation \( v \). More precisely, we also say that the pair \( (k', v') \) is a completion of the pair \( (k, v) \).

Let \( (k'', v'') \) be another completion of \( (k, v) \). Then there exists a \( k \)-isomorphism \( \sigma : k' \to k'' \) such that \( v' = v'' \circ \sigma \). Thus a completion is essentially unique, and hence \( (k', v') \) is often called the completion of \( (k, v) \). By the definition, each \( x' \) in \( k' \) is the limit of a sequence of points, \( x_1, x_2, \ldots, k \) in the \( v' \)-topology:

\[
x' = \lim_{n \to \infty} x_n.
\]

Then

\[
v'(x') = \lim_{n \to \infty} v'(x_n) = \lim_{n \to \infty} v(x_n).
\]

Hence if \( x' \neq 0 \), then \( v'(x') = v(x_n) \) for all sufficiently large \( n \). It follows that

\[
v'(k'^x) = v(k^x), \quad \mathfrak{t}' = \mathfrak{t},
\]

so that

\[
e(v'/v) = f(v'/v) = 1
\]

in this case. It is also clear that if \( (k', v') \) is a completion of \( (k, v) \) and if \( \mu = \alpha v \), \( \alpha > 0 \), then \( (k', \mu) \), with \( \mu' = \alpha v' \), is a completion of \( (k, \mu) \).

**Example 4.** Let \( K \) be an extension of \( k \) and let \( \mu \) be an extension of \( v \) on \( k \) to the extension field \( K : \mu \mid k = v \). Suppose that \( \mu \) is complete. Let \( k' \) denote the closure of \( k \) in \( K \) in the \( \mu \)-topology. Then \( k' \) is a subfield of \( K \), and \( (k', v') \), with \( v' = \mu \mid k' \), is a completion of \( (k, v) \).

To study a valuation \( v \) on a field \( k \), we often imbed \( (k, v) \) in its completion \( (k', v') \), investigate the complete valuation \( v' \), and then deduce from it the desired properties of \( v \). For example, in this manner we can deduce from Proposition 1.1 that if \( K \) is an algebraic extension of \( k \), then every valuation on \( k \) has at least one extension on \( K \).

### 1.2. Complete Fields

Let \( v \) be a valuation of a field \( k \). We say that \( k \) is a complete field with respect to \( v \), or, simply, that \( (k, v) \) is a complete field, if \( v \) is a complete, normalized valuation of \( k \).†

Let \( v \) be a normalized valuation of a field \( k \), not necessarily complete, and let \( (k', v') \) be the completion of \( (k, v) \). Then \( v'(k'^x) = v(k^x) = \mathbb{Z} \) by

† Some authors call a field a complete field if it is associated with a complete valuation, not necessarily normalized.
Section 1.1. Since $\nu'$ is complete, $(k',\nu')$ is a complete field. Many natural examples of complete fields are obtained in this manner.

**Example 5.** Let $p$ be a prime number and let $\nu_p$ be the $p$-adic valuation of the rational field $\mathbb{Q}$ in Example 2, Section 1.1. Since $\nu_p$ is a normalized valuation, the completion $(k',\nu')$ of $(\mathbb{Q},\nu_p)$ is a complete field. $k'$ is nothing but the classical $p$-adic number field $\mathbb{Q}_p$, and $\nu'$, often denoted again by $\nu_p$, is the standard $p$-adic valuation of $\mathbb{Q}_p$. For $(\mathbb{Q}_p, \nu_p)$, the valuation ring is the ring $\mathbb{Z}_p$ of $p$-adic integers and the maximal ideal is $p\mathbb{Z}_p$ so that the residue field is $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$, the prime field with $p$ elements. Note that $\nu_p(p) = 1$.

**Example 6.** Let $F$ be a field, $T$ an indeterminate, and $F((T))$ the set of all formal Laurent series of the form
\[ \sum_{-\infty < n} a_n T^n, \quad a_n \in F, \]
where $-\infty < n$ indicates that there are only a finite number of terms $a_n T^n$ with $n < 0$, $a_n \neq 0$. Then $k = F((T))$ is an extension field of $F$ in the usual addition and multiplication of Laurent series. Let $\nu(0) = +\infty$ and let $\nu(x) = i$ if
\[ x \neq 0, \quad x = \sum_{n=i}^{\infty} a_n T^n, \quad \text{with } a_i \neq 0. \]

Then one checks easily that $(k,\nu)$ is a complete field. The valuation ring is the ring $F[[T]]$ of all (integral) power series in $T$ over $F$, the maximal ideal is $TF[[x]]$, the residue field is $F[[T]]/TF[[T]] \cong F$, and $\nu(T) = 1$. The field $k$ contains the subfield $F(T)$ of all rational functions of $T$ with coefficients in $F$, and the restriction $\nu | F(T)$ is the normalized valuation of $F(T)$ in Example 3, Section 1.1. Furthermore, $(k,\nu)$ is the completion of $(F(T),\nu | F(T))$.

Now, let $(k,\nu)$ be any complete field and let $\mathfrak{o}$, $\mathfrak{p}$, and $\mathfrak{f} = \mathfrak{o}/\mathfrak{p}$ denote, respectively, the valuation ring, the maximal ideal, and the residue field of the valuation $\nu$. They are also called the valuation ring, and so on, of the complete field $(k,\nu)$. Since $\nu(k^\times) = \mathbb{Z}$, there exists an element $\pi$ in $k$ such that
\[ \nu(\pi) = 1. \]

Any such element $\pi$ is called a prime element of $(k,\nu)$. Fix $\pi$. Since $\mathfrak{p} = \{ x \in k \mid \nu(x) \geq 1 \}$ in this case,
\[ \mathfrak{p} = (\pi) = \mathfrak{o}\pi. \]
Hence, for any integer $n \geq 0$,
\[ \mathfrak{p}^n = (\pi^n) = \mathfrak{o}\pi^n = \{ x \in k \mid \nu(x) \geq n \}. \]

In general, let $\mathfrak{a}$ be an $\mathfrak{o}$-submodule of $k$, different from $\{0\}, k$. As $\mathfrak{a} \neq k$, the set $\{ \nu(x) \mid x \in \mathfrak{a}, x \neq 0 \}$ is bounded below in $\mathbb{Z}$, and if $n$ denotes the
minimum of the integers in this set, then
\[ \alpha = \{ x \in k \mid v(x) \geq n \} = \mathcal{O}\pi^n. \]

Such an \( \mathcal{O} \)-submodule \( \alpha \) of \( k \), \( \alpha \neq \{0\} \), \( k \), is called an ideal of \( (k, v) \). The set of all ideals of \( (k, v) \) forms an abelian group with respect to the usual multiplication of \( \mathcal{O} \)-submodules of \( k \). By the above, it is an infinite cyclic group generated by \( \mathfrak{p} \).

An ideal of \( (k, v) \), contained in \( \mathcal{O} \), is nothing but a non-zero ideal of the ring \( \mathcal{O} \) in the usual sense. Hence the sequence
\[ \{0\} \subset \cdots \subset \mathfrak{p}^n \subset \cdots \subset \mathfrak{p}^2 \subset \mathfrak{p} \subset \mathfrak{p}^0 = \mathcal{O} \]
gives us all ideals of the ring \( \mathcal{O} \). Since \( \mathfrak{p}^n = (\pi^n) \), \( \mathcal{O} \) is a principal ideal domain. Furthermore, in this case \( v(x) \geq n \Leftrightarrow v(x) > n - 1 \) for any \( n \in \mathbb{Z} \). Hence all the ideals \( \mathfrak{p}^n, n \geq 0 \), in (1.1) are at the same time open and closed in \( k \), and they form a base of open neighbourhoods of \( 0 \) in the \( v \)-topology of \( k \). Since \( \mathfrak{p}^n = (\pi^n) \neq \{0\} \), the field \( k \) is totally disconnected and non-discrete as a topological space.

Next, we consider the multiplicative group \( k^\times \) of \( k \). Let \( \langle \pi \rangle \) denote the cyclic subgroup of \( k^\times \), generated by a prime element \( \pi \). Then the isomorphism \( k^\times / U \cong v(k^\times) = \mathbb{Z} \) in Section 1.1 implies
\[ k = \langle \pi \rangle \times U, \quad \langle \pi \rangle \cong \mathbb{Z}. \]

Let \( U_0 = U \), \( U_n = 1 + \mathfrak{p}^n = \{ x \in \mathcal{O} \mid x \equiv 1 \mod \mathfrak{p}^n \} \), for \( n \geq 1 \), and let \( \mathfrak{t}^+ \) and \( \mathfrak{t}^\times \) denote the additive group and the multiplicative group of \( \mathfrak{t} = \mathcal{O}/\mathfrak{p} \), respectively. Then we have a sequence of subgroups of \( k^\times \):
\[ \{1\} \subset \cdots \subset U_n \subset \cdots \subset U_1 \subset U_0 = U \subset k^\times \]
such that
\[ U_0/U_1 \cong \mathfrak{t}^\times, \quad U_n/U_{n+1} \cong \mathfrak{t}^+, \quad \text{for } n \geq 1. \]

In fact, the canonical ring homomorphism \( \mathcal{O} \rightarrow \mathfrak{t} = \mathcal{O}/\mathfrak{p} \) induces a homomorphism of multiplicative groups, \( U \rightarrow \mathfrak{t}^\times \), which in turn induces \( U_0/U_1 \cong \mathfrak{t}^\times \). On the other hand, for \( n \geq 1 \), if we write an element of \( U_n = 1 + \mathfrak{p}^n = 1 + o\pi^n \) in the form \( 1 + x\pi^n \) with \( x \in \mathcal{O} \), then the map
\[ 1 + x\pi^n \mod U_{n+1} \mapsto x \mod \mathfrak{p} \]
defines an isomorphism \( U_n/U_{n+1} \cong \mathfrak{t}^+ \). The multiplicative group \( k^\times \) is a topological abelian group in the topology induced by the \( v \)-topology of \( k \). The groups \( U_n, n \geq 0 \), are open and closed subgroups of \( k^\times \) and they form a base of open neighbourhoods of \( 1 \) in the topological group \( k^\times \). Hence \( k^\times \) is again totally disconnected and non-discrete as a topological space.

So far we have not yet used the fact that \( v \) is a complete valuation of \( k \). But, now, this will be used in an essential manner. Let \( A \) be a complete set of representatives of the residue field \( \mathfrak{t} = \mathcal{O}/\mathfrak{p} \) in \( \mathcal{O} \)—that is, a subset of \( \mathcal{O} \) such that each residue class of \( \mathcal{O} \mod \mathfrak{p} \) contains a unique element in \( A \). We assume that \( A \) contains 0, namely, that 0 is the representative of \( \mathfrak{p} \) in \( A \). For
each $n \in \mathbb{Z}$, fix an element $\pi_n$ in $k$ such that

$$v(\pi_n) = n,$$

and consider an infinite sum of the form

$$\sum_{-\infty < n} a_n \pi_n,$$

where the $a_n$'s are elements of $A$ and the sum over $-\infty < n$ means the same as in Example 6 above. Since $v$ is complete and since $v(a_n \pi_n) = v(a_n) + v(\pi_n) \geq n$ so that $v(a_n \pi_n) \to +\infty$ as $n \to +\infty$, such an infinite sum always converges to an element in $k$.

**Proposition 1.2.** (i) Each $x$ in $k$ can be uniquely expressed in the form

$$x = \sum_{-\infty < n} a_n \pi_n, \quad \text{with } a_n \in A.$$

If $x \neq 0$ and if $a_i \neq 0$, $a_n = 0$ for all $n < i$, then

$$v(x) = i.$$

(ii) Let

$$x = \sum a_n \pi_n, \quad y = \sum b_n \pi_n, \quad a_n, b_n \in A.$$

Then, for any integer $i$,

$$v(x - y) \geq i \iff a_n = b_n \quad \text{for all } n < i.
$$

**Proof.** We first prove (ii). If $a_n = b_n$ for all $n$, then $x = y$, $v(x - y) = +\infty$, and statement (ii) is trivial. Hence, assume that there is an integer $m$ such that $a_m \neq b_m$, $a_n = b_n$ for all $n < m$. Then

$$x - y = \sum_{n=m}^{\infty} (a_n - b_n) \pi_n.$$

Since $a_m, b_m \in A$, $a_m \neq b_m$ implies $a_m \neq b_m \mod p$ so that

$$v(a_m - b_m) = 0, \quad v((a_m - b_m) \pi_m) = m.$$

Therefore, for $n > m$, $v((a_n - b_n) \pi_n) \geq v(\pi_n) = n > m = v((a_m - b_m) \pi_m)$, and it follows that

$$v(x - y) = v((a_m - b_m) \pi_m) = m.$$

Statement (ii) is then obvious. The argument also proves the uniqueness and the formula $v(x) = i$ in (i). Therefore, it only remains to show that each $x \in k$ can be expanded into an infinite series as in (i). We may assume that $x \neq 0$, $v(x) = i < +\infty$. Now, by the definition of $A$,

$$0 = A + p = \{a + p \mid a \in A\}.$$

Since $p^n = \{x \in k \mid v(x) \geq n\} = \omega \pi_n$ for $n \in \mathbb{Z}$, it follows that

$$p^n = A \pi_n + p^{n+1} = A \pi_n + A \pi_{n+1} + \cdots + A \pi_m + p^{m+1}, \quad \text{for all } m \geq n.$$
As \( x \in \mathfrak{p}^i \), we see that there exists a sequence of elements in \( A \), \( a_i, a_{i+1}, a_{i+2}, \ldots \), such that
\[
x \equiv \sum_{n=i}^{j} a_n \pi_n \mod \mathfrak{p}^{j+1}, \quad \text{for any } j \geq i.\]

It then follows that
\[
x = \lim_{j \to \infty} \sum_{n=i}^{j} a_n \pi_n = \sum_{n=i}^{\infty} a_n \pi_n.\]

Let \( A^\infty \) denote the set of all sequences \((a_0, a_1, a_2, \ldots)\), where \( a_n \) are taken arbitrarily from the set \( A \) defined above. Thus \( A^\infty \) is the set-theoretical direct product of the sets \( A_n = A \) for all \( n \geq 0 \):
\[
A^\infty = \prod_{n=0}^{\infty} A_n, \quad A_n = A.
\]

Introduce a topology on \( A^\infty \) as the direct product of discrete spaces \( A_n \), \( n \geq 0 \).

**Corollary of Proposition 1.2.** The map
\[
(a_0, a_1, a_2, \ldots) \mapsto \sum_{n=0}^{\infty} a_n \pi_n
\]
defines a homeomorphism of \( A^\infty \) onto the valuation ring \( \mathfrak{o} \) of \((k, \nu)\).

**Proof.** (i) shows that the map is bijective and (ii) implies that it is a homeomorphism.

Let \( \pi \) be a prime element of \( k : \nu(\pi) = 1 \). Then we may choose \( \pi^n \) as \( \pi_n \) in the above proposition. Hence we see that each \( x \in k \) can be uniquely expressed in the form
\[
x = \sum_{-\infty < n} a_n \pi^n, \quad \text{with } a_n \in A,
\]
and that if \( x \neq 0 \), \( a_i \neq 0 \), and \( a_n = 0 \) for \( n < i \), then
\[
\nu(x) = \nu\left(\sum_{n=i}^{\infty} a_n \pi^n\right) = i.
\]

It follows in particular that
\[
0 = \left\{ \sum_{n=0}^{\infty} a_n \pi^n \mid a_n \in A \right\}, \quad \mathfrak{p} = \left\{ \sum_{n=1}^{\infty} a_n \pi^n \mid a_n \in A \right\}.
\]

**Example 7.** Let \((k, \nu) = ( \mathbb{Q}_p, \nu_p)\) in Example 5. Then we may set
\[
A = \{0, 1, \ldots, p-1\}, \quad \pi = p
\]
so that each \( x \in 0 = \mathbb{Z}_p \); that is, each \( p \)-adic integer \( x \) can be uniquely
expressed in the form
\[ x = \sum_{n=0}^{\infty} a_n p^n, \quad a_n \in \mathbb{Z}, \quad 0 \leq a_n < p. \]

This is of course the well-known $p$-adic expansion of $x$. Next, let $(k, \nu)$ be the complete field in Example 6: $k = F((T))$. In this case, we may set
\[ A = F, \quad \pi = T. \]

For $x \in \mathfrak{o}$, the expansion
\[ x = \sum_{n=0}^{\infty} a_n T^n, \quad a_n \in A = F \]
mentioned above, is then nothing but the formal expression for $x$ as an element of the power series ring $\mathfrak{o} = F[[T]]$.

**Remark.** Let $k$ be a field with a non-trivial, discrete, complete valuation $\mu$ on it. Then $\mu$ is equivalent to a unique normalized valuation $\nu$ of $k: \mu \sim \nu$, and $\nu$ is again complete so that $(k, \nu)$ is a complete field. Since the valuation ring, the maximal ideal, the residue field, and so on, are the same for $\mu$ and $\nu$, to study a complete field is essentially the same as investigating a field $k$ with such a valuation $\mu$.

### 1.3. Finite Extensions of Complete Fields

A complete field $(k', \nu')$ is called an *extension* of a complete field $(k, \nu)$ if $k'$ is an extension field of $k$ and if the restriction of $\nu'$ on $k$ is equivalent to $\nu$:
\[ k \subseteq k', \quad \nu' | k \sim \nu. \]

In such a case, we shall also say that $(k', \nu')$ is a complete extension of $(k, \nu)$, or, in short, that $k' / k$ is an extension of complete fields.

Let $(k, \nu)$ and $(k', \nu')$ be as above and let
\[ \mu = \nu' | k, \quad e = e(\nu'/\mu), \quad f = f(\nu'/\mu). \]
e and $f$ are then denoted also by $e(k'/k)$ and $f(k'/k)$, respectively, and they are called the ramification index and the residue degree of the extension $k' / k$ of complete fields:
\[ e = e(k'/k) = e(\nu'/\mu), \quad f = f(k'/k) = f(\nu'/\mu). \]

Let $\mu = \alpha \nu$, $\alpha > 0$. Then $\mu(k^\times) = \alpha \nu(k^\times) = \alpha \mathbb{Z}$ so that
\[ e = [\nu'(k'^\times) : \mu(k^\times)] = [\mathbb{Z} : \alpha \mathbb{Z}] = \alpha. \]

Therefore
\[ \nu' | k = ev. \tag{1.5} \]

This characterizes $e = e(k'/k)$ and it also proves that
\[ e(k'/k) < +\infty. \]
Let \( \mathcal{O}_l = \mathcal{O}_l / \mathfrak{p} \) and \( \mathcal{O}_l' = \mathcal{O}_l'/\mathfrak{p}' \) be the residue fields of \((k, \nu)\) and \((k', \nu')\), respectively. Since \( \mu \sim \nu \), \( \mathcal{O}_l \) is also the residue field of \( \mu \) so that
\[
f = [\mathcal{O}_l' : \mathcal{O}_l].
\] (1.6)

In general, \( f(k'/k) \) is not finite. However, it is clear from (1.5) and (1.6) that if \((k'', \nu'')\) is a complete extension of \((k', \nu')\), then
\[
e(k''/k) = e(k''/k')e(k'/k), \quad f(k''/k) = f(k''/k')f(k'/k).
\] (1.7)

Now, with the notation introduced above, let \( \omega_1, \ldots, \omega_s \) be any finite number of elements in \( \mathcal{O}_l' \), which are linearly independent over \( \mathcal{O}_l \), and for each \( i, 1 \leq i \leq s \), choose an element \( \xi_i \) in \( \mathcal{O}_l' \) that belongs to the residue class \( \omega_i \) in \( \mathcal{O}_l = \mathcal{O}_l'/\mathfrak{p}' \). Fix a prime element \( \pi' \) of \( k' \) and let
\[
\eta_{ij} = \xi_i \pi'^j, \quad 1 \leq i \leq s, \quad 0 \leq j < e = e(k'/k).
\]

**Lemma 1.3.** (i) Let
\[
y' = \sum_{i=1}^{s} y_i \xi_i, \quad \text{with } y_i \in k.
\]
Then
\[
v'(y') = \min(ev(y_i), 1 \leq i \leq s)
\]
and \( \xi_1, \ldots, \xi_s \) are linearly independent over \( k \).

(ii) Let
\[
x' = \sum_{i,j} x_{ij} \eta_{ij}, \quad \text{with } x_{ij} \in k, \quad 1 \leq i \leq s, \quad 0 \leq j < e.
\]
Then
\[
v'(x') = \min(ev(x_{ij}) + j, 1 \leq i \leq s, 0 \leq j < e)
\]
and the elements \( \eta_{ij}, 1 \leq i \leq s, 0 \leq j < e, \) are linearly independent over \( k \).

**Proof.** (i) If \( y_1 = \cdots = y_s = 0 \), then \( y' = 0 \), and the statement is trivial. Hence, renumbering if necessary, let
\[
v(y_1) = \cdots = v(y_r) < v(y_i), \quad \text{for } r < i \leq s.
\]
Put \( z_i = y_i / y_1 \), \( 1 \leq i \leq s \). Then \( z_1 = 1, z_i \in \mathcal{O} \) for all \( i \), and
\[
y'/y_1 = \sum_{i=1}^{s} z_i \xi_i \in \mathcal{O}'.
\]
If \( y'/y_1 \in \mathfrak{p}' \), it would follow from the above that \( \omega_1 \) is a linear combination of \( \omega_2, \ldots, \omega_s \) with coefficients in \( \mathcal{O}_l = \mathcal{O}_l'/\mathfrak{p} \), contradicting the assumption that \( \omega_1, \ldots, \omega_s \) are linearly independent over \( \mathcal{O}_l \). Therefore, \( y'/y_1 \notin \mathfrak{p}' \)—that is, \( v'(y'/y_1) = 0 \)—and we have
\[
v'(y') = v'(y_i) = ev(y_i) = \min(ev(y_i), 1 \leq i \leq s).
\]
Assume now that \( \sum_{i=1}^{s} y_i \xi_i = 0 \) for some \( y_i \in k \). Then it follows from \( v'(0) = +\infty \) that \( v(y_i) = +\infty \)—that is, \( y_i = 0 \) for all \( i \). Hence \( \xi_1, \ldots, \xi_s \) are linearly independent over \( k \).
(ii) Let
\[ y_j = \sum_{i=1}^{s} x_{ij} \xi_i, \quad 0 \leq j < e \]
so that
\[ x' = \sum_{j=0}^{e-1} y_j \pi'^j. \]
By (i), if \( y_j \neq 0 \), then \( v'(y_j) \) is a multiple of \( e \) by (1.5) so that \( v'(y_j \pi'^j) \equiv j \mod e \). Hence the finite values in \( v'(y_0), \ldots, v'(y_{e-1}) \) are distinct, and it follows that
\[ v'(x') = \min(v'(y_j \pi'^j), 0 \leq j < e). \]
As \( v'(y_j) = \min(ev(x_{ij}), 1 \leq i \leq s) \), we obtain
\[ v'(x') = \min(ev(x_{ij}) + j, 1 \leq i \leq s, 0 \leq j < e). \]
The linear independence of \( \eta_{ij}, 1 \leq i \leq s, 0 \leq j < e \), can be proved similarly as that of \( \xi_1, \ldots, \xi_s \) in (i).

**Lemma 1.4.** Let \((k', v')\) be a complete extension of a complete field \((k, v)\). Assume that \( f(k'/k) \) is finite. Then \( k'/k \) is a finite extension and
\[ [k':k] = ef, \quad e = e(k'/k), \quad f = f(k'/k). \]

**Proof.** Let \( \omega_1, \ldots, \omega_f \) be a basis of \( \mathfrak{f}' \) over \( \mathfrak{f} \) and let \( \xi_i \in \mathcal{O}' \) be an element, taken from the residue class \( \omega_i \) in \( \mathfrak{f}' = \mathcal{O}' / \mathfrak{p}' \). As in Proposition 1.2, let \( A \) be a complete set of representatives of \( \mathfrak{f} = \mathcal{O} / \mathfrak{p} \) in \( \mathcal{O} \), containing 0, and let
\[ A' = \left\{ \sum_{i=1}^{f} a_i \xi_i \mid a_1, \ldots, a_f \in A \right\}. \]
Then \( A' \) is a complete set of representatives of \( \mathfrak{f}' = \mathcal{O}' / \mathfrak{p}' \) in \( \mathcal{O}' \). Fix a prime element \( \pi \) of \( k \) and a prime element \( \pi' \) of \( k' \): \( v(\pi) = v'(\pi') = 1 \). Writing each integer \( m \) in the form
\[ m = te + j, \quad t = 0, \pm 1, \pm 2, \ldots, \quad j = 0, 1, \ldots, e - 1, \]
we put
\[ \pi'_m = \pi' \pi'^j. \]
Since \( v' | k = ev \), we then have
\[ v'(\pi'_m) = et + j = m. \]
Hence we may apply Proposition 1.2 for \((k', v'), A', \) and \( \pi'_m \), and see that each \( x' \in k' \) can be uniquely written in the form
\[ x' = \sum_{-\infty < m} a'_m \pi'_m, \quad \text{with } a'_m \in A'. \]
Let
\[ a'_m = \sum_{i=1}^{f} a_{i,m} \xi_i, \quad a_{i,m} \in A. \]
Then
\[ x' = \sum_m \sum_{i=1}^f a_{i,m} \xi_i \pi_m = \sum_{i,j} x_{ij} \xi_i \pi^j, \quad 1 \leq i \leq f, \quad 0 \leq j < e, \]
where
\[ x_{ij} = \sum_{-\infty < t} a_{i,te+j} \pi^t \in k. \]

Thus every \( x' \) in \( k' \) is a linear combination of \( \eta_{ij} = \xi_i \pi^j, 1 \leq i \leq f, 0 \leq j < e \), with coefficients in \( k \). However, the elements \( \eta_{ij} \) are linearly independent over \( k \) by Lemma 1.3. Therefore, \( [k' : k] = ef < +\infty \). \( \blacksquare \)

With these lemmas, we are now able to prove the following

**Proposition 1.5.** Let \((k, \nu)\) be a complete field, and \( k' \) a finite extension of \( k \). Then there exists a unique normalized valuation \( \nu' \) on \( k' \) such that

\[ \nu' | k \sim \nu. \]

\((k', \nu')\) is then a complete extension of \((k, \nu)\) and

\[ [k' : k] = ef, \quad \text{for } e = e(k'/k), \quad f = f(k'/k), \]

\[ \nu'(x') = \frac{1}{f} \nu(N_{k'/k}(x')), \quad \text{for } x' \in k'. \]

**Proof.** By Proposition 1.1, there is a unique valuation \( \mu' \) on \( k' \) such that \( \mu' | k = \nu \). Furthermore, such a valuation \( \mu' \) is complete and it satisfies

\[ \mu'(x') = \frac{1}{n} \nu(N_{k'/k}(x')), \quad \text{for } x' \in k', \]

with \( n = [k' : k] \). Since \( \nu(k^\infty) = \mathbb{Z} \), it follows that

\[ \mu'(k^\infty) \subseteq \frac{1}{n} \mathbb{Z} \]

so that \( \mu' \) is discrete. Hence, there exists a unique normalized valuation \( \nu' \) on \( k' \) such that \( \nu' \sim \mu' \). It then follows that \( \nu' \) is the unique normalized valuation on \( k' \) such that \( \nu' | k \sim \nu \). As \( \mu' \) is complete, \( \nu' \) is also complete, and \((k', \nu')\) is a complete extension of \((k, \nu)\). Let \( \omega_1, \ldots, \omega_s \) be any finite number of elements in \( f' \) that are linearly independent over \( f \) and let \( \xi_i \) be an element in the residue class \( \omega_i, 1 \leq i \leq s, \) in \( t' = o'/p' \). Then, by Lemma 1.3, \( \xi_1, \ldots, \xi_s \) are linearly independent over \( k \) so that \( s \leq n = [k' : k] \). This implies that \( f = f(k'/k) = [f' : f] \leq n < +\infty \). Therefore, by Lemma 1.4, \( n = ef \).

Now, since \( \nu' \sim \mu' \)—that is, \( \nu' = \alpha \mu' \), \( \alpha > 0 \)—we have

\[ \nu'(x') = \beta \nu(N_{k'/k}(x')), \quad \text{for } x' \in k', \]

with \( \beta = \alpha/n > 0 \). For \( x \in k \), this implies

\[ \nu'(x) = \beta \nu(x^n) = \beta n \nu(x). \]
However, \( v'(x) = ev(x) \) by (1.5). As \( n = ef \), it follows that \( \beta = 1/f \) so that

\[
v'(x') = \frac{1}{f} v(N_{k'/k}(x')) \quad \text{for } x' \in k'.
\]

Now, let \( \{ \alpha_1, \ldots, \alpha_n \} \) denote the elements

\[
\eta_{ij} = \xi_i \pi^{ij}, \quad 1 \leq i \leq f, \quad 0 \leq j < e
\]

in Lemma 1.3, arranged in some order. In the proof of Lemma 1.4, we saw that \( ef = [k':k] = n \) and that \( \{ \alpha_1, \ldots, \alpha_n \} \) is a basis of \( k' \) over \( k \). Let

\[
x' = \sum_{i=1}^{n} x_i \alpha_i, \quad x_i \in k.
\]

Then it follows from Lemma 1.3 (ii) that for any integer \( r \),

\[
v'(x') = v(x_i) \quad \text{for } i = 1, \ldots, n.
\]

For \( r = 0 \), this means that \( \{ \alpha_1, \ldots, \alpha_n \} \) is a free basis of the \( \mathfrak{o}-\)module \( \mathfrak{o}' : \mathfrak{o}' = \mathfrak{o} \alpha_1 \oplus \cdots \oplus \mathfrak{o} \alpha_n \). Let \( k^n \) (resp. \( \mathfrak{o}^n \)) denote the direct sum of \( n \) copies of \( k \) (resp. \( \mathfrak{o} \)) and let \( k^n \) be given the product topology of the \( v \)-topology on \( k \). The above equivalence then shows that the \( k \)-linear map

\[
k^n \to k',
\]

\[
(x_1, \ldots, x_n) \mapsto x' = \sum_{i=1}^{n} x_i \alpha_i,
\]

is a topological isomorphism and it induces a topological \( \mathfrak{o} \)-isomorphism

\[
\mathfrak{o}^n \to \mathfrak{o}' = \mathfrak{o} \alpha_1 \oplus \cdots \oplus \mathfrak{o} \alpha_n.
\]

Let \( (k, v) \) and \( (k', v') \) be the same as in Proposition 1.5, and let \( \mathfrak{o} \) and \( \mathfrak{o}' \) be their valuation rings. Then the trace map and the norm map of the finite extension \( k'/k \):

\[
T_{k'/k} : k' \to k, \quad N_{k'/k} : k' \to k,
\]

are continuous in the \( v \)-topology of \( k \) and the \( v' \)-topology of \( k' \), and

\[
T_{k'/k}(\mathfrak{o}') \subseteq \mathfrak{o}, \quad N_{k'/k}(\mathfrak{o}') \subseteq \mathfrak{o}.
\]

Proof. Let \( x' \in k' \) and let

\[
x' \alpha_i = \sum_{j=1}^{n} x_{ij} \alpha_j, \quad x_{ij} \in k,
\]

for the basis \( \{ \alpha_1, \ldots, \alpha_n \} \) stated above. Then \( x_{ij} \) depends continuously on \( x' \in k' \). Since \( T_{k'/k}(x') \) and \( N_{k'/k}(x') \) are the trace and the determinant of the \( n \times n \) matrix \( (x_{ij}) \), respectively, the first half is proved. If \( x' \in \mathfrak{o}' \), then \( x_{ij} \in \mathfrak{o} \) for all \( i, j \) by (1.8). Therefore, the second half is also clear.

Now, let \( \mathfrak{a}' \) be an ideal of \( (k', v') \)—that is, an \( \mathfrak{o}' \)-submodule of \( k' \) different from \( \{0\}, k' \) (cf. Section 1.2). We define the norm \( N_{k'/k}(\mathfrak{a}') \) of
\( \alpha' \) to be the \( \mathfrak{o} \)-submodule of \( k \) generated by \( N_{k'/k}(x') \) for all \( x' \in \alpha' \). Then \( N_{k'/k}(\alpha') \) is an ideal of \( (k, \nu) \) and it follows from the formula for \( \nu'(x') \) in Proposition 1.5 that if \( \alpha' = \mathfrak{p}^m, \ m \in \mathbb{Z} \), then

\[
N_{k'/k}(\alpha') = \mathfrak{p}^m, \quad \text{with } f = f(k'/k).
\]

Hence, in particular,

\[
N_{k'/k}(\mathfrak{o}') = \mathfrak{o}, \quad N_{k'/k}(\mathfrak{p}') = \mathfrak{p}^f.
\]
Chapter II
Local Fields

A complete field, defined in Section 1.2, is called a *local field* when its residue field is a finite field. In this chapter, we shall discuss some preliminary basic results on such local fields.

2.1. General Properties

Let \((k, v)\) be a local field. By the definition, \((k, v)\) is a complete field and its residue field \(\mathfrak{f} = o/p\) is a finite field. Let \(q\) be the number of elements in \(\mathfrak{f}\)—that is,

\[
\mathfrak{f} = \mathbb{F}_q,
\]

\(\mathbb{F}_q\) denoting, in general, a finite field with \(q\) elements. When \(\mathfrak{f}\) is a field of characteristic \(p\)—namely, when \(q\) is a power of a prime number \(p\)—the local field \((k, v)\) is called a *p-field*. This happens if and only if

\[p \circ 1_k \leq p, \text{ that is, } v(p \cdot 1_k) > 0\]

where \(1_k\) denotes the identity element of the field \(k\). Hence it follows that if \((k, v)\) is a p-field, then the characteristic of the field \(k\) is either 0 or \(p\).

**Example 1.** Let \(\mathbb{Q}_p\) be the \(p\)-adic number field, and \(v_p\) the \(p\)-adic valuation on \(\mathbb{Q}_p\) (cf. Example 5, Section 1.2). Then \((\mathbb{Q}_p, v_p)\) is a complete field and its residue field is

\[
\mathfrak{f} = o/p = \mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p.
\]

Hence \((\mathbb{Q}_p, v_p)\) is a p-field of characteristic 0. On the other hand, let \(F\) be any finite field of characteristic \(p\); for example, \(F = \mathbb{F}_p\). Let \(k = F((T))\) be the field of formal Laurent series in \(T\) with coefficients in \(F\), and let \(v_T\) be the standard valuation of \(k\) (cf. Example 6, Section 1.2). Then \((k, v_T)\) is a complete field and its residue field is

\[
\mathfrak{f} = o/p = F[[T]]/TF[[T]] = F.
\]

Therefore \((k, v_T)\) is a p-field of characteristic \(p\).

**Example 2.** Let \(k\) be a finite algebraic number field—that is, a finite extension of the rational field \(\mathbb{Q}\)—and let \(o\) denote the ring of all algebraic integers in \(k\). It is known that each maximal ideal \(m\) of \(o\) defines a normalized valuation \(v\) of \(k\) with finite residue field. Hence the completion \((k', v')\) of \((k, v)\) is a local field. In fact, if \(p\) is the prime number contained in \(m\), then \((k', v')\) is a p-field. \((\mathbb{Q}_p, v_p)\) in Example 1 is a special case of such \((k', v')\) for \(k = \mathbb{Q}, m = p\mathbb{Z}\). Application of the theory of local fields for algebraic number fields is based on this fact. Compare Lang [17].
**Proposition 2.1.** Let \((k, v)\) be a local field. Then \(k\) is a non-discrete, totally disconnected, locally compact field in its \(v\)-topology. The valuation ring \(\mathfrak{o}(=v^0)\) and the ideals \(p^n\) of \(\mathfrak{o}\), \(n \geq 1\), are open, compact subgroups of the additive group of the field \(k\), and they form a base of open neighborhoods of \(0\) in \(k\). Furthermore, \(\mathfrak{o}\) is the unique maximal compact subring of \(k\).

**Proof.** Let \(A\) be a complete set of representatives of \(f = \mathfrak{o}/p\) in \(\mathfrak{o}\), containing \(0\) (cf. Section 1.2). Since \(f\) is a finite field, \(A\) is a finite set. Hence the set \(A = \prod_{n=0}^{\infty} A_n\), \(A_n = A\), in the Corollary of Proposition 1.2 is a compact set as a direct product of finite sets \(A_n\), \(n \geq 0\). Therefore, by the same Corollary, \(\mathfrak{o}\) is compact in the \(v\)-topology. We already stated in Section 1.2 that each \(p^n\), \(n \geq 0\), is at the same time open and closed in \(k\) and that the \(p^n\)'s in (1.1) gives us a base of open neighbourhoods of \(0\) in \(k\) so that \(k\) is a non-discrete, totally disconnected topological field. Since \(\mathfrak{o}\) is compact, \(k\) is locally compact, and since \(p^n\) is closed in \(\mathfrak{o}\), \(p^n\) is also compact. Let \(R\) be any compact subring of \(k\). Then the compactness implies that the set \(\{v(x) \mid x \in R\}\) is bounded below in the real field \(\mathbb{R}\). If \(x \in R\), then \(x^n \in R\) and \(v(x^n) = nv(x)\) for all \(n \geq 1\). Hence, by the above remark, \(v(x) \geq 0\)—that is, \(x \in \mathfrak{o}\). This proves that \(R \subseteq \mathfrak{o}\) so that \(\mathfrak{o}\) is the unique maximal compact subring of the field \(k\).

It is known that if \(k\) is a non-discrete locally compact field, then \(k\) is either the real field \(\mathbb{R}\), the complex field \(\mathbb{C}\), or a local field in its \(v\)-topology.† Thus, as a topological field, a local field is characterized by the property that it is locally compact, but is neither discrete nor connected.

Now, let \(\pi\) be a prime element of a local field \((k, v)\): \(v(\pi) = 1\). Since \(p^n = \mathfrak{o} \pi^n\), \(n \geq 0\), the map \(x \mapsto x \pi^n\), \(x \in \mathfrak{o}\), induces an isomorphism of \(\mathfrak{o}\)-modules:

\[
\mathfrak{o}/p \cong p^n/p^{n+1}, \quad \text{for } n \geq 0.
\]

Since \(f = \mathbb{F}_q\), \([\mathfrak{o}:p] = q\), it follows that

\[
[\mathfrak{o}:p^n] = q^n, \quad \text{for } n \geq 0.
\]

Thus \(\mathfrak{o}/p^n\) is a finite ring with \(q^n\) elements. Since \(\mathfrak{o}\) is compact and the intersection of all \(p^n\), \(n \geq 0\), is \(0\), we see that

\[
\mathfrak{o} = \lim_{\leftarrow} \mathfrak{o}/p^n,
\]

where the inverse limit is taken with respect to the canonical maps \(\mathfrak{o}/p^m \rightarrow \mathfrak{o}/p^n\) for all \(m \geq n \geq 0\). Therefore, if \((k, v)\) is a \(p\)-field so that \(q\) is a power of \(p\), then the additive group of \(\mathfrak{o}\) is an abelian pro-\(p\)-group—that is, an inverse limit of a family of finite abelian \(p\)-groups (cf. Section 2.2).

For the proof of the next proposition, we first prove the following

**Lemma 2.2.** Let \(f = \mathfrak{o}/p = \mathbb{F}_q\) for a \(p\)-field \((k, v)\). Then, for each \(x \in \mathfrak{o}\), the

† Compare Weil [24]. Note that a local field in that book is, by definition, a non-discrete locally compact field.
Local Class Field Theory

\[ \omega(x) = \lim_{n \to \infty} x^{q^n} \]

exists in \( \mathfrak{m} \), and the map \( \omega : \mathfrak{m} \to \mathfrak{m} \) has the following properties:

\[ \omega(x) = x \mod \mathfrak{p}, \quad \omega(x)^q = \omega(x), \quad \omega(xy) = \omega(x)\omega(y). \]

**Proof.** By induction, we shall prove the congruences

\[ x^{q^n} \equiv x^{q^{n-1}} \mod \mathfrak{p}^n \]

for all \( n \geq 1 \). For \( n = 1 \), \( x^q \equiv x \mod \mathfrak{p} \) follows from the fact that \( \mathfrak{m} = \mathfrak{m}/\mathfrak{p} \) is a finite field with \( q \) elements. Assume the congruence for \( n \geq 1 \) so that \( x^{q^n} = x^{q^{n-1}} + y \) with \( y \in \mathfrak{p}^n \). Then

\[ x^{q^{n+1}} = \sum_{i=0}^{q} \binom{q}{i} x^{iq^{n-1}} y^{q^{-i}}. \]

For \( 0 < i < q \), the integer

\[ \binom{q}{i} = \frac{q}{i} \frac{(q-1)}{i-1} \]

is divisible by \( p \) so that \( (q)^{q^{-i}} \) is contained in \( \mathfrak{p}^{n+1} \). Since the same is obviously true for \( i = 0 \), we obtain

\[ x^{q^{n+1}} \equiv x^{q^n} \mod \mathfrak{p}^{n+1}. \]

Now, we see from these congruences that \( \{x^{q^n}\}_{n \geq 1} \) is a Cauchy sequence in \( \mathfrak{m} \) in the \( \nu\)-topology. As \( \nu \) is complete and \( \mathfrak{m} \) is closed in \( k \), the sequence converges to an element \( \omega(x) \) in \( \mathfrak{m} \). It is clear that the congruences yield \( x^{q^n} \equiv x \mod \mathfrak{p} \) for all \( n \geq 1 \). Hence \( \omega(x) \equiv x \mod \mathfrak{p} \). We also see

\[ \omega(x)^q = \lim_{n \to \infty} x^{q^{n+1}} = \omega(x), \quad \omega(xy) = \lim_{n \to \infty} x^q y^q = \omega(x)\omega(y). \]

**Proposition 2.3.** Let \( (k, \nu) \) be as stated above and let

\[ V = \{ x \in k \mid x^{q-1} = 1 \}, \quad A = V \cup \{ 0 \} = \{ x \in k \mid x^q = x \}. \]

Then \( A \) is a complete set of representatives of \( \mathfrak{m} = \mathfrak{m}/\mathfrak{p} \) in \( \mathfrak{m} \), containing \( 0 \); \( V \) is the set of all \((q-1)\)st roots of unity in \( k \); and the canonical ring homomorphism \( \mathfrak{m} \to \mathfrak{m}/\mathfrak{p} \) induces an isomorphism of multiplicative groups:

\[ V \cong \mathfrak{m}^\times. \]

In particular, \( V \) is a cyclic group of order \( q - 1 \).

**Proof.** Let \( A' = \{ \omega(x) \mid x \in \mathfrak{m} \} \). As \( \omega(x) \equiv x \mod \mathfrak{p} \), each residue class of \( \mathfrak{m} \mod \mathfrak{p} \) contains at least one element in \( A' \), and as \( \omega(x)^q = \omega(x) \), \( A' \) is a subset of \( A \). However, the number of elements \( x \) in \( k \) satisfying \( x^q - x = 0 \) is at most \( q \), while the number of elements in \( \mathfrak{m} = \mathfrak{m}/\mathfrak{p} \) is \( q \). Hence \( A = A' \) and
A is a complete set of representatives of \( f = \mathbb{O}/p \) in \( \mathbb{O} \). Obviously, \( 0 = \omega(0) \in A \). Since \( \omega(xy) = \omega(x)\omega(y) \), the other statements on \( V \) are clear.

**Remark.** This proposition is also an easy consequence of the well-known Hensel's Lemma.†

**Proposition 2.4.** Let \((k, v)\) be a \( p \)-field of characteristic \( 0: \mathbb{Q} \subseteq k \). Let \( e = v(p) \), where \( p = p \cdot 1_k \) and let \( f = \mathbb{F}_q, q = p' \), for the residue field \( f = \mathbb{O}/p \). Then \((k, v)\) is a complete extension of the \( p \)-adic number field \((\mathbb{Q}_p, v_p)\), and

\[
[k: \mathbb{Q}_p] = ef < +\infty.
\]

Furthermore, the valuation ring \( \mathbb{O} \) of \((k, v)\) is a free \( \mathbb{Z}_p \)-module of rank \( ef = [k: \mathbb{Q}_p] \).

**Proof.** Let \( \lambda = v| \mathbb{Q} \). Since \((k, v)\) is a \( p \)-field and \( p = p \cdot 1_k \neq 0 \),

\[
0 < \lambda(p) = v(p) < +\infty.
\]

However, it is known that such a valuation \( \lambda \) on \( \mathbb{Q} \) is equivalent to the \( p \)-adic valuation \( v_p \) of \( \mathbb{Q} \) (cf. the remark in Example 2, Section 1.1.). Let \( k' \) denote the closure of \( \mathbb{Q} \) in \( k \). As \((k, v)\) is complete, \( (k', v | k') \) is a completion of \((\mathbb{Q}, \lambda)\) (cf. Example 4, Section 1.1). It then follows from \( \lambda \sim v_p \) that \( k' = \mathbb{Q}_p \) and \( v | \mathbb{Q}_p \sim v_p \). Hence \((k, v)\) is a complete extension of \((\mathbb{Q}_p, v_p)\) in the sense of Section 1.3. Since \( v_p(p) = 1, v(p) = e, \) and \( v | \mathbb{Q}_p = e(k/\mathbb{Q}_p)v_p \), we obtain \( e(k/\mathbb{Q}_p) = e \). On the other hand, \( f = \mathbb{F}_q, q = p' \), and \( Z_p/pZ_p = \mathbb{F}_p \) imply \( f(k/\mathbb{Q}_p) = f < +\infty \). Therefore, \([k: \mathbb{Q}_p] = ef \) by Proposition 1.4. That \( \mathbb{O} \) is a free \( \mathbb{Z}_p \)-module of rank \( ef \) is a special case of (1.8) in Section 1.4.

**Proposition 2.5.** Let \((k, v)\) be a \( p \)-field of characteristic \( p \) with \( f = \mathbb{O}/p = \mathbb{F}_q \) and let \((\mathbb{F}_q((T)), v_T)\) denote the \( p \)-field of Laurent series in \( T \) stated in Example 1. Then \( k \) contains \( \mathbb{F}_q \) as a subfield and there exists an \( \mathbb{F}_q \)-isomorphism

\[
(k, v) \simeq (\mathbb{F}_q((T)), v_T),
\]

namely, an \( \mathbb{F}_q \)-isomorphism \( k \simeq \mathbb{F}_q((T)) \), which transfers the valuation \( v \) of \( k \) to the valuation \( v_T \) of \( \mathbb{F}_q((T)) \).

**Proof.** Since \( k \) is a field of characteristic \( p \), the set \( A = \{x \in k \mid x^q = x\} \) in Proposition 2.3 is a subfield of \( k \) with \( q \) elements. Then \( \mathbb{F}_q = A \subseteq k \). Now, fix a prime element \( \pi \) of \( k \) and apply Proposition 1.2 for \( A = \mathbb{F}_q \) and \( \pi_n = \pi^n, n \in \mathbb{Z} \). We then see that the map

\[
\sum_n a_n \pi^n \mapsto \sum_n a_n T^n, \quad a_n \in \mathbb{F}_q,
\]

defines an \( \mathbb{F}_q \)-isomorphism \((k, v) \simeq (\mathbb{F}_q((T)), v_T)\).

† Compare van der Waerden [23].
2.2. The Multiplicative Group $k^\times$

Let $(k, \nu)$ be again a $p$-field with residue field $f = o/p = F_q$. We shall next study the multiplicative group $k^\times$ of the field $k$.

**Proposition 2.6.** The group $k^\times$ is a non-discrete, totally disconnected, locally compact abelian group in the topology induced by the $\nu$-topology of $k$. The unit group $U (=U_0)$ and its subgroups $U_n = 1 + \nu^n$, $n \geq 1$, are open, compact subgroups of $k^\times$, and they form a base of open neighbourhoods of 1 in $k^\times$. Furthermore, $U$ is the unique maximal compact subgroup of $k^\times$.

**Proof.** By Proposition 2.1, $U_n = 1 + \nu^n$, $n \geq 1$, are open, compact subgroups of $k^\times$. Since $U/U_1 \cong \mathbb{F}_q$ by (1.3), $U/U_1$ is a finite group. Hence $U$ is also an open, compact subgroup of $k^\times$. That $U$ is the unique maximal compact subgroup of $k^\times$ can be proved similarly as the fact that $o$ is the unique maximal compact subring of $k$. The rest of the proposition is clear from what we mentioned in Section 1.2.

Now, let $\tau$ be a prime element of $(k, \nu)$. By Section 1.2, we have

$$k^\times = \langle \tau \rangle \times U, \quad \langle \tau \rangle = \mathbb{Z},$$

$$U/U_1 \cong \mathbb{F}_q, \quad U_n/U_{n+1} \cong \mathbb{F}_q^\times, \quad \text{for } n \geq 1.$$ 

Since $f = F_q$, it follows that

$$[U:U_1] = q - 1, \quad [U_n:U_{n+1}] = q$$

so that

$$[U:U_n] = (q - 1)q^{n-1}, \quad [U_1:U_n] = q^{n-1}, \quad \text{for } n \geq 1. \quad (2.1)$$

We also know that the canonical ring homomorphism $\nu \to f = o/p$ induces the isomorphism $U/U_1 \cong \mathbb{F}_q^\times$. However, by Proposition 2.3, the same ring homomorphism induces $V \cong \mathbb{F}_q^\times$, where $V = \{x \in k \mid x^{q-1} = 1\}$ is a subgroup of $U = \{x \in k \mid \nu(x) = 0\}$. Hence we obtain

$$U = V \times U_1, \quad k^\times = \langle \pi \rangle \times V \times U_1, \quad (2.2)$$

where $\langle \pi \rangle = \mathbb{Z}$, $V = \mathbb{Z}/(q - 1)\mathbb{Z}$. Therefore, the structure of the abelian group $k^\times$ will be completely known if we can determine the structure of $U_1$.

In general, let $G$ be a finite abelian $p$-group. Then $G$ can be regarded as a module over $\mathbb{Z}/p^n\mathbb{Z}$ whenever $n$ is sufficiently large. As $\mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p/p^n\mathbb{Z}_p$, we see that we can canonically define a structure of $\mathbb{Z}_p$-module on such a group $G$. Let $G$, now, be an abelian pro-$p$-group—that is,

$$G = \lim \leftarrow G_i,$$

where $\{G_i\}$ is a family of finite abelian $p$-groups. Since every $G_i$ is a $\mathbb{Z}_p$-module in the natural manner, the inverse limit $G$ can also be made into a $\mathbb{Z}_p$-module, and one checks easily that the structure of $\mathbb{Z}_p$-module on $G$ thus defined is independent of the way $G$ is expressed as an inverse limit of
finite abelian $p$-groups. In short, each abelian pro-$p$-group $G$ is a $\mathbb{Z}_p$-module in a canonical manner.

Now, just as $\mathfrak{o}$ is the inverse limit of $\mathfrak{o}/\mathfrak{o}^n$, $n \geq 0$, the compact group $U_1$ is the inverse limit of finite abelian $p$-groups $U_1/U_n$ with respect to the canonical maps $U_1/U_m \to U_1/U_n$ for $m \geq n \geq 0$:

$$U_1 = \lim_{\leftarrow} U_1/U_n.$$ 

Thus $U_1$ is a $\mathbb{Z}_p$-module by the above remark, and one also sees that the $U_n$, $n \geq 1$, are $\mathbb{Z}_p$-submodules of $U_1$. We shall next study the structure of the $\mathbb{Z}_p$-module $U_1$.

Let $(k, v)$ be a $p$-field of characteristic 0. By Proposition 2.4, $k$ is a finite extension of the $p$-adic number field $\mathbb{Q}_p$ and its degree $d = [k: \mathbb{Q}_p]$ is given by

$$d = ef,$$

where $e = e(k/\mathbb{Q}_p) = v(p)$, and where $f = f(k/\mathbb{Q}_p)$ is the exponent of $q = p^f$. Let

$$W = \text{the set of all roots of unity with p-power orders in } k.$$ 

Since (2.2) induces $k^\times/U_1 \cong \mathbb{Z} \oplus \mathbb{Z}/(q - 1)\mathbb{Z}$, we see that $W$ is a subgroup of $U_1$; in fact, $W$ is the torsion submodule of the $\mathbb{Z}_p$-module $U_1$.

**Proposition 2.7.** Let $(k, v)$ be a $p$-field of characteristic 0 and let $W$ be the group of all $p$-power roots of unity in $k$. Then $W$ is a finite cyclic subgroup of $U_1 = 1 + p$ and $U_1/W$ is a free $\mathbb{Z}_p$-module of rank $d = [k: \mathbb{Q}_p]:$

$$U_1/W \cong \mathbb{Z}_p^d, \quad U_1 = W \oplus \mathbb{Z}_p^d, \quad W = \mathbb{Z}/p^a \mathbb{Z}, \quad a \geq 0.$$ 

**Proof.** Let $n > e = v(p)$ and let $U_n^p = \{x^p \mid x \in U_n\}$. ($U_n^p$ is not the direct sum of $p$-copies of $U_n$.) $U_n^p$ is the image of the compact group $U_n$ under the continuous endomorphism $x \mapsto x^p$ so that it is a compact subgroup of $U_n$. Now, since $n > e$,

$$U_n^p = (1 + p^n)^p \equiv 1 + p^np^n \mod p^{2n},$$ 

where $p^np^n = p^{n+e}$, $p^{2n} \equiv p^{n+e+1}$. Hence we have

$$U_{n+e} = U_n^p U_{n+e+1}.$$ 

As this holds for any $n > e$, we also obtain

$$U_{n+e} = U_n^p U_m, \quad \text{for all } m \geq n + e + 1.$$ 

This shows that $U_{n+e}$ is the closure of the compact subgroup $U_n^p$ of $U_n$ so that

$$U_{n+e} = U_n^p, \quad \text{for } n \geq e,$$

and it follows that

$$[U_n : U_n^p] = [U_n : U_{n+e}] = q^e = p^{ef} = p^d.$$
Local Class Field Theory

In general, it is easy to see (the proof is left to the reader as an exercise) that if $A$ is a compact $\mathbb{Z}_p$-module (in additive notation) such that $A/pA$ is finite, then $A$ is finitely generated over $\mathbb{Z}_p$. Since

$$[U_1 : U_n^p] \leq [U_1 : U_n^p] = [U_1 : U_n][U_n : U_n^p] < +\infty,$$

$U_1$ is finitely generated over $\mathbb{Z}_p$. Hence its torsion submodule $W$ is finite. Furthermore, as a finite subgroup of the multiplicative group $k^\times$ of the field $k$, $W$ is also cyclic. Now, choose $n > e$ large enough so that $W \cap U_n = 1$. By the structure theorem for finitely generated $\mathbb{Z}_p$-modules, we see from $[U_n : U_n^p] = p^d$, $[U_1 : U_n] < +\infty$ that $U_1/W \simeq \mathbb{Z}_p^d$, $U_1 = W \oplus \mathbb{Z}_p^d$.

**Corollary.** For a $p$-field $(k, \nu)$ of characteristic 0,

$$k^\times = \langle \pi \rangle \times U = \langle \pi \rangle \times V \times U_1 = \langle \pi \rangle \times V \times W \times U'$$

$$= \mathbb{Z} \oplus \mathbb{Z}/(q - 1)\mathbb{Z} \oplus \mathbb{Z}/p^a\mathbb{Z}_p \oplus \mathbb{Z}_p^d, \quad a \geq 0, \quad d = [k : \mathbb{Q}_p].$$

Hence $V \times W$ is the group of all roots of unity in $k$ and it is a finite cyclic group of order $(q - 1)p^a$.

**Remark.** The proposition can be proved also by using the $p$-adic logarithm for $k$:†

$$\log(1 + x) = x - \frac{x^2}{2} + \frac{x^3}{3} + \cdots, \quad x \in \mathfrak{p}.$$ 

We now consider the $\mathbb{Z}_p$-module $U_1 = U_1(k)$ for a $p$-field $(k, \nu)$ of characteristic $p$. By Proposition 2.5, we may assume that

$$k = \mathbf{F}_q((T)), \quad U_1 = 1 + \mathfrak{p} = 1 + T \mathbf{F}_q[[T]]$$

where $q = p^f$, $f = [\mathbf{F}_q : \mathbf{F}_p] \geq 1$. Let $\{\omega_1, \ldots, \omega_f\}$ be a basis of $\mathbf{F}_q$ over the prime field $\mathbf{F}_p$. For each integer $n \geq 1$, prime to $p$, let $A_n$ denote the direct product of $f$ copies of $\mathbb{Z}_p$. Take any element $\alpha$ in $A_n$: $\alpha = (a_1, \ldots, a_f)$, $a_i \in \mathbb{Z}_p$. We define an element $g_n(\alpha)$ in $U_1 = 1 + \mathfrak{p}^n$ by

$$g_n(\alpha) = \prod_{i=1}^{f} (1 + \omega_i T^n)^{a_i}.$$ 

Let $b_i \in \mathbb{Z}$, $a_i = b_i \mod p\mathbb{Z}_p$ for $1 \leq i \leq f$ and let $\omega = \sum_{i=1}^{f} b_i \omega_i \in \mathbf{F}_q$. Then

$$g_n(\alpha) = \prod_{i=1}^{f} (1 + \omega_i T^n)^{b_i} = 1 + \omega T^n \mod \mathfrak{p}^{n+1}.$$ 

Let $m = np^s$, $s \in \mathbb{Z}$, $s \geq 0$. Since $k$ is a field of characteristic $p$, we have

$$g_n(p^s \alpha) = g_n(\alpha)^{p^s} = 1 + \omega T^m \mod \mathfrak{p}^{n+1}.$$ 

When $\alpha$ ranges over all elements of $A_n$, $\omega$ and, hence, $\omega T^m$ run over all elements of $\mathbf{F}_q$. Therefore, we see from the above that

$$U_m = g_n(p^s A_n)U_{m+1}, \quad \text{for } m = np^s. \quad (2.3)$$

† See Lang [17], Chapter IX.
Note also that \( g_n(p^r \alpha) \equiv 1 \mod p^{m+1} \iff \omega = 0 \iff b_i \equiv 0 \mod p, \ 1 \leq i \leq f \iff a_i \equiv 0 \mod pZ_p, \ 1 \leq i \leq f \iff \alpha \in pA_n. \) Thus
\[
\alpha \notin pA_n \iff g_n(p^r \alpha) \notin U_{m+1}, \quad \text{for } m = np^s.
\] (2.4)

**Proposition 2.8.** Let \((k, \nu)\) be a \(p\)-field of characteristic \(p\). Then the \(\mathbb{Z}_p\)-module \(U_1 = U_1(k)\) is topologically isomorphic to the direct product of countably infinite copies of \(\mathbb{Z}_p\).

**Proof.** Keeping the notation introduced above, let \(A\) be the direct product of the \(\mathbb{Z}_p\)-modules \(A_n\) for all integers \(n \geq 1\), prime to \(p\):
\[
A = \prod_n A_n.
\]
\(A\) is a compact \(\mathbb{Z}_p\)-module in an obvious manner. We define a map \(g: A \to U_1\) by
\[
g(\xi) = \prod_n g_n(\alpha_n), \quad \text{for } \xi = (\ldots, \alpha_n, \ldots) \in A, \quad \alpha_n \in A_n.
\]
Since \(g_n(\alpha_n) \in U_n\), the product on the right converges in \(U_1\) and \(g\) defines a continuous \(\mathbb{Z}_p\)-homomorphism. Let \(m\) be any positive integer and let \(m = np^s\), \((n, p) = 1, s \geq 0\). Since \(g_n(A_n) \subseteq g(A)\), it follows from (2.3) that each coset of \(U_m/U_{m+1}\) is represented by an element of \(g(A)\). Hence \(g(A)\) is dense in \(U_1\). However, as \(A\) is compact and \(g\) is continuous, \(g(A)\) is compact, hence closed, in \(U_1\). Therefore, \(g(A) = U_1\)—that is, \(g\) is surjective.

Next, let \(\xi = (\ldots, \alpha_n, \ldots) \in A, \ \xi \neq 0\). Then \(\alpha_n \neq 0\) for some \(n\). Such an \(\alpha_n\) can be uniquely written as \(\alpha_n = p^s \beta_n\) with \(s = s(\alpha_n) \geq 0\) and \(\beta_n \in A_n\). \(\beta_n \notin pA_n\). It then follows from (2.4) that
\[
g_n(\alpha_n) \in U_m, \quad g_n(\alpha_n) \notin U_{m+1}, \quad \text{for } m = m(\alpha_n) = np^s.
\]
Since the \(n\)'s are prime to \(p\), the integers \(m(\alpha_n)\) are distinct for all \(\alpha_n\)'s, \(\alpha_n \neq 0\). Hence, let \(n\) denote the integer, prime to \(p\), such that \(\alpha_n \neq 0\) and \(m(\alpha_n) < m(\alpha_{n'})\) for all \(n' \neq n\) with \(\alpha_{n'} \neq 0\). Then, for all \(n' \neq n\),
\[
g_n(\alpha_{n'}) \in U_{m+1}, \quad \text{with } m = m(\alpha_n) < m(\alpha_{n'}).
\]
Therefore,
\[
g(\xi) = g_n(\alpha_n) \equiv 1 \mod U_{m+1}, \quad g(\xi) \neq 1,
\]
and this proves that \(g\) is injective. Thus \(g: A \to U_1\). Since \(A\) is obviously the direct product of countably infinite copies of \(\mathbb{Z}_p\), the proposition is proved.

By (2.2) and Propositions 2.7 and 2.8, the structure of the multiplicative group \(k^\times\) of a local field \(k\) is completely determined.

**2.3. Finite Extensions**

Let \((k, \nu)\) be a local field with residue field \(\mathfrak{f} = \mathcal{O}/p = \mathbb{F}_q\). Let \(k'\) be any finite extension over \(k\). By Proposition 1.5, there is a unique normalized valuation
\( \nu' \) on \( k' \) such that \( \nu' \mid k \sim \nu \), and \( (k', \nu') \) is then a complete extension of \( (k, \nu) \) with
\[
[k' : k] = ef,
\]
where
\[
e = e(k'/k), \quad f = f(k'/k).
\]

Let \( \mathfrak{f}' = \mathfrak{o}'/\mathfrak{p}' \) be the residue field of \( (k', \nu') \). Then
\[
[k' : k] = ef, \quad e = e(k'/k), \quad f = f(k'/k).
\]
so that \( \mathfrak{f}' \) is a finite field with \( q^f \) elements: \( \mathfrak{f}' = \mathbb{F}_{q^f} \), \( q' = q^f \). Therefore, \( (k', \nu') \) is a local field; it is a \( p \)-field if \( (k, \nu) \) is a \( p \)-field. In this manner, a finite extension \( k' \) of \( k \) always provides us a local field \( (k', \nu') \). In such a circumstance, we shall often say, without specifying the valuations, that \( k'/k \) is a family of \( p \)-extensions.

Taking account of the above remark, we can get from Propositions 2.4 and 2.5, the following simple description of the family of all \( p \)-fields for a given prime number \( p \), although the statement here is not as precise as in those propositions:

**Theorem 2.9.** A field \( k \) is a \( p \)-field of characteristic 0 if and only if it is a finite extension of the \( p \)-adic number field \( \mathbb{Q}_p \), and \( k \) is a \( p \)-field of characteristic \( p \) if and only if it is a finite extension of the Laurent series field \( \mathbb{F}_p((T)) \).

Now, let \( k'/k \) be a finite extension of local fields and let
\[
n = [k' : k] = ef,
\]
where
\[
e = e(k'/k), \quad f = f(k'/k).
\]
The extension \( k'/k \) is called an unramified extension if
\[
e = 1, \quad f = n,
\]
and it is called a totally ramified extension if
\[
e = n, \quad f = 1.
\]
In general, let \( \pi \) and \( \pi' \) denote prime elements of \( k \) and \( k' \), respectively:
\[
\nu(\pi) = \nu'(\pi') = 1.
\]
Then it follows from (1.5) and Proposition 1.5 that
\[
e = \nu'(\pi), \quad f = \nu(N_{k'/k}(\pi')).
\]
Therefore, the extension \( k'/k \) is unramified if and only if a prime element \( \pi \) is also a prime element of \( k' \), and \( k'/k \) is totally ramified if and only if the norm \( N_{k'/k}(\pi') \) of a prime element \( \pi' \) of \( k' \) is a prime element of \( k \). Let \( k'' \) be a finite extension of \( k' \):
\[
k \subseteq k' \subseteq k''.
\]
Then it follows from (1.7) that \( k''/k \) is unramified (resp. totally ramified) if and only if both \( k''/k' \) and \( k'/k \) are unramified (resp. totally ramified).

Let \( k'/k \) be again an arbitrary finite extension of local fields and let, as before, \( n = [k' : k] = ef \) and \( \mathfrak{f} = \mathbb{F}_q, \mathfrak{f}' = \mathbb{F}_{q^f} \), for the residue fields with \( q' = q^f \). Further, let
\[
A' = \{ y \in k' \mid y^{q'} = y \}, \quad k_0 = k(A'), \quad k \subseteq k_0 \subseteq k'.
\]
**Lemma 2.10.** $k_0$ is a splitting field of the polynomial $x^{q'} - x$ over $k$ and $k_0/k$ is an unramified cyclic extension with degree $[k_0:k] = f$.

**Proof.** By Proposition 2.3, $A'$ is a complete set of representatives of $\mathfrak{p}' = \mathfrak{o}'/\mathfrak{p}' = \mathbb{F}_{q'}$. in $\mathfrak{o}'$ so that it contains $q'$ elements—that is, all roots of $X^{q'} - X$. Hence $k_0 = k(A')$ is a splitting field of $X^{q'} - X$ over $k$. As $X^{q'} - X$ has $q'$ distinct roots, $k_0/k$ is a separable, hence Galois, extension. Let $\mathfrak{f}_0$ denote the residue field of $k_0: \mathfrak{f} \subseteq \mathfrak{f}_0 \subseteq \mathfrak{f}'$. Then $A' \subseteq k_0$ implies $\mathfrak{f}_0 = \mathfrak{f}' = \mathbb{F}_{q'}$, $q' = q'$. As $\mathfrak{f}$ is a finite field, $\mathfrak{f}_0 (= \mathfrak{f}')$ is a cyclic extension of degree $f$ over $\mathfrak{f}$. Now, by the Corollary of Proposition 1.1, each $\sigma$ in the Galois group $\text{Gal}(k_0/k)$ induces an automorphism $\sigma'$ in $\text{Gal}(\mathfrak{f}_0/\mathfrak{f})$, and the map $\sigma \mapsto \sigma'$ defines a homomorphism

$$\text{Gal}(k_0/k) \to \text{Gal}(\mathfrak{f}_0/\mathfrak{f}).$$

Assume that $\sigma' = 1$—that is, $\sigma \mapsto 1$. Since the set $A'$ of all roots of $X^{q'} - X$ is mapped onto itself by $\sigma$ and since $A'$ is also a complete set of representatives of $\mathfrak{f}_0 = \mathfrak{o}_0/\mathfrak{p}_0$ in the valuation ring $\mathfrak{o}_0$ of $k_0$, $\sigma' = 1$ implies that $\sigma$ fixes every element of $A'$. As $k_0 = k(A')$, it follows that $\sigma = 1$. Thus the above homomorphism $\text{Gal}(k_0/k) \to \text{Gal}(\mathfrak{f}_0/\mathfrak{f})$ is injective, and we obtain

$$[k_0:k] = [\text{Gal}(k_0/k):1] \leq [\text{Gal}(\mathfrak{f}_0/\mathfrak{f}):1] = [\mathfrak{f}_0:\mathfrak{f}].$$

On the other hand, by Proposition 1.5,

$$[\mathfrak{f}_0:\mathfrak{f}] = f(k_0/k) \leq [k_0:k].$$

Therefore,

$$[k_0:k] = f(k_0/k) = [\mathfrak{f}_0:\mathfrak{f}] = [\mathfrak{f}':\mathfrak{f}] = f$$

and $k_0/k$ is an unramified Galois extension of degree $f$. It also follows that the above homomorphism of Galois groups is an isomorphism:

$$\text{Gal}(k_0/k) \cong \text{Gal}(\mathfrak{f}_0/\mathfrak{f})$$

so that $\text{Gal}(k_0/k)$ is a cyclic group of order $f$.

**Proposition 2.11.** Let $(k, \nu)$ be a local field with residue field $\mathfrak{f} = \mathfrak{o}/\mathfrak{p} = \mathbb{F}_q$. Then, for each integer $n \geq 1$, there exists an unramified extension $k'/k$ with degree $[k':k] = n$, and $k'$ is unique up to an isomorphism over $k$. The field $k'$ is a splitting field of the polynomial $X^n - X$ over $k$, and it is a cyclic extension of degree $n$ over $k$. Let $\mathfrak{f}'$ be the residue field of the local field $(k', \nu')$. Then each element $\sigma$ of $\text{Gal}(k'/k)$ induces an automorphism $\sigma'$ of $\mathfrak{f}'/\mathfrak{f}$, and the map $\sigma \mapsto \sigma'$ defines an isomorphism

$$\text{Gal}(k'/k) \cong \text{Gal}(\mathfrak{f}'/\mathfrak{f}).$$

**Proof.** Since the finite field $\mathfrak{f}$ has a separable extension of degree $n$ over it, there exists a monic irreducible polynomial $g(X)$ with degree $n$ in $\mathfrak{f}[X]$. Let $f(X)$ be a monic polynomial of degree $n$ in $\mathfrak{o}[X]$ such that $g(X)$ is the reduction of $f(X)$ mod $\mathfrak{p}$. Let $w$ be a root of $f(X): f(w) = 0$, and let $k' = k(w)$. If $f(X) = X^n + \sum_{i=0}^{n-1} a_i X^i$, $a_i \in \mathfrak{o}$, then $w^n = -\sum_{i=0}^{n-1} a_i w^i$, $a_i \in \mathfrak{o}$,
and this implies that \( v'(w) \geq 0 \) —that is, \( w \in \mathfrak{o}' \), \( \mathfrak{o}' \) being the valuation ring of \( (k', v') \). Hence, let \( \omega \) denote the residue class of \( w \) in \( \mathfrak{t}' = \mathfrak{o}'/\mathfrak{p}' \) for \( (k', v') \). Then clearly \( g(\omega) = 0 \). As \( g(X) \) is irreducible in \( \mathfrak{t}[X] \), it follows that \( [\mathfrak{t}(\omega) : \mathfrak{t}] = \deg g(X) = n \). On the other hand, \( f(w) = 0 \) implies \( [k' : k] = [k(w) : k] \leq \deg f(X) = n \). Hence, by Proposition 1.5,

\[
  n = [\mathfrak{t}(\omega) : \mathfrak{t}] \leq [\mathfrak{t}' : \mathfrak{t}] = f(k'/k) \leq [k' : k] \leq n,
\]
and it follows that \( [k' : k] = f(k'/k) = n \) so that \( k'/k \) is an unramified extension of degree \( n \). This proves the existence of \( k' \).

Now, let \( k' \) be any unramified extension of degree \( n \) over \( k \). Apply the above lemma for \( k'/k \). Since \( n = f \) in this case, we see that \( k' = k_0 \) so that the field \( k' \) has the properties stated in the proposition. Furthermore, as a splitting field of \( X^{q^n} - X \) over \( k \), such a field \( k' \) is unique for \( n \geq 1 \) up to an isomorphism over \( k \). Hence the proposition is proved.

Now, since \( \mathfrak{t} = \mathbb{F}_q \), the Galois group \( \text{Gal}(\mathfrak{t}'/\mathfrak{t}) \) in the above proposition is generated by the automorphism

\[
  \omega \mapsto \omega^q, \quad \text{for } \omega \in \mathfrak{t}'.
\]

Let \( \varphi \) denote the automorphism of \( k'/k \), corresponding to the above automorphism of \( \mathfrak{t}'/\mathfrak{t} \) under the isomorphism \( \text{Gal}(k'/k) \cong \text{Gal}(\mathfrak{t}'/\mathfrak{t}) \) in Proposition 2.11. Then \( \varphi \) is a generator of the cyclic group \( \text{Gal}(k'/k) \) and it is uniquely characterized by the property that

\[
  \varphi(y) = y^q \mod \mathfrak{p}', \quad \text{for all } y \in \mathfrak{o}'.
\]

This \( \varphi \) is called the Frobenius automorphism of the unramified extension \( k'/k \); it will play an essential role throughout the following.

Next, let \( k'/k \) be again an arbitrary, not necessarily unramified, finite extension of local fields and let \( e = e(k'/k) , f = f(k'/k), n = [k' : k] = ef, q' = q^f \).

Proposition 2.12. The splitting field \( k_0 \) of \( X^{q^n} - X \) over \( k \) in Lemma 2.10 is the unique maximal unramified extension over \( k \), contained in \( k' \). \( k'/k \) is a totally ramified extension and

\[
  [k' : k_0] = e, \quad [k_0 : k] = f.
\]

Proof. We already know that \( k_0/k \) is an unramified extension with \( [k_0 : k] = f \). Let \( k_1 \) be any unramified extension of \( k \), contained in \( k' \), and let \( f_i = f(k_i/k) = [k_1 : k], q'' = q^f_i \). By Proposition 2.11, \( k_1 \) is the splitting field, in \( k' \), of the polynomial \( X^{q''} - X \) over \( k \). As \( f = f(k'/k) = f(k'/k_1)f(k_1/k) \), \( f_1 \) is a factor of \( f \) so that \( q'' - 1 \) divides \( q' - 1 \), and \( X^{q''} - X \) divides \( X^{q'} - X \) in \( k[X] \). Therefore, \( k_1 \) is contained in the splitting field \( k_0 \), in \( k' \), of \( X^{q'} - X \) over \( k \). This proves that \( k_0 \) is the unique maximal unramified extension of \( k \), contained in \( k' \). Now, \( f(k_0/k) = [k_0 : k] = f = f(k'/k) \) implies \( f(k'/k_0) = 1 \)—namely, that \( k'/k_0 \) is totally ramified. As \( ef = n = [k' : k], f = [k_0 : k] \), we also have \( [k' : k_0] = e \).
The field $k_0$ in the above proposition is called the inertia field of the extension $k'/k$.

2.4. The Different and the Discriminant

Let $k'/k$ still be a finite extension of local fields and let $f = o/p$, $f' = o'/p'$, and so on, be defined as above. Throughout this section, we assume that $k'/k$ is a separable extension.

By Proposition 1.6, the trace map $T_{k/k'}: k' \to k$ is continuous and $T_{k'/k}(o') \subseteq o$. Let $T = T_{k'/k}$ for simplicity, and define

$$m = \{ x' \in k' \mid T(x' o') \subseteq o \}.$$

Since $k'/k$ is separable, there exists an element $x' \in k'$ such that $T(x') \neq 0$. Hence $T(k') = k$, and it follows from the definition that $m$ is an $o'$-submodule of $k'$, different from $k'$. Furthermore, $T(o') \subseteq o$ implies that $o' \subseteq m$, $m \neq \{0\}$. Therefore $m$ is an ideal of $(k', o')$ (cf. Section 1.2), containing $o'$ so that its inverse $\mathcal{D} = m^{-1}$ is a non-zero ideal of the ring $o'$. We call $\mathcal{D}$ the different of the extension $k'/k$ and denote it by $\mathcal{D}(k'/k)$:

$$\mathcal{D}(k'/k) = \mathcal{D} = m^{-1} \subseteq o'.$$

Let

$$D(k'/k) = N_{k'/k}(\mathcal{D}(k'/k)).$$

This is a non-zero ideal of $o$ and it is called the discriminant of $k'/k$.

To find a simple description of the different $\mathcal{D}(k'/k)$, we need the following

**Lemma 2.13.** There exists an element $w$ in $o'$ such that $1, w, \ldots, w^{n-1}$ form a free basis of the $o$-module $o'$:

$$o' = o \oplus o w \oplus \cdots \oplus o w^{n-1}.$$

In particular, we have

$$o' = o[w],$$

where $o[w]$ denotes the ring of all elements of the form $h(w)$ with $h(X) \in o[X]$.

**Proof.** We first note that $f' = f(\omega)$ for some $\omega \in f'$, because $f'/f$ is a separable extension. Let $g(X)$ be the minimal polynomial of $\omega$ over $f$; $g(X)$ is a monic polynomial in $f[X]$ with $\deg g(X) = \lceil f' : f \rceil = f(k'/k) = f$. Let $f(X)$ be a monic polynomial of degree $f$ in $o[X]$ such that $g(X)$ is the reduction of $f(X) \bmod p$, and let $w$ be an element of $o'$, belonging to the residue class $\omega$ in $f' = o'/p'$. Clearly, $g(\omega) = 0$ implies $f(w) \equiv 0 \bmod p'$. Let $w' = w + \pi'$, where $\pi'$ is a prime element of $k'$. Then $w'$ again belongs to the same residue class $\omega$, and

$$f(w') \equiv f(w) + f'(w) \pi' \bmod p'^2,$$

where $f' = df/dX$. However, as $f' = f(\omega)$ is a separable extension of $f$, we
have \( g'(\omega) \neq 0 \) for \( g' = dg/dX \), and this implies \( f'(w) \neq 0 \mod p' \). Therefore, it follows from the above congruence that either \( f(w) \equiv 0 \mod p'^2 \) or \( f(w') \equiv 0 \mod p'^2 \). Replacing \( w \) by \( w' \) if necessary, we see that the residue class \( \omega \) contains an element \( w \) such that \( f(w) \equiv 0 \mod p' \), \( f(w') \equiv 0 \mod p'^2 \). Thus \( f(w) \) is a prime element of \( k' \). Since 1, \( \omega, \ldots, \omega'^{-1} \) form a basis of \( \mathfrak{f}' \) over \( \mathfrak{f} \), the proof of (1.8) shows that the \( e_f \) elements

\[
\eta_i = w'^{-1}f(w)^i, \quad 1 \leq i \leq f, \quad 0 \leq j < e
\]

form a basis of the \( \mathfrak{o} \)-module \( \mathfrak{o}' \). Since \( ef = n \), \( \deg f(X) = f \), it follows that 1, \( w, \ldots, w'^{n-1} \) generate the \( \mathfrak{o} \)-module \( \mathfrak{o}' \). Then those \( n \) elements also generate the \( k \)-module \( k' \) so that they form a basis of \( k' \) over \( k \). Therefore,

\[
\mathfrak{o}' = \mathfrak{o} \oplus \omega \mathfrak{o} \oplus \cdots \oplus \omega^n \mathfrak{o} = \mathfrak{o}[w].
\]

**Corollary.** Let \( k'/k \) be totally ramified and let \( \pi' \) be any prime element of \( k' \). Then

\[
\mathfrak{o}' = \mathfrak{o} \oplus \mathfrak{o} \pi' \oplus \cdots \oplus \mathfrak{o} \pi'^n = \mathfrak{o}[\pi'].
\]

**Proof.** In this case, \( f(k'/k) = 1 \) so that \( \mathfrak{f}' = \mathfrak{f} \). Hence, in the above proof, we may set \( \omega = 0, \quad g(X) = f(X) = X, \quad w = \pi' \).}

**Proposition 2.14.** Let \( w \) be an element of \( \mathfrak{o}' \) as in Lemma 2.13 and let \( f(X) \) denote the minimal polynomial of \( w \) over \( k \). Then

\[
\mathcal{O}(k'/k) = f'(w)\mathfrak{o}'
\]

where \( f'(X) = df/dX \).

**Proof.** Let \( f(X) = X^n + \sum_{i=0}^{n-1} a_i X^i, \quad a_i \in k \). Since \( \mathfrak{o}' = \mathfrak{o} \oplus \omega \mathfrak{o} \oplus \cdots \oplus \omega^{n-1} \mathfrak{o} \), \( w^n \) is a linear combination of 1, \( w, \ldots, w^{n-1} \) with coefficients in \( \mathfrak{o} \). Hence \( a_i \in \mathfrak{o} \) for \( 0 \leq i < n \). Let \( w_1, \ldots, w_n \) be the roots of \( f(X) \) in an algebraic closure of \( k' \). Since \( k'/k \) is separable, these roots are distinct and they are the conjugate of \( w \) over \( k \). By a classical formula of Euler,

\[
\frac{1}{f(X)} = \sum_{i=1}^{n} \frac{1}{f'(w_i)} \frac{1}{X - w_i}.
\]

Putting \( Y = X^{-1} \), we obtain as formal power series

\[
\frac{Y^n}{1 + a_{n-1} Y + \cdots + a_0 Y^n} = \sum_{i=1}^{n} \frac{1}{f'(w_i)} \frac{Y}{1 - w_i Y} = \sum_{m=1}^{\infty} T \left( \frac{w^{m-1}}{f'(w)} \right) Y^m.
\]

Since \( a_i \in \mathfrak{o} \) for \( 0 \leq i < n \), it follows that \( T(w^i f'(w)^{-1}) \in \mathfrak{o} \) for all \( i \geq 0 \) and that

\[
T(w^{n-1} f'(w)^{-1}) = 1, \quad T(w^i f'(w)^{-1}) = 0, \quad \text{for } 0 \leq i < n - 1. \quad (2.5)
\]

Now, let \( y \in k' \) and let

\[
y = \sum_{i=0}^{n-1} b_i w^i, \quad b_i \in k.
\]
Then
\[ yf'(w)^{-1} \in m = \mathcal{D}^{-1} \iff T(yf'(w)^{-1}w^j) \in \mathfrak{o}, \quad \text{for } 0 \leq j < n \]
\[ \iff \sum_{i=0}^{n-1} b_i T(w^i + f'(w)) \in \mathfrak{o}, \quad \text{for } 0 \leq j < n. \]

By (2.5), this condition for \( j = 0, 1, \ldots, n - 1 \) yields successively \( b_n \in \mathfrak{o}, \ldots, b_0 \in \mathfrak{o} \). Hence

\[ yf'(w)^{-1} \in \mathcal{D}^{-1} \iff y \in \mathfrak{o}' = \mathfrak{o} \oplus \mathfrak{o}w \oplus \cdots \oplus \mathfrak{o}w^{n-1} \]

so that \( \mathcal{D}^{-1} = \mathfrak{o}'f'(w)^{-1} \)—that is, \( \mathcal{D} = f'(w)\mathfrak{o}' \).

**Proposition 2.15.** Let \( y_1, \ldots, y_n \) be a basis of \( k' \) over \( k \) such that \( \mathfrak{o}' = \mathfrak{o}y_1 \oplus \cdots \oplus \mathfrak{o}y_n \) (e.g., 1, \( w \), \ldots, \( w^{n-1} \) in Lemma 2.13). Then

\[ D(k'/k) = \det(T_{k'/k}(y_iy_j))\mathfrak{o}. \]

**Proof.** It is easy to see that the right-hand side of the above equality is independent of the choice of \( \{y_1, \ldots, y_n\} \) such that \( \mathfrak{o}' = \mathfrak{o}y_1 \oplus \cdots \oplus \mathfrak{o}y_n \). Hence we may assume that \( \{y_1, \ldots, y_n\} = \{1, w, \ldots, w^{n-1}\} \). As in the proof of Proposition 2.14, let \( w_1, \ldots, w_n \) denote the conjugates of \( w \) over \( k \). Then

\[
(T(y_iy_j)) = \begin{pmatrix}
1, & 1, & \ldots, & 1

w_1, & w_2, & \ldots, & w_n

\vdots & \vdots & \ddots & \vdots

w_1^{n-1}, & w_2^{n-1}, & \ldots, & w_n^{n-1}
\end{pmatrix}
\begin{pmatrix}
1, w_1, \ldots, w_1^{n-1} \\
\vdots & \vdots & \ddots & \vdots \\
1, w_n, \ldots, w_n^{n-1}
\end{pmatrix}
\]

so that

\[
\det(T(y_iy_j)) = \prod_{i \neq j} (w_i - w_j)^2 = \pm \prod_{i=1}^n f'(w_i) = \pm N_{k'/k}(f'(w)).
\]

Hence, by Proposition 2.14,

\[
det(T(y_iy_j))\mathfrak{o} = N_{k'/k}(f'(w))\mathfrak{o} = N_{k'/k}(f'(w)\mathfrak{o}') = N_{k'/k}(\mathcal{D}(k'/k)) = D(k'/k).
\]

**Proposition 2.16.** Let \( k''/k \) be a finite separable extension of local fields and let \( k \subseteq k' \subseteq k'' \). Then

\[ \mathcal{D}(k''/k) = \mathcal{D}(k''/k')\mathcal{D}(k'/k). \]

**Proof.** Let \( m = \mathcal{D}(k'/k)^{-1} \), \( m' = \mathcal{D}(k''/k')^{-1} \), \( m'' = \mathcal{D}(k''/k)^{-1} \). Let \( \mathfrak{o}' \) denote the valuation ring of \( k'' \) and let \( m = \mathfrak{m}'' = \pi^a \mathfrak{o}' \), where \( \pi' \) is a prime element of \( k' \). Since \( \mathfrak{o}'' = \mathfrak{m}'' \mathfrak{o}' \),

\[
T_{k''/k}(z \mathfrak{o}'') = T_{k''/k}(T_{k'/k}(z \mathfrak{o}')(\mathfrak{o}')).
\]
for any $z \in k''$. Hence

\[ z \in m'' \iff T_{k''/k}(z o'') \subseteq o \iff T_{k''/k}(T_{k''/k'}(z o'')) \subseteq o \]

\[ \iff T_{k''/k}(z o'') \subseteq m = \pi^a o \iff T_{k''/k}(\pi^{-a} z o'') \subseteq o' \]

\[ \iff \pi^{-a} z \in m' \iff z \in \pi^a m' = mm'. \]

Therefore, $m'' = mm'$—namely, $\mathcal{D}(k''/k') = \mathcal{D}(k''/k') \mathcal{D}(k'/k)$.

We now consider the different $\mathcal{D}(k'/k)$ in the case where $k'/k$ is either unramified or totally ramified. Suppose first that $k'/k$ is unramified. Let $w$ and $f(X)$ be as in Proposition 2.14 and let $\omega$ denote the residue class of $w \mod p': \omega \in \mathfrak{t}' = \varpi'/p'$. Since \( \varpi' = \varpi \oplus \omega \varpi \oplus \cdots \oplus \omega \varpi^{n-1} \) and \([\mathfrak{t}' : \mathfrak{t}] = [k'/k] = n\), we see that $\mathfrak{t}' = \mathfrak{t}(\omega)$ and the minimal polynomial $g(X)$ of $\omega$ over $\mathfrak{t}$ is the reduction of $f(X) \mod p$. As $\mathfrak{t}'/\mathfrak{t}$ is separable, $g'(\omega) \neq 0$. Hence $f'(\omega) \neq 0 \mod p'$, and it follows from Proposition 2.14 that

\[ \mathcal{D}(k'/k) = \mathcal{O}'. \]

Next, let $k'/k$ be totally ramified and let $e = n = [k': k] > 1$. By the Corollary of Lemma 2.13, we have then $\omega' = \omega \oplus \omega \pi' \oplus \cdots \oplus \omega \pi'^{n-1}$ for any prime element $\pi'$ of $(k', \nu')$. Let

\[ f(X) = X^n + \sum_{i=0}^{n-1} a_i X^i, \quad a_i \in \varpi \]

be the minimal polynomial of $\pi'$ over $k$. From $f(\pi') = 0$ and $\nu' | k = ev = nv$, we then see that $\nu(a_i) > 0$—that is, $a_i \in p$, for $0 \leq i \leq n - 1$. It then follows that

\[ f'(\pi') = n \pi'^{n-1} + \sum_{i=0}^{n-1} i a_i \pi'^{i-1} \equiv 0 \mod p' \]

so that

\[ \mathcal{D}(k'/k) = f'(\pi') \mathcal{O}' \neq \mathcal{O}'. \]

**Proposition 2.17.** Let $k'/k$ be a finite separable extension of local fields. Then $k'/k$ is unramified if and only if $\mathcal{D}(k'/k) = \mathcal{O}'$—that is, if and only if $D(k'/k) = 0$.

**Proof.** Let $k_0$ denote the inertia field of the extension $k'/k : k \subseteq k_0 \subseteq k'$ (cf. Proposition 2.12). Then

\[ \mathcal{D}(k'/k) = \mathcal{D}(k'/k_0) \mathcal{D}(k_0/k) = \mathcal{D}(k'/k_0) \]

because $\mathcal{D}(k_0/k) = \mathfrak{o}_0$ by the above remark. By the same remark, $\mathcal{D}(k'/k_0) = \mathcal{O}'$ if and only if $e = [k': k_0] = 1$. Hence the proposition is proved.

**2.5. Finite Galois Extensions**

Let $k'/k$ now be a finite Galois extension of local fields and let $G = \text{Gal}(k'/k)$.
Let $\sigma$ be any element of $G$. By the Corollary of Proposition 1.1,
\[ \sigma(o') = o', \quad \sigma(p^n) = p'^n, \quad \text{for } n \geq 1, \]
o' and $p'$ being the valuation ring and the maximal ideal of $k'$. Hence, for each $n \geq 1$, $\sigma$ induces a ring automorphism
\[ \sigma_n: o'/p'^{n+1} \cong o'/p''^{n+1}. \]
The map $\sigma \mapsto \sigma_n$ then defines a homomorphism of $G$ into the group of automorphisms of the ring $o'/p'^{n+1}$. Let $G_n$ denote the kernel of this homomorphism:
\[ G_n = \{ \sigma \in G \mid \sigma(y) \equiv y \pmod{p''^{n+1}} \quad \text{for all } y \in o' \}. \]
$G_n$ is a normal subgroup of $G$ and $G_{n+1} \subseteq G_n$ for $n \geq 0$. Furthermore, if $\sigma \neq 1$, then there exists $y \in o'$ such that $\sigma(y) \neq y$, so $\sigma(y) \neq y \pmod{p''^{n+1}}$ for sufficiently large $n$. Therefore, $G_m = 1$ for all large $m$, and we have a sequence of normal subgroups of $G$:
\[ 1 = \cdots = G_m \subseteq G_{m-1} \subseteq \cdots \subseteq G_1 \subseteq G_0 \subseteq G. \]
These groups $G_n$ are called the ramification groups (in the lower numbering) of the Galois extension $k'/k$.

**Proposition 2.18.** Let $k_0$ be the inertia field of the extension $k'/k$ (cf. Proposition 2.12). Then
\[ G_0 = \text{Gal}(k'/k_0), \quad G/G_0 = \text{Gal}(k_0/k) \cong \text{Gal}(\overline{f}/f), \]
so that $G/G_0$ is a cyclic group and
\[ [G_0:1] = e, \quad [G:G_0] = f. \]

**Proof.** Each $\sigma$ in $G$ induces an automorphism $\sigma' = (\sigma_0)$ of $f' = o'/p'$, and $\sigma'$ obviously fixes elements of $\overline{f}$. Hence $\sigma \mapsto \sigma'$ defines a natural homomorphism $G = \text{Gal}(k'/k) \to \text{Gal}(\overline{f}/f)$, and by definition, $G_0$ is the kernel of this homomorphism. For the Galois extension $k_0/k$, we have a similar natural homomorphism $\text{Gal}(k_0/k) \to \text{Gal}(\overline{f}_0/f_0)$, where $\overline{f}_0$ denotes the residue field of $k_0$. Since $k \subseteq k_0 \subseteq k'$, $\overline{f} \subseteq \overline{f}_0 \subseteq \overline{f}'$, there also exist canonical homomorphisms $\text{Gal}(k'/k) \to \text{Gal}(k_0/k)$ and $\text{Gal}(\overline{f}'/f) \to \text{Gal}(\overline{f}_0/f_0)$, and those maps define a commutative diagram
\[ \begin{array}{ccc}
\text{Gal}(k'/k) & \xrightarrow{\alpha} & \text{Gal}(\overline{f}'/f) \\
\downarrow{\beta} & & \downarrow \\
\text{Gal}(k_0/k) & \longrightarrow & \text{Gal}(\overline{f}_0/f).
\end{array} \]
However, by Proposition 2.12, $f(k'/k_0) = 1$, $\overline{f}' = \overline{f}_0$ and by Proposition 2.11, $\text{Gal}(k_0/k) \cong \text{Gal}(\overline{f}_0/f)$. Hence
\[ G_0 = \text{Ker}(\alpha) = \text{Ker}(\beta) = \text{Gal}(k'/k_0). \]
The rest of the proposition then follows immediately from Propositions 2.11 and 2.12.

**Proposition 2.19.** For each \( n \geq 0 \), there exists an injective homomorphism 
\[
G_n/G_{n+1} \to U'_n/U'_{n+1},
\]
where \( U'_0 = U' \) is the unit group of \( k' \) and \( U'_i = 1 + \mathfrak{p}'^i \) for \( i \geq 1 \).

**Proof.** Let \( \pi' \) be any prime element of \( k' \). Then \( \sigma \in G_n \) implies 
\[
\sigma(\pi') = \pi' \mod \mathfrak{p}'^n
\]
so that \( \sigma(\pi')\pi'^{-1} \equiv 1 \mod \mathfrak{p}'^n \)—that is, \( \sigma(\pi')\pi'^{-1} \in U'_n \). If \( \pi'' \) is another prime element of \( k' \), then \( \pi'' = \pi'u \) with \( u \in U' \), and 
\[
\sigma(u) \equiv u \mod \mathfrak{p}'^n
\]
implies \( \sigma(u)u^{-1} \equiv 1 \mod \mathfrak{p}'^{n+1} \) so that 
\[
\sigma(\pi')\pi'^{-1} \equiv \sigma(\pi'')\pi''^{-1} \mod U'_{n+1}.
\]
Hence the map 
\[
\lambda_n : G_n \to U'_n/U'_{n+1},
\]
\[
\sigma \mapsto \sigma(\pi')\pi'^{-1} \mod U'_{n+1}
\]
is independent of the choice of the prime element \( \pi' \). Let \( \tau \in G_n \). Then 
\( \pi'' = \tau(\pi') \) is another prime element of \( k' \). Hence, it follows from 
\[
\sigma\tau(\pi')\pi'^{-1} = (\sigma(\pi'')\pi''^{-1})(\tau(\pi')\pi'^{-1})
\]
that 
\[
\lambda_n(\sigma\tau) = \lambda_n(\sigma)\lambda_n(\tau),
\]
namely, that \( \lambda_n : G_n \to U'_n/U'_{n+1} \) is a homomorphism. Let \( \lambda_n(\sigma) = 1 \) for \( \sigma \in G_n \). This means \( \sigma(\pi')\pi'^{-1} \equiv 1 \mod \mathfrak{p}'^{n+2} \) so that \( \sigma(\pi') = \pi' \mod \mathfrak{p}'^{n+2} \). Let \( k_0 \) be as in Proposition 2.18 and let \( v_0 \) be the valuation ring of \( k_0 \). Since \( k'/k_0 \) is totally ramified by Proposition 2.12, it follows from the Corollary of Lemma 2.13 that \( \sigma' = v_0[\pi'] \). Hence, for \( \sigma \in G_n \subseteq G_0 = \text{Gal}(k'/k_0) \), 
\[
\sigma(\pi') \equiv \pi' \mod \mathfrak{p}'^{n+2}
\]
holds if and only if \( \sigma(y) = y \mod \mathfrak{p}'^{n+2} \) for every \( y \in \mathfrak{p}' \)—that is, \( \sigma \in G_{n+1} \). Thus \( \ker(\lambda_n) = G_{n+1} \), and \( \lambda_n \) induces an injective homomorphism 
\[
G_n/G_{n+1} \to U'_n/U'_{n+1}.
\]

**Corollary.** A finite Galois extension \( k'/k \) of local fields is always a solvable extension—that is, \( \text{Gal}(k'/k) \) is a solvable group.

**Proof.** \( G/G_0 \) is cyclic by Proposition 2.18 and \( G_n/G_{n+1} \) is abelian for \( n \geq 1 \) by Proposition 2.19. Since \( G_m = 1 \) for sufficiently large \( m \), \( G = \text{Gal}(k'/k) \) is a solvable group.

Now, suppose that \( k \) is a \( p \)-field so that both \( q \) and \( q' \) are powers of \( p \). By (1.3) for \((k', v')\), 
\[
U'_0/U'_1 \cong \mathfrak{p}'^\times, \quad U'_n/U'_{n+1} \cong \mathfrak{p}'^+ \quad \text{for } n \geq 1.
\]
Hence, it follows from Proposition 2.19 that 
\[
G_0/G_1 = \text{a cyclic group}, \quad [G_0 : G_1] \mid (q' - 1),
\]
\[
G_n/G_{n+1} = \text{an abelian group of type } (p, \ldots, p), \quad [G_n : G_{n+1}] \mid q', \quad \text{for } n \geq 1.
\]
In particular, \([G_0 : G_1] \) is prime to \( p \) and \([G_1 : 1] \) is a power of \( p \).
Chapter III

Infinite Extensions
of Local Fields

This chapter consists of preliminary results for the remaining chapters. In the first part, some infinite extensions of local fields are discussed and then, in the second part, power series with coefficients in the valuation rings of those infinite extensions are studied. Here and in the following chapters we need some fundamental facts on infinite Galois extensions and their Galois groups—namely, profinite groups. A brief account of these can be found in Cassels–Fröhlich [3], Chapter V.

3.1. Algebraic Extensions and Their Completions

Let \((k, v)\) be a local field with residue field \(\mathfrak{f} = \mathfrak{o}/p = \mathbb{F}_q\). Let \(\Omega\) be a fixed algebraic closure of \(k\), and \(\mu\) the unique extension of \(v\) on \(\Omega\) (cf. Proposition 1.1). We denote by \((\Omega, \bar{\mu})\) the completion of \((\Omega, \mu)\). Let \(F\) be any intermediate field of \(k\) and \(\bar{\Omega}\):

\[ k \subseteq F \subseteq \Omega \subseteq \bar{\Omega}. \]

The closure \(\bar{F}\) of \(F\) in \(\bar{\Omega}\) in the \(\bar{\mu}\)-topology is a subfield of \(\bar{\Omega}\). Let

\[ \mu_F = \mu \mid F, \quad \bar{\mu}_F = \bar{\mu} \mid \bar{F}. \]

Then \(\mu_F\) is the unique extension of \(v\) on the algebraic extension \(F\) over \(k\), and \((\bar{F}, \mu_F)\) is the completion of \((F, \mu_F)\). Now, any algebraic extension over \(k\) is \(k\)-isomorphic to a field \(F\) such as mentioned above. Hence, in order to study algebraic extensions over \(k\) and their completions, it is sufficient to consider the pairs \((F, \mu_F)\) and \((\bar{F}, \mu_F)\) as stated above. Let

\[ \mathfrak{o}_F = \text{the valuation ring of } \mu_F, \]
\[ p_F = \text{the maximal ideal of } \mu_F, \]
\[ \mathfrak{f}_F = \mathfrak{o}_F/p_F = \text{the residue field of } \mu_F, \]

and let \(\mathfrak{o}_{\bar{F}}, p_{\bar{F}}, \) and \(\mathfrak{f}_{\bar{F}}\) be defined similarly for \(\mu_{\bar{F}}\). Since \(f(\mu_{\bar{F}}/\mu_F) = 1\), the injection \(\mathfrak{o}_F \rightarrow \mathfrak{o}_{\bar{F}}\) identifies \(\mathfrak{f}_F\) with \(\mathfrak{f}_{\bar{F}}\):

\[ \mathfrak{f}_F = \mathfrak{f}_{\bar{F}}. \]

Let \(\sigma\) be any automorphism of \(F\) over \(k\). Then, by the Corollary of Proposition 1.1, \(\sigma\) is a topological automorphism of \(F\) in the \(\mu_F\)-topology, and by continuity, it can be uniquely extended to a topological automorph-
An isomorphism $\tilde{\sigma}$ of $\tilde{F}$ in the $\mu_\mathbb{F}$-topology. We then have

$$
\begin{align*}
\mu_\mathbb{F} \circ \sigma &= \mu_\mathbb{F}, & \sigma(\mathcal{O}_\mathbb{F}) &= \mathcal{O}_\mathbb{F}, & \sigma(p^n_\mathbb{F}) &= p^n_\mathbb{F}, \\
\mu_\mathbb{F} \circ \tilde{\sigma} &= \mu_\mathbb{F}, & \tilde{\sigma}(\mathcal{O}_\mathbb{F}) &= \mathcal{O}_\mathbb{F}, & \tilde{\sigma}(p^n_\mathbb{F}) &= p^n_\mathbb{F}, \quad n \geq 1,
\end{align*}
$$

and $\sigma$ and $\tilde{\sigma}$ induce the same automorphism of $\mathfrak{t}_\mathbb{F} = \mathfrak{t}_\mathbb{F}$ over $\mathfrak{f}$.

**Lemma 3.1.** Let $E$ be a finite extension of $F$ in $\Omega : k \subseteq F \subseteq E \subseteq \Omega \subseteq \tilde{\Omega}$, and let $\tilde{E}$ denote the closure of $E$ in $\tilde{\Omega}$. Then

$$
E\tilde{F} = \tilde{E}.
$$

Furthermore, if $E/F$ is a separable extension, then

$$
E \cap \tilde{F} = F.
$$

**Proof.** Clearly $\tilde{F} \subseteq E\tilde{F} \subseteq \tilde{E}$ and $E\tilde{F}/\tilde{F}$ is a finite extension. Since $\mu_\mathbb{F}$ is complete, it follows from Proposition 1.1 that $\tilde{\mu} | E\tilde{F}$ is a complete valuation on $E\tilde{F}$ so that $E\tilde{F}$ is closed in $\tilde{\Omega}$ in the $\tilde{\mu}$-topology. Hence $E\tilde{F} = \tilde{E}$. Assume now that $E/F$ is separable. Since $E/F$ is separable, there is a finite Galois extension $E'$ over $F$, containing $E : F \subseteq E \subseteq E'$, and in order to prove $E \cap \tilde{F} = F$, it is sufficient to show that $E' \cap \tilde{F} = F$. Hence, replacing $E$ by $E'$, we may suppose that $E/F$ itself is a finite Galois extension. Then $\tilde{E} = E\tilde{F}$ is a finite Galois extension over $\tilde{F}$ and

$$
[E : F][E : \mathcal{O}] = [E : E \cap \tilde{F}].
$$

Now, by continuity, each $\sigma$ in $\text{Gal}(E/F)$ can be uniquely extended to an automorphism $\tilde{\sigma}$ in $\text{Gal}(\tilde{E}/\tilde{F})$, and $\sigma \mapsto \tilde{\sigma}$ defines a monomorphism $\text{Gal}(E/F) \to \text{Gal}(\tilde{E}/\tilde{F})$. Hence

$$
[E : F] \leq [\tilde{E} : \tilde{F}] = [E : E \cap \tilde{F}].
$$

Since $F \subseteq E \cap \tilde{F} \subseteq E$, it follows that $E \cap \tilde{F} = F$. $\blacksquare$

**Remark.** Obviously, the second part of the lemma can be generalized for any separable algebraic extension $E/F$, not necessarily of finite degree.

### 3.2. Unramified Extensions and Totally Ramified Extensions

Let $k \subseteq F \subseteq \Omega$ be as above. We call $F/k$ an **unramified extension** if every finite extension $k'$ over $k$ in $F$, $k \subseteq k' \subseteq F$, is unramified in the sense of Section 2.3—that is, $e(k'/k) = 1$. It is clear that if $F/k$ is unramified and $k \subseteq F' \subseteq F$, then $F'/k$ is also unramified.

**Lemma 3.2.** Let $k \subseteq F \subseteq \Omega$. Then $F/k$ is unramified if and only if $\mu_\mathbb{F}(= \mu | F)$ is a normalized valuation on $F : \mu(F^{\times}) = \mathbb{Z}$.

**Proof.** In general, let $k'$ be any finite extension over $k$ in $\Omega : k \subseteq k' \subseteq \Omega$. By Section 2.3, $k'$ is a local field with respect to a unique normalized valuation $\nu'$ such that $\nu' | k \sim \nu$, and $\nu' | k = e\nu$ with $e = e(k'/k)$. Since $\mu_\mathbb{k} | k = \nu$ for $\mu_\mathbb{k} = \mu | k'$, it follows from the uniqueness that $\nu' = e\mu_\mathbb{k}$ so that $\mu_\mathbb{k}(k^{\times}) = (1/e)\nu'(k^{\times}) = (1/e)\mathbb{Z}$. Hence $k'/k$ is unramified—that is,
If $e = 1$—if and only if $\mu(k'^e) = \mu_{k'}(k'^e) = \mathbb{Z}$. This proves the lemma for a finite extension $k'/k$. The case for an arbitrary algebraic extension $F/k$ then follows immediately. ■

For each integer $n \geq 1$, there exists a unique unramified extension $k_{ur}^n$ over $k$ in $\Omega$ with degree $[k_{ur}^n:k] = n$, namely, the splitting field of the polynomial $X^n - X$ over $k$ in $\Omega$ (cf. Proposition 2.11). Since $k_{ur}^n/k$ is a cyclic extension, one sees immediately that

$$k_{ur}^n \subseteq k_{ur}^m \iff n \mid m, \quad \text{for } n, m \geq 1.$$  

Hence the union $k_{ur}$ of all $k_{ur}^n$, $n \geq 1$, is a subfield of $\Omega$:

$$k_{ur} = \bigcup_{n \geq 1} k_{ur}^n, \quad k \subseteq k_{ur} \subseteq \Omega.$$  

For simplicity, we shall often write $K$ for $k_{ur}$:

$$K = k_{ur}.$$  

It is clear that $k_{ur}/k$ is an unramified extension. On the other hand, if $F$ is an unramified extension over $k$ in $\Omega$ and if $\alpha \in F$, then $k' = k(\alpha)$ is a finite extension of $k$ in $F$ so that $k'/k$ is unramified. Hence $k' = k_{ur}^n$ for $n = [k':k]$ and $\alpha \in k_{ur}^n \subseteq k_{ur}$. Thus

$$k \subseteq F \subseteq k_{ur}.$$  

Therefore $k_{ur}$ is the unique maximal unramified extension over $k$ in $\Omega$.

For $n \geq 1$, let $\mathfrak{o}^n$ and $\mathfrak{f}^n$ denote the valuation ring and the residue field of $k_{ur}^n$, respectively, and let $\mathfrak{f}_k = \mathfrak{o}_K/p_K$ be the residue field of $K = k_{ur}$.

**Proposition 3.3.** $\mathfrak{f}_K$ is an algebraic closure of the residue field $\mathfrak{f} (= \mathfrak{f}_k)$ of $k$. Each $\sigma$ in $\text{Gal}(k_{ur}/k)$ induces an automorphism $\sigma'$ of $\mathfrak{f}_K/\mathfrak{f}$, and the map $\sigma \mapsto \sigma'$ defines a natural isomorphism

$$\text{Gal}(k_{ur}/k) \simeq \text{Gal}(\mathfrak{f}_K/\mathfrak{f}).$$

**Proof.** If $m \mid n$, then $k \subseteq k_{ur}^m \subseteq k_{ur}^n \subseteq k_{ur}$ so that $\mathfrak{f} \subseteq \mathfrak{f}^m \subseteq \mathfrak{f}^n \subseteq \mathfrak{f}_K$. Since $\mathfrak{o}_K$ is clearly the union of $\mathfrak{o}^n$ for all $n \geq 1$, $\mathfrak{f}_K$ is the union of $\mathfrak{f}^n$ for all $n \geq 1$. Since $[\mathfrak{f}^n : \mathfrak{f}] = [k_{ur}^n : k] = n$, and since the finite field $\mathfrak{f}$ has a unique extension with degree $n$ in any algebraic closure, it follows that $\mathfrak{f}_K$ is an algebraic closure of $\mathfrak{f}$. Now, it is clear that

$$\text{Gal}(k_{ur}/k) = \operatorname{lim} \text{Gal}(k_{ur}^n/k),$$  

$$\text{Gal}(\mathfrak{f}_K/\mathfrak{f}) = \operatorname{lim} \text{Gal}(\mathfrak{f}_n/\mathfrak{f}),$$  

where the inverse limits are taken with respect to the canonical maps $\text{Gal}(k_{ur}^m/k) \to \text{Gal}(k_{ur}^n/k)$, $\text{Gal}(\mathfrak{f}^m/\mathfrak{f}) \to \text{Gal}(\mathfrak{f}^n/\mathfrak{f})$ for $n \mid m$, $m, n \geq 1$. As explained in general in Section 3.1, each $\sigma$ in $\text{Gal}(k_{ur}/k)$ induces an automorphism $\sigma'$ in $\text{Gal}(\mathfrak{f}_K/\mathfrak{f})$. However, by Proposition 2.11, the map $\sigma \mapsto \sigma'$ induces an isomorphism $\text{Gal}(k_{ur}^n/k) \simeq \text{Gal}(\mathfrak{f}^n/\mathfrak{f})$ for each $n \geq 1$. 

Hence it follows that $\sigma \mapsto \sigma'$ defines an isomorphism $\text{Gal}(k_{ur}/k) \cong \text{Gal}(f_K/f)$.

Since $\bar{f} = \mathbb{F}_q$, the map $\omega \mapsto \omega^q$, $\omega \in \bar{f}_K$, defines an automorphism of $\bar{f}_K$ over $\bar{f}$. Let $\varphi$ denote the corresponding element in $\text{Gal}(k_{ur}/k)$ under $\text{Gal}(k_{ur}/k) \cong \text{Gal}(\bar{f}_K/\bar{f})$—namely, the unique element in $\text{Gal}(k_{ur}/k)$ satisfying

$$\varphi(\alpha) = \alpha^q \mod p_K, \quad \text{for all } \alpha \in \mathfrak{o}_K, \quad K = k_{ur}.$$

As $\varphi$ is uniquely associated with the local field $k$ (with $\Omega$ fixed) in this manner, it is called the Frobenius automorphism of $k_{ur}/k$, or, of $k$, and is denoted by $\varphi_k$. It is clear that $\varphi_k$ induces on each $k_{ur}^n$, $n \geq 1$, the Frobenius automorphism $\varphi_n$ of $k_{ur}^n/k$ (cf. Section 2.3). Since $\text{Gal}(k_{ur}^n/k)$ is the cyclic group of order $n$ generated by $\varphi_n$, the map $a \mod n \mapsto \varphi_n^a$, $a \in \mathbb{Z}$, defines an isomorphism

$$\mathbb{Z}/n\mathbb{Z} \cong \text{Gal}(k_{ur}^n/k).$$

For $n \mid m$, let $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be the natural homomorphism defined by $a \mod m \mapsto a \mod n$, $a \in \mathbb{Z}$, and let

$$\hat{\mathbb{Z}} = \lim \leftarrow \mathbb{Z}/n\mathbb{Z}$$

with respect to those maps for $n \mid m$. Since $\varphi_m \mid k_n = \varphi_k \mid k_n = \varphi_n$ for $n \mid m$, the diagram

$$\begin{array}{ccc}
\mathbb{Z}/m\mathbb{Z} & \twoheadrightarrow & \text{Gal}(k_{ur}^m/k) \\
\downarrow & & \downarrow \\
\mathbb{Z}/n\mathbb{Z} & \twoheadrightarrow & \text{Gal}(k_{ur}^n/k)
\end{array}$$

is commutative. Hence we obtain an isomorphism of profinite (totally disconnected, compact) abelian groups:

$$\hat{\mathbb{Z}} \cong \text{Gal}(k_{ur}/k) = \lim \leftarrow \text{Gal}(k_{ur}^n/k). \quad (3.1)$$

Now, the natural homomorphisms $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $n \geq 1$, induce a monomorphism $\mathbb{Z} \to \hat{\mathbb{Z}}$ so that $\mathbb{Z}$ may be regarded as a dense subgroup of $\hat{\mathbb{Z}}$. In the isomorphism (3.1), 1 in $\mathbb{Z}$ is then mapped to the Frobenius automorphism $\varphi_k$ of $k$ so that (3.1) induces

$$\mathbb{Z} \cong \langle \varphi_k \rangle,$$

$$n \mapsto \varphi_n^a$$

between the subgroups. Since $\mathbb{Z}$ is dense in $\hat{\mathbb{Z}}$, the cyclic group $\langle \varphi_k \rangle$ is dense in $\text{Gal}(k_{ur}/k)$. Hence $k$ is the fixed field of $\varphi_k$ in $k_{ur}$ and the topological isomorphism (3.1) is uniquely characterized by the fact that $1 \mapsto \varphi_k$.

**Remark.** For each prime number $p$, let $\mathbb{Z}_p^+$ denote the additive group of
all $p$-adic integers. It is easy to see that $\hat{\mathbb{Z}}$ is topologically isomorphic to the direct product of the compact groups $\mathbb{Z}_p^+$ for all prime numbers $p$.

Let $k$ be a $p$-field so that $q$ is a power of $p$, and let $V_\infty$ be the multiplicative group of all roots of unity in $\Omega$ with order prime to $p$. For $n \geq 1$, let $V_n$ denote the subgroup of all $(q^n - 1)^{\text{st}}$ roots of unity in $\Omega$. Then

$$V_\infty = \bigcup_{n \geq 1} V_n.$$ 

Since $k_{ur}^n$ is the splitting field of $X^{q^n} - X$ over $k$ in $\Omega$, we have

$$k_{ur}^n = k(V_n), \quad k_{ur} = k(V_\infty). \quad (3.2)$$

On the other hand, we see from Proposition 2.3 that the canonical ring homomorphism $\varphi_K : \mathfrak{t}_K = \mathfrak{p}_K$ induces an isomorphism

$$V_\infty \cong \mathfrak{t}_K^\mathfrak{e}. \quad (3.3)$$

Hence it follows from $\varphi_k(\eta) \equiv \eta^q \mod \mathfrak{p}_K$ that

$$\varphi_k(\eta) = \eta^q, \quad \text{for } \eta \in V_\infty. \quad (3.4)$$

The above equality also uniquely characterizes the Frobenius automorphism $\varphi_k$ of $k$.

Let $k'$ be any finite extension of $k$ in $\Omega$ so that $k'$ is again a local field. Then it follows from (3.2) that $k'k_{ur} = k'(V_\infty)$. Hence $k'k_{ur}$ is the maximal unramified extension $k'_{ur}$ over $k'$ in $\Omega$:

$$k'_{ur} = k'k_{ur}.$$ 

Let $\varphi_k'$ be the Frobenius automorphism of $k'$ and let $f = f(k'_{ur}/k)$. Then $\mathfrak{f}' = \mathbb{F}_q^f$ with $q' = q^f$ for the residue field $\mathfrak{f}'$ of $k'$. Hence $\varphi_k'(\eta) = \eta^{q'} = \eta^{qf}$ for all $\eta \in V_\infty$, and it follows that

$$\varphi_k' | k_{ur} = \varphi_k^f, \quad \text{with } f = f(k'_{ur}/k).$$

Now, let $F$ be an algebraic extension of $k$ in $\Omega$: $k \subseteq F \subseteq \Omega$. Similarly as for unramified extensions, we define $F/k$ to be a totally ramified extension if every $k'$ such that $k \subseteq k' \subseteq F$, $[k' : k] < +\infty$, is a totally ramified extension—that is, $f(k'/k) = 1$. Clearly, if $k \subseteq F' \subseteq F$ and $F/k$ is totally ramified, then $F'/k$ is also totally ramified. Let $k'$ be any finite extension of $k$ in $\Omega$ and let $k_0$ denote the inertia field of the extension $k'/k$ (cf. Proposition 2.12). Then $k_0 = k' \cap k_{ur}$ and $[k_0 : k] = f(k'/k)$ by Proposition 2.12. Therefore $k'/k$ is totally ramified if and only if $k' \cap k_{ur} = k$. It follows that in general $F/k$ is totally ramified if and only if

$$F \cap k_{ur} = k.$$ 

Let $L$ be an algebraic extension of $k$ such that

$$L = Fk_{ur}, \quad k = F \cap k_{ur}.$$ 

Then $L/F$ is a Galois extension, and the restriction map $\sigma \mapsto \sigma | k_{ur}$ defines
an isomorphism
\[ \text{Gal}(L/F) \cong \text{Gal}(k_{ur}/k). \]
Hence there exists a unique element \( \psi \) in \( \text{Gal}(L/F) \) such that \( \psi \mid k_{ur} = \varphi_k \), the Frobenius automorphism of \( k \). In other words, \( \varphi_k \) has a unique extension \( \psi \) in \( \text{Gal}(L/F) \). Let \( F \subseteq F' \subseteq L \). Then it follows from the above isomorphism that
\[ [F' \cap k_{ur} : k] = [F' : F]. \]
Hence \( F'/k \) is totally ramified only when \( F' = F \), and we see that \( F \) is a maximal totally ramified extension over \( k \) contained in \( L \).

**Lemma 3.4.** Let \( E \) be a Galois extension over \( k \), containing \( k_{ur} \). Let \( \psi \) be an element of \( \text{Gal}(E/k) \) such that \( \psi \mid k_{ur} = \varphi_k \) and let \( F \) be the fixed field of \( \psi \) in \( E \). Then
\[ Fk_{ur} = E, \quad F \cap k_{ur} = k, \quad \text{Gal}(E/F) \cong \text{Gal}(k_{ur}/k). \]
In particular, \( F \) is a maximal totally ramified extension over \( k \) in \( E \).

**Proof.** Clearly \( F \cap k_{ur} \) is the fixed field of \( \varphi_k = \psi \mid k_{ur} \) in \( k_{ur} \). Hence \( F \cap k_{ur} = k \). Let \( M \) be any field such that
\[ F \subseteq M \subseteq E, \quad [M : F] = n < +\infty, \]
and let \( F' = Fk_{ur}^n, F'' = F'M \). Since \( F \cap k_{ur} = k \), we have \([F' : F] = n \). Hence \( F'' \) is a finite extension over \( F \), containing both \( M \) and \( F' \). As \( F \) is the fixed field of \( \psi \) in \( E \), \( \langle \psi \rangle \) is dense in \( \text{Gal}(E/F) \) so that \( \text{Gal}(F''/F) \) is a finite cyclic group, generated by \( \psi \mid F'' \). Therefore it follows from \([M : F] = [F' : F] = n \) that \( M = F' = Fk_{ur}^n \subseteq Fk_{ur} \). Since this holds for any \( M \), we obtain \( Fk_{ur} = E \).

### 3.3. The Norm Groups

For each algebraic extension \( F/k \), \( k \subseteq F \subseteq \Omega \), let \( U(F) \) denote the unit group of \( F \):
\[ U(F) = \text{Ker}(\mu_F : F^\times \to \mathbb{R}^+). \]

**Lemma 3.5.** Let \( k'/k \) be a finite extension: \( k \subseteq k' \subseteq \Omega \). Then \( N_{k'/k}(U(k')) \) is a compact subgroup of \( U = U(k) \), and \( N_{k'/k}(k'^\times) \) is a closed subgroup of \( k^\times \).

**Proof.** By Proposition 1.6, the norm map \( N_{k'/k} : k' \to k \) is continuous, and by Proposition 2.6, \( U(k') \) is compact. Hence \( N_{k'/k}(U(k')) \) is a compact subgroup of \( k^\times \) and is closed in \( k^\times \). Furthermore, the formula for \( v'(x') \) in Proposition 1.5 shows
\[ N_{k'/k}(U(k')) = N_{k'/k}(k'^\times) \cap U(k) \subseteq U = U(k). \]
Since \( U \) is open in \( k^\times \), it follows from the above that \( N_{k'/k}(k'^\times)/N_{k'/k}(U(k')) \) is a discrete subgroup of \( k^\times/N_{k'/k}(U(k')) \). Hence \( N_{k'/k}(k'^\times) \) is closed in \( k^\times \).
Infinite Extensions of Local Fields

For any algebraic extension \( F/k \), we now define
\[
N(F/k) = \bigcap_k N_{k'/k}(k'^\times), \quad NU(F/k) = \bigcap_k N_{k'/k}(U(k')),
\]
where the intersections are taken over all fields \( k' \) such that
\[
k \subseteq k' \subseteq F, \quad [k':k] < +\infty.
\]
We call \( N(F/k) \), and \( NU(F/k) \) the norm group and the unit norm group of the extension \( F/k \), respectively. Clearly, if \( F/k \) is finite, then \( N(F/k) = N_{F/k}(F^\times) \), \( NU(F/k) = N_{F/k}(U(F)) \). In general, it follows from Lemma 3.5 that \( N(F/k) \) is a closed subgroup of \( k^\times \) and \( NU(F/k) \) is a compact subgroup of \( U = U(k) \). In fact,
\[
NU(F/k) = N(F/k) \cap U(k).
\]
It is clear from the definition that if \( k \subseteq F \subseteq F' \subseteq \Omega \), then
\[
N(F'/k) \subseteq N(F/k), \quad NU(F'/k) \subseteq NU(F/k).
\]
Furthermore, if \( \{k_i\} \) is a family of fields such that
\[
k \subseteq k_i \subseteq F, \quad [k_i:k] < +\infty, \quad F = \text{the union of all } k_i,
\]
then
\[
N(F/k) = \bigcap_i N_{k_i/k}(k_i), \quad NU(F/k) = \bigcap_i N_{k_i/k}(U(k_i)).
\]
We shall next consider such norm groups for unramified extensions and totally ramified extensions.

**Lemma 3.6.** Let \( k'/k \) be a finite unramified extension. Then
\[
NU(k'/k) = U(k).
\]

**Proof.** As before, let \( \mathfrak{f} \) and \( \mathfrak{f}' \) denote the residue field of \( k \) and \( k' \), respectively. By (1.3), a prime element \( \pi \) of \( k \) defines isomorphisms
\[
U/U_1 \cong \mathfrak{f}_1^\times, \quad U_i/U_{i+1} \cong \mathfrak{f}_i^+, \quad \text{for } i \geq 1,
\]
where \( U = U_0 = U(k) \) and \( U_i = 1 + p^i, \ i \geq 1 \). Now, as \( k'/k \) is unramified, \( \pi \) is also a prime element of \( k' \) (cf. Section 2.3). Hence it also defines similar isomorphisms for \( k' \):
\[
U'/U'_1 \cong \mathfrak{f}'_1^\times, \quad U'_i/U'_{i+1} \cong \mathfrak{f}'_i^+, \quad \text{for } i \geq 1,
\]
where \( U' = U'_0 = U(k') \). \( U'_i = 1 + p'^i, \ i \geq 1 \). By Proposition 2.11, there is a natural isomorphism \( \text{Gal}(k'/k) \cong \text{Gal}(\mathfrak{f}'/\mathfrak{f}) \). Therefore, we obtain the following commutative diagrams:
\[
\begin{array}{ccc}
U'/U'_1 & \xrightarrow{\sim} & \mathfrak{f}'_1^\times \\
\downarrow N & & \downarrow N' \\
U/U_1 & \xrightarrow{\sim} & \mathfrak{f}_1^\times
\end{array}
\begin{array}{ccc}
U'_i/U'_{i+1} & \xrightarrow{\sim} & \mathfrak{f}'_i^+ \\
\downarrow N & & \downarrow T' \\
U_i/U_{i+1} & \xrightarrow{\sim} & \mathfrak{f}_i^+
\end{array}
\]
where \( N = N_{k'/k} \), and \( T' \), \( N' \) are the trace map and the norm map of the extension \( f'/f \), respectively. However, since \( f'/f \) is an extension of finite fields, both \( T' \) and \( N' \) are surjective maps. Hence it follows from the above diagrams that the maps \( N \) are also surjective so that

\[
N_{k'/k}(U')U_i = U, \quad \text{for all } i \geq 1.
\]

Since \( N_{k'/k}(U') \) is compact, hence, closed, in \( U \), we obtain \( N_{k'/k}(U') = U \).

**Proposition 3.7.** Let \( F/k \) be an unramified algebraic extension. then

\[
NU(F/k) = U(k).
\]

If, furthermore, \( F/k \) is an infinite extension, then

\[
N(F/k) = U(k).
\]

In particular,

\[
N(k_{ur}/k) = NU(k_{ur}/k) = U(k).
\]

**Proof.** The first part is an immediate consequence of Lemma 3.6. Let \( k'/k \) be the unramified extension of degree \( n \geq 1 \): \( k' = k'_{ur} \). Then a prime element \( \pi \) of \( k \) is also a prime element of \( k' \) so that \( k'^{\times} = (\pi) \times U(k') \). Hence

\[
N_{k'/k}(k'^{\times}) = (\pi^n) \times N_{k'/k}(U(k')) = (\pi^n) \times U(k)
\]

\[
\subseteq k^{\times} = (\pi) \times U(k).
\]

If \( F/k \) is an infinite extension, there exists \( k' \) such that \( k \subseteq k' \subseteq F \) with arbitrarily large \( n = [k':k] \). Hence the second part is proved.

**Proposition 3.8.** An algebraic extension \( F/k \) is totally ramified if and only if \( N(F/k) \) contains a prime element of \( k \).

**Proof.** Suppose first that \( F \) is not totally ramified—that is, \( F \cap k_{ur} \neq k \). Then \( k \subseteq k_{ur}^{n} \subseteq F \) for some \( n \geq 2 \), and the proof of Proposition 3.6 shows that

\[
N(F/k) \subseteq N(k_{ur}^{n}/k) = (\pi^n) \times U(k).
\]

Since \( n \geq 2 \), \( N(F/k) \) contains no prime element of \( k \).

Suppose next that \( F/k \) is totally ramified. For each finite extension \( k'/k \) such that \( k \subseteq k' \subseteq F \), let \( S(k') \) denote the set of all prime elements of \( k \), contained in \( N(k'/k) \). Let \( \pi' \) be a prime element of \( k' \). Since \( k'/k \) is totally ramified, \( N_{k'/k}(\pi) \) is then a prime element of \( k \) (cf. Section 2.3), and we see

\[
S(k') = N_{k'/k}(\pi' U(k')) = N_{k'/k}(\pi')NU(k'/k).
\]

Hence \( S(k') \) is a non-empty compact subset of the compact set \( S(k) = \pi U(k) \), \( \pi \) being a prime element of \( k \). Furthermore, if both \( k'_1/k \) and \( k'_2/k \) are finite extensions in \( F \), then clearly \( S(k'_1/k'_2) \subseteq S(k'_1) \cap S(k'_2) \). Therefore, it follows from the compactness of \( S(k) \) that the intersection of \( S(k') \) for all \( k' \)
is non-empty, and any element in that intersection is a prime element of $k$, contained in $N(F/k)$.

3.4. Formal Power Series

In general, for any commutative ring $R$ with identity $1 \neq 0$, let

$$S = R[[X_1, \ldots, X_n]]$$

denote the commutative ring of all formal power series

$$f(X_1, \ldots, X_n) = \sum_{i} a_{i_1, \ldots, i_n} X_1^{i_1} \cdots X_n^{i_n}, \quad a_{i_1, \ldots, i_n} \in R,$$

where $X_1, \ldots, X_n$ are indeterminates and $i = (i_1, \ldots, i_n)$ ranges over all $n$-tuples of integers $\geq 0$. For $f, g \in S$ and for any integer $d \geq 0$, we write

$$f \equiv g \text{ mod } d$$

if the power series $f - g$ contains no terms of total degree less than $d$. Let $Y_1, \ldots, Y_m$ be another set of indeterminates that let $g_1, \ldots, g_n$ be power series in $R[[Y_1, \ldots, Y_m]]$ such that $g_i \equiv 0 \text{ mod } d$ for $1 \leq i \leq n$. For any $f(X_1, \ldots, X_n)$ in $S$, one can then substitute $g_i$ for $X_i$, $1 \leq i \leq n$, and obtain a well-defined power series

$$f(g_1(Y_1, \ldots, Y_m), \ldots, g_n(Y_1, \ldots, Y_m))$$

in $R[[Y_1, \ldots, Y_m]]$. We shall often denote the above power series by $f \circ (g_1, \ldots, g_n)$.

Let $X$ be an indeterminate and let $M$ be the ideal of $R[[X]]$, generated by $X$: $M = (X) = X \cdot R[[X]]$. $M$ is the set of all $f(X)$ in $R[[X]]$ such that $f \equiv 0 \text{ mod } d$. Let $f, g \in M$. As a special case of the above $(n = m = 1)$, the power series $f \circ g$ is defined and it again belongs to $M$. Thus $M$ becomes a semi-group with respect to the multiplication $f \circ g$ and the power series $X$ is the identity element of this semi-group: $X \circ f = f \circ X = f$. Hence, if $f \circ g = g \circ f = X$ for $f, g \in M$, we write $f = g^{-1}$, $g = f^{-1}$. Let

$$f(X) = \sum_{n=1}^{\infty} a_n X^n, \quad a_n \in R.$$ 

Then $f$ is invertible (i.e., it has the inverse $f^{-1}$) in $M$ if and only if $a_1$ is invertible in the ring $R$—that is, $a_1 b = 1$ for some $b$ in $R$.

In the following, we consider the case where $R$ is a topological ring. In such a case, we introduce a topology on $S = R[[X_1, \ldots, X_n]]$ so that the map

$$f = \sum_{i} a_{i_1, \ldots, i_n} X_1^{i_1} \cdots X_n^{i_n} \rightarrow \{a_{i_1, \ldots, i_n}\}_{i_1, \ldots, i_n \geq 0}$$

defines a homeomorphism of $S$ onto the direct product of infinitely many copies of the topological space $R$, indexed by $i = (i_1, \ldots, i_n)$. $S$ then becomes a topological ring.
As in Section 3.1, let
\[ f_\Omega = \mathfrak{o}_\Omega / \mathfrak{p}_\Omega \]
be the residue field of \( \Omega \). We apply the above for the topological ring \( \mathfrak{o}_\Omega \). Let
\[ f = \sum_i a_{i_1, \ldots, i_n} X_1^{i_1} \cdots X_n^{i_n}, \quad a_{i_1, \ldots, i_n} \in \mathfrak{o}_\Omega, \]
and let \( g_1, \ldots, g_n \) be power series in \( \mathfrak{o}_\Omega[[Y_1, \ldots, Y_m]] \) such that the constant terms of \( g_1, \ldots, g_n \) are contained in \( \mathfrak{p}_\Omega \). Then we can see easily that
\[ \sum_i a_{i_1, \ldots, i_n} g_1(Y_1, \ldots, Y_m)^{i_1} \cdots g_n(Y_1, \ldots, Y_m)^{i_n} \]
converges in \( \mathfrak{o}_\Omega[[Y_1, \ldots, Y_m]] \) in the above-mentioned topology on \( \mathfrak{o}_\Omega[[Y_1, \ldots, Y_m]] \). The resulting power series will be denoted again by \( f_\Omega(g_1, \ldots, g_n) \). In particular, for any \( \alpha_1, \ldots, \alpha_n \) in \( \mathfrak{p}_\Omega \), the value of \( f(X_1, \ldots, X_n) \) at \( X_1 = \alpha_1, \ldots, X_n = \alpha_n \)—namely, \( f(\alpha_1, \ldots, \alpha_n) \)—is well defined in \( \mathfrak{o}_\Omega \).

\textbf{Lemma 3.9.} Let \( \alpha \in \mathfrak{p}_\Omega \) and suppose \( f(\alpha) = 0 \) for a power series \( f(X) \) in \( \mathfrak{o}_\Omega[[X]] \). Then \( f(X) \) is divisible by \( X - \alpha \) in \( \mathfrak{o}_\Omega[[X]] \)—namely,
\[ f(X) = (X - \alpha)g(X), \quad \text{with } g(X) \in \mathfrak{o}_\Omega[[X]]. \]

\textit{Proof.} Let \( f(X) = \sum_{i=0}^\infty \alpha_i X^i, \alpha_i \in \mathfrak{o}_\Omega \), and let
\[ \beta_i = \sum_{j=0}^\infty a_{i+j+1} \alpha^j, \quad \text{for } i \geq 0. \tag{3.5} \]
Since \( \alpha \in \mathfrak{p}_\Omega \), such sums converge in \( \mathfrak{o}_\Omega \) and
\[ g(X) = \sum_{i=0}^\infty \beta_i X^i \]
satisfies \( f(X) = (X - \alpha)g(X) \).

In the above, let \( \alpha \) be algebraic over \( k \)—that is, \( \alpha \in \mathfrak{p}_\Omega \) (\( \alpha \in \Omega, \mu(\alpha) > 0 \))—and let \( f(X) \) be a power series in the subring \( \mathfrak{o}[[X]] \) of \( \mathfrak{o}_\Omega[[X]] \), \( \mathfrak{o} \) being the valuation ring of \( k \). Take a finite extension \( k' \) over \( k \) such that \( \alpha \in k' \subseteq \Omega \). Then \( k' \) is a local field and the infinite sum (3.5) converges in the valuation ring \( \mathfrak{o}' \) of \( k' \). Hence \( f(X) = (X - \alpha)g(X) \) holds with \( g(X) \in \mathfrak{o}'[[X]] \).

\textbf{Lemma 3.10.} Let \( h(X) \) be a monic polynomial in \( \mathfrak{o}[X] \) such that
\[ h(X) = \prod_{i=1}^m (X - \alpha_i) \]
with distinct \( \alpha_1, \ldots, \alpha_m \) in \( \mathfrak{p}_\Omega \). Let \( f(X) \) be a power series in \( \mathfrak{o}[[X]] \) such that
\( f(\alpha_i) = 0 \) for \( 1 \leq i \leq m. \) Then

\[
f(X) = h(X)g(X)
\]

with a power series \( g(X) \) in \( \mathfrak{o}[[X]]. \)

**Proof.** Let \( k' = k(\alpha_1, \ldots, \alpha_n) \). Then \( k' \) is a finite Galois extension over \( k \) in \( \Omega \), and by the above remark, \( f(X) \) is divisible by \( h(X) = \prod_{i=1}^m (X - \alpha_i) \) in \( \mathfrak{o}'[[X]] \)—namely, \( f(X) = h(X)g(X) \) with \( g(X) \) in \( \mathfrak{o}'[[X]] \). For each \( \sigma \) in \( \text{Gal}(k'/k) \), let \( f^\sigma(X) \) denote the power series in \( \mathfrak{o}'[[X]] \) obtained from \( f(X) \) by replacing each coefficient \( \alpha \) of \( f(X) \) by \( \sigma(\alpha) \). Then we have \( f^\sigma(X) = h^\sigma(X)g^\sigma(X) \), where \( g^\sigma(X) \) and \( h^\sigma(X) \) are defined similarly as \( f^\sigma(X) \). Here, \( f^\sigma = f, \ h^\sigma = h \) because \( f, g \in \mathfrak{o}'[[X]] \subseteq k[[X]] \). Hence it follows from \( f = hg = hg^\sigma \) that \( g = g^\sigma \). As this holds for every \( \sigma \) in \( \text{Gal}(k'/k) \), \( g(X) \) is a power series in \( \mathfrak{o}'[[X]] \).

### 3.5. Power Series over \( \mathfrak{o}_K \)

As in Section 3.2, let \( K \) denote the maximal unramified extension of the local field \( k \) in \( \Omega : K = k_{ur} \). Let \( \varphi_k \) be the Frobenius automorphism of \( k : \varphi_k \in \text{Gal}(K/k) \), and let \( \bar{\varphi}_k \) be the natural extension of \( \varphi_k \) on the closure (completion) \( \bar{K} \) of \( K \) in \( \bar{\Omega} \) (cf. Section 3.1). For simplicity, we shall denote both \( \varphi_k \) and \( \bar{\varphi}_k \) by \( \varphi \). By definition, \( \varphi \) induces the automorphism \( \omega \mapsto \omega^q \) on the residue field \( f_k = f_{\bar{K}} = \mathfrak{o}_K / \mathfrak{p}_K \) so that

\[
a^\varphi = a^q \mod \mathfrak{p}_K, \quad \text{for all } a \in \mathfrak{o}_K.
\]

Now, let \( \mathfrak{o}_K \) also denote the additive group of the valuation ring \( \mathfrak{o}_K \) and let \( U(\bar{K}) \) be the multiplicative group of units in the complete field \( \bar{K} \). We consider the endomorphisms

\[
\varphi - 1 : \mathfrak{o}_K \to \mathfrak{o}_K,
\]

\[
\alpha \mapsto (\varphi - 1)(\alpha) = \varphi(\alpha) - \alpha,
\]

\[
\varphi - 1 : U(\bar{K}) \to U(\bar{K}),
\]

\[
\xi \mapsto \xi^q = \varphi(\xi)/\xi.
\]

**Lemma 3.11.** The following sequences are exact:

\[
0 \to \mathfrak{o}_k \to \mathfrak{o}_{\bar{K}} \to \mathfrak{o}_{\bar{K}} \to 0,
\]

\[
1 \to U(k) \to U(\bar{K}) \to U(\bar{K}) \to 1.
\]

**Proof.** Since the proofs are similar in both cases, we shall prove here only the exactness of the second sequence. By Proposition 3.3, \( f_{\bar{K}} \) (= \( f_K \)) is algebraically closed. Hence the maps \( f_{\bar{K}} \to f_{\bar{K}} \) defined by \( \omega \mapsto \omega^q - \omega \) and \( \omega \mapsto \omega^{q-1} \) are both surjective. This implies that

\[
(\varphi - 1)\mathfrak{o}_K + \mathfrak{p}_K = \mathfrak{o}_K, \quad U(\bar{K})^{q-1}(1 + \mathfrak{p}_K) = U(\bar{K}). \tag{3.6}
\]
Let \( \xi \in U(\bar{K}) \). We shall define, by induction, a sequence of elements \( \{\eta_n\}_{n \geq 0} \) in \( U(\bar{K}) \) satisfying
\[
\xi = \eta_{n+1}^{q^{-1}} \mod p_K^{n+1}, \quad \eta_n = \eta_{n+1} \mod p_K^{n+1}, \quad \text{for all } n \geq 0. \tag{3.7}
\]
By (3.6), there exists \( \eta_0 \in U(\bar{K}) \) such that \( \xi \equiv \eta_0^{q^{-1}} \mod p_K \). Hence, suppose that we have found \( \eta_0, \eta_1, \ldots, \eta_n, \) \( n \geq 0 \), which satisfy the required conditions. Let \( \pi \) be a prime element of \( k \). Since \( K/k \) is unramified, \( \pi \) is then also a prime element of \( K \) and of \( \bar{K} \): \( p_K = \pi \circ \bar{k} \). Hence, by (3.7):
\[
\xi \eta_n^{q^{-1}} = 1 + \alpha \pi^{n+1}, \quad \text{with } \alpha \in \bar{k}.
\]
By (3.6), there exists \( \beta \in \bar{k} \) such that \( \alpha \equiv (\varphi - 1)\beta \mod p_K \). Let
\[
\eta_{n+1} = \eta_n (1 + \beta \pi^{n+1}).
\]
Then, clearly, \( \eta_{n+1} \in U(\bar{K}) \) and \( \eta_n = \eta_{n+1} \mod p_K^{n+1} \). Since \( \varphi(\pi) = \pi \) for \( \pi \in k \), we also have
\[
\eta_n^{q^{-1}} = \eta_n^{q^{-1}} (1 + (\varphi(\beta) - \beta) \pi^{n+1}) = \eta_n^{q^{-1}} (1 + \alpha \pi^{n+1}) = \xi \mod p_K^{n+2}.
\]
Thus the existence of the sequence \( \{\eta_n\}_{n \geq 0} \) is proved. Since \( \bar{K} \) is complete, it then follows that \( \eta = \lim_{n \to \infty} \eta_n \) exists in \( U(\bar{K}) \) and satisfies \( \eta^{q^{-1}} = \xi \). Hence the exactness of \( U(\bar{K}) \to U(\bar{K}) \to 1 \) is verified.

It is obvious that \( U(k) \) is contained in the kernel of \( U(\bar{K}) \to U(\bar{K}) \). Suppose that \( \xi^{q^{-1}} = 1 \)—that is, \( \varphi(\xi) = \xi \)—for an element \( \xi \) in \( U(\bar{K}) \). It follows from (3.3) that the set \( A = \{0\} \cup V_\infty \) is a complete set of representatives for \( t_K (= t_{k}) \) in \( \bar{k} \). With \( \pi \) as above, it follows from Proposition 1.2 that the element \( \xi \) in \( U(\bar{K}) \subseteq \bar{k} \) can be uniquely expressed in the form
\[
\xi = \sum_{n=0}^{\infty} a_n \pi^n, \quad \text{with } a_n \in A = \{0\} \cup V_\infty.
\]
Applying \( \varphi \), we obtain
\[
\xi = \varphi(\xi) = \sum_{n=0}^{\infty} \varphi(a_n) \pi^n.
\]
However, by (3.4), \( \varphi(a) = a^q \in A \) for every \( a \in A \). Hence, by the uniqueness,
\[
a_n = \varphi(a_n) = a_n^q, \quad \text{for all } n \geq 0.
\]
Therefore, either \( a_n = 0 \) or \( a_n \) is an element of the cyclic group \( V \) of order \( q - 1 \) in Proposition 2.3. Consequently, \( \xi \in k \cap U(\bar{K}) = U(k) \), and the exactness of \( 1 \to U(k) \to U(\bar{K}) \to U(\bar{K}) \) is also proved. \( \square \)

Now, for each power series
\[
f(X_1, \ldots, X_n) = \sum_{i} a_{i_1, \ldots, i_n} X_1^{i_1} \cdots X_n^{i_n}, \quad a_{i_1, \ldots, i_n} \in \bar{k},
\]
in \( \bar{k}[[X_1, \ldots, X_n]] \), let \( f^\varphi \) denote the power series of \( \bar{k}[[X_1, \ldots, X_n]] \).
Infinite Extensions of Local Fields

defined by

\[ f^\varphi(X_1, \ldots, X_n) = \sum_i \varphi(a_{i_1, \ldots, i_n})X_1^{i_1} \cdots X_n^{i_n}. \]

By Lemma 3.2, \( \mu_K \equiv \mu | K \) is a normalized valuation on \( K \). Hence \( \mu_{\tilde{K}} \equiv \mu | \tilde{K} \) is a normalized valuation on the completion \( \tilde{K} \) of \( K \).

**Proposition 3.12.** Let \( \pi_1 \) and \( \pi_2 \) be prime elements of \( \tilde{K} \): \( \mu_{\tilde{K}}(\pi_1) = \mu_{\tilde{K}}(\pi_2) = 1 \), and let \( f_1 \) and \( f_2 \) be power series in \( \mathcal{O}_{\tilde{K}}[[X]] \) such that

\[ f_1(X) = \pi_1(X), \quad f_2(X) = \pi_2X \mod \deg 2, \quad f_1(X) = f_2(X) = X^q \mod \wp_{\tilde{K}}, \]

\( q \) being the number of elements in the residue field \( \mathfrak{r} \) of the ground field \( k \). Let

\[ L(X_1, \ldots, X_m) = \alpha_1X_1 + \cdots + \alpha_mX_m, \quad \alpha_i \in \mathcal{O}_{\tilde{K}} \]

be a linear form in \( X_1, \ldots, X_m \) over \( \mathcal{O}_{\tilde{K}} \) such that

\[ \pi_1L(X_1, \ldots, X_m) = \pi_2L^\varphi(X_1, \ldots, X_m). \]

Then there exists a unique power series \( F = F(X_1, \ldots, X_m) \) in \( \mathcal{O}_{\tilde{K}}[[X_1, \ldots, X_m]] \) such that

\[ F = L \mod \deg 2, \quad f_1 \circ F = F^\varphi \circ f_2, \]

namely,

\[ f_1(F(X_1, \ldots, X_m)) = F^\varphi(f_2(X_1), \ldots, f_2(X_m)). \]

**Proof.** Let \( F_1 = L \). Then the assumptions on \( f_1, f_2, \) and \( L \) imply

\[ f_1 \circ F_1 = F_1^\varphi \circ f_2 \mod \deg 2. \]

Let \( n \geq 1 \) and suppose that we have found a polynomial \( F_n \) of total degree \( \leq n \) in \( \mathcal{O}_{\tilde{K}}[X_1, \ldots, X_m] \) such that

\[ f_1 \circ F_n = F_n^\varphi \circ f_2 \mod \deg n + 1. \]

(3.8)

Let \( H_{n+1} \) be a homogeneous polynomial of degree \( n + 1 \) in \( \mathcal{O}_{\tilde{K}}[[X_1, \ldots, X_m]] \) and let

\[ F_{n+1} = F_n + H_{n+1}. \]

Then \( F_{n+1} \) is a polynomial of total degree \( \leq n + 1 \) in \( \mathcal{O}_{\tilde{K}}[X_1, \ldots, X_m] \) and it satisfies

\[ F_{n+1} = F_n \mod \deg n + 1. \]

We shall next show that there exists a unique \( H_{n+1} \) such that the above \( F_{n+1} \) satisfies

\[ f_1 \circ F_{n+1} = F_{n+1}^\varphi \circ f_2 \mod \deg n + 2. \]

(3.9)

To see this, let

\[ G_{n+1} = f_1 \circ F_n - F_n^\varphi \circ f_2. \]
Then, by (3.8), \( G_{n+1} = 0 \mod \deg n + 1 \). Since \( f_1 = \pi_1 X, f_2 = \pi_2 X \mod \deg 2 \),

\[
\begin{align*}
  f_1 \circ F_{n+1} &= f_1(F_n + H_{n+1}) \equiv f_1 \circ F_n + \pi_1 H_{n+1} \mod \deg n + 2, \\
  F_{n+1}^\varphi \circ f_2 &= F_n^\varphi \circ f_2 + H_{n+1}^\varphi \circ f_2 \equiv F_n^\varphi \circ f_2 + \pi_2^{n+1} H_{n+1}^\varphi \mod \deg n + 2.
\end{align*}
\]

Hence (3.9) is equivalent to the congruence

\[
G_{n+1} + \pi_1 H_{n+1} - \pi_2^{n+1} H_{n+1}^\varphi \equiv 0 \mod \deg n + 2. \tag{3.10}
\]

On the other hand, since \( f_1 = f_2 \equiv X^q \mod p_k \) and \( \alpha^\varphi = \alpha^q \mod p_k \) for \( \alpha \in \mathfrak{o}_k \), we see from the definition of \( G_{n+1} \) that

\[
G_{n+1} = F_n(X_1, \ldots, X_m)^q - F_n^\varphi(X_1^q, \ldots, X_m^q) \equiv 0 \mod p_k.
\]

Now, take a monomial \( X^i = X_1^{i_1} \cdots X_m^{i_m} \) of degree \( n + 1 \) in \( \mathfrak{o}_k[X_1, \ldots, X_m] \). By the above, the coefficient of \( X^i \) in \( G_{n+1} \) is an element of the form \(-\pi_1 \beta\) with \( \beta \in \mathfrak{o}_k \). Let \( \alpha \) be the coefficient of \( X^i \) in \( H_{n+1} \). Then the coefficient of the same \( X^i \) in \( \pi_1 H_{n+1} - \pi_2^{n+1} H_{n+1}^\varphi \) is \( \pi_1 \alpha - \pi_2^{n+1} \alpha^q \). Since \( G_{n+1} \equiv 0 \mod \deg n + 1 \), we see that (3.10) holds if and only if the coefficient \( \alpha \) of \( X^i \) in \( H_{n+1} \) satisfies

\[-\pi_1 \beta + \pi_1 \alpha - \pi_2^{n+1} \alpha^q = 0\]

for every monomial \( X^i \) of degree \( n + 1 \). Let \( \gamma = \pi_1^{-1} \pi_2^{n+1} \) so that \( \mu_k(\gamma) = n \geq 1 \). Then the above equation for \( \alpha \) can be written as

\[
\alpha - \gamma \alpha^q = \beta \tag{3.11}
\]

where \( \beta \) and \( \gamma \) are known quantities. However, since \( \mu_k(\gamma) \geq 1 \),

\[
\alpha = \beta + \gamma \beta^q + \gamma^1 \beta^q \beta^2 + \cdots \tag{3.12}
\]

converges in \( \mathfrak{o}_k \) and it obviously satisfies (3.11). Furthermore, if both \( \alpha_1 \) and \( \alpha_2 \) are solutions of (3.11), then

\[
\alpha_1 - \alpha_2 = \gamma (\alpha_1^q - \alpha_2^q),
\]

so that \( \mu_k(\alpha_1 - \alpha_2) = +\infty \), \( \alpha_1 = \alpha_2 \). Therefore, for each \( X^i \), the equation (3.11) has a unique solution \( \alpha \) in \( \mathfrak{o}_k \), and it follows that there exists a unique \( H_{n+1} \) satisfying (3.10), and so \( F_{n+1} \) satisfying (3.9). Now, starting from \( F_1 = L \), we can define successively a sequence of polynomials \( F_n, \ n \geq 1 \), in \( \mathfrak{o}_k[X_1, \ldots, X_m] \) such that \( \deg F_n \leq n \) and

\[
f_1 \circ F_n = F_n^\varphi \circ f_2, \quad F_{n+1} = F_n \mod \deg n + 1, \quad \text{for all } n \geq 1.
\]

The second congruence shows that there exists a power series \( F \) in \( \mathfrak{o}_k[[X_1, \ldots, X_m]] \) such that \( F = F_n \mod \deg n + 1 \) for all \( n \geq 1 \). It is then clear that this power series \( F \) satisfies

\[
F = F_1 = L \mod \deg 2, \quad f_1 \circ F = F^\varphi \circ f_2.
\]

Finally, to prove the uniqueness, let \( F' \) be any power series in \( \mathfrak{o}_k[[X_1, \ldots, X_m]] \), satisfying the conditions for \( F \) as above. For \( n \geq 1 \), let \( F'_n \)
denote the sum of the terms of degree \(\leq n\) in the power series \(F'\) and let \(F'_{n+1} = F'_n + H'_{n+1}\). Then \(F' \equiv L \mod \deg 2\) implies \(F'_1 = L = F_1\), and the uniqueness of \(H_{n+1}\) in the above proof yields successively \(F'_n = F_n\) for all \(n \geq 1\). Hence \(F' = F\).

Now, let \(k'\) be the unramified extension of degree \(n\) over \(k\) in \(\Omega : k' = k^n_{\text{ur}}\), \(k \subseteq k' \subseteq K \subseteq \bar{K}\), and let \(\mathcal{O}'\) denote the valuation ring of \(k'\). Let \(\pi_1\) and \(\pi_2\) be prime elements of \(k'\). Since \(K/k'\) is unramified, \(\pi_1\) and \(\pi_2\) are also prime elements of \(K\) and \(\bar{K}\). In the above proposition, suppose further that \(f_1, f_2 \in \mathcal{O}'[[X]]\) and \(L \in \mathcal{O}'[X_1, \ldots, X_m]\). Since \(k'\) is complete and \(\varphi(k') = k'\), the element \(\alpha\) in (3.11) belongs to \(\mathcal{O}'\), and it follows that the power series \(F\) in the proposition has coefficients in \(\mathcal{O}'\):

\[
F(X_1, \ldots, X_m) \in \mathcal{O}'[[X_1, \ldots, X_m]].
\]

(3.13)

This remark will be used often later.
Chapter IV

Formal Groups $F_f(X, Y)$

In this chapter, we shall first briefly explain the general notion of formal groups, and then study a certain family of formal groups over the ring $R = \mathcal{O}_K$, which will play an essential role in the subsequent chapters. Notations introduced in Chapter III will be retained.

4.1. Formal Groups in General

We shall first briefly discuss some fundamental facts on formal groups in general.† Let $R$ be a commutative ring with $1 \neq 0$ and let $X$, $Y$, and $Z$ be indeterminates. A power series $F(X, Y)$ in $R[[X, Y]]$ is called a formal group over $R$ if it satisfies the following conditions:

(i) $F(X, Y) \equiv X + Y \text{ mod } \deg 2$,

(ii) $F(F(X, Y), Z) = F(X, F(Y, Z))$,

(iii) $F(X, Y) = F(Y, X)$.

Note that (i) implies $F(0, 0) = 0$ so that both sides of (ii) are well-defined power series in $R[[X, Y, Z]]$. In the general theory of formal groups, a power series such as $F(X, Y)$ above is called, more specifically, a one-dimensional, commutative formal group (or, formal group law) over the ring $R$. However, we shall call it here simply a formal group, because no other type of formal groups will appear in the following.

Let $Y = Z = 0$ in (i) and (ii). Then we obtain

$$F(X, 0) \equiv X \text{ mod } \deg 2, \quad F(F(X, 0), 0) = F(X, 0).$$

From the first congruence, we see that $f(X) = F(X, 0)$ has an inverse $f^{-1}$ in $M = XR[[X]]$ in the sense of Section 3.4. It then follows from the second equality that $F(X, 0) = X$. Similarly, or by (iii), $F(0, Y) = Y$. Therefore,

$$F(X, Y) = X + Y + \sum_{i,j=1}^{\infty} c_{ij} X^i Y^j, \quad c_{ij} \in R,$

(4.1)

namely, $F$ contains no terms like $X^2$. We then see easily that the equation $F(X, Y) = 0$ can be uniquely solved for $Y$ in $M$—namely, that there is a unique power series

$$i_F(X) = -X + \sum_{i=2}^{\infty} b_i X^i, \quad b_i \in R,$$

such that

$$F(X, i_F(X)) = 0.$$

(4.2)

† For the theory of formal groups, see Fröhlich [8].
For \( f, g \in M = XR[[X]] \), let

\[
f \overset{f}{\mapsto} g = F(f(X), g(X)).
\]

Then \( f \overset{f}{\mapsto} g \) again belongs to \( M \), and it follows from (ii), (iii), and (4.2), that the set \( M \) forms an abelian group with respect to the addition \( f \overset{f}{\mapsto} g \), with inverse \( i_F(f) \) for \( f \). We denote it by \( M_F \).

Now, let \( G(X, Y) \) be another formal group over \( R \) and let \( f(X) \) be a power series in \( M = XR[[X]] \) such that

\[
f(F(X, Y)) = G(f(X), f(Y)). \tag{4.3}
\]

We call such \( f \) a morphism from \( F \) to \( G \), and write

\[
f : F \to G.
\]

If, in particular, \( f \) has the inverse \( f^{-1} \) in \( M \), then \( f^{-1} \) is a morphism from \( G \) to \( F \). In such a case, we call \( f \) an isomorphism and write

\[
f : F \cong G.
\]

As before, when there is no risk of confusion, an equality like (4.3) will be simply written as

\[
f \circ F = G \circ f.
\]

In general, if \( F(X_1, \ldots, X_m) \) is any power series in \( R[[X_1, \ldots, X_m]] \) and if \( f \in M = XR[[X]] \) is invertible in \( M : f^{-1} \in M \), then we define a power series \( F^f(X_1, \ldots, X_m) \) in \( R[[X_1, \ldots, X_m]] \) by

\[
F^f(X_1, \ldots, X_m) = f \circ F \circ f^{-1} = f(F(f^{-1}(X_1), \ldots, f^{-1}(X_m))).
\]

One checks easily that if \( F(X, Y) \) is a formal group over \( R \), then \( G = F^f \) is again a formal group over \( R \) and

\[
f : F \cong G.
\]

Let

\[
\text{Hom}_R(F, G) = \text{the set of all morphisms } f : F \to G,
\]

\[
\text{End}_R(F) = \text{Hom}_R(F, F).
\]

For simplicity, these will also be denoted by \( \text{Hom}(F, G) \) and \( \text{End}(F) \), respectively.

**Lemma 4.1.** \( \text{Hom}(F, G) \) is a subgroup of the abelian group \( M_G \), and \( \text{End}(F) \) is a ring with respect to the addition \( f \overset{f}{\mapsto} g \) and the multiplication \( f \circ g \).

**Proof.** Let \( f, g \in \text{Hom}(F, G) \) and let \( h = f \overset{f}{\mapsto} g \). Then

\[
h \circ F = f \circ F \overset{f}{\mapsto} g \circ F = G \circ f \overset{f}{\mapsto} G \circ g = G(G \circ f, G \circ g),
\]

where \( G \circ f = G(f(X), f(Y)) \), \( G \circ g = G(g(X), g(Y)) \). Using (ii), (iii), for \( G \),
we obtain
\[ G(G \circ f, G \circ g) = G(G(f(X), g(X)), G(f(Y), g(Y))) = G((f \circ_G g)(X), (f \circ_G g)(Y)) = G \circ h. \]

Hence \( h = f \circ_G g \) belongs to \( \text{Hom}(F, G) \). As stated earlier, \( i_G(f) = i_G \circ f \) is the inverse of \( f \) in the abelian group \( M_G \). Again by (ii), (iii), for \( G \), we obtain
\[ G(G(X, Y), G(i_G(X), i_G(Y))) = G(G(X, i_G(X)), G(Y, i_G(Y))) = G(0, 0) = 0, \]
that is, \( G \circ i_G = i_G \circ G \). Hence
\[ i_G(f) \circ F = i_G \circ f \circ F = i_G \circ G \circ f = G \circ i_G \circ f = G \circ i_G(f) \]
so that \( i_G(f) \in \text{Hom}(F, G) \). Since clearly \( 0 \in \text{Hom}(F, G) \), this proves that \( \text{Hom}(F, G) \) is a subgroup of \( M_G \). To see that \( \text{End}(F) \) is a ring, we have only to note that if \( f \in \text{End}(F) \), \( g, h \in M \), then
\[ f \circ (g \circ f) = f(F(g(X), h(X))) = f(f(g(X)), f(h(X))) = f \circ g \circ f. \]

Note also that \( X \) is the identity element of the ring \( \text{End}(F) \). 

Now, let \( \theta \) be an isomorphism from \( F \) to \( G \):
\[ \theta : F \cong G, \quad \text{that is, } F^\theta = G. \]

Let \( f \in \text{End}(F) : f \circ F = F \circ f \). Then we have
\[ f^\theta \circ F^\theta = F^\theta \circ f^\theta, \quad f^\theta \in \text{End}(G). \]

Since
\[ F(f, g)^\theta = F^\theta(f^\theta, g^\theta) = G(f^\theta, g^\theta), \quad (f \circ g)^\theta = f^\theta \circ g^\theta \]
for \( f, g \in \text{End}(F) \), we see that the map \( f \mapsto f^\theta \) defines a ring isomorphism
\[ \theta : \text{End}(F) \cong \text{End}(G). \]

Let
\[ G_a(X, Y) = X + Y. \]

Obviously \( G_a \) is a formal group over \( R \). It is called the additive (formal) group over \( R \).

**Lemma 4.2.** Suppose that \( R \) is a commutative algebra over the rational field \( \mathbb{Q} \). Then, for each formal group \( F(X, Y) \) over \( R \), there exists a unique isomorphism
\[ \lambda : F \cong G_a \]
such that \( \lambda(X) = X \mod \deg 2 \).

**Proof.** Let \( F_1 = \partial F / \partial Y \). Differentiating, with respect to \( Z \), both sides of
(ii) in the definition of $F(X, Y)$, we obtain
\[ F_i(F(X, Y), Z) = F_i(X, F(Y, Z))F_i(Y, Z). \]
Since $F(X, 0) = X$, it follows that
\[ F_i(F(X, Y), 0) = F_i(X, Y)F_i(Y, 0). \quad (4.4) \]
Now, as $F(X, Y) = X + Y \mod \deg 2$ implies $F_i(X, 0) = 1 \mod \deg 1$, there is a power series $\psi(X)$ in $R[[X]]$ such that
\[ \psi(X)F_i(X, 0) = 1, \quad \psi(X) = 1 + \sum_{n=1}^{\infty} a_n X^n, \quad a_n \in R. \]
Let
\[ \lambda(X) = X + \sum_{n=1}^{\infty} \frac{a_n}{n} X^n, \quad \text{with } \frac{a_n}{n} \in R, \]
so that $d\lambda/dX = \psi$. Then (4.4) can be written as
\[ \psi(F(X, Y))F_i(X, Y) = \psi(Y), \quad \text{that is, } \frac{\partial}{\partial Y} \lambda(F(X, Y)) = \frac{\partial}{\partial Y} \lambda(Y). \]
Therefore, $\lambda(F(X, Y)) = \theta(X) + \lambda(Y)$ with a power series $\theta(X)$ in $R[[X]]$. But, putting $Y = 0$ in this equality, we find that $\lambda(X) = \theta(X)$. Thus
\[ \lambda(F(X, Y)) = \lambda(X) + \lambda(Y), \quad \lambda : F \approx G_a. \]
To see the uniqueness of such $\lambda$, it is sufficient to consider the case $F = G_a$. Hence, let $\lambda : G_a \approx G_a$ be any automorphism of $G_a$, satisfying $\lambda(X) = X \mod \deg 2$. Then $\lambda \circ G_a = G_a \circ \lambda$—that is,
\[ \lambda(X + Y) = \lambda(X) + \lambda(Y), \quad \lambda(X) = X \mod \deg 2. \]
For $\lambda'(X) = d\lambda/dX$, we then have
\[ \lambda'(X + Y) = \lambda'(X), \quad \lambda'(X) = 1 \mod \deg 1. \]
Therefore, $\lambda'(Y) = \lambda'(0) = 1$. Since $R$ is a $\mathbb{Q}$-algebra, it follows that
\[ \lambda(X) = X. \]
Thus $\lambda$ is unique.

Remark. The lemma can be applied for formal groups over any field of characteristic $0$. Note also that the argument in the second half yields that $\text{End}(G_a)$ consists of precisely $aX$ for $a \in R$.

4.2. Formal Groups $F_f(X, Y)$

Let $(k, v)$ be a local field with residue field $\frak{f} = o/p = F_q$ and let $\Omega$, $\bar{\Omega}$, $K = k_{ur}$, $\bar{K}$, $\frak{f}_K = o_K/p_K$, $\varphi = \varphi_K = \bar{\varphi}_K$, and so on, be the same as in Section 3.5. We shall next define a special type of formal group $F_f(X, Y)$ over $R = o_K$. 


For each prime element \( \pi \) of \( \tilde{K} \), \( \mu_\tilde{K}(\pi) = 1 \), let \( \mathcal{F}_\pi \) denote the family of all power series \( f(X) \) in \( R[[X]] \) such that

\[
f(X) \equiv \pi X \mod \deg 2, \quad f(X) \equiv X^q \mod \mathfrak{p}_\tilde{K}.
\]

For example, the polynomial \( \pi X + X^q \) belongs to \( \mathcal{F}_\pi \). It is also clear that if \( f \in \mathcal{F}_\pi \), then \( f^q \in \mathcal{F}_{\varphi(\pi)} \). The union of the sets \( \mathcal{F}_\pi \), for all prime elements \( \pi \) of \( \tilde{K} \), will be denoted by \( \mathcal{F} \).

**Proposition 4.2.** For each \( f \in \mathcal{F}_\pi \), there exists a unique formal group \( F_f(X, Y) \) over \( R \) such that \( f \in \text{Hom}_R(F_f, F_f^q) \)—that is,

\[ f \circ F_f = F_f^q \circ f. \]

**Proof.** Apply Proposition 3.12 for \( \pi_1 = \pi_2 = \pi \), \( f_1 = f_2 = f \), and \( L(X, Y) = X + Y \), \( m = 2 \). Then there exists a unique power series \( F(X, Y) \) in \( R[[X, Y]] \) such that

\[
F(X, Y) \equiv X + Y \mod \deg 2, \quad f \circ F = F^q \circ f. \tag{4.5}
\]

Let

\[
F_1(X, Y, Z) = F(F(X, Y), Z), \quad F_2(X, Y, Z) = F(X, F(Y, Z)).
\]

It follows from (4.5) that

\[
F_1(X, Y, Z) \equiv F(X, Y) + Z \equiv X + Y + Z \mod \deg 2, \quad f \circ F_1 = F^q(f(F(X, Y)), f(Z)) \equiv F^q(F^q(f(X), f(Y)), f(Z)) = F_1^q \circ f.
\]

Similarly,

\[
F_2(X, Y, Z) \equiv X + Y + Z \mod \deg 2, \quad f \circ F_2 = F_2^q \circ f.
\]

Hence the uniqueness of Proposition 3.12 with \( L(X, Y, Z) = X + Y + Z \), \( m = 3 \), implies \( F_1 = F_2 \)—namely

\[
F(F(X, Y), Z) = F(X, F(Y, Z)).
\]

Next, let \( G(X, Y) = F(Y, X) \). Then

\[
G(X, Y) \equiv X + Y \mod \deg 2, \quad f \circ G = G^q \circ f.
\]

Since \( F(X, Y) \) is the only power series in \( R[[X, Y]] \) satisfying (4.5), we obtain \( F = G \)—namely,

\[
F(X, Y) = F(Y, X).
\]

Thus \( F(X, Y) \) is a formal group over \( R \). It is then clear that \( F^q \) is also a formal group over \( R \). Writing \( F_f \) for \( F \), we see that \( F_f \) is the unique formal group over \( R \) such that \( f \circ F_f = F_f^q \circ f \)—that is, \( f \in \text{Hom}(F_f, F_f^q) \). \( \blacksquare \)

Now, it follows from \( f \circ F_f = F_f^q \circ f \) that

\[
F_f^q \circ f^q = (F_f^q)^q \circ f^q,
\]
and this implies
\[ F_f^q = F_{f^q}, \quad \text{where } f^q \in \mathcal{F}_{q(\pi)}. \] (4.6)

Let \( f \) be again a power series in \( \mathcal{F} \) and let \( a \) be any element in the valuation ring \( \mathfrak{o} \) of \( k \). Applying Proposition 3.12 for \( L(X) = aX, m = 1 \), we see that there exists a unique power series \( \phi(X) \) in \( R[[X]] \) such that 
\( \phi(X) = aX \mod \deg 2, f \circ \phi = \phi^q \circ f \). We denote this power series \( \phi(X) \) by \([a]_f : \phi = [a]_f \). Thus \([a]_f \) is the unique power series in \( R[[X]] \) satisfying 
\[ [a]_f = aX \mod \deg 2, \quad f \circ [a]_f = [a]_f^q \circ f. \] (4.7)

**Proposition 4.4.** For each \( a \in \mathfrak{o} \), \([a]_f \) belongs to \( \text{End}_R(F_f) \), and the map 
\( a \mapsto [a]_f \) defines an injective ring homomorphism 
\[ \mathfrak{o} \to \text{End}_R(F_f). \]

**Proof.** Let \( \phi = [a]_f \). Then
\[
\begin{align*}
(f \circ \phi \circ F_f) & = \phi^q \circ f \circ F_f = \phi^q \circ F_f \circ f = (\phi \circ F_f)^q \circ f, \\
(f \circ F_f \circ \phi) & = F_f^q \circ f \circ \phi = F_f^q \circ \phi^q \circ f = (F_f \circ \phi)^q \circ f, \\
\phi \circ F_f & = F_f \circ \phi = a(X + Y) \mod \deg 2.
\end{align*}
\]

Hence, by the uniqueness of Proposition 3.12,
\[ \phi \circ F_f = F_f \circ \phi, \quad \text{that is, } [a]_f \in \text{End}_R(F_f). \]

Let \( a, b \in \mathfrak{o} \), then
\[
f \circ ([a]_f + [b]_f) = f \circ F_f([a]_f, [b]_f) = F_f(f \circ [a]_f, f \circ [b]_f) = F_f^q([a]_f^q \circ f, [b]_f^q \circ f) = (\phi \circ F_f)^q \circ f,
\]
\[ [a]_f + [b]_f = a + b \mod \deg 2.
\]

By the Definition (4.7) for \([a + b]_f \), we then see
\[ [a]_f + [b]_f = [a + b]_f. \]

Similarly,
\[ [a]_f \circ [b]_f = [ab]_f. \]

Hence \( a \mapsto [a]_f \) defines a ring homomorphism \( \mathfrak{o} \to \text{End}_R(F_f) \). Since 
\([a]_f = aX \mod \deg 2 \), the homomorphism is injective.

Let \( \pi \) and \( \pi' \) be prime elements of \( \mathcal{K} \) and let \( f \in \mathcal{F}_\pi, f' \in \mathcal{F}_{\pi'} \). We shall next compare the formal groups \( F_f \) and \( F_{f'} \) over \( R = \mathfrak{o}_K \). Since \( \mu_K(\pi) = \mu_K(\pi') = 1 \),
\[ \pi' = \pi \xi, \quad \text{with } \xi \in U(\mathcal{K}). \]
By Lemma 3.11, there exists an element $\eta$ of $U(\tilde{K})$ such that

$$\xi = \eta^{q-1}.$$  

Let $L(X) = \eta X$. Then

$$\pi' L(X) = \pi L^q(X).$$

Hence, applying Proposition 3.12 for $f_1 = f'$, $f_2 = f$, $\pi_1 = \pi'$, $\pi_2 = \pi$, $L(X) = \eta X$, $m = 1$, we see that there exists a unique power series $\theta(X)$ in $R[[X]]$ such that

$$\theta(X) = \eta X \mod \deg 2, \quad f' \circ \theta = \theta^q \circ f. \quad (4.8)$$

Since $\eta \in U(\tilde{K})$, $\theta(X)$ is invertible in $M = XR[[X]]: \theta^{-1} \in M$.

**Proposition 4.5.** The above $\theta(X)$ has the following properties:

$$\theta : F_f \simeq F'_{f'}, \quad \text{that is, } F^\theta_f = F'_{f'}, \quad [a]^\theta_f = [a]_{f'}, \quad \text{for } a \in o.$$  

**Proof.**

$$f' \circ \theta \circ F_f = \theta^q \circ f \circ F_f = \theta^q \circ F^\theta_f \circ f = (\theta \circ F_f)^q \circ f,$$

$$f' \circ F^\theta_f \circ \theta = F^\theta_{f'} \circ f' \circ \theta = F^\theta_{f'} \circ \theta^q \circ f = (F^\theta_f \circ \theta)^q \circ f,$$

$$\theta \circ F_f = F^\theta_f \circ \theta = \eta(X + Y) \mod \deg 2.$$

Hence, by the uniqueness of Proposition 3.12 with $L(X, Y) = \eta(X + Y)$,

$$\theta \circ F_f = F_{f'} \circ \theta, \quad \text{that is, } F^\theta_f = F_{f'}.$$  

The proof for $[a]^\theta_f = [a]_{f'}$ is similar. \[\square\]

It follows in particular from the above proposition that the formal groups $F_f$ over $R$ are isomorphic to each other for all power series $f$ in the family $\mathcal{F}$. The isomorphism $\theta(X)$ in this proposition will be used quite often in the sequel.

**Example.** Let $k$ be the $p$-adic number field: $k = Q_p$, and let $\pi = p$. Then

$$f(X) = (1 + X)^p - 1 = pX + \binom{p}{2}X^2 + \cdots + X^p$$

belongs to the family $\mathcal{F}_p$. Let

$$F(X, Y) = (1 + X)(1 + Y) - 1 = X + Y + XY.$$  

One checks immediately that $F$ is a formal group over $Z_p$, hence over $R = o_K$, satisfying $f \circ F = F^q \circ f$. Therefore,

$$F_f = F = X + Y + XY.$$  

For each $a \in Z_p$, define

$$(1 + X)^a = \sum_{n=0}^{\infty} \binom{a}{n}X^n$$
where
\[
\binom{a}{n} = \frac{a(a - 1) \cdots (a - n + 1)}{n!} \in \mathbb{Z}_p \quad \text{for } n \geq 0.
\]

Then it follows from the definition of \([a]_f\) in (4.8) that
\[
[a]_f = (1 + X)^a - 1 = \sum_{n=1}^{\infty} \binom{a}{n} X^n, \quad \text{for } a \in \mathbb{Z}_p.
\]

For \(n \geq 0\), let (cf. Section 4.3 below)
\[
W^n_f = \{ \alpha \in \mathcal{V}_\bar{\Omega} \mid [p^{n+1}]_f(\alpha) = 0 \}.
\]

Since \([p^{n+1}]_f(X) = (1 + X)^{p^{n+1}} - 1\),
\[
W^n_f = \{ \xi - 1 \mid \xi \in \mathcal{V}_\bar{\Omega}, \xi^{p^{n+1}} = 1 \}.
\]

Hence \(\mathbb{Q}_p(W^n_f)\) is the cyclotomic field of \(p^{n+1}\)th roots of unity over \(\mathbb{Q}_p\) in \(\Omega\). It is a well-known classical fact that such a cyclotomic field \(\mathbb{Q}_p(W^n_f)\) is an abelian extension over \(\mathbb{Q}_p\) and that the Galois group of \(\mathbb{Q}_p(W^n_f)/\mathbb{Q}_p\) is naturally isomorphic to the factor group \(\mathbb{Z}_p^*/(1 + p^{n+1}\mathbb{Z}_p)\). In the following sections, we shall show in general that similar results can be proved for an arbitrary local field \((k, \nu)\) and for the extension \(k(W^n_f)\), defined by means of the formal group \(F_f(X, Y)\) introduced above.

### 4.3. The \(\mathfrak{o}\)-Modules \(W^n_f\)

As before, let \(\mathfrak{o}_\bar{\Omega}/\mathcal{V}_\bar{\Omega}\) be the residue field of the completion \(\bar{\Omega}\) of a fixed algebraic closure \(\Omega\) of \(k\). For simplicity, let \(m\) denote the maximal ideal \(\mathcal{V}_\bar{\Omega}\) of \(\mathfrak{o}_\bar{\Omega}\):

\[
m = \mathcal{V}_\bar{\Omega} = \{ \alpha \in \bar{\Omega} \mid \tilde{\mu}(\alpha) > 0 \}.
\]

Let \(\bar{K}\) be the completion of \(K = k_{ur}\) and let \(F_f(X, Y)\) be the formal group over \(R = o_{\bar{K}}\) in Section 4.2, associated with a power series \(f\) in the family \(\mathcal{F}\). For \(\alpha, \beta \in m\) and for any \(a\) in the valuation ring \(\mathfrak{o}\) of the ground field \(k\), let

\[
\alpha \hat{+} \beta = F_f(\alpha, \beta), \quad a \cdot \alpha = [a]_f(\alpha), \quad (4.9)
\]

\([a]_f(X)\) being the power series in (4.7). By the general remark in Section 3.4, both \(F_f(\alpha, \beta)\) and \([a]_f(\alpha)\) are well defined in \(\mathfrak{o}_{\bar{\Omega}}\). Furthermore, it follows from \(F_f(X, Y) \equiv 0, [a]_f(X) \equiv 0 \mod \deg 1\) that those elements again belong to \(m \subseteq \mathfrak{o}_{\bar{\Omega}}\):

\[
\alpha \hat{+} \beta, a \cdot \alpha \in m, \quad \text{for } \alpha, \beta \in m, \ a \in o.
\]

By (ii), (iii), and (4.2) in Section 4.1, we see immediately that \(m\) is an abelian group with respect to the addition \(\alpha \hat{+} \beta\), the inverse of \(\alpha\) being given by \(i_F(\alpha)\) for \(F = F_f\) in (4.2). By Proposition 4.4—that is, \([a]_F \circ F_f = \cdots\)—
Local Class Field Theory

$F_f \circ [a]_f$, and so on—we then also see that the map

$$o \times m \rightarrow m,$$

$$(a, \alpha) \mapsto a \cdot \alpha$$

defines an o-module structure on m. We shall denote m by $m_f$ when it is viewed as an o-module in this manner. For integers $n \geq -1$, define

$$p^{n+1} ; \alpha = \{a ; \alpha \mid a \in p^{n+1}\}, \text{ for } \alpha \in m_f,$$

$$W_f^n = \{\alpha \in m_f \mid p^{n+1} ; \alpha = 0\}.$$

Then we obtain a sequence of o-submodules of $m_f$:

$$\{0\} = W_f^{-1} \subseteq W_f^0 \subseteq \cdots \subseteq W_f^n \subseteq \cdots \subseteq W_f,$$

where $W_f$ denotes the union of $W_f^n$ for all $n \geq -1$.

Now, let $f'$ be another power series in the family $\mathcal{F}$. Let $\theta(X)$ denote the power series in $X \mathbb{R}[[X]]$, satisfying (4.8). Then $\theta(X)$ has an inverse $\theta^{-1}(X)$ in $X \mathbb{R}[[X]]$ and $F_f^\theta = F_{f'}$, $[a]_f^\theta = [a]_{f'}$ by Proposition 4.5. Hence it follows from (4.9) that $\theta$ defines an isomorphism of o-modules:

$$\theta : m_f \cong m_{f'},$$

$$\alpha \mapsto \theta(\alpha),$$

which induces o-isomorphisms

$$\theta : W_f^n \cong W_{f'}^n, \quad W_f \cong W_{f'}, \quad n \geq -1. \quad (4.10)$$

**Lemmas.** For $f \in \mathcal{F}$ and $i \geq 0$, let

$$f_i = f^{\psi^i}, \quad g_i = f_i \circ f_{i-1} \circ \cdots \circ f_0, \quad g_{-1}(X) = X.$$

Then

$$W_f^n = \{\alpha \in m \mid g_n(\alpha) = 0\}, \quad \text{for } n \geq -1.$$

**Proof.** Since $W_f^{-1} = \{0\}$, $g_{-1}(X) = X$, the statement is clear for $n = -1$. Let $n \geq 0$. Let $f'$ and $\theta$ be as stated above so that $f' \circ \theta = \theta \psi \circ f$. Then we have

$$f_i' \circ \theta \psi^i = \theta \psi^{i+1} \circ f_i, \quad f_i' = \theta \psi^{i+1} \circ f_i \circ \theta^{-\psi^i}, \quad i \geq 0,$$

and

$$g_n' = f_n' \circ f_{n-1}' \circ \cdots \circ f_0' = \theta \psi^{n+1} \circ g_n \circ \theta^{-1}, \quad n \geq 0.$$

Since $\theta(m) = m$, $\theta(W_f^n) = W_{f'}^n$, we see that if the lemma holds for $f$, then it also holds for $f'$, and $\Delta$. Now, let $\pi$ be a prime element of $(k, \nu)$. Since $K/k$ is unramified, $\pi$ is then also a prime element of $K$ and $\bar{K}$. Hence

$$f(X) = \pi X + X^q$$

belongs to the family $\mathcal{F}$. Since $\pi \in o$, $f = \pi X \mod \deg 2$ and $f \circ f = f^{\psi} \circ f$, it follows from (4.7) that

$$f = [\pi]_f, \quad f_i = f, \quad g_n = f \circ \cdots \circ f = [\pi^{n+1}]_f.$$
As \( p^{n+1} = o \pi^{n+1} \), we obtain

\[
W_f^n = \{ \alpha \in m_f \mid p^{n+1}; \alpha = 0 \} = \{ \alpha \in m \mid g_n(\alpha) = 0 \}.
\]

By the earlier remark, the lemma then holds for an arbitrary \( f \) in \( \mathcal{F} \).

Fix an integer \( m \geq 1 \) and let \( k' \) denote the unique unramified extension of degree \( m \) over \( k \) in \( \Omega \):

\[
k' = k^m_{\text{ur}}.
\]

Let \( \mathfrak{t}' = o'/\mathfrak{p}' \) be the residue field of \( k' \) and let \( \pi \) be any prime element of \( k' \). Then

\[
f(X) = \pi X + X^q
\]

is a polynomial in \( o'[X] \), belonging to the family \( \mathcal{F} \). Hence, checking the proofs of Proposition 4.3 and of (4.7), we see from the Remark (3.13) that

\[
F(X, Y) \in o'[[X, Y]], \quad [a_f(X) \in o'[[X]], \quad \text{for } a \in o. \quad (4.11)
\]

Let

\[
h_n(X) = \pi q^n + g_{n-1}(X)^{q-1}, \quad \text{for } n \geq 0.
\]

Then

\[
g_n = f_n \circ g_{n-1} = f^{q^n} \circ g_{n-1} = h_n(X)g_{n-1}(X), \quad n \geq 0,
\]

so that

\[
g_n(X) = h_n(X)h_{n-1}(X) \cdots h_0(X)X.
\]

**Lemma 4.7.**

(i) \( h_n(X) \) is a monic separable polynomial of degree \( (q - 1)q^n \) in \( o'[X] \) and it is irreducible even in the polynomial ring \( \bar{K}[X] \),

(ii) \( g_n(X) \) is a monic separable polynomial of degree \( q^n + 1 \) in \( o'[X] \) and \( W_f^n \) is the set of all roots of \( g_n(X) \) in \( \Omega \). Hence the order of \( W_f^n \) is \( q^n + 1 \) and \( k'(W_f^n) \) is a finite Galois extension over \( k' \).

(iii) Let \( h_n(\alpha_0) = 0 \) for \( n \geq 0 \), \( \alpha_0 \in \Omega \). Then

\[
\alpha_0 \in W_f^n, \quad \alpha_0 \notin W_f^{n-1}, \quad (q - 1)q^n = [k''(\alpha_0) : k'] \leq [k'(W_f^n) : k']
\]

and

\[
\varphi^n(\pi)(= \pi^{q^n}) = N(-\alpha_0) \in N(k'(\alpha_0)/k')
\]

where \( N \) denotes the norm of the extension \( k'(\alpha_0)/k' \).

**Proof.** It follows from \( g_n = f_n \circ \cdots \circ f_0 \) that

\[
g_n(X) = a_nX + \cdots + X^{q^n+1} \equiv X^{q^n+1} \mod \mathfrak{p}', \quad a_n = \pi^{1+q+\cdots+q^n}, \quad (4.12)
\]

\[
h_n(X) = \pi^{q^n} + (a_{n-1}X + \cdots + X^{q^n})^{q-1} \equiv X^{(q-1)q^n} \mod \mathfrak{p}'
\]

so that \( g_n(X) \) and \( h_n(X) \) are monic polynomials in \( o'[X] \) with degrees \( q^n+1 \) and \( (q - 1)q^n \), respectively. Since \( \pi^{q^n} (= \varphi^n(\pi)) \) is a prime element in \( \bar{K} \), we also see from the above that \( h_n(X) \) is a so-called Eisenstein polynomial in \( R[X], \ R = o_{\bar{K}} \). Hence, it is irreducible even in \( \bar{K}[X] \).

† Compare Lang [16].
is a \( p \)-field so that \( q \) is a power of \( p \). Then
\[
\frac{dq_n}{dX} = (q - 1)a_{n-1}^{q-1}X^{q-2} + \cdots, \quad a_{n-1} = \pi^{1+\varphi+\cdots+\varphi^{n-1}}
\]
where \((q - 1)a_{n-1}^{q-1} \neq 0\) even when the characteristic of \( k \) (and of \( \tilde{K} \)) is \( p \). Hence \( h_n(X) \) is a separable irreducible polynomial of degree \((q - 1)q^n\) in \( \tilde{K}[X] \). Therefore, \( h_i(X) \neq h_t(X) \) for \( i \neq j \) so that \( g_n = h_n \cdots h_0X \) is again a separable polynomial—that is a polynomial without multiple roots. Let \( \alpha \in W^n \). By Lemma 4.6, \( \alpha \) is an element of \( m = p_{\Omega} \) such that \( g_n(\alpha) = 0 \). But, as \( g_n(X) \) is a polynomial in \( o'[X] \subset k'[X] \), \( \alpha \) is a root of \( g_n \) in the algebraic closure \( \Omega \) of \( k \). Conversely, if \( g_n(\alpha) = 0 \) for \( \alpha \in \Omega \), then it follows from (4.12) that \( \tilde{\mu}(\alpha) > 0 \), \( \alpha \in m_f \). Therefore, \( W^n \) is the set of all roots of the separable polynomial \( g_n(X) \) of degree \( q^{n+1} \), contained in \( \Omega \). This of course implies that the order of \( W^n \) is \( q^{n+1} : [W^n : 0] = q^{n+1} \) and that \( k'(W^n) / k' \) is a finite Galois extension. Thus (i) and (ii) are proved. The first part of (iii) follows from (i) and from \( h_i(X) \neq h_t(X) \) for \( i \neq j \). The second part is clear from (4.12) for \( h_n(X) \).

**Remark.** Actually equality holds in (iii) above. Compare Proposition 5.2(ii) below.

**Lemma 4.8.** Let \( f \) be any power series in the family \( \mathcal{F} \) in \( R[[X]] \). Then:

(i) The order of the \( o \)-module \( W^n \) is \( q^{n+1} : [W^n : 0] = q^{n+1}, n \geq 1 \).

(ii) Fix an element \( \alpha_0 \in W^n, \alpha_0 \notin W^{n-1}, n \geq 0 \). Then \( W^n \) is the set of \( \alpha_0 \) and the map \( a \mapsto a \alpha_0 \) induces an isomorphism
\[
o / p^{n+1} \\cong W^n.
\]

(iii) \( p^n \) is a prime element of \( k \) of \( n \). Then \( \alpha_0 \in W^n, \alpha_0 \notin W^{n-1} \), implies \( p^n ; \alpha_0 \in W^{n-1}, \alpha_0 \notin W^{n-2} \). Therefore, by (ii), \( p^n ; \alpha_0 = 0 ; \alpha_0 = W^n \).

**Proof.** (i) This is clear from (4.10) and Lemma 4.7.

(ii) Note first that since \([W^n : 0] = q^{n+1}, [W^{n-1} : 0] = q^n\), there exists \( \alpha_0 \in W^n, \alpha_0 \notin W^{n-1} \). Clearly \( a \mapsto a \alpha_0 \) defines an \( o \)-homomorphism \( o \rightarrow W^n \).

Since \( p^{n+1} ; \alpha_0 = 0, p^n ; \alpha_0 \neq 0 \), the kernel of the homomorphism is an ideal of \( o \), containing \( p^{n+1} \) but not \( p^n \). Hence the kernel is \( p^{n+1} \). It then follows from \([o : p^{n+1}] = [W^n : 0] = q^{n+1}\) that \( o \rightarrow W^n \) induces an isomorphism \( o / p^{n+1} \cong W^n \) so that \( W^n = o ; \alpha_0 \).

(iii) Let \( \pi \) be a prime element of \( k : p = \pi_0 \). Then \( \alpha_0 \in W^n, \alpha_0 \notin W^{n-1} \), implies \( \pi^n ; \alpha_0 \in W^{n-1}, \pi^n ; \alpha_0 \notin W^{n-2} \). Therefore, by (ii), \( \pi^n ; \alpha_0 = 0 ; \pi^n ; \alpha_0 = W^n \).

Let \( f \) again be any power series in \( \mathcal{F} \) and let

\[
\text{End}(W^n) = \text{the ring of all endomorphisms of the } o \text{-module } W^n,
\]
\[
\text{Aut}(W^n) = \text{the group of all automorphisms of the } o \text{-module } W^n,
\]

\[
= \text{the multiplicative group of all invertible elements in the }
\]
\[
\text{ring } \text{End}(W^n).
\]
For each $a \in \mathfrak{o}$, let

$$\varepsilon_a : W^n_f \to W^n_f, \quad \beta \mapsto a \cdot \beta = [a]_f(\beta).$$

Then $\varepsilon_a$ is an endomorphism of $W^n_f : \varepsilon_a \in \text{End}(W^n_f)$. If, in particular, $a \in U = U(k)$, the unit group of $k$, then $[a^{-1}]_f = [a]_f^{-1}$ implies $\varepsilon_{a^{-1}} = \varepsilon_a^{-1}$ so that $\varepsilon_a \in \text{Aut}(W^n_f)$. It is then clear that the map $a \mapsto \varepsilon_a$ defines homomorphisms of rings and groups:

$$\mathfrak{o} \to \text{End}(W^n_f), \quad U \to \text{Aut}(W^n_f).$$

**Proposition 4.9.** The above homomorphisms induce a ring isomorphism

$$\mathfrak{o}/p^{n+1} \cong \text{End}(W^n_f)$$

and a group isomorphism

$$U/U_{n+1} \cong \text{Aut}(W^n_f), \quad n \geq 0$$

where $U_{n+1} = 1 + p^{n+1}$.

**Proof.** Fix $\alpha_0 \in W^n_f$, $\alpha_0 \notin W^n_f^{-1}$ so that $W^n_f = \mathfrak{o} \cdot \alpha_0$ by Lemma 4.7(ii). Let $\varepsilon \in \text{End}(W^n_f)$. Then $\varepsilon(\alpha_0) \in W^n_f = \mathfrak{o} \cdot \alpha_0$ so that $\varepsilon(\alpha_0) = a \cdot \alpha_0$ for some $a \in \mathfrak{o}$. Since $W^n_f = \mathfrak{o} \cdot \alpha_0$, it follows that $\varepsilon(\alpha) = a \cdot \alpha$ for all $\alpha \in W^n_f$—that is, $\varepsilon = \varepsilon_a$. Hence $\mathfrak{o} \to \text{End}(W^n_f)$ is surjective. As $p^{n+1}, W^n_f = 0$, $p^n, W^n_f = W^n_f^{-1} \neq 0$ (cf. Lemma 4.8(iii)), the kernel of $\mathfrak{o} \to \text{End}(W^n_f)$ is $p^{n+1}$ so that $\mathfrak{o}/p^{n+1} \cong \text{End}(W^n_f)$. Since $U/U_{n+1}$ is the multiplicative group of the ring $\mathfrak{o}/p^{n+1}$, the group isomorphism $U/U_{n+1} \cong \text{Aut}(W^n_f)$ follows from this ring isomorphism just proved.

**Remark.** Although the isomorphism $\mathfrak{o}/p^{n+1} \cong W^n_f$ in Lemma 4.8 is defined by means of a choice of $\alpha_0 \in W^n_f$, $\alpha_0 \notin W^n_f^{-1}$, both isomorphisms in the above proposition are canonical.

### 4.4. Extensions $\tilde{L}^n/\tilde{K}$

Let $n \geq 0$ and let $W^n_f$ be the $\mathfrak{o}$-module of the last section, associated with a power series $f$ in $\mathfrak{F} : W^n_f \subseteq \mathfrak{m}_f = \mathfrak{m} \subseteq \tilde{\mathfrak{O}}$. We shall next consider the subfield $\tilde{K}(W^n_f)$ of $\tilde{\mathfrak{O}}$.

**Lemma 4.10.** $\tilde{K}(W^n_f)$ is a finite Galois extension over $\tilde{K}$ and it does not depend on the choice of $f$ in the family $\mathfrak{F}$.

**Proof.** Let $f(X) = \pi X + X^q$ as in Lemma 4.7, $\pi$ being a prime element of $k' = k'_{\mu}$. By (ii) of the same lemma, $k'(W^n_f)/k'$ is a finite Galois extension. Since $k'$ is a subfield of $\tilde{K}$, $\tilde{K}(W^n_f)/\tilde{K}$ is then also a finite Galois extension. Since $\tilde{K}$ is complete in the $\mu_{\tilde{K}}$-topology, it follows from Proposition 1.1 that $\tilde{K}(W^n_f)$ is also complete and is a closed subfield of $\tilde{\mathfrak{O}}$ in the $\mu$-topology. Now, let $f'$ be any power series in $\mathfrak{F}$ and let $\theta(X)$ be the power series in (4.8) so that

$$\theta(W^n_f) = W^n_f, \quad \theta^{-1}(W^n_{f'}) = W^n_f$$
by (4.10). Since \( \theta \in R[[X]] \), \( R = \mathfrak{o}_K \), and since \( \bar{K}(W_f^n) \) is closed in \( \bar{\Omega} \), we see that
\[
W_f^n = \theta(W_f^n) \subseteq \bar{K}(W_f^n), \quad \bar{K} \subseteq \bar{K}(W_f^n) \subseteq \bar{K}(W_f^n).
\]
Therefore, \( \bar{K}(W_f^n) \) is a finite extension of \( \bar{K} \) and, hence, is closed in \( \bar{\Omega} \). It then follows similarly that
\[
W_f^n = \theta^{-1}(W_f^n) \subseteq \bar{K}(W_f^n)
\]
so that \( \bar{K}(W_f^n) = \bar{K}(W_f^n) \).

In the following, we shall denote the field \( \bar{K}(W_f^n) \) by \( \bar{L}^n \):
\[
\bar{L}^n = \bar{K}(W_f^n), \quad \text{for every } f \in \mathcal{F}, \ n \geq -1.
\]
As the notation indicates, \( \bar{L}^n \) is in fact the closure in \( \bar{\Omega} \) of a certain subfield \( L^n \) of \( \Omega \). Choosing a special \( f \) in \( \mathcal{F} \), this will be proved in Proposition 5.2(i). Note that \( \bar{L}^{-1} = \bar{K} \) because \( W_f^{-1} = \{0\} \).

**Proposition 4.11.** For \( n \geq 0 \), there exists a natural homomorphism
\[
\delta^n : U = U(k) \to \text{Gal}(\bar{L}^n/\bar{K})
\]
such that for each \( u \) in \( U \),
\[
\delta^n(u)(\alpha) = u \cdot \alpha \quad (= [u]_f(\alpha))
\]
for every \( f \) in \( \mathcal{F} \) and for every \( \alpha \) in \( W_f^n \). The homomorphism \( \delta^n \) induces an isomorphism
\[
U/U_{n+1} \cong \text{Gal}(\bar{L}^n/\bar{K})
\]
so that \( \bar{L}^n/\bar{K} \) is an abelian extension with degree \([\bar{L}^n : \bar{K}] = (q - 1)q^n\).

**Proof.** Again, let \( f(X) = \pi X + X^q \) and \( h_n(\alpha_0) = 0 \) as in Lemma 4.7. By (i) of the same lemma, \( h_n(X) \) is an irreducible polynomial of degree \((q - 1)q^n\) in \( \bar{K}[X] \). Hence
\[
(q - 1)q^n = [\bar{K}(\alpha_0) : \bar{K}] \leq [\bar{K}(W_f^n) : \bar{K}] = [\bar{L}^n : \bar{K}] = (4.13)
\]
Let \( \sigma \) be any element of \( \text{Gal}(\bar{L}^n/\bar{K}) \). Since \( \sigma \) is continuous and since \( F_f(X, Y) \) and \( [a]_f(X) \), for \( a \in \mathfrak{o} \), are power series with coefficients in \( \bar{R} = \mathfrak{o}_K \subseteq \bar{K} \), one has
\[
\begin{align*}
(\alpha \cdot \beta)^\sigma &= F_f(\alpha, \beta)^\sigma = F_f(\alpha^\sigma, \beta^\sigma) = \alpha^\sigma \cdot \beta^\sigma, \\
(a \cdot \beta)^\sigma &= [a]_f(\alpha)^\sigma = [a]_f(\alpha^\sigma) = a \cdot \alpha^\sigma
\end{align*}
\]
for \( \alpha, \beta \in \mathfrak{m}_f \) and \( a \in \mathfrak{o} \). Thus \( \sigma \) defines an automorphism of the \( \mathfrak{o} \)-module \( \mathfrak{m}_f \) and it induces an automorphism \( \sigma' \) of the \( \mathfrak{o} \)-submodule \( W_f^n = \{ \alpha \in \mathfrak{m}_f \mid p^{n+1} \cdot \alpha = 0 \} \) in \( \mathfrak{m}_f \). Clearly the map \( \sigma \mapsto \sigma' \) defines a homomorphism
\[
\text{Gal}(\bar{L}^n/\bar{K}) \to \text{Aut}(W_f^n),
\]
and since \( \tilde{L}^n = \bar{K}(W^n_f) \), this homomorphism is injective. As \([\text{Aut}(W^n_f):1] = [U:U_{n+1}] = (q-1)q^n\) by Proposition 4.9, it follows that
\[
[\tilde{L}^n: \bar{K}] \leq (q-1)q^n.
\]
Comparing this with (4.13), we see that
\[
\tilde{L}^n = \bar{K}(\alpha_0), \quad [\tilde{L}^n: \bar{K}] = (q-1)q^n, \quad \text{Gal}(\tilde{L}^n/\bar{K}) \cong \text{Aut}(W^n_f). \quad (4.14)
\]
Let \(\delta^n\) denote the product of the sequence of maps
\[
U \to U/U_{n+1} \cong \text{Aut}(W^n_f) \cong \text{Gal}(\tilde{L}^n/\bar{K}),
\]
where \(U \to U/U_{n+1}\) is the canonical homomorphism, \(U/U_{n+1} \cong \text{Aut}(W^n_f)\) is the isomorphism of Proposition 4.9, and \(\text{Aut}(W^n_f) \cong \text{Gal}(\tilde{L}^n/\bar{K})\) is the inverse of the isomorphism in (4.14). Then \(\delta^n: U \to \text{Gal}(\tilde{L}^n/\bar{K})\) obviously induces \(U/U_{n+1} \cong \text{Gal}(\tilde{L}^n/\bar{K})\), and checking the definitions of the maps in the above sequence, we find easily that \(\delta^n(u)(\alpha) = [u]_f(\alpha) = u \cdot \alpha\) for \(u \in U, \alpha \in W^n_f\).

Now, let \(f'\) be any power series in the family \(\mathcal{T}\) and let \(\theta(X)\) be the power series in (4.8) so that \(W^n_{f'} = \theta(W^n_f)\) by (4.10). Let \(\alpha' \in W^n_{f'}\) and let \(\alpha' = \theta(\alpha)\) with \(\alpha \in W^n_f\). Then, for \(u \in U, \alpha' \in W^n_{f'}\), we have
\[
u(f') \cdot \alpha' = [u]_f(\alpha') = [u]_f(\theta(\alpha)) = \theta([u]_f(\alpha)) = \theta(\delta^n(u)(\alpha)).
\]
However, since \(\theta(X) \in R[[X]]\), where \(R = \mathfrak{o}_K\), and since \(\delta^n(u) \in \text{Gal}(\tilde{L}^n/ \bar{K})\), we have
\[
\theta(\delta^n(u)(\alpha)) = \delta^n(u)(\theta(\alpha)) = \delta^n(u)(\alpha')
\]
so that
\[
\delta^n(u)(\alpha') = u(f') \cdot \alpha', \quad \text{for } f' \in \mathcal{T}, \alpha' \in W^n_{f'}.
\]
This completes the proof of the proposition.

Since \(W^n_f \subseteq W^n_{f+1}\) and \(W_f\) is the union of all \(W^n_f, n \geq -1\), we have a sequence of subfields of \(\mathfrak{Q}\):
\[
\bar{K} = \tilde{L}^{-1} \subseteq L^0 \subseteq \cdots \subseteq \tilde{L}^n \subseteq \cdots \subseteq \bar{L} \subseteq \mathfrak{Q},
\]
where
\[
\tilde{L} = \text{the union of all } \tilde{L}^n, n \geq -1 = \bar{K}(W_f), \quad \text{for any } f \in \mathcal{T}.
\]

**Proposition 4.12.** \(\tilde{L}/\bar{K}\) is an abelian extension and there exists a topological isomorphism
\[
\delta: U = U(\mathfrak{k}) \cong \text{Gal}(\tilde{L}/\bar{K})
\]
which induces the homomorphism \(\delta^n: U \to \text{Gal}(\tilde{L}^n/\bar{K})\) in Proposition 4.11 for each \(n \geq 0\).

**Proof.** It is clear from Proposition 4.11 that \(\delta^n\) is the product of \(\delta^{n+1}\) and the canonical homomorphism \(\text{Gal}(\tilde{L}^{n+1}/\bar{K}) \to \text{Gal}(\tilde{L}^n/K)\). Hence we
have

\[ \delta : U = \lim U/U_{n+1} \cong \text{Gal}(\bar{L}/\bar{K}) = \lim \text{Gal}(\bar{L}^n/\bar{K}). \]

Since the structure of the compact group \( U = U(k) \) is explicitly described in Section 2.2, the structure of the Galois group \( \text{Gal}(\bar{L}/\bar{K}) \) is now completely determined.
Chapter V  
Abelian Extensions Defined by Formal Groups

Still keeping the notation introduced earlier, let \( \tilde{K} \) denote the completion of the maximal unramified extension \( K = k_{ur} \) of a local field \( (k, \nu) \). In the last chapter, we constructed certain abelian extensions of \( \tilde{K} \) by means of the formal groups \( F_f(X, Y) \) over \( R = \mathcal{O}_{\tilde{K}} \). In the present chapter, we shall similarly construct abelian extensions of the ground field \( k \), by choosing suitable power series \( f \) in the family \( \mathcal{F} \). We shall then study the properties of such abelian extensions.

5.1. Abelian Extensions \( L^n \) and \( k_{\pi, n}^m \)

For each integer \( m \geq 1 \), let \( \mathcal{O}^m \) again denote the valuation ring of the unique unramified extensions \( k_{ur}^m \) of degree \( m \) over \( k \) in \( \Omega \). Let \( \pi \) be a prime element of \( k_{ur}^m \) so that it is also a prime element of \( K = k_{ur} \) and of \( \tilde{K} \). Let \( \mathcal{F}_\pi \) be the family of power series in \( R[[X]] \), \( R = \mathcal{O}_K \), as defined in Section 4.2, and let

\[
\mathcal{F}_\pi^m = \mathcal{F}_\pi \cap \mathcal{O}^m[[X]].
\]

For example, \( f(X) = \pi X + X^q \) in Lemma 4.7 belongs to \( \mathcal{F}_\pi^m \). We put

\[
\begin{align*}
\mathcal{F}^m &= \text{the union of } \mathcal{F}_\pi^m \text{ for all prime elements } \pi \text{ of } k_{ur}, \\
\mathcal{F}^\omega &= \text{the union of } \mathcal{F}^m \text{ for all integers } m \geq 1.
\end{align*}
\]

**Lemma 5.1.** Let \( m \geq 1 \), \( n \geq 0 \).

(i) Let \( f \in \mathcal{F}_\pi^m \). Then the field \( k_{ur}(W_f^n) \) depends only on \( m, n, \) and \( \pi \), and is independent of the choice of \( f \) in the family \( \mathcal{F}_\pi^m \).

(ii) Let \( f \in \mathcal{F}^\omega \). Then the field \( K(W_f^n) \) depends only on \( n \) and is independent of the choice of \( f \) in \( \mathcal{F}^\omega \).

**Proof.** (i) The proof is similar to that of Lemma 4.10. Namely, let \( f(X) = \pi X + X^q \) and let \( f'(X) \) be any other power series in \( \mathcal{F}_\pi^m \). Since we may put \( \pi = \pi' \), \( \xi = \eta = 1 \) in the proof of (4.8), it follows from the remark (3.13) that in this case, the power series \( \theta(X) \) in (4.8) belongs to \( \mathcal{O}^m[[X]] \). By Lemma 4.7(ii), \( k_{ur}^m(W_f^n) \) is a finite Galois extension over \( k_{ur}^m \). Hence it is a local field and is closed in \( \tilde{\Omega} \). Since \( \theta(X) \in \mathcal{O}^m[[X]] \), we see from (4.10) that

\[
W_f^n = \theta(W_f^n) \subseteq k_{ur}^m(W_f^n), \quad k \subseteq k_{ur}^m(W_f^n) \subseteq k_{ur}^m(W_f^n).
\]

It then follows that \( k_{ur}^m(W_f^n) \) is again a local field so that \( k_{ur}^m(W_f^n) \subseteq k_{ur}^m(W_f^n) \) since also \( \theta^{-1}(X) \in \mathcal{O}^m[[X]] \). Hence \( k_{ur}^m(W_f^n) = k_{ur}^m(W_f^n) \) for any \( f' \in \mathcal{F}_\pi^m \).
(ii) Let \( f \in \mathcal{F}^\infty \). Then \( f \) belongs to \( \mathcal{F}_\pi^m \) for some \( m \geq 1 \) and \( \pi \in k_{ur}^m \). Let
\[
E = K(W_f^n) = K \cdot k_{ur}^m(W_f^n)
\]
and let \( \tilde{E} \) denote the closure of \( E \) in \( \tilde{\Omega} \). By (i) above and by Lemma 4.7, \( k_{ur}^m(W_f^n)/k_{ur}^m \) is a finite Galois extension for any \( f \in \mathcal{F}_\pi^m \). Hence \( E/K \) is also a finite Galois extension, and by Lemma 3.1 and the definition of \( \tilde{L}^n \),
\[
\tilde{E} = E\tilde{K} = \tilde{K}(W_f^n) = \tilde{L}^n, \quad K = E \cap \tilde{K}.
\]
Let \( f' \) be another power series in \( \mathcal{F}^\infty \) and let \( E' = K(W_{f'}^n) \). Then \( E'/K \) is again a finite Galois extension and \( \tilde{E}' = \tilde{L}^n \). Let \( M = E\tilde{E}' \). Since both \( M/E \) and \( M/E' \) are finite Galois extensions, it follows from Lemma 3.1 that
\[
E = M \cap \tilde{E} = M \cap \tilde{L}^n = M \cap \tilde{E}' = E',
\]
amely, \( K(W_f^n) = K(W_{f'}^n) \).

In view of the above lemma, we put
\[
k_{\pi}^{m,n} = k_{ur}^m(W_f^n), \quad \text{for any } f \in \mathcal{F}_\pi^m, \quad n \geq -1,
\]
\[
L^n = K(W_f^n), \quad \text{for any } f \in \mathcal{F}^\infty, \quad n \geq -1.
\]
Note that
\[
k_{\pi}^{m,n-1} = k_{ur}^m, \quad L^{-1} = k_{ur} \quad (= K)
\]
because \( W_f^{-1} = \{0\} \).

**Proposition 5.2.** Let \( m \geq 1, \ n \geq 0 \), and let \( \pi \) be a prime element of \( k_{ur}^m \).
(i) The field \( \tilde{L}^n \) in Section 4.4 is the closure of \( L^n \) in \( \Omega \), and
\[
\tilde{L}^n = \tilde{K}L^n, \quad K = \tilde{K} \cap L^n, \quad \text{Gal}(\tilde{L}^n/\tilde{K}) \cong \text{Gal}(L^n/K).
\]
(ii) \( L^n = Kk_{\pi}^{m,n} \), \( k_{\pi}^{m,n} = K \cap k_{\pi}^{m,n} \) so that \( k_{\pi}^{m,n} \) is a maximal totally ramified extension over \( k_{ur}^m \) in \( L^n \) and
\[
\text{Gal}(L^n/k_{ur}^m) = \text{Gal}(L^n/k_{\pi}^{m,n}) \times \text{Gal}(L^n/K) \cong \text{Gal}(K/k_{ur}^m) \times \text{Gal}(k_{\pi}^{m,n}/k_{ur}^m).
\]
(iii) \( L^n/k \), \( L^n/K \), \( k_{\pi}^{m,n}/k \), and \( k_{\pi}^{m,n}/k_{ur}^m \) are abelian extensions and
\[
[L^n : K] = [k_{\pi}^{m,n} : k_{ur}^m] = (q - 1)q^n, \quad [k_{\pi}^{m,n} : k] = m(q - 1)q^n.
\]

**Proof.** It was already proved above that both \( L^n/K \) and \( k_{\pi}^{m,n}/k_{ur}^m \) are finite Galois extensions and that \( \tilde{E} = E\tilde{K}, \ K = E \cap \tilde{K} \) for \( E = K(W_f^n) = L^n \). Hence \( \text{Gal}(\tilde{L}^n/\tilde{K}) \cong \text{Gal}(L^n/K), \ [L^n : K] = [\tilde{L}^n : \tilde{K}] = (q - 1)q^n \) by Proposition 4.11, proving (i). It is clear that
\[
L^n = Kk_{\pi}^{m,n}, \quad k_{ur}^m \subseteq K \cap k_{\pi}^{m,n} \subseteq k_{\pi}^{m,n},
\]
so that
\[
(q - 1)q^n = [L^n : K] = [k_{\pi}^{m,n} : K \cap k_{\pi}^{m,n}] \leq [k_{\pi}^{m,n} : k_{ur}^m]. \tag{5.1}
\]
Let \( f(X) = \pi X + X^q, \ \pi \in k_{ur}^m \), and let \( h_n(\alpha_0) = 0 \) as in Lemma 4.7(iii). Then
\[
W_f^n = \{ a \theta_f(\alpha_0) \mid a \in \sigma \}.
\]
by Lemma 4.8(ii). However, since \( f \in \mathfrak{o}^m[[X]] \), it follows from (4.7) and the remark (3.13) that \([a]_f \) belongs to \( \mathfrak{o}^m[[X]] \). Hence

\[
W_f^n \subseteq k_{ur}^m(\alpha_0), \quad k_{\pi}^{m,n} = k_{ur}^m(W_f^n) = k_{ur}^m(\alpha_0),
\]

and, by Lemma 4.7(iii),

\[
[k_{\pi}^{m,n} : k_{ur}^m] = [k_{ur}^m(\alpha_0) : k_{ur}^m] = (q - 1)q^n.
\]

Comparing this with (5.1), we obtain \( k_{ur}^m = K \cap k_{\pi}^{m,n} \). This proves (ii). The statement on \( L^n/K \) and \( k_{\pi}^{m,n}/k_{ur}^m \) in (iii) are consequences of (i), (ii), and Proposition 4.11. To see that \( L^n/k \) is abelian, take a prime element \( \pi \) of the ground field \( k \). By (i), (ii),

\[
\text{Gal}(\tilde{L}/\tilde{K}) \cong \text{Gal}(L^n/K) \cong \text{Gal}(k_{\pi}^{m,n}/k_{ur}^m),
\]

where \( k_{ur}^1 = k \). Hence \( k_{\pi}^{1,n}/k \) is abelian by Proposition 4.11. Since \( L^n = Kk_{\pi}^{1,n} \) and \( K/k \) is abelian, \( L^n/k \) is also an abelian extension. The rest of (iii) follows from this and from (i) and (ii).

The following proposition is an immediate consequence of Proposition 4.11 and Proposition 5.2 above:

**PROPOSITION 5.3.**

(i) For each \( n \geq 0 \), there exists a homomorphism

\[
\delta^n : U = U(k) \rightarrow \text{Gal}(L^n/K)
\]

such that for each \( f \in \mathbb{F}^\infty \), each \( u \in U \), and each \( \alpha \in W_f^n \),

\[
\delta^n(u)(\alpha) = u \cdot \alpha(= [u]_f(\alpha)),
\]

and it induces an isomorphism

\[
U/U_{n+1} \cong \text{Gal}(L^n/K).
\]

(ii) Let \( m \geq 1 \) and let \( \pi \) be a prime element of \( k_{ur}^m \). Then \( \delta^n \) induces a homomorphism

\[
\delta^n_{\pi} : U = U(k) \rightarrow \text{Gal}(k_{\pi}^{m,n}/k_{ur}^m)
\]

such that for each \( f \in \mathbb{F}^m_{\pi} \), each \( u \in U \), and each \( \alpha \in W_f^n \),

\[
\delta^n_{\pi}(u)(\alpha) = u \cdot \alpha(= [u]_f(\alpha)),
\]

and \( \delta^n_{\pi} \) in turn induces an isomorphism

\[
U/U_{n+1} \cong \text{Gal}(k_{\pi}^{m,n}/k_{ur}^m).
\]

**COROLLARY.** Let \( 0 \leq i \leq n \). Then the isomorphism \( U/U_{n+1} \cong \text{Gal}(k_{\pi}^{m,n}/k_{ur}^m) \) induces

\[
U_{i+1}/U_{n+1} \cong \delta^n_{\pi}(U_{i+1}) = \text{Gal}(k_{\pi}^{m,n}/k_{\pi}^{m,i}).
\]

**Proof.** It is clear from the above proposition that \( \delta^n_{\pi}(u) \mid k_{\pi}^{m,i} = \delta^i_{\pi}(u) \) for \( u \in U \) so that

\[
u \in U_{i+1} \iff \delta^i_{\pi}(u) = 1 \iff \delta^n_{\pi}(u) \mid k_{\pi}^{m,i} = 1 \iff \delta^n_{\pi}(u) \in \text{Gal}(k_{\pi}^{m,n}/k_{\pi}^{m,i}).
\]

Hence \( U_{i+1}/U_{n+1} \cong \delta^n_{\pi}(U_{i+1}) = \text{Gal}(k_{\pi}^{m,n}/k_{\pi}^{m,i}) \).
Proposition 5.4. Let \( m \geq 1, n \geq 0 \) and let \( \pi \) be a prime element of \( \kappa_{ur}^m \). Then:

(i) \( k_{\pi}^{m,n}/k_{ur}^m \) is a totally ramified finite abelian extension and \( \pi \) is contained in the norm group of \( k_{\pi}^{m,n}/k_{ur}^m : \pi \in N(k_{\pi}^{m,n}/k_{ur}^m) \).

(ii) Let \( f \in \mathcal{F}_{\pi}^m \) and let \( \alpha \in W^n_f, \alpha \notin W_f^{n-1} \). Then \( \alpha \) is a prime element of the local field \( k_{\pi}^{m,n} \) so that

\[
k_{\pi}^{m,n} = k_{ur}^m(\alpha), \quad \varpi^{m,n} = \varpi^m[\alpha],
\]

\( \varpi^{m,n} \) and \( \varpi^m \) being the valuation rings of \( k_{\pi}^{m,n} \) and \( k_{ur}^m \), respectively.

Proof. (i) Since \( K \cap k_{\pi}^{m,n} = k_{ur}^m \), the extension \( k_{\pi}^{m,n}/k_{ur}^m \) is totally ramified. By Lemma 4.7(iii), \( \varphi^n(\pi) \) is contained in \( N(k_{\pi}^{m,n}/k_{ur}^m) \). Since \( k_{\pi}^{m,n}/k \) is abelian by Proposition 5.2, the automorphism \( \varphi \) of \( k_{ur}^m/k \) can be extended to an automorphism of \( k_{\pi}^{m,n}/k \) such that \( \varphi(N(k_{\pi}^{m,n}/k_{ur}^m)) = N(k_{\pi}^{m,n}/k_{ur}^m) \). Hence \( \pi \in N(k_{\pi}^{m,n}/k_{ur}^m) \).

(ii) Let \( f(X) = \pi X + X^q \). Let \( f' \) be any power series in \( \mathcal{F}_{\pi}^m \) and let \( \alpha' \in W^n_f, \alpha' \notin W_f^{n-1} \). Put \( \alpha_0 = \theta^{-1}(\alpha') \), where \( \theta(X) \) is the power series in (4.8). Then, by (4.10), \( \alpha_0 \in W^n_f, \alpha_0 \notin W_f^{n-1} \). Hence \( h_n(\alpha_0) = 0 \) and \( \varphi^n(\pi) = N(-\alpha_0) \) by Lemma 4.7. Since \( \varphi^n(\pi) \) is a prime element of \( k_{ur}^m \), it follows that \( -\alpha_0 \) and, hence, \( \alpha_0 \) are prime elements of \( k_{\pi}^{m,n} \). The proof of Lemma 5.1(i) shows that \( \theta(X) \in \varpi^m[[X]] \) and \( \theta(X) \equiv X \mod \deg 2 \). Therefore, \( \alpha' = \theta(\alpha) \) is also a prime element of \( k_{\pi}^{m,n} \) and it follows from the Corollary of Lemma 2.13 that \( \varpi^{m,n} = \varpi^m[\alpha'] \), \( k_{\pi}^{m,n} = k_{ur}^m(\alpha') \). Changing the notation from \( f' \) to \( f \), we see that (ii) is proved.

Corollary. Let \( f \in \mathcal{F}_{\pi}^m \) and let \( \alpha \in W^n_f, \alpha \notin W_f^{n-1} \) so that \( k_{\pi}^{m,n} = k_{ur}^m(\alpha) \).

(i) The complete set of conjugates of \( \alpha \) over the subfield \( k_{ur}^m \) is given by the set of all \( \beta \in W^n_f, \beta \notin W_f^{n-1} \).

(ii) For \( 0 \leq i \leq n \), the complete set of conjugates of \( \alpha \) over this subfield \( k_{\pi}^{m,i} \) is given by

\[
\alpha \overset{f}{\mapsto} W_f^{n-i-1} = \{ \alpha \overset{f}{\mapsto} \gamma \mid \gamma \in W_f^{n-i-1} \}.
\]

Proof. (i) Since \( k_{\pi}^{m,n} = k_{ur}^m(\alpha) \), it follows from Proposition 5.3(ii) that the complete set of conjugates of \( \alpha \) over \( k_{ur}^m \) is given by the elements \( u_j \alpha \) for all \( u \in U \). By Lemma 4.8(ii), (iii), this is the set of all \( \beta \in W_f = \sigma_f \alpha, \beta \notin W_f^{n-1} = \varpi^1_f \alpha \).

(ii) By the Corollary of Proposition 5.3, the complete set of conjugates of \( \alpha \) over \( k_{\pi}^{m,i} \) is given by \( u_j \alpha \) for all \( u \in U_{i+1} = 1 + \varpi^{i+1} \)—namely, by the set

\[
(1 + \varpi^{i+1})_f \alpha = \alpha \overset{f}{\mapsto} \varpi^{i+1}_f \alpha,
\]

where \( \varpi^{i+1}_f \alpha = W_f^{n-i-1} \) by Lemma 4.8(iii).

Example 1. Let us consider the case \( n = 0 \) in the above. Let \( f(X) = \pi X + X^q, \alpha \in W^n_f, \alpha \notin W_f^{n-1} = \{0\} \)—that is, \( \alpha \neq 0 \). Then

\[
\alpha = q^{-1}\sqrt{-\pi}, \quad k_{\pi}^{m,0} = k_{ur}^m(q^{-1}\sqrt{-\pi}).
\]
As in Section 2.1, let \( U = V \times U_1 \), where \( V \) is a cyclic group of order \( q - 1 \), and let \( \omega(u) \), for \( u \in U \), denote the unique element of \( V \) such that \( u \equiv \omega(u) \mod p \). Since \( [u]_f = uX \mod \deg 2 \), we then have
\[
\delta^0(u)(\alpha) = [u]_f(\alpha) = u\alpha = \omega(u)\alpha \mod p_2^2.
\]
However, since \( \alpha = q^{-\frac{1}{2}} - \pi \), its conjugate \( \delta^0(u)(\alpha) \) over \( k_{ur}^n \) must be an element of the form \( \eta\alpha \) with \( \eta \in V \). It then follows from \( V \preceq \mathfrak{f}^\times \) that
\[
\omega(u) = \eta, \quad \delta^0(u)(\alpha) = \omega(u)\alpha, \quad \text{for } u \in U.
\]

**Example 2.** Let us consider the example stated at the end of Section 4.2—namely, the case:

\[
k = \mathbb{Q}_p, \quad \pi = p, \quad f(X) = (1 + X)^p - 1 \in \mathcal{F}_p^1,
\]

\[
F_f(X, Y) = (1 + X)(1 + Y) - 1.
\]

In this case, we know that
\[
W_f^\pi = \{ \zeta - 1 \mid \zeta \in \Omega, \; \zeta^{p+1} = 1 \}, \quad \text{for } n \geq 0
\]
so that \( k_{ur}^1 = \mathbb{Q}_p(W_f^\pi) \) is the cyclotomic field of \( p^{n+1} \)th roots of unity over \( \mathbb{Q}_p = k_{ur}^1 \). Let \( u \in U \), \( \alpha = \zeta - 1 \in W_f \). Then \( \delta^u_p(u) \) in Proposition 5.4 satisfies
\[
\delta^u_p(u)(\alpha) = [u]_f(\alpha) = (1 + \alpha)^u - 1, \quad \text{that is, } \delta^u_p(u)(\zeta) = \zeta^u,
\]
and \( \delta^u_p \) induces an isomorphism
\[
U/U_{n+1} = \mathbb{Z}_p^\times / (1 + p^{n+1}\mathbb{Z}_p) \simeq \text{Gal}(\mathbb{Q}_p(W_f^\pi)/\mathbb{Q}_p).
\]

Furthermore, by Proposition 5.5, we also know that \( \mathbb{Q}_p(W_f^\pi)/\mathbb{Q}_p \) is a totally ramified abelian extension of degree \( (p - 1)p^n \) and that \( p \) is a norm from the extension \( \mathbb{Q}_p(W_f^\pi)/\mathbb{Q}_p \).

### 5.2. The Norm Operator of Coleman

In this section, we shall study the field \( k_{\pi}^{m,n} \) for \( m = 1, \pi \in k = k_{ur}^1 \), and denote it simply by \( k_{\pi}^n \):
\[
k_{\pi}^n = k_{ur}^{1,n}, \quad n \geq -1.
\]

These \( k_{\pi}^n, n \geq -1 \), are the abelian extensions of \( k \), originally introduced by Lubin-Tate [19]. Let \( S \) denote the power series ring \( \mathfrak{o}[[X]] \), and \( S^\times \) the multiplicative group of the ring \( S \):
\[
S = \mathfrak{o}[[X]]
\]
\[
S^\times = \{ g(X) \in S \mid g(0) \neq 0 \mod p, \quad \text{that is, } g(0) \in U \}.
\]

Since the valuation ring \( \mathfrak{o} \) of the local field \( (k, \nu) \) is compact, \( S \) is a compact ring in the topology introduced in Section 4.1. Let \( \pi \) be a prime element of \( k \) and let \( f(X) \) be a power series in the family \( \mathcal{F}_\pi^1 = \mathcal{F}_\pi \cap S \).

† Compare Coleman [5].
**Lemma 5.5.** Let $g(X)$ be a power series in $S$ such that
\[ g(W_f^0) = 0, \quad \text{that is, } g(\gamma) = 0, \quad \text{for all } \gamma \in W_f^0. \]
Then $g(X)$ is divisible by $[\pi]_f$ in $S$:
\[ g(X) = [\pi]_f h(X), \quad h(X) \in S. \]

**Proof.** First, consider the case where $f(X) = \pi X + X^q$. Since $\pi \in \mathfrak{o}$, it follows from (4.7) that
\[ f(X) = [\pi]_f. \]
By Lemma 4.7(ii), $W_f^0$ is the set of all roots, in $\Omega$, of the separable polynomial $f (= g_0)$ in $\mathfrak{o}[X]$. Hence, if $g(W_f^0) = 0$, then $g$ is divisible by $f = [\pi]_f$ in $S$ by Lemma 3.10. In general, let $f'(X)$ be any power series in $S\mathfrak{F}_\pi$ and let $\theta(X)$ be the power series in (4.8). As stated in the proof of Lemma 5.1(i), $\theta(X)$ then belongs to $S = \mathfrak{o}[X]$. Now, let $g'(X)$ be a power series in $S$ such that $g'(W_f^0) = 0$. Since $W_f^0 = \theta(W_f^0)$ by (4.10), we then have $(g' \circ \theta)(W_f^0) = 0$ with $g' \circ \theta \in S$. Therefore, by the above,
\[ g' \circ \theta = [\pi]_f h, \quad g' = ([\pi]_f \circ \theta^{-1})(h \circ \theta^{-1}), \quad \text{with } h, h \circ \theta^{-1} \in S. \]
However, $[\pi]_f \circ \theta^{-1} = \theta^{-1} \circ [\pi]_f$, by Proposition 4.5, and $\theta^{-1}(X)$ is divisible by $X$ in $S$. Hence $g'(X)$ is divisible by $[\pi]_f$ in $S$. \hfill \Box

**Remark.** By a similar argument, we can also prove that if $g(W_f^0) = 0$ for $g \in S$, then $g(X)$ is divisible by $[\pi^{n+1}]_f$ in $S$.

In the following, we shall fix a power series $f$ in $S\mathfrak{F}_\pi = S \cap S$ and omit, for simplicity, the suffix $f$ in $[a]_f$, $W_f^0$, and so on.

Let
\[ f_n = \mathfrak{o}_n/p_n, \quad n \geq -1, \]
be the residue field of $k^n_\pi = k(W^n)$ and let $\alpha \in W^n \subseteq m = p_\Omega$. Since $\alpha \in p_n = m \cap k^n_\pi$, it follows from the general remark in Section 3.4 that $F_f(X, \alpha)$ is a well-defined power series in $\mathfrak{o}_n[[X]]$. Let
\[ X + \alpha = X + \frac{1}{f} \alpha = F_f(X, \alpha). \]
Then $X + \alpha = \alpha \mod \deg 1$ by (4.1). Hence, if $g(X)$ is any power series in $S = \mathfrak{o}[[X]]$, it again follows from the same remark that $g(X + \alpha)$ is a well-defined power series in $\mathfrak{o}_n[[X]]$.

**Lemma 5.6.** Let $g(X)$ be a power series in $S$ satisfying
\[ g(X + \gamma) = g(X), \quad \text{for all } \gamma \in W^0. \]
Then there exists $h(X)$ in $S$ such that
\[ g = h \circ [\pi]. \]

**Proof.** Let $a_0 = g(0) \in \mathfrak{o}$ and let $h_1 = g - a_0$. Then $h_1(\gamma) = g(\gamma) - g(0) =
0 for all $\gamma \in W^n$. Hence, by Lemma 5.5, $h_1$ is divisible by $[\pi]$ in $S$:

$$h_1 = g_1[\pi], \quad g = a_0 + [\pi]g_1, \quad g_1 \in S.$$ 

Since

$$[\pi](X + \gamma) = [\pi](X) + [\pi](\gamma) = [\pi](X),$$

it follows that $g_1(X + \gamma) = g_1(X)$ for all $\gamma \in W^n$. Therefore, by the same argument,

$$g_1 = a_1 + [\pi]g_2, \quad a_1 = g_1(0) \in o, \quad g_2 \in S$$

so that

$$g = a_0 + a_1[\pi] + [\pi]^2g_2$$

where $g_2(X)$ again satisfies $g_2(X + \gamma) = g_2(X)$ for all $\gamma \in W^n$. Thus we can find a sequence, $a_0, a_1, a_2, \ldots$ in $o$ and a sequence $g_1, g_2, \ldots$ in $S$ such that

$$g = a_0 + a_1[\pi] + \cdots + a_n[\pi]^n + [\pi]^{n+1}g_{n+1}, \quad \text{for all } n \geq 0.$$ 

Hence $g = h \circ [\pi]$ with $h(X) = a_0 + a_1X + \cdots + a_nX^n + \cdots$ in $S$. 

Remark. Again the lemma can be generalized for $W^n$ and $[\pi]^{n+1}$.

The power series $h$ in Lemma 5.6 is unique for $g$. This is a consequence of the following lemma:

Lemma 5.7. Let $g = h \circ [\pi]$ for $g, h \in S$ and let $\mathfrak{p}$ be as before the maximal ideal of $k$. Then, for each $n \geq 0$,

$$g \equiv 0 \pmod{\mathfrak{p}^n} \iff h \equiv 0 \pmod{\mathfrak{p}^n}.$$ 

Consequently,

$$g = 0 \iff h = 0.$$ 

Proof. $\Leftarrow$ is obvious. We prove $\Rightarrow$ by induction on $n$. For $n = 0$, this is trivial. Hence, let $g \equiv 0 \pmod{\mathfrak{p}^n}$, $n \geq 1$. Then $g \equiv 0 \pmod{\mathfrak{p}^{n-1}}$, $g = \pi^{n-1}g_1$, with $g_1 \in S$. By the induction assumption, we have $h \equiv 0 \pmod{\mathfrak{p}^{n-1}}$, $h = \pi^{n-1}h_1$ with $h_1 \in S$, and it follows from $g = h \circ [\pi]$ that $g_1 = h_1 \circ [\pi]$. However, $g \equiv 0 \pmod{\mathfrak{p}^n}$ implies $g_1 = 0 \pmod{\mathfrak{p}}$. Since $[\pi] = f(X) = X^q \pmod{\mathfrak{p}}$, we see

$$h_1(X^q) \equiv h_1 \circ [\pi] = g_1 \equiv 0 \pmod{\mathfrak{p}}$$

so that $h_1(X) \equiv 0 \pmod{\mathfrak{p}}$. Hence $h = \pi^{n-1}h_1 \equiv 0 \pmod{\mathfrak{p}^n}$. 

Remark. The proof shows that the lemma holds also for power series $g, h$ in $R = \mathfrak{o}_k[[X]]$ and for the maximal ideal $p_k$ of $K$.

Now, let $h(X)$ be any power series in $S = \mathfrak{o}[[X]]$ and let

$$h_1(X) = \prod_{\gamma} h(X + \gamma), \quad \gamma \in W^n.$$ 

Then $h_1(X)$ is a power series in $\mathfrak{o}_0[[X]]$, $\mathfrak{o}_0$ being the valuation ring of
$k_\pi^0 = k(W^0)$. By the Corollary 1 of Proposition 5.4 for $m = 1$, all $\gamma \in W^0$, $\gamma \neq 0$, are conjugate to each other over $k$. Hence

$$h_1^\sigma = h_1, \text{ for all } \sigma \in \text{Gal}(k_\pi^0/k)$$

so that $h_1(X)$ belongs to $S = \mathcal{O}[[X]]$. Furthermore, since

$$(X + \gamma) + \gamma' = X + (\gamma + \gamma'), \text{ for } \gamma, \gamma', \gamma + \gamma' \in W^0,$$

$h_1(X)$ satisfies $h_1(X + \gamma) = h_1(X)$ for all $\gamma \in W^0$. Therefore, by Lemmas 5.6 and 5.7,

$$h_1 = h_2 \circ [\pi]$$

with a unique power series $h_2(X)$ in $S$. We shall denote this $h_2$ by $N_f(h)$, or simply, by $N(h)$. Thus $N(h) = N_f(h)$ is the unique power series in $S$ such that

$$N(h) \circ [\pi] = \prod_{\gamma} h(X + \gamma), \quad \gamma \in W^0. \quad (5.2)$$

The map

$$N (= N_f): S \rightarrow S$$

is called the norm operator on $S$, associated with $f \in \mathcal{F}_\pi^1$. We shall next prove some basic properties of the operator $N$.

**Lemma 5.8.**

(i) $N(h_1h_2) = N(h_1)N(h_2)$, for $h_1, h_2 \in S$.

(ii) $N(h) \equiv h \mod \mathfrak{p}$, for $h \in S$.

(iii) $h \in X_i S^\times$ for $i \geq 0 \Rightarrow N(h) \in X_i S^\times$, $S^\times$ being the multiplicative group of the ring $S$.

(iv) $h \equiv 1 \mod \mathfrak{p}^i$, $i \geq 1 \Rightarrow N(h) \equiv 1 \mod \mathfrak{p}^{i+1}$.

**Proof.** (i) is obvious from the uniqueness in (5.2).

(ii) $[\pi] = f(X) \equiv X^q \mod \mathfrak{p}$ implies

$$N(h) \circ [\pi] = N(h)(X^q) \mod \mathfrak{p}.$$

On the other hand, $\gamma \in W^0 \subseteq \mathfrak{p}_0$ and $[W^0:0] = q$, if $\mathfrak{o}/\mathfrak{p} = \mathbb{F}_q$ imply

$$X + \gamma = X \mod \mathfrak{p}_0, \quad \prod_{\pi} h(X + \gamma) \equiv h(X)(X^q) = h(X^q) \mod \mathfrak{p}_0.$$

Hence, it follows from (5.2) that $(Nh)(X^q) \equiv h(X^q) \mod \mathfrak{p}$ so that $(Nh)(X) \equiv h(X) \mod \mathfrak{p}$.

(iii) Let $h \in S^\times$—that is, $h(0) \neq 0 \mod \mathfrak{p}$. Then $N(h)(0) \equiv h(0) \neq 0 \mod \mathfrak{p}$ by (ii) so that $N(h) \in S^\times$. For $h(X) = X$, $X + 0 = X$ implies

$$N(X) = Xh_1(X), \quad \text{with } h_1 \in S. \quad (5.3)$$

Hence, by (5.2),

$$[\pi](h_1 \circ [\pi]) = X \prod_{\gamma \neq 0} (X + \gamma), \quad \gamma \in W^0.$$
Dividing the both sides by $X$ and putting $X = 0$, we obtain

$$\pi h_1(0) = \prod_{\gamma \neq 0} \gamma, \quad \gamma \in W^0.$$ 

By the Corollary (i) of Proposition 5.4, the product on the right is the norm of $\gamma \neq 0$ in $W^0$ for the extension $k^0_\pi/k$. By Proposition 4.2(ii) and Proposition 5.4(ii), such a $\gamma$ is a prime element of the totally ramified extension $k^0_\pi$ over $k$. Hence the norm of $\gamma$—namely, $\pi h_1(0)$—is a prime element of $k$. Therefore, $h_1(0)$ is a unit of $k$ and it follows from (5.3) that $N(X) \in X'S^\times$. By (i), we now see that $h \in X'S^\times$ implies $N(h) \in X'S^\times$.

(iv) Write $h$ in the form $h = 1 + \pi h_1$, $i \geq 1$, $h_1 \in S$. Then

$$N(h) [\pi] = \prod_{\gamma} (1 + \pi h_1(X + \gamma)) \equiv (1 + \pi h_1(X))^q \mod \pi^i p_0$$

$$= 1 + q \pi h_1(X) + \cdots + \pi^q h_1(X)^q \equiv 1 \mod \pi^i p_0.$$ 

Let $N(h) = 1 + h_2$, $h_2 \in S$. Then it follows that

$$h_2 \circ [\pi] \equiv 0 \mod \pi^i p_0,$$ 

hence, $\mod \pi^{i+1}$.

Therefore, $h_2 \equiv 0 \mod \pi^{i+1}$—namely, $N(h) \equiv 1 \mod \pi^{i+1}$—by Lemma 5.7.

We now define the iteration $N^n$ of the norm operator $N$ on $S$ by

$$N^0(h) = h, \quad N^n(h) = N(N^{n-1}(h)) = N(N(\ldots(N(h))\ldots)),$$ 

for $n \geq 1$.

**Lemma 5.9.** (i) $N^n(h) \circ [\pi^n] = \prod_{\alpha} h(X + \alpha)$, for $\alpha \in W^{n-1}$, $n \geq 0$.

(ii) If $h \in X'S^\times$, $i \geq 0$, then $N^{n+1}(h)/N^n(h) \in S^\times$ and

$$N^{n+1}(h) / N^n(h) \equiv N^n(h) \mod \pi^{n+1}, \quad n \geq 0.$$ 

**Proof.** (i) For $n = 0, 1$, this is trivial. Let $n \geq 2$ and assume that the equality in (i) holds for $n - 1$. Let $A$ be a set of representatives for $W^{n-1}/W^0$ in $W^{n-1}$: $W^{n-1} = A + W^0 = \{\alpha + \gamma \mid \alpha \in A, \gamma \in W^0\}$. Then

$$\prod_{\alpha \in W^{n-1}} h(X + \alpha) = \prod_{\alpha \in A} \prod_{\gamma \in W^0} h(X + \alpha + \gamma) = \prod_{\alpha \in A} N(h)[[\pi](X + \alpha)],$$ 

where

$$[\pi](X + \alpha) = [\pi](X) + [\pi](\alpha) = [\pi](X) + \pi \cdot \alpha, \quad \alpha \in A.$$ 

Since $W^{n-2} = \pi \cdot W^{n-1} = \pi \cdot A$, it follows that

$$\prod_{\alpha \in W^{n-1}} h(X + \alpha) = \prod_{\beta \in W^{n-2}} N(h)[[\pi](X + \beta)],$$ 

and by the induction assumption, the last term is equal to

$$N^{n-1}(N(h)) \circ [\pi^{n-1}([\pi](X))] = N^n(h) \circ [\pi^n].$$

(ii) By Lemma 5.8(iii), $h \in X'S^\times$, $i \geq 0$, implies $N^n(h) \in X'S^\times$ for all $n \geq 0$. Hence $N^{n+1}(h)/N^n(h) \in S^\times$. By Lemma 5.8(ii), we have

$$h_1 \equiv 1 \mod \pi, \quad \text{for } h_1 = N(h)/h \in S^\times.$$
Hence, by (iv) of the same lemma, we obtain successively
\[ N(h_1) \equiv 1 \mod p^2, \ldots, N^n(h_1) \equiv 1 \mod p^{n+1}. \]
Since \( N^a(h_1) = N^{a+1}(h)/N^a(h) \), the assertion in (ii) is proved.

We still keep fixed a power series \( f(X) \) in \( \mathbb{F}_p^1 = \mathbb{F}_p \cap S \) and choose an element \( \alpha \) such that \( \alpha \in W^n, \alpha \not\in W^{n-1}, n \geq 0 \). Let
\[ \alpha_i = \pi^{n-i} \cdot \alpha = [\pi^{n-i}] (\alpha), \quad \text{for } 0 \leq i \leq n. \]
Then \( \alpha_i \in W^i \subseteq k^i_\pi, \alpha_i \not\in W^{i-1} \) so that by Proposition 5.4(ii) for \( m = 1 \), \( \alpha \) is a prime element of \( k^i_\pi \), and
\[ o_i = o[\alpha_i], \quad p_i = o_0 \alpha_i \]
for the valuation ring and the maximal ideal of \( k^i_\pi \).

**Lemma 5.10.** Let \( \beta_i \in \pi^{-i} p_0 o_i \) for \( 0 \leq i \leq n \). Then there exists a power series \( h(X) \) in \( S = o[[X]] \) such that
\[ h(\alpha_i) = \beta_i, \quad \text{for } 0 \leq i \leq n. \]

**Proof.** Let
\[ g_i(X) = [\pi^{n+1}] [\pi^{i+1}] / [\pi^{i+1}], \quad 0 \leq i \leq n. \]
Since \( [\pi^j] \equiv \pi^j X \mod \deg 2 \) for \( j \geq 0 \),
\[ [\pi^{n+1}] = [\pi^{n-i}] \circ [\pi^{i+1}] = \pi^{n-i} [\pi^{i+1}] \mod \deg 2 \text{ in } [\pi^{i+1}]. \]
Hence
\[ g_i(X) = (\pi^{n-i} + a_1 [\pi^{i+1}] + a_2 [\pi^{i+1}]^2 + \cdots) [\pi^j], \quad a_1, a_2, \ldots \in o \]
so that \( g_i \in S \). Now, it follows from \( [\pi^j] (\alpha_i) = a_0, [\pi^{i+1}] (\alpha_i) = 0 \) that
\[ g_i(\alpha_i) = \pi^{n-i} a_0. \]
If \( 0 \leq j < i \), then \( [\pi^j] (\alpha_j) = 0 \) implies \( g_i(\alpha_j) = 0 \); and if \( i < j \leq n \), then \( [\pi^{i+1}] (\alpha_j) = \alpha_{j-i-1} \not= 0 \) and \( [\pi^{i+1}] (\alpha_j) = 0 \) imply again \( g_i(\alpha_j) = 0 \). Since \( \beta_i \in \pi^{-i} p_0 o_i \), where \( p_0 o_i = a_0 o[\alpha_i] \), we may write \( \beta_i \) in the form
\[ \beta_i = \pi^{n-i} a_0 h_i(\alpha_i), \quad \text{with } h_i(X) \in o[X]. \]
Then
\[ h = \sum_{i=0}^n g_i h_i \]
belongs to \( S \) and it clearly satisfies \( h(\alpha_i) = \beta_i \) for \( 0 \leq i \leq n \).

We now prove a main result of Coleman [5].

**Proposition 5.11.** Let \( \pi \) be a prime element of \( k (= k^1_{ur}) \) and let \( f \in \mathbb{F}_p^1 = \mathbb{F}_p \cap o[[X]]. \) Fix an element \( \alpha \in W^n, \alpha \not\in W^{n-1}, n \geq 0 \), and let \( \alpha_i = \pi^{n-i} \cdot \alpha \) for \( 0 \leq i \leq n \). Let \( \xi \) be any element of \( U(k^i_n) \) and let
\[ \xi_i = N_{n,i}(\xi), \quad 0 \leq i \leq n, \]
where \( N_{n,i} \) denotes the norm from \( k^n \) to \( k^i \). Then there exists a power series \( h(X) \) in \( \mathcal{O}[[X]] \) such that

\[
\xi_i = h(\alpha_i), \quad \text{for } 0 \leq i \leq n.
\]

**Proof.** Since \( U(k^n) \subseteq \mathcal{O} = \mathcal{O}[\alpha] \), we have

\[
\xi = h_1(\alpha), \quad \text{with } h_1(X) \in \mathcal{O}[X].
\]

Furthermore, \( \xi \in U(k^n) \) implies that \( h_1(0) \neq 0 \mod \mathfrak{p} \) so that \( h_1(X) \in S^\times \) in \( S = \mathcal{O}[[X]] \). By Lemma 5.9(i),

\[
N_{n,i}(h_1) \circ [\pi^{n-i}] = \prod_{\gamma} h_1(X + \gamma), \quad \gamma \in \mathcal{W}^{n-i-1}, \quad 0 \leq i \leq n.
\]

Put \( X = \alpha \) in the above. Then, by the Corollary of Proposition 5.4,

\[
N_{n,i}(h_1)(\alpha_i) = \prod_{\gamma} h_1(\alpha + \gamma) = N_{n,i}(h_1(\alpha)) = N_{n,i}(\xi) = \xi_i, \quad 0 \leq i \leq n.
\]

Let \( h_2 = N^n(h_1) \in S^\times \). Then, by Lemma 5.9(ii),

\[
N_{n,i}(h_1) = N_{n,i+1}(h_1) = \cdots = N^n(h_1) = h_2 \mod \mathfrak{p}^{n-i+1}.
\]

Putting \( X = \alpha_i \), we obtain

\[
\xi_i = N_{n,i}(h_1)(\alpha_i) = h_2(\alpha_i) \mod \mathfrak{p}^{n-i+1}
\]

so that

\[
\beta_i = \xi_i - h_2(\alpha_i) \in \pi^{n-i+1} \mathcal{O}_i \subseteq \pi^{n-i} \mathcal{O}_i, \quad 0 \leq i \leq n.
\]

Therefore, by Lemma 5.10, \( \beta_i = h_3(\alpha_i), 0 \leq i \leq n \), with some \( h_3 \in S \). Consequently,

\[
\xi_i = h(\alpha_i), \quad 0 \leq i \leq n,
\]

for \( h = h_2 + h_3 \) in \( S = \mathcal{O}[[X]] \).  

---

### 5.3. Abelian Extensions \( L \) and \( k_\pi \)

Let \( \pi \) be a prime element of \( k_{ur}^m, m \geq 1 \). Since \( W_{f}^{n-1} \subseteq W_{f}^{n} \) for \( f \in \mathcal{F} \), it follows from the definition of \( k_{\pi}^{m,n} \) and \( L^n \) in Section 5.1 that

\[
k = k_{ur}^m = k_{\pi}^{m,-1} \subseteq k_{\pi}^{m,0} \subseteq \cdots \subseteq k_{\pi}^{m,n} \subseteq \cdots \subseteq \Omega,
\]

\[
k_{ur} = K = L^{-1} \subseteq L^2 \subseteq \cdots \subseteq L^n \subseteq \cdots \subseteq \Omega.
\]

Let

\[
k_{\pi}^{m,\infty} = \text{the union of } k_{\pi}^{m,n} \text{ for all } n \geq -1,
\]

\[
L = \text{the union of } L^n \text{ for all } n \geq -1.
\]

Clearly

\[
k_{\pi}^{m,\infty} = k_{ur}(W_f), \quad \text{for any } f \in \mathcal{F}_\pi^m,
\]

\[
L = k_{ur}(W_f), \quad \text{for any } f \in \mathcal{F}_\pi^\infty.
\]
PROPOSITION 5.12. \( L \) is an abelian extension over \( k \) and

\[ L = k_{ur}k_\pi^{m,\infty}, \quad k_{ur}^m = k_{ur} \cap k_\pi^{m,\infty}. \]

Hence \( k_\pi^{m,\infty} \) is a maximal totally ramified extension over \( k_{ur}^m \) in \( L \) and

\[ \text{Gal}(L/k_{ur}^m) = \text{Gal}(L/k^{m,\infty}) \times \text{Gal}(L/k_{ur}) \]

\[ \cong \text{Gal}(k_{ur}/k_{ur}^m) \times \text{Gal}(k_\pi^{m,\infty}/k_{ur}^m). \]

**Proof.** By Proposition 5.2(iii), each \( L_n/k \) is an abelian extension. Hence \( L/k \) is also an abelian extension. The rest is a consequence of Proposition 5.2(ii). \( \square \)

PROPOSITION 5.13. There exist topological isomorphisms

\[ \delta : U \cong \text{Gal}(L/k_{ur}), \]

\[ \delta_\pi : U \cong \text{Gal}(k_\pi^{m,\infty}/k_{ur}^m), \]

which induce, for each \( n \geq 0 \), the homomorphisms \( \delta^n \) and \( \delta^n_\pi \), respectively, of Proposition 5.3.

**Proof.** Similar to the proof of Proposition 4.12. \( \square \)

Note that by Proposition 5.3, \( \delta \) has the property:

\[ \delta(u)(\alpha) = u \frac{1}{f} \alpha, \quad u \in U, \quad \alpha \in W_f^n \]

for any \( n \geq 0 \) and for any \( f \) in \( \mathcal{F}^\infty \). Similarly for \( \delta_\pi \).

For \( m = 1 \) and \( \pi \in k = k_{ur}^1 \), let \( k_\pi^{1,\infty} \) be denoted by \( k_\pi \):

\[ k_\pi = k_\pi^{1,\infty} = \text{the union of } k_\pi^n = k_\pi^{1,n} \text{ for all } n \geq -1. \]

As a special case of the above proposition, we see that

\[ L = k_{ur}k_\pi, \quad k = k_{ur} \cap k_\pi \]

so that \( k_\pi \) is a maximal totally ramified extension over \( k \) in \( L \) and

\[ \text{Gal}(L/k) = \text{Gal}(L/k_\pi) \times \text{Gal}(L/k_{ur}) \]

\[ \cong \text{Gal}(k_{ur}/k) \times \text{Gal}(k_\pi/k), \quad (5.4) \]

\[ \delta_\pi : U \cong \text{Gal}(k_\pi/k). \]

Now, fix a prime element \( \pi \) of \( k \) and an integer \( m \geq 1 \). Let

\[ k' = k_{ur}^m, \quad \varphi' = \varphi_{k'} = \text{the Frobenius automorphism of } k'. \]

Clearly \( \varphi' = \varphi^m \), \( \varphi = \varphi_k \) being the Frobenius automorphism of \( k \). Let \( \pi' \) be any prime element of \( k' \). Since \( \pi \) is also a prime element of \( k' \), we have

\[ \pi' = \pi \xi, \quad \text{with } \xi \in U(k'). \]

Let

\[ u = N_{k'k}(\xi) \in U(k). \]
The following lemma relates the action of the Frobenius automorphism on the formal groups for $\pi$ and $\pi'$ to the action of the endomorphism $[u]_f$.

**Lemma 5.14.** Let $f \in \mathcal{F}_\pi^1$, $f' \in \mathcal{F}_{\pi'}$, and let $\theta(X)$ be the power series in (4.8). Then

$$\theta^{\varphi'} = \theta \circ [u]_f.$$  

**Proof.** Let $g_{m-1}$ and $g'_{m-1}$ be defined for $f$ and $f'$ as in Lemma 4.6. The proof of the same lemma shows that

$$g'_{m-1} \circ \theta = \theta \circ \varphi' \circ g_{m-1}.$$  

Let

$$x = N_{k'/k}(\pi') = \pi^m u.$$  

It is clear from the definition of $g'_{m-1}$ that $g'_{m-1}(X) = xX \mod \deg 2$. On the other hand, since $f' \in \mathcal{F}_{\pi'}$, $f' \varphi' = f'$, we see from the definition of $g'_{m-1}$ that $f' \circ g'_{m-1} = g'_{m-1} \circ f'$. Hence, by the uniqueness in (4.8) and Proposition 4.5,

$$g'_{m-1} = [x]_f = [x]_{\varphi'}, \quad g'_{m-1} \circ \theta = \theta \circ [x]_f = \theta \circ [u]_f \circ [\pi^m]_f.$$  

However, since $f$ belongs to $\mathcal{F}_\pi^1$, we have $f = [\pi]_f$, $g_{m-1} = [\pi^m]_f$. Therefore, it follows from (5.5) that

$$\theta \circ [u]_f \circ [\pi^m]_f = \theta \circ \varphi' \circ [\pi^m]_f.$$  

As $[\pi^m]_f = [\pi]_f \circ \cdots \circ [\pi]_f$, the equality of the lemma follows from the remark after Lemma 5.7. \hfill \Box

**Lemma 5.15.** Let $\pi'$ be another prime element of $k$ and let $\pi' = \pi u$ with $u \in U_{n+1}$. Then

$$k^n_{\pi'} = k^n_{\pi'}, \quad \langle \pi \rangle \times U_{n+1} \subseteq N(k^n_{\pi}/k), \quad n \geq -1.$$  

**Proof.** Apply the preceding lemma for $m = 1$, $\varphi = \varphi'$, $\pi' = \pi u$. Let $\alpha' \in W^n_{f'}$. By (4.9), $W^n_{f'} = \theta(W^n_{f})$ so that $\alpha' = \theta(\alpha)$ with $\alpha \in W^n_{f}$. By Lemma 5.14,

$$\theta^{\varphi}(\alpha) = \theta([u]_f(\alpha)).$$  

But, as $u \in U_{n+1}$, $\alpha \in W^n_f$, it follows from Proposition 5.4(ii) that $[u]_f(\alpha) = \alpha$ so that $\theta^{\varphi}(\alpha) = \theta(\alpha)$. On the other hand, since $k_{ur} \cap k^n_{\pi} = k$ by Proposition 5.2(ii) for $m = 1$, the Frobenius automorphism $\varphi$ of $k_{ur}/k$ can be extended to the Frobenius automorphism of $L^n = k_{ur} k^n_{\pi}$ over $k^n_{\pi}$ and, hence, to an automorphism of its closure $\bar{L}^n$ over $k^n_{\pi}$. As $\alpha \in W^n_{f} \subseteq k^n_{\pi}$, we then obtain

$$\theta(\alpha)' = \theta^{\varphi}(\alpha)' = \theta(\alpha), \quad \alpha' = \theta(\alpha) \in L^n = k_{ur}(W^n_{f'}).$$  

Therefore, $\alpha' = \theta(\alpha) \in k^n_{\pi'}$ because $\varphi$ is the Frobenius automorphism of $L^n/k^n_{\pi}$. Thus

$$k^n_{\pi'} = k(W^n_{f'}) \subseteq k^n_{\pi'}.$$  

Since $\pi = u^{-1} \pi'$, $u^{-1} \in U_{n+1}$, we obtain similarly $k^n_{\pi} \subseteq k^n_{\pi'}$. Hence $k^n_{\pi} = k^n_{\pi'}$.  

for \( \pi' = \pi u, \ u \in U_{n+1} \). By Proposition 5.4(i) both \( \pi \) and \( \pi' \) are contained in \( N(k^n_{\pi}/k) = N(k^n_{\pi'}/k) \). Consequently, \( u = \pi'/\pi \in N(k^n_{\pi}/k) \) for every \( u \in U_{n+1} \)—namely, \( U_{n+1} \subseteq N(k^n_{\pi'}/k) \). Hence \( \langle \pi \rangle \times U_{n+1} \subseteq N(k^n_{\pi'}/k) \). 

**Proposition 5.16.** For any prime element \( \pi \) of \( k \),

\[
N(k^n_{\pi'}/k) = \langle \pi \rangle \times U_{n+1}, \quad \text{for } n \geq -1.
\]

**Proof.** Since we know

\[
\langle \pi \rangle \times U_{n+1} \subseteq N(k^n_{\pi'}/k) \subseteq k^x = \langle \pi \rangle \times U,
\]

it is sufficient to show that

\[
NU(k^n_{\pi'}/k) = U \cap N(k^n_{\pi'}/k) \subseteq U_{n+1}.
\]

Let \( u \in NU(k^n_{\pi'}/k) \)—namely, \( u = N'(\xi) \), where \( \xi \in U(k^n_{\pi}) \) and \( N' \) denotes the norm of the extension \( k^n_{\pi'}/k \). Fix an element \( \alpha \in W^f, \ \alpha \not\in W^f \). As in the proof of Proposition 5.11, we then have

\[
\xi = h_1(\alpha), \quad \text{with } h_1(X) \in S^x.
\]

By Lemma 5.9(ii),

\[
N^n(h_1), N^{n+1}(h_1) \in S^x, \quad N^{n+1}(h_1) = N^n(h_1) \mod p^{n+1}.
\]

Let \( u_1 = N^n(h_1)(0), \ u_2 = N^{n+1}(h_1)(0) \). Then it follows from the above that

\[
u_1, u_2 \in U = U(k), \quad u_2 \equiv u_1 \mod p^{n+1}.
\]

However, by Lemma 5.9(i)

\[
u_1 = \prod_{\beta \in W^{n-1}} h_1(\beta), \quad u_2 = \prod_{\beta \in W^n} h_1(\beta)
\]

so that

\[
u_2/\nu_1 = \prod_{\beta} h_1(\beta), \quad \text{where } \beta \in W^f, \ \beta \not\in W^{n-1}.
\]

Therefore, by the Corollary (i) of Proposition 5.4 for \( m = 1 \),

\[
u_2/\nu_1 = N'(h_1(\alpha)) = N'(\xi) = u.
\]

Hence \( u_2 \equiv u_1 \mod p^{n+1} \) implies \( u \equiv 1 \mod p^{n+1} \)—namely, \( u \in U_{n+1} \). Thus \( NU(k^n_{\pi'}/k) \subseteq U_{n+1} \).

**Proposition 5.17.** For any prime element \( \pi \) of \( k \),

\[
N(k^n_{\pi}/k) = \langle \pi \rangle.
\]

More generally, if \( F \) is a totally ramified extension over \( k \) in \( \Omega \), containing \( k : k \subseteq F \subseteq \Omega \), then

\[
N(F/k) = \langle \pi \rangle.
\]

**Proof.** Since the intersection of \( U_{n+1} = 1 + p^{n+1} \) for all \( n \geq 0 \) is 1, the first part follows immediately from Proposition 5.16. Let \( F \) be as stated
above. Then

\[ N(F/k) \subseteq N(k_\pi/k) = \langle \pi \rangle. \]

However, since \( F/k \) is totally ramified, \( N(F/k) \) contains, by Proposition 3.8, a prime element of \( k \). Since \( \pi \) is the only prime element of \( k \) in \( \langle \pi \rangle \), it follows that \( \pi \in N(F/k) \) so that \( N(F/k) = \langle \pi \rangle \).

\textbf{Remark.} The fields \( k_{\pi, n}^{m, n} \) in Section 5.1 were introduced by de Shalit [61] as generalizations of the abelian extensions \( k_\pi^n \) in Lubin-Tate [19]. He also generalized the result of Sections 5.2 and 5.3 and proved, for example, that

\[ N(k_{\pi, n}^{m, n}/k) = \langle N_{k_\pi^n/k}(\pi) \rangle \]

for any prime element \( \pi \) of \( k' = k_{\pi, n}^{m, n} \). However, since Proposition 5.17 (i.e., the case \( m = 1 \) in the above equality) is sufficient for our applications in Chapter VI, we discussed here only the classical case of \( k_\pi^n \) for the sake of simplicity.
Chapter VI

Fundamental Theorems

Let $k_{ab}$ denote the maximal abelian extension, in $\Omega$, of the local field $(k, \nu)$. Using the results on the abelian extensions $L^n$, $k_{\pi}^m$, and $k_{\pi}^n$ over $k$ obtained in the last chapter, we are now going to prove fundamental theorems in local class field theory. Namely, we shall define the so-called norm residue map

$$\rho_k : k^\times \rightarrow \text{Gal}(k_{ab}/k)$$

and then discuss the functorial properties of $\rho_k$ with respect to a change of the ground field $k$.

6.1. The Homomorphism $\rho_k$

In Section 5.3, we introduced an abelian extension $L$ of the local field $(k, \nu)$. $L$ will be denoted also by $L_k$ when the ground field $k$ is varied. Clearly

$$k \subseteq L \subseteq k_{ab},$$

where $k_{ab}$ is, as stated above, the maximal abelian extension over $k$ in $\Omega$. For each prime element $\pi$ of $(k, \nu)$, we also defined in Section 5.3 an abelian extension $k_{\pi}$ of $k$, contained in $L$. Let $\varphi_k$ denote, as before, the Frobenius automorphism of $k$: $\varphi_k \in \text{Gal}(k_{ur}/k)$. Since

$$\text{Gal}(L/k_{\pi}) \cong \text{Gal}(k_{ur}/k)$$

by (5.4), there exists a unique element $\psi_{\pi}$ in $\text{Gal}(L/k)$ such that

$$\psi_{\pi} | k_{ur} = \varphi_k, \quad \psi_{\pi} | k_{\pi} = 1. \quad (6.1)$$

As $\langle \varphi_k \rangle$ is dense in $\text{Gal}(k_{ur}/k)$, $\langle \psi_{\pi} \rangle$ is a dense subgroup of $\text{Gal}(L/k_{\pi})$ so that $k_{\pi}$ is the fixed field of $\psi_{\pi}$ in $L$.

Now, fix a prime element $\pi_0$ of $(k, \nu)$ and, for simplicity, write $\psi$ for $\psi_{\pi_0}$. Since $k^\times = \langle \pi_0 \rangle \times U$, each $x$ in $k^\times$ can be written uniquely in the form

$$x = \pi_0^m u, \quad m \in \mathbb{Z}, \quad u \in U.$$ 

In fact, here $m = \nu(x)$. For such an $x$, let

$$\rho(x) = \psi^m \delta(u^{-1}), \quad (6.2)$$

where

$$\delta : U \cong \text{Gal}(L/k_{ur})$$

is the isomorphism in Proposition 5.13. It is then clear that the map $x \mapsto \rho(x)$ defines a homomorphism of abelian groups

$$\rho : k^\times \rightarrow \text{Gal}(L/k)$$
satisfying
\[ \rho(x) \mid k_{ur} = \psi^m \mid k_{ur} = \varphi_k^m, \quad \text{with } m = \nu(x). \] (6.3)

**Lemma 6.1.** Let \( \pi' \) be a prime element of \( k' = k_{ur}^m, m \geq 1 \), and let
\[ x = N_{k'/k}(\pi'). \]
Then \( \rho(x) \) is the unique element \( \sigma \) of \( \text{Gal}(L/k) \) such that
\[ \sigma \mid k_{ur} = \varphi_k^m, \quad \sigma \mid k_{\pi', 0}^m = 1. \]

**Proof.** Since \( \varphi_k^m \) is the Frobenius automorphism \( \varphi_k \cdot \) of \( k': \varphi_k^m = \varphi_k \in \text{Gal}(k_{ur}/k') \), it follows from Proposition 5.12 that there is a unique element \( \sigma \) in \( \text{Gal}(L/k) \) with the properties stated above. As \( \rho(x) \) satisfies (6.3), it is sufficient to prove that \( \rho(x) \mid k_{\pi', 0}^m = 1 \) (namely, that
\[ \rho(x) \mid k_{\pi', 0}^m = 1, \quad \text{for all } n \geq 1. \]
Now, the prime element \( \pi_0 \) of \( k \) is also a prime element of the unramified extension \( k' \) over \( k \). Hence
\[ \pi' = \pi_0 \xi \]
with some \( \xi \) in \( U(k') \), so that
\[ x = N_{k'/k}(\pi') = \pi_0^m u, \quad u = N_{k'/k}(\xi) \in U = U(k). \]
Let \( f \in \mathcal{F}_{\pi_0}, f' \in \mathcal{F}_{\pi}', \) and let \( \theta(X) \) be the power series in (4.8) for \( f, f' \). Then, by Lemma 5.14,
\[ \theta^{\pi'} = \theta \circ [u]_f, \]
where \( \varphi' \) denotes the extension of \( \varphi_k \cdot \) on the completion \( \tilde{K} \) of \( K = k_{ur} \). Let \( \alpha' \in W_{\pi}' = \theta(W_{\pi}') \) and let \( \alpha' = \theta(\alpha), \alpha \in W_{\pi}. \) By (6.2) and Proposition 5.3,
\[ \rho(x)(\alpha) = \delta([u^{-1}](\alpha) = [u^{-1}]_f(\alpha). \]
Using the fact that \( \theta(X) \in o_k[[X]] \) and that \( \rho(x) \) extends to \( \varphi' \) on \( \tilde{K} \), we see from \( \alpha' = \theta(\alpha) \) that
\[ \rho(x)(\alpha') = \theta^{\pi'}(\rho(x)(\alpha)) = \theta \circ [u]_f \circ [u^{-1}]_f(\alpha) = \theta(\alpha) = \alpha'. \]
Since \( k_{\pi', 0}^m = k'(W_{\pi}') \), we obtain \( \rho(x) \mid k_{\pi', 0}^m = 1. \]

**Remark.** The above proof shows why we define \( \rho(x) \) by (6.2) instead of \( \rho(x) = \psi^m \delta(u). \)

**Proposition 6.2.** There exists a unique homomorphism
\[ \rho_k : k^\times \rightarrow \text{Gal}(L/k) \]
such that
\[ \rho_k(\pi) = \psi_\pi \]
for every prime element \( \pi \) of \( k \).

**Proof.** Applying Lemma 6.1 for \( m = 1, \pi' = \pi \), we see that \( \rho(\pi) \) is the
unique element of \( \text{Gal}(L/k) \) such that
\[
\rho(\pi) \mid k_{ur} = \varphi_k, \quad \rho(\pi) \mid k_{\pi} = 1.
\]
Hence \( \rho(\pi) = \psi_\pi \) by (6.1). Thus the homomorphism \( \rho: k^\times \to \text{Gal}(L/k) \),
defined above by means of a fixed prime element \( \pi_0 \) of \( k \), has the property mentioned in the proposition. Let \( u \in U \) and let \( \pi' \) be a prime element of \( k \).
Then \( \pi'' = \pi'u \) is again a prime element of \( k \) and \( u = \pi''/\pi' \). Hence the multiplicative group \( k^\times \) is generated by the prime elements of \( k \). This implies the uniqueness of \( \rho_k \). 

Since \( \rho_k = \rho \), it follows from (6.2) that \( \rho_k \) induces the topological isomorphism
\[
U \cong \text{Gal}(L/k_{ur}),
\]
\[
\delta(u^{-1})
\]
on the subgroup \( U \) of \( k^\times \). Let \( \pi \) be a prime element of \( k \) and let
\[
x = \pi^m u, \quad m = \nu(x) \in \mathbb{Z}, \quad u \in U,
\]
for an element \( x \) of \( k^\times \). Then
\[
\rho_k(x) = \rho_k(\pi)^m \rho_k(u) = \psi_\pi^m \delta(u^{-1}),
\]
\[
\rho_k(x) \mid k_{ur} = \psi_\pi^m \mid k_{ur} = \varphi_k^m, \quad m = \nu(x).
\]
Thus (6.2) and (6.3) hold not only for the particular prime element \( \pi_0 \) but also for any prime element \( \pi \) of \( k \). (This is also clear from the fact that \( \rho = \rho_k \) is independent of the choice of \( \pi_0 \).)

**Proposition 6.3.** (i) \( \rho_k \) is injective and is continuous in the \( \nu \)-topology of \( k^\times \) and Krull topology of the Galois group \( \text{Gal}(L/k) \).

(ii) The image of \( \rho_k \) is a dense subgroup of \( \text{Gal}(L/k) \) and consists of all elements \( \sigma \) in \( \text{Gal}(L/K) \) such that \( \sigma \mid k_{ur} = \varphi_k^m \) for some integer \( m \). In particular, if \( \sigma \mid k_{ur} = \varphi_k \), then there is a unique prime element \( \pi \) of \( k \) such that \( \sigma = \rho_k(\pi) \).

**Proof.** (i) Let \( \rho_k(x) = 1 \) for \( x = \pi^m u \) in (6.5). Then \( \varphi_k^m = \rho_k(x) \mid k_{ur} = 1 \), and since \( \langle \varphi_k \rangle = \mathbb{Z} \), it follows that \( m = 0 \), \( x = u \), \( \delta(u^{-1}) = \rho_k(u) = \rho_k(x) = 1 \). As \( \delta \) is an isomorphism, we then see that \( u = 1 \)—namely, \( x = 1 \). Thus \( \rho_k \) is injective. The continuity of \( \rho_k \) follows from the fact that it induces a topological isomorphism \( U \cong \text{Gal}(L/k_{ur}) \) on the open subgroup \( U \) of \( k^\times \).

(ii) By (5.4), \( \text{Gal}(L/K) = \text{Gal}(L/k_{\pi}) \times \text{Gal}(L/k_{ur}) \). Hence the first part of (ii) is a consequence of (6.5), \( \rho_k(U) = \text{Gal}(L/k_{ur}) \), and the fact that \( \langle \psi_\pi \rangle \) is a dense subgroup of \( \text{Gal}(L/k_{\pi}) \). The second part is also clear from (6.5) for \( m = 1 \). 

Now, let \( k'/k \) be a finite extension of local fields and let
\[
\rho_k: k^\times \to \text{Gal}(L_k/k), \quad \rho_{k'}: k'^\times \to \text{Gal}(L_{k'}/k')
\]
be the associated homomorphisms given by Proposition 6.2. We shall next prove an important preliminary result on the relation between \( \rho_k \) and \( \rho_{k'} \).
For simplicity, let \( L = L_k, L' = L_{k'} \), and let \( E = L \cap L' \).

Since \( k \subseteq E \subseteq L \) and \( L/k \) is abelian, \( \rho_k(x) \), for \( x \in k^\times \), induces an automorphism of \( E/k \). Let \( x' \in k'^\times \). Then \( \rho_{k'}(x') \) is an automorphism of \( L' \) over \( k' \), and hence, over \( k \). Therefore, \( \rho_{k'}(x') \) also induces an automorphism of \( E/k \).

**Lemma 6.4.** Suppose that \( k'/k \) is a totally ramified finite extension of local fields. Then

\[
\rho_{k'}(x') \mid E = \rho_k(N_{k'/k}(x')) \mid E, \quad \text{for all } x' \in k'^\times.
\]

**Proof.** Since \( k'^\times \) is generated by the prime elements of \( k' \), it is sufficient to prove the above equality for a prime element \( \pi' \) of \( k' \). Extend \( \rho_{k'}(\pi') \) in \( \text{Gal}(L'/k') \) to an automorphism \( \tau \) of the algebraic closure \( \Omega \) over \( k \) and let \( F \) denote the fixed field of \( \tau \) in \( \Omega \). Since the fixed field of \( \psi_{\pi'} = \rho_{k'}(\pi') \) in \( L' \) is \( k'_{\pi'} \) by (6.1),

\[
F \cap L' = k_{\pi'}, \quad F \cap k'_{ur} = k_{\pi'} \cap k'_{ur} = k'
\]

so that \( F/k' \) is totally ramified and \( k' \subseteq k_{\pi'} \subseteq F \). Hence, by Proposition 5.17,

\[
N(F/k') = \langle \pi' \rangle. \tag{6.6}
\]

On the other hand, \( \tau \mid k'_{ur} = \rho_{k'}(\pi') \mid k'_{ur} = \varphi_k \) by (6.5) and \( \varphi_k \mid k_{ur} = \varphi_k \) because \( k'/k \) is totally ramified so that \( \text{Gal}(k'_{ur}/k') \subset \text{Gal}(k_{ur}/k) \). Hence

\[
\tau \mid k_{ur} = (\tau \mid k'_{ur}) \mid k_{ur} = \varphi_k \mid k_{ur} = \varphi_k.
\]

Let \( \sigma = \tau \mid L \). Then \( \sigma \mid k_{ur} = \varphi_k \) by the above. Therefore, by Proposition 6.3(ii),

\[
\sigma = \rho_k(\pi)
\]

for some prime element \( \pi \) of \( k \). Since \( k_{\pi} \) is the fixed field of \( \rho_k(\pi) \) in \( L \) by (6.1),

\[
k \subseteq k_{\pi} \subseteq F = \text{the fixed field of } \tau \text{ in } \Omega,
\]

and since both \( F/k' \) and \( k'/k \) are totally ramified, \( F/k \) is also totally ramified. Hence, again by Proposition 5.17,

\[
N(F/k) = \langle \pi \rangle.
\]

It then follows from (6.6) that

\[
N_{k'/k}(\pi') \in N(F/k) = \langle \pi \rangle.
\]

However, as \( k'/k \) is totally ramified, \( N_{k'/k}(\pi') \) is a prime element of \( k \). Therefore, we see from the above that

\[
N_{k'/k}(\pi') = \pi
\]

so that

\[
\rho_{k'}(\pi') \mid E = \tau \mid E = \sigma \mid E = \rho_k(\pi) \mid E = \rho_k(N_{k'/k}(\pi')) \mid E.
\]

\[\blacksquare\]
**Corollary.** Let \( k'/k \) be a totally ramified finite extension of local fields such that \( k \subseteq k' \subseteq L_k \). Then
\[
\rho_k(N(k'/k)) \mid k' = 1.
\]

**Proof.** Clearly \( k \subseteq k' \subseteq E = L \cap L' \). Hence
\[
\rho_k(N(k'/k)) \mid k' = \rho_{k'}(k'^\infty) \mid k' = 1.
\]

### 6.2. Proof of \( L_k = k_{ab} \)

In this section, we shall prove that the abelian extension \( L (= L_k) \) over \( k \) introduced in Section 5.3 is actually the maximal abelian extension \( k_{ab} \) of \( k \).

We first prove the following key lemma:

**Lemma 6.5.** Let \((k, v)\) be a \( p \)-field and let \((k', v')\) be a cyclic extension of degree \( p \) over \( k \)—that is, \([k': k] = p\). Then
\[
N(k'/k) \neq k^\times.
\]

**Proof.** Let \( G = \text{Gal}(k'/k) \) and let \( G_n, n \geq 0 \), be the ramification groups of \( k'/k \) defined in Section 2.5. Since \( G \) is a cyclic group of order \( p \), each \( G_n \) is either \( G \) or \( 1 \). Suppose first that \( G_0 = 1 \). By Proposition 2.18, \( k'/k \) is then unramified: \( e(k'/k) = 1, f(k'/k) = p \), and it follows from the formula in Proposition 1.5 that \( v(N_{k'/k}(x')) \) is divisible by \( p \) for every \( x' \in k^\times \). Hence a prime element \( \pi \) of \( k \) is not contained in \( N(k'/k) \), and consequently \( N(k'/k) \neq k^\times \).

Next, suppose that \( G_0 = G \) so that \( k'/k \) is totally ramified by Proposition 2.18. By the remark after the Corollary of Proposition 2.19, the index \([G_0: G_1]\) is prime to \( p \). Hence there is an integer \( s \geq 1 \) such that
\[
G = G_0 = G_1 = \cdots = G_s, \quad G_{s+1} = G_{s+2} = \cdots = 1.
\]

Fix a prime element \( \pi' \) of \((k', v')\) and let \( f(X) \) denote the minimal polynomial of \( \pi' \) over \( k \). By the corollary of Proposition 2.13 and Proposition 2.14, the different \( D = D(k'/k) \) of \( k'/k \) is given by \( D = f'(\pi')\sigma' \), where \( f' = df/dX, \sigma' \) is the valuation ring of \((k', v')\). Clearly \( f'(\pi') = \prod_{\sigma} (\pi' - \sigma(\pi')) \) with \( \sigma \) ranging over all elements \( \neq 1 \) in \( G \). Since \( G = G_s, G_{s+1} = 1 \) implies \( v'(\pi' - \sigma(\pi')) = s + 1 \) for all \( \sigma \neq 1 \), we obtain
\[
v'(f'(\pi')) = (p-1)(s+1), \quad D = p^{(p-1)(s+1)},
\]
where \( \pi' \) being the maximal ideal of \((k', v')\). Now, let \( x' \in U_{s+1} = 1 + p^{s+1} \) and let \( x' = 1 + y', y' \in y^{s+1} \). Then
\[
N_{k'/k}(x') = \prod_{\sigma} (1 + \sigma(y')), \quad \sigma \in G,
\]
where \( \lambda \) ranges over all elements of the form \( \lambda = \sigma_1 + \cdots + \sigma_s, 1 \leq t \leq s \).
Fundamental Theorems

$p - 1$, in the group ring $\mathbb{Z}[G]$, with distinct $\sigma_1, \ldots, \sigma_p$ in $G$. Since $p$ is a prime, if $\sigma \neq 1$, then $\sigma\lambda \neq \lambda$ for any such $\lambda$. Hence $\lambda, \sigma\lambda, \ldots, \sigma^{p-1}\lambda$ are distinct elements of $\mathbb{Z}[G]$, and

$$\sum_{\mu} y^{\mu} = T_{k'/k}(y^\lambda)$$

for the partial sum on $\mu = \lambda, \sigma\lambda, \ldots, \sigma^{p-1}\lambda$. However, since $k'/k$ is totally ramified, $y' \in p^{s+1}$ implies

$$\mathcal{D} y^\lambda \in p^{(p-1)(s+1)+(s+1)} = p^{p(s+1)} = p^{s+1}$$

for the maximal ideal $p$ of $(k, \nu)$. Therefore,

$$T_{k'/k}(y^\lambda) \in T_{k'/k}(p^{s+1}\mathcal{D}) = p^{s+1}T_{k'/k}(\mathcal{D}) \subseteq p^{s+1}$$

by the definition of $\mathcal{D} = \mathcal{D}(k'/k)$. On the other hand, by Proposition 1.5, $y' \in p^{s+1}$ also implies $N_{k'/k}(y') \in p^{s+1}$. Hence it follows from (6.7) that

$$N_{k'/k}(x') = 1 \mod p^{s+1}, \quad \text{for } x' = 1 + y' \in U_{s+1}.$$ 

Thus $N_{k'/k}(U_{s+1}) \subseteq U_{s+1}$, and the norm map $N_{k'/k}$ induces a homomorphism

$$U'/U_{s+1} \rightarrow U/U_{s+1}. \quad (6.8)$$

Let $\xi = \sigma(\pi')/\pi'$ for the prime element $\pi'$ of $(k', \nu')$ and for $\sigma \neq 1$ in $G$. Then it follows from $\nu'(\sigma(\pi') - \pi') = s + 1$ that $\xi \in U'_{s+1}$, $\xi \notin U_{s+1}$. Since $N_{k'/k}(\xi) = 1$, we see that the above homomorphism is not injective. However, since $k'/k$ is totally ramified and $\nu'/p' = \nu/p = F_q$, it follows from (2.1) that

$$[U': U_{s+1}] = [U : U_{s+1}] = (q - 1)q^s.$$ 

Hence (6.8) is not surjective. This implies $N_{k'/k}(U') \neq U$ and consequently $N(k'/k) = N_{k'/k}(k'^\times) \neq k^\times$. \hfill \Box

Remark. By the so-called fundamental equality in local class field theory (cf. Section 7.1 below),

$$[k^\times : N(k'/k)] = [k'^\times : k] = p.$$ 

Hence the lemma is trivial if one is allowed to use the above equality. For a $p$-field $(k, \nu)$ of characteristic 0, it may also be proved by using Herbrand quotients. Compare Lang [17], Chap. IX, §3.

Lemma 6.6. Let $(k, \nu)$ be a $p$-field and let $k'/k$ be a cyclic extension of degree $p$: $k \subseteq k' \subseteq k_{ab}$. Then $k'$ is contained in $L$: $k \subseteq k' \subseteq L \subseteq k_{ab}$.

Proof. Assume that $k'$ is not contained in $L$. Since $[k' : k] = p$, it follows that

$$k' \cap L = k, \quad \Gal(k' L/k) \cong \Gal(k'/k) \times \Gal(L/k).$$

Let $\pi$ be any prime element of $k$. Then $\Gal(L/k) \cong \Gal(k_{ur}/k) \times \Gal(k_{\pi}/k)$ by (5.4). Hence we see that $k'k_{\pi} \cap k_{ur} = k$ so that $k'k_{\pi}$ is a totally ramified extension over $k$, containing $k_{\pi}$. Therefore, by Proposition 5.17, $N(k'k_{\pi}/k)$
Local Class Field Theory

Since \( k^\times \) is generated by the prime elements of \( k \), it would then follow \( N(k'/k) = k^\times \), which contradicts Lemma 6.5. Hence \( k' \subseteq L \).

**Lemma 6.7.** Let \( p \) be a prime number and let \( k \) be a field (not necessarily a local field), containing a primitive \( p \)th root of unity \( \zeta_p \). Let \( k' \) be a cyclic extension of degree \( p^s \), \( s \geq 0 \), over \( k \). Suppose that \( k' \) is contained in a cyclic extension \( k'' \) of degree \( p^{s+1} \) over \( k \). Then \( \zeta_p \) is the norm of an element of \( k' \).

**Proof.** Let \( \sigma \) be a generator of \( \text{Gal}(k''/k) \) and let \( \tau = \sigma^p \), so that \( \tau \) is a generator of \( \text{Gal}(k''/k') \). Since \( \zeta_p \in k' \subseteq k'' \), it follows from Kummer theory that \( k'' \) contains an element \( \alpha \) such that

\[
k'' = k'((\alpha), \quad \alpha^{\tau - 1} = \zeta_p.
\]

Let \( \beta = \alpha^{\sigma - 1} \). Then

\[
\beta^{\tau - 1} = (\alpha^{\tau - 1})^{\sigma - 1} = \zeta_p^{\sigma - 1} = 1.
\]

Hence \( \beta \) is an element of \( k' \). Since

\[
\tau - 1 = (\sigma - 1) \sum_i \sigma^i, \quad 0 \leq i < p^s,
\]

\( \beta \) satisfies

\[
N_{k''/k}(\beta) = \alpha^{\tau - 1} = \zeta_p.
\]

**Remark.** The converse of the lemma is also true if \( s > 1 \). See Exercise 7 in Bourbaki, Algebra, Chap. V, §11.

Let \((k, \nu)\) be a \( p \)-field. We now prove \( kab = L \) in several steps.

(i) Since \( k \subseteq k_{ur} \subseteq k_{ab} \), extend the Frobenius automorphism \( \varphi_k \) of \( k \) to an automorphism \( \psi \) of \( k_{ab} \) over \( k \). Let \( F \) denote the fixed field of \( \psi \) in \( k_{ab} \). Then

\[
F_{k_{ur}} = k_{ab}, \quad F \cap k_{ur} = k, \quad \text{Gal}(k_{ab}/F) \cong \text{Gal}(k_{ur}/k)
\]

by Lemma 3.4. Let \( \sigma = \psi \mid L \). Then \( \sigma \mid k_{ur} = \psi \mid k_{ur} = \varphi_k \), and it follows from Proposition 6.3(ii) that \( \sigma = \rho_k(\pi) \) for some prime element \( \pi \) of \( k \). Since \( \sigma = \psi \mid L \), \( L \cap F \) is the fixed field of \( \sigma \) in \( L \) and since \( \sigma = \rho_k(\pi) = \psi_{\pi} \), we see from the remark after (6.1) that

\[
k \subseteq k_{\pi} = L \cap F \subseteq F.
\]

We shall prove that \( k_{\pi} = F \).

(ii) Let \( k' \) be a finite extension of \( k \) such that

\[
k \subseteq k_{\pi} \subseteq k' \subseteq F.
\]

Since \( k_{ur} \cap F = k \), \( k'/k \) is a totally ramified finite abelian extension and \( t = t' = F_{q} \) for the residue fields of \( k \) and \( k' \). Therefore, by the remark at the end of Section 2.5, the degree \( [k':k] \) is the product of a factor of \( q - 1 \) and a power of \( p \). However, \( [k_{\pi}^0:k] = q - 1 \) by Proposition 5.2(iii) for \( m = 1 \). Hence \( [k':k_{\pi}^0] \) is a power of \( p \) for any \( k' \) as above.
(iii) Assume now that

\[ k_\pi \neq F. \]

Then there exists a finite cyclic extension \( E'/k \) such that

\[ k \subseteq E' \subseteq F, \quad E' \nsubseteq k_\pi. \]

By (ii), \([E':E' \cap k_\pi] = [E'k_\pi:k_\pi] \) is a power of \( p \), while \([E' \cap k_\pi:k] \) is prime to \( p \). Hence, there is a cyclic extension \( E/k \) of \( p \)-power degree such that

\[ E(E' \cap k_\pi) = E', \quad E \cap (E' \cap k_\pi) = k. \]

Since \( E' \nsubseteq k_\pi \), \( E \) is not contained in \( k_\pi \). Replacing \( E \) by a subfield if necessary, we see that there exists a finite cyclic extension \( E/k \) with \( p \)-power degree such that

\[ k \subseteq E \subseteq F, \quad [E:E \cap k_\pi] = p. \]

Let

\[ k' = E \cap k_\pi, \quad [k':k] = p^s, \quad [E:k] = p^{s+1}, \quad s \geq 0. \]

By (6.4) and \( \text{Gal}(L/k_{ur}) \cong \text{Gal}(k_\pi/k) \), \( \rho_k \) induces an isomorphism

\[ U \cong \text{Gal}(k_\pi/k). \]

Let \( U' \) be the subgroup of \( U \) such that

\[ U' \rightarrow \text{Gal}(k_\pi/k'), \]

under the above isomorphism. Since \( U/U' \cong \text{Gal}(k'/k) \), \( U/U' \) is a cyclic group of order \( p^s \). Hence there is a character \( \chi \) of \( U/U' \) with order \( p^s \), which we view as a continuous character of the compact group \( U \) with \( \text{Ker}(\chi) = U' \). We shall next show that there is a continuous character \( \lambda \) of \( U \) with order \( p^{s+1} \) such that

\[ \chi = \lambda^p. \]

Consider first the case where \( k \) contains no primitive \( p \)th root of unity. By Proposition 2.7 (for \( a = 0 \)) or Proposition 2.8, \( U_1 = 1 + p \) is isomorphic to the direct product of finitely or infinitely many copies of \( \mathbb{Z}_p \). Since \( U = V \times U_1 \) by (2.2) and since \( \chi(V) = 1 \) for the group \( V \) of order \( q - 1 \), the existence of \( \lambda \) is clear because the character group of \( \mathbb{Z}_p \) is isomorphic to \( \mathbb{Q}_p/\mathbb{Z}_p \), a divisible group. Suppose next that \( k \) contains a primitive \( p \)th root of unity \( \xi_p \). In this case, the \( p \)-field \( k \) has characteristic 0. Since \( k' \) is contained in a cyclic extension \( E \) of degree \( p^{s+1} \) over \( k \), it follows from Lemma 6.7 that \( \xi_p \in N(k'/k) \). Hence, by the Corollary of Proposition 6.4, \( \rho_k(\xi_p) \mid k' = 1 \), so that \( \xi_p \in U' \), \( \chi(\xi_p) = 1 \). It then follows again from Proposition 2.7 and (2.2) that there is a character \( \lambda \) of \( U \) satisfying \( \chi = \lambda^p \).

(iv) Let \( \chi \) and \( \lambda \) be as above. Let \( U'' = \text{Ker}(\lambda) \) and let \( k'' \) be the subfield of \( k_\pi \), corresponding to \( U'' \):

\[ U'' \cong \text{Gal}(k_\pi/k''), \quad U/U'' \cong \text{Gal}(k''/k). \]
Then
\[ k \subseteq k' \subseteq k'' \subseteq k_\pi, \quad E \cap k'' = k', \]
and both \( E/k \) and \( k''/k \) are cyclic extensions of degree \( p^{n+1} \) with \( [E:k'] = [k'':k'] = p \). Hence there exists a cyclic extension \( k^*/k \) with \( [k^*:k] = p \) such that
\[ E k'' = k^* k''. \]
However, by Lemma 6.6, \( k^* \) is contained in \( k_\pi = L \cap F \). Hence \( E \subseteq k^* k'' \subseteq k_\pi \), and this contradicts \( k' = E \cap k_\pi \neq E \). Thus the assumption \( F \neq k_\pi \) in (iii) leads to a contradiction and it is proved that
\[ F = k_\pi, \quad k_{ab} = k_{ur} F = k_{ur} k_\pi = L. \]

**Theorem 6.8.** For each local field \((k, \nu)\),
\[ k_{ab} = L_k, \]

namely,
\[ k_{ab} = k_{ur} k_\pi \]
for any prime element \( \pi \) of \( k \).

**Example.** Let \((k, \nu) = (Q_p, \nu_p)\). In Example 2 of Section 5.1, we have seen that in this case
\[ k_p^n = Q_p(W_{p^{n+1}}), \quad n \geq -1, \]
with \( W_{p^{n+1}} \) the group of all \( p^{n+1} \)-th roots of unity in \( \Omega \). Hence
\[ k_p = \bigcup_n k_p^n = Q_p(W_{p^\infty}), \]
\( W_{p^\infty} \) being the group of all \( p \)-power roots of unity in \( \Omega \). On the other hand, by (3.2),
\[ k_{ur} = Q_p(V_\infty), \]
where \( V_\infty \) is the group of all roots of unity in \( \Omega \) with order prime to \( p \). Therefore, for \((k, \nu) = (Q_p, \nu_p)\), Theorem 6.8—that is, \( k_{ab} = k_{ur} k_p \)—states that the maximal abelian extension \((Q_p)_{ab}\) of \( Q_p \) is generated over \( Q_p \) by all roots of unity in \( \Omega \). Obviously, this is the analogue for \( Q_p \) of the classical theorem of Kronecker, which states that the maximal abelian extension of the rational field \( Q \) is generated over \( Q \) by all roots of unity in the algebraic closure of \( Q \).

### 6.3. The Norm Residue Map

By Proposition 6.2 and Theorem 6.8, we now see that with each local field \((k, \nu)\) is associated a homomorphism
\[ \rho_k : k^\times \to \text{Gal}(k_{ab}/k). \]
\( \rho_k \) is called the **norm residue map**, or, **Artin map**, of the local field \((k, \nu)\).

Some of the properties of \( \rho_k \) were already given by Proposition 6.3 and
(6.4). For convenience, we shall restate such properties of \( \rho_k : k^\times \to \text{Gal}(k_{ab}/k) \) below:

(i) \( \rho_k \) is injective and is continuous in the \( \nu \)-topology of \( k^\times \) and Krull topology of \( \text{Gal}(k_{ab}/k) \).

(ii) The image of \( \rho_k \) is a dense subgroup of \( \text{Gal}(k_{ab}/k) \) and consists of all elements \( \sigma \) in \( \text{Gal}(k_{ab}/k) \) such that \( \sigma | k_{ur} = \varphi_k^m \) for some integer \( m \). In particular, if \( \sigma | k_{ur} = \varphi_k \), then there is a unique prime element \( \pi \) of \( k \) such that \( \rho_k(\pi) = \sigma \).

(iii) \( \rho_k \) induces a topological isomorphism

\[
U \cong \text{Gal}(k_{ab}/k_{ur}),
\]

\[
u \mapsto \delta(u^{-1})
\]
on the subgroup \( U \) of \( k^\times \), where \( \delta : U \cong \text{Gal}(k_{ab}/k_{ur}) \) is the isomorphism in Proposition 5.13. For any prime element \( \pi \) of \( k \), it also induces

\[
U \cong \text{Gal}(k_{ab}/k),
\]

\[
u \mapsto \delta_\pi(u^{-1}),
\]

where \( \delta_\pi \) is the isomorphism in (5.4).

We shall next study how \( \rho_k \) depends upon the ground field \( (k, \nu) \). Let \( k'/k \) be a finite extension of local fields and let

\[
\rho_k : k^\times \to \text{Gal}(k_{ab}/k),
\]

\[
\rho_{k'} : k'^\times \to \text{Gal}(k'_{ab}/k')
\]
be their norm residue maps. Since \( k_{ab}k'/k' \) is an abelian extension, we have

\[
k \subseteq k_{ab} \subseteq k_{ab}k' \subseteq k'_{ab}
\]
so that the map \( \sigma \mapsto \sigma | k_{ab}, \sigma \in \text{Gal}(k'_{ab}/k') \), defines a homomorphism

\[
\text{res} : \text{Gal}(k'_{ab}/k') \to \text{Gal}(k_{ab}/k).
\]

**Theorem 6.9.** Let \( N_{k'/k} : k'^\times \to k^\times \) be the norm map of \( k'/k \). Then the following diagram is commutative:

\[
\begin{array}{ccc}
k'^\times & \longrightarrow & \text{Gal}(k'_{ab}/k') \\
\downarrow{N} & & \downarrow{\text{res}} \\
k^\times & \longrightarrow & \text{Gal}(k_{ab}/k).
\end{array}
\]

In other words,

\[
\rho_{k'}(x') | k_{ab} = \rho_k(N_{k'/k}(x)), \quad \text{for all } x' \in k'^\times.
\]

**Proof.** Let \( k_0 \) be the inertia field of the finite extension \( k'/k \) so that \( k_0/k \) is unramified and \( k'/k_0 \) is totally ramified (cf. Section 2.3). It is clear that if the theorem holds for the extensions \( k_0/k \) and \( k'/k_0 \), then it also holds for
$k'/k$. Hence it is sufficient to prove the theorem in the cases where $k'/k$ is either unramified or totally ramified. In the latter case, the theorem is an immediate consequence of Lemma 6.4 because we now know by Theorem 6.8 that

$$L_k = k_{ab}, \quad L_{k'} = k'_{ab}, \quad E = L_k \cap L_{k'} = k_{ab}.$$  

Hence, suppose that $k'/k$ is unramified and let $k' = k_m^{m'}, m = [k':k]$. As usual, it is enough to show that for any prime element $\pi'$ of $k'$,

$$\rho_{k'}(\pi') \mid k_{ab} = \rho_k(N_{k'/k}(\pi')).$$  

By Proposition 5.4(i), $k_m^{m'}/k_m^{m'}$ is a totally ramified finite abelian extension and $\pi'$ is contained in $N(k_m^{m'}/k_m^{m'})$. Therefore, applying the Corollary of Lemma 6.4 for $k' = k_m^{m'} \subseteq k_m^{m'} \subseteq L_k = k_{ab}$, we see that $\rho_{k'}(\pi') \mid k^{m'}_{m'} = 1$ for all $n \geq 0$. Noting that $k \subseteq k_m^{m'} \subseteq k_{ab}$ by Proposition 5.2(iii), we find

$$\sigma \mid k_m^{m'} = 1, \quad \text{for } \sigma = \rho_k(\pi') \mid k_{ab}.$$  

On the other hand,

$$\sigma \mid k_{ur} = \rho_{k'}(\pi') \mid k_{ur} = \varphi_{k'} = \varphi_k^m$$

by (6.5). Hence, by Lemma 6.1,

$$\rho_{k'}(\pi') \mid k_{ab} = \sigma = \rho_k(N_{k'/k}(\pi')).$$  

**Corollary.** Let $k'/k$ be a finite extension of local fields and let $x \in k^{\infty}$. Then

$$\rho_k(x) \mid (k' \cap k_{ab}) = 1 \iff x \in N(k'/k).$$  

**Proof.** Let $x = N_{k'/k}(x')$, $x' \in k^{\infty}$. Then

$$\rho_k(x) \mid (k' \cap k_{ab}) = \rho_{k'}(x') \mid (k' \cap k_{ab}) = 1$$

because $\rho_{k'}(x') \in \text{Gal}(k_{ab}^{m'}/k')$. Conversely, suppose that $\rho_k(x) \mid (k' \cap k_{ab}) = 1$. Since $\text{Gal}(k_{ab}^{m'}/k') \supseteq \text{Gal}(k_{ab}^{m'} \cap k_{ab})$, $\rho_k(x)$ can be extended to an automorphism in $\text{Gal}(k_{ab}^{m'}/k')$ and, then, to an automorphism $\sigma$ of $\text{Gal}(k_{ab}^{m'}/k')$ such that $\sigma \mid k_{ab} = \rho_k(x)$. Let

$$k_{ur} = k' \cap k_{ur} = (k' \cap k_{ab}) \cap k_{ur}, \quad m \geq 1.$$  

Then $\rho_k(x) \mid k_{ur} = 1$ so that $\rho_k(x) \mid k_{ur}$ is, by (6.4), a power of the Frobenius automorphism $\varphi_k^m$ over $k_{ur}$. Since $\text{Gal}(k_{ur}^{m'}/k') \supseteq \text{Gal}(k_{ur}^{m'}/k_{ur})$, $\sigma \mid k_{ur}^{m'}$ is then a power of the Frobenius automorphism $\varphi_k^m$ over $k'$, and it follows again from Proposition 6.3(ii) that

$$\sigma = \rho_{k'}(x'), \quad \text{for some } x' \in k^{\infty}.$$  

Therefore, by the theorem above,

$$\rho_k(x) = \sigma \mid k_{ab} = \rho_k(N_{k'/k}(x')).$$  

Since $\rho_k$ is injective by Proposition 6.3(i), it follows

$$x = N_{k'/k}(x') \in N(k'/k).$$
In Proposition 6.2, we defined the map $\rho_k$ by means of $\psi_\pi$ in (6.1), which in turn depends on the field $k_\pi$ constructed by the formal group $F_f(X, Y)$ for $f \in \mathcal{F}_\pi$ (cf. Section 5.3). However, we are now able to give a simple description of the norm residue map $\rho_k$ as follows:

**Theorem 6.10.** $\rho_k$ is uniquely characterized as a homomorphism

$$\rho : k^x \to \text{Gal}(k_{ab}/k)$$

with the following two properties:

(i) For each prime element $\pi$ of $k$, $\rho(\pi) | k_{ur} = \varphi_k$, $\varphi_k$ being the Frobenius automorphism of $k$.

(ii) For each finite abelian extension $k'$ over $k$, $\rho(N(k'/k)) | k' = 1$.

**Proof.** By (6.5) and the Corollary of Theorem 6.9, $\rho_k$ has properties (i) and (ii). Let $\rho : k^x \to \text{Gal}(k_{ab}/k)$ be any homomorphism satisfying (i) and (ii), and let $\pi$ be any prime element of $k$. Since $\pi \in N(k'_\pi/k)$ by Proposition 5.4(i) for $m = 1$, it follows from (ii) that $\rho(\pi) | k'_n = 1$ for all $n \geq 0$. Hence $\rho(\pi) | k'_{\pi} = 1$. As $\rho(\pi) | k_{ur} = \varphi_k$, we see from (6.1) that $\rho(\pi) = \psi_\pi = \rho_k(\pi)$. Therefore, $\rho(x) = \rho_k(x)$ for every $x \in k^x$—that is, $\rho = \rho_k$. 

We can see now that $\rho_k$ is naturally associated with the local field $(k, \nu)$ in the following sense. Namely, let

$$\sigma : (k, \nu) \cong (k', \nu')$$

be an isomorphism of local fields—that is, an isomorphism $\sigma : k \cong k'$ such that $\nu = \nu' \circ \sigma$. We can extend $\sigma$ to an isomorphism of fields

$$\sigma : k_{ab} \cong k'_{ab}$$

and define an isomorphism of Galois groups:

$$\sigma^* : \text{Gal}(k_{ab}/k) \cong \text{Gal}(k'_{ab}/k'),$$

$$\sigma \mapsto \sigma \tau \sigma^{-1}.$$  

We then have the following theorem:

**Theorem 6.11.** The following diagram is commutative:

$$\begin{array}{ccc}
k^x & \xrightarrow{\rho_k} & \text{Gal}(k_{ab}/k) \\
\downarrow{\sigma} & & \downarrow{\sigma^*} \\
k^x & \xrightarrow{\rho_k'} & \text{Gal}(k'_{ab}/k').
\end{array}$$

**Proof.** It is clear that $\sigma : k_{ab} \cong k'_{ab}$ and $\sigma^* : \text{Gal}(k_{ab}/k) \cong \text{Gal}(k'_{ab}/k')$ induce

$$\sigma : k_{ur} \cong k'_{ur}, \quad \sigma^* : \text{Gal}(k_{ur}/k) \cong \text{Gal}(k'_{ur}/k')$$

and

$$\sigma^*(\varphi_k) = \sigma \varphi_k \sigma^{-1} = \varphi_k.$$
on $k'_{ur}$. Let
\[
\rho' = \sigma^* \circ \rho_k \circ \sigma^{-1} : k' \to \text{Gal}(k'_{ab}/k'),
\]
and let $\pi'$ be any prime element of $k'$. Since $\nu = \nu' \circ \sigma$, $\pi = \sigma^{-1}(\pi')$ is a prime element of $k$. Hence
\[
\begin{align*}
\rho_k \circ \sigma^{-1}(\pi') &\mid k_{ur} = \rho_k(\pi) \mid k_{ur} = \varphi_k, \\
\rho'(\pi') &\mid k'_{ur} = \sigma^*(\varphi_k) = \varphi_{k'}.
\end{align*}
\]
Let $E'$ be any finite abelian extension over $k'$ and let $E = \sigma^{-1}(E')$. Then $E/k$ is a finite abelian extension over $k$ and
\[
\sigma : N(E/k) \cong N(E'/k'), \quad \sigma^* : \text{Gal}(E/k) \cong \text{Gal}(E'/k').
\]
Hence
\[
\begin{align*}
\rho_k \circ \sigma^{-1}(N(E'/k')) &\mid E = \rho_k(N(E/k)) \mid E = 1, \\
\rho'(N(E'/k')) &\mid E' = \sigma^*(\rho_k(N(E/k))) \mid E' = 1.
\end{align*}
\]
Therefore, by Theorem 6.10, $\rho' = \rho_k'$. \hfill \qed

**COROLLARY.** Let $\sigma$ be an automorphism of a local field $(k, \nu)$. Then
\[
\rho_k(\sigma(x)) = \sigma \rho_k(x) \sigma^{-1}, \quad \text{for all } x \in k^\times,
\]
where $\sigma$ on the right denotes any automorphism of $k'_{ab}$, which extends the given $\sigma : k \cong k$.

**Proof.** Apply the theorem for $k = k'$.

**Remark.** Theorem 6.11 can also be proved directly by going back to the definition of $\rho_k$ in Proposition 6.2.

To explain the next result on $\rho_k$, we need some preparations. Let $\Omega_s$ denote the maximal Galois extension over the local field $(k, \nu)$ and let $k'$ be a finite separable extension over $k$ so that
\[
k \subseteq k' \subseteq \Omega_s \subseteq \Omega, \quad n = [k' : k] < +\infty.
\]
Let
\[
G = \text{Gal}(\Omega_s/k), \quad G' = \text{Gal}(\Omega_s/k'_{ab}),
\]
\[
H = \text{Gal}(\Omega_s/k'), \quad H' = \text{Gal}(\Omega_s/k'_{ab}).
\]
Then $H$ is an open subgroup of the compact group $G$ with index $[G : H] = [k' : k] = n$, and $G'$ and $H'$ are the topological commutator subgroups of $G$ and $H$, respectively. Let $\{\tau_1, \ldots, \tau_n\}$ be a set of representatives for the left cosets $H\tau$, $\tau \in G$:
\[
G = \bigcup_{i=1}^n H\tau_i.
\]
Then, for each $\sigma \in G$ and each index $i$, $1 \leq i \leq n$, there exist a unique element $h_i \in H$ and a unique index $i'$, $1 \leq i' \leq n$, such that
\[
\tau_i \sigma = h_i \tau_{i'}.
\]
Denoting the above \( h_i \) by \( h_i(\sigma) \), we define an element \( t_{G/H}(\sigma) \) in \( H/H' = \text{Gal}(k_{ab}/k') \) by

\[
t_{G/H}(\sigma) = \prod_{i=1}^{n} h_i(\sigma) H', \quad \text{for } \sigma \in G. \tag{6.9}
\]

It is known from group theory that \( t_{G/H}(\sigma) \) depends only upon \( \sigma \in G \), namely, that it is independent of the choice of the representatives \( \tau_1, \ldots, \tau_n \) for the left cosets \( H\tau \), and that \( \sigma \mapsto t_{G/H}(\sigma) \) defines a homomorphism

\[
t_{G/H} : G \to H/H',
\]

which is called the transfer map from \( G \) to \( H \).† In the following, we shall denote \( t_{G/H} \) also by \( t_{k'/k} \) and call it the transfer map from \( k \) to \( k' \). Since \( H/H' \) is an abelian group, the homomorphism \( t_{k'/k} (= t_{G/H}) \) can be factored as

\[
G \to G/G' \to H/H'.
\]

For convenience, the induced map \( G/G' \to H/H' \) will also be denoted by \( t_{k'/k} \). Thus for each finite separable extension \( k'/k \), \( t_{k'/k} \) denotes homomorphisms of Galois groups

\[
\text{Gal}(\Omega_s/k) \to \text{Gal}(k'_{ab}/k'), \quad \text{Gal}(k_{ab}/k) \to \text{Gal}(k'_{ab}/k').
\]

We shall next describe some properties of the transfer maps which follow from the Definition (6.9) by purely group-theoretical arguments:

1. If \( k \subseteq k' \subseteq k'' \), then

\[
t_{k''/k} = t_{k'/k} \circ t_{k'/k}. \]

2. For \( \sigma \in G = \text{Gal}(\Omega_s/k) \), \( n = [k' : k] = [G : H] \),

\[
t_{k'/k}(\sigma) G' = \sigma^n G', \quad \text{that is, } t_{k'/k}(\sigma) \big| k_{ab} = \sigma^n \big| k_{ab}.
\]

3. Let \( k'/k \) be a Galois extension and let \( \sigma \in H = \text{Gal}(\Omega_s/k') \). Then

\[
t_{k'/k}(\sigma) = \prod_{\tau} \tau \sigma \tau^{-1} H' = \left( \prod_{\tau} \tau \sigma \tau^{-1} \right) k_{ab},
\]

where \( \tau \) ranges over a set of representatives for the factor group \( G/H = \text{Gal}(k'/k) \).

4. Let \( k'/k \) be a cyclic extension and let \( \sigma H \) be a generator of \( G/H = \text{Gal}(k'/k) \). Then \( t_{k'/k}(\sigma) = \sigma^n H' \) — that is,

\[
t_{k'/k}(\sigma) = \sigma^n \big| k_{ab}, \quad n = [k' : k] = [G : H].
\]

Now, for a finite separable extension \( k'/k \) of local fields, consider the

† For group-theoretical properties of transfer maps, see, for example, Hall [10].
Local Class Field Theory

where the vertical map on the left is the natural injection of \( k^\times \) into \( k'^\times \). We shall prove below that the above diagram \((k'/k)\) is commutative. We first establish some preliminary results.

**Lemma 6.12.** Suppose that \((k'/k)\) is commutative. Then \( t_{k'/k} : \text{Gal}(k_{ab}/k) \to \text{Gal}(k'_a/k') \) is injective.

**Proof.** Let \( t_{k'/k}(\sigma) = 1 \) for \( \sigma \in \text{Gal}(k_{ab}/k) \). Extend \( \sigma \) to an automorphism of \( \text{Gal}(\Omega_s/k) \) and call it again \( \sigma \). Then, by (2) above,

\[
\sigma^n(= \sigma^n | k_{ab}) = t_{k'/k}(\sigma) | k_{ab} = 1, \quad n = [k':k].
\]

Since \( \text{Gal}(k_{ur}/k) \cong \hat{\mathbb{Z}} \) and \( \hat{\mathbb{Z}} \) is a torsion-free abelian group (cf. Section 3.2), it follows that \( \sigma \in \text{Gal}(k_{ab}/k_{ur}) \). Hence, by (6.4), \( \sigma = \rho_k(u) \) for some \( u \in U \).

As \((k'/k)\) is commutative, we then have

\[
\rho_k(u) = t_{k'/k}(\rho_k(u)) = t_{k'/k}(\sigma) = 1.
\]

Since \( \rho_k \) defines \( U' \cong \text{Gal}(k'_{ab}/k'_u) \), it follows that \( u = 1, \sigma = \rho_k(u) = 1 \). □

**Lemma 6.13.** Let \( k \subseteq k' \subseteq k'' \).

(i) If both \((k''/k')\) and \((k'/k)\) are commutative, then so is \((k''/k)\).

(ii) If both \((k''/k')\) and \((k'/k)\) are commutative, then so is \((k'/k)\).

**Proof.** Consider the diagram

\[
\begin{array}{ccc}
\kappa^\times & \longrightarrow & \text{Gal}(k_{ab}/k) \\
(k'/k) & \downarrow & \text{Gal}(k'_a/k') \\
\kappa'^\times & \longrightarrow & \text{Gal}(k''/k') \\
(k''/k') & \downarrow & \text{Gal}(k''_a/k'') \\
\kappa'' & \longrightarrow & \text{Gal}(k''_a/k'')
\end{array}
\]

By (1) above, the outside rectangle of the above diagram is \((k''/k)\). Hence (i) is obvious. If \((k''/k')\) is commutative, then

\[
t_{k''/k'} : \text{Gal}(k'_{ab}/k') \to \text{Gal}(k''_a/k'')
\]

is injective by Lemma 6.12. Hence (ii) follows.

**Lemma 6.14.** Let \( k'/k \) be a finite Galois extension and let \( x \in N(k'/k) \). Then

\[
\rho_{k'}(x) = t_{k'/k}(\rho_k(x)).
\]
**Proof.** Let \( x = N_{k'/k}(x') \), \( x' \in k'^\times \), namely,

\[
x = \prod_{\tau} \tau(x')
\]

where \( \tau \) ranges over all elements of \( \text{Gal}(k'/k) = G/H \). Extend each \( \tau \) to an automorphism in \( \text{Gal}(\Omega_2,k) = G \) and denote it again by \( \tau \). Then it follows from (3) above that for \( \sigma = \rho_k(x') \in \text{Gal}(k'_{ab}/k') \) and for \( t_{k'/k} : \text{Gal}(k_{ab}/k) \to \text{Gal}(k'_{ab}/k') \),

\[
t_{k'/k}(\sigma |_{k_{ab}}) = \prod_{\tau} \tau \sigma \tau^{-1}
\]
on \( k_{ab}' \). Here

\[
\sigma |_{k_{ab}} = \rho_k(x') |_{k_{ab}} = \rho_k(N_{k'/k}(x')) = \rho_k(x)
\]

by Theorem 6.9. On the other hand, on \( k_{ab}' \),

\[
\rho_k(x) = \prod_{\tau} \rho_k(\tau(x')) = \prod_{\tau} \tau \rho_k(x') \tau^{-1} = \prod_{\tau} \tau \sigma \tau^{-1}
\]
by the Corollary of Theorem 6.11. Hence \( \rho_k(x) = t_{k'/k}(\rho_k(x)) \). \( \blacksquare \)

**Lemma 6.15.** If \( k'/k \) is unramified, then the diagram \((k'/k)\) is commutative.

**Proof.** Since \( k^\times \) is generated by the prime elements of \( k \), it is sufficient to prove

\[
\rho_k(\pi') = t_{k'/k}(\rho_k(\pi))
\]
for any prime element \( \pi \) of \( k \). In this case, \( k_{ab}'/k \) is a Galois extension. Hence, extend \( \psi_\pi = \rho_k(\pi) \) to an automorphism \( \psi \) of \( k_{ab}' \) over \( k \) and let \( F \) denote the fixed field of \( \psi \) in \( k_{ab}' \). Since \( \psi |_{k_{ur}} = \psi_\pi |_{k_{ur}} = \varphi_k \), it follows from Lemma 3.4 that

\[
F_{k_{ur}} = k_{ab}', \quad F \cap k_{ur} = k, \quad \text{Gal}(k_{ab}'/F) \cong \text{Gal}(k_{ur}/k).
\]
Furthermore,

\[
F \cap k_{ab} = k_{\pi}, \quad k \subset k_{\pi} \subset F
\]
because \( F \cap k_{ab} \) is the fixed field of \( \psi_\pi = \psi |_{k_{ab}} \) in \( k_{ab} \). Hence, by Proposition 5.17,

\[
N(F/k) = \langle \pi \rangle.
\]
Let \( k' = k''_{ur} \), \( n = [k':k] \), and let

\[
F' = Fk''_{ur}, \quad \psi' = \psi^n.
\]
Then \( F' \) is the fixed field of \( \psi' \) in \( k_{ab}' \) and

\[
\psi' |_{k_{ur}} = \psi^n |_{k_{ur}} = \varphi_k^n = \varphi_k'.
\]
Therefore, by Proposition 6.3, there exists a prime element \( \pi' \) of \( k' \) such that

\[
\psi' = \rho_k(\pi'), \quad F' = k'_\pi',
\]
and by Proposition 5.17,
\[ N(F'/k') = N(k'_x/k') = \langle \pi' \rangle. \]

Now, let \( E \) be any finite extension of \( k \) in \( F: k \subseteq E \subseteq F, [E:k] < +\infty. \) Since \( F \cap k' = k \), we then have
\[ [Ek':k'] = [E:k], \quad N(E/k) \subseteq N(Ek'/k'). \]

As \( F' (= Fk') \) is the union of all such fields \( Ek' \), it follows that
\[ \langle \pi \rangle = N(F/k) \subseteq N(F'/k') = \langle \pi' \rangle. \]

Hence \( \pi = \pi' \) because both \( \pi \) and \( \pi' \) are prime elements of \( k' \). Now extend \( \psi \) to an automorphism \( \sigma \) of \( \Omega \), over \( k \), so that \( \sigma |_{k_{ab}} = \psi |_{k_{ab}} = \rho_k(\pi). \)

Then it follows from (4) above that
\[ t_{k'/k}(\rho_k(\pi)) = t_{k'/k}(\sigma) = \sigma^n | k'_{ab} = \psi' = \rho_k(\pi') = \rho_k(\pi). \]

We are now ready to prove the following

**Theorem 6.16** Let \( k'/k \) be a finite separable extension of local fields. Then the diagram

\[
\begin{array}{ccc}
k^\times & \xrightarrow{\rho_k} & \text{Gal}(k_{ab}/k) \\
(k'/k) \downarrow & & \downarrow t_{k'/k} \\
k'^\times & \xrightarrow{\rho_k} & \text{Gal}(k'_{ab}/k')
\end{array}
\]

is commutative. In other words,
\[ \rho_{k'}(x) = t_{k'/k}(\rho_k(x)), \quad \text{for all } x \in k^\times. \]

**Proof.** Since \( k'/k \) is separable, \( k' \) can be imbedded in a finite Galois extension \( k'' \) over \( k: k \subseteq k' \subseteq k'' \). By Lemma 6.13(ii), we see that it suffices to prove the theorem in the case where \( k'/k \) is a finite Galois extension. But, by the Corollary of Proposition 2.19, \( \text{Gal}(k'/k) \) is then a solvable group. Hence, by Lemma 6.13(i), we may even assume that \( k'/k \) is an abelian extension. Let
\[ n = [k':k], \quad E = k'_{ur}, \quad E' = Ek', \]
and let \( \pi \) be a prime element of \( k \). Then \( \rho_{k}(\pi) \mid E (= q_{k} \mid k'_{ur}) \) is a generator of \( \text{Gal}(E/k) \) and \( \rho_{E}(\pi) = t_{E/k}(\rho_{k}(\pi)) \) by Lemma 6.15. Since \( k \subseteq k' \subseteq k_{ab} \subseteq E_{ab} \), \([k':k] = n\), it follows from (4) above applied for \( E/k \) that
\[ \rho_{E}(\pi) \mid k' = t_{E/k}(\rho_{k}(\pi)) \mid k' = \rho_{k}(\pi)^n \mid k' = 1. \]

Hence \( \rho_{E}(\pi) \mid E' = 1 \) for the finite abelian extension \( E' \) over \( E \), and it follows from the Corollary of Theorem 6.9 that \( \pi \in N(E'/E) \). Therefore, by Lemma 6.14,
\[ \rho_{E'}(\pi) = t_{E'/E}(\rho_{E}(\pi)) = t_{E'/E}(t_{E/k}(\rho_{k}(\pi))) = t_{E'/k}(\rho_{k}(\pi)). \]
Since \( k^\times \) is generated by prime elements, this shows that the diagram \((E'/k)\) is commutative. Since \((E'/k')\) is commutative by Lemma 6.15, it follows from Lemma 6.13(ii) that \((k'/k)\) is also commutative.

**Corollary.** The transfer map

\[ t_{k'/k}: \text{Gal}(k_{ab}/k) \to \text{Gal}(k'_{ab}/k') \]

is injective.

**Proof.** Since \((k'/k)\) is commutative, this follows from Lemma 6.12.
Chapter VII

Finite Abelian Extensions

In this chapter we shall first prove some important results on finite abelian extensions of local fields that constitute the main theorems of local class field theory in the classical sense. We shall then discuss the ramification groups, in the upper numbering, for such finite abelian extensions.

7.1. Norm Groups of Finite Abelian Extensions

Keeping the notation introduced in the last chapter, let

$$\rho_k : k^\times \to \text{Gal}(k_{ab}/k)$$

denote the norm residue map of a local field \((k, v)\). Let \(k'\) be any finite abelian extension over \(k: k \subseteq k' \subseteq k_{ab}\), \([k':k] < +\infty\). We denote by \(\rho_{k'/k}\) the product of \(\rho_k\) and the canonical restriction homomorphism

$$\text{Gal}(k_{ab}/k) \to \text{Gal}(k'/k) = \text{Gal}(k_{ab}/k)/\text{Gal}(k_{ab}/k').$$

Thus

$$\rho_{k'/k} : k^\times \to \text{Gal}(k'/k).$$

**Theorem 7.1.** Let \(k'/k\) be a finite abelian extension of local fields. Then the above homomorphism \(\rho_{k'/k}\) induces an isomorphism

$$k^\times/N(k'/k) \cong \text{Gal}(k'/k).$$

Furthermore,

$$N(k'/k) = \rho_k^{-1}(\text{Gal}(k_{ab}/k'))$$

and \(\text{Gal}(k_{ab}/k')\) is the closure of \(\rho_k(N(k'/k))\) in \(\text{Gal}(k_{ab}/k)\).

**Proof.** By the Corollary of Theorem 6.9, the kernel of \(\rho_{k'/k}\) is \(N(k'/k)\). By (ii) at the beginning of Section 6.3, the image of \(\rho_k\) is a dense subgroup of \(\text{Gal}(k_{ab}/k)\). Since \(\text{Gal}(k_{ab}/k')\) is an open normal subgroup of \(\text{Gal}(k_{ab}/k)\), \(\rho_{k'/k}\) is surjective. Hence

$$k^\times/N(k'/k) \cong \text{Gal}(k'/k)$$

and

$$N(k'/k) = \rho_k^{-1}(\text{Gal}(k_{ab}/k')).$$

The isomorphism shows that \(\rho_k\) maps each coset of \(k^\times\) mod \(N(k'/k)\) into a coset of \(\text{Gal}(k_{ab}/k)\) mod \(\text{Gal}(k_{ab}/k')\). Since the cosets are closed and since the image of \(\rho_k\) is dense in \(\text{Gal}(k_{ab}/k)\) and \(\rho_k(N(k'/k)) \subseteq \text{Gal}(k_{ab}/k')\), it follows that \(\text{Gal}(k_{ab}/k')\) is precisely the closure of \(\rho(N(k'/k))\) in \(\text{Gal}(k_{ab}/k)\).

**Corollary.** For a finite abelian extension \(k'/k\) of local fields,

$$[k^\times : N(k'/k)] = [k': k].$$

The above equality is called the **fundamental equality** in local class field
theory because in the classical approach, the proof of this equality is one of the first important steps in building up local class field theory. We also note that the norm residue map \( \rho_k \) is so named because it induces an isomorphism of the residue class group of \( k^\times \) modulo the norm group \( N(k''/k) \) onto the Galois group \( \text{Gal}(k''/k) \).

**Proposition 7.2.** (i) Let \( k'/k \) be any finite extension of local fields. Then

\[
N(k'/k) = N((k' \cap k_{ab})/k), \quad [k^\times : N(k'/k)] \leq [k' : k].
\]

Equality holds in the second part if and only if \( k'/k \) is an abelian extension.

(ii) Let \( k'/k \) be a finite extension and \( k''/k \) a finite abelian extension of local fields. Then

\[
N(k'/k) \subseteq N(k''/k) \iff k \subseteq k'' \subseteq k'.
\]

**Proof.** (i) Applying the Corollary of Theorem 6.9 for \( k'/k \) and \( (k' \cap k_{ab})/k \), we obtain

\[
x \in N(k'/k) \iff \rho_k(x) \mid k' \cap k_{ab} = 1 \iff x \in N((k' \cap k_{ab})/k)
\]

for \( x \in k^\times \). Hence \( N(k'/k) = N((k' \cap k_{ab})/k) \). It then follows from the Corollary of Theorem 7.1 for \( (k' \cap k_{ab})/k \) that

\[
[k^\times : N(k'/k)] = [k^\times : N((k' \cap k_{ab})/k)] = [k' \cap k_{ab} : k] \leq [k' : k].
\]

Equality holds if and only if \( k' \cap k_{ab} = k' \)—namely, when \( k'/k \) is abelian.

(ii) Since \( k''/k \) is abelian,

\[
k \subseteq k'' \subseteq k' \iff k \subseteq k'' \subseteq k' \cap k_{ab} \subseteq k_{ab} \iff \text{Gal}(k_{ab}/(k' \cap k_{ab})) \subseteq \text{Gal}(k_{ab}/k'').
\]

By Theorem 7.1, the last inclusion is equivalent to

\[
N(k'/k) = N((k' \cap k_{ab})/k) \subseteq N(k''/k).
\]

Now, let \( k'/k \) be a finite abelian extension of local fields and let

\[
k \subseteq k'' \subseteq k'.
\]

Consider the diagram

\[
\begin{array}{ccc}
k^\times /N(k'/k) & \sim \rightarrow & \text{Gal}(k'/k) \\
\downarrow & & \downarrow \\
k^\times /N(k''/k) & \sim \rightarrow & \text{Gal}(k''/k),
\end{array}
\]

where the horizontal isomorphisms are those in Theorem 7.1, the vertical map on the left is the one defined by the inclusions \( N(k'/k) \subseteq N(k''/k) \subseteq k^\times \) (cf. Proposition 7.2(ii)), and the vertical map on the right is the canonical (restriction) homomorphism.
Proposition 7.3. The above diagram is commutative. Hence the isomorphism $k^\times /N(k'/k) \cong \text{Gal}(k'/k)$ induces

$$N(k''/k) / N(k'/k) \cong \text{Gal}(k'/k').$$

In other words,

$$\rho_{k'/k}(N(k''/k)) = \text{Gal}(k'/k').$$

Proof. The commutativity of the diagram follows from the fact that both horizontal isomorphisms are induced by the same $\rho_k : k^\times \to \text{Gal}(k_{ab}/k)$. Hence the diagram yields an isomorphism between the kernels of the vertical maps—namely, $N(k''/k)/N(k'/k) \cong \text{Gal}(k'/k')$. ■

Lemma 7.4. Let $m \geq 1$, $n \geq 0$ and let $\pi$ be a prime element of a local field $(k, v)$. Let

$$E = k_{ur}^m k_{\pi}^n$$

with the abelian extensions $k_{ur}^m$ and $k_{\pi}^n$ over $k$, defined in Sections 3.2 and 5.2, respectively. Then

$$N(E/k) = \langle \pi^m \rangle \times U_{n+1}.$$

Proof. By Proposition 5.4(i) for $m = 1$, $k_{\pi}^n$ is a totally ramified abelian extension over $k$ and $\pi$ is the norm of a prime element $\pi'$ of $k_{\pi}^n$. $E = k_{ur}^m k_{\pi}^n$ is then an unramified extension of degree $m$ over $k_{\pi}^n$ so that

$$N(E/k_{\pi}^n) = \langle \pi'^m \rangle \times U(k_{\pi}^n),$$

as shown in the proof of Proposition 3.7. However, $NU(k_{\pi}^n/k) = U_{n+1}$ by Proposition 5.16. Hence, taking the norm from $k_{\pi}^n$ to $k$, we obtain from the above that

$$N(E/k) = \langle \pi^m \rangle \times U_{n+1}.$$

We note in passing that the field $E = k_{ur}^m k_{\pi}^n$ above is actually $k_{\pi}^{m \cdot n}$ of Section 5.1 for $\pi$ in $k$. ■

Theorem 7.5. For each closed subgroup $H$ of $k^\times$ with finite index, there exists a unique finite abelian extension $k'/k$ such that

$$H = N(k'/k).$$

Proof. Let $m = [k^\times : H] < +\infty$. Then $\pi^m \in H$ for a prime element $\pi$ of $k$. Since $H \cap U$ is a closed subgroup of $U = U(k)$ with $[U : H \cap U] \leq m < +\infty$, there is an integer $n \geq 0$ such that $U_{n+1} \subseteq H \cap U \subseteq H$. Hence, by Lemma 7.4,

$$N(E/k) = \langle \pi^m \rangle \times U_{n+1} \subseteq H \subseteq k^\times$$

for $E = k_{ur}^m k_{\pi}^n$. Now, by Theorem 7.1, $\rho_{E/k}$ induces

$$k^\times /N(E/k) \cong \text{Gal}(E/k).$$

(7.1)

Therefore, there exists a field $k'$ such that

$$k \subseteq k' \subseteq E, \quad H/N(E/k) \cong \text{Gal}(E/k').$$
under the above isomorphism (7.1). However, by Proposition 7.3, 
\[ N(k'/k)/N(E/k) \cong \text{Gal}(E/k') \]
also under (7.1). Hence \( H = N(k'/k) \). The uniqueness of \( k' \) follows from Proposition 7.2(ii).

Classically, the above result is referred to as the \textit{existence theorem} and \textit{uniqueness theorem} in local class field theory.

Let \( k'/k \) be a finite extension of local fields. By Proposition 3.5 and Proposition 7.2(i), the norm group \( N(k'/k) \) is a closed subgroup of finite index in \( k^\times \). Therefore, we see from Theorem 7.5 that the map \( k' \mapsto H = N(k'/k) \) defines a one-one correspondence between

the family of all finite abelian extensions \( k' \) over \( k \) (in \( \Omega \))
and

the family of all closed subgroups \( H \) with finite indices in \( k^\times \).

Furthermore, by Proposition 7.2(ii), this correspondence reverses inclusion, namely, if \( k_1 \mapsto H_1, \ k_2 \mapsto H_2 \), then
\[ k_1 \subseteq k_2 \Leftrightarrow H_1 \subseteq H_2. \]

Hence
\[ N(k'k''/k) = N(k'/k) \cap N(k''/k), \quad N((k' \cap k'')/k) = N(k'/k)N(k''/k) \]
for any finite abelian extensions \( k'/k \) and \( k''/k \).

\textbf{Remark.} The one-one correspondence mentioned above can be extended to a similar one-one correspondence between the family of all abelian extensions of \( k \) (in \( \Omega \)) and the family of all closed subgroups of \( k^\times \). See Artin [1].

\textbf{Theorem 7.6.} Let \( k'/k \) be a finite extension of local fields. Let \( E \) be any finite abelian extension of \( k \) and let \( E' = Ek' \). Then
\[ N(E'/k') = \{ x' \in k' \mid N_{k'/k}(x') \in N(E/k) \}. \]

\textbf{Proof.} Note first that \( E'/k' \) is a finite abelian extension and that \( k \subseteq E' \subseteq k_{ab}' \). Let \( x' \in k' \), \( x = N_{k'/k}(x') \). Then, by Theorem 6.9,
\[ \rho_k(x') \mid E = \rho_k(x) \mid E. \]

Since \( E' = Ek' \), it follows from Theorem 7.1 that
\[ x' \in N(E'/k') \Leftrightarrow \rho_k(x') \mid E' = 1 \Leftrightarrow \rho_k(x') \mid E = 1 \]
\[ \Leftrightarrow \rho_k(x) \mid E = 1 \Leftrightarrow x \in N(E/k). \]

\section*{7.2. Ramification Groups in the Upper Numbering}

Let \( k'/k \) be a finite Galois extension of local fields and let \( G = \text{Gal}(k'/k) \).
In Section 2.5, we defined a sequence of normal subgroups $G_n$, $n \geq 0$, of $G$:

$$1 \subseteq \cdots \subseteq G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n \subseteq G,$$

called the ramification groups (in the lower numbering) for the extension $k'/k$. Let

$$k \subseteq k'' \subseteq k', \quad H = \text{Gal}(k'/k'') \subseteq G$$

and let $H_n$, $n \geq 0$, be the ramification groups for $k'/k''$. Then it follows immediately from the definition of $G_n$ and $H_n$ that

$$H_n = G_n \cap H, \quad \text{for } n \geq 0.$$

Suppose now that $k''/k$ is a Galois extension so that $H$ is a normal subgroup of $G$ and

$$G/H = \text{Gal}(k''/k).$$

Let $(G/H)_n$, $n \geq 0$, be the ramification groups for the extension $k''/k$. A natural relation one may expect between $G_n$ and $(G/H)_n$ might be that $(G/H)_n$ is the image of $G_n$ under the canonical (restriction) homomorphism $G = \text{Gal}(k'/k) \rightarrow G/H = \text{Gal}(k''/k)$.

However, this is not true in general, and in order to obtain a simple relation between $G_n$ and $(G/H)_n$, we have to change the "numbering" of the ramification groups, as discussed below.

Let $G_n$, $n \geq 0$, be as above. For each real number $r \geq -1$, we define a subgroup $G_r$ of $G$ as follows:

$$G_{-1} = G,$$

$$G_r = G_n, \quad \text{if } n - 1 < r \leq n, \quad n \in \mathbb{Z}, \quad n \geq 0.$$

Let

$$g_r = [G_r : 1], \quad \text{for } r \geq -1.$$

Then $g_r = g_n$ for $n - 1 < r \leq n$, $n \geq 0$, and

$$g_0 = [G_0 : 1] = e(k'/k)$$

by Proposition 2.18. We consider a real-valued function $\phi(r)$ for $r \geq -1$ with the following two properties:

(i) $\phi(r)$ is a continuous, piecewise linear function of $r \geq -1$ with $\phi(0) = 0$,

(ii) The derivative $\phi'(r)$ of $\phi$ at $r \notin \mathbb{Z}$ is equal to $g_r/g_0$.

Drawing the graph of $\phi(r)$, we see easily that there exists a unique such function $\phi(r)$ and that in fact

$$\phi(r) = r, \quad \text{for } -1 \leq r \leq 0,$$

$$= \frac{1}{g_0} (g_1 + \cdots + g_{n-1} + (r - n + 1)g_n), \quad \text{for } n - 1 < r \leq n, \quad n \geq 1, \quad n \in \mathbb{Z}.$$

(7.2)
Since \( g_j \) is a factor of \( g_i \) for integers \( i, j, 0 \leq i \leq j \), it follows from the above that if \( \phi(r) \) is an integer, then so is \( r \).

For each \( \sigma \) in \( G = \text{Gal}(k'/k) \), let

\[
i(\sigma) = \min(v'(\sigma(y) - y) \mid y \in o'),
\]

where \( o' \) is the valuation ring of the normalized valuation \( v' \) of \( k' \). Since \( \sigma(y) - y \in o' \), we always have \( i(\sigma) \geq 0 \), and, in particular, \( \sigma(1) = +\infty \). On the other hand, if \( \sigma \neq 1 \), then \( \sigma(y) \neq y \) for some \( y \in o' \). Hence

\[
0 \leq i(\sigma) < +\infty, \quad \text{for all } \sigma \neq 1 \text{ in } G.
\]

By Lemma 2.13, there exists an element \( w \) in \( o' \) such that \( o' = o[w] \). If \( y \) is an element of \( o' = o[w] \), then \( \sigma(y) - y \) is divisible by \( \sigma(w) - w \) in \( o' = o[w] \). Hence

\[
v'(\sigma(y) - y) \geq v'(\sigma(w) - w), \quad \text{for all } y \in o',
\]

and it follows that

\[
i(\sigma) = v'(\sigma(w) - w), \quad \text{for } \sigma \in G. \tag{7.3}
\]

It is then clear from the definition of \( G_r \) that

\[
G_r = \{ \sigma \in G \mid i(\sigma) \geq r + 1 \}
\]

\[
= \{ \sigma \in G \mid v'(\sigma(w) - w) \geq r + 1 \}, \quad r \geq -1.
\]

Consider now a function \( \lambda(r), r \geq -1 \), defined by

\[
\lambda(r) = -1 + \frac{1}{g_0} \sum_{\sigma \in G} \min(i(\sigma), r + 1).
\]

Clearly \( \lambda(r) \) is continuous and piecewise linear because each \( \min(i(\sigma), r + 1) \) is such a function. Furthermore \( \lambda(0) = -1 + (g_0/g_0) = 0 \), and for \( r \) in the open interval \( i - 1 < r < i \), \( i \in \mathbb{Z}, i \geq 0 \), \( \lambda(r) \) is given by

\[
\lambda(r) = a + \frac{b}{g_0} (r + 1),
\]

where \( a \) and \( b \) are constants and \( b \) is the number of \( \sigma \)'s in \( G \) such that \( i(\sigma) \geq r + 1 \)—namely, \( b = |G_r : 1| = g_r \). Hence \( \lambda'(r) = g_r/g_0 \), and it follows from the definition of \( \phi(r) \) that \( \phi(r) = \lambda(r) \)—that is,

\[
\phi(r) = -1 + \frac{1}{g_0} \sum_{\sigma \in G} \min(i(\sigma), r + 1), \quad \text{for } r \geq -1. \tag{7.4}
\]

Since \( \phi(r) \) is, by (7.2), a strictly increasing function of \( r \geq -1 \), let \( \psi(r) \) denote the inverse function of \( \phi(r) \):

\[
\phi(\psi(r)) = \psi(\phi(r)) = r, \quad \text{for } r \geq -1.
\]

We then define subgroups \( G' \) of \( G \) by

\[
G' = G_{\psi(r)}, \quad G^{\phi(s)} = G_s, \quad \text{for real } r, s \geq -1.
\]
For example,
\[ G^{-1} = G_{-1} = G, \quad G^r = G_r = G_0, \quad \text{for } -1 < r \leq 0. \]

These subgroups \( G^r, r \geq -1 \), are called the \textit{ramification groups}, \textit{in the upper numbering}, for the finite Galois extension \( k'/k \).

Now, as mentioned above, let \( k'' \) be a Galois extension of \( k \), contained in \( k' \), and let
\[
H = \text{Gal}(k'/k''), \quad G/H = \text{Gal}(k''/k).
\]

Then we have the following theorem:

\textbf{Theorem 7.7.} Let \( G^r \) and \( (G/H)^r \), \( r \geq -1 \), be the ramification groups in the upper numbering for \( k'/k \) and \( k''/k \), respectively. Then \( (G/H)^r \) is the image of \( G^r \) under the canonical homomorphism \( G \to G/H \):
\[
(G/H)^r = G^r H/H, \quad \text{for } r \geq -1.
\]

We shall next prove this theorem in several steps.

(i) For each \( \sigma' \in G/H \),
\[
i_{G/H}(\sigma') = \frac{1}{e'} \sum_{\sigma} i_G(\sigma),
\]
where \( i_{G/H} \) denotes the \( i \)-function for \( k''/k \), \( e' = e(k'/k'') \), and the sum on the right is taken over all elements \( \sigma \in G \) such that \( \sigma \mapsto \sigma' \) under \( G \to G/H \)—that is, \( \sigma' = \sigma H \).

\textbf{Proof.} If \( \sigma' = 1 \), then both sides are \( +\infty \). Hence assume \( \sigma' \neq 1 \). Let \( \mathfrak{o}'' \) be the valuation ring of the normalized valuation \( \nu'' \) on \( k'' \). By Lemma 2.13, there exist elements \( w \) and \( z \) such that
\[
\mathfrak{o}' = \mathfrak{o}[w], \quad \mathfrak{o}'' = \mathfrak{o}[z].
\]

Since \( \nu' \mid k'' = e' \nu'' \), it follows from (7.3) that
\[
i_G(\sigma) = \nu'(\sigma(w) - w), \quad i_{G/H}(\sigma') = \nu''(\sigma'(z) - z) = \frac{1}{e'} \nu'(\sigma(z) - z).
\]

Fix an element \( \sigma \in G \) such that \( \sigma' = \sigma H \). Since
\[
\frac{1}{e'} \sum_{\tau \in H} i_G(\sigma \tau) = \frac{1}{e'} \sum_{\tau \in H} \nu'(\sigma \tau(w) - w) = \frac{1}{e'} \nu'\left( \prod_{\tau \in H} (\sigma \tau(w) - w) \right),
\]
the equality to be proved is equivalent to the following:
\[
\nu'(\sigma(z) - z) = \nu'\left( \prod_{\tau \in H} (\sigma \tau(w) - w) \right).
\]

Let \( s = [H:1] = [k':k''] \) and let \( g(X) \) denote the minimal polynomial of \( w \) over \( k'' \). Since \( k' = k''(w) \) and \( \nu'(\tau(w)) = \nu'(w) \geq 0 \), we see that
\[
g(X) = \prod_{\tau \in H} (X - \tau(w)) = X^s + a_1 X^{s-1} + \cdots + a_s, \quad a_i \in \mathfrak{o}'', \quad 1 \leq i \leq s.
\]
Let
\[ g^\sigma(X) = X^s + \sigma(a_1)X^{s-1} + \cdots + \sigma(a_s), \quad \sigma(a_i) \in \mathfrak{o}'' \]
\[ = \prod_{\tau \in H} (X - \sigma\tau(w)). \]
Then
\[ g^\sigma(w) - g(w) = \prod_{\tau \in H} (w - \sigma\tau(w)). \]
However, the coefficients \( \sigma(a_i) - a_i \) of \( g^\sigma(X) - g(X) \) are divisible by \( \sigma(z) - z \) in \( \mathfrak{o}'' = \mathfrak{o}[z] \). Hence we obtain
\[ \nu'(\prod_{\tau \in H} (w - \sigma\tau(w))) \geq \nu'(\sigma(z) - z). \]
On the other hand, it follows from \( z \in \mathfrak{o}'' \subseteq \mathfrak{o}' = \mathfrak{o}[w] \) that there is a polynomial \( h(X) \) in \( \mathfrak{o}[X] \) such that
\[ z = h(w). \]
As \( h(X) - z \) is a polynomial of \( \mathfrak{o}'[X] \) that vanishes for \( X = w \), it follows that
\[ h(X) - z = g(X)g_1(X), \quad \text{with } g_1(X) \in \mathfrak{o}'[X]. \]
Applying \( \sigma \) to the coefficients of both sides and using \( h(X) \in \mathfrak{o}[X] \subseteq k[X] \), we obtain
\[ h(X) - \sigma(z) = g^\sigma(X)g_1^\sigma(X), \]
where \( g_1^\sigma(X) \) is a polynomial of \( \mathfrak{o}'[X] \), defined similarly as \( g^\sigma(X) \). Put \( X = w \) in the above. Then
\[ z - \sigma(z) = g^\sigma(w)g_1^\sigma(w) = \prod_{\tau \in H} (w - \sigma\tau(w))g_1^\sigma(w), \]
where \( g_1^\sigma(w) \in \mathfrak{o}' \). Hence
\[ \nu'(z - \sigma(z)) \geq \nu'(\prod_{\tau \in H} (w - \sigma\tau(w))). \]
This completes the proof of (i).

(ii) For \( \sigma' \in G/H \), let
\[ j(\sigma') = \max(i_G(\sigma) \mid \sigma \in G, \sigma H = \sigma'). \]
Then
\[ i_{G/H}(\sigma') - 1 = \phi_{k'/k''}(j(\sigma') - 1), \]
where \( \phi_{k'/k''} \) denotes the \( \phi \)-function for the extension \( k'/k'' \).

**Proof.** We may again assume \( \sigma' \neq 1 \). Fix an element \( \sigma \in G \) such that \( \sigma H = \sigma' \), \( j(\sigma') = i_G(\sigma) \). Let \( n = j(\sigma') \geq 0 \). By (7.4) for \( k'/k'' \),
\[ \phi_{k'/k''}(j(\sigma') - 1) = \phi_{k'/k''}(n - 1) = -1 + \frac{1}{e'} \sum_{\tau \in H} \min(i_H(\tau), n). \]
Suppose \( i_H(\tau) \geq n \) so that \( \min(i_H(\tau), n) = n \). Then \( \tau \in H_{n-1} = H \cap G_{n-1} \). Since \( i_G(\sigma) = n \), so that \( \sigma \in G_{n-1} \), it follows that \( \sigma \tau \in G_{n-1} \), \( i_G(\sigma \tau) \geq n \). By the choice of \( \sigma \), we then obtain \( i_G(\sigma \tau) = n = \min(i_H(\tau), n) \). Next, suppose \( i_H(\tau) < n \). Then \( \tau \notin H_{n-1} = H \cap G_{n-1} \). Since \( \sigma \in G_{n-1} \), it follows that \( i_G(\sigma \tau) = i_H(\tau) = \min(i_H(\tau), n) \) also in this case. Therefore, by (i),

\[
\phi_{k'/k'}(j(\sigma') - 1) = -1 + \frac{1}{e'} \sum_{\tau \in H} i_G(\sigma \tau) = -1 + i_{G/H}(\sigma').
\]

(iii) (Herbrand's Theorem). Let \( s = \phi_{k'/k'}(r) \), \( r \geq -1 \). Then

\[
G_r H/H = (G/H)_s.
\]

**Proof.** \( \sigma' \in G_r H/H \Leftrightarrow i_G(\sigma) \geq r + 1 \) for some \( \sigma \in G \) such that \( \sigma' = \sigma H \)

\[
\Leftrightarrow j(\sigma') \geq r + 1
\]

\[
\Leftrightarrow \phi_{k'/k'}(j(\sigma') - 1) \geq \phi_{k'/k'}(r), \text{ because } \phi_{k'/k'} \text{ is an increasing function}
\]

\[
\Leftrightarrow i_{G/H}(\sigma') - 1 \geq s, \text{ by (ii)}
\]

\[
\Leftrightarrow \sigma' \in (G/H)_s.
\]

(iv) \( \phi_{k'/k} = \phi_{k''/k} \circ \phi_{k'/k''} \), \( \psi_{k'/k} = \psi_{k''/k} \circ \psi_{k'/k} \).

**Proof.** Since \( \psi \) is the inverse function of \( \phi \), it is sufficient to prove the first equality. Let \( \lambda = \phi_{k'/k'} \circ \phi_{k'/k''} \). It is clear that \( \lambda \) is continuous, piecewise linear, and \( \lambda(0) = 0 \). Let \( r \geq -1, r \notin \mathbb{Z} \). Then \( \phi_{k'/k'}(r) \notin \mathbb{Z} \) by the remark after (7.2), and the derivatives satisfy

\[
\lambda'(r) = \phi_{k''/k}(s) \phi_{k'/k'}(r), \quad \text{with } s = \phi_{k'/k''}(r),
\]

where

\[
\phi_{k''/k}(s) = \frac{1}{e''} [(G/H)_s : 1], \quad \phi_{k'/k''}(r) = \frac{1}{e'} [H_r : 1]
\]

with \( e' = e(k'/k'') \), \( e'' = e(k''/k) \). However, by (iii) above,

\[
(G/H)_s = G_r H/H \cong G_r/(G_r \cap H) = G_r H_r.
\]

Since \( e'e'' = e = e(k'/k) \), it follows that

\[
\lambda'(r) = \frac{1}{e} [G_r : 1] = \phi_{k'/k'}(r).
\]

Therefore, by the uniqueness of the function \( \phi(r) \), \( \phi_{k'/k'}(r) = \lambda(r) \) for \( r \geq -1 \).}

We are now ready to complete the proof of Theorem 7.7. Let \( s = \psi_{k'/k'}(r) \), \( r \geq -1 \), so that \( G' = G_s \). By (iii) above,

\[
G'H/H = G_r H/H = (G/H)_t, \quad \text{with } t = \phi_{k'/k'}(s).
\]

By (iv),

\[
\phi_{k'/k'}(t) = \phi_{k''/k}(\phi_{k'/k''}(s)) = \phi_{k''/k}(s) = \phi_{k'/k'}(\psi_{k'/k'}(r)) = r.
\]
Hence
\[ G'H/H = (G/H)_t = (G/H)' .\]

**Corollary of Theorem 7.7.** Let both \( k_1/k \) and \( k_2/k \) be finite Galois extensions of local fields (in \( \Omega \)) and let \( k' = k_1k_2 \). Then
\[ \text{Gal}(k_1/k)' = 1, \quad \text{Gal}(k_2/k)' = 1 \iff \text{Gal}(k'/k)' = 1. \]

**Proof.** By the theorem, the left hand side yields
\[ \text{Gal}(k'/k)' \subseteq \text{Gal}(k_1'/k_1)' \quad \text{and} \quad \text{Gal}(k'/k)' \subseteq \text{Gal}(k_2'/k_2)' .\]
However, since \( k' = k_1k_2 \), the intersection of \( \text{Gal}(k_1'/k_1)' \) and \( \text{Gal}(k_2'/k_2)' \) is 1. Hence \( \text{Gal}(k'/k)' = 1 \). The converse is clear.

**Lemma 7.8.** Let \( k'/k \) be a finite Galois extension of local fields. Let \( \mathfrak{p}' \) denote the maximal ideal of \( k' \) and let
\[ \mathfrak{D}(k'/k) = \mathfrak{p}'^a, \quad a \geq 0, \]
for the different \( \mathfrak{D}(k'/k) \) of the extension \( k'/k \). Then
\[ a = \sum_{\sigma \neq 1} i(\sigma) = \sum_{n=0}^{\infty} (g_n - 1), \quad \sigma \in G = \text{Gal}(k'/k), \]
where \( g_n = [G_n : 1], \ n = 0, 1, 2, \ldots \).

**Proof.** By Proposition 2.14,
\[ \mathfrak{D}(k'/k) = f'(w)\mathfrak{o}', \]
where \( w \) is an element of \( \mathfrak{o}' \) as in Lemma 2.13 and \( f'(X) \) is the derivative of the minimal polynomial \( f(X) \) of \( w \) over \( k \). Since
\[ f(X) = \prod_{\sigma} (X - \sigma(w)), \quad \sigma \in G, \]
it follows from (7.3) that
\[ a = v'(f'(w)) = \sum_{\sigma \neq 1} v'(w - \sigma(w)) = \sum_{\sigma \neq 1} i(\sigma). \]
Let \( g'_n = g_n - 1 \). Since \( i(\sigma) = n \) if and only if \( \sigma \in G_{n-1}, \ \sigma \notin G_n \), we see that
\[ \sum_{\sigma \neq 1} i(\sigma) = \sum_{n=0}^{\infty} n(g'_n - g'_n) = (g'_0 - g'_1) + 2(g'_1 - g'_2) + \cdots = g'_0 + g'_1 + g'_2 + \cdots . \]

7.3. **The Special Case** \( k_{\pi}^{m,n}/k \)

Let \( m \geq 1, \ n \geq 0 \) and let \( \pi \) be a prime element of \( k_{ur}^m \). Let
\[ G = \text{Gal}(k_{\pi}^{m,n}/k) \]
for the finite abelian extension \( k_{\pi}^{m,n} \) over \( k \), defined in Section 5.1. We shall next determine the ramification groups \( G_r \) and \( G' \), \( r \geq 1 \), for the extension
Let \( H = \text{Gal}(k_{\pi,n}^m/k_{ur}^m) \).

By Proposition 5.2, \( k_{ur} \cap k_{\pi,n}^m = k_{ur}^m \)—namely, \( k_{ur}^m \) is the inertia field of the extension \( k_{\pi,n}^m/k \). Hence \( G_0 = H \) so that
\[
G_i = H_i, \quad \text{for all integers } i \geq 0.
\]

Therefore, we also have
\[
G_r = H_r, \quad G' = H', \quad \text{for all real } r \geq 0.
\]

Since
\[
G_{r-1} = G^{-1} = G, \quad G_r = G' = H, \quad \text{for } -1 < r \leq 0,
\]
we see that it is sufficient to determine \( H_r \) and \( H' \) for the totally ramified extension \( k_{\pi,n}^m/k_{ur}^m \).

**Lemma 7.9.** Let \( \delta_n^\pi : U \to H \) be the surjective homomorphism in Proposition 5.3(ii) and let \( \sigma = \delta_n^\pi(u) \in H \) with \( u \in U = U(k) \). If \( u \in U_i, \; u \not\in U_{i+1}, \; 0 \leq i \leq n \), then
\[
i_H(\sigma) = q^i,
\]
where \( i_H \) is the function on \( H \) defined in Section 7.2 and \( q \) is the number of elements in the residue field \( t = \mathfrak{o}/\mathfrak{p} \) of \( k \).

**Proof.** Let \( f = F_n^m \) and let \( \alpha \in W_f^i, \; \alpha \not\in W_f^{i-1} \). By Proposition 5.4(ii), \( \alpha \) is a prime element of \( k_{\pi,n}^m \) and \( \mathfrak{o}_{\pi,n}^m = \mathfrak{o}^m[\alpha] \). Hence, by (3.3),
\[
i_H(\sigma) = v'(\sigma(\alpha) - \alpha),
\]
where \( v' \) denotes the normalized valuation of the local field \( k_{\pi,n}^m \). Let \( u \in U, \; u \not\in U_1 \)—that is, \( u \equiv 1 \text{ mod } \mathfrak{p} \). Since \( v'(\alpha) = 1, \; v'(u - 1) = 0 \), we then have
\[
\sigma(\alpha) = [u]_f(\alpha) = u\alpha \mod \alpha^2, \quad v'(\sigma(\alpha) - \alpha) = 1.
\]

Therefore, the lemma is proved for \( i = 0 \). Let now \( u \in U_i, \; u \not\in U_{i+1} \) for \( 1 \leq i \leq n \). Write \( u \) in the form \( u = 1 + v \) with \( v \in \mathfrak{p}_f^i, \; v \not\in \mathfrak{p}_f^{i+1} \). Then
\[
\sigma(\alpha) = [u]_f(\alpha) = u_j \alpha = \alpha + v \alpha \; \alpha = \alpha + \beta,
\]
where \( \beta = v \; \alpha \in \mathfrak{p}_f \; \alpha = W_f^{-n-i}, \; \beta \not\in \mathfrak{p}_f^{i+1} \; \alpha = W_f^{-n-i-1} \) by Lemma 4.8. Therefore, by Proposition 5.4(ii), \( \beta \) is a prime element of \( k_{\pi,n}^m \). Since \( k_{\pi,n}^m/k_{ur}^m \) and, hence, \( k_{\pi,n}^m/k_{\pi,n}^m \) are totally ramified, we see from Proposition 5.2(iii) that
\[
v'(\beta) = [k_{\pi,n}^m : k_{\pi,n}^{m-i}] = q^i.
\]

On the other hand, it follows from (4.1) that
\[
\alpha + \beta = F_f(\alpha, \beta) = \alpha + \beta \mod \alpha \beta.
\]
Therefore,
\[ i_H(\sigma) = v'(\sigma(\alpha) - \alpha) = v'((\alpha + j \beta) - \alpha) = v'(\beta) = q^i. \]

We now consider \( H_r \) and \( H' \) for real numbers \( r \geq 0 \). Let \( j \) be an integer such that \( q^a \leq j < q^{a+1} \) for \( a \in \mathbb{Z}, 0 \leq a \leq n \). Then, for \( \sigma = \delta^n_u(\nu) \) in Lemma 7.9,
\[ \sigma \in H_j \Leftrightarrow i_H(\sigma) \geq j + 1 \Leftrightarrow q^i \geq j + 1 \Leftrightarrow i = a + 1 \Leftrightarrow \nu \in U_{a+1}. \]

Hence, by the Corollary of Proposition 5.3,
\[ H_j = \delta^n(U_{a+1}) = \text{Gal}(k_{\pi}^{m,n}/k_{\pi}^{m,a}). \]

Let \([H_j:1] = h_j\). Noting that \( k_{\pi}^{m,n}/k_{\pi}^{m,a} \) is totally ramified, we obtain from the above the following table for \( H_j \) and \( h_j \):

- \( H_{-1} = H_0 = \text{Gal}(k_{\pi}^{m,n}/k_{\pi}^{m,a}), \quad h_0 = (q - 1)q^n, \)
- \( H_1 = \cdots = H_{q^a-1} = \text{Gal}(k_{\pi}^{m,n}/k_{\pi}^{m,0}), \quad h_j = q^n, \)
- \( \cdots \)
- \( H_{q^a} = \cdots = H_{q^a+1} = \text{Gal}(k_{\pi}^{m,n}/k_{\pi}^{m,a}), \quad h_j = q^{n-a}, \)
- \( \cdots \)
- \( H_{q^n-1} = \cdots = H_{q^n} = \text{Gal}(k_{\pi}^{m,n}/k_{\pi}^{m,n-1}), \quad h_j = q, \)
- \( H_{q^n} = H_{q^n+1} = \cdots = 1, \quad h_j = 1. \)

Now, by the definition of \( H_r \) for real \( r \geq -1 \), the map \( r \mapsto H_r \) is continuous on the left—that is, \( H_r = H_{r-\epsilon} \) for small \( \epsilon > 0 \). The above table shows that \( r \mapsto H_r \) is discontinuous on the right exactly at \( r = 0, q - 1, \ldots, q^n - 1 \). Since \( H_r = H^{\phi(r)} \) with a continuous function \( \phi(r) \), we see that the map \( r \mapsto H' \) is continuous on the left and the discontinuity on the right occurs exactly at
\[ r = \phi(0), \phi(q - 1), \ldots, \phi(q^n - 1). \]

However, by (7.2),
\[ \phi(i) = \frac{1}{h_0} (h_1 + \cdots + h_i) \]
for integers \( i \geq 0 \). Hence it follows from the above table that
\[ \phi(q^a - 1) = \frac{1}{h_0} (a(q - 1)q^n) = a, \quad \text{for } 0 \leq a \leq n. \]

By the remark on the relation between \( G_r, G' \) and \( H_r, H' \) mentioned earlier, we now obtain the following result:

**Proposition 7.10.** For the finite abelian extension \( k_{\pi}^{m,n}/k \), the ramification
groups in the upper numbering, \( G' \) are given as follows:

\[
G' = \begin{cases} 
\text{Gal}(k^{m,n}_\pi/k), & \text{for } r = -1. \\
\text{Gal}(k^{m,n}_\pi/k_{ur}^m), & \text{for } -1 < r \leq 0. \\
\text{Gal}(k^{m,n}_\pi/k_{m,i}^\mu), & \text{for } i - 1 < r \leq i, i \in \mathbb{Z}, 1 \leq i \leq n. \\
1 & \text{for } r > n.
\end{cases}
\]

Hence

\[
1 = G^{n+1} \subset G^n \subset \cdots \subset G^1 \subset G^0 \subset G^{-1} = G.
\]

\[
[G : G^0] = m, \quad [G^0 : G^1] = q - 1, \quad [G^i : G^{i+1}] = q, \quad \text{for } 1 \leq i \leq n.
\]

**Proposition 7.11.** Let \( o' \) denote the valuation ring of \( k^{m,n}_\pi \), and \( p_0 \) the maximal ideal of \( k^{m,0}_\pi \). Then

\[
\mathcal{D}(k^{m,n}_\pi/k) = \mathcal{D}(k^{m,n}_\pi/k_{ur}^m) = p^{n+1}p_0^{-1}o',
\]

\( p \) being, as usual, the maximal ideal of \( k \).

**Proof.** Since \( k^{m,n}_\pi/k \) is unramified, the first equality follows from Propositions 2.16, 2.17. Let \( p' \) be the maximal ideal of \( k^{m,n}_\pi \) and let

\[
\mathcal{D}(k^{m,n}_\pi/k_{ur}^m) = p'^a, \quad a \geq 0.
\]

Using the values of \( h_i = [H_i : 1] \) in the table obtained above, we see from Lemma 7.8 that

\[
a = \sum_{i=0}^{\infty} (h_i - 1)
= (q - 1)q^n - 1 + (q - 1)(q^n - 1) + (q - 1)q(q^{n-1} - 1) + \cdots
+ (q - 1)q^{n-1}(q - 1)
= (n + 1)(q - 1)q^n - q^n.
\]

Since \( k^{m,n}_\pi/k_{ur}^m \) is totally ramified and \([k^{m,n}_\pi : k_{ur}^m] = (q - 1)q^n\), \([k^{m,n}_\pi : k^{m,0}_\pi] = q^n\), \( p_0' \), and \( p_0o' \) are the \((q - 1)q^n\)th and \(q^n\)th powers of \( p' \), respectively. Therefore,

\[
\mathcal{D}(k^{m,n}_\pi/k_{ur}^m) = p'^a = p^{n+1}p_0^{-1}o'.
\]

---

### 7.4. Some Applications

Let \( k'/k \) be a finite abelian extension of local fields and let

\[
\rho_{k'/k} : k^\times \to G = \text{Gal}(k'/k)
\]

be the homomorphism defined in Section 7.1.

**Theorem 7.12.** Let \( G' \), \( r \geq -1 \), denote the ramification groups in the upper numbering for \( k'/k \). Then

\[
G' = \rho_{k'/k}(U_i), \quad \text{for } i - 1 < r \leq i, i \in \mathbb{Z}, i \geq 0.
\]
Proof. Fix a prime element \( \pi \) of \( k \) so that
\[
k \subseteq k' \subseteq k_{ab} = k_{ur} k_{\pi}
\]
by Theorem 6.8. Let \( f \in \mathcal{F}_k \). Then, by the definitions in Sections 5.1 and 5.2,
\[
k^n_{\pi} = k^1_{\pi} = k(W^n_f), \quad k^n_{ur}(W^n_f) = k_{ur} k^n_{\pi}, \quad L^n = k_{ur}(W^n_f) = k_{ur} k^n_{\pi}.
\]
As \( k_{ur} \) is the union of \( k^m_{ur} \) for all \( m \geq 1 \) and \( k_{\pi} \) is the union of \( k^n_{\pi} \) for all \( n \geq 0 \), it follows that \( k_{ur} k_{\pi} \) is the union of the fields \( k^n_{\pi} = k^m_{ur} k^n_{\pi} \) for all \( m \geq 1 \), \( n \geq 0 \).

Hence
\[
k \subseteq k' \subseteq E = k^n_{\pi} = k^n_{ur} k^n_{\pi}
\]
for sufficiently large \( m \geq 1 \) and \( n \geq 0 \). By definition, \( \rho_{k'/k} \) is then the product of \( \rho_{E/k} : k^n \rightarrow \text{Gal}(E/k) \) and the canonical (restriction) homomorphism \( \text{Gal}(E/k) \rightarrow \text{Gal}(k'/k) \). However, by Theorem 7.7, \( G' = \text{Gal}(k'/k) \) is the image of \( \text{Gal}(E/k) \), \( r \geq -1 \), under the same homomorphism \( \text{Gal}(E/k) \rightarrow \text{Gal}(k'/k) \). Therefore, it is sufficient to prove the equalities of the theorem for the extension \( E/k \) instead of \( k'/k \). Now, by Lemma 7.4 and Proposition 7.10,
\[
N(k_{\pi}^{m,i-1}/k) = N(k_{ur} k_{\pi}^{i-1}/k) = \langle \pi^m \rangle \times U_i,
\]
\[
\text{Gal}(E/k)^r = \text{Gal}(E/k_{\pi}^{m,i-1}), \quad \text{for } i - 1 < r \leq i, \ i \geq 0,
\]
with \( k_{\pi}^{m,-1} = k_{\pi}^{-1} = k \). On the other hand, by Proposition 7.3,
\[
\rho_{E/k}(N(k_{\pi}^{m,i-1}/k)) = \text{Gal}(E/k_{\pi}^{m,i-1}).
\]
Since \( \langle \pi^m \rangle \) is contained in the kernel \( N(E/k) = \langle \pi^m \rangle \times U_{n+1} \) of \( \rho_{E/k} : E^n \rightarrow \text{Gal}(E/k) \), we obtain
\[
\rho_{E/k}(U_i) = \rho_{E/k}(\langle \pi^m \rangle \times U_i) = \text{Gal}(E/k_{\pi}^{m,i-1}) = \text{Gal}(E/k)^r.
\]

Let \( k'/k \) now be any finite Galois extension of local fields and let \( G = \text{Gal}(k'/k) \). The definition of the subgroups \( G_r, \ r \geq -1, \) of \( G \) in Section 7.2 states that \( G_r = G_i \) if \( i \) is the integer satisfying \( i - 1 < r \leq i, \ i \geq 0 \). Hence it is natural to ask whether similar equalities:
\[
G^r = G^i, \quad \text{for } i - 1 < r \leq i, \ i \geq 0, \ i \in \mathbb{Z}
\]
hold also for the ramification groups \( G^r \) in the upper numbering. This is not true in general.† However, for an abelian extension \( k'/k \), we have the following theorem of Hasse-Arf, which is an immediate consequence of the above Theorem 7.12:

**Theorem 7.13.** Let \( k'/k \) be a finite abelian extension of local fields and let \( r \) be a real number \( \geq -1 \). Then
\[
G^r = G^i, \quad \text{for } i - 1 < r \leq i, \ i \in \mathbb{Z}, \ i \geq 0.
\]

Let \( k'/k \) still be a finite abelian extension. It is clear from Theorem 7.12

† See Serre [21], p. 84.
that
\[ U_n \subseteq N(k'/k) \Leftrightarrow \rho_{k'/k}(U_n) = 1 \Leftrightarrow \text{Gal}(k'/k)^n = 1, \quad n \geq 0. \]
Since any of these equivalent statements holds whenever the integer \( n \) is sufficiently large, let \( c(k'/k) \) denote the minimal integer \( n \geq 0 \) for which the above conditions are satisfied, and define
\[ \hat{t}(k'/k) = \wp^{c(k'/k)}, \]
\( \wp \) being, as usual, the maximal ideal of \( k \). The ideal \( \hat{t}(k'/k) \) of \( k \) is called the conductor of the abelian extension \( k'/k \). It follows immediately from the definition that
\[ \hat{t}(k'/k) = \wp \Leftrightarrow c(k'/k) = 0 \Leftrightarrow \text{Gal}(k'/k)^0 = 1 \Leftrightarrow k'/k \text{ is unramified,} \]
namely, by Proposition 2.16,
\[ \hat{t}(k'/k) = \wp \Leftrightarrow D(k'/k) = \wp' \Leftrightarrow D(k'/k) = \wp, \]
\( \wp \) and \( \wp' \) being the valuation rings of \( k \) and \( k' \), respectively. If \( k'/k \) is ramified, then \( \hat{t}(k'/k) \subseteq \wp \) and it is the largest ideal of \( \wp \) such that
\[ \rho_{k'/k}(1 + \hat{t}(k'/k)) = 1. \]
We shall next discuss the relation between \( \hat{t}(k'/k) \) and \( D(k'/k) \) for finite abelian extensions \( k'/k \).

Let \( G_n \) again denote the ramification groups, in the lower numbering, for the abelian extension \( k'/k \). Let \( g_n = [G_n : 1] \) and let \( \phi \) be the increasing function associated with \( k'/k \) (cf. Section 7.2). Let
\[ k \subseteq k'' \subseteq k', \quad H = \text{Gal}(k'/k''), \quad G/H = \text{Gal}(k''/k). \]

**Lemma 7.14.** Suppose \( G_n \nsubseteq H \), \( G_{n+1} \subseteq H \) for an integer \( n \geq -1 \). Then
\[ c(k''/k) = 1 + \phi(n) \]
\[ = \frac{1}{g_0} (g_0 + g_1 + \cdots + g_n), \]
where the last sum is meant to be zero if \( n = -1 \).

**Proof.** By Theorem 7.7,
\[ G_r H/H = G^{\phi(r)} H/H = (G/H)^{\phi(r)}. \]
Since \( G_r = G_{n+1} \) for \( n < r \leq n + 1 \) and since \( \phi \) is continuous, it follows from the assumption that
\[ (G/H)^{\phi(n)} \neq 1, \quad (G/H)^{\phi(n) + \varepsilon} = 1, \quad \text{for small } \varepsilon > 0. \]
Hence, by Theorem 7.13, \( \phi(n) \) is an integer, and
\[ (G/H)^{\phi(n)} \neq 1, \quad (G/H)^{\phi(n) + 1} = 1. \]
Therefore, by (7.2) and by the definition of \( c(k''/k) \),
\[ c(k''/k) = 1 + \phi(n) = \frac{1}{g_0} (g_0 + g_1 + \cdots + g_n). \]
COROLLARY. Let $G_n \neq 1$, $G_{n+1} = 1$ for an integer $n \geq -1$. Then

$$c(k'/k) = 1 + \phi(n) = \frac{1}{g_0} (g_0 + g_1 + \cdots + g_n).$$

REMARK. $\phi(n) = c(k'/k) - 1$ motivated the definition of the function $\phi(r)$.

Now, for each character $\chi$ of the finite abelian group $G = \text{Gal}(k'/k)$, let

- $H_\chi$ be the kernel of the homomorphism $\chi : G \to \mathbb{C}^\times$,
- $k_\chi$ be the fixed field of $H_\chi$ in $k'$,
- $\tilde{\ell}(\chi) = \ell(k_\chi/k)$, the conductor of $k_\chi/k$.

**Theorem 7.15.** Let $D(k'/k)$ be the discriminant of the finite abelian extension $k'/k$. Then

$$D(k'/k) = \prod_\chi \tilde{\ell}(\chi),$$

where the product is taken over all characters $\chi$ of $\text{Gal}(k'/k)$.

**Proof.** Let $\mathcal{D}(k'/k)$ be the different of $k'/k$ and let $\mathcal{D}(k'/k) = p^a$, $a \geq 0$. Then, by Sections 1.3 and 2.4,

$$D(k'/k) = N_{k'/k}(\mathcal{D}(k'/k)) = p^a,$$

where $f = f(k'/k) = g/g_0$ with $g = [G:1] = [k':k]$, $g_0 = [G_0:1] = e(k'/k)$. By Lemma 7.8,

$$a = \sum_{i=1}^{\infty} (g_i - 1), \text{ for } g_i = [G_i:1], i \geq 0.$$

Hence the equality of the theorem is equivalent to

$$\frac{g}{g_0} \sum_{i=0}^{\infty} (g_i - 1) = \sum_\chi c(k_\chi/k),$$

where $c(k_\chi/k)$ is defined as above. Now, fix a character $\chi$, and for each $i \geq 0$, let

$$\chi(G_i) = \frac{1}{g_0} \sum_{\sigma} \chi(\sigma), \text{ with } \sigma \in G_i.$$

Then

$$\chi(G_i) = 1, \text{ if } \chi \mid G_i = 1, \text{ that is, } G_i \subseteq H_\chi,$$

$$= 0, \text{ if } \chi \mid G_i \neq 1, \text{ that is, } G_i \nsubseteq H_\chi.$$

Let $\chi \neq 1$ so that $H_\chi \neq G$ and $G_n \nsubseteq H_\chi$, $G_{n+1} \subseteq H_\chi$ for some $n \geq -1$. By Lemma 7.14, we then see

$$c(k_\chi/k) = \frac{1}{g_0} \sum_{i=0}^{\infty} g_i (1 - \chi(G_i)).$$
If \( \chi = 1 \), \( H_x = G \), then \( k_x = k \), \( c(k_x/k) = 0 \), while \( \chi(G_i) = 1 \) for all \( i \geq 0 \). Hence the above equality holds also in this case. When \( i \) is fixed and \( \chi \) ranges over all characters of \( G \),

\[
\sum_{\chi} \chi(G_i) = \text{the number of characters } \chi \text{ of } G \text{ such that } G_i \subseteq H_x = \text{the number of characters of } G/G_i
\]

\[
= g/g_i.
\]

Therefore,

\[
\sum_{\chi} c(k_x/k) = \frac{1}{g_0} \sum_{i=0}^{\infty} g_i \left( g - \frac{g}{g_i} \right) = \frac{g}{g_0} \sum_{i=0}^{\infty} (g_i - 1).
\]

This theorem is called the \textit{conductor-discriminant theorem} for finite abelian extensions of local fields.

\textbf{Example.} Let \( k'/k \) be a cyclic extension of degree \( l \), a prime number. Then

\[
\chi = 1 \Rightarrow H_x = G, \quad k_x = k, \quad \hat{\mathfrak{f}}(\chi) = \hat{\mathfrak{f}}(k/k) = 0,
\]

\[
\chi \neq 1 \Rightarrow H_x = 1, \quad k_x = k', \quad \hat{\mathfrak{f}}(\chi) = \hat{\mathfrak{f}}(k'/k).
\]

Hence

\[
D(k'/k) = \hat{\mathfrak{f}}(k'/k)^{-1}.
\]

Theorem 7.15 is a generalization of the above equality, originally obtained by Takagi.

In the above discussions, we deduced Theorem 7.12 and, hence, Theorem 7.13 from Theorems 6.8 and 7.7 and Proposition 7.10 on the ramification groups of \( k_{m,n}^\prime/k \). We shall next show that, conversely, Theorem 6.8 is a consequence of Theorems 7.7 and 7.13 and Proposition 7.10.

\textbf{Lemma 7.16.} Let \( k'/k \) be a totally ramified, finite, Galois extension of local fields and let \( q \) be the number of elements in the residue field of \( k : \mathfrak{f} = \mathbb{F}_q \). Suppose that (7.5) holds for the ramification groups \( G' \) of \( k'/k \) for all real \( r \geq -1 \). Then

\[
[G^0 : G^1] | (q - 1), \quad [G^n : G^{n+1}] | q, \quad \text{for } n \geq 1
\]

so that

\[
[G : G^{n+1}] | (q - 1)q^n, \quad \text{for every } n \geq 0.
\]

\textbf{Proof.} Since \( k'/k \) is totally ramified, \( G = G_0 = G^0 \) and the number of elements, \( q' \), in the residue field of \( k' \) is equal to \( q \). Let \( n \) be any integer \( \geq 0 \) and let \( n = \phi(m) \), \( n + 1 = \phi(m') \) for the increasing function \( \phi \) associated with \( k'/k \). By the remark after (7.2), \( m \) and \( m' \) are integers. Since \( \phi(m) < \phi(m') \), we have \( m < m' \)—that is, \( 0 \leq m < m + 1 \leq m' \). Let \( r = \phi(m + 1) \). Then \( n < r \leq n + 1 \) so that \( G' = G^{n+1} \) by (7.5). Since \( G^\phi(s) = G_s \),
s \geq -1$, it follows that

$$G^n = G_m, \quad G^{n+1} = G' = G_{m+1}, \quad [G^n : G^{n+1}] = [G_m : G_{m+1}].$$

If $n = 0$, then $m = 0$, and $[G^0 : G^1] = [G_0 : G_1]$. If $n \geq 1$, then $m > 0$—that is, $m \geq 1$. Since $q = q'$, $G = G^0$, the lemma now follows from the remark at the end of Section 2.5.

Now, assume Theorems 7.7 and 7.13 and Proposition 7.10. As shown in part (i) of the proof of Theorem 6.8, there exists a field $F$ and a prime element $\pi$ of $k$ such that

$$F k_{ur} = k_{ab}, \quad F \cap k_{ur} = k, \quad k \subseteq k_{\pi} \subseteq F \subseteq k_{ab}.$$ 

Let $k'$ be any finite extension over $k$ in $F$: $k \subseteq k' \subseteq F$, $[k' : k] < +\infty$. Then $\text{Gal}(k'/k)^{n+1} = 1$ for some $n \geq 0$. Let

$$k'' = k' k^n_{\pi}.$$ 

Since $\text{Gal}(k''/k)^{n+1} = 1$ by Proposition 7.10 for $m = 1$, it follows from the Corollary of Theorem 7.7 that

$$\text{Gal}(k''/k)^{n+1} = 1.$$ 

As $k \subseteq k'' \subseteq F$, $k''/k$ is a totally ramified, finite, abelian extension. Hence, by Theorem 7.13 and Lemma 7.16, we obtain

$$[k'' : 1] = [\text{Gal}(k''/k) : 1] | (q - 1)q^n.$$ 

However, we know by Proposition 5.2 for $m = 1$ that $[k^n_{\pi} : k] = (q - 1)q^n$. As $k \subseteq k^n_{\pi} \subseteq k''$, it follows that

$$k'' = k^n_{\pi}, \quad k \subseteq k' \subseteq k^n_{\pi} \subseteq k_{\pi}.$$ 

Thus every finite extension over $k$ in $F$ is contained in $k_{\pi}$. Hence

$$F = k_{\pi}, \quad k_{ab} = k_{ur} k_{\pi} = L_k.$$ 

The above is the idea of the proof of Theorem 6.8 in Gold [9] and Lubin [18]. One sees that if Theorem 7.7 and various properties of the abelian extensions $k^n_{\pi}/k$ are taken for granted, then Theorem 6.8—that is, $k_{ab} = L_k$—and Theorem 7.13 (Hasse-Arf Theorem) are essentially equivalent.

† For another proof of Theorem 6.8 for a local field of characteristic 0, see Rosen [20].
Chapter VIII

Explicit Formulas

In this chapter, we shall prove formulas of Wiles [25] that generalize the classical explicit formulas of Artin-Hasse [2] for the norm residue symbols of local cyclotomic fields over $\mathbb{Q}_p$.

8.1. $\pi$-Sequences

Let $(k, v)$ be a local field with residue field $k = \mathcal{O}/\mathfrak{p}$ and let $\pi$ be a prime element of $(k, v)$. In the following, we consider a pair $(f, \omega)$ where $f$ is a power series in the family $\mathcal{F}_\pi$ of Section 5.1 and where

$$\omega = \{\omega_n\}_{n \geq 0}$$

is a sequence of elements in the abelian group $W_f = \bigcup_n W^n_f$ of Section 4.3, satisfying, for $f = (\pi)_f$,

$$\omega_0 \in W^n_f, \quad \omega_0 \neq 0, \quad \omega_n = f(\omega_{n+1}) = \pi \cdot \omega_{n+1}, \quad \text{for all } n \geq 0.$$

Such a pair will be called a $\pi$-sequence for $k$. Given $f \in \mathcal{F}_\pi$, there always exists a $\pi$-sequence $(f, \omega)$ for $k$ because $\pi \cdot W^n_f = W^n_f$ by Lemma 4.8(iii).

It also follows from the same lemma that $\omega_n$ has the properties

$$\omega_n \in W^n_f, \quad \omega_n \notin W^n_{f^{-1}}, \quad W^n_f = \omega \cdot \omega_n,$$

so that $\omega_n$ is a prime element of $k^n_{\pi} = k(\mathfrak{p}^n_f)$ by Proposition 5.4(ii).

Let $(f', \omega')$ be another $\pi$-sequence for $k$ and let $\omega' = \{\omega'_n\}_{n \geq 0}$. Suppose $h(X)$ is a power series in $\mathfrak{O}[[X]]$, invertible in $M = X\mathfrak{O}[[X]]$ (cf. Section 3.4), such that

$$h \circ f \circ h^{-1} = f', \quad h(\omega_n) = \omega'_n, \quad \text{for all } n \geq 0.$$

We shall call such an $h$ an isomorphism from $(f, \omega)$ to $(f', \omega')$ and write

$$h : (f, \omega) \simeq (f', \omega').$$

It then follows that $h$ defines isomorphisms over $\mathfrak{o}$:

$$F_f \simeq F_{f'}, \quad W^n_f \simeq W^n_{f'}, \quad W_f \simeq W_{f'}.$$

Lemma 8.1. Let $(f, \omega)$ be a $\pi$-sequence for $k$ with $\omega = \{\omega_n\}_{n \geq 0}$. Let $g(X)$ be a power series in $\mathfrak{O}[[X]]$ such that $g(\omega_i) = 0$ for $0 \leq i \leq n$. Then $g(X)$ is divisible by $[\pi^{n+1}]$ in $\mathfrak{O}[[X]]$. If $g(\omega_i) = 0$ for all $i \geq 0$, then $g(X) = 0$.

Proof. By the Corollary of Proposition 5.4, the elements $\beta \in W^n_f$, $\beta \notin W^n_{f^{-1}}$, are the conjugates of $\alpha_i$ over $k (= k_{ur})$. Since $g(X) \in \mathfrak{O}[[X]]$, $g(\omega_i) = 0$ implies $g(\beta) = 0$ for all $\beta \in W^n_f$, $\beta \notin W^n_{f^{-1}}$. As this holds for $0 \leq i \leq n$, we see that $g(\alpha) = 0$ for all $\alpha \in W^n_f$. By the remark after Lemma 5.5, $g(X)$ is then divisible by $[\pi^{n+1}]_f$ in $\mathfrak{O}[[X]]$. Now, since $[\pi]_f = f$ for
Explicit Formulas

117

\[ f \in \mathcal{F}_n, [\pi]_f \text{ is contained in the maximal ideal } (\pi, X) \text{ of } \mathcal{o}[X], \text{ generated by } \pi \text{ and } X. \]

Hence \([\pi^{n+1}]_f = [\pi]_f \cdot \cdots [\pi]_f \] belongs to the \((n + 1)\)th power \((\pi, X)^{n+1}\) of \((\pi, X)\) in \(\mathcal{o}[X]\). Therefore, if \(g(\omega_i) = 0\) for all \(i \geq 0\), then \(g(X) \in (\pi, X)^{n+1}\) for all \(n \geq 0\) so that \(g(X) = 0\).

**Proposition 8.2.** Let \((f, \omega)\) and \((f', \omega')\) be \(\pi\)-sequences for \(k\). Then there exists a unique isomorphism

\[ h : (f, \omega) \rightarrow (f', \omega'). \]

Furthermore, if \(\omega = \omega'\), then \(h(X) = X\) so that \(f = f'\).

**Proof.** Since \(f, f' \in \mathcal{F}_n\), it follows from the proof of Lemma 5.1(i) that there is a power series \(\theta(X)\) in \(\mathcal{o}[X]\) such that \(\theta(X) = X \mod \deg 2\), \(\theta \circ f = f' \circ \theta\) (cf. (4.8)). Let \(\omega'' = \{\omega''_n\}\), where \(\omega''_n = \theta(\omega_n), n \geq 0\). Then \(\theta : (f, \omega) \cong (f', \omega'')\). Hence, to prove the existence of \(h : (f, \omega) \cong (f', \omega')\), we may assume that \(f = f'\). In this case, since \(\omega_n, \omega'_n \in W^f, \omega_n, \omega'_n \notin W^{n+1}\), it follows from Lemma 4.8(ii) (iii) that there exists \(u_n \in U = U(k)\) such that \(u_n \cdot \omega_n = \omega'_n\) and such \(u_n\) is uniquely determined in \(U \mod U_{n+1} = (1 + p^{n+1})\). Let \(m \geq n \geq 0\). Then

\[ u_m \cdot \omega_n = u_m \cdot \pi^{m-n} \cdot \omega_m = \pi^{m-n} \cdot \omega'_m = u'_n, \]

whereas \(u_n \cdot \omega_n = \omega'_n\). Hence it follows from the above remark that \(u_m \equiv u_n \mod U_{n+1}\) for \(0 \leq n \leq m\). Consequently, there exists \(u \in U\) such that \(u \equiv u_n \mod U_{n+1}\) for all \(n \geq 0\), and such an element \(u\) satisfies \(u \cdot \omega_n = \omega'_n\) for all \(n \geq 0\). Let \(h = [u]_f\) so that \(h(\omega_n) = \omega'_n, n \geq 0\). Since \(h \circ f \circ h^{-1} = f\) because \(f = f'\), we obtain \(h : (f, \omega) \cong (f', \omega')\). To prove the uniqueness of \(h : (f, \omega) \cong (f', \omega')\), it is sufficient to show that \(\omega = \omega'\) implies \(h(X) = X\). Let \(g(X) = h(X) - X\). Then \(\omega_i = \omega'_i = h(\omega_i)\) implies \(g(\omega_i) = 0\) for all \(i \geq 0\). Hence \(g(X) = 0\) by Lemma 8.1.

For \(0 \leq n \leq m\), let \(N_{m,n}\) denote the norm map of the extension \(k^n/k\). A \(\pi\)-sequence \((f, \omega)\) for \(k\) will be called *normed* if it satisfies

\[ N_{m,n}(\omega_m) = \omega_n, \quad \text{for all } 0 \leq n \leq m. \]

We shall next see that this property of \((f, \omega)\) actually depends only on \(f\).

**Lemma 8.3.** A \(\pi\)-sequence \((f, \omega)\) is normed if and only if

\[ [\pi]_f(X) = \prod \gamma (X + \gamma), \quad \gamma \in W^f, \]

namely,

\[ N_f(X) = X \]

for the norm operator \(N_f\) in Section 5.2.

**Proof.** Assume the above equality. Let \(n \geq 0\). By the Corollary of Proposition 5.4, \(\omega_{n+1} \cdot W^f\) is the complete set of conjugates of \(\omega_{n+1}\) over \(k^n\). Hence

\[ N_{n+1,n}(\omega_{n+1}) = \prod \gamma (\omega_{n+1} + \gamma) = [\pi]_f(\omega_{n+1}) = \pi \cdot \omega_{n+1} = \omega_n, \quad \gamma \in W^f. \]
Therefore \((f, \omega)\) is normed. Conversely, suppose that \((f, \omega)\) is normed and let
\[
g(X) = \lfloor \pi \rfloor f(X) - \prod_{\gamma} (X + \gamma), \quad \gamma \in \mathbb{W}.
\]
Then
\[
g(\omega_0) = \pi; \omega_0 - \prod_{\gamma} (\omega_0 + \gamma) = 0
\]
because \(\omega_0 + \mathbb{W} = \mathbb{W}\) and \(\mathbb{W}\) contains \(0\). For \(n \geq 0\),
\[
g(\omega_{n+1}) = \pi; \omega_{n+1} - \prod_{\gamma} (\omega_{n+1} + \gamma) = \omega_n - N_{n+1,m}(\omega_{n+1}) = 0, \quad \gamma \in \mathbb{W}.
\]
Hence \(g(X) = 0\) by Lemma 8.1.

For convenience, a power series \(f\) in \(\mathbb{F}'\) will be called \textit{normed} if it satisfies \(N_f(X) = X\). Thus Lemma 8.3 simply states that a \(\pi\)-sequence \((f, \omega)\) is normed if and only if \(f\) is normed.

**Example.** Let \((k, \nu)\) be a \(p\)-field. Let \(p > 2\), \(f(X) = \pi X + X^q \in \mathbb{F}'\), and let \((f, \omega)\) be a \(\pi\)-sequence for \(k\). Then \(f(\omega_{n+1}) = \lfloor \pi \rfloor f(\omega_{n+1}) = \omega_n\). Since \(k_{n+1}^\pi = k(\omega_{n+1}) = k_{n+1}^\omega(\omega_{n+1}), \ [k_{n+1}^\pi : k_n^\pi] = q = \deg(f)\) by Propositions 5.2 and 5.4(ii), we see that \(f(X) - \omega_n\) is the minimal polynomial of \(\omega_{n+1}\) over \(k_n^\pi\) so that \(N_{n+1,n}(-\omega_{n+1}) = -\omega_n\). Since \(q\) is a power of \(p\) and is odd, it follows that \(N_{n+1,n}(\omega_{n+1}) = \omega_n\) for \(n \geq 0\). Hence \((f, \omega)\) is a normed \(\pi\)-sequence for \(k\). In the case \(p = 2\), we can see similarly that \((f, \omega)\) is normed for \(f(X) = \pi X - X^q \in \mathbb{F}'\).

For \(n \geq 0\), let
\[
B_n = (k_n^\pi)^\times = \text{the multiplicative group of the field } k_n^\pi,
\]
and let
\[
B = \lim \leftarrow B_n,
\]
where the inverse limit is taken with respect to the norm maps
\[
N_{m,n}: (k_m^\pi)^\times \to (k_n^\pi)^\times, \quad \text{for } 0 \leq n \leq m.
\]
\(B\) is a multiplicative abelian group and an element \(\beta\) in \(B\) is a sequence:
\[
\beta = (\beta_0, \beta_1, \ldots, \beta_n, \ldots), \quad \beta_n \in B_n = (k_n^\pi)^\times,
\]
such that \(N_{m,n}(\beta_m) = \beta_n\) for \(0 \leq n \leq m\). Let \(N_n\) denote the norm map of \(k_n^\pi/k\). Then \(N_n(\beta_n)\) is an element of \(k\), independent of \(n \geq 0\). Hence we define an integer \(\nu(\beta)\) by
\[
\nu(\beta) = \nu(N_n(\beta_n)), \quad \text{for any } n \geq 0,
\]
\(\nu\) being the valuation of the ground field \(k\). For example, if \((f, \omega)\) is a normed \(\pi\)-sequence for \(k\) with \(\omega = (\omega_0, \omega_1, \ldots)\), then \(\omega\) belongs to \(B\) and \(\nu(\omega) = 1\) because each \(\omega_n\) is a prime element of \(k_n^\pi\). Clearly
\[
\nu(\beta \beta') = \nu(\beta) + \nu(\beta'), \quad \text{for } \beta, \beta' \in B,
\]
and the group \(B\) is generated by the \(\beta\)'s with \(\nu(\beta) = 1\).
Theorem 8.4.† (i) Let (f, ω) be a π-sequence for k and let β ∈ B with
ν(β) = 0. Then there exists a unique power series t(X) in o[[X]]π such that
t(ωn) = βn, for all n ≥ 0.

(ii) If (f, ω) is normed, then for any β ∈ B with arbitrary e = ν(β), there
again exists a unique power series t(X) in Xe o[[X]] such that
t(ωn) = βn, for all n ≥ 0.

Proof. (i) Since ν(β) = ν(Nn(βn)) = 0, βn is a unit of kπ. Hence it
follows from Proposition 5.11 that for each n ≥ 0, there exists t(X) ∈ o[[X]]
such that
tn(ωi) = βi, for 0 ≤ i ≤ n.

It then follows that
tn+1(ωi) − tn(ωi) = βi − βi = 0, for 0 ≤ i ≤ n,
so that by Lemma 8.1,
tn+1 = tn mod [πn+1]f.

Since [πn+1]f ∈ (π, X)n+1, we see that the limit

t = limn→∞ tn

exists in o[[X]] in the compact topology on o[[X]] defined in Section 3.4. As
t clearly satisfies t = tn mod [πn+1]f, it follows from πn+1; ωn = 0 that
t(ωn) = tn(ωn) = βn, for n ≥ 0.

Since t(X) belongs to o[[X]] in the compact topology on o[[X]] defined in Section 3.4. As
t clearly satisfies t = tn mod [πn+1]f, it follows from πn+1; ωn = 0 that

(ii) Since (f, ω) is normed, ω = (ω0, ω1, . . . ) is an element of B with
ν(ω) = 1. Let β ∈ B, ν(β) = e, and let

β' = ω−εβ = (β0', β1', . . . ), βn' = ω−εβn, n ≥ 0.

Then β' ∈ B, ν(β') = 0. Hence, by (i), there is a power series t'(X) in
o[[X]]π such that t'(ωn) = βn' for all n ≥ 0. It then follows that t = Xe't' is a
power series in Xe'o[[X]] with the property t(ωn) = βn for all n ≥ 0. The
uniqueness of t follows from that of t'.

Now, fix a normed π-sequence (f, ω). By the above proposition, for each
β ∈ B, ν(β) = e, there exists a unique power series tβ(X) in Xe'o[[X]]π such that
tβ(ωn) = βn, for all n ≥ 0.

For example, tω(X) = X for ω = (ω0, ω1, . . . ) ∈ B. By the uniqueness, we have
tββ' = tβtβ', for β, β' ∈ B.

Suppose ν(β) = 1 for β ∈ B. Then tβ ∈ Xe'o[[X]]π so that tβ is invertible in M

† Compare Coleman [5].
and
\[ f_\beta = t_\beta \circ f \circ t_\beta^{-1} \in \mathcal{F}^1. \]

Since \( t_\beta(\omega_n) = \beta_n \) for \( n \geq 0 \), we see that the pair \((f_\beta, \beta)\) is a normed \( \pi \)-sequence for \( k \) and
\[ t_\beta : (f, \omega) \sim (f_\beta, \beta). \]

By Proposition 8.2, \( f_\beta \) is the unique power series in \( \mathfrak{o}[[X]] \) such that \((f_\beta, \beta)\) is a \( \pi \)-sequence for \( k \). Hence \( f_\beta \) depends only on \( \beta \in B \) (with \( \nu(\beta) = 1 \)) and it is independent of \((f, \omega)\). Furthermore, if \((f', \omega')\) is any normed \( \pi \)-sequence for \( k \), then \( \omega' \in B, \nu(\omega') = 1 \). Hence \((f_\omega, \omega)\) is a normed \( \pi \)-sequence for \( k \) so that \( f' = f_\omega \) by Proposition 8.2. Thus we see that the family of pairs:
\[ \{ (f_\beta, \beta) \}, \quad \text{for all } \beta \in B \text{ with } \nu(\beta) = 1, \]
is nothing but the set of all normed \( \pi \)-sequences for \( k \).

8.2. The Pairing \((\alpha, \beta)_f\)

Let \( \pi \) be a prime element of \((k, \nu)\) and let \( f \in \mathcal{F}^1 \). As before, we denote the residue field of \( k^\nu_n, n \geq 0 \), by \( \mathfrak{o}_n/\mathfrak{p}_n \).

**Lemma 8.5.** Let \( n \geq 0 \). (i) For each \( \alpha \in \mathfrak{p}_n \), there exists an element \( \xi \in \mathfrak{m}_f (= \mathfrak{p}_\Omega) \) such that \( \pi^{n+1} \cdot \xi = \alpha \). Let \( k' = k^\nu_\pi(\xi) \). Then \( k'/k^\nu_\pi \) is an abelian extension with \([k' : k^\nu_\pi] \leq q^{n+1} \), and \( k' \) depends only on \( \alpha \) and it is independent of the choice of \( \xi \) such that \( \pi^{n+1} \cdot \xi = \alpha \).

(ii) In particular, if \( \alpha \) is a prime element of \( k^\nu_\pi \), then \( k'/k^\nu_\pi \) is a totally ramified extension of degree \( q^{n+1} \). \( \xi \) is a prime element of \( k' \), \( \xi + W^\nu_f \) is the complete set of conjugates of \( \xi \) over \( k^\nu_\pi \), and \( \text{Gal}(k'/k^\nu_\pi) \simeq W^\nu_f \).

**Proof.** (i) An argument similar to that in the proof of Lemma 5.1(i) shows that it is sufficient to prove the results for the special case: \( f(X) = \pi X + X^q \). In this case, \([\pi^{n+1}]_f = f \circ f \circ \cdots \circ f \) is a polynomial of degree \( q^{n+1} \) in \( \mathfrak{o}[X] \) and the equation \([\pi^{n+1}]_f[X] - \alpha = 0 \) has a solution \( \xi \) in \( \mathfrak{p}_\Omega \) (cf. the proof of Lemma 4.6). Thus \( \pi^{n+1} \cdot \xi = \alpha \), and \( \xi + W^\nu_f \) is then the set of all roots of \([\pi^{n+1}]_f - \alpha = 0 \) in \( \Omega \). As \( \alpha \) and \( W^\nu_f \) are contained in \( k^\nu_\pi \), \( k'/k^\nu_\pi \) is a finite Galois extension, depending only on \( \alpha \). Let \( \sigma \in \text{Gal}(k'/k^\nu_\pi) \). Since \( \pi^{n+1} \cdot \xi = \alpha \) implies \( \pi^{n+1} \cdot \sigma(\xi) = \alpha \), it follows from the above that
\[ \sigma(\xi) \sim \xi \in W^\nu_f \subseteq k^\nu_\pi. \]
Hence, for \( \sigma, \tau \in \text{Gal}(k'/k^\nu_\pi) \),
\[ (\sigma \tau)(\xi) \sim \xi \]
so that the map \( \sigma \mapsto \sigma(\xi) \sim \xi \) defines a homomorphism: \( \text{Gal}(k'/k^\nu_\pi) \rightarrow W^\nu_f \).

As \( k' = k^\nu_\pi(\xi) \), the homomorphism is injective. Therefore, \( \text{Gal}(k'/k^\nu_\pi) \) is an abelian group with order \( \leq q^{n+1} = [W^\nu_f : 0] \).

(ii) \([\pi^{n+1}]_f = X^{q^{n+1}} \pmod{\mathfrak{p}} \) and \( \mathfrak{p} \subseteq \mathfrak{p}_n = \alpha \mathfrak{o}_n \) imply
\[ \alpha = \pi^{n+1} \cdot \xi \equiv \xi^{q^{n+1}} \pmod{\xi \mathfrak{p}}, \]
hence, \( \text{mod } \xi \alpha \).
Therefore, $\mu(\alpha) = q^{n+1} \mu(\xi)$ for the valuation $\mu$ on $\Omega$ in Section 3.1. As $\alpha$ is a prime element of $k_n^\infty$, it follows that

$$e(k'/k_n^\infty) \geq q^{n+1} = [W_f^\gamma : 0] \geq [k':k_n^\infty] \geq e(k'/k_n^\infty)$$

so that

$$[k':k_n^\infty] = [W_f^\gamma : 0] = q^{n+1} = e(k'/k_n^\infty),$$

and all statements in (ii) follow.

For $n \geq 0$, let $\rho_n$ denote the norm residue map $\rho_E$ for $E = k_n^\infty$:

$$\rho_n : B_n = (k_n^\infty)^\times \to \text{Gal}(k_{n,ab}^\infty/k_n^\infty).$$

Fix $f \in \mathfrak{P}_n^1$ and let

$$\alpha \in \mathfrak{m}_n, \quad \beta \in B_n.$$

Let $\pi_{n+1} \xi = \alpha$, $k' = k_n^\infty(\xi)$ as stated above. Since $k'/k_n^\infty$ is abelian—that is, $k_n^\infty \subseteq k' \subseteq k_{n,ab}^\infty$, $\rho_n(\beta) \mid k'$ is an element of $\text{Gal}(k'/k_n^\infty)$. Let

$$(\alpha, \beta)_{n,f} = \rho_n(\beta)(\xi) \overset{f}{\to} \xi.$$

Then $(\alpha, \beta)_{n,f}$ is an element of $W_f^n$ and it is independent of the choice of $\xi$ such that $\pi_{n+1} \xi = \alpha$, because if $\pi_{n+1} \xi' = \alpha$, $\xi' \in \xi \overset{f}{\to} W_f^n$, $W_f^n \subseteq k_n^\infty$, so that

$$\rho_n(\beta)(\xi') \overset{f}{\to} \xi' = \rho_n(\beta)(\xi) \overset{f}{\to} \xi.$$

We shall next study the properties of the symbol $(\alpha, \beta)_{n,f}$. When $f$ is fixed, the suffix $f$ in $(\alpha, \beta)_{n,f}$, $\alpha \overset{f}{\to} \beta$, and so on will often be omitted.

**Lemma 8.6.** (i) $(\alpha_1 \cdot \alpha_2, \beta)_n = (\alpha_1, \beta)_n \cdot (\alpha_2, \beta)_n$,

$$(\alpha, \beta_1 \beta_2)_n = (\alpha, \beta_1)_n \cdot (\alpha, \beta_2)_n,$$

$$(\alpha \cdot \alpha, \beta)_n = \alpha \cdot (\alpha, \beta)_n, \quad \text{for } a \in 0.$$

(ii) $(\alpha, \beta)_n = 0 \iff \beta \in N(k_n^\infty(\xi)/k_n^\infty)$, $\pi_{n+1} \xi = \alpha$.

(iii) Let $f$ be normed and let $\alpha$ be a prime element of $k_n^\infty$. Then

$$(\alpha, \alpha)_{n,f} = 0.$$

**Proof.** (i) If $\xi_1$, $\xi_2$ are elements of $m_f$ such that $\pi_{n+1} \xi_1 = \alpha_1$, $\pi_{n+1} \xi_2 = \alpha_2$, then $\pi_{n+1} \cdot (\xi_1 + \xi_2) = \alpha_1 + \alpha_2$. Hence the first equality follows. The third equality can be proved similarly. Since $\rho_n(\beta') = \rho_n(\beta) \rho_n(\beta')$, the second equality follows from the fact that $\sigma \mapsto \sigma(\xi) \overset{f}{\to} \xi$ defines a homomorphism: $\text{Gal}(k_n^\infty(\xi)/k_n^\infty) \to W_f^n$.

(ii) It follows from Theorem 7.1 that

$$\rho_n(\beta)(\xi) = \xi \iff \rho_n(\beta) \mid k_n^\infty(\xi) = 1 \iff \beta \in N(k_n^\infty(\xi)/k_n^\infty).$$

(iii) Let $\pi_{n+1} \xi = \alpha$. Since $f$ is normed, $N_f(X) = X$. Hence $N_f^\gamma(X) = N_f(N_f(\cdots))(X) = X$ so that by Lemma 5.9(i),

$$[\pi_{n+1}]_f = \prod_\gamma (X + \gamma), \quad \gamma \in W_f^n.$$
Therefore,
\[\alpha = \pi^{n+1} \xi = \prod_{\gamma} (\xi \hat{+} \gamma), \quad \gamma \in W_f^{\eta}.\]

However, by Lemma 8.5(ii), \(\xi \hat{+} W_f^{\eta}\) is the complete set of conjugates of \(\xi\) over \(k^n\). Hence \(\alpha\) is the norm of \(\xi\) for the extension \(k^n(\xi)/k^n\), and it follows from (ii) that \((\alpha, \alpha)_{n,f} = 0.\)

Let \(0 \leq n \leq m\). Then the maximal ideal \(p_n\) of \(k^n\) is contained in the maximal ideal \(p_m\) of \(k^m\). Hence, if \(\alpha \in p_n\), then \(\pi^{m-n} \alpha \in p_n \subseteq p_m\).

**Lemma 8.7.** (i) Let \(0 \leq n \leq m\). Let \(\alpha \in p_n\), \(\alpha' = \pi^{m-n} \alpha \in p_n \subseteq p_m\), \(\beta' \in B_m = (k^m)^\times\), and \(\beta = N_{m,n}(\beta') \in B_n = (k^n)^\times\). Then
\[(\alpha', \beta')_m = (\alpha, \beta)_n.\]

(ii) Let \(f, f' \in \mathcal{T}_n\) and \(h : F_f \cong F_{f'}\) over \(\mathfrak{o}\). Then
\[h((\alpha, \beta)_{n,f}) = (h(\alpha), \beta)_{n,f}.\]

For each \(n \geq 0\), let
\[A_n = p_n = \text{the maximal ideal of } k^n\]
and let
\[A_f = \lim A_n,\]
where the direct limit is taken with respect to the maps
\[A_n \rightarrow A_m, \quad \alpha \mapsto \pi^{m-n} \alpha\]
for \(0 \leq n \leq m\). Since each \(A_n (= p_n)\) is an \(\mathfrak{o}\)-module, the limit \(A_f\) is also an \(\mathfrak{o}\)-module in the obvious manner. By Lemma 8.6(i), the map \(\{\alpha, \beta\} \mapsto (\alpha, \beta)_{n,f}\) defines a pairing of abelian groups:
\[(, )_{n,f} : A_n \times B_n \rightarrow W_f^n.\]

By Lemma 8.7(i), we then see these pairings \((, )_{n,f}\) for all \(n \geq 0\), define a pairing
\[(, )_f : A_f \times B \rightarrow W_f.\]
More precisely, let \( \alpha \in A_f \), \( \beta = (\beta_0, \beta_1, \ldots) \in B \), and let \( \alpha \) be represented by \( \alpha_n \in A_n \)—that is, \( \alpha_n \mapsto \alpha \) in \( A_n \to A_f \) for some \( n \geq 0 \). Then \( (\alpha_n, \beta_n)_{n,f} \) is defined and is an element of \( W_f^n \in W_f \). Let \( m \geq n \geq 0 \). Then \( \alpha \) is represented in \( A_m \) by \( \alpha_m = \pi^{m-n} \alpha_n \), while \( N_{m,n}(\beta_m) = \beta_n \). Hence, by Lemma 8.7(i),

\[
(\alpha_n, \beta_n)_{n,f} = (\alpha_m, \beta_m)_{m,f}.
\]

Therefore, for any \( \alpha \in A_f \) and \( \beta \in B \), we can define a well-determined element \( (\alpha, \beta)_f \) in \( W_f \) by

\[
(\alpha, \beta)_f = (\alpha_n, \beta_n)_{n,f},
\]

if \( \alpha \) is represented by \( \alpha_n \) in \( A_n \). It is clear that the map \( (\ , )_f : A_f \times B \to W_f \) defined in this manner is a pairing of abelian groups \( A_f \) and \( B \) into \( W_f \). Furthermore, Lemmas 8.6 and 8.7 show that the pairing has the properties:

\[
(a_f \alpha, \beta)_f = a_f (\alpha, \beta)_f, \quad \text{for } a \in \mathcal{O},
\]

\[
h((\alpha, \beta)_f) = (h(\alpha), \beta)_f, \quad \text{if } h : F_f \cong F_{f'}.
\]

### 8.3. The Pairing \([\alpha, \beta]_\omega\)

From now on, we assume that \((k, \nu)\) is a \( p \)-field of characteristic 0. Let \( \pi \) be a prime element of \((k, \nu)\), and \( f \) a power series in \( \mathbb{F}_1^1 \). By Lemma 4.2, there is a unique isomorphism over \( k \):

\[
\lambda_0 : F_f \cong G_a
\]

such that \( \lambda_0(X) \equiv X \mod \deg 2 \). For \( u \in U = U(k) \), let \( \lambda(X) = u \lambda_0(X) \). Then \( \lambda \) is the unique isomorphism over \( k \):

\[
\lambda : F_f \cong G_a
\]

such that \( \lambda(X) \equiv uX \mod \deg 2 \). All such isomorphisms, for \( u \in U \), will be called the logarithms of the formal group \( F_f \). Since \( F_f(X, Y) \in \mathcal{O}[[X, Y]] \), the power series \( \psi(X) \) in the proof of Lemma 4.2 belongs to \( \mathcal{O}[[X]] \). Hence \( \lambda(X) \) above is a power series of the form

\[
\lambda(X) = \sum_{n=1}^{\infty} \frac{c_n}{n} X^n, \quad c_1 = u, \quad c_n \in \mathcal{O}, \quad \text{for all } n \geq 1. \tag{8.1}
\]

Let \( f' \) be another power series in \( \mathbb{F}_1^1 \) and let \( h : F_{f'} \cong F_f \) be an isomorphism over \( \mathcal{O} \). Then \( h(X) \equiv u'X \mod \deg 2 \) with \( u' \in U \). Hence

\[
\lambda \circ h : F_{f'} \cong G_a, \quad \lambda \circ h(X) \equiv uu'X \mod \deg 2
\]

with \( uu' \in U \) so that \( \lambda \circ h \) is a logarithm for \( F_{f'} \). It is customary to define the logarithm of \( F_f \) to be the unique isomorphism \( \lambda_0 : F_f \cong G_a \) over \( k \) such that \( \lambda_0(X) \equiv X \mod \deg 2 \). However, we generalized the definition slightly so that if \( h : F_f \to F_{f'} \) over \( \mathcal{O} \) and if \( \lambda \) is a logarithm of \( F_f \), then \( \lambda \circ h \) is a logarithm of \( F_{f'} \).
LEMMA 8.8. Let \( \lambda \) be a logarithm of \( F_f \). Then:

(i) \( \lambda(\alpha) \) converges in \( \bar{\Omega} \) for any \( \alpha \in m_f \). If, in particular, \( \alpha \in v_m, \ m \geq 0 \), then \( \lambda(\alpha) \in k_n^m \).

(ii) \( \lambda(\alpha + \beta) = \lambda(\alpha) + \lambda(\beta), \ \lambda(\alpha \cdot \alpha) = a\lambda(\alpha), \) for \( \alpha, \beta \in m_f, \ a \in o. \)

**Proof.** (i) For simplicity, the valuation \( \bar{\mu} \) on \( \bar{\Omega} \) (cf. Section 3.1) will be denoted by \( \mu. \) Let \( e = \mu(p) > 0 \) and let \( p^e, \ e \geq 0, \) be the exact power of \( p \) dividing \( n. \) Then \( p^e \leq n, \mu(n) = ee \leq e \log_p n. \) Since \( c_n \in o, \ \mu(c_n) \geq 0 \) in (8.1),

\[
\mu \left( \frac{c_n}{n} \alpha^n \right) = n\mu(\alpha) - e \log_p n,
\]

where \( \mu(\alpha) > 0 \) for \( \alpha \in m_f = v_\Omega. \) Hence \( (c_n/n)\alpha^n \to 0 \) as \( n \to +\infty, \) and \( \lambda(\alpha) = \sum_{n=1}^\infty (c_n/n)\alpha^n \) converges in \( \bar{\Omega}. \) The rest is clear.

(ii) \( \lambda: F_f \to G_a \) means \( \lambda(F_f(X, Y)) = \lambda(X) + \lambda(Y). \) Hence the first equality is clear. We also have

\[
\lambda \circ [a] \circ \lambda^{-1} \in \text{End}_K(G_a), \quad \lambda \circ [a] \circ \lambda^{-1} = aX \mod \deg 2.
\]

By the remark after Proposition 4.2, we then see that

\[
\lambda \circ [a] \circ \lambda^{-1} = aX, \quad \text{that is,} \quad \lambda \circ [a] = a\lambda.
\]

This yields the second equality. 

We now fix a normed \( \pi \)-sequence \((f, \omega), \ \omega = \{\omega_n\}_{n=0}, \) for \( k. \) Let \( \lambda(X) \) be a logarithm of \( F_f. \) For each \( \beta = (\beta_0, \beta_1, \ldots) \) in \( B, \) we define

\[
\delta(\beta)_n = \frac{1}{\lambda'(\omega_n)} \frac{t'_\beta(\omega_n)}{t_\beta(\omega_n)}, \quad \text{for } n \geq 0,
\]

(8.2)

where \( t_\beta(X) \) is the power series in Theorem 8.4 such that \( t_\beta(\omega_m) = \beta_m \) for all \( m \geq 0 \) and where \( \lambda' = d\lambda/dX, \ t'_\beta = dt_\beta/dX. \) Since \( t_\beta(\omega_n) = \beta_n \neq 0 \) and since

\[
\lambda'(X) = u + \sum_{n=1}^\infty c_n X^{n-1}, \quad c_n \in o,
\]

so that \( \mu(\lambda'(\omega_n)) = 0, \ \lambda'(\omega_n) \neq 0, \) we see that \( \delta(\beta)_n \) is a well-defined element in \( k_n^m \). Note that \( \delta(\beta)_n \) depends not only on \( \beta \) and \( n \geq 0 \) but also on \((f, \omega)\) and the choice of the logarithm \( \lambda \) for \( F_f. \)

**LEMMA 8.9.** (i) \( \delta(\beta\beta')_n = \delta(\beta)_n + \delta(\beta')_n, \) for \( \beta, \beta' \in B. \)

(ii) \( \delta(\beta)_n \in v_n^{-1} \) for all \( \beta \in B. \)

(iii) Let \( 0 \leq n \leq m \) and let \( T_{m,n} \) denote the trace map of \( k^n/\pi k^n. \) Then

\[
T_{m,n}(\delta(\beta)_m) = \pi^{m-n}\delta(\beta)_n, \quad \text{for } \beta \in B.
\]

**Proof.** (i) This follows immediately from \( t_{\beta\beta'} = t_\beta t_{\beta'}, \) and from the definition (8.2) of \( \delta(\beta)_n. \)

(ii) Let \( v(\beta) = 1 \) (cf. Section 8.1). Then \( \beta_n = t_\beta(\omega_n) \) is a prime element of \( k_n^m \). Since \( \mu(\lambda'(\omega_n)) = 0 \) as stated above, it follows from (8.2) that
\( \delta(\beta)_n \in v_n^{-1} \). By (i), the same result then holds for any \( \beta \in B \) because \( B \) is generated by the \( \beta \)'s with \( v(\beta) = 1 \).

(iii) Again, we may assume that \( v(\beta) = 1 \) so that \( (f', \beta) \), where \( f' = f_\beta \circ f \circ t_\beta^{-1} \), is a normed \( \pi \)-sequence for \( k \) (cf. Section 8.1). Then, by Lemma 8.3,

\[
[\pi]_{f'} = \prod_{\gamma'} (X \frac{d}{dX} \gamma'), \quad \gamma' \in W^0_f.
\]

Since \( t_\beta : F_f \simeq F_{f'} \), \( [\pi]_{f'} = t_\beta \circ [\pi]_f \circ t_\beta^{-1} \), and \( W^0_f = t_\beta(W^0_{f'}) \), it follows that

\[
t_\beta \circ [\pi] = \prod_{\gamma'} (t_\beta(X) \frac{d}{dX} \gamma') = \prod_{\gamma} t_\beta(X \frac{d}{dX} \gamma), \quad \gamma \in W^0_f.
\]

Logarithmically differentiating with respect to \( X \), we obtain

\[
\left( \frac{t'_\beta [\pi]_f}{t_\beta [\pi]_f} \right) \frac{d}{dX} [\pi]_f = \sum_{\gamma} \left( \frac{t'_\beta(X \frac{d}{dX} \gamma)}{t_\beta(X \frac{d}{dX} \gamma)} \right) \frac{d}{dX} \left( X \frac{d}{dX} \gamma \right).
\]

However, \( \lambda([\pi]_f)(X) = \pi \lambda(X) \), \( \lambda'(X \frac{d}{dX} \gamma) = \lambda(X) + \lambda(\gamma) \) implies

\[
(\lambda'^{\circ} [\pi]_f) \frac{d}{dX} [\pi]_f = \pi \lambda'(X), \quad \lambda'(X \frac{d}{dX} \gamma) \frac{d}{dX} (X \frac{d}{dX} \gamma) = \lambda'(X).
\]

Hence

\[
\frac{\pi}{\lambda'^{\circ} [\pi]_f} \cdot \frac{t'_\beta [\pi]_f}{t_\beta [\pi]_f} = \sum_{\gamma} \frac{1}{\lambda'(X \frac{d}{dX} \gamma)} \left( \frac{t'_\beta(X \frac{d}{dX} \gamma)}{t_\beta(X \frac{d}{dX} \gamma)} \right), \quad \gamma \in W^0_f.
\]

Put \( X = \omega_{n+1} \) in the above. Since \( \omega_{n+1} \frac{d}{dX} W^0_f \) is the complete set of conjugates of \( \omega_{n+1} \) over \( k^n_\pi \) (cf. the Corollary of Proposition 5.4), it follows that

\[
\pi \delta(\beta)_n = T_{n+1,n}(\delta(\beta)_{n+1}), \quad n \geq 0.
\]

Therefore, \( T_{m,n}(\delta(\beta)_m) = \pi^{m-n} \delta(\beta)_n \) for \( 0 \leq n \leq m \).

Let \( n \geq 0 \) and let \( \alpha_n \in A_n (= v_n), \beta \in B \). We define

\[
x_n(\alpha_n, \beta) = \frac{1}{\pi^{n+1}} T_n(\lambda(\alpha_n) \delta(\beta)_n)
\]

where \( T_n \) denotes the trace map of \( k^n_\pi/k \) and \( \lambda \) is the logarithm of \( F_f \) mentioned above. If \( \lambda \) is replaced by another logarithm \( u\lambda, u \in U \), then \( \lambda(\alpha_n) \) is replaced by \( u\lambda(\alpha_n) \), and \( \delta(\beta)_n \) by \( u^{-1} \delta(\beta)_n \) (cf. (8.2)). Hence \( x_n(\alpha_n, \beta) \) is unchanged. Thus \( x_n(\alpha_n, \beta) \) is an element of \( k \), depending on \( n, \alpha_n, \beta \), and the fixed normed \( \pi \)-sequence \((f, \omega)\), but not on the choice of \( \lambda \).

**Lemma 8.10.** Let \( \alpha_n, \alpha'_n \in A_n, \beta, \beta' \in B \).

(i) \( x_n(\alpha_n \frac{d}{dX} \alpha_n, \beta) = x_n(\alpha_n, \beta) + x_n(\alpha'_n, \beta) \),

\[
x_n(\alpha_n \frac{d}{dX} \alpha_n, \beta) = ax_n(\alpha_n, \beta), \quad a \in \omega,
\]

\[
x_n(\alpha_n, \beta \beta') = x_n(\alpha_n, \beta) + x_n(\alpha_n, \beta').
\]
(ii) \( x_m(\pi^{m-n}; \alpha_n, \beta) = \pi^{m-n} x_n(\alpha_n, \beta) \), for \( 0 \leq n \leq m \).

**Proof.**  (i) follows Lemma 8.8(ii) and Lemma 8.9(i).

(ii) By Lemma 8.8(ii) and Lemma 8.9(iii),

\[
x_m(\pi^{m-n}; \alpha_n, \beta) = \frac{1}{\pi^{m+1}} T_m(\lambda(\pi^{m-n}; \alpha_n)\delta(\beta)_m)
= \frac{1}{\pi^{n+1}} T_n(\lambda(\alpha_n)\delta(\beta)_n)
= \pi^{m-n} x_n(\alpha_n, \beta).
\]

Now, let

\[
\alpha \in A_f = \lim A_n, \quad \beta \in B = \lim B_n,
\]

and suppose that \( \alpha \) is represented by \( \alpha_n \in A_n \). Then, for \( 0 \leq n \leq m \), \( \alpha \) is also represented by \( \alpha_m = \pi^{m-n} \alpha_n \) in \( A_m \) and \( x_m(\alpha_n, \beta) = \pi^{m-n} x_n(\alpha_n, \beta) \) by the above lemma. Hence, if \( m \) is sufficiently large, then \( x_m(\alpha_m, \beta) \) belongs to \( \mathfrak{o} \) so that \( x_m(\alpha_m, \beta) ; \omega_m \) is defined, \( \omega_m \) being the \( m \)th element in \( \omega = (\omega_0, \omega_1, \ldots) \) for the fixed normed \( \pi \)-sequence \( (f, \omega) \). Let \( m' \geq m \). By Lemma 8.10(ii),

\[
x_m(\alpha_m, \beta) = \pi^{m'-m} x_m(\alpha_m, \beta) \in \mathfrak{o},
\]

\[
x_m(\alpha_m, \beta) ; \omega_m = x_m(\alpha_m, \beta) \pi^{m'-m} ; \omega_m = x_m(\alpha_m, \beta) ; \omega_m.
\]

Thus, whenever \( m \) is large enough, \( x_m(\alpha_m, \beta) ; \omega_m \) is defined and it is independent of \( m \). Clearly \( x_m(\alpha_m, \beta) ; \omega_m \in W_f \). Therefore, for any \( \alpha \in A_f \) and \( \beta \in B \), we define an element \([\alpha, \beta]_\omega\) of \( W_f \) by

\[
[\alpha, \beta]_\omega = x_m(\alpha_m, \beta) ; \omega_m
= \left[ \frac{1}{\pi^{n+1}} T_n(\lambda(\alpha_m)\delta(\beta)_m) \right] ; \omega_m
\]

with any sufficiently large \( m \). It is then clear from Lemma 8.10 that

\[
[\ , ]_\omega : A_f \times B \to W_f
\]

is a pairing of the abelian groups \( A_f \) and \( B \) into \( W_f \), satisfying

\[
[a ; \alpha, \beta]_\omega = a ; [\alpha, \beta]_\omega, \quad \text{for } a \in \mathfrak{o}.
\]

Note that the pairing depends only on the normed \( \pi \)-sequence \( (f, \omega) \).

Now, let \( (f', \omega') \) be another normed \( \pi \)-sequence for \( k \) and let

\[
h : (f, \omega) \simeq (f', \omega').
\]

By Proposition 8.2, such an isomorphism exists. Then \( h \) induces an isomorphism \( h : F_f \to F_{f'} \) over \( \mathfrak{o} \) and \( \alpha \mapsto h(\alpha) \) defines \( \mathfrak{o} \)-isomorphisms

\[
W_f \simeq W_{f'}, \quad A_f \simeq A_{f'}.
\]
**Lemma 8.11.** For \( \alpha \in A_f, \beta \in B \),
\[
h([\alpha, \beta])_\omega = [h(\alpha), \beta]_\omega,
\]
where \([ , ]_\omega\) is the pairing defined by \((f', \omega')\).

**Proof.** Let \( \lambda : F_f \simeq G_a \) be a logarithm of \( F_f \). As mentioned earlier,
\[
\tilde{\lambda} = \lambda \circ h^{-1} : F_f' \simeq G_a
\]
is a logarithm of \( F_f' \). For \( \beta \in B \),
\[
\tilde{t}_\beta = t_\beta \circ h^{-1}
\]
is clearly the unique power series in Theorem 8.4 for \((f', \omega')\) such that
\[
\tilde{t}_\beta(\omega'_n) = \beta_n \quad \text{for all } n \geq 0.
\]
Differentiating both sides of \( \tilde{t}_\beta = t_\beta \circ h \), we obtain \((\tilde{t}_\beta \circ h)' = t_\beta'\) with derivatives \( t_\beta' = dt_\beta/dX \), and so on. Since \( h(\omega_n) = \omega'_n \), it follows
\[
\tilde{t}_\beta'(\omega'_n)h'(\omega_n) = t_\beta'(\omega_n).
\]

Similarly, \( \tilde{\lambda} \circ h = \lambda \) yields
\[
\tilde{\lambda}'(\omega'_n)h'(\omega_n) = \lambda'(\omega_n).
\]
As \( h(X) = vX \mod \deg 2 \) with \( v \in U \), we see that \( h'(X) = v \mod \deg 1, h'(\omega_n) \neq 0 \). Hence it follows from the above that
\[
\delta(\beta)_n = \frac{1}{\lambda'(\omega_n)} \frac{t_\beta'(\omega_n)}{\beta_n} = \frac{1}{\tilde{\lambda}'(\omega'_n)} \frac{\tilde{t}_\beta'(\omega'_n)}{\beta_n} = \tilde{\delta}(\beta)_n,
\]
\( \tilde{\delta}(\beta)_n \) being the expression (8.2) for the normed \( \pi \)-sequence \((f', \omega')\).

Therefore,
\[
x_n = \frac{1}{\pi^{n+1}} T_n(\lambda(\alpha_n)\delta(\beta)_n) = \frac{1}{\pi^{n+1}} T_n(\tilde{\lambda}(h(\alpha_n))\tilde{\delta}(\beta)_n)
\]
for \( \alpha_n \in A_n \), representing \( \alpha \). Consequently, for large \( n \),
\[
h([\alpha, \beta])_\omega = h(x_n; \omega_n) = x_n f h(\omega_n) = x_n f \omega'_n
\]
\[
= [h(\alpha), \beta]_\omega.
\]

**8.4. The Main Theorem**

Still fixing a normed \( \pi \)-sequence \((f, \omega)\) for the \( p \)-field \((k, v)\) of characteristic 0, we shall prove the formula
\[
(\alpha, \beta)_f = [\alpha, \beta]_\omega, \quad \text{for } \alpha \in A_f, \beta \in B,
\]
where \(( , )_f\) and \([ , ]_\omega\) are the pairings \( A_f \times B \to W_f \), defined in Sections 8.2 and 8.3, respectively. We first prove some elementary lemmas.

**Lemma 8.12.** Let \( e = v(p) = \mu(p) > 0 \), where \( \mu \) is the extension of \( v \) on \( \Omega \) and \( \tilde{\Omega} \). Let \( \gamma \in \tilde{\Omega} \), \( \mu(\gamma) \geq e \). Then
\[
\mu(\gamma^j/j) \geq 2\mu(\gamma) - e, \quad \text{for all integers } j \geq 2.
\]
Proof. Let \( j = p^aq^r, \ a \geq 0, (j', p) = 1 \). Then
\[
\mu(\gamma/j) = j\mu(\gamma) - \mu(j) = j\mu(\gamma) - ae.
\]
Hence the lemma is trivial if \( a = 0 \). For \( a \geq 1 \),
\[
\mu(\gamma/j) - 2\mu(\gamma) + e = (j - 2)\mu(\gamma) - (a - 1)e \geq (j - 1 - a)\mu(\gamma),
\]
where \( j - 1 - a \geq p^a - 1 - a \geq 0 \) for \( a \geq 1 \).

**Lemma 8.13.** Let \( \mathfrak{o}_n \) denote, as before, the valuation ring of \( k_\alpha^n \). Let \( \gamma \in \pi^\alpha\mathfrak{o}_n \), where \( e \leq a \leq n \). Then
\[
N_n(1 + \gamma)^{-1} - 1 = -T_n(\gamma) \mod \pi^{3a - e},
\]
\( T_n \) and \( N_n \) being the trace and the norm map of \( k_\alpha^n/k \), respectively.

**Proof.**
\[
N_n(1 + \gamma) = \prod_{\gamma} (1 + \gamma^\sigma) = 1 + \sum_{\sigma} \gamma^\sigma + \sum_{\sigma, \tau} \gamma^\sigma\gamma^\tau \mod \pi^{3a},
\]
where \( \sigma, \tau \in \text{Gal}(k_\alpha^n/k) \) and the second sum on the right is taken over all pairs \((\sigma, \tau)\) such that \( \sigma \neq \tau \). Hence
\[
\sum_{\sigma} \gamma^\sigma = T_n(\gamma), \quad \sum_{\sigma, \tau} \gamma^\sigma\gamma^\tau = \frac{1}{2} \left( \left( \sum_{\sigma} \gamma^\sigma \right)^2 - \sum_{\sigma, \tau} \gamma^{2\sigma} \right)
\]
\[
= \frac{1}{2}(T_n(\gamma)^2 - T_n(\gamma^2)).
\]
By Proposition 7.11, \( \pi^{-n}\mathfrak{o}_n \subseteq \mathcal{D}(k_\alpha^n/k)^{-1} \) for the different \( \mathcal{D}(k_\alpha^n/k) \). Hence \( \gamma \in \pi^\alpha\mathfrak{o}_n \) and \( T_n(\mathcal{D}(k_\alpha^n/k)^{-1}) \subseteq \mathfrak{o} \) imply
\[
T_n(\gamma) \in p^{a+n}, \quad T_n(\gamma^2) \in p^{2a+n}, \quad T_n(\gamma)^2 \in p^{2a+2n}.
\]
(8.3)
Since \( \mu(2) = 0 \) or \( e \) according as \( p > 2 \) or \( p = 2 \), we obtain
\[
\sum_{\sigma, \tau} \gamma^\sigma\gamma^\tau \equiv 0 \mod \pi^{2a+n - e}
\]
so that
\[
N_n(1 + \gamma) = 1 + T_n(\gamma) \mod \pi^{3a - e}.
\]
Using \( T_n(\gamma)^2 \in p^{2a+2n} \subseteq p^{3a} \), we then see that
\[
N_n(1 + \gamma)^{-1} = 1 - T_n(\gamma) \mod \pi^{3a - e}.
\]

**Lemma 8.14.** For each \( \alpha \in A_f \), there exists an integer \( c \geq 0 \) such that for any \( n \geq c \), \( \alpha \) is represented in \( A_n \) by \( \alpha_n \), which satisfies
\[
\mu(\alpha_n) \geq n - c.
\]

**Proof.** In general, let \( \gamma \in \mathfrak{m}_f \). Since
\[
[\pi]_f \equiv X^q \mod p, \quad [\pi]_f \in X\mathfrak{o}[[X]],
\]
we see that
\[
\mu(\pi; \gamma) \geq \min(\mu(\gamma^q), \mu(\pi\gamma)) = \min(q\mu(\gamma), \mu(\gamma) + 1).
\]
Hence, if \( \mu(\gamma) < 1/(q - 1) \) so that the minimum is \( q\mu(\gamma) \), then \( \mu(\pi; \gamma) \geq q\mu(\gamma) \). Therefore, in any case there always exists an integer \( j \geq 0 \) such that
$\mu(\pi_j^i; \gamma) \geq 1/(q - 1)$, and it then follows from the above inequality that

$$\mu(\pi_j^{i+1}; \gamma) \geq \mu(\pi_j^i; \gamma) + i \geq i, \quad \text{for all } i \geq 0.$$

Now, let $\alpha$ in $A_f$ be represented by $\alpha_j \in A_j$ for some $j'$. Putting $\gamma = \alpha_j$, $c = j + j'$, $n = i + j + j' \geq c$ in the above, we obtain the lemma.

We now prove the following key lemma:

**Lemma 8.15.** Let $(f, \omega)$ be a normed $\pi$-sequence for $k$. Then

$$(\alpha, \omega)_f = [\alpha, \omega]_\omega$$

for every $\alpha \in A_f$.

**Proof.** Note first that $\omega = \{\omega_n\}_{n=0}^\infty$ belongs to $B$. Let

$$n \geq 3c + e + 5$$

for $e = \mu(p)$ and for the integer $c \geq 0$ in Lemma 8.14. Then $\alpha$ is represented by $\alpha_n \in A_n$ and

$$\alpha_n \cdot f \omega_n = F_f(\alpha_n, \omega_n) = \alpha_n + \omega_n + \sum_{i,j} c_{ij} \alpha_n^i \omega_n^j, \quad c_{ij} \in \mathbb{O}, \quad i, j \geq 1$$

by (4.1). Hence, if we put

$$\alpha_n \cdot f \omega_n = \omega_n(1 + \gamma_n), \quad \gamma_n = \frac{\alpha_n}{\omega_n} + \sum_{i,j} c_{ij} \alpha_n^i \omega_n^{j-1}, \quad i, j \geq 1,$$

then $\mu(\alpha_n/\omega_n) < \mu(c_{ij} \alpha_n^i \omega_n^{j-1})$ so that

$$\mu(\gamma_n) = \mu(\alpha_n) - \mu(\omega_n) \geq n - c - 1 > 0,$$

$$\mu(\alpha_n \cdot f \omega_n) = \mu(\omega_n).$$

This shows that $\alpha_n \cdot f \omega_n$, as well as $\omega_n$, is a prime element of $k^n_\pi$. It then follows from Lemma 8.6(iii) that

$$(\omega_n, \omega_n)_{n,f} = (\alpha_n \cdot f \omega_n, \alpha_n \cdot f \omega_n)_{n,f} = 0.$$

However, omitting the suffix $f$, we have

$$(\alpha_n + \omega_n, \alpha_n + \omega_n)_n = (\alpha_n + \omega_n, \omega_n(1 + \gamma_n))_n,$$

$$= (\alpha_n, \omega_n)_n + (\alpha_n, 1 + \gamma_n)_n + (\omega_n, \omega_n)_n + (\omega_n, 1 + \gamma_n)_n.$$

Hence

$$(\alpha, \omega)_f = (\alpha_n, \omega_n)_n = \gamma (\alpha_n, 1 + \gamma_n)_n = (\omega_n, 1 + \gamma_n)_n. \quad (8.5)$$

We shall next compute $(\alpha_n, 1 + \gamma_n)_n$ and $(\omega_n, 1 + \gamma_n)_n$.

Since $\pi^{n+1} \cdot \omega_2n+1 = \omega_n+1$, $\omega_2n+1 \in k_{ab}$, we see that

$$(\omega_n, 1 + \gamma_n)_n = \rho_n(1 + \gamma_n)(\omega_2n+1) - \omega_2n+1, \quad \text{by the definition of } (\ , \ )_n,$$

$$= \rho_k(N_n(1 + \gamma_n))(\omega_2n+1) - \omega_2n+1, \quad \text{by Theorem 6.9},$$

$$= (N_n(1 + \gamma_n)^{-1} - 1)j \omega_2n+1, \quad \text{by (6.4)}.$$
Since $\gamma_n \in \pi^{n-c-1}o_n$ by (8.4), it follows from Lemma 8.13 for $a = n - c - 1$ that

$$N_n(1 + \gamma_n)^{-1} - 1 = -T_n(\gamma_n) \mod \pi^m,$$

where $m = 3(n - c - 1) - e \geq 2n + 2$. It also follows from (8.3) that

$$T_n(\gamma_n) \equiv 0 \mod \pi^{n+(n-c-1)}$$

hence $\mod \pi^{n+1}$.

(8.6)

Therefore, we obtain from the above that

$$(\omega_n, 1 + \gamma_n)n = (-T_n(\gamma_n)) \cdot \omega_{2n+1} = \left(-\frac{1}{\pi^{n+1}} T_n(\gamma_n)\right) \cdot \pi^{n+1} \cdot \omega_{2n+1}$$

$$= \left(-\frac{1}{\pi^{n+1}} T_n(\gamma_n)\right) \cdot \omega_n.$$  \hspace{1cm} (8.7)

As before, let $\lambda$ denote a logarithm for $F_f$. Then, by (8.1)

$$\lambda(X) = \sum_{i=1}^{\infty} \frac{c_i}{i} X^i, \quad c_1 = u, \quad c_i \in o, \quad \text{for } i \geq 1.$$

Hence it follows from $\alpha_n + \omega_n = \omega_n(1 + \gamma_n)$ that

$$\lambda(\alpha_n) + \lambda(\omega_n) = \lambda(\omega_n(1 + \gamma_n)) = \sum_{i=1}^{\infty} \frac{c_i}{i} \omega_n^i(1 + \gamma_n)^i,$$

where

$$\frac{(1 + \gamma_n)^i}{i} = \frac{1}{i} + \gamma_n + \sum_{j=2}^{i} \frac{(i - 1)}{j} \frac{1}{j} \gamma_n^j.$$

By Lemma 8.12,

$$\mu(\gamma_n^i/j) \geq 2\mu(\gamma_n) - e \geq 2(n - c - 1) - e, \quad \text{for } j \geq 2.$$

Therefore,

$$\lambda(\alpha_n) + \lambda(\omega_n) = \lambda(\omega_n) + \gamma_n \omega_n \lambda'(\omega_n) \mod \pi^{2(n-c-1)-e},$$

where $\lambda' = d\lambda/dX$. Since

$$\delta(\omega)_n = \frac{1}{\lambda'(\omega_n)\omega_n} \in p_n^{-1},$$

we obtain from (8.2) and from the above that

$$\lambda(\alpha_n) \delta(\omega)_n \equiv \gamma_n \mod \pi^{2(n-c-1)-e-1}.$$

Consequently, by (8.3),

$$T_n(\lambda(\alpha_n) \delta(\omega)_n) \equiv T_n(\gamma_n) \mod \pi^{m'},$$

where

$$m' = 2(n - c + 1) - e - 1 + n \geq 2n + 2$$

because of $n \geq 3c + e + 5$. Since $T_n(\gamma_n) \in o$ by (8.6), $T_n(\lambda(\alpha_n) \delta(\omega)_n)$ also belongs to $o$, and it follows from $m' \geq 2n + 2$ that

$$\frac{1}{\pi^{n+1}} T_n(\lambda(\alpha_n) \delta(\omega)_n) \equiv \frac{1}{\pi^{n+1}} T_n(\gamma_n) \mod \pi^{n+1}.$$
so that by (8.7),

\[ (\omega_n, 1 + \gamma_n)_n = -\left(\frac{1}{\pi^{n+1}} T_n(\gamma_n)\right) \cdot \omega_n \]

\[ = -\left(\frac{1}{\pi^{n+1}} T_n(\lambda(\alpha_n)\delta(\omega)_n)\right) \cdot \omega_n \]

\[ = -[\alpha, \omega]_\omega. \tag{8.8} \]

To compute \((\alpha_n, 1 + \gamma_n)_n\), let \(\pi^{c+1} f \xi = \alpha_0\), \(k' = k_c(\xi)\) for the integer \(c \geq 0\) above. Since \(n \geq c\), it follows from Lemma 8.7(i), that

\[(\alpha_n, 1 + \gamma_n)_n = (\alpha_c, N_{n,c}(1 + \gamma_n))_c = \rho_c(N_{n,c}(1 + \gamma_n))(\xi) - \xi.\]

However, (8.4)—that is, \(\gamma_n \in \pi^{n-c-1} \omega_n\)—implies

\[ N_{n,c}(1 + \gamma_n) \equiv 1 \mod \pi^{n-c-1}. \]

By Lemma 3.5 and Proposition 7.2, \(N(k' / k_{\xi})\) is a closed subgroup of finite index in \((k_c)^\times\). Therefore, the above congruence shows that \(N_{n,c}(1 + \gamma_n)\) is contained in \(N(k' / k_{\xi})\) whenever \(n\) is large enough. For such an \(n\), we then have \(\rho_c(N_{n,c}(1 + \gamma_n)) | k' = 1\) by Theorem 7.1 so that

\[(\alpha_n, 1 + \gamma_n)_n = \rho_c(N_{n,c}(1 + \gamma_n))(\xi) - \xi = 0. \tag{8.9} \]

Finally, we see from (8.5), (8.8), and (8.9) that for sufficiently large \(n\),

\[(\alpha, \omega)_f = - (\alpha_n, 1 + \gamma_n)_n - (\omega_n, 1 + \gamma_n)_n \]

\[= [\alpha, \omega]_\omega. \]

We are now ready to prove the following theorem:

**Theorem 8.16.** Let \((f, \omega)\) be any normed \(\pi\)-sequence for \(k\). Then

\[ (\alpha, \beta)_f = [\alpha, \beta]_\omega, \quad \text{for } \alpha \in A_f, \beta \in B. \]

Furthermore, if \(\alpha\) is represented by \(\alpha_n\) in \(A_n\), \(n \geq 0\), then the element

\[ x_n = \frac{1}{\pi^{n+1}} T_n(\lambda(\alpha_n)\delta(\beta)_n) \]

belongs to \(\omega\), and

\[(\alpha, \beta)_f = x_n j \omega_n = \left[\frac{1}{\pi^{n+1}} T_n(\lambda(\alpha_n)\delta(\beta)_n)\right] j \omega_n. \]

**Proof.** The group \(B\) is generated by the \(\beta\)'s with \(v(\beta) = 1\). Hence, in order to prove \((\alpha, \beta)_f = [\alpha, \beta]_\omega\), we may assume that \(v(\beta) = 1\). By the remark at the end of Section 8.1, we have

\[ h(= t_\beta): (f, \omega) \simeq (f', \beta), \]

where \(f' = f_\beta = t_\beta \circ f \circ t_\beta^{-1}\). Therefore, by Lemma 8.7(ii) and Lemma 8.11, it is sufficient to prove

\[(\alpha', \beta)_f = [\alpha', \beta]_\beta, \quad \text{for all } \alpha' \in A_f. \]
However, this is exactly Lemma 8.15 for the normed $\pi$-sequence $(f', \beta)$. Thus the first half of the theorem is proved. Let $\alpha$ be represented by $\alpha_n \in A_n$. For large $m \geq n$, we know that $x_m (= x_m(\alpha_m, \beta))$ belongs to $\omega$ and

$$(\alpha, \beta)_f = [\alpha, \beta]_\omega = x_m \omega_m.$$  

However, since $\alpha$ is represented by $\alpha_n \in A_n$, it follows from the definition of $\alpha, (\alpha, \beta)_f = (\alpha_n, \beta_n)_n,f \in \mathcal{W}_f^\pi$. Hence, by Lemma 4.8(ii),

$$\pi^{n+1} x_m \omega_m = 0, \quad \pi^{n+1} x_m \in \mathcal{V}^{n+1}.$$  

As $x_m = \pi^{m-n} x_n$ by Lemma 8.10(ii), we obtain

$$\pi^{m+1} x_n \in \mathcal{V}^{m+1}, \quad \text{that is, } x_n \in \omega.$$  

Let $(f, \omega)$ now be any $\pi$-sequence for $k$, not necessarily normed. By Theorem 8.4, for each $\beta \in B$ with $\nu(\beta) = 0$, there exists a unique power series $t_\beta(X)$ in $\omega[[X]]^\times$ such that $t_\beta(\omega_n) = \beta_n$ for all $n \geq 0$. With this $t_\beta$, one can define $\delta(\beta)_n$ by (8.3) and, hence, $x_n(\alpha, \beta)$ and $[\alpha, \beta]_\omega$ for $\beta \in B$ with $\nu(\beta) = 0$. Take a normed $\pi$-sequence $(f', \omega')$ for $k$ and let

$$h : (f, \omega) \simeq (f', \omega').$$  

Since Theorem 8.16 holds for $(f', \omega')$, it follows from Lemma 8.11 that Theorem 8.16 holds also for $(f, \omega)$, provided that $\nu(\beta) = 0$.

We shall next formulate the above result in a form more convenient for applications. For this, we need the following lemma.

**Lemma 8.17.** Let $\beta_n \in B_n = (k^\pi_n)^\times$. Then $\beta_n$ is the $n$th component of an element $\beta = (\beta_0, \beta_1, \ldots)$ in $B$ if and only if $N_n(\beta_n)$ is a power of $\pi$: $N_n(\beta_n) \in \langle \pi \rangle$.

**Proof.** Let $\beta_n$ be the $n$th component of $\beta = (\beta_0, \beta_1, \ldots)$ in $B$. Then $N_m(\beta_m) = N_n(\beta_n)$ for all $m \geq 0$. Hence $N_n(\beta_n) \in N(k^\pi_n/k) = \langle \pi \rangle$ by Proposition 5.17. Suppose, conversely, that $N_n(\beta_n) \in \langle \pi \rangle$. Apply Theorem 7.6 for

$$k' = k^\pi_n, \quad E = k^\pi_{n+1}, \quad E' = Ek' = k^\pi_{n+1}.$$  

Since $N_n(\beta_n) \in \langle \pi \rangle = N(k^\pi_n/k) \subseteq N(k^\pi_{n+1}/k)$, $\beta_n$ belongs to $N(k^\pi_{n+1}/k)_n$ by that theorem. Therefore,

$$\beta_n = N_{n+1,n}(\beta_{n+1})$$  

for some $\beta_{n+1} \in B_{n+1} = (k^\pi_{n+1})^\times$. Since $N_{n+1}(\beta_{n+1}) = N_n(\beta_n) \in \langle \pi \rangle$, we can similarly find $\beta_{n+2} \in B_{n+2}$ such that $N_{n+2,n+1}(\beta_{n+2}) = \beta_{n+1}$. In this manner, we obtain a sequence $\beta_n, \beta_{n+1}, \beta_{n+2}, \ldots$, satisfying $N_{m+1,m}(\beta_{m+1}) = \beta_m$ for all $m \geq n$. Putting $\beta_m = N_{n,m}(\beta_n)$ for $0 \leq m \leq n$, we see that $\beta_n$ is the $n$th component of $\beta = (\beta_0, \beta_1, \ldots)$ in $B$.

It is now clear that Theorem 8.16 yields the following theorem of Wiles [25]:

**Theorem 8.18.** Let $n \geq 0$ and let $(f, \omega)$ be any normed $\pi$-sequence for $k$. Let $\alpha_n$ be an element of $\mathcal{V}_n (= A_n)$, $\beta_n$ an element of $(k^\pi_n)^\times (= B_n)$ such that
Explicit Formulas

133

where \( \lambda(X) \) is a logarithm of \( F_f \) and \( \beta \) is any element of \( B \) such that \( \beta_n \) is the \( n \)th component of \( \beta \). Then \( x_n \) belongs to \( \varnothing \), \( x_n \) is independent of the particular \( \beta \) chosen, and

\[
(\alpha_n, \beta_n)_{n, f} = x_n ; \omega_n = \left[ \frac{1}{\pi^x + 1} T_n \left( \frac{1}{\lambda'(\omega_n)} \right) \right] ; \omega_n.
\]

Furthermore, if \( \beta_n \) is a unit of \( k^n_\pi \), then the same formula holds for any \( \pi \)-sequence \( \langle f, \omega \rangle \), not necessarily normed.

8.5. The Special Case for \( k = \mathbb{Q}_p \)

In this section, we shall see what Theorem 8.16 states in the special case:

\[(k, \nu) = (\mathbb{Q}_p, \nu_p), \quad \pi = p.\]

Suppose first that \( p > 2 \) and let

\[f(X) = (1 + X)^p - 1 \in \mathcal{F}^{1}_p . \]

Then (cf. the example in Section 4.2)

\[F_f(X, Y) = (1 + X)(1 + Y) - 1, \quad [a]_f = (1 + X)^a - 1, \quad \text{for } a \in \varnothing = \mathbb{Z}_p , \]

and

\[W_f^p = \{ \xi - 1 \mid \xi \in \Omega, \xi^{p^{n+1}} = 1 \}, \]

\[k^n_\pi = \mathbb{Q}_p(W_f^p) = \mathbb{Q}_p(W_{p^{n+1}}), \]

where \( W_{p^{n+1}} \) denotes the group of all \( p^{n+1} \)th roots of unit in \( \Omega \). Since \( \alpha \hat{f} \beta = (1 + \alpha)(1 + \beta) - 1 \), the map \( \xi \mapsto \xi - 1 \) defines an isomorphism

\[
\kappa : W_{p^{n+1}} \cong W_f^p ,
\]

Let

\[
\omega = \{ \omega_n \}_{n \geq 0}, \quad \omega_n = \xi_n - 1 \in W_f^p ,
\]

where

\[
\xi_0 \neq 1, \quad \xi_0^p = 1, \quad \xi_n^p = \xi_{n-1}, \quad \text{for } n \geq 1 .
\]

As \([\pi]_f = f , \]

\[
\pi \hat{f} \omega_n = f(\xi_n - 1) = \xi_n^p - 1 = \xi_{n-1}^p - 1 = \omega_{n-1} , \quad \text{for } n \geq 1 ,
\]

so that \( (f, \omega) \) is a \( \pi \)-sequence for \( k = \mathbb{Q}_p \) and \( \pi = p \). Furthermore,

\[
X \hat{f} (\xi - 1) = (1 + X)\xi - 1, \quad \text{for } \xi - 1 \in W_f^0 , \text{ that is, for } \xi \in W_p .
\]

Since \( p \) is odd, it follows that

\[
\prod_{\xi} (X \hat{f} (\xi - 1)) = (1 + X)^p - 1 = f(X) = [\pi]_f .
\]
Therefore, by Lemma 8.3, \((f, \omega)\) is a normed \(\pi\)-sequence. (This can also be seen directly from \(N_{m,n}(\xi_n - 1) = \xi_n - 1\) for \(0 \leq n \leq m\).)

Now, let \(\alpha_n \in A_n = \wp_n\), \(\beta_n \in B_n = (k^n_\pi)^x\). Since \([\pi^{n+1}]_f = f \circ \cdots \circ f = (1 + X)^{p^{n+1}} - 1\), \(\pi^{n+1} ; \xi = \alpha_n\) means that
\[
\xi = \sqrt[p^{n+1}]{1 + \alpha_n - 1}.
\]

Let
\[
\eta = \sqrt[p^{n+1}]{1 + \alpha_n}, \quad \sigma = \rho_n(\beta_n).
\]

Then \(k^n_\pi(\xi) = k^n_\pi(\eta)\), and as \(W_{\pi^{n+1}} \subseteq k^n_\pi\), \(k^n_\pi(\xi)/k^n_\pi\) is a Kummer extension and
\[
\sigma(\eta) = \zeta \eta, \text{ that is, } (\sqrt[p^{n+1}]{1 + \alpha_n})^{\sigma - 1} = \zeta,
\]
for some \(\zeta\) in \(W_{p^{n+1}}\). We then see that
\[
(\alpha_n, \beta_n)_{n,f} = \rho_n(\beta_n)(\xi) \cdot \xi = \sigma(\eta - 1) \cdot (\eta - 1)
\]
\[
= (\zeta \eta - 1) \cdot (\eta - 1) = \zeta - 1
\]
because \((\zeta - 1) \cdot (\eta - 1) = \zeta \eta - 1\). Thus, if \(\alpha \in A_f\) is represented by \(\alpha_n \in A_n\) and if \(\beta = (\beta_0, \beta_1, \ldots, \beta_n, \ldots) \in B\), then
\[
(\alpha, \beta)_f = \zeta - 1 = \kappa(\zeta)
\]
where \(\kappa: W_{p^{n+1}} \cong W_f^n\) and
\[
\zeta = (\sqrt[p^{n+1}]{1 + \alpha_n})^{\sigma - 1}, \quad \sigma = \rho_n(\beta_n).
\]

In general, let \(m \geq 1\) and let \(k'\) be a local field containing primitive \(m\)th roots of unity. For any \(x, y \in k'^\times\), let
\[
\{x, y\} = (\sqrt[m]{y})^{\sigma - 1}, \text{ where } \sigma = \rho_{k'}(x).
\]

Then \(\{x, y\}\) is an \(m\)th root of unity, and such a symbol \(\{x, y\}\) is called the norm residue symbol for \(k'\) with exponent \(m\). The above result shows that
\[
(\alpha, \beta)_f = \kappa(\{\beta_n, 1 + \alpha_n\}) \quad (8.10)
\]
for the norm residue symbol \(\{\ , \ \}\) for \(k^n_\pi = \mathbb{Q}_p(W_{p^{n+1}})\) with exponent \(p^{n+1}\).
Thus we see that in this special case, the pairing \((\ , \ )_f: A_f \times B \rightarrow W_f\) is given, up to the isomorphism \(\kappa\), by the norm residue symbols of \(\mathbb{Q}_p(W_{p^{n+1}})\) for \(n \geq 0\).

We shall next describe \([\alpha, \beta]_\omega\). For this, let
\[
\lambda(X) = \log(1 + X) = X - \frac{X^2}{2} + \frac{X^3}{3} - \cdots.
\]

Then \(\lambda(X) \in \mathbb{Q}_p[[X]]\) and
\[
\lambda((1 + X)(1 + Y) - 1) = \log(1 + X)(1 + Y)
\]
\[
= \log(1 + X) + \log(1 + Y) = \lambda(X) + \lambda(Y).
\]
Hence $\lambda: F_f \cong G_a$ is the unique logarithm of $F_f$ with $\lambda(X) \equiv X \mod \deg 2$. Since

$$\lambda'(X) = \frac{1}{1 + X}, \quad \lambda'(\omega_n) = \zeta_n^{-1},$$

we have

$$\lambda(\alpha_n) = \log(1 + \alpha_n), \quad \delta(\beta_n) = \frac{\zeta_n}{\beta_n} t'_\beta(\omega_n),$$

$$x_n = \frac{1}{p^{n+1}} T_n \left( \frac{\zeta_n}{\beta_n} t'_\beta(\omega_n) \log(1 + \alpha_n) \right).$$

Therefore, for sufficiently large $n$,

$$[\alpha, \beta]_\omega = x_n; \quad \omega_n = [x_n]_f(\zeta_n - 1) = \zeta_n^{r_n - 1} = \kappa(\zeta_n^{r_n}). \quad (8.11)$$

Now, by Theorem 8.16, $(\alpha, \beta)_f = [\alpha, \beta]_\omega$ and (8.11) holds whenever $\alpha$ is represented by $\alpha_n \in A_n$. Hence it follows from (8.10) that if $\alpha_n$ is any element of $p_n = A_n$ and if $\beta_n$ is the $n$th component of an element $\beta$ in $B$, then

\[
\{\beta_n, 1 + \alpha_n\} = \zeta_n^{r_n}, \quad x_n = \frac{1}{p^{n+1}} T_n \left( \frac{\zeta_n}{\beta_n} t'_\beta(\omega_n) \log(1 + \alpha_n) \right)
\]

for the norm residue symbol $\{ , \}$ of $Q_p(W_{p^{n+1}})$ with exponent $p^{n+1}$. As a special case, let

$$\beta = (\zeta_0, \zeta_1, \ldots, \zeta_n, \ldots) \in B.$$

Then $t_\beta(X) = 1 + X$, $t'_\beta(X) = 1$ so that for any $\alpha_n \in p_n$,

$$\{\zeta_n, 1 + \alpha_n\} = \zeta_n^b, \quad \text{where } a = \frac{1}{p^{n+1}} T_n(\log(1 + \alpha_n)).$$

Next, let

$$\beta = \omega = (\zeta_0 - 1, \zeta_1 - 1, \ldots, \zeta_n - 1, \ldots) \in B.$$

Then $t_\beta(X) = X$, $t'_\beta(X) = 1$ so that for $\alpha_n \in p_n$,

$$\{\zeta_n - 1, 1 + \alpha_n\} = \zeta_n^b, \quad \text{where } b = \frac{1}{p^{n+1}} T_n \left( \frac{\zeta_n}{\zeta_n - 1} \log(1 + \alpha_n) \right).$$

Let us now quickly discuss the case: $p = 2$, $k = Q_2$, $\pi = p = 2$. In this case, let

$$f(X) = 1 - (1 - X)^2.$$

Then $f \in F_{\pi}^1$ and

$$F_f(X, Y) = 1 - (1 - X)(1 - Y), \quad [a]_f = 1 - (1 - X)^a, \quad \text{for } a \in \Omega,$$

$$W^f_n = \{1 - \xi \mid \xi \in W_{2^{n+1}}\}, \quad k^\pi_n = Q_p(W^f_n) = Q_p(W_{2^{n+1}}),$$

$W_{2^{n+1}}$ being the group of all $2^{n+1}$th roots of unity in $\Omega$. The unique logarithm
The local class field theory \( \lambda: F_r \to G_a \) with \( \lambda(X) \equiv X \mod \text{deg } 2 \) is given by

\[
\lambda(X) = -\log(1 - X) = X + \frac{X^2}{2} + \frac{X^3}{3} + \cdots.
\]

Let

\[
\zeta_0 = -1, \quad \zeta_{n+1}^2 = \zeta_n, \quad \omega_n = 1 - \zeta_n, \quad \text{for } n \geq 0.
\]

Then \( (f, \omega), \omega = \{\omega_n\}_{n \geq 0} \), is a normed \( \pi \)-sequence for \( k = \mathbb{Q}_2 \). Since \( \lambda'(X) = 1/(1 - X) \), \( \lambda'(\omega_n) = \zeta_n^{-1} \), we obtain, as for \( p > 2 \),

\[
x_n = \frac{1}{2^{n+1}} \frac{1}{\beta_n} T_n \left( -\frac{\zeta_n}{\beta_n}, t_\rho(\omega_n) \log(1 - \alpha_n) \right).
\]

On the other hand, in this case \( \pi^{n+1} \cdot \xi = \alpha_n \) means

\[
\xi = 1 - \sqrt[2^{n+1}]{1 - \alpha_n}.
\]

Hence, similarly as for \( p > 2 \), we have the formula:

\[
\{\beta_n, 1 - \alpha_n\} = \zeta_{x_n} \beta_n, \quad \text{for } \alpha_n \in \mathcal{P}_n, \quad \beta \in B,
\]

with \( x_n \) as above. Here \( \{,\} \), of course, denotes the norm residue symbol for \( \mathbb{Q}_p(W_{2n+1}) \) with exponent \( 2^{n+1} \). In particular, let

\[
\beta = (-\zeta_0, -\zeta_1, \ldots, -\zeta, \ldots) \in B.
\]

(Note that \( (\zeta_0, \zeta_1, \ldots, \zeta_n, \ldots) \notin B \) in this case.) Then

\[
\{-\zeta_n, 1 - \alpha_n\} = \zeta_n^a, \quad \text{where } a = \frac{1}{2^{n+1}} T_n(\log(1 - \alpha_n)),
\]

and for \( \beta = \omega \), we also obtain

\[
\{1 - \zeta_n, 1 - \alpha_n\} = \zeta_n^b, \quad \text{where } b = \frac{1}{2^{n+1}} T_n \left( \frac{\zeta_n}{\zeta_n - 1}, \log(1 - \alpha_n) \right).
\]

Those formulas for \( \{,\} \), for \( p > 2 \) and \( p = 2 \), are essentially the same as the classical explicit formulas of Artin–Hasse [2] for the norm residue symbols of \( \mathbb{Q}_p(W_{p^{n+1}}) \) with exponent \( p^{n+1} \). Thus Theorem 8.16 may be regarded as a generalization of those classical results for arbitrary local fields of characteristic 0. For the relation between Artin–Hasse formulas and Theorem 8.16, see also Iwasawa [12] and Kudo [15], and for applications of Theorem 8.16 and more recent results on explicit formulas, see Coates–Wiles [4] and de Shalit [6], [7].
Appendix

In this Appendix, we shall first briefly discuss Brauer groups of local fields which play a central role in the cohomological method in local class field theory, but which have not come up in the text in our formal-group theoretical approach. We shall then sketch, again briefly, the main ideas of Hazewinkel [11] for building up local class field theory.

A.1. Galois Cohomology Groups

In this section, we shall sketch some basic facts on Galois cohomology groups. For the most part, proofs are omitted. For details, we refer the reader to Cassels–Fröhlich [2], Chapters IV and V, or Serre [21], Chapter VII.

Let $G$ be a profinite group—that is, a totally disconnected compact group—and let $A$ be a discrete $G$-module. We assume that the action of $G$ on $A$ is continuous—namely, that the map $G \times A \to A$, defined by $(\sigma, a) \mapsto \sigma a$, is continuous. For $n \geq 0$, let $G^n$ denote the direct product of $n$ copies of $G$: $G^n = G \times \cdots \times G$, and let $C^n (= C^n(G, A))$ be the set of all continuous maps $f : G^n \to A$. For $n = 0$, this means that $G^0 = \{1\}$, $C^0 = A$. Note that the $C^n$, $n \geq 0$, are abelian groups in an obvious manner. For $f \in C^n$, we define an element $\delta^n f$ in $C^{n+1}$ by

$$(\delta^n f)(\sigma_1, \ldots, \sigma_{n+1}) = \sigma_1 f(\sigma_2, \ldots, \sigma_{n+1})$$

$$+ \sum_{i=1}^n (-1)^i f(\sigma_1, \ldots, \sigma_i \sigma_{i+1}, \ldots, \sigma_{n+1})$$

$$+ (-1)^{n+1} f(\sigma_1, \ldots, \sigma_n).$$

Then $f \mapsto \delta^n f$ defines a homomorphism

$$\delta^n : C^n \to C^{n+1}, \quad n \geq 0,$$

such that

$$\delta^n \circ \delta^{n-1} = 0, \quad \text{Im}(\delta^{n-1}) \subseteq \text{Ker}(\delta^n), \quad \text{for } n \geq 1.$$ Hence, let

$$H^n(G, A) = \text{Ker}(\delta^n)/\text{Im}(\delta^{n-1}), \quad \text{for } n \geq 0,$$

where we put $\text{Im}(\delta^{-1}) = 0$ if $n = 0$. The abelian groups $H^n(G, A)$, thus defined, are called the cohomology groups of the $G$-module $A$. For $n = 0, 1, 2$, $\delta^n$ is given as follows:

$$\delta^0(a)(\sigma) = \sigma a - a, \quad \text{for } a \in C^0 = A, \quad \sigma \in G,$$

$$\delta^1(f)(\sigma, \tau) = \sigma f(\tau) - f(\sigma \tau) + f(\sigma), \quad \text{for } f = f(\sigma) \in C^1, \quad \sigma, \tau \in G,$$

$$\delta^2(f)(\sigma, \tau, \rho) = \sigma f(\tau, \rho) - f(\sigma \tau, \rho) + f(\sigma, \tau \rho) - f(\sigma, \tau),$$

for $f = f(\sigma, \tau) \in C^2, \quad \sigma, \tau, \rho \in G.$
Thus, for example,

$$H^0(G, A) = A^G = \{ a \in A \mid \sigma a = a, \text{ for all } \sigma \in G \}. $$

Let $G'$ be another profinite group, acting continuously on a discrete modulo $A'$, and let

$$\gamma : G' \to G, \quad \alpha : A \to A'$$

be continuous homomorphisms such that

$$\alpha(\gamma'(\sigma') a) = \sigma'(\alpha(a)), \quad \text{for } \sigma' \in G', \ a \in A. \quad (A.1)$$

In such a case, we call the pair $\lambda = (\gamma, \alpha)$ a morphism from $(G, A)$ to $(G', A')$ and write

$$\lambda : (G, A) \to (G', A').$$

Let $f \in C^1(G, A)$—that is, a continuous map from $G$ into $A$. Then the product

$$f' : G' \to G' \to A'$$

belongs to $C^1(G', A')$, and $f \mapsto f'$ defines a homomorphism

$$C^1(G, A) \to C^1(G', A').$$

Similarly, $C^n(G, A) \to C^n(G', A')$ are defined for all $n \geq 0$, and because of $(A.1)$, they induce homomorphisms of cohomology groups:

$$H^n(G, A) \to H^n(G', A'), \quad \text{for } n \geq 0.$$

There are two important special cases of such homomorphisms. Let $H$ be a closed subgroup of $G$. Then $H$ is a profinite group and it acts continuously on $A$. Let $i : H \to G$ denote the natural injection and let $id : A \to A$ be the identity map. Then

$$(i, id) : (G, A) \to (H, A)$$

is a morphism in the sense defined above. The associated homomorphisms of cohomology groups:

$$\text{res} : H^n(G, A) \to H^n(H, A), \quad n \geq 0,$$

are called the restriction maps. Next, let $H$ be a closed normal subgroup of $G$ and let

$$A^H = \{ a \in A \mid \tau a = a \text{ for all } \tau \in H \}.$$ 

Then the factor group $G/H$ is again a profinite group and it acts continuously on $A^H$. Let $\gamma : G \to G/H$ be the canonical homomorphism and let $i : A^H \to A$ denote the natural injection. Then

$$(\gamma, i) : (G/H, A^H) \to (G, A)$$

is a morphism so that we obtain homomorphisms:

$$\text{inf} : H^n(G/H, A^H) \to H^n(G, A), \quad n \geq 0,$$
called the inflation maps. We shall now state two important results involving res and inf; for the proofs, see the references mentioned earlier.

**Proposition A.1.** Let \((G, A)\) be as above and let \(H\) be a closed normal subgroup of \(G\). Then the sequence

\[
0 \to H^1(G/H, A^H) \xrightarrow{\text{inf}} H^1(G, A) \xrightarrow{\text{res}} H^1(H, A)
\]

is exact. If \(H^1(H, A) = 0\), then

\[
0 \to H^2(G/H, A^H) \xrightarrow{\text{inf}} H^2(G, A) \xrightarrow{\text{res}} H^2(H, A)
\]

is also exact.

Next, let \(\{U\}\) denote the family of all open normal subgroups of \(G\). Let \(U' \subseteq U\) for two such subgroups \(U\) and \(U'\). Let \(\gamma: G/U' \to G/U\) be the canonical homomorphism, and \(\alpha: A^U \to A^{U'}\) the natural injection. Then \((\gamma, \alpha): (G/U, A^U) \to (G/U', A^{U'})\) is a morphism so that we have

\[
\inf_{U/U'}: H^n(G/U, A^U) \to H^n(G/U', A^{U'}), \quad n \geq 0.
\]

It is clear that if \(U'' \subseteq U' \subseteq U\), then \(\inf_{U/U''} = \inf_{U'/U''} \circ \inf_{U/U'}\). Hence

\[
\lim H^n(G/U, A^U)
\]

is defined with respect to the maps \(\inf_{U/U'}\) for all \(U\) and \(U'\) with \(U' \subseteq U\).

**Proposition A.2.** The inflation maps \(H^n(G/U, A^U) \to H^n(G, A)\) for open normal subgroups \(U\) of \(G\) induce an isomorphism

\[
\lim H^n(G/U, A^U) \simeq H^n(G, A), \quad n \geq 0.
\]

We also state below two elementary lemmas which are easy consequences of the definition of \(H^1(G, A)\) and \(H^2(G, A)\). Namely, let \(G\) now be a finite cyclic group of order \(n \geq 1\). Fix a generator \(\rho\) of \(G\): \(G = \langle \rho \rangle\), \(\rho^n = 1\), and let

\[
N(A) = (1 + \rho + \cdots + \rho^{n-1})A.
\]

Clearly, \(N(A) \subseteq A^G \subseteq A\). For each \(a \in A^G\), we define \(g(\sigma, \tau)\) in \(C^2\) by

\[
g(\rho^i, \rho^j) = 0, \quad \text{for } 0 \leq i, j < n, \quad i + j < n,
\]

\[
= a, \quad \text{for } 0 \leq i, j < n, \quad i + j \geq n.
\]

We check immediately that \(g\) belongs to \(\operatorname{Ker}(\delta^2)\). Hence, let \(c_a\) denote the residue class of \(g\) in \(H^2(G, A) = \operatorname{Ker}(\delta^2)/\operatorname{Im}(\delta^1)\). Then:

**Lemma A.3.** The map \(a \mapsto c_a\) induces an isomorphism

\[
A^G/N(A) \simeq H^2(G, A). \quad \text{(A.2)}
\]

Note that the isomorphism depends on the choice of the generator \(\rho\) of \(G\) and, hence, is not canonical. It is also easy to see that there is a similar
isomorphism

\[ A_N/(1 - \rho)A \cong H^1(G, A) \]

where \( A_N = \{ a \in A \mid (1 + \rho + \cdots + \rho^{n-1})a = 0 \} \).

Next, let \( H \) be a subgroup of the above \( G = \langle \rho \rangle \) and let

\[ [G:H] = m, \quad [H:1] = d, \quad n = md. \]

Then \( H = \langle \rho^m \rangle \) and \( G/H = \langle \tilde{\rho} \rangle \) with \( \tilde{\rho} = \rho H \). By Lemma A.3 for \((G/H, A^H)\), \( \tilde{\rho} \) defines an isomorphism

\[ (A^H)^{G/H}/N(A^H) \cong H^2(G/H, A^H), \]

where

\[ (A^H)^{G/H} = A^G, \]

\[ N(A^H) = (1 + \tilde{\rho} + \cdots + \tilde{\rho}^{m-1})A^H = (1 + \rho + \cdots + \rho^{m-1})A^H. \]

Since

\[ (1 + \rho^m + \cdots + \rho^{m(d-1)})A^H = dA^H, \]

\[ (1 + \rho + \cdots + \rho^{m-1})(1 + \rho^m + \cdots + \rho^{(d-1)m}) = 1 + \rho + \cdots + \rho^{m-1}, \]

we have

\[ dN(A^H) \subseteq N(A) \]

so that the endomorphism of \( A^G \), defined by \( a \mapsto da \) induces a homomorphism

\[ d : (A^H)^{G/H}/N(A^H) \to A^G/N(A). \]

**Lemma A.4.** The diagram

\[
\begin{array}{ccc}
(A^H)^{G/H}/N(A^H) & \xrightarrow{\sim} & H^2(G/H, A^H) \\
\downarrow d & & \downarrow \text{inf}
\end{array}
\]

\[ A^G/N(A) \xrightarrow{\sim} H^2(G, A) \]

is commutative.

Now, let \( K \) be a Galois extension of a field \( F \) and let \( G = \text{Gal}(K/F) \). Then \( G \) is a profinite group. Therefore, if \( G \) acts continuously on a discrete module \( A \), the cohomology groups \( H^n(G, A) \), \( n \geq 0 \), are defined. Such groups are called Galois cohomology groups. For example, \( G \) acts continuously on the multiplicative group \( K^\times \) of \( K \), viewed as a discrete group. Hence \( H^n(G, K^\times) \), \( n \geq 0 \), are defined. For simplicity, \( H^n(G, K^\times) \) will also be denoted by \( H^n(K/F) \):

\[ H^n(K/F) = H^n(\text{Gal}(K/F), K^\times), \quad n \geq 0. \]

Let \( \{ E \} \) be the family of all finite Galois extensions of \( F \), contained in \( K \):

\[ F \subset E \subset K, \quad [E:F] < +\infty. \]
Let $U = \text{Gal}(K/E)$ for such a field $E$. Then $U$ is an open normal subgroup of $G$ and

$$\text{Gal}(E/F) = G/U, \quad (K^\times)^U = E^\times.$$ 

Hence it follows from Proposition A.2 that

$$H^n(K/F) = \lim_{\to} H^n(E/F), \quad (A.3)$$

where the direct limit is taken with respect to the family $\{E\}$—namely, with respect to the family $\{U\}$, as stated in that proposition.

**Proposition A.5.** For any Galois extension $K/F$,

$$H^1(K/F) = 0.$$ 

*Proof.* It is one of the fundamental theorems in Galois theory that $H^1(E/F) = 0$ for any finite Galois extension $E/F$. Hence the proposition follows from (A.3). 

**Proposition A.6.** Let $K/F$ be a Galois extension and let $E$ be any Galois extension over $F$, contained in $K$: $F \subseteq E \subseteq K$. Then the sequence

$$0 \longrightarrow H^2(E/F) \longrightarrow H^2(K/F) \longrightarrow H^2(K/E)$$

is exact.

*Proof.* This follows immediately from Propositions A.1 and A.5.

As a consequence, we can imbed $H^2(E/F)$ in $H^2(K/F)$ by means of the inflation map:

$$H^2(E/F) \subseteq H^2(K/F).$$

(A.3) then shows that $H^2(K/F)$ is the union of the subgroups $H^2(E/F)$ when $E$ ranges over all finite Galois extensions over $F$, contained in $K$:

$$H^2(K/F) = \bigcup_{E} H^2(E/F). \quad (A.4)$$

Let $k$ be any field and let $\Omega_s$ denote the maximal Galois extension over $k$—that is, the maximal separable extension over $k$, contained in an algebraic closure of $k$. Let

$$\text{Br}(k) = H^2(\Omega_s/k).$$

Since $\Omega_s$ is unique for $k$ up to $k$-isomorphism, $\text{Br}(k)$ is indeed canonically associated with the given field $k$. It is called the Brauer group of $k$. In the next section, we shall discuss the structure of the Brauer group $\text{Br}(k)$ in the case where $k$ is a local field.

**A.2. The Brauer Group of a Local Field**

Let $(k, v)$ be a local field. We shall consider the Brauer group $\text{Br}(k) = H^2(\Omega_s/k)$. As in Section 3.2, let $K$ denote the maximal unramified extension
local class field theory

Let \( k_{ur} \) over \( k \) in a fixed algebraic closure \( \Omega \) of \( k \):

\[
K = k_{ur}.
\]

Since \( K/k \) is abelian, we have

\[
k \subseteq K \subseteq \Omega.
\]

Hence, by Proposition A.6, we obtain an exact sequence:

\[
0 \rightarrow H^2(K/k) \xrightarrow{\text{inf}} \text{Br}(k) \xrightarrow{\text{res}} \text{Br}(K).
\]  

We shall first study \( H^2(K/k) \).

By Sections 2.3 and 3.2, for each integer \( n \geq 1 \), there exists a unique unramified extension \( k_{ur}^n \) over \( k \) in \( \Omega \) with \( [k_{ur}^n : k] = n \) and

\[
K = k_{ur} = \bigcup_{n=1}^{\infty} k_{ur}^n.
\]

Clearly \( \{k_{ur}^n\}_{n=1}^{\infty} \) is the family of all finite Galois extensions over \( k \) in \( K \). Hence, by (A.3),

\[
H^2(K/k) = \lim_{\text{inf}} H^2(k_{ur}^n/k).
\]

Let \( \varphi \) be the Frobenius automorphism of \( k \): \( \varphi \in \text{Gal}(K/k) \). Then \( \text{Gal}(k_{ur}^n/k) \) is a cyclic group of order \( n \), generated by \( \varphi_n = \varphi | k_{ur}^n \), and by Lemma A.3, \( \varphi_n \) defines an isomorphism

\[
k^\times / N(k_{ur}^n/k) \cong H^2(k_{ur}^n/k).
\]  

Let \( \pi \) be a prime element of \( k \). Then

\[
N(k_{ur}^n/k) = U(k), \quad N(k_{ur}^n/k) = \langle \pi^n \rangle \times U(k)
\]

by Lemma 3.6. Hence the isomorphism

\[
\nu : k^\times / U(k) \cong \mathbb{Z},
\]

defined by the normalized valuation \( \nu \) of \( k \), induces

\[
k^\times / N(k_{ur}^n/k) \cong \mathbb{Z}/n\mathbb{Z}
\]

so that \((1/n)\nu\) defines an isomorphism

\[
k^\times / N(k_{ur}^n/k) \cong \frac{1}{n} \mathbb{Z}/\mathbb{Z}.
\]

The product of the inverse of (A.6) and the above isomorphism then yields

\[
H^2(k_{ur}^n/k) \cong \frac{1}{n} \mathbb{Z}/\mathbb{Z}.
\]  

Since this isomorphism is quite important, let us explicitly describe the map according to the above definition. For each \( x \in k^\times \), let \( c_x \) denote the residue class of \( g(\sigma, \tau) \) in \( H^2(k_{ur}^n/k) = \text{Ker}(\delta^2)/\text{Im}(\delta^1) \) (cf. Section A.1), where \( g \) is
defined by
\[ g(q^i_n, q^j_n) = 1, \quad \text{for } 0 \leq i, j < n, \quad i + j < n, \]
\[ = x, \quad \text{for } 0 \leq i, j < n, \quad i + j \geq n. \]

Then \( H^2(k_{ur}/k) \) consists of such \( c_x \) for all \( x \in k^\times \) and the isomorphism (A.7) is given by
\[ c_x \mapsto \frac{v(x)}{n} \mod \mathbb{Z}, \quad x \in k^\times. \]

It follows in particular that \( H^2(k_{ur}/k) \) is a cyclic group of order \( n \) generated by \( c_\pi \), \( \pi \) being any prime element of \( k \).

Now, let \( k \subseteq k_m \subseteq k_n, \quad n = dm. \) Since \( \varphi_m = \varphi_n \mid k_{ur}^m \), we see from Lemma A.4 that the following diagram is commutative:

\[
\begin{array}{ccc}
H^2(k_{ur}^m/k) & \xrightarrow{\sim} & k^\times/N(k_{ur}^m/k) \\
\downarrow \text{inf} & & \downarrow d \\
H^2(k_{ur}^n/k) & \xrightarrow{\sim} & k^\times/N(k_{ur}^n/k) \\
\end{array}
\]

Here the vertical map on the extreme right is the natural injection of \((1/m)\mathbb{Z}/\mathbb{Z}\) in \((1/n)\mathbb{Z}/\mathbb{Z}\). Therefore, denoting the additive group of the rational field \( \mathbb{Q} \) again by \( \mathbb{Q} \), we obtain
\[ H^2(K/k) = \lim_{\rightarrow} H^2(k_{ur}^n/k) \cong \lim_{\rightarrow} \mathbb{Z}/\mathbb{Z} = \mathbb{Q}/\mathbb{Z}. \]

Thus:

**Theorem A.7.** Let \( k_{ur} (= K) \) be the maximal unramified extension of a local field \( k \). Then the Forbenius automorphism \( \varphi \) of \( k \) defines a natural isomorphism
\[ H^2(k_{ur}/k) \cong \mathbb{Q}/\mathbb{Z}. \]

Next, we consider \( \text{Br}(K) = H^2(\Omega_s/K) \).

**Lemma A.8.** Let \( L \) be a finite Galois extension over \( K \). Then there exists a finite sequence of fields:
\[ K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_s = L, \]
such that
\[ (i) \quad \text{each } K_i \text{ is the maximal unramified extension of a local field } k_i; \]
\[ K_i = (k_i)_{ur}, \text{ and} \]
\[ (ii) \quad K_i/K_{i-1} \text{ is a cyclic extension for } i = 1, \ldots, s. \]

**Proof.** It is easy to see that there exists a field \( F \) such that \( FK = L \) and that \( F \) is a finite Galois extension over \( k' = k_{ur}^n \) for some large \( n \geq 0 \).
Replacing $k'$ by $F \cap K$ is necessary, we may assume that $F \cap K = k'$ so that $\text{Gal}(L/K) \cong \text{Gal}(F/k')$. By the Corollary of Proposition 2.19, there exists a sequence of fields:

$$k' = k_0 \subseteq k_1 \subseteq \cdots \subseteq k_s = F$$

such that each $k_i/k_{i-1}$, $1 \leq i \leq s$, is a cyclic extension. Then the fields $K_i = k_i K = (k_i)_{ur}$, $0 \leq i \leq s$, have properties (i) and (ii) stated in the lemma.

**Theorem 1.9.** $H^2(\Omega_s/K) = 0$.

**Proof.** By (A.3), it is sufficient to prove $H^2(L/K) = 0$ for any finite Galois extension $L/K$. By Proposition A.6 and Lemma A.8, the proof can be further reduced to the case where $L/K$ is a cyclic extension. As in the proof of Lemma A.8, let

$$FK = L, \quad F \cap K = k' = k_{ur}^n, \quad \text{Gal}(L/K) \cong \text{Gal}(F/k').$$

Let $m \geq n$ and let

$$d = [L : K] = [F : k'], \quad E = Fk_{ur}^m, \quad E' = Ek_{ur}^{m+d} = Fk_{ur}^{m+d}.$$ 

Then $K \cap E = k_{ur}^m$ so that both $E/k_{ur}^m$, $k_{ur}^{m+d}/k_{ur}^m$ are cyclic extensions of degree $d$. Hence for any $x \in (k_{ur}^m)^\times$, $x^d$ is the norm of $x$ for the extensions $E/k_{ur}^m$ and $k_{ur}^{m+d}/k_{ur}^m$. Therefore, $x \in N(E'/k_{ur}^{m+d})$ by Theorem 7.6. Since

$$E'K = FK = L, \quad E' \cap K = k_{ur}^{m+d},$$

we then see that $x \in N(L/K)$. Hence $(k_{ur}^m)^\times \subseteq N(L/K)$ for all $m \geq n$ and, consequently $N(L/K) = K^\times$. By Lemma A.3, we then have $H^2(L/K) = 0$.

By (A.5) and Theorems A.7 and A.9, we now obtain the following result:

**Theorem A.10.** Let $k_{ur}$ be the maximal unramified extension of a local field $k$. Then

$$\inf : H^2(k_{ur}/k) \cong H^2(\Omega_s/k) = \text{Br}(k).$$

Hence there exists a canonical isomorphism:

$$\text{Br}(k) \cong \mathbb{Q}/\mathbb{Z}.$$ 

The image of $c$ in $\text{Br}(k)$ under the above isomorphism is denoted by $\text{inv}(c)$.

Next, let $k'$ be any finite separable extension over $k$. Since

$$k \subseteq k' \subseteq \Omega_s,$$

the restriction map

$$\text{res} : \text{Br}(k) = H^2(\Omega_s/k) \to H^2(\Omega_s/k') = \text{Br}(k')$$

is defined.
THEOREM A.11. Let $d = [k' : k]$. Then the diagram

$$
\begin{array}{ccc}
\text{Br}(k) & \xrightarrow{\text{res}} & \mathbb{Q}/\mathbb{Z} \\
\downarrow & & \downarrow d \\
\text{Br}(k') & \xrightarrow{\text{res}} & \mathbb{Q}/\mathbb{Z}
\end{array}
$$

is commutative.

Proof. Let $e = e(k'/k)$, $f = f(k'/k)$. Let $\varphi$, $\varphi'$ be the Frobenius automorphisms of $k$ and $k'$, respectively, and let $v$, $v'$ denote the normalized valuations of $k$ and $k'$, respectively. Then, by Chapter II,

$$ef = d, \quad v'|k = ev, \quad \varphi'|K = \varphi'. $$

By (A.4) and Theorem A.10,

$$\text{Br}(k) = H^2(k_{nr}/k) = \bigcup_{n \geq 1} H^2(k_{nr}^n/k),$$

and similarly for $\text{Br}(k')$. Hence, if $c \in \text{Br}(k)$, then $c \in H^2(k_{nr}^n/k)$ for some integer $n \geq 1$ with $f \mid n$. By an earlier remark, $c = c_x$ for some $x \in k^\times$—namely, $c$ is represented by $g(\sigma, \tau)$ such that

$$g(\varphi_n^i, \varphi_n^j) = 1, \quad \text{for } 0 \leq i, j < n, \quad i + j < n,$$

$$= x, \quad \text{for } 0 \leq i, j < n, \quad i + j \geq n.$$

Let

$$n' = n/f, \quad \varphi_{n'}^i = \varphi'|k_{nr}^{n'}.$$

Since $\varphi'|K = \varphi'$, it follows from the definition of the restriction map that $\text{res}(c)$ in $H^2(k_{nr}^{n'}/k')$ is represented by $h(\sigma', \tau')$, where

$$h(\varphi_{n'}^i, \varphi_{n'}^j) = 1, \quad \text{for } 0 \leq i', j' < n', \quad i' + j' < n',$$

$$= x, \quad \text{for } 0 \leq i', j' < n', \quad i' + j' \geq n'.$$

But, then

$$\text{inv}(c) = \frac{v(x)}{n} \mod \mathbb{Z}, \quad \text{inv}(\text{res}(c)) = \frac{v'(x)}{n'} \mod \mathbb{Z},$$

where

$$\frac{v'(x)}{n'} = ef \frac{v(x)}{n} = d \frac{v(x)}{n}.$$

Hence $\text{inv}(\text{res}(c)) = d \text{inv}(c)$, and the theorem is proved.

In the above theorem, let $k'/k$ be in particular a finite Galois extension. By Proposition A.5,

$$H^2(k'/k) = \text{Ker}(\text{res}: \text{Br}(k) \rightarrow \text{Br}(k')).$$

Hence, it follows from the theorem that \( \text{inv} : \text{Br}(k) \cong \mathbb{Q}/\mathbb{Z} \) induces a natural isomorphism

\[
\text{inv} : H^2(k'/k) \cong \frac{1}{d} \mathbb{Z}/\mathbb{Z}, \quad d = [k' : k],
\]

which generalizes (A.7). The element \( c \) of \( H^2(k'/k) \) such that

\[
\text{inv}(c) = \frac{1}{d} \text{mod} \mathbb{Z}
\]
is called the fundamental class in \( H^2(k'/k) \). By means of Theorems A.10 and A.11 and the above result, we see that separable extensions of a local field provide us a so-called class formation. However, we shall not discuss this cohomological approach here any further. Compare Serre [21].

A.3. The Method of Hazewinkel

Let \((k, \nu)\) be a local field and let \( k' \) be a finite Galois extension of \( k \). Let

\[
K = k_{ur}, \quad L = k'_ur = k'K
\]

and let \( \bar{K} \) and \( \bar{L} \) be their completions (in \( \mathfrak{O} \)). Clearly \( L/K \) is a finite Galois extension and by Lemma 3.1,

\[
\bar{K}L = \bar{L}, \quad \bar{K} \cap L = K.
\]

Hence \( \bar{L}/\bar{K} \) is also a finite Galois extension and \( \sigma \mapsto \sigma \mid L \mapsto \sigma \mid k' \) defines

\[
\text{Gal}(\bar{L}/\bar{K}) \cong \text{Gal}(L/K) \cong \text{Gal}(k'/k_0),
\]

where \( k_0 = k' \cap K \) is the inertia field of the extension \( k'/k \). It then follows from the Corollary of Proposition 2.19 that \( \bar{L}/\bar{K} \) and \( L/K \) are solvable extensions.

**Proposition A.12.** Let \( N(\bar{L}/\bar{K}) \) denote the norm group of the finite extension \( \bar{L}/\bar{K} \). Then

\[
N(\bar{L}/\bar{K}) = \bar{K}.
\]

**Proof.** Since \( \bar{L}/\bar{K} \) is solvable, it is sufficient to prove the proposition for the case where \( \bar{L}/\bar{K} \) is a cyclic extension of prime degree. For the proof of this, see Serre [21], Chap. V, §3, where norm maps for finite extensions of complete fields (cf. Section 1.2) are discussed in detail. A slightly different proof can be found in Iwasawa [13]. ■

Now, let

\[
V(\bar{L}/\bar{K}) = \text{the subgroup of } U(\bar{K}), \text{ generated by all elements of the form }
\]

\[
\xi^{\sigma^{-1}} = \sigma(\xi)/\xi \text{ for } \sigma \in \text{Gal}(\bar{L}/\bar{K}) \text{ and } \xi \in U(\bar{L}).
\]

By Lemma 3.2, \( \mu_k (= \mu \mid K) \) and, hence, \( \mu_{\bar{K}} (= \bar{\mu} \mid \bar{K}) \) are normalized valuations. Therefore \((\bar{K}, \mu_{\bar{K}})\) is a complete field in the sense of Section 1.2.
and it follows from Section 1.3 that $\bar{L}$ is also a complete field with respect to a normalized valuation, equivalent to $\mu_\bar{L} (= \bar{\mu} | \bar{L})$. Let $\pi'$ be any prime element of $\bar{L}$. For any $\sigma$ in $\text{Gal}(\bar{L}/\bar{K})$, $\pi'^{\sigma-1} (= \sigma(\pi')/\pi')$ then belongs to $U(\bar{L})$ so that a map

$$\text{Gal}(\bar{L}/\bar{K}) \to U(\bar{L})/V(\bar{L}/\bar{K}),$$

$$\sigma \mapsto \pi'^{\sigma-1} \mod V(\bar{L}/\bar{K})$$

is defined. It is easy to check (cf. the proof of Proposition 2.13) that the above map is a homomorphism, independent of the choice of the prime element $\pi'$. Since $U(\bar{L})/V(\bar{L}/\bar{K})$ is an abelian group, it then induces a homomorphism

$$i : \text{Gal}(\bar{L}/\bar{K})^{ab} \to U(\bar{L})/V(\bar{L}/\bar{K})$$

where $\text{Gal}(\bar{L}/\bar{K})^{ab}$ denotes the factor commutator group of $\text{Gal}(\bar{L}/\bar{K})$. Let $N (= N_{\bar{L}/\bar{K}})$ denote the norm map of the finite extension $\bar{L}/\bar{K}$. Then we have the following

**Proposition A.13.** *The sequence*

$$1 \to \text{Gal}(\bar{L}/\bar{K})^{ab} \to U(\bar{L})/V(\bar{L}/\bar{K}) \to U(\bar{K}) \to 1$$

*is exact.*

**Proof.** See Hazewinkel [11]. He proved this by elementary arguments, without using cohomology groups. However, if one is allowed to make use of the cohomology groups of Tate for the finite group $\text{Gal}(\bar{L}/\bar{K})$, it can also be derived from the long exact sequence of such cohomology groups, associated with the exact sequence

$$1 \to U(\bar{L}) \to \bar{L}^* \to \mathbb{Z} \to 1,$$

defined by the normalized valuation of $\bar{L}$. Compare Serre [22]. In any case, the essential source of the proof is Proposition A.12 above.

We now assume that $k'/k$ is a finite abelian extension. Then the extensions $L/k$, $L/K$, and $\bar{L}/\bar{K}$ are also abelian. Hence, identifying $\text{Gal}(\bar{L}/\bar{K})$ with $\text{Gal}(L/K)$, we obtain from Proposition A.13 an exact sequence as follows:

$$1 \to \text{Gal}(L/K) \to U(\bar{L})/V(\bar{L}/\bar{K}) \to U(\bar{K}) \to 1. \quad (A.8)$$

Let $\phi$, $\psi$, and $\phi_0$ denote the Frobenius automorphisms over $k$, $k'$ and $k_0 = k' \cap K$, respectively. Extend these to automorphisms of $L$ and, then, to automorphisms of $\bar{L}$, and denote them again by the same letters $\phi$, $\psi$, and $\phi_0$. Then $\phi$, $\psi$, and $\phi_0$ commute with every $\sigma$ in $\text{Gal}(\bar{L}/\bar{K}) = \text{Gal}(L/K)$. In particular,

$$(\xi^{\sigma-1})^{\psi^{-1}} = (\xi^{\psi^{-1}})^{\sigma-1}, \quad \text{for } \sigma \in \text{Gal}(\bar{L}/\bar{K}), \quad \xi \in U(\bar{L}).$$

Hence

$$V(\bar{L}/\bar{K})^{\psi^{-1}} \subseteq V(\bar{L}/\bar{K})$$
so that the homomorphism $\psi - 1: U(\bar{L}) \rightarrow U(\bar{L})$ induces an endomorphism

$$\alpha = \psi - 1: U(\bar{L})/V(\bar{L}/\bar{K}) \rightarrow U(\bar{L})/V(\bar{L}/\bar{K}).$$

Let

$$\beta = \varphi_0 - 1: U(\bar{K}) \rightarrow U(\bar{K})$$

and let

$$\gamma: \text{Gal}(L/K) \rightarrow \text{Gal}(L/K)$$

be the trivial endomorphism of $\text{Gal}(L/K)$, mapping every element of $\text{Gal}(L/K)$ to the identity element. With these maps $\alpha$, $\beta$, and $\gamma$, consider the diagram

$$
\begin{array}{c}
1 \rightarrow \text{Gal}(L/K) \xrightarrow{i} U(\bar{L})/V(\bar{L}/\bar{K}) \xrightarrow{N} U(\bar{K}) \rightarrow 1 \\
\downarrow \gamma \quad \downarrow \alpha \quad \downarrow \beta \\
1 \rightarrow \text{Gal}(L/K) \xrightarrow{i} U(\bar{L})/V(\bar{L}/\bar{K}) \xrightarrow{N} U(\bar{K}) \rightarrow 1,
\end{array}
$$

where the rows are the exact sequence (A.8). Let

$$A = \text{Ker}(\alpha), \quad B = \text{Ker}(\beta), \quad C = \text{Coker}(\gamma), \quad D = \text{Coker}(\alpha).$$

Then we see (cf. Lemma 3.11) that the above diagram is commutative and

$$A = U(k')V(\bar{L}/\bar{K}), \quad B = U(k_0), \quad C = \text{Gal}(L/K), \quad D = 1.$$ 

Hence the maps $N$ and $i$ induce homomorphisms $A \rightarrow B$ and $C \rightarrow D$ respectively, and by the Snake Lemma, there exists a homomorphism

$$\delta: B \rightarrow C$$

such that

$$A \xrightarrow{N} B \xrightarrow{\delta} C \xrightarrow{i} D$$

is exact. Since

$$\text{Ker}(\delta) = \text{Im}(N) = N(U(k')V(\bar{L}/\bar{K})) = N_{k'/k_0}(U(k')) = NU(k'/k_0),$$

$\delta$ induces an isomorphism

$$U(k_0)/NU(k'/k_0) \cong \text{Gal}(L/K). \quad (A.9)$$

Checking the definition of the isomorphism, we find that if $u \mod NU(k'/k_0) \rightarrow \sigma$ for $u \in U(k_0)$, then

$$u^{\varphi^{-1}} \mod NU(k'/k_0) \rightarrow \varphi \sigma \varphi^{-1} \sigma^{-1} = 1.$$ 

Hence,

$$U(k_0)^{\varphi^{-1}} \subseteq NU(k'/k_0).$$

However, as $k_0/k$ is an unramified extension, one can see (cf. Lemma 3.6)
that the norm map $N_{k'/k}: U(k_0) \to U(k)$ is surjective and its kernel is $U(k_0)^{\sigma-1}$. Therefore, it induces

$$U(k_0)/NU(k'/k_0) \cong U(k)/NU(k'/k).$$

Thus we obtain from (A.9) a fundamental isomorphism

$$U(k)/NU(k'/k) \cong \text{Gal}(L/K) = \text{Gal}(k'/k_0), \quad (A.10)$$

where $k'/k$ is any finite abelian extension of local fields and $k_0$ is the inertia field of $k'/k$.

Let $e = e(k'/k)$, $f = f(k'/k)$ for the above $k'/k$. Then (A.10) and Proposition 2.12 yield

$$[U(k):NU(k'/k)] = [k':k_0] = e.$$

Since $ef = [k':k]$, $v(N(k'/k)) = f\mathbb{Z}$ by Proposition 1.5, it follows that

$$[k:N(k'/k)] = [k:N(k'/k)U(k)][N(k'/k)U(k):N(k'/k)]$$

$$= [\mathbb{Z}:f\mathbb{Z}][U(k):NU(k'/k)] = f \cdot e$$

$$= [k':k].$$

This is the proof of the fundamental equality (Corollary of Theorem 7.1) in Hazewinkel [11]. Starting from (A.10), we can also define the norm residue map $\rho_k : k^\times \to \text{Gal}(k_{ab}/k)$ by this method. For the details, we refer the reader to Iwasawa [13].
Bibliography

Table of Notations

### General Notations

- **Z**: the ring of rational integers,
- **Q**: the field of rational numbers,
- **R**: the field of real numbers,
- **C**: the field of complex numbers,
- **F_q**: a finite field with \( q \) elements,
- **R**: a commutative ring with identity \( 1 \neq 0 \),
- **R^+**: the additive group of \( R \), often denoted also by \( R \),
- **R^x**: the multiplicative group of all invertible elements in \( R \).

### Chapter I

1.1. \( \nu, \nu_0, \nu_p, \varnothing, \nu, \tilde{\nu} (= \varnothing/\nu), U, e(\nu'/\nu) (= e), f(\nu'/\nu) (= f) \)
1.2. \( (k, \nu), (Q_p, \nu_p), (F((T)), \nu_T), \omega(x), V \)
1.3. \( e(k'/k), f(k'/k), N_{k'/k}(\alpha') \)

### Chapter II

2.1. \( (k, \nu), q, (Q_p, \nu_p), (F((T)), \nu_T), \omega(x), V \)
2.2. \( W \)
2.3. \( \varphi, k_0 \)
2.4. \( \mathcal{D}, \mathcal{D}(k'/k), D(k'/k), \omega[w] \)
2.5. \( G_n \)

### Chapter III

3.1. \( \Omega, \mu, \tilde{\Omega}, \tilde{\mu}, (F, \mu_F), (\tilde{F}, \mu_F), \tilde{\nu}_F = \varnothing_F/p_F, \tilde{\nu}_F = \varnothing_F/p_F \)
3.2. \( k_\text{ur}^n, k_\text{ur}, K, \varnothing^n, \tilde{\nu}_K = \varnothing_K/p_K, \varnothing_k, \varnothing_n, \hat{L}, V_n, V_\infty \)
3.3. \( U(F), N(F/k), NU(F/k) \)
3.4. \( R[[X_1, \ldots, X_n]], \mod \deg d, f \circ (g_1, \ldots, g_n), M, f \circ g, f^{-1}, \tilde{\nu}_\Omega = \varnothing_\Omega/p_\Omega, f^\varnothing \)
3.5. \( \varphi (= \varnothing_k, \tilde{\varnothing}_k), \tilde{\nu}_k = \varnothing_k/p_K, f^\varnothing \)

### Chapter IV

4.1. \( F(X, Y), i_F(X), M_F, F^i(= f \circ F \circ f^{-1}), \text{Hom}(F, G), \text{End}(F), G_a(X, Y), \lambda(X) \)
4.2. \( R (= \varnothing_K), \mathcal{F}_x, \mathcal{F}, F_f(X, Y), [a]_f, \theta(X) \)
4.3. \( m (= \varnothing_\Omega), \alpha \neq \beta, a; \alpha, m_f, W_f^n, W_f, f_n, g_n, h_n, \text{End}(W_f^n), \text{Aut}(W_f^n) \)
4.4. \( \tilde{L}^n, \delta^n, \tilde{L}_f, \delta_f \)
Chapter V

5.1. $\sigma^m, \mathcal{F}_\pi^m, \mathcal{F}^m, \mathcal{F}_\pi^\infty, k_{\pi}^{m,n}, L^n, \sigma^{m,n}, \delta^n, \delta_n^{\pi}$

5.2. $k_{\pi}^m, S, S^\infty, \mathfrak{f}_n = \mathfrak{o}_n/p_n, X + \alpha, N(h) (= N_f(h)), N^n$

5.3. $k_{\pi}^{m,\infty}, L, \delta, \delta^n, \delta_\pi, k_\pi (= k_{\pi}^{1,\infty})$

Chapter VI

6.1. $k_{ab}, L_k, \psi_\pi, \psi, \rho_k$

6.3. $\rho_k, \Omega_s, t_{G/H}, t_{k''/k}, (k''/k)$

Chapter VII

7.1. $\rho_{k''/k}$

7.2. $G_r, g_r, \phi(r), i_G(\sigma) (= i(\sigma)), \psi(r), G'$

7.4. $c(k''/k), \mathfrak{f}(k''/k), H_\chi, k_\chi, \mathfrak{f}(\chi)$

Chapter VIII

8.1. $(f, \omega), N_{m,n}, B_n, B, N_n, \nu(\beta)$

8.2. $\rho_n, (\alpha, \beta)_{n,f}, A_n, A_f, (\alpha, \beta)_f$

8.3. $\lambda_0, \lambda, \delta(\beta)_n, T_{m,n}, x_\pi(\alpha_n, \beta), [\alpha, \beta]_w$

8.4. $T_n, N_n$

8.5. $\kappa, \{x, y\}$

Appendix

A.1. $C^n (= C^n(G, A)), \delta^n, H^n(G, A), \lambda = (\alpha, \gamma)$, res, inf, $H^n(K/F), \Omega_s, Br(k)$

A.2. $\text{inv}(c)$

A.3. $V(L/K)$
Index

additive (formal) group, 52
Artin map, 88
Brauer group, 141
cohomology group, 137
complete field, 7
complete valuation, 5
completion (of a valuation), 7
conductor, 112
conductor-discriminant theorem, 114
different, 29
discrete valuation, 5
discriminant, 29
equivalent valuations, 4
existence theorem, 101
extension of a complete field, 12
extension of a valuation, 5
finite extension of a local field, 26
formal group, 50
Frobenius automorphism, 28, 38
fundamental class, 146
fundamental equality, 98
Galois cohomology group, 140
Hasse-Arf (Theorem of), 111
ideal of \((k, v)\), 9
inertia field, 29
inf (= inflation map), 139
isomorphism of formal groups, 51
local field, 18
logarithm, 123
maximal ideal of a valuation, 4
maximal unramified extension, 37
morphism of formal groups, 51
\(\nu\)-topology, 4
norm group, 41
norm of an ideal, 16
norm operator, 72
norm residue map, 88
norm residue symbol, 134
normalized (normal) valuation, 5
normed (power series) \(f\), 118
normed \(\pi\)-sequence, 117
\(\pi\)-sequence, 116
\(p\)-adic number field, 8
\(p\)-adic valuation, 3
\(p\)-field, 18
prime element, 8
ramification groups in the lower numbering, 33
ramification groups in the upper numbering, 104
ramification index \(e(v'/v)\), 6
ramification index \(e(k'/k)\), 12
res (= restriction map), 138
residue degree \(f(v'/v)\), 6
residue degree \(f(k'/k)\), 12
residue field of a valuation, 4
restriction of a valuation, 5
totally ramified extension, 26, 39
transfer map, 93
trivial valuation, 3
uniqueness theorem, 101
unit group, 4
unit norm group, 41
unramified extension, 26, 36
valuation, 3
valuation ring, 4